

Network Working Group	C. Bran
Internet-Draft	Plantronics
Intended status: Standards Track	M.K. Kaufman
Expires: May 02, 2012	Skype
	C. Jennings
	Cisco
	J.R. Rosenberg
	Skype
	October 30, 2011

WebRTC Network Address Translation
draft-cbran-rtcweb-nat-02

Abstract

This document outlines the network address translation (NAT) traversal requirements and for WebRTC client applications.

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 May 02, 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.

This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

Table of Contents

- *1. [Introduction](#)
- *2. [Terminology](#)
- *3. [Connection Management Requirements](#)
 - *3.1. [NAT Traversal Requirements](#)
 - *3.2. [Data Transmission Requirements](#)
 - *3.3. [IPv4 to IPv6 Transition Requirements](#)
 - *3.4. [Legacy Phone System Interoperability Requirements](#)
- *4. [Connection Management Mechanism](#)
 - *4.1. [ICE](#)
 - *4.1.1. [ICE as a Consent Mechanism](#)
 - *4.2. [Web Browsers and ICE](#)
 - *4.2.1. [Native ICE Support](#)
 - *4.2.2. [STUN Configuration](#)
- *5. [IANA Considerations](#)
- *6. [Security Considerations](#)
- *7. [Acknowledgements](#)
- *8. [References](#)
- *[Authors' Addresses](#)

1. Introduction

An integral part of the of the Web Real Time Communications (WebRTC) will be the ability for client application implementations to have native, secure Network Address Translation (NAT) [\[RFC1631\]](#) traversal capabilities. This document provides requirements and implementation specifications WebRTC client NAT traversal.

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. Connection Management Requirements

This section identifies the requirements for RTC-Web client applications to connection requirements.

3.1. NAT Traversal Requirements

A majority of WebRTC clients will be web browsers and used behind a NAT and or firewall. WebRTC clients will use a UDP-based data transmission scheme for multimedia sessions [Open Issue: what draft should be cited for this requirement?]. UDP has well know NAT traversal problems and without native capabilities to traverse a NAT, WebRTC clients will be extremely limited in their functionality. Fortunately NAT traversal for UDP is a solved problem, but solutions require that clients transmitting media between each other need to use the same NAT traversal algorithms. Without a consistent, well specified NAT traversal mechanism WebRTC client implementations would likely be inoperable with each other. To address the identified problems WebRTC clients are REQUIRED to implement the NAT traversal mechanism as defined in [Section 4](#).

3.2. Data Transmission Requirements

Whenever a calling WebRTC client attempts to establish a connection, the receiving WebRTC client MUST provide consent before the calling client can transmit data to the receiver. Providing consent on the receiving end before data transmission commence is needed to help to prevent malicious attacks by the calling client. All WebRTC clients are REQUIRED to implement connection management that provides a consent mechanism for media transmission. Furthermore it is REQUIRED that consent be given by the recipient before an WebRTC client can transmit media.

As a note providing consent to open a media connection does not involve user-level consent, rather it is the responsibility of the WebRTC client application (e.g. web browser) to enforce this requirement.

3.3. IPv4 to IPv6 Transition Requirements

RTC-Web clients MUST support IPv4 to IPv6 transition.

3.4. Legacy Phone System Interoperability Requirements

There is no way to meet all the connection management requirements and maintain compatibility with all legacy phone systems. It is highly desirable that the WebRTC connection management mechanism be interoperable with legacy phone systems such as a VOIP endpoints, PSTN gateways and SIP trunks.

4. Connection Management Mechanism

This section specifies the connection management system that will address the identified requirements.

4.1. ICE

To address the NAT traversal, data transmission, and interoperability requirements all WebRTC client applications are REQUIRED to implement ICE [\[RFC5245\]](#). Implicit to ICE, and listed here for clarity, WebRTC client implementations will are also REQUIRED to implement STUN [\[RFC3489\]](#) and TURN [\[RFC5766\]](#).

Additional ICE requirements:

- *Support of ICE's Aggressive Nomination is REQUIRED

- *Support of ICE's Regular Nomination is OPTIONAL

- *WebRTC media gateways MAY implement ICE-Lite instead of full ICE

4.1.1. ICE as a Consent Mechanism

Of the connection management requirements listed above, the least obvious is how ICE will satisfy being a consent mechanism for data transmission [Section 3.2](#). The reason ICE can satisfy this requirement is due to its reliance on STUN transactions to succeed in order to establish a connection. The success of a STUN transaction can be viewed as semantically the same thing as a recipient providing consent to transmit data. Conversely the failure of the STUN transaction would semantically map to the recipient rejecting the request to transmit data.

4.2. Web Browsers and ICE

This section specifies the web browser implementation requirements for WebRTC client connection management.

4.2.1. Native ICE Support

To meet the WebRTC connectivity requirements, web browser vendors MUST natively support ICE [\[RFC5245\]](#). Access to the web browser's ICE implementation will be defined in the W3C WebRTC-API specification[\[I.D.w3c-webrtc\]](#).

Alternate proposals have been made that advocate for natively exposing STUN[\[RFC3489\]](#) APIs in the web browser. The ICE implementation would be realized via a JavaScript library that uses the browser's native STUN API. After reviewing the alternate proposals the solution several issues were identified.

1. JavaScript running within "real world" web applications cannot reliably handle the ICE timing and pacing requirements. An example of this is long running JavaScript code from embedded advertisers. A big JavaScript file can take a significant amount of time to execute and can prevent web application timers from firing in correctly. Given the pacing requirements for ICE are in the 20ms range, it is highly likely that ICE will break if it is implemented in a JavaScript library.
2. Multiple implementations of a JavaScript ICE library is a logistical nightmare. Coordinating updates, bug fixes, enhancements and a testing matrix for interoperability at Internet scale will simply be impossible.

4.2.2. STUN Configuration

Web browsers MUST provide a mechanism to configure access to a STUN server.

Below are some proposed mechanisms by which the STUN server could be configured:

- *A preference page, similar to the what web browser's use for configuring web proxy settings

- *Exposed as a JavaScript API and added to the W3C WebRTC-API specification

Regardless of the mechanism adopted by the web browser vendor, the following configuration data is REQUIRED to be exposed and settable through the web browsers configuration mechanism:

- *STUN Server Address - the IPv4 or IPv6 address of the STUN server

- *STUN Server Port

- *Credentials to access the STUN server (these are not STUN generated credentials)

5. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

6. Security Considerations

To guard against spoofing RTC-Web client applications are REQUIRED to:

- *Internally encapsulate the generation of STUN transaction IDs

*Block read/write access to the generated STUN transaction IDs

7. Acknowledgements

This draft incorporates ideas and text from the IETF mailing list. In particular we would like to acknowledge, and say thanks for, work we incorporated from Timothy Terriberry and Christopher Blizzard.

8. References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels" , BCP 14, RFC 2119, March 1997.
[RFC5245]	Rosenberg, J., " Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols ", RFC 5245, April 2010.
[RFC3489]	Rosenberg, J., Weinberger, J., Huitema, C. and R. Mahy, " STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) ", RFC 3489, March 2003.
[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.
[I.D.w3c-webrtc]	Bergkvist, A., Burnett, D.C., Jennings, C. and A. Narayanan, "WebRTC 1.0: Real-time Communication Between Browsers", October 2011.

Authors' Addresses

Cary Bran Bran Plantronics 345 Encinal Street Santa Cruz, CA 95060
USA Phone: +1 206 661-2398 EMail: cary.bran@plantronics.com

Matthew Kaufman Kaufman Skype 3210 Porter Drive Palo Alto,
California 94304 US Phone: +1 831 440 8771 EMail:
matthew.kaufman@skype.net

Cullen Jennings Jennings Cisco 170 West Tasman Drive San Jose, CA
95134 USA Phone: +1 408 421-9990 EMail: fluffy@cisco.com

Jonathan Rosenberg Rosenberg Skype 3210 Porter Drive Palo Alto,
California 94304 US EMail: jdrosen@skype.net