Microsoft Teams: SBC Certification Program to Interop between Phone System Direct Routing Interface and Certified Session Border Controllers

Version : 1.0

Draft: July 2018

Microsoft Corporation Technical Documentation License Agreement (Standard)

READ THIS! THIS IS A LEGAL AGREEMENT BETWEEN MICROSOFT CORPORATION (“MICROSOFT”) AND THE RECIPIENT OF THESE MATERIALS, WHETHER AN INDIVIDUAL OR AN ENTITY (“YOU”). IF YOU HAVE ACCESSED THIS AGREEMENT IN THE PROCESS OF DOWNLOADING MATERIALS (“MATERIALS”) FROM A MICROSOFT WEB SITE, BY CLICKING “I ACCEPT”, DOWNLOADING, USING OR PROVIDING FEEDBACK ON THE MATERIALS, YOU AGREE TO THESE TERMS. IF THIS AGREEMENT IS ATTACHED TO MATERIALS, BY ACCESSING, USING OR PROVIDING FEEDBACK ON THE ATTACHED MATERIALS, YOU AGREE TO THESE TERMS.

1. For good and valuable consideration, the receipt and sufficiency of which are acknowledged, You and Microsoft agree as follows:

(a) If You are an authorized representative of the corporation or other entity designated below (“**Company**”), and such Company has executed a Microsoft Corporation Non-Disclosure Agreement that is not limited to a specific subject matter or event (“**Microsoft NDA**”), You represent that You have authority to act on behalf of Company and agree that the Confidential Information, as defined in the Microsoft NDA, is subject to the terms and conditions of the Microsoft NDA and that Company will treat the Confidential Information accordingly;

(b) If You are an individual, and have executed a Microsoft NDA, You agree that the Confidential Information, as defined in the Microsoft NDA, is subject to the terms and conditions of the Microsoft NDA and that You will treat the Confidential Information accordingly; or

I If a Microsoft NDA has not been executed, You (if You are an individual), or Company (if You are an authorized representative of Company), as applicable, agrees: (a) to refrain from disclosing or distributing the Confidential Information to any third party for five (5) years from the date of disclosure of the Confidential Information by Microsoft to Company/You; (b) to refrain from reproducing or summarizing the Confidential Information; and (c) to take reasonable security precautions, at least as great as the precautions it takes to protect its own confidential information, but no less than reasonable care, to keep confidential the Confidential Information. You/Company, however, may disclose Confidential Information in accordance with a judicial or other governmental order, provided You/Company either (i) gives Microsoft reasonable notice prior to such disclosure and to allow Microsoft a reasonable opportunity to seek a protective order or equivalent, or (ii) obtains written assurance from the applicable judicial or governmental entity that it will afford the Confidential Information the highest level of protection afforded under applicable law or regulation. Confidential Information shall not include any information, however designated, that: (i) is or subsequently becomes publicly available without Your/Company’s breach of any obligation owed to Microsoft; (ii) became known to You/Company prior to Microsoft’s disclosure of such information to You/Company pursuant to the terms of this Agreement; (iii) became known to You/Company from a source other than Microsoft other than by the breach of an obligation of confidentiality owed to Microsoft; or (iv) is independently developed by You/Company. For purposes of this paragrap“, "Confidential Informat”on" means nonpublic information that Microsoft designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential by Recipien“. "Confidential Informat”on" includes, without limitation, information in tangible or intangible form relating to and/or including released or unreleased Microsoft software or hardware products, the marketing or promotion of any Microsoft product, Micros’ft's business policies or practices, and information received from others that Microsoft is obligated to treat as confidential.

2. You may review these Materials only (a) as a reference to assist You in planning and designing Your product, service or technolog“ ("Prod”ct") to interface with a Microsoft Product as described in these Materials; and (b) to provide feedback on these Materials to Microsoft. All other rights are retained by Microsoft; this agreement does not give You rights under any Microsoft patents. You may not (i) duplicate any part of these Materials, (ii) remove this agreement or any notices from these Materials, or (iii) give any part of these Materials, or assign or otherwise provide Your rights under this agreement, to anyone else.

3. These Materials may contain preliminary information or inaccuracies, and may not correctly represent any associated Microsoft Product as commercially released. All Materials are provided entire“y "AS ”S." To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

4. If You are an entity and (a) merge into another entity or (b) a controlling ownership interest in You changes, Your right to use these Materials automatically terminates and You must destroy them.

5. You have no obligation to give Microsoft any suggestions, comments or other feedbac“ ("Feedb”ck") relating to these Materials. However, any Feedback you voluntarily provide may be used in Microsoft Products and related specifications or other documentation (collectivel“, "Microsoft Offeri”gs") which in turn may be relied upon by other third parties to develop their own Products. Accordingly, if You do give Microsoft Feedback on any version of these Materials or the Microsoft Offerings to which they apply, You agree: (a) Microsoft may freely use, reproduce, license, distribute, and otherwise commercialize Your Feedback in any Microsoft Offering; (b) You also grant third parties, without charge, only those patent rights necessary to enable other Products to use or interface with any specific parts of a Microsoft Product that incorporate Your Feedback; and (c) You will not give Microsoft any Feedback (i) that You have reason to believe is subject to any patent, copyright or other intellectual property claim or right of any third party; or (ii) subject to license terms which seek to require any Microsoft Offering incorporating or derived from such Feedback, or other Microsoft intellectual property, to be licensed to or otherwise shared with any third party.

6. Microsoft has no obligation to maintain confidentiality of any Microsoft Offering, but otherwise the confidentiality of Your Feedback, including Your identity as the source of such Feedback, is governed by Your NDA.

7. This agreement is governed by the laws of the State of Washington. Any dispute involving it must be brought in the federal or state superior courts located in King County, Washington, and You waive any defenses allowing the dispute to be litigated elsewhere. If there is litigation, the losing party must pay the other party’s reasonable attorneys’ fees, costs and other expenses. If any part of this agreement is unenforceable, it will be considered modified to the extent necessary to make it enforceable, and the remainder shall continue in effect. This agreement is the entire agreement between You and Microsoft concerning these Materials; it may be changed only by a written document signed by both You and Microsoft.

Table of Contents

1.0 Revision History

Revision	Date	Description
0.4	Nov 2017	Original Document shared with partners
0.5	March 2018	Added DTLS requirements for bypass, Icelite clarifications and Test cases for certification
0.6	March 2018	Section 5.7 - Changed the m line descriptor for SDP containing DTLS or DTLS and SDES, added a few more tests in SRTP section, clarified some requirements in Icelite and Failover sections
0.7	May 2018	Clarified /Updated offer Answer expectation for ByPass Mode.Added/removed test cases. Test cases matrix is attached along with this document. Added test case for ICELite to ICELite Scenario
0.8	June 2018	Added the Self- Test criteria for SBC Models REFER made as Mandatory for Non-Media Bypass and Media Bypass Transfer scenarios
0.9	June 2018	Modified steps for Consultative transfer test cases Changed BYOT to Direct Routing, Added a row for partner training for Microsoft support organization, pairing and SBC troubleshooting. Added Clarification on the Number of samples for Product samples table.
1.0	July 2018	Modified transfer test cases with REFER Replaced 'Teams SIP Proxy' with 'Direct Routing interface' in the test cases Removed not supported test cases

2.0 Introduction to Microsoft Teams Direct Routing SBC Certification Program

Microsoft Teams partner solution certification programs are designed to help partners bring premium communication experiences to the market. The *Direct Routing SBC certification* shall also be referred to as the *certification program* in this document. Microsoft Teams customerstrust the certification as an assurance that the partner solutions have been tested to provide the quality, compatibility, and reliability that ensures the best communication experience, and that the partner solutions are backed by best in class product support.

Solutions which pass the technical and process requirements outlined in this specification are eligible to:

- Use the certification logo and associated Microsoft related branding as outlined in the certification contract
- Be listed on Microsoft sites including Microsoft product documentation as certified devices
- Participate in integrated support with Microsoft

2.1 Prerequisites to becoming a Partner

- A long-term interest in developing product lines for the Microsoft Teams or Skype for Business platform;
- A proven record of developing and marketing enterprise grade communication solutions;
- Established enterprise sales channels;
- Established high-quality customer support network;
- Commitment to acquire a Premier support contract;
- Program membership at the Certified or Gold Certified membership level, as such terms are defined in the applicable Microsoft Partner Program documentation. Join at a level that aligns with your business strategies.

2.2 Certification and Re-testing timelines

Partner solutions are expected to build to the latest published specification at the time of development, and to update their solution at regular intervals to maintain compliance with program updates.

We define two terms:

Enforcement Period – this is the time from when a specification is published until all newly submitted products must meet the new specification.
Recertification Period – this is the time by which any existing certified products must be updated and retested against a new specification or newer versions of the Microsoft UC solution.

Category	Enforcement period	Recertification period

Shipped product	6 months	9 months

* Recertification for partner operated service requires compliance against any new requirements and may include targeted retesting against previous requirements

Though all efforts are made to ensure that the specification is final at the time of publication, and to allow partners a reasonable time to accommodate new changes, it is possible that urgent changes may need to be made outside of the normal enforcement and recertification periods. Microsoft will communicate directly with partners to coordinate any such hotfixes.

2.2.1 Delivery of updated solution

Once a solution is certified against the latest specification, or if an interim update is required due to either a hotfix or update in any Microsoft SDK components, partners are expected to facilitate and encourage customers to update.

2.3 Overview of the Certification Process

Certification entails more than simply testing a product against a test plan. It also includes a variety of process alignments between Microsoft and the partner (e.g., for support) as well as structured customer feedback. The following steps must be completed to achieve and maintain a certification:

Action	Owner
Complete legal contracts: NDA, Certification Program Brand Licensing Agreement	Partner
Notify the certification program team at Microsoft if the candidate product has any unique features or if there is any question about which certification category applies to the product.	Partner
Develop product to meet requirements (including self-testing)	Partner
Develop hooks for test automation, synthetic transactions and telemetry (as applicable for program and solution delivery method).	Partner
Plan and execute customer TAP or Preview (if applicable)	Partner/Microsoft
Perform certification testing (at Partner expense)	Lab
If failures are identified by lab testing, fix and resubmit to lab (additional fees may apply)	Partner
Review final lab test results and TAP bugs or feedback (identify resolution plan)	Microsoft
Support process alignment (including training, drills, and sample product)	Partner/Microsoft
Draft detailed product documentation, configuration guidance & marketing content	Partner
Review product documentation & marketing content for compliance with program scope	Microsoft
Approve certification	Microsoft
Prepare and conduct training for Microsoft support organization on how to pair the SBC and troubleshooting methodology	Partner
Publish certification on Microsoft websites	Microsoft

Perform post-certification requirements (e.g., Noc-Noc or support drills, telemetry and business metric reviews, fix temporary waivers, customer education / training sessions, recertification)	Partner/Microsoft

2.4 Product samples

Partner must provide product samples to Microsoft and independent lab for purposes of testing, and other evaluation purposes

2.4.1 Use of samples provided to Microsoft

Microsoft adds all devices that are being certified in the engineering development lab. The devices are used for making test calls in production and pre-production environment. Microsoft will not release new code until all tests against the certified SBCs completed successfully in the preproduction environment.

The samples provided to Microsoft will not be returned, however samples provided to independent labs may be reclaimed after certification test cycle completion. The sample must be GA versions, unless otherwise agreed. The product samples must be supported by the partner.

Deliver to	Number of samples
Microsoft	As agreed with Microsoft. At least two per each certified platform. If several SBC share the platform only one SBC is required. Criteria that define if an SBC belongs to the same platform are in section 2.7
Test Lab*	As described in the Test Topology section

*Partner can request lab to complete relevant NDA before delivery

2.5 Qualification Testing

Qualification testing normally is conducted at an approved independent test lab that is trained by Microsoft.

The certification partner is responsible for:

- Scheduling the lab testing
- Providing samples and all necessary product documentation to the lab
- Paying testing fees directly to the lab (and any re-test fees if necessary)

The independent lab is responsible for:

- Committing a schedule for test completing and fulfilling the schedule commitment unless delays are due to product defects or lack of product documentation or other collateral.
- Providing a standardized test report to Microsoft indicating the candidate solution’s performance relative to the specification.

2.6 Prerequisites for Self-Testing

For the SBCs that share the same platform validation only once SBC is required. All other models, sharing the platform with validated SBC can use self-test method.

Eligibility for self-validation option:

- The SBCs should have the same firmware code
- DSP type of the SBCs is the same across models,
- SBCs have the same CPU family
- SBCs Perform transcoding in the same manner
- SBCs handle voice in the same fashion

2.7 Criteria for recertification

Every new firmware version requires re-certification.

If any of the firmware version number changes, the SBC partners requires to recertify the SBCs. Any re-test requires paying a fee to selected CTCs.

2.8 Product support and live-site operations

All certification partners are required to maintain first-tier quality of support for their certified products, which means a support level that meets or exceeds the support provided for the company's non-certified products and is among the best across peers in the solution category.

To support first-tier support, partners are required to have a Microsoft Premier support contract. All post-certification (in-market) support is expected to route through this support channel rather than through the Microsoft certification program team.

In addition, partner is required to perform a variety of support integration activities, to ensure that the two support organizations work well together.

2.8.1 Support benefit options

SBC partners must have a premier support contract that allows partners to open support tickets on behalf of the customer in addition to several other benefits. More information on the Premier Support for Partners program can be found here.

2.8.2 Support integration requirements

2.8.2.1 Support Training

Partners are required to develop training content and a step-by step troubleshooting guide which will be delivered to Microsoft support organization's regional trainers. The training is typically 1-2 hours of content delivered as a presentation with leave-behind collateral. Partners are expected to deliver updated training after recertification if there are major changes to the product. The objective of this training is to educate the Microsoft support organization on the product to the degree that they can speak generally about the product, perform basic troubleshooting and collect enough information to efficiently initiate a support hand-off to the partner. Training must also include information for how to configure specific features supported by the SBC in order to integrate with the Microsoft cloud service.

2.8.2.2 Customer facing documentation

Partners are required to provide and maintain step-by step troubleshooting and configuration guides to the customers by publishing them on the partners web site. Partners are required to update documentation if Microsoft adds new functionality which requires changes in partner interconnection instructions.

2.8.2.3 Live-site support (NOC to NOC support)

SBC partners are required to have additional support requirements as described below:

24hr Global Premium Support – Partner has to have a premium support center staffed at all times able to take calls and get domain experts on phone bridges in short order to solve customer high priority, high severity incidents.
NOC to NOC Support – Partner must provide NOC-NOC support process documentation prior to certification that describes:
Process for Microsoft to contact partner support in case if a Sev 0 / Major incident.
Commands that need to be executed to reproduce an issue
Steps to be carried out to collect logs from a customer's SBC

A sev1 incident involving a certified SBC is an outage impacting several users, such that users are unable to place to or from Teams via their Direct Connect certified SBC. The partner is expected to acknowledge the incident within 15 minutes and get on each other's Sev 0 incident bridge within 30 min of contact initiation to provide short term resolution, root cause analysis and a longer-term resolution plan, if applicable,
Noc-Noc drill – in order to practice the support engagement process for high priority issues that require real-time investigation by Microsoft dev-ops team, Microsoft and the partner will conduct drills before certification and at a regular cadence (no less than once a quarter) after the service is live. Microsoft and Partners are expected to acknowledge the incident within 15 minutes and get on each other's, Sev0 incident bridge within 30 minutes.

3.0 Data reporting

Partners have to provide on quarterly basis the following information:

- Bugs reported by Direct Routing customers across the various SBC models certified;

4.0 Publishing your certification

On receiving formal approval from certification program team, the partner must work with Microsoft marketing to provide device images, company logo and marketing content for posting to Microsoft websites.

Partner and Microsoft will periodically review the list of qualified products to be removed from the active **the partner solutions catalog** listing because of end of life, field issues, or replacement by newer models. Additionally, Microsoft will remove any product that fails to maintain certification status for any reason.

4.1 Contacting Microsoft

For any questions regarding requirements detailed in any of the specifications, please contact the certification program team at drsbccertification@microsoft.com

5.0 Product Specifications

5.1 Scope of Certification

A Session Border Controller deployed on the customer's network can interface with the Direct Routing interface in Microsoft Teams service in the cloud, allowing the customer to terminate PSTN traffic to and from their Teams client using the customer's own SIP trunk provider. This Service is known as Direct Routing. More information about direct routing is available here. This document describes all the requirements for a Session Border Controller (SBC) to be certified with Direct Routing interface.

The SBC connected to the Direct Routing must support the following

- ICE Lite per RFC 5245 to support Media Bypass;
- Protect RTP traffic using SRTP. SBC must be able to establish keys using both SDES (RFC 3711 and RFC 4771) and DTLS-SRTP (RFC 5764) methods[1]
- Ability to either:
  - Recommended: transcode SILK or
  - Supported for certification: Support SILK Passthrough mode[2]
- Support RTCP Multiplexing;
- Support using TLS v1.2 to protect SIPSupport of handling REFER on SBC [3]
- Support of the following codecs – SILK, G729, G711, optionally OPUS;
- Support of adding Certificates from the 3rd party Certification authorities to protect connection between the SBC and the Direct Routing interface. The list of Certification authorities supported by Direct Routing interface is available on https://aka.ms/drplandirectrouting
- Support of handling Refer locally with no limitations of number of symbols in Refer header. Direct Routing interface can send Refer header with up to 1000 symbols[3]

1. Please refer to appendix for the examples of using DTLS-SRTP and SDES in this document. Direct Routing prefers using SDES, but in case if the WebRTC client only supports DTLS, DTLS will be

used. This approach requires SBC in Media Bypass mode on invite sending two methods in the same message: SDES and DTLS-SRTP

2. Even though Microsoft supports SILK passthrough, Microsoft will not recommend SBC that use only SILK passthrough to the customers if SIP trunk, connected to the SBC does not support SILK codec. Reason: from our telemetry and customer feedback we see that using G.711 or G729 over internet is not optimal from end user experience point of view. G.711 is not susceptible to internet conditions (no QoS end to end, potential delays of the packets) and, therefore, we observer issues with voice quality. On the other side, SILK was designed by Microsoft to work over the internet and compensate potential issues with network conditions. The difference in terms of end user experience between using G.711 and SILK is notable with SILK providing much better voice quality if traffic flows via internet. If SBC only supports SILK pass through, the only case where Microsoft will recommend using SBC with SILK passthrough is when SIP trunk behind the SBC supports SILK codec.

3. Ability to handle REFER is mandatory when using Media Bypass mode and non-Media Bypass mode. If calls are transferred the Direct Routing will always send REFER to SBC

Detailed requirements for Media and Sip protocol described in:

- Appendix 1. Direct Routing SIP Protocol description;
- Appendix 2. Media Encryption Offer / Answer Requirement for SBC in BYPASS Mode

If any portion of the document is not clear or you have feedback on the specification, please consult with drsbccertification@microsoft.com

5.2 End to End Scenarios

The section below outlines the details tests cases required to pass during the certification process. The certification test performed by TekVizion lab.

The tests performed with Teams and Skype for Business (once supported) Windows Clients unless the case description indicates use of a different client

5.2.1 Definitions

- **Outbound call.** Call from a Teams or SfB client to a PSTN Number (Teams/SfB Cleint-> Direct Routing -> SBC -> SIP/TDM Trunk);
- **Inbound call**. Call from a PSTN number to a Teams or SfB user (SIP/TDM Trunk -> SBC -> Direct Routing -> Teams/SfB Client)

5.2.2 Simple Inbound/Outbound PSTN Calls and Call Handling

5.2.2.1 Device supports ptime of 20 ms for an inbound call to Teams user

ID	43920
Priority	1
Summary	[Objective] Device must be able to establish a call with the configured ptime (= 20ms). [Pre-condition] - Configure Device to have ptime value of 20ms.

Step	Action	Expected Result
1	PSTN user calls Teams user	Direct Routing interface receives INVITE from Device. The INVITE's SDP ptime value is set to 20ms.
2	Teams user picks up the call	Call is connected with bi-directional audio, voice is clear and no echo.
3	PSTN user hangs up	Call is disconnected

5.2.2.2 Device sends its own FQDN in the contact header

ID	43922
Priority	1
Summary	[Objective] Device sends its own FQDN in contact header as described in "Appendix 1 Direct Routing SIP protocol Description" for a call from PSTN user to Teams user. [Pre-Condition] - Device FQDN is set during the setup - Device FQDN should match the FQDN found in Device certificate Subject Name/SAN

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2		Verify that the Contact header in all request messages sent from the device has its own FQDN
3	PSTN user hangs up	Call is disconnected

5.2.2.3 Device is capable to perform manipulation of phone number on outbound call according to the carrier requirement

ID	47275
Priority	1
Summary	[Objective] Validate that the device is capable of manipulating number in the Request URI and To headers according to the carrier requirement. [Pre-Condition] - Device is configured to manipulate phone numbers on outgoing calls

Step	Action	Expected Result
1	Teams user calls PSTN user	Device receives INVITE from Direct Routing interface with number in Request URI and To headers, which does not match the carrier requirement
2		Verify that device performs manipulation of the number according to the carrier requirement
3	PSTN user picks up	Call is connected with bi-directional audio
4	Teams user hangs up	Call is disconnected

5.2.2.4 Device is capable to perform manipulation of phone number on inbound call according to Direct Routing interface requirement

ID	47276
Priority	1
Summary	[Objective] Validate the ability of the device to manipulate phone number on inbound call. [Pre-Condition] - Teams user configured with E.164 number as DID - Device is configured to send only E.164 format numbers to Direct Routing interface

Step	Action	Expected Result
1	PSTN user calls Teams user	Device sends INVITE with only E.164 format numbers to Direct Routing interface
2	Teams user picks up	Call is established with bi-directional audio
3	PSTN user hangs up	Call is disconnected

5.2.2.5 Device accepts call from Teams user where the user's calling line identity is set to anonymous

ID	49028
Priority	1
Summary	[Objective] Device accepts call from Teams user where the user's calling line identity is set to anonymous and process the call towards PSTN/customer SIP Trunk. [Pre-Condition] - Set the Teams user's calling line identity as anonymous. 1. Create a new calling line identity using New-CsCallingLineIdentity command. *New-CsCallingLineIdentity -Identity Anonymous -Description "Anonymous policy" -CallingIDSubstitute Anonymous -EnableUserOverride $false* 2. Assign the new calling line identity policy to the Teams user using the below command. *Grant-CsCallingLineIdentity -Identity "amos.marble@contoso.com" -PolicyName Anonymous*

Step	Action	Expected Result
1	Teams user calls PSTN user	PSTN user rings and displays the caller ID as 'Anonymous' for the ringing call
2	PSTN user picks up	Call is connected with bi-directional audio
3	Teams user hangs up	Call is disconnected

5.2.3 Hold (Music On Hold Disabled)

5.2.3.1 Teams user places inbound call from PSTN on hold and then resumes

ID	43924
Priority	1
Summary	[Objective] Device is able to process Hold-Resume initiated by Teams user for an inbound call from PSTN user.

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Teams user initiates call hold	Call goes on hold with no way audio

3		Direct Routing interface sends a=inactive in the re-INVITE and Device responds with a=inactive (or connection information 0.0.0.0) in the 200 OK
4		Device should send SRTCP packets during hold
5	Teams user resumes the call	Call is resumed with bi-directional audio
6	PSTN user hangs up	Call is disconnected

5.2.3.2 Teams user places outbound call to PSTN on hold and then resumes

ID	43925
Priority	1
Summary	[Objective] Device is able to process Hold-Resume initiated by Teams user in an outbound call to PSTN user.

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Teams user initiates call hold	Call goes on hold with no way audio
3		Direct Routing interface sends a=inactive in the re-INVITE and Device responds with a=inactive (or connection information 0.0.0.0) in the 200 OK
4		Device should send SRTCP packets during hold
5	Teams user resumes the call	Call is resumed with bi-directional audio
6	Teams user hangs up	Call is disconnected

5.2.3.3 Teams user places outbound call to PSTN on hold for over 15 minutes and then resumes

ID	43926
Priority	1
Summary	[Objective] Audio is re-established when Teams user resumes a call after placing it on hold for 15 minutes.

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is established with bi-directional audio
2	Teams user places the call on hold for 15 minutes	Call goes on hold with no way audio
3		Direct Routing interface sends a=inactive in the re-INVITE and Device responds with a=inactive (or connection information 0.0.0.0) in the 200 OK
4		Device should send SRTCP packets during hold
5	Teams user resumes the call after 15 minutes	Call is resumed with bi-directional audio successfully
6	Teams user hangs up	Call is disconnected

5.2.3.4 Teams user places an inbound call from PSTN on hold for over 15 minutes and then resumes

ID	43927
Priority	1
Summary	[Objective] Audio is re-established when Teams user resumes a call after placing it on hold for 15 minutes.

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is established with bi-directional audio
2	Teams user places the call on hold for 15 minutes	Call goes on hold with no way audio
3		Direct Routing interface sends a=inactive in the re-INVITE and Device responds with a=inactive (or connection information 0.0.0.0) in the 200 OK
4		Device should send SRTCP packets during hold
5	Teams user resumes the call after 15 minutes	Call is resumed with bi-directional audio successfully
6	PSTN user hangs up	Call is disconnected

5.2.3.5 Teams user places outbound call to PSTN on hold after 30 minutes and then resumes

ID	43928
Priority	1
Summary	[Objective] When an outbound call has been active for 30 minutes, audio can be re-established if Teams user places call on hold and then resumes.

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is established with bi-directional audio
2	Call is kept connected with active talk path in both directions	SRTP packets are continuously streamed in both directions and two-way audio is still present
3	Teams user places the call on hold after 30 minutes	No audio is present while call is on hold
4		Device sends and receives SRTCP packets while call is on hold and call does not drop
5	Teams user resumes the call	Bi-directional audio is established
6	Teams user hangs up	Call is disconnected

5.2.3.6 Teams user places inbound call from PSTN on hold after 30 minutes and then resumes

ID	43929
Priority	1
Summary	[Objective] When an inbound call has been active for 30 minutes, audio can be re-established if Teams user places call on hold and then resumes.

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is established with bi-directional audio
2	Call is kept connected with active talk path in both directions	SRTP packets are continuously streamed in both directions and two-way audio is still present

3	Teams user places the call on hold after 30 minutes	No audio is present while call is on hold
4		Device sends and receives SRTCP packets while call is on hold and call does not drop
5	Teams user resumes the call	Bi-directional audio is established
6	PSTN user hangs up	Call is disconnected

5.2.3.7 Teams user places outbound call on hold and then disconnects during hold

ID	49672
Priority	1
Summary	[Objective] Device is able to handle the termination made by Teams user when the call is on hold.

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Teams user initiates call hold	Call goes on hold with no way audio
3	Teams user hangs up during the hold	Call is disconnected

5.2.3.8 Teams user places inbound call on hold and then disconnects during hold

ID	49673
Priority	1
Summary	[Objective] Device is able to handle the termination made by Teams user when the call is on hold.

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Teams user initiates call hold	Call goes on hold with no way audio
3	Teams user hangs up during the hold	Call is disconnected

5.2.4 Disconnect

5.2.4.1 PSTN user disconnects inbound call to Teams user before it is answered

ID	43940
Priority	1
Summary	[Objective] Device is able to CANCEL the call before it gets connected.

Step	Action	Expected Result
1	PSTN user calls Teams user	Teams user rings and ring back is heard on PSTN user
2	PSTN user hangs up the call while Teams user is ringing	Teams user stops ringing and call is disconnected on PSTN user
3		Device sends CANCEL to Direct Routing interface and receives 200 OK for the CANCEL
4		Device receives and processes 487 Request Terminated from Direct Routing interface
5		Device responds with ACK to the 487 Request Terminated received

5.2.4.2 Teams user disconnects outbound call to PSTN user before it is answered

ID	43941
Priority	1
Summary	[Objective] Device handles CANCEL sent by Direct Routing interface before the call gets connected.

Step	Action	Expected Result
1	Teams user calls PSTN user	PSTN user rings and ring back is heard on Teams user
2	Teams user hangs up the call while PSTN user is ringing	Device receives, and processes CANCEL from Direct Routing interface
3		Device responds to the CANCEL with 200 OK
4		Device sends 487 Request Terminated to the Direct Routing interface

5.2.4.3 PSTN user disconnects an inbound connected call

ID	43942
Priority	1
Summary	[Objective] Device should handle the disconnect from PSTN user for an inbound connected call.

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

5.2.4.4 PSTN user disconnects an outbound connected call

ID	43943
Priority	1
Summary	[Objective] Device should handle the disconnect from PSTN user for an outbound connected call.

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

5.2.4.5 Teams user disconnects an inbound connected call

ID	43944
Priority	1
Summary	[Objective] Device should handle the disconnect from Teams user for an inbound connected call.

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Teams user hangs up	Call is disconnected

5.2.4.6 Teams user disconnects an outbound connected call

ID	43945
Priority	1

Summary	[Objective] Device should handle the disconnect from Teams user for an outbound connected call.	
Step	**Action**	**Expected Result**
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Teams user hangs up	Call is disconnected

5.2.4.7 Device can disconnect a call forked to Teams users set to "Do not disturb"

ID	43946	
Priority	1	
Summary	[Objective] Device can disconnect a forked call when all Teams users are set to 'Do not Disturb'. [Pre-Condition] - Teams user logged into multiple locations - Status is set to 'Do not Disturb' in Teams Client	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Direct Routing interface forks the call to each location as the Teams user is logged into multiple locations
2	Direct Routing interface sends local 183 Session Progress with SDP first and then sends 480 Temporarily Unavailable to the Device	Device processes the 480 Temporarily Unavailable message and disconnects the call

5.2.4.8 Device responds with 488 Not Acceptable for outbound call

ID	43948	
Priority	1	
Summary	[Objective] Validate that the device can handle properly misconfigured requests (for example, codec misconfiguration, media security method or media security mode mismatch). Proper response on misconfigured requests - respond with 488 Not Acceptable for an outbound call should be sent by Device. [Pre-Condition] - Configure Device to have a misconfiguration which triggers 488 response	
Step	**Action**	**Expected Result**
1	Teams user calls PSTN user	Device receives an INVITE from Direct Routing interface
2	Devices sends "488 Not Acceptable"	Direct Routing interface receives the "488 Not Acceptable" from device and disconnects the call

5.2.5 Early media

5.2.5.1 Device supports Early Media for a call from PSTN to Teams

ID	43949
Priority	1
Summary	[Objective] Device sends Early media support parameters to Direct Routing interface for a call from PSTN user to Teams user.

	[Pre-Condition] - Configure device to support Early media towards Direct Routing interface

Step	Action	Expected Result
1	PSTN user calls Teams user	Teams user rings and ringing is heard on PSTN user
2	Device sends Early media support parameters to Direct Routing interface	The INVITE message sent by device includes SDP
3	Teams user answers the call	Verify if the call is established with two-way audio and there is no audio clipping
4	PSTN user hangs up	Verify if the call is disconnected

5.2.5.2 Device supports Early Media for a call from Teams to PSTN

ID	43950
Priority	1
Summary	[Objective] Device supports Early media towards Direct Routing interface for a call from Teams to PSTN. [Pre-Condition] - Configure device to support Early media towards Direct Routing interface

Step	Action	Expected Result
1	Teams user calls PSTN user	PSTN user rings
2	Device receives INVITE from Direct Routing interface with SDP	Device sends 18x provisional response with SDP as a part of Early media negotiation
3	PSTN user answers the call	Verify if the call is established with two-way audio and there is no audio clipping
4	Teams user hangs up	Verify if the call is disconnected

5.2.5.3 PSTN user calls Teams user that is set to simultaneously ring an IVR number and IVR responds

ID	43953
Priority	1
Summary	[Objective] Device should be able to support the simultaneous ring functionality set on Teams Client. [Pre-Condition] - Configure Teams user simultaneously ring to IVR number on PSTN side

Step	Action	Expected Result
1	PSTN user calls Teams user	Teams user rings and the IVR number also rings simultaneously
2	Device receives the INVITE for IVR number from Direct Routing interface	Device process the simultaneous call towards PSTN
3	Allow the IVR endpoint to answer the call	Device receives 200 OK from PSTN side for the IVR number call and forwards the same to Direct Routing in the second call leg
4	Call gets established between the PSTN user and IVR endpoint	Verify if the PSTN end point is able to hear the IVR menu played after 200 OK
5	PSTN user hangs up	Call is disconnected

5.2.6 Transfers

Device must be able to handle **REFER** based transfers and the **Referred-by** header which carries information of the referrer or the transferring party in a call transfer to PSTN scenario.

Note: Direct Routing sends REFER message with more than 1000 characters in Referred-by header and the device must be able to handle it. Please refer section 6.8 Size of Refer message considerations.

5.2.6.1 Blind Transfer with REFER

5.2.6.1.1 Inbound PSTN Call to Teams blind transferred to Skype For Business user

ID	43955
Priority	1
Summary	[Objective] Device should handle REFER requests for Blind transfer call initiated by Teams user [Pre-Condition] - REFER support enabled on Device

Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Teams user answers the call and call is connected with bidirectional audio
2	Teams user transfers the call to Skype for Business user	Device processes the REFER sent by Direct Routing interface and responds with 202 Accepted
3	Device sends a new INVITE containing "Referred-By" header to Direct Routing interface	Call is connected with bidirectional audio between PSTN user and Skype for Business user
4	PSTN user hangs up	Call is disconnected

5.2.6.1.2 Inbound PSTN Call to Teams blind transferred to second Teams User

ID	43956
Priority	1
Summary	[Objective] Device should handle REFER requests for Blind transfer call initiated by Teams user [Pre-Condition] - REFER support enabled on Device

Step	**Action**	**Expected Result**
1	PSTN user calls Teams user 1	Teams user 1 answers the call and call is connected with bidirectional audio
2	Teams user 1 transfers the call to Teams user 2	Device processes the REFER sent by Direct Routing interface and responds with 202 Accepted
3	Device sends a new INVITE containing “Referred-By" header to Direct Routing interface	Call is connected with bidirectional audio between PSTN user and Teams user 2
4	PSTN user hangs up	Call is disconnected

5.2.6.1.3 Inbound PSTN Call to Teams blind transferred to second PSTN User

ID	43957
Priority	1
Summary	[Objective] Device handles the REFER for a blind transfer call initiated by the Teams user to a second PSTN user [Pre-Condition] - REFER support enabled on Device

Step	Action	Expected Result
1	PSTN user 1 calls Teams user	Call is connected with bi-directional audio
2	Teams user blind transfers the call to PSTN user 2	Device processes the REFER sent by Direct Routing interface and responds with 202 Accepted
3	Device sends a new INVITE containing “Referred-By" header to Direct Routing interface	Call is connected with bidirectional audio between PSTN user 1 and PSTN user 2
4	PSTN user 1 hangs up	Call is disconnected

5.2.6.1.4 Outbound PSTN call from Teams user blind transferred to Skype for Business User

ID	43958
Priority	1
Summary	[Objective] Device should handle REFER requests for Blind transfer call initiated by Teams user [Pre-Condition] - REFER support enabled on Device

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is established with bi-directional audio
2	Teams user transfers the call to Skype for Business user	Device processes the REFER sent by Direct Routing interface and responds with 202 Accepted
3	Device sends a new INVITE containing "Referred-By" header to Direct Routing interface	Call is connected with bidirectional audio between PSTN user and Skype for Business user
4	PSTN user hangs up	Call is disconnected

5.2.6.1.5 Outbound PSTN call from Teams user blind transferred to second Teams User

ID	43959
Priority	1
Summary	[Objective] Device should handle REFER requests for Blind transfer call initiated by Teams user [Pre-Condition] - REFER support enabled on Device

Step	Action	Expected Result
1	Teams user 1 calls PSTN user	Call is connected with bi-directional audio
2	Teams user 1 transfers the call to Teams user 2	Device processes the REFER sent by Direct Routing interface and responds with 202 Accepted

3	Device sends a new INVITE containing "Referred-By" header to Direct Routing interface	Call is connected with bidirectional audio between PSTN user and Teams user 2
4	PSTN user hangs up	Call is disconnected

5.2.6.1.6 *Outbound PSTN call from Teams user blind transferred to second PSTN User*

ID	43960
Priority	1
Summary	[Objective] Device handles the REFER for a blind transfer call initiated by the Teams user to a second PSTN user [Pre-Condition] - REFER support enabled on Device

Step	Action	Expected Result
1	Teams user calls PSTN user 1	Call is connected with bi-directional audio
2	Teams user blind transfers the call to PSTN user 2	Device processes the REFER sent by Direct Routing interface and responds with 202 Accepted
3	Device sends a new INVITE containing "Referred-By" header to Direct Routing interface	Call is connected with bidirectional audio between PSTN user 1 and PSTN user 2
4	PSTN user 1 hangs up	Call is disconnected

5.2.6.1.7 *Inbound call to Teams user transferred to Teams pure online user that has set call forward to PSTN (Microsoft calling plan)*

ID	43962
Priority	1
Summary	[Objective] Device handles REFER for a transferred call [Pre-Condition] - Pure Online user (with Microsoft Calling Plan license) has set call forward to another PSTN user - REFER support enabled on Device

Step	Action	Expected Result
1	PSTN user 1 calls Teams user	Call is established with bi-directional audio
2	Teams user transfers the call to Teams pure online user	PSTN user 2 rings
3	PSTN user 2 picks up	Call is established with bi-directional audio between PSTN user 1 and PSTN user 2
4	PSTN user 1 hangs up	Call is disconnected

5.2.6.1.8 *Device maintains the original session when the blind transferred call fails*

ID	49220
Priority	1
Summary	[Objective] Device maintains the original session when a blind transferred call fails.

	[Pre-Condition] - REFER support enabled on Device

Step	Action	Expected Result
1	Teams user calls PSTN user 1	Device receives INVITE and call is connected with bi-directional audio
2	Teams user transfers the call to an invalid PSTN number	Device processes the REFER sent by Direct Routing interface and responds with 202 Accepted
3	Device forwards the appropriate cause received from PSTN side for the second call leg to Direct Routing interface	Second call leg is disconnected and the first call leg with PSTN user 1 is in hold state
4	Teams user resumes the first call leg with PSTN user 1	Call is connected with bi-directional audio
5	PSTN user hangs up	Call is disconnected

5.2.6.2 Consultative Transfer with REFER

5.2.6.2.1 Inbound PSTN Call to Teams consultative transferred to Skype for Business user

ID	43969
Priority	1
Summary	[Objective] Device is able to handle a consultative transfer performed on Teams side [Pre-Condition] - REFER support enabled on Device

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Teams user makes a consultation call to Skype for Business user	PSTN user goes on hold and Skype for business user rings
3	Skype for Business user picks up	Call is established between Skype for Business user and Teams user with bi-directional audio
4	Teams user transfers the call with PSTN user to Skype for Business user	Device accepts the REFER from Direct Routing interface and transfer is successful
5		Call is established between PSTN user and Skype for Business user with bi-directional audio
6	PSTN user hangs up	Call is disconnected

5.2.6.2.2 Inbound PSTN Call to Teams consultative transferred to Teams User

ID	43970
Priority	1
Summary	[Objective] Device is able to handle a consultative transfer performed on Teams side [Pre-Condition] - REFER support enabled on Device

Step	Action	Expected Result
1	PSTN user calls Teams user 1	Call is connected with bi-directional audio

2	Teams user 1 makes a consultation call to Teams user 2	PSTN user goes on hold and Teams user 2 rings
3	Teams user 2 picks up	Call is established between Teams user 2 and Teams user 1 with bi-directional audio
4	Teams user 1 transfers the call with PSTN user to Teams user 2	Device accepts the REFER from Direct Routing interface and transfer is successful
5		Call is established between PSTN user and Teams user 2 with bi-directional audio
6	PSTN user hangs up	Call is disconnected

5.2.6.2.3 Inbound PSTN Call to Teams consultative transferred to another PSTN User

ID	43971
Priority	1
Summary	[Objective] Device is able to handle a consultative transfer performed on Teams side [Pre-Condition] - REFER support enabled on Device

Step	Action	Expected Result
1	PSTN user 1 calls Teams user	Call is connected with bi-directional audio
2	Teams user makes a consultation call to PSTN user 2	PSTN user 1 goes on hold and PSTN user 2 rings
3	PSTN user 2 picks up	Call is established between PSTN user 2 and Teams user with bi-directional audio
4	Teams user transfers the call with PSTN user 1 to PSTN user 2	Device accepts the REFER from Direct Routing interface and transfer is successful
5		Call is established between PSTN user 1 and PSTN user 2 with bi-directional audio
6	PSTN user 1 hangs up	Call is disconnected

5.2.6.2.4 Outbound PSTN call from Teams user consultative transferred to Skype for Business User

ID	43972
Priority	1
Summary	[Objective] Device is able to handle a consultative transfer performed on Teams side [Pre-Condition] - REFER support enabled on Device

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Teams user makes a consultation call to Skype for Business user	PSTN user goes on hold and Skype for business user rings
3	Skype for Business user picks up	Call is established between Skype for Business user and Teams user with bi-directional audio
4	Teams user transfers the call with PSTN user to Skype for Business user	Device accepts the REFER from Direct Routing interface and transfer is successful
5		Call is established between PSTN user and Skype for Business user with bi-directional audio

6	PSTN user hangs up	Call is disconnected

5.2.6.2.5 *Outbound PSTN call from Teams user consultative transferred to Teams User*

ID	43973
Priority	1
Summary	[Objective] Device is able to handle a consultative transfer performed on Teams side [Pre-Condition] - REFER support enabled on Device

Step	**Action**	**Expected Result**
1	Teams user 1 calls PSTN user	Call is connected with bi-directional audio
2	Teams user 1 makes a consultation call to Teams user 2	PSTN user goes on hold and Teams user 2 rings
3	Teams user 2 picks up	Call is established between Teams user 2 and Teams user 1 with bi-directional audio
4	Teams user 1 transfers the call with PSTN user to Teams user 2	Device accepts the REFER from Direct Routing interface and transfer is successful
5		Call is established between PSTN user and Teams user 2 with bi-directional audio
6	PSTN user hangs up	Call is disconnected

5.2.6.2.6 *Outbound PSTN call from Teams user consultative transferred to PSTN User*

ID	43974
Priority	1
Summary	[Objective] Device is able to handle a consultative transfer performed on Teams side [Pre-Condition] - REFER support enabled on Device

Step	**Action**	**Expected Result**
1	Teams user calls PSTN user 1	Call is connected with bi-directional audio
2	Teams user makes a consultation call to PSTN user 2	PSTN user 1 goes on hold and PSTN user 2 rings
3	PSTN user 2 picks up	Call is established between PSTN user 2 and Teams user with bi-directional audio
4	Teams user transfers the call with PSTN user 1 to PSTN user 2	Device accepts the REFER from Direct Routing interface and transfer is successful
5		Call is established between PSTN user 1 and PSTN user 2 with bi-directional audio
6	PSTN user 1 hangs up	Call is disconnected

5.2.6.2.7 *Device maintains the original session when the consultative transferred call fails*

ID	49255
Priority	1
Summary	[Objective] Device maintains the original session when the consultative transferred call made by

	Teams user fails. [Pre-Condition] - REFER support enabled on Device

Step	Action	Expected Result
1	PSTN user 1 calls Teams user	Teams user picks up and call is connected with bi-directional audio
2	Teams user initiates a consultation call to PSTN user 2	Device receives and processes a hold re-INVITE with a=inactive from Direct Routing interface for the call with PSTN user 1
3		First call between Teams user and PSTN user 1 goes on hold
4		Device receives and processes INVITE from Direct Routing interface for the call with PSTN user 2
5		Second call between Teams user and PSTN user 2 is established
6	Teams user transfers the first call to PSTN user 2, in between the transfer PSTN user 2 hangs up	Transfer fails and first call is still on hold
7	Teams user is able to resume the first call with PSTN user 1	Call is connected with bi-directional audio
8	PSTN user 1 hangs up	Call is disconnected

5.2.7 Call forward, Simultaneous Ring and Call forking

Device must be able to handle **PAI** header with SIP and Tel URI as received from the PSTN Azure edge and forward to the carrier. If along with the PAI header the Device receives a Privacy:id header from the Direct Routing interface then the Device must keep the asserted identity private outside the network trust domain.

Device must be able to handle **history-info** header as received by the Azure PSTN edge in simultaneous ringing and call forward scenarios.

Device must be able to provide **early media** in these scenarios

5.2.7.1 *PSTN User calls a Teams user that has forwarded calls to Delegates*

ID	43981
Priority	1
Summary	[Objective] Device can handle an inbound call to Teams user forwarded to its delegates. [Pre-Condition] - Add delegates for the Teams user - Set call forward to 'Delegates' in Teams client

Step	Action	Expected Result
1	PSTN user calls Teams user	Delegates starts ringing and ring back is heard
2	One of the delegates picks up	Other delegates stop ringing and call is connected with bi-directional audio

3	PSTN user hangs up	Call is disconnected

5.2.7.2 *Inbound call to Teams that is forwarded to voicemail after no response and voicemail is deposited*

ID	43983
Priority	1
Summary	[Objective] Device handles an inbound call from PSTN to Teams user which is forwarded to Voicemail. [Pre-Condition] - Teams user has Voicemail enabled - Unanswered calls forward to voicemail is set in Teams Client settings

Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Teams user rings
2	Teams user does not answer the call	Call is forwarded to Voicemail due to no response timeout
3	PSTN user leaves voicemail	Voicemail is successfully deposited
4	Use DTMF to navigate the voicemail system	Verify that DTMF tones are recognized by the voicemail system

5.2.7.3 *Inbound call to Teams that is forwarded to voicemail after no response and disconnected without leaving voicemail*

ID	43984
Priority	1
Summary	[Objective] Device is able to handle an inbound call to Teams user forwarded to voicemail after no response. [Pre-Condition] - Teams user has Voicemail enabled - Unanswered calls forward to voicemail is set in Teams Client settings

Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Teams user starts ringing
2	Teams user does not answer the call	Call gets forwarded to voicemail due to no response timeout
3	PSTN user disconnects the call without leaving voicemail	Call is disconnected

5.2.7.4 *PSTN user calls Teams user that simultaneously rings second PSTN user and second PSTN user answers*

ID	43985
Priority	1
Summary	[Objective] Device is able to support the simultaneous ring functionality set on Teams user side. [Pre-Condition] - Configure Teams user to simultaneous ring at second PSTN user - Enable Forward Call History and PAI on Teams tenant trunk configuration

Step	Action	Expected Result
1	PSTN user 1 calls Teams user	Both the Teams user and PSTN user 2 ring and ring back is heard on PSTN user 1
2	PSTN user 2 picks up	PSTN user 2 and PSTN user 1 are connected with bi-directional audio
3	PSTN user 1 hangs	Call is disconnected

5.2.7.5 PSTN user calls Teams user that simultaneously rings second PSTN user and Teams user answers

ID	43986
Priority	1
Summary	[Objective] Device is able to support the simultaneous ring functionality set on Teams user side. [Pre-Condition] - Configure Teams user to simultaneous ring at second PSTN user - Forward Call History and PAI on Teams tenant trunk configuration is enabled

Step	Action	Expected Result
1	PSTN user 1 calls Teams user	Both the Teams user and PSTN user 2 ring and ring back is heard on PSTN user 1
2	Teams user picks up	Teams user and PSTN user 1 are connected with bi-directional audio
3	Device processes the CANCEL received for the call to PSTN user 2	Call to PSTN user 2 is terminated successfully
4	PSTN user 1 hangs up	Call is disconnected

5.2.7.6 PSTN user calls Teams user that simultaneously rings delegates and PSTN user hangs up while ringing

ID	43987
Priority	1
Summary	[Objective] Device should handle an inbound call to Teams user who is set to simultaneous ring on delegates. [Pre-Condition] - Teams user set to simultaneous ring on delegates

Step	Action	Expected Result
1	PSTN user calls Teams user	Teams user and its delegates ring simultaneously
2	PSTN user hangs up while ringing	Call is cancelled successfully

5.2.7.7 PSTN user calls Teams user that simultaneously rings delegates and one of the delegates responds

ID	43988
Priority	1
Summary	[Objective] Device should handle an inbound call to Teams user who is set to simultaneous ring on delegates and one of the delegates answers. [Pre-Condition] - Teams user set to simultaneous ring on delegates

Step	Action	Expected Result
1	PSTN user calls Teams user	Teams user and its delegates ring simultaneously
2	One of the delegates picks up	Call is connected with bi-directional audio
3	PSTN user hangs up	Call is disconnected

5.2.7.8 *PSTN user calls Teams user that is logged into two different clients and Teams user responds from one of the client*

ID	43989
Priority	1
Summary	[Objective] Device should handle an inbound call forked to Teams user logged in different devices and answered at any one device. [Pre-Condition] - Login Teams user in different devices (example: Teams Client, Teams Mobile App and Web Browser)

Step	Action	Expected Result
1	PSTN user calls Teams user	Teams user starts ringing in all the devices wherever logged in
2	Teams user in any one of the device answers	Call is connected with bi-directional audio
3	PSTN user hangs up	Call is disconnected

5.2.7.9 *PSTN user calls Teams user that is forwarded to second PSTN user*

ID	47070
Priority	1
Summary	[Objective] Device is able to handle the forwarded call by Teams user to second PSTN user. [Pre-Condition] - Teams user is set call forward unconditional to PSTN number - Forward Call History and PAI on Teams tenant trunk configuration is enabled

Step	Action	Expected Result
1	PSTN user 1 calls Teams user	PSTN user 2 rings
2	PSTN user 2 picks up	Call is established with bi-directional audio between PSTN user 1 and PSTN user 2
3	PSTN user 1 hangs up	Call is disconnected

5.2.8 1:1 to Group Call Escalation

5.2.8.1 *Teams user calls another Teams user and then adds another PSTN user and participants mutes and unmute themselves*

ID	44001
Priority	1
Summary	

Step	Action	Expected Result
1	Teams user 1 calls Teams user 2	Teams user 1 and Teams user 2 are connected with bi-directional audio
2	Teams user 1 escalates the ongoing call to a group call by adding a PSTN user	PSTN user rings
3	PSTN user picks up	PSTN user joins the group call successfully
4	Teams user 1 mutes himself	Other participants can still hear each other but not Teams user 1. Teams user 1 can hear both participants
5	Teams user 1 unmutes himself	All participants can hear each other
6	Repeat steps 4 & 5 with Teams user 2	
7	Teams user 1 removes the PSTN user	PSTN user leaves group call and PSTN call is disconnected. Teams users can still hear each other

5.2.8.2 Teams user calls PSTN user and then adds another PSTN user and participants mute and unmute the PSTN users

ID	44002
Priority	1
Summary	

Step	Action	Expected Result
1	Teams user calls PSTN user 1	Call is connected with bi-directional audio
2	Teams user escalates the ongoing call to a group call by adding PSTN user 2	PSTN user 2 rings
3	PSTN user 2 picks up	PSTN user 2 joins the group call successfully and all participants can hear each other
4	Teams user mutes PSTN user1	Participants can hear each other but nobody can hear PSTN user1. PSTN user 1 can hear both participants
5	Teams user removes the PSTN user 2 from the group call	PSTN user 2 leaves group call
6	PSTN user 1 disconnects	PSTN user 1 leaves group call

5.2.8.3 PSTN user calls Teams user who escalates the call to group call by adding another PSTN user

ID	44003
Priority	1
Summary	

Step	Action	Expected Result
1	PSTN user 1 calls Teams user	Call is connected with bi-directional audio
2	Teams user escalates the ongoing call to group call by adding PSTN user 2	PSTN user 2 rings
3	PSTN user 2 picks up	PSTN user 2 joins the group call successfully
4	PSTN user 1 and 2 disconnects	PSTN user 1 and 2 leaves group call

5.2.8.4 Teams user calls PSTN user and then adds another teams user

ID	49222
Priority	1
Summary	[Objective] Teams user calls PSTN user and then adds another teams user by escalating the call to group call

Step	Action	Expected Result
1	Teams user 1 calls PSTN user	Call is connected with bi-directional audio
2	Teams user 1 escalates the call to group call by adding Teams user 2 to the call	All three users are connected
3	Teams user 1 removes Teams user 2 from the group call	Teams user 2 gets disconnected
4	Remaining users disconnect their respective calls	Users are disconnected

5.2.8.5 PSTN user calls Teams user and then adds another Teams user

ID	49380
Priority	1
Summary	[Objective] PSTN user calls Teams user and then adds another teams user by escalating the call to group call

Step	Action	Expected Result
1	PSTN user calls Teams user 1	Call is connected with bi-directional audio
2	Teams user 1 escalates the call to group call by adding Teams user 2 to the call	All three users are connected
3	Teams user 1 removes Teams user 2 from the group call	Teams user 2 gets disconnected
4	Remaining users disconnect their respective calls	Users are disconnected

5.2.9 Auto Attendant (Required for V2)

5.2.9.1 Inbound call to a Teams auto attendant transferred to a Teams user after menu option selection

ID	44006
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN to Teams auto attendant number [Pre-Condition] - Auto Attendant configured on Teams side

Step	Action	Expected Result
1	PSTN user calls Teams Auto Attendant number	Call is connected with Auto Attendant

2	PSTN user navigates the menu to select the transfer to user option and inputs the Teams user identity	Call is transferred to Teams user
3	Teams user answers the call	Teams user and PSTN user are connected with bi-directional audio
4	PSTN user hangs up	Call is disconnected

5.2.9.2 *Inbound call to Teams user transferred to a Skype for Business auto attendant number after menu option selection*

ID	44007
Priority	1
Summary	[Objective] Device is able to handle a transfer initiated by Teams to Skype for Business user's auto attendant number [Pre-Condition] - Auto attendant is configured on Skype for Business user side

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Teams user blind transfers the call to Skype for Business auto attendant number	Call is transferred successfully and PSTN user hears the auto attendant menu
3	PSTN user navigates the menu and requests for a transfer to Skype for Business user	Skype for Business user rings
4	Skype for Business user picks kup	Call is connected with bi-directional audio between PSTN user and Skype for Business user
5	PSTN user hangs up	Call is disconnected

5.2.10 Call Queues (required for V2)

5.2.10.1 *Inbound calls to a Teams call queue plays music on hold and then rings the teams call agents assigned to that queue*

ID	44008
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN user to Teams call queue number [Pre-Condition] - Call queue is configured on Teams side with a PSTN number assigned - Teams users are assigned to the Call queue as agents

Step	Action	Expected Result
1	PSTN user calls Teams Call queue	PSTN user hears MOH/greeting configured for the call queue and the teams call agents rings
2	One of agent picks up	Call is connected with bi-directional audio between the PSTN user and Teams call agent
3	PSTN user hangs up	Call is disconnected

5.3 Codec support

Device must support SILK, G711, G729 codecs

5.3.1 SILK codec support

5.3.1.1 *Teams User Calls PSTN User with SILK and other Codecs enabled at tenant and all the same codecs offered by the customer's SIP Trunk*

ID	44009
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user to PSTN user with SILK codecs present in the offer SDP. When transcoding is disabled in device, a codec which is common to PSTN side and Direct Routing interface side should be negotiated. [Pre-Condition] - SILK Codec enabled on Teams side - SILK Codec enabled on Device side - SILK codec Transcoding disabled on Device

Step	**Action**	**Expected Result**
1	Teams user calls PSTN user	The INVITE from Teams has SILK and other Codecs enabled at tenant
2	PSTN user rings	Call is connected with bi-directional audio
3	Teams user hangs up	Call is disconnected

5.3.1.2 *PSTN User calls Teams user with SILK and other Codecs offered by customer's trunk and the same codecs enabled at the tenant*

ID	44010
Priority	1
Summary	[Objective] Device should be able to accept and handle the codecs from PSTN side and towards Direct Routing interface [Pre-Condition] - Configure device to use SILK codecs and other codecs towards Direct Routing interface - Configure device to use the supported codecs on PSTN side - SILK codec Transcoding disabled on Device

Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Call is answered and established with bi-directional audio
2	Device sends INVITE to Direct Routing interface with SILK codecs included in the SDP	The SDP part contains SILK codecs along with the other supported codecs
3	PSTN user hangs up	Call is disconnected

5.3.1.3 *Device must not offer SILK and other codecs in final offer unless it supports transcoding to and from SILK codec*

ID	44011
Priority	1

Summary	[Objective] Device is able to handle an outbound call from Teams user to PSTN user with SILK codecs present in the offer SDP. When the PSTN side does not support SILK codec, Device should not offer SILK codec in its final offer response to Direct Routing interface. [Pre-Condition] - SILK Codec enabled on Teams side - SILK Codec enabled on Device side - SILK codec Transcoding disabled on Device

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Device does not offer SILK codec in its final offer	SILK codec is not negotiated
3		Codec negotiated and used is other than SILK codec between Device and Direct Routing interface
4	Teams user hangs up	Call is disconnected

5.3.2 SILK Codec Transcoding (Required to be supported by Dec 2018)

5.3.2.1 PSTN User calls Teams user when only SILK Codec is enabled on the Device trunk towards Teams but not on the Device trunk towards customer's SIP trunk

ID	49026
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN user to Teams user when only SILK codec is enabled on the trunk towards Direct Routing interface but not on the trunk towards customer's SIP Trunk [Pre-Condition] - SILK Codec enabled on Device towards Teams - SILK Codec disabled on Device towards customer SIP Trunk - Transcoding enabled on Device

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Device offers only SILK codec towards Direct Routing interface	Call is established with SILK codec between Device and Direct Routing interface
3	Device does not respond with SILK codec towards customer's SIP trunk	Call is established with any codec other than SILK between Device and customer's SIP trunk
4	PSTN user hangs up	Call is disconnected

5.3.2.2 Teams user calls PSTN user when only SILK Codec is enabled on the Device trunk towards Teams but not on the Device trunk towards customer's SIP trunk

ID	49027
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user to PSTN user when only SILK codec is enabled on the trunk towards Direct Routing interface but not on the trunk

	towards customer’s SIP Trunk [Pre-Condition] - SILK Codec enabled on Device towards Teams - SILK Codec disabled on Device towards customer SIP Trunk - Transcoding enabled on Device	
Step	**Action**	**Expected Result**
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Device does not offer SILK codec towards customer’s SIP trunk	Call is established with any codec other than SILK between Device and customer’s SIP trunk
3	Device responds with only SILK codec towards Direct Routing interface	Call is established with SILK codec between Device and Direct Routing interface
4	Teams user hangs up	Call is disconnected

5.3.3 OPUS Codec Support (Optional)

5.4 Media Requirements

5.4.1 Support for IceLite for Media Bypass

Support for ICE Lite as described in RFC 5245, is required to bypass Media Processor (MP) in the cloud. The Device must respond to connectivity checks and include only host candidates for any media stream.

Teams will perform aggressive nomination, Device should use the highest priority candidate pair for which checks are received for media flow, before end of connectivity checks.
At the end of connectivity checks, Device will receive Re-Invite with the final local and remote candidates selected by connectivity checks. Device must validate and respond to STUN binding requests and periodic keepalives (STUN binding requests).

The credentials will be sent via SIP for every session (short-term credential mechanism)

- a=ice-pwd:<password>
- a=ice-ufrag:<ufrag>

5.4.1.1 *Device can establish a direct media connection with Teams client for an outbound all to IVR*

ID	44026	
Priority	1	
Summary	[Objective] Device must be able to accept Icelite candidates and accept direct media connection with Teams client [Pre-condition] - Ensure the Teams user is behind the firewall, in the same network as the Device	
Step	**Action**	**Expected Result**
1	Teams client calls PSTN user (IVR)	Device responds with Ice candidates in the 183 SDP

2	Call is answered from IVR end	Call is connected with bi-directional audio
3		Device receives re-invite with final local and remote candidates and uses this path for bi-directional media
4	Teams client hangs up the call	Call is disconnected

5.4.1.2 *Device can establish a direct media connection with Teams client for an inbound call*

ID	44027
Priority	1
Summary	[Objective] Device must be able to accept Icelite candidates and accept direct media connection with Teams client [Pre-condition] - Ensure the Teams client is behind the firewall, in the same network as the Device

Step	Action	Expected Result
1	PSTN user calls Teams user	Device offers ICE candidates in the INVITE SDP, teams user rings and ring back is heard on PSTN side
2		Call is connected with bi-directional audio
3		Device receives re-invite with final local and remote candidates and uses this path for bi-directional media
4	PSTN user hangs up the call	Call is disconnected

5.4.1.3 *Device can establish media connection with Teams client behind a firewall in a different network (eg home) for outbound call to IVR*

ID	44030
Priority	1
Summary	[Objective] Device can establish media connection with Teams client behind a firewall in a different network (eg: home network) for outbound call [Pre-condition] - Ensure the Teams user is in a different network (eg: home network)

Step	Action	Expected Result
1	Teams user calls PSTN user (IVR)	Device responds with Ice candidates in the 183 SDP
2	Call is answered from IVR end	Call is connected with bi-directional audio
3		Device receives re-invite with final local and remote candidates and uses this path for bi-directional media
4	Teams user hangs up the call	Call is disconnected

5.4.1.4 Device can establish media connection with Teams client behind a firewall in a different network (eg home) for inbound call

ID	44031
Priority	1
Summary	[Objective] Device can establish media connection with Teams client behind a firewall in a different network (eg: home network) for inbound call [Pre-condition] - Ensure the Teams user is in a different network (eg: home network)

Step	Action	Expected Result
1	PSTN user calls Teams user	Device offers ICE candidates in the INVITE SDP, teams user rings and ring back is heard on PSTN side
2		Call is connected with bi-directional audio
3		Device receives re-invite with final local and remote candidates and uses this path for bi-directional media
4	PSTN user hangs up the call	Call is disconnected

5.4.1.5 Device can establish media connection with Teams client behind a firewall in a different network via relay server for outbound call to IVR

ID	49008
Priority	1
Summary	[Objective] Device can establish media connection with Teams client behind a firewall in a different network (eg: home network) for outbound call [Pre-condition] - Ensure the Teams user is in a different network (eg: home network) and block the reflexive IP of the Teams client from being able to access the Device IP

Step	Action	Expected Result
1	Teams user calls PSTN user (sends relay candidates with higher priority)	Device responds with Ice candidates in the 183 SDP
2		Teams user can hear early media from the IVR which is established via the relay server
3	Call is answered from IVR end	Call is connected with bi-directional audio
4		Device receives re-invite with final local and remote candidates and uses this path for bi-directional media
5	Teams client hangs up the call	Call is disconnected

5.4.1.6 Device can establish media connection with Teams client behind a firewall in a different network via relay server for inbound call

ID	49009
Priority	1

Summary	[Objective] Device can establish media connection with Teams client behind a firewall in a different network (eg: home network) for inbound call [Pre-condition] - Ensure the Teams user is in a different network (eg: home network) and block the reflexive IP of the Teams client from being able to access the Device IP

Step	Action	Expected Result
1	PSTN user calls Teams user	Device offers ICE candidates in the INVITE SDP, teams user rings and ring back is heard on PSTN side
2		Call is connected with bi-directional audio
3		Device receives re-invite with final local and remote candidates and uses this path for bi-directional media via the relay server
4	PSTN user hangs up the call	Call is disconnected

5.4.1.7 Device can route calls from Teams user in Tenant-A to Teams user in Tenant-B

ID	49671
Priority	1
Summary	[Objective] Device can route the calls from a Teams user in Tenant-A to Teams user in Tenant-B when the Teams user is called using DID. [Pre-Condition] - Device is paired with Tenant-A and Tenant-B - Device is configured with internal call routing for calls between two tenants using DID

Step	Action	Expected Result
1	Teams user (Tenant-A) calls Teams user (Tenant-B)	Call is connected with bi-directional audio
2		Call is routed Via the SBC without going to the PSTN.
3	Teams user (Tenant-A) hangs up	Call is disconnected

5.4.2 SRTP

The Device must support SRTP encryption cipher AES_CM_128_HMAC_SHA1_80 for offer and answer. Only non-MKI mode must be used. Example of crypto attribute in SDP offer from the Device:

a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:V/Lr6Lsvhad/crSB9kCQ28jrYDxR2Yfk5bXryH5V|2^31

When the Device is configured with SRTP as the Media Security mode and SDES as the Media Security method, the SDP of offer/answer from device should be like below:

m=audio 52884 RTP/SAVP 111 103 104 9 0 8 106 13 110 112 113 126
a=crypto:0 AES_CM_128_HMAC_SHA1_32 inline:Hr4D2cgUu9+Uza5Igz/JkVx59DAxDbaxJg862ibQ|2^31
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:JPEaIxHegfuv53ykBPZk8hV0GO8kTiiqRMfHimEE|2^31

```
a=rtcp:52884
a=rtcp-mux
```

Device may also be configured to support SDES with DTLS-SRTP optional as below:

```
m=audio 54056 RTP/SAVP 0 8 76 77 18 9 101 13
a=rtcp:54056
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:krXco0QRglwErMqtbMs2zSw29tBdmdgXpEYZhQmp|2^31
a=fingerprint:sha-256
AE:24:07:15:5C:B7:45:1A:E4:45:60:C1:1E:68:0E:CC:8D:A6:78:3B:76:65:BB:B0:77:88:07:F8:98:18:62:34
a=setup:actpass
a=rtcp-mux
```

Note: In this section media bypass is disabled on Teams side.

5.4.2.1 Device sends crypto attributes in SDP for call from PSTN user to Teams user

ID	43905
Priority	1
Summary	[Objective] Device is able to send crypto attributes in SDP for a TLS-SRTP call [Pre-Condition] - SRTP enabled on Device - SRTP enabled on Teams side - Media Bypass OFF on Teams side

Step	Action	Expected Result
1	PSTN user calls Teams user	Device sends crypto attributes in the INVITE's SDP sent to Direct Routing interface
2	Teams user picks up	Call is established with bi-directional audio
3	PSTN user hangs up	Call is disconnected

5.4.2.2 Device sends crypto attributes in SDP for call from Teams user to PSTN user

ID	43906
Priority	1
Summary	[Objective] Device is able to send crypto attributes in SDP for a TLS-SRTP call [Pre-Condition] - SRTP enabled on Device - SRTP enabled on Teams side - Media Bypass OFF on Teams side

Step	Action	Expected Result
1	Teams user calls PSTN user	Device sends crypto attributes in the response message (18x, 200) SDP sent to Direct Routing interface
2	PSTN user picks up	Call is established with bi-directional audio
3	Teams user hangs up	Call is disconnected

5.4.2.3 Teams users make outgoing calls via web browser (Microsoft Edge)

ID	47915
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user logged in using web browser to PSTN user [Pre-Condition] - Teams user logged in using web browser (Microsoft Edge)

Step	Action	Expected Result
1	Teams user from web browser calls PSTN user	Call is connected with bi-directional audio
2	Teams user hangs up	Call is disconnected

5.4.2.4 Teams users receives inbound calls via web browser (Microsoft Edge)

ID	47916
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN user to a Teams user logged in via web browser [Pre-Condition] - Teams user logged in using web browser (Microsoft Edge)

Step	Action	Expected Result
1	PSTN user calls Teams user logged in using web browser	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

5.4.2.5 Teams users make outgoing calls via web browser (Mozilla Firefox)

ID	47917
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user logged in using web browser to PSTN user [Pre-Condition] - Teams user logged in using web browser (Mozilla Firefox)

Step	Action	Expected Result
1	Teams user from web browser calls PSTN user	Call is connected with bi-directional audio
2	Teams user hangs up	Call is disconnected

5.4.2.6 Teams users receives inbound calls via web browser (Mozilla Firefox)

ID	47918
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN user to a Teams user logged in via web browser

	[Pre-Condition] - Teams user logged in using web browser (Mozilla Firefox)

Step	Action	Expected Result
1	PSTN user calls Teams user logged in using web browser	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

5.4.2.7 Teams users make outgoing calls via web browser (Chrome)

ID	47919
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user logged in using web browser to PSTN user [Pre-Condition] - Teams user logged in using web browser (Chrome)

Step	Action	Expected Result
1	PSTN user calls Teams user logged in using web browser	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

5.4.2.8 Teams users receives inbound calls via web browser (Chrome)

ID	47920
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN user to a Teams user logged in via web browser [Pre-Condition] - Teams user logged in using web browser (Chrome)

Step	Action	Expected Result
1	PSTN user calls Teams user logged in using web browser	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

5.4.2.9 Device does not change the SSRC of an established inbound secure RTP session

ID	49010
Priority	1
Summary	[Objective] During an inbound call, the SSRC field in the secure RTP packets is not changed. The SSRC value remains unchanged from the time the secure RTP session was established to the end of the session.

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Check the SSRC field in the secure RTP packets from Device	SSRC value is non-zero
3	Leave the call connected for 120 seconds	SSRC value remains same as what was sent in the first secure RTP packet
4	PSTN user hangs up	Call is disconnected

5.4.2.10 Device does not change the SSRC of an established inbound secure RTCP session

ID	49011
Priority	1
Summary	[Objective] During an inbound call, the SSRC field in the secure RTCP packets is not changed. The SSRC value remains unchanged from the time the secure RTCP packets being sent by Device till the end of the session.

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Check the SSRC field in the secure RTCP packets from Device	SSRC value is non-zero
3	Leave the call connected for 120 seconds	SSRC value remains same as what was sent in the first secure RTCP packet
4	PSTN user hangs up	Call is disconnected

5.4.2.11 Device does not change the SSRC of an established outbound secure RTP session

ID	49012
Priority	1
Summary	[Objective] During an outbound call, the SSRC field in the secure RTP packets is not changed. The SSRC value remains unchanged from the time the secure RTP session was established to the end of the session.

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Check the SSRC field in the secure RTP packets from Device	SSRC value is non-zero
3	Leave the call connected for 120 seconds	SSRC value remains same as what was sent in the first secure RTP packet
4	Teams user hangs up	Call is disconnected

5.4.2.12 Device does not change the SSRC of an established outbound secure RTCP session

ID	49013
Priority	1
Summary	[Objective] During an outbound call, the SSRC field in the secure RTCP packets is not changed. The SSRC value remains unchanged from the time the secure RTCP packets being sent by Device till the end of the session.

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Check the SSRC field in the secure RTCP packets from Device	SSRC value is non-zero
3	Leave the call connected for 120 seconds	SSRC value remains same as what was sent in the first secure RTCP packet
4	Teams user hangs up	Call is disconnected

5.4.3 DTLS-SRTP

Refer 7.0 Appendix 2 Media Encryption Offer / Answer Requirement for SBC in BYPASS mode for the formats of SDP required

5.4.3.1 Teams users make outgoing calls via web browser (Microsoft Edge)

ID	45952
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user logged in using web browser to PSTN user [Pre-Condition] - Teams user logged in using web browser (Microsoft Edge)

Step	**Action**	**Expected Result**
1	Teams user from web browser calls PSTN user	Call is connected with bi-directional audio
2	Teams user hangs up	Call is disconnected

5.4.3.2 Teams users receives inbound calls via web browser (Microsoft Edge)

ID	45953
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN user to a Teams user logged in via web browser [Pre-Condition] - Teams user logged in using web browser (Microsoft Edge)

Step	**Action**	**Expected Result**
1	PSTN user calls Teams user logged in using web browser	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

5.4.3.3 Teams users make outgoing calls via web browser (Mozilla Firefox)

ID	47280
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user logged in using web browser to PSTN user [Pre-Condition] - Teams user logged in using web browser (Mozilla Firefox)

Step	**Action**	**Expected Result**
1	Teams user from web browser calls PSTN user	Call is connected with bi-directional audio
2	Teams user hangs up	Call is disconnected

5.4.3.4 Teams users receives inbound calls via web browser (Mozilla Firefox)

ID	47281
Priority	1

Summary	[Objective] Device is able to handle an inbound call from PSTN user to a Teams user logged in via web browser [Pre-Condition] - Teams user logged in using web browser (Mozilla Firefox)

Step	Action	Expected Result
1	PSTN user calls Teams user logged in using web browser	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

5.4.3.5 *Teams users make outgoing calls via web browser (Chrome)*

ID	47282
Priority	1
Summary	[Objective] Device is able to handle an outbound call from Teams user logged in using web browser to PSTN user [Pre-Condition] - Teams user logged in using web browser (Chrome)

Step	Action	Expected Result
1	PSTN user calls Teams user logged in using web browser	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

5.4.3.6 *Teams users receives inbound calls via web browser (Chrome)*

ID	47283
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN user to a Teams user logged in via web browser [Pre-Condition] - Teams user logged in using web browser (Chrome)

Step	Action	Expected Result
1	PSTN user calls Teams user logged in using web browser	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

5.4.3.7 *Teams user receives inbound calls via Teams client installed in windows operating system (desktop)*

ID	47921
Priority	1
Summary	[Objective] Device is able to handle an inbound call from PSTN user to a Teams user logged in using Teams client installed in windows operating system (desktop) [Pre-Condition] - Teams user logged in using Teams client installed in windows operating system (desktop)

Step	Action	Expected Result

1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

5.4.3.8 Teams user make outgoing calls via Teams client installed in windows operating system (desktop)

ID	47922	
Priority	1	
Summary	[Objective] Device is able to handle an outbound call from Teams user logged in using Teams client installed in windows operating system (desktop) to PSTN user [Pre-Condition] - Teams user logged in using Teams client installed in windows operating system (desktop)	
Step	**Action**	**Expected Result**
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Teams user hangs up	Call is disconnected

5.4.3.9 Teams user receives inbound calls via Teams client installed in mac operating system

ID	47923	
Priority	1	
Summary	[Objective] Device is able to handle an inbound call from PSTN user to a Teams user logged in using Teams client installed in mac operating system (desktop) [Pre-Condition] - Teams user logged in using Teams client installed in mac operating system (desktop)	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	PSTN user hangs up	Call is disconnected

5.4.3.10 Teams user make outgoing calls via Teams client installed in mac operating system

ID	47924	
Priority	1	
Summary	[Objective] Device is able to handle an outbound call from Teams user logged in using Teams client installed in mac operating system (desktop) to PSTN user [Pre-Condition] - Teams user logged in using Teams client installed in mac operating system (desktop)	
Step	**Action**	**Expected Result**
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Teams user hangs up	Call is disconnected

5.4.4 DTMF support

5.4.4.1 Device offers DTMF payload type in the range of 96-127 to Direct Routing interface

ID	43907
Priority	1
Summary	[Objective] Device must offer DTMF payload type in the range of 96-127 and must indicate support for telephony events. [Pre-condition] - Set the DTMF transport type on the Device to support RFC 2833.

Step	Action	Expected Result
1	PSTN user calls Teams user	Direct Routing interface receives INVITE from Device
2		The INVITE's SDP contains the DTMF payload type in the range of 96-127
3		Events parameter associated with the telephone-event media type is included and indicates support for events 0-15 or 0-16
4		Call is established with bi-directional audio
5	Teams user hangs up	Call is disconnected

5.4.4.2 Teams user calls an IVR number and navigates through the IVR menu after call connection

ID	43908
Priority	1
Summary	[Objective] Teams user is able to navigate through the Interactive Voice Response Menu and Device is able to process the DTMF digits received from Direct Routing interface. The digits are sent to Device after 200 OK is received and RTP stream established.

Step	Action	Expected Result
1	Teams user calls an IVR number	IVR menu is played after 200 OK is received from Device
2	Navigate through the IVR menu (ANY LEVEL of the IVRMENU)	Call is not dropped and digits are recognized by the remote system
3	Teams user hangs up	Call is disconnected

5.4.4.3 Teams user calls an IVR number and navigates through the IVR menu before call connection

ID	43909
Priority	1
Summary	[Objective] Teams user is able to navigate the Interactive Voice Response Menu and Device processes the DTMF digits received from Direct Routing interface.

Step	Action	Expected Result
1	Teams user calls IVR number	IVR menu is played before 200 OK is received from Device
2	Navigate through the IVR menu (ANY LEVEL of the IVRMENU)	Call is not dropped and digits entered by the Teams user are recognized by the remote system
3	Teams user hangs up	Call is disconnected

5.4.4.4 Teams user calls into an external conference bridge and pastes a string of conference ID into Teams which is recognized by Device and IVR

ID	43910
Priority	1
Summary	[Objective] This Test case aims to verify Rapid DTMF Digit Handling by the Device when user pastes a string of digits such as a Conference ID into Teams Client.

Step	Action	Expected Result
1	Teams user calls IVR number for joining a conference by ID (external conference such as Webex)	Call is connected, 200 OK is received from Device
2	Join the conference by pasting a conference ID from the client	Call is not dropped and digits pasted by the Teams Client are recognized by the Device and IVR
3	Teams user hangs up	Call is disconnected

5.4.5 Comfort Noise Passthrough and Generation

5.4.5.1 Device offers comfort noise payload in the INVITE's SDP to Direct Routing interface even when not offered by the carrier

ID	43911
Priority	1
Summary	[Objective] Device should offer/negotiate comfort noise payload in the SDP to Direct Routing interface even when the carrier does not offer them. [Pre-condition] - Comfort Noise enabled on Device.

Step	Action	Expected Result
1	PSTN user calls Teams user	Device sends INVITE to Direct Routing interface. The SDP contains the Comfort Noise payload type 13.
2	Teams user answers the call	Call is established with bi-directional audio
3	PSTN user hangs up	Call is disconnected

5.4.5.2 Device sends comfort noise packets to Direct Routing interface when PSTN user mutes an outbound call

ID	43912
Priority	1
Summary	[Objective] After Comfort Noise negotiation, Device sends Comfort Noise packets when PSTN user mutes the call. [Pre-condition] - Comfort Noise enabled on Device

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio

2	Mute the call on the PSTN user for 3 minutes	Verify Comfort Noise packets are sent from the Device to Direct Routing interface
3		Unidirectional audio from Teams user to the PSTN user
4		Call stays connected on mute for 3 minutes
5	Teams user hangs up	Call is disconnected

5.4.5.3 Device sends comfort noise packets to Direct Routing interface when PSTN user mutes an inbound call

ID	43913
Priority	1
Summary	[Objective] After Comfort Noise negotiation, Device sends Comfort Noise packets when PSTN user mutes the call. [Pre-condition] - Comfort Noise enabled on Device

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Mute the call on the PSTN user for 3 minutes	Verify that Comfort Noise packets are sent from the Device to Direct Routing interface
3		Unidirectional audio from Teams user to the PSTN user
4		Call stays connected on mute for 3 minutes
5	PSTN user hangs up	Call is disconnected

5.4.5.4 Teams user mutes an Inbound call from PSTN and then unmutes

ID	43936
Priority	1
Summary	[Objective] Device is able to handle an inbound call muted on Teams user and is able to keep the call connected on receiving comfort noise packets during the mute [Pre-Condition] - Comfort Noise enabled on Device

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Teams user mutes the call for 3 minutes	Media capture indicates Comfort Noise packets are received by Device from Direct Routing interface
3		Unidirectional audio is present from PSTN user to Teams user
4		Call stays connected on mute for 3 minutes
5	PSTN user hangs up	Call is disconnected

5.4.5.5 Teams user mutes an Outbound call to PSTN and then unmutes

ID	43937
Priority	1

Summary	[Objective] Device is able to handle an outbound call muted on Teams user and is able to keep the call connected on receiving comfort noise packets during the mute [Pre-Condition] - Comfort Noise enabled on Device

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Teams user mutes the call for 3 minutes	Media capture indicates Comfort Noise packets are received by Device from Direct Routing interface
3		Unidirectional audio is present from PSTN user to Teams user
4		Call stays connected on mute for 3 minutes
5	Teams user hangs up	Call is disconnected

5.4.5.6 Teams user mutes outbound call to PSTN for over 30 minutes and then unmutes

ID	43938
Priority	1
Summary	[Objective] Device is able to handle an outbound call muted by Teams user and is able to keep the call connected for 30 minutes on receiving comfort noise packets during the mute [Pre-Condition] - Comfort Noise enabled on Device

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Teams user mutes the call for 30 minutes	Media capture indicates Comfort Noise packets are received by Device from Direct Routing interface
3		Unidirectional audio is present from PSTN user to Teams user
4		Call stays connected on mute for 30 minutes
5	Teams user unmutes the call	Bi-directional audio is present
6	Teams user hangs up	Call is disconnected

5.4.5.7 Teams user mutes inbound call from PSTN for over 30 minutes and then unmutes

ID	43939
Priority	1
Summary	[Objective] Device is able to handle an inbound call muted by Teams user and is able to keep the call connected for 30 minutes on receiving comfort noise packets during the mute [Pre-Condition] - Comfort Noise enabled on Device

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Teams user mutes the call for 30 minutes	Media capture indicates Comfort Noise packets are received by Device from Direct Routing interface

3		Unidirectional audio is present from PSTN user to Teams user
4		Call stays connected on mute for 30 minutes
5	Teams user unmutes the call	Bi-directional audio is present
6	PSTN user hangs up	Call is disconnected

5.4.5.8 PSTN user mutes outbound call to PSTN for over 30 minutes and then unmutes

ID	47927
Priority	1
Summary	[Objective] Device can handle an outbound call muted on PSTN side and is able to keep the call connected for 30 minutes on sending comfort noise packets during the mute [Pre-Condition] - Comfort Noise enabled on Device

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	PSTN user mutes the call for 30 minutes	Media capture indicates Comfort Noise packets are sent by device
3		Unidirectional audio is present from Teams user to PSTN user
4		Call stays connected on mute for 30 minutes
5	Unmute the call	Two-way audio is present
6	Teams user hangs up	Call is disconnected

5.4.5.9 PSTN user mutes inbound call to Teams user for over 30 minutes and then unmutes

ID	47928
Priority	1
Summary	[Objective] Device can handle an inbound call muted on PSTN side and is able to keep the call connected for 30 minutes on sending comfort noise packets during the mute [Pre-Condition] - Comfort Noise enabled on Device

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	PSTN user mutes the call for 30 minutes	Media capture indicates Comfort Noise packets are sent by device
3		Unidirectional audio is present from Teams user to PSTN user
4		Call stays connected on mute for 30 minutes
5	Unmute the call	Two-way audio is present
6	PSTN user hangs up	Call is disconnected

5.4.6 SRTCP

5.4.6.1 SRTCP Pass-through and Generation

5.4.6.1.1 Device must provide SRTCP received from the far end for a transcoded inbound call when service provider or gateway sends SRTCP

ID	44016
Priority	1
Summary	[Objective] Device is able to passthrough SRTCP packets offered by service provider or the PSTN gateway to Direct Routing interface [Pre-Condition] - SRTCP passthrough enabled on Device - Transcoding enabled on Device

Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Call is connected
2	Device involves in transcoding	Two-way audio is present
3	Device passthrough the SRTCP packets received from Service provider or the PSTN gateway to Direct Routing interface	Direct Routing interface receives SRTCP packets during the call
4	PSTN user hangs up	Call is disconnected

5.4.6.1.2 Device must provide SRTCP received from the far end for a transcoded outbound call when service provider or gateway sends SRTCP

ID	44017
Priority	1
Summary	[Objective] Device is able to passthrough SRTCP packets offered by service provider or the PSTN gateway to Teams [Pre-Condition] - SRTCP passthrough enabled on Device - Transcoding enabled on Device

Step	**Action**	**Expected Result**
1	Teams user calls PSTN user	Call is connected
2	Device involves in transcoding	Two-way audio is present
3	Device passthrough the SRTCP packets received from Service provider or the PSTN gateway to Direct Routing interface	Direct Routing interface receives SRTCP packets during the call
4	Teams user hangs up	Call is disconnected

5.4.6.1.3 Device must provide SRTCP received from the far end for an inbound call that doesn’t involve transcoding when service provider or gateway sends SRTCP

ID	44018
Priority	1
Summary	[Objective] Device is able to passthrough SRTCP packets offered by service provider or the PSTN gateway to Direct Routing interface

	[Pre-Condition] - SRTCP passthrough enabled on Device - Transcoding disabled on Device

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Device passthrough the SRTCP packets received from Service provider or the PSTN gateway to Direct Routing interface	Direct Routing interface receives SRTCP packets during the call
3	PSTN user hangs up	Call is disconnected

5.4.6.1.4 Device must provide SRTCP received from the far end for an outbound call that doesn't involve transcoding when service provider or gateway sends SRTCP

ID	44019
Priority	1
Summary	[Objective] Device is able to passthrough SRTCP packets offered by service provider or the PSTN gateway to Direct Routing interface [Pre-Condition] - SRTCP passthrough enabled on Device - Transcoding disabled on Device

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Device passthrough the SRTCP packets received from Service provider or the PSTN gateway to Direct Routing interface	Direct Routing interface receives SRTCP packets during the call
3	Teams user hangs up	Call is disconnected

5.4.6.1.5 Device must provide SRTCP for a transcoded inbound call when service provider or gateway does not send SRTCP

ID	44020
Priority	1
Summary	[Objective] Device is able to generate SRTCP packets towards Direct Routing interface when the service provider or PSTN gateway does not provide SRTCP [Pre-Condition] - SRTCP enabled on Device - Transcoding enabled on Device

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected
2	Device involves in transcoding	Two-way audio is present
3	Device generates SRTCP packets towards Direct Routing interface when Service provider or PSTN gateway does not provide SRTCP	Direct Routing interface receives SRTCP packets during the call
4	PSTN user hangs up	Call is disconnected

5.4.6.1.6 Device must provide SRTCP for a transcoded outbound call when service provider or gateway does not send SRTCP

ID	44021
Priority	1
Summary	[Objective] Device is able to generate SRTCP packets towards Direct Routing interface when the service provider or PSTN gateway does not provide SRTCP [Pre-Condition] - SRTCP enabled on Device - Transcoding enabled on Device

Step	Action	Expected Result
1	Teams user calls PSTN user	Call is connected
2	Device involves in transcoding	Two was audio is present
3	Device generates SRTCP packets towards Direct Routing interface when Service provider or PSTN gateway does not provide SRTCP	Direct Routing interface receives SRTCP packets during the call
4	Teams user hangs up	Call is disconnected

5.4.6.1.7 Device must provide SRTCP for an inbound call that doesn’t involve transcoding when service provider or gateway does not send SRTCP

ID	44022
Priority	1
Summary	[Objective] Device is able to generate SRTCP packets towards Direct Routing interface when the service provider or PSTN gateway does not provide SRTCP [Pre-Condition] - SRTCP enabled on Device - Transcoding disabled on Device

Step	Action	Expected Result
1	PSTN user calls Teams user	Call is connected with bi-directional audio
2	Device generates SRTCP packets towards Direct Routing interface when Service provider or PSTN gateway does not provide SRTCP	Direct Routing interface receives SRTCP packets during the call
3	PSTN user hangs up	Call is disconnected

5.4.6.1.8 Device must provide SRTCP for an outbound call that doesn’t involve transcoding when service provider or gateway does not send SRTCP

ID	44023
Priority	1
Summary	[Objective] Device is able to generate SRTCP packets towards Direct Routing interface when the service provider or PSTN gateway does not provide SRTCP [Pre-Condition] - SRTCP enabled on Device - Transcoding disabled on Device

Step	Action	Expected Result

1	Teams user calls PSTN user	Call is connected with bi-directional audio
2	Device generates SRTCP packets towards Direct Routing interface when Service provider or PSTN gateway does not provide SRTCP	Direct Routing interface receives SRTCP packets during the call
3	Teams user hangs up	Call is disconnected

5.4.6.2 SRTCP Multiplexing (RFC 8035)

5.4.6.2.1 Device must indicate support for RTCP multiplexing by including the a=rtcp-mux attribute in the offer

ID	44024	
Priority	1	
Summary	[Objective] Device must indicate support for SRTCP multiplexing by including the a=rtcp-mux attribute in the offer SDP for an inbound call to Direct Routing interface [Pre-Condition] - SRTCP multiplexing enabled on Device	
Step	**Action**	**Expected Result**
1	PSTN user calls Teams user	Device sends a=rtcp-mux attribute in the offer SDP indicating support for SRTCP multiplexing
2	Device receives response from Direct Routing interface with a=rtcp-mux attribute	Call is connected with bi-directional audio
3	Device accepts SRTCP packets sent by Direct Routing interface	SRTCP packets are received on the SRTP port itself
4	PSTN user hangs up	Call is disconnected

5.4.6.2.2 Device must respond with a=rtcp-mux attribute in the SDP response if the offer contains the same attribute

ID	44025	
Priority	1	
Summary	[Objective] Device must indicate support for SRTCP multiplexing by including the a=rtcp-mux attribute in the answer SDP for an outbound call from Direct Routing interface [Pre-Condition] - SRTCP multiplexing enabled on Device	
Step	**Action**	**Expected Result**
1	Teams user calls PSTN user	Device receives a=rtcp-mux attribute in the offer SDP
2	Device sends a=rtcp-mux attribute in the answer SDP indicating support for SRTCP multiplexing	Call is connected with bi-directional audio
3	Device sends SRTCP packets to Direct Routing interface	SRTCP packets are sent on the SRTP port itself
4	Teams user hangs up	Call is disconnected

5.5 Security Requirements

5.5.1 TLS v1.2

5.5.1.1 Device must support TLS v1.2

ID	44033
Priority	2
Summary	[Objective] Device must support TLS version 1.2 or higher. [Pre-Condition] - Configure TLS version 1.2 on the Device and disable TLS 1.0, TLS 1.1 support

Step	Action	Expected Result
1	Device involves in TLS Handshake messages with Direct Routing interface	TLS version is mentioned by the Device
2	PSTN user calls Teams user	Call is connected with bi-directional audio
3	PSTN user hangs up	Call is disconnected

5.6 Support for OPTIONS and Failover

SBC must send OPTIONS to all three proxy FQDNs.

The connection point for Direct Connect are three FQDNs:

- **sip.pstnhub.microsoft.com** – Global FQDN, must be tried first. When SBC sends request to resolve this name, the Microsoft Azure DNS servers returns an IP address pointing to the primary Azure datacenter assigned to the SBC. The assignment is based on performance metrics of the datacenters and geographical proximity to the SBC. The IP address returned corresponds to the primary FQDN
- **sip2.pstnhub.microsoft.com** – Secondary FQDN, geographically maps to the second priority region;
- **sip3.pstnhub.microsoft.com** – Tertiary FQDN, geographically maps to the third priority region

Placing these three FQDNs in order above required to:

- Provide the failover when connection from an SBC is established to a datacenter which is experiencing a temporary issue. See About FDN of SIP Proxy and Failover mechanism for more details

Failover Mechanism:

The SBC makes DNS query to resolve sip.pstnhub.microsoft.com. Based on geographical proximity and the datacenters performance metrics the primary datacenter is selected. If during the connection the primary datacenter experiences an issue, the SBC will try the sip2.pstnhub.microsoft.com which resolves to the second assigned datacenter, and in rare case if datacenters in two regions are not available the SBC retries the last FQDN (sip3.pstnhub.microsoft.com) which provides the tertiary datacenter IP.

The table below summarizes the relationships between primary, secondary and tertiary datacenters:

If SBC is located in	**EMEA**	**NOAM**	**ASIA**
The secondary datacenter (sip2.pstnhub.microsoft.com)	US	EU	US

The tertiary datacenter (sip3.pstnhub.microsoft.com)	ASIA	ASIA	EU

SBC must send OPTIONS to all three datacenters.

The connection point for Direct Connect are three FQDNs:

- **sip.pstnhub.microsoft.com** – Global FQDN, must be tried first. When SBC sends request to resolve this name, the Microsoft Azure DNS servers returns an IP address pointing to the primary Azure datacenter assigned to the SBC. The assignment is based on performance metrics of the datacenters and geographical proximity to the SBC. The IP address returned corresponds to the primary FQDN
- **sip2.pstnhub.microsoft.com** – Secondary FQDN, geographically maps to the second priority region;
- **sip3.pstnhub.microsoft.com** – Tertiary FQDN, geographically maps to the third priority region

Placing these three FQDNs in order above required to:

- Provide the failover when connection from an SBC is established to a datacenter which is experiencing a temporary issue. See About FDN of SIP Proxy and Failover mechanism for more details

Failover Mechanism:

The SBC makes DNS query to resolve sip.pstnhub.microsoft.com. Based on geographical proximity and the datacenters performance metrics the primary datacenter is selected. If during the connection the primary datacenter experiences an issue, the SBC will try the sip2.pstnhub.microsoft.com which resolves to the second assigned datacenter, and in rare case if datacenters in two regions are not available the SBC retries the last FQDN (sip3.pstnhub.microsoft.com) which provides the tertiary datacenter IP.

The table below summarizes the relationships between primary, secondary and tertiary datacenters:

If SBC is located in	**EMEA**	**NOAM**	**ASIA**
The secondary datacenter (sip2.pstnhub.microsoft.com)	US	EU	US
The tertiary datacenter (sip3.pstnhub.microsoft.com)	ASIA	ASIA	EU

When the SBC receives a 503 with a Retry-After header in response to an INVITE the SBC must terminate that connection, perform a new DNS request and retry the PSTN hub

5.6.1 Device responds to OPTIONS messages sent by the Direct Routing interface

ID	33882
Priority	1
Summary	[Objective] Device responds to SIP OPTIONS message sent by Direct Routing interface

Step	**Action**	**Expected Result**

1	Direct Routing interface sends OPTIONS message after Device has sent OPTIONS	Device responds to the OPTIONS with 200 OK indicating that Device's SIP signaling is up
2	Check this over a period of 7 minutes	Device responds to each of the OPTIONS messages received

5.6.2 Device sends SIP OPTIONS message to all three datacenters

ID	33883
Priority	1
Summary	[Objective] Device sends periodic OPTIONS message to all datacenters – primary, secondary and tertiary datacenter. But does not load balance calls. [Pre-Condition] - Device is configured to send SIP OPTIONS every 60 seconds to all three datacenter FQDNs

Step	Action	Expected Result
1	Device sends SIP OPTIONS to ping all three datacenters every 60 seconds	Device receives OPTIONS response from Direct Routing interface and marks the SIP Peer is up
2		Verify if the FROM and CONTACT header in the OPTIONS message sent by Device has its own FQDN

5.6.3 Device tries the secondary datacenter when there is no response from the primary datacenter (cannot establish TLS/TCP connection)

ID	47815
Priority	1
Summary	[Objective] Device when not able to establish TLS/TCP connection with primary datacenter, will try the secondary datacenter, due to ACL blocking outbound connection to the primary datacenter address [Pre-Condition] - Device is configured to failover between three datacenters.

Step	Action	Expected Result
1	PSTN user calls Teams user	Device tries primary datacenter and fails to establish TLS/TCP connection
2	Device failover the call to secondary datacenter	Device can establish TLS/TCP connection successfully
3	Teams user answers the call	Call is established with two-way audio
4	PSTN user hangs up	Call is disconnected

5.6.4 Device tries the secondary datacenter when there is no response from the primary datacenter (no response to invite)

ID	47817
Priority	1
Summary	[Objective] Device sends INVITE and tries the secondary datacenter when there is no response for the INVITE from the primary datacenter [Pre-Condition] - Device is configured to failover between three datacenters.

Step	Action	Expected Result
1	PSTN user calls Teams user	Device sends INVITE to primary datacenter
2	Device tries secondary datacenter when there is no response for the INVITE	Device sends INVITE to secondary datacenter
3	Teams user answers the call	Call is established with two-way audio
4	PSTN user hangs up	Call is disconnected

5.6.5 Device honors the retry-after timer in the 503 message received for the INVITE

ID	49024
Priority	1
Summary	[Objective] Device honors the retry-after timer in the 503 message received for the INVITE if present. Device clears the connection on receiving 503 and failover the call to secondary server. Device retries the same FQDN after the retry-after timer value is expired.

Step	Action	Expected Result
1	PSTN user calls Teams user	Device sends the INVITE to primary datacenter FQDN (sip.pstnhub.microsoft.com)
2	Direct Routing interface returns 503 Service Unavailable with retry-after header	Device clears the connection upon receiving 503 and failover the call to secondary server. Device re-resolves the FQDN and initiates a new connection with the same FQDN after the timer value present in retry-after header expires.

6.0 Appendix 1. Direct Routing SIP Protocol description

6.1 Introduction

This portion of the document covers specific requirements to SIP Headers, size of SDP considerations and requirements to the domain names in Office 365 tenant.

The SIP Hub component of Microsoft Direct Routing uses SIP protocol, based on RFC 3261. The SIP Hub mandates using some SIP parameters, described in the RFC 3261. The document covers mandatory parameters when configuring connection between SBCs and Microsoft Direct Routing. The document also has detailed examples of flow where the described parameters used.

The audience for the document is SBC vendors or SBC administrators who configure the connection between the SBC and the SIP Hub service.

6.2 Terminology

Recommended – not required, but simplifies the troubleshooting if configured as in following examples

Must – strict requirement, the system does not work as expected without the configuration of the parameters as described in this document

SIP Hub – internet facing component of Microsoft Phone System Hybrid Connect component to interop with the SBC

6.3 Specific requirements for SIP Protocol

The t SIP Hub has specific requirements for the following SIP protocol elements:

- Request-URI;
- Headers: Contact and Record-Route

6.4 Processing the incoming request

Example of the SIP Invite message:

Parameter name	**Example of the value**
Request-URI	INVITE sip:+18338006777@sip.pstnhub.microsoft.com SIP /2.0
Via Header	Via: SIP/2.0/TLS sbc1.adatum.biz:5058;alias;branch=z9hG4bKac2121518978
Max-Forwards header	Max-Forwards:68
From Header	From: sip:+17168712781@sbc1.adatum.biz;transport=udp;tag=1c747237679
To Header	To: sip:+183338006777@sip.pstnhub.microsoft.com
CSeq header	CSeq: 1 INVITE
Contact Header	Contact: <sip: +17168712781@sbc1.adatum.biz;transport=tls>

During the connection the Microsoft SIP Hub uses two fields Request-URI and Contact header to:

- Check that the FQDN part of the Contact header matches the Common Name or Subject Alternative name of the presented certificate;
- Validate the FQDN part of the Contact header with list of paired in Office 365 SBCs FQDNs;

- Perform the lookup of the user number in the Request-URI within a specific tenant and convert it to the SIP URI of the user;
- Find and apply specific parameters for this SBC as configured by the administrator during the call (for example if P-Asserted-Identity field should be send)

It is not supported to have a 3rd party SIP Proxy or User Agent Server between the Microsoft SIP Hub and the paired SBC, which might modify the Request URI, created by the paired SBC

6.5 Detailed requirements for Contact Header and Request-URI

6.5.1 Contact header

For all incoming calls to Microsoft SIP Hub, the Contact Header MUST have the paired SBC FQDN in URI hostname:

*Syntax: Contact: <sip:phone or sip address@**FQDN of the SBC;transport=tls>***

This name also MUST be in Common Name or Subject Alternative name field (s) of the presented certificate.

It is allowed using wildcard values of the name (s) in the Common Name or Subject Alternative Name fields. The support of wildcard according to the https://tools.ietf.org/html/rfc2818#section-3.1), specifically

*"Names may contain the wildcard character * which is considered to match any single domain name component or component fragment. E.g., *.a.com matches foo.a.com but not bar.foo.a.com. f*.com matches foo.com but not bar.com.".*

If more than one value in the Contact header presented, only the FQDN portion of the first value of the Contact header used.

6.5.2 Request-URI

For all incoming calls, the Request-URI used to match the phone number to a user.

The phone number MUST contain "+" sign.

Correct value:

- INVITE sip:+18338006777@sip.pstnhub.microsoft.com SIP /2.0

Incorrect value:

- INVITE sip:18338006777@sip.pstnhub.microsoft.com SIP /2.0

6.5.3 Detailed flow

Step 1. On the initial connection, the Direct Routing takes the FQDN name presented in the Contact header and matches it to the Common Name or Subject Alternative name of the presented certificate. The SBC name MUST match either option below:

- Option 1. The full FQDN name presented in the Contact header matches the Common Name/Subject Alternative name of the presented certificate OR
- Option 2. Domain portion of the FQDN name presented in the Contact header (for example adatum.biz of the FQDN name sbc1.adatum.biz) MUST matches the wildcard value in Common Name/Subject Alternative Name (for example *.adatum.biz)

Step 2. Check if the FQDN name from the Contact header is a registered DNS name in any Office 365 tenant. Goal to allow only the connections that are originating from an SBC from a valid (registered in any Office 365 tenant) FQDN.

Step 3. Take the phone number presented in the Request-URI and perform the reverse number lookup. Match the presented phone number to a user SIP URI withing the tenant found on the previous step. tenant.

6.5.4 Example

Headers to inspect:

Check incoming phone number:

- Request-URI: INVITE sip:+18338006777@sip.pstnhub.microsoft.com SIP /2.0

Check the SBC name and find the tenant:

- Contact: <sip: +17168712781@sbc1.adatum.biz;transport=tls>

Detailed steps

- **Step 1**. Certificate check using the FQDN name of the SBC from the Contact header. To complete the check for the example above, the certificate MUST have one of the options below:
    - Option 1. Common name = sbc1. adatum.biz OR
    - Option 2. Subject Alternative name = sbc1.adatum.biz OR
    - Option 3. Common or Subject Alternative name = *.adatum.biz

  If presented certificate matches, request allowed, if not request rejected;

- **Step 2**. Find and note which tenant in Office 365 has sbc1.adatum.biz registered as a domain name. If the tenant found, proceed to Step 4, if tenant with domain name sbc1.adatum.biz does not exist, proceed to Step 3;
- **Step 3**. Remove the host portion from the SBC FQDN. Result adatum.biz Find and note which tenant in Office 365 has adatum.biz registered as a domain name. If the tenant found, proceed to Step 4, if such tenant does not exist, reject the request;
- **Step 4**. Perform reverse number lookup of the number +18338006777 to a user in the tenant found in either Step 2 or Step 3;
- **Step 5**. Find the parameters set by tenant admin for this SBC (for example, preferred codec)

The requirements for two lookups, one for sbc1.adatum.biz and the second adatum.biz is for the scenario where one SBC interconnected to many tenants (carrier scenario) and covered later in the document.
Note, If the tenant found in Step 2, the Step 3 skipped.

6.6 Considerations about use of Contact and Record-Route headers

The SIP Hub needs to calculate the next hop FQDN in new in-dialog client transactions (for example Bye or Re-Invite), and when replying to SIP Options. Either Contact or Record-Route used.

According to the RFC 3261 is it mandatory to use Contact header in any request which can result in the establishing a new dialog. The Record-Route only required if a proxy wants to stay on the path of future requests in a dialog.

If both Contact and Record-Route presented, the Record-Route has higher priority. However, we do recommend using Contact and do not present Record-Route to the SIP Hub. The reasons explained below.

1. Per RFC 3261, the Record -Route is used if a proxy wants to stay on the path of future requests in a dialog, which is not essential as all traffic goes between the Microsoft SIP Hub and the paired SBC. There is no need for an intermediate proxy server between the SBC and Microsoft SIP Hub.
2. The other factor, the Microsoft SIP Hub uses Contact header to determine the next hop when sending outbound ping Options (and not Record-Route). Configuring only one parameter (Contact) instead of two (Contact and Record-Route) simplifies the administration.

Therefore, using only Contact header is strongly recommended.

However, if the Record-Route header presented in the SIP message, it has the higher priority than Contact header.

To calculate the next hop the SIP Hub uses:

- Priority 1. Top-level Record-Route. If the top-level Record-Route contains the FQDN name or IP, the FQDN name or IP used to make outbound in-dialog connection;
- Priority 2. Contact header. If Record-Route does not exist, the SIP hub will look up the value of the Contact header to make the outbound connection (recommended configuration)

Based on the value, the outgoing connection established. Use of IP address is not supported in either Record-Route or Contact. The only supported option is an FQDN Name, which also MUST be in either Common Name or Subject Alternative Name of the SBC certificate (wildcard values in the certificate supported).

If an IP address presented in the Record-route or Contact, the certificate check fails and calling experience breaks.

If FQDN does not match the value of the Common or Subject Alternative Name in the presented certificate, the call also fails.

6.7 Size of SDP Considerations

The Teams interface might send the SIP message exceeding 1500 bytes. The size of SDP primarily causes this. However, if there is a UDP trunk behind the SBC, it might reject such message if forwarded from Microsoft SIP Hub to the Trunk unmodified. We do recommend stripping some values in SDP on SBC when sending the message to the UDP trunks. For example, the ICE candidates or unused codes can be removed.

6.8 Size of Refer message considerations

The Direct Routing always sends Refer message in case of transferring the calls. This is applicable for both bypass and non-bypass cases. The size of the Refer header can be more than 1000 symbols, The SBC must support handling Refer messages with size more than 1000 symbols.

Example of refer message:

```
REFERRED-BY: <sip:sip.pstnhub-ppe.skype.net:5061;x-m=8:orgid:610b9123-1cd9-406d-ad88-
8a1173213440;x-t=8bd26852-6bec-4491-8527-29ee61dd6aa3;x-
a=Asy/aMh9Bz9bZJnmorltTcJhn6iMd3ChCPlJIYILM50O99TjiC0WWVg37hGHR4JXdRDjqCuZOaLSJP4OzrW
4T8zAOdduZemwh2pN8Gcig9Z9EuTMQ5TYGpQA6a900qOIrWhH7avf30lQx4vNq+EG9cCKOLE9ocP1QIve
GOCsLMEa+eY//MiA9aTl2ggyUP8KhNoNZWHvw9UzmHH5LjLOefzZqhUyG714SbZoU1oRrmPQnzNea6bW
OK/LfJ1BaFAl+1K/ZealfYuZe+U5qeODefSJFW5NeERDyYVkIam2Yl7ZdPjnHNqHQb4xqQu/pz6l/FEkTr2aAQk
jrUUlDS3lCm1zrcj47QE8dz/lFBrgsM6cCwgsKMSXyOk9NGjwYaVXfjXwfld5qPPNyOSboVCpkN0Ty68txe93V
N+aeSod2KEdYfF9NqKX68Mwya7qj61MOXr34dE7sfRdPS55WjIHiaWqHDdfV43d9DaNex6DaD5zn9IkwjjB
vS9RlDK4KV615zxWnh/Star+v4XrLDGdy7yLxxxnvRImC2pMp+26wj/RxlSSCodt+MwH9gidO08XqYbi5+9qr
QcADbD05ag/ObeNsj4HVNaVY7dGh1Nl/iTt6cuTnpM/aMejy9mk7Il5hZHxBunHbVEZDq36LKW88FFtZg7L
WbrC/A+H7+jWVRdy77GAC6Bg6BQqSbBw8sueGkrmiJbCF/Q9, msgLen = 1517.
296 06262018 212053.429509:1.01.00.36030.Info    .SIPCM: SipFeSocketRecvMsg - msg =
DsyilhWO73iMWlxySc+bej3UoONPkSI4E4cGi6Y6qyze4j6InzHR>
```

6.9 Requirements to the Domain Names registered in Office 365 Administrator Center

The Microsoft Phone System Hybrid Connection uses the domain name registered in Office 365 administrator center to validate if an SBC can be paired with this tenant.

To pair an SBC tenant administrator needs to connect to Office 365 PowerShell (description how to connect to Office 365 PowerShell), run a command New-CSOnlinePSTNGateway command and specify the FQDN of the SBC which is being paired.

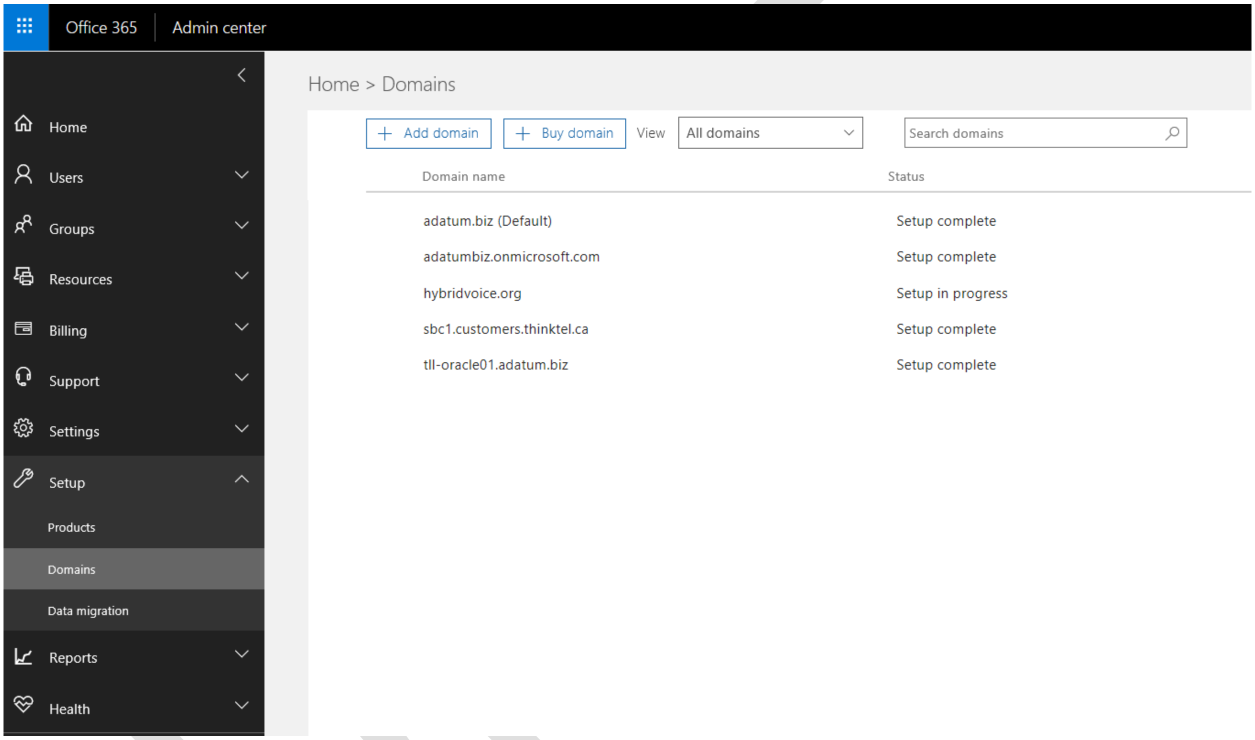
During connection to Office 365 PowerShell the tenant administrator provides the credentials, so the session established only for a specific tenant.

When command run, it checks if the FQDN name of SBC belongs to one of the domain names registered in tenant for which New-CSOnlinePSTNGateway command run.

The FQDN portion of the SBC name can be from any domain registered, except the domain names *.onmicrosoft.com and with status “Setup Complete” in the Office 365 administrator center.

Once FQDN name for SBC chosen and the SBC paired, it can serve users with any SIP addresses valid for this tenant.

For example, the picture below shows that there are five domains registered in Office 365 tenant.



Domain name	Status
adatum.biz (Default)	Setup complete
adatumbiz.onmicrosoft.com	Setup complete
hybridvoice.org	Setup in progress
sbc1.customers.thinktel.ca	Setup complete
tll-oracle01.adatum.biz	Setup complete

Domain name	Status	Can be used for FQDN name of SBC	Valid SIP addresses
adatum.biz	Setup complete	Yes	user1@adatum.biz; user2@sbc1.customers.thinktel.ca user3@tll-oracle01.adatum.biz user4@adatumbiz.onmicrosoft.com
adatumbiz.onmicrosoft.com	Setup complete	No. This is a name assigned by Microsoft. You cannot create your own A record or get a certificate for any FQDN in this domain	

hybridvoice.org	Setup in progress	No. Domains must be in status Setup complete	
sbc1.customers.thinktel.ca	Setup complete	Yes	
tll-oracle01.adatum.biz	Setup complete	Yes	

During the pairing there are two checks:

- Check 1. If the full FQDN name in format <host>.<domainname> (for example, sbc1.customers.thinktel.ca) is a registered domain in the tenant with which pairing is tried. If success, the SBC will be paired, if no, go to Check 2
- Check 2. If the <domainname> portion of the FQDN name (for example customers.thinktel.ca) is a registered domain in the tenant with which pairing is tried. If success, the SBC paired, if no, an error is thrown in PowerShell interface

Example 1. A tenant administrator tries to pair SBC with FQDN Name sbc1.customers.thinktel.ca with the tenant configured as in the table above.

- Check 1. Is sbc1.customers.thinktel.ca is a valid registered domain name for this tenant – YES, pairing successful, check 2 skipped
- Check 2. Skipped

Example 2. A tenant administrator tries to pair SBC with FQDN Name sbc1.adatum.biz with the tenant configured as in the table above.

- Check 1. Is sbc1.adatum.biz is a valid registered domain name for this tenant – NO, go to Check 2
- Check 2. Is adatum.biz is a valid registered domain name for this tenant – YES, pairing successful

Example 3. A tenant administrator tries to pair SBC with FQDN Name sbc1.contoso.com with the tenant configured as in the table above.

- Check 1. Is sbc1.contoso.com is a valid registered domain name for this tenant – NO, go to Check 2
- Check 2. Is contoso.com is a valid registered domain name for this tenant – NO, show the error in PowerShell

Example 4. A tenant administrator tries to pair SBC with FQDN Name sbc1.hybridvoice.org with the tenant configured as in the table above.

- Check 1. Is sbc1.hybridvoice.org is a valid registered domain name for this tenant – NO, go to Check 2
- Check 2. Is contoso.com is a valid registered domain name for this tenant – NO, even though it presented on the list of the domain names, the status is “Setup in progress” , only domain names with status “Setup Complete” can be used, show the error in PowerShell

Example 5. A tenant administrator tries to pair SBC with FQDN Name sbc1.adatumbiz.onmicrosoft.com with the tenant configured as in the table above.

- Check 1. Is sbc1.adatumbiz.onmicrosoft.com is a valid registered domain name for this tenant – NO, go to Check 2
- Check 2. Is adatumbiz.onmicrosoft.com is a valid registered domain name for this tenant – – YES, pairing successful. But tenant administrator will not be able to add an A record sbc1.adatumbiz.onmicrosoft.com to the Name Server which serves the adatumbiz.onmicrosoft.com domain name or get a certificate for this name.

6.10 SBC hosting scenario

The need of two checks for FQDN name during pairing and processing incoming requests as described above is needed to minimize the cost of managing for the scenario where one SBC is connected to many tenants and is hosted by a third party (not customer or Microsoft). This scenario is described in the section below in Option 2.

6.10.1 User Story

Imagine a situation where there is a carrier that wants to sell to their customers the SIP trunks interconnected to the Microsoft Teams. The carrier will charge for these services separately. Carrier has one SBC and two clients.

For the example below:

- Adatum – a carrier in Estonia, which serves many customers providing them internet, and telephony services. Adatum.biz – a domain namespace of the carrier;
- Fourth Coffee – a small coffee shop in Estonia employed 15 people. Fourth Coffee gets internet connection and the telephony services from the Adatum carrier. Fourth Coffee does not have own internal network, all users use Internet to share files or send an email. They pay approx. $125 USD a month for all services. Fourthcoffeee.com is their domain name;
- Tailspin Toys – a medium size manufacturer of toys in Estonia, employed 148 people. The company gets internet connection and the telephony services from the Adatum carrier. They have own network which has some file servers and Exchange server. They pay approx. $300 USD a month for all services to Adatum. Tailspintoys.com is their domain

Adatum also is a Microsoft Cloud Solution Provider (https://partner.microsoft.com/en-us/cloud-solution-provider).

Adatum sales people recently saw Microsoft Teams and started using them internally. They loved the product and offered it to both Fourth Coffee and Tail Spin Toys along with Office 365 subscription.

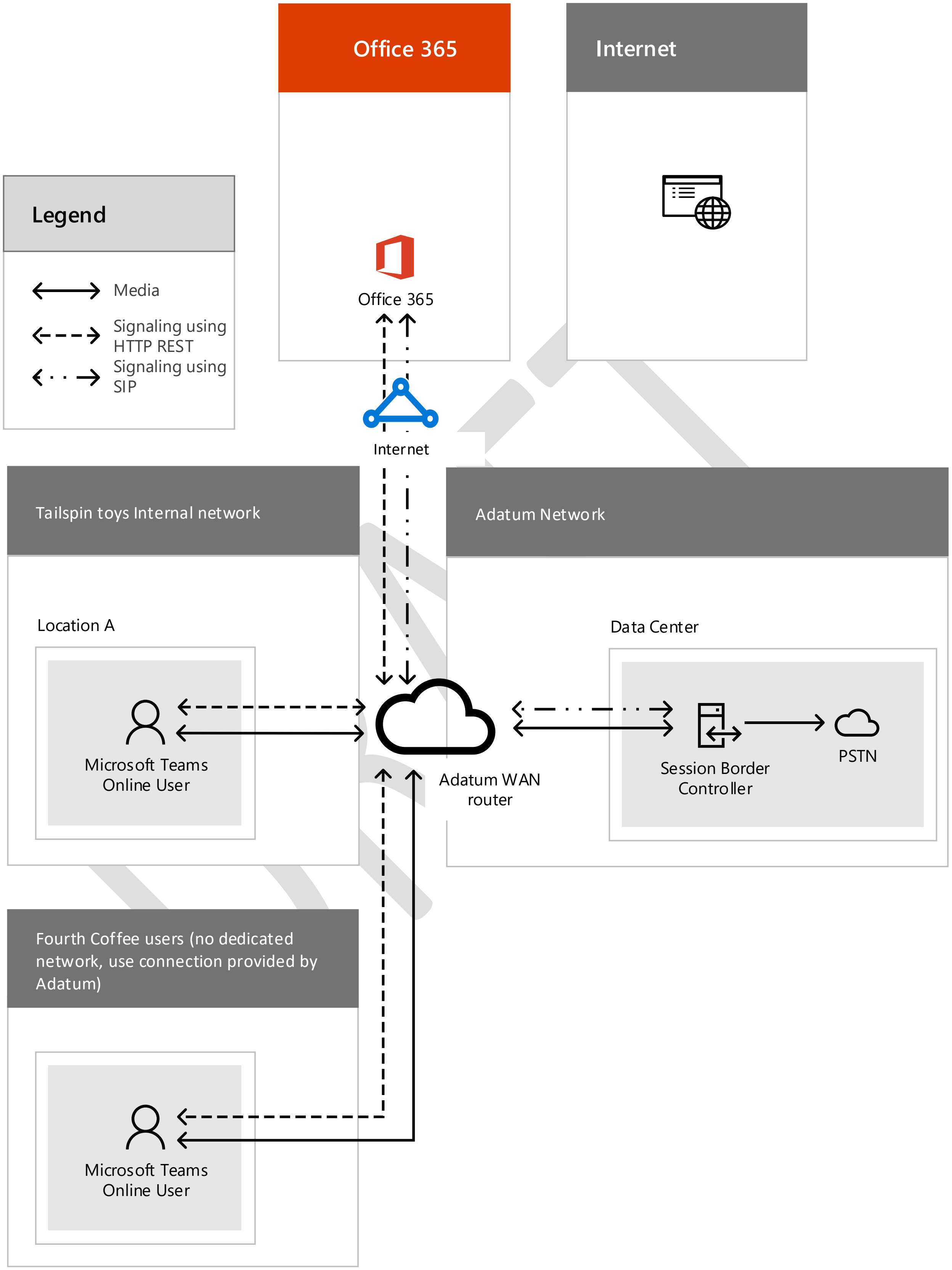
For Fourth Coffee the main selling points were option to have cloud file storage in Office 365 and an Organizational Auto Attendant in the cloud, so they don’t need to maintain any PBX for that.

For Tail Spin Toys the main selling points were moving to the Cloud and getting rid of need to host own file servers, Exchange, improvements in collaboration by using Teams Chats and option to replace their aging PBX with the Microsoft Phone System.

Both companies are buying Office 365 with Cloud PBX add on and will be paying a separate bill to Adatum for the Calling provided to Teams clients.

All connections to Internet for both companies managed by Adatum. Adatum configures routing and manages quality of the network connections.

The schema of the configuration


Office 365
Internet
Legend
Media
Signaling using HTTP REST
Signaling using SIP
Office 365
Internet
Tailspin toys Internal network
Adatum Network
Location A
Data Center
Microsoft Teams Online User
Adatum WAN router
Session Border Controller
PSTN
Fourth Coffee users (no dedicated network, use connection provided by Adatum)
Microsoft Teams Online User

For each customer Adatum created a new Office 365 tenant and registered domain names in the “Domains” tab of Office 365 Administrator center.

The names are:

- Fourthcoffee.com for Fourth Coffee
- Tailspintoys.com for Tailspin Toys

Adatum also created a SIP trunk in their SBC for every company and dedicated set of phone numbers.

But Adatum knows that every connection in a tenant is checked with a certificate and user lookup is performed based on the Domain name in Contact header of the SBC. There are two option to configure the envirionment.

6.10.2 Option 1. Registering the FQDN name for SBC in customer owned domains, the customer owned FQDN is in Contact header and in the certificate.

Adatum asks:

- Fourth Coffee

  Create an A record for sbc1.fourthcoffee.com using Fourth Coffee Name Server provider and point it to Adatum owned SBC public address;
  - Run command using the tenant administrator credentials: New-CSOnlinePSTNGateway -Fqdn sbc1.fourthcoffeee.com -SipSignalling port 5068
- Tailspin Toys
  - Create an A record for sbc1.tailspintoys.com using Tailspin Toys Name Server provider and point it to Adatum owned SBC public address;
  - Run command using the tenant administrator credentials: New-CSOnlinePSTNGateway -Fqdn sbc1.tailspintoys.com -SipSignalling port 5068

When placing calls to Fourth Coffee users the Adatum SBC presents to the SIP Hub the name sbc1.fourthcoffee.com in the contact header, and presents the certificate which has sbc1.fourthcoffeee.com or *.fourthcoffee.com as CN or SAN.

The same applies to the calls which are going to Tailspin Toys users. Adatum SBC presents the name sbc1.tailspintoys.com when calls are placed for Tailspin Toys users and presents the certificate which has sbc1.tailspintoys.com or *.tailspintoys.com as CN or SAN.

But this option requires keeping multiple SAN entries (one per a customer), which is complex and requires written agreement from a customer every time the certificate needs to be renewed. Also, this approach requires to register A records for SBC for every customer using their Name Server Provider.

6.10.3 Option 2. Registering the FQDN name for SBC in carrier owned domain name space, the carrier owned FQDN is in Contact header and in the certificate.

Adatum creates a separate sub domain for every customer:

- sbc1.customers.adatum.biz for Fourth Coffee tenant;
- sbc2.customers. adatum.biz for Tailspin Toys tenant

Note the adatum.biz is a registered domain, sbc1.customers.adatum.biz is a subdomain of the adatum.biz domain (please use RFC 1034 for reference)

Adatum asks:

- Fourth Coffee
  - Register domain name sbc1.customers.adatum.biz in Office 365 Administrator Center;
  - Run command using the tenant administrator credentials: New-CSOnlinePSTNGateway -Fqdn sbc1.customers.adatum.biz -SipSignalling port 5068
- Tailspin Toys
  - Register domain name sbc2.customers.adatum.biz in Office 365 Administrator Center;
  - Run command using the tenant administrator credentials: New-CSOnlinePSTNGateway -Fqdn sbc1.customers.adatum.biz -SipSignalling port 5068

Adatum adds to the certificate on the SBC the SAN *.customers.adatum.biz.

When call is placed to a Fourth Coffee User the Adatum SBC presents the name sbc1.customers.adatum.biz, and, based on the logic defined in this document, the phone name resolved to the user SIP URI in Fourth Coffee tenant.

The same applies to calls going to Tailspin Toys users. When call is placed to a Tailspin Toys user the Adatum SBC presents the name sbc2.customers.adatum.biz, and, based on the logic defined in this document, the phone name resolved to the user SIP URI in Tailspin Toys tenant.

Adatum chose Option 2.

7.0 Appendix 2. Media Encryption Offer / Answer Requirement for SBC in BYPASS Mode

7.1 Format for Offer from SBC in BYPASS (Offer must contain SDES and DTLS Optional in the following format)

```
 m=audio 54056 UDP/TLS/RTP/SAVP 0 8 76 77 18 9 101 13
a=rtcp:54056
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:krXco0QRglwErMqtbMs2zSw29tBdmdgXpEYZhQmp|2^31
a=fingerprint:sha-256
AE:24:07:15:5C:B7:45:1A:E4:45:60:C1:1E:68:0E:CC:8D:A6:78:3B:76:65:BB:B0:77:88
:07:F8:98:18:62:34
a=setup:actpass
```

```
a=rtcp-mux
```

7.2 Format for Answer to SBC in BYPASS mode will be one of two:

7.3 Format for Answer containing SDES to SBC

```
m=audio 54056 RTP/SAVP 111 103 104 9 0 8 106 13 110 112 113 126
a=rtcp:54056
a=crypto:2 AES_CM_128_HMAC_SHA1_80
inline:fBc61ikv1kMy0sF85DblNqTzVAbFa7hJQ9GKb6Yj|2^31|1:1
a=crypto:3 AES_CM_128_HMAC_SHA1_80
inline:O1qT9tWbs/NwJVwhfrgF5tCrbNOxnVDqkIqTx4rz|2^31
a=rtcp-mux
```

7.3.1 Format for Answer containing DTLS to SBC

```
m=audio 58760 UDP/TLS/RTP/SAVP 104 102 9 0 8 103 97 13 118 101
a=rtcp:58761
a=fingerprint:sha-256
A9:74:8A:28:BB:0E:94:48:8D:6A:F1:A1:79:F3:4F:AF:06:7F:F1:40:F9:D9:C9:81:C8:8A
:FC:5A:62:EB:28:14
a=rtcp-mux
a=setup:active
```

7.4 Format for Offer from Teams to SBC could be one of three

7.4.1 Format for SDES only offer to SBC

```
m=audio 52884 RTP/SAVP 111 103 104 9 0 8 106 13 110 112 113 126
a=crypto:0 AES_CM_128_HMAC_SHA1_32
inline:Hr4D2cgUu9+Uza5Igz/JkVx59DAxDbaxJg862ibQ|2^31
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:JPEaIxHegfuv53ykBPZk8hV0GO8kTiiqRMfHimEE|2^31
a=rtcp:52884
a=rtcp-mux
```

7.4.2 Format for DTLS Only Offer to SBC

```
a=group:BUNDLE media_0
m=audio 54056 UDP/TLS/RTP/SAVP 111 103 104 9 0 8 106 13 110 112 113 126
a=rtcp:54056
a=setup:actpass
a=fingerprint:sha-256
47:DB:97:E9:D5:5D:01:A7:79:29:7E:D3:FD:BB:89:6B:9B:69:17:87:7A:A3:54:1A:24:
F5:7F:DB:3A:3A:3A:0B
a=rtcp-mux
```

7.4.3 Format for Offer to SBC containing SDES and DTLS

```
m=audio 58760 UDP/TLS/RTP/SAVP 104 102 9 0 8 103 97 13 118 101
a=rtcp:58761
a=crypto:2 AES_CM_128_HMAC_SHA1_80
inline:fBc61ikv1kMy0sF85DblNqTzVAbFa7hJQ9GKb6Yj|2^31|1:1
a=crypto:3 AES_CM_128_HMAC_SHA1_80
inline:O1qT9tWbs/NwJVwhfrgF5tCrbNOxnVDqkIqTx4rz|2^31
a=fingerprint:sha-256
A9:74:8A:28:BB:0E:94:48:8D:6A:F1:A1:79:F3:4F:AF:06:7F:F1:40:F9:D9:C9:81:C8:8A
:FC:5A:62:EB:28:14
a=rtcp-mux
```

7.5 Format for DTLS Answer from SBC

```
m=audio 58760 UDP/TLS/RTP/SAVP 104 102 9 0 8 103 97 13 118 101
a=rtcp:58760
a=fingerprint:sha-256
A9:74:8A:28:BB:0E:94:48:8D:6A:F1:A1:79:F3:4F:AF:06:7F:F1:40:F9:D9:C9:81:C8:8A:
FC:5A:62:EB:28:14
a=rtcp-mux
a=setup:active
```

8.0 Test cases matrix

The Matrix is the summary of cases listed in 5.2 End to end scenarios and provided as an additional document. If you did not receive the matrix or have questions, please send an email to drsbccertification@microsoft.com

8.0 Noc-to-Noc process

The Noc-to-Noc process documented in a separate document. If you did not receive the document or have questions, please send an email to drsbccertification@microsoft.com