Network Working Group	M. Petit-Huguenin
Internet-Draft	(Unaffiliated)
Intended status: Standards Track	March 01, 2010
Expires: September 2, 2010	

TOC

Traversal Using Relays around NAT (TURN) Resolution Mechanism
draft-ietf-behave-turn-uri-10

Abstract

This document defines a resolution mechanism to generate a list of server transport addresses that can be tried to create a Traversal Using Relays around NAT (TURN) allocation.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

TOC

The TURN specification (Rosenberg, J., Mahy, R., and P. Matthews, “Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN),” July 2009.) [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 does not allow the TURN client to discover this preference. This document defines an S-NAPTR application (Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” January 2005.) [RFC3958] for this purpose. This application defines "RELAY" as an application service tag and "turn.udp", "turn.tcp", and "turn.tls" as application protocol tags.

Another usage of the resolution mechanism described in this document would be Remote Hosting as described in [RFC3958] (Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” January 2005.) 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 managing them as it sees fit.

[TURN-URI] (Petit-Huguenin, M., “Traversal Using Relays around NAT (TURN) Uniform Resource Identifiers,” February 2010.) can be used as a convenient way of carrying the four components needed by the resolution mechanism described in this document. A reference implementation is available [REF-IMPL] (Petit-Huguenin, M., “Reference Implementation of TURN resolver and TURN URI parser,” January 2010.).

2. Terminology

TOC

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

3. Resolution Mechanism

TOC

The resolution mechanism is used only to create an allocation. All other transactions use the IP address, transport and port used for a successful allocation creation. The resolution mechanism only selects the transport used between the TURN client and the TURN server. The transport used by the allocation itself is selected by the REQUESTED-TRANSPORT attribute as described in section 6.1 of [TURN] (Rosenberg, J., Mahy, R., and P. Matthews, “Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN),” July 2009.).

The resolution algorithm uses a boolean flag, <secure>; an IP address or domain name, <host>; a port number that can be empty, <port>; and a transport name that can be "udp", "tcp" or empty, <transport> as input. This four parameters are part of the user configuration of the TURN client. The resolution mechanism also uses as input a list ordered by preference of TURN transports (UDP, TCP, TLS) supported that is provided by the application using the TURN client. This list reflects the capabilities and preferences of the application code that is using the S-NAPTR resolver and TURN client, as opposed to the configuration parameters that reflect the preferences of the user of the application. The output of the algorithm is a list of {IP address, transport, port} tuples that a TURN client can try in order to create an allocation on a TURN server.

An Allocate error response as specified in section 6.4 of [TURN] (Rosenberg, J., Mahy, R., and P. Matthews, “Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN),” July 2009.) is processed as a failure as specified by [RFC3958] (Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” January 2005.) section 2.2.4. The resolution stops when a TURN client gets a successful Allocate response from a TURN server. After an allocation succeeds or all the allocations fail, the resolution context MUST be discarded and the resolution algorithm MUST be restarted from the beginning for any subsequent allocation. Servers blacklisted as described in section 6.4 of [TURN] (Rosenberg, J., Mahy, R., and P. Matthews, “Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN),” July 2009.) MUST NOT be used for the specified duration even if returned by a subsequent resolution.

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

- If <secure> is false and <transport> is defined as "udp" but the list of TURN transports supported by the application does not contain UDP then the resolution MUST stop with an error.

- If <secure> is false and <transport> is defined as "tcp" but the list of TURN transports supported by the application does not contain TCP then the resolution MUST stop with an error.

- If <secure> is true and <transport> is defined as "udp" then the algorithm MUST stop with an error.

- If <secure> is true and <transport> is defined as "tcp" but the list of TURN transports supported by the application does not contain TLS then the resolution MUST stop with an error.

*If <secure> is true and <transport> is not defined but the list of TURN transports supported by the application does not contain TLS then the resolution MUST stop with an error.

*If <transport> is defined but unknown then the resolution MUST stop with an error.

After verifying the validity of the parameters, the algorithm filters the list of TURN transports supported by the application by removing the UDP and TCP TURN transport if <secure> is true. If the list of TURN transports is empty after this filtering, the resolution MUST stop with an error.

After filtering the list of TURN transports supported by the application, the algorithm applies the steps described below. Note that in some steps, <secure> and <transport> have to be converted to a TURN transport. If <secure> is false and <transport> is defined as "udp" then the TURN UDP transport is used. If <secure> is false and <transport> is defined as "tcp" then the TURN TCP transport is used. If <secure> is true and <transport> is defined as "tcp" then the TURN TLS transport is used. This is summarized in Table 1.

<secure>	<transport>	TURN Transport
false	"udp"	UDP
false	"tcp"	TCP
true	"tcp"	TLS

Table 1

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 [TURN] (Rosenberg, J., Mahy, R., and P. Matthews, “Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN),” July 2009.) for the "turn" SRV service name if <secure> is false, or the "turns" SRV service name if <secure> is true MUST be used for contacting the TURN server. If <transport> is defined then <secure> and <transport> are converted to a TURN transport as specified in Table 1. If <transport> is not defined, the filtered 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 supported by the application 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 <secure> and <transport> are converted to a TURN transport as specified in Table 1. If <transport> is not defined, the filtered TURN transports supported by the application are tried in preference order. The TURN client can choose the order to contact the resolved IP addresses in any implementation-specific way. If the TURN client cannot contact a TURN server with this port, the transport or list of transports, and the 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 the SRV algorithm defined in [RFC2782] (Gulbrandsen, A., Vixie, P., and L. Esibov, “A DNS RR for specifying the location of services (DNS SRV),” February 2000.) is used to generate a list of IP address and port tuples. <host> is used as Name, a value of false for <secure> as "turn" for Service, a value of true for <secure> as "turns" for Service and <transport> as Protocol in the SRV algorithm. <secure> and <transport> are converted to a TURN transport as specified in Table 1 and this transport is used with each tuple for contacting the TURN server. 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 [TURN] (Rosenberg, J., Mahy, R., and P. Matthews, “Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN),” July 2009.) for the "turn" SRV service name if <secure> is false, or the "turns" SRV service name if <secure> is true MUST be used for contacting the TURN server. Also in this case, this specification modifies the SRV algorithm by recommending an A and AAAA query. If the TURN client cannot contact a TURN server at any of the IP address and port tuples returned by the SRV algorithm with the transport converted from <secure> and <transport> then the resolution MUST stop with an error.

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] (Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” January 2005.) by using <host> as the initial target domain name and "RELAY" as the Application Service Tag. The filtered list of 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 Application Protocol Tags is provided by the ranking of the first set of NAPTR records. If multiple Application Protocol Tags have the same ranking, the preferred order set by the application is used. If the first NAPTR query fails, the processing continues in step 5. 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.

5. If the first NAPTR query in the previous step does not return any result then the SRV algorithm defined in [RFC2782] (Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)," February 2000.) is used to generate a list of IP address and port tuples. The SRV algorithm is applied by using each transport in the filtered list of TURN transports supported by the application for the Protocol, <host> for the Name, "turn" for the Service if <secure> is false or "turns" for the Service if <secure> is true. The same transport that was used to generate a list of tuples is used with each of these tuples for contacting the TURN server. 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 [TURN] (Rosenberg, J., Mahy, R., and P. Matthews, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)," July 2009.) for the "turn" SRV service name if <secure> is false, or the "turns" SRV service name if <secure> is true MUST be used for contacting the TURN server. Also in this case, this specification modifies the SRV algorithm by recommending an A and AAAA query. If the TURN client cannot contact a TURN server at any of the IP address and port tuples returned by the SRV algorithm with the transports from the filtered list then the resolution MUST stop with an error.

4. Examples

TOC

TOC

4.1. Multiple Protocols

With the DNS RRs in Figure 1 and an ordered TURN transport list of {TLS, TCP, UDP}, the resolution algorithm will convert the parameters <secure> with a value of false, <host> with a value of "example.net" and <port> and <transport> been empty to the list of IP addresses, port and protocol tuples in Table 2.

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

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

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

_turn._udp.example.net.
IN SRV   0 0 3478 a.example.net.

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

a.example.net.
IN A     192.0.2.1
```

Figure 1

Order	Protocol	IP address	Port
1	UDP	192.0.2.1	3478
2	TLS	192.0.2.1	5349
3	TCP	192.0.2.1	5000

Table 2

4.2. Remote Hosting

TOC

In the example in Figure 2, a VoIP provider (example.com) is using the TURN servers managed by the administrators of the example.net domain (defined in Figure 1). The resolution algorithm using the ordered TURN transport list of {TLS, TCP, UDP} would convert the same parameters than in the previous example but with the <host> parameter equal to "example.com" to the list of IP addresses, port and protocol tuples in Table 2.

```
     example.com.
     IN NAPTR 100 10 "" RELAY:turn.udp:turn.tcp:turn.tls "" example.net.
```

Figure 2

4.3. Compatibility with TURN

TOC

In deployments where it is not possible to guarantee that all TURN clients will support the resolution mechanism described in this document, the DNS configuration should be done in a way that works with both this resolution mechanism and the mechanism described in [TURN] (Rosenberg, J., Mahy, R., and P. Matthews, “Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN),” July 2009.). The DNS RRs in Figure 3 can be used in conjunction with the DNS RRs in Figure 1 and Figure 2 for this purpose.

```
     _turn._udp.example.com.
     IN SRV   0 0 3478 a.example.net.

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

     _turns._tcp.example.com.
     IN SRV   0 0 5349 a.example.net.
```

Figure 3

5. Security Considerations

TOC

Security considerations for TURN are discussed in [TURN] (Rosenberg, J., Mahy, R., and P. Matthews, “Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN),” July 2009.).

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] (Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” January 2005.).

[RFC3958] (Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” January 2005.) requests that an S-NAPTR application defines some form of end-to-end authentication to ensure that the correct destination has been reached. This is achieved by the Long-Term Credential Mechanism defined in [RFC5389], which is mandatory for [TURN] (Rosenberg, J., Mahy, R., and P. Matthews, “Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN),” July 2009.).

Additionally the usage of TLS (Dierks, T. and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” August 2008.) [RFC5246] has the capability to address the requirement. In this case the client MUST verify the identity of the server by following the identification procedure in section 7.2.2 of [RFC5389] (Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, “Session Traversal Utilities for NAT (STUN),” October 2008.) and by using the value of the <host> parameter as the identity of the server to be verified.

An implication of this is that the server's certificate could need to be changed when SRV or NAPTR records are added. For example, a client using just A/AAAA records, and configured with "turnserver.example.net", expects to find the name "turnserver.example.net" in the certificate. If a second client uses SRV records and is configured with <host> parameter "example.com", it expects to find "example.com" in the certificate, even if the SRV record at _turns._tcp.example.com points to turnserver.example.net.

TOC

6. IANA Considerations

This section contains the registration information for one S-NAPTR Application Service Tag and three S-NAPTR Application Protocol Tags (in accordance with [RFC3958] (Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” January 2005.)).

6.1. RELAY Application Service Tag Registration

TOC

Application Protocol Tag: RELAY
Intended usage: See Section 3 (Resolution Mechanism).
Interoperability considerations: N/A
Security considerations: See Section 5 (Security Considerations).
Relevant publications: This document.
[Note to RFC Editor: Replace "This document" with reference to this document]
Contact information: Marc Petit-Huguenin <petithug@acm.org>
Author/Change controller: The IESG

6.2. turn.udp Application Protocol Tag Registration

TOC

Application Protocol Tag: turn.udp
Intended usage: See Section 3 (Resolution Mechanism).
Interoperability considerations: N/A
Security considerations: See Section 5 (Security Considerations).
Relevant publications: This document.
[Note to RFC Editor: Replace "This document" with reference to this document]
Contact information: Marc Petit-Huguenin <petithug@acm.org>
Author/Change controller: The IESG

6.3. turn.tcp Application Protocol Tag Registration

TOC

Application Protocol Tag: turn.tcp
Intended usage: See Section 3 (Resolution Mechanism).
Interoperability considerations:
Security considerations: See Section 5 (Security Considerations).
Relevant publications: This document.
[Note to RFC Editor: Replace "This document" with reference to this document]

Contact information: Marc Petit-Huguenin <petithug@acm.org>
Author/Change controller: The IESG

6.4. turn.tls Application Protocol Tag Registration

TOC

Application Protocol Tag: turn.tls
Intended usage: See Section 3 (Resolution Mechanism).
Interoperability considerations: N/A
Security considerations: See Section 5 (Security Considerations).
Relevant publications: This document.
[Note to RFC Editor: Replace "This document" with reference to this document]
Contact information: Marc Petit-Huguenin <petithug@acm.org>
Author/Change controller: The IESG

7. Acknowledgements

TOC

Thanks to Cullen Jennings, Alexey Melnikov, Scott Bradner, Spencer Dawkins, Pasi Eronen, 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 their comments, suggestions and questions that helped to improve this document.
This document was written with the xml2rfc tool described in [RFC2629] (Rose, M., “Writing I-Ds and RFCs using XML,” June 1999.).

8. References

TOC

8.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2782]	Gulbrandsen, A., Vixie, P., and L. Esibov, “A DNS RR for specifying the location of services (DNS SRV),” RFC 2782, February 2000 (TXT).
[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 (TXT).
[RFC5246]	Dierks, T. and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” RFC 5246, August 2008 (TXT).
[RFC5389]	Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, “Session Traversal Utilities for NAT (STUN),” RFC 5389, October 2008 (TXT).
[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-16 (work in progress), July 2009 (TXT).

8.2. Informative References

TOC

[RFC2629]	Rose, M., “Writing I-Ds and RFCs using XML,” RFC 2629, June 1999 (TXT, HTML, XML).
[TURN-URI]	Petit-Huguenin, M., “Traversal Using Relays around NAT (TURN) Uniform Resource Identifiers,” draft-petithuguenin-behave-turn-uri-bis-01 (work in progress), February 2010 (TXT).
[REF-IMPL]	Petit-Huguenin, M., “Reference Implementation of TURN resolver and TURN URI parser,” January 2010.

Appendix A. Release notes

TOC

This section must be removed before publication as an RFC.

A.1. Modifications between ietf-10 and ietf-09

TOC

- Clarified that the resolution mechanism is for choosing the transport between the TURN client and the TURN server, not the transport used by the allocation.

A.2. Modifications between ietf-09 and ietf-08

TOC

- Clarified that the identity to use for server certificate verification is <host>

- *Moved the reference implementation reference to the informative references and changed the URL to something more stable.

A.3. Modifications between ietf-08 and ietf-07

TOC

- *Added reference to TLS RFC.
- *Removed usused references.
- *Fixed reference to URI.

A.4. Modifications between ietf-07 and ietf-06

TOC

- *Clarified "application code" meaning.

A.5. Modifications between ietf-06 and ietf-05

TOC

- *Updated the short title to "TURN Resolution".
- *Shorten I-D references.
- *Nits
- *Changed SHOULD NOT to MUST NOT for blacklist rule.
- *Added notes to RFC editor.

A.6. Modifications between ietf-05 and ietf-04

TOC

- *Moved the URI stuff to [TURN-URI] (Petit-Huguenin, M., “Traversal Using Relays around NAT (TURN) Uniform Resource Identifiers,” February 2010.).

A.7. Modifications between ietf-04 and ietf-03

TOC

- Improved the algorithm steps.

- It is possible to use a TLS transport event if the scheme is turn:.

- Clarified when to stop the resolution with an error in step 2.

- Added transport list filtering process.

- Improved security section following sec-dir review.

- Fixed nits reported by gen-art review.

- Added example for remote hosting.

- Removed URIs section.

- Editorial modification.

A.8. Modifications between ietf-03 and ietf-02

TOC

- A turn:<host>?transport=TCP URI fails if the list of supported transports contains only TLS. Using a TLS transport in this case was underspecified.

- Reordered paragraphes in section 4.

- Added table for conversion of <scheme> and <transport> to TURN transport.

- Various editorial modifications.

- SRV algorithm changed to "...recommending an A and AAAA query."

- Put back the changelog for the versions before been accepted as WG item.

A.9. Modifications between ietf-02 and ietf-01

TOC

- Shorten the abstract so it does not overflow on the second page.

- *Added text to explicitly say that the resolution is only to create an allocation.

- *Added text about failures.

- *Fixed the default port for TLS in the example.

- *Changed some priority in the example for RFC3958 section 2.2.5.

- *Fixed the service/protocol order for the SRV RR in the example.

- *Removed reference to draft-wood-tae-specifying-uri-transports as it has an experimental status.

A.10. Modifications between ietf-01 and ietf-00

TOC

- *Fixed the contact email.

- *Changed the IPR to trust200902.

- *Added case for transport defined but unknown.

- *Moved RFC 3958 to Normative References.

- *Added study of draft-wood-tae-specifying-uri-transports in TODO list.

A.11. Modifications between ietf-00 and petithuguenin-03

TOC

- *Renamed the document to "draft-ietf-behave-turn-uri".

- *Changed author affiliation.

- *Fixed the text in the IANA considerations.

A.12. Modifications between petithuguenin-03 and petithuguenin-02

TOC

- *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.13. Modifications between petithuguenin-02 and petithuguenin-01

TOC

- *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.14. Modifications between petithuguenin-01 and petithuguenin-00

TOC

- *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.15. Design Notes

TOC

- The Application Service Tag is "RELAY" so other relaying mechanisms than TURN (e.g., TWIST) can be registered as Application Protocol Tags.
- S-NAPTR was preferred to U-NAPTR because there is no use case for U-NAPTR.
- Adding optional capabilities (IPv6 allocation, preserve bit, etc...) in the resolution process was rejected at the Dublin meeting.

Author's Address

TOC

Marc Petit-Huguenin
(Unaffiliated)
Email: petithug@acm.org