Network Traffic Evolution

Prof. Anja Feldmann, Ph.D.

Testbed

- tst1.inet.tu-berlin.de
- tst2.inet.tu-berlin.de

- user/password: measurement17/Meter17

Example trace

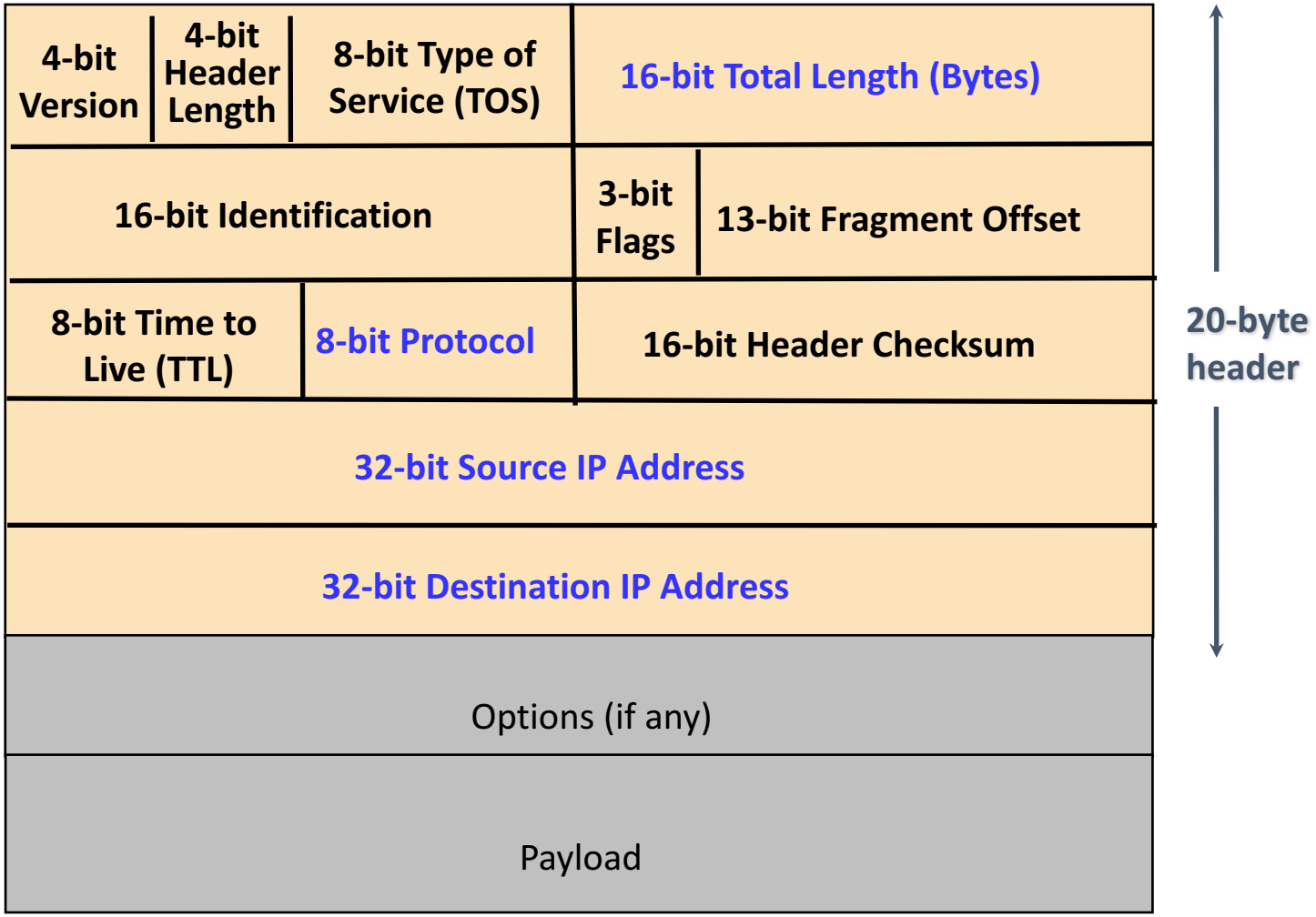
Name	*Port*	*%bytes*	*%packets*	*bytes per packet*
world-wide-web	80	???	???	???
netnews	119	???	???	???
pop-3-mail	110	???	???	???

Passive Measurements

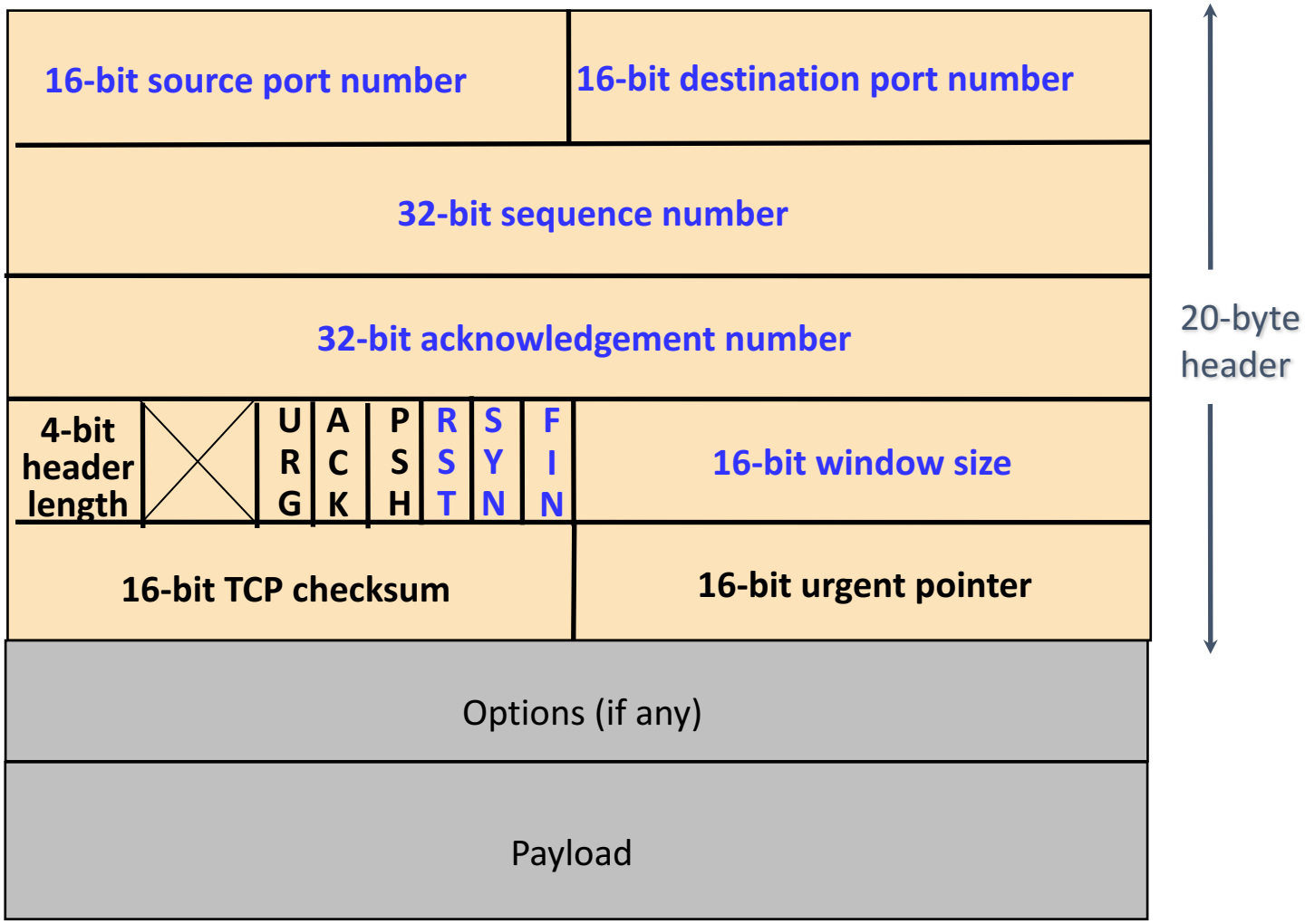
- Definition:
  - Observing traffic into the network
  - Computing metrics on the monitored traffic
  - In our case: Application Mix

- Packet monitors
  - Available data:
    - All protocol information
    - All content

IP header format



TCP header format



Tools

- *ipsumdump*
  - Good for quick summaries
- *tcpdump*
  - Good for in depth details
  - Basis for wireshark
- *wireshark*
  - Good for visual inspection of in depth details
- *Bro*
  - Good for in depth scripted analysis
  - Security analysis
  - Application analysis

ipsumdump (subset)

```
'Ipsumdump' reads IP packets from tcpdump(1) files, or network interfaces,
and summarizes their contents in an ASCII file.

Usage: ipsumdump [DATA OPTIONS] [-i DEVNAMES | FILES] > SUMMARYFILE

General data options:
  -t, --timestamp            Include packet timestamp.
  -T, --first-timestamp      Include flow-begin timestamp.
  -c, --packet-count         Include packet count (usually 1).
      --wire-length          Include wire length (with link header/trailer).
      --link                 Include link number (NLANR/NetFlow).

Ethernet data options:
      --eth-src              Include Ethernet source address.
      --eth-dst              Include Ethernet destination address.

IP data options:
  -s, --src                  Include IP source address.
  -d, --dst                  Include IP destination address.
  -l, --length               Include IP length.
  -p, --protocol             Include IP protocol.
  -g, --fragment             Include IP fragment flags ('F' or '.').
  -G, --fragment-offset      Include IP fragment offset.
      --ip-id                Include IP ID.
      --ip-sum               Include IP checksum.
      --ip-opt               Include IP options.
      --ip-ttl               Include IP time to live.
      --ip-tos               Include IP type of service.
      --ip-hl                Include IP header length.
      --capture-length       Include length of captured IP data.
```

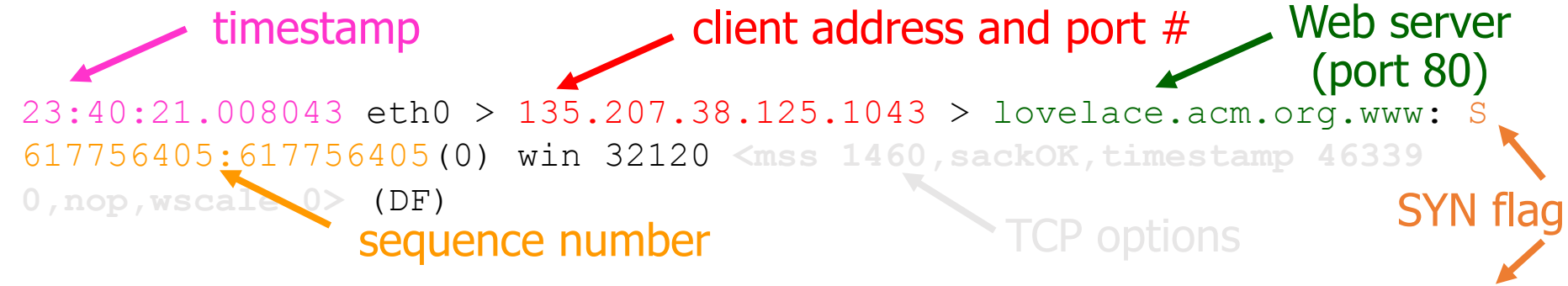
tcpdump (subset)

```
tcpdump version 4.9.0
libpcap version 1.6.2
OpenSSL 1.0.1t  3 May 2016
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
```

tcpdump (subset)

```
TCPDUMP(8)                    System Manager's Manual                    TCPDUMP(8)

NAME
       tcpdump - dump traffic on a network

SYNOPSIS
       tcpdump [ -AbdDefhHIJKlLnNOpqStuUvxX# ] [ -B buffer_size ]
               [ -c count ]
               [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
               [ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
               [ --number ] [ -Q in|out|inout ]
               [ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ]
               [ -E spi@ipaddr algo:secret,...  ]
               [ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
               [ --time-stamp-precision=tstamp_precision ]
               [ --immediate-mode ] [ --version ]
               [ expression ]

DESCRIPTION
       Tcpdump prints out a description of the contents of packets on a network interface that match the boolean expression; the description is pre-
       ceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight.  It can also  be  run  with
       the  -w  flag,  which causes it to save the packet data to a file for later analysis, and/or with the -r flag, which causes it to read from a
       saved packet file rather than to read packets from a network interface.  It can also be run with the -V flag, which causes it to read a  list
       of saved packet files. In all cases, only packets that match expression will be processed by tcpdump.

       Tcpdump  will, if not run with the -c flag, continue capturing packets until it is interrupted by a SIGINT signal (generated, for example, by
       typing your interrupt character, typically control-C) or a SIGTERM signal (typically generated with the kill(1) command); if run with the  -c
       flag, it will capture packets until it is interrupted by a SIGINT or SIGTERM signal or the specified number of packets have been processed.
```

Tcpdump output
(three-way TCP handshake and HTTP request message)




```
23:40:21.008043 eth0 > 135.207.38.125.1043 > lovelace.acm.org.www: S
617756405:617756405(0) win 32120 <mss 1460,sackOK,timestamp 46339
0,nop,wscale 0> (DF)

23:40:21.036758 eth0 < lovelace.acm.org.www > 135.207.38.125.1043: S
2598794605:2598794605(0) ack 617756406 win 16384 <mss 512>

23:40:21.036789 eth0 > 135.207.38.125.1043 > lovelace.acm.org.www: .
1:1(0) ack 1 win 32120 (DF)

23:40:21.037372 eth0 > 135.207.38.125.1043 > lovelace.acm.org.www: P
1:513(512) ack 1 win 32256 (DF)

23:40:21.085106 eth0 < lovelace.acm.org.www > 135.207.38.125.1043: .
1:1(0) ack 513 win 16384

23:40:21.085140 eth0 > 135.207.38.125.1043 > lovelace.acm.org.www: P
513:676(163) ack 1 win 32256 (DF)

23:40:21.124835 eth0 < lovelace.acm.org.www > 135.207.38.125.1043: P
1:179(178) ack 676 win 16384
```

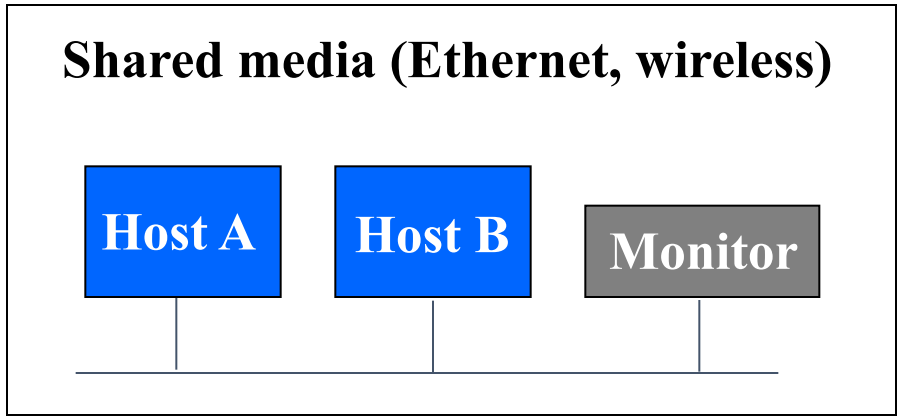
wireshark (subset)

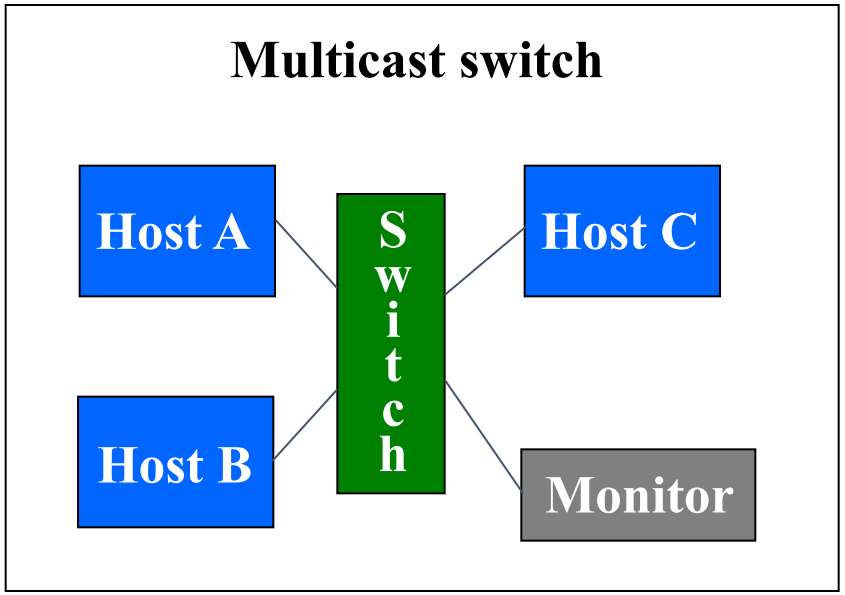
```
Usage: wireshark [options] ... [ <infile> ]

Capture interface:
  -i <interface>           name or idx of interface (def: first non-loopback)
  -f <capture filter>      packet filter in libpcap filter syntax
  -s <snaplen>             packet snapshot length (def: 65535)
  -p                       don't capture in promiscuous mode
  -k                       start capturing immediately (def: do nothing)
  -S                       update packet display when new packets are captured
  -l                       turn on automatic scrolling while -S is in use
  -I                       capture in monitor mode, if available
  -B <buffer size>         size of kernel buffer (def: 2MB)
  -y <link type>           link layer type (def: first appropriate)
  -D                       print list of interfaces and exit
  -L                       print list of link-layer types of iface and exit

Capture stop conditions:
  -c <packet count>        stop after n packets (def: infinite)
  -a <autostop cond.> ...  duration:NUM - stop after NUM seconds
                           filesize:NUM - stop this file after NUM KB
                              files:NUM - stop after NUM files
Capture output:
  -b <ringbuffer opt.> ... duration:NUM - switch to next file after NUM secs
                           filesize:NUM - switch to next file after NUM KB
                              files:NUM - ringbuffer: replace after NUM files
Input file:
  -r <infile>              set the filename to read from (no pipes or stdin!)

Processing:
  -R <read filter>         packet filter in Wireshark display filter syntax
  -n                       disable all name resolutions (def: all enabled)
  -N <name resolve flags>  enable specific name resolution(s): "mntC"
```

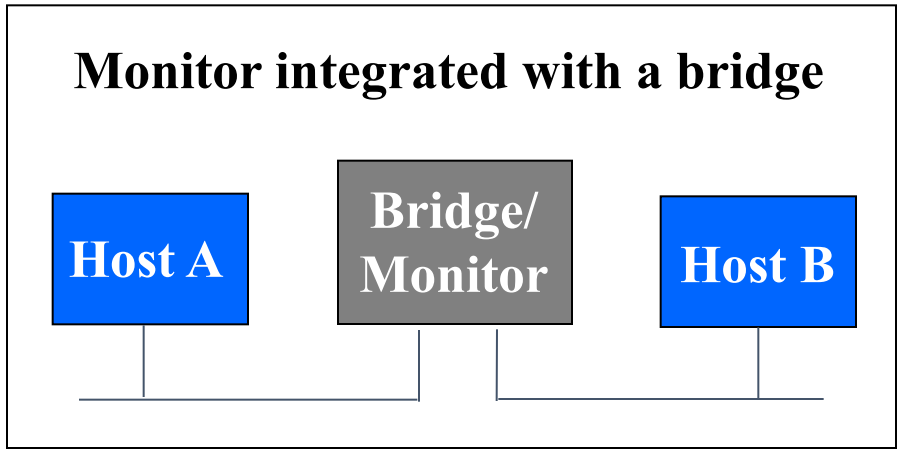
Selecting traffic

- *Filter* to focus on a subset of the packets
  - IP addresses/prefixes (e.g., to/from specific Web sites, client machines, DNS servers, mail servers)
  - Protocol (e.g., TCP, UDP, or ICMP)
  - Port numbers (e.g., HTTP, DNS, BGP, Napster)
- Collect first n bytes of packet (snap length)
  - Medium access control header (if present)
  - IP header (typically 20 bytes)
  - IP+UDP header (typically 28 bytes)
  - IP+TCP header (typically 40 bytes)
  - Application-layer message (entire packet)

Monitoring a LAN link







Monitoring a WAN link