Week 5: Traffic measurements

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

Interface counts

- Pro: Lightweight and supported broadly
- Con: Coarse-grained
- Use: everywhere
  - Tracking link utilizations and detecting anomalies
  - Generating bills for traffic on customer links
  - Inference of the offered load (i.e., traffic matrix)

Packet monitoring

- Pro: Detailed per-packet measurements
- Con: High collection overhead
- Use: Selected locations; on-demand
  - Analyzing the small time-scale behavior of traffic
  - Troubleshooting specific problems on demand
  - Network edge for intrusion detection

Flow monitoring

- Pro: More details than interface counts, less than packet captures
- Con: Medium collection overhead controlled with sampling
- Use: Selective, e.g,. network edge
  - Tracking the application mix
  - Direct computation of the traffic matrix
  - Input to denial-of-service attack detection