DSCP and the Evil Bit

Runa Barik (UiO), Michael Welzl (UiO), Ahmed Elmokashfi (SRL)

maprg @96th IETF Meeting
Berlin, Germany
18th July 2015
The Internet could ideally use the IP header for special treatment to the packet; but, which bits in the header can be used?

Middleboxes in private networks also modify/drop the packets limiting the protocol innovations.

This work complements to our paper in ANRW’16 ¹.

In this context, we focus on:

- How middleboxes react to packets with different DSCP values, and Evil bit.

¹Runa Barik, Michael Welzl, Ahmed Elmokashfi, “How to say that you’re special: Can we use bits in the IPv4 header?”, in ANRW’16
Test methodology

ICMP packet (Echo Request), id=id1

TCP SYN, id=id1

ICMP packet (Echo Reply), id=id2

TCP SYN/ACK, id=id2

Extreme
Location of Drop

ICMP packet (Echo Request)

ICMP packet (Echo Reply)

TCP SYN, id=id1

Server

Router

Middlebox

Router

Client

Traceroute

id=id1

Timeout

5

Extreme

traceroute or tracebox like testing
Test Locations

(a) Travel to India
(b) Malaysia
Change of DSCP values

x-axis: the lower (larger) number is the original DSCP value, the upper (smaller) number is the changed value. The brackets on the top show the absolute number of paths (IP address pairs).

x-axis: the lower (larger) number is the original DSCP value, the upper (smaller) number is the changed value. The brackets on the top show the absolute number of paths (IP address pairs).
Change of DSCP values

Fraction of distinct paths

DSCP values

-(0: 128), (2: 2), (4: 20), (6: 1)
-(10: 1), (12: 2), (36: 11), (62: 1)
-(14: 2), (46: 11), (62: 1)
### Table: DSCP packet-drop noticed in Countries

<table>
<thead>
<tr>
<th>Src. Countries</th>
<th>Dst. Countries</th>
<th>DSCP initial</th>
<th>Change Location</th>
<th>Drop Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oregon</td>
<td>Kuala Lumpur, Malaysia</td>
<td>CS1</td>
<td></td>
<td>Amazon Tech. Inc.</td>
</tr>
<tr>
<td>Norway (ISP2)</td>
<td>Kuala Lumpur, Malaysia</td>
<td>AF42</td>
<td>TELIANET (4)</td>
<td>TMNet Telekom Malaysia</td>
</tr>
<tr>
<td></td>
<td>TELIANET (6)</td>
<td>EF</td>
<td>TELIANET (6)</td>
<td>TMNet Telekom Malaysia</td>
</tr>
</tbody>
</table>

### Graph: TTL (DSCP change) vs DSCP (original)

- **Client-side**
- **Server-side**
The brackets on the top show (DSCP value in ICMP: number of packets)
DSCP/TOS values in IPv4 header and payload of ICMP time-exceeded message

Y-axis: Fraction of different DSCP values in IP header of ICMP messages, while the payload IP header contains DSCP values of 0, 2, 4, or 6
Y-axis: Fraction of different DSCP values in IP header of ICMP messages, while the payload IP header contains DSCP values of 8, 10, 18, or 36
Y-axis: Fraction of different DSCP/TOS values in IP header of ICMP messages, while the payload IP header contains DSCP/TOS values of 32, 40, 46, or 3 (CE)
In 169 out of 205 paths, packets with Evil bit set passed successfully.

However, DSCP values are stripped or remain unchanged in around 165 paths.

No modification to Evil bit on successful paths.
Thank you!