

# Packet Capture in 10-GigE Environments using Contemporary Commodity Hardware

Fabian Schneider · Jörg Wallerich · Anja Feldmann

## CHALLENGE

- Capturing packets in high speed networks with commodity hardware in high-speed environments

## APPROACH

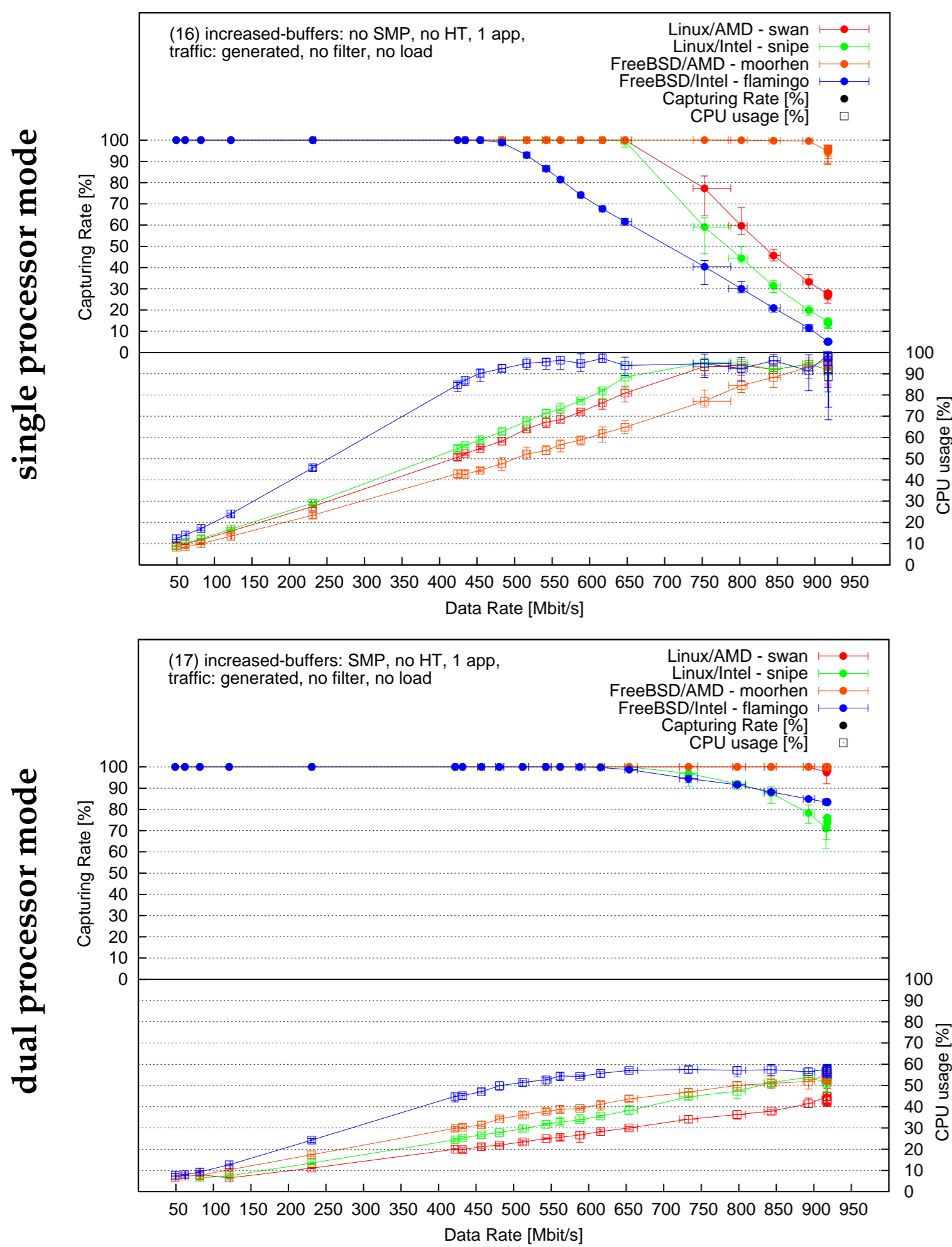
- Split 10-GigE traffic stream across multiple 1-GigE links
- Performance evaluation of 1-GigE systems for various operating system/architecture pairs

## SUMMARY OF RESULTS

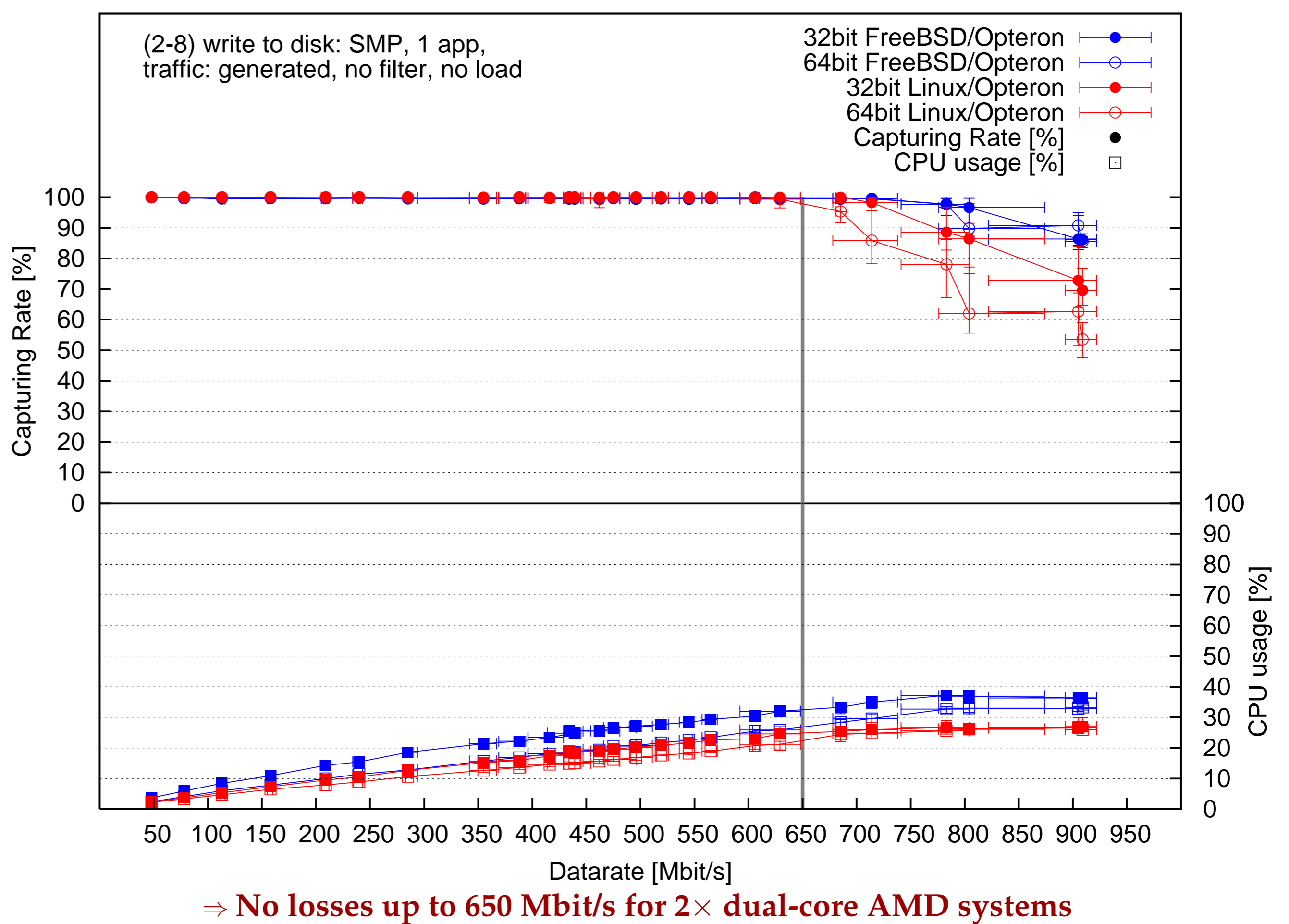
- The link aggregation feature enables traffic splitting with reasonable cost Ethernet switches.
- IP address based load-balancing works well.
- Capturing traffic up to 650 Mbit/s to disk is feasible.
- Multiprocessors systems help
- Given its benefit BPF filtering is cheap
- In general the FreeBSD/AMD Opteron combination performs best

## MAIN RESULTS

### Packet capture (without tracefile generation)

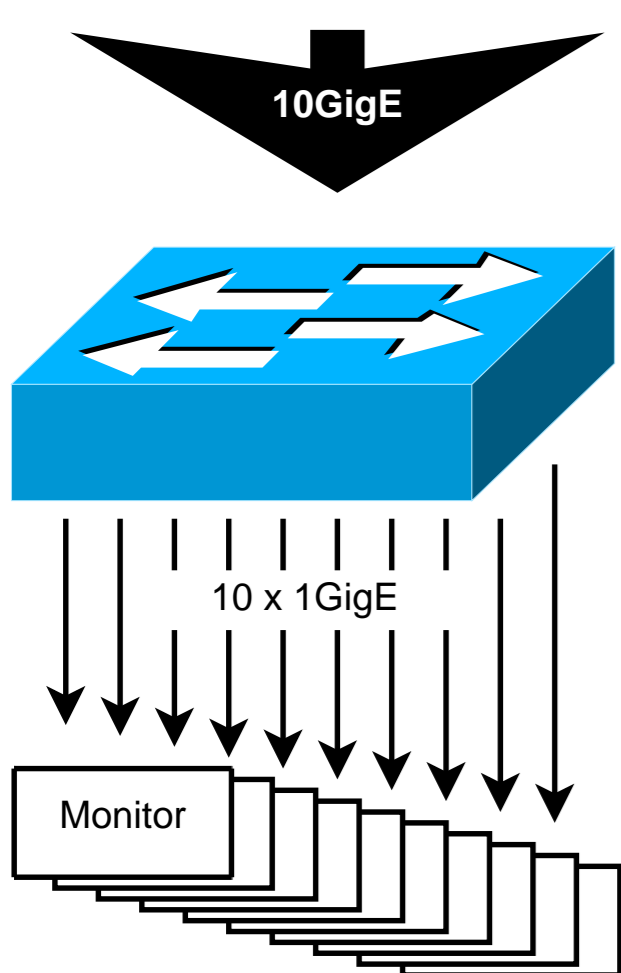


### Packet capture to disk (including content)



⇒ No losses up to 650 Mbit/s for 2x dual-core AMD systems

## HOW TO SPLIT TRAFFIC



Tested on a Cisco 3750:

- 1 GigE to 10 FE
- "EtherChannel"
- Load-balancing:
  - simple switches: MAC addresses
  - e.g., Cisco 3750: IPs and/or MACs
  - e.g., Cisco 6500: MACs, IPs and/or Port Numbers

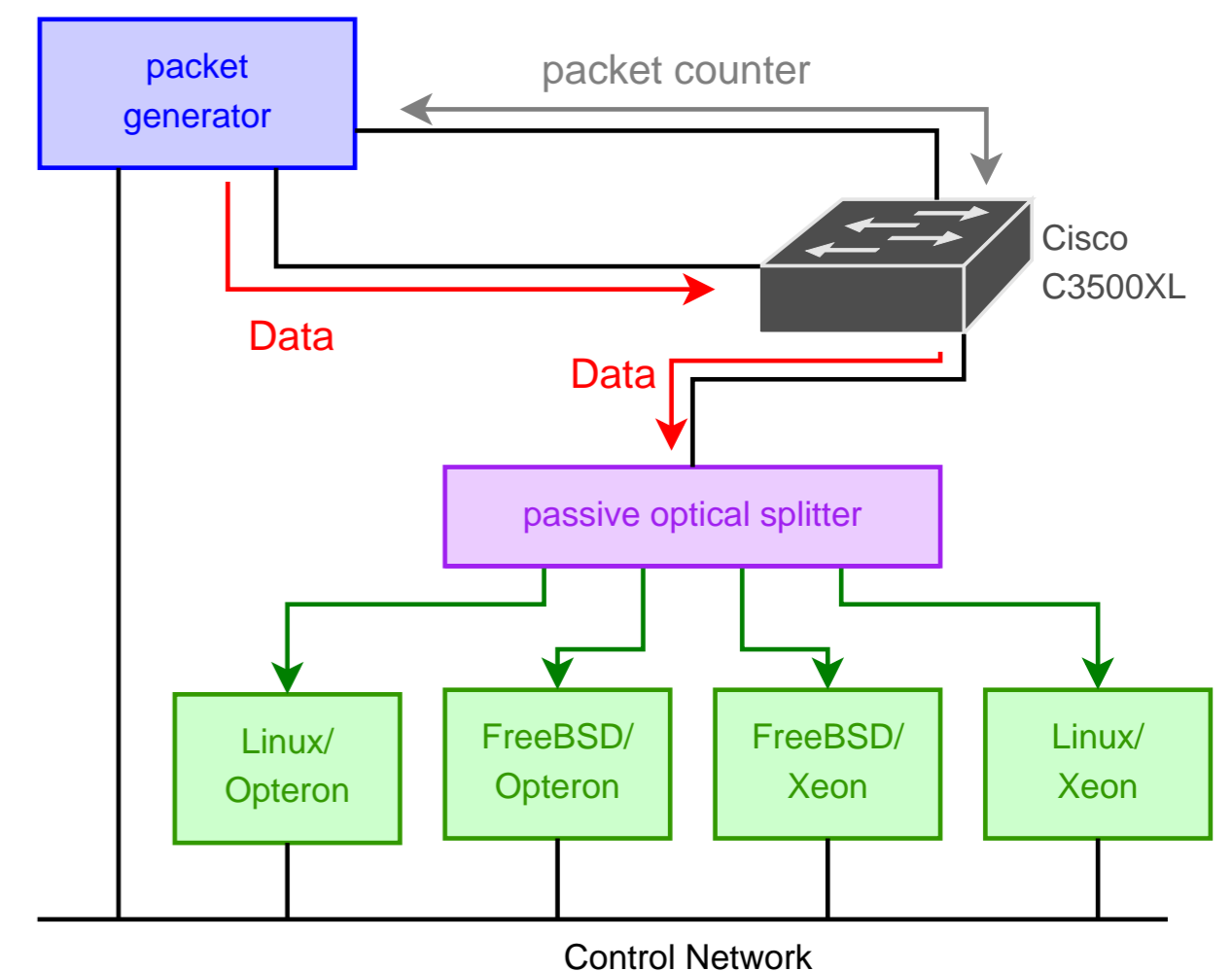
## SYSTEMS UNDER TEST

Four (+two) commodity systems with:

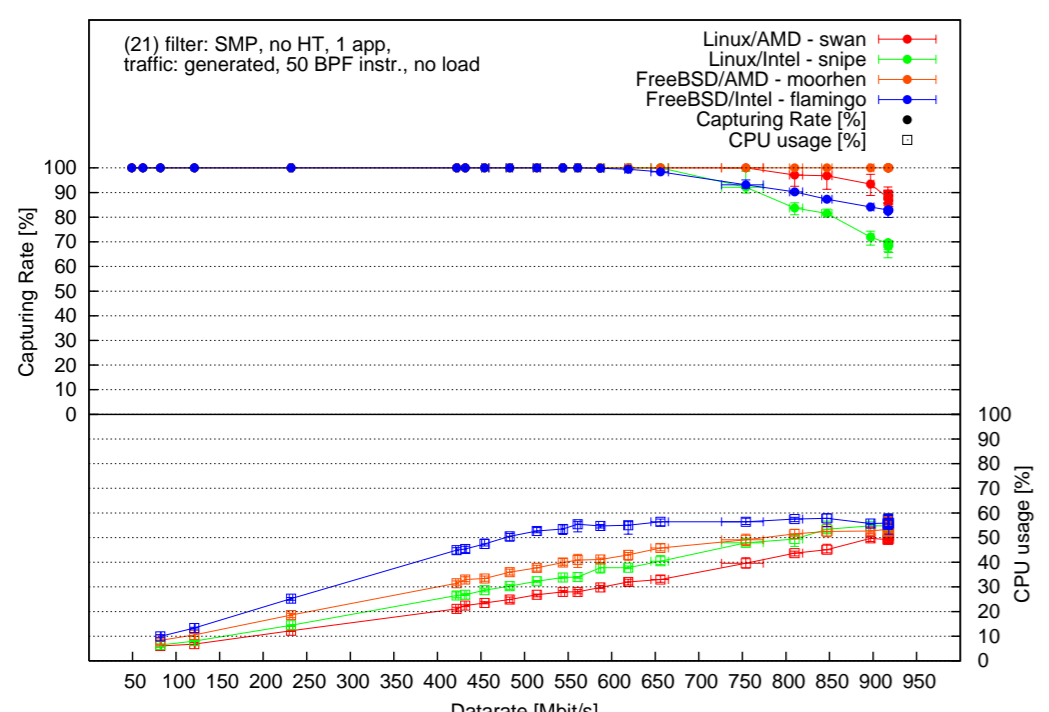
- RAM:** 2 Gbytes
- NIC:** Intel 82544EI Gigabit (Fiber)
- RAID:** 3ware PATA (+HP Smart Array SCSI)
- Space:** at least 450 Gbytes of harddisks

Architecture	OS
AMD Opteron 244	Linux 2.6.11.x
AMD Opteron 244	FreeBSD 5.4
Intel Xeon 3.06GHz	FreeBSD 5.4
Intel Xeon 3.06GHz	Linux 2.6.11.x
(+AMD Opteron 277	Linux 2.6.16.x)
(+AMD Opteron 277	FreeBSD 6.1)

## TEST SETUP

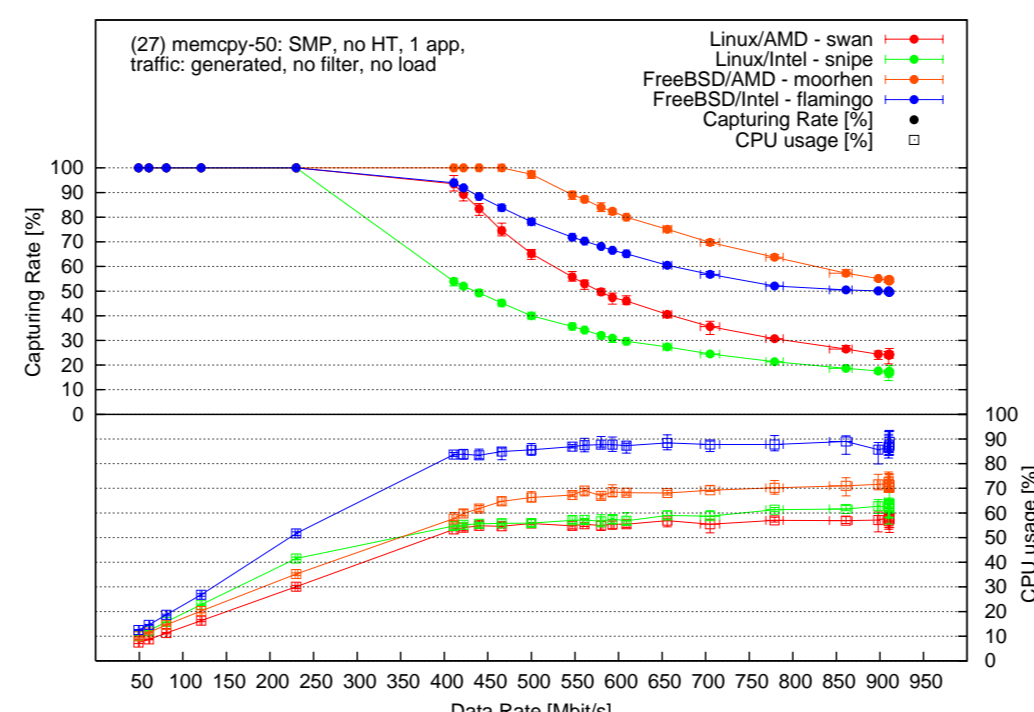


### incl. BPF filter that accepts all packets



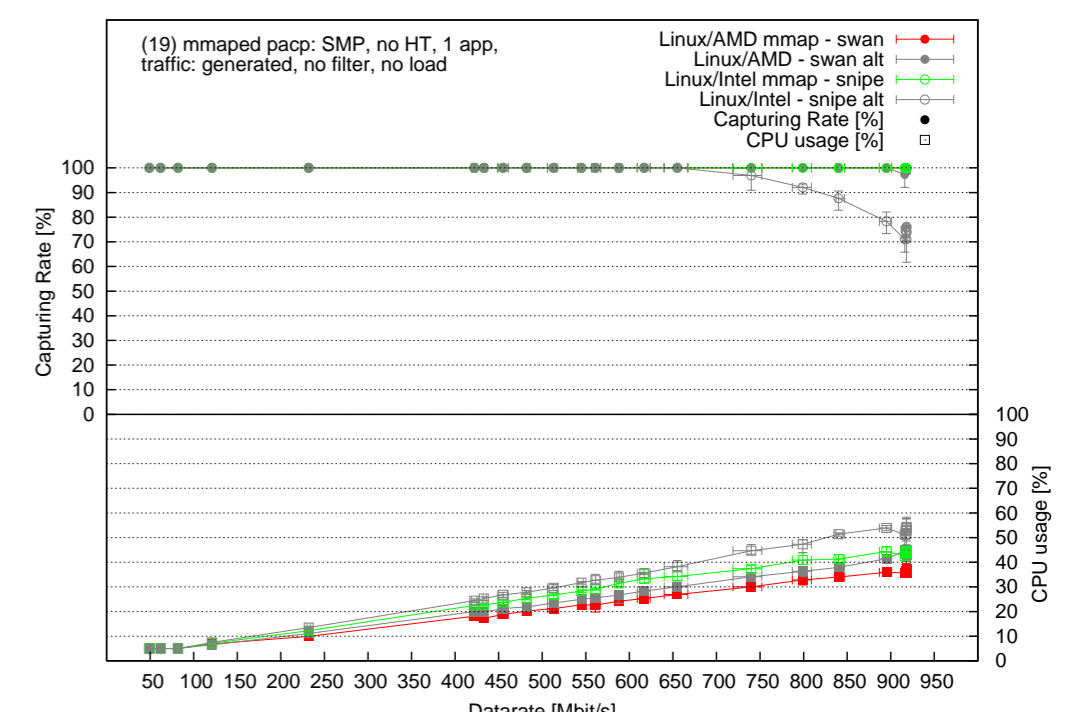
⇒ negligible additional load

### incl. 50 packet copy operations



⇒ dramatical deterioration, especially for Linux systems

### with memory-map patch



for Linux ⇒ performance increase

## ADDITIONAL RESULTS