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

Traffic matrix: Definition

- Representation of traffic volume flowing from sources to destinations

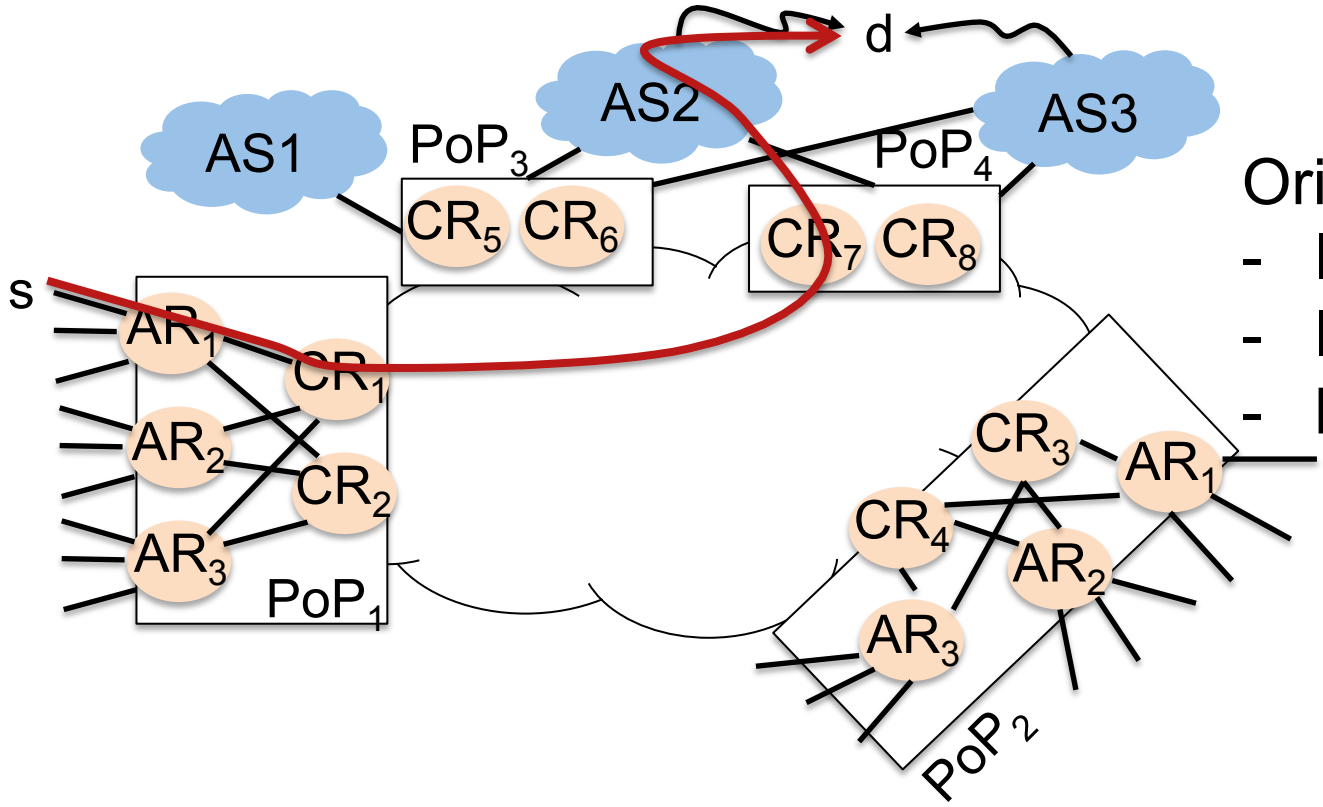
- Links
- Routers
- Points of Presence (PoPs)
- Networks

- Bytes
- Packets
- Flows, etc.

Usage

- Capacity planning
- Traffic engineering (IGP and BGP)
- Billing
- Peering analysis
- Anomaly detection
- Design of new protocols

Origin to destination (OD) matrix



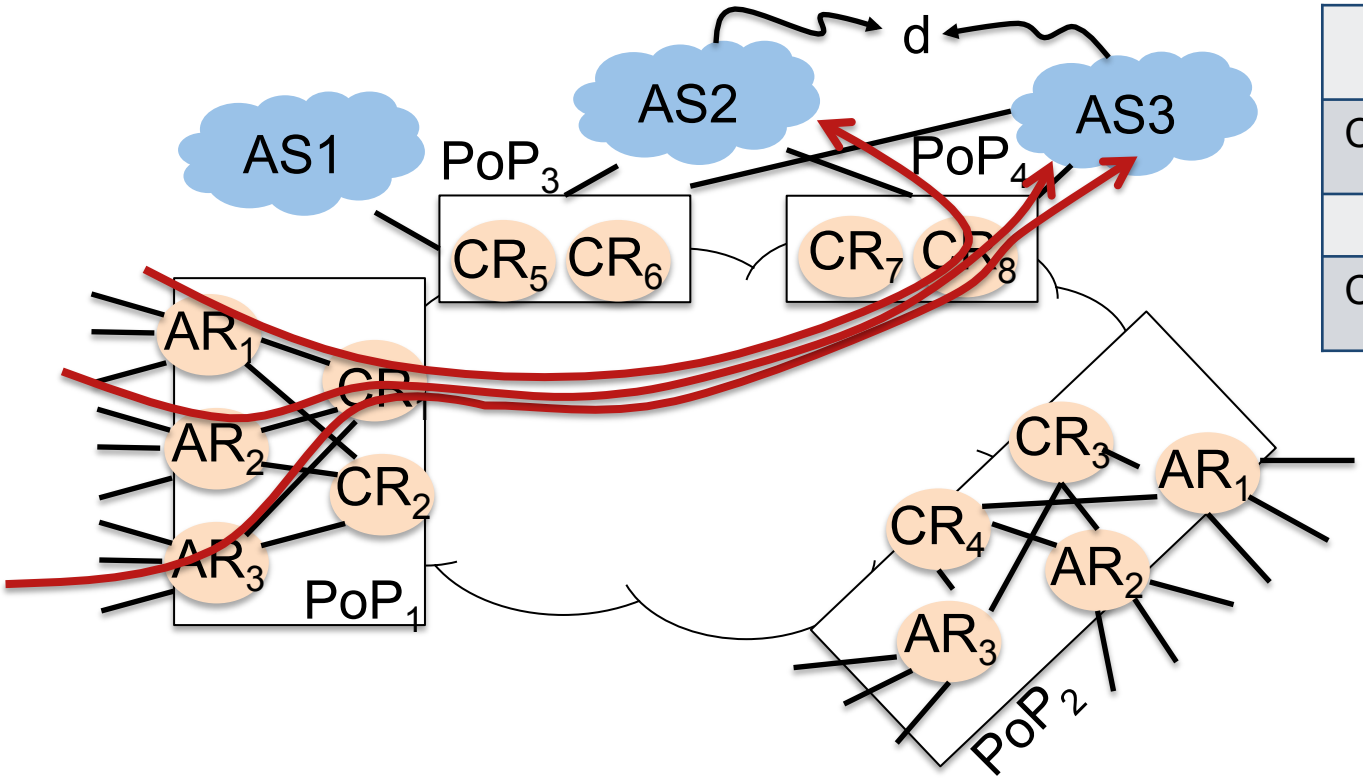
Origin, destination:

- IP address
- IP prefix
- Network

Challenges

- Large matrices are hard to work with
  - E.g.: 2^{32} IPv4 addresses (worse for IPv6)
  - Computational/storage problems
  - Very sparse matrix
- No single entity sees the entire OD matrix
  - Cannot be fully measured
  - Instead, operators work with ingress to egress (IE) matrix

Ingress router to egress router matrix



	CR_1	...	CR_8
CR_1			
...			
CR_8			

Measuring the traffic matrix

- Packet capture
  - Gives the most detailed view of traffic
  - But, expensive and high collection overhead
- Flow capture
  - Enough to build traffic matrix
  - Lower collection overhead (in particular with sampling)
- Interface counts
  - Cannot directly measure traffic matrix, must estimate
  - Lowest overhead, widely available