2018 30th International Teletraffic Congress

Can WebRTC QoS Work? A DSCP Measurement Study

Runa Barik, Michael Welzl
Department of Informatics
University of Oslo, Oslo, Norway
{runabk,michawe}@ifi.uio.no

Ahmed Elmokashfi, Thomas Dreibholz
Centre for Digital Engineering
Simula Research Laboratory, Fornebu, Norway
{ahmed,dreibh}@simula.no

Stein Gjessing
Department of Informatics
University of Oslo, Oslo, Norway
steing@ifi.uio.no

***Abstract*—DiffServ was designed to implement service provider quality of service (QoS) policies, where ingress and egress routers change the DiffServ Code Point (DSCP) in the IP header. However, nowadays, applications are beginning to directly set the DSCP themselves, in the hope that this will yield a more appropriate service for their respective video, audio and data streams. WebRTC is a prime example of such an application.**

As a first step towards understanding whether "WebRTC QoS works", we measured, for both IPv4 and IPv6, what happens to DSCP values along Internet paths. Our study is based on end-to-end measurements from 160 IPv4 and 65 IPv6 geographically spread controlled probe clients to 34 IPv4 and 18 IPv6 servers respectively. Clearly, when the DSCP value is changed, the net result may not be what the application desired. We find that this happens often, and conclude with recommendations on how to improve WebRTC and other applications using the DSCP.

***Index Terms*—Measurement, Fling, DSCP, Ingress, Egress**

I. Introduction

The Differentiated Services Code Point (DSCP) [1], [2] field in the IP header is used for marking and differentiating traffic within a single domain. This is often done at the ingress of a network, and in some cases *within* the network to shape traffic. Egress points are likely to remove or change a DSCP marking. Internet Service Providers (ISP) which do not use/trust the DSCP might zero it at the ingress. Accordingly, the DSCP is traditionally not meant to be set by end systems. However, setting the DSCP was found to occasionally work, and there may not be much harm in trying to use it. It is therefore now proposed as a method for WebRTC [3].

Motivated by [4], we would like to better understand the effect of such DSCP markings. While a full investigation would require sending significant amounts of media payloads and measuring if routers treat traffic differently, as a first step, it makes sense to understand what happens to the DSCP value along an Internet path. If, for example, a client's home gateway already zeroes the DSCP, no router beyond it can use this field to differentiate packets. The longer into an Internet path a value survives, the more likely it is for the mechanism in [4] to be useful. If setting DSCP values "works", but routers do not currently implement any special treatment for DSCP-marked packets that end systems may emit, there is at least reason to hope that large-scale applications like WebRTC could provoke a change in the behavior of ISPs. Either way, to understand the potential of the mechanism, we must first investigate what routers and other middleboxes do to the DSCP field itself.

II. Related Work

The increasing popularity of middleboxes has motivated several efforts to characterize their deployment and assess their impact on data plane performance. Medina et al. [5], [6] actively probed a set of web servers using TBIT [7] to assess the interaction between middleboxes and transport protocols. Honda et al. [8] developed TCPExposure to test whether TCP options are supported. TraceBox [9] improved over TCPExposure by proposing a Traceroute-like approach to pinpoint routers that alter or discard TCP options. Recently, Craven et al. [10] proposed TCP HICCUPS, a tool that reveals TCP header manipulation to both ends of a TCP connection. PATHspider [11] allows for A/B testing of a baseline configuration against an experimental configuration. Other papers focused on investigating specific types of middleboxes, such as web proxies [12], transparent HTTP proxies in cellular networks [13], firewalls and NATs policies in cellular networks [14], and carrier grade NATs [15]. Trammel et al. [16] proposed correlating measurements from diverse vantage points to build a map of middlebox-induced path impairments in the Internet.

So far, only a handful of studies focused on the DSCP field: following a smaller-scale [17] and a one-sided study [18], Fairhurst et al. [19] analyze the DSCP modification behavior by middleboxes in mobile broadband (MBB) edge networks. MBB networks usually deploy middleboxes that interfere with traffic. The analyses of this paper therefore provide a valuable starting point for further analyses. To complement the MBB edge measurements from [19], we focus on fixed networks. The contribution of this paper is therefore:

- Analysis of DSCP modification behavior in heterogeneous fixed networks (i.e. research networks, business-grade connections, consumer-grade connections like ADSL),
- Comparison of differences between IPv4 and IPv6,
- Insights on behavior inside the core networks,

Together with the MBB measurements from [19], our fixed network measurements offer a global view on DSCP modification behavior in the Internet. This can help currently ongoing

978-0-9883045-5-0/18/$31.00 ©2018 ITC
DOI 10.1109/ITC30.2018.00034

discussions on DSCP usage in different working groups of the IETF (e.g. RTCWeb, TSVWG, and ICCRG).

III. Measurement Methodology

For this work, we use the *fling* middlebox measurement platform[1] [20]. This platform allows testing whether an arbitrary sequence of packets can be exchanged between a *fling* client and a *fling* server. For our tests, *fling* used 34 IPv4 and 18 IPv6 nodes as servers. Regarding the choice of the measurement hosts, we believe that a typical WebRTC use case is users at the edge calling each other or calling a company's technical support via the browser. Hence, having endpoints at the edge seems to be the right choice. This has motivated us to choose NorNet Core servers, since they have "consumer-grade" connectivity. We also have a server from Amazon cloud as part of our dataset. We ran the client tool from 160 (IPv4) / 65 (IPv6) Ark[2], PlanetLab[3] and NorNet Core[4] nodes to perform a simple UDP packet exchange with different DSCP values. This gave us measurements across a total of approximately 10k unidirectional IPv4 paths and more than 2k unidirectional IPv6 paths. We tested the DSCP values CS1, AF42, and EF due to their importance for WebRTC (see Table I).

We designate a test as "failed" if any packet of the test was dropped. To eliminate the effect of sporadic random drops, we only decide that a packet was dropped as a result of a specific DSCP value if it is consistently dropped in three tests. If a packet is dropped or modified on the path, depending on the direction of its traversal, the sender of the packet resends it with increasing TTL (TraceBox-like test) to attempt to pinpoint the router that interfered with the DSCP value. In this process, we collect ICMP packets with Time-to-Live Exceeded messages from the network nodes and parse them to see whether they contain the original packet that triggered the ICMP response. If a device remarks the DSCP upon forwarding, we can only observe this behavior correctly by considering the ICMP error message from a node (we hereby call it *responder*) at the next hop on the path.

A. Infrastructure

We ran the *fling* client from 111 vantage points on CAIDA's Ark platform. These vantage points, being located in people's homes, universities and offices, are spread across 44 countries (e.g. 36 from US, 7 from CA, 5 from DE, 4 from ZA, etc). From these vantage points, we got 111 IPv4 and 46 IPv6 addresses for our measurements. We also received information about the vantage points, such as the AS (Autonomous System) number, organization name, AS classification and geographic locations of the vantage points.

PlanetLab [22] is a group of computers available as a testbed for computer networking and distributed systems research. Its nodes are mostly devices located at universities. We ran the *fling* tool from 14 IPv4 PlanetLab Europe (PLE) nodes, as these allow raw sockets out of the box. PlanetLab Central (PLC) nodes support *safe* raw sockets for ICMP, UDP and TCP packets, but using them would have required a significant change to our Python-based tool.

DSCP value	Description (RFC 4594 [21])	WebRTC [4] Flow Type / Priority
CS1*	Low-priority data	Any / Very Low
AF42*	Multimedia conferencing	1 / Medium or High
EF*	Telephony	1 / Medium or High
CS0	Standard	Any / Low
AF11, AF12, AF13	High-throughput data	4 / Medium (AF11 only)
AF21	Low-latency data	4 / High
AF31	Multimedia streaming	3 / High
AF41	Multimedia conferencing	2 / High
CS4	Real-time interactive	not defined
CS5	Signaling	not defined
CS7	Reserved for future use	not defined
1, 2, 4, 6, 41	Undefined values	not defined

Table I: DSCP values that we encountered in our measurements and their meaning. Values that we used as input are marked with a *. WebRTC flow types: 1: Audio; 2: Interactive video with or without audio; 3: Non-interactive video with or without audio; 4: Data.

The NorNet Core testbed [23]–[25] is a large-scale Internet testbed for multi-homed systems. Unlike PlanetLab, NorNet Core also provides support for IPv6. Furthermore, NorNet Core sites are not only connected to a site's local research network ISP, but also have "consumer-grade" connectivity with many home-user ADSL and fiber subscriptions. This makes NorNet Core a realistic Internet test platform for experiencing the "normal" user's QoS. Furthermore, we got the possibility to run *fling* directly on the routers of the testbed, providing unrestricted access to the public IP addresses.

We host our *fling* servers on the routers in NorNet Core. We have a total of 31 IPv4 and 18 IPv6 nodes from NorNet Core for *fling* servers, covering 5 countries (21 from Norway, 4 from Germany, 3 from China, 2 from America, 1 from Sweden). We also deployed three additional *fling* servers in the United Kingdom (it has an IPv4 and an IPv6 addresses), India (only IPv4 address), and the USA (only IPv4 address). Further, we ran the *fling* client tool on all nodes above.

B. Data Processing

After running the measurements, we collected the data from a total of 160 IPv4 and 65 IPv6 nodes (IPv6 addresses and their corresponding IPv4 addresses belong to the same interfaces). Of the 160 IPv4 addresses, 112 addresses are public and 48 addresses are behind NAT boxes. We extracted all the IPv4 and IPv6 addresses from the ICMP packets obtained from our TraceBox-like test. For IP-to-AS mapping, we used the Whois database provided by Team Cymru[5]. We resolved all IPv4 router aliases using the tools Kapar[6] followed by MIDAR[7]. For IPv6 addresses, we used the tool Speedtrap[8]. We extracted 7721 IPv4 and 1503 IPv6 addresses. After

[1] *fling*: http://fling-frontend.nntb.no.
[2] Ark: https://www.caida.org/projects/ark/.
[3] PlanetLab: https://www.planet-lab.org.
[4] NorNet: https://www.nntb.no.
[5] Team Cymru: https://www.team-cymru.org/IP-ASN-mapping.html.
[6] Kapar: https://www.caida.org/tools/measurement/kapar/.
[7] MIDAR: https://www.caida.org/tools/measurement/midar/.
[8] Speedtrap: https://www.caida.org/tools/measurement/scamper/.

Figure 1: Geographical *fling* host locations. Green: clients, Blue: servers.

performing alias resolution, we collected 416 routers in IPv4 and 127 routers in IPv6 with multiple addresses. Since we do not carry out our TRACEBOX-like test when all packets reach the other end unmodified, the number of paths for which we have TRACEBOX-like information is smaller than the total number of paths. The whole measurement gave us TRACEBOX-like test details for a total of 8217 unidirectional paths for IPv4, and 1585 for IPv6. We categorize all client nodes from the three platforms into three groups:

1) Home Networks: This covers 39 IPv4 (12 from NORNET CORE and 27 from ARK) and 11 IPv6 (7 from NORNET CORE and 4 from ARK) addresses of residential nodes.
2) Research and Education Networks: We consider the PLANETLAB nodes as part of research and education networks. In this group, in addition to the 14 nodes from PLANETLAB, we have 19 nodes from NORNET CORE and 38 nodes from ARK (i.e., a total of 71 IPv4 addresses). In the IPv6 case, we have 34 nodes. Of these 34 nodes, 23 nodes are from ARK and the remaining 11 nodes belong to NORNET CORE.
3) Commercial Networks: Business, commercial and infrastructure type nodes fall in this group. We have a total of 50 IPv4 and 20 IPv6 addresses from commercial networks. Of the 50 IPv4 addresses, only 4 belong to NORNET CORE and the rest is from ARK. Only 1 IPv6 address is from NORNET CORE; the remaining 19 IPv6 nodes belong to ARK.

IV. PATH TRAVERSAL

First, we analyze the DSCP effect on path traversal from the end-hosts' perspective and compare some of our results

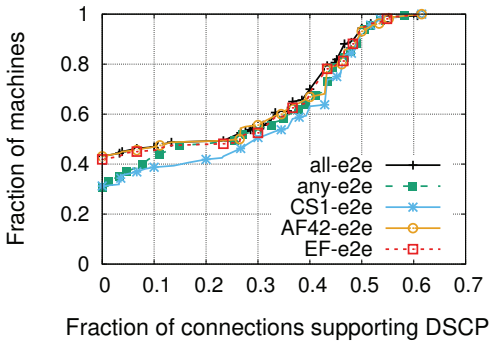
DSCP Value	Preserved paths (our work)	Preserved paths ([19], Table V)
EF	23%	23.8%
CS1	30%	24%
AF42 / AF41	22%	23.1%

Table II: End-to-end transparency results from 9992 (our work) and 9202 [19] IPv4 paths. We combine AF41 and AF42 because they are in the same general category [21].

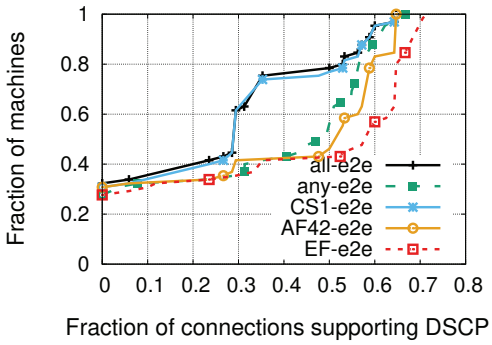
to the results published in [19]. Different from our work, [19] focuses only on IPv4, but also considers TCP, finding only a marginal difference in behavior between TCP and UDP. Table II summarizes some findings from our own tests and [19]; differences between code points are notable, but not very large: CS1 survives end-to-end in slightly less than a third of the cases, compared to slightly less than a quarter for EF and AF42.

Figures 2(b) and 2(d) show the fraction of connections supporting DSCP end-to-end in IPv6 network in both the forward (client to server) and reverse (server to client) directions. Here, EF and AF42 are much more likely to survive (≈40%) end-to-end than CS1 (≈30%). We found this to be primarily the effect of one AS, AS2116, which consistently mapped CS1 to AF11 on 121 out of our 1170 total IPv6 paths. This AS consistently changed CS1 to AF11, while AF42 and EF remained unchanged.

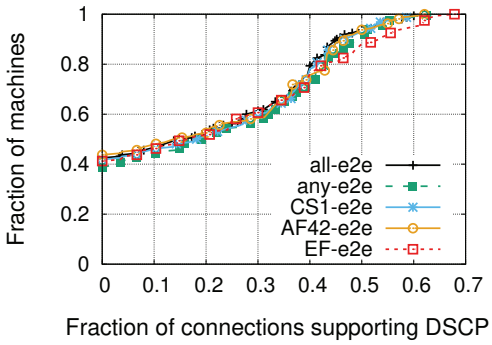
Figures 2(a) and 2(c) show the fraction of connections supporting DSCP end-to-end in IPv4 network in both the forward (client to server) and reverse (server to client) directions. Note that we also removed all paths that exhibited two or more instances of DSCP remarking, of which the last remarked it to the original value. For both protocols, reverse and forward paths exhibit similar characteristics, except that CS1's slightly better chance of end-to-end "survival" in the IPv4 case is only



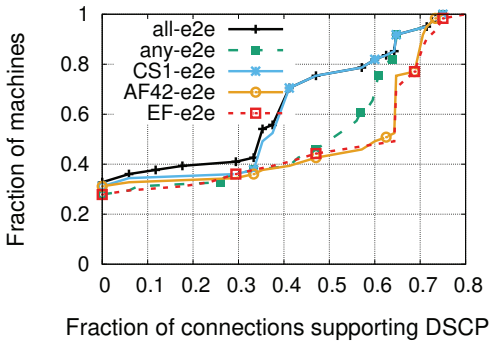
(a) Forward path in IPv4



(b) Forward path in IPv6



(c) Reverse path in IPv4



(d) Reverse path in IPv6

Figure 2: End-to-end DSCP "survival" in forward (client-to-server) and backward direction (server-to-client).

DSCP value provoking drop	Direction	Total # failures	# clients	# servers
CS1	Forward	18	6	10
CS1	Backward	74	27	31
AF42	Forward	28	9	16
AF42	Backward	74	27	28
EF	Forward	28	9	17
EF	Backward	76	23	32
All	Forward	13	3	6
All	Backward	27	11	15

Table III: Blackholing: consistent (3 times) losses when a DSCP value was used (CS0 worked on all these paths). In contrast, no test failed consistently on 4951 forward and 4833 backward paths.

visible in the forward direction.

Confirming the two previous studies [17], [18], we found cases of IPv4 DSCP "blackholing", where routers consistently (i.e., in 3 consecutive tests) dropped all packets only when a certain DSCP value was used. Table III provides an overview of these cases. While the number of paths where this happened was small, this behavior is problematic enough to justify implementing safety measures (falling back to DSCP 0 in case of complete connectivity loss). Notably, none of these drops happened with TTL=1 or 2 (we explain why we use these two values in Subsection V-A), i.e. it seems that these drops were not caused by a home gateway. Geographically, both the clients and servers involved in these consistent packet drops were in diverse regions: of the 40 clients, 12 were in the USA, 5 in Norway, 4 in Germany, 2 in Sweden, 2 in Canada and 15 in others. Of the 34 servers, 21 were in Norway, 4 in Germany, 3 in China, 3 in the USA, 1 in Sweden, 1 in France and 1 in India.

V. DSCP Treatment in Different Network Parts

In this section, we investigate how DSCP code points are treated in different parts of the network – inside the home network, within and beyond the first-hop ISP. The goal of this analysis is to determine which parts of the end-to-end path are likelier to remark DSCP code points. The total number of client ASes is 118 for IPv4 addresses and 54 for IPv6 addresses. With one exception (noted in Subsection V-C), all the behavior described here happened *persistently*, i.e. routers and gateways exhibited the same behavior in multiple tests, as all measurements were done from multiple clients to multiple servers.

A. Will a host's DSCP mark make it to its own ISP?

In the following, we quantify DSCP treatment in the home network. We blame the home gateway for remarking the DSCP if we discover a change at TTL=1.

We observe that the home gateways of 8 commercial, 11 residential and 9 research clients always reset the DSCP values to 0 (CS0), irrespectively of the input value. These are 17% (28 out of 160) of the total number of machines with IPv4 addresses. However, it happens for only 10% (7 out of 65) of the machines with IPv6 addresses.

We also observe that some of the gateways persistently reset the DSCP values to a fixed value, irrespective of the incoming DSCP value. For IPv4, the gateways of 2 out of 51 commercial clients change the incoming DSCP values to a decimal value of 63 (unregistered code point). Similarly,

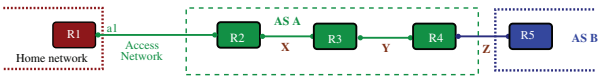


Figure 3: IP a1 belongs to AS A and $R2$ is the access router in AS A. We categorize DSCP changes as follows: X (*access network*): DSCP changed by $R2$ and detected by $R3$, Y (*in-network*): DSCP changed by $R3$ ($R2 \neq R3$) and detected by $R4$; Z (*egress*): DSCP changed by $R4$ (AS A) and detected by R5 (AS B)

2 of the 39 residential nodes detected a change of the DSCP value to CS1 (which commonly encodes "less than best effort" behavior, see Table I). Only one residential client in an IPv6 network experiences a persistent DSCP re-write; it is always changed to the unregistered decimal value of 4.

Some home gateways generate specific DSCP values depending on incoming values. 2 commercial and 1 residential clients in IPv4 detected different DSCP values depending on input values. For example, for one commercial client we observed that the AF42 (multimedia conferencing, see Table I) code point is changed to CS4 (real-time interactive); EF (telephony) is changed to CS5 (signaling), while CS1 remains unchanged. This mapping could just be the result of bleaching the lower 3 bits of incoming DSCP values. The home gateways of one commercial and one residential appear to bleach the higher 3 bits of the DSCP. However, we did not see a single case of such DSCP mapping for IPv6 probes.

To summarize, we have seen that home gateways treat DSCP in a myriad of ways. However, overall, only 21% and 12% of our IPv4 and IPv6 probes experienced a change of the DSCP value at the home gateway. This is encouraging: even with IPv4, the DSCP value often remained intact, and IPv6 makes this success even more likely, possibly giving an additional reason to favor IPv6 over IPv4. Except for one case, DSCP values are typically not demoted. We are left with 125 IPv4 and 57 IPv6 clients that did not experience a DSCP change at the first hop. The number of client ASes for these IPv4 and IPv6 addresses are 97 and 47, respectively[9]. Next, we will look at what happens further "down the road", inside these client ASes.

B. DSCP Treatment by First-Hop ISP

We now turn to investigating how DSCP markings, which survive the home network, are treated by the first-hop ISP. Of the remaining 125 IPv4 clients, 67 are affected by their own ISPs. These clients belong to 41% of all measured ASes. The chance is lower for IPv6, with only 20 of the remaining 57 addresses experiencing a change of DSCP in their own ISP. Overall, the majority of first-hop ISPs do not interfere with DSCP code points; 59% and 67% for IPv4 and IPv6 respectively. We categorize the DSCP change in the ISP as *access network*, *egress* and *in-network*, depending on the location inside the ISP network, where the change occurs. Figure 3 explains how we categorize DSCP changes. If DSCP remarking routers in an AS appear in multiple places

[9]This is larger than the total number of client ASes minus the ASes of machines with an interfering gateway because some client ASes have several clients.

	#ASes (IPv4)	#ASes (IPv6)	#ASes setting DSCP to 0 (IPv4)	#ASes setting DSCP to 0 (IPv6)
DSCP change at Access network	15	3	11	3
DSCP change at In-network	6	5	5	5
DSCP change at Egress	13	3	9	3
DSCP change at Mixed	6	2	4	1
No Change	57	34	0	0
Total	97	47	29	12

Table IV: DSCP change in first-hop ISP; "Mixed" means that ASes changed the DSCP in multiple places (multiple routers remarking the DSCP)

(i.e., different routers in different places), we call the DSCP remarking in that AS *mixed*.

To study the *access network*, we consider the first public IP after the home gateway to be the first-hop ISP ingress router. This is usually a router that is two hops away from the client i.e. TTL=2. This mapping can be incorrect if the first-hop ISP configures its access network to use private IPs e.g. in presence of carrier grade NATs. However, our dataset does not involve paths with private IP hops with TTL>1.Table IV presents the total number of ASes that remark the DSCP at the access network in both IPv4 and IPv6 ISP networks. 15 out of 97 ASes in IPv4 networks remark the DSCP at the access network. Most of these set DSCP to CS0. Four ASes, however, map incoming DSCP to a new value as it enters the AS. For example, irrespective of all incoming DSCP values, one AS remarks to AF11 (i.e. high-throughput data), while another AS changes to CS1 (i.e. less than best effort) at the access network in IPv4. Another two ASes bleach the higher 3 bits of incoming IPv4 DSCP. This mapping results in unregistered code points (other than CS1 and CS0), making the traffic unclassified. IPv6 is different, with only 3 out of 47 ASes remarking the DSCP (all to CS0).

In Table IV, we see that 6 ASes for IPv4 clients remark DSCP *in-network* and 5 of them remark to DSCP 0. Only one AS remarks CS1 and EF to the decimal value of 1, while AF42 is reset to 0. For IPv6, we detect 3 ASes, and all of them reset the DSCP to 0.

We categorize the location of the DSCP change as *egress* when the last router of the client's AS changes the DSCP and the *responder* belongs to another AS. In Table IV, we see that 13 ASes in IPv4 remark the DSCP at the egress, and 9 of them simply reset it to CS0. In case of IPv6, three ASes reset the DSCP to 0 at the egress. In two ASes in IPv4, we see *egress* remarking with the mapping CS1→0, EF→6, AF42→4. One AS changes the DSCP to a decimal value of 2 when it forwards the traffic to another AS. At the egress of yet another AS, we observe a DSCP remarking to the unregistered code point 41.

Six out of 97 ASes (i.e., 6%) in IPv4 and 2 out of 47 ASes in IPv6 were categorized as *mixed*. In the IPv4 case, four of them reset the DSCP to CS0. In a particular AS, at the access network for both, IPv4 and IPv6 clients, we see a DSCP change only for AF42 (to AF41), while CS1 and EF remain unchanged.

To understand the importance of marking in the first-hop ISP, we investigate the number of ASes that let a DSCP value

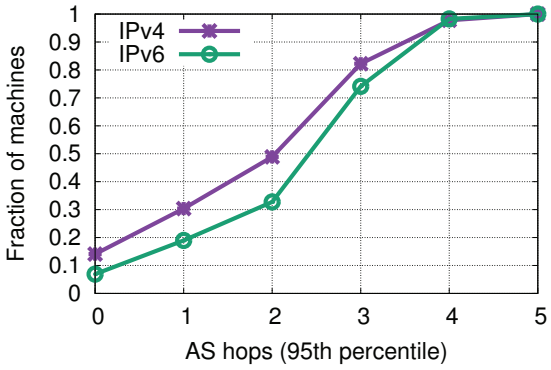


Figure 4: The number of ASes hops before the DSCP is remarked.

Parts of the network	#clients in IPv4	#clients in IPv6
Home network	35	8
First hop AS	67	20
Beyond the first hop AS	58	37
Total	160	65

Table V: A summary of the number of clients' DSCP getting affected in different parts of the network in IPv4 and IPv6

"survive" before it first becomes changed. Figure 4 provides a high-level overview of how long into the path DSCP code points remain unchanged. For each client we identify all paths with DSCP changes and the responsible AS-hop (the AS-hop where the DSCP value changes for the first (and possibly only) time). Then we use the 95th percentile of the responsible AS-hop as a measure of where changes typically occur, and subtract 1 from the value for plotting to show the AS number just *before* the AS that changed it. The DSCP markings survive the first hop AS (i.e. own AS) for 70% and 80% of the IPv4 and IPv6 clients, respectively. Notably, DSCP markings by 5% of all clients traverse 4 ASes without being remarked.

To summarize, we found that the most common re-marking behavior of the first-hop ASes (which we assumed to be the clients' and server's own ISP) was to zero the DSCP. Generally, as with the home gateways, chances of DSCP "survival" seem better with IPv6 than with IPv4. Also, with the exception of one AS, it appears that the choice of input DSCP value does not matter: the DSCP either remained unchanged, was zeroed, or changed into undefined values in our tests. Beyond the first-hop AS, 58 of the total of 160 IPv4 clients (IPv6: 37 out of 65) still have their DSCP value intact (see the Table. V). This is perhaps already good news for an application that may want to use the DSCP. Even more importantly, we have seen that a chosen DSCP can sometimes traverse several ASes before first becoming remarked. This also means that the DSCP could potentially be quite useful on short paths (e.g., within the same ISP).

C. DSCP Treatment beyond the first hop AS

In the following, we investigate the cases where DSCP markings survived past the first-hop ASes. The total number of ASes detected in our measurement is 298 for IPv4 addresses and 119 for IPv6 addresses. Excluding the clients' ASes from our measurement data, we found 180 ASes in IPv4 and 65 ASes in IPv6 core networks, respectively. We find that about 32% of the core ASes remark the DSCP code points. This percentage is consistent for both IPv4 and IPv6.

On some paths, DSCP values were changed multiple times. Table VI shows an example where they were changed particularly often, for a client from AS35432 that sent the code points CS1, AF42 and EF to a server in AS680. On this path, we saw the following decimal values of code points: 0 (CS0); 8 (CS1); 18 (AF21); 32 (CS4); 36 (AF42); 40 (CS5); 46 (EF). The table also presents the list of ASes whose routers respond with a code point received (inside the ICMP payload) over different TTL values. We explain the DSCP treatments by different ASes on the path in the following:

- [TTL 1-2]: At the home gateway, we observe a mapping EF→CS5, AF42→CS4, CS1→CS1 (remarking lower 3-bits to 000).
- [TTL 2-3]: No DSCP change was detected at the *egress* of the client's own AS (AS35432, CABLENET-AS, CY).
- [TTL 3-4]: At the *ingress* to AS1299, we detect a DSCP change to CS1 (CS4→CS1, CS5→CS1).
- [TTL 4-5]: At the *ingress* to AS174, the code points were changed to AF21.
- [TTL 8-9]: We observe a DSCP change to CS1 at the *egress* to AS174.
- [TTL 12-]: At an *in-network* router of AS680, DSCP was modified to CS0.

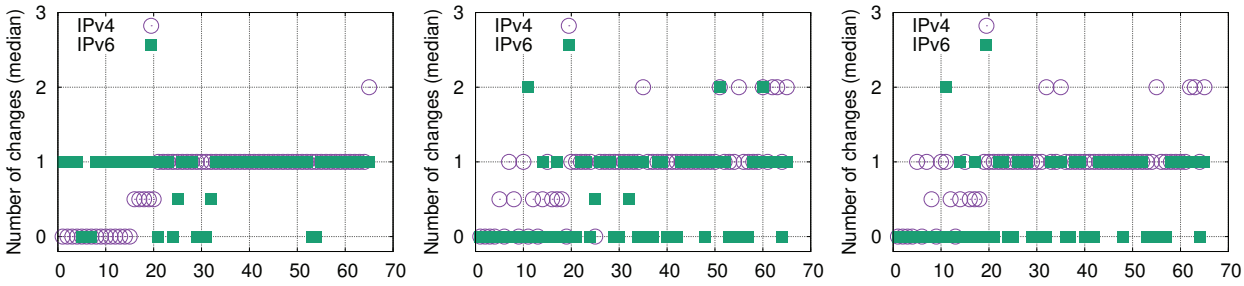
From the table, we observe that CS1 has changed 3 times while both AF42 and EF have changed 5 times.

Fig. 5 plots the fraction of paths both in IPv4 and IPv6 networks exhibiting the number of times a given code point (CS1, AF42 and EF) has changed over them. 25-27% of the paths in IPv4 networks do not change the DSCP code points whereas in IPv6 networks, AF42 and EF survive end-to-end on ≈44% of the paths, while CS1 survives on ≈32% of the paths.

We then compare the treatments of the code points inside the core networks for the clients that have both IPv4 and IPv6 addresses (a total of 65 clients). For each client, we consider all the forward paths and compute the number of modifications to each DSCP code point on each path. Fig. 6(a) presents the dot plot of the medians of the number of modifications for CS1 for all the clients with IPv4 and IPv6 addresses. The clients are sorted on the basis of increasing order of their median values for IPv4 paths. Figures 6(b) and 6(c) represent the dot plots for code points AF42 and EF. 36 clients with EF and 34 clients with AF42 have zero median in IPv6 paths while only 10 clients with CS1 have zero median. This shows clients with EF or AF42 are more likely to remain unchanged. However, IPv4 clients show a very different picture: only 7-15 clients with all code points observe no change in the DSCP values.

TTL	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ASes	35432	35432	1299	174	174	174	174	174	680	680	680	680	680	680	680
CS1 (8)	8	8	8	8	18	18	18	18	8	8	8	8	0	0	0
AF42 (36)	36	32	32	8	18	18	18	18	8	8	8	8	0	0	0
EF (46)	46	40	40	8	18	18	18	18	8	8	8	8	0	0	0

Table VI: An example showing the DSCP values (CS1, AF42, and EF) changing multiple times on a path



(a) CS1 in IPv4 and IPv6 (b) AF42 in IPv4 and IPv6 (c) EF in IPv4 and IPv6

Figure 6: Each dot represents the *median* of the distributions of the number of times a given DSCP has changed over all the forward paths from a host.

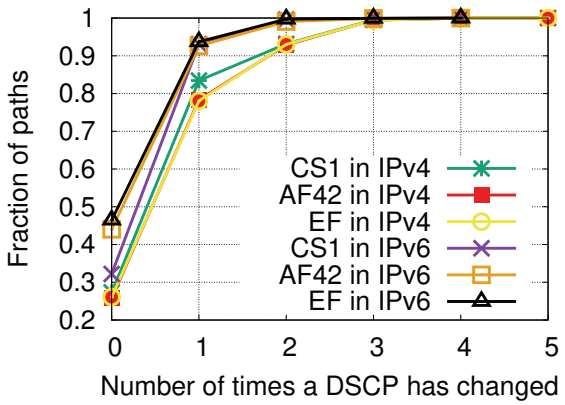


Figure 5: The number of times the DSCP values have changed over all the IPv4 and IPv6 paths

DSCP Policy	Description	#ASes
R-1	Remark higher 3-bits to 000 (for example, AF42→4)	18
R-2	Remark higher 3-bits to 001 (AF42→AF12)	5
R-3	Remark higher 3-bits to 010 (AF42→AF22)	2
R-4	Remark lower 3-bits to 000 (AF42→CS4)	2
R-5	Others e.g. all→ {AF11, AF21, AF31, CS1, CS0, CS4, CS7, 1, 2, 4, 6}	48

Table VII: DSCP policies. In the following, policy R-5 is indicated by the name of the code point—e.g., policy "CS0" means a remarking of "all→CS0".

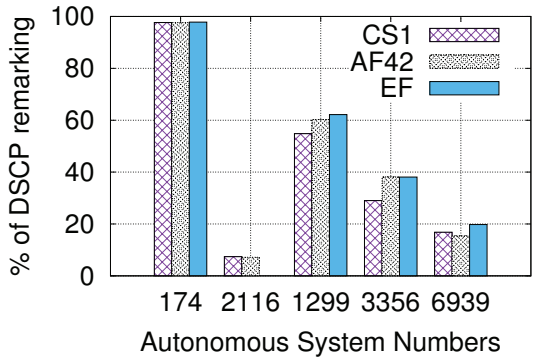
We collect and categorize the remarking policies followed by all the ASes that lie between the client and server ASes. Table VII presents all the identified DSCP policies along with the number of ASes that have exhibited them. The ASes in which a certain DSCP policy is applied are not mutually exclusive; for example, AS1299 exhibited seven different policies R-1, R-2, CS0, CS1, AF11, AF21 and 2.

Looking closer at individual ASes, we find evidence that some ASes implement policies based on AS relationships. For example, Cogent marks traffic from its peers as AF21 (low-latency data) and traffic from its customers as AF11 (high-throughput data).[10] Other ASes, however, do not seem to account for business relationships when remarking packets. In fact some ASes, like Telia, can remark packets from the same origin AS differently, which hints at an absence of a customer- or peering-agreement-specific' remarking policy.

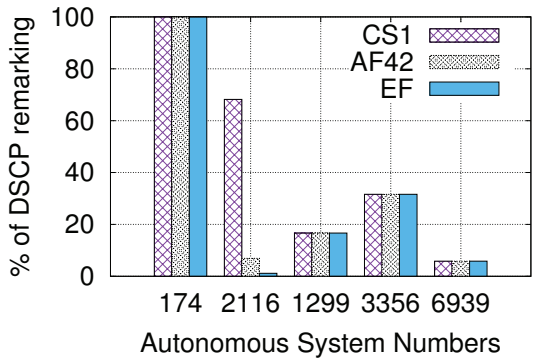
Figures 7(a) and 7(b) present the percentage of DSCP remarking by routers in a set of ASes for IPv4 and IPv6 topologies, respectively. These ASes are the top 5 ASes in each topology in terms of number of measured paths that cross them after removing educational networks. We remove education networks as we would like to focus on prominent transit providers. Thus, the top-five networks include four major global transit providers: Level-3 (AS3356), Telia (AS1299), Cogent (AS174), and HE (AS6939). In addition, they include Broadnet (AS2116), which is a major Norwegian transit provider. Broadnet is present on the top-five list because most of the NorNet servers and clients are located in Norway.

For each AS, we plot the percentage of DSCP remarking for each input DSCP value (CS1, AF42 and EF). Cogent remarks almost all IPv4 and IPv6 packets, while HE allows

[10]This marking behavior appears to be in line with a description given at https://groups.google.com/a/measurementlab.net/forum/#!msg/discuss/vcQnaZJO6nQ/ltfi_3Aif9gJ; this statement is, however, relatively old, and we have no evidence that this policy is still in place.



(a) IPv4



(b) IPv6

Figure 7: Percentage of DSCP remarking in ASes.

most marked packets to pass, especially for IPv6. Telia is more aggressive for IPv4, but Level-3 demonstrate a comparable chance of remarking for both IPv4 and IPv6. Finally, Broadnet allows most packets to pass, except that it always remarks IPv6 packets with a CS1 code point, which get remarked. Next, we provide more details about the remarking policies of these ASes.

1) Cogent: Cogent remarks all incoming packets, except for 3%, to either AF21 or AF11. The unchanged 3% correspond to the case where Cogent receives packets with AF21 and AF11 code points, i.e. the same values that are used when remarking. For example, AS2914, AS701 remark any DSCP values to AF21 at the egress before forwarding the packets to Cogent. We also detect the same code point AF21 when packets traverse from Cogent to AS220 or AS4538.

2) Broadnet: In IPv6 networks, we observe only *ingress* and *in-network* DSCP remarking in *Broadnet* — no DSCP remarking is observed at the egress. 68% of packets with CS1 are remarked; these packets are mainly traversing from AS2603 which is an educational network interconnecting Nordic countries. Some routers inside AS2116 networks also remark CS1 to AF11 or CS0. However, in IPv4 networks, we

DSCP Policy	Neighboring ASes (observed)	
	in IPv4 networks	in IPv6 networks
R-1	1299, 8966	1299
R-2	1299, 12956, 3701	-
CS0	5511, 6079, 6774, 29695, 30950	6774, 8422, 29695, 30950
CS1	680, 2119, 7922	680
AF11	2495	2495
AF21	174, 3741, 2200	-
CS7	34224	-

Table VIII: DSCP Policy in Level-3

observe only *in-network* DSCP remarking with CS1 to AF11 or CS0, AF42 to CS0 and EF remains unchanged. Incoming packets with DSCP value CS0 traverse this AS unchanged.

3) HE: HE seems to remark packets as they exit its network. There is no consistent remarking policy for all affected neighbors. However, the low extent of remarking and the lack of a consistent policy hint that these remarkings are possibly not carried by HE but rather by its neighboring ASes. This is in fact stems from a limitation in our methodology for identifying which end of a link has actually manipulated the DSCP code point. For example, in Fig. 3, R5 may remark the DSCP code point, for packets received from R4, before sending the ICMP response. Consequently, we blame the remarking on R4.

4) Telia: Telia appear to remark packets exchanged with 48 neighboring IPv4 ASes out of a total of 83 that are visible in our data set, as well as 4 out of the 28 visible IPv6 neighbors. We count a total of 8 remarking policies that happen at both egresses and ingresses. This large number of inconsistent policies highlights the need for further investigations to determine whether Telia can actually be blamed for all the remarkings.

5) Level-3: Table. VIII presents the DSCP policies along with the neighboring ASes in IPv4 and IPv6 networks. For *Level-3*, we only observe remarkings at the egress affecting 17 out of 65 IPv4 neighboring ASes and 7 out of 23 neighboring IPv6 ASes. The marking policies are consistent for neighbors that are present in both the IPv4 and IPv6 topologies, but inconsistent across neighbors. As for HE, this observation hints the measured remarkings are likely to be carried out by Level-3 neighbors.

In summary, the measured ASes employ a diverse set of remarking policies. Accordingly, it is unclear whether transit ASes are actively leveraging the DSCP code points in signaling. One AS – Cogent, however, seems to follow a specific remarking policy depending on whether packets traverse from a customer or a peer AS. We also observe that both Level-3 and HE do not seem to implement a remarking policy. This is good news since Level-3 and HE are the largest transit providers for IPv4 and IPv6, respectively.

VI. Conclusion

We set out on this investigation to answer whether a mechanism like the proposed QoS scheme for WebRTC [4] can work, in the hope of being able to give implementation advice. We were, in fact, afraid that this advice might turn out to be

complex: different input DSCP values can provoke different output DSCP values, and so highly detrimental things might happen, e.g., a low-latency request turning into lower-than-best effort marking. We found that such behavior hardly exists. Generally, the DSCP was kept intact, zeroed, or statically set to a certain value irrespective of the input. When the output *was* indeed a function of the input, the result was usually one of a set of undefined values, rather than a clear change of the expected semantics.

From our results, but also concurring with previously published work, we conclude that the DSCP is often changed, and particularly often zeroed. There is, however, hardly any evidence of a DSCP choice being counterproductive – with the rare but important exception of *blackholing*, i.e. the consistent deletion of packets only in the presence of a certain DSCP value. We therefore recommend that applications incorporate individual tests for all the values that they intend to use, to fall back to CS0 or a different value if consistent loss is seen with one of the others.

While we often saw that the DSCP value is changed or deleted along Internet paths, the number of ASes that a value "survives" can be significant, and – quite unsurprisingly – different ASes implement different DSCP policies. Thus, if an application has a choice between paths, possibly traversing different ISPs (as it is the case for our NORNET CORE nodes), it is worth testing them to see where the DSCP works better. This includes the possibility of favoring shorter paths over longer ones, to reduce the number of traversed ASes. Finally, we recommend to favor IPv6 over IPv4 if the DSCP is to be used. On IPv6 paths, the DSCP is much more likely to remain intact.

As WebRTC is being rolled out, a logical next step would be to passively measure if the chosen DSCP values really have an impact on the behavior the traffic sees, and if that behavior is in accordance with the DiffServ specification.

VII. ACKNOWLEDGMENTS

This work was partially funded by the European Union's Horizon 2020 Research and Innovation Programme through the NEAT project under Grant Agreement no. 644334. The views expressed are solely those of the authors.

REFERENCES

[1] D. Black and P. Jones, "Differentiated Services (Diffserv) and Real-Time Communication," IETF, Informational RFC 7657, Nov. 2015, ISSN 2070-1721.

[2] K. Nichols, S. Blake, F. Baker, and D. L. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," IETF, Standards Track RFC 2474, Dec. 1998, ISSN 2070-1721.

[3] H. T. Alvestrand, "Overview: Real Time Protocols for Brower-based Applications," IETF, Internet Draft draft-ietf-rtcweb-overview-19, Nov. 2017.

[4] P. E. Jones, S. Dhesikan, C. Jennings, and D. Druta, "DSCP Packet Markings for WebRTC QoS," IETF, Internet Draft draft-ietf-tsvwg-rtcweb-qos-18, Aug. 2016.

[5] A. Medina, M. Allman, and S. Floyd, "Measuring Interactions Between Transport Protocols and Middleboxes," in *Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC)*, Oct. 2004, pp. 336–341, ISBN 1-58113-821-0.

[6] ——, "Measuring the Evolution of Transport Protocols in the Internet," *SIGCOMM Computer Communication Review*, vol. 35, no. 2, pp. 37–52, Apr. 2005, ISSN 0146-4833.

[7] J. Pahdye and S. Floyd, "On Inferring TCP Behavior," in *Proceedings of the ACM SIGCOMM Conference*, Oct. 2001, pp. 287–298, ISBN 1-58113-411-8.

[8] M. Honda, Y. Nishida, C. Raiciu, A. Greenhalgh, M. Handley, and H. Tokuda, "Is it still possible to extend TCP?" in *Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC)*, Nov. 2011, ISBN 978-1-4503-1013-0.

[9] G. Detal, B. Hesmans, O. Bonaventure, Y. Vanaubel, and B. Donnet, "Revealing Middlebox Interference with Tracebox," in *Proceedings of the 13th ACM Internet Measurement Conference (IMC)*, Barcelona, Catalonia/Spain, Oct. 2013, ISBN 978-1-4503-1953-9.

[10] R. Craven, R. Beverly, and M. Allman, "A Middlebox-Cooperative TCP for a Non-End-to-End Internet," in *Proceedings of the ACM SIGCOMM Conference*, 2014, pp. 151–162, ISBN 978-1-4503-2836-4.

[11] I. R. Learmonth, B. Trammell, M. Kühlewind, and G. Fairhurst, "PATHspider: A Tool for Active Measurement of Path Transparency," in *Proceedings of the ACM, IRTF and ISOC Applied Networking Research Workshop (ANRW)*, Jul. 2016, ISBN 978-1-4503-4443-2.

[12] N. Weaver, C. Kreibich, M. Dam, and V. Paxson, "Here Be Web Proxies," in *Proceedings of the Passive and Active Measurement Workshop (PAM)*, Los Angeles, California/U.S.A., Mar. 2014, pp. 183–192, ISBN 978-3-319-04917-5.

[13] X. Xu, Y. Jiang, T. Flach, E. Katz-Bassett, D. Choffnes, and R. Govindan, "Investigating Transparent Web Proxies in Cellular Networks," in *Proceedings of the Passive and Active Measurement Workshop (PAM)*, New York/U.S.A., Mar. 2015, pp. 262–276, ISBN 978-3-319-15509-8.

[14] Z. Wang, Z. Qian, Q. Xu, Z. Mao, and M. Zhang, "An Untold Story of Middleboxes in Cellular Networks," in *Proceedings of the ACM SIGCOMM Conference*, Aug. 2011, pp. 374–385, ISBN 978-1-4503-0797-0.

[15] A. Müller, F. Wohlfart, and G. Carle, "Analysis and Topology-based Traversal of Cascaded Large Scale NATs," in *Proceedings of the ACM Workshop on Hot Topics in Middleboxes and Network Function Virtualization (HotMiddlebox)*, Dec. 2013, pp. 43–48, ISBN 978-1-4503-2574-5.

[16] B. Trammell and M. Kühlewind, "Observing Internet Path Transparency to Support Protocol Engineering," in *Proceedings of IRTF/ISOC RAIM Workshop*, Yokohama/Japan, Oct. 2015.

[17] R. Barik, M. Welzl, and A. Elmokashfi, "How to Say That You'Re Special: Can We Use Bits in the IPv4 Header?" in *Proceedings of the ACM, IRTF and ISOC Applied Networking Research Workshop (ANRW)*, Berlin/Germany, Jul. 2016, pp. 68–70, ISBN 978-1-4503-4443-2.

[18] B. Trammell, M. Kühlewind, P. D. Vaere, I. R. Learmonth, and G. Fairhurst, "Tracking Transport-layer Evolution with PATHspider," in *Proceedings of the ACM, IRTF and ISOC Applied Networking Research Workshop (ANRW)*, Prague/Czech Republic, Jul. 2017, pp. 20–26, ISBN 978-1-4503-5108-9.

[19] A. Custura, A. Venne, and G. Fairhurst, "Exploring DSCP Modification Pathologies in Mobile Edge Networks," in *Proceedings of the Network Traffic Measurement and Analysis Conference (TMA)*, Jun. 2017, pp. 1–6, ISBN 978-3-901882-95-1.

[20] R. Barik, M. Welzl, A. M. Elmokashfi, S. Gjessing, and S. Islam, "fling: A Flexible Ping for Middlebox Measurements," in *Proceedings of the 29th International Teletraffic Congress (ITC)*, Genoa/Italy, Sep. 2017, ISBN 978-0-9883045-3-6.

[21] J. Babiarz, K. H. Chan, and F. Baker, "Configuration Guidelines for DiffServ Service Classes," IETF, Informational RFC 4594, Aug. 2006, ISSN 2070-1721.

[22] L. Peterson and T. Roscoe, "The Design Principles of PlanetLab," *Operating Systems Review*, vol. 40, no. 1, pp. 11–16, Jan. 2006, ISSN 0163-5980.

[23] E. G. Gran, T. Dreibholz, and A. Kvalbein, "NorNet Core – A Multi-Homed Research Testbed," *Computer Networks, Special Issue on Future Internet Testbeds*, vol. 61, pp. 75–87, Mar. 2014, ISSN 1389-1286.

[24] T. Dreibholz, "NorNet – Building an Inter-Continental Internet Testbed based on Open Source Software," in *Proceedings of the LinuxCon Europe*, Berlin/Germany, Oct. 2016.

[25] ——, "An Introduction to Multi-Path Transport at Hainan University," Keynote Talk at Hainan University, College of Information Science and Technology (CIST), Haikou, Hainan/People's Republic of China, Dec. 2017.