Avaya Flare™ Experience

Avaya Ethernet Routing Switches

Engineering

> Avaya Flare™ for Avaya Data Technical Configuration Guide

Avaya Data Solutions

Document Date: March 2011

Document Number: NN48500-613

Document Version: 1.0

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http:// www.avaya.com/support.

Abstract

This Technical Solution Guide defines the recommended best practices for configuring Avaya Ethernet Routing Switches to support the Avaya Flare™ Experience. This guide is specifically focused on best practices and recommendations for Avaya data products at the core, distribution, access and data center layers of the network and complements the general best practice recommendations outlined in the Small, Medium, Large and Super Large Technical Solution Guides.

This Technical Solution Guide is intended for Avaya Sales teams, Partner Sales teams and end-user customers who are deploying the Avaya Flare™ Experience on Avaya data products. All of these groups can benefit from understanding the best practices and recommendations outlined in this guide.

Acronym Key

Throughout this guide the following acronyms will be used:

- ADAC – Automatic Detect Automatic Config
- ADVD – Avaya Desktop Video Device
- ASCs – Avaya Service Classes
- B-MAC – Backbone MAC
- BEB – Backbone Edge Bridge
- DHCP – Dynamic Host Configuration Protocol
- D-MLT – Distributed Multilink Trunk
- DSCP – Differentiated Services Code Point
- GRT – Global Route Table
- I-SID – Backbone Service Instance Identifier
- IGP – Interior Gateway Protocol
- IP – Internet Protocol
- IS-IS – Intermediate System To Intermediate System
- IST – Inter Switch Trunk
- LAG – Link Aggregation Group
- LLDP – Link Layer Discovery Protocol
- MAC – Media Access Control
- MLT – Multilink Trunk
- PBB – Provider Backbone Bridge
- QoS – Quality of Service
- RSMLT – Routed Split Multilink Trunk
- SMLT – Split Multilink Trunk
- SPB – Shortest Path Bridging
- SPBM – Shortest Path Bridging MAC
- VLAN – Virtual LAN
- VRF – Virtual Routing and Forwarding
- VRRP – Virtual Router Redundancy Protocol
- VSN – Virtual Services Network

Revision Control

No	Date	Version	Revised By	Remarks
1	March 2011	1.0	K. Marshall	Initial Draft

Table of Contents

Figures

Tables

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols

Tip – Highlights a configuration or technical tip.

Note – Highlights important information to the reader.

Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

```
ERS5520-48T# show running-config
```

Output examples from Avaya devices are displayed in a Lucida Console font:

```
ERS5520-48T# show sys-info

Operation Mode:          Switch
MAC Address:             00-12-83-93-B0-00
PoE Module FW:           6370.4
Reset Count:             83
Last Reset Type:         Management Factory Reset
Power Status:            Primary Power
Autotopology:            Enabled
Pluggable Port 45:       None
Pluggable Port 46:       None
Pluggable Port 47:       None
Pluggable Port 48:       None
Base Unit Selection:     Non-base unit using rear-panel switch
sysDescr:                Ethernet Routing Switch 5520-48T-PWR
                         HW:02       FW:6.0.0.10  SW:v6.2.0.009
                         Mfg Date:12042004    HW Dev:H/W rev.02
```

1. Introduction

Avaya's data architecture includes four standard designs for small, medium, large and super large campus environments and involves strategic products, innovative features, and best practices for each campus size. Although the definition of small, medium, large and very large vary between customers and geographic region, the overall concept of the designs and required feature sets are consistent providing a highly scalable, always-on communications platform capable of supporting real-time communication systems such as Avaya Aura and the Avaya Flare experience.

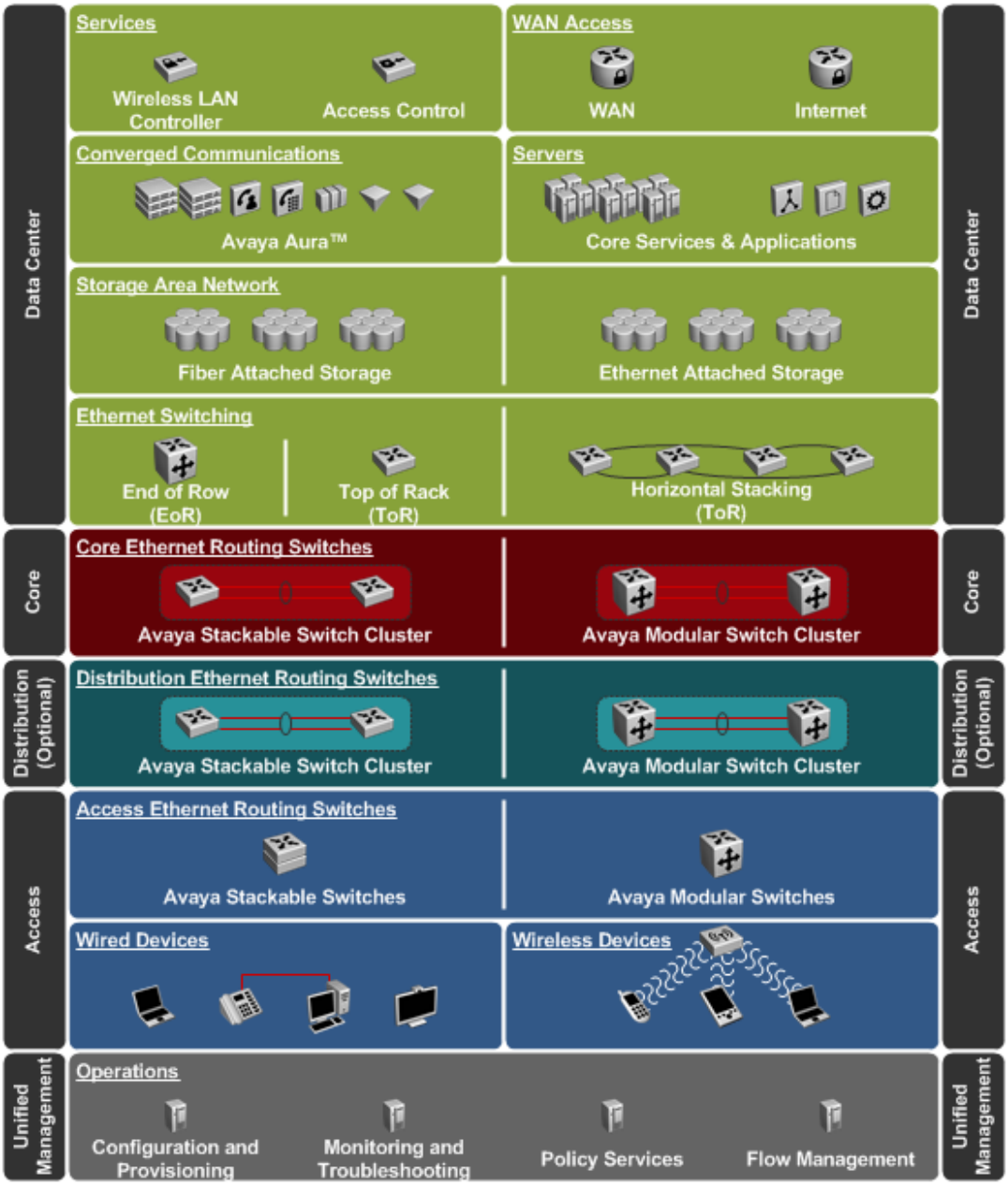


Figure 1 – Avaya Converged Campus Architecture

2. Solution Components

The solution components outlined in this guide focus solely on the campus network and include Avaya Aura Servers, Avaya Media Gateways, Avaya Desktop Video Devices and Avaya Ethernet switching platforms. The following section provides a high level overview of the individual solution components which provide the Avaya Flare experience along with the individual Avaya Ethernet Switching platforms that can be selected and deployed in the core, optional distribution, access and data center layers for each campus size.

2.1.1 Avaya Aura

The Avaya Flare experience is groundbreaking software that offers a uniquely compelling multi-modal collaboration experience. Delivered on the Avaya Desktop Video Device, the Avaya Flare Experience offers quick and easy access to real-time communications and collaboration tools. Capabilities include desktop video, social media, audio/video/web conferencing, multiple directories, presence, instant messaging, and contextual history. It eliminates the need to use different interfaces and different directories to communicate across various types of tools.

The Avaya Desktop Video Device is a fit-for-purpose collaboration tool with high definition video and high quality audio combined with an interactive touch screen interface. The Avaya Flare Experience and Desktop Video Device together enhance user productivity and enable easy collaboration.

The Avaya Flare Experience leverages the SIP based Avaya Aura communications platform to deliver improved real-time, multi-session and multi-modal communications to the desktop. Users communicate and collaborate without regard to type of network or how to access that network. The Avaya Flare Experience utilizes the Avaya Aura advanced unified communication features and services, application enablement and management capabilities. Avaya Aura delivers real time communications services, providing a single infrastructure, administration and management tool. Social network interfaces such as Facebook are implemented locally and are independent of Avaya Aura applications. Point-to-point video calls do not require a video conferencing server though multi-party conferencing is enabled by Avaya Aura Conferencing.

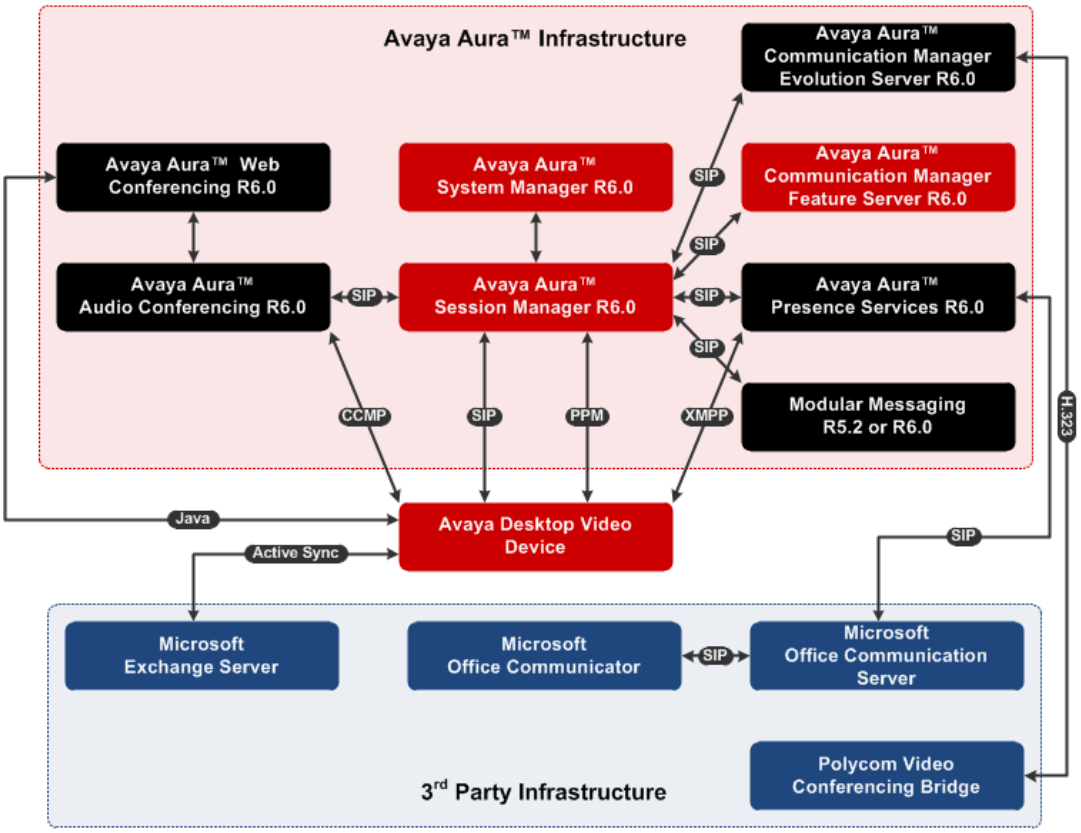


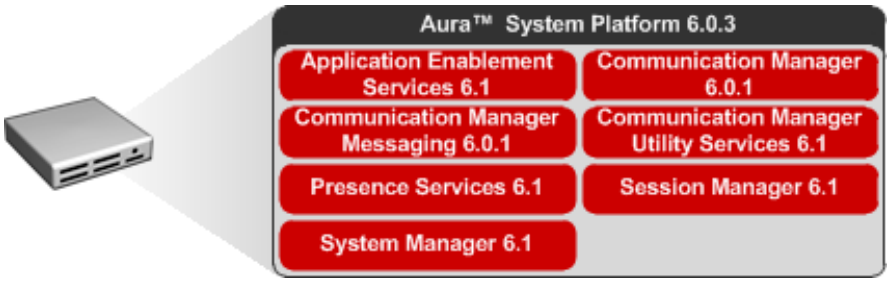
Figure 2.1.1 – Avaya Flare Architecture

The Avaya Flare Experience can be enabled in existing Avaya Aura 6.0 deployments as well as legacy Avaya, Nortel and third-party communication systems. For large deployments Avaya Aura services can be deployed on individual Avaya servers providing a highly scalable and available converged communications platform. For greenfield, legacy or trial environments Avaya offers the Avaya Aura Solution for Midsize Enterprises which packages all the necessary Avaya Aura services and applications in a easy to deploy single server solution. The Avaya Aura Conferencing Standard Edition Server adds multi-party video conferencing and web-conferencing capabilities.

In March 2011 the Avaya Aura Collaboration Server has been replaced with the Avaya Aura Solution for Midsize Enterprises.

2.1.2 Avaya Aura Solution for Midsize Enterprises

The Avaya Aura Solution for Midsize Enterprises provides all required Avaya Aura services and applications in a single easy to deploy server solution that can support up to 1,000 SIP endpoints. The Avaya Aura Solution for Midsize Enterprises offers basic voice conferencing for up to 6 participants and point-to-point video conferencing. Advanced voice conferencing and multi-party video conferencing is enabled by deploying an additional Avaya Aura Conferencing Standard Edition Server.



Avaya Aura Solution for Midsize Enterprises Highlights

Supported SIP Endpoints

- Avaya Video Conference Solution components, Avaya Desktop Video Device (powered by the Avaya Flare Experience), and SIP enabled phones (96x1 series)

Virtualization

- Avaya Aura System Platform 6.0.3

Utility Services

- Communication Manager Utility Services 6.1

Voice & Video Platform

- Communication Manager and Communication Manager Messaging 6.0.1

Session Management

- Avaya Aura Session Manager 6.1

Management

- Avaya Aura System Manager 6.1

Presence

- Avaya Aura Presence Services 6.1

Application Integration

- Avaya Aura Application Enablement Services 6.1

Maximum SIP Endpoints

- 250 – 1,000

Remote Access and Alarming

- SAL and VPN

Server Hardware

- Avaya Aura Midsize Enterprise leverages Avaya Aura System Platform virtualization and Avaya sourced servers

Figure 2.1.2 – Avaya Aura Solution for Midsize Enterprises

2.1.3 Avaya Aura Conferencing 6.0 Standard Edition

Avaya Aura Conferencing enables real-time conferencing and collaboration anytime, anywhere, and offers scalable conferencing configurations for businesses of every size. Avaya Aura Conferencing is easily deployed on premise for audio only, or as an integrated combination of audio, video, and web conferencing. Integration to Unified Communications applications from Avaya and third parties lets users leverage familiar desktop applications and interfaces for increased conference control.

Conferencing Standard Edition is an on premises suite of multimedia conferencing applications that provides easy to use audio, video and web conferencing tools that allow for high touch communications between employees, partners and customers. Simplifying how virtual teams connect, Conferencing Standard Edition offers audio conferencing and fully integrated web conferencing with video capabilities for both moderators and participants. This robust capacity allows enterprise wide usage and typically addresses the needs of companies with up to 5,000 employees or more.

Conferencing Standard Edition allows for essentially unlimited growth of capacity and conferencing capabilities with a direct upgrade path to Avaya Aura Conferencing Enterprise Edition. Sharing a common software base with Conferencing Enterprise Edition businesses can reuse the same hardware and simply uplift the licenses as their needs evolve to roll out conferencing services to progressively larger user communities or expand from simple to more sophisticated conferencing solution sets.

Avaya Aura Conferencing 6.0 Standard Edition Highlights

Convenient Reservationless or Scheduled Conferencing

- With unlimited conferencing configurations of up to 500 concurrent users. Organize yourself or workgroups with an easy to use web-based scheduling tool

Recording and playback

- With simple to use DTMF or GUI audio controls

In-bound and outbound dialing

- Have the bridge call you through a reservation in your Microsoft outlook calendar. Need another resource on the call? Pull them in to get the answers you need.

Touchtone (DTMF) commands

- Provides professional conferences with easy access to quality and management controls such as mute (for noisy bridges), lock conference (for security), participant count, music on hold

Reporting

- System and user level reporting to understand utilization and allow for billing

Localization for all major markets

- Including English, Simplified Chinese, Japanese, Korean, and German

Disaster Response

- Providing emergency notification, disaster response, all at no incremental cost to the business using the 'Blast Dial' capability

Easy Access

- As a 24x7 on net globally accessible resource

Scaling

- 500 audio conferencing ports
- 500 web conferencing ports

Figure 2.1.3 – Avaya Aura Conferencing 6.0 Standard Edition

2.1.4 Avaya Desktop Video Device

The Avaya Desktop Video Device is a cost-effective video desktop collaboration endpoint. In addition to HD video, device features include telephone, web conferencing, social media, calendar, and scheduling from a single user interface on a multi-touch device. The Desktop Video Device with the Avaya Flare Experience can be used to consolidate tools such as a desk phone, speaker phone and video endpoint. It enables ad hoc, person-to-person collaboration for enterprise workers. Used as a customer service kiosk, the device allows customers to get information and click to communicate with contact center experts.

Avaya Desktop Video Device Highlights

Audio

- Dual Microphones
- Stereo Speakers

Authentication (Wireless)

- 802.1X (MD5, PEAP, TLS, TTLS, PSK)

Battery

- Removable Lithium Polymer (3 Hours Minimum)

Base Station

- The Avaya Desktop Video Device is mobile and can be docked to a base station that has its own set of network connections, USB slots, sub-woofer speaker, etc.

Bluetooth 2.0/2.1

- The Avaya Desktop Video Device supports speakerphones, headsets, and smart phone integration for synchronization of contacts list.

Handset and Cradle

- The handset and cradle support private conversations with wideband audio (7KHz) and a TDD acoustic coupler w/o an adaptor.

High Definition LCD Screen

- 11.6” (1366 x 768 resolution)
- Multi-touch

Networking

- 10/100BASE-T Ethernet
- 802.11b/g/n

QoS

- IEEE 802.1p
- DiffServ Code Point

USB Support

- Keyboard, mouse, external speakers, cellular modem, external storage, charger for cell phones, etc. can be attached easily to either the display or the base station.

Video

- 5MP Camera

Figure 2.1.4 – Avaya Desktop Video Device

2.2 Avaya Ethernet Switching

Avaya offers various stackable and modular switching platforms which can be deployed in small, medium, large or super large campus environments to support the Avaya Flare experience. The Avaya Virtual Services and Ethernet Routing Switch portfolios provide an industry leading always-on, efficient and highly scalable Ethernet infrastructure that is ideally suited to support next generation applications and real-time collaboration tools such as the Avaya Flare experience.

Avaya Virtual Services Platform and Ethernet Routing Switches provide ultimate flexibility and choice when deploying small or large highly scalable networks by offering highly available network architectures leveraging Avaya's innovative features such as Split Multilink Trunking (SMLT), Routed Split Multilink Trunking (RSMLT) and more recently IEEE 802.1aq Shortest Path Bridging MAC (SPBM). These innovations allow enterprises to architect two-tier or optionally three-tier networks to suite the specific application and topology requirements. In contrast other vendors require complex spanning-tree protocols or end-to-end routing to provide the same level of availability offered by Avaya Ethernet switching platforms which are hard to manage or impose topology limitations on the network, thus reducing flexibility.

Avaya offers a full suite of stackable and modular switches which can be deployed in the core, optional distribution, access and data center layers for small, medium, large and super large campus environments. Each platform is designed for a specific size of network and includes the necessary features required to build an always-on, efficient and highly scalable Ethernet network.

The choice of which Avaya switch to deploy at the core, distribution, access and data center layers will vary depending on the customer's specific requirements. Common requirements include the physical environment where the Avaya Ethernet switches are to be deployed, the applications the customer is supporting and any special devices such as IP phones, video end-points, access points, storage and virtualized servers which are be connected to the network. The customer may also have a preference between chassis or stackable form-factors and may have budget constraints which will additionally influence the decision.

To aide in the decision process as to which Avaya Ethernet switch to deploy, Avaya has published reference architectures for small, medium, large and super large campus deployments as well as various reference architectures for the data center. A brief overview of the small, medium, large and super large campus architectures is provided in Section 3.0 of this guide.

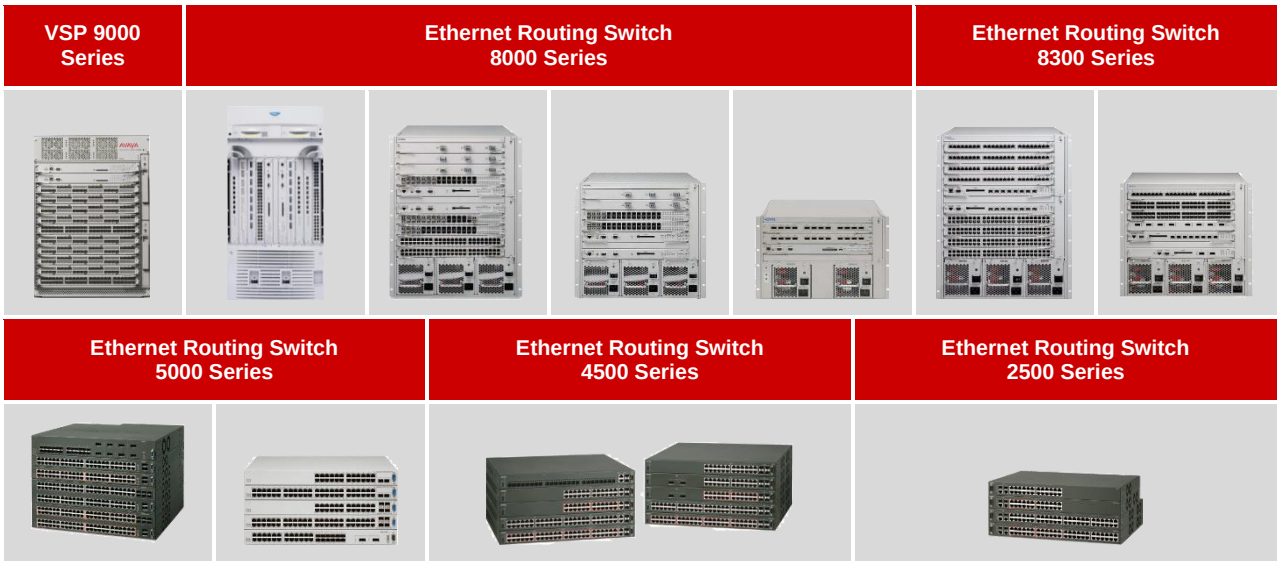


Figure 2.2 – Avaya Ethernet Switches

2.2.1 Avaya Switching Software

Each Avaya Ethernet Routing Switches and the Virtual Services Platforms each run Avaya Switching Software which supports industry standards based protocols and methods along with Avaya innovations and enhancements. The Avaya Switching Software provides the necessary core switching and routing features required to deploy and maintain an always-on, efficient and highly scalable network with innovations specifically designed to support real-time applications such as Avaya Aura or the Avaya Flare experience.

The majority of the Avaya Switching Software core features are available on all Avaya Switching platforms; however certain features and protocols are targeted for specific applications such as the core and are only available on the hardware platforms specifically targeted for that application. For example SMLT support is only available on Avaya Ethernet switching platforms which can be used in the core of the small through super large networks while IP routing is supported on all platforms.

The following table highlights the core features supported by the Avaya Switching Software that can be enabled in small, medium, large and super-large campus networks to support next-generation real-time applications:

Avaya Switching Software Feature Highlights

Convergence

- 802.1AB Link Layer Discovery Protocol
- Automatic QoS
- Automatic Detection and Automatic Configuration (ADAC) of Avaya Phones
- Energy Saver

IP Routing and Virtualization

- 802.1aq Shortest Path Bridging MAC (SPBM)
- Split Multilink Trunking (SMLT)
- Routed Split Multilink Trunking (RSMLT)
- Virtual LANs (VLANs)
- Virtual Routing & Forwarding
- VRRP with Backup Master

IP Services

- DHCP Relay
- Hardware based Unicast Routing
- Hardware based Multicast Routing
- IPv4 Tunneling for IPv6

Link Aggregation

- 802.3ad Link Aggregation
- Multilink Trunking / Distributed Multilink Trunking
- Virtual Link Aggregation Control Protocol (VLACP)

Loop Prevention

- 802.1D Spanning Tree Protocol
- 802.1w Rapid Spanning Tree Protocol
- 802.1s Multiple Spanning Tree Protocol
- BPDU Filtering
- Simple Loop Prevention Protocol (SLPP)

Network Access Control

- MAC Based Authentication
- 802.1X Extensible Authentication over LAN (EAPoL)

Security

- DHCP Snooping
- Dynamic ARP Inspection (DAI)
- IP Source Guard

Traffic Management

- L2 – l7 Classification, Marking and Filtering
- Ethernet Quality of Service (802.1p)
- Internet Group Management Protocol (IGMPv1, v2,v3).
- Ingress Policing / Egress Shaping
- IP Quality of Service (DSCP)
- Unicast / Multicast Rate Limiting

Figure 2.2.1 – Avaya Switching Software

2.2.2 Virtual Services Platform 9000

The Avaya Virtual Services Platform 9000 (VSP 9000) is an agile, streamlined, next-generation modular Ethernet switching solution that delivers high-performance, high-capacity, and high-availability for mission-critical data centers and very large campus core networks.

The VSP 9000 is a next-generation switching solution designed for mission-critical data centers and campus core networks focused on the needs of large enterprise 10 Gigabit Ethernet deployments as well as multi-tenant operators. The VSP 9000 rises to meet current and future customer requirements delivering a future-proof ultra-reliable platform that easily and cost-effectively facilitates services integration. It simplifies the network and helps reduce the time and cost of deploying new services. The VSP 9000 enables the building of a dynamic data center and campus core networks, helping to deliver 24x7 uninterrupted access to enterprise applications and services.

The VSP 9000 delivers industry-leading performance and scalability, with immediate support for very high-density 1 and 10 Gigabit Ethernet, in addition to being future-ready for the emerging 40 and 100 Gigabit Ethernet standards. The fully scalable architecture helps ensure that network capacity seamlessly scales in line with performance requirements, without complex or expensive re-engineering.

Avaya Virtual Services Platform 9000 Highlights

- A future-proof platform, offering an unmatched architecture that scales up to 27 terabits per second
- Delivers very high-density 1 and 10 Gigabit Ethernet today, meeting immediate performance and reliability needs
- Is future-ready for a seamless evolution to 40 and 100 Gigabit Ethernet
- An ultra-reliable platform, helping to ensure uninterrupted business operations
- Helps to lower operating costs, by reducing management complexity and simplifying the architecture

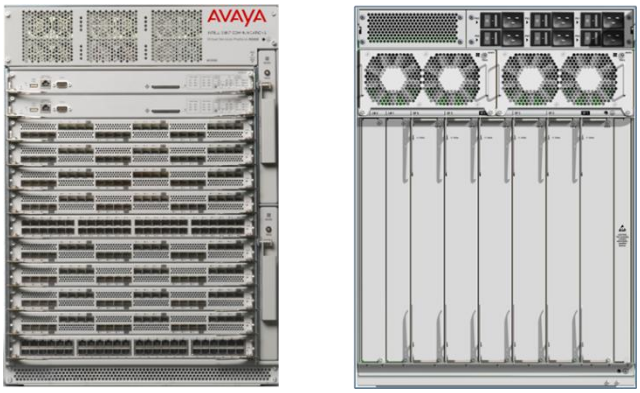


Figure 2.2.2 – Virtual Services Platform 9000 Chassis

The following table highlights the modules available for the VSP 9000 chassis:

Module	Ports	Type
9024XL	24	24 ports of SFP+ supporting 1GbE and 10GbE transceivers
9048GB	48	48 ports of SFP supporting 100M and 1GbE transceivers
9048GT	48	48 ports supporting 10/100/1000 BASE-T
9090SF	N/A	Switch Fabric
9080CP	N/A	Control Processor (CPU module)

9024XL

9048GB

9048GT

9090SF

9080CP

Table 2.2.2 – Virtual Services Platform 9000 Modules

2.2.3 Ethernet Routing Switch 8600/8800 Series

The Avaya Ethernet Routing Switch 8600/8800 (ERS 8600/8800) is a fully-resilient, totally-flexible, and highly-scalable modular Ethernet switching platform that delivers versatile network virtualization, exceptional value and cost-effectiveness, and one of the Industry's highest 10G Ethernet densities.

The ERS 8600/8800 is a proven, tested, resilient, and intelligent network solution that scales, delivering hundreds of Gigabits per second (Gbps) and hundreds of millions of packets per second (Mpps) of real-world performance to the core. This flexible architecture reduces the complexity of network design, making it ideal for large-scale Enterprise Campuses.

The ERS 8600/8800 is a balanced solution, unconstrained by bottlenecks imposed by inferior designs. In addition to establishing a solid foundation for unified communications, the ERS 8600/8800 delivers a flexible networking infrastructure that fosters growth by enabling businesses to leverage new, emerging applications and technologies with a unique architecture which always ensures optimum performance.

The following table provides a brief overview of the Avaya Ethernet Routing Switch 8600/8800 portfolio:

Avaya Ethernet Routing Switch 8600/8800 Highlights

- Innovates with Enhanced Shortest Path Bridging, delivering a game-changing Layer 2 connectivity and routing paradigm
- Simplified configuration & management including efficient service activation – free of error & delay
- Optimized traffic separation - ensuring multi-tenant partitioning & regulatory compliance
- Delivery of the industry's only optimized end-to-end cloud architecture
- Offers the Industry's leading resiliency model – Avaya's Switch Clustering empowering the most demanding applications and boosting performance by forwarding Layer 2 & 3 traffic across all available links
- Features unique field-reprogrammable NPU-based Interface Modules that, unlike conventional ASIC-based hardware, maintain full hardware-based performance and optimization as functionality and services evolve
- Enables flexible virtualized Layer 3 deployment scenarios with device and network options: VRF-Lite, Avaya's innovative IP VPN-Lite, MPLS, & IETF IP VPN
- Enables consistent IP VPN services delivered across the campus and metro; leveraging the same infrastructure to seamlessly extend service provider MPLS-networks into the LAN
- Supports high-performance IPv6 networking – a key scalability tool for demanding and expanding networks
- Offers high-density 10G, very high-density Gigabit and 10/100/1000 Ethernet for enterprise core and aggregation applications, delivering competitively-high value, flexibility, and enhanced slot conservation with a Combo option
- Best-in-class Switch Clustering resiliency model is extended to VMware Server virtualization in an iSCSI storage area network environment
- Supported by Avaya's Unified Communication Management framework featuring consistent AJAX-compliant Web-based common services, authentication and audit logging, also benchmarks network traffic and identifies anomalous behavior using Standards-based IP Flow Information Export (IPFIX)

3 Slot Chassis **6 Slot Chassis** **10 Slot Chassis** **10 Slot CO Chassis**

Figure 2.2.3 – Ethernet Routing Switch 8600/8800 Chassis Options

The following table highlights the modules available for the ERS 8600/8800 3-slot, 6-slot and 10-slot chassis:

Module	Ports	Type
8895SF	0	256Gbps Switch Fabric with 10/100/1000 OOB Management Port
8692SF w/ Mezzanine	0	256Gbps Switch Fabric with 10/100 OOB Management Port
8648GTRS	48	48 port 10/100/1000 BASE-T
8648GBRS	48	48 port Gigabit SFP baseboard
8634XGRS	34	8 port 10/100/1000 BASE-T, 24 SFP, 2 XFP (LAN Phy)
8612XLRS	12	12 port 10Gigabit XFP baseboard

8612XLRS

8648GBRS

8648GTRS

8634XGRS

889X SF/CPU

Table 2.2.3 – Ethernet Routing Switch 8600/8800 Modules

2.2.4 Ethernet Routing Switch 8300

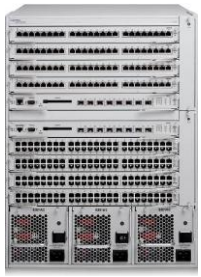
The Avaya Ethernet Routing Switch 8300 (ERS 8300) is a modular Ethernet switching solution delivering compelling performance & features for mid-tier enterprise core & high-end wiring closet applications.

The Avaya Ethernet Routing Switch 8300 continues to evolve into the core switch of choice for the mid-sized enterprise campus, delivering simplified yet superior networking, creating one network using less but more intelligent equipment - increasing availability and performance while minimizing costs. In addition, the Ethernet Routing Switch 8300 remains a premier wiring closet switch for large networks, meeting and exceeding the requirements of enterprises embarking on convergence as part of their strategic plan for success.

The following table provides a brief overview of the Avaya Ethernet Routing Switch 8300 portfolio:

Avaya Ethernet Routing Switch 8300 Highlights	
▪ Virtualized and advanced IP Routing for network design flexibility ▪ Enables large-scale convergence deployments of IP Telephony, Unified Communications and Wireless LAN mobility ▪ Simplified, automated optimization of application performance ▪ Supports Avaya's "Switch Cluster" technology for delivering 99.999% end-to-end resilient application availability ▪ 6 & 10-slot chassis, with 1GbE & 10GbE pluggable, and 10/100 & 10/100/1000 copper modules; class-leading 10GbE port density	▪ Optional redundant N-1 Switch Fabric and N+1 power supplies ▪ "Pay-as-you-grow" options for both hardware & software capabilities ▪ Standards-based Power-over- Ethernet with Dynamic Power Management ▪ Enhanced network security with access control and host integrity checking delivered via Avaya's Identity Engines solution

6 Slot Chassis



10 Slot Chassis

Figure 2.2.4 – Ethernet Routing Switch 8300 Chassis Options

The following table highlights the modules available for the ERS 8300 6-slot and 10-slot chassis:

Module	Ports	Type
8393SF	8	288Gbps Switch Fabric with 8 1GbE SFP ports
8394SF	2	288Gbps Switch Fabric with 2 10GbE XFP ports
8348TX	48	48 port 10/100 BASE-T
8348TX-PWR	48	48 port 10/100 BASE-T with 802.3af PoE
8324GTX	24	24 port 10/100/1000 BASE-T
8348GTX	48	48 port 10/100/1000 BASE-T
8348GTX-PWR	48	48 port 10/100/1000 BASE-T with 802.3af PoE
8348GB	48	48 port 1GbE SFP
8308XL	8	8 port 10GbE XFP

8308XL

8394SF

8393SF

8348GTX-XXX

Table 2.2.4 – Ethernet Routing Switch 8300 Modules

2.2.5 Ethernet Routing Switch 5000

The Avaya Ethernet Routing Switch 5000 (ERS 5000) series switches are a set of premium stackable Ethernet switching platforms providing the resiliency, security and convergence readiness required for today's high-end wiring closets, high-capacity data centers and smaller core environments.

Avaya's industry-leading resilient stackable chassis provides high-availability for delay-sensitive and business-critical data and voice applications. Up to eight Ethernet Routing Switch 5000 units can form a resilient stacked solution, manageable as a single entity, of up to 400 ports, with maximized uptime even if an individual switch within the stack should fail.

Recognizing that networking requirements vary from business to business – with differing needs at the edge, core and distribution layer, Avaya offers the highly flexible Ethernet Routing Switch 5000 Series which encompasses the original 5500 series models and the new 5600 series models offering a versatile portfolio of ten models. This provides Enterprises the ability to choose the model that best fits their networking requirements and offers 100% cross-product stacking compatibility.

The following table provides a brief overview of the Avaya Ethernet Routing Switch 5000 series portfolio:

Avaya Ethernet Routing Switch 5000 Series Highlights

Resilient

- Up to 1.2Tbps stacking, distributed trunking, split multilink trunking and power redundancy

Efficient

- Reduced power consumption, simplified converged deployments through PoE, advanced QoS and IP Phone port auto-configuration

Powerful

- Wire-speed performance

Scalable

- Up to eight switches per stack
- Up to 400 10/100/1000 ports
- 10GE Support

Secure

- Comprehensive standards-based 802.1X, advanced filtering and Avaya's Identity Engines solution

Flexible

- Wiring closet, distribution switch, small core or data center, comprehensive IPv4 and IPv6 routing support

Avaya Ethernet Routing Switch 5000 Series Portfolio

Ethernet Routing Switch 5698TFD

- 96 ports 10/100/1000
- 6 Shared SFP ports
- 2 XFP ports (10Gig)

Ethernet Routing Switch 5698TFD-PWR

- 96 ports 10/100/1000 with PoE
- 6 Shared SFP ports
- 2 XFP ports (10Gig)

Ethernet Routing Switch 5650TD

- 48 ports 10/100/1000
- 2 XFP ports (10Gig)

Ethernet Routing Switch 5650TD-PWR ▪ 48 ports 10/100/1000 with PoE ▪ 2 XFP ports (10Gig)	
Ethernet Routing Switch 5632FD ▪ 24 SFP ports ▪ 8 XFP ports (10Gig)	
Ethernet Routing Switch 5530-24TFD ▪ 12 10/100/1000 ports ▪ 12 Shared (SFP or 10/100/1000) ▪ 2 XFP ports (10Gig)	
Ethernet Routing Switch 5520-48T-PWR ▪ 48 10/100/1000 ports with PoE ▪ 4 Shared SFP ports	
Ethernet Routing Switch 5520-24T-PWR ▪ 24 10/100/1000 ports with PoE ▪ 4 Shared SFP ports	
Ethernet Routing Switch 5510-48T ▪ 48 10/100/1000 ports ▪ 2 Shared SFP ports	
Ethernet Routing Switch 5510-24T ▪ 24 10/100/1000 ports ▪ 2 Share SPF ports	

Table 2.2.5 – Ethernet Routing Switch 5000 Series Portfolio

2.2.6 Ethernet Routing Switch 4500

The Avaya Ethernet Routing Switch 4500 series switches are a stackable Ethernet switching portfolio providing high-performance, convergence-ready, secure and resilient Ethernet switching connectivity. Available as a range of 11 model variants supporting 10/100 and 10/100/1000 switching and routing, Power-over-Ethernet and 10 Gigabit Ethernet uplink options, the Ethernet Routing Switch 4500 Series is ideally suited for Enterprise wiring closet and other network edge deployments.

The following table provides a brief overview of the Avaya Ethernet Routing Switch 4500 series portfolio:

Avaya Ethernet Routing Switch 4500 Series Highlights

Resilient

- 320Gbps stacking, distributed trunking and power redundancy

Efficient

- Reduced power consumption, simplified converged deployments through PoE, advanced QoS and IP Phone port auto-configuration

Powerful

- Wire-speed performance

Scalable

- Up to eight switches per stack
- Up to 400 10/100/1000 ports
- 10GE Support

Secure

- Comprehensive standards-based 802.1X, advanced filtering and Avaya's Identity Engines solution

Flexible

- Mix-and-match best-in-class stacking capabilities; Fast Ethernet and Gigabit Ethernet in the same stack, and 1GbE and 10GbE uplinks

Avaya Ethernet Routing Switch 4500 Series Portfolio

Ethernet Routing Switch 4526T

- 24 ports 10/100
- 2 combo ports (SFP or 10/100/1000)

Ethernet Routing Switch 4526T-PWR

- 24 ports 10/100 with PoE
- 2 combo ports (SFP or 10/100/1000)

Ethernet Routing Switch 4550T

- 48 ports 10/100
- 2 combo ports (SFP or 10/100/1000)

Ethernet Routing Switch 4550T-PWR

- 48 ports 10/100 with PoE
- 2 combo ports (SFP or 10/100/1000)

Ethernet Routing Switch 4524GT

- 24 ports 10/100/1000
- 4 shared SFP ports

Ethernet Routing Switch 4524GT-PWR ▪ 24 ports 10/100/1000 with PoE ▪ 4 shared SFP ports	
Ethernet Routing Switch 4548GT ▪ 48 ports 10/100/1000 ▪ 4 shared SFP ports	
Ethernet Routing Switch 4548GT-PWR ▪ 48 ports 10/100/1000 with PoE ▪ 4 shared SFP ports	
Ethernet Routing Switch 4526GTX ▪ 24 ports 10/100/1000 ▪ 2 XFP ports (10 Gig LAN Phy)	
Ethernet Routing Switch 4526GTX-PWR ▪ 24 ports 10/100/1000 with PoE ▪ 2 XFP ports (10 Gig LAN Phy)	
Ethernet Routing Switch 4526FX ▪ 24 ports 100FX ▪ 2 combo ports (SFP or 10/100/1000)	

Table 2.2.6 – Ethernet Routing Switch 4500 Series Portfolio

2.2.7 Ethernet Routing Switch 2500

The Avaya Ethernet Routing Switch 2500 (ERS 2500) series switches are a family of cost effective, stackable 10/100BASE-TX Ethernet switching platforms perfectly suited for branch offices or enterprise edge applications requiring a low-cost but feature-rich solution in the wiring closet.

Ideal for enterprises with big plans but not-so-big budgets, the ERS 2500 offers the flexibility, scalability and cost-effectiveness to deploy next-generation technology today - while providing the high resiliency and performance you need.

The following table provides a brief overview of the Avaya Ethernet Routing Switch 2500 series portfolio:

Avaya Ethernet Routing Switch 2500 Series Highlights	
Resilient ▪ 32 Gbps stacking, distributed trunking and power redundancy **Efficient** ▪ Reduced power consumption, simplified converged deployments through PoE, advanced QoS and IP Phone port auto-configuration **Powerful** ▪ Wire-speed performance	**Scalable** ▪ Up to eight switches per stack ▪ Up to 384 ports 10/100 ports ▪ Up to 16 ports 10/100/1000/SFP Combo ports **Secure** ▪ Comprehensive standards-based 802.1X, advanced filtering and Avaya's Identity Engines solution **Flexible** ▪ Low cost Fast Ethernet edge with Gigabit uplinks, stacking and enterprise features

Avaya Ethernet Routing Switch 2500 Series Portfolio	
Ethernet Routing Switch 2526T ▪ 24 ports 10/100 ▪ 2 combo ports (SFP or 10/100/1000)	
Ethernet Routing Switch 2526T-PWR ▪ 24 ports 10/100 (12 with PoE) ▪ 2 combo ports (SFP or 10/100/1000)	
Ethernet Routing Switch 2550T ▪ 48 ports 10/100 ▪ 2 combo ports (SFP or 10/100/1000)	
Ethernet Routing Switch 2550T-PWR ▪ 48 ports 10/100 (24 with PoE) ▪ 2 combo ports (SFP or 10/100/1000)	

Table 2.2.7 – Ethernet Routing Switch 2500 Series Portfolio

2.3 Avaya Wireless LAN 8100

The Avaya WLAN 8100 Series combines the latest 802.11n wireless standard with a new and truly unified wireless/wired architecture for a stellar result – an advanced product that delivers wired performance to wireless users at a lower total cost of ownership.

The WLAN 8100 Series architecture incorporates an innovative design that allocates separate resources to management, control, and data forwarding, and enables network intelligence to be optionally distributed to the wireless edge. By combining the operational advantages of centralized management and intelligence with the scalability, efficiency and performance of distributed switching, the optimized wireless controller/switch architecture is able to deliver an optimized WLAN switching system.

The WLAN 8100 is complete solution that's ideal for today's leading enterprises looking to move users to wireless access, IP Telephony and converged multimedia applications.

The following table provides a brief overview of the Avaya Wireless LAN 8100 series portfolio:

Avaya Wireless LAN 8100 Series Highlights	
▪ Provides higher performance, throughput, reliability for next generation 802.11n deployments ▪ Common network access security capabilities that can be set for all users and devices, both wired and wireless; Support for popular authentication types & security standards ▪ Optimized for voice and multimedia applications; Supports industry-leading wireless voice call densities and introduces the industry's first solution to extend E-911 location support to wireless devices	▪ Offers end-to-end solutions, including fixed-mobile convergence (e.g., WLAN infrastructure, WLAN handsets, data, voice, Mobile Unified Communications solutions), to extend reach and increase worker productivity ▪ Delivers an integrated wireless/wired infrastructure that simplifies deployment ▪ Centralized management common to both wireless and wired networks removes cost and complexities of supporting multiple networks

Avaya Wireless LAN 8100 Series Portfolio	
WC 8180-16L ▪ 16 Access Points (Upgradable to 512) ▪ 12 10/100/1000 ports, 12 SFP ports ▪ 2 XFP ports (10Gig)	
WC 8180 ▪ 64 Access Points (Upgradable to 512) ▪ 12 10/100/1000 ports, 12 SFP ports ▪ 2 XFP ports (10Gig)	
AP 8120 ▪ Dual Radio 802.11n ▪ 802.3af power (full performance) ▪ 1 10/100/1000 port ▪ Up to 16 SSIDs per radio (32 per Access Point) ▪ Up to 200 associations per radio	

Table 2.3 – Avaya Wireless LAN 8100 Portfolio

3. Campus Reference Architectures

Avaya converged campus architectures are built using the fundamental strategic values of the Avaya Data Solutions organization. By adhering to these core values, Avaya provides a solid campus network infrastructure on which the Avaya Flare experience can be deployed upon. With this solid infrastructure, the enterprise can solve their business challenges by enabling services easily and without worry. Avaya offers a unique value proposition in its ability to provide this infrastructure while still offering best-in-class total cost of ownership.

Figure 3 – Avaya Data Solutions Strategic Values

The Avaya campus solutions have been broken into small, medium, large and super large to address specific requirements of each enterprise. A major objective of these architectures is to provide a blueprint and starting point for the customer network design. By providing solutions that have been architected, validated, and documented, the building block for the network is now in place and ready for the specific customization required by each individual network. This customization comes in the form of specific VLANs required, protocols being used, number of edge devices to connect, and application requirements for the infrastructure.

3.1 Avaya Ethernet Routing Switches

The following section provides various Avaya Ethernet Routing Switch options and recommended topologies for small, medium, large and super large campus deployments. Specific implementation details and best practice recommendations are provided in complementary technical solution guides reference at the end of each section.

3.1.1 Small Campus

The small campus reference design is intended to support 1 to 1,500 network devices. The upper limit of 1,500 devices is not a hard number, but rather a general guideline to base designs upon.

The small campus reference architecture consists of a cluster of Ethernet Routing Switch 5000 series switches in the core and Ethernet Routing Switch 2500, 4500 or 5000 series switches at the access layer. IP routing for each Virtual LAN (VLAN) is provided in core with Virtual Routing Redundancy Protocol (VRRP) providing default gateway redundancy.

Small Campus Reference Architecture

Core:

- Ethernet Routing Switch 5000

Access:

- Ethernet Routing Switch 2500
- Ethernet Routing Switch 4500
- Ethernet Routing Switch 5000

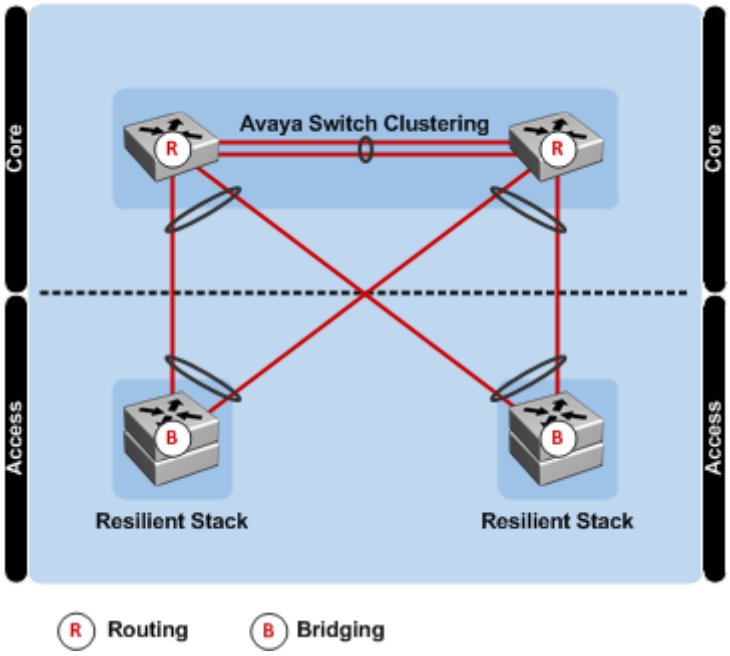


Figure 3.1.1 – Small Campus Reference Architecture

Details and best practices for the small campus design are provided in the Avaya document titled ***Small Campus Technical Solutions Guide (NN48500-573)*** available for download on https://support.avaya.com/css/Products/P0846/All_Documents.

3.1.2 Medium Campus

The medium campus reference design is intended to support up to 3,000 network devices. The upper limit of 3,000 devices is not a hard number, but rather a general guideline to base designs upon.

The medium campus reference architecture consists of a cluster of Ethernet Routing Switch 8300 series switches in the core and Ethernet Routing Switch 2500, 4500, 5000 or 8300 series switches at the access layer. IP routing for each Virtual LAN (VLAN) is provided in the core with Routed Split Multilink Trunking (RSMLT) Edge or Virtual Routing Redundancy Protocol (VRRP) providing default gateway redundancy.

Medium Campus Reference Architecture

Core:

- Ethernet Routing Switch 8300

Access:

- Ethernet Routing Switch 2500
- Ethernet Routing Switch 4500
- Ethernet Routing Switch 5000
- Ethernet Routing Switch 8300

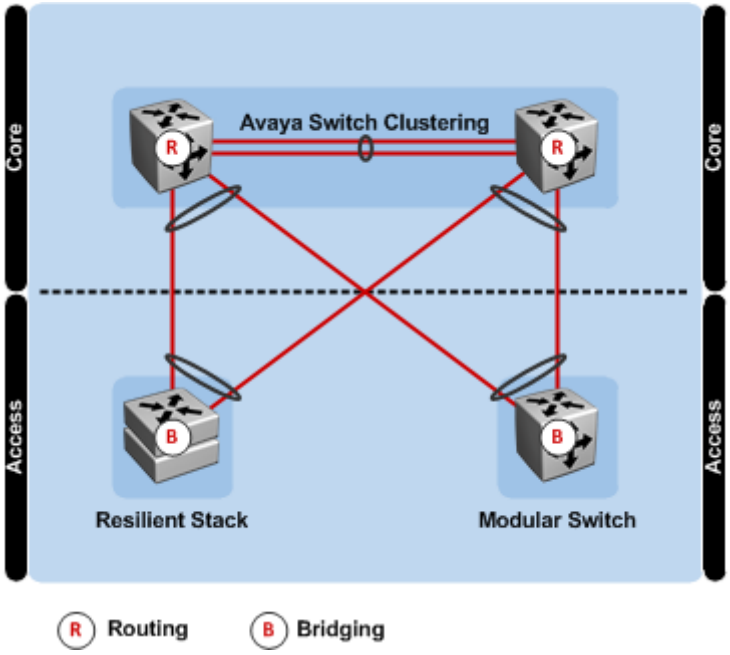


Figure 3.1.2 – Medium Campus Reference Architecture

Details and best practices for the medium campus design are provided in the Avaya document titled ***Medium Campus Technical Solutions Guide (NN48500-574)*** available for download on https://support.avaya.com/css/Products/P0846/All_Documents.

3.1.3 Large Campus

The large campus reference design is intended to support more than 2,500 network devices. The lower limit of 2,500 devices is not a hard number, but rather a general guideline to base designs upon.

The large campus reference architecture consists of a cluster of Ethernet Routing Switch 8000 series switches in the core, optional clustered Ethernet Routing Switch 8000, 8300 or 5000 series switches in the distribution layer and Ethernet Routing Switch 2500, 4500, 5000 or 8300 series switches at the access layer. IP routing for each Virtual LAN (VLAN) is provided in the core with Routed Split Multilink Trunking (RSMLT) Edge or Virtual Routing Redundancy Protocol (VRRP) providing default gateway redundancy. IP routing may also optionally be enabled in the distribution layer depending on the topology and customer requirements.

Large Campus Reference Architecture

Core:

- Ethernet Routing Switch 8000

Distribution (Optional):

- Ethernet Routing Switch 8800
- Ethernet Routing Switch 8300
- Ethernet Routing Switch 5000

Access:

- Ethernet Routing Switch 2500
- Ethernet Routing Switch 4500
- Ethernet Routing Switch 5000
- Ethernet Routing Switch 8300

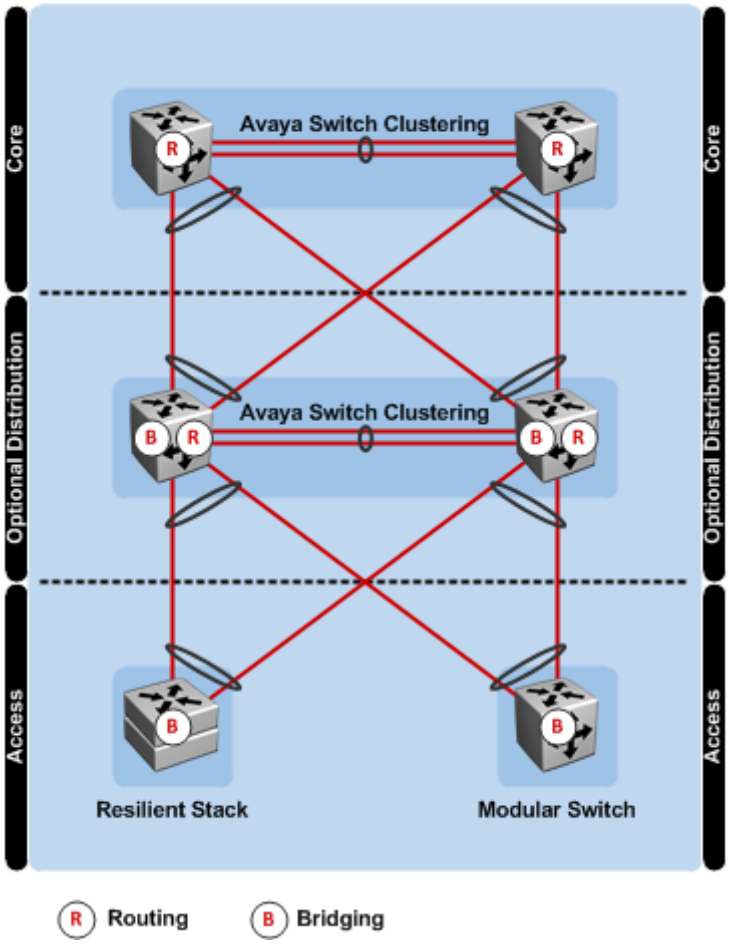


Figure 3.1.3 – Large Campus Reference Architecture

Details and best practices for the large campus design are provided in the Avaya document titled ***Large Campus Technical Solutions Guide (NN48500-575)*** available for download on https://support.avaya.com/css/Products/P0846/All_Documents.

3.1.4 Super Large Campus

The super large campus reference design is intended as a blueprint for highly scalable 10Gbps networks containing more than 5,000 network devices. The lower limit of 5,000 devices is not a hard number, but rather a general guideline to base designs upon.

The super large campus reference design architecture consists of a cluster of Virtual Services Platform 9000 series switches in the core, optional clustered Ethernet Routing Switch 8000 or 8300 series switches in the distribution layer and Ethernet Routing Switch 2500, 4500, 5000 or 8300 series switches at the access layer. IP routing for each Virtual LAN (VLAN) is provided in the core with Routed Split Multilink Trunking (RSMLT) Edge or Virtual Routing Redundancy Protocol (VRRP) providing default gateway redundancy. IP routing may also optionally be enabled in the distribution layer depending on the topology and customer requirements.

Super Large Campus Reference Architecture

Core:

- Virtual Services Platform 9000

Distribution (Optional):

- Ethernet Routing Switch 8800
- Ethernet Routing Switch 8300

Access:

- Ethernet Routing Switch 2500
- Ethernet Routing Switch 4500
- Ethernet Routing Switch 5000
- Ethernet Routing Switch 8300

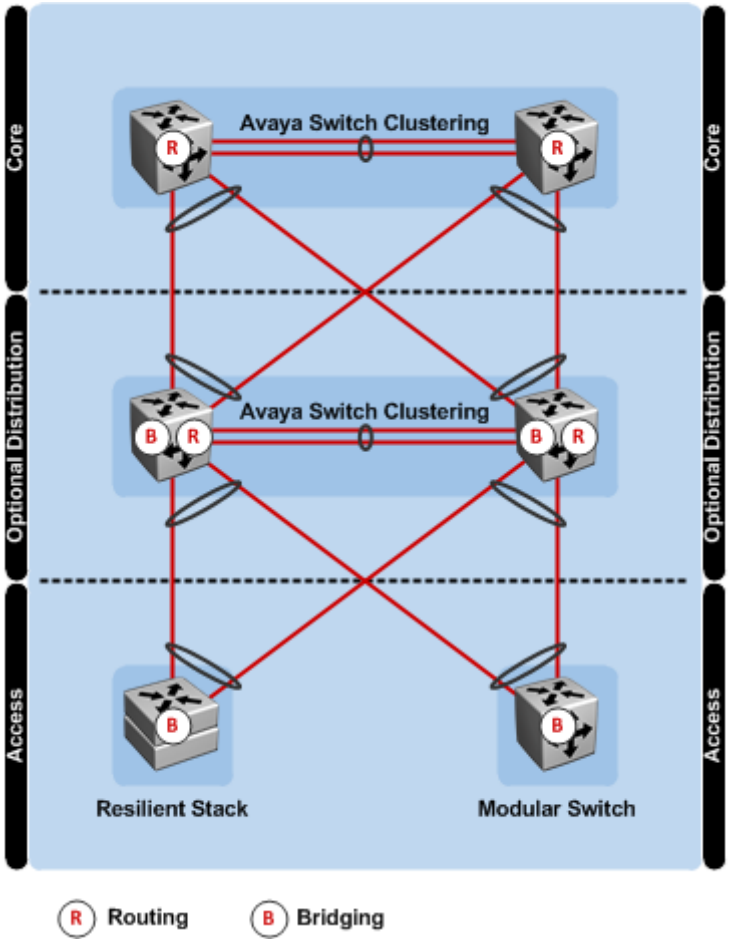


Figure 3.1.4 – Super Large Campus Reference Architecture

Details and best practices for the super large campus design are provided in the Avaya document titled ***Super Large Campus Technical Solutions Guide (NN48500-609)*** available for download on https://support.avaya.com/css/Products/P0846/All_Documents.

3.1.5 Data Center

The Avaya Aura and third-party communication infrastructure devices are typically deployed in a data center which connects to the core of the network. For performance a data center typically requires stackable or modular 10/100/1000 Ethernet switches to connect Avaya Aura servers, application servers, SAN, firewalls, routers, wireless controllers, and gateways to the network.

The physical layout of the data center will influence how the data center switches are deployed. Some data centers may aggregate all the Ethernet connections to the end of each rack where the Ethernet switches reside. Newer data centers designs may include stackable Ethernet switches at the top of each rack (referred to as top of rack switches) which backhaul traffic directly to a data center distribution switch or the core. For performance and availability the data center switches typically use redundant 10 Gigabit Ethernet links.

The Avaya Ethernet Routing Switches can provide multiple layers of redundancy within the data center by supporting redundant power, resilient stacking, standard link aggregation and split multilink trunking. The data center switches can be tied to the core using resilient load-shared links while critical applications and services can be connected to multiple I/O modules or switches within a stack using standards based link aggregation.

Avaya Aura servers leveraging System Platform can be dual connected to multiple I/O modules or switches in a stack using standards base 802.3ad link aggregation or active / standby link layer redundancy. Avaya G400 series media gateways can leverage active / standby link aggregation or rapid spanning tree protocol. Older media gateways such as the Avaya G650 leverage multiple IPSI Ethernet connections to redundant control networks.

Details and best practices for the data center are provided in the Avaya document titled ***Data Center Access Solution Guide (NN48500-557)*** available for download on https://support.avaya.com/css/Products/P0845/All_Documents.

3.1.5.1 End of Row Switches

For data centers that aggregate the Ethernet connections to the end of each rack, the Avaya Ethernet Routing Switch 8800, 8300, 5000 and 4500 all provide high-density 10/100/1000 copper ports along with non-blocking switching, redundant power, QoS and 10 Gigabit Ethernet support. Device level redundancy is provided by distributing uplink ports and device links between different I/O modules in a chassis or different switches in a stack. Avaya end of row switches can offer up to 400 10/100/1000 ports with 1G SFP and/or 10G XFP uplink ports.

End of Row Switches

Small Data Center:

- Ethernet Routing Switch 4500
- Ethernet Routing Switch 5600

Medium / Large Data Centers:

- Ethernet Routing Switch 8800
- Ethernet Routing Switch 8300
- Ethernet Routing Switch 4500
- Ethernet Routing Switch 5000

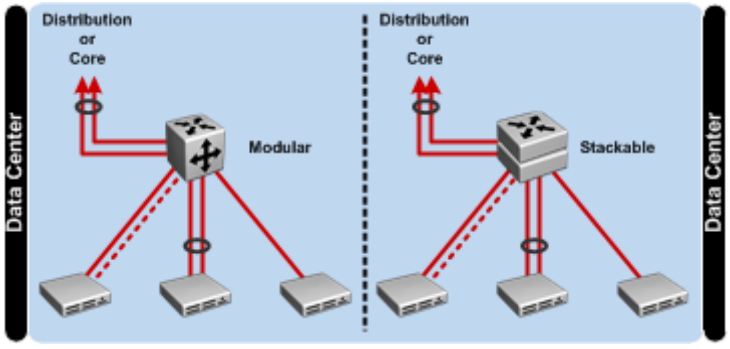


Figure 3.1.5.1 – End of Row Data Center Reference Architecture

3.1.5.2 Top of Rack Switching

For data centers that require standard top-of-rack switching, the Avaya Ethernet Routing Switch 5000 and 4500 series stackable switches provide high-density 10/100/1000 copper ports along with non-blocking switching, redundant power, QoS and 10 Gigabit Ethernet support. Device level redundancy is provided by stacking two switches in each rack then distributing uplink ports and device links between different switches in a stack. Avaya end of top of rack switches can offer up to 400 10/100/1000 ports with 1G SFP and/or 10G XFP uplink ports.

Top of Rack Switches – Standalone Switches / Stacks

Data Center:

- Ethernet Routing Switch 4500
- Ethernet Routing Switch 5000

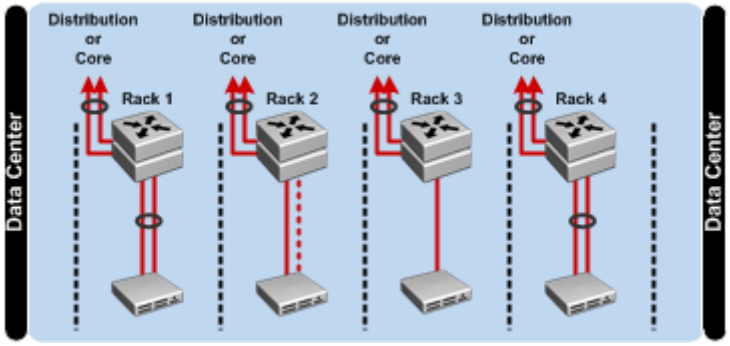


Figure 3.1.5.2-1 – Top of Rack Data Center Reference Architecture

Avaya's Flexible Advanced Stacking Architecture (FAST) allows top of rack switches to be inter-connected using horizontal stacking. By strategically interconnecting the stacking ports, Avaya Ethernet Routing Switches in each rack can be interconnected to form a single logical switch providing up to 1.2Tbps of stacking bandwidth, 400 x 10/100/1000 copper ports and 16 x 10 Gigabit Ethernet ports.

A single horizontal stack provides high-speed interconnectivity between up to 8 racks but with limited availability as devices can only be connected to a single switch. Aura server and media gateway device level redundancy can be provided by deploying and inter-connecting two switches at the top of each rack then distributing uplink ports and device links between both switches in a stack. With this deployment model a horizontal stack of 8 switches would support 4 racks.

Top of Rack Switches – Horizontal Stacking

Data Center:

- Ethernet Routing Switch 4500
- Ethernet Routing Switch 5000

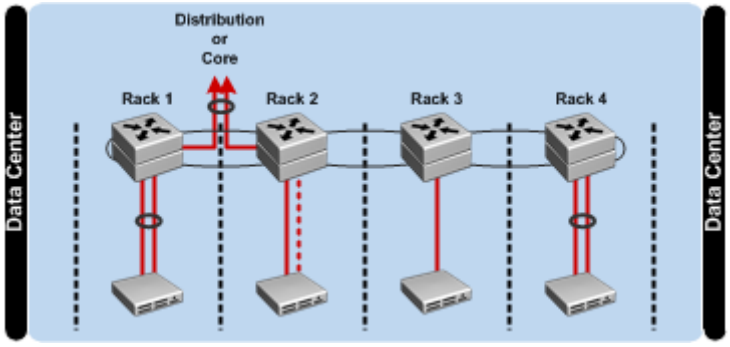


Figure 3.1.5.2-2 – Horizontal Stacking Data Center Reference Architecture

For additional availability two horizontal stacks can be clustered together using Avaya's split multilink trunking technology. A horizontal stack cluster allows devices within the rack to be dual-connected to the network using standards based link aggregation ensuring no single point of failure. A horizontal stack cluster also allows maintenance and software upgrades to be performed in a stack without impacting the availability of critical services and applications in the data center. A horizontal stack cluster can support up to 800 x 10/100/1000 copper ports and 32 x 10 Gigabit Ethernet ports.

Top of Rack Switches – Horizontal Stacking with Avaya Switch Clustering

Data Center:

- Ethernet Routing Switch 5000

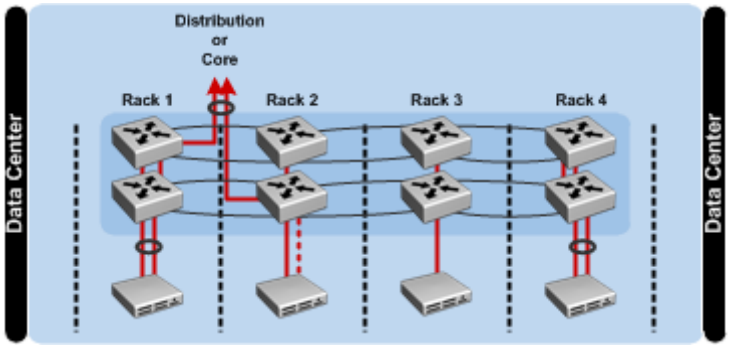


Figure 3.1.5.2-3 – Horizontal Stack Switch Cluster Data Center Reference Architecture

3.2 Wireless LAN 8100

The Avaya Wireless LAN 8100 series is a Wireless LAN platform specifically designed to address the current autonomous Access Point and thin Access Point architecture limitations for next generation 802.11n deployments. Initially deployed as an overlay, the Avaya Wireless LAN 8100 solution will evolve to support an innovative split-plane architecture which has multiple benefits. First and foremost, it allows wireless user traffic to be offloaded to select Avaya Ethernet Routing Switches completely bypassing the Wireless Controller. This allows small, medium and large customers to deploy high performance 802.11n wireless networks without fear of oversubscribing the Wireless Controller or data center links, as well as extending the resiliency capabilities of the wired core switching to the wireless forwarding plane. In addition, this enabled controller virtualization, leveraging VMware and the latest developments in cloud computing and extending it to the network services of Access Point control and management.

The Wireless LAN 8100 reference architecture consists of one or more WC 8180/8180-16L Wireless Controllers in the data center connected to a data center switch or directly to the core. AP 8120 Access Points are connected to the access layer switches at the edge of the network.

In the initial release all wireless user traffic is tunneled from the Access Points to the Wireless Controllers in the data center using standards based CAPWAP over IPv4. As the solution evolves customers can offload wireless user traffic to split-plane enabled Avaya Ethernet Routing Switches deployed in the access layer, distribution layer or core of the network offloading the Wireless Controllers. The Wireless Controllers are then re-purposed to provide pure configuration and control functions, or the other control services could be migrated to a VMware server in the data center.

Wireless LAN 8100 Overlay Reference Architecture

Data Center:

- Wireless Controller 8180
- Wireless Controller 8180-16L

Access:

- Access Point 8120

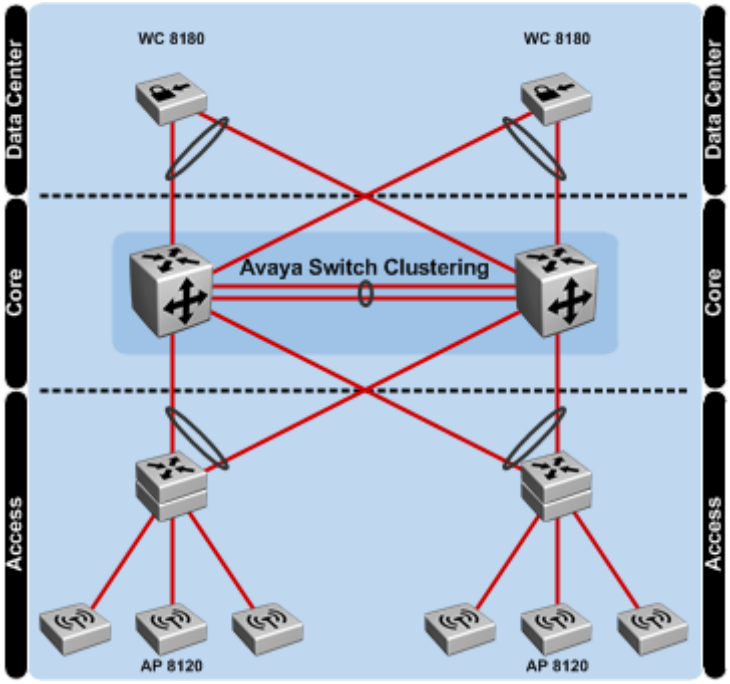


Figure 3.2 – Wireless LAN 8100 Overlay Reference Architecture

Details and best practices for the Wireless LAN 8100 design are provided in the Avaya document titled ***Wireless LAN 8100 Series Design Guide*** (NN48500-587) available for download on https://support.avaya.com/css/Products/P0846/All_Documents.

Best Practices and Recommendations:

- As each 802.11n Access Point is capable of forwarding 600Mbps of user-data onto the network, whenever possible it is recommended that the WC 8180 Wireless Controllers be directly connected to the core. While the WC 8180 will be physically located in the data center, connecting them to the core layer ensures the data center switches will not be oversubscribed with wireless user-traffic.

4. Design Details

4.1 Avaya Aura System Platform

Avaya Aura services and applications leverage System Platform technology that simplifies the deployment of Unified Communications and Contact Center applications. This framework leverages virtualization technology, predefined templates, common installation, licensing, and support infrastructure.

System Platform enables the Avaya Aura applications and services to operate in a virtualized environment. The System Platform manages the allocation and sharing of physical server hardware resources, including the CPU, memory, disk storage, and network interfaces. The System Platform is delivered solely through an appliance model which includes an Avaya S8300D, Avaya S8510, Avaya S8800, Dell R610 or HP DL360 common servers, System Platform software and the Avaya software applications. The specific server memory, CPU and HDD configuration is dependent on the Avaya Aura applications that are being deployed.

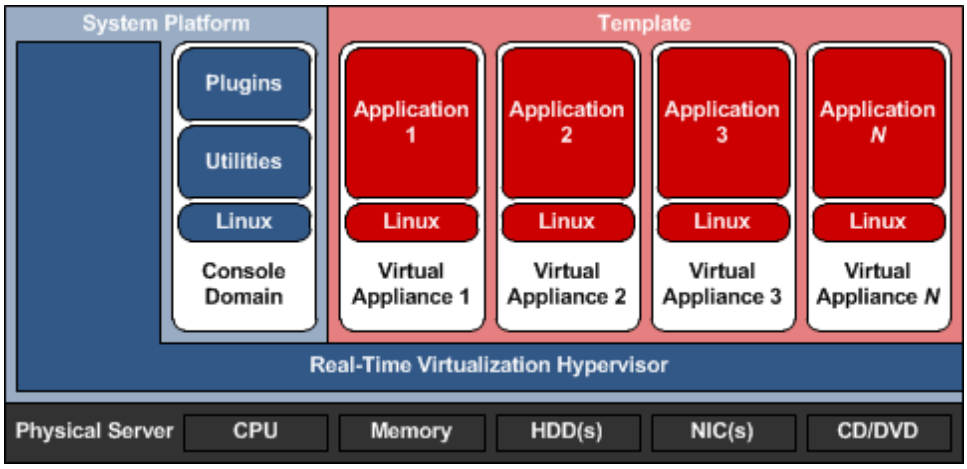


Figure 4.1 – System Platform Architecture

The Avaya Aura architecture supports application layer and physical layer redundancy options. Application layer redundancy allows certain Aura services such as Communication Manager or Session Manager to be distributed geographically providing always-on services to end-points, media gateways and applications in the event of a physical server, network or data center failure. Physical layer redundancy is available for any Avaya Aura service running on System Platform and ensures always-on services in the event of a data center, Ethernet switch or I/O module failure.

Physical layer redundancy is provided within System Platform by enabling NIC teaming on two or more physical Gigabit Ethernet interfaces installed within in the physical server. System platform supports various NIC teaming modes each of which provide varying levels of fault tolerance. However for compatibility with Avaya Ethernet switches in the data center only certain NIC teaming modes are recommended.

Method	Description
Round Robin	System Platform transmits packets in sequential order from the first available NIC through the last available NIC. This mode provides load balancing and fault tolerance.
Active / Backup	Only one NIC in the team is active. A slave NIC only becomes active if the active NIC fails. The NIC teams MAC address is only visible on the active NIC in the team to avoid confusing the Ethernet Switches.
XOR Policy	System Platform transmits based on [(Source MAC XOR'd with Destination MAC) slave NIC count]. This teaming mode selects the same slave NIC for each destination MAC address. This mode provides load balancing and fault tolerance.
Broadcast	System Platform will transmit all packets on all slave interfaces. This mode provides fault tolerance.
IEEE 802.3ad	Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification.
Adaptive TX Load Balancing	Channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.
Adaptive Load Balancing	Includes balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different peers use different hardware addresses for the server.

Table 4.1 – System Platform NIC Teaming Modes

4.1.1 Active / Backup Link Layer Redundancy

The Active / backup NIC teaming mode can be enabled on System Platform servers to provide active / standby fault-tolerance. In this mode of operation only one port in the NIC team is active and carrying traffic at a time. The standby link in in the NIC team only becomes active if the primary link fails.

The Active / backup teaming mode is supported by any Avaya Ethernet Routing Switch and does not require any special configuration on the Avaya Ethernet switches to be supported. System Platform servers can be connected to a cluster of Avaya Ethernet Routing Switches, a horizontal or vertical stack of Avaya Ethernet Routing Switches or two separate standalone Avaya Ethernet Routing Switches.

Active / backup teaming provides basic failover only and can only detect a failure if the physical link fails. Active / backup teaming does not provide path continuity and cannot detect if the upstream switch is able to forward traffic. As such certain Ethernet switch failure scenarios may not be detected.

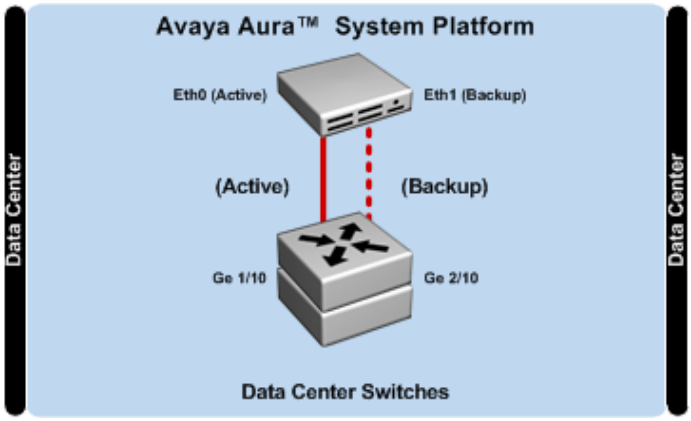


Figure 4.1.1 – System Platform Active / Backup Link Layer Redundancy

Best Practices and Recommendations:

- Active / Backup teaming is recommended if System Platform servers are connected to two independent standalone Avaya Ethernet Routing Switches in the data center.
- No link aggregation should be enabled on the Avaya Ethernet Routing Switches.
- It is required that the active and standby ports be connected to data center switch ports with autonegotiation enabled and capable of supporting the same speed and duplex modes.
- All ports in the team must be connected to switch ports supporting the same Converged VLAN ID. This ensures System Platform can communicate correctly regardless of which port in the team is active.
- For fast failover it is recommended that System Platform be connected to switch ports with spanning tree faststart or edge modes enabled. This ensures the ports can forward traffic as soon as they become active.

4.1.2 IEEE 802.3ad Link Layer Redundancy

The IEEE 802.3ad dynamic link aggregation NIC teaming mode can be enabled on System Platform servers to provide active / active fault-tolerance as well as load-sharing. In this mode of operation two or more ports on the physical server form a link aggregation group (LAG) and each port actively carries's traffic. If one link in the LAG fails, the remaining port members in the LAG share the load. The only limitation is that all ports in the LAG must operate at the same speed and duplex modes.

IEEE 802.3ad dynamic link aggregation mode requires special configuration on Avaya Ethernet Routing Switches and is compatible with all Avaya Ethernet Routing Switches along with Avaya's split multilink trunking and routed split multilink trunking technologies. System Platform servers can be connected to a cluster of Avaya Ethernet Routing Switches, a horizontal or vertical stack of Avaya Ethernet Routing Switches or a horizontal stack cluster of Avaya Ethernet Routing Switches.

The IEEE 802.3ad teaming mode provides the additional benefit of being able to detect link failures as well as path continuity. The ports in the LAG only become active if Link Aggregation Control Protocol (LACP) is enabled and operational and both parties negotiate. Ports in the LAG will only remain active if LACP remains operational on both parties. If either party in the team is unable to forward traffic due to a software or hardware failure, LACP will cease to function and the appropriate links will be removed from the LAG.

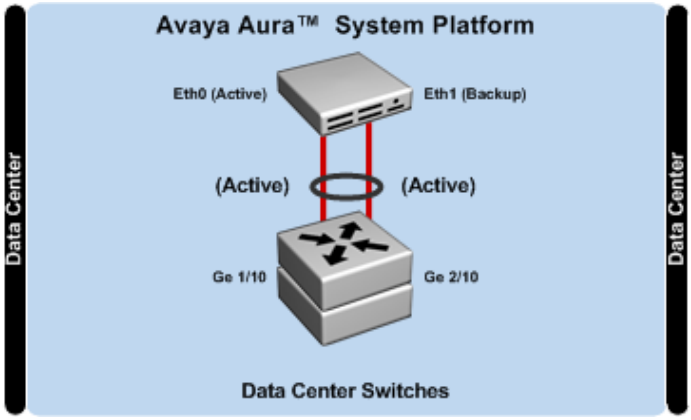


Figure 4.1.2 – System Platform 802.3ad

Best Practices and Recommendations:

- IEEE 802.3ad link aggregation is recommended if connecting System Platform servers to a cluster of Avaya Ethernet Routing Switches, a horizontal / vertical stack of Avaya Ethernet Routing Switches or a horizontal stack cluster of Avaya Ethernet Routing Switches.
- LACP support must be enabled on the Avaya Ethernet Routing Switches.
- It is required that all ports in the LAG be connected to switch ports with autonegotiation enabled and capable of supporting the same speed and duplex modes.
- When implementing Split Multilink Trunking with LACP it is recommended that you follow the implementation best practices outlined in the Small, Medium, Large and Super Large Campus Solution Guides.

4.2 Avaya G250 / G350 / G4x0 Media Gateways

The Avaya G250 / G350 / G430 and G450 series Media Gateways each support multiple configurations of Ethernet ports which can be used to connect the Media Gateways to data center switches, a wide area network (WAN) as well as support IP Phones and other data devices.

Avaya Media Gateways support two methods of link-layer redundancy which can be enabled to provide redundant interconnections to Avaya Ethernet data center switches which include active / backup fault tolerance and IEEE 802.1w Rapid Reconfiguration of Spanning Tree (RSTP). Either method can be deployed to ensure an active network path is available in the event of a single data center switch failure.

The Active / backup teaming mode is supported by Avaya G250 / G350 / G430 and G450 Media Gateways and does not require any special configuration on the Avaya Ethernet Routing Switch to be supported. Avaya Media Gateways can be connected to a cluster of Avaya Ethernet Routing Switches, a horizontal or vertical stack of Avaya Ethernet Routing Switches or two separate standalone Avaya Ethernet Routing Switches. The only requirement is that the Aura Services VLAN is present on all the data center ports that the Media Gateways are connected to.

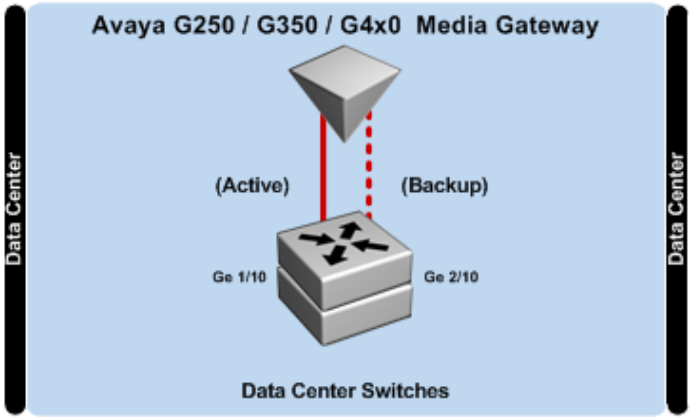


Figure 4.2-1 – Media Gateway Active / Backup Link Layer Redundancy

The Avaya G250 / G350 / G430 and G450 Media Gateways also support IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) which allows the Media Gateways to be connected to two or more Avaya Ethernet Routing Switches in a RSTP domain. RSTP provides redundancy by connecting an Avaya Media Gateway to one or more data center switches ports in the Aura Services VLAN which creates a layer 2 loop. The RSTP protocol detects the available paths between the Avaya Media Gateways and the Avaya Ethernet Routing Switches on the Aura Services VLAN and will only permit traffic over one of the paths. Redundant network path between the devices will be blocked eliminating the layer 2 loop. If the primary path fails, the traffic is then forwarded over one of the remaining available network paths.

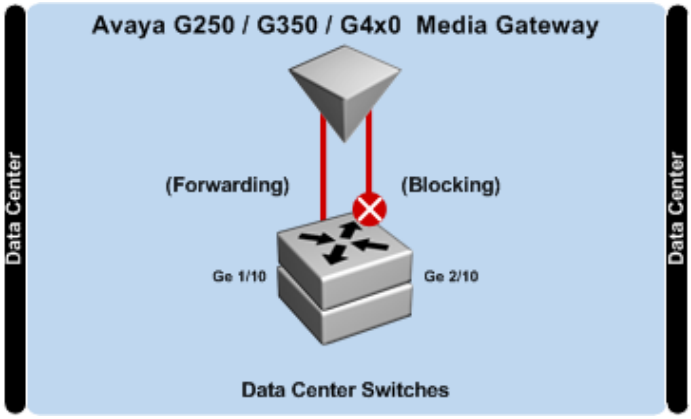


Figure 4.2-2 – Media Gateways with RSTP

It's important to note that for the layer 2 loop to be detected in the data center, RSTP must be enabled on the end of row or horizontal stack of Avaya Ethernet Routing Switches where the Media Gateways connect. RSTP cannot be extended between different instances of SMLT connected data center switches. SMLT is an alternative to spanning tree and will not permit spanning tree BPDUs to be forwarded through the distribution or core. As such RSTP can only be supported in individual instances of SMLT attached top of rack or end of row data center switches and introduces unnecessary complexity into the data center. In addition with the above limitation RSTP adds the potential of introducing un-foreseen network loops in the data center.

Best Practices and Recommendations:

- Whenever possible it is recommended that the Avaya Media Gateways be connected to the datacenter switches using Active / Backup redundancy. This eliminates the need for deploying RSTP in the datacenter adding unnecessary complexity to the network.

4.3 Virtual LANs

Virtual LANs (VLANs) can be deployed within an enterprise network for multiple reasons such as separating applications, minimizing broadcast domains and isolating protocols. In most cases a VLAN is considered equivalent to a broadcast domain and has a single IPv4 subnet assigned, however with the advent of IPv6 being supported by current operating systems, most VLANs will now commonly support an IPv4 and IPv6 subnet.

In most campus environments an enterprise will deploy one or more VLANs in the data center to support various applications as well as one or more user and application VLANs in the access layer where the users and devices connect to the network. The number, type and location of VLANs will vary greatly from design to design.

To support the Avaya Flare experience it is recommended that dedicated VLANs be deployed in both the data center and access layers. In the data center it is recommended that the Avaya Aura servers and gateways be connected to a dedicated Aura Services VLAN while in the access layer Avaya IP Phones, Avaya Desktop Video Devices and third-party video devices be connected to a dedicated Converged VLAN.

While it is not necessary to deploy separate VLANs in the data center and access layer to support the Flare experience, this recommendation allows organizations to separate the real-time traffic from data center and user traffic which can protect the Avaya Aura servers, applications, media gateways and converged communication devices from malicious traffic, allows the devices to be firewalled and additionally aids in troubleshooting. With wire-speed routing now being available on all Avaya Ethernet Routing Switch platforms there is no longer any performance penalty for isolating applications and devices into separate VLANs.

4.3.1 Access Layer

Converged devices such as the Avaya IP Phones and Desktop Video Devices connect to Avaya Ethernet Routing Switches in the access layer. Avaya recommends that a converged VLAN be created and assigned to access layer ports connecting to the Avaya IP Phones and Desktop Video Devices. The converged VLAN can be used to connect additional converged devices including third-party video conferencing end-points.

The number of converged VLANs to deploy will vary depending on the number of converged devices and the geographic nature of the network. For small campus deployments a single converged VLAN will typically suffice while medium, large and super large campus networks may require a converged VLAN to be deployed per floor, building or department. As a general best practice it is recommended that the VLAN not exceed 254 devices, however this is a general recommendation which cannot always be applied in larger network deployments.

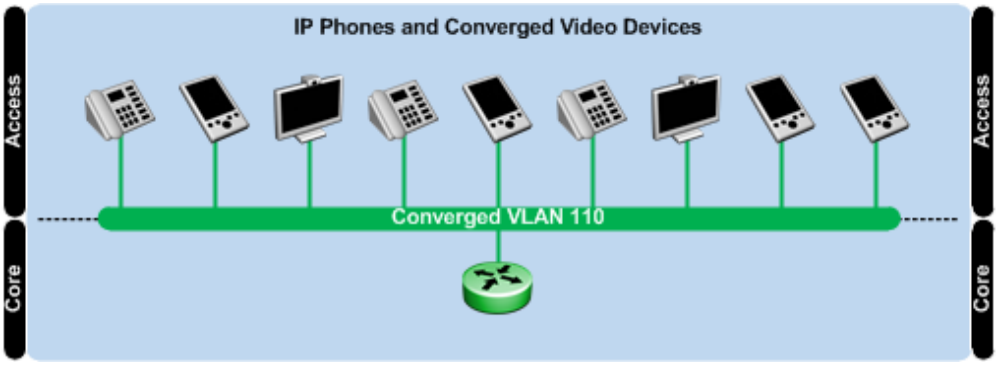


Figure 4.3.1-1 – Small Campus Example with Single Converged VLAN

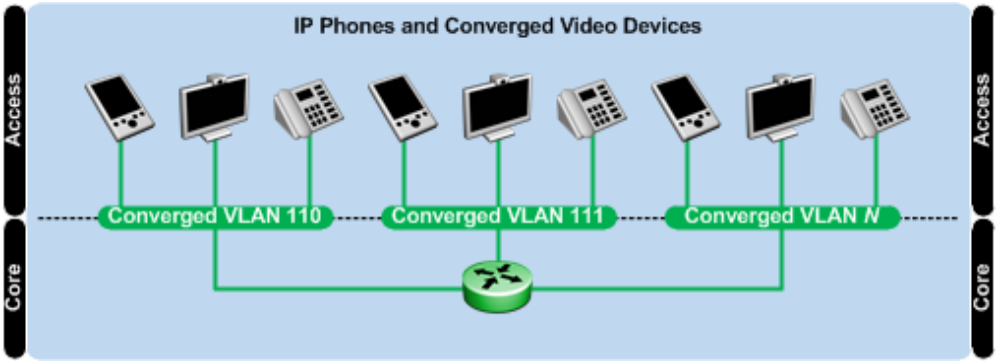


Figure 4.3.1-2 – Medium / Large Campus Example with Multiple Converged VLAN

Best Practices and Recommendations:

- For small campus deployments it is recommended that a single Converged VLAN be deployed at the access layer. Additional Converged VLANs can be deployed as required if more than 254 converged devices are connected to the network.
- For medium and large deployments it is recommended that one Converged VLAN be deployed at the access layer per department, floor or building. The number of Converged VLANs required may vary based on topology and the overall network design.

4.3.2 Data Center

Avaya Aura servers, applications and media gateways connect to the Ethernet network in the data center. Avaya recommends that a dedicated Aura Services VLAN be created in the data center specifically for Avaya Aura servers and gateways that partitions control and real-time traffic from other services and applications hosted in the data center.

For campus deployments with a single data center a single Aura Services VLAN can be deployed to connect all Aura servers, applications and media gateways to the network. The single Aura Services VLAN can be used for non-redundant deployments with a single instance of Avaya Aura Solution for Midsized Enterprises or a fully redundant deployment with multiple instances of Communication Manager, System Manager, Aura Session Manager, Presence Services and Conferencing.

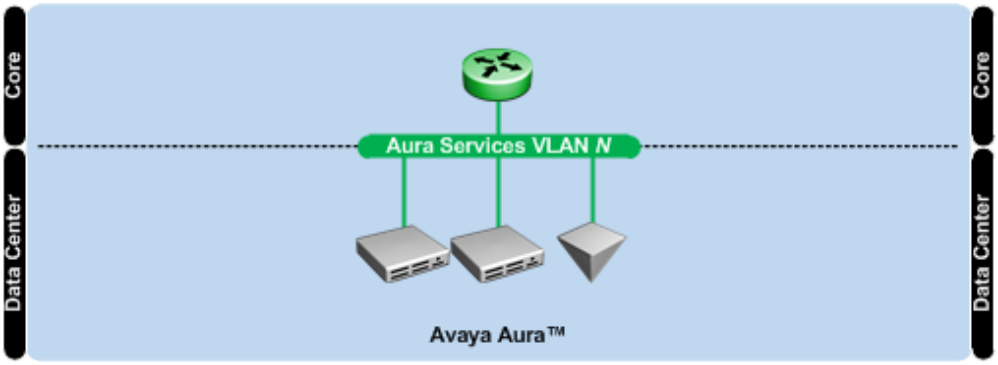


Figure 4.3.2-1 – Single Data Center Example with Aura Services VLAN

For campus deployments with multiple data centers, the Avaya Aura best practice recommendation is to deploy individual Aura Services VLANs in each data center. The data centers can be inter-connected using a traditional WAN, Ethernet interconnects, SPBM or a MPLS service. The Avaya Aura services such as Communication Manager, System Manager and Session Manager as well as various Applications can be distributed between data centers and provide native mechanisms for fail-over. If any component within the data center fails, media gateways and end-points can seamlessly failover to an alternative instance of the service.

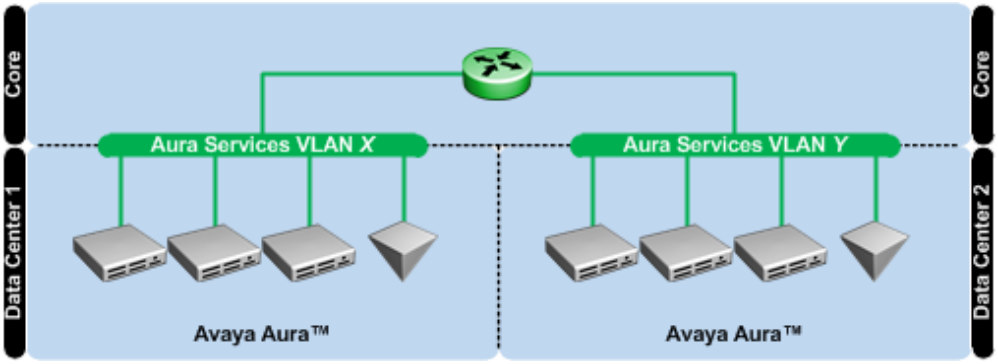


Figure 4.3.2-2 – Dual Data Center Example with Two Aura Services VLANs

Best Practices and Recommendations:

- For a single data center deployment it is recommended that a single Aura Services VLAN be deployed and used to connect all the Aura servers and media gateways to the network.
- For a multiple data center deployments in a single campus, a single Aura Services VLAN may be deployed.
- For a multiple geo-graphically separate data center deployments, it is recommended to deploy individual Aura Services VLANs in each data center.

4.3.3 Shortest Path Bridging MAC

The evolution of Ethernet technologies continues with the IEEE 802.1aq Shortest Path Bridging MAC (SPBM) standard which revolutionizes the design, deployment and operations of data center and campus networks. The benefits of the technology will be clearly evident in its ability to provide massive scalability while at the same time reducing the overall complexity of the network. SPBM brings the features and benefits required by carrier grade deployments to the enterprise market without the complexity of alternative technologies such as MPLS.

SPBM allows administrators to build highly scalable enterprise networks with shared services and applications as well as fully virtualized networks where Virtual Services Networks (VSNs) are created for individual customers, departments or application. The VSNs run over a Virtual Services Fabric (VSF) which is created between Avaya Ethernet Routing Switches using standards based IEEE 802.1aq SPBM. The fabric becomes the backbone of the enterprise network and interconnects the applications and services. The VSF can be enabled in conjunction with existing network infrastructure, making the transition to the fabric non-disruptive and at the pace of the customer. In addition VSNs that run across the fabric are only provisioned on the fabric edge with no changes required in the core of the fabric.

SPBM brings the features and benefits required by Carrier grade deployments to the Enterprise market without the complexity of alternative technologies traditionally used in Carrier deployments (typically MPLS). The IEEE has been actively working on Layer 2 virtualization techniques for over a decade with each subsequent standard addressing the previous standards disadvantages.

Standard	Year	Name	Loop Prevention	Service IDs	Provisioning	Virtualization of
IEEE 802.1Q	1998	Virtual LANs (VLAN Tagging)	Spanning Tree SMLT	4096	Core, Distribution, Access	Layer 2
IEEE 802.1ad	2005	Provider Bridging (QinQ)	Spanning Tree SMLT	4096 x 4096	Core, Distribution, Access	Layer 2
IEEE 802.1h	2008	Provider Backbone Bridging (MacInMac)	Spanning Tree SMLT	16 Million	Core, Distribution, Access	Layer 2
IEEE 802.1aq	Expected 2011	Shortest Path Bridging (SPBM)	IS-IS	16 Million	Only Service Access Points	Layer 2 Layer 3

Table 4.3.3 – Ethernet Virtualization Evolution

Details and best practices for Shortest Path Bridging are provided in the Avaya document titled ***Shortest Path Bridging for ERS 8600 & ERS 8800 Technical Configuration Guide (NN48500-617)*** available for download on https://support.avaya.com/css/Products/P0846/All_Documents.

4.3.3.1 SPBM Global Route Table Shortcuts

SPBM with Global Route Table (GRT) shortcuts allows large scale campus networks to be deployed in a similar manner to how three tier routed networks are built today when IP routing is provided in the core and distribution layers. Applications and services over the shortest path bridging network are not virtualized or isolated and operate over a common IS-IS backbone.

GRT shortcuts provide IP routing between Aura Services and Converged VLANs and no virtual services networks (VSNs) or virtual router forwarders (VRFs) are used. IP is enabled globally via SPBM on the backbone edge bridge (BEB) switches with some method of route redistribution into IS-IS (i.e. direct, static, BGP, OSPF or RIP) which provides IP forwarding of traffic between BEBs over the IS-IS backbone. You can also enable SPB IP globally on the backbone core bridges (BCB) if you wish to manage the BCBs via the GRT routing table.

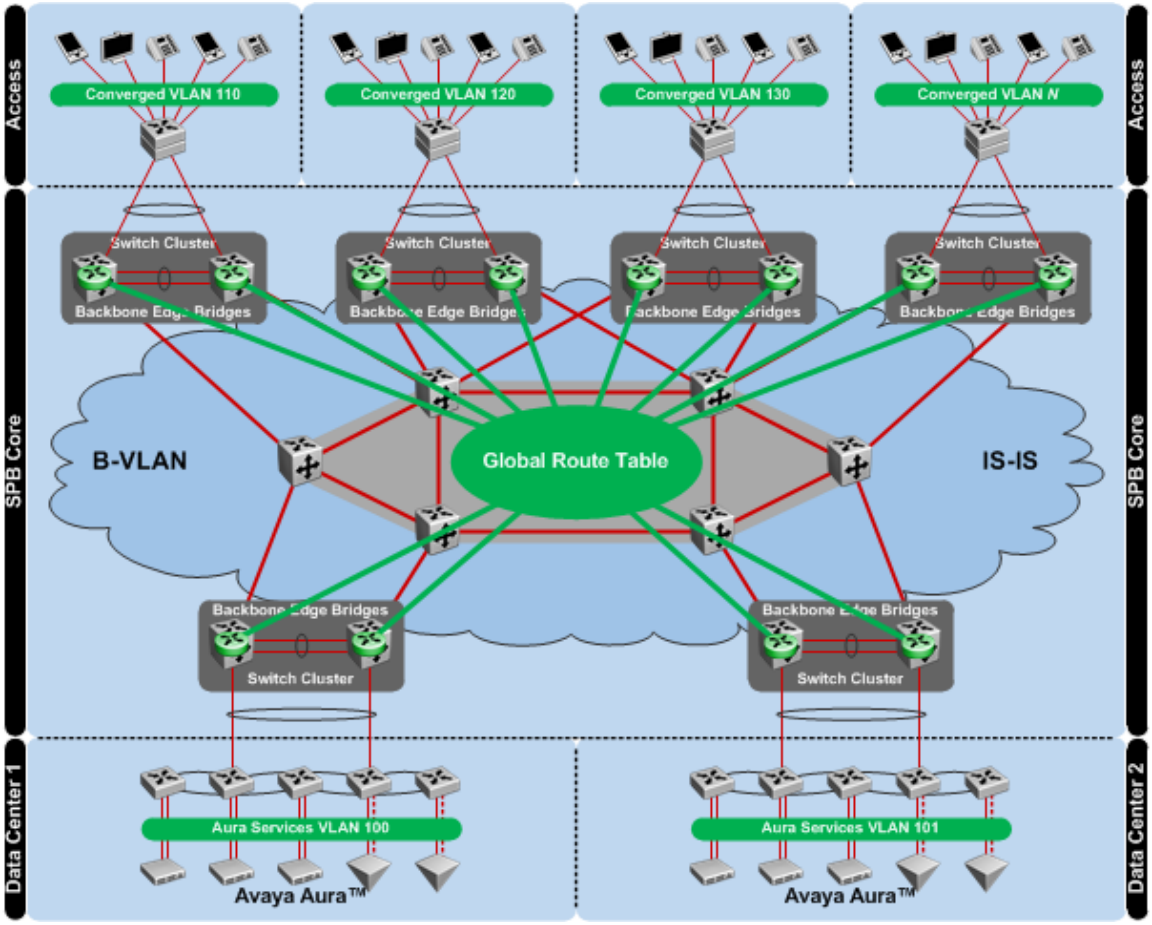


Figure 4.3.3.1 – GRT Shortcuts

Availability for the access and data center layers is provided by deploying a cluster of BEBs and connecting the access layer and data center switches to the BEBs switch cluster using SMLT. Default gateway redundancy for each Aura Services and Converged VLAN is provided by deploying VRRP or RSMLT Edge for each VLAN terminated on the BEB cluster.

4.3.3.2 SPBM Layer 2 Virtual Services Networks (L2VSN)

A SPB L2 VSN topology is simply made up of a number of Backbone Edge Bridges (BEB) used to terminate Layer 2 VSNs. The control plane uses IS-IS for forwarding at a Layer 2 level. Only the BEB bridges are aware of any VSN and associated MAC addresses while the backbone bridges simply forward traffic at the Backbone MAC (B-MAC) level. The backbone switches will know how to reach every B-MACs using the shortest path determined by IS-IS. All switches in the backbone will only learn B-MAC addresses to make forwarding decisions while the BEB will learn both the B-MACs and Customer MACs (C-MAC) for each VSN.

A Backbone Service Instance Identifier (I-SID) will be assigned on the BEB to each VLAN. All VLANs in the network that share the same I-SID will be able to participate in the same VSN. If SMLT clusters are used, two backbone VLANs (B-VLAN) are required with a primary B-VLAN and a secondary B-VLAN. In general two backbone VLANs should always be used (even if no SMLT cluster is in use) since the use of 2 backbone VLANs allows IS-IS to compute equal cost trees. If 2 shortest equal cost paths exist, SPBM will load balance VSN traffic across both paths.

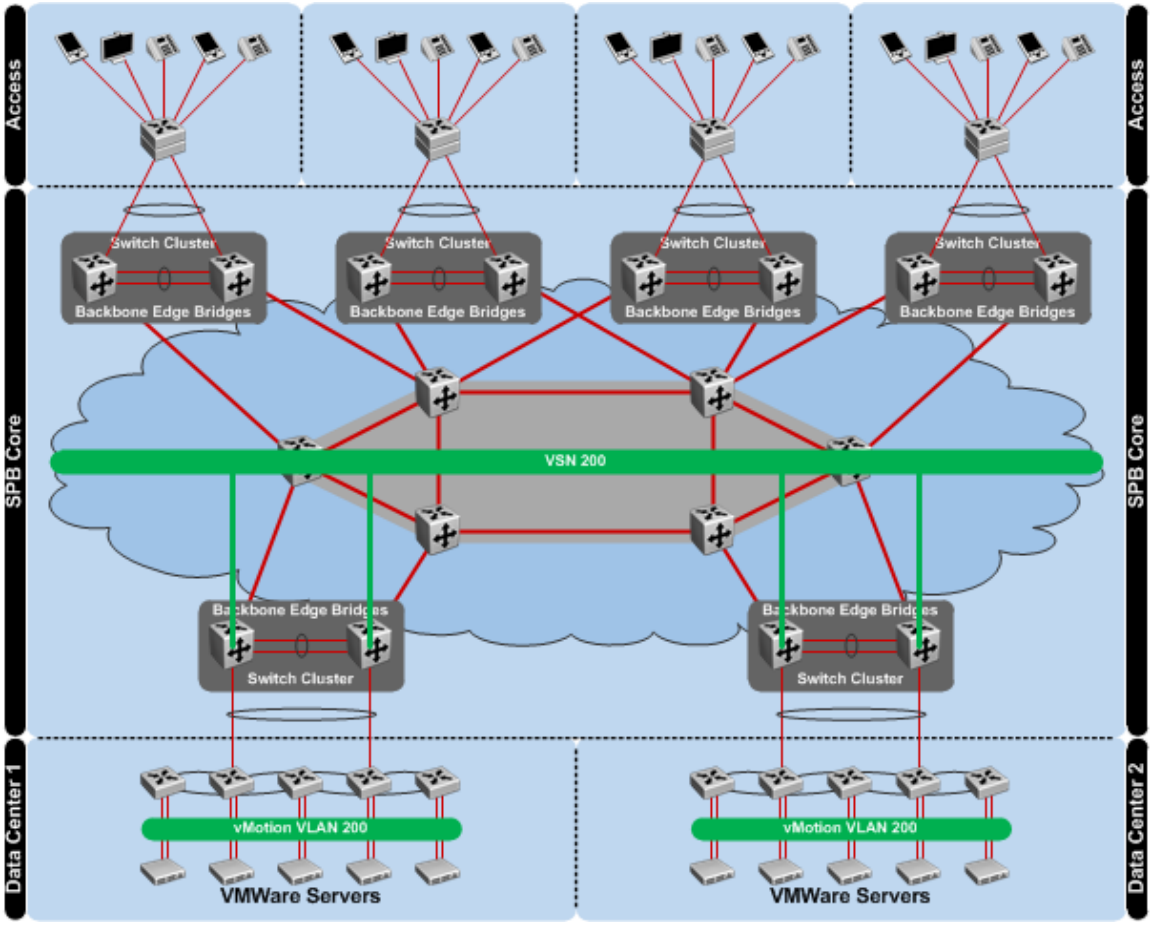


Figure 4.3.3.2 – Layer 2 Virtual Service Networks

L2VSN services are used whenever you wish to simply provide Layer 2 services across an IS-IS core. A good example would be to provide VMware vMotion between two separate data centers. vMotion requires that the ESX servers providing the vMotion service be on the same subnet. This requirement can easily be meet using a L2VLSN between the data centers. However Layer 2 services do not apply to Avaya Aura or the Avaya Desktop Video Devices and is only mentioned to provide context for the other available SPBM services.

4.3.3.3 SPBM Layer 3 Virtual Services Networks (L3VSN)

SPBM with layer 3 virtual services networks (VSNs) provides a logical topology similar to GRT shortcuts but adds support for network virtualization. With layer 3 VSNs, a Backbone Service Instance Identifier (I-SID) will be assigned at a Virtual Router (VRF) level. Any number of VLANs where each VLAN will can contain over-lapping addresses used in other VRF instances or the GRT be assigned to this VRF. All VRFs in the network that share the same I-SID will be able to participate in the same VSN.

IS-IS within the SPBM is used to forward traffic between the BEBs and BCBs. Traffic is forwarded based on the B-MAC (System-ID) where each switch has a unique B-MAC address. The SPBM IPVSN Reachability TLV 184 is used to distribute IPVSN reachability between IS-IS peers. It is possible to forward traffic between VRFs using redistribution policies.

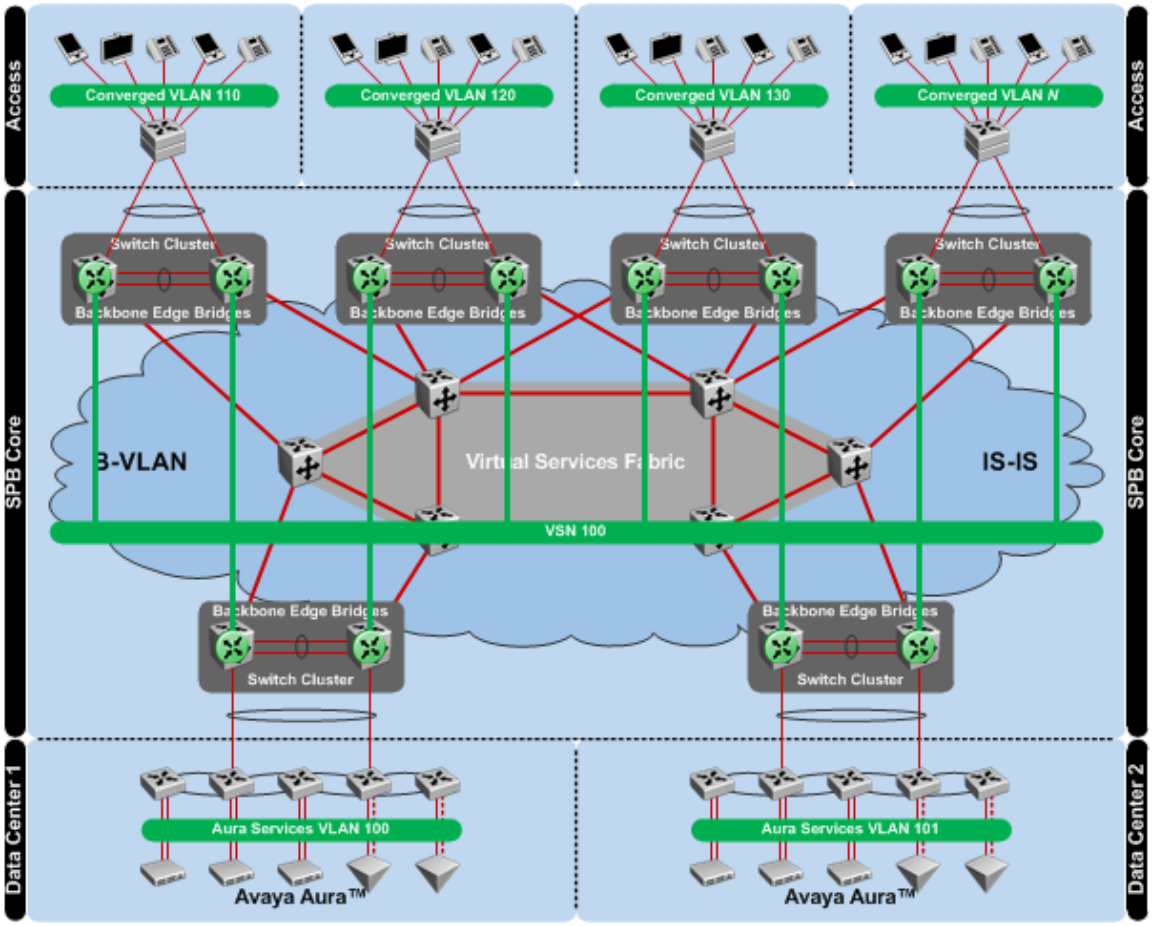


Figure 4.3.3.3 – Layer 3 Virtual Service Networks

Availability for the access and data center layers is provided by deploying a cluster of BEBs and connecting the access layer and data center switches to the BEBs switch cluster using SMLT. Default gateway redundancy for each Aura Services and Converged VLAN is provided by deploying VRRP or RSMLT Edge for each VLAN on the BEB cluster.

Layer 3 VSNs isolate the Aura Services and Converged VLANs from other Layer 3 VSNs. If communication between layer 3 VSNs or other VRFs is required, VRFs can be interconnected using external layer 3 devices, firewalls or by leaking routes between VRFs.

4.3.3.4 SPBM Inter VSN Routing

Layer 2 VSNs (L2VSN) by default are used to tunnel Layer 2 traffic across an SPBM core where there is a one-to-one mapping of a single VLAN to a Backbone Service Instance Identifier (I-SID). All L2VSNs in the network that share the same I-SID will be able to participate in the same VSN.

Inter VSN allows routing between IPv4 networks on Layer 2 VLANs. Inter VSN can be performed via GRT or via a VRF. If GRT, simply add an IP address to the L2 VLAN on a BEB switch. Or for redundancy, enable IP on two or more BEB switch that terminate the L2VSN and run VRRP between them. Inter VSN can also be performed by simply creating a VRF anywhere in the network (BEB or BCB), adding two or more I-SID values used on each L2VSN service to this VRF instance, and adding a corresponding IP address to each VLAN instance to be used for IP routing. For redundancy, Inter VSN can also be configured on another switch with VRRP to eliminate a single point of failure.

With inter-VSN routing Aura Services and Converged VLANs terminate on BEBs which map the individual VLANs into VSNs. Routing between the VSNs if using virtual router forwarders (VRFs) as shown below, are deployed on the BEBs or backbone core bridges (BCBs) that terminate the VSNs and use VRRP for added resilience.

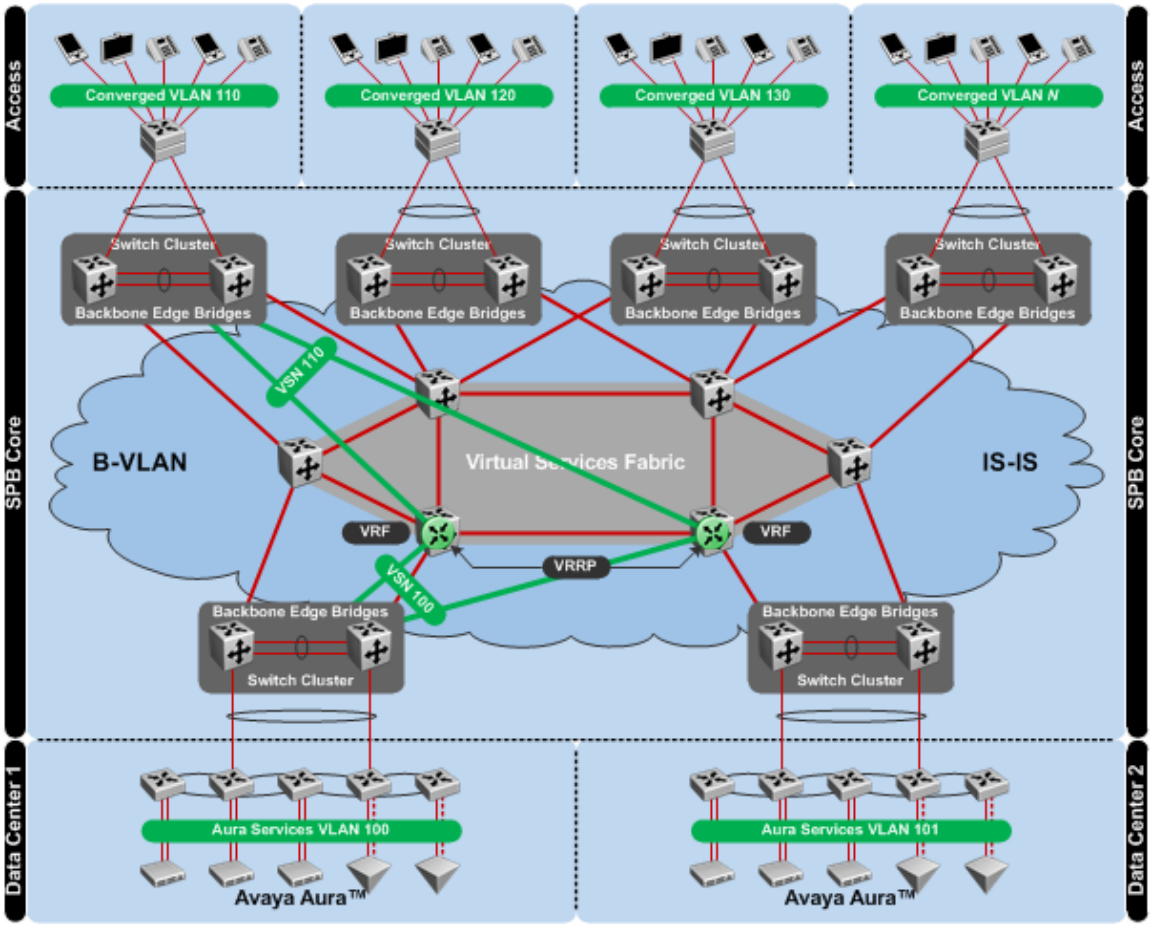


Figure 4.3.3.4 – Inter VSN Routing

Availability for the access and data center layers is provided by deploying a cluster of BEBs and connecting the access layer and data center switches to the BEBs switch cluster using SMLT. Default gateway redundancy for each Aura Services and Converged VLAN is provided by deploying VRRP

between VRFs terminating the VSNs in the BCB core. Two VRFs are necessary in the core to provide default gateway redundancy.

Like layer 3 VSNs, inter-VSN routing isolates the Aura Services and Converged VLANs from other applications and services in the network. The VRF only provides IP routing between the VSNs it terminates. If IP communications are required between VLANs serviced by other VRFs, the VRFs can be interconnected using external layer 3 devices, firewalls or by leaking routes between VRFs.

4.3.4 Wireless LANs

The Wireless LAN 8100 system can be deployed today as traditional overlay solution where the AP 8120 Access Points will transport all the wireless user traffic to a WC 8180 Wireless Controller located in the data center but physically connected to the core. The VLANs clients are assigned is determined by the Network Profile configuration on the WC 8180 Wireless Controllers for each wireless service. Users and devices can either be assigned to a static VLAN determined by the Network Profile or alternatively when AAA is authenticating a session a dynamic VLAN assigned by the AAA server.

4.3.4.1 Network Profiles

Network Profiles define the wireless services that the Wireless LAN 8100 system supports. Each Network Profile defines the Service Set Identifier (SSID) name advertised to wireless users as well as the encryption / authentication options, static VLAN membership and QoS support. The Network Profiles are assigned to groups of 2.4 GHz and/or 5 GHz radios servicing wireless clients using Radio Profiles.

Each Wireless LAN 8100 system can support multiple Network Profiles which can be configured to support specific devices or applications and each site will typically include separate Network Profiles tailored to support converged communications, corporate users and if required guest user access. Additional Network Profiles may be deployed to support legacy devices that cannot support the latest encryption and authentication standards or require a dedicated VLAN.

The Avaya Desktop Video Device includes a 2.4 GHz 802.11n radio and supplicant that supports the latest 802.11i encryption and authentication standards. Avaya Desktop Video Devices can connect to wireless services supporting WPA2 with pre-shared keys as well as wireless services with WPA2 requiring EAP authentication. The Avaya Desktop Video Device also supports legacy WEP and WPA authentication and encryption schemes; however for security and 802.11n standards support it is recommended that a Converged Network Profile using WPA2 with pre-shared keys or EAP be deployed.

To support the Avaya Desktop Video Devices it is recommended that one Converged Network Profile be defined with CCMP encryption that supports either pre-shared key or EAP authentication. The Converged Network Profile can support the Avaya Desktop Video Devices as well as Avaya handsets, Polycom handsets and Vocera badges. As the Avaya Desktop Video Devices do not support 5 GHz operation, the Converged Network Profile must be assigned to a Radio Profile supporting 2.4 GHz radios at the site.

Parameter	Value
Name	User Defined Value
SSID	User Defined Value
Hide SSID	No
Mobility VLAN Name	Converged VLAN Name
Security Mode	WPA-Personal OR WPA-Enterprise
WPA Version	WPA2
WPA Encryption	CCMP
Client QoS	Enabled

Table 4.3.4.1 – Converged Network Profile

Best Practices and Recommendations:

- It is recommended that each Converged Network Profile be configured to support WPA2 with pre-shared keys or EAP authentication.
- The Converged Network Profile must be assigned to a Radio Profile supporting 2.4 GHz radios.
- If pre-shared key authentication is utilized, it is recommended that the passphrase include a minimum of 20 random characters.
- If EAP authentication is utilized, a RADIUS Authentication Profile must be defined.

4.3.4.2 Virtual LANs

The WC 8180 Wireless Controller assigns wireless users connected to an SSID to a mobility VLAN based on the static mobility VLAN name assigned to the network profile or a dynamic mobility VLAN name assigned from the AAA server. If a Converged Network Profiles is deployed using WPA2 pre-shared key authentication, VLAN membership is assigned using the mobility VLAN name assigned to the Network Profile. If a Converged Network Profile is deployed using WPA2 with EAP authentication, VLAN membership can be assigned using the mobility VLAN name assigned to the Network Profile or a mobility VLAN name assigned from the AAA server. In the case where a VLAN name is provided by both sources, the VLAN name from the AAA server will take precedence.

If the assigned mobility VLAN is local to the WC 8180 Wireless Controller, the WC 8180 Wireless Controller will switch the wireless user traffic locally out of its GE or 10GE ports where the mobility VLAN is assigned. If the mobility VLAN is not local, the WC 8180 Wireless Controller will tunnel the wireless user traffic over a mobility tunnel to a peer WC 8180 Wireless Controller where the mobility VLAN resides.

Whenever possible it is recommended to deploy a single Network Profile and Converged VLAN which is extended to each WC 8180 Wireless Controller in the data center. This provides seamless mobility by allowing the converged devices to roam seamlessly between Access Points throughout the campus site while maintaining VLAN membership. In additional this provides VLAN redundancy as the Converged VLAN is local to all WC 8180 Wireless Controllers in the data center providing a network path in the event of a single WC 8180 Wireless Controller failure while eliminating mobility tunneling.

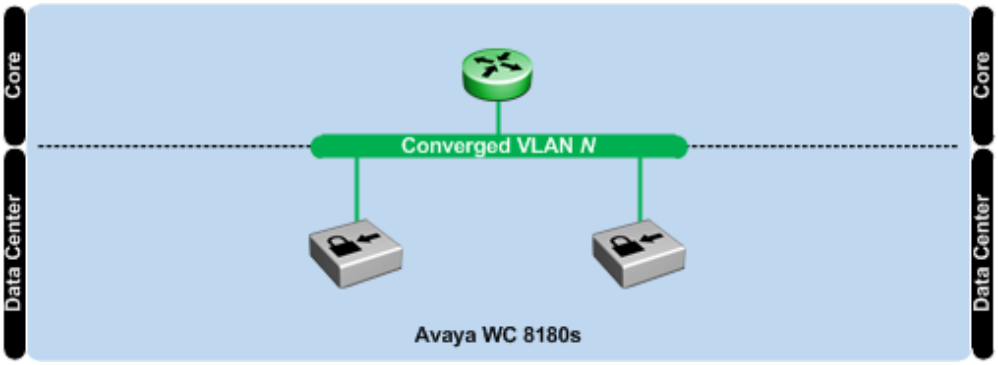


Figure 4.3.4.2-1 – Data Center Example with One Wireless Converged VLAN

If a large number of Avaya Desktop Video Devices are deployed or WC 8180 Wireless Controllers are distributed across multiple data centers, it may be necessary to deploy additional Network Profiles and Wireless Converged VLANs. A unique Network Profile and Converged VLAN can be deployed in each data center with a common SSID name to permit mobility between the Access Points managed by WC 8180 Wireless Controllers in each data center. If WPA2 with EAP authentication is deployed, Avaya Dekstop Video Devices can also be dynamically placed into Wireless Converged VLANs from the AAA server permitting a single Network Profile to be deployed in both data centers. Additional features such as ARP Suppression may also be enabled in the Network Profile to eliminate un-necessary broadcast traffic on the wireless medium.

When multiple Converged VLANs are deployed it is strongly recommended that each Wireless Converged VLAN be extended to at least two WC 8180 Wireless Controllers in the mobility domain so that each VLAN is available in the event that a single WC 8180 Wireless Controller becomes unavailable. If the Wireless Converged VLAN is only local to one WC 8180 Wireless Controller in the mobility domain, user traffic cannot be forwarded to the wired network if the WC 8180 Wireless Controller terminating the mobility VLAN fails.

When multiple Wireless Converged VLANs are deployed, wireless user traffic maybe tunneled between WC 8180 Wireless Controllers within the mobility domain. This provides seamless mobility to Avaya Desktop Video Devices as they roam between AP 8180 Access Points managed by different WC 8120 Wireless Controllers.

If the AP 8120 Access Points are managed by WC 8180 Wireless Controllers in different data centers and the mobility VLANs are unique, it is important to ensure that adequate bandwidth be available between the data centers to support the mobility traffic and latency is low. If bandwidth is constrained or the latency is high, you may want to consider managing all the AP 8120 Access Points in a single data center where the other data center maintains standby controllers. This allows mobility tunneled traffic to be switched locally within the data center rather than being tunneled over congested or high latency links between the data centers.

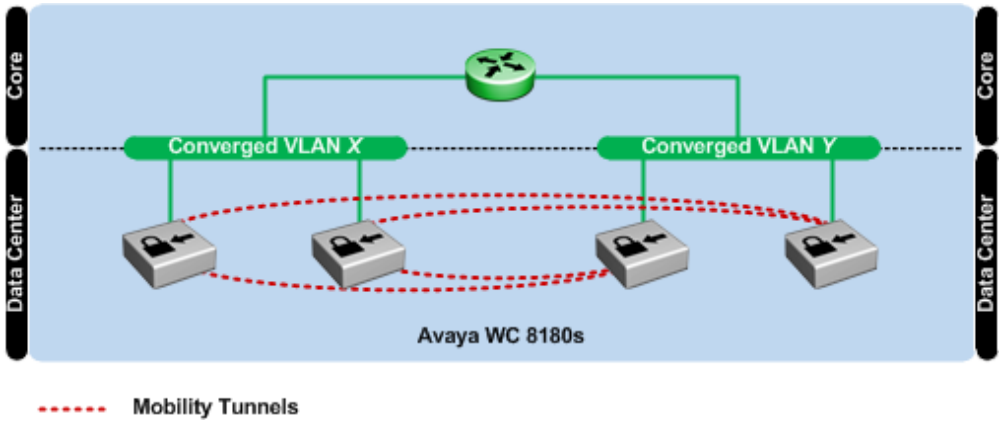


Figure 4.3.4.2-2 – Data Center Example with Multiple Wireless Converged VLANs

Best Practices and Recommendations:

- Whenever possible it is recommended that a single Wireless Converged VLAN be deployed in the data center that is extended to all WC 8180 Wireless Controllers in the data center.
- If multiple Wireless Converged VLANs are deployed, for availability it is recommended that each Wireless Converged VLAN be extended to at least two WC 8180 Wireless Controllers in the mobility domain.
- When AP 8120 Access Points are managed by WC 8180 Wireless Controllers across multiple data centers, it is strongly recommended that low latency high bandwidth links be available between the data centers to support any mobility traffic that may be tunneled between the data centers.
- To reduce unnecessary ARP broadcast traffic from being flooded onto the wireless medium, consider enabling ARP Suppression in the network profiles.

4.3.5 Default Gateway Redundancy

Each Aura Services and Converged VLAN will require a virtual IP interface to provide Inter VLAN routing to allow Avaya Desktop Video Devices to communicate with other Avaya Desktop Video Devices as well as Avaya Aura applications, services and media gateways deployed in the data center. Deployments that follow Avaya's small, medium, large or super large campus reference architectures will typically perform IP routing at the switch cluster located in the core of the network, however in some larger networks routing be provided at the distribution or access layers.

Default gateway redundancy should be enabled on each switch cluster that is providing IP routing services to the access and data center layers to ensure that the default gateway is always available to hosts in the event of outage. Default gateway redundancy can be provided using the industry standards based VRRP protocol with Avaya's backup master extensions or Avaya's routed split multilink trunking (RSMLT) edge protocol. Both VRRP and RSMLT edge protocols provide sub-second failure detection and recovery in the event of a switch failure allowing IP traffic to be routed with no interruption to the end user. In addition Avaya innovations further enable both switches to actively route IP traffic ensuring both switches are operating to their full potential and are not sitting idle.

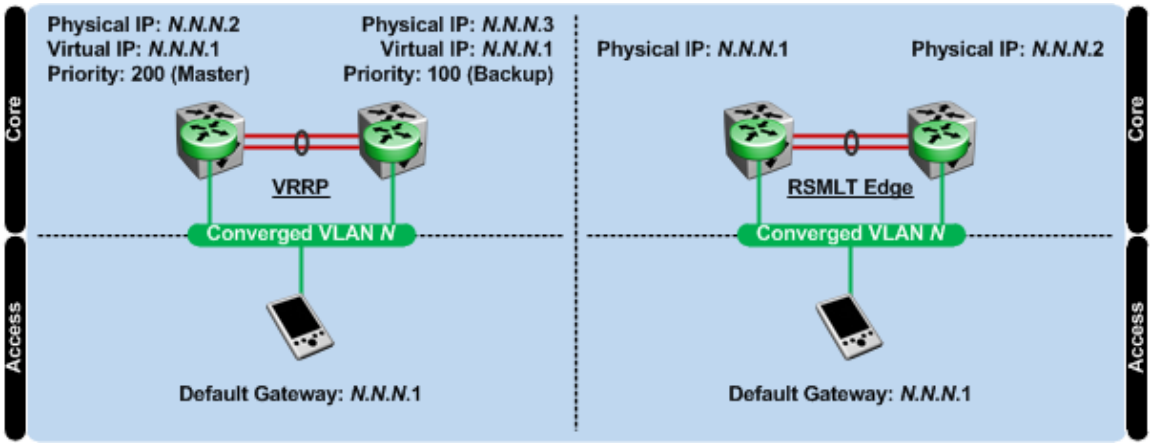


Figure 4.3.5 – Default Gateway Redundancy

Best Practices and Recommendations:

- Each VRRP instance requires two real IP addresses and one virtual IP address to be allocated per Aura Services and Converged VLAN.
- Each VRRP instance requires a unique VRRP id to be allocated.
- For IP load-sharing, each VRRP instance requires backup / master extensions to be enabled.
- Each RSMLT edge requires two real IP addresses to be allocated per Aura Services and Converged VLAN.
- Each RSMLT edge instance requires the hold-up timer to be set to infinity (9999).

4.3.6 Dynamic Host Configuration Protocol (DHCP)

For plug and play deployments Avaya IP Phones and Avaya Desktop Video Devices require dynamic host configuration protocol (DHCP) services to be available on each Converged VLAN to provide the devices with the necessary network information to allow the devices to communicate over the network. Avaya IP Phones and Desktop Video Devices require basic network information such as IP addressing, default gateway, domain name system (DNS) servers and domain name and optionally can be supplied with Avaya vendor specific information which can supply VLAN information as well as configuration file locations.

While a DHCP server can be deployed locally on each Converged VLAN, most enterprises will prefer to deploy a centralized DHCP server in the data center to simplify administration and management as well as minimize the cost of server hardware. In such configurations DHCP relay must be enabled on the Avaya Ethernet Routing Switches providing IP routing services in order to forward DHCP requests from hosts to the centralized DHCP server. DHCP relay is supported by all Avaya Ethernet Routing Switch platforms.

The centralized DHCP server must be configured with a DHCP scope and options for each Converged VLAN that it serves. When a host on a Converged VLAN requests an IP address, the DHCP relay agent on the core cluster of Avaya Ethernet Routing Switches will forward the DHCP Requests as unicast packets to the centralized DHCP server. The DHCP server determines which address pool to assign addressing information from based on the source IP address of the relay agent. The DHCP server matches the DHCP relay IP address to the address range of a DHCP scope then provides a DHCP Offer to the host from the appropriate DHCP scope.

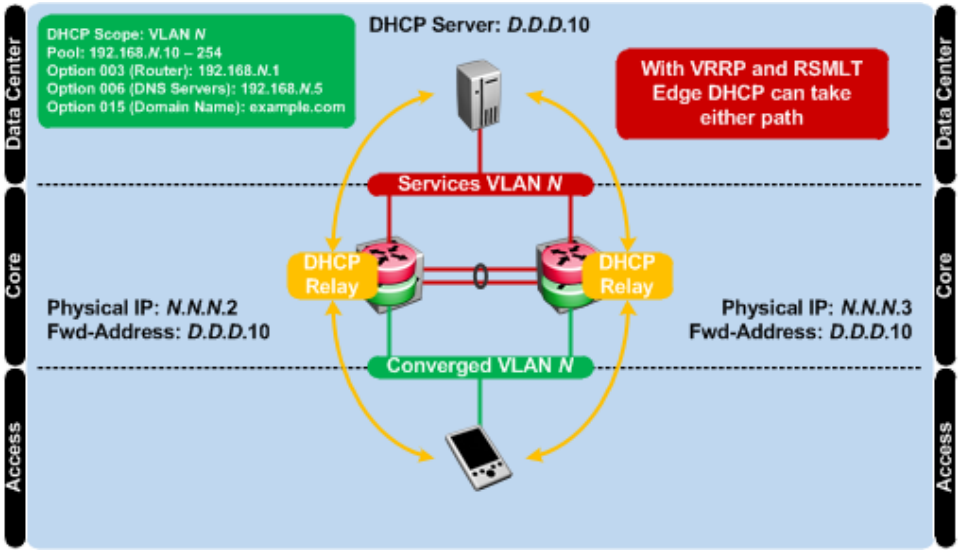


Figure 4.3.6 – DHCP Relay

Best Practices and Recommendations:

- A DHCP scope must be defined for each wired and wireless Converged VLAN.
- When enabling DHCP relay with VRRP, the DHCP relay agent must be assigned to each physical IP interface on the core Avaya Ethernet switch and not the virtual IP address.
- When enabling DHCP relay with RSMLT edge, the DHCP relay agent must be assigned to each physical IP interface on the core Avaya Ethernet switch.

4.4 Discovery and Configuration

Device provisioning has evolved over the years and Avaya now offers several methods that can be deployed in a campus environment (independently or together) to automatically detect Avaya IP Phones and Avaya Desktop Video Devices when they are connected to the network, automatically provision VLAN and QoS trust on the access layer ports and automatically configure the Avaya IP Phones and Avaya Desktop Video Devices. Manual provisioning is also supported, however this adds additional configuration and management overhead and introduces the opportunity for configuration errors.

4.4.1 Automatic Access Layer Port Provisioning

Automatic discovery and provisioning provides enterprises with the means for allowing the network infrastructure to automatically detect the Avaya Desktop Video Devices as they are connected to the network then automatically provision VLAN, QoS trust and device settings on the access layer ports the devices are connected to. This greatly simplifies new deployments as well as eliminates the IT overhead associated with performing moves, adds and changes (MAC).

For automatic port provisioning the Avaya Ethernet Routing Switches supports Auto Detect Auto Config (ADAC) which can be enabled on all access layer ports to automatically detect Avaya IP Phones and Avaya Desktop Video Devices as they are connected to an Avaya Ethernet Routing Switch. ADAC can detect devices using MAC address or IEEE 802.1AB Link Layer Discovery Protocol (LLDP) and can provision the port with an 802.1Q tagged or untagged Converged VLAN, untagged Data VLAN and trust QoS markings from the Avaya Desktop Video Device simplifying QoS configuration.

LLDP is not currently supported by the Avaya Desktop Video Device and will be added in a future firmware release.

Device	ADAC with MAC Detection	ADAC with LLDP Detection
Avaya Desktop Video Device	Yes	No (Future Firmware Release)
Avaya IP Phones	Yes	Yes

Table 4.4.1-1 – ADAC Detection Support

When deploying Avaya Desktop Video Devices in existing Avaya IP Phone environments, it is recommended that the ADAC be enabled on all access layer ports with the operation mode set to tagged-frames. This provides a full plug-n-play environment that allows both Avaya IP Phones and Desktop Video Devices to co-exist while simultaneously supporting data devices. Avaya IP Phones and Desktop Video Devices register and communicate using the 802.1Q tagged Converged VLAN while data devices connected to Avaya IP Phones or directly to an access layer port will communicate using the untagged Data VLAN. This ADAC implementation allows an enterprise to identically configure all the access layer ports in the wiring closet and can support individual data devices, individual IP Phones and Avaya Desktop Video Devices as well as IP Phones with data devices connected.

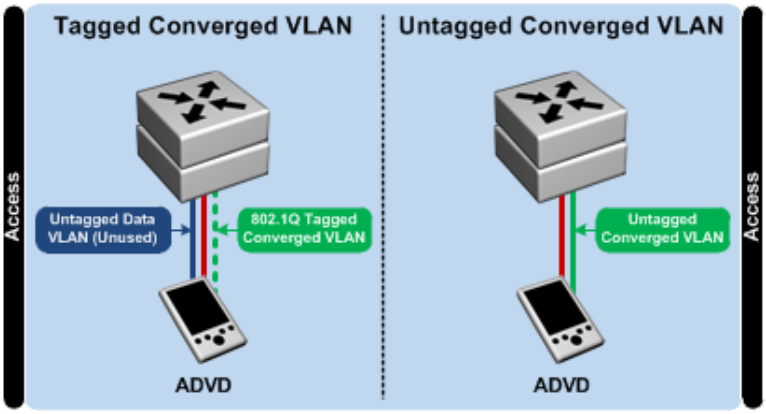


Figure 4.4.1.1 – Avaya Desktop Video Device VLAN Options

For greenfield deployments with no existing Avaya IP Phones, an alternative deployment strategy is to configure ADAC to support an untagged Converged VLAN. When an Avaya Desktop Video Device is connected to an Avaya Ethernet Routing Switch port it will be automatically provisioned with an untagged Converged VLAN. Data devices connected an access layer port will be automatically provisioned with an untagged Data VLAN. This ADAC implementation can support individual Avaya IP Phones, Avaya Desktop Video Devices as well as data devices but will not permit separate Converged and Data VLANs to be simultaneously supported on an access layer port.

To implement the automatic detection of Avaya Desktop Video Devices using ADAC, the Avaya Ethernet Routing Switches must be configured with a list of device MAC addresses which are assigned to the Avaya Desktop Video Devices. Currently Avaya has allocated two blocks of MAC address to the Avaya Desktop Video Devices which are assigned to Ethernet, 802.11n and Bluetooth interfaces. These MAC address ranges must be defined on all the access layer switches for ADAC to be able to successfully detect the Avaya Desktop Video Devices.

MAC Address Start	MAC Address End
00-1B-4F-4C-E1-A5	00-1B-4F-4D-56-D4
B4-B0-17-7A-90-00	B4-B0-17-7C-1F-FF

Table 4.4.1-2 – ADVD MAC Address Range

Best Practices and Recommendations:

- Whenever possible it is recommended that ADAC be enabled on all access layer ports and configured to support 802.1Q tagged Converged VLANs. This allows both the Avaya IP Phones and Avaya Desktop Video Devices to be deployed in the enterprise using a common Converged VLAN but also supports data devices that are connected to Avaya IP Phones or directly to the access layer ports.
- For ADAC to be able to successfully detect the Avaya Desktop Video Devices, the ADAC MAC address table must be updated to include the Avaya Desktop Video Devices MAC address ranges.
- The ADAC Voice VLAN should be assigned to the Converged VLAN ID.

4.4.2 Manual Access Layer Port Provisioning

If automatic provisioning is not desired, it is recommended that all access layer ports be manually configured with an 802.1Q tagged Converged VLAN and an untagged Data VLAN. Configuring the access layer ports in this manner allows the access layer ports to support either Avaya Desktop Video Devices or data devices without re-configuration.

Alternatively each access layer port can be manually configured with an untagged Converged or Data VLAN. However this strategy forces each port into individual role which can either support data devices or Avaya IP Phones or Avaya Desktop Video devices. This approach can be more costly to manage and requires re-configuration if devices are moved or exchanged.

Manually provisioning the access layer ports also requires a QoS strategy to be considered. ADAC allows the access layer ports to automatically trust the QoS markings for the Converged VLAN from the Avaya Desktop Video Devices as they are discovered on a port. Manually provisioning the access layer ports requires the decision to be made as to trust or un-trust the QoS markings made by the end device since the identity of the device (Avaya IP Phone, Avaya Desktop Video Device, malicious user laptop, etc.) connected to the port isn't truly known or established through the trust model of ADAC.

When access layer ports are manually provisioned with an 802.1Q tagged Converged VLAN and an untagged Data VLAN it is recommended that all access layer ports be un-trusted (default) and QoS policies be deployed which will classify and mark audio, control and video traffic as it ingresses the Avaya Ethernet Routing Switch. If the access layer ports are configured with an untagged Converged VLAN, each port can be placed into a specific role (i.e. Converged or Data) which permits audio, control and video markings to be trusted if desired.

Please reference Section 4.5 for recommendations and best practices for implementing QoS to support Avaya Desktop Video Devices.

Best Practices and Recommendations:

- If ADAC is note implemented, it is recommended that all access layer ports be manually configured with an 802.1Q tagged Converged VLAN and an untagged Data VLAN. This allows the access layer ports to support data or Avaya Desktop Video Devices without re-configuration. The access layer port must be configured to untag the Data VLAN.
- When deploying an 802.1Q tagged Converged VLAN it is recommended that QoS be untrusted and QoS policies deployed that classifies and marks audio, control and video traffic as it ingresses the Avaya Ethernet Routing Switch access layer ports.

4.4.3 Dynamic Host Configuration Protocol (DHCP)

Each Avaya Desktop Video Device requires IP addressing and certain network information so that it can communicate over the IP network and register with the Avaya Aura services and applications in the data center. Each Avaya Desktop Video Device can be manually provisioned with IP addressing, VLAN and SIP configuration which requires each device to be staged before deployment. Alternatively for plug-n-play deployments each Avaya Desktop Video Device can be fully provisioned using Dynamic Host Configuration Protocol (DHCP) and a centralized HTTP/HTTPS server.

DHCP allows administrators to fully deploy new Avaya Desktop Video Devices without pre-staging or pre-configuration. DHCP scope options can be enabled to assign network parameters such as IP address, subnet mask, default gateway and DNS along with the Converged VLAN ID and Ethernet port tagging configuration. In addition DHCP can supply the Avaya Desktop Video Devices with a HTTP/HTTPS server IP address, port and directory where the devices configuration and firmware resides. Using DHCP and HTTP/HTTPS together allows the Avaya Desktop Video Devices to be quickly and easily deployed with zero touch while providing consistency between the device configurations.

DHCP Option	Description
003 (Router)	Default gateway IP Address on the Access Layer VLAN.
006 (DNS Servers)	One or more Name server IP addresses.
015 (Domain Name)	Organizations Domain Name.
242 (Vendor Specific)	Avaya Vendor Specific DHCP options and values provided as a comma separate string to the Avaya Desktop Video Devices: ▪ HTTPSRVR – IP Address or hostname of the HTTP Server ▪ HTTPDIR – HTTP server path to pre-append to all configuration and data files. ▪ HTTPPORT – Destination port of the HTTP server (Default = 80) ▪ L2Q – 802.1Q Tagging Mode (0 = Automatic, 1 = On, 2 = Off) ▪ L2QVLAN – 802.1Q Tagged Converged VLAN ID (0 = Untagged, 1-4094 = Tagged) ▪ PROCPSWD – Local Administrative Password (Default = 27238) ▪ SIP_CONTROLLER_LIST – One or more SIP / Proxy Server IP Addresses or hostnames. ▪ SNTPSRVR – IP Address or hostname of the SNTP Time Server ▪ TLSSRVR – IP Address or hostname of the HTTPS Server ▪ TLSDIR – HTTPS server path to pre-append to all configuration and data files. ▪ TLSPORT – Destination port of the HTTPS server (Default = 443) ▪ VLANTEST – Number of seconds to wait for a DHCP offer on a non-zero VLAN (Default = 60 Seconds)

Table 4.4.3 – Example ADVD DHCP Options

Please refer to http://support.avaya.com for the latest Avaya Desktop Video Device configuration file.

The Avaya Desktop Video Device supports the same VLAN deployment options as Avaya IP Phones and can be connected to an Avaya Ethernet Routing Switch port that is manually or automatically provisioned with an 802.1Q tagged Converged VLAN or an untagged Converged VLAN. This allows the Avaya Desktop Video Devices to be easily deployed in existing Avaya IP Phone or greenfield environments regardless if manual or automatic port provisioning is enabled or if a tagged or untagged Converged VLAN is deployed.

4.4.3.1 DHCP with 802.1Q Tagged Converged VLAN

When the Avaya Desktop Video Device is connected to an access layer port provisioned with an 802.1Q tagged Converged VLAN and an untagged Data VLAN, the Avaya Desktop Video Device uses DHCP scope options assigned to the Data VLAN to discover the Converged VLAN ID. The Avaya Desktop Video Device will then transition to the Converged VLAN and use DHCP scope options to obtain its device configuration and firmware.

The Avaya Desktop Video Device uses the following DHCP process:

1) The Avaya Desktop Video Device will broadcast a DHCP discover packet on to the untagged Data VLAN which is relayed by the network to a centralized DHCP server.
2) The DHCP server will respond with an IP address and standard options from the Data VLAN scope with Avaya DHCP option 242 that enables 802.1Q tagging and provides the Converged VLAN ID.

Example Data VLAN Scope Options:

```
L2Q=1,L2QVLAN=110,VLANTEST=60
```

3) The Avaya Desktop Video Device will transition its Ethernet port to the Converged VLAN ID and broadcast a second DHCP discover packet on to the 802.1Q tagged Converged VLAN.
4) The DHCP server will respond with an IP address and standard options from the Converged VLAN scope with Avaya DHCP option 242 that provides the HTTP/HTTPS server IP address and path where the firmware and device configuration file resides.

Example Data VLAN Scope Options:

```
HTTPSRVR=192.168.10.20,HTTPDIR=ADVD/
```

5) If necessary the Avaya Desktop Video Device will download the latest firmware from the centralized HTTP/HTTPS server.
6) Once the firmware is current, the Avaya Desktop Video Device will download the device configuration file from the centralized HTTP/HTTPS server and will register with the Avaya Aura SIP services in the data center.

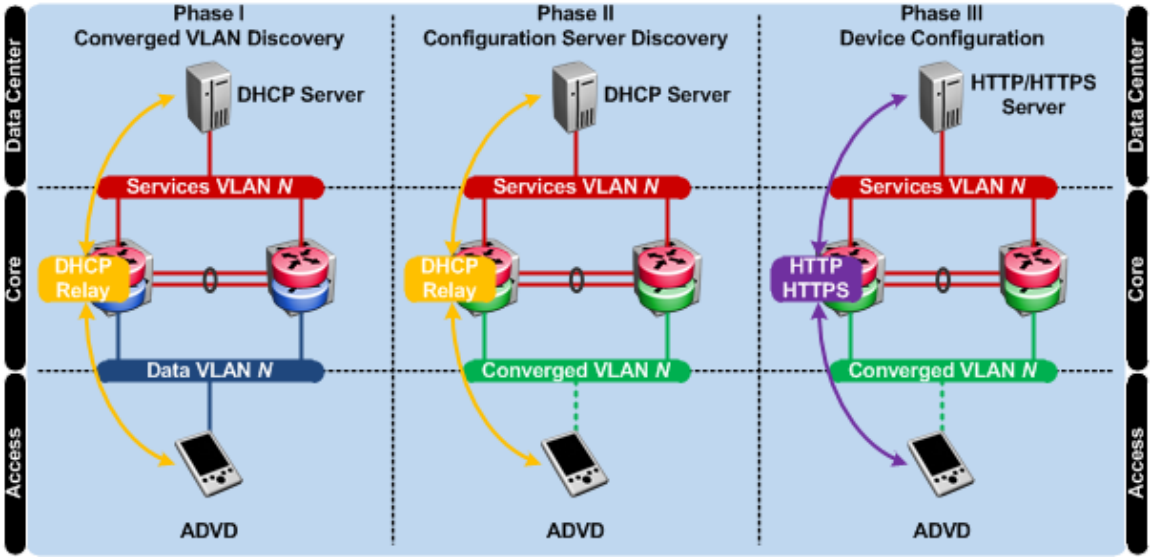


Figure 4.4.3.1 – DHCP with 802.1Q Tagged Converged VLAN

Best Practices and Recommendations:

- For Converged VLAN discovery, each Data VLAN scope must be provisioned to include Avaya Option 242 which configures the Ethernet port for 802.1Q tagging and defines the Converged VLAN ID.
- Each Converged VLAN scope must be provisioned to include Avaya Option 242 which provides the HTTP/HTTPS server IP Address and Path where the device firmware and configuration files reside.

4.4.3.2 DHCP with Untagged Converged VLAN

When the Avaya Desktop Video Device is connected to an access layer port provisioned with an untagged Converged VLAN, the Avaya Desktop Video Device uses DHCP scope options directly assigned to the Converged VLAN to obtain its device configuration and firmware.

The Avaya Desktop Video Device uses the following DHCP process:

1) The Avaya Desktop Video Device will broadcast a DHCP discover packet on to the untagged Converged VLAN which is relayed to a centralized DHCP server.
2) The DHCP server will respond with an IP address and standard options from the Converged VLAN scope with Avaya DHCP option 242 that provides the HTTP/HTTPS server IP address and path where the firmware and device configuration file resides.

Example Data VLAN Scope Options:

HTTPSRVR=192.168.10.20,HTTPDIR=ADVD/

3) If necessary the Avaya Desktop Video Device will download the latest firmware from the centralized HTTP/HTTPS server.
4) Once the firmware is current, the Avaya Desktop Video Device will download the device configuration file from the centralized HTTP/HTTPS server and will register with the Avaya Aura SIP services in the data center.

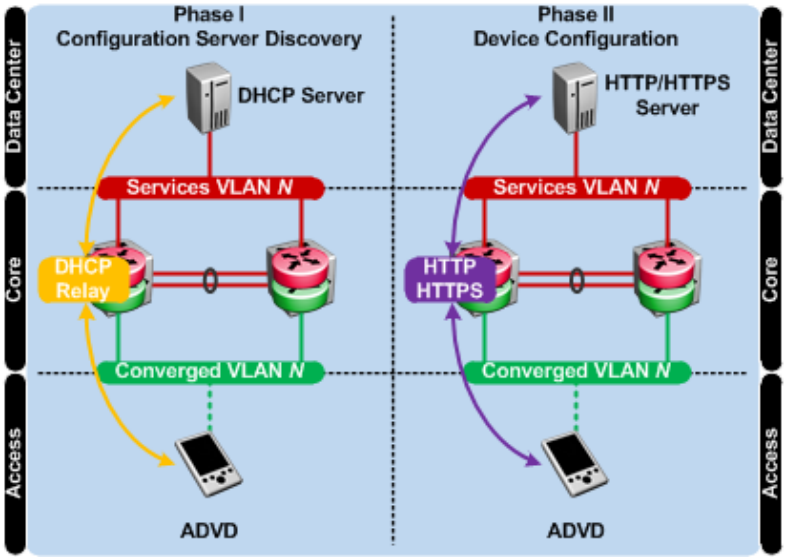


Figure 4.4.3.2 – DHCP with Untagged Converged VLAN

Best Practices and Recommendations:

- No provisioning is required for the DHCP scope on the Data VLAN which is unused.
- Each Converged VLAN scope must be provisioned to include Avaya Option 242 which provides the HTTP/HTTPS server IP Address and Path where the device firmware and configuration files reside.

4.5 Quality of Service

Avaya supports industry standard based QoS on all Avaya Aura servers and IP endpoints to ensure the correct prioritization and forwarding treatment of control, audio and video traffic as it is forwarded over an enterprise network. Avaya devices implement and support the IEEE 802.1p standard for providing prioritization of IEEE 802.1Q tagged Ethernet frames and IP Differentiated Services (DiffServ) for providing prioritization of IPv4 datagrams.

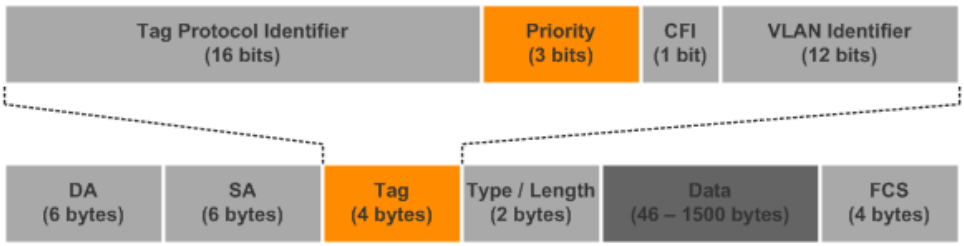


Figure 4.5-1 – 802.1Q Ethernet Frame

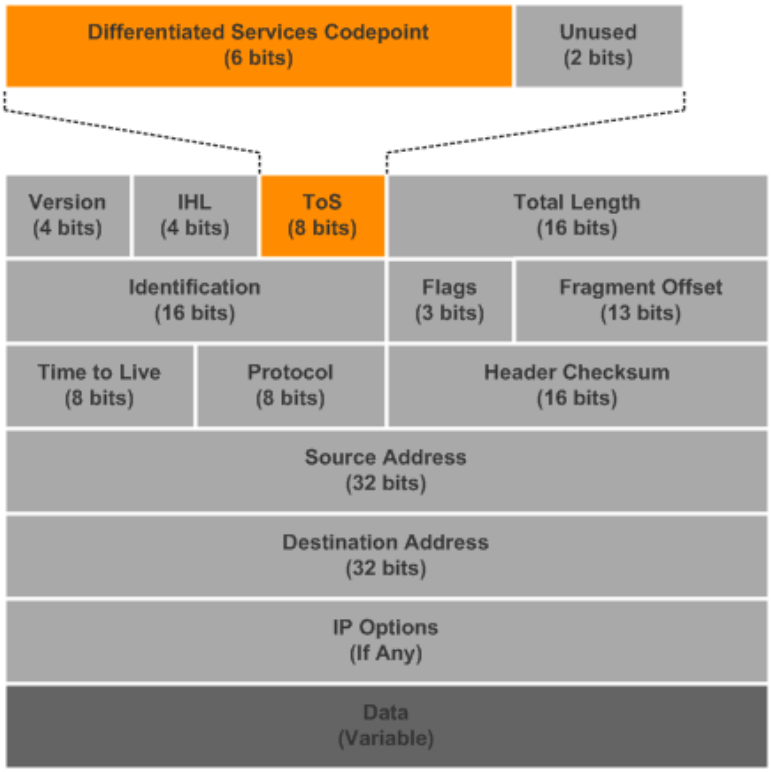


Figure 4.5-2 – IPv4 Datagram

For a QoS implementation to be successful, QoS must be implemented end-to-end throughout the core, distribution, access and data center layers as well as over the wide area network. In most QoS deployments traffic is untrusted at the edge of the network (i.e. access and data center layers) but is trusted through the core and distribution layers. Traffic may also be trusted at the access layer if the edge device can be identified and authenticated such as when Auto Detect Auto Config (ADAC) is enabled to support IP Phones and Avaya Desktop Video Devices.

4.5.1 Avaya Service Classes

To simply QoS deployments Avaya has standardized default QoS configurations and traffic forwarding behaviors on all its data products in the form of Avaya Service Classes (ASCs). ASCs are a superset of the QoS classes defined in the ITU-T Y.1541 standard and have been designed to provide the appropriate forwarding and treatment for most common types of enterprise applications over Avaya data products.

Using ACSs an enterprise can quickly create and assign QoS policies at the access and data center layers that can classify control, audio and video traffic then then assign each traffic type to a specific ASC. The ASC in turn defines the IEEE 802.1p (for tagged ports) and/or DSCP markings for each traffic flow as it is forwarded throughout the enterprise network.

QoS policies can be defined and managed on individual devices using Avaya Command Line Interface (ACLI) or Enterprise Device Manager (EDM) as well as centrally using Enterprise Policy Manager (EPM). EPM allows QoS policies to be quickly deployed and managed across multiple devices eliminating configuration errors and ensuring the consistent treatment of audio, control and video flows over all points of the network.

Traffic Category	Example Application	Avaya Service Class	Egress 802.1p	Egress DSCP
Network Control	Critical Alarms	Critical	7	CS7
	Routing, Billing, Operations, Administration, and Maintenance	Network		CS6
Interactive	IP Telephony	Premium	6	EF
	Video Conferencing, Interactive Gaming	Platinum	5	AF41
Responsive	Streaming Audio / Video	Gold	4	AF31
	Client / Server Transactions	Silver	3	AF21
Timely	E-mail, non-critical Operations, Administration, and Maintenance	Bronze	2	AF11
	Best Effort	Standard	0	CS0

Table 4.5.1 – Avaya Service Classes

4.5.2 Access Layer

Avaya Desktop Video Devices connect to the wired network at the access layer. As a general best practice industry recommendation QoS markings should not be trusted at the access layer. By default all ports on Avaya Ethernet Routing Switches are configured to un-trust QoS markings and will reset all IEEE 802.1p priorities and DSCP values to 0 as they ingress the Avaya Ethernet Routing Switch. This ensures that only critical applications and services that administrators specifically define are prioritized over the network.

It is recommended that all automatic and manually configured device facing ports remain untrusted. Manually configured ports will require QoS policies be defined to identify audio, control and video traffic and assign each flows to specific ASCs. Automatically configured ports will utilize ADAC which will automatically trust audio, control and video traffic from the Converged VLAN. Uplink ports that connect the access layer switches to the core or distribution layers should be configured as trusted ports to ensure flows maintain their IEEE 802.1p and DSCP markings as they are forwarded between access, distribution, core and data center layers.

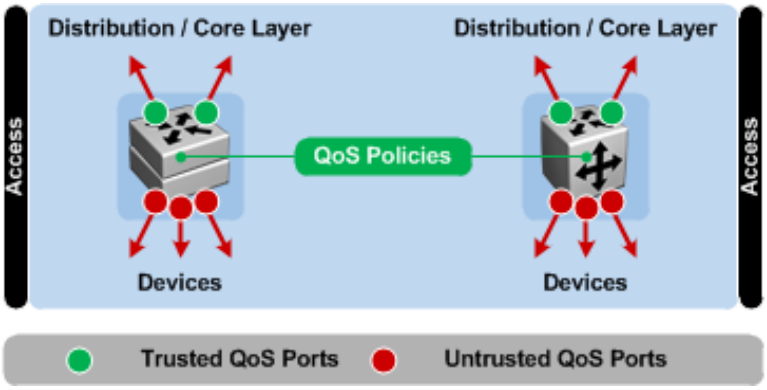


Figure 4.5.2 – Data Center Layer QoS Port Configuration

4.5.2.1 Automatic Access Layer Port Provisioning

When Auto Detect Auto Config (ADAC) is enabled on access layer ports to detect Avaya Desktop Video Devices, ADAC will automatically trust IEEE 802.1p and DSCP QoS markings made by the Avaya Desktop Video Devices on the Converged VLAN. ADAC will configure the access layer port to trust QoS markings only over the Converged VLAN and not the Data VLAN. QoS marked traffic forwarded over the Data VLAN will not be trusted or prioritized.

When ADAC is deployed it's important that the Avaya Desktop Video Device be configured to mark the correct 802.1p and DSCP values which align with the Avaya Service Classes. The default QoS markings can be manually configured on each Avaya Desktop Video Device using the admin menu or centrally defined on a configuration file stored on a centralized HTTP/HTTPS server which is downloaded by all Avaya Desktop Video Devices. Whenever possible it is recommended to manage and maintain the configuration centrally which ensures the QoS configuration is consistent on each Avaya Desktop Video Device.

The following table highlights the recommended IEEE 802.1p priorities and DSCP values for Avaya Desktop Video Devices which can be manually or centrally provisioned. The recommended audio and control traffic markings align to Premium ASC while recommended video markings aligned with the Platinum ASC.

Traffic Type	IEEE 802.1p	DSCP
Audio (RTP)	6	46 (EF)
Video	5	34 (AF41)
Control (SIP)	6	40 (CS5)

Table 4.5.2.1 – Recommended ADVD QoS Values

The following figure provides the recommended 802.1p and DSCP settings for the Avaya Desktop Video Device configuration file which is stored centrally on a HTTP/HTTPS server. The configuration file is automatically downloaded by the Avaya Desktop Video Device when the Avaya DHCVP option 242 and appropriate values are assigned to the Converged VLAN DHCP scope.

```
##################  802.1P/Q SETTINGS  ###################
##
##   Those settings does not apply to Wi-Fi interfaces.
##
## Telephone Frame Tagging
##   Controls whether layer 2 frames generated by the
##   telephone have IEEE 802.1Q tags.
##   0 for Auto, 1 for On, and 2 for Off
## SET L2Q 0
##
## Voice VLAN Identifier
##   VLAN identifier to be used by IP telephones. This
##   parameter should only be set when IP telephones are to
##   use a VLAN that is separate from the default data VLAN.
## SET L2QVLAN 0
##
## Audio Priority Value
##   Sets the layer 2 priority value for audio packets
##   from the phone. (0-7)
## SET L2QAUD 6
##
## Signaling Priority Value
##   Sets the layer 2 priority value for signaling
##   protocol messages from the phone. (0-7)
## SET L2QSIG 6
##
## Video Priority Value
##   Sets the layer 2 priority value for video packets
##   from the phone. (0-7)
## SET L2QVID 5
##
```

```
#################### DSCP SETTINGS ########################
##
##  DSCPAUD Sets the DiffServ value for audio streams from
##  the phone. The default is 46 and valid values are 0-63.
## SET DSCPAUD 46
##
##  DSCPVID Sets the DiffServ value for video streams from
##  the phone. The default is 26 and valid values are 0-63.
## SET DSCPVID 34
##
##  DSCPSIG Sets the DiffServ value for signaling protocol
##  messages from the phone. The default is 34 and valid
##  values are 0-63.
## SET DSCPSIG 40
##
```

Figure 4.5.2.1 – Recommended ADVD Configuration File QoS Settings

Best Practices and Recommendations:

- For audio, control and video traffic to be treated appropriately, the Avaya Desktop Video Devices must be configured to mark the recommended IEEE 802.1p and DSCP values as outlined above.

4.5.2.2 Manual Access Layer Port Provisioning

When access layer ports are manually provisioned, QoS policies must be defined on the Avaya Ethernet Routing Switches to classify and mark audio, control and video traffic received from Avaya Desktop Video Devices. QoS policies can be defined individually on each Avaya Ethernet Routing Switch using ACLI / EDM or centrally across multiple Avaya Ethernet Routing Switches using Enterprise Policy Manager (EPM). A separate QoS policy will need to be defined for audio, control and video traffic mapping each traffic flow to a specific Avaya Service Class (ASC). Each ASC determines the IEEE 802.1p priority and DSCP QoS values for each flow as well as the internal QoS treatment that each flow will receive as it is bridged or routed by each hop in the network. Additionally the ASC determines the egress hardware queues each flow is serviced by as it is forwarded by each Avaya Ethernet Routing Switch.

The following table highlights the default UDP ports used by Avaya for audio, control and video traffic along with the recommended Avaya Service Class assignments which can be used to build QoS policies on Avaya Ethernet Routing Switches deployed in the access layer when ADAC is not utilized for automatic port provisioning:

Traffic Type	Protocol	Ports	ASC
Audio	UDP	5000 - 5005	Premium
Video	UDP	5024 - 5044	Platinum
Control	TCP	5060 (TCP) & 5061 (TLS)	Premium

Table 4.5.2.2 – Avaya Default Audio, Control and Video UDP Ports

Best Practices and Recommendations:

- For audio, control and video traffic to be prioritized, QoS policies must be deployed in the access layer to classify audio, control and video traffic then assign each traffic class to the appropriate ASC when ADAC is not utilized for automatic port provisioning.
- For consistency and ease of management, it is recommended that QoS policies be centrally using Enterprise Policy Manager (EPM).

4.5.2.3 Queue Sets

The Ethernet Routing Switch 2500, 4500 and 5000 series stackable switches can support up to 8 hardware queues which are defined using QoS queue sets. The Avaya Ethernet Routing Switch 5000 and 4500 series support 8 hardware queues while the Avaya Ethernet Routing Switch 2500 series supports 4 hardware queues.

Each stackable Avaya Ethernet Routing Switch includes pre-defined QoS queue sets that controls the number of egress hardware queues implemented by the switch, queue service discipline, queue bandwidth allocation, queue service order and queue buffer size. Each stackable switch is assigned one QoS queue set and buffer configuration which is applied to all ports on the switch/stack. The QoS queue set determines the number of hardware egress queues available for different traffic ASCs and ultimately the egress hardware queue each ASC is serviced by.

To provide differentiation between audio, video and control traffic, Avaya recommends using the QoS queue set 4 which permits audio, control and video traffic to be serviced by unique queues while providing additional hardware queues for other traffic that may additionally need to be prioritized. Avaya recommends setting the QoS buffer size to Large for the Ethernet Routing Switch 5000, Medium for the Ethernet Routing Switch 4500 and Maximum for the Ethernet Routing Switch 2500.

Avaya Service Class	Egress Hardware Queue (Queue Set 4)
Critical	2
Network	
Premium ***(Audio, Control)***	1
Platinum ***(Video)***	3
Gold	4
Silver	
Bronze	
Standard	

Table 4.5.2.3-1 – ERS 2500 / 4500 / 5000 Queue Sets

The following table highlights the recommended QoS queue set and buffer configuration for Avaya Ethernet Routing Switch 2500, 4500 and 5000 series switches deployed in the access layer.

Switching Platform	Default Queue Set Values	Recommended
Ethernet Routing Switch 5000	2 (Large)	4 (Large)
Ethernet Routing Switch 4500	2 (Medium)	4 (Medium)
Ethernet Routing Switch 2500	4 (Maximum)	4 (Maximum)

Table 4.5.2.3-2 – ERS 2500 / 4500 / 5000 Queue Set and Buffer Size

Best Practices and Recommendations:

- Avaya recommends using queue-set 4 on all Avaya Ethernet Routing Switch 2500, 4500 and 5000 series switches deployed in the access layer.
- Avaya recommends using the default queue configuration for all Avaya Ethernet Routing Switch 8300 series switches deployed in the access layer.

4.5.3 Distribution / Core

Avaya Ethernet Routing Switches deployed in the core and optional distribution layers aggregate traffic between the access layers as well as aggregate traffic between the access and data center layers. As audio, control and video traffic flows are classified and marked at the access layers and trusted in the data center layer, the traffic flows can be trusted in the core and distribution layers.

As a general best practice it is recommended that all inter-switch ports in the core and distribution layers be configured to trust QoS so that IEEE 802.1p (for tagged ports) and DSCP values marked at the access and data center layers are maintained and honored as flows traverse the core and distribution layers.

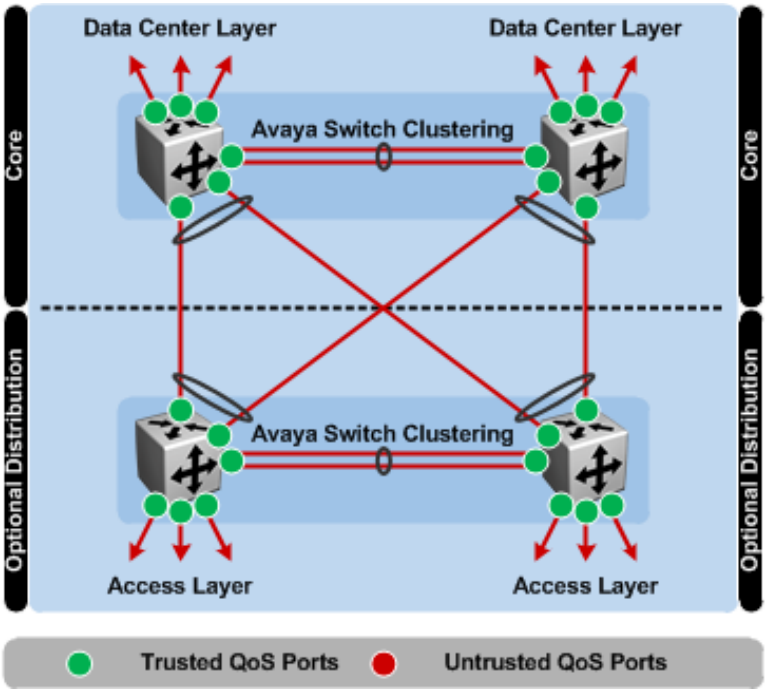


Figure 4.5.3 – Core / Distribution Layer QoS Port Configuration

Each of the Avaya Ethernet Routing Switches that can be positioned in the core and distribution layers can support a specific number of hardware queues. By default the Avaya Virtual Services Platform 9000, Avaya Ethernet Routing Switch 8600 / 8800 and the Avaya Ethernet Routing Switch 8300 are pre-configured to implement 8 hardware queues per port which is adequate for most core / distribution deployments. The Ethernet Routing Switch 8600 / 8800 with R and RS modules can support up to 64 hardware queues if necessary.

The Avaya Ethernet Routing Switch 5000 series switches can support up to 8 hardware queues per port but is pre-configured to support 2 hardware queues by default. When deploying an Avaya Ethernet Routing Switch 5000 series switch in the core or distribution layers it is recommended that the queue set is modified to support 4 hardware queues. This queue set recommendation is consistent with the queue set recommendations for the access and data center layers.

Best Practices and Recommendations:

- Avaya recommends using the default queue configuration for all Avaya Virtual Services Platform 9000, Ethernet Routing Switch 8600 / 8800 and 8300 series switches deployed in the core / distribution layers.
- Avaya recommends using the QoS queue set 4 on all Avaya Ethernet Routing Switch 5000 series switches deployed in the core / distribution layers.

4.5.4 Data Center

The data center switches connect critical services and applications that support the business to the network. Aura servers, application servers, appliances, firewalls, routers and other critical infrastructure devices all connect to the enterprise network using end of row or top of rack switches.

As a general best practice it is recommended that QoS be trusted for all ports that connect to Avaya Aura servers, media gateways and application servers as well as network infrastructure devices that participate in the QoS domain such as routers, firewalls and VPN appliances. In addition inter-switch ports that connect the data center switches to the core or data center distribution layers must also be trusted.

Ports that connect to additional physical or visualized servers should be untrusted to ensure the integrity of the QoS eco-system, however this decision should be made at the discretion of the network administrator on a per server or application basis. Whenever possible QoS policies should be defined and assigned to prioritize specific business critical applications and services.

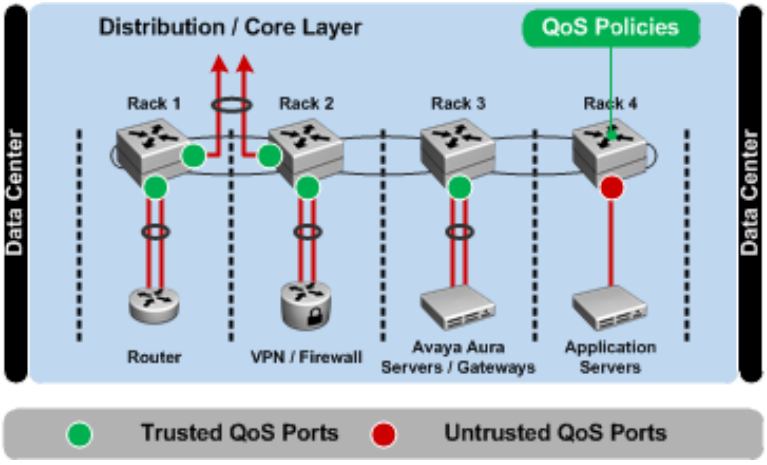


Figure 4.5.4 – Data Center Layer QoS Port Configuration

Trusting the ports that connect to Avaya Aura servers, media gateways and application servers greatly simplifies the QoS configuration in datacenter as Aura uses a large number of protocols and ports for real-time communications, control and inter-server communications which would need to be individually defined when building QoS policies. The QoS policies would need to be continuously maintained and updated as new Aura services and features are added to the network which would be hard to maintain. Trusting the ports greatly simplifies the overall management of the Aura system and eliminates errors.

The following table highlights the recommended IEEE 802.1p and DSCP values which need to be modified on Aura servers, media gateways and application servers to ensure the correct treatment of audio, control and video traffic forwarded within the data center as well as audio, control and video traffic forwarded to the access layers.

Traffic Type	IEEE 802.1p	DSCP
Audio (RTP)	6	46 (EF)
Video	5	34 (AF41)
Control (SIP)	6	40 (CS5)
IPSI ←→ Communication Manager	6	46 (EF)

Table 4.5.4 – Recommended Avaya Aura Server / Media Gateway QoS Values

Each of the Avaya Ethernet Routing Switches that can be positioned in the data center as end-of-row or top-of-rack switches can support a specific number of hardware queues. By default the Avaya Ethernet Routing Switch 8600 / 8800 and the Avaya Ethernet Routing Switch 8300 are pre-configured to implement 8 hardware queues per port which adequate for most data center deployments.

The Avaya Ethernet Routing Switch 4500 and 5000 series switches can support up to 8 hardware queues per port but are pre-configured to support 2 hardware queues by default. When deploying an Avaya Ethernet Routing Switch 4500 or 5000 series switches in the data center it is recommended that the queue set is modified to support 4 hardware queues. This queue set recommendation is consistent with the queue set recommendations for the access, distribution and core layers.

Best Practices and Recommendations:

- Avaya recommends trusting QoS markings on ports connecting to Avaya Aura servers, Avaya Media Gateways and network infrastructure devices such as IP Routers, VPN Gateways and Firewalls participating in the QoS domain.
- Avaya recommends using queue-set 4 on all Avaya Ethernet Routing Switch 2500, 4500 and 5000 series switches deployed in the data center layer.
- Avaya recommends using the default queue configuration for all Avaya Ethernet Routing Switch 8600 / 8800 and 8300 series switches deployed in the data center.
- QoS values on Aura servers, media gateway and application servers must be modified to match the recommended values provided in table 4.5.4.

4.5.5 Wireless LAN

When Avaya Desktop Video Devices are being deployed over an Avaya Wireless LAN 8100 solution, additional QoS mechanisms are used to provide over-the-air prioritization on the wireless medium. The Wireless LAN 8100 system uses IEEE 802.1p and DSCP to prioritize traffic that is forwarded over the wired medium while 802.11 wireless clients and Access Points leverage IEEE 802.11e / WMM standards for over-the-air prioritization of 802.11 based frames.

All wireless traffic forwarded between the WC 8180 Wireless Controllers and AP 8120 Access Points is encapsulated in CAPWAP over IPv4. To provide end-to-end QoS, the WC 8180 Wireless Controllers and AP 8120 Access Points will mark the DSCP values in the CAPWAP IPv4 headers using the DSCP values set by the Avaya Desktop Video Devices, Aura servers and Media Gateways for audio, control and video traffic.

Each CAPWAP packet is marked individually based on the original DSCP value marked for the audio, control or video payload. The original DSCP value is maintained so that QoS can be provided once the packet is de-encapsulated and forwarded onto the wired network. Additionally the original payload DSCP values are also copied to mobility tunnel IPv4 headers so that QoS integrity can be maintained for mobility traffic forwarded between WC 8180 Wireless Controllers.

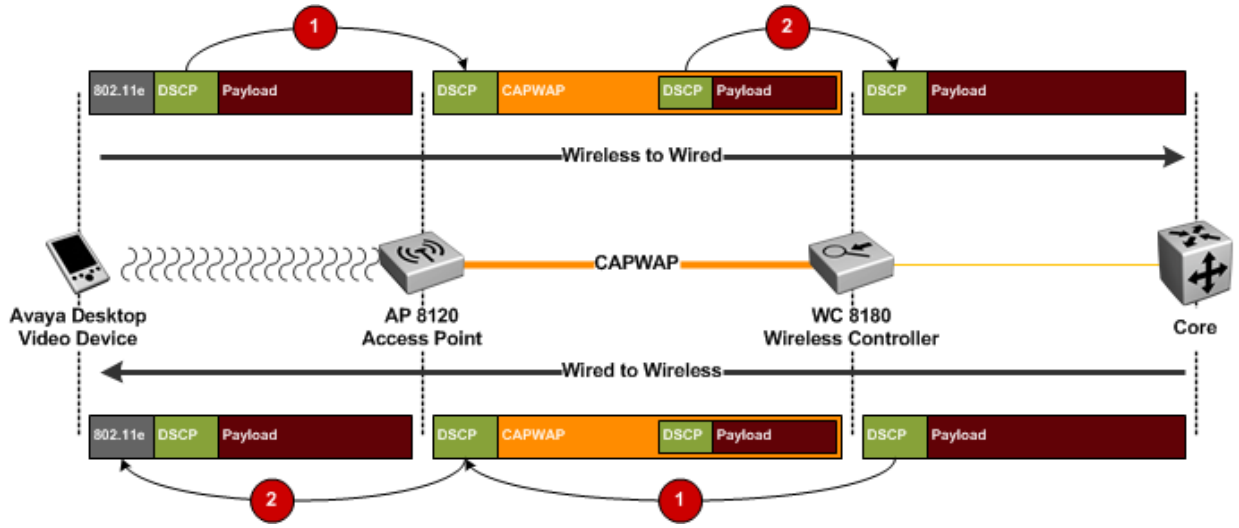


Figure 4.5.5 – Wireless QoS for Avaya Desktop Video Device Traffic

Traffic that is destined to a wireless Avaya Desktop Video Device has an additional step where the DSCP value in the CAPWAP IPv4 header is used to determine the WMM forwarding queue the traffic is serviced by which in turn determines the over-the-air priority. When the CAPWAP packet is received by the AP 8120 Access Point, it will inspect the IPv4 header in the CAPWAP packet and use a DSCP → WMM table to determine the WMM Access Category (AC) to assign the traffic to. The AP 8120 Access Point will de-encapsulate the payload, place the traffic in the appropriate forwarding queue then mark the appropriate WMM fields and forward the frame onto the wireless medium.

Traffic forwarded from the Avaya Desktop Video Device will be marked with a DSCP value based on the Avaya Desktop Video Device configuration as well as with WMM fields. The WMM fields determine the over-the-air prioritization frames are to receive, while the DSCP value determines the prioritization the audio, video and control traffic is to receive over the wired network.

For IPv4 traffic, the AP 8120 Access Points use the DSCP value to mark the DSCP in the CAPWAP IPv4 header and the 802.11e / WMM fields are ignored. The WMM fields are only used to mark DSCP in the CAPWAP IPv4 header for non IPv4 traffic.

4.5.5.1 WC 8180 Wireless Controllers

The WC 8180 Wireless Controllers connect to Avaya Ethernet Routing Switches in the core layer to ensure adequate bandwidth is available to support the high-throughput demands of 802.11n clients. By default all the switch ports on WC 8180 Wireless Controllers are pre-configured to trust QoS traffic, however some minor software configuration needs to be performed on the WC 8180 Wireless Controllers to ensure wireless traffic is trusted and treated appropriately over the wireless system.

For wireless QoS traffic to be maintained, the AP-Client-QoS setting needs to be globally enabled for the Wireless Domain for AP → Wireless Client traffic and the Client-QoS setting needs to be enabled for each Network Profile that is to support Avaya Desktop Video Devices for Wireless Client → AP traffic. No additional configuration is required as all the QoS mapping tables are pre-defined and align to the Avaya Service Classes.

Ethernet ports on the Virtual Services Platform 9000 or Avaya Ethernet Routing Switch 8800 / 8600, 8300 or 5000 series switches in the core to which the WC 8180 Wireless Controllers connect must be configured to trust QoS to ensure that QoS markings for management control, CAPWAP, mobility tunnels as well as de-encapsulated audio, control and video traffic is maintained. Trusting these ports will ensure that wireless system traffic will maintain their correct QoS markings as well as ensure traffic destined to wireless hosts will be forwarded out of the appropriate WMM queues when received by AP 8120 Access Points.

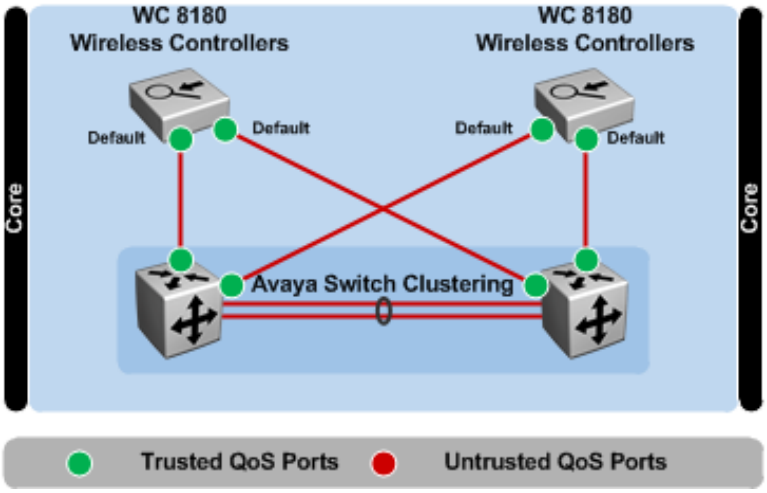


Figure 4.5.5.1 – Wireless LAN QoS Port Configuration

Best Practices and Recommendations:

- The AP-Client-QoS option must be globally enabled for the Wireless Domain.
- The Client-QoS option must be enabled for each Network Profile that is to support Avaya Desktop Video Devices.
- Avaya recommends trusting QoS markings on ports in the core connecting to WC 8180 Wireless Controllers so that QoS markings are maintained for management control, CAPWAP, mobility tunnels and de-encapsulated audio, video and control traffic is maintained.

4.5.5.2 AP 8120 Access Points

The AP 8120 Access Points connect to Avaya Ethernet Routing Switches in the access layer and are managed by the WC 8180 Wireless Controllers in the core. Wireless user traffic is exchanged between the AP 8120 Access Points and WC 8180 Wireless Controllers using CAPWAP over IPv4. The DSCP values in the CAPWAP IPv4 headers are marked by the AP 8120 Access Points when forwarding wireless traffic destined to wired or wireless hosts. Likewise the WC 8180 Wireless Controllers will mark the DSCP values in the CAPAP IPv4 headers when forwarding wireless or wired traffic destined to a wireless host. The DSCP values in the CAPWAP IPv4 headers are used by the AP 8120 to determine the 802.11e / WMM queues and over-the-air prioritization the traffic is to receive. If no DSCP value is defined, the traffic is treated as best effort.

To ensure QoS integrity is maintained, all access ports connecting the AP 8120 Access Points to the access layer must be configured as trusted. Trusting the ports allows the DSCP values set in the CAPWAP IPv4 headers to be maintained as the AP 81280 Access Points forward wireless traffic to the WC 8180 Wireless Controllers in the core. Likewise trusting the QoS markings allows the DSCP values in the CAPWAP IPv4 headers to be maintained when traffic is forwarded from WC 8180 Wireless Controllers in the core to the AP 8120 Access Points in the access layer allowing the wireless traffic to be serviced by the correct WMM forwarding queues and be provided the appropriate airtime over-the-air prioritization.

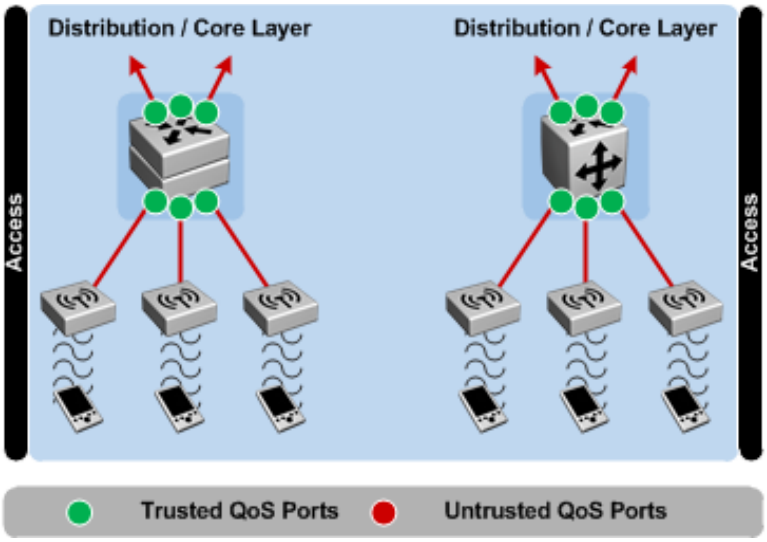


Figure 4.5.5.2 – Data Center Layer QoS Port Configuration

Best Practices and Recommendations:

- Avaya recommends trusting QoS markings on access layer ports connecting AP 8120 Access Points to the access layer.

4.5.5.3 Avaya Desktop Video Device

The Avaya Desktop Video Device uses the manually defined or centrally provisioned DSCP values for audio, control and video traffic to determine the WMM Access Category (AC) traffic is assigned and the local forwarding queue traffic is serviced by when the traffic if forwarded onto the wireless medium. The Avaya Desktop Video Device determines the WMM AC and queue mapping by inspecting the first three precedence bits of the DSCP value for the traffic. The WMM AC is selected based on the mappings provided in the following table.

IPv4 Precedence Bits	WMM Access Category
000	BE (Best Effort)
001	BK (Background)
010	BK (Background)
011	BE (Best Effort)
100	VI (Video)
101	VI (Video)
110	VO (Voice)
111	VO (Voice)

Table 4.5.5.3 – ADVD DSCP → WMM Mapping Table

The current version of the Avaya Desktop Video Device firmware currently has a limitation where the recommended DSCP values for audio and control traffic will not assign the traffic to the Voice (VO) AC. With the current firmware the DSCP values CS6 or CS7 are the only two DSCP values which can assign audio and control traffic to the Voice AC. These DSCP values are reserved for network control traffic and should not be used for other traffic types.

The following table highlights the recommended DSCP values for Avaya Desktop Video Devices which can be manually or centrally provisioned. The recommended audio, control and video markings align each traffic class to the WMM Video (VI) AC which ensures real-time traffic is forwarded by the Avaya Desktop Video Devices before best effort data traffic. These DSCP values are consistent with the recommended values highlighted in Section 4.5.2.1 for wired traffic ensuring the real-time traffic is treated appropriately over the wireless system and campus infrastructure. Additionally as the audio, control and video the traffic is IPv4 based, the Wireless LAN 8100 system will use the defined DSCP values and not the WMM AC to determine the DSCP values to mark in the CAPWAP and mobility tunnel IPv4 headers. The only impact of this limitation is that over-the-air prioritization of audio and control traffic is downgraded to Video while the audio and control traffic will be treated correctly throughout the wired network.

Traffic Type	DSCP	WMM Access Category
Audio (RTP)	46 (EF)	VI (Video)
Video	34 (AF41)	VI (Video)
Control (SIP)	40 (CS5)	VI (Video)

Table 4.5.5.3 – Recommended ADVD Wireless QoS Values

5. Reference Documentation

Publication Number	Description
NN48500-573	Small Campus Technical Solutions Guide
NN48500-574	Medium Campus Technical Solutions Guide
NN48500-575	Large Campus Technical Solutions Guide
NN48500-587	Wireless LAN 8100 Design Guide
NN48500-609	Super Large Campus Technical Solutions Guide
NN48500-617	Shortest Path Bridging Technical Configuration Guide
N/A	Avaya Aura Release 6.0 Documentation Library