Internet Engineering Task Force (IETF)
Request for Comments: 7064
Category: Standards Track
ISSN: 2070-1721

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

November 2013

URI Scheme for the Session Traversal Utilities for NAT (STUN) Protocol

Abstract

This document specifies 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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7064.

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 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 stand-alone STUN server or any Internet host performing the operations of a STUN server in the context of STUN usages (Section 14 of 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 implies that endpoints and/or applications must be provisioned with the appropriate configuration to identify the STUN server. Having an inconsistent syntax adds ambiguity and can result in non-interoperable solutions and implementation limitations. The "stun" and "stuns" URI schemes help alleviate most of these issues by providing a consistent way to describe, configure, and exchange the information identifying a STUN server.

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

"stun" and "stuns" URIs have 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 stand-alone STUN server or any Internet host performing the operations of a STUN server in the context of STUN usages (Section 14 of 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 Section 9 of RFC 5389, the "stun" URI scheme implies UDP as the transport protocol for SRV lookup, and the "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. 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.

Although a "stun" or "stuns" URI does not itself 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 the 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, "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 parameterized, e.g., with commensurate strength ciphersuites.

5. 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.

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 with a need to identify a STUN server to be used for NAT traversal.

Interoperability considerations: N/A

Security considerations: See Section 4

Contact: Suhas Nandakumar <snandaku@cisco.com>

Author/Change controller: The IESG

References: RFC 7064

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 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 4

Contact: Suhas Nandakumar <snandaku@cisco.com>

Author/Change controller: The IESG

References: RFC 7064

6. Acknowledgements

The authors would like to extend a very special thanks to Cullen Jennings for bringing to our attention to WebRTC's 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 Area Director, for sponsoring this document as well as his careful reviews.

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] 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 the "stun" and "stuns" URI schemes. 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 the 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.

- 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.

Authors' Addresses

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

EMail: snandaku@cisco.com

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

EMail: gsalguei@cisco.com

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

EMail: paulej@packetizer.com

Marc Petit-Huguenin
Impedance Mismatch

EMail: petithug@acm.org