Workgroup: Network Working Group
Internet-Draft:
draft-engi-siptrunkingcapability-link-02
Published: 15 September 2022
Intended Status: Standards Track
Expires: 19 March 2023
Authors: K. Inamdar (Unaffiliated) S. Narayanan (Cisco) D. Engi (Cisco) G. Salgueiro (Cisco)

The 'sipTrunkingCapability' Link Relation Type

Abstract

This specification defines the 'sipTrunkingCapability' link relation type that may be used for the retrieval of capabilities and configuration requirements from Internet Telephony Service Providers (ITSPs). A Session Initiation Protocol (SIP) trunking capability set is defined to allow the transfer of technical requirements needed for seamless peering between SIP-based enterprise telephony networks and ITSPs where an exchange of parameters and configuration information is required.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 19 March 2023.

Copyright Notice

document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

RFC 8288 [RFC8288] defined a way of indicating relationships between resources on the Web. This document specifies the 'sipTrunkingCapability' link relation type according to the rules of RFC 8288 [RFC8288]. Links with this relationship type can be used to exchange capability information between potential peer devices. In the event that systems require additional parameters and configuration to negotiate communication, a well-known URI can be utilized to deliver information to potential peers including machine-readable instructions and parameters needed for peering.

The 'sipTrunkingCapability' link relation type may be used on web resources hosted by Internet Telephony Service Providers (ITSPs) to provide a structured and detailed capability set document. The capability set document encapsulates a set of characteristics of an ITSP, which when retrieved by enterprise telephony network devices allows for automated establishment of Session Initiation Protocol (SIP) trunking between the two telephony networks.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. The 'sipTrunkingCapability' Link Relation Type

A capability set document is hosted via web resources by the ITSP. A unique location of the document can be preconfigured and provided to

each peer by the ITSP, or a centrally published resource can be used that dynamically generates the capability set document based on Uniform Resource Identifier(s) [RFC3986] determined by the peering device. The document describes the configuration parameters required to successfully establish SIP trunking between an enterprise and service provider SIP telephony network. The capability set document SHOULD be composed of structured and machine-readable parameters that could be easily converted into configuration data to meet the communication requirements of the service provider. The need for an enterprise telephony network to obtain a capability set document from an Internet Telephony Service Provider (ITSP) is documented in Automatic Peering for SIP Trunks [I-D.ietf-asap-sip-auto-peer].

4. Example Usage

This section provides an example of possible use of the 'sipTrunkingCapability' relation type. The enterprise network device solicits the location of the capability document from the well-known URI hosted by the SIP service provider using the WebFinger protocol [RFC7033].

```
GET /.well-known/webfinger?
   resource=acct%3Atrunkent1456%40example.com&
   rel=sipTrunkingCapability
   HTTP/1.1
Host: ssp1.example.com
```

The capability set location is returned to the source device referencing the URI that contains parameters for peering.

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/jrd+json
{
   "subject" : "acct:trunkent1456@example.com",
   "links" :
   [
      {
         "rel" : "sipTrunkingCapability",
         "href" :"https://capserver.ssp1.com/capserver/capdoc.json"
      }
   ]
}
```

The ITSP may use an authentication framework such as OAuth 2.0 [RFC6749] to determine the identity of the enterprise telephony network and provide the appropriate capability set document.

5. IANA Considerations

IANA is instructed to register the sipTrunkingCapability link relation under the "Link Relation Types" Registry, with a reference to this document, using the following template:

Relation Name: sipTrunkingCapability

Description: A capability document that defines parameters or configuration requirements for automated peering and communication channel negotiation of the Session Initiation Protocol (SIP).

Reference: RFCXXXX

[[NOTE TO RFC EDITOR: Please change XXXX to the number assigned to this specification, and remove this paragraph on publication.]]

6. Security Considerations

The 'sipTrunkingCapability' relation type is not known to introduce any new security issues not already discussed in RFC 8288 [RFC8288] for generic use of web linking mechanisms. However, it is recommended to exercise caution when publishing potentially sensitive capability information over unencrypted or unauthenticated channels.

7. Acknowledgements

This document resulted from the discussions in the ASAP working group, especially the detailed and thoughtful comments of Paul Jones, Marc Petit-Huguenin, Cullen Jennings, Jonathan Rosenberg, Jon Peterson and Chris Wendt.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/

RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8288] Nottingham, M., "Web Linking", RFC 8288, DOI 10.17487/RFC8288, October 2017, <https://www.rfc-editor.org/info/rfc8288>.

8.2. Informative Reference

[I-D.ietf-asap-sip-auto-peer] Inamdar, K., Narayanan, S., and C. Jennings, "Automatic Peering for SIP Trunks", October 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-asap-sip-auto-peer>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/info/rfc6749>.

[RFC7033] Jones, P., Salgueiro, G., Jones, M., and J. Smarr, "WebFinger", RFC 7033, DOI 10.17487/RFC7033, September 2013, <https://www.rfc-editor.org/info/rfc7033>.

Authors' Addresses

Kaustubh Inamdar
Unaffiliated

Email: kaustubh.ietf@gmail.com

Sreekanth Narayanan
Cisco

Email: sreenara@cisco.com

Derek Engi
Cisco
Ann Arbor, MI
US

Phone: +1 919 392 7966
Email: deengi@cisco.com

Gonzalo Salgueiro
Cisco
7200-12 Kit Creek Rd.
Research Triangle Park, NC 27709
US

Phone: +1 919 392 3266
Email: gsalguei@cisco.com