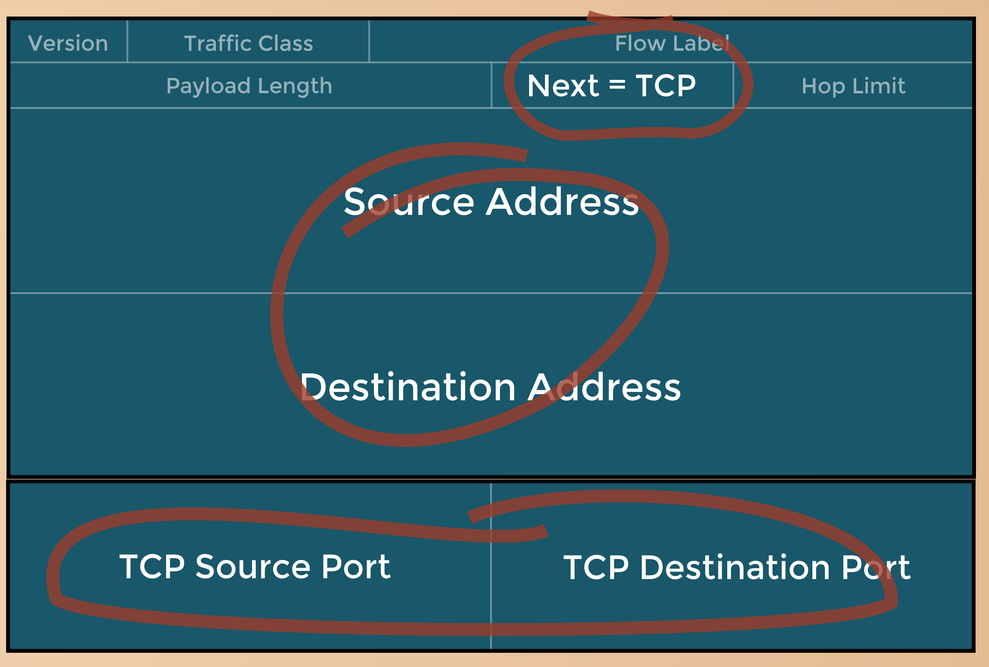
what you see != what you get

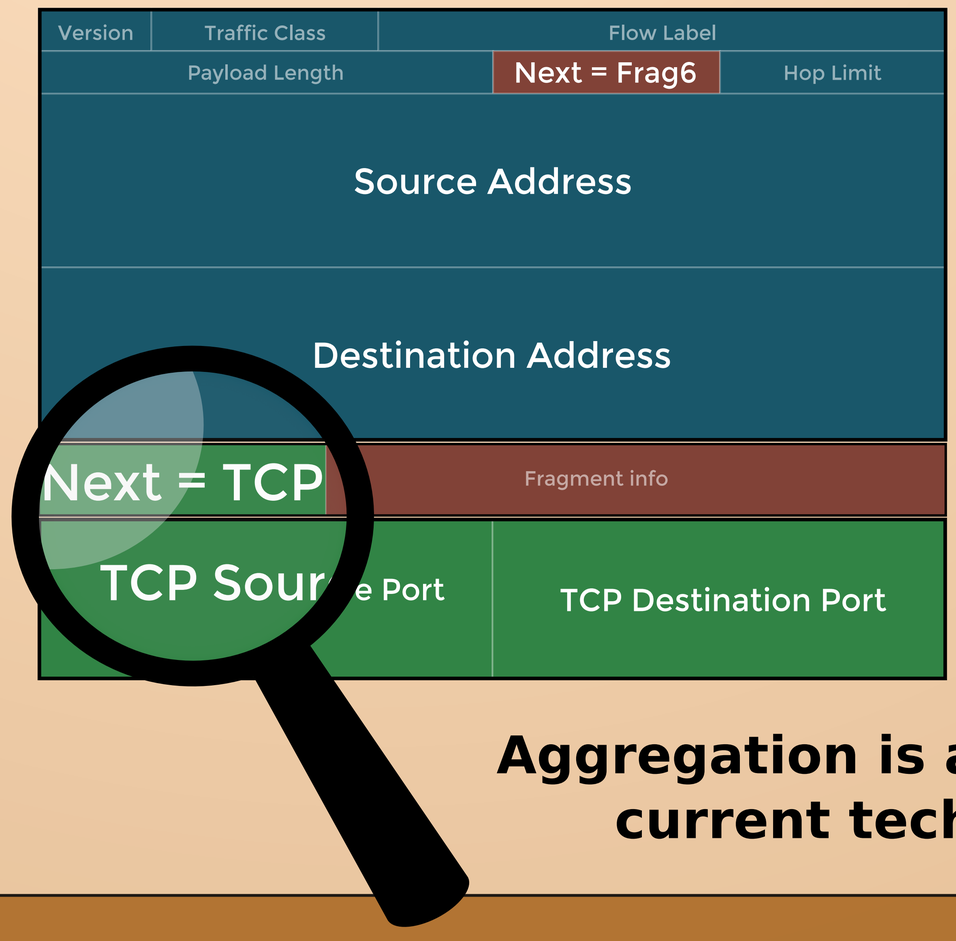
Measurements on IPv6

Luuk Hendriks,
Ricardo de O. Schmidt,
Aiko Pras
Design and Analysis of Communication Systems
University of Twente, the Netherlands
luuk.hendriks@utwente.nl

Measurement tools are not ready for IPv6.
Many IPv6 threats have been described in the literature, but are they actually occurring in the Internet? Operators anxiously drop traffic that is considered dangerous, like fragmented IPv6, but do they know what is actually in there? Time for measurements! But do our tools give us the full picture?



Flow-based solutions provide an overview based on the classic 5-tuple



IPv6 headers vastly differ from IPv4: measurement technologies should too.
With the dynamic nature of Extension Headers in IPv6, measurement tools need to look further into a packet to get the actual higher layer information. This requires more extensive parsing, and more intelligent aggregation. Without these efforts, the actual 5-tuple is hidden, resulting in a skewed view on network traffic.

Aggregation is as powerful as it is dangerous: current technologies hide information

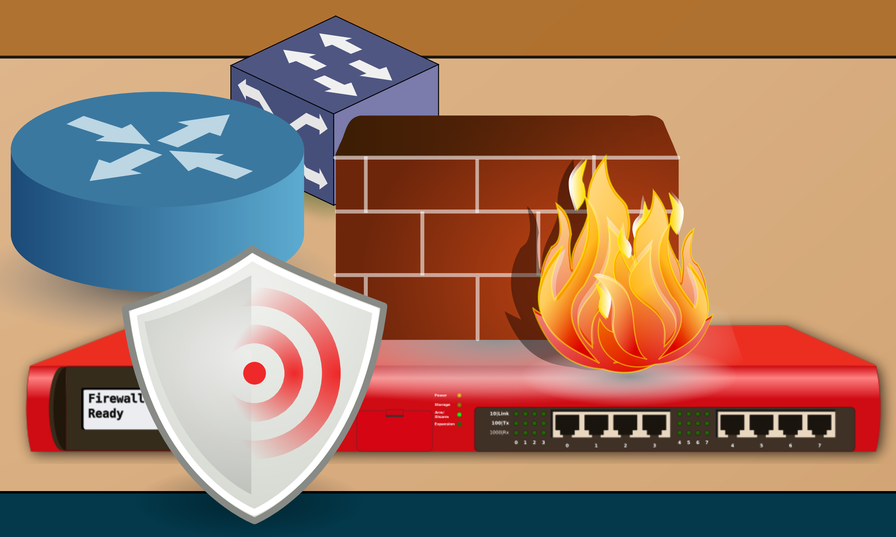
***What new information on traffic** provides insights for operators, vendors, and security researchers?*

***How should measurement technologies be adapted** to give a complete and realistic view?*

***How are currently deployed security solutions affected** and how can we identify misuse?*

How can measurement technologies be assessed** on their completeness and accuracy, and **what role do standardisation bodies have in this process?

Sounds familiar?
Forwarding devices have troubles processing Extension Headers, and middleboxes are evaded by them. Both get much attention. Our measurements need that attention too.



DACS
Design and Analysis of Communication Systems

UNIVERSITY OF TWENTE.

SURF NET