Notice
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
“Documentation” means information published in various mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees 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 websites referenced within this site or Documentation 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 Avaya hardware and software. 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 website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS documentation or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service
THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE. HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACQUIRES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHICH YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS Avaya SOFTWARE, PURCHASED FROM Avaya INC., ANY Avaya AFFILIATE, OR AN Avaya CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH Avaya OR AN Avaya CHANNEL PARTNER. 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 CHANNEL PARTNER. 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”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types
Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., workforce or helpdesk), IP or Voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Heritage Nortel Software
“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment.
Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright
Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product 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 unless expressly authorized by Avaya. 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.

Virtualization
The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components
"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefitting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO, NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider
THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws
You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud
“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company’s behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention
If you suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Helpdesk at +1-800-043-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities
Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation
For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support
See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, 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, Hosted Service(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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Java is a registered trademark of Oracle and/or its affiliates.
Contents

Chapter 1: New in this release........................................................................................................ 6
  Features........................................................................................................................................ 6
  Other changes.............................................................................................................................. 6

Chapter 2: High Availability overview.................................................................................... 7

Chapter 3: Geo-redundant split SIP Core architecture................................................................. 8
  Application Server 5300 Geo-reference network......................................................................... 10
  Physical reference network............................................................................................................ 10
  Logical reference network............................................................................................................ 13
  Enterprise IP network considerations............................................................................................ 14

Chapter 4: Planning and engineering......................................................................................... 16
  Preparing the secondary site......................................................................................................... 18

Chapter 5: Traffic flow analysis................................................................................................ 19
  Single campus normal traffic flows.............................................................................................. 19

Chapter 6: Failure scenario analysis........................................................................................... 23
  Link failures................................................................................................................................. 23
  Switch and router failure.............................................................................................................. 25
  Server and network element failures........................................................................................... 26
  Media server and gateway failure................................................................................................. 27
  Site failure..................................................................................................................................... 27

Chapter 7: Multiple LSC-only Geo-Redundant campus or enclave............................................ 29
  EBC consideration......................................................................................................................... 29
  Normal Multiple LSC signaling flow............................................................................................. 30
  Master LSC failure recovery........................................................................................................ 31
  Slave LSC failure recovery........................................................................................................... 32

Chapter 8: SS-LSC Geo-Redundant campus or enclave............................................................... 34
  Normal LSC-SS signaling flow....................................................................................................... 34
  Master LSC failure recovery........................................................................................................ 35
  SS SESM failure recovery............................................................................................................ 36

Chapter 9: Limitations and restrictions....................................................................................... 38
Chapter 1: New in this release

The following sections detail what's new in Avaya Aura® Application Server 5300 High Availability Fundamentals, NN42040-115 for Avaya Aura® Application Server 5300 Release 3.0.

Navigation

- **Features** on page 6
- **Other changes** on page 6

---

**Features**

This document is new for Avaya Aura® Application Server 5300 Release 3.0. For more information on the new features, see *Avaya Aura® Application Server 5300 Release Delta, NN42040-201*.

---

**Other changes**

The following changes were made that were not associated with features:

**Revision history**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 2017</td>
<td>Updated the legal page for Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>June 2012</td>
<td>Standard 03.01. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>May 2010</td>
<td>Standard 01.02. This document is issued to support Avaya Aura® Application Server 5300 Release 2.0. Editorial changes were made.</td>
</tr>
<tr>
<td>April 2010</td>
<td>Standard 01.01. This document is issued to support Avaya Aura® Application Server 5300 Release 2.0.</td>
</tr>
</tbody>
</table>
Chapter 2: High Availability overview

A successful Avaya Aura® Application Server 5300 deployment in a mission critical environment requires a high availability service network. Application Server 5300 uses various software and hardware fault protection and recovery strategies for the SIP core signaling and OAMP components to maximize system availability.

The AS 5300 Session Manager is the Application Server 5300 call signaling processing engine. Application Server 5300 supports a one-to-one redundant Call Processing autofailover mechanism using a pair of AS 5300 Session Manager. All active call information is checkpointed from the active AS 5300 Session Manager to the standby AS 5300 Session Manager to maintain service integrity after the autofailover. The standby AS 5300 Session Manager monitors the health of the active Call Processing over a common Voice Local Area Network (VLAN) and takes over the call processing functions when the active AS 5300 Session Manager fails. All active calls remain up after failover. For more information about Application Server 5300 embedded fault resilient capabilities, see Avaya Aura® Application Server 5300 Planning and Engineering, NN42040-200.

The Application Server 5300 active/standby redundant architecture for failover can be further extended for Application Server 5300 L2 Geo-Redundant Split SIP core architecture to build a disaster-survivable service network using two data centers. The disaster-survivable service network is achieved by stretching the common (single or multiple) VLANs across two separated locations and splitting the server and component pairs over these locations (for example, OAM 1 and AS 5300 SESM 1 servers at the primary site, OAM 2 and AS 5300 SESM 2 servers at the secondary site).

Because the underlying Layer 2 (L2) topology is invisible to the Application Server 5300 functional components, the peer components act as if they are collocated, as long as the delay introduced between two locations meets the delay requirement. Application Server 5300 Geo-redundant Split Core architecture allows critical services continue to operate when the primary data center becomes inoperable.

Navigation

- Geo-redundant split SIP Core architecture on page 8
- Planning and engineering on page 16
- Traffic flow analysis on page 19
- Failure scenario analysis on page 23
- Multiple LSC-only Geo-Redundant campus or enclave on page 29
- SS-LSC Geo-Redundant campus or enclave on page 34
- Limitations and restrictions on page 38
Chapter 3: Geo-redundant split SIP Core architecture

The Application Server 5300 architecture consists of a collection of network elements (NE) that can be grouped into the Application Server 5300 SIP core, Avaya Media Server (MS), PRI media gateway, and access client categories. For the Single SIP Core Redundant Architecture, the high availability of a SIP Core is achieved through deploying a pair of redundant servers for all SIP Core NEs at a single data center location.

To achieve high availability for Avaya MS, multiple Avaya MS pools with multiple servers for each pool can be created for the Avaya MS services. Application Server 5300 uses the subscriber information to determine a proper pool, local or remote, for the requested service.

To achieve high availability for the PRI gateway, additional gateways can be provisioned for servicing the calls. Application Server 5300 distributes the calls over all the available gateways for call processing. Should one gateway fail, Application Server 5300 will distribute the calls to the remaining gateways.

The following figure shows a Single SIP Core Site Redundant Architecture.

Figure 1: Application Server 5300 Single SIP Core redundant architecture

The single SIP core site redundant architecture provides a lower cost approach meeting the high availability requirements of many smaller enterprises. Given the possibility of a variety of natural and man made disasters such as hurricanes, earthquakes, snow storms, flooding, power outages, and
terrorism, the single core site architecture is no longer sufficient for providing continuous communications under those conditions.

The Application Server 5300 L2 Geo-redundant Split SIP core architecture (shown in the following figure) protects the subscriber services from the single data center failure in the event of a natural disaster or other emergencies.

![Application Server 5300 Geo-redundant split SIP Core architecture](image)

**Figure 2: Application Server 5300 Geo-redundant split SIP Core architecture**

As shown in the above figure, the Geo-redundant architecture splits the single SIP Core Network Elements (and their associated servers) into two locations. Initially, the primary data center servers host the active SIP core components and the secondary data center is where the standby SIP core components and servers reside. Although the secondary SIP core components are called the standby SIP core, the components such as Avaya Aura® Provisioning and Personal Agent Managers are all actively serving requests in the secondary location. Application Server 5300 Geo-Redundant Split Core architecture allows the signaling, media, and OAMP packets continue to flow when the primary data center becomes inoperable. Note that the architecture does not require extra servers to be deployed.

In large enterprises, the media servers and PRI gateways are commonly deployed in their own Media Center locations outside of the SIP Core data centers and close to subscribers they serve. This deployment helps avoid backhauling media traffic to the data center and then back down to the subscriber sites. It also minimizes the switching, routing, and bandwidth performance impacts on networking devices due to large media traffic concentration at the data center. Additional media servers and gateways can be added at any location to improve the service quality for the local subscribers.

When there are media server pools and PRI gateways deployed in the data centers, Avaya recommends that the media server pool is not split across the common VLAN between the primary and secondary data centers. This is because localizing media resources within a data center helps to eliminate the cross site media traffic over the L2 network, thus removing the restriction of supporting only two Meet Me servers in a pool, and simplifying the geo-redundant migration process.
Application Server 5300 Geo-reference network

Application Server 5300 can be deployed many different ways. Instead of enumerating all possible scenarios, this section uses one reference network to simplify the discussion.

- **Physical reference network** on page 10
- **Logical reference network** on page 13

---

Physical reference network

The Application Server 5300 SIP Core and Avaya MS servers use high-end IBM hardware which has built-in redundant Hot Swap SAS Disks, hot-swap redundant power supplies, hot-swap redundant fans, and dual integrated 10/100/1000 Mbps Ethernet interfaces. The Application Server 5300 SIP Core and Server platform runs on the Red Hat Enterprise Linux version 5.4 (RHEL 5.4). The Red Hat Enterprise Linux binds the dual integrated Ethernet interfaces into a single channel (that is, a bonded interface). The channel bonding protects the server from a single network interface and/or network link failure. When the bonding driver detects failure of the active interface, it switches to the standby interface transparently to the applications running on the server.

To achieve high availability, the AudioCodes Primary Rate Interface (PRI) gateway High Availability configuration contains redundant modules for every part of the system, including redundant Gigabit Ethernet connections, redundant power nodules, redundant fans, and redundant VoIP blades. The smaller lower cost AudioCodes MG1000 gateway supports two Ethernet ports for redundant network connections.
In the reference network diagram above, the Application Server 5300 SIP core servers and the associated network elements are deployed in both primary and secondary data center locations. The Avaya MS media servers and PRI gateways are pooled resources that can be deployed where they are needed to support the local subscribers. The Avaya MS and PRI servers can also be deployed in the primary and secondary Data centers, but the collocation with SIP core servers is not a requirement.

As shown in the following diagram, Application Server 5300 must be connected using redundant networking devices (for example, standalone L2 and L3 switches, or integrated L2/L3 switches) to ensure there is no single point of failure anywhere in the network and there are at minimum of two physical paths exist between any two endpoints. To eliminate the fiber trunking failure resulting from a single switch or a switch module failure, each pair of fibers must be connected to a different switch or a switch module (that is, a chassis based switch). These fiber pairs are aggregated into a single logical connection using the IEEE 802.3ad protocol to provide Ethernet MAC layer failover transparency for protocols running above the trunks. Similarly, the redundant L2 switches must also be attached to separate L3 switch/routers for supporting IP routing redundancy.
Figure 4: Physical redundancy eliminating a single point of failure

Depending on the supported Ethernet standards and the types of fiber used, the distance between the primary and secondary locations can be of a few or a few tens of kilometers apart (see Table 1: Maximum fiber distance for Ethernet on page 12). Other technologies such as fiber optical repeater and multiple self-healing optical rings (for example, Resilient Packet Ring [RPR]) can be used when the distance needs to be extended beyond what is supported by a single span of a fiber cable.

RPR uses Ethernet switching and a dual counter-rotating ring topology to provide SONET-like network resiliency. RPR uses physical-layer alarm information and Layer 2 protocol communications to detect node and/or link failures. RPR can restore network failure in less than 50 ms.

For Application Server 5300, the maximum distance between the primary and secondary locations must be restricted so that the one-way delay is limited to 20 ms and packet loss is less than 10^-3. This restriction ensures that the AS 5300 Session Manager heartbeats and responses are communicated timely and correctly.

Table 1: Maximum fiber distance for Ethernet

<table>
<thead>
<tr>
<th>IEEE Ethernet Standard</th>
<th>Data Rate</th>
<th>Fiber Type</th>
<th>IEEE Maximum Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet (10Base-FL)</td>
<td>10 Mbps</td>
<td>50 or 62.5 Multimode @ 850nm</td>
<td>2km</td>
</tr>
<tr>
<td>Fast Ethernet (100Base-FX)</td>
<td>100 Mbps</td>
<td>50 or 62.5 Multimode @ 1300nm</td>
<td>2km</td>
</tr>
<tr>
<td>Fast Ethernet (100Base-SX)</td>
<td>100 Mbps</td>
<td>50 or 62.5 Multimode @ 850nm</td>
<td>300m</td>
</tr>
<tr>
<td>Gigabit Ethernet (1000Base-SX)</td>
<td>1000 Mbps</td>
<td>50 Multimode @ 850nm</td>
<td>550m</td>
</tr>
<tr>
<td>Gigabit Ethernet (1000Base-SX)</td>
<td>1000 Mbps</td>
<td>62.5 Multimode @ 850nm</td>
<td>220m</td>
</tr>
<tr>
<td>Gigabit Ethernet (1000Base-LX)</td>
<td>1000 Mbps</td>
<td>50 or 62.5 Multimode @ 1300nm</td>
<td>550m</td>
</tr>
<tr>
<td>Gigabit Ethernet (1000Base-LX)</td>
<td>1000 Mbps</td>
<td>9 Single mode @1310nm</td>
<td>5km</td>
</tr>
<tr>
<td>Gigabit Ethernet (1000Base-LH)</td>
<td>1000 Mbps</td>
<td>9 Single mode @1550nm</td>
<td>70km</td>
</tr>
</tbody>
</table>
Logical reference network

The logical reference networks define a functionally equivalent physical reference network. The logical reference networks provide the service representations of the physical network; hence they are useful for understanding how different types of traffic flow traversing the network. Based on the Application Server 5300 functional components and their attachments to the configured subnet/VLANs, two logical reference networks are presented here: Single Subnet/VLAN Logical Reference Network and Multisubnet/VLAN Logical Reference Network.

The following figure depicts a logical reference network for the Application Server 5300 physical reference network supporting single subnet/VLAN connections to all Application Server 5300 functional components.

![Figure 5: Single subnet/VLAN logical reference network](image)

The following figure shows a logical reference network for the Application Server 5300 physical reference network supporting multiple subnet/VLAN connections to all Application Server 5300 functional components. In the Data Centers, the OAMP components, such as AS 5300 Element Manager (AS 5300 EM), Fault Performance Manager (FPM), Database Manager (DB), and Provisioning Manager (PROV), are attached to both External OAMP Subnet/VLAN and Internal OAMP Subnet/VLAN. The signaling components, such as AS 5300 Session Manager (AS 5300 SESM) and Personal Agent Manager (PA), are attached to both Signaling Subnet/VLAN and Internal OAMP Subnet/VLAN.
Figure 6: Multisubnet VLAN Logical reference network

In the Media Centers, the media resources are attached to Signaling Subnet/VLAN, Internal OAMP Subnet VLAN, and Media Subnet/VLAN.

**Enterprise IP network considerations**

The L1/L2 fault resiliency and failover transparency prevent routing instability from occurring in the enterprise network. However, when routing failures do occur, the choice of an IP routing protocol becomes very important for a faster network recovery. This is because slow recovery from a routing failure can cause excessive packet losses which can severely degrade service quality.

When a failure (for example, link or device up or down) occurs in an IP network, all L3 routing devices must exchange routing updates for changes happened in the network. The exchange of routing updates helps all routing devices to update their routing table so that traffic can be forwarded around a failed link or device. A network “convergence” describes a state that all routing devices share a consistent routing map of the network. The network convergence time is the time for a L3 routing device to detect the failure (detection time), plus the time to propagate the updates (propagation time) to all other L3 routing devices, and the time for all affected L3 routing devices to calculate their forwarding tables. For a speedy routing failure recovery, a link-state based routing protocol, such as OSPF, is highly recommended for the enterprise Application Server 5300 service network. Avaya also recommends maintaining the network convergence time within 10 seconds.

At the service network edge, the use of Virtual Router Redundancy Protocol (VRRP) protocol (RFC 2338) enables fast (that is, from a subsecond to 3 seconds) default route recovery for the
Application Server 5300 SIP Core servers and media servers. The VRRP protocol allows the redundant L3 routing devices to protect a default route IP address. VRRP operates transparently to the endpoints and requires no special configuration on host devices. When endpoints use a default router virtual IP address, it eliminates the single point-of-failure when the configured default router for an end station is lost. VRRP protocol increases network resiliency for the LAN segments where Application Server 5300 servers and gateways are located.

Figure 7: Primary site inject lower cost routes

Finally, the network administrator, from the primary data center, must inject lower cost IP routes for the stretched signaling and internal OAMP subnets into the service network and inject lower cost external OAMP subnet into the external OSS network (see the diagram above). This is to ensure that when the primary data center is up and running, all traffic is sent to the primary data center for processing. It also ensures that all signaling traffic continues to flow to the primary data center in the “Split Brain” condition when both centers believe that they are the surviving one. This can happen in an unlikely event that the dual fiber-pairs failed between the sites and the secondary data center is partitioned from the primary data center and start to assume the service IP address.
Chapter 4: Planning and engineering

Application Server 5300 has no specific requirements for a particular brand of networking equipment for Ethernet connections. However, the following requirements are expected from the network that is planning to implement the Application Server 5300 L2 Geo-Redundancy capability to ensure that there is no single point of failure embedded in the network that can hinder the Application Server 5300 operations.

- The Data and Media centers must provide independently protected power sources for all Application Server 5300 components (that is, SIP Core servers, media servers, and gateways) and all Application Server 5300 components must be connected to separate power sources for more power protection.
- Two redundant L2 switching devices/modules must be deployed for supporting the noninterrupt operation of all Application Server 5300 components.
- The enterprise network must provide redundant L3 routing/switching devices for the redundant L2 switching devices/modules.
- The two redundant L2 switching devices/modules must be connected to separate L3 routing devices for more IP routing protection.
- The maximum distance between the primary and secondary locations must be restricted so that the one-way delay is limited to 20 ms and packet loss is less than 10^-3.
- The two redundant L2 switch pairs are connected using two pairs of dedicated fibers providing full-duplex gigabit capable Ethernet transmission between the primary and secondary sites.
- The fiber pairs must be connected to different switches/modules. This eliminates the total trunking failure resulting from a single switch/module failure.
- These fiber pairs must be aggregated into a single logical connection using IEEE 802.3ad standard link aggregation protocol, which provides Ethernet MAC failover transparency for the VLAN trunks. In addition to supporting 802.3ad protocol, the switches must be able to detect end-to-end failures such as far-end failures, unidirectional, bidirectional link failures irrespective of intermediary devices. They must also enable link recovery in less than one second. This mechanism prevents the peer from continue sending traffic down the failed link.
- To ensure no single point of failure anywhere in the network, the network must provide a minimum of two physical paths between any two end points in the network.
- The Data and Media centers should use Virtual Router Redundancy Protocol (VRRP) (RFC 2338) running on the center’s default routers (that is, not across the primary and secondary centers) to support fast default route recovery for Application Server 5300 servers and gateways. Normal VRRP convergence time is about 3 seconds. However, some proprietary extension of VRRP can achieve sub-second failover time.
• For a fast routing failure recovery, a link-state based routing protocol such as OSPF is recommended. The network convergence time should be kept within ten seconds for each of the service network when possible.

• The L3 routing devices supporting the primary data center must inject lower costs for the primary data center Signaling and Internal OAMP subnets into the campus core network and External OAMP subnet into the external OSS network. This is to direct all traffic to the primary site for processing.

• There should be no routing protocol communicated over the common links connecting the primary and secondary data centers to prevent undesired back door routing over the links.

• There should be sufficient contiguous server and service IP address space reserved for each Application Server 5300 subnet to accommodate the future expansion.

• All Application Server 5300 components must be connected to separate L2 networking devices for more network protection.

• The standby AS 5300 Session Manager (AS 5300 SESM) monitors the health of the active SESM over a common VLAN. Therefore the signaling subnet must be stretched across the 2 sites. Similarly, the OAMP subnet must be stretched across the two sites to preserve the AS 5300 Element Manager (AS 5300 EM), Fault Performance manager (FPM), Provisioning Manager (PROV), Accounting Manager (ACCT) and Database Manager (DB) redundancy functionality over common internal and external OAMP VLANs.

• Both the primary and the secondary data centers contain the same number of SIP core servers to ensure the integrity of L2 geo-redundancy configuration.

• The system must provide sufficient signaling, media, and OAMP processing capacities to handle the subscriber failover demands. This requires engineering each service site with sufficient capacity to handle the extra media traffic loads (for example, Media Center 2 carries the extra media traffic loads as result of Media Center 1 failure).

• When Avaya Media Server (MS) servers and PRI gateways must be deployed in the primary and secondary data centers, they must be deployed in their own local data center media subnet/VLAN, which is not stretched across two data centers. This is to avoid a large volume of media traffic traversing over the inter-site fiber links.

• The geo-redundant DNS configuration must be provided to support Prov and PA in a L2 geo-redundant configuration. Both Prov and PA use DNS to allow for Active/Active round-robin support.

• The geo-redundant LDAP configuration must be provided to support SS SESM, LSC SESM, and Prov in a L2 geo-redundant configuration. The SS SESM DoD Hybrid Routing (HR) and Local Number Portability (LNP) function and LSC SESM Commercial Cost Avoidance (CCA) function use LDAP for optimal routing lookup and Prov uses LDAP for subscriber routing updates.

• Edge Boundary Controller (EBC) is an optional ARTS architecture appliance located at the edge of a campus/enclave. When EBC is deployed, it is recommended that a pair of active/hot-standby EBCs is deployed for supporting high availability operations. Additionally, the EBC pair must support the service IP address takeover and the media, signaling and session state checkpointing to ensure no calls are dropped during the failover.
Preparing the secondary site

Application Server 5300 installation is performed according to normal procedures. The steps before and after the start of the standby SIP core servers at the secondary data center are summarized below. Before executing these steps, it is assumed that the Application Server 5300 system has already been installed and is running properly at the primary data center.

- Allocate IP addresses for the standby SIP core servers at the secondary data center
- Configure L2 and L3 switches for the standby SIP core servers at the secondary site.
- Configure the VLANs and subnets at the secondary data center.
- Make sure the primary data center and secondary data center communicating properly over the VLANs and subnets between two data centers.
- Follow the backup procedures on all servers. For more information, see Avaya Aura® Application Server 5300 Administration, NN42040-600
- Shut down and move all standby servers to the secondary data center.
- After starting the servers at the secondary data center, run separate IPv4 and IPv6 scripts to modify the default route pointing to the default routers located at the secondary data center.
- Make sure the time zone information is the same for both locations.
- If not already done at the primary site, from the AS 5300 Element Manager Console, under the Network Data folder, add a new site, "Site2". Then update the configuration of the servers that have been moved to reference this site.
- Attach the servers to the service network at the secondary site.
Chapter 5: Traffic flow analysis

Having discussed the physical reference network, logical reference networks, and the IP network recommendation, in the following sections, we will discuss the failure scenarios in the network and how the Application Server 5300 behaves under those conditions. The traffic flows will be depicted over the previously defined multi-subnet/VLAN logical reference network. This section first describes the normal Application Server 5300 traffic flows and the recovery flows of various failure conditions within a campus. The section then describes the intercampus normal and recovery flows for LSC/SS configurations.

Single campus normal traffic flows

The following figure shows the normal signaling flows traversing between clients, media servers, gateways, and the network elements (that is, SESM and PA) on the primary data center signaling subnet. The signaling flows are secured by establishing TLS/TCP connections between the endpoints. Note the AS 5300 Session Manager (AS 5300 SESM) in the chart can be either a regular (Non DoD) SESM, or a DoD SESM (that is, PBX1, LSC, or SS).
Figure 8: Normal signaling flow example

The following figure shows the normal OAMP flows traversing between the media servers, gateways and the Application Server 5300 OAMP elements on the primary data center Internal OAMP subnet. The OAMP flows between Application Server 5300 and the external OSS elements are communicated using the External OAMP subnet. Depending on the types of OAMP flows, they are secured by establishing either the TLS/TCP or IPSEC connections between the endpoints.
Figure 9: Normal OAMP flow example

The following figure shows the normal media flows traversing between clients, media servers and gateways over the media center Media subnet. The media flows can be secured using SRTP. Note that when the media centers are deployed outside of data centers, the media flows do not traverse and, therefore, impact the switching, routing, and bandwidth capacities of the data center networks.
Traffic flow analysis

Figure 10: Normal media flow example
Chapter 6: Failure scenario analysis

The failure conditions will be discussed include link failures, L2 switch failures, router failures, server failures, Application Server 5300 network element failures, media server and gateway failures, and site failures. The failure scenarios analysis provides better understanding of how Application Server 5300 L2 Geo-Redundancy configuration improves the survivability of an Application Server 5300 service network under various fault and disastrous conditions.

Navigation

• [Link failures](#) on page 23
• [Switch and router failure](#) on page 25
• [Server and network element failures](#) on page 26
• [Media server and gateway failure](#) on page 27
• [Site failure](#) on page 27

---

**Link failures**

The types of link failures include the server-L2 switch link failure, the L2 switch-L3 switch/router link failure, and the data center intersite link failure. These links are protected by subsecond failover, using redundant links, bonded interface, and 802.3ad logical trunk (see Figure 4: Physical redundancy eliminating a single point of failure on page 12). However, in a very unlikely event that there is a double link failure:

• Between an active server and L2 switch: the standby server will take over the active server functions and the requests will now be routed to the standby server using the primary data center stretched subnets. The endpoints will need to establish new TLS and IPsec sessions, but there is no impact to existing media traffic.
Failure scenario analysis

---

**Figure 11: Active server double link failure recovery example**

- Between a standby server and L2 switch: The requests will continue to flow to the active servers and there is no impact on the requests. There is no impact to existing media traffic.

- Between the primary data center L2 switch and the routers: The primary data center routers will stop advertising the data center subnets. Because the secondary data center routers are still advertising the data center subnets, the signaling and OAMP requests will continue to flow to the active servers using the secondary data center stretched subnets for processing. There is no impact to existing media traffic.

---

**Figure 12: Primary data center L2 switch double link failure recovery example**
• Between the secondary data center L2 switch and the routers: The requests will continue to flow to the active servers using the primary data center subnets. There is no impact to existing media traffic.

• Between the primary and secondary data centers: The primary and secondary data centers are isolated because all L1/L2 connections between the L2 switches are down. The standby servers start taking over the service IP addresses because they cannot receive the heartbeat responses from the active servers. This is the so-called Split-brain condition. Because the primary data center routers are advertising lower cost IP routes for the data center to the campus core network, the requests will continue to flow to the active servers using the primary data center switch/routers. When the inter-site connections are restored, the standby server will revert back to the standby state. There is no impact to existing media traffic. Note this is an extreme case, we do not expect it will happen in a properly protected networking environment.

Switch and router failure

The switching and routing functions are protected by using redundant switch and router pairs, server bonded interface, 802.3ad logical trunk, VRRP, and routing convergence. The failover time ranges from sub-second to a few seconds. Nevertheless, in a rare event, there can be a double switch or router failure conditions occur in the data centers:

• Both L2 Switches fail at the primary data center: The requests will continue to flow to the active servers using the secondary data center stretched subnets. There is no impact to existing media traffic.

Figure 13: Primary data center L2 switch double failure recovery example
• Both upstream routers/L3 switches fail at the primary data center: This case is similar to both L2 switch failure condition. The requests will continue to flow to the active servers using the secondary data center stretched subnets. There is no impact to existing media traffic.

• Both L2 Switches fail at the secondary data center: The requests will continue to flow to the active servers using the primary data center subnets. There is no impact to existing media traffic.

• Both upstream routers/L3 switches fail at the secondary data center: The requests will continue to flow to the active servers using the primary data center subnets. There is no impact to existing media traffic.

Server and network element failures

Application Server 5300 uses redundant server pair to protect single server failure condition. When an active Server and its associated network elements fail, it triggers failover to standby server instances. In the case of a PA server, the server failure can result in overall capacity reduction. However, in both cases, the services will continue. The endpoints will need to establish new TLS and IPsec sessions with the new active servers, but there is no impact to existing media traffic.

Figure 14: Server and network element failure recovery example
Media server and gateway failure

Application Server 5300 uses redundant media servers and gateways to protect the total media server or total PRI gateway failure conditions. When there are media servers and gateway failures, Application Server 5300 continues to provide services by distributing calls to the remaining media resources. The active calls connecting to the failed media resources will be dropped and new calls will need to be made to establish new media sessions. It is important that the service planners engineer Application Server 5300 with sufficient media resources capacity for processing the additional traffic resulting from media server and gateway failures. The data center network failures have no impact on the media resources if they are not deployed in the primary and secondary data centers.

![Media resource failure recovery example](image)

**Figure 15: Media resource failure recovery example**

Site failure

The following figure depicts the traffic flows after the primary site failure. After IP routing convergence, the endpoints will establish new TLS and IPsec sessions with the new active servers. All new requests will continue to flow to the secondary data center for services. The primary site failure has no impact on existing media traffic. All media resources are available to the SESMs running in the secondary data center as long as the reachability to the media centers is maintained. Note that there is no configuration change necessary for using the media resources from the secondary data center servers.
Failure scenario analysis

When the secondary data center fails, all new requests will continue to be processed at the primary data center as usual. If media resources are deployed in the data centers, the clients will need to re-establish the media sessions with the remaining media resources. There will be media resources reduction as result of a site failure.

Figure 16: Primary site failure recovery example
Chapter 7: Multiple LSC-only Geo-Redundant campus or enclave

When deploying LSC and SS SESMs, Application Server 5300 supports LSC SESM (LSC) only, SS SESM (SS) only, or both LSC+SS SESM types in a system. For a system contains only LSCs, Application Server 5300 requires only one Master LSC be configured and the remaining LSCs configured as Slave LSCs. All inter-enclave calls must traverse the Master LSC. If there is EBC fronting the enclave, the EBC must be configured to route all incoming calls to the Master LSC. The Master LSC will then route the call to end user or to the next Slave LSC for forwarding. The PRI gateways must be configured to route calls to the Master LSC. The Master LSC SESM can communicate with only one EBC.

Navigation

- EBC consideration on page 29
- Normal Multiple LSC signaling flow on page 30
- Master LSC failure recovery on page 31
- Slave LSC failure recovery on page 32

EBC consideration

Edge Boundary Controller (EBC) is an optional ARTS architecture appliance located at the edge of a campus/enclave. When EBC is deployed, it is recommended that a pair of EBCs be deployed for supporting high availability operations. Because the Master LSC SESM can communicate with only one EBC, the EBC pair must support the service IP address takeover when one of them fails. Additionally, the EBC pair must support the checkpointing of media, signaling and session state information to ensure the existing calls are not dropped during the takeover.
Normal Multiple LSC signaling flow

The following figure shows the signaling flow of a Slave LSC subscriber making a call to a remote enclave person. The call is first processed by the subscriber’s home Slave LSC, which execute translations to determine where the call should be sent next. The translations determine this is an interenclave call and because it is a slave LSC, the call needs to be routed through Master LSC. Because there is EBC fronting the enclave, the calls must be routed to EBC for forwarding.
Master LSC failure recovery

When the current active Master LSC fails, the Slave LSC will forward the calls to the new active Master LSC over the stretched signaling subnet for processing. The following diagram shows an example of Master LSC failure recovery flow.
Slave LSC failure recovery

When the current home Slave LSC fails, the calls are sent to the new active Slave LSC in the secondary data center over the stretched signaling subnet for processing. The calls then are forwarded to the Master LSC located in the primary data center for forwarding to the fronting EBC. The following figure shows an example of Slave LSC failure recovery flow.
Figure 20: Slave LSC failure recovery example
Chapter 8: SS-LSC Geo-Redundant campus or enclave

For an enclave that has more than one LSC SESM, only one LSC is the Master LSC and the remaining LSCs are Slave LSCs. The Master LSC is associated with only one local MFSS Softswitch (SS) SESM. Each SS SESM must be associated with all of the local or downstream LSC SESMs it serves. The PRI gateway must be configured to route calls to a local SS, which can be any one of the SS SESMs in the enclave where there are more than one SSs in the enclave.

Navigation
- Normal LSC-SS signaling flow on page 34
- Master LSC failure recovery on page 35
- SS SESM failure recovery on page 36

Normal LSC-SS signaling flow

All inter-enclave calls will traverse the Master LSC and its serving SS. The diagram below shows the signaling flow of a LSC subscriber making a call to a remote enclave person. The call is routed using the home LSC, SS, and the fronting EBC of the enclave.
Master LSC failure recovery

When the active LSC fails, the standby LSC takes over the service IP address. All calls into the primary data center will be forwarded to the new active Master LSC over the stretched signaling subnet for processing. After executing the translations, the LSC determines it is an inter-enclave call. The LSC forwards the call to its configured local SS, which then routes the call the fronting EBC. The following figure shows an example of Master LSC failure recovery flow.
SS SESM failure recovery

When the active SS fails, the standby SS takes over the service IP address. All calls into the primary data center will first be processed by subscriber’s home LSC, which is the only LSC. After executing the translations, the LSC determines it is an inter-enclave call. The LSC forwards the call over the stretched signaling subnet to the service IP of the SS located at the secondary data center. The SS then routes the call the fronting EBC. The following figure shows an example of SS SESM failure recovery flow.
Figure 23: SS SESM failure recovery example
Chapter 9: Limitations and restrictions

The Layer 2 (L2) Geographic Redundancy has the following limitations and restrictions.

- Application Server 5300 Simplex systems cannot support L2 Geographic Redundancy.
- Application Server 5300 Small Configuration does not support L2 Geographic Redundancy. To support L2 Geographic Redundancy, the system must be either configured as Medium or Large Configuration.
- Both the primary and the secondary data centers contain the same number of SIP core servers to ensure the integrity of L2 Geographic Redundancy configuration.
- Application Server 5300 is split between 2 separate sites, up to 500km as limited by customer LAN implementation and latency (that is, less than 20 ms one way delay)
- VLAN and L2 Geographic Redundancy support are not available until after the Application Server 5300 Release 1.0 to Release 2.0 upgrade is completed
- It is understood that if the Primary Database site is lost that the Avaya Aura® Provisioning Client and Avaya Aura® Application Server 5300 Personal Agent can only run in Read-Only mode because the Backup DB is Read-only. The Primary site and Database must be recovered or re-synchronized following the event to bring the system back to read/write mode.
- DNS is required to allow for Active/Active Prov/PA round-robin support. LDAP is required to support Department of Defense Hybrid Routing (HR), Local Number Portability (LNP) and Commercial Cost Avoidance (CCA) features. Both DNS and LDP, provided by the customer, must remain accessible in various geo-failure scenarios.
- Only two Avaya Media Server (MS) servers are permitted in a pool when the pool is extended between the primary and secondary sites. This limitation has no impact on Ad hoc, Announcements and Branding, Unified Communications, IM Chat, and Music on Hold server pools, but will reduce the Avaya MS Meet Me servers in a pool from eight to two.
- Current limitations on AudioCodes Element Management System will be the same for single- or split-site.
- Fault tolerance L2 Geographic Redundancy is supported for IPv6 in the same manner as for IPv4. However, the IPv6 SESM IP is not monitored, but will follow the failover of the IPv4 SESM IP address. If the IPv4 fails over to the secondary site, the IPv6 failover will also occur.