RTCWEB
Internet-Draft
Intended status: Standards Track
Expires: April 27, 2012

S. Nandakumar
G. Salgueiro
P. Jones
Cisco Systems

October 25, 2011

URI Scheme for Session Traversal Utilities for NAT (STUN) Protocol
draft-nandakumar-rtcweb-stun-uri-00

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 April 27, 2012.

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/stuns' URI scheme is 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.

The 'stun/stuns' URI scheme adheres to the generic syntax defined in RFC 3986 [RFC3986].

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 RFC 2119 [RFC2119].

3. URI Scheme Definition

3.1. URI Scheme Syntax

The 'stun/stuns' URI takes the following form (the syntax below is non-normative):

stun:<userinfo>@<host>:<port>

stuns:<userinfo>@<host>:<port>

Where <userinfo> with the "@" (at) sign character, as well as the <port> part and the preceding ":" (colon) character, is OPTIONAL.

The normative syntax of the 'stun' URI is defined as shown in the following Augmented Backus-Naur Form (ABNF) [RFC5234]. rule:

```
stun-uri      = stun-scheme ":" [ userinfo "@" ] host [ ":" port ]
stun-scheme   = "stun"/"stuns"
userinfo      = user
user          = 1*(%x21-24 / %x26-39 / %x3B-3F / %x41-7F
                / escaped)
                    ; The symbols "%", ":", "@", and symbols
                    ; with a character value below 0x21 may
                    ; be represented as escaped sequences.
host          = hostname / IPv4address / IPv6reference
hostname      = *( domainlabel "." ) toplabel [ "." ]
domainlabel   = alphanum / alphanum *( alphanum / "-" ) alphanum
toplabel      = ALPHA / ALPHA *( alphanum / "-" ) alphanum
IPv4address   = 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT
IPv6reference = "[" IPv6address "]"
IPv6address   = hexpart [ ":" IPv4address ]
hexpart       = hexseq / hexseq "::" [ hexseq ] / "::" [ hexseq ]
hexseq        = hex4 *( ":" hex4 )
hex4          = 1*4HEXDIG
port          = 1*DIGIT
```

```
alphanum      = ALPHA / DIGIT
escaped       = "%" HEXDIG HEXDIG
```

The current ABNF proposal doesn't specify a mechanism for handling different transports. We have identified a possible solution and will be included in the future version of the draft.

The <host>, <port> and <userinfo> rules are described in Appendix A of RFC 3986 [RFC3986]. The core rules <ALPHA>, <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 SHALL be used when STUN is run over TLS-over-TCP (or DTLS-over-UDP in the future) and the 'stun' scheme SHALL be used otherwise. The <host> part of the 'stun' URI, which is REQUIRED, denotes the STUN server host. The <userinfo> part is OPTIONAL and MAY NOT be utilized within the 'stun/stuns' URI scheme.

It is provided so as to be compatible with certain non-standard standalone STUN server implementations that enforce clients to authenticate. The <port> part, if present,denotes the port on which the STUN server is awaiting connection requests. For a standalone STUN server the port SHALL default to 3478 for both UDP and TCP. The default port for TLS SHALL be 5349.

4. Examples

URI identifying a STUN Server at example.com listening on port 1234:

```
stun:example.com:1234
```

A URI to identify a STUN server at example.com listening on the default TLS port 5349:

```
stuns:example.com
```

URI to identify a short-term or a long-term credential for the connection to STUN server, example.com, on port 1234:

stun:username:password@example.com:1234

5. IANA Considerations

This document instructs IANA to register the 'stun' and 'stuns' URI schemes in the "Permanent URI Schemes" sub-registry in the "Uniform Resource Identifier (URI) Schemes" IANA registry [URIREG]. These registrations follows the URI Scheme Registration Template detailed in Section 5.4 of RFC 4395 [RFC4395].

5.1. The 'stun' URI Scheme Registration

IANA registration of the the 'stun' URI scheme:

URI scheme name: stun

Status: Permanent

URI scheme syntax: see Section 3.1 of RFC XXXX [This document]

URI scheme semantics: see Section 3.2 of RFC XXXX [This document]

URI scheme encoding considerations: there are no other encoding considerations for 'stun' URIs that are not described in RFC 5389 [RFC5389].

Protocols that use the scheme: Session Traversal Utilities for NAT (STUN)

Security Considerations: see Section 6 of RFC XXXX [This document]

Contact: IESG <iesg@ietf.org>

Author/Change controller: IETF <ietf@ietf.org>

References: See Section 8 of RFC XXXX [This document]

5.2. The 'stuns' URI Scheme Registration

IANA registration of the the 'stuns' URI scheme:

URI scheme name: stuns

Status: Permanent

URI scheme syntax: see Section 3.1 of RFC XXXX [This document]

URI scheme semantics: see Section 3.2 of RFC XXXX [This document]

URI scheme encoding considerations: there are no other encoding considerations for 'stuns' URIs that are not described in RFC 5389 [RFC5389].

Protocols that use the scheme: Session Traversal Utilities for NAT (STUN) when run over TLS-over-TCP.

Security Considerations: see Section 6 of RFC XXXX [This document]

Contact: IESG <iesg@ietf.org>

Author/Change controller: IETF <ietf@ietf.org>

References: See Section 8 of RFC XXXX [This document]

6. Security Considerations

Generic security considerations for the usage of URIs are discussed in Section 7 of RFC 3986 [RFC3986]

The URI Scheme defined by this document for the Session Traversal Utilities for NAT (STUN) protocol does not introduce any security considerations beyond those detailed in Section 16 of RFC 5389 [RFC5389].

The STUN protocol supports two opional credential mechanisms as described in the Section 10 of RFC 5389 [RFC5389]. For the short-term credential mechanism (Section 10.1 of RFC 5389 [RFC5389]), the security of such a credential SHALL be the responsibility of the STUN usage mechanism, say ICE (RFC 5245 [RFC5245]). For the long-term credential mechanism (Section 10.2 of RFC 5389 [RFC5389]), such a credential MUST be passed over a secure transport such as HTTPS (RFC 2818 [RFC2818]).

7. Acknowledgements

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

We acknowledge the existence of draft-petithuguenin-behave-turn-uri-bis-04 document as a parallel effort in defining the URI scheme for TURN. Awareness of this draft came late in the process and we have not had to time to reach out to the author of that memo and discuss opportunities to collaborate on a single document. It is our intentions to do so.

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.

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

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

8.2. Informative References

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

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

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

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment

(ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, April 2010.

[URIREG] Internet Assigned Numbers Authority (IANA) Registry, "Uniform Resource Identifier (URI) Schemes", <http://www.iana.org/assignments/uri-schemes.html> .

[WEBRTC] W3C, "WebRTC 1.0: Real-time Communication Between Browsers", <http://dev.w3.org/2011/webrtc/editor/webrtc.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