Capturing network traffic

An introduction to Ethereal and Tcpdump

Jon-Olov Vatn

Network sniffers

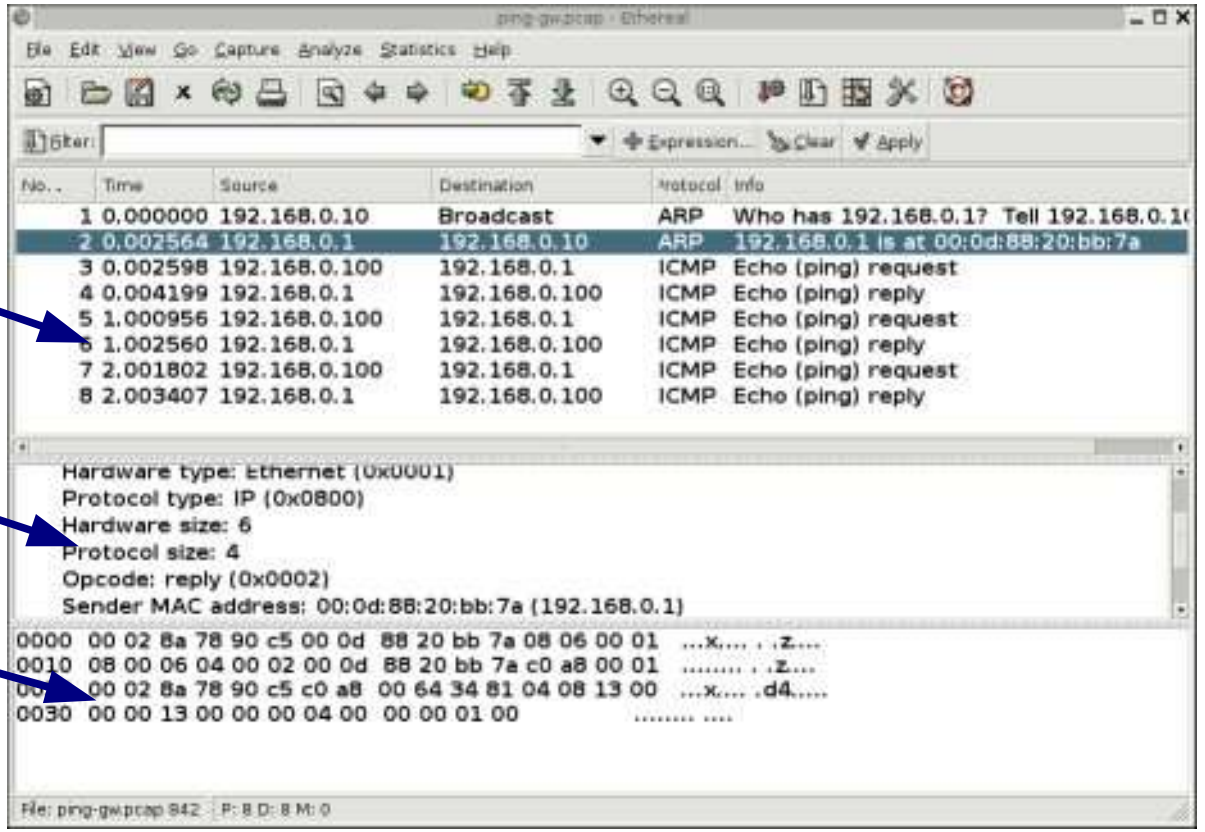
- Purpose of using them
  - Educational
  - Troubleshooting
  - Network measurements and analysis
  - Eavesdropping data communication
- Common tools
  - Ethereal (graphical), http://www.ethereal.com
  - Tcpdump (console), http://www.tcpdump.org

Ethereal (graphical)

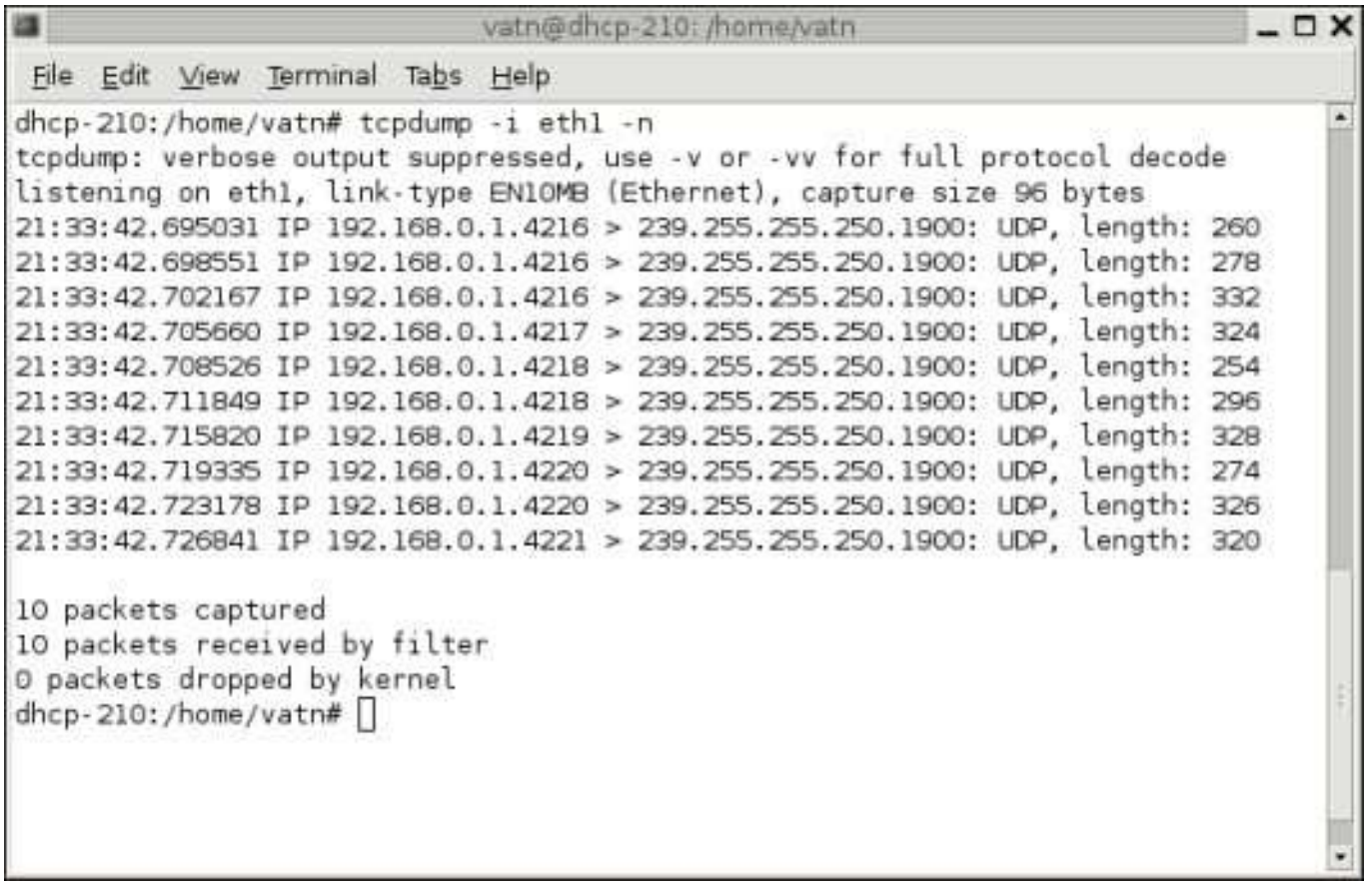
Packet list pane

Tree view pane

Byte view pane



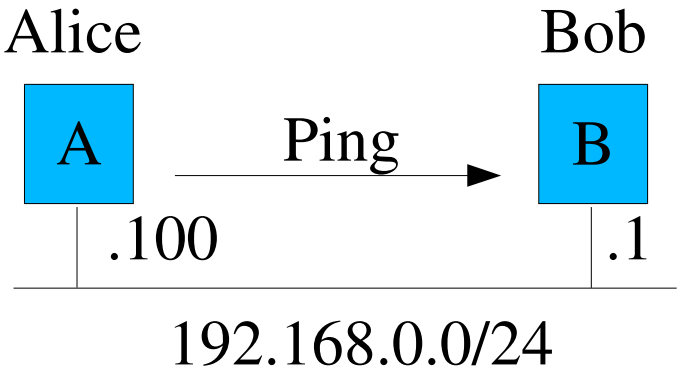
Tcpdump (console)



A simple example

- Alice likes to “ping” Bob
- What packets will we see?
- Encapsulations
  - Have a look at the link layer headers!
  - Have a look at the higher layers!

[file: ping-gw.pcap]



Filtering out relevant traffic

Capture filters:

- Smaller files
- “Tcpdump”-syntax,
- See ethereal “help” or “man tcpdump” for more info

[live capture]

Display filters:

- Displays a subset of the captured data
- “Ethereal” has its own syntax, see ethereal “help”

[apply display filter]

Observing DNS traffic

- Example: Testing if DNS look-up is faster the 2nd time. (My home network, WLAN router attached via ADSL to ISP)
- First test: looking up "www.it.kth.se"
  - Files: [dns1.pcap, dns2.pcap]
  - Surprise, no caching effect was observed. Strange!
- Second test: looking up "www.whitehouse.gov"
  - File: [dns-whitehouse.pcap]
  - The delay was even larger the 2nd time. For further investigation!!

Example with DHCP traffic

- Dynamic Host Configuration protocol (DHCP, RFC 2131) enables a host to dynamically acquire an IP address as well as other relevant paramenters from a DHCP server.
- 4-way message exchange (Discover, Offer, Request, and Reply)
  - Should be fast, right?
  - Will we see additional messages?

  Files [dhcp-linux.pcap, dhcp-winxp.pcap]

Analyzing measured data

Commonly one wants to analyze measured data, compute delays, calculate statics etc.

Many alternatives exist:

- Scripts (perl, awk)
- Spreadsheets
- Network analysis tools, e.g., “tcptrace”. See tcpdump and ethereal pages for more info.

Time-sequence plot created by tcptrace and displayed by xplot

Eavesdropping attacks

- Do you send confidential information in clear-text?
- Network security is important, in particular when sending data over wireless links.

File: [web-mail.pcap]