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

Traversal Using Relays around NAT (TURN) Uniform Resource Identifiers

Abstract

   This document specifies the syntax of Uniform Resource Identifier
   (URI) schemes for the Traversal Using Relays around NAT (TURN)
   protocol. It defines two URI schemes to provision the TURN
   Resolution Mechanism (RFC 5928).

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/rfc7065.

Table of Contents

1. Introduction

   This document specifies the syntax and semantics of the Uniform
   Resource Identifier (URI) scheme for the Traversal Using Relays
   around NAT (TURN) protocol.

   The TURN protocol is a specification allowing hosts behind NAT to
   control the operation of a relay server. The relay server allows
   hosts to exchange packets with its peers. The peers themselves may
   also be behind NATs. RFC 5766 [RFC5766] defines the specifics of the
   TURN protocol.

   The "turn" and "turns" URI schemes are used to designate a TURN
   server (also known as a relay) on Internet hosts accessible using the
   TURN protocol. 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 TURN server to carry out the
   TURN protocol. This implies that endpoints and/or applications must
   be provisioned with the appropriate configuration to identify the
   TURN server. Having an inconsistent syntax adds ambiguity and can
   result in non-interoperable solutions and implementation limitations.
   The "turn" and "turns" URI schemes help alleviate most of these
   issues by providing a consistent way to describe, configure, and
   exchange the information identifying a TURN server.

   [RFC5928] defines a resolution mechanism to convert a secure flag, a
   host name or IP address, a potentially empty port, and a potentially
   empty transport to a list of IP address, port, and TURN transport
   tuples.

   To simplify the provisioning of TURN clients, this document defines
   the "turn" and "turns" URI schemes that can carry the four components
   needed for the resolution mechanism.

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. Definitions of the "turn" and "turns" URI

3.1. URI Scheme Syntax

   The "turn" and "turns" URIs have the following formal ABNF syntax
   [RFC5234]:

```
turnURI       = scheme ":" host [ ":" port ]
                [ "?transport=" transport ]
scheme        = "turn" / "turns"
transport     = "udp" / "tcp" / transport-ext
transport-ext = 1*unreserved
```

   <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 "turn" and "turns"
   schemes are hierarchical URIs. Developers MUST NOT use a generic
   hierarchical URI parser to parse a "turn" or "turns" URI.

   The <host>, <port>, and <transport> components are passed without
   modification to the [RFC5928] algorithm. <secure> is set to false if
   <scheme> is equal to "turn", and set to true if <scheme> is equal to
   "turns" and passed to the [RFC5928] algorithm with the other
   components.

3.2. URI Scheme Semantics

   The "turn" and "turns" URI schemes are used to designate a TURN
   server (also known as a relay) on Internet hosts accessible using the
   TURN protocol. The TURN protocol supports sending messages over UDP,
   TCP, or TLS-over-TCP. The "turns" URI scheme MUST be used when TURN
   is run over TLS-over-TCP (or, in the future, DTLS-over-UDP), and the
   "turn" scheme MUST be used otherwise.

   The required <host> part of the "turn" URI denotes the TURN server
   host.

   As specified in [RFC5766] and [RFC5928], the <port> part, if present,
   denotes the port on which the TURN server is awaiting connection
   requests. If it is absent, the default port is 3478 for both UDP and
   TCP. The default port for TURN over TLS is 5349.

4. Security Considerations

   Security considerations for the resolution mechanism are discussed in
   Section 5 of [RFC5928]. Note that this section contains normative
   text defining authentication procedures to be followed by turn
   clients when TLS is used.

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

   Although a "turn" or "turns" URI does not itself include the username
   or password that will be used to authenticate the TURN 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 "turns" 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 "turns" URI. For this
   reason, a TURN client MUST ensure that the username, password,
   "turns" URI, and any other security-relevant parameters are received
   with equivalent security before using the "turns" 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.

5. IANA Considerations

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

5.1. "turn" URI Registration

   URI scheme name: turn

   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 "turn" URI scheme is intended to be used by applications with
      a need to identify a TURN server to be used for NAT traversal.

   Interoperability considerations: N/A

   Security considerations: See Section 4.

   Contact: Marc Petit-Huguenin <petithug@acm.org>

   Author/Change controller: The IESG

   References: RFC 7065

5.2. "turns" URI Registration

   URI scheme name: turns

   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 "turns" URI scheme is intended to be used by applications with
      a need to identify a TURN server to be used for NAT traversal over
      a secure connection.

   Interoperability considerations: N/A

   Security considerations: See Section 4.

   Contact: Marc Petit-Huguenin <petithug@acm.org>

   Author/Change controller: The IESG

   References: RFC 7065

6. Acknowledgements

   Thanks to Margaret Wasserman, Magnus Westerlund, Juergen
   Schoenwaelder, Sean Turner, Ted Hardie, Dave Thaler, Alfred E.
   Heggestad, Eilon Yardeni, Dan Wing, Alfred Hoenes, and Jim Kleck for
   the comments, suggestions, and questions that helped improve
   "Traversal Using Relays around NAT (TURN) Uniform Resource
   Identifiers" by M. Petit-Huguenin (October 2011).

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.

   [RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "Traversal Using
              Relays around NAT (TURN): Relay Extensions to Session
              Traversal Utilities for NAT (STUN)", RFC 5766, April 2010.

   [RFC5928] Petit-Huguenin, M., "Traversal Using Relays around NAT
              (TURN) Resolution Mechanism", RFC 5928, August 2010.

7.2. Informative References

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

   [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 how the <secure>, <port>, and <transport> components
   are populated from various URIs. For all these examples, the <host>
   component is populated with "example.org".

```
+-------------------------------+----------+--------+-------------+
| URI                           | <secure> | <port> | <transport> |
+-------------------------------+----------+--------+-------------+
| turn:example.org              | false    |        |             |
| turns:example.org             | true     |        |             |
| turn:example.org:8000         | false    | 8000   |             |
| turn:example.org?transport=udp| false    |        | UDP         |
| turn:example.org?transport=tcp| false    |        | TCP         |
| turns:example.org?transport=tcp| true    |        | TLS         |
+-------------------------------+----------+--------+-------------+
```

                               Table 1

Appendix B. Design Notes

   o 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 STUN URI
      does not have a ";proto=" parameter and we would have lost the
      symmetry between the TURN and STUN URIs.

   o Following the advice of Section 2.2 of RFC 4395, and because the
      TURN URI does not describe a hierarchical structure, the TURN URIs
      are opaque URIs.

   o <password> is not used in the URIs because it is deprecated
      [RFC3986]. <username> and <auth> are not used in the URIs because
      they do not guide the resolution mechanism.

   o As discussed at IETF 72 in Dublin, there are no generic parameters
      in the URI to prevent compatibility issues.

Authors' Addresses

   Marc Petit-Huguenin
   Impedance Mismatch

   EMail: petithug@acm.org

   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