Exploring DSCP modification pathologies in mobile edge networks

Ana Custura
University of Aberdeen

Andre Venne
University of Aberdeen

Gorry Fairhurst
University of Aberdeen

***Abstract*—Differentiated Services (DiffServ) provides a means for applications to classify traffic into Quality of Service (QoS) classes by reading the Differentiated Services Code Point (DSCP) field in the IP header and then mapping traffic to a specific QoS forwarding treatment. This paper provides new measurement data that examines how the DSCP is altered as packets traverse mobile broadband access networks. Results are presented for entire paths, differentiating between the access network behaviour and the rest of the path. Observing the DSCP seen at each router can be used to infer whether a packet is likely to receive an appropriate QoS treatment, and hence the level of support for DiffServ QoS. Our results identify two remarking pathologies, one for the mobile networks and the other for the Internet path.**

I. Introduction

Mobile networks have become performance-focused as a result of devices being used for streaming media content and for interactive applications [1]. These applications have a diverse range of network needs, many are sensitive to packet loss, performance is often impacted by delay, and some applications can consume significant capacity. The DiffServ model allows applications to classify traffic into QoS treatment classes by setting the DiffServ field in the header of an IPv4 or IPv6 packet. The marking in this field, or DSCP, informs the QoS treatment those packets receive.

Against the backdrop of increased interest in inter-domain DiffServ, the Prioritisation and Resilience in Emergency Communications (PREC) Experiment of the Measuring Mobile Broadband Networks (MONROE) Project is exploring whether mobile services can be combined with prioritised radio services to offer a QoS framework that is resilient and degrades gracefully following major network disruption. A prerequisite for this work is to understand the extent to which mobile networks pass DSCP markings, and specifically to understand how and where any changes take place. The desire for transport encryption further motivates a DiffServ approach, since options such as deep packet inspection can not be used to classify encrypted network traffic.

This paper explores path-level behaviour of DiffServ enabled packets in mobile networks to potentially identify behaviour which does not comply with the IETF specification or which has an undesired effect. For example, unexpected packet drops due to the use of a DSCP or instances of "priority inversion" where higher priority packets are remarked to a lower priority while other priorities are not remarked. Our study presents results from a survey using the MONROE platform. The measurement explore how DiffServ-marked packets are treated within a mobile operator's network and at its boundaries.

The following sections discuss the background to our study and details the experiment design. The results are then presented and discussed in the context of ongoing work in the IETF concerning WebRTC QoS [2] and DiffServ Interconnection [3]. We also present the implications of our results for DiffServ-enabled applications in a mobile environment and summarise our findings in the conclusion.

II. Background to Differentiated Services

The classification of traffic in Internet networks was first provided by the 8-bit Type of Service (ToS) field of the IPv4 header [4]. The first three of these bits served to classify traffic into 8 priority classes, and the remainder to specify the type of traffic sent. The small number of usable classes and the lack of support for relative priorities and drop precedence lead to the replacement of this framework.

In 1998 the DiffServ architecture repurposed the ToS field[5] [6], allocating the first 6 bits to specify a DSCP. The last 2 bits in the field were reserved for Explicit Congestion Notification, Explicit Congestion Notification (ECN).

The DSCP values are divided into three pools. The first pool of 32 codepoints is assigned to the IETF, of which 22 have registered well-known meanings. Table I specifies the commonly used codepoints and the classes inherited from backwards compatibility with the ToS field painted by the Class Selector (CS) codepoints.

Applications can implement QoS using DiffServ by setting the DSCP in the IP header. Routers at the ingress to a DiffServ domain [5] read the DSCP of each packet, and use this to decide how to treat the packet within the network. At the edge of a domain traffic conditioners determine if the DSCP marking is permitted. Unexpected DSCP values may be remarked (e.g., resetting to the default DSCP), packets may be shaped or dropped (the latter is not recommended [7]).

The DiffServ field controls admission to QoS classes when the DSCPs are mapped to a Behaviour Aggregate (BA) [5]. This causes the packet to enter a queue serviced by one of a set of specified forwarding treatments, known as Per-Hop Behaviours (PHBs). A simple treatment could map all DSCPs to a default (FIFO) PHB, the same as a network that does not implement DiffServ. The IETF also defines a range of standard PHBs and associates each with a well-known DSCP or collection of DSCPs, including the Assured

TABLE I
COMMONLY USED CODEPOINTS

Binary	Decimal	PHB class	Priority
000000	0	BE	Default, CS0
001000	8	CS1	Priority, Class Selector 1
001010	10	AF11	Low drop probability
001100	12	AF12	Medium drop probability
001110	14	AF13	High drop probability
010000	16	CS2	Immediate, Class Selector 2
010010	18	AF21	Low drop probability
010100	20	AF22	Medium drop probability
010110	22	AF23	High drop probability
011000	24	CS3	Flash, Class Selector 3
011010	26	AF31	Low drop probability
011100	28	AF32	Medium drop probability
011110	30	AF33	High drop probability
100000	32	CS4	Flash Override, Class Selector 4
100010	34	AF41	Low drop probability
100100	36	AF42	Medium drop probability
100110	38	AF43	High drop probability
101000	40	CS5	Critical/ECP, Class Selector 5
101100	44	VA	Voice Admit
101110	46	EF	Expedited Forwarding
110000	48	CS6	Internetwork Control, Class Selector 6
111000	56	CS7	Network control, Class Selector 7

Forwarding (AF) PHB [8] and the Expedited Forwarding (EF) PHB [9]. Operators may also implement their own PHBs and 16 codepoints (pool 2) are assigned for local operator use, and a further 16 have been provisionally assigned but may be utilised for future standardised assignments.

During its transmission across the Internet, a packet is likely to cross many networks and DiffServ domains. The ability to provide QoS treatment across networks relies on coordinated network operator effort to implement service policies. Where there is no such cooperation, there are no guarantees that the packet will receive the expected treatment, or that the contents of the DiffServ field will be forwarded intact. This has lead to DiffServ being perceived as an unreliable mechanism for requesting QoS treatment beyond the local network or administrative domain.

Recent work in ITU-T [10] and the IETF [3] has shown renewed interest in inter-domain use of DiffServ to help realise consistent QoS treatment within networks using MPLS. A recent GSMA document [11] that provides guideline for mobile backbones also helps coordinate inter-domain use of DSCPs within mobile networks.

III. RELATED WORK

A recent small-scale study [12] provided insight into end-to-end path behaviour when sending DSCP-marked packets from edge networks (mostly wireless), with mixed results. Results were presented for 185 paths showing DSCP-related failure for 10 to 13% of packets with specific codepoints. It also identified remarking behaviour on paths, most notably remarking to 0 and remarking to unassigned DSCPs. In comparison, this paper focuses on mobile edge networks to classify behaviour of routers along a path in the context of the DiffServ architecture.

A number of techniques have been used to measure various modifications of packets along Internet paths. The Tracebox [13] tool has measured modifications of the DiffServ field along the paths of 14,373 address pairs. It found a 5.75% modification rate for this field, but did not further explore the modifications. A study by CAIDA [14] analysed ICMP quotations resulting from sending probes to 84393 web servers, finding an in-flight modification rate of 2.9% for the DSCP/ECN byte, but did not seek to identify where and in what way this modification occurred.

A large scale measurement study [15] investigated the end-to-end path transparency for Explicit Congestion Notification, ECN across the Alexa top 1 million web servers. The study found that for IPv4 hosts, 94.8% successfully received the ECN codepoint intact. In the context of this paper, we note that the ECN field is a part of the same byte as the DSCP field in the IP header. This provides some evidence that the majority of routers in the core of the Internet do not bleach (set to zero) the whole byte.

PATHspider [16] recently added a DSCP plugin for testing codepoint-dependent connectivity failure. Tests were run in September 2016 and January 2017 to test for connectivity failure in the Internet core from seven vantage points hosted by Digital Ocean in Amsterdam, Frankfurt, London, New York, San Francisco, Singapore, Toronto and Bangalore. Connections to the same 673,230 IP addresses from each vantage point found no evidence of DSCP-dependent failure for 99.95% of the targets tested for DSCP 46 (EF). The implication for this study is that packets which exit a mobile access network will not experience DSCP-dependent connectivity failure for the remainder of their path.

IV. EXPERIMENT DESIGN

We developed a tool used for measuring the DSCP marking behaviour of deployed mobile networks, inspired by [13]. The tool has three components: an active traffic generator, a packet capture module and an analysis module. Figure 1 illustrates the tool architecture. It is important to note this tool does not assess the deployment of PHBs, since we do not have a way to measure the QoS experienced at the received endpoint nor the level of congestion at the routers on the network path.

The traffic generator component is based on the Scapy[1] packet forging library and sent packets towards a target IP address. A packet capture module ran in the background, recording all received Internet Control Message Protocol (ICMP) type 11 messages associated with the test. A measurement vantage point is the system and associated network interface that forwarded the generated traffic and captured the ICMP replies. Initially, packets are sent with an IPv4 Time-to-Live (TTL) (or IPv6 Hop Count) value of 1. Each router forwarding a packet decrements the TTL. If a router finds that the TTL has expired (has a value 0), an ICMP type 11 (Time to Live Exceeded in Transit) or ICMPv6 type 3 (Hop Limit Exceeded in Transit) message is generated and sent to the sender of the packet. These ICMP messages also contain a quotation of the

[1] http://www.secdev.org/projects/scapy/

packet that triggered their generation, typically containing at least the IP and transport layer headers.

After each round of captured ICMP messages, the requests and ICMP messages were recorded and grouped into flows. Autonomous System (AS) information was added for the routers originating the ICMP messages were determined using RIPEstat API[2]. The TTL was then incremented, and the process repeated, up to a maximum of 30 hops. The flow and AS information for each hop were then processed by an analysis module, enabling us to make path observations. Some routers are known to either filter ICMP packets, or to rate-limit their generation. This will result in no collected samples for these routers. A study [17] on traffic differentiation and loss rate measured the correlation between packet loss and ICMP type 11 rate limiting for probes sent at different intervals and found that one probe per second per path did not trigger rate limiting in routers.

Our tool was used in a measurement campaign between December 2016 and February 2017 to collect DiffServ path-level data for packets sent from mobile-edge sources. We tested both TCP (using SYN packets with a high-numbered TCP port) and UDP (using datagrams with a high-numbered UDP port). Port 53 was not used for UDP, since we observed that some mobile operators block DNS queries to encourage use of a carrier-provided DNS service. Similarly, traffic with TCP port 80 may be redirected to web proxies in the mobile edge network. The target IP addresses were drawn from a random selection from the Alexa Topsites list[3].

We used the MONROE mobile platform. This provides dedicated infrastructure for Mobile Broadband (MBB) experimentation [18] and comprises over 250 mobile connected nodes distributed in four European countries: Italy, Spain, Norway and Sweden. Each node on the platform is connected to up to three MBB providers and often also to WiFi. The platform was designed for experiments to measure the performance and reliability of MBB networks and has support for metadata collection. It provides "Experiments as a Service" to its external users facilitating experiment executions via Docker containers. The number of vantage points for our measurements in each country and the list of providers is detailed in table II.

V. Results

Data from over 107 mobile vantage points spanning 12 MBB providers was collected against a target list of 86 IPv4 targets, for a total of 9202 different source-destination pairs. For each pair, for both TCP and UDP, the following codepoints were sent: Best Effort (BE), CS1, AF11, AF21 AF31, AF41, CS5, EF, and the unassigned codepoints: 2 and 3.

Finally, due to the scheduling availability of nodes within the platform, the amount of data collected for each DSCP and transport protocol varies. Different DSCPs will not be compared against each other unless a significant amount of data has been collected from the same vantage point.

[2]https://stat.ripe.net/

[3]http://www.alexa.com/topsites

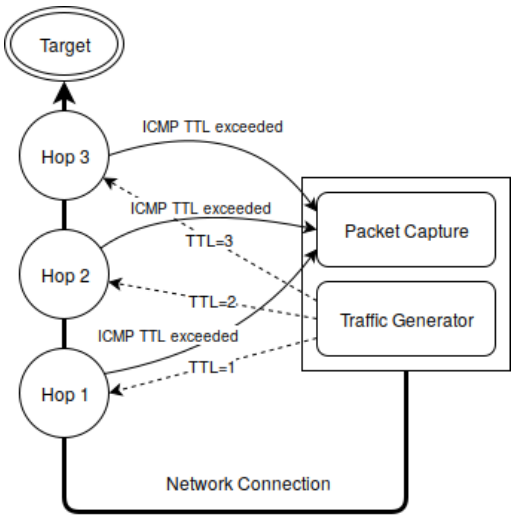

Fig. 1. Block diagram illustrating the architecture of our traceroute-like tool used in our measurements and the flow of traffic during use.

TABLE II
Country/MBB operator information

Country	Italy	Spain	Sweden	Norway
Operator 1	Vodafone	Orange	Telenor	Telenor
Operator 2	TIM	Yoigo	Telia	Telia
Operator 3	WIND	Vodafone	HI3G	NetCom
Vantage points	38	36	23	10

A. Transport-Dependent Remarking

To detect transport dependent remarking, we used data collected from the same 16 vantage points considering TCP and UDP flows. This used 1376 address-destination pairs per transport, distributed across 8 mobile operators in 3 countries.

We compared the remarking results for UDP traffic against those for TCP traffic. Table III presents DSCP modification pathology data, while table IV presents the percentage for TCP versus UDP at the last observed hop when sending EF.

The results for TCP and UDP agreed within a margin of 1%. We suggest this small difference is a result of transient measurement conditions such as congestion or ICMP rate limiting, and conclude we saw no evidence of transport-dependent remarking of a DSCP. This is consistent with our expectation that DiffServ processing occurs at the network-layer. We therefore combine results for TCP and UDP tests

TABLE III
Summary results for DSCP modification pathologies, TCP versus UDP summary

TCP 478 *routers*		**UDP** 461 *routers*		**Description**
routers	pct	routers	pct	
411	85.9%	399	86.5%	Transparent
30	3.4%	26	5.6%	Reset DiffServ field
24	1.0%	24	5.2%	Reset upper 3 bits of DiffServ field
12	2.5%	20	2.6%	Other remarking

TABLE IV
SUMMARY RESULTS FOR THE CODEPOINTS SEEN AT THE LAST OBSERVED HOP OF THE PATH FOR THE EF CODEPOINT, TCP VERSUS UDP

TCP 581 *paths*		**UDP** 581 *paths*		**DSCP Observed**
paths	pct	paths	pct	
223	38.3%	225	38.7%	BE
281	48.3%	278	47.8%	EF
46	7.9%	49	8.4%	6 †
14	2.4%	14	2.4%	CS1
7	1.2%	7	1.2%	41 ‡
10	1.7%	8	1.3%	Others

† This non-standard codepoint can be the result of the higher 3 bits of the DSCP field being bleached.
‡ This is a non-standard codepoint whose presence cannot be explained by common bit level manipulations that have been observed.

TABLE V
NUMBER OF NETWORKS TRAVERSED WITHOUT MANIPULATION OF A CODEPOINT (9202 *paths*)

	1	2	3	4	5	>5	∞
BE	28.6%	22.9%	22.7%	22.6%	22.3%	22%	21.4%
3	15.2%	8.3%	8.3%	8.3%	7.5%	7.2%	6.3%
CS1	40.4%	35.6%	35.6%	35.0%	31.2%	28.1%	24.0%
AF11	46.4%	39.1%	38.8%	37.9%	34.2%	30.7%	25.8%
AF21	43.4%	38.8%	38.8%	34.9%	30.7%	27.0%	23.1%
AF31	40.5%	35.6%	35.6%	35.0%	31.5%	28.0%	24.1%
AF41	40.4%	35.6%	35.6%	35.2%	31.6%	27.5%	23.1%
CS4	39.6%	34.8%	34.8%	34.5%	30.6%	27.1%	23.1%
EF	40.3%	35.6%	35.6%	35.3%	31.5%	28.0%	23.8%

from distinct vantage points in the following subsections to increase our dataset. This combined data spans 12 mobile operators in 4 countries and 9202 address-destination pairs.

B. Preservation of DSCP marking across networks

Mobile networks usually place their IPv4 users behind a NAT, to conserve public address space. On average, the packets we sent traversed at least 2 (2.58) hops before exiting an operator network. This was calculated as the number of hops up to the first public address seen on the path. However, these first hops on the path are the most likely to have been affected by ICMP rate limiting, and expect this number to be higher [19]. Table V considers DSCP remarking by number of hops traversed.

Between 8.3% and 39.1% of DSCPs traversed the second hop on the path without remarking. This is an indication of remarking within operator networks, with almost two-thirds of the DSCPs overwritten within the first hops on the path. Surprisingly, this is also the case for DSCP 0, which was expected to remain unchanged, but saw a 77.1% change before exiting the operator's network. Unknown codepoint 3 sees by far the most aggressive remarking, with more than 90% of packets remarked before exiting the operator's network.

Table VI shows remarking at the first hop of the operator network. Each row shows the DSCP sent, and the rate of remarking for that DSCP. At the first hop on the path, we observed that packets were remarked irrespective of the initial DSCP value, to either 0 (BE), 10 (AF11), 12 (AF12), 14 (AF13) and 18 (AF21). No other remarking was observed. Between 53.7% and 84.8% of packets were remarked at this hop.

TABLE VI
COMMON REMARKING SEEN AT FIRST HOP

	BE	AF11	AF12	AF21	AF14	Total
0 (BE)	N/A	12.6%	21%	10.5%	27.2%	71.3%
3	10.3%	12.8%	23.1%	12.7%	25.8%	84.8%
8 (CS1)	2.9%	5.9%	11.9%	2.9%	35.7%	59.5%
10 (AF11)	3.1%	N/A	11.9%	2.9%	35.7%	53.7%
18 (AF21)	3.0%	5.9%	11.9%	N/A	35.7%	56.5%
26 (AF31)	2.9%	5.9%	11.9%	2.9%	35.6%	59.4%
34 (AF41)	2.9%	5.9%	11.8%	2.9%	35.7%	59.5%
40 (CS4)	4.0%	4.0%	12.1%	4.0%	36.2%	60.4%
46 (EF)	3.0%	4.0%	12.1%	2.9%	35.7%	57.9%

TABLE VII
COMMON REMARKING AT THE LAST HOP OF THE OPERATOR NETWORK

	BE	Unchanged	6	AF11	Others
0 (BE)	N/A	73.4%	8.9%	10.0%	7.5%
3	60.3%	8.33%	12.3%	10.9%	8.0%
8 (CS1)	53.9%	35.8%	2.3%	2.1%	5.7%
10 (AF11)	53.9%	37.7%	2.3%	N/A%	5.9%
18 (AF21)	53.9%	36.1%	2.3%	2.1%	5.3%
26 (AF31)	53.8%	35.6%	2.3%	2.1%	6.0%
34 (AF41)	53.8%	35.6%	2.3%	2.1%	6%
40 (CS4)	52.9%	34.7%	3.2%	2.8%	6.2%
46 (EF)	48.1%	35.6%	2.3%	2.1%	11.7%

Table VII shows the percentages of DSCPs observed at the last hop within the operator network. Each row shows a sent DSCP. This shows evidence of a second round of remarking, specifically, DSCP values being reset to BE. Overall, only up to 35% of DSCPs traverse the operator network unchanged, and between 29% and 58% of the packets exit the operator network with a DSCP of 0 (BE). AF11 and the unassigned DSCP 6 also consistently appear at the last hop on the path. DSCP 6 is explored in the following subsection, and is consistent with routers that perform operations based on ToS semantics.

C. DSCP remarking pathologies

This section studies the remarking pathologies of 705 routers across 63 ASs, each of which saw half or more the number of initial DSCPs sent. Table VIII shows the result across all hops seen.

82.9% of the surveyed routers were transparent to DSCP, abiding by [7] hat recommends unassigned marks are forwarded unchanged within a DiffServ domain.

6.4% of routers bleached the DiffServ field. [5] recommends using a default PHB when no other agreements are in place when transiting networks. 4.7% of routers reset the upper 3 bits of the DiffServ field. Table IX shows the remarking pathologies for hops in the operator networks, up to the first public IP address. The percentage of unmodified DSCPs drops significantly compared to the total observed in the previous table. Only 5% of routers were transparent to DSCP. The next prevalent behaviour is remarking all packets to AF13 (48.3%), followed by remarking to AF12 (21.6%), AF11(13.3%) and

TABLE VIII
SUMMARY FOR DSCP MANIPULATION PATHOLOGIES OBSERVED IN INDIVIDUAL ROUTERS

Observations 701 $routers$		Description
routers	pct	
581	82.8%	Transparent
45	6.4%	Reset DiffServ field
33	4.7%	Reset upper 3 bits of DiffServ field
22	3.1%	Reset to AF13
8	1.1%	Reset to AF11 and AF12
12	1.7%	Other remarking

TABLE IX
DSCP MANIPULATION PATHOLOGIES OBSERVED IN OPERATOR NETWORKS

Observations 60 $routers$		Description
routers	pct	
3	5.0%	Transparent
8	13.3%	Reset to AF11
13	21.6%	Reset to AF12
29	48.3%	Reset to AF13
6	10%	Reset to AF21
1	1.6%	Reset DiffServ field

AF21(10%). There is little evidence of DSCP bleaching and no evidence of ToS-based remarking within the operator networks.

D. Country and operator dependent remarking

We explored observed remarking pathologies, grouping results by country and operator. The Spanish, Italian and Swedish operators fully remarked all codepoints for the dataset. Italian operators remarked to AF11 (Wind, TIM) and AF12 (Vodafone); Spanish operators remarked to AF21 (Orange), AF12 (Yoigo, Vodafone occasionally) and AF11 (Vodafone); Norwegian operators remarked to AF13 (Telenor, Telia, NetCom), but not consistently; and Swedish ones to BE (Telenor), AF11 (HI3G) and AF13 (Telia Mobile). Packets with a DSCP of AF21 were remarked to BE for Vodafone in Spain, whereas packets with other marks were remarked to AF21.

VI. DISCUSSION

A. Impact of MBB remarking

Inside the operator networks that we studied, we observed remarking to several values dependent on country and mobile operator. This was irrespective of the DSCP sent, implying a remarking to a non-BE default PHB or a different network-wide DiffServ policy. In the case of Orange in Spain, all traffic was remarked to AF21, apart from AF21 traffic itself. This is an example priority inversion, because traffic marked CS1 was remarked to AF21, while AF21 traffic was remarked to BE. The same happens for Italy in the case of AF11 for WIND, where all codepoints get remarked to AF11, apart from AF11 traffic itself which is remarked to BE.

4.6% of routers reset the DiffServ field. Based on table VII this appears the prevalent behaviour at the last hop of an operator network, with BE constituting more than 48% of DSCPs observed at the first public address on a path. This bleaching causes all packets to be treated as part of the same BA for the remainder of their path.

B. Impact of ToS-based remarking

The most prevalent observed pathology was for routers to reset only the highest three bits of the DiffServ field, implying that there are still many routers(4.7%) that apply the former ToS semantics to this field. However, changing the high-order bits of the field without updating the remainder of the field can lead to unknown DSCPs on the remainder of the path. As an example, we observed DSCP 6 at the end of path results for nearly all original DSCP values. Moreover, 38.2% of the surveyed routers in the operator network remark packets with a DSCP of AF13 (14) within the first few hops of the path. ToS bleaching performed on DSCP 14 results in packets being assigned DSCP 6 for the remainder of the path, which explains this DSCPs observed in the results at the end of path.

Although not ideal, the use of DiffServ with routers using ToS semantics can be considered safe, even packets will likely then not receive the desired PHB for the remainder of the traversed path. If routers were configured to use DiffServ, the rate of unknown codepoints at the end of path would significantly reduce. For example, all routers currently resetting the first three bits would reset the entire DiffServ field instead (leading to codepoint 0). A better alternative would be to pass the DSCP value unchanged.

C. Recommendations for applications selecting a DSCP

WebRTC provides web browsers and mobile applications with Real-Time Communication (RTC) capabilities. A set of DSCPs for Internet use have been recommended [2]. BE is recommended for low priority, EF for voice, and a set of AF class markings for video traffic. Our results show that traffic with these markings was deterministically remarked within mobile networks. However, in the case of transparent mobile networks, ToS bleaching and DiffServ bleaching were also encountered further in the path, and may impact the ability of the remote endpoint to determine the desired DSCP and apply this at the remote edge. This is a pity for WebRTC, which often utilises peer-to-peer connections.

Our results show that it is safe to enable DSCP marking for applications. There is very little evidence of packet loss due to using a specific DSCP or priority inversion caused by remarking. A mobile application can expect to sometimes exploit the benefits the DiffServ locally, but is likely to also experience aggressive remarking in the mobile network. Beyond the carrier network, routers using ToS semantics are the greatest hindrance, because these can lead to unknown codepoints that prevent packets from receiving the desired PHB in the later part of the path.

D. Recommendations for DiffServ Intercon

Work on DiffServ Interconnection [3] defines a set of four common QoS classes and four auxiliary classes, to which DiffServ marked traffic may be mapped. This comes as a recent

operator interest in deploying PHBs supported by DiffServ markings in their networks. It specifically targets the desire to simplify operations between separately administered networks using MPLS Short-Pipe tunnel mode for interconnection. This has the potential to extend consistent DiffServ treatment across network boundaries.

While there is evidence that the mobile operators already use DiffServ within their networks, none of the non-BE markings recommended by Intercon were amongst the ones observed to be used by European mobile providers. We also did not observe evidence that using any of the recommended well-known codepoints will significantly increase or decrease the probability of successful traversal through current mobile networks.

VII. Conclusion and next steps

This work explored DSCP traversal pathologies in mobile networks in four countries to a set of Internet paths. Results show remarking within the mobile networks. In most cases, the remarking was irrespective of the initial DSCP. This suggests that setting a DSCP value is unlikely to influence the full path over which a packet travels. There is a high chance (47% and 100%) that any mark will be replaced within the first two hops of the path. The survivability of markings was not dependent on the transport. All DSCPs were uniformly treated by the mobile networks.

The paths beyond the mobile network display transparency, although some unwanted pathologies remain resulting in non-standard DSCP re-marking. ToS semantics were observed in the remarking patterns. The measurement techniques presented in this paper help identify which routers require updating. The remarking could be be avoided by replacing or reconfiguring old equipment.

VIII. Acknowledgements

This work is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 644399 (MONROE) through the Open Call. The European Commission is not responsible for any use that may be made of that information.

References

[1] F. Agboma and A. Liotta, "Quality of experience management in mobile content delivery systems," *Telecommunication Systems*, vol. 49, no. 1, p. 8598, 2010.

[2] S. Dhesikan, D. Druta, P. Jones, and C. Jennings, "DSCP Packet Markings for WebRTC QoS," Internet Engineering Task Force, Internet-Draft draft-ietf-tsvwg-rtcweb-qos-18, Aug. 2016, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-ietf-tsvwg-rtcweb-qos-18

[3] R. Geib and D. L. Black, "Diffserv-Interconnection classes and practice," Internet Engineering Task Force, Internet-Draft draft-ietf-tsvwg-diffserv-intercon-14, Dec. 2016, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-ietf-tsvwg-diffserv-intercon-14

[4] J. Postel, "Internet Protocol," RFC 791 (INTERNET STANDARD), Internet Engineering Task Force, Sep. 1981, updated by RFCs 1349, 2474, 6864. [Online]. Available: http://www.ietf.org/rfc/rfc791.txt

[5] K. Nichols, S. Blake, F. Baker, and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," RFC 2474 (Proposed Standard), Internet Engineering Task Force, Dec. 1998, updated by RFCs 3168, 3260. [Online]. Available: http://www.ietf.org/rfc/rfc2474.txt

[6] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services," RFC 2475 (Informational), Internet Engineering Task Force, Dec. 1998, updated by RFC 3260. [Online]. Available: http://www.ietf.org/rfc/rfc2475.txt

[7] D. Grossman, "New Terminology and Clarifications for Diffserv," RFC 3260 (Informational), Internet Engineering Task Force, Apr. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3260.txt

[8] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski, "Assured Forwarding PHB Group," RFC 2597 (Proposed Standard), Internet Engineering Task Force, Jun. 1999, updated by RFC 3260. [Online]. Available: http://www.ietf.org/rfc/rfc2597.txt

[9] B. Davie, A. Charny, J. Bennet, K. Benson, J. L. Boudec, W. Courtney, S. Davari, V. Firoiu, and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)," RFC 3246 (Proposed Standard), Internet Engineering Task Force, Mar. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3246.txt

[10] *Quality of service mapping and interconnection between Ethernet, Internet protocol and multiprotocol label switching networks*, International Telecommunication Union ITU-T Recommendation Y.1566, Jul. 2012. [Online]. Available: https://www.itu.int/rec/T-REC-Y.1566-201207-I/en

[11] GSM Association, "Guidelines for IPX Provider Networks Version 12.0," 2016, http://www.gsma.com/newsroom/wp-content/uploads/IR.34-v12.0.pdf.

[12] R. Barik, M. Welzl, and A. Elmokashfi, "How to say that you're special," *Proceedings of the 2016 workshop on Applied Networking Research Workshop - ANRW 16*, 2016.

[13] G. Detal, B. Hesmans, O. Bonaventure, Y. Vanaubel, and B. Donnet, "Revealing middlebox interference with tracebox," 2013.

[14] D. Malone and M. Luckie, "Analysis of ICMP Quotations," in *Proceedings of the 8th International Conference on Passive and Active Network Measurement*, ser. PAM'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 228–232. [Online]. Available: http://dl.acm.org/citation.cfm?id=1762888.1762920

[15] B. Trammell, M. Kühlewind, D. Boppart, I. Learmonth, G. Fairhurst, and R. Scheffenegger, "Enabling Internet-Wide Deployment of Explicit Congestion Notification," in *Passive and Active Measurement Conference*, Brooklyn, USA, 2015, pp. 193–205.

[16] I. R. Learmonth, B. Trammell, M. Kühlewind, and G. Fairhurst, "PATHspider: A tool for active measurement of path transparency," in *Proceedings of the 2016 Applied Networking Research Workshop*, July 2016, pp. 62–64.

[17] Y. Zhang, Z. M. Mao, and M. Zhang, "Detecting traffic differentiation in backbone isps with netpolice," in *Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement*, ser. IMC '09. New York, NY, USA: ACM, 2009, pp. 103–115. [Online]. Available: http://doi.acm.org/10.1145/1644893.1644905

[18] Ö. Alay, A. Lutu, D. Ros, R. Garcia, V. Mancuso, A. F. Hansen, A. Brunstrom, M. A. Marsan, and H. Lonsethagen, "Monroe: Measuring mobile broadband networks in europe," in *Proceedings of the IRTF & ISOC Workshop on Research and Applications of Internet Measurements (RAIM)*, 2015.

[19] J. Postel, "Internet Control Message Protocol," RFC 792 (INTERNET STANDARD), Internet Engineering Task Force, Sep. 1981, updated by RFCs 950, 4884, 6633, 6918. [Online]. Available: http://www.ietf.org/rfc/rfc792.txt