Avaya Port Matrix:

Avaya Aura® Contact Center 7.1.2.0 and Avaya Contact Center Select 7.1.2.0

Issue 1.0
Aug, 2021

ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC. DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA INC. MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE INFORMATION PROVIDED HEREIN WILL ELIMINATE SECURITY THREATS TO CUSTOMERS' SYSTEMS. AVAYA INC., ITS RELATED COMPANIES, DIRECTORS, EMPLOYEES, REPRESENTATIVES, SUPPLIERS OR AGENTS MAY NOT, UNDER ANY CIRCUMSTANCES BE HELD LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THE INFORMATION PROVIDED HEREIN. THIS INCLUDES, BUT IS NOT LIMITED TO, THE LOSS OF DATA OR LOSS OF PROFIT, EVEN IF AVAYA WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS INFORMATION CONSTITUTES ACCEPTANCE OF THESE TERMS.

1. Avaya Aura Contact Center and Avaya Contact Center Select Components

The following section covers components used by Avaya Aura Contact Center and Avaya Contact Center Select products.

Data flows and their sockets are owned and directed by an application. For all applications, sockets are created on the network interfaces on the server. For the purposes of firewall configuration, these sockets are sourced from the server, so the firewall (iptables service) should be running on the same server.

Application components within the AACC and AACS application are listed as follows. Any ACCS specific detail will be preceeded by the lable “ACCS:” , all other details that are not lablled as “**ACCS:**” apply to both AACC and ACCS.

1.1 SIP Gateway Manager (SGM)

Component	Protocol	Description
SIP Avaya Aura Contact Center - SIP Gateway Manager (SGM)	TCP/TLS/UDP	SIP , SIMPLE , WebService, TLS traffic to/from SGM on this interface. SGM handles Voice and Instant Messaging traffic over SIP (to SM, AMS) , TLS (to AES) and Web Services (SOAP to XMPP adapter) **ACCS:** SGM handles TLS and TCP to/from IP Office for AACS
SIP Avaya Aura Contact Center – XMPP Adapter	XMPP Protocol / Web Services	Avaya Presense Server communicates with SIP AACC via the XMPP adapter via XMPP protocol which in turn communicates with SIP SGM via Web Services (SOAP)
SIP Avaya Aura Contact Center – Management Client	RMI	Management Client mointers the transport connections that SGM maintains during its running stage and indicates if one or more of the connections has been lost in realtime.

1.2 Contact Center Manager Administration (CCMA)

Component	Protocol	Description
Avaya Aura Contact Center – Real Time Display Service	TCP\UDP	The real-time display service process the real-time IP multicast\unicast data streams from the Contact Center Manager Servers(CCMS) and subsequently make this real-time data available over its own IP multicast\unicast data streams for client use.
Avaya Aura Contact Center – Emergency Help Service	UDP	Provides real-time display notification to supervisors when an agent presses the emergency key. This real-time notification is over a IP multicast stream.

Component	Protocol	Description
Avaya Aura Contact Center – License Manager Service	UDP	The license manager service communicates with the Avaya Aura License Manager server for Report Creation Wizard (RCW) licensing.
Microsoft Internet Information Server (IIS)	HTTP	IIS is a web application server used to host the Avaya Aura Contact Center Manager Administration (CCMA) application and supported web services.
CCMAReportService	TCP	This is used to run historical reports
ACCS: IP Office and ACCS Sync Service to IP Office	TCP	This is a User Synchronisation Service that synchronises supervisor and agent accounts on ACCS with their corresponding user accounts on the IP Office. For example, an agent created on ACCS will have a user account automatically created for this agent on IP Office. A user account specifies the telephone details on IP Office.

1.3 Communication Control Toolkit (CCT)

Component	Protocol	Description
CCT Server Service	TCP / HTTP Web Services	The CCT Server Service provides the interfaces for CCT Clients via TCP and the interface to the CMF through CMF Web Services via HTTP.
CCT Integration Portal	HTTP	The CCT Integration Portal is hosted on IIS and provides interfaces for CCT Clients via WebSockets over HTTP.
CCT Web Admin	HTTP	The CCT Web Administration tool is hosted in a Tomcat application server and provides a web based interface for configuration of CCT.
CCT DAL Web Service Layer	HTTP	The CCT DAL Web Service layer provides a web service interface to the CCT DAL component. The CCT DAL component manages interaction with the CCT Database. The CCT DAL Web Service Layer is used by the CCT Web Admininstration tool for interactions with the CCT Database.
TAPI Connector / TAPI Service Provider	TCP	The TAPI Connector / TAPI Service Provider manages the interactions between CCT and the CCMS server in AML environments, and the direct connect to the CS1K in Knowledge Worker environments.
CCT Licensing	UDP	The CCT Licensing service connects to the License Manager to handle licensing in CCT.
System Management and Monitoring Component (SMMC)	TCP	SMMC is installed on the CCT server in High Availablitiy configurations and handles communication between the Active and Standby CCT servers.

1.4 Avaya Agent Desktop (AAD)

Component	Protocol	Description
Avaya Agent Desktop		This is the client Application used by Supervisors & Agents to login to Elite or AACC and handle Customer requests. The AAD does not open any deicated ports for communication but in the table of Ports in section 2 table 4 we have provided a list and port number of all the backend systems it is possible for this client to connect to. There is also a description of the purpose of each connection. Note that no one system will use all 13 connections listed there.

1.5 Contact Center Manager Server (CCMS)

Component	Protocol	Description
Avaya Aura Contact Center – Control Service	TCP	Service Controller for CCMS services. Monitors CCMS services aswell if Service Monitoring is enabled in a High Availability setup.
Avaya Aura Contact Center – MAS Service Manager	TCP	Responsible for the safe and continued operator of all registered CCMS services.
Avaya Aura Contact Center – MAS Service Daemon	TCP	Started and restarts the MAS Service Manager when required.
Avaya Aura Contact Center – MAS Security	TCP	Provides access, password encryption, administrative and audit services for CCMS.
Avaya Aura Contact Center – MAS Event Scheduler	TCP	Schedules and executes CCMS-related service requests to remote fat and thin clients.
Avaya Aura Contact Center – MAS OM Server	TCP	Provides monitoring services of CMMS-related resources.

Component	Protocol	Description
Avaya Aura Contact Center – MAS Configuration Manager	TCP	Provides a wide-ranging data services to requesting components about the state of the CCMS.
Avaya Aura Contact Center – Naming Service	TCP	Resolves logical CCMS addresses into physical IP addresses.
Avaya Aura Contact Center – Operations, Administration and Maintenance (OAM) Service	TCP/UDP/TLS	Framework that provides data, controls and communicates changes made to core CCMS data.
Avaya Aura Contact Center – NBTSM Service	TCP	Implements the Service Provider Abstraction Layer to the rest of CCMS components.
Avaya Aura Contact Center – Audit Service	TCP	Processes all notifications created by the local OA&M service and generates appropriate actions.
Avaya Aura Contact Center – NINCC Audit Service	TCP	Service that runs on an Avaya Aura Contact Center NCC setup only which polls the database connectivity to Nodal Servers
Avaya Aura Contact Center – Nodal Operations, Administration and Maintenance (NDLOAM) Service	TCP/UDP	Service that runs on an Avaya Aura Contact Center with Networking enabled (nodal server) that processes OAM messages to/from a single dedicated NCC CCMS.

Component	Protocol	Description
Avaya Aura Contact Center – NCC Operations, Administration and Maintenance (NCCOAM) Service	TCP/UDP	Service that runs on an Avaya Aura Contact Center NCC setup(nodal server) that processes OAM messages to/ from satelite NDL CCMS.
Avaya Aura Contact Center – NITSM Service	TCP	Dependant on NBTSM Service.
Avaya Aura Contact Center – Historical Data Collector (HDC) Service	TCP	Calculates CCMS historical reporting statistics from agent workflow and contact processing events.
Avaya Aura Contact Center – XMPP Service	TCP	XMPP adaptor for the Aura Presence Server.
Avaya Aura Contact Center – Agent Skillset Management (ASM) Service	TCP/UDP	Responsible for agent management and skillset queuing.
Avaya Aura Contact Center – Content Management Framework (CMF) OAM Bridge Service	TCP/UDP	Service that allows communication between OAM and CMF.
Avaya Aura Contact Center – Statisical Data Management Configuration and Administration (SDMCA) Service	TCP/UDP	Provides a cache of CCMS agent and skillset IDs and assignments and other OAM data for use by the Stastical Data Manager components.

Component	Protocol	Description
Avaya Aura Contact Center – Task Flow Administration (TFA) Service	TCP/UDP/TLS	CORBA / Win32 Service to allow 3rd party applications to register for Call Data.
Avaya Aura Contact Center – Task Flow Execution (TFE) Service	TCP/UDP	Responsible for the routing of Telephone Calls and Multimedia contacts.
Avaya Aura Contact Center – MLSM Service	TCP/UDP	Allows third party CTI applications call control ability.
Avaya Aura Contact Center – Voice Services Management (VSM) Service	TCP/UDP	Provides the ability to play Voice Services to calls placed to the contact center.
Avaya Aura Contact Center – Session Inititiation Protocol (SIP) Service	TCP/UDP	SIP Gateway
Avaya Aura Contact Center – Event Broker (EB) Service	TCP/UDP	Distributes internal CCMS agent workflow and contact processing events to the reporting services.
Avaya Aura Contact Center – Real-time Data Collector (RDC) Service	TCP/UDP	Calculates CCMS real-time reporting statistics from agent workflow and contact processing events.
Avaya Aura Contact Center – Historical Data Collector (HDC) Service	TCP/UDP	Manages the bulk loading of CCMS historical reporting data into the databaseand consolidates

Component	Protocol	Description
Avaya Aura Contact Center – ES Service	TCP/UDP	CORBA Service to allow 3rd party applications to recieve Agent related events.
Avaya Aura Contact Center – Statistical Data Propagation (SDP) Service	TCP/UDP	Propagates CCMS real-time statistical data to reporting clients.
Avaya Aura Contact Center – Contact Center Web Statistics (CCWS) Service	TCP/TLS	Contact Center Web Stats Server
Avaya Aura Contact Center – RSM Service	TCP/TLS	CORBA / IP Multicast to provide basic status reporting capability to third-party application.
Avaya Aura Contact Center – Intrinsic Statistics (IS) Service	TCP	Provides contact intrinsic statistics data to the CCMS task flow engine for use in scripting.
Avaya Aura Contact Center – Task Flow Administration (TFA) Bridge Service	TCP/UDP/TLS	Win32 Proxy service to allow for RPC calls to CORBA.
Avaya Aura Contact Center – Task Flow Execution (TFE) Bridge Connector Service	TCP/UDP	TFE Bridge Connector for Cisco integration
Avaya Aura Contact Center – MAS Time Service	TCP	Allows CCMS server time to be synched on a continuous basis with the M1 Switch.

Component	Protocol	Description
Avaya Aura Contact Center – NBMSM Service	TCP	Multimedia Services Manager
Avaya Aura Contact Center – Universal Networking Engine (UNE) Service	TCP	Universal Networking Engine
Avaya Aura Contact Center – Event Broker Web Service (EBWS) Service	TCP/HTTP	Provides a SOAP interface to legacy reporting components.
Avaya Aura Contact Center – Avaya Reporting (AR) Connector Service	TCP	Avaya Reporting Connector for AACC events.

1.6 License Manager (LM)

Component	Protocol	Description
CC_LM	UDP	AACC License manager server, PLICD.exe
NILM	UDP	AACC License manager client interface for LM Clients e.g. CCMS, CCMA LMService, CCT, CCMM LM Service and AACC HA shadowing licenses. This is an internal AACC component.

1.7 Intersystems Cache Database

Component	Protocol	Description
CCDSInstance	TCP	AACC Cache Database Instance
System management portal	HTTP	Intersystems Cache System management tool for DB management. Installed on AACC for use by Avaya Support. End-user access not granted.
Cache Terminal	TCP	Telnet client application for Cache DB support, utilities, for use by Avaya Support
Cache SNMP	TCP	Internal Cache service, for sending SNMP traps raised by AACC database and HA feature.

1.8 Contact Center Multimedia (CCMM)

Component	Protocol	Description
Avaya Aura Contact Center – Campaign Scheduler Service	TCP	Avaya Contact Center Real Time Aware Outbound Campaign Scheduler Service
Avaya Aura Contact Center – Email Manager	TCP	Avaya Contact Center Multimedia Email Manager Service provides Email handling functionality
Avaya Aura Contact Center – License Service	UDP	Avaya Contact Center MultiMedia Licensing Service
Avaya Aura Contact Center – Multimedia Contact Manager	TCP	Avaya Contact Center Multimedia Contact Manager Client Service (MCMC)
Avaya Aura Contact Center – OAM Service	TCP	Avaya Contact Center Multimedia OAM Service.

Component	Protocol	Description
Avaya Aura Contact Center - Predictive Outbound Blending	TCP	Contact Center Multimedia Predictive Outbound Blending Service
Avaya Aura Contact Center - Predictive Outbound Service	TCP	CCMM Predictive Outbound Service
Avaya Aura Contact Center - Starter Service	TCP	Avaya Contact Center MultiMedia Starter Service
Avaya Aura Contact Center – POMProxy Service	TCP	Avaya Contact Center POMProxy Service proxies all traffic to the POM Agent Manager Service
Avaya Aura Contact Center – POM Reporting Service	TCP	Avaya Contact Center POM Reporting Service communicates POM reporting events to EB.

1.9 Avaya Aura Media Server

Component	Protocol	Description
Avaya Aura Media Server	The Avaya Aura Media Server (AAMS) delivers advanced multimedia processing features to a broad range of products and applications. AAMS deploys on standard server hardware. It is a highly scalable software based solution that utilizes the latest open standards for media control and media processing. Network traffic in and out of AAMS can be broken into the four main categories described below. Each category of traffic can optionally be assigned to a separate physical network interface on the server.	
	Signalling	AAMS communicates with other telephony infrastructure elements via multiple signaling protocols and supports UDP, TCP and TLS transport options. When used with AACC, AAMS communicates directly with AACC over SIP and HTTP (RESTful web services).
	Media	Media traffic to/from AAMS is in the form of RTP/RTCP streams. Media traffic is not relayed through AACC but negotiated for direct exchange with the media endpoints (eg. telephone sets and media gateways) involved in contact center calls.

Component	Protocol	Description
	Cluster	AAMS servers can be configured to operate in a clustered fashion, for load balancing and resiliency purposes. AAMS utilizes a number of proprietary and standard protocols to allow for co-operation between multiple servers in a cluster.
	OAM	Operations, Administration and Maintenance (OAM) activities are primarily performed via a web-based administration interface named 'Element Manager'. In addition to this, AAMS also supports a SOAP-based web-service interface for administration, content store management and application invocation. Unlike the above traffic categories, which are typically associated with a specific physical network interface on the host machine, OAM traffic is generally always configured to be accepted by any network interface (including the local loopback interface).

1.10 Avaya Greeting Recorder

Component	Protocol	Description
Agent Greeting Recorder	The Agent Greeting (AG) recorder application allows contact center agents to pre-record customer greetings via a telephony user interface. These recordings are subsequently played back to customers via AAMS when agents answer incoming customer calls. AG recorder utilizes AAMS features including the RESTful User Agent interface and VXML interpreter to perform its function. The AG recorder operates atop the Contact Center Tomcat application server installed along with CCMS.	
	SIP	AG accepts inbound SIP calls from a SIP proxy, via UDP, TCP or TLS transport protocols (TCP by default).
	HTTP(S)	AG initiates outbound communications to both CCMA and AAMS via REST and SOAP web services over HTTP(S) connections. AG also accepts inbound HTTP(S) requests from AAMS to serve VXML dialogs to the AAMS VXML interpreter and from browsers in order to host a basic web service-based administrative interface.

1.11 Enterprise Web Chat

Component	Protocol	Description
Agent Controller	WebSockets	Communication end-point for Agent to Customer interaction.
Customer Controller	RESTFul Web Services, WebSockets, SOAP	Communication end-point for Customer to Agent interaction.
Ejabberd	REST & TCP	Provides and endpoint for Agent Custom Desktop to facilatate Chat.

1.12 Workspaces Cluster

Component	Protocol	Description
kafka topics	Own protocol based on TCP	messaging system that collects and processes extensive amounts of data in real-time
admin-adapter	TCP	Allow communication between AACC and kafka topics
istio	HTTP/HTTPS	The network deployed services with load balancing
kubernetes dashboard		web-based Kubernetes user interface
api server	TLS	validates and configures data for the api objects which include pods, services, replication controllers, and others
etcd	TLS	lets any of the nodes in the Kubernetes cluster read and write data
kublet	TLS	responsible for maintaining a set of pods, which are composed of one or more containers, on a local system

2. Port Usage Tables

2.1 Port Usage Table Heading Definitions

Ingress Connections (In): This indicates connection requests that are initiated from external devices to open ports on this product. From the point of view of the product, the connection request is coming "In". (Note that in most cases, traffic will flow in both directions.)

Egress Connections (Out): This indicates connection requests that are initiated from this product to known ports on a remote device. From the point of view of the product, the connection request is going "Out". (Note that in most cases, traffic will flow in both directions.)

Intra-Device Connections: This indicates connection requests that both originate and terminate on this product. Normally these would be handled on the loopback interface, but there may be some exceptions where modules within this product must communicate on ports open on one of the physical Ethernet interfaces. These ports would not need to be configured on an external firewall, but may show up on a port scan of the product.

Destination Port: This is the default layer-4 port number to which the connection request is sent. Valid values include: 0 – 65535. A "(C)" next to the port number means that the port number is configurable. Refer to the Notes section after each table for specifics on valid port ranges.

Network/Application Protocol: This is the name associated with the layer-4 protocol and layers-5-7 application.

Optionally Enabled / Disabled: This field indicates whether customers can enable or disable a layer-4 port changing its default port setting. Valid values include: Yes or No

"No" means the default port state cannot be changed (e.g. enable or disabled).

"Yes" means the default port state can be changed and that the port can either be enabled or disabled.

Default Port State: A port is either open, closed, filtered or N/A.

Open ports will respond to queries

Closed ports may or may not respond to queries and are only listed when they can be optionally enabled.

Filtered ports can be open or closed. Filtered UDP ports will not respond to queries. Filtered TCP will respond to queries, but will not allow connectivity.

N/A is used for the egress default port state since these are not listening ports on the product.

External Device: This is the remote device that is initiating a connection request (Ingress Connections) or receiving a connection request (Egress Connections).

2.2 Port Tables

Below are the tables which document the port usage for this product.

2.2.2 Contact Center (inc CCMS,CCMA,SGM,CCT,Agent Greeting Recorder,Licence Manager,Cache)

Source (Client)		Destination (Server)					
System	**Port (Configurable Range)**	**System**	**Port (Configurable Range)**	**Network / Application Protocol**	**Optionally Enabled / Disabled?**	**Default Port State**	**Description**
Web Browser + IP Office	Ephemeral	IIS (CCMA) + IIS (CCMA Web Services)	80	HTTP	Yes	Open	HTTP port used by Internet Information Server (IIS) ACCS: Ports on the ACCS platform that are used by Sync Service to communicate with IP Office
Web Browser + IP Office	Ephemeral	IIS (CCMA) + IIS (CCMA Web Services)	443	HTTPS	Yes	Open	HTTPS port used by Internet Information Server (IIS) for secure communication using SSL ACCS: Ports on the ACCS platform that are used by Sync Service to communicate with IP Office using SSL
AACC/ACCS RSM Clients	Ephemeral	AACC / ACCS RSM	6020,6030,6040,6050,6060, 6070, 6080, 6090,6100,6110,6120,6130	UDP	Yes	Open	Multicast ports used by multicast statistical data. CCMA Real-Time Reporting and Agent Desktop Displays use RSM.

Web Browser	Ephemeral	CCMA ICEEmHlpService Service	8200	UDP	Yes	Open	Port used by the Emergency Help component on the client PC
CCMA IceRTDService Service	7020, 7030,, 7040, 7050, 7060, 7070, 7080, 7090, 7100, 7110, 7120, 7130,7140,7150	Web Browser		UDP	Yes	Open	Ports used by the CCMA server to send IP multicasting data to client PCs (needed for Real-Time Reporting and Agent Desktop Displays).
CCMA IceRTDService Service	7025, 7035, 7045, 7055, 7065, 7075, 7085, 7095, 7105, 7115, 7125, 7135,7145,7155	Web Browser		UDP	Yes	Open	Ports used by the CCMA server to send IP unicast data to client PCs
CCMA Historical Reporting	25			SMTP	Yes	Open	For the Historical Reporting component to send email notifications when reports are printed and saved.
CCMA Server	Ephemeral	IP Office	8443	HTTPS	No	Open	**ACCS:** Port on the IP Office platform used by the IP Office-CC Sync Service to communicate to the IP Office

AACC/ACCS Server	Ephemeral	AACC/ACCS Server	445	TCP	Yes	Open	Windows File and Printer Sharing. Required when copying data between active and standby servers using Windows File Sharing
AACC Toolkit Applications	Ephemeral	CCMS	10000	TCP	No	Open	Inter-process communication using CCMS Toolkit.
License Manager Clients	Ephemeral	License Manager	3998	UDP	No	Open	License Manager destination port.
CCMA Server	Ephemeral	License Manager	3999 - 4007	UDP	No	Open	License Manager destination source port.

SIP Stack (SGM)	Ephemeral	AAMS/SM/Lync/CS1K/IPO	5060	TCP/UDP	No	Open	Listening port for SIP TCP/UDP communication
SIP Stack (SGM)	Ephemeral	AAMS/SM/CS1K/IPO	5061	TLS	Yes	Open	Listening port for SIP TLS communication.
SIP Stack (SGM)	Ephemeral	AAMS	5070	TCP/UDP	No	Open	Listening port for SIP TCP/UDP communication to AAMS when AAMS is installed co-resident with AACC In 7.0.3 AMS is changing from Port **5070** to **5060** Recommendation to close port **5070** after upgrade to 7.0.3
SIP Stack (SGM)	Ephemeral	AAMS	5071	TLS	Yes	Open	Listening port for SIP TLS communication to AAMS when AAMS is installed co-resident with AACC. In 7.0.3 AMS is changing from Port **5071** to **5061** Recommendation to close port **5071** after upgrade to 7.0.3

SIP Stack (Agent Greeting Recorder / Announcement Recorder)	Ephemeral	SM	5080	TCP/UDP	No	Open	Listening port for Agent Greeting Recording / Announcement Recorder
SIP Stack (Agent Greeting Recorder / Announcement Recorder)	Ephemeral	SM	5081	TLS	Yes	Open	Listening port (TLS) for Agent Greeting Recording / Announcement Recorder
SGM	Ephemeral	Management Client	8100	TCP (JMX)	Yes	Open	**INTERNAL ONLY** JMX Management client which monitors SGM transport states.
SGM	Ephemeral	JMX Client (OAM)	3413	SSL (JMX)	Yes	Open	**INTERNAL ONLY** JMX client which monitors SGM transport states (OAM) tunneled over SSL.

SGM	Ephemeral	JMX Client (SIP)	3571	SSL (JMX)	Yes	Open	**INTERNAL ONLY** JMX client which monitors SGM transport states (SIP) tunneled over SSL.
SGM	Ephemeral	IP Office	50796	TLS	No	Open	**ACCS Specific:** Egress port for all CTI message communications between IP Office and ACCS
Web Browser	Ephemeral	AACC - Tomcat	8081	HTTP	No	Open	Default non-SSL HTTP port of the Contact Center Tomcat Instance which hosts the following applications: Agent Greeting, Announcement Recorder, CCT Web Administration. McAfee Agent Common Services (macmnsvc.exe) or McAfee Framework Service (FrameworkService.exe) are services that can use port 8081. If these services are required, then the Apache Tomcat port must be changed. Refer to section: "Adding Communication Control Toolkit to CCMA" in the commissioning guide to change the CCT Console port used. If these services are not required then they can be stopped and configured not to run on startup in Windows Services..

CCT Remote Admin Client – local really	Ephemeral	AACC - DAL	9000	HTTP	No	Open	Data Access Layer Service listens for requests from CCT Remote Administration Console.
CCT Client and AAD	Ephemeral	AACC – CCT Server	29373	TCP	No	Open	Listens for requests from CCT client applications.
3rd Party Clients	Ephemeral	AACC – CCT OI	9080,9083, 9090	HTTP/HTTPS SOAP	Yes	Open	CCT Open Interfaces, CTI Web Services, OI Splash page
Web Browser	Ephemeral	AACC - Tomcat	8445	HTTPS	No	Open	Default HTTPS port of the Contact Center Tomcat Instance which hosts the following applications: Agent Greeting, Announcement Recorder, CCT Web Administration

Simple Browser Based Agent Client	Ephemeral	AACC - IIS	443	HTTPS	No	Open	CCT Integration Portal. Default HTTPS port for IIS which Integration Portal server used by the Simple Browser Based Agent Client
AACC/ACCS Server	Ephemeral	AACC/ACCS Server	3000	TCP	Yes	Open	**INTERNAL ONLY** For TAP Iswitch connection through MLS (CCMS server). This port is required for the contact center subnet.
AACC/ACCS Server	Ephemeral	GigaSpaces	4174	TCP	No	Open	Nicmfjvm service
AACC/ACCS Server	Ephemeral	GigaSpaces	8098	TCP	No	Open	**INTERNAL ONLY** JINI remote access to a SP Container.
CCT Server	Ephemeral	CMF Host	11111	HTTP	No	Open	**INTERNAL ONLY** Used by the CCT Server service for the CMF Web Service – Web server port.

CMF Host	Ephemeral	AACC – CCT Server	11110	HTTP	No	Open	**INTERNAL ONLY** Used by the CCT Server service for the CMF Web Service - Callback port.
CCT Server	Ephemeral	AACC - CCT	5000	TCP	Yes	Open	**INTERNAL ONLY**
CCT Components	Ephemeral	AACC - CCT DAL	1972	TLS	No	Open	**INTERNAL ONLY** For CCT services to access the CCT database.
Cache	Ephemeral	AACC	1972 8085	TLS	Yes	Open	Cache CCDSInstance port, used for SQL gateway connection between NCC,Nodes , Integrated reporting and shadowing

Cache CCDSInstance	Ephemeral	AACC/ACCS	4001	HTTP	Yes	Open	Cache License server runs on default port 4001
Cache System Management Portal	Ephemeral	AACC / ACCS Cache	57772	HTTP	Yes	Open	**INTERNAL ONLY** The port number to use for the Web server. A standard Caché installation sets the Web server port number to the first unused port number greater than or equal to 57772
JDBC Gateway port	Ephermeral	AACC/ACCS	62972	UDP	Yes	Open	Port number for the JDBC Gateway
License Manager	Ephermeral	AACC/ACCS	3998	UDP	Yes	Open	License Manager Desitination port
License Manager	Ephermeral	WebLM	8444	TLS	Yes	Open	Secure Port (TLS) for Licence Manager Server by default when WebLM is local (Co-Res) Configurable in TomCat Server.xml and LM configuration utility.

LM Clients	4000-4036	AACC/ACCS	Ephermeral	UDP	Yes	Open	The ports used are based off the client ID. So CCMS with 10000, ports 4000-4003, CCMA 10001 port 4004-4007
AACC/ACCS	Ephermeral	AACC/ACCS HA	445	TCP	Yes	Open	TCP port used Windows File and Printer Sharing for Microsoft Networks. Required when copying data between active and standby servers using Windows File Sharing.
HDX CAPI Client Applications	Ephermeral	AACC/ACCS HDX	1150	TCP	Yes	Open	1550 is the request port for RPC applications. 3rd party applications communicating with HDX.
Applications looking for AACC / ACCS CORBA services.	Ephermeral	TAO Naming Service	4422	TCP	Yes	Open	Port 4422 is the naming service port for Corba applications.

Toolkit Naming Service	Ephermeral	AACC/ACCS	1000	TCP	Yes	Open	Toolkit Naming Service
Toolkit Naming Service	Ephermeral	AACC/ACCS	1000	TCP	Yes	Open	Toolkit Naming Service
AACC/ACCS Networking	Ephermeral	AACC/ACCS Node	10001-10082	TCP	Yes	Open	AACC/ACCS Local/Remote site nodes
AACC/ACCS Networking	Ephermeral	AACC/ACCS Node	10039	TCP	Yes	Open	NCP_CHANNEL—This channel is used to communicate between the NCP of one node to the NCP of another node. The NCP on one node sends sanity messages to the other node
AACC/ACCS Networking	Ephermeral	AACC/ACCS Node	10038	TCP	Yes	Open	ASM_CHANNEL—Different modules like NCP and TFE send messages to ASM through this channel.

AACC/ACCS Networking	Ephermeral	AACC/ACCS Node	10040	TCP	Yes	Open	NCP_ASM_CHANNEL—ASM uses this channel to send messages to NCP.
AACC/ACCS Networking	Ephermeral	AACC/ACCS Node	10060	TCP	Yes	Open	ASM_Service—The ASM service runs on this port. The Service Control Manager can send messages such as START, STOP, and RESTART to the ASM service through this port.
AACC/ACCS Networking	Ephermeral	AACC/ACCS Node	10062	TCP	Yes	Open	NCP_Service—The NCP service runs on this port. The Service Control Manager can send messages such as START, STOP, and RESTART to NCP on this port.
Remote Desktop Client	3389	AACC/ACCS Desktop and AAMS when installed co-resident with AACC/ACCS	Ephermeral	TCP	Yes	Open	Remote Desktop Connection Support

3rd Party Clients	9070-9073	AACC/ACCS OI - Open Networking	Ephermeral	HTTP-HTTPS	Yes	Open	CCMS Open Interfaces Open Q and Open Networking
AAD	Ephermeral	AACC/ACCS Web Statistics	9086	TCP	Yes	Open	CC Web Statistics
SMMCService.exe / NetworkManagement.dll	Ephermeral	AACC/ACCS	57012	UDP	Yes	Open	UDP Listener, initiated by networkManagement.dll.System Management and Monitoring Component (SMMC) system tray. Used by the High Availability feature.
SystemController	Ephermeral	AACC/ACCS	49244 / 49247	TCP	Yes	Open	java.exe / SystemController
java.exe / SystemController	Ephermeral	AACC/ACCS	61616	TCP	Yes	Open	local ActiveMQ Broker, started as Spring Bean. local java.exe / smmc-systemtray-0.0.1-SNAPSHOT.jar, local SMMCService.exe remote java.exe / SystemController

java.exe / SystemController	Ephermeral	AACC/ACCS HA	1099	TCP	Yes	Open	JMX Exposure
Universal Networking	Ephermeral	AACC/ACCS UNE	9119	HTTPS	Yes	Open	Universal Networking port.
CCT REST	Ephermeral	AACC/ACCS	9085, 9091	HTTP/HTTPS	Yes	Open	CCT REST
AACC / ACCS	Ephermeral	CCMS ASM	5055	TCP	Yes	Open	

AACC / ACCS	Ephermeral	CCMS TFE	5056	TCP	Yes	Open	
AACC / ACCS	Ephermeral	CCMS EBWS	7081	TCP	Yes	Open	

2.2.3 Contact Center Multi Media (CCMM)

Source (Client)		Destination (Server)		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
AACC/ACCS	Ephemeral	Caché database	1972	TLS	Yes	Open	Port opened on database for reporting. Caché database, and Caché shadowing in High Availability solutions.
CCMM	Ephemeral	E-mail server	110	POP3	Yes	Open	Receiving e-mail
CCMM	Ephemeral	Windows File and Printer Sharing for Microsoft Networks.	445	TCP	Yes	Open	Windows File and Printer Sharing for Microsoft Networks. Required when copying data between active and standby servers using Windows File Sharing.
CCMM	Ephemeral	E-mail server POP3 over TLS	995	POP3 over TLS	Yes	Open	Receiving secure e-mail
CCMM	Ephemeral	E-mail server	25	SMTP	Yes	Open	Sending e-mail
Any Web services client (Agent Desktop, OCMT, and third-party Web services)	Ephemeral	CCMM	80	HTTP - SOAP	Yes	Open	Accessing http Web services
SMMCService.exe / NetworkManagement.dll	Ephermeral	CCMM	57012	UDP	Yes	Open	System Management and Monitoring Component (SMMC) system tray. Used by the High Availability feature.
CCMM	Ephemeral	LDAP Server	389	TCP/UDP	Yes	Open	Address book service used to retrieve entries from LDAP. Can be TCP or UDP.

CCMM	Ephemeral	IMAP Server	143	TCP	Yes	Open	Used by EmailManager Service to connect to mailbox over IMAP protocol for email retrieval
CCMM	Ephemeral	POM Server	9970	TCP	Yes	Open	Used by POMProxy Service to exchange messages with POM Agent Manager Service
CCMM	Ephemeral	Ejabberd	4369	TCP	No	Open	Responsible for Clustering on HA installations. Erlang epmd.
CCMM	Ephemeral	Ejabberd	50000	TCP	No	Open	Responsible for Clustering on HA installations. Only used for HA switchover.
CCMM	Ephemeral	Ejabberd	50001	TCP	No	Open	Responsible for Clustering on HA installations. Only used for HA switchover.
External Web Server	Ephemeral	Tomcat	8445	HTTPS	No	Open	Tomcat web server with security on.
External Web Server	Ephemeral	Tomcat	8081	HTTP	No	Open	Tomcat web server with security off.

2.2.4 Aura Agent Desktop (AAD)

Source (Client)		Destination (Server)		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Avaya Agent Desktop	Ephemeral	CCMM Server	80	HTTP	Yes	Open	HTTP port connected to by AAD to call Web services via Internet Information Server (IIS) on the CCMM Server. This retrieve all the data related to Multimedia contacts and Customers.
Avaya Agent Desktop	Ephemeral	CCMM Server	443	HTTPS	Yes	Open	HTTPS port connected to by AAD for Internet Information Server (IIS) for secure communication using TLS on the CCMM Server
Avaya Agent Desktop	Ephemeral	CCMS Server	7081	HTTP	Yes	Open	HTTP port connected to by AAD to call Web services on the CCMS Server. This connection is used to report on Peer to Peer IMs.
Avaya Agent Desktop	Ephemeral	Avaya Presence Server	5222 (fixed, jabber protocol)	TCP	Yes	Open	Port connected to by AAD when communicating with Avaya Aura Presence Server to retrieve/puiblish Presence information and Ims chats.

Avaya Agent Desktop	Ephemeral	CCMS Server	9086	HTTP	Yes	Open	HTTP port connected to by AAD to call Web services on the CCMS Server. This connection is required to display Agent Web Statistics on the AAD.
Avaya Agent Desktop	Ephemeral	Communication Manager	(6225 - 106275)	.H323	Yes	Open	.H323 connection for direct control of workstations or use of the inbuilt softphone on a Avaya switch.
Avaya Agent Desktop	Ephemeral	Microsoft Lync Server	5060	TCP	Yes	Open	Port connected to by AAD when communicating with Microsoft Lync as a Presence/IM provider.
Avaya Agent Desktop	Ephemeral	Microsoft Lync Server	5061	TLS	Yes	Open	Port connected to by AAD when communicating securely with Microsoft Lync as a Presence/IM provider.
Avaya Agent Desktop	Ephemeral	Predictive sever	40000	TCP	Yes	Open	Port connected to by AAD when communicating with the SER Predictive Server in a Predictive Outbound environment with a SER dialer.
Avaya Agent Desktop	Ephemeral	CCMS Server	9086	HTTP	Yes	Open	HTTP port connected to by AAD to call Web services on the CCMS Server. This connection is required to display Agent Web Statistics on the AAD.
Avaya Agent Desktop	Ephemeral	CCMM Server	8445	HTTPS	No	Open	Tomcat web server with security on.
Avaya Agent Desktop	Ephemeral	CCMM Server	8081	HTTP	No	Open	Tomcat web server with security off.

2.2.5 Avaya Aura Media Server (AMS)

Source		Destination		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
SSH Client	Ephermeral	AAMS on Red Hat Linux only	22	TCP	Yes	Open	Accessing AAMS Red Hat Linux server using SSH (e.g. putty)
AAMS	Ephermeral	SNTP Server	123	UDP	No	Open	AACC/ACCS/AAMS accessing Simple Network Time Protocol Server (SNTP)
SNMP Client	Ephermeral	AACC/ACCS/AAMS	161	UDP	Yes	Open	UDP port for receiving SNMP queries
AAMS	Ephermeral	SNMP Client	162	UDP	Yes	Open	UDP port for sending SNMP trap messages
MySQL Server on other AMS	Ephermeral	MySql Server on AMS	3306	TCP	No		MySQL Server Listening port
Windows Remote Desktop client	Ephermeral	Microsoft Remote Desktop for Windows Servers	3389	TCP			**WINDOWS ONLY**
AAMS Linux HA	Ephermeral	AAMS HA System monitor	1028	TCP	No*	Open if HA	AAMS HA system monitor uses 1028 to communicate heartbeat to AAMS HA peer.
AAMS	Ephermeral	AAMS SC process	4005	TCP	No	Open	Used by AAMS Session Controller for receiving command related to external session connections
AAMS	Ephermeral	AAMS Content Store	20005	TCP	No	Open	Used by Content Store to receive CStore commands from Session Controller
AAMS	Ephermeral	AAMS Content Store	20007	TCP	No	Open	Used by Content Store for transferring files (eg. audio media) between CStore and remote clients

AAMS	Ephermeral	AAMS IVRMP process	20009	TCP	No	Open	Used by IVR Media Processor for transferring files between AAMS servers
AACC Agent Greeting	Ephermeral	AAMS Web User Agent	7150	TCP	No	Open	HTTP REST services used by Agent Greeting Recording
AACC Agent Greeting	Ephermeral	AAMS Web User Agent	7151	TCP	No	Open	HTTPS REST services used by Agent Greeting Recording secured using TLS
AACC Licensing/Prompt Management	Ephermeral	AAMS SOAP interface	7410	TCP	No	Open	AAMS SOAP services used by AACC
AACC Licensing/Prompt Management	Ephermeral	AAMS SOAP interface	7411	TLS	No	Open	AAMS SOAP services used by AACC secured using TLS
Internet Browser	Ephermeral	Element Manager on AAMS	8443	TCP	No	Open	Element Manager HTTPS
Remote Media endpoints	Ephermeral	Linux AAMS	6000-32599	UDP	No	Open	Default media port ranges for Linux AAMS
Remote Media endpoints	Ephermeral	Windows AAMS	20000-45499	UDP	No	Open	**WINDOWS ONLY**: Default media port ranges for Windows AAMS
AAMS IvrMP MSLink	Ephermeral	AAMS IvrMP MSLink	4001	TCP	No	Closed	**INTERNAL ONLY:** IvrMP MSLink
AAMS SIP UA MSLink	Ephermeral	AAMS SIP UA MSLink	4004	TCP	No	Closed	**INTERNAL ONLY:** SIP UA MSLink
AAMS Resource Mgr External Session	Ephermeral	AAMS Resource Mgr External Session	4005	TCP	No	Closed	**INTERNAL ONLY:** AAMS Resource Mgr External Session
IvrMP Command Interface	Ephermeral	IvrMP Command Interface	4011	TCP	No	Closed	**INTERNAL ONLY:** IvrMP Command Interface
SIP UA Command Interface	Ephermeral	SIP UA Command Interface	4014	TCP	No	Closed	**INTERNAL ONLY:** SIP UA Command Interface
Resource Manager Command Interface	Ephermeral	Resource Manager Command Interface	4015	TCP	No	Closed	**INTERNAL ONLY:** Resource Manager Command Interface
ConfMP MSLink	Ephermeral	ConfMP MSLink	7080	TCP	No	Closed	**INTERNAL ONLY:** ConfMP MSLink
Stream Source Data	Ephermeral	Stream Source Data	19999	TCP	No	Closed	**INTERNAL ONLY:** Stream Source Data
Resource Manager IPC	Ephermeral	Resource Manager IPC	20011	TCP	No	Closed	**INTERNAL ONLY:** Resource Manager IPC
Video Media Processor	Ephermeral	Video Media Processor	4016	TCP	Yes	Closed	**INTERNAL ONLY:** Video Media Processor. Required for video
Video Media Processor	Ephermeral	Video Media Processor	7081	TCP	Yes	Closed	**INTERNAL ONLY:** Video Media Processor. Required for video
FNTMP MSLink	Ephermeral	AAMS IvrMP MSLink	7093	TCP	Yes	Closed	**INTERNAL ONLY:** FNTMP MSLink. Required for firewall NAT tunneling media Processing.

VoiceXML IPC	Ephermeral	VoiceXML IPC	21000 to 21031	TCP	Yes	Closed	**INTERNAL ONLY:** VoiceXML Interpreter Inter Process Communication. Required for VXML applications

2.2.6 Workspaces Cluster (WS)

Source (Client)		Destination (Server)		Network / Application Protocol	Optionally Enabled / Disabled?	Default Port State	Description
System	Port (Configurable Range)	System	Port (Configurable Range)				
Workspaces	Ephemeral	admin-adapter	31796	TCP	No	Open	Port used by the AACC to send data to the Kafka topics through admin-adapter
Workspaces	Ephemeral	kafka topics	32090 32091 32092	Own protocol based on TCP	Yes	Open	External access to Kafka brokers
Workspaces	Ephemeral	istio	31380	HTTP	No	Open	31380 – binds to 80 port
Workspaces	Ephemeral	istio	31390	HTTPS	No	Closed	31390–binds to 443 port
Workspaces	Ephemeral	istio	30634	TLS	No	Closed	GRCP for certificates
Workspaces	Ephemeral	kubernetes dashboard	32000	HTTP	No	Open	Access to kubernetes dashboard
Workspaces	Ephemeral	kubernetes api-server	6443	TLS	No	Open	Access to kubernetes api-server
Workspaces	Ephemeral	etcd	2379 2380	TLS	No	Open	Access to etcd database
Workspaces	Ephemeral	kubelet	10250	TLS	No	Open	Access to kubelet

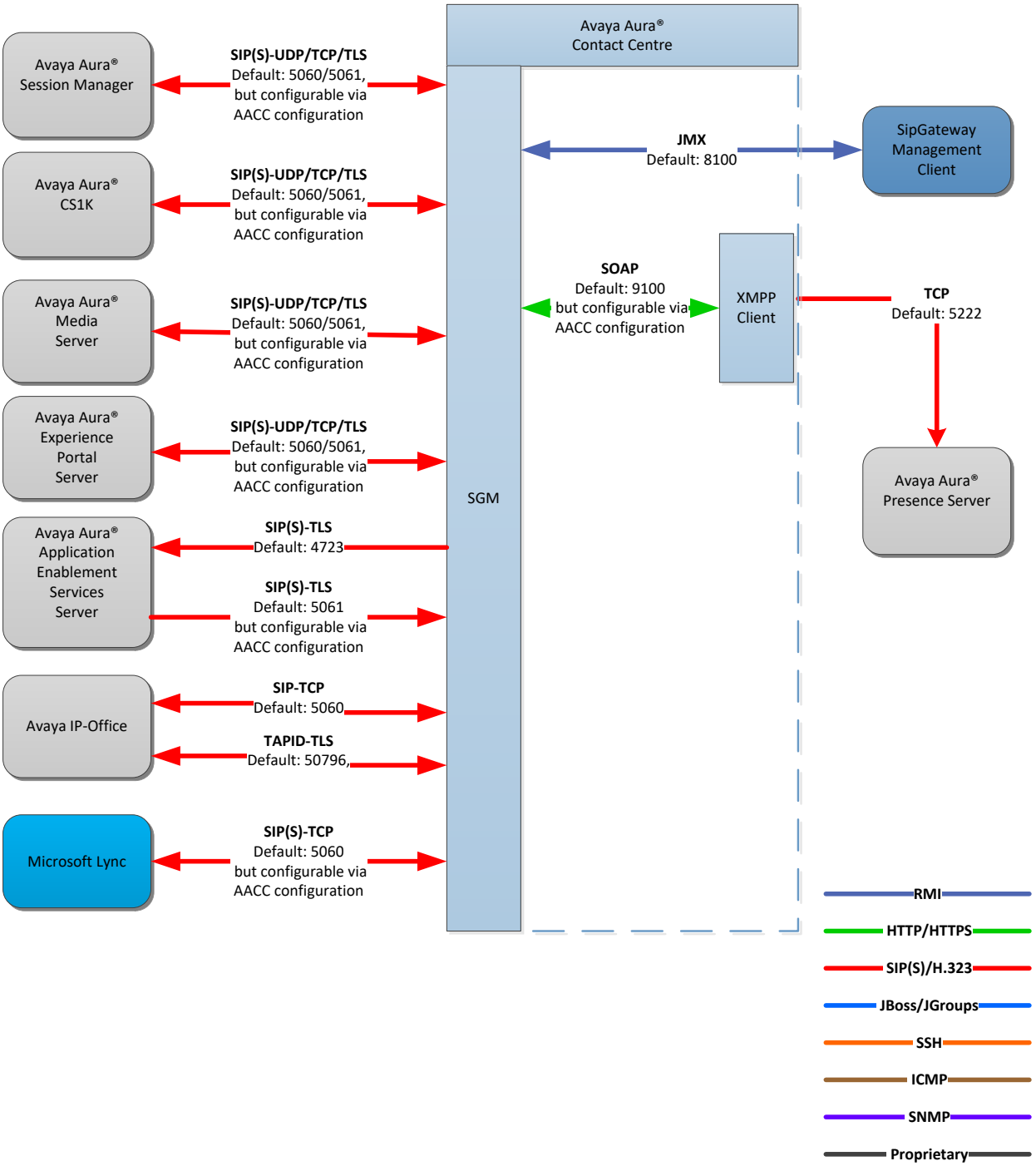
2.3 Port Table Changes

2.3.1 Avaya Aura Media Server

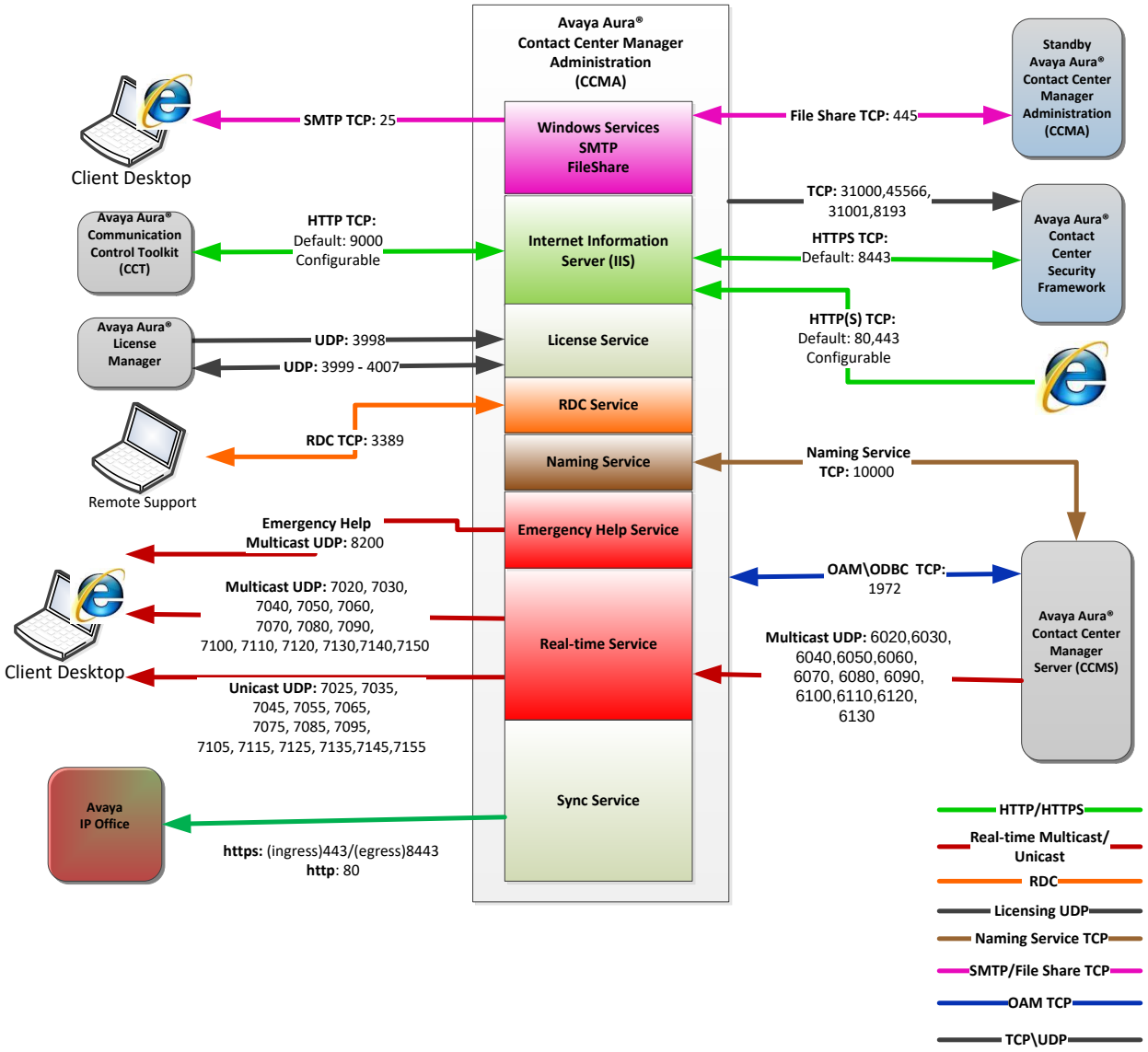
No.	Added / Changed / Removed	Port	Network / Application Protocol	New port	Notes
1	Changed	80	HTTP	7410	SOAP Server default ports changed between AAMS 7.0 and 7.5
2	Changed	443	HTTPS	7411	SOAP Server default ports changed between AAMS 7.0 and 7.5
3	Removed	51080	SOAP	7410	AAMS installed co-resident with AACC can now use 7410 as this does not conflict with AACC.
4	Removed	51443	SOAP/TLS	7411	AAMS installed co-resident with AACC can now use 7411 as this does not conflict with AACC.
5	Added		HTTP	7150	AAMS introduced new RESTful web service interface in release 7.7
6	Added		HTTPS	7151	AAMS introduced new RESTful web service interface in release 7.7
7	Removed	8009	AJP		Agent Greeting relocated to AACC server as of AACC 7.0. Dedicated Tomcat instance for AG on AAMS host no longer required.
8	Removed	6080	HTTP		Agent Greeting relocated to AACC server as of AACC 7.0. Dedicated Tomcat instance for AG on AAMS host no longer required.

3 Port Usage Diagrams

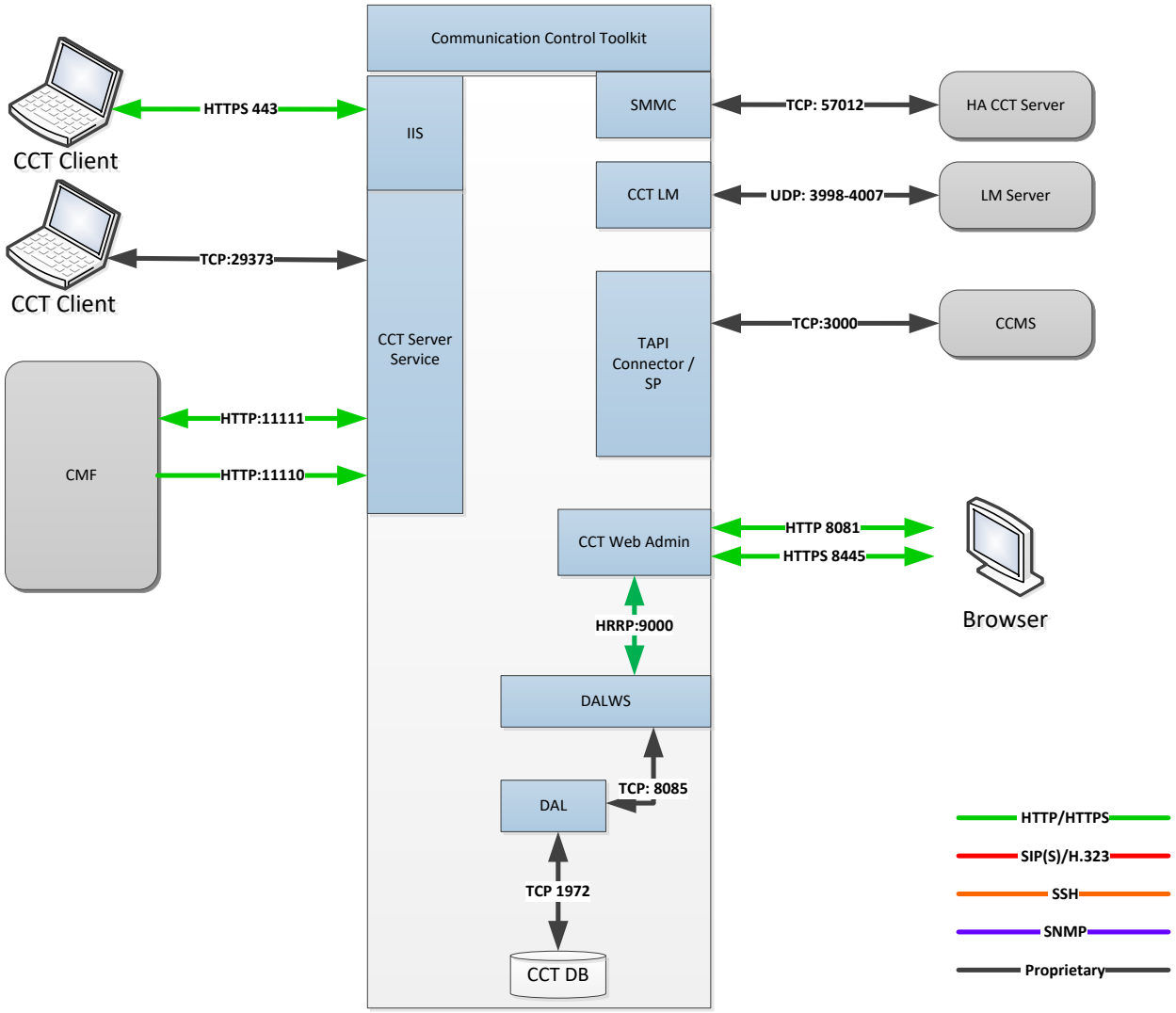
3.3 SIP Gateway Manager (SGM)



3.4 Contact Center Manager Administration (CCMA)



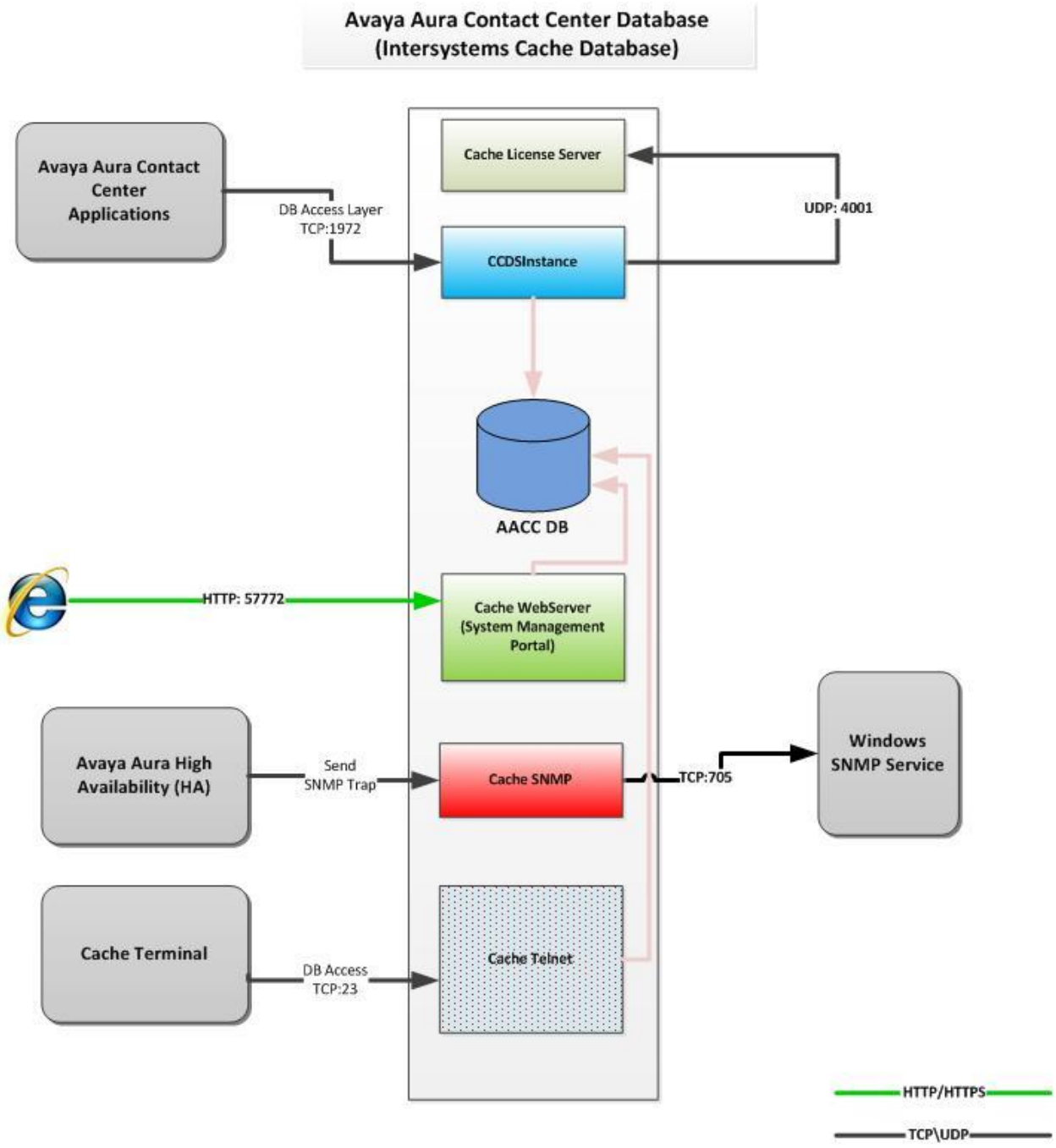
3.5 Communication Control Toolkit (CCT)



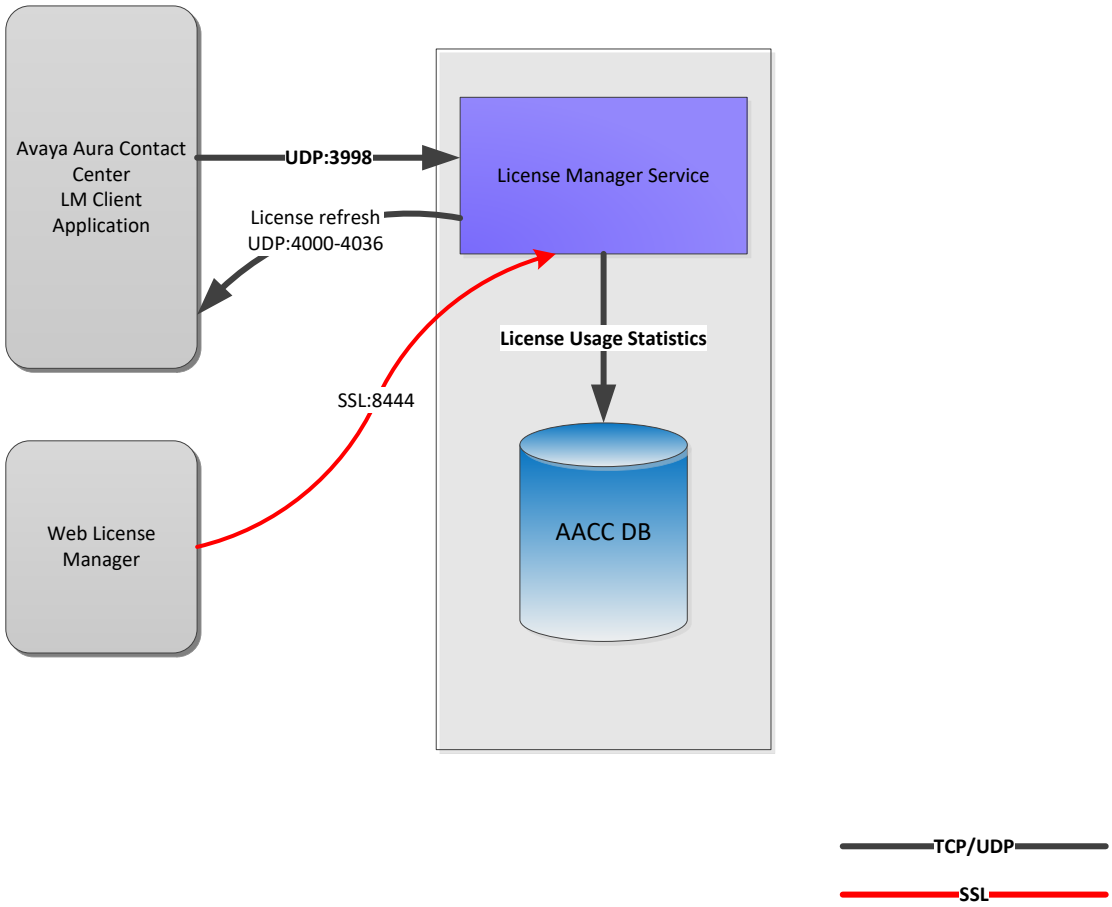
3.6 Avaya Agent Desktop (AAD)

- Not Applicable

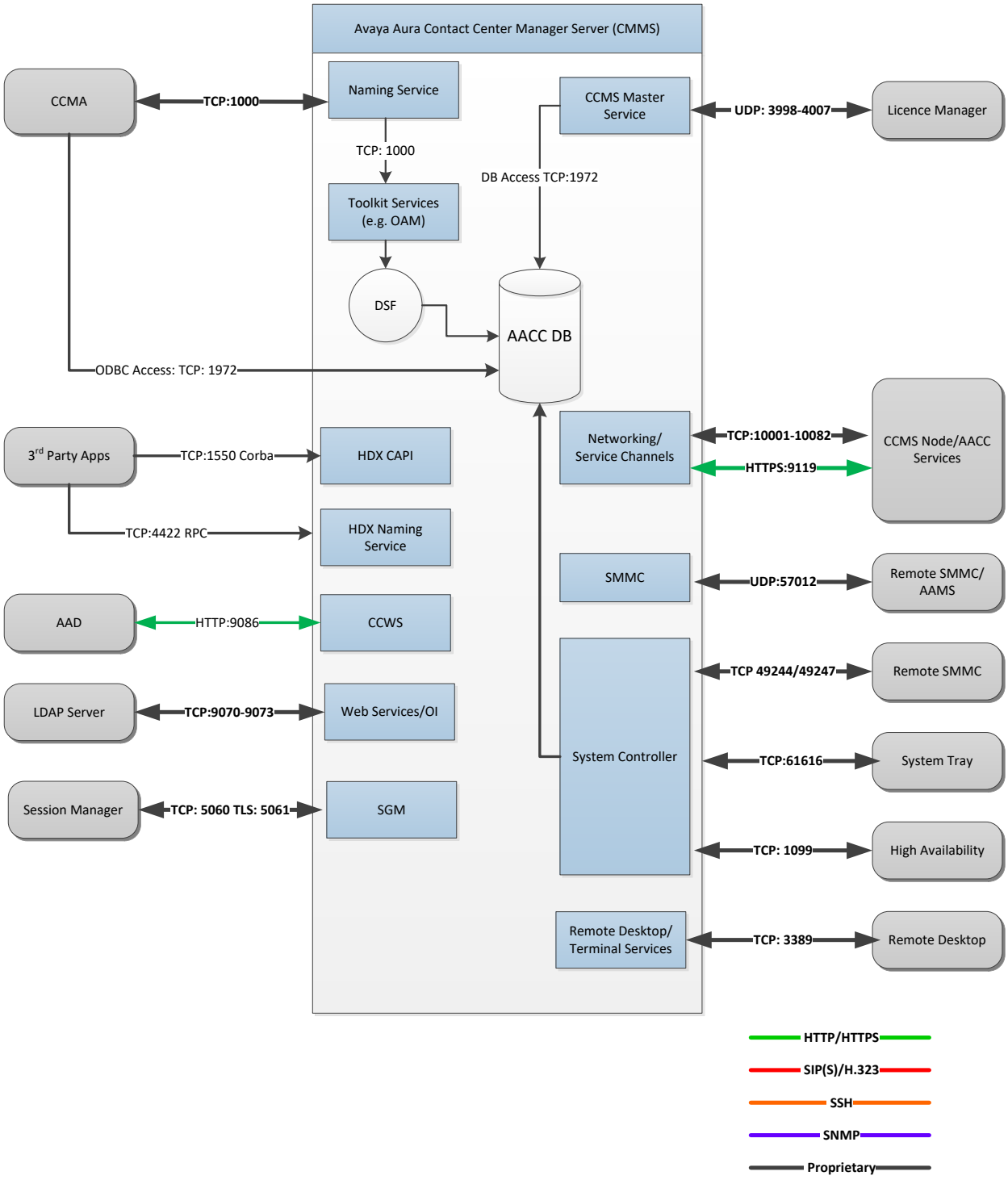
3.7 Intersystems Cache Database



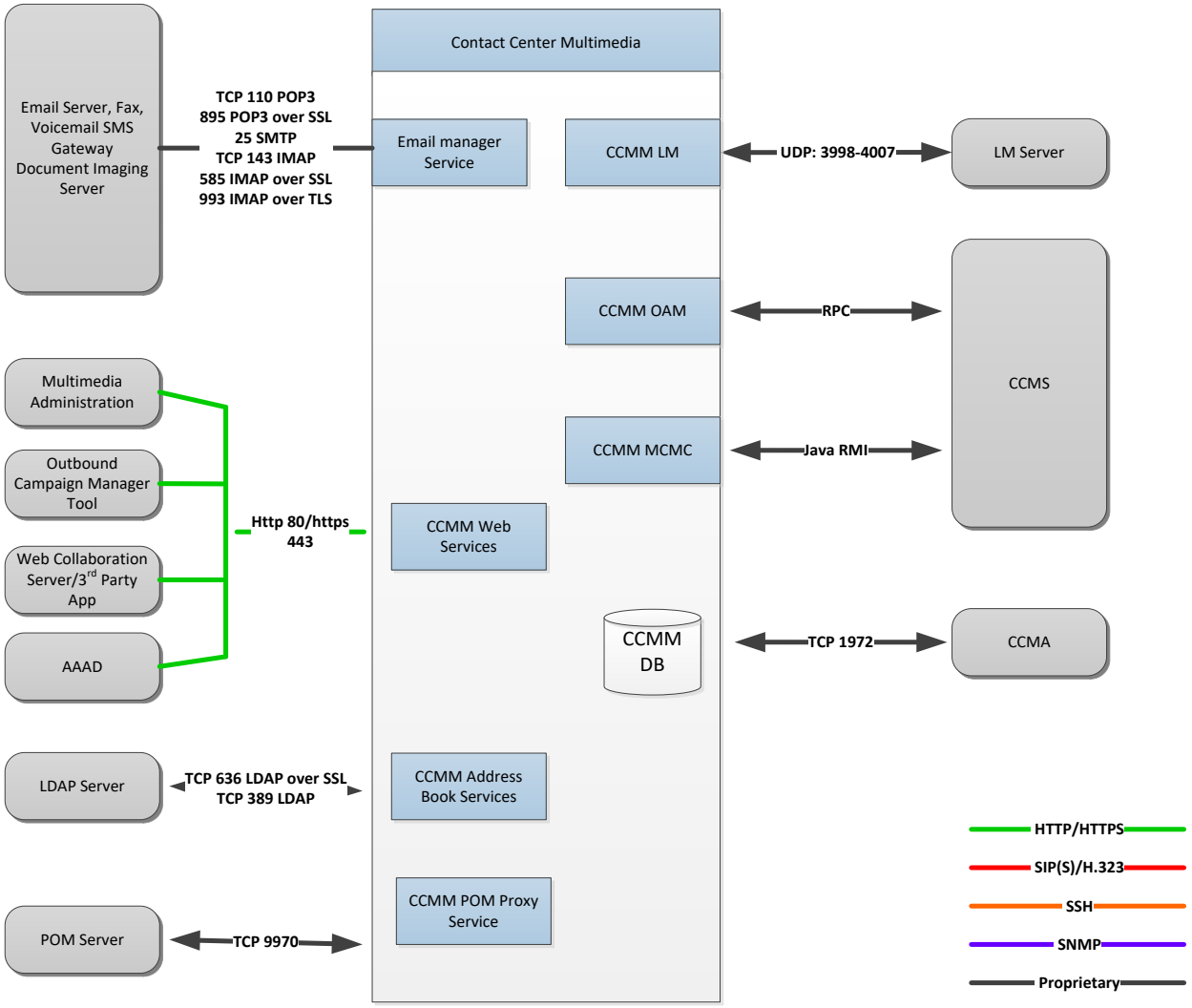
3.8 License Manager (LM)



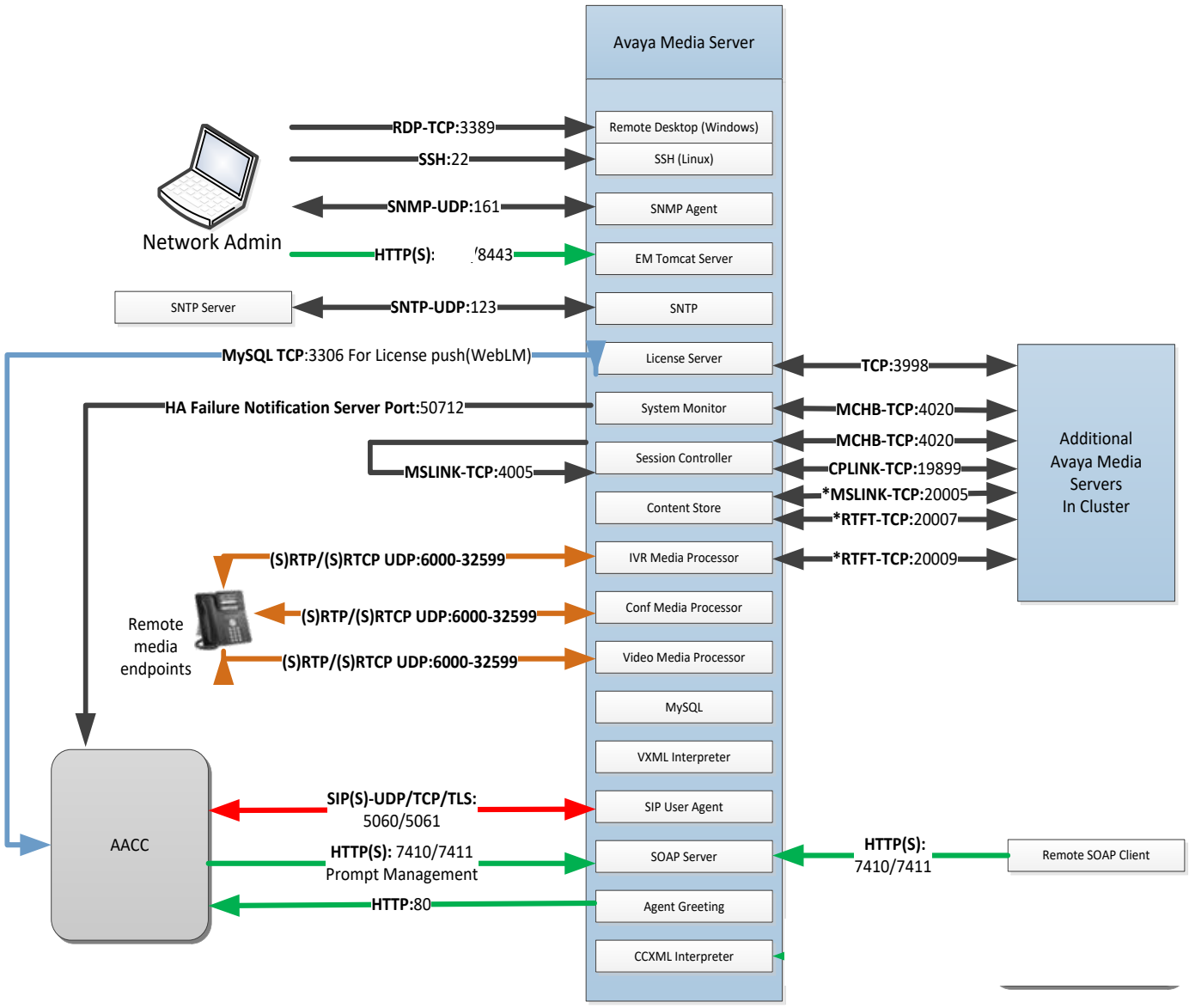
3.9 Contact Center Manager Server (CCMS)



3.10 Contact Center Multimedia (CCMM)



3.11 Avaya Aura Media Server (AAMS)



***** *Previous versions of AAMS use ports 52005/52007/52009. These will remain in use for upgraded AAMS servers hence these ports remain open in the firewall policy. New AAMS installations use ports 20005/20007/20009.*

**7.0.3 AACC/ACCS no longer supports AAMS running on Windows. This has been replaced with a Linux AAMS running as a Hyper-V virtual server. AAMS installed on Windows used port 5070/5071 for SIP TCP/TLS connection with AAMS. All AACC/ACCS 7.0.3 deployments now use port 5060/5061 for SIP TCP/TLS connection between AACC/ACCS and AAMS. Firewall can now be changed to block ports 5070/5071 after upgrade.*

Appendix A: Overview of TCP/IP Ports

What are ports and how are they used?

TCP and UDP use ports (defined at http://www.iana.org/assignments/port-numbers) to route traffic arriving at a particular IP device to the correct upper layer application. These ports are logical descriptors (numbers) that help devices multiplex and de-multiplex information streeams. Consider your desktop PC. Multiple applications may be simultaneously receiving information. In this example, email may use destination TCP port 25, a browser may use destination TCP port 80 and a telnet session may use destination TCP port 23. These logical ports allow the PC to de-multiplex a single incoming serial data packet stream into three mini-streeams inside the PC. Furthermore, each of the mini-streams is directed to the correct high-level application because the port numbers identify which application each data mini-stream belongs. Every IP device has incoming (Ingress) and outgoing (Egress) data streams.

Ports are used in TCP and UDP to name the ends of logical connections which carry data flows. TCP and UDP streams have an IP address and port number for both source and destination IP devices. The pairing of an IP address and a port number is called a socket (discussed later). Therefore, each data stream is uniquely identified with two sockets. Source and destination sockets must be known by the source before a data stream can be sent to the destination. Some destination ports are “open” to receive data streams and are called “listening” ports. Listening ports actively wait for a source (client) to make contact to a destination (server) using a specific port that has a known protocol associate with that port number. HTTPS, as an example, is assigned port number 443. When a destination IP device is contacted by a source device using port 443, the destination uses the HTTPS protocol for that data stream conversation.

Port Type Ranges

Port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic Ports (sometimes called Private Ports).

Well Known Ports are those numbered from 0 through 1023.

Registered Ports are those numbered from 1024 through 49151

Dynamic Ports are those numbered from 49152 through 65535

The Well Known and Registered ports are assigned by IANA (Internet Assigned Numbers Authority) and are found here: http://www.iana.org/assignments/port-numbers.

Well Known Ports

For the purpose of providing services to unknown clients, a service listen port is defined. This port is used by the server process as its listen port. Common services often use listen ports in the well known port range. A well known port is normally active meaning that it is “listening” for any traffic destined for a specific application. For example, well known port 23 on a server is actively waiting for a data source to contact the server IP address using this port number to establish a Telnet session. Well known port 25 is waiting for an email session, etc. These ports are tied to a well understood application and range from 0 to 1023.

In UNIX and Linux operating systems, only root may open or close a well-known port. Well Known Ports are also commonly referred to as “privileged ports”.

Registered Ports

Unlike well known ports, these ports are not restricted to the root user. Less common services register ports in this range. Avaya uses ports in this range for call control. Some, but not all, ports used by Avaya in this range include: 1719/1720 for H.323, 5060/5061 for SIP, 2944 for H.248 and others. The registered port range is 1024 – 49151. Even though a port is registered with an application name, industry often uses these ports for different applications. Conflicts can occur in an enterprise when a port with one meaning is used by two servers with different meanings.

Dynamic Ports

Dynamic ports, sometimes called “private ports”, are available to use for any general purpose. This means there are no meanings associated with these ports (similar to RFC 1918 IP Address Usage). These are the safest ports to use because no application types are linked to these ports. The dynamic port range is 49152 – 65535.

Sockets

A socket is the pairing of an IP address with a port number. An example would be 192.168.5.17:3009, where 3009 is the socket number associated with the IP address. A data flow, or conversation, requires two sockets – one at the source device and one at the destination device. The data flow then has two sockets with a total of four logical elements. Each data flow must be unique. If one of the four elements is unique, the data flow is unique. The following three data flows are uniquely identified by socket number and/or IP address.

Data Flow 1:	172.16.16.14:1234	-	10.1.2.3:2345
Data Flow 2:	172.16.16.14.123**5**	-	10.1.2.3:2345
Data Flow 3:	172.16.16.14:1234	-	10.1.2.4:2345

Data flow 1 has two different port numbers and two different IP addresses and is a valid and typical socket pair.
Data flow 2 has the same IP addresses and the same port number on the second IP address as data flow 1, but since the port number on the first socket differs, the data flow is unique.
Therefore, if one IP address octet changes, or one port number changes, the data flow is unique.

Figure 1, below, is an example showing ingress and egress data flows from a PC to a web server.

Socket Example Diagram

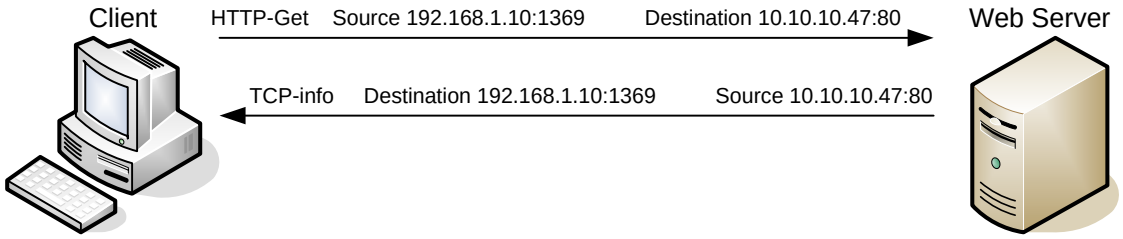


Figure 1. Socket Example

Notice the client egress stream includes the client’s source IP and socket (1369) and the destination IP and socket (80). The ingress stream has the source and destination information reversed because the ingress is coming from the server.

Understanding Firewall Types and Policy Creation

Firewall Types

There are three basic firewall types:

- Packet Filtering
- Application Level Gateways (Proxy Servers)
- Hybrid (Stateful Inspection)

Packet Filtering is the most basic form of the firewalls. Each packet that arrives or leaves the network has its header fields examined against criterion to either drop the packet or let it through. Routers configured with Access Control Lists (ACL) use packet filtering. An example of packet filtering is preventing any source device on the Engineering subnet to telnet into any device in the Accounting subnet.

Application level gateways (ALG) act as a proxy, preventing a direct connection between the foreign device and the internal destination device. ALGs filter each individual packet rather than blindly copying bytes. ALGs can also send alerts via email, alarms or other methods and keep log files to track significant events.

Hybrid firewalls are dynamic systems, tracking each connection traversing all interfaces of the firewall and making sure they are valid. In addition to looking at headers, the content of the packet, up through the application layer, is examined. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Stateful inspection firewalls close off ports until the connection to the specific port is requested. This is an enhancement to security against port scanning[1].

Firewall Policies

The goals of firewall policies are to monitor, authorize and log data flows and events. They also restrict access using IP addresses, port numbers and application types and sub-types.

This paper is focused with identifying the port numbers used by Avaya products so effective firewall policies can be created without disrupting business communications or opening unnecessary access into the network.

Knowing that the source column in the following matrices is the socket initiator is key in building some types of firewall policies. Some firewalls can be configured to automatically create a return path through the firewall if the initiating source is allowed through. This option removes the need to enter two firewall rules, one for each stream direction, but can also raise security concerns.

Another feature of some firewalls is to create an umbrella policy that allows access for many independent data flows using a common higher layer attribute. Finally, many firewall policies can be avoided by placing endpoints and the servers that serve those endpoints in the same firewall zone.

[1] The act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.