Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 25, 2016

S. Dhesikan
C. Jennings
Cisco Systems
D. Druta, Ed.
AT&T
P. Jones
Cisco Systems

January 22, 2016

DSCP and other packet markings for WebRTC QoS
draft-ietf-tsvwg-rtcweb-qos-08

Abstract

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

Table of Contents

1. Introduction 2
2. Relation to Other Standards 3
3. Terminology 4
4. Inputs 4
5. DSCP Mappings 5
6. Security Considerations 7
7. IANA Considerations 7
8. Downward References 7
9. Acknowledgements 7
10. Dedication 7
11. Document History 8
12. References 8
  12.1. Normative References 8
  12.2. Informative References 9
Authors' Addresses 9

1. Introduction

Differentiated Services Code Points (DSCP) [RFC2474] packet marking can help provide QoS in some environments. This specification proposes how WebRTC applications can mark packets, but does not contradict or redefine any advice from previous IETF RFCs. Rather, it merely provides a simple set of recommendations for implementers based on the previous RFCs.

There are many use cases where such marking does not help, but it seldom makes things worse if packets are marked appropriately. As one example of where it does not help, 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).

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

1. Private, wide-area networks.

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 wireless network, marking may help.

Traditionally DSCP values have been thought of as being site specific, with each site selecting its own code points for controlling per-hop-behavior to influence the QoS for transport-layer flows. However in the WebRTC use cases, the browsers need to set them to something when there is no site specific information. In this document, "browsers" is used synonymously with "Interactive User Agent" as defined in the HTML specification, [W3C.REC-html5-20141028]. This document describes a subset of DSCP code point values drawn from existing RFCs and common usage for use with WebRTC applications. These code points are solely defaults.

This specification defines some inputs that the browser in a WebRTC application can consider to aid in determining how to set the various packet markings and defines the mapping from abstract QoS policies (flow type, priority level) to those packet markings.

2. Relation to Other Standards

This document exists as a complement to [I-D.ietf-dart-dscp-rtp], which describes the interaction between DSCP and real-time communications. It covers the implications of using various DSCP values, particularly focusing on Real-time Transport Protocol (RTP) [RFC3550] streams that are multiplexed onto a single transport-layer flow.

There are a number of guidelines specified in [I-D.ietf-dart-dscp-rtp] that should be followed when marking traffic sent by WebRTC applications, as it is common for multiple RTP streams to be multiplexed on the same transport-layer flow. Generally, the RTP streams would be marked with a value as appropriate from Table 1. A WebRTC application might also multiplex data channel [I-D.ietf-rtcweb-data-channel] traffic over the same 5-tuple as RTP streams, which would also be marked as per that table. The guidance in [I-D.ietf-dart-dscp-rtp] says that all data channel traffic would be marked with a single value that is typically different than the value(s) used for RTP streams multiplexed with the data channel traffic over the same 5-tuple, assuming RTP streams are marked with a value other than default forwarding (DF). This is expanded upon further in the next section.

This specification does not change or override the advice in any other standards about setting packet markings. It simply selects a subset of DSCP values that is relevant in the WebRTC 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 any place in the network for a variety of reasons to any other DSCP value, including default forwarding (DF) value to provide basic best effort service. The mitigation for such action is through an authorization mechanism. Such authorization mechanism is outside the scope of this document. There is benefit in marking traffic even if it only benefits the first few hops.

3. 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 [RFC2119].

4. Inputs

WebRTC entities transmit and receive two types of media of significance to this document: RTP streams [I-D.ietf-rtcweb-rtp-usage] and data channels [I-D.ietf-rtcweb-data-channel]. Each of the RTP streams and distinct data channels consists of all of the packets associated with an independent media entity and are not alway equivalent to a transport-layer flow defined by a 5-tuple (source address, destination address, source port, destination port, and protocol). There may be multiple RTP streams and data channels multiplexed over the same 5-tuple, with each having a different level of importance to the application and, therefore, potentially marked using different DSCP values than another RTP stream or data channel within the same transport-layer flow. (Note that there are restrictions with respect to marking different data channels carried within the same SCTP association as outlined in Section 5.)

The following are the inputs that the browser provides to the media engine:

- o Flow 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.
- o Application Priority: Another input is the relative importance of an RTP stream or data channel flow. Many applications have multiple flows of the same Flow Type and often some flows are more important than others. For example, in a video conference where there are usually audio and video flows, the audio flow may be more important than the video flow. JavaScript applications can tell the browser whether a particular flow is high, medium, low or very low importance to the application.

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

5. DSCP Mappings

The DSCP markings for each flow type of interest to WebRTC given the application priority is shown in the following table. The DSCP values for each flow type listed are a reasonable subset 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]. DF is default forwarding which provides the basic best effort service.

Flow Type	Very Low	Low	Medium	High
Audio	CS1 (8)	DF (0)	EF (46)	EF (46)
Interactive Video with	CS1	DF	AF42, AF43	AF41, AF42

or without audio	(8)	(0)	(36, 38)	(34, 36)
Non-Interactive Video with or without audio	CS1 (8)	DF (0)	AF32, AF33 (28, 30)	AF31, AF32 (26, 28)
Data	CS1 (8)	DF (0)	AF11	AF21

Table 1: Recommended DSCP Values for WebRTC Applications

The application priority, indicated by the columns "very low", "low", "Medium", and "high", signifies the relative importance of the flow within the application. It is an input that the browser receives to assist it in selecting the DSCP value. Application priority does not refer to priority in the network transport.

The above table assumes that packets marked with CS1 are 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 actual priority (or, more precisely, the per-hop-behavior) of the packets may be changed from what is intended. It is common for CS1 to be treated the same as DF, so anyone using CS1 cannot assume that CS1 will be treated differently than DF. Implementers should also note that excess EF traffic is dropped. This could mean that a packet marked as EF may

not get through as opposed to a packet marked with a different DSCP value.

The browser SHOULD first select the flow type of the flow. Within the flow type, the relative importance of the flow SHOULD be used to select the appropriate DSCP value.

The combination of flow type and application priority provides specificity and helps in selecting the right DSCP value for the flow. All packets within a flow SHOULD have the same application priority. In some cases, the selected application priority cell may have multiple DSCP values, such as AF41 and AF42. These offer different drop precedences. The different drop precedence values provides additional granularity in classifying packets within a flow. For example, in a video conference, the video flow may have medium application 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.

For reasons discussed in Section 6 of [I-D.ietf-dart-dscp-rtp], if multiple flows are multiplexed using a reliable transport (e.g., TCP) then all of the packets for all flows multiplexed over that transport-layer flow MUST be marked using the same DSCP value. Likewise, all WebRTC data channel packets transmitted over an SCTP association MUST be marked using the same DSCP value, regardless of how many data channels (streams) exist or what kind of traffic is carried over the various SCTP streams. In the event that the browser wishes to change the DSCP value in use for an SCTP association, it MUST reset the SCTP congestion controller after changing values. Frequent changes in the DSCP value used for an SCTP association are discouraged, though, as this would defeat any attempts at effectively managing congestion. It should also be noted that any change in DSCP value that results in a reset of the congestion controller puts the SCTP association back into slow start, which may have undesirable effects on application performance.

For the data channel traffic multiplexed over an SCTP association, it is RECOMMENDED that the DSCP value selected be the one associated with the highest priority requested for all data channels multiplexed over the SCTP association. Likewise, when multiplexing multiple flows over a TCP connection, the DCSP value selected should be the one associated with the highest priority requested for all multiplexed flows.

If a packet enters a QoS domain that has no support for the above defined flow types/application priority (service class), then the network node at the edge will remark the DSCP value based on

policies. This could result in the flow not getting the network treatment it expects based on the original DSCP value in the packet. Subsequently, if the packet enters a QoS domain that supports a larger number of 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.

In summary, there are no guarantees or promised level of service with the use of DSCP. The service provided to a packet is dependent upon the network design along the path, as well as the congestion levels at every hop.

6. Security Considerations

This specification 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 [RFC4594]. Please also see [I-D.ietf-rtcweb-security] 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

Thanks To David Black, Magnus Westerland, Paolo Severini, Jim Hasselbrook, Joe Marcus, Erik Nordmark, and Michael Tuexen for their invaluable input.

10. Dedication

This document is dedicated to the memory of James Polk, a long-time friend and colleague. James made important contributions to this specification, including being one of its primary authors. The IETF global community mourns his loss and he will be missed dearly.

11. 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.

12. References

12.1. Normative References

[I-D.ietf-dart-dscp-rtp]
Black, D. and P. Jones, "Differentiated Services (DiffServ) and Real-time Communication", draft-ietf-dart-dscp-rtp-10 (work in progress), November 2014.

[I-D.ietf-rtcweb-data-channel]
Jesup, R., Loreto, S., and M. Tuexen, "WebRTC Data Channels", draft-ietf-rtcweb-data-channel-13 (work in progress), January 2015.

[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-25 (work in progress), June 2015.

[I-D.ietf-rtcweb-security]
Rescorla, E., "Security Considerations for WebRTC", draft-ietf-rtcweb-security-08 (work in progress), February 2015.

[I-D.ietf-rtcweb-transports]
Alvestrand, H., "Transports for WebRTC", draft-ietf-rtcweb-transports-10 (work in progress), October 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4594] Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes", RFC 4594, DOI 10.17487/RFC4594, August 2006, <http://www.rfc-editor.org/info/rfc4594>.

12.2. 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, DOI 10.17487/RFC2474, December 1998, <http://www.rfc-editor.org/info/rfc2474>.

[RFC2597] Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski, "Assured Forwarding PHB Group", RFC 2597, DOI 10.17487/RFC2597, June 1999, <http://www.rfc-editor.org/info/rfc2597>.

[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, DOI 10.17487/RFC3246, March 2002, <http://www.rfc-editor.org/info/rfc3246>.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550, July 2003, <http://www.rfc-editor.org/info/rfc3550>.

[W3C.REC-html5-20141028] Hickson, I., Berjon, R., Faulkner, S., Leithead, T., Navara, E., O'Connor, E., and S. Pfeiffer, "HTML5", World Wide Web Consortium Recommendation REC-html5-20141028, October 2014, <http://www.w3.org/TR/2014/REC-html5-20141028>.

Authors' Addresses

Subha Dhesikan
Cisco Systems

Email: sdhesika@cisco.com

Cullen Jennings
Cisco Systems

Email: fluffy@cisco.com

Dan Druta (editor)
AT&T

Email: dd5826@att.com

Paul E. Jones
Cisco Systems

Email: paulej@packetizer.com