Avaya Workforce Engagement

ACR Advanced Recorder VoIP Delivery Deployment Reference Guide

October 17, 2025
Revision 1.14

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 varying media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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: http://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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided 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 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 ACCESSES 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 WHOM 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 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 Global Software License Terms ("Software License Terms") are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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, 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. Unless otherwise stated, 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
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
WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE 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 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 to comply 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, please contact your Avaya Sales Representative.

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).

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 LLC.
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.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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.

Contents

About this guide

This Deployment Reference Guide (DRG) describes the recording and telephony site preparation you are required to perform in advance of system deployment.

Intended audience

This guide is designed for:

- Customers responsible for preparing the site for Recorder deployment.
- Business Partner professional services staff responsible for planning and setting up recording systems.

Document revision history

Revision	Description of changes
1.14	Included Limitations for SIPREC.
1.13	Added additional configuration option of speaker separation for Gateway speaker separation.
1.12	Minor text edits.
1.11	In the *VoIP Delivery* chapter, under *Recording Methods*, *SIPREC*, and in the *Gateway-side forking* topic, specified that an IP Recorder configured for gateway-side SIPREC forking *cannot* be configured with any station-side interception capture.
1.10	Added new section "Line-side forking" under SIPREC.
1.09	• Noted that SIP Trunk Delivery is a deprecated recording technology. • The "SIPREC" section is modified. • In the "Device and Media Call Control" topic, the text refers the reader to the *Avaya Integration Guide* for more details.

Revision	Description of changes
1.08	The following updates were made for V15.2 2020R1: • Removed Tape Drives and DVD-RAM, DVD RW, +/-, 4.7 GB from list of supported Archive devices for writing. • Avaya rebranding.
1.07	Updated the topic 'Calculating the number of ports required' to include RTSA and Real-Time Monitoring ports.
1.06	The following updates were made for HFR7: • Avaya rebranding • Added Amazon S3 and Azure Blob Storage as supported Archive devices • Removed "DMCC recording conbines both sides of the conversation into mono audio files." from the "Device and Media Call Control" topic.
1.05	Removed limitations around the use of a dedicated SBC.
1.04	Removed Acquisition Recorder and Siemens Trading.
1.03	The following changes are new with V15.2 HFR3: • Updated with new document template.
1.02	Added a new topic called "Calculating the number of ports required."
1.01	Removed references to Acme in VoIP Interception chapter. Revised Limitations in the VoIP Delivery chapter. Moved Archive content to separate chapter.
1.00	The following changes have been made for this release: • Added "Archiving site preparation" chapter.

Chapter 1

VoIP Delivery

To record contacts in a VoIP contact center, IP traffic is monitored by the Recorder. This section provides an overview of the Recorder VoIP Delivery architecture, solutions, integrations and delivery methods.

Topics

Architecture

In a VoIP contact center, the IP traffic is monitored and recorded. When recording is triggered, the Recorder assembles the relevant packets and stores the contacts in standard audio file formats. You can set up Full and Selective VoIP Delivery environments.

The architecture of a VoIP Delivery solution will depend upon your third-party integration — refer to your *Integration Guide* for more information (including diagrams) specific to your environment.

Recording Methods

The Recorder supports the following VoIP Delivery methods:

- Device and Media Call Control (page 8)
- Duplicate Media Streaming (page 8)
- SIP Trunk Delivery (Deprecated) (page 8)
- SIPREC (page 10)

Device and Media Call Control

Avaya Device and Media Call Control (DMCC) (previously Communication Manager API [CMAPI]) is a software connector that provides a programming interface for device and media control on the Avaya Communication Manager switch.

Avaya DMCC allows for both dedicated, selective, and a combination of recording modes. Refer to the *Avaya Integration Guide* for details.

Related information

Avaya Integration Guide

Duplicate Media Streaming

Duplicate Media Streaming (DMS) for contact centers employing Avaya CS1K switches sends duplicate audio streams from the agent's extension directly to the Recorder. As both sides of the conversation are duplicated, the resulting recorded audio is in stereo.

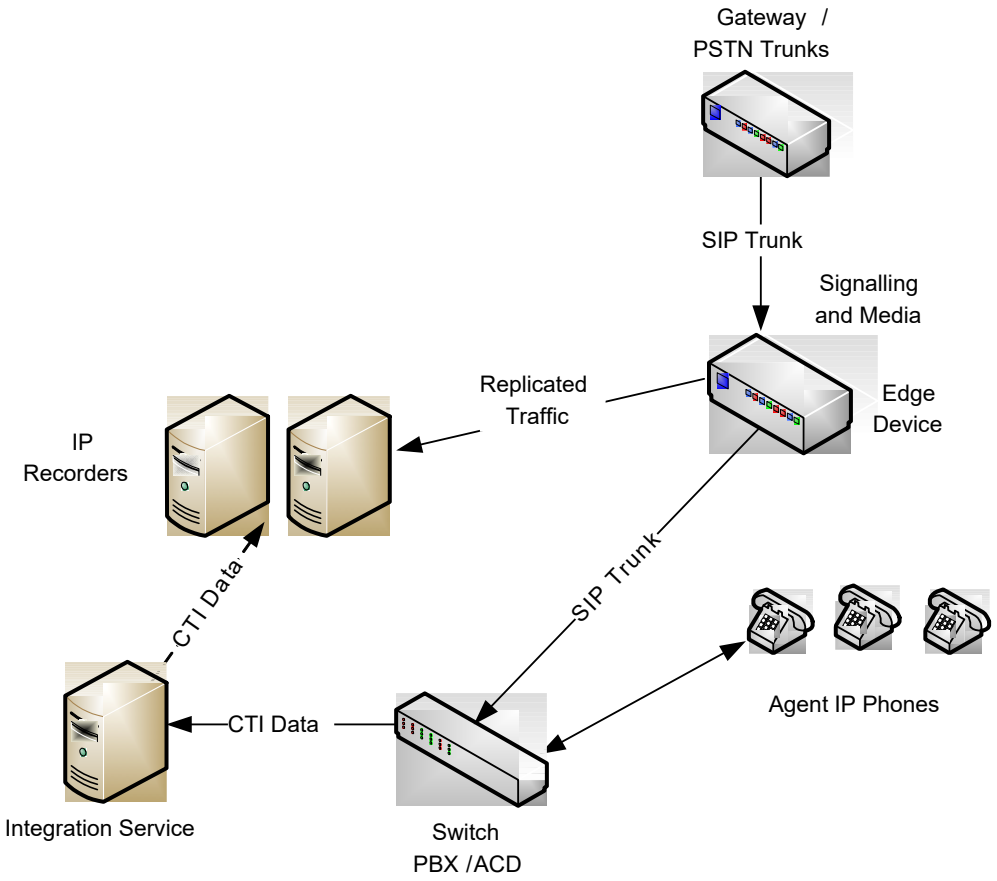
Avaya NES CS1000 Contact Center Manager (Symposium)—This solution uses a capability introduced by Avaya NES for transmitting a duplicate Real-time Transport Protocol (RTP) stream from the agent's extension directly to IP Capture or the IP Recorder. Initiating and terminating the audio stream is done through a dedicated interface to the Avaya NES Contact Center Manager (Symposium), via the existing Meridian Link Service (MLS) protocol. Using this feature, IP Capture or the IP Recorder will initiate and terminate the RTP transmission using CTI Link Active CTI interface. CTI Link will then issue a Start RTP/Stop RTP command to the phones (through the Symposium). In response, RTP packets will be delivered directly from the phones to the ports requested by IP Capture or the IP Recorder.

SIP Trunk Delivery (Deprecated)

> SIP Trunk Delivery is a deprecated recording technology. We recommend using SIPREC for VoIP Delivery recording.

SIP trunk delivery allows for the delivery of SIP signaling and media directly from the edge device to the Recorders. The edge device collects the signaling and media from the Gateway or directly from

PSTN SIP trunks. The edge device then replicates the SIP trunk session to the Recorder, as shown in the diagram below.



The edge device provides the Recorder with both signaling and media. However, as the SIP signaling does not carry the agent's phone extension, the agent's phone extension cannot be used to correlate the SIP trunk audio session to the switch call. To correlate the audio session to the call coming through the switch, the system allows for configuration of a non-extension based field (such as unique call ID) in both the SIP signaling and in the CTI data sent from the switch to the Recorder Integration Service. In Avaya environments, configure SIP Trunks on the Avaya PBX side for shared UCID generation.

Supported Features

In addition to recording SIP trunks, the following recording scenarios are supported with SIP Trunk Delivery:

- Recording in SIP and TDM mixed trunk environments.
- Recording SIP trunk traffic from multiple switch combinations.
- Full Delivery.

Limitations

- Recording encrypted calls is not supported for SIP Trunk Interception and SIP session replication. (It is supported in SIP Trunk Delivery.)
- Real-time Monitoring is not available in VOX fallback mode. When CTI is disconnected, the extension data is not tagged to the recording, so no real-time monitoring is available.
- Searches in VOX fallback mode must be based on start time, as searching by extension is not available.

The following apply only to SIP Trunk Recording in Interception environments.

- IP Analyzer does not support RFC 2003 interception, therefore this release does not support integration with an SBC through IP Analyzer.
- In Gateway Correlation environments, a Correlation Key (which can be specified within a data source member group but is typically provided internally by the Integration Service) is used to establish an association between a recording and its CTI attributes. The IP Extension Status screen in Recorder Manager will only display calls that are already correlated, and not active calls with VOX-only recordings.

The following apply only to SIPREC selective recording environments:

- Performance and Liability modes are not supported in SIPREC selective recording. If CTI is not received for the call, no recording will happen.
- N+N is not supported in SIPREC delivery (only 1+1 for Recorder Integration Service redundancy, and N+M all shared for Recorder redundancy).

Supported Environments for SIP Trunk Delivery

Please see the appropriate Integration Guide to determine whether SIP Trunk Delivery is supported for a particular switch integration.

SIPREC

Session Initiation Protocol Recording (SIPREC) is a recording standard and a type of VoIP Delivery recording.

A SIPREC recording solution involves a Communication Session flowing through a SIP device. The SIP device initiates a Recording Session from the SIP device that is directly related to the Communication Session. The Recording Session lives only as long as the Communication Session exists.

The forked SIPREC call (that is, the Recording Session) contains an XML portion with metadata about the underlying Communication Session. Most SIPREC devices offer the ability to customize the data provided in this XML body.

The integration can receive SIPREC traffic from a switch, or session replicating device such as a Session Border Controller (SBC). An SBC typically lives at the network edge. The SBC provides separation between the external and internal networks.

The SIPREC call is delivered to a Session Recording Server (SRS). The recording site implements an SRS endpoint by means of the Generic SIPREC Adapter. The Generic SIPREC Adapter can live on either the Recorder Integration Service (RIS) or the Recorder Adapter Proxy Service (RAPS).

The SIPREC adapter manages the SIP signaling, routes the RTP to an associated IP recorder, and tags appropriate information extracted from the SIP signaling. Default tagging includes any custom attributes and any relevant data found in the SIPREC XML. Default tagging also includes the data source ID and the member group ID. The Recorder Integration Service uses this tagged information to correlate the call with the CTI. Correlation attributes are intended to be call-specific identifiers. These identifiers can be matched to the real-time CTI feed.

> Refer to the *Recorder Configuration and Administration Guide* for details about correlation attributes.

Codec and encryption support

Most SBCs just reflect the RTP traffic for the Communication Session out on the Recording Session. Some SBCs offer codec conversion, but this action is resource intensive and not advised. The Verint Recorders support a suite of codecs. You can restrict the SRS to offer only specific codecs by configuration on the SIPREC adapter itself. The default behavior offers all supported codecs to the SBC.

Media encryption is also typically reflected out to the Recording Session. Some SBCs can take an unencrypted Communication Session and send encrypted sRTP payloads to the SRS. However, if the Communication Session is already sending encrypted sRTP packets, these same packets are used on the Recording Session with the same keys. Some SBCs offer rekeying operations, but these operations are resource intensive and not advised.

The SBC can change codecs or keys on the streams at any time and the recording site can handle those changes.

Related topics

SIPREC gateway-side forking (page 11)

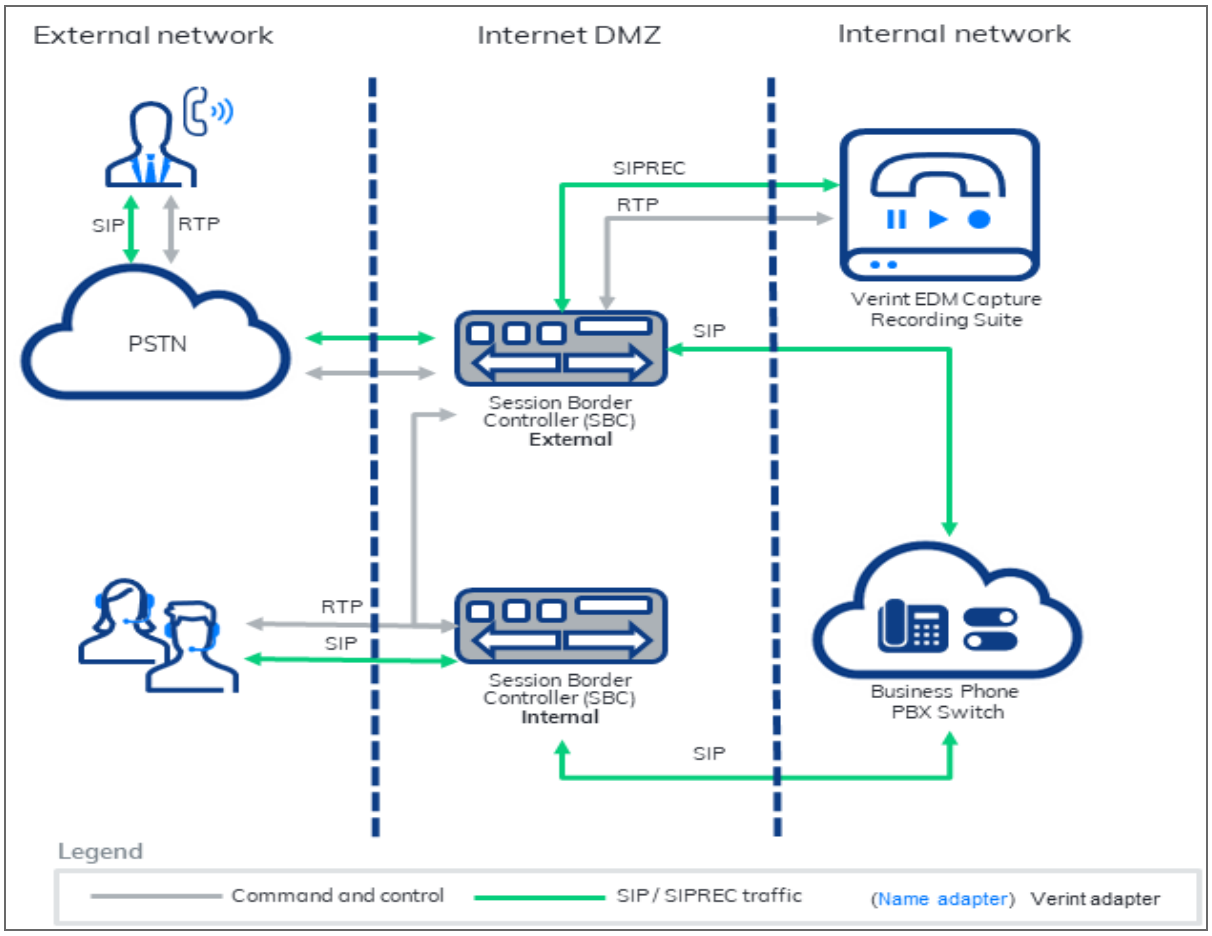
SIPREC line-side forking (page 12)

Speaker separation (page 14)

SIPREC gateway-side forking

Gateway-side forking is a supported Session Initiation Protocol Recording (SIPREC) deployment. In a gateway-side forking configuration, a device between the external Public Switched Telephone Network

(PSTN) trunks and the internal Private Branch Exchange (PBX) switch forks the audio of a call or the communication session.



Because the Session Border Controller (SBC) does not interface directly with the agent devices, the communication session is for the external device. This deployment is effective for recording all inbound and outbound traffic. However, this deployment cannot capture internal calls because there is no external component.

An IP Recorder configured for gateway-side SIPREC forking *cannot* be configured with any station-side interception capture. If it is necessary to capture both gateway-side forking and station-side interception capture, separate recorder servers *must* be deployed for each.

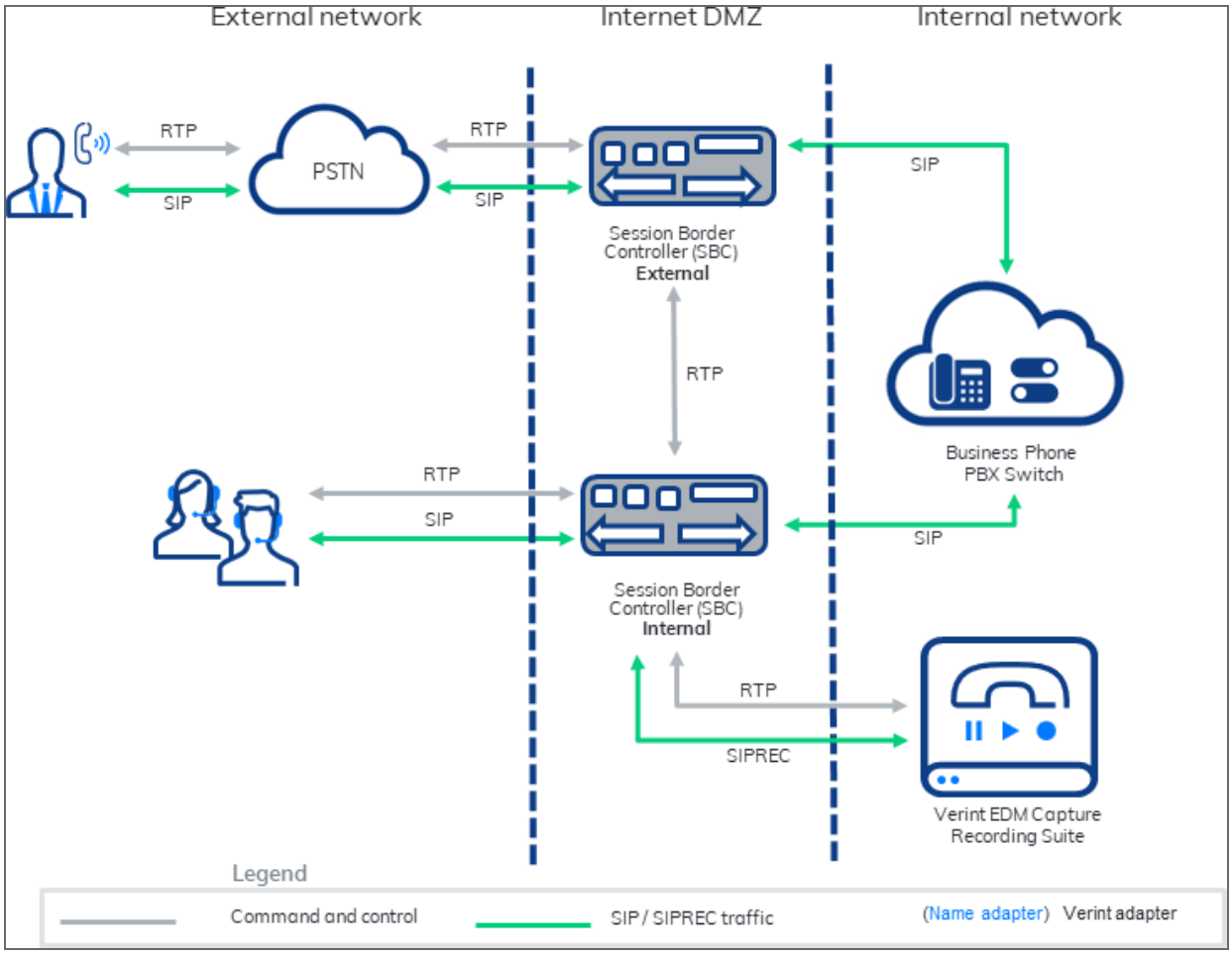
Related topics

SIPREC (page 10)

SIPREC line-side forking

Deploy line-side Session Initiation Protocol Recording (SIPREC) when you need to record inbound and outbound customer calls and internal calls between agents. Line-side forking is a supported Session Initiation Protocol Recording (SIPREC) deployment. In a line-side configuration, a device between the

internal user devices and the internal Private Branch Exchange (PBX) switch forks the audio of a call or the communication session.



The communication session is for the internal device since the Session Border Controller (SBC) connects directly with the agent devices. The call and agent device are identified by the SBC's metadata. This deployment can record all call traffic-inbound, outbound, and internal.

The SIPREC metadata provides precise and timely information in response to any changes in the underlying communication session. The recordings match both a unique call identifier and a monitored device identifier. As the call information or participant list changes, the SIPREC metadata must be updated.

Related topics

SIPREC (page 10)

Speaker separation

Speaker Gateway-side

In a gateway environment, identifying the internal and external participants of the call can be tricky. Some SBC vendors provide a deterministic algorithm for identifying the participants. Other vendors require significant configuration to identify partcipants.

Oracle SBC

The Oracle SBC does not offer a deterministic algorithm for identifying the internal and external participants. To identify the streams properly, the customer configures far-end and near-end identifiers on the data source. The customer can configure either an IP address or a host name for these identifiers. The system extracts out the participants from the SIPREC metadata XML and compares them to the configuration.

There is no guaranteed way to write the code that identifies the internal and external participants on the call. Typically, customers begin with the external PSTN trunk addresses and the internal trunk addresses. In the following XML example, two participants are identified:

- sip:7705551234@**172.10.20.75**
- 8001234567@**172.10.30.6**

```
<?xml version='1.0' encoding='UTF-8'?>
<recording xmlns='urn:ietf:params:xml:ns:recording'>
    <datamode>complete</datamode>
    <session id="KY62Egt4SFhz3a7hN3MJVw==">
        <associate-time>2022-08-29T12:17:02</associate-time>
        <extensiondata xmlns:apkt="http://acmepacket.com/siprec/extensiondata">
            <apkt:ucid>00FA080020E8D6630CE67E;encoding=hex</apkt:ucid>
            <apkt:callerOrig>true</apkt:callerOrig>
        </extensiondata>
    </session>
    <participant id="OwMEdo9qRopDUiHlEn6HPA=="
session="KY62Egt4SFhz3a7hN3MJVw==">
        <nameID aor="sip:7705551234@172.10.20.75">
            <name>7705551234</name>
        </nameID>
```

```
        <send>m0gMJXkATsdUjsygMnS6ug==</send>
        <associate-time>2022-08-29T12:17:02</associate-time>
        <extensiondata xmlns:apkt="http://acmepacket.com/siprec/extensiondata">
            <apkt:callingParty>true</apkt:callingParty>
        </extensiondata>
    </participant>
    <participant id="MjJXBODPSyBu7YC3WFqNxQ=="
session="KY62Egt4SFhz3a7hN3MJVw==">
        <nameID aor="sip:8001234567@172.10.30.6">
            <name>8001234567</name>
        </nameID>
        <send>ImL+QesGT/FSMjNJ2zQq4A==</send>
        <associate-time>2022-08-29T12:17:02</associate-time>
        <extensiondata xmlns:apkt="http://acmepacket.com/siprec/extensiondata">
            <apkt:callingParty>false</apkt:callingParty>
        </extensiondata>
    </participant>
    <stream id="m0gMJXkATsdUjsygMnS6ug==" session="KY62Egt4SFhz3a7hN3MJVw==">
        <label>774770595</label>
        <mode>separate</mode>
        <associate-time>2022-08-29T12:17:02</associate-time>
    </stream>
    <stream id="ImL+QesGT/FSMjNJ2zQq4A==" session="KY62Egt4SFhz3a7hN3MJVw==">
        <label>774770596</label>
        <mode>separate</mode>
        <associate-time>2022-08-29T12:17:02</associate-time>
    </stream>
</recording>
```

Configure SIPREC adapters for directional speaker stream ordering

In certain deployments, media stream ordering for far-end and near-end speakers is direction-dependent. Typically:

- Inbound calls present the far-end (customer) audio first.
- Outbound calls present the near-end (agent) audio first.

To support this behavior, configure two SIPREC adapters:

- One for inbound traffic
- One for outbound traffic

Both adapters should reference the same data source, but listen on separate ports. Use the CustomerStreamFirst advanced key to define stream priority:

- Set `CustomerStreamFirst` = `true` on the inbound adapter
- Set `CustomerStreamFirst` = `false` on the outbound adapter

Update the Session Border Controller (SBC) to route SIPREC traffic accordingly:

- Send inbound traffic to the inbound adapter
- Send outbound traffic to the outbound adapter

If you are using custom configurations, such as attribute extraction then apply them to each adapter individually.

Avaya Session Border Controller for Enterprise (SBCE)

The Avaya SBCE release v8.1.2 and later provides a deterministic algorithm for identifying the internal and external participants. The SBCE tags the external media streams with the label of "10." The SBCE tags internal media streams with the label of "20."

Sonus SBC

The Sonus SBC provides a deterministic algorithm for identifying the internal and external participants. The SBC offers the external media stream first and the internal media stream second.

Related topics

SIPREC (page 10)

Speaker Line-side

In a line-side environment, there is always an internal device on the call. The recording system identifies the internal device through the SIPREC metadata participants. The participant fields indicate who is talking on the relative media streams. The participants XML element will contain the relevant device identifier within the user information portion of the SIP URI.

Related topics

SIPREC (page 10)

Limitations

The Recorder Integration Service (RIS) cannot record additional media streams that are introduced after the initial SIP INVITE message. The following are the details:

- The RIS captures only the first media stream defined in the initial SIP INVITE.
- Any subsequent SDP changes (such as, new media streams) introduced through later SIP INVITE messages are not recorded.

For example, if a call starts with one audio stream and a new SIP INVITE is sent to add a second audio stream, the RIS will not capture the second stream.

Related topics

SIPREC (page 10)
Recording Methods (page 8)

Supported Integration Environments

The following table lists the integration environments that support VoIP Delivery.

	CTI Server or Middleware Protocol	Full VoIP Delivery	Selective VoIP Delivery	N+M All shared	N (dedicated) +M (shared)
Avaya Communication Manager	CVLAN, TSAPI or Genesys (using DMCC)	✓	✓	✓	**
Avaya Communication Manager	DLG or ICM	✓	*	*	
Avaya NES (formerly Nortel) CS 1000	CCMS		✓	✓	

* For Selective VoIP delivery or N+M (all shared) redundancy, environment must be combined with a second middleware or CTI Server protocol that supports shared resources.

** Avaya DMCC Single-Step Conferencing is the only supported recording method for the M (shared) Recorders.

Chapter 2

VoIP Delivery Site Preparation

This section focuses on the preparation you must perform on-site in advance of Recorder deployment. The site must be ready to be connected to the Recorder.

Topics

Network Configuration Requirements

The following sections describe the delivery NIC IP and port requirements, how to calculate the number of ports required, and additional network considerations.

Delivery NIC and IP and Port Requirements

An IP address and a consecutive series of UDP ports must be available for the delivery NIC on the Recorder. This is the destination IP to which the media is streamed from the phones / media proxies / edge devices. These ports must be enabled in the firewall so that the media can reach the Recorder.

Calculating the number of ports required

VoIP Delivery recording requires a large port range of UDP ports. The UDP port range must begin at 1024 or higher to avoid conflicts with other services. In addition, make sure that the port range falls outside of the ephemeral port range (49152-65535).

- For VoIP Delivery, open the ports based on the formula: **`<number of configured channels> * 4 * 1.2`**. Suggested port range is **16384-29999**.
  A minimum of 100 ports range is required (even if the calculation yields a lower number).
  Configure the VoIP Delivery ports in the Recorder Manager.
- For Real-Time Speech Analytics (RTSA), open the ports based on the formula: **`<number of configured channels> * 2`**. Default port range is **30000-35500**
  Configure the RTSA ports in the Enterprise Manager.
- For Real-Time Monitoring, open the ports based on the formula: **`<number of concurrent real-time monitoring> * 2`**. Default port range is **36000-36998**.
  Configure the Real-Time Monitoring ports in the Enterprise Manager.

Related information

Configure network cards and filters (*Workforce Optimization Recorder Configuration and Administration Guide*)

Recorder Analytics Framework server role settings (*Enterprise Manager Configuration and Administration Guide*)

Content Server server role settings (*Enterprise Manager Configuration and Administration Guide*)

Extensions

For VoIP Delivery, you must configure the extensions that you want to record in Enterprise Manager. See the *Recorder Configuration and Administration Guide*.

N+M Redundancy in VoIP Delivery

Please note the following:

- For Full recording environments with dedicated resources, N is dedicated and M is shared. For Selective recording environments with shared resources, N and M are both shared.
- The supported tapping mode of the shared VoIP modules is VoIP Delivery using Avaya DMCC, with Single-Step Conferencing (SSCONF). For further information refer to Avaya Integration with Recorders Guide.

See Supported Integration Environments (page 18) for a complete list of supported environments.

Chapter 3

Archiving site preparation

This chapter outlines the site preparation requirements for deployments implementing the Recorder Archive solution.

Topics

Archiving

Archiving for the Recorder is the process of transferring recorded content stored locally on Recorder servers to storage media for long-term storage or for disaster recovery.

The *Archive Administration Guide* provides an overview of archive functionality, supported archive devices, components, and data flows. It also includes the procedures for setting up and administering archiving.

Before you can set up archiving, though, you must establish the prerequisites on site and gather required information.

Related topics

Archiving site preparation (page 22)

Archiving requirements

Configure a separate physical drive for archiving recordings.

Archive Drive

For each archive drive and media type configured, provide the following information:

- The type of drive configured, such as RDX drive (Removable Disk Technology)
- A logical name for the drive
- The archive drive path and folder name
  - For SAN drives provide a full UNC path (including \\), a local path, or a mapped drive path. For a file share path:
    - Configure the archive processes with access and read/write/delete to the path.
    - Run the archive service under a named Windows account (not *LocalSystem*) with rights to the share.
  - For FTP, provide the user name and password and the port. The default port is 21.
  - For EMC Centera, determine where to place the Pool Entry Authorization (PEA) file and the format of the connection string.
  - For Hitachi HCP, provide a URL in the following format:

    http(s)://namespace.tenant.HitachiserverFQDN

    For example: https://archive1.tenant1.hcpvm.lab.local
    - *archive1* is the namespace to which the media is written.
    - *tenant1* is the tenant that owns the namespace.
    - *hcpvm.lab.local* is the FQDN (Fully Qualified Domain Name) of the Hitachi server.

    For Hitachi HCP, provide the user name and password of the tenant that has access to the namespace to which media is written.
  - For Amazon S3, provide the path that was given when the object storage hosted service account was opened. You must also provide the customer AWS Signature Version, Bucket Name, Authentication type (Access Key or Role), and the Access Key ID, and Secret Access Key or Role Name and External ID.
  - For Azure Blob Storage, provide the path in the blob storage. Default is 2019/10/30/11. Maximum 24 characters. Value included here must be a valid path with a path separator, /, such as calls/video. Example: If the Path setting is calls/video, the blob storage uses the path hierarchy, calls/video/2019/10/30/11. If the Path setting is blank, the path used is 2019/10/30/11.

    You also need the following information for Azure Blob Storage:

- Account Name
- Account Key
- Container Name
- Endpoint Protocol
- Endpoint Suffix

- Archive Database service name

Campaigns

Provide specific criteria for configuring campaigns. For example, “Archive all Calls for 365 days” or "Archive Call by DNIS = 123 for 365 days”. Be as specific as possible.

Bandwidth

If you require network throttling for archiving, specify the throttle rate (MB/Min).

Schedule

Specify whether you require continuous 24-hour archiving, or a specific archiving schedule. For scheduling, you must specify archiving times for each day of the week, with up to half an hour resolution. For example: Sundays: 16:00 to 19:00, Mondays: 08:00 to 11:30 and 14:30 to 18:30.

Related topics

Archiving site preparation (page 22)