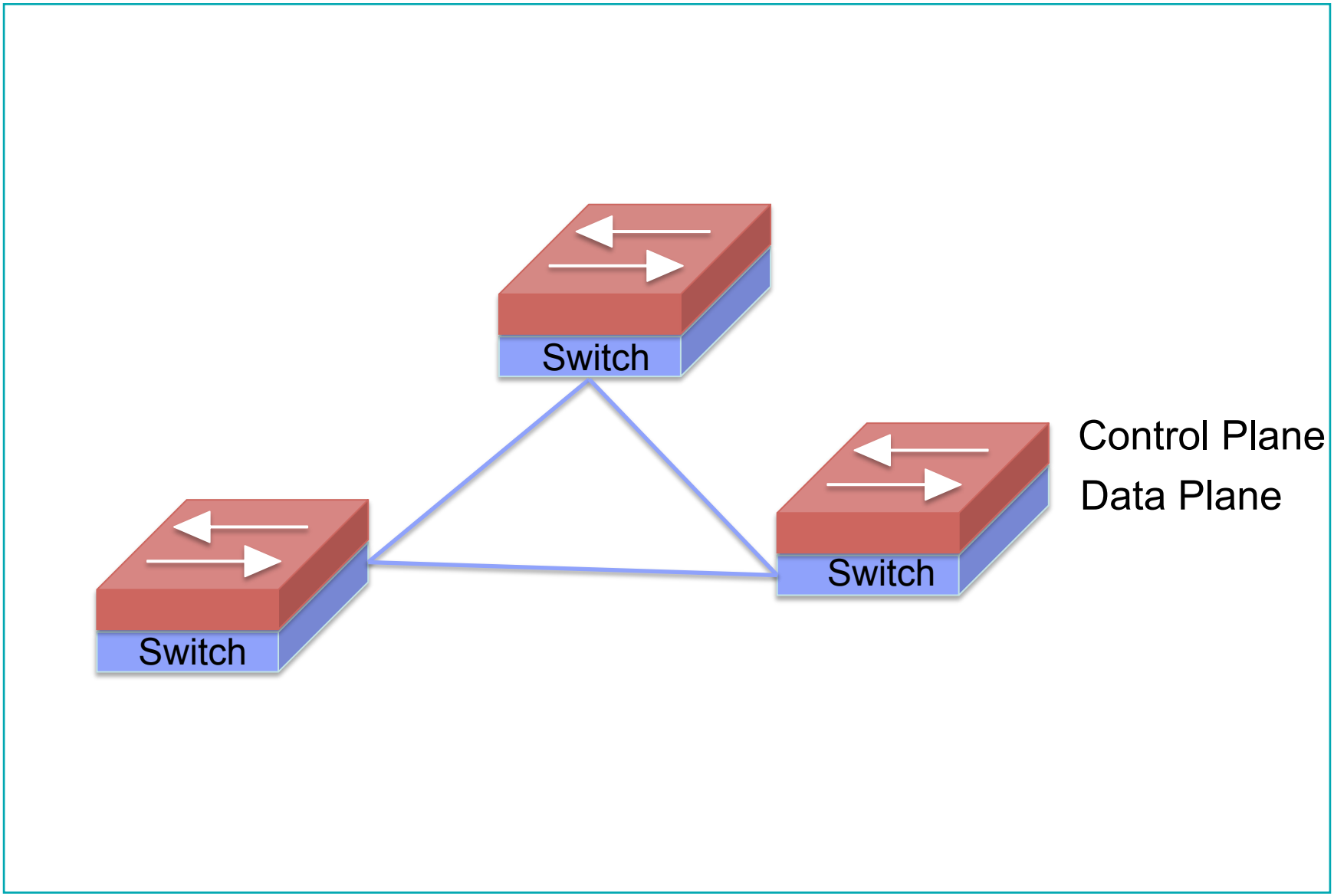
BEUTH HOCHSCHULE FÜR TECHNIK BERLIN
University of Applied Sciences

SDN Security: Lösung oder Problem

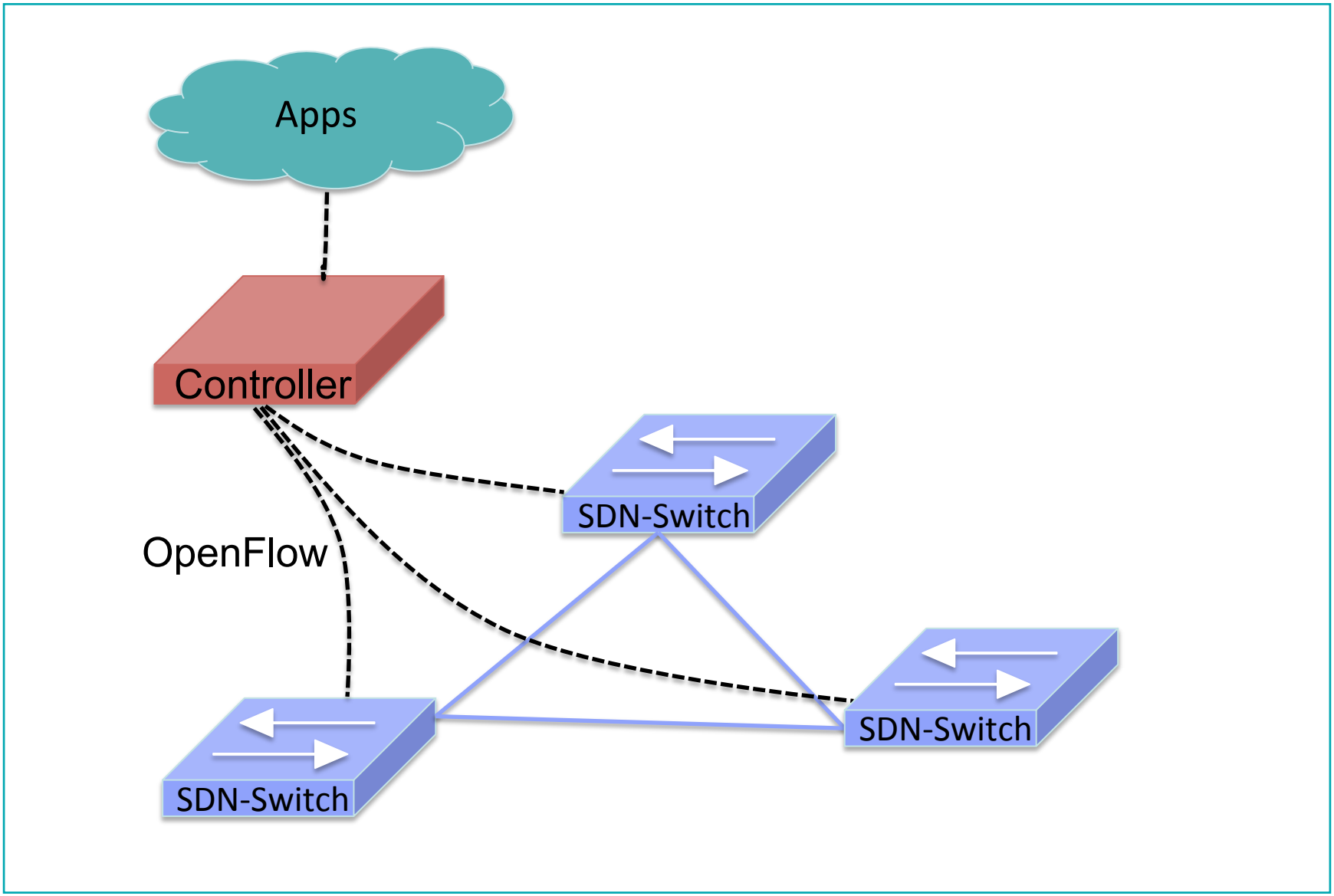
Thomas Scheffler

Hamburg, Februar 2017

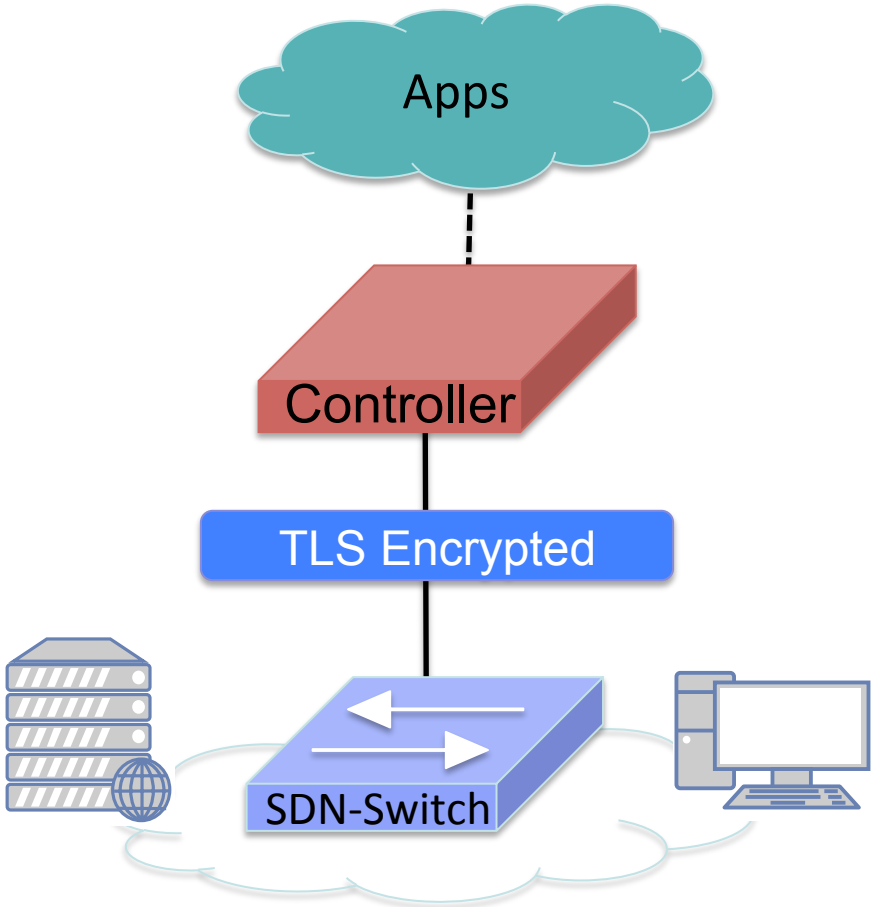
A traditional network architecture



An SDN network architecture



Is it secure?



“If you think cryptography is the solution to your problem, you don’t know what your problem is.”

Roger Needham

Isssues with SDN security

Dagstuhl Seminar 16361 (September 2016)

Network Attack Detection and Defense – Security Challenges and Opportunities of Software-Defined Networking

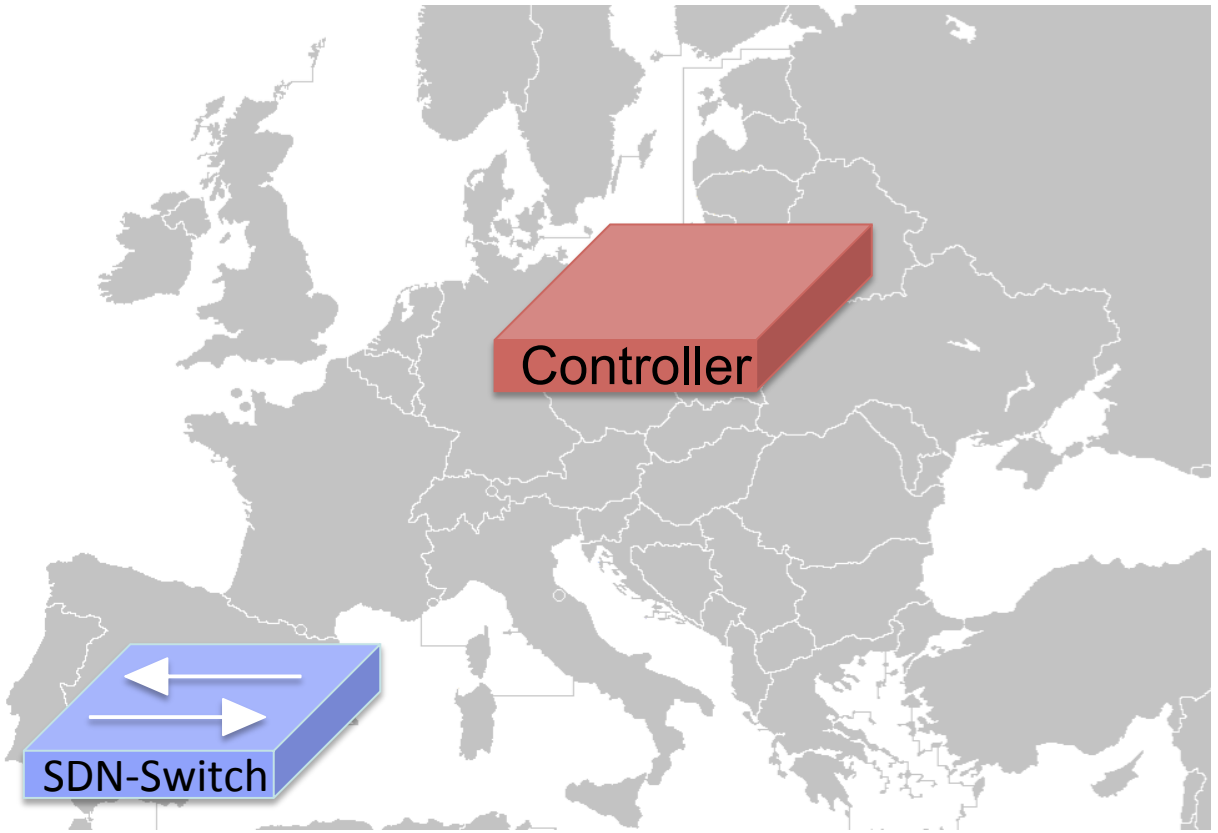
Isssues with SDN security

Dagstuhl Seminar 16361

- How to securely implement and deploy “network apps”? How to design the northbound interface so it is secure and expressive?
- How to implement access control and authorization in SDN networks?
- How can we protect the controller itself?
- How can we perform intrusion detection and anomaly detection in SDNs?
- How can we deal with misbehaving/rogue applications?
- How to mitigate attacks?
- How can you operate SDN in presence of untrusted HW components?
- How do we ensure the software quality of the SDN infrastructure (controller, HW, . . .)?
- ...

Controller Placement in SDN-WANs

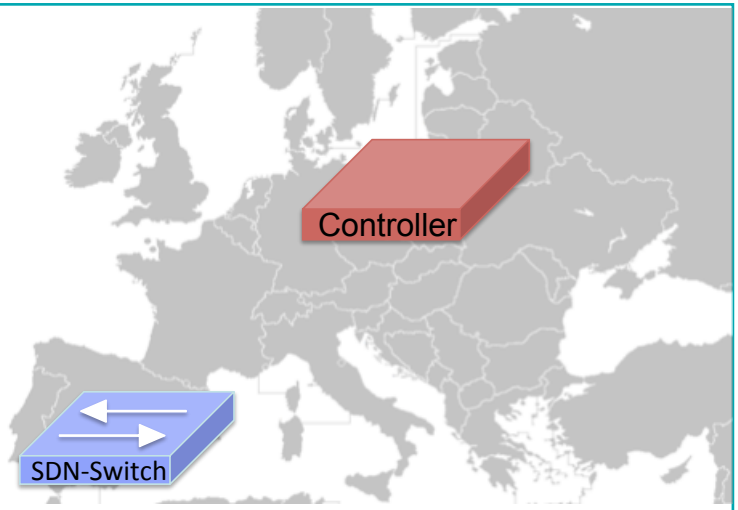
- Depending on (architecture, circumstances, bad-luck) your SDN-WAN could end up looking like this:



Controller Placement in SDN-WANs

Implications:

High Propagation delay
between Controller and Switch



Example:

Barcelona – Frankfurt

1000km (line of sight), ~1500km (fibre run)

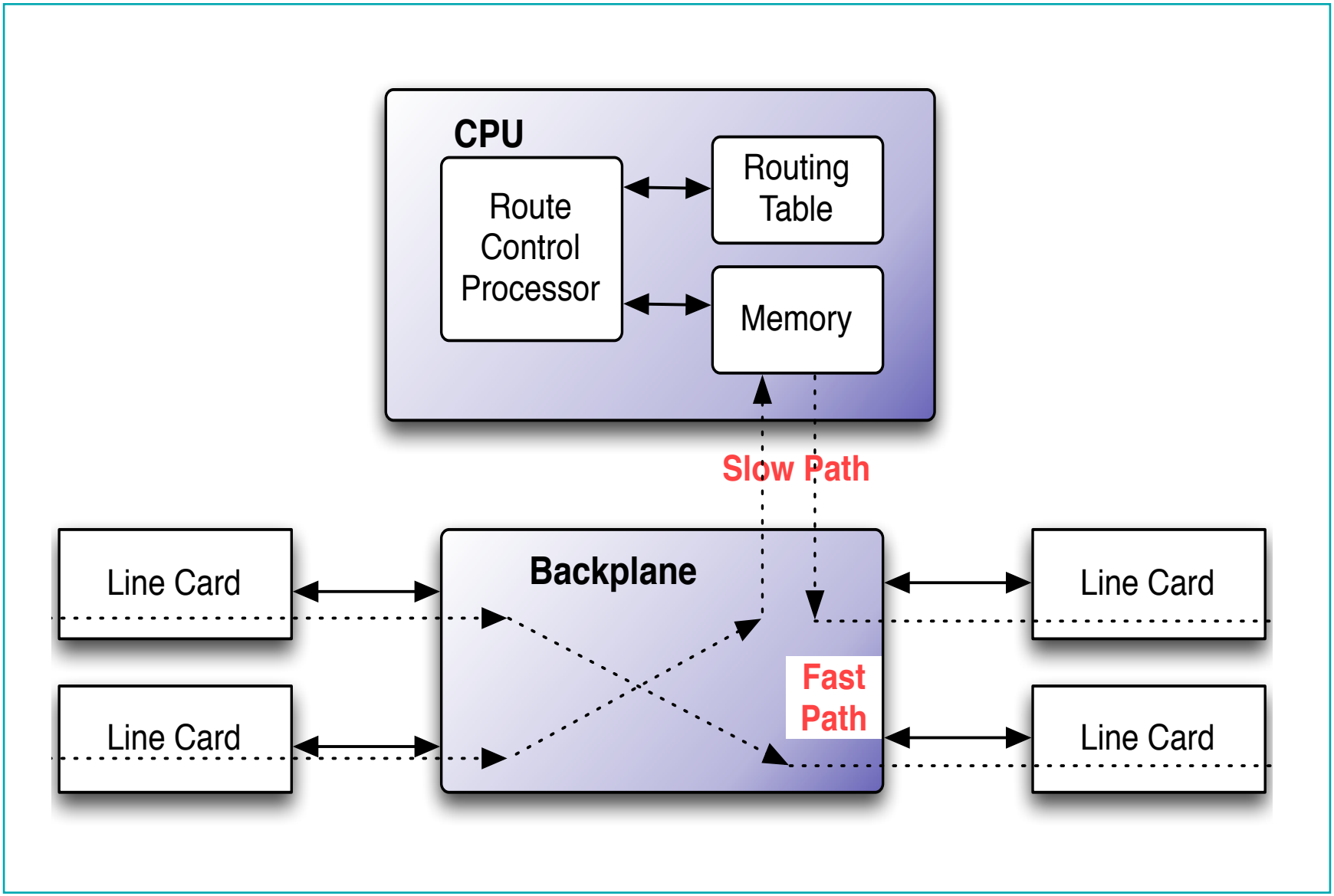
- 10-15ms added propagation delay

Boston – San Francisco

4333km (line of sight), ~5000km (fibre run)

- 40-50ms added propagation delay

Delay Paths in Device Architectures



Emulating various Delay-Paths for SDN Controllers

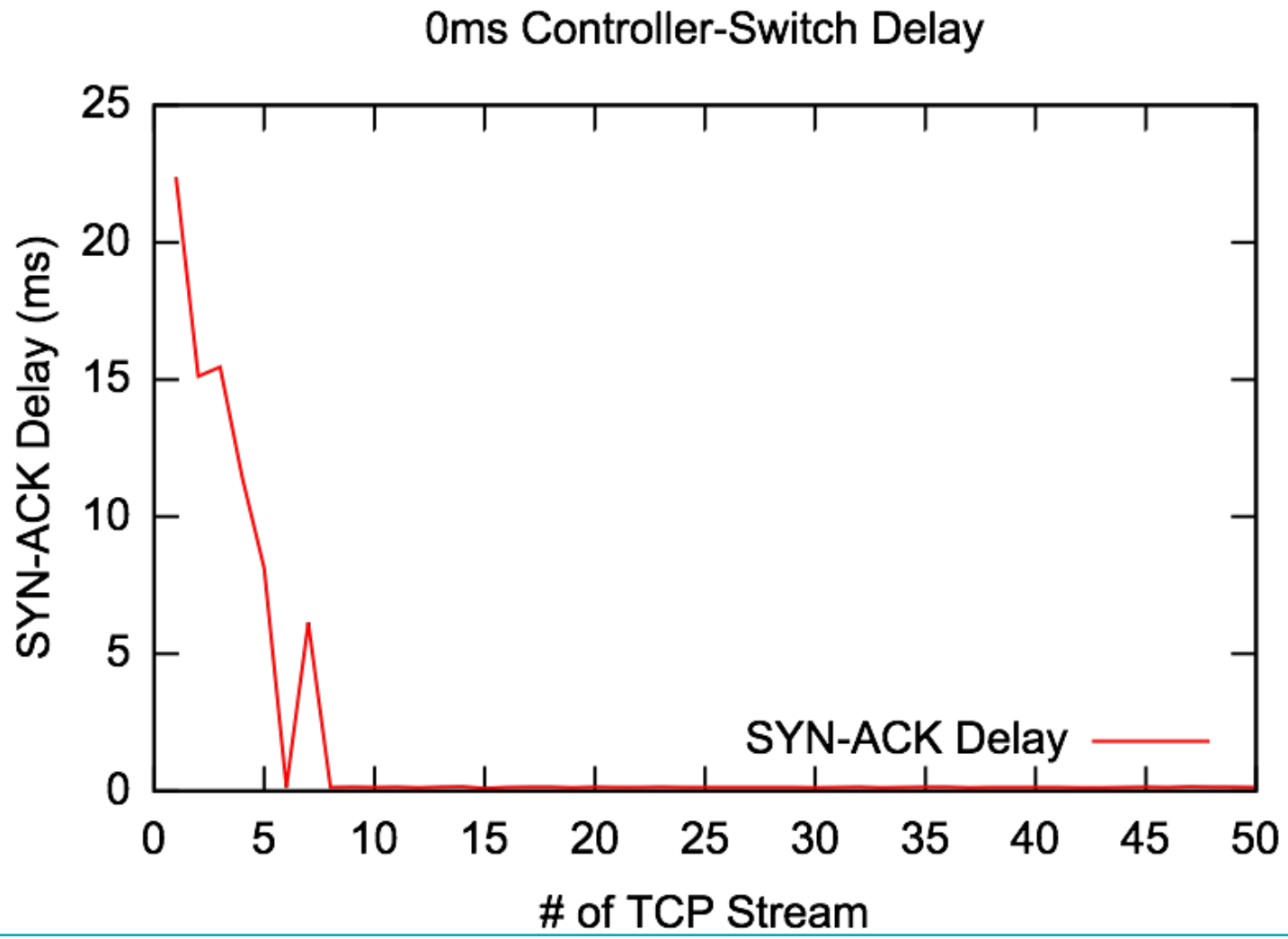
Load

- Simulating ‚simultaneous' TCP connections
  (1 new connection every 4 ms)
- First connection triggers a new flow-event in the switch)
- No ARP (entries were hard coded)

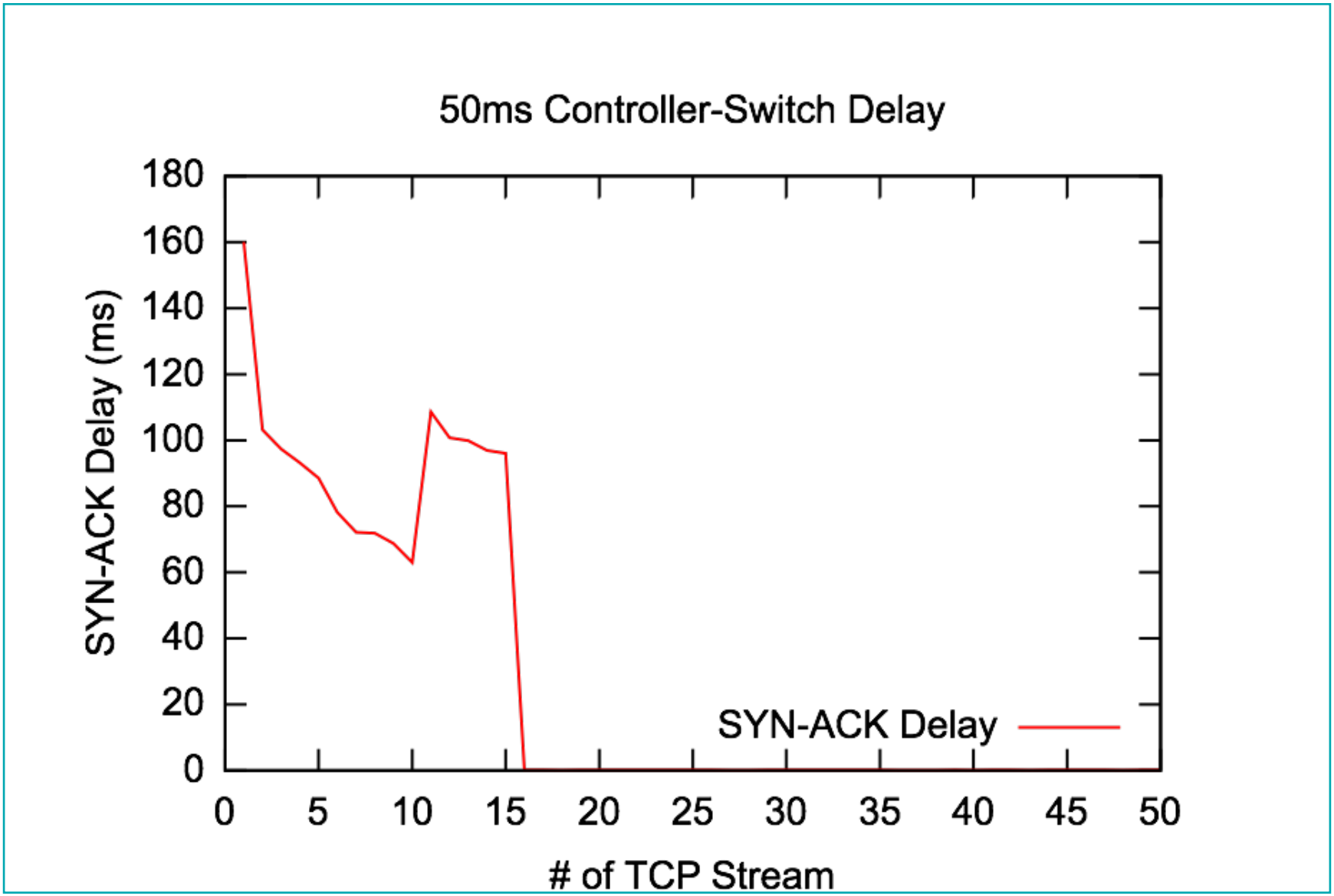
Very simple application

- First ‚packet-in' triggers installation of 2 flows (in/out)
- Forwarding based on hard-coded MAC-addresses
- No fancy processing

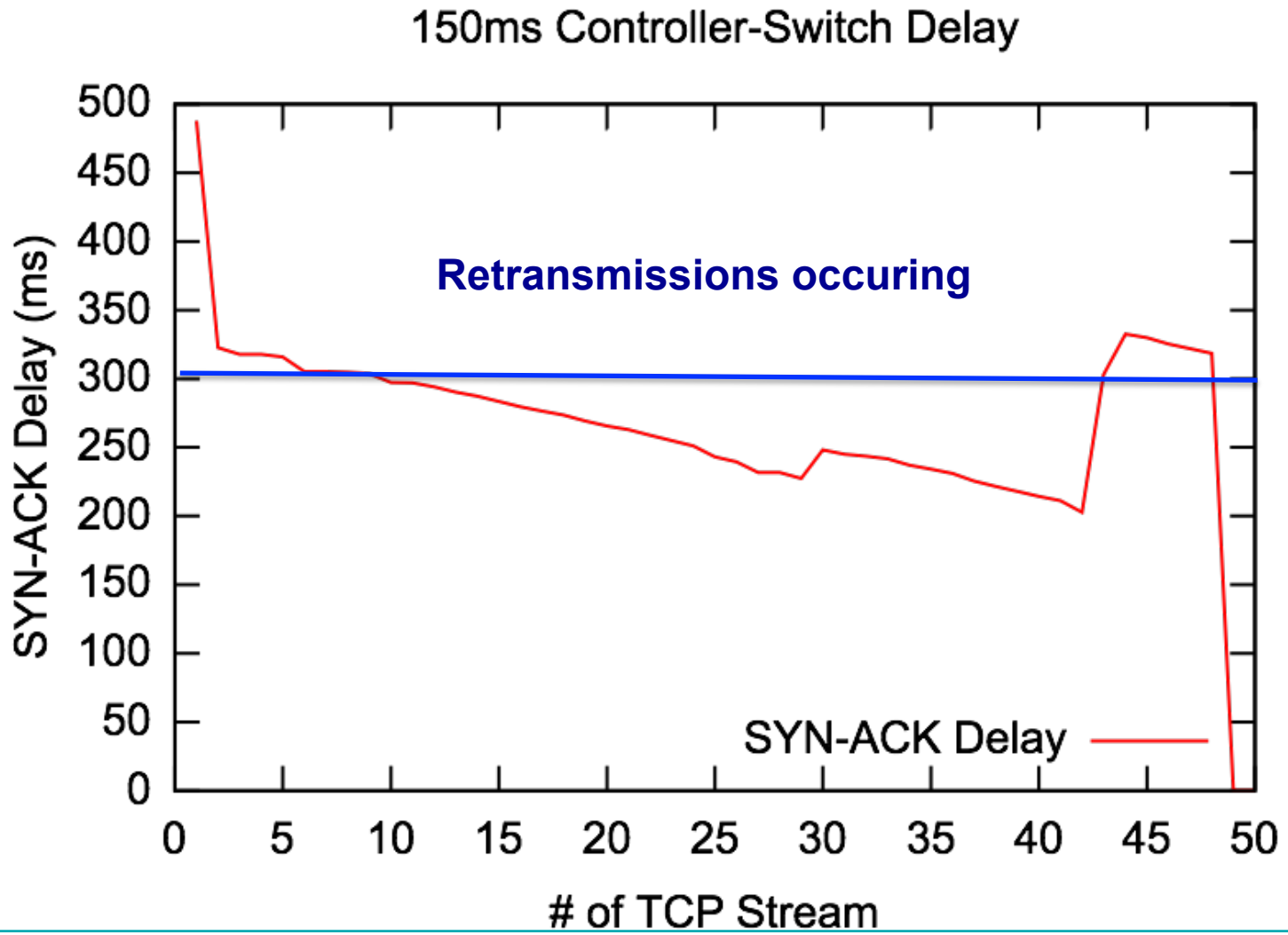
Measurements



Measurements



Measurements



Discussion

Issues with high Controller switch delay:

- Overload Controller processing and or Switch/Controller link (with possibility of DoS)
- Impacts end-point communication
- Delay could also stem from other sources such as sync-/ processing delay of apps

Questions

Thomas Scheffler

Email: scheffler@beuth-hochschule.de
WWW: prof.beuth-hochschule.de/scheffler

Testbed

Controller

- RYU (Core i5-2400)

Webserver

- Apache webserver
- Single HTML page (<10kbyte)

Load generation

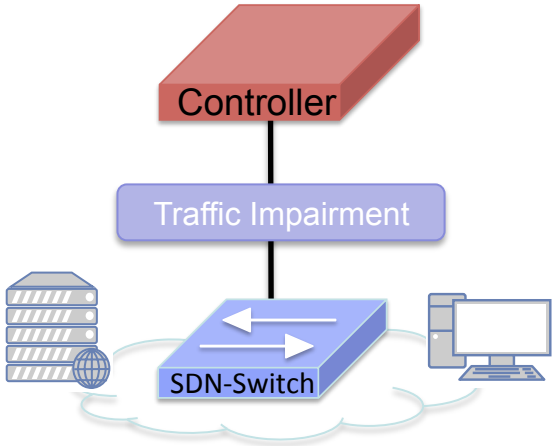
- Apache JMeter

Impairment

- Linux `netem` directly on the Controller

Switch

- Brocade VDX 6740T
  - 48 port 1/10GbE
  - Four 40 GbE QSFP+



Observations

- **Number of users did not really matter**, because only one source for load generation (1000 users only take longer to run...).
- **JMeter not ideal load testing tool for switches**, better Tcpreplay, dedicated appliance, etc.
  - One new connection request every 4ms on our (old, old) hardware.
- **Ryu is slow** (at least on our machine)
  - >20ms for packet_in, 2 flow updates, packet_out
- Beginning with the 150ms delay settings, we see that **TCP-retransmissions** occur, adding to the traffic.