

RTCWEB  
Internet-Draft  
Intended status: Informational  
Expires: November 10, 2013

T. Reddy  
Cisco  
J. Kaippallimalil  
Huawei  
Ram. Mohan. Ravindranath  
Cisco  
R. Ejzak  
Alcatel-Lucent  
May 09, 2013

Considerations with WebRTC in Mobile Networks  
draft-reddy-rtcweb-mobile-03

## Abstract

This document discusses some of the issues with WebRTC applications in Mobile Networks.

## 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 November 10, 2013.

## Copyright Notice

Copyright (c) 2013 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.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction . . . . .</a>	<a href="#">2</a>
<a href="#">2.</a>	<a href="#">Notational Conventions . . . . .</a>	<a href="#">3</a>
<a href="#">3.</a>	<a href="#">Scope . . . . .</a>	<a href="#">3</a>
<a href="#">4.</a>	<a href="#">Cellular Networks - QOS . . . . .</a>	<a href="#">3</a>
<a href="#">4.1.</a>	<a href="#">RTP Session Multiplexing . . . . .</a>	<a href="#">4</a>
<a href="#">4.1.1.</a>	<a href="#">Disable RTP Multiplexing . . . . .</a>	<a href="#">5</a>
<a href="#">4.1.2.</a>	<a href="#">Extend Packet Filter to include RTP SSRC . . . . .</a>	<a href="#">5</a>
<a href="#">4.1.3.</a>	<a href="#">Extend Packet Filter to include RTP payload type . . . . .</a>	<a href="#">6</a>
<a href="#">4.1.4.</a>	<a href="#">Data Channel multiplexed with RTP . . . . .</a>	<a href="#">6</a>
<a href="#">4.2.</a>	<a href="#">Bearer Resource Modification triggered by UE . . . . .</a>	<a href="#">7</a>
<a href="#">4.3.</a>	<a href="#">WebRTC server deployed in 3GPP Network . . . . .</a>	<a href="#">8</a>
4.4.	WebRTC server deployed in a 3rd party network trusted by Mobile Network . . . . .	<a href="#">8</a>
<a href="#">4.5.</a>	<a href="#">Deep Packet Inspection . . . . .</a>	<a href="#">8</a>
<a href="#">5.</a>	<a href="#">Mobility . . . . .</a>	<a href="#">9</a>
<a href="#">5.1.</a>	<a href="#">3GPP SIPTO . . . . .</a>	<a href="#">9</a>
<a href="#">5.2.</a>	<a href="#">IPv4 traffic offload for Proxy Mobile IPv6 . . . . .</a>	<a href="#">10</a>
<a href="#">5.3.</a>	<a href="#">IPv6 Prefix with Mobility . . . . .</a>	<a href="#">11</a>
<a href="#">6.</a>	<a href="#">Security Considerations . . . . .</a>	<a href="#">11</a>
<a href="#">7.</a>	<a href="#">IANA Considerations . . . . .</a>	<a href="#">11</a>
<a href="#">8.</a>	<a href="#">Acknowledgments . . . . .</a>	<a href="#">12</a>
<a href="#">9.</a>	<a href="#">Informative References . . . . .</a>	<a href="#">12</a>
<a href="#">Appendix A.</a>	<a href="#">OS Support . . . . .</a>	<a href="#">14</a>
	<a href="#">Authors' Addresses . . . . .</a>	<a href="#">16</a>

## [1.](#) Introduction

The use of cellular broadband for accessing the Internet and other data services via smartphones, tablets, and notebook/netbook computers has increased rapidly as a result of high-speed packet data networks such as HSPA and HSPA+; and now Long-Term Evolution (LTE) is being deployed. Browsers on these devices are becoming similar in capability to their desktop counterparts. So, from that perspective, it is feasible to run WebRTC applications in them. This draft enumerates concerns when real time applications like WebRTC are used on such devices in the above listed networks.

This note focuses on QOS and traffic offload aspects, and does not

address other mobile network related topics like power consumption, interface switching and congestion control related issues already being discussed in [[I-D.isomaki-rtcweb-mobile](#)].

## [2.](#) Notational Conventions

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](#)].

This note uses terminology defined in [[RFC6459](#)]

UE, MS, MN, and Mobile : The terms UE (User Equipment), MS (Mobile Station), MN (Mobile Node), and mobile refer to the devices that are hosts with the ability to obtain Internet connectivity via a 3GPP network.

WebRTC Server : Web Server which supports WebRTC.

## [3.](#) Scope

This document can be used as a tool to design solution(s) for WebRTC QoS and traffic offload in cellular broadband networks. It describes key use cases, factors common to the use cases, and key solution elements. This note aids WebRTC server designers and network architects to facilitate proper deployment of WebRTC in mobile networks. The WebRTC server could either be deployed in the Mobile Network, in a 3rd party network trusted by the Mobile Network, or in a public network as a Public WebRTC server.

## [4.](#) Cellular Networks - QoS

3GPP has standardized QoS for EPC (Enhanced Packet Core) from Release 8 [[TS23.107](#)]. 3GPP QoS policy configuration defines access agnostic QoS parameters that can be used to provide service differentiation in multi vendor and operator deployments. The concept of a bearer is used as the basic construct for which QoS treatment is applied for uplink and downlink packet flows between the MN and gateway [[TS23.401](#)]. A bearer may have more than one packet filter associated and this is called a Traffic Flow Template (TFT). IP source address,

source port, IP destination, destination port, L4 protocol, Type of service/Traffic class type, Security parameter index etc identify a packet filter. Each MN can have one or multiple bearers associated with its registration, each supporting different QoS characteristics. An UpLink Traffic Flow Template (UL TFT) is the set of uplink packet filters in a TFT. A DownLink Traffic Flow Template (DL TFT) is the set of downlink packet filters in a TFT.

The access agnostic QoS parameters associated with each bearer are QCI (QoS Class Identifier), ARP (Allocation and Retention Priority), MBR (Maximum Bit Rate) and optionally GBR (Guaranteed Bit Rate). QCI is a scalar that defines packet forwarding criteria in the network.

Mapping of QCI values to DSCP is well understood and GSMA has defined standard means of mapping between these scalars [[GSMA-IR34](#)]. Primarily LTE offers two types of bearer: Guaranteed Bit rate bearer for real time communication, e.g., Voice calls etc. and Non-Guaranteed bit rate bearer, e.g., best effort traffic for web access etc. Packets mapped to the same EPS bearer receive the same bearer level packet forwarding treatment.

The Web Real-Time communication (WebRTC) [[I-D.ietf-rtcweb-overview](#)] framework provides the protocol building blocks to support direct, interactive, real-time communication using audio, video, collaboration, games, etc., between two peers' web-browsers. WebRTC application would use Interactive Connectivity Establishment (ICE) protocol [[RFC5245](#)] for gathering candidates, prioritizing them, choosing default ones, exchanging them with the remote party, pairing them and ordering them into check lists. Once all of the above have been completed then the participating ICE agents can begin a phase of connectivity checks and eventually select the pair of candidates that will be used for real-time communication.

The following subsections describe different aspects of QoS for WebRTC application in a 3GPP Network.

#### [4.1](#). RTP Session Multiplexing

[I-D.ietf-rtcweb-rtp-usage] in [section 4.4](#) suggests to put interactive audio and interactive video over the same 5-tuple {dest addr, source addr, protocol, dest port, source port}. Without special handling, the same QoS treatment will be applied to the audio

and video flows in the 5-tuple. One potential solution is for the endpoints to set DSCP appropriately on a per-packet basis, as proposed in [[I-D.dhesikan-tsvwg-rtcweb-qos](#)]. The packet filters in UL TFT and DL TFT created for each media stream must also include DSCP values, so that multiplexed upstream and downstream traffic is separated and mapped to the correct bearer. That means that there could be multiple bearers (packet filters) with the same 5-tuple but with different DSCP values.

In all cases where the browser multiplexes different priority media flows on a single 5-tuple and RTP session, the browser should ensure that the RTCP packets for each media flow receive the same or better priority as the corresponding RTP packets. One way for the browser to ensure this is to construct compound RTCP packets only with RTCP packets of the same priority.

RTCWEB is designed for Internet calling, so there are occasions where the remote peer will not be on the same carrier's network, might be on DSL, might be on a DOCSIS network. In that situation, the DSCP

bits might not be preserved across the remote peer's network, over the Internet, and into the local carrier's network. When this occurs DSCP markings set by the remote peer are likely to be modified by the intervening network(s). Also, DSCP markings requested by a JS application for upstream traffic may not survive on the path to the radio modem because of OS limitations. Given the limitations described above the following techniques can be used to solve the problem :

#### [4.1.1](#). Disable RTP Multiplexing

[I-D.ietf-rtcweb-rtp-usage] in [section 4.4](#) also proposes not to multiplex interactive audio and interactive video over the same 5-tuple for compatibility with legacy systems. If DSCP cannot be propagated to differentiate the required QoS treatment of the traffic within the same 5-tuple then RTP Multiplexing can be disabled by either the JS application or a middle box involved in signaling. Even though DSCP markings are frequently modified by intervening equipment, it is preferable to set them appropriately at each browser to reduce the chance of blocking of higher priority packets in common queues on the path between each browser and their corresponding radio bearer(s).

#### [4.1.2.](#) Extend Packet Filter to include RTP SSRC

RTCWEB is pursuing a option where SSRC(s) for each flow be explicitly signaled in the SDP, thus providing an other way of identifying each flow (i.e., filtering on five-tuple and SSRC value). If 3GPP agrees to extend the packet filter definition to include RTP SSRC, then the UL and DL TFTs would not include any DSCP values and the system would be able to assign each flow to the appropriate bearer/QoS based solely on the assigned SSRC values within the 5-tuple. This requires modification to the 3GPP specifications to extend the TFT filtering mechanism to also support matching on RTP SSRC values. With this extension, multiplexed audio and video media streams using known RTP SSRC values can to be mapped to different EPS bearers, thus receiving different packet forwarding treatment.

The TFT with RTP SSRC might not be applicable in some non-WebRTC use cases and in some WebRTC use cases involving interoperation with legacy peers. In some applications the SSRC value associated with a particular media flow might change over time due to resource switching. In any case where the SSRC value might not be known for every media flow, a signaling level entity can either disable multiplexing, assign only media flows that are intended to receive the same QoS treatment to any one 5-tuple, establish another means of determining the SSRC value for each flow so that the TFT can be updated, or introduce a media gateway to map the SSRC value in each

flow to an explicitly signaled value. Any solution other than the first (disabling multiplexing) requires further study.

#### [4.1.3.](#) Extend Packet Filter to include RTP payload type

BUNDLE requires that each payload type (PT) value used across media lines in a bundled group is unique, thus providing a way of identifying the media flow(s) associated with an m line (i.e., filtering on five-tuple and PT values). If 3GPP agrees to extend the packet filter definition to include RTP PT, then the system would be able to assign the flow(s) associated with each m line to the appropriate bearer/QoS based solely on the PT values within the RTP header of packets in the 5-tuple. With this extension, multiplexed audio and video media streams using known RTP PT values can to be mapped to different EPS bearers, thus receiving different packet

forwarding treatment.

Although this approach is applicable to any use of BUNDLE, there are some limitations. Since a typical m line negotiates the use of multiple payload type values, the TFTs for a typical m line are likely to be more complex than those based on SSRC. Note that if multiple media flows are associated with a particular m line then the network could not distinguish among them and they would of necessity receive the same QoS treatment. Most significantly, since the PT field has a different meaning in RTCP packets, the TFTs for RTP packets do not apply to RTCP and there is no information in the RTCP packets to identify the priority treatment they should receive, even if only RTCP packets of the same intended priority are assembled in any one compound RTCP packet (assuming the DSCP value cannot be trusted). The only solution in this case is to create a TFT for all RTCP packets to assign them the highest priority assigned to any of the RTP packets in the bundle. It is not desirable to use higher priority bandwidth for lower priority RTCP packets but it is less desirable to assign high priority RTCP packets to a lower priority bearer under congestion. SSRC and PT seem viable solutions and could be used in future based on further study.

#### 4.1.4. Data Channel multiplexed with RTP

RTCWEB is pursuing designs which multiplex non-RTP flows with RTP flows in the same 5-tuple. In particular for WebRTC, data channel will use SCTP/DTLS/UDP, potentially on the same 5-tuple as SRTP/UDP. Further a data channel could have multiple streams with different priorities multiplexed within it as explained in section 5.1 of [[I-D.ietf-rtcweb-data-channel](#)] and a mechanism is required to identify and provide differential QoS per stream. If DSCP marking set by the remote peer is preserved and the OS allows setting per-packet DSCP then data channel can be multiplexed with the media

streams. However when DSCP is changed along the path or OS does not allow setting per-packet DSCP then the following aspects needs to be considered :

Since SCTP stream IDs are encrypted, there is no way to enhance the TFT definition to enable differential QoS treatment among the multiple streams multiplexed within an single SCTP association on a 5-tuple. It is possible to provide the same treatment to all streams

within the SCTP association, using one of the following two approaches: 1) after assigning traffic that matches on specific RTP SSRC values within a 5-tuple to certain EPC bearers, assign the remaining traffic within the 5-tuple to another EPC bearer/QoS; or 2) create new TFT extensions to allow identification of other protocols and protocol-specific flow IDs to the extent this information is available in unencrypted fields. Approach 1) is available if only the RTP SSRC or RTP payload extension is defined for TFTs. Approach 2) is for further study. The browser can still provide differential treatment to streams with different priority within the available bandwidth provided for a data channel among packets it transmits within a 5-tuple.

#### 4.2. Bearer Resource Modification triggered by UE

If the UE is using a Public WebRTC server then the UE can request bearer resource modification for an E-UTRAN as explained in [section 5.4.5](#) of [TS23.401]. The procedure allows the UE to request modification of bearer resources (e.g., allocation or release of resources) for one traffic flow aggregate with a specific QoS demand. Alternatively, the procedure allows the UE to request modification of the packet filters used for an active traffic flow aggregate, without changing QoS. If accepted by the network, the request invokes either the Dedicated Bearer Activation Procedure or the Bearer Modification Procedure.

Problems with this approach are:

- o When the UE initiates a call using WebRTC application and candidate pairs are successfully nominated for each media stream then WebRTC application should signal the packet filter, QCI and GBR values for each media stream that would initiate bearer resource modification or dedicated bearer activation. The WebRTC application needs to be aware of the QCI/GBR values required for the media streams.
- o The WebRTC application requires API's to indicate to the OS/Modem the packet filters for each media stream to be added, modified or deleted. The WebRTC application would need API's to indicate to the OS/Modem the QCI and GBR values for each of the packet

filters. The OS/Modem would in turn signal this information to



the 3GPP network that would result in either bearer resource modification or creation using the Dedicated Bearer Activation Procedure.

- o WebRTC application may also need API's to trigger the modification of the GBR value for existing packet filters.

This problem is not unique to WebRTC and is applicable to any other application that wants to trigger bearer resource modification from the MN.

#### [4.3.](#) WebRTC server deployed in 3GPP Network

Currently 3GPP networks prioritize flows by examining the SDP in SIP signaling. As WebRTC also uses SDP in signaling to establish a PeerConnection, similar mechanisms can be used to deploy a WebRTC server in a 3GPP network.

- o 3GPP network cannot prioritize all a=candidate lines described in [\[RFC5245\]](#) until WebRTC server receives an indication of the active media path from the controlling ICE agent. WebRTC server is aware of the active media path only after the controlling ICE endpoint follows the procedures in [Section 11.1 of \[RFC5245\]](#), specifically to send updated offer if the candidates in the m and c lines for the media stream (called the DEFAULT CANDIDATES) do not match ICE's SELECTED CANDIDATES (also see [Appendix B.9 of \[RFC5245\]](#)).
- o WebRTC server deployed in 3GPP network would need "Rx" interface to the Policy and Charging Rules Function (PCRF). The PCRF is the policy server in the EPC. WebRTC server would act as "Application Function". Dynamic PCC (policy and charging control) rules are derived within the PCRF from information supplied by the AF (such as requested bandwidth for the 5-tuple, Application Identity etc). PCRF forwards PCC rules for the media stream to the Policy Charging and Enforcement Function (PCEF) for packet scheduling, data packet (Diffserv) marking, etc., to allow QoS to be provisioned in the EPC. Bearers would have be modified/created for media streams, assigned and installed on the UE.

#### [4.4.](#) WebRTC server deployed in a 3rd party network trusted by Mobile Network

TODO

#### [4.5.](#) Deep Packet Inspection

3GPP has a current work item on "Service Awareness and Privacy Policies" that is chartered to add DPI-related extensions to the PCC architecture [[TS23.203](#)]. The (optional) DPI entity in the EPC is called "Traffic Detection Function" (TDF), and it performs application detection and reporting of detected application and its service data flow description to the Policy Control and Charging Rules Function (PCRF) for performing functions such as traffic blocking, redirection, policing for selected flows.

If UE is using Public WebRTC server then

- o The session signaling between the WebRTC application running in the browser and the web server could be using TLS. Moreover WebRTC does not enforce a particular session signaling protocol to be used, so network gateways in 3GPP network would fail to inspect the signalling to identify the 5-tuple used for media stream and thus fail to prioritize media traffic. Hence derived service identification [[RFC5897](#)] would not succeed.
- o Network Gateways by inspecting L7 traffic can only identify RTP but fail to distinguish between IPTV vs. Multimedia, Gaming vs. Voice Chat, Gaming vs. Voice Chat #2 etc as explained in [section 3.1 - 3.3](#) of [[RFC5897](#)].

## [5.](#) Mobility

The following section lists the potential problems If UE uses Public WebRTC server :

### [5.1.](#) 3GPP SIPTO

Given the exponential growth in the mobile data traffic, Mobile Operators are looking for ways to offload some of the IP traffic flows at the nearest access edge that has an Internet peering point. This approach results in efficient usage of the mobile packet core and helps lower the transport cost. Since Release 10, 3GPP starts supporting of Selected IP Traffic Offload (SIPTO) function defined in [[TS23.060](#)], [[TS23.401](#)]. The SIPTO function allows an operator to offload certain types of traffic at a network node close to the UE's point of attachment to the access network. Limited Mobility support available with SIPTO is explained in section 2.3.3 of [[I-D.zuniga-dmm-gap-analysis](#)].

If SIPTO is carried out in a Traffic offload Function (TOF) entity located at the interface of the Radio Access Network i.e. In the path between the Radio stations and the Mobile Gateway (MGW). The

TOF decides which traffic to offload and enforces NAT for that traffic. The deployment of a TOF is totally transparent for the UE

and hence does not know which traffic is subject to TOF (NATed at the TOF) and which traffic is processed by the MGW.

The problem with WebRTC application in such network is that

- o TOF is not aware of the 5-tuple that will be used for media and data channels. ICE agent would gather server reflexive candidates using STUN and relayed candidates are obtained through TURN. If STUN messages are offloaded at TOF then UE would learn the External IP Address/Port provided by the NAT at TOF. Similarly ICE connectivity checks could also be offloaded at TOF. If UE roams, though host candidate addresses may not change but NAT will change resulting in failure to reach the remote peer for the existing media and data channels. If the media and data channels are offloaded at the TOF then UE Mobility would result in disruption of media and data channel traffic.
- o If UE is using local relayed candidate to reach the remote peer and roams out of the coverage of RNC/HNB GW then NAT between UE and TURN server changes, so UE cannot use the previous TURN allocations and fail to reach the remote peer using local relayed candidate.

[I-D.wing-mmusic-ice-mobility] can be used in such scenarios to provide media session mobility.

## [5.2.](#) IPv4 traffic offload for Proxy Mobile IPv6

Proxy Mobile IPv6 (or PMIPv6, or PMIP) is a network-based mobility management protocol specified in [[RFC5213](#)]. Network-based mobility management enables the same functionality as Mobile IP, without any modifications to the host's Protocol stack. With PMIP the host can change its point-of-attachment to the Internet without changing its IP address. [[I-D.ietf-netext-pmipv6-sipto-option](#)] defines a way to signal the Traffic Offload capability of a Mobile Access Gateway (MAG) to the Local Mobility Anchor (LMA) in Proxy Mobile IP Networks. Mobile access gateway has the ability to offload some of the IPv4 traffic flows based on the traffic selectors it receives from the local mobility anchor. Using IP Traffic Offload Selector option

[[I-D.ietf-netext-pmipv6-sipto-option](#)] mobile access gateway will negotiate IP Flows that can be offloaded to the local access network.

The problem with WebRTC application in such network is that

- o MAG and LMA are not aware of the 5-tuple that will be used for media and data channels. If STUN messages are offloaded at local access network then UE would learn the External IP Address/Port provided by the NAT at local access network. Similarly ICE connectivity

checks could also be offloaded at local access network. If UE roams out of the coverage of Local Access Network though host candidate addresses may not change but NAT will change resulting in failure to reach the remote peer for the existing media and data channels. If the media and data channels are offloaded at the local access network then UE Mobility will result in disruption of media and data channel traffic.

- o If UE is using local relayed candidate to reach the remote peer and roams out of the coverage of Local Access Network then NAT between UE and TURN server changes, so UE cannot use the previous TURN allocations and fail to reach the remote peer using local relayed candidate.

[[I-D.wing-mmusic-ice-mobility](#)] can be used in such scenarios to provide media session mobility.

### [5.3.](#) IPv6 Prefix with Mobility

The [[I-D.korhonen-dmm-prefix-properties](#)] proposes extensions to Prefix Information Option [[RFC4861](#)] with a mobility flag bit. This would allow for network based mobility solutions, such as Proxy Mobile IPv6 [[RFC5213](#)] or GTP [[TS.29274](#)] to explicitly indicate that their prefixes have mobility and therefore, the UE IP stack can make an educated selection between prefixes that have mobility and those that do not. If WebRTC application requires mobility for media streams then it can pick source addresses generated from prefixes with 'M' Flag set to 1 in Prefix Information Option or pick IPv6 prefixes without 'M' flag set to 1 if both the endpoints support [[I-D.wing-mmusic-ice-mobility](#)]. If WebRTC application requires mobility for media streams and the remote peer does not support [[I-D.wing-mmusic-ice-mobility](#)] then it can still pick prefixes

without 'M' flag set to 1 when it uses relayed local candidates for the media streams and TURN supports Mobility as explained in [section 5](#) of [[I-D.wing-mmusic-ice-mobility](#)].

TODO: This section needs more details to be added for WebRTC application to pick suitable prefix.

## [6.](#) Security Considerations

This document does not define an architecture nor a protocol; as such it does not raise any security concern.

## [7.](#) IANA Considerations

This document does not require any action from IANA.

Reddy, et al.	Expires November 10, 2013	[Page 11]
---------------	---------------------------	-----------

---

Internet-Draft	WebRTC in Mobile Networks	May 2013
----------------	---------------------------	----------

## [8.](#) Acknowledgments

Authors would like to thank Dan Wing, Basavraj Patil, Magnus Westerlund, Markus Isomaki, Cullen Jennings, Harold Lassers, Thomas Anderson, Charles Eckel, Subha Dhesikan , Parthasarathi R, Reinaldo Penno, Prashanth Patil for their comments and review.

## [9.](#) Informative References

[GSMA-IR34]

, "Inter-Service Provider Backbone Guidelines 5.0, 22 December 2010", September 2012.

[I-D.dhesikan-tsvwg-rtcweb-qos]

Dhesikan, S., Druta, D., Jones, P., and J. Polk, "DSCP and other packet markings for RTCWeb QoS", [draft-dhesikan-tsvwg-rtcweb-qos-01](#) (work in progress), March 2013.

[I-D.ietf-netext-pmipv6-sipto-option]

Gundavelli, S., Zhou, X., Korhonen, J., and R. Koodli, "IPv4 Traffic Offload Selector Option for Proxy Mobile IPv6", [draft-ietf-netext-pmipv6-sipto-option-12](#) (work in progress), February 2013.

[I-D.ietf-rtcweb-data-channel]

Jesup, R., Loreto, S., and M. Tuexen, "RTCWeb Data Channels", [draft-ietf-rtcweb-data-channel-04](#) (work in progress), February 2013.

[I-D.ietf-rtcweb-overview]

Alvestrand, H., "Overview: Real Time Protocols for Browser-based Applications", [draft-ietf-rtcweb-overview-06](#) (work in progress), February 2013.

[I-D.ietf-rtcweb-rtp-usage]

Perkins, C., Westerlund, M., and J. Ott, "Web Real-Time Communication (WebRTC): Media Transport and Use of RTP", [draft-ietf-rtcweb-rtp-usage-06](#) (work in progress), February 2013.

[I-D.isomaki-rtcweb-mobile]

Isomaki, M., "RTCweb Considerations for Mobile Devices", [draft-isomaki-rtcweb-mobile-00](#) (work in progress), July 2012.

[I-D.korhonen-dmm-prefix-properties]

Korhonen, J., Patil, B., Gundavelli, S., Seite, P., and D. Liu, "IPv6 Prefix Mobility Management Properties", draft-

Reddy, et al.

Expires November 10, 2013

[Page 12]

---

Internet-Draft

WebRTC in Mobile Networks

May 2013

korhonen-dmm-prefix-properties-03 (work in progress),  
October 2012.

[I-D.wing-mmusic-ice-mobility]

Wing, D., Patil, P., Reddy, T., and P. Martinsen, "Mobility with ICE (MICE)", [draft-wing-mmusic-ice-mobility-03](#) (work in progress), January 2013.

[I-D.zuniga-dmm-gap-analysis]

Zuniga, J., Bernardos, C., Melia, T., and C. Perkins, "Mobility Practices and DMM Gap Analysis", [draft-zuniga-dmm-gap-analysis-03](#) (work in progress), December 2012.

[RFC2119]

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

[RFC4861]

Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#),

September 2007.

- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", [RFC 5213](#), August 2008.
- [RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", [RFC 5245](#), April 2010.
- [RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", [RFC 5389](#), October 2008.
- [RFC5897] Rosenberg, J., "Identification of Communications Services in the Session Initiation Protocol (SIP)", [RFC 5897](#), June 2010.
- [RFC6459] Korhonen, J., Soininen, J., Patil, B., Savolainen, T., Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", [RFC 6459](#), January 2012.
- [TS.29274] 3GPP, , "3GPP, "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)", 3GPP TS 29.060 8.11.0, December 2010.", September 2012.
- [TS23.060]

Reddy, et al.	Expires November 10, 2013	[Page 13]
---------------	---------------------------	-----------

---

Internet-Draft	WebRTC in Mobile Networks	May 2013
----------------	---------------------------	----------

3GPP, , ""General Packet Radio Service (GPRS); Service description; Stage 2", June 2012.", September 2012.

- [TS23.107] 3GPP, , "End-to-End Quality of Service (QoS) Concept and Architecture, Release 10, 3GPP TS 23.207, V10.0.0 (2011-03)", September 2012.

- [TS23.203] 3GPP, , "3GPP, "Policy and charging control architecture", 3GPP TS 23.203 10.5.0, December 2011.", September 2012.

[TS23.401]

3GPP, , "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 11), 3GPP TS 23.401, V11.2.0 (2012-06).", September 2012.

## Appendix A. OS Support

- o TODO : In Windows setsockopt is completely disabled. See Knowledge Base Article <http://support.microsoft.com/kb/248611>.
- o DSCP is supported and user settable on Symbian S60, Linux, MacOS X.

The below program is to set DSCP value of 0x2E was tested on Linux successfully.

(Linux k2-server-lnx1 2.6.38-8-generic #42-Ubuntu)

```
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <errno.h>
#include <unistd.h>

#define MSG "Hello, World!"

int
main(void) {
    int sock = -1;
    struct sockaddr *local_addr = NULL;
    struct sockaddr_in sockin, host;
```

```
int tos = 46 << 2; /* Expedited forwarding (0x2e) */
socklen_t socksiz = 0;
char *buffer = NULL;
```



```

sock = socket(AF_INET, SOCK_DGRAM, 0);
if (sock < 0) {
    fprintf(stderr, "Error: %s\n", strerror(errno));
    exit(-1);
}

memset(&sockin, 0, sizeof(sockin));
sockin.sin_family = PF_INET;
sockin.sin_addr.s_addr = inet_addr("10.104.52.145");
socksiz = sizeof(sockin);

local_addr = (struct sockaddr *) &sockin;
/* Set ToS/DSCP */
if (setsockopt(sock, IPPROTO_IP, IP_TOS, &tos,
    sizeof(tos)) != 0) {
    printf("Error setting TOS: %s\n", strerror(errno));
}
/* Bind to a specific local address */
if (bind(sock, local_addr, socksiz) != 0) {
    printf("Error binding to socket: %s\n", strerror(errno));
    close(sock); sock=-1;
    exit(-1);
}

buffer = (char *) malloc(strlen(MSG) + 1);
if ( buffer == NULL ) {
    printf("Error allocating memory: %s\n", strerror(errno));
    close( sock ); sock=-1;
    exit(-1);
}
strncpy(buffer, MSG, strlen(MSG) + 1);
memset(&host, 0, sizeof(host));
host.sin_family = PF_INET;
host.sin_addr.s_addr = inet_addr("10.106.3.95");
host.sin_port = htons(12345);
if (sendto(sock, buffer, strlen(buffer), 0,
    (struct sockaddr *) &host, sizeof(host)) < 0) {
    printf("Error sending message: %s\n", strerror(errno));
    close(sock); sock=-1;
    free(buffer); buffer=NULL;
    exit(-1);
}
free(buffer); buffer=NULL;
close(sock); sock=-1;

```

```
    return 0;  
}
```

#### Authors' Addresses

Tirumaleswar Reddy  
Cisco Systems, Inc.  
Cessna Business Park, Varthur Hobli  
Sarjapur Marathalli Outer Ring Road  
Bangalore, Karnataka 560103  
India

Email: [tiredy@cisco.com](mailto:tiredy@cisco.com)

John Kaippallimalil  
Huawei  
5340 Legacy Drive, Suite 175  
Plano Texas 75024

Email: [john.kaippallimalil@huawei.com](mailto:john.kaippallimalil@huawei.com)

Ram Mohan Ravindranath  
Cisco Systems, Inc.  
Cessna Business Park, Varthur Hobli  
Sarjapur Marathalli Outer Ring Road  
Bangalore, Karnataka 560103  
India

Email: [rmohanr@cisco.com](mailto:rmohanr@cisco.com)

Richard Ejzak  
Alcatel-Lucent  
1960 Lucent Lane  
Naperville, Illinois 60563-1594  
US

Email: [richard.ejzak@alcatel-lucent.com](mailto:richard.ejzak@alcatel-lucent.com)

