Avaya one-X® Agent

Port Settings

Issue: 1.0
May 2011

Contents

Avaya one-X Agent PC port settings 3

Telephony (H.323 protocol ports) 3

Non-TTS 3

TTS 5

RTP streams for audio (My Computer mode) 6

PC ports 6

Far-end ports 6

RTP streams for video (AVTS) 7

Central Management communication to Avaya one-X Agent 7

Central Management to System Manager / SAL 8

PC ports for Desktop Sharing 8

Presence Services (XMPP) client 8

Active Directory authentication 9

Database (Postgres) 9

Avaya one-X Agent PC port settings

This document applies to different releases of Avaya one-X Agent and explains how to change the ports for their firewall traversal rules. These applications are hereafter referred to as the PC application or the application. The PC application uses different connections (sockets) and local PC ports for signaling and media (audio and video) communications. The number of sockets used, the values of the ports selected for these sockets are dependent on the release of PC applications and its configuration. Due to these differences, the port/connection information is grouped into the following main sections.

Telephony (H.323 protocol ports)

Non-TTS

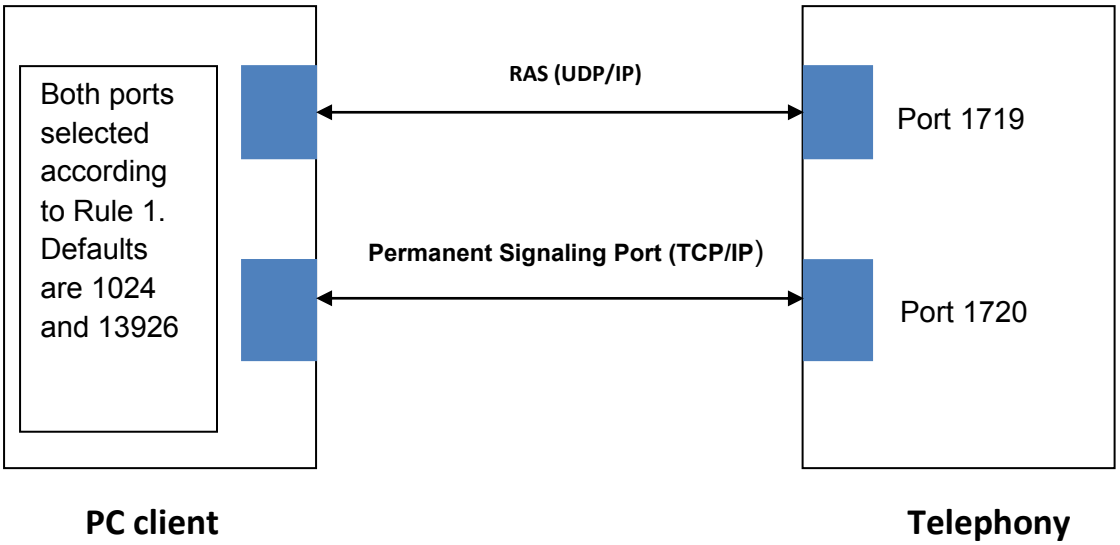
The network region does not allow Time To Service (TTS) if Avaya one-X Agent 2.0 earlier than SP3 is used. A network region—marked near-end establishes signaling socket (allow TTS)—can negotiate with a non-TTS capable endpoint at RAS (Registration, Admission, and Status) to allow a non-TTS operation with Avaya one-X Agent before 2.0 SP3.

Avaya one-X Agent requires two different IP ports on PC for telephony, RAS port (UDP), and a (permanent) Signaling Port (TCP)[1].

Rule 1: The ports selected are controlled by a parameter pair in the Spark configuration file, config.xml file, and SigPortLow-to-SigPortRange. SigPortLow-to-SigPortRange is known as high port in Avaya IP Agent. The RAS port is selected as the lowest available port in the bottom 20% of this range. The signaling port is selected as the first available port in the next 50% of this range.

The ports on the Communication Manager side for non-TTS operation are port 1719 for RAS and port 1720 for signaling.

[1] A third port, a discovery port was originally needed by IP Agent iClarity. IP Agent iClarity is not used by one-X Agent and the Spark Emulator any longer. This port was originally chosen from the top 20% of the signaling port range.



You can locate the Spark configuration files in the PC at `%APPDATA%\Avaya\one-XAgent\2.x`. folder. Further, you must set the HKLM registry value **DataFileExtension** to the installer default of `Avaya\one-X Agent\2.0`, or else the Spark Emulator will not find these modified files.[2] If you have not modified the config.xml file or the Spark Emulator is unable to find the config.xml file, the system uses 1024 and 64511 as default values[3].

Example to over-ride the default settings

The two parameters in the config.xml file to change the default low port and port range and set the signaling port range to 2048-6047 appear as follows:

```
<parameter>
   <name>SigPortLow</name>
   <value>2048</value>
</parameter>
<parameter>
  <name>SigPortRange</name>
  <value>4000</value>
</parameter>
```

The RAS port search then starts at 2048, and the signaling port search at 2848 (2048 + 20% of 4000). You can enter this text at any convenient point in the file.

[2] This registry value is set correctly by the one-X Agent installer, and this value has not been altered (it must not be), then this registry check is not needed.

[3] Thus, port 13926 is chosen for the PC side of the signaling connection if the application defaults are used.

The RAS port is chosen from the bottom 20% of the range and the main signaling socket from the middle 50% of the range. The top 30% is unused, a remnant from earlier times when this was used by a discovery process that is no longer used.

If the low port and port range are modified, the minimum range must be at least 100 wide, and that the low port number must be chosen so that there is no conflict with other port usage on the PC.

TTS

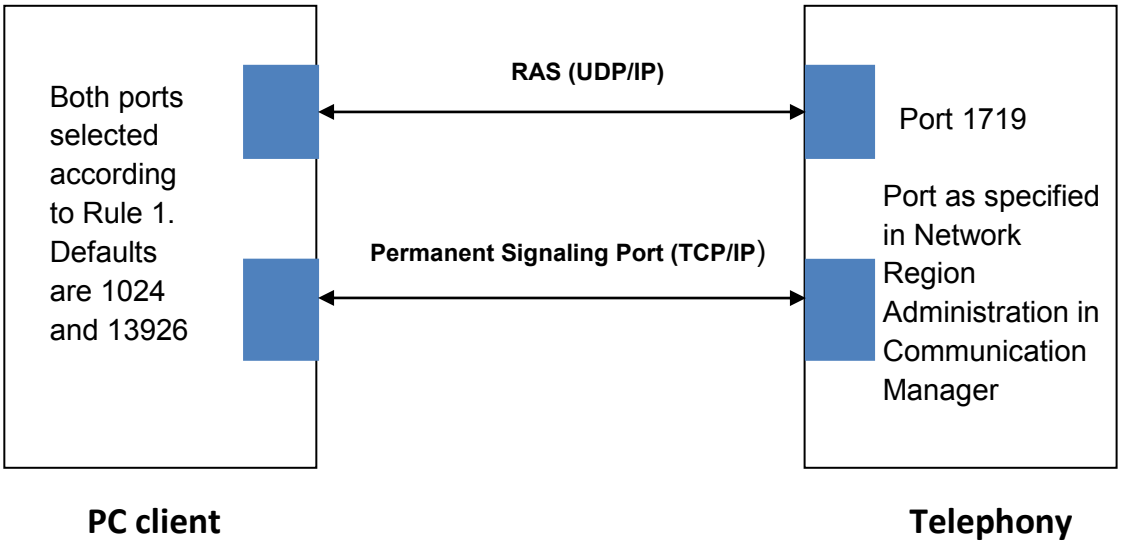
Communication Manager controls the TTS operation and the setting in the Network Region of the registering extensions. Check the box in this administration that reads “Local Initiation” for the signaling socket. Local refers to the switch side in switch administration.

The same RAS port and the main signaling port are also needed for TTS operation. These operate and are controlled as described in the non-TTS section.

The main signaling connection in TTS is originated from Communication Manager, and not from the PC client. This is, indeed, the major characteristic and advantage of TTS operation.

The ports on the Communication Manager side for TTS operation are port 1719 for RAS and signaling defined on page 2 of Network Region Settings in Communication Manager.

The default range is 61440 and 61443.



Note: Avaya one-X Agent has no control over what port is selected by Communication Manager.

RTP streams for audio (My Computer mode)

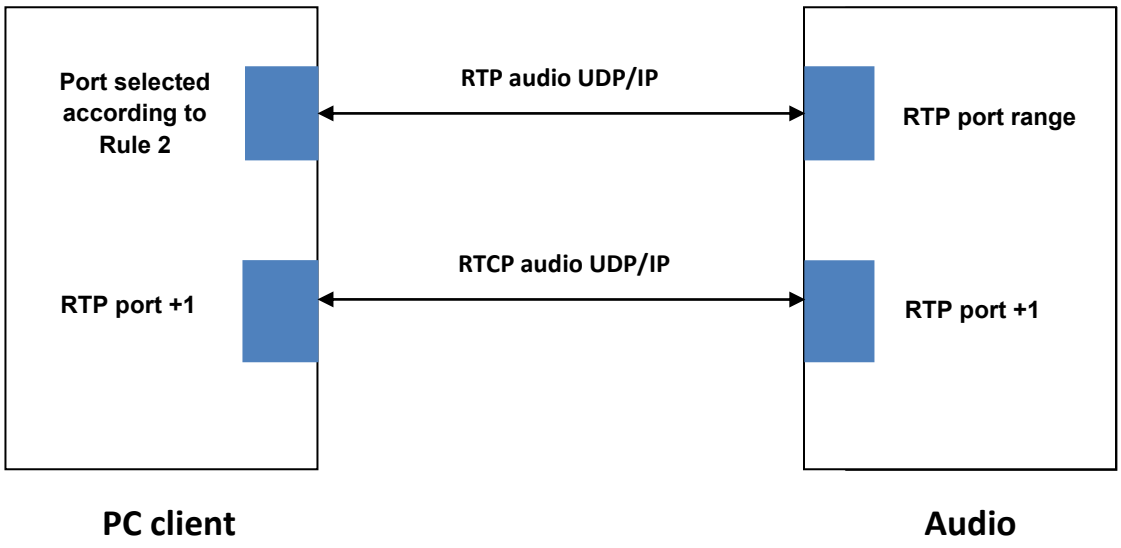
PC ports

For each RTP stream terminating on the PC, you must open two ports. These are chosen from the range **RtpPortLow** to **RtpPortRange**.

Rule 2: Avaya one –X Agent starts searching for ports at the bottom of the range, and linearly searches up the range for an available port. The RTCP port associated with an RTP port is one higher than the media port.

You can set these two parameters by editing the XML file that is located at the following location: `$APPDATA$\Data\Avaya\one-X Agent\2.0\config.xml`.

These are parameters used by the Spark Emulator. The default values are 2048 and 2951. Unlike Avaya IP Agent, the RTP port range and the signaling port range can be different. The RTP port is selected randomly from this range, and the corresponding RTCP port is one higher.



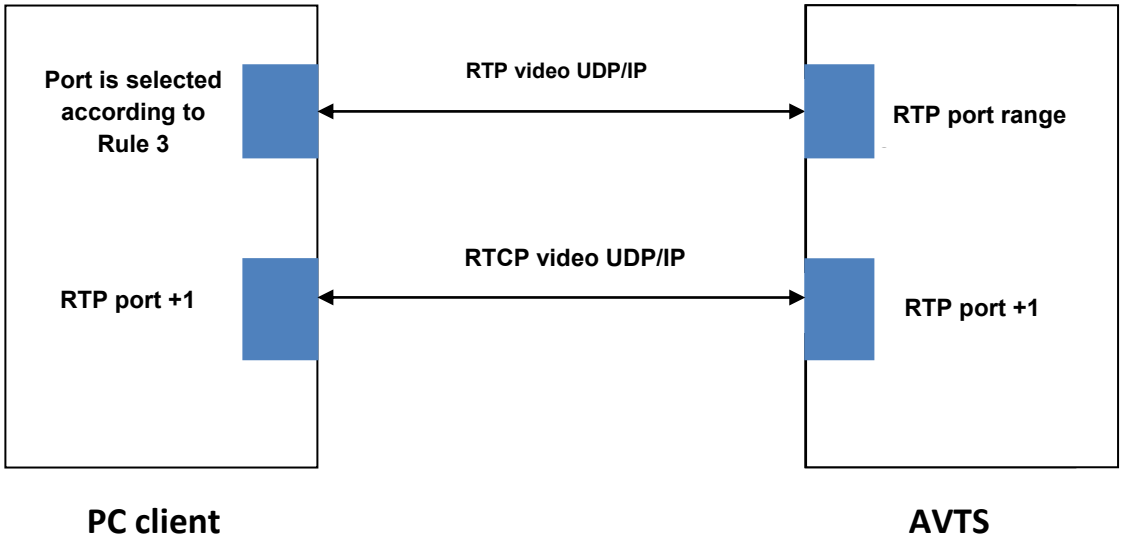
Far-end ports

Avaya one-X Agent has no control of the far-end ports selected for RTP/RTCP. These are set by the far-end point, and are supplied to Avaya one-X Agent during media channel setup.

RTP streams for video (AVTS)

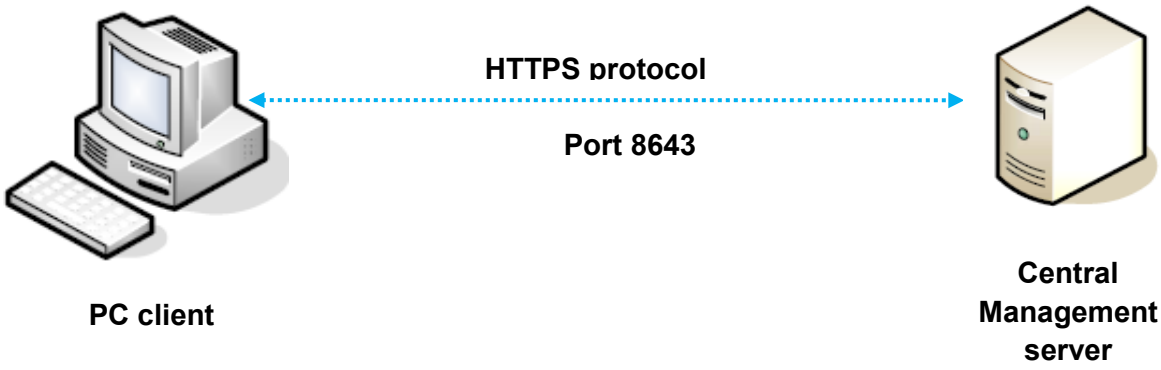
For video RTP streams, the port selection range is defined by **VideoRtpPortLow** and **VideoRtpPortRange**.

Rule 3: The default values are 3523 and 1475. Otherwise, the behavior of the video RTP is the same as the audio RTP, and can be redefined.



Central Management communication to Avaya one-X Agent

Communication from the PC client to the Central Management server is through a standard HTTPS protocol. The port 8643 must be open on the Communication Management server. It is the other end of the HTTPS communication socket to the Avaya one-X Agent client.



Central Management to System Manager / SAL

Secure Access Link (SAL) Agent on Central Management uses a standard HTTPS port (that is 443) to communicate with System Manager. All the listen ports started by SAL Agent are used for inter-process communication on the local machine. Port 32000 is used for communication between the SAL Agent wrapper process. The wrapper process starts the SAL Agent Java Virtual Machine (JVM) and the SAL Agent JVM. SAL Agent uses anonymous port for Java Management Extensions (JMX) communication with its Command Line Interface tool (SpiritAgentCLI). The agent starts the JMX Mbean server using an anonymous port, and therefore a different port will be used every time SAL Agent is restarted.

The SAL Agent functionality works even if a customer blocks access to these two listen ports from external machines.

PC ports for Desktop Sharing

A listener port must be open at each PC. The application starts looking at port 5900, and picks the first unused one it finds. It releases this port when the desktop sharing session ends. For each new active session, another port must be opened. Again, the application starts to search from 5900 and selects the first unused one it finds.

Presence Services (XMPP) client

Unlike telephony and video, Avaya one-X Agent 2.0 SP3 has no range controls on the ports that must be opened at the client for XMPP communication. The current implementation chooses to open a free port in the range 2048 and higher, starting at the bottom, to avoid conflict with the

Well Known ports in this lower range. The standard XMPP port 5222 must be open on the Presence Services server.

Active Directory authentication

LDAP Services port 389 and Microsoft Global Catalog port 3268 must be open on the Microsoft Active Directory Server. If Active Directory is used for other enterprise authentication, these ports must already be open. Central Management and Presence Services (optional) require no further special treatment.

Database (Postgres)

Central Management uses Postgres and the 5432 and 53418 posts must be open on the local machine for connection to Central Management. There is no exposure of these ports to the network.

If Presence Services is installed on a separate machine, the machine installs its own local copy of Postgres that similarly uses these two internal sockets and will not be exposed to the network.