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

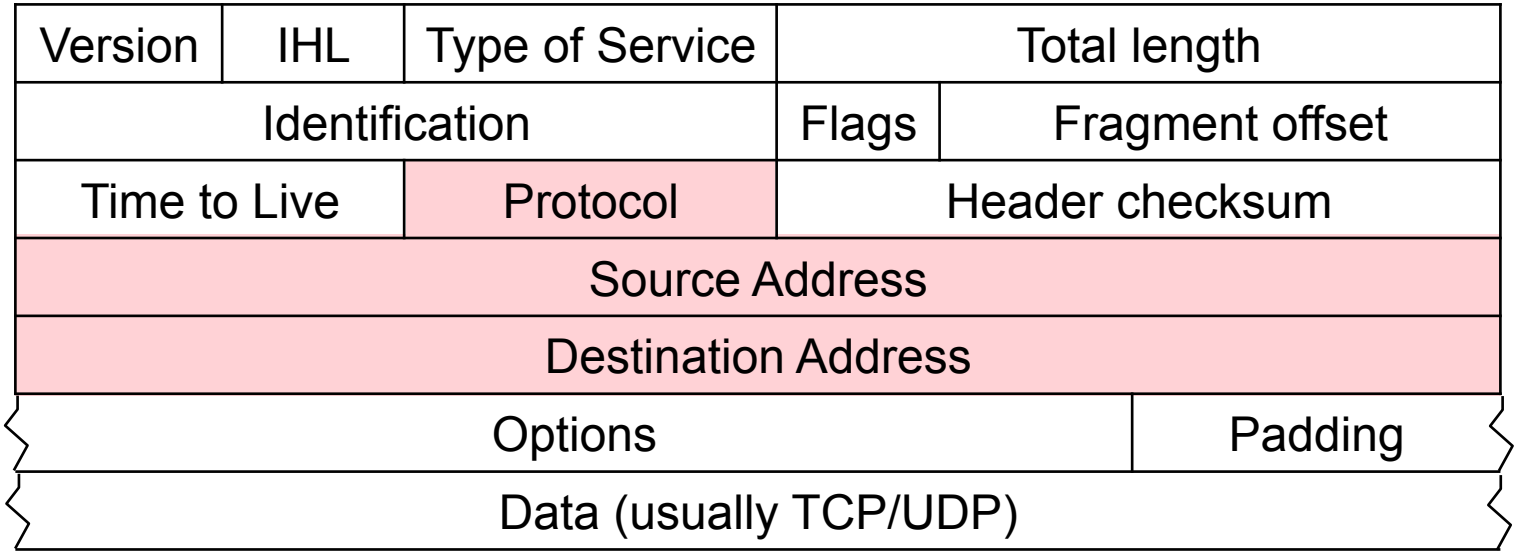
Why measure traffic?

- Performance analysis
- Anomaly and intrusion detection
- Network engineering

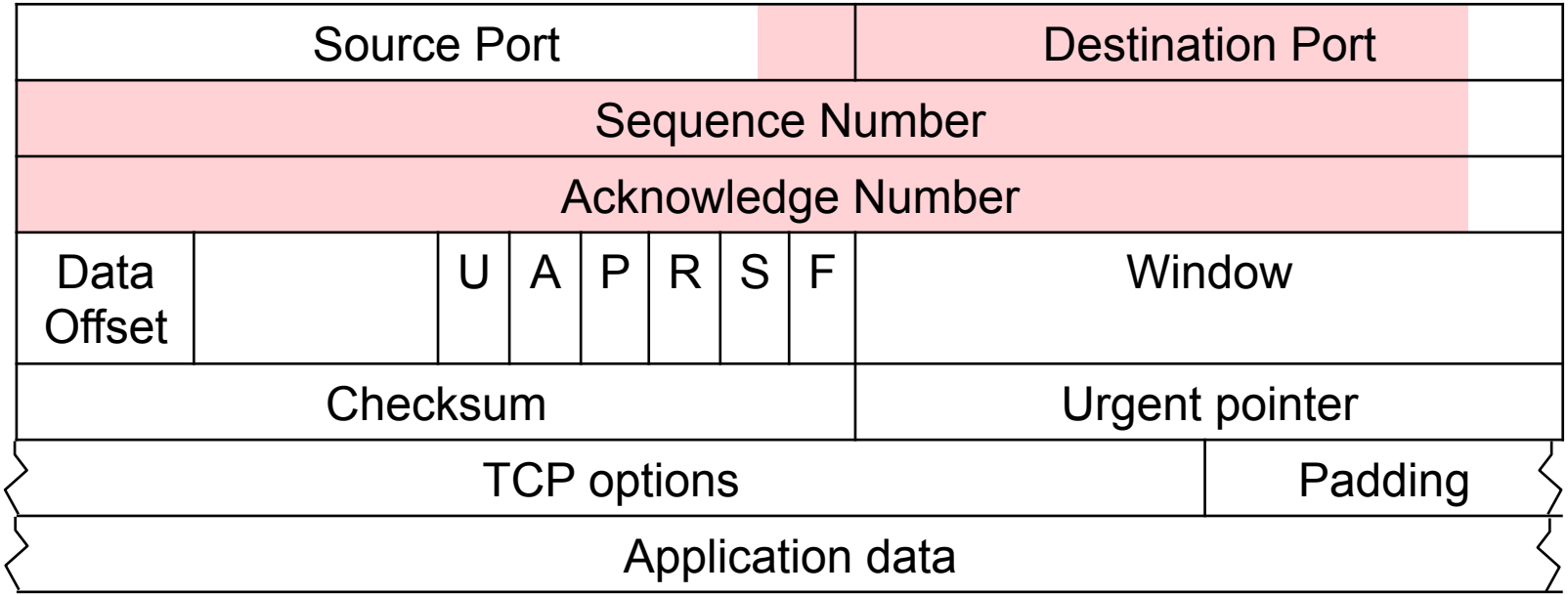
Traffic at different granularities

- IP-level packets
  - Capture per-packet information
- Flows
  - Statistics of packets grouped into flows
- Network interface
  - Statistics of packets that traverse a network interface

IP header


Version
IHL
Type of Service
Total length
Identification
Flags
Fragment offset
Time to Live
Protocol
Header checksum
Source Address
Destination Address
Options
Padding
Data (usually TCP/UDP)

TCP header


Source Port
Destination Port
Sequence Number
Acknowledge Number
Data Offset
U
A
P
R
S
F
Window
Checksum
Urgent pointer
TCP options
Padding
Application data

Outline of this week

- Tools for measuring traffic
  - Packet capture
  - Interface counts
  - Flow capture
- Traffic matrix
- Anonymization of packet traces
- Conclusion