

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 Traversal Using Relays around NAT (TURN) Protocol
draft-nandakumar-rtcweb-turn-uri-00

Abstract

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

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

URI Scheme for TURN

October 2011

Table of Contents

1.	Introduction	3
2.	Terminology	3
3.	URI Scheme Definition	3
3.1.	URI Scheme Syntax	3
3.2.	URI Scheme Semantics	4
4.	Examples	5
5.	IANA Considerations	5
5.1.	The 'turn' URI Scheme Registration	5
5.2.	The 'turns' URI Scheme Registration	6
6.	Security Considerations	6
7.	Acknowledgements	7
8.	References	8
8.1.	Normative References	8
8.2.	Informative References	8
	Authors' Addresses	9

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/turns' URI scheme is 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 also implies those endpoints and/or applications to be provisioned with appropriate configuration required to identify the TURN 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 'turn/turns' URI scheme helps alleviate most of these issues by providing a consistent way to describe, configure and exchange the information identifying a TURN 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 'turn/turns' 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 'turn' URI takes the following form (the syntax below is non-normative):

turn:<userinfo>@<host>:<port>

turns:<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 'turn' URI is defined as shown in the following Augmented Backus-Naur Form (ABNF) [[RFC5234](#)] rule:

```
turn-uri      = turn-scheme ":" [ userinfo "@" ] host [ ":" port ]
turn-scheme   = "turn"/"turns"
userinfo      = user [ ":" password ]
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.
password      = 1*(%x21-24 / %x26-3F / %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 TURN protocol supports sending messages over UDP, TCP or TLS-over-TCP. The 'turns' URI scheme SHALL be used when TURN is run over

TLS-over-TCP (or in the future DTLS-over-UDP) and the 'turn' scheme SHALL be used otherwise. The <host> part of the 'turn' URI, which is REQUIRED, denotes the TURN server host. The <userinfo> part, identifies the credential required for the long-term credential mechanism as described in the [section 10.2 of RFC 5389 \[RFC5389\]](#). The <port> part, if present, denotes the port on which the TURN server is awaiting connection requests. If it is absent, the default port SHALL be 3478 for both UDP and TCP. The default port for TURN over TLS SHALL be 5349.

[4.](#) Examples

URI to identify a long-term credential for the TLS-over-TCP connection to TURN server, example.com, on default port 5349:

```
turns:username:password@example.com
```

URI to identify a long-term credential for the connection to TURN server, example.com, on default port 3478:

```
turn:username:password@example.com
```

[5.](#) IANA Considerations

This document instructs IANA to register the 'turn' and 'turns' 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 'turn' URI Scheme Registration

IANA registration of the the 'turn' URI scheme:

URI scheme name: turn

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 'turn' URIs that are not described in [RFC 5766](#) [[RFC5766](#)].

Protocols that use the scheme: Traversal Using Relays around NAT (TURN)

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 'turns' URI Scheme Registration

IANA registration of the the 'turns' URI scheme:

URI scheme name: turns

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 'turns' URIs that are not described in [RFC 5766](#) [[RFC5766](#)].

Protocols that use the scheme: Traversal Using Relays around NAT (TURN) 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

The URI Scheme defined by this document for the Traversal Using Relays around NAT (TURN) protocol needs to consider the security considerations detailed in [Section 17 of RFC 5766](#) [[RFC5766](#)].

As described in [Section 3.2.1](#) of STD 66 [[RFC3986](#)], having authentication information (specifically passwords) in a URI means that the URI must be handled carefully:

The passing of authentication information in clear text has proven to be a security risk in almost every case where it has been used.

[Section 3.2.1](#) contains advice on handling URI that contain passwords in the userinfo portion. Implementations of this specification MUST implement that advice.

Specifically if a URI that contains credentials leaks, then it would

allow an attacker to use the TURN server which is referenced by the URI. Such an attack has two major impacts. First, it uses up the operator's bandwidth. Second, if the operator bills the user for TURN server usage, then it may expose the user to costs incurred by the attacker. However, the attacker never obtains the user's private information, nor does this attack allow for traffic amplification.

The expected use environment mitigates to some degree concerns about TURN URIs compared to other URIs, such as HTTPS. First, users do not dereference TURN URIs directly. Instead, they are passed to the TURN stack. Thus, concerns about confusion or leakage due to the URI being displayed to the user are significantly reduced; indeed the URI need never be available to the user at all.

One of the primary use cases for a TURN URI with credentials is WebRTC. In this case, a web server will be offering a calling service and may have an associated TURN server it can use. In this case, the browser will need to use the TURN server and the browser has no long term or preexisting relationship with the TURN server. The web server needs to provide some credential to the client which it can use to access the TURN server. Since TURN authentication is via username and password, this implies that the credential is a username/password pair. While this must be transmitted securely (i.e., over HTTPS), the security properties are the same whether the password is carried separately or is part of the URL. Moreover, because the web server and TURN servers can cooperate, a new password can be issued for every call, making short-term credentials feasible and thus significantly mitigating the risk.

If a TURN URI is transferred between hosts, it MUST be done over a protocol that provides confidentiality such as HTTPS [[RFC2818](#)]. It is RECOMMENDED that the credential only be valid for a single call and preferably for no more than one day. that "preferably" is bad.

[7.](#) Acknowledgements

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

[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 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.
- [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.

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.
- [RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", [RFC 5389](#), October 2008.
- [URIREG] Internet Assigned Numbers Authority (IANA) Registry, "Uniform Resource Identifier (URI) Schemes", [<http://www.iana.org/assignments/uri-schemes.html>](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>](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

