Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 25, 2014

S. Dhesikan
C. Jennings
Cisco
D. Druta, Ed.
ATT
P. Jones
J. Polk
Cisco

June 23, 2014

DSCP and other packet markings for RTCWeb QoS
draft-ietf-tsvwg-rtcweb-qos-01

Abstract

Many networks, such as service provider and enterprise networks, can provide per packet treatments based on Differentiated Services Code Points (DSCP) on a per-hop basis. This document provides the recommended DSCP values for browsers to use for various classes of traffic.

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 December 25, 2014.

Copyright Notice

Table of Contents

1. Introduction

Differentiated Services Code Points (DSCP)[RFC2474] style packet marking can help provide QoS in some environments. There are many use cases where such marking does not help, but it seldom makes things worse if packets are marked appropriately. In other words, if too many packets, say all audio or all audio and video, are marked for a given network condition then it can prevent desirable results. Either too much other traffic will be starved, or there is not enough capacity for the preferentially marked packets (i.e., audio and/or video).

This draft proposes how WebRTC applications can mark packets. This draft does not contradict or redefine any advice from previous IETF RFCs but simply provides a simple set of recommendations for implementers based on the previous RFCs.

There are some environments where priority markings frequently help. These include:

1. Private networks (Wide Area).

2. Residential Networks: If the congested link is the broadband uplink in a Cable or DSL scenario, often residential routers/NAT support preferential treatment based on DSCP.

3. Wireless Networks: If the congested link is a local WiFi network, marking may help.

Traditionally DSCP values have been thought of as being site specific, with each site selecting its own code points for each QoS level. However in the RTCWeb use cases, the browsers need to set them to something when there is no site specific information. Browsers, in this document is used synonmously with "interactive User Agent" as defined in teh HTML specification, [W3C.WD-html-20110525]. This document describes a reasonable default set of DSCP code point values drawn from existing RFCs and common usage. These code points are solely defaults. Future drafts may define mechanisms for site specific mappings to override the values provided in this draft.

This draft defines some inputs that the browser in an WebRTC application can look at to determine how to set the various packet markings and defines the mapping from abstract QoS policies (data type, priority level) to those packet markings.

2. Relation to Other Standards

This specification does not change or override the advice in any other standards about setting packet markings. It simply provides a summary of them and provides the context of how they relate in the RTCWeb context. In some cases, such as DSCP where the normative RFC leaves open multiple options from which to choose, this clarifies which choice should be used in the RTCWeb context. This document also specifies the inputs that are needed by the browser to provide to the media engine.

The DSCP value set by the endpoint is not always trusted by the network. Therefore, the DSCP value may be remarked at the network edge through policy to any other DSCP value, including best effort. The mitigation for such action is through an authorization mechanism. Such authorization mechanism is outside the scope of this document.

3. Terminology

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as described in [RFC2119].

4. Inputs

The below uses the concept of a media flow, however these are commonly not equivalent to a transport flow, i.e. as defined by a 5-tuple (source address, destination address, source port, destination port, and protocol). Instead each media flow contains all the packets associated with an independent media entity within

one 5-tuple. There may be multiple media flows within the same 5-tuple. These media flows might consist of different media types and have different priorities. The following are the inputs that the browser provides to the media engine:

- Data Type: The browser provides this input as it knows if the flow is audio, interactive video with or without audio, non-interactive video with or without audio, or data.
- Priority: Another input is the relative treatment of the flow within that data type. Many applications have multiple media flows of the same data type and often some are more important than others. Likewise, in a video conference where the flows in the conference is of the same data type but contains different media types, the flow for audio may be more important than the video flow. JavaScript applications can tell the browser whether a particular media flow is high, medium, low or very low importance to the application.

When it comes to data transmission, a media (data) flow is the SCTP stream under a common congestion control (currently within the same SCTP association).

[I-D.ietf-rtcweb-transports] defines in more detail what an individual media flow is within the WebRTC context.

5. DSCP Mappings

Below is a table of DSCP markings for each data type of interest to RTCWeb. These DSCP values for each data type listed are a reasonable default set of code point values taken from [RFC4594]. A web browser SHOULD use these values to mark the appropriate media packets. More information on EF can be found in [RFC3246]. More information on AF can be found in [RFC2597].

Data Type	Very Low	Low	Medium	High
Audio	CS1 (8)	BE (0)	EF (46)	EF (46)
Interactive Video with or without audio	CS1 (8)	BE (0)	AF42, AF43 (36, 38)	AF41, AF42 (34, 36)
Non-Interactive Video with or without audio	CS1 (8)	BE (0)	AF32, AF33 (28, 30)	AF31, AF32 (26, 28)

Data	CS1 (8)	BE (0)	AF1x (10, 12, 14)	AF2x (18, 20, 22)

Table 1

The columns "very low", "low", "Medium" and "high" are the priority levels. The browser SHOULD first select the data type of the media flow. Within the data type, the priority of the media flow SHOULD be selected. All packets within a media flow SHOULD have the same priority. In some cases, the selected cell may have multiple DSCP values, such as AF41 and AF42. These offer different drop precedences. One may select difference drop precedences for the different packets in the media flow. Therefore, all packets in the stream SHOULD be marked with the same priority but can have difference drop precedences.

The combination of data type and priority provides specificity and helps in selecting the right DSCP value for the media flow. In some cases, the different drop precedence values provides additional granularity in classifying packets within a media flow. For example, in a video conference, the video media flow may be medium priority. If so, either AF42 or AF43 may be selected. If the I frames in the stream are more important than the P frames then the I frames can be marked with AF42 and the P frames marked with AF43.

The above table assumes that packets marked with CS1 is treated as "less than best effort". However, the treatment of CS1 is implementation dependent. If an implementation treats CS1 as other than "less than best effort", then the priority of the packets may be changed from what is intended.

If a packet enters a QoS domain that has no support for the above defined Data Types/Application (service) classes, then the network node at the edge will remark the DSCP value based on policies. Subsequently, if the packet enters a QoS domain that supports a larger number of Data types/Application (service) classes, there may not be sufficient information in the packet to restore the original markings. Mechanisms for restoring such original DSCP is outside the scope of this document.

6. Security Considerations

This draft does not add any additional security implication other than the normal application use of DSCP. For security implications on use of DSCP, please refer to Section 6 of RFC 4594. Please also see work-in-progress draft draft-ietf-rtcweb-security-04 as an additional reference.

7. IANA Considerations

This specification does not require any actions from IANA.

8. Downward References

This specification contains a downwards reference to [RFC4594] however the parts of that RFC used by this specification are sufficiently stable for this downward reference.

9. Acknowledgements

Cullen Jennings was one of the authors of this text in the original individual submission but was unceremoniously kicked off by the chairs when it became a WG version. Thanks To David Black, Magnus Westerland, Paolo Severini, Jim Hasselbrook, Joe Marcus, and Erik Nordmark for their help.

10. Document History

Note to RFC Editor: Please remove this section.

This document was originally an individual submission in RTCWeb WG. The RTCWeb working group selected it to be become a WG document. Later the transport ADs requested that this be moved to the TSVWG WG as that seemed to be a better match. This document is now being submitted as individual submission to the TSVWG with the hope that WG will select it as a WG draft and move it forward to an RFC.

11. References

11.1. Normative References

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

[RFC4594] Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes", RFC 4594, August 2006.

11.2. Informative References

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[RFC2597] Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski, "Assured Forwarding PHB Group", RFC 2597, June 1999.

[RFC3246] Davie, B., Charny, A., Bennet, J., Benson, K., Le Boudec, J., Courtney, W., Davari, S., Firoiu, V., and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)", RFC 3246, March 2002.

Authors' Addresses

Subha Dhesikan
Cisco

Email: sdhesika@cisco.com

Cullen Jennings
Cisco

Email: fluffy@cisco.com

Dan Druta (editor)
ATT

Email: dd5826@att.com

Paul Jones
Cisco

Email: paulej@packetizer.com

James Polk
Cisco

Email: jmpolk@cisco.com