On the Usage of DSCP and ECN Codepoints in Internet Backbone Traffic Traces for IPv4 and IPv6

Nils Rodday*†, Klement Streit*, Gabi Dreo Rodosek*, Aiko Pras†
*Research Institute CODE, Bundeswehr University Munich
{nils.rodday, klement.streit, gabi.dreo}@unibw.de
†DACS Research Group, University of Twente
a.pras@utwente.nl

***Abstract*—Differentiated Services Code Points are values that can be used on IP packets to mark traffic and allow for different Quality of Service treatment during the traversal through a network. Explicit Congestion Notifications are used to indicate that congestion on a network occurred. Both values are encoded in the previously called Type of Service field in the IP header. In this paper, we look at codepoint values for DSCP and ECN in relation to the ports used on the transport layer, which lets us infer the application that is generating the traffic. We provide new measurement data by analyzing traffic from Internet backbone links collected by CAIDA from the months March, April, and May 2018 in New York City. Our results show that DSCP codepoints are rarely used in IPv4 but even less in IPv6. Moreover, most traffic using DSCP codepoints is only using default values and not values designed for prioritization of packets. ECN-enabled traffic is scarce in IPv4, while in IPv6 it appears to be neglectable. However, we could observe differences for certain application traffic in the usage of DSCP and ECN codepoints and elaborate on their distribution.**

***Index Terms*—Internet Measurements, Traffic Analysis, Quality of Service, Type of Service, Differentiated Services Code Point, Explicit Congestion Notification**

I. Introduction

The Internet only provides best effort services and does not provide delivery or performance guarantees. However, since the very beginning of the standardization of the Internet Protocol (IP), Quality of Service (QoS) was recognized as an important topic. The Type of Service (TOS) and Traffic Class (TC) fields were included in the IPv4 and IPv6 headers, reserving 8 bits for the use of QoS mechanisms to allow prioritization of packets on their way through the routing infrastructure. In IPv6, an additional 20 bit flow label was added to the header. Later on the need for more advanced QoS mechanisms arose and Differentiated Services Code Point (DSCP) and Explicit Congestion Notification (ECN) were encoded into the existing 8 bit field.

This paper aims at providing insights into the actual use of DSCP and ECN values. We therefore take real world Internet traffic traces and analyze those by looking at DSCP and ECN values in the IP header. In order to draw conclusions on the actual use of applications emitting the traffic, we also look at the port in the TCP and UDP headers. The combination of both gives us the opportunity to make statements about the distribution of DSCP and ECN codepoints in traffic of specific applications.

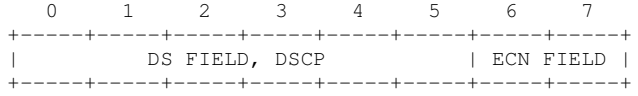


Fig. 1. DSCP and ECN

The TOS field underwent several redefinitions introduced by multiple Request for Comments (RFCs). RFC 791 originally defined the first 3 bits as precedence bits, followed by 3 bits for TOS behaviour and the last 2 bits set to zero [1]. Those last 2 bits were included for usage in the TOS field in RFC 1122, while RFC 1349 again declared the last bit as Must Be Zero [2] [3]. RFC 2474 renamed the TOS octet of the IPv4 header, and Traffic Class octet of the IPv6 header, to the Differentiated Services (DS) field [4]. According to the definition, the DS field takes up the first 6 bits, leaving 2 bits as Currently Unused (CU) bits. 64 Differentiated Services Code Points (DSCP) were defined and encoded in the DS field to represent the priority of a packet. Those DSCP values themselves are contained in categories called Class Selectors (CS), which can be found in Table I. In order to support legacy systems that do not implement the newest standard, the first 3 bits in the Class Selector range are mapping to the precedence bits of the previous interpretation. Therefore, even systems following the old standards are still able to understand primitive QoS commands issued by the sender. The latest RFC 3168 specified that the CU bits are now being used for Explicit Congestion Notifications (ECNs), again utilizing all available 8 bits of the field [5]. Figure 1 illustrates the latest definition.

978-1-7281-1244-2/19/$31.00 ©2019 IEEE

TABLE I
QOS MAPPING IN THE IP HEADER

DSCP	Binary	IP Precedence	Assured Forwarding class
CS0	000 xxx	Routine	Best effort
CS1	001 xxx	Priority	AF11/AF12/AF13
CS2	010 xxx	Immediate	AF21/AF22/AF23
CS3	011 xxx	Flash	AF31/AF32/AF33
CS4	100 xxx	Flash Override	AF41/AF42/AF43
CS5	101 xxx	Critical	Expedited Forwarding
CS6	110 xxx	Internet	
CS7	111 xxx	Network	

Within CS1 - CS4 we find Assured Forwarding (AF) classes that relate to drop probabilities. The lower the AF class within each CS the lower the drop probability, meaning that a packet of AF13 will more likely be dropped than AF12 or AF11 once all queues are filled up. Expedited Forwarding (EF) is only using the DSCP codepoint '101110' and provides latency sensitive application support.

The ECN-Capable Transport (ECT) is expected to use the codepoint '00' in case the packet is not using ECN. Either of the ECT codepoints '10' and '01' can be used by the originator to indicate that end-points are ECN-capable. However, it is recommended to use '10' by default for ECN-capable transport. The remaining codepoint '11' is standardized as Congestion Experienced (CE), which will indicate to the sender that during traversal of the network the packet experienced congestion.

The remainder of this paper is organized as follows. Section II provides insights into previous work in this area of research. Section III gives an overview over the datasets we used and how the data was provided and utilized. Section IV explains the methodology we followed and section V shows the results of this work. We close this paper with a conclusion and outlook for future work in section VI.

II. RELATED WORK

Since Differentiated Services (DiffServ) was standardized by the IETF in 1998, most publications regarding QoS measurements are fairly old. Our work is inspired by Li et al. from 2000 [6]. The authors also analyze QoS mechanisms in combination with most frequently used ports and infer the applications used based on that information. It turned out, that 90 % of the traffic did not use any TOS field markings. Firstly, the aforementioned paper is quite old and we could not rely on such old data for further research. Secondly, they only look at pre-Diffserv Internet traffic and analyze the TOS field as a whole, while we take the analysis a step further by differentiating between DSCP and ECN codepoints. Also, we elaborate on their specific shares in our dataset for each of the dominant codepoints.

Harju & Kivimki [7] and Fgee et al. [8] look at differences in performance of IntServ and DiffServ but do not touch on how often different DiffServ classes are used. John & Tafvelin [9] also look at the TOS field as a whole. According to their analysis, 83.10 % of traffic is leaving the entire TOS field unmarked.

TABLE II
DATASET DETAILS

Parameter Name	Parameter Value
Size	862 GB
IP Packets	23.068.218.935
IPv4 Packets	22.378.254.175 (97,01 %)
IPv6 Packets	690.664.760 (2,99 %)
TCP Packets	18.839.683.956 (81,67 %)
TCP over IPv4	18.325.521.937 (79,44 %)
TCP over IPv6	514.162.019 (2,23 %)
UDP Packets	3.830.798.847 (16,61 %)
UDP over IPv4	3.700.615.725 (16,04 %)
UDP over IPv6	130.183.123 (0,56 %)
ICMP Packets	201.741.395 (0,88 %)
ICMP over IPv4	155.645.965 (0,68 %)
ICMP over IPv6	46.095.430 (0,2 %)
Other Packets	195.994.737 (0,85 %)
Other over IPv4	195.770.549 (0,85 %)
Other over IPv6	224.188 (0,00 %)
DSCP == '000000' in IPv4	20.455.206.506 (91.41 %)
DSCP != '000000' in IPv4	1.922.347.669 (8.59 %)
DSCP == '000000' in IPv6	660.345.745 (95.61 %)
DSCP != '000000' in IPv6	30.319.018 (4.39 %)
ECN == '00' in IPv4	21.207.872.956 (94.77 %)
ECN != '00' in IPv4	1.169.681.219 (5.23 %)
ECN == '00' in IPv6	685.293.610 (99.22 %)
ECN != '00' in IPv6	5.371.150 (0.78 %)
TOS == '00000000' in IPv4	19.661.731.517 (87.86 %)
TOS != '00000000' in IPv4	2.715.822.658 (12.14 %)
TOS == '00000000' in IPv6	657.351.261 (95.18 %)
TOS != '00000000' in IPv6	33.313.499 (4.82 %)

Custura et. al. performed two recent studies in which they analyzed DSCP modification pathologies in mobile edge networks and the Internet [10] [11]. Their measurements focus on manipulations that happen to DSCP codepoints while traversing the network and which implications such modifications could have for providing QoS. They have developed their own tool to perform active measurements, which is called PathTrace. According to the authors, it was designed to be lightweight and performs post-processing of the measurement data after all probes have been finished. There have been other tools developed by the research community using the same mechanism to detect changes in packets along the way, such as TraceBox [12] and PathSpider [13]. All of the aforementioned tools exploit the fact that RFC 1812 recommends quoting the original message in the reply packet in case the TTL value becomes zero. By provoking such behavior the authors are able to compare the original packet values between two hops and draw conclusions on middlebox interference in between.

III. Data

The data used during this study has been collected and made available by CAIDA [14]. CAIDA maintains several network monitors on high-speed Internet backbone links and provides one hour (1-2 pm UTC) of passive traffic traces for each month. We limit our study to the months March, April, and May in 2018 for computational efficiency. The dataset comprises together almost 1 Terabyte of data. For easy of use, it is split and provided in one minute chunks.

All traces have been anonymized by CAIDA using the CryptoPan prefix-preserving anonymization and only contain header information, stripping out the actual payload that has been transmitted [15]. As our aim is to get clues on the usage of QoS mechanisms in relation to the applications used, these header files are sufficient. We focus on the 8 bit TOS and TC header fields in the IPv4 and IPv6 headers at the network layer and the source and destination ports at the transport layer.

Half of the files were marked as 'DirA', while the other half was marked with 'DirB'. We observed that for all files from the dataset marked with 'DirB', which stands for direction B, certain DSCP values were presumably removed. Such patterns in comparison with traffic from 'DirA' cannot be natural. We assume that a firewall close to the vantage point had a policy set that bleached the TOS field for all IP precedence values (Table I), as we encountered such behavior for the DSCP codepoints starting with '001xxx', '010xxx', '011xxx', '100xxx' and '101xxx'. The behavior was the same for IPv4 and IPv6.

In order to strip out the required information we used Python scripts in combination with the packet crafting library Scapy [1]. Our scripts and measurement results can be found on GitHub [2].

IV. Methodology

During this research our methodology was a sequential action of three steps. Firstly, we analyzed the dataset to find the ports with the largest share of traffic. This was accomplished by counting the occurrences of ports in each packet and calculating the percentages from the overall amount. Secondly, we analyzed the overall distribution of DSCP and ECN values in the dataset. For each DSCP and ECN codepoint we counted the number of packet occurrences. Thirdly, we looked at specific distributions of DSCP and ECN codepoints in relation to the previously determined ports. This was accomplished by only choosing the specific subset of traffic, e.g. traffic on port 25, and then counting all occurrences of DSCP and ECN codepoints within this subset. We then compare the outcome of the overall analysis and the analysis for specific ports with each other. For our calculations we used the amount of packets as a base for determining the distribution. For port specific measurements we chose the source port to be relevant.

[1]https://scapy.net/

[2]https://github.com/nrodday/ISNCC-2019-paper

V. Results

Statistics on the overall dataset are displayed in Table II. The dataset contains on average 97,01 % IPv4 and 2,99 % IPv6 traffic. All percentages are calculated from the total amount of packets contained in the dataset. We included the presumably three most prevalent packet types: TCP (81.67 %), UDP (16.61 %), and ICMP (0.88 %). Packets not matching any of the three protocols have been collected under the Other Packets (0.85 %) counter. Examples are packets of protocols such as IGMP and OSPF.

A. Port Frequencies

The distribution of traffic within our dataset is presented in Table III, which is sorted by port. We counted all instances of packets in the dataset for each port for source and destination. The total is a sum of the two percentages, as we assume that the other end of the connection is using a randomly chosen high-port and we therefore do not count packets twice. This assumption holds true for all listed protocols, except NTP which generally communicates from port 123 to 123. We therefore calculated for this protocol the average from source and destination and listed it as a total. The ports that contribute more than 0.50 % of traffic to the overall amount have been highlighted in Table III. We are going to focus in the upcoming analysis of DSCP and ECN values for specific ports on this subset of traffic. It consists of the five protocols DNS, HTTP, NTP, HTTPS, and SMB. It is worth mentioning that the amount of HTTPS traffic compared to unencrypted HTTP is twice as high. Together, web traffic amounts to about 64 % in the dataset. The share of DNS traffic is 2.11 %, while the shares of SMB and NTP traffic amount to 0.59 % and 0.52 %, respectively.

TABLE III
Most utilized well-known ports

Port	Service	Total %
22	SSH	0.22
23	TelNet	0.36
25	SMTP	0.20
53	DNS	2.11
80	HTTP	18.63
81	Alternate HTTP	0.11
110	POP3	0.08
111	RPC	0.07
123	NTP	0.53
161	SNMP	0.02
389	LDAP	0.08
443	HTTPS	45.00
445	SMB	0.60
465	SMTP over SSL	0.04
514	Syslog	0.06
587	SMTP	0.07

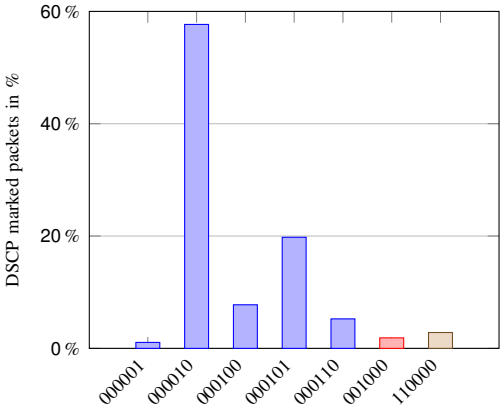


Fig. 2. Share of DSCP codepoints in IPv4 (≥1 %)

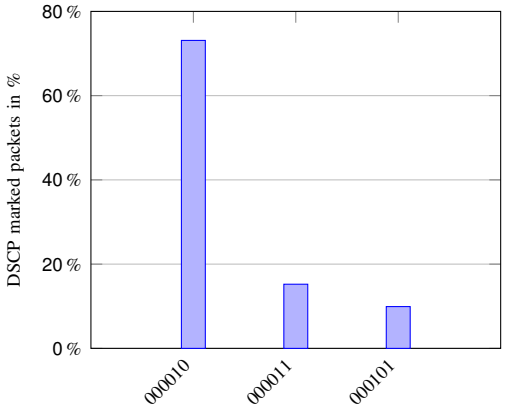


Fig. 3. Share of DSCP codepoints in IPv6 (≥1 %)

Interestingly, a subset of 102.648 packets in the sample (out of 23.068.218.935 packets) is using port 0 either as source or destination. Port 0 is a wildcard port used by applications to request a dynamic port from the OS, it should not be used for TCP/IP traffic in the Internet. We assume that either the traffic was generated by faulty applications or has to be attributed to malicious actors as part of their fingerprinting activities.

TABLE IV
SHARE OF DSCP ENABLED TRAFFIC PER PORT IN IPV4

Port	Protocol	DSCP disabled	DSCP enabled
53	DNS	96.55 %	3.45 %
80	HTTP	87.49 %	12.51 %
123	NTP	93.33 %	6.67 %
443	HTTPS	88.99 %	11.01 %
445	SMB	98.09 %	1.91 %

B. DSCP Analysis

In IPv4 8.59 % of traffic is using DSCP values, leaving the DSCP bits in 91.41 % of traffic unmarked. The subset of marked traffic was used as a baseline in Figure 2, which shows the distribution of the most commonly used DSCP values in IPv4. The DSCP codepoints ’000010’, ’000101’, ’000100’, ’000110’, ’000001’ have a share of 57.68 %, 19.78 %, 7.76 %, 5.25 %, and 1.06 %, respectively, and specify ”Routine” traffic with no specific Per-Hop-Behavior (PHB). Together, CS0 traffic constitutes 91.53 % of DSCP enabled traffic. CS0 traffic has been colored blue in the figure. It basically tells the router that QoS is enabled, but only Best-Effort services are needed for these packets. However, the different codepoints request different priorities within CS0. Codepoint ’110000’ has the fifth largest share with 2.82 % and is a member of the CS6 class, which requests very high priority. It has been colored red. The sixth largest share is codepoint ’001000’ with 1.87 %, which relates to the CS5 class. It has been colored grey. The figure shows a total of 96,22 % of DSCP enabled traffic. The remaining 3,78 % is distributed over the other 57 DSCP codepoints and has been left out for readability.

For the ports we identified in Table III as most used ports, we determined the overall distribution in the dataset of DSCP enabled traffic in IPv4, which can be found in Table IV. We observe that HTTP and HTTPS traffic have quite a large amount of DSCP enabled traffic, while the other three protocols fall behind. For our subsequent analysis, we will only focus on the share of DSCP enabled traffic. For better readability, the values for the CS0 class are presented in Table V while all other DSCP classes are displayed in Figure 4. For each of the five ports one color highlights the distribution. Firstly, we observe in Table V that the range of CS0 traffic reaches from 81.71 - 96.16 % in IPv4. NTP is rarely using DSCP codepoints different from ’000xxx’, while SMB traffic has a share of 18.29 %. Figure 4 is presenting the distribution of the codepoint classes CS1 - CS7 in more detail. CS1 is being used by all applications, except NTP, whereby the codepoints ’001000’ and ’001010’ make up almost all traffic for all applications. CS2 is almost only used by SMB traffic, with the codepoint ’010010’. CS3 is mostly used by SMB traffic, only a small portion of DNS traffic is also using it. The codepoints in CS3 that contribute most are ’011010’ and ’011100’. In CS4 SMB traffic is again the only consumer with codepoint ’100100’. CS5 is again used by multiple protocols. HTTP and HTTPS are mostly using codepoint ’101000’, while SMB traffic is solely using codepoint ’101100’. CS6 is dominated by DNS and NTP traffic, mostly using codepoint ’110000’, while the last class CS7 is very rarely used.

In IPv6 only 4.39 % of traffic is using DSCP values, while 95.61 % is unmarked. The adoption of DSCP within IPv6 is therefore lower compared to IPv4. Again, only focusing on the DSCP enabled traffic, in IPv6 even fewer DSCP codepoints are used frequently, compared to IPv4. Figure 3 displays these values. All codepoints are members of the CS0 class and request only Best-Effort services. Codepoint ’000010’ has a share of 73.11 %, while the codepoints ’000011’ and ’000101’ have a share of 15.23 % and 9.92 %,

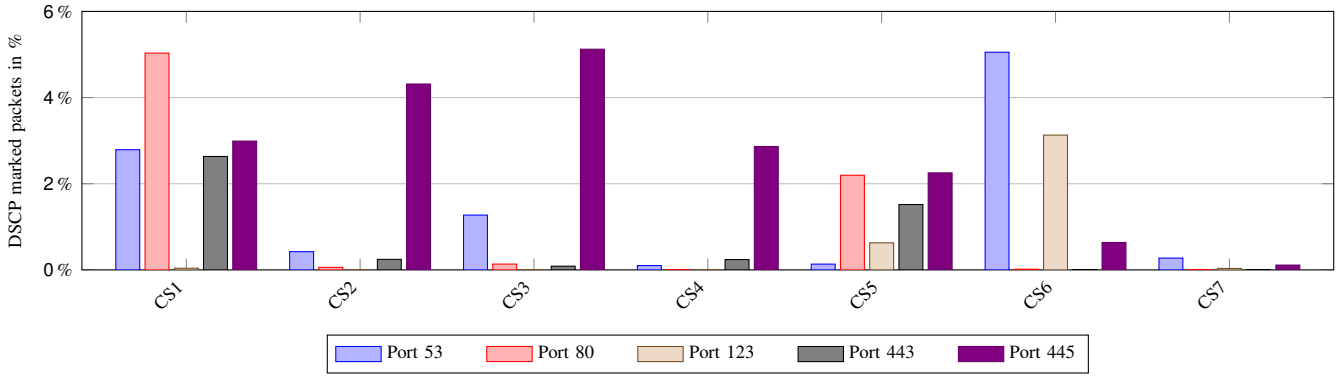


Fig. 4. Share of DSCP codepoints classes in IPv4 per port

TABLE V
CS0 PER PORT IN IPV4

Port	Protocol	Share of CS0
53	DNS	89.95 %
80	HTTP	92.56 %
123	NTP	96.16 %
443	HTTPS	94.53 %
445	SMB	81.71 %

respectively. Together, CS0 traffic constitutes 98.26 % of DSCP marked traffic.

By determining the DSCP distributions per port in IPv6 we observed that 96.28 % of DNS traffic is unmarked. The codepoint '000010' is used in 3.60 % of the cases. HTTP traffic is only using the codepoints '000010' and '000011' with shares of 58.32 % and 0.64 %, respectively, leaving 41.03 % unmarked. Therefore, only the CS0 class is used. With only 18.146 packets for port 123 (NTP), we cannot comment on the distribution as the amount of data is too small. HTTPS traffic is leaving 47.94 % unmarked. Then again only using CS0 with 27.83 % and 23.99 % for codepoints '000010' and '000011', respectively. There appears to be no traffic on port 445 using IPv6 in our dataset. Interestingly, all ports that have been identified in Table III as the ports carrying most traffic in our dataset turned out to make quite frequent use of DSCP CS0 codepoints in IPv6. However, we think that this specific subset of results might be biased as the amount of IPv6 traffic on those port is quite low, allowing single connections to have great impact on our measurement results.

C. ECN Analysis

In IPv4 5.23 % of packets set the ECN field to the codepoints '01', '10' or '11', while the codepoint '00' is used in 94.77 %. Figure 5(a) shows the share of ECN codepoints over the former subset of traffic. In this subset 94.46 % of traffic is marked with the codepoint '11'. Traffic with the ECT-enabled codepoints '01' (0.91 %) and '10' (4.63 %) is very rare.

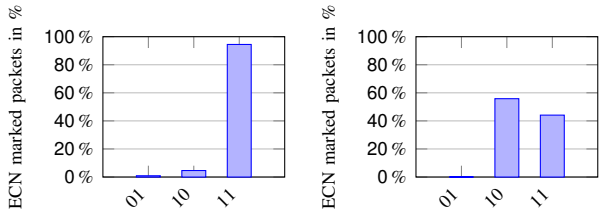
As we can see in Table VI the overall measurements for ECN in IPv4 traffic deviate from the more specific measurements we conducted for the selection of ports in Table III. The rate of packets that do not carry ECN codepoints is constantly above 99 %. We calculated the inverse (sum of all other codepoints) and used it as a baseline for the percentage values in the following lines in order to demonstrate the share of other ECN codepoints in ECN enabled traffic. We observed that for port 53 almost all ECN enabled traffic was carrying codepoint '11', which stands for "Congestion Experienced". For port 80 this share is with 11.55 % significantly lower, while 88.22 % can be attributed to codepoint '10'. For port 123 all analyzed ECN enabled traffic is marked with '11', while for port 443 it is 98.85 % for codepoint '10'. SMB traffic on port 445 is mostly distributed between codepoints '10' and '11'. It is worth pointing out that HTTP and HTTPS traffic seems to have way more ECN enabled traffic carrying codepoint '10' than traffic on other ports.

In IPv6 only 0.78 % of packets set the ECN field to the codepoints '01', '10' or '11', while in 99.22 % of traffic the codepoint '00' is used. Therefore, the share of ECT in IPv6 traffic is neglectable. Figure 5(b) shows the share of ECN codepoints over the former subset of traffic. We observe, that in 55.82 % codepoint '10' and in 44.11 % codepoint '11' is used. The remaining 0.07 % can be attributed to codepoint '01'.

Considering the ports from Table III we observed that on ports 53, 123 and 445 all traffic is without ECN markings. For port 80 we found that 11.69 % of traffic carried the codepoint '10', the remaining 88.31 % carried '00'. For port 443 only 0.1 % was marked as '10', the remaining 99.9 % of traffic could be attributed to codepoint '00'. Therefore we conclude that ECN in IPv6 is almost not used on the ports 53, 123, 443 and 445. Only port 80 is carrying ECN enabled traffic in IPv6.

TABLE VI
SHARE OF ECN CODEPOINTS IN IPV4 PER PORT

ECN	Port 53	Port 80	Port 123	Port 443	Port 445
00	99.28 %	99.74 %	99.75 %	99.70 %	99.97 %
Invert to 00	0.72 %	0.26 %	0.25 %	0.30 %	0.03 %
01	0.00 %	0.22 %	0.00 %	0.04 %	1.05 %
10	1.24 %	88.22 %	0.00 %	98.85 %	58.53 %
11	98.76 %	11.55 %	100 %	1.15 %	40.42 %



(a) IPv4 Traffic (b) IPv6 Traffic

Fig. 5. Share of ECN codepoints

VI. CONCLUSION AND FUTURE WORK

This work provided new insights into DSCP and ECN usage of backbone Internet traffic. We analyzed which ports have most share of traffic and performed an analysis of DSCP and ECN codepoints for the whole dataset as well as for the subset of previously defined ports. The results we got for DSCP codepoints can be summarized as follows:

- The use of DSCP codepoints is at 8.59 % for IPv4 and at 4.39 % for IPv6.
- CS0 traffic constitutes 91.53 % for IPv4 and 98.26 % for IPv6. Other classes are rarely used.
- HTTP traffic (12.51 %) and HTTPS traffic (11.01 %) in IPv4 have the largest share of DSCP enabled traffic among the investigated protocols and therefore the highest adoption.
- HTTP traffic (58.32 %) and HTTPS traffic (52.06 %) in IPv6 have a very high adoption rate but their share in overall traffic is quite low.

The results we got for ECN codepoints can be summarized as follows:

- Only 5.23 % of traffic is using ECN codepoints in IPv4 while in IPv6 the share is with 0.78 % neglectable.
- For the ports 53, 80, 123, 443, and 445 an adoption rate of less than 1 % in IPv4 was determined, meaning that traffic on these ports is almost never carrying ECN enabled packets.
- Only port 80 in IPv6 is carrying ECN enabled traffic (11.69 %). The other ports 53, 123, 443, and 445 do not.

For future research we would like to extend our current approach for other protocols running on top of the network layer, such as IGMP and OSPF. Also, our current analysis relies only on data from 2018. We would like to include more datasets from previous years to draw conclusions on how the adoption has changed over time. Moreover, we need to add more data to reduce the likelihood of measurement errors, especially in IPv6 traffic.

ACKNOWLEDGMENT

The authors would like to thank CAIDA for providing the traffic traces used in this study. Also, we would like to thank the Chair for Communication Systems and Network Security, headed by Prof. Gabi Dreo Rodosek, and the Research Institute CODE as well as Dr. Jair Santanna from the University of Twente for their comments and improvements.

REFERENCES

[1] J. Postel, "Internet Protocol," RFC 791, Sep. 1981. [Online]. Available: https://rfc-editor.org/rfc/rfc791.txt
[2] R. T. Braden, "Requirements for Internet Hosts - Communication Layers," RFC 1122, Oct. 1989. [Online]. Available: https://rfc-editor.org/rfc/rfc1122.txt
[3] P. Almquist, "Type of Service in the Internet Protocol Suite," RFC 1349, Jul. 1992. [Online]. Available: https://rfc-editor.org/rfc/rfc1349.txt
[4] D. B. Grossman, "New Terminology and Clarifications for Diffserv," RFC 3260, Apr. 2002. [Online]. Available: https://rfc-editor.org/rfc/rfc3260.txt
[5] S. Floyd, D. K. K. Ramakrishnan, and D. L. Black, "The Addition of Explicit Congestion Notification (ECN) to IP," RFC 3168, Sep. 2001. [Online]. Available: https://rfc-editor.org/rfc/rfc3168.txt
[6] F. Li, N. Seddigh, B. Nandy, and D. Matute, "An empirical study of today's internet traffic for differentiated services IP QoS," in *Proceedings ISCC 2000. Fifth IEEE Symposium on Computers and Communications*, July 2000, pp. 207–213.
[7] E. . Fgee, J. D. Kenney, W. J. Phillips, W. Robertson, and S. Sivakumar, "Comparison of QoS performance between IPv6 QoS management model and IntServ and DiffServ QoS models," in *3rd Annual Communication Networks and Services Research Conference (CNSR'05)*, May 2005, pp. 287–292.
[8] J. Harju and P. Kivimaki, "Co-operation and comparison of DiffServ and IntServ: performance measurements," in *Proceedings 25th Annual IEEE Conference on Local Computer Networks. LCN 2000*, Nov 2000, pp. 177–186.
[9] W. John and S. Tafvelin, "Analysis of Internet Backbone Traffic and Header Anomalies Observed," in *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement*, ser. IMC '07. New York, NY, USA: ACM, 2007, pp. 111–116. [Online]. Available: http://doi.acm.org/10.1145/1298306.1298321
[10] A. Custura, A. Venne, and G. Fairhurst, "Exploring DSCP modification pathologies in mobile edge networks," in *2017 Network Traffic Measurement and Analysis Conference (TMA)*, June 2017, pp. 1–6.
[11] A. Custura, R. Secchi, and G. Fairhurst, "Exploring DSCP modification pathologies in the internet," *Computer Communications*, vol. 127, pp. 86–94, 2018.
[12] G. Detal, B. Hesmans, O. Bonaventure, Y. Vanaubel, and B. Donnet, "Revealing middlebox interference with tracebox," in *Proceedings of the 2013 conference on Internet measurement conference*. ACM, 2013, pp. 1–8.
[13] I. R. Learmonth, B. Trammell, M. Kuhlewind, and G. Fairhurst, "PATHspider: A tool for active measurement of path transparency," in *Proceedings of the 2016 Applied Networking Research Workshop*. ACM, 2016, pp. 62–64.
[14] The CAIDA UCSD Anonymized Internet Traces. (2018). [Online]. Available: http://www.caida.org/data/passive/passive_dataset.xml
[15] J. Fan, J. Xu, M. H. Ammar, and S. B. Moon, "Prefix-preserving IP Address Anonymization: Measurement-based Security Evaluation and a New Cryptography-based Scheme," *Comput. Netw.*, vol. 46, no. 2, pp. 253–272, Oct. 2004. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2004.03.033