Problems with WebRTC in Mobile Networks
draft-reddy-rtcweb-mobile-00

Abstract

This document describes a set of scenarios in which WebRTC applications have problems 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 July 18, 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

1. Introduction ............................................. 3
2. Notational Conventions ................................. 3
3. Scope .................................................. 3
4. Cellular Networks - QOS ............................... 3
   4.1. RTP Session Multiplexing ......................... 4
   4.2. Bearer Resource Modification triggered by UE .... 5
   4.3. WebRTC server deployed in 3GPP Network .......... 6
   4.4. Deep Packet Inspection ............................ 6
5. Mobility ............................................... 7
   5.1. 3GPP SIPTO ........................................ 7
   5.2. IPv4 traffic offload for Proxy Mobile IPv6 ....... 8
   5.3. IPv6 Prefix with Mobility ........................ 9
6. Security Considerations ............................... 9
7. IANA Considerations ................................... 9
8. Acknowledgments ....................................... 9
9. Informative References ............................... 9
Appendix A. OS Support ................................. 11
Authors’ Addresses ...................................... 13
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, HSPA+, and now Long-Term Evolution (LTE) being deployed. Browsers on these devices are becoming close to their desktop counterparts. So, from that perspective, it is feasible to run WebRTC applications in them. This draft enumerates problems when WebRTC application is used on such devices in the above listed networks.

This note focuses on QOS, traffic offload problems 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.

3. Scope

This document can be used as a tool to design solution(s) mitigating the encountered issues. Describing the use case allows to identify what is common between the use cases and then would help during the solution design phase. This note aids WebRTC server designers and network architects to facilitate proper deployment of WebRTC in the mobile network. WebRTC server could either be deployed in the Mobile Network or WebRTC server deployed in a 3rd party network trusted by Mobile Network or 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). The IP five tuple (IP source address, source port, IP destination, destination port, protocol) identifies a packet filter. TFT has other attributes like Type of Service (TOS)/DSCP. 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, 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.

Problems with WebRTC application in 3GPP Network are that

### 4.1. RTP Session Multiplexing

- [I-D.ietf-rtcweb-rtp-usage] in section 4.4 suggests to put interactive audio, interactive video over the same 5-tuple. This means that QoS cannot be applied to the 5-tuple, even if it were known. QoS can only be applied by the endpoint by setting DSCP appropriately on a per-packet basis. This problem can possibly be solved by the proposal in [I-D.ietf-rtcweb-qos]. But 3GPP
networks uses TFT’s packet filtering information to identify and map packets to specific bearers. So DSCP value in TFT for the bearer will not match the DSCP value in the RTP packets sent by the UE and 3GPP network may not honor the DSCP value in the RTP packets. In other words both audio/video media streams would be mapped to the same EPS bearer thus receiving the same bearer level packet forwarding treatment.

- [I-D.ietf-rtcweb-rtp-usage] in section 4.4 also proposes not to multiplex interactive audio, interactive video over the same 5-tuple for compatibility with legacy systems. Mobile Device using WebRTC application in 3GPP network should prefer this method until a technique to solve the above problem is identified and deployed in the 3GPP network.

4.2. Bearer Resource Modification triggered by UE

If UE is using Public WebRTC server then the UE can request bearer resource modification procedure for an E-UTRAN as explained in section 5.4.5 of [TS23.401]. The procedure allows the UE to request for a 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 for the 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:

- 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 (5-tuple), QCI and GBR values for each media stream that would initiate bearer resource modification or dedicated bearer activation. WebRTC application need to be aware of the QCI/GBR values required for the media streams.

- This means WebRTC application requires API’s to indicate OS/Modem the packet filters for each media stream to be added, modified or deleted. WebRTC application would need API’s to indicate OS/Modem the QCI and GBR values for each of the packet filters. OS/Modem would in turn signal this information to the 3GPP network that would result in either bearer resource modification or creation of Dedicated Bearer Activation Procedure.

- WebRTC application may also need API’s to trigger the modification of the GBR value for existing packet filters.
4.3. WebRTC server deployed in 3GPP Network

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

- 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]).

- WebRTC server deployed in 3GPP network would need "Rx" like 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 to be modified/created for media streams, assigned and installed on the UE.

4.4. 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

- 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.
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 the 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 a network is that

- TOF is not aware of the 5-tuple that will 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.
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 stream 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.iert-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.iert-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

- MAG and LMA are not aware of the 5-tuple that will 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.

- 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 stream mobility.
5.3. IPv6 Prefix with Mobility

[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. WebRTC application for media streams must pick source addresses generated from prefixes with ‘M’ Flag set to 1 in Prefix Information Option.

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.

8. Acknowledgments

Authors would like to thank Dan Wing, Basavraj Patil, Magnus Westerlund and Markus Isomaki for valuable inputs to the document.

9. Informative References

[GSMA-IR34]
"Inter-Service Provider Backbone Guidelines 5.0, 22 December 2010", September 2012.

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

[I-D.ietf-rtcweb-overview]

[I-D.ietf-rtcweb-qos]

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

[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]

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

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


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


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


Appendix A. OS Support

Moreover WebRTC application cannot mark DSCP values on Operating Systems like Windows:

- 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)

```c
#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));
    }
}
```

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: tireddy@cisco.com

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

Email: john.kaippallimalil@huawei.com