RTCWEB
Internet-Draft
Intended status: Standards Track
Expires: March 17, 2013

S. Nandakumar
G. Salgueiro
P. Jones
Cisco Systems
M. Petit-Huguenin
Impedance Mismatch
January 23, 2013

URI Scheme for Session Traversal Utilities for NAT (STUN) Protocol
draft-nandakumar-rtcweb-stun-uri-03

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. This document may not be modified, and derivative works of it may not be created, except to format it for publication as an RFC or to translate it into languages other than English.

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 17, 2013.

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].

3. Definition of the STUN or STUNS URI

3.1. URI Scheme Syntax

The "stun" URI takes the following form (the example below is non-normative):

stun:<stun-host>:<stun-port>

stuns:<stun-host>:<stun-port>

Note that the <port> part and the preceding ":" (colon) character, is OPTIONAL.

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

```
stunURI       = scheme ":" stun-host [ ":" stun-port ]
scheme        = "stun" / "stuns"
stun-host     = IP-literal / IPv4address / reg-name
stun-port     = *DIGIT
IP-literal    = "[" ( IPv6address / IPvFuture  ) "]"
IPvFuture     = "v" 1*HEXDIG "." 1*( unreserved / sub-delims / ":" )
IPv6address   =                            6( h16 ":" ) ls32
                /                       "::" 5( h16 ":" ) ls32
                / [               h16 ] "::" 4( h16 ":" ) ls32
                / [ *1( h16 ":" ) h16 ] "::" 3( h16 ":" ) ls32
                / [ *2( h16 ":" ) h16 ] "::" 2( h16 ":" ) ls32
                / [ *3( h16 ":" ) h16 ] "::"    h16 ":"   ls32
                / [ *4( h16 ":" ) h16 ] "::"              ls32
                / [ *5( h16 ":" ) h16 ] "::"              h16
                / [ *6( h16 ":" ) h16 ] "::"
h16           = 1*4HEXDIG
ls32          = ( h16 ":" h16 ) / IPv4address
IPv4address   = dec-octet "." dec-octet "." dec-octet "." dec-octet
dec-octet     = DIGIT                 ; 0-9
                / %x31-39 DIGIT       ; 10-99
                / "1" 2DIGIT          ; 100-199
                / "2" %x30-34 DIGIT   ; 200-249
                / "25" %x30-35        ; 250-255
reg-name      = *( unreserved / pct-encoded / sub-delims )
```

<unreserved>, <sub-delims>, and <pct-encoded> are specified in [RFC3986]. The core rules <DIGIT> and <HEXDIGIT> are used as described in Appendix B of RFC 5234 [RFC5234].

3.2. URI Scheme Semantics

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 <stun-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.

The <stun-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 RFC 5389 [RFC5389].

4. Security Considerations

The "stun" and "stuns" URI schemes do not introduce any specific security issues beyond the security considerations discussed in [RFC3986].

5. IANA Considerations

This section contains the registration information for the "stun" and "stuns" URI Schemes (in accordance with [RFC4395]).

5.1. 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 that might need access to a STUN server.

Interoperability considerations: N/A

Security considerations: See Section 4.

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.]]

5.2. 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 "stuns" URI scheme is intended to be used by applications that might need access to a STUN server over a secure connection.

Interoperability considerations: N/A

Security considerations: See Section 4.

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. Acknowledgements

Many thanks to Cullen Jennings for his detailed review and thoughtful comments on this document.

Thanks to Ted Hardie, Bjoern Hoehrmann for their comments, suggestions and questions that helped to improve the this document.

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

7. References

7.1. 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.

7.2. 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.

[WEBRTC] W3C, "WebRTC 1.0: Real-time Communication Between Browsers".

<http://dev.w3.org/2011/webrtc/editor/webrtc.html>.

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 of ";proto=" for the STUN URI cannot be sufficiently explained and supporting it would render into an incomplete specification. This would also result in loosing 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>

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