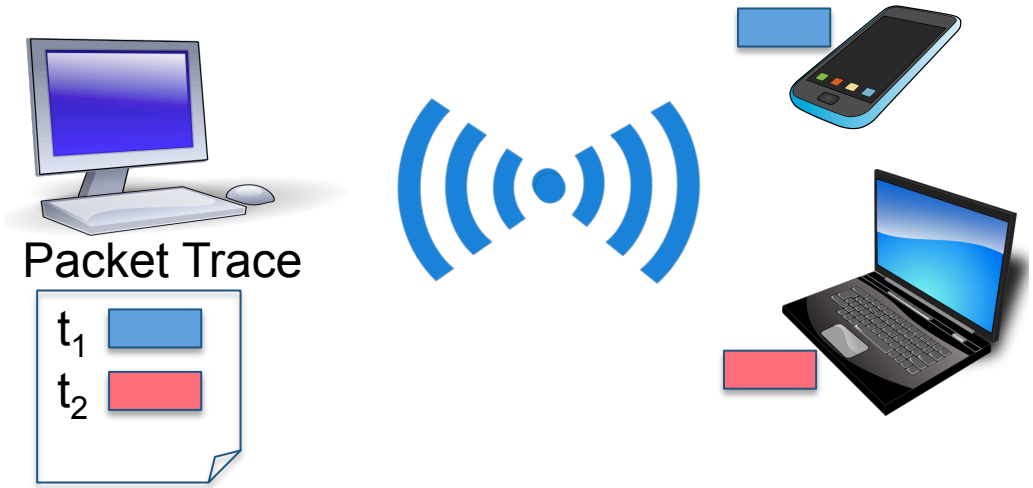
Week 5: Traffic measurements

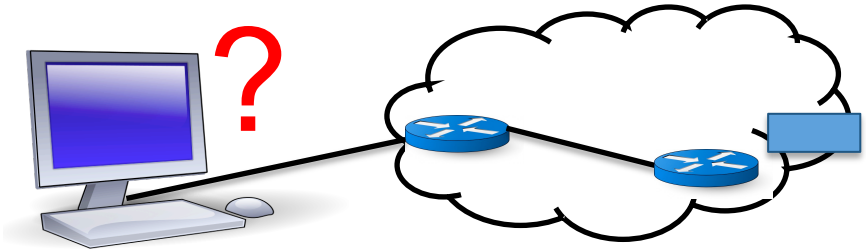
1. Introduction
2. **Packet capture**
   A. End systems
   B. **Network**
3. Interface counts
4. Flow capture
5. Traffic matrix
6. Anonymization of packet traces
7. Conclusion

How to capture packets of a network?

- In broadcast LANs (e.g., WiFi)
  - Set interface in promiscuous mode
  - Then, same as end system packet capture

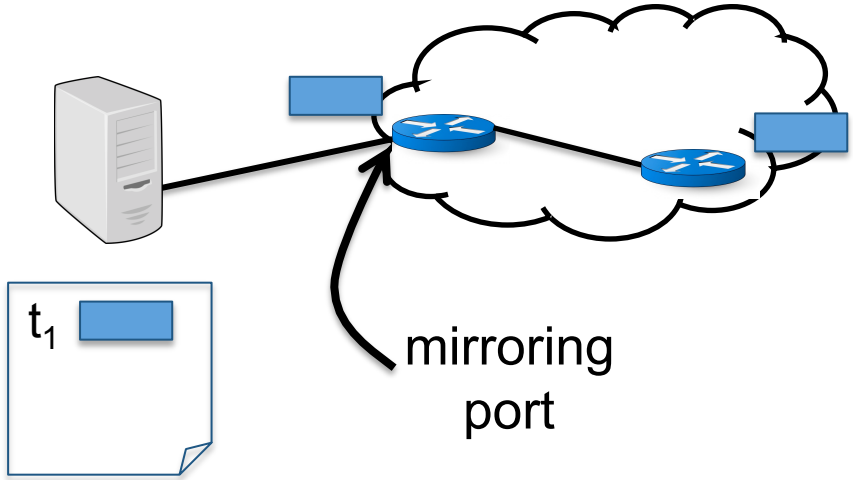


How to capture packets on point-to-point links?



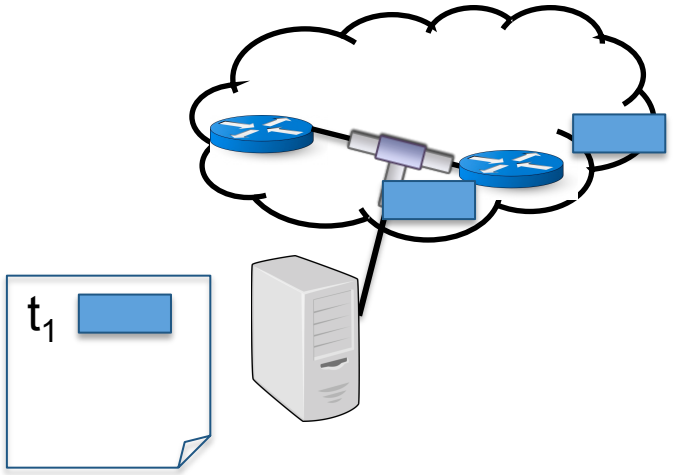
Port mirroring

- Basic method
  - Copies packets from one or more ports to a mirroring port
  - Run packet capturing tool on host connected to mirroring port



Network Tap

- Basic method
  - Electrical or optical splitter on monitored link
  - Monitoring host with specialized network interface and interface driver



Comparison

Port mirroring

- Pros
  - Easy to setup
  - Low cost
- Cons
  - Hardware and media errors are dropped
  - Packets may be dropped at high utilization

Tap

- Pros
  - Monitor all packets
  - Eliminates risk of dropped packets
- Cons
  - Expensive

Picture credits

- **Desktop computer clip art** by OpenClipArt.org (public domain) (slides 2 & 3)
- **WIFI icon** by Canopus49, https://commons.wikimedia.org/wiki/File:WIFI_icon.svg (CC BY-SA 3.0)
- **Smartphone clip art** by OCAL, www.clker.com (public domain) (slide 2)
- **Laptop clip art** by OCAL, www.clker.com (public domain) (slide 2)
- **Server Linux box clip art** by OCAL, www.clker.com (public domain) (slides 4 & 5)
- **Network pipe icon** by TpdkDesign.net (Free for non-commercial use) (slide 5)
- **Router clip art** by OCAL, www.clker.com (public domain) (slides 3, 4 & 5)