RTCWEB
Internet-Draft
Intended status: Standards Track
Expires: March 31, 2014

S. Nandakumar
G. Salgueiro
P. Jones
Cisco Systems
M. Petit-Huguenin
Impedance Mismatch

September 27, 2013

# URI Scheme for Session Traversal Utilities for NAT (STUN) Protocol
# draft-nandakumar-rtcweb-stun-uri-08

## Abstract

This document is the specification of the syntax and semantics of the Uniform Resource Identifier (URI) scheme for the Session Traversal Utilities for NAT (STUN) protocol.

## 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 http://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 March 31, 2014.

## Copyright Notice

Table of Contents



## 1. Introduction

This document specifies the syntax and semantics of the Uniform Resource Identifier (URI) scheme for the Session Traversal Utilities for NAT (STUN) protocol.

STUN is a protocol that serves as a tool for other protocols in dealing with Network Address Translator (NAT) traversal. It can be used by an endpoint to determine the IP address and port allocated to it by a NAT, to perform connectivity checks between two endpoints, and used as a keepalive protocol to maintain NAT bindings. RFC 5389 [RFC5389] defines the specifics of the STUN protocol.

The "stun" and "stuns" URI schemes are used to designate a standalone STUN server or any Internet host performing the operations of a STUN server in the context of STUN usages (Section 14 RFC 5389 [RFC5389]). With the advent of standards such as WEBRTC [WEBRTC], we anticipate a plethora of endpoints and web applications to be able to identify and communicate with such a STUN server to carry out the STUN protocol. This also implies those endpoints and/or applications to be provisioned with appropriate configuration required to identify the STUN server. Having an inconsistent syntax has its drawbacks and can result in non-interoperable solutions. It can result in solutions that are ambiguous and have implementation limitations on the different aspects of the syntax and alike. The 'stun/stuns' URI scheme helps alleviate most of these issues by providing a consistent way to describe, configure and exchange the information identifying a STUN server. This would also prevent the shortcomings inherent with encoding similar information in non-uniform syntaxes such as the ones proposed in the WEBRTC Standards [WEBRTC], for example.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] when they appear in ALL CAPS. When these words are not in ALL CAPS (such as "should" or "Should"), they have their usual english meanings, and are not to be interpreted as RFC 2119 key words.

## 3. Definition of the STUN or STUNS URI

### 3.1. URI Scheme Syntax

A STUN/STUNS URI has the following formal ABNF syntax [RFC5234]:

```
stunURI       = scheme ":" host [ ":" port ]
scheme        = "stun" / "stuns"
```

<host>, and <port> are specified in [RFC3986]. While these two ABNF productions are defined in [RFC3986] as components of the generic hierarchical URI, this does not imply that the stun and stuns URI schemes are hierarchical URIs. Developers MUST NOT use a generic hierarchical URI parser to parse a stun or stuns URI.

### 3.2. URI Scheme Semantics

The "stun" and "stuns" URI schemes are used to designate a standalone STUN server or any Internet host performing the operations of a STUN server in the context of STUN usages (Section 14 RFC 5389 [RFC5389]). The STUN protocol supports sending messages over UDP, TCP or TLS-over-TCP. The "stuns" URI scheme MUST be used when STUN is run over TLS-over-TCP (or in the future DTLS-over-UDP) and the "stun" scheme MUST be used otherwise.

The required <host> part of the "stun" URI denotes the STUN server host.

For the optional DNS Discovery procedure mentioned in the Section 9 of RFC5389, "stun" URI scheme implies UDP as the transport protocol for SRV lookup and "stuns" URI scheme indicates TCP as the transport protocol.

As specified in [RFC5389], the <port> part, if present, denotes the port on which the STUN server is awaiting connection requests. If it is absent, the default port is 3478 for both UDP and TCP. The default port for STUN over TLS is 5349 as per Section 9 of [RFC5389].

## 4. Implementation Status

Note to RFC Editor: Please remove this section and the reference to [RFC6982] before publication.

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC6982]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [RFC6982], "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

### 4.1. libjingle

Organization: Google Inc.

Name: libjingle revision 4831 https://code.google.com/p/chromium/codesearch#chromium/src/third_party/libjingle/source/talk/app/webrtc/peerconnection.cc

Description: Libjingle is a set of components provided by Google to implement Jingle protocols XEP-166 (http://xmpp.org/extensions/xep-0166.html) and XEP-167 (http://xmpp.org/extensions/xep-0167.html).

Level of maturity: Beta.

Coverage: Implements draft-nandakumar-rtcweb-stun-uri-07 without IPv6. The stun and stuns schemes are parsed, and TLS is used when the secure bit is set.

Licensing: BSD 3-clauses license.

Contact: https://code.google.com/p/chromium/

URL: https://code.google.com/p/chromium/codesearch#chromium/src/third_party/libjingle/source/talk/app/webrtc/peerconnection.cc

### 4.2. Firefox

Organization: Mozilla

Name: Firefox Aurora 21 http://hg.mozilla.org/mozilla-central/rev/6b5016ab9ebb

Description: Mozilla Firefox is a free and open source web browser.

Level of maturity: Beta.

Coverage: Implements draft-nandakumar-rtcweb-stun-uri-03. The mozilla code parses the turn and turns schemes but does not seems to use TLS.

Licensing: Mozilla Public License, v. 2.0.

Contact: http://www.mozilla.org/en-US/firefox/channel/

URL: http://hg.mozilla.org/mozilla-central/file/4ff1e574e509/media/webrtc/signaling/src/peerconnection/PeerConnectionImpl.cpp

## 5. Security Considerations

The "stun" and "stuns" URI schemes do not introduce any specific security issues beyond the security considerations discussed in [RFC3986]. These URI schemes are intended for use in specific environments that involve NAT traversal. Users of the scheme need to carefully consider the security properties of the context in which they are using them.

While the stun and stuns URIs do not themselves include the username or password that will be used to authenticate the STUN client, in certain environments, such as WebRTC, the username and password will almost certainly be provisioned remotely by an external agent at the same time as a stuns URI is sent to that client. Thus, in such situations, if the username and password were received in clear there would be little or no benefit to using a stuns URI. For this reason a STUN client MUST ensure that the username, password, and stuns URI and any other security-relevant parameters are received with equivalent security before using the stuns URI. Receiving those parameters over another TLS session can provide the appropriate level of security, if both TLS sessions are similarly parameterised, e.g. with commensurate strength ciphersuites.

## 6. IANA Considerations

This section contains the registration information for the "stun" and "stuns" URI Schemes (in accordance with [RFC4395]). Note that these URI schemes are intended for use in very specific NAT traversal environments, and should not be used otherwise on the open Web or Internet.

### 6.1. STUN URI Registration

URI scheme name: stun

Status: permanent

URI scheme syntax: See Section 3.1.

URI scheme semantics: See Section 3.2.

Encoding considerations: There are no encoding considerations beyond those in [RFC3986].

Applications/protocols that use this URI scheme name:

> The "stun" URI scheme is intended to be used by applications with a need to identify a STUN server to be used for NAT traversal.

Interoperability considerations: N/A

Security considerations: See Section 5.

Contact: Suhas Nandakumar <snandaku@cisco.com>

Author/Change controller: The IESG

References: RFCXXXX

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

### 6.2. STUNS URI Registration

URI scheme name: stuns

Status: permanent

URI scheme syntax: See Section 3.1.

URI scheme semantics: See Section 3.2.

Encoding considerations: There are no encoding considerations beyond those in [RFC3986].

Applications/protocols that use this URI scheme name:

> The "stun" URI scheme is intended to be used by applications with a need to identify a STUN server to be used for NAT traversal over a secure connection.

Interoperability considerations: N/A

Security considerations: See Section 5.

Contact: Suhas Nandakumar <snandaku@cisco.com>

Author/Change controller: The IESG

References: RFCXXXX;

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

## 7. Acknowledgements

The authors would like to extend a very special thanks to Cullen Jennings for bringing to our attention the WebRTC need for this document, as well as his detailed review and thoughtful comments on this document.

This document has benefited from extensive discussion and review of many of the members of the RTCWEB and BEHAVE working groups. The authors would also like to acknowledge Ted Hardie, Bjoern Hoehrmann, Russ Housley, Subramanian Moonesamy, Hadriel Kaplan, Graham Klyne, Peter Saint-Andre, Ted Lemon, Barry Leiba, Pete Resnick, Spencer Dawkins, Stephen Farrell and Harald Alvestrand for their invaluable input, reviews, feedback comments, and suggestions that helped to improve this document.

The authors would also like to express their gratitude to Dan Wing for his assistance in shepherding this document. We also want to thank Gonzalo Camarillo, the Real-time Applications and Infrastructure Director, for sponsoring this document as well his careful reviews.

This document was written with the xml2rfc tool described in [RFC2629].

## 8. References

### 8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

### 8.2. Informative References

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC4395] Hansen, T., Hardie, T., and L. Masinter, "Guidelines and Registration Procedures for New URI Schemes", BCP 35, RFC 4395, February 2006.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, October 2008.

[RFC6982] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", RFC 6982, July 2013.

[WEBRTC] Bergkvist, A., Burnett, D., Jennings, C., and A. Narayanan, "WebRTC 1.0: Real-time Communication Between Browsers", World Wide Web Consortium WD WD-webrtc-20120821, August 2012, <http://www.w3.org/TR/2012/WD-webrtc-20120821>.

## Appendix A. Examples

Table 1 shows examples for 'stun/stuns'uri scheme. For all these examples, the <host> component is populated with "example.org".

| URI |
|---|
| stun:example.org |
| stuns:example.org |
| stun:example.org:8000 |

Table 1

## Appendix B. Design Notes

- One recurring comment was to stop using the suffix "s" on URI scheme, and to move the secure option to a parameter (e.g., ";proto=tls"). We decided against this idea because the need for ";proto=" for the STUN URI cannot be sufficiently explained and supporting it would render an incomplete specification. This would also result in lost symmetry between the TURN and STUN URIs. A more detailed account of the reasoning behind this is available at <http://blog.marc.petit-huguenin.org/2012/09/on-design-of-stun-and-turn-uri-formats.html>

- Following the advice of Section 2.2 of [RFC4395], and because the STUN URI does not describe a hierarchical structure, the STUN URIs are opaque.

## Appendix C. Release notes

NOTE TO RFC EDITOR: This section must be removed before publication as an RFC.

### C.1. Modifications between draft-nandakumar-rtcweb-stun-uri-08 and draft-nandakumar-rtcweb-stun-uri-07

- Changed the ABNF to use references from RFC 3986 instead of copying them.
- Converted the design note about hierarchical parsers into a MUST NOT statement.
- Updated the RFC 6982 forms for Chrome and Firefox.
- Added text in security section about verifying that username, password and uris are received over a secure connection.

## Authors' Addresses

Suhas Nandakumar
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134
US

Email: snandaku@cisco.com

Gonzalo Salgueiro
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: gsalguei@cisco.com

Paul E. Jones
Cisco Systems
7025 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: paulej@packetizer.com

Marc Petit-Huguenin
Impedance Mismatch

Email: petithug@acm.org