Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 11, 2009

M. Petit-Huguenin
8x8, Inc.

October 8, 2008

Traversal Using Relays around NAT (TURN) Uniform Resource Identifiers
draft-petithuguenin-behave-turn-uri-03

Status of this Memo

Abstract

This document defines two URI schemes and the resolution mechanism to convert these URIs to a list of server transport addresses that can be used between a Traversal Using Relays around NAT (TURN) client and server.

Table of Contents

1. Introduction 3
2. Terminology 3
3. Syntax of a TURN or TURNS URI 3
4. TURN or TURNS URI Resolution 4
5. Example 6
6. Security Considerations 6
7. IANA Considerations 7
7.1. TURN URI Registration 7
7.2. TURNS URI Registration 7
7.3. RELAY Application Service Tag Registration 8
7.4. turn.udp Application Protocol Tag Registration 8
7.5. turn.tcp Application Protocol Tag Registration 9
7.6. turn.tls Application Protocol Tag Registration 9
8. Running Code Considerations 10
9. Acknowledgements 10
10. References 10
10.1. Normative References 10
10.2. Informative References 11
Appendix A. Release notes 11
A.1. Modifications between -03 and -02 11
A.2. Modifications between -02 and -01 11
A.3. Modifications between -01 and -00 11
A.4. Design Notes 12
A.5. TODO List 12
Author's Address 12
Intellectual Property and Copyright Statements 13

1. Introduction

The TURN specification [I-D.ietf-behave-turn] defines a process for a TURN client to find TURN servers by using DNS SRV resource records, but this process does not let the TURN server administrators provision the preferred TURN transport protocol between the client and the server and for the TURN client to discover this preference. This document defines a S-NAPTR application [RFC3958] for this purpose. This application defines "RELAY" as application service tag and "turn.udp", "turn.tcp", and "turn.tls" as application protocol tags.

To simplify the provisioning of TURN clients, this document also defines a TURN and a TURNS URI scheme and a resolution mechanism to convert these URIs into a list of IP addresses, ports and TURN transport protocols.

Another usage of the resolution mechanism described in this document would be Remote Hosting as described in [RFC3958] section 4.4. For example a VoIP provider who does not want to deploy TURN servers could use the servers deployed by another company but could still want to provide configuration parameters to its customers without explicitly showing this relationship. The mechanism permits one to implement this indirection, without preventing the company hosting the TURN servers from manage them as it see fit.

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 [RFC2119].

3. Syntax of a TURN or TURNS URI

A TURN/TURNS URI has the following ABNF syntax [RFC5234]:

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

<host>, <port> and <unreserved> are specified in [RFC3986].

4. TURN or TURNS URI Resolution

The URI resolution algorithm uses <scheme>, <host>, <port> and <transport> as input. It also uses a list ordered by preference of TURN transports (UDP, TCP, TLS) supported by the application using the TURN client. The output of the algorithm is a list of {IP address, transport, port} tuples that a TURN client can try in order to contact a TURN server.

The resolution stops when a TURN client gets a successful Allocate response from a TURN server. After receiving a successful Allocate response, the resolution context MUST be discarded and the URI resolution algorithm MUST be restarted from the beginning for any subsequent allocation.

In some steps <transport> and <scheme> have to be converted to a TURN transport. If <scheme> is defined as "turn" and <transport> is defined as "udp" then the TURN UDP transport is used. If <scheme> is defined as "turn" and <transport> is defined as "tcp" then the TURN TCP transport is used. If <scheme> is defined as "turns" and <transport> is defined as "tcp" then the TURN TLS transport is used.

First the resolution algorithm checks that the URI can be resolved with the list of TURN transports supported:

- If <scheme> is defined as "turn" and <transport> is defined as "udp" but the list of TURN transports does not contain UDP then the resolution MUST stop with an error.
- If <scheme> is defined as "turn" and <transport> is defined as "tcp" but the list of TURN transports does not contain TCP or TLS then the resolution MUST stop with an error.
- If <scheme> is defined as "turns" and <transport> is defined as "udp" then the algorithm MUST stop with an error.
- If <scheme> is defined as "turns" and <transport> is defined as "tcp" but the list of TURN transports does not contain TLS then the resolution MUST stop with an error.
- If <scheme> is defined as "turns" and <transport> is not defined but the list of TURN transports does not contain TLS then the resolution MUST stop with an error.

Then the algorithm applies the following steps.

1. If <host> is an IP address then it indicates the specific IP address to be used. If <port> is not defined, the default port declared in [I-D.ietf-behave-turn] for the SRV service name defined in <scheme> is used. If <transport> is defined then <scheme> and <transport> are converted to a TURN transport as specified above. If <transport> is not defined, the TURN

transports supported by the application are tried by preference order. If the TURN client cannot contact a TURN server with this IP address and port on any of the transports then the resolution MUST stop with an error.

2. If <host> is a domain name and <port> is defined, then <host> is resolved to a list of IP addresses via DNS A and AAAA queries. If <transport> is defined then <scheme> and <transport> are converted to a TURN transport as specified above. If <transport> is not defined, the TURN transports supported by the application are tried by preference order. If the TURN client cannot contact a TURN server with this port and any combination of transports and resolved IP addresses then the resolution MUST stop with an error.
3. If <host> is a domain name and <port> is not defined but <transport> is defined then <host> is converted to a list of IP address and port tuples via a DNS SRV query as defined in [I-D.ietf-behave-turn] section 6.1. <scheme> is used for the service name and <transport> is used for the protocol name in the SRV algorithm [RFC2782]. If the TURN client cannot contact a TURN server at any of the IP address, port and transport tuples returned by the SRV algorithm then the resolution MUST stop with an error. The SRV algorithm recommends doing an A query if the SRV query returns an error or no SRV RR. In this case the default port declared in [I-D.ietf-behave-turn] for the SRV service name defined in <scheme> must be used for contacting the TURN server. Also in this case, this specification modifies the SRV algorithm by recommending an A or AAAA query.
4. If <host> is a domain name and <port> and <transport> are not defined, then <host> is converted to an ordered list of IP address, port and transport tuples via the S-NAPTR algorithm defined in [RFC3958] with a "RELAY" Application Service Tag. The TURN transports supported by the application are converted in Application Protocol Tags by using "turn.udp" if the TURN transport is UDP, "turn.tcp" if the TURN transport is TCP and "turn.tls" if the TURN transport is TLS. The order to try the protocol tags is provided by the ranking of the first set of NAPTR records. If multiple protocol tags have the same ranking, the preferred order set by the application is used. If the TURN client cannot contact a TURN server with any of the IP address, port and transport tuples returned by the S-NAPTR algorithm then the resolution MUST stop with an error. If the first NAPTR SRV query does not return any result then <host> is converted to a list of IP address and port tuples by using the algorithm specified in step 3 for each of the TURN transports supported by the application by order of preference.

5. Example

With the DNS RRs in Figure 1 and a preferred protocol list of {TLS, TCP, UDP}, the resolution algorithm will convert the "turn: example.com" URI to the list of IP addresses, port and protocol tuples in Table 1.

```
example.com.
IN NAPTR 100 10 "" "RELAY:turn.udp" "" datagram.example.com.
IN NAPTR 200 10 "" "RELAY:turn.tcp:turn.tls" "" stream.example.com.

datagram.example.com.
IN NAPTR 100 10 "S" "RELAY:turn.udp" "" _udp._turn.example.com.

stream.example.com.
IN NAPTR 100 10 "A" "RELAY:turn.tls" "" a.example.com.
IN NAPTR 200 10 "S" "RELAY:turn.tcp" "" _tcp._turn.example.com.

_udp._turn.example.com.
IN SRV   0   0  5000 a.example.com.

_tcp._turn.example.com.
IN SRV   0   0  5000 a.example.com.

a.example.com.
IN A     192.0.2.1
```

Figure 1

Order	Protocol	IP address	Port
1	UDP	192.0.2.1	5000
2	TLS	192.0.2.1	3478
3	TCP	192.0.2.1	5000

Table 1

6. Security Considerations

Security considerations for TURN are discussed in [I-D.ietf-behave-turn].

The Application Service Tag and Application Protocol Tags defined in

this document do not introduce any specific security issues beyond the security considerations discussed in [RFC3958].

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

7. IANA Considerations

7.1. TURN URI Registration

This section contains the registration information for the TURN URI scheme in accordance with [RFC4395].

URI scheme name: turn

Status: permanent

URI scheme syntax: See Section 3.

URI scheme semantics: See Section 4.

Encoding considerations: There are no encoding considerations beyond those in [RFC3986].

Applications/protocols that use this URI scheme name:

> The "turn:" URI is intended to be used by applications that might need access to a TURN server.

Interoperability considerations: N/A

Security considerations: See Section 6.

Contact: Marc Petit-Huguenin <petithug@8x8.com>

Author/Change controller: The IESG

References: This document.

7.2. TURNS URI Registration

This section contains the registration information for the TURNS URI scheme in accordance with [RFC4395].

URI scheme name: turns

Status: permanent

URI scheme syntax: See Section 3.

URI scheme semantics: See Section 4.

Encoding considerations: There are no encoding considerations beyond those in [RFC3986].

Applications/protocols that use this URI scheme name:

The "turn:" URI is intended to be used by applications that might need access to a TURN server.

Interoperability considerations: N/A

Security considerations: See Section 6.

Contact: Marc Petit-Huguenin <petithug@8x8.com>

Author/Change controller: The IESG

References: This document.

7.3. RELAY Application Service Tag Registration

This section contains the registration information for the RELAY Application Service Tag in accordance with [RFC3958].

Application Protocol Tag: RELAY

Intended usage: See Section 4.

Interoperability considerations: N/A

Security considerations: See Section 6.

Relevant publications: This document.

Contact information: Marc Petit-Huguenin <petithug@8x8.com>

Author/Change controller: The IESG

7.4. turn.udp Application Protocol Tag Registration

This section contains the registration information for the turn.udp Application Protocol Tag in accordance with [RFC3958].

Application Protocol Tag: turn.udp

Intended usage: See Section 4.

Interoperability considerations: N/A

Security considerations: See Section 6.

Relevant publications: This document.

Contact information: Marc Petit-Huguenin <petithug@8x8.com>

Author/Change controller: The IESG

7.5. turn.tcp Application Protocol Tag Registration

This section contains the registration information for the turn.tcp Application Protocol Tag in accordance with [RFC3958].

Application Protocol Tag: turn.tcp

Intended usage: See Section 4.

Interoperability considerations:

Security considerations: See Section 6.

Relevant publications: This document.

Contact information: Marc Petit-Huguenin <petithug@8x8.com>

Author/Change controller: The IESG

7.6. turn.tls Application Protocol Tag Registration

This section contains the registration information for the turn.tls Application Protocol Tag in accordance with [RFC3958].

Application Protocol Tag: turn.tls

Intended usage: See Section 4.

Interoperability considerations: N/A

Security considerations: See Section 6.

Relevant publications: This document.

Contact information: Marc Petit-Huguenin <petithug@8x8.com>

Author/Change controller: The IESG

8. Running Code Considerations

The SIP client of the free and open source Zap project [1] uses the resolution mechanism and TURN URI described in this document.

9. Acknowledgements

Thanks to Eilon Yardeni, Dan Wing, Alfred Hoenes and Jim Kleck for their comments, suggestions and questions that helped to improve this document.

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

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[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.

[I-D.ietf-behave-turn] Rosenberg, J., Mahy, R., and P. Matthews, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", draft-ietf-behave-turn-10 (work in progress), September 2008.

10.2. Informative References

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC3958] Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)", RFC 3958, January 2005.

[RFC4395] Hansen, T., Hardie, T., and L. Masinter, "Guidelines and Registration Procedures for New URI Schemes", BCP 115, RFC 4395, February 2006.

URIs

[1] <http://www.croczilla.com/zap>

Appendix A. Release notes

This section must be removed before publication as an RFC.

A.1. Modifications between -03 and -02

- Added Running Code Consideration section.
- Added Remote Hosting example in introduction.
- Changed back to opaque URIs because of [RFC4395] Section 2.2. Now use "?" as separator.
- Added IANA considerations section.
- Added security considerations section.

A.2. Modifications between -02 and -01

- Receiving a successful Allocate response stops the resolution mechanism and the resolution context must be discarded after this.
- Changed from opaque to hierarchical URIs because the ";" character is used in <reg-name>.
- Various nits.

A.3. Modifications between -01 and -00

- Added <transport-ext> in the ABNF.
- Use the <rulename> and "literal" usages for free-form text defined by [RFC5234].
- Fixed various typos.
- Put the rule to convert <scheme> and <transport> to a TURN transport in a separate paragraph.

- Modified the SRV usage to be in line with RFC 2782.
- Clarified that the NAPTR protocol ranking must be used before the application ranking.
- Added an example.
- Added release notes.

A.4. Design Notes

- The Application Service Tag is "RELAY" so other relaying mechanisms (e.g. TWIST) than TURN can be registered as Application Protocol Tags.
- S-NAPTR was preferred to U-NAPTR because there is no use case for U-NAPTR.
- <password> is not used in the URIs because it is deprecated. <username> is not used in the URIs because it is not used to guide the resolution mechanism.
- As discussed in Dublin, there is no generic parameters in the URI to prevent compatibity issues.
- Adding optional capabilities (IPv6 allocation, preserve bit, etc...) in the resolution process was rejected at the Dublin meeting.

A.5. TODO List

(Empty)

Author's Address

Marc Petit-Huguenin
8x8, Inc.
3151 Jay Street
Santa Clara, CA 95054
US

Phone: +1 408 654 0875
Email: marc@8x8.com

Full Copyright Statement

Intellectual Property