netwerk activiteit bekijken

LUGN#130

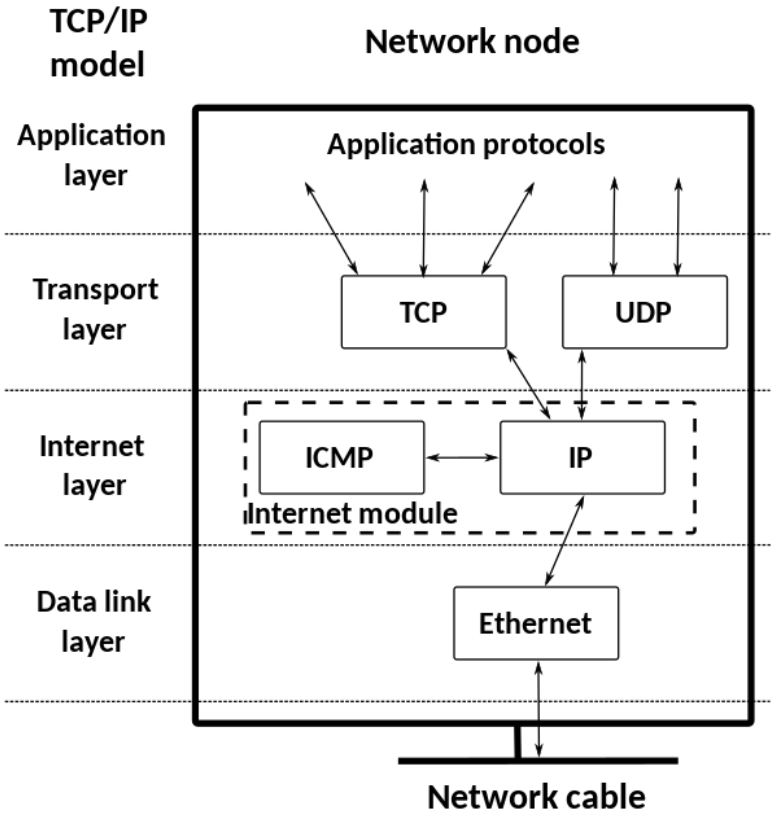
Waarom

Begrip van “networking” helpt in het duiden van netwerk gerelateerde issues

Aan bod komt:

- Inleiding TCP/IP
- Tooling. Uitleg en gebruik van de tooling zal helpen voor:
  - meer begrip over “networking” in het algemeen
  - beter inzicht in de netwerk configuratie
  - beter netwerk gerelateerde issues kunnen duiden/oplossen

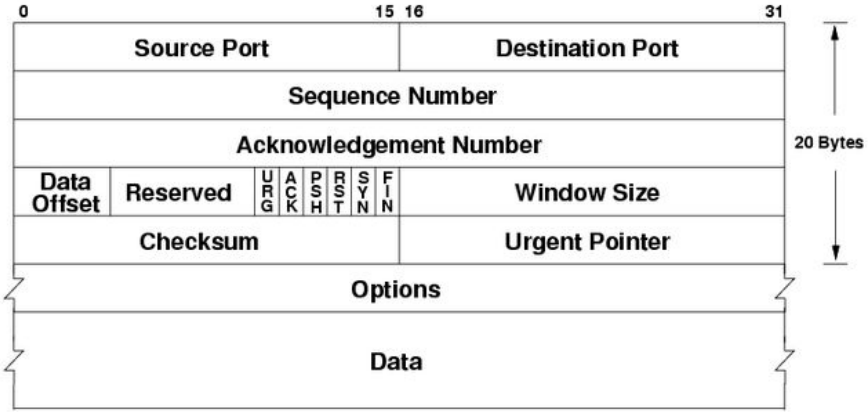
Kleine netwerk inleiding - TCP/IP stack

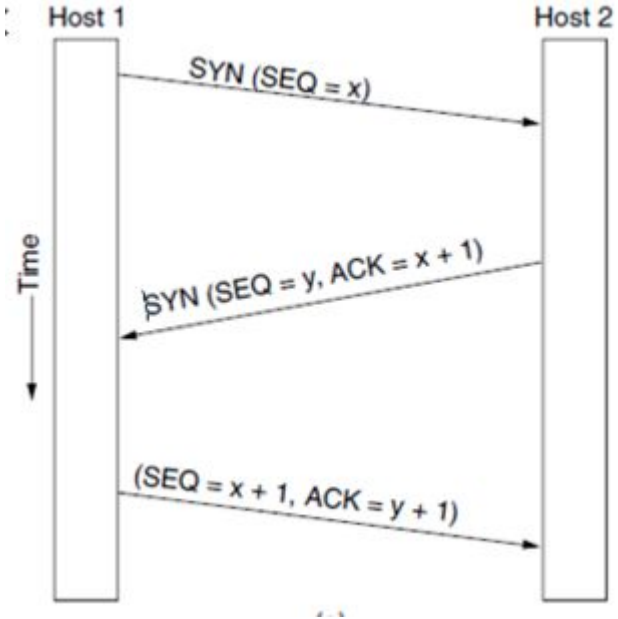


TCP/UDP: laag 4
IP: laag 3
MAC-addressen: laag 2

Kleine netwerk inleiding - TCP

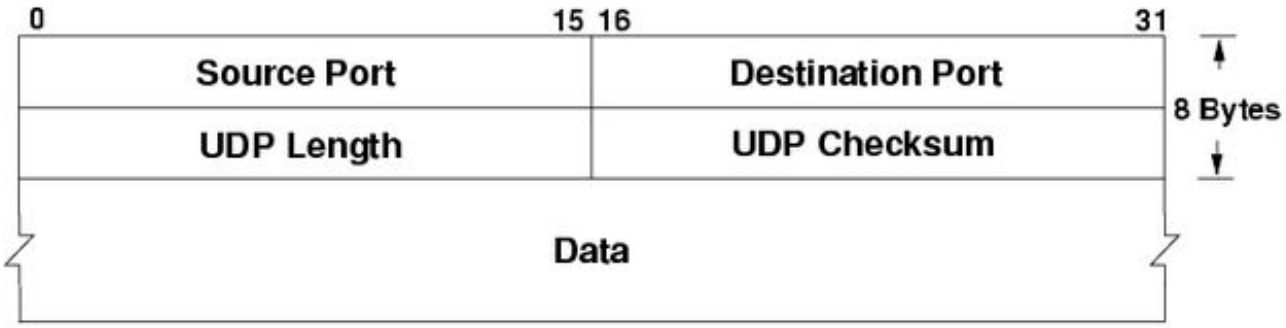
- TCP
  - betrouwbare verbinding (*connection oriented*)
  - meer overhead dan UDP -> langzamer
  - TCP *segments*
  - *email, ftp, www*





Kleine netwerk inleiding - UDP

- UDP
  - minder betrouwbare verbinding (*connection less*)
  - minder overhead dan TCP -> sneller
  - UDP *datagrams*
  - live streaming, video chat, online gaming



Kleine netwerk inleiding - ICMP

- ICMP
  - vooral status en foutmeldingen
    - 0: Echo Reply
    - 3: Destination Unreachable
    - 4: Source Quench
    - 5: Redirect
    - 8: Echo
    - 11: Time Exceeded

Tooling - Toon alle connecties

- `netstat -a`
  - -t -> tcp
  - -u -> udp
  - -n geen naam resolutie
  - -p toon pid/command
- `ss -a`
  - -t -> tcp
  - -u -> udp
  - -n geen naam resolutie
  - -p toon pid/command

Tooling - Wat luister er?

- `netstat -l`
  - -t -> tcp
  - -u -> udp
  - -n geen naam resolutie
  - -p toon pid/command
- `ss -l`
  - -t -> tcp
  - -u -> udp
  - -n geen naam resolutie
  - -p toon pid/command

Tooling - route en interface info

- `netstat -r`
- `netstat -i`

- `ip r(oute)`
- `ip -s linl`

Tooling - Wat wordt er gebruikt?

- `lsof` - list open files
  - -i TCP:22 - welke processen gebruiken poort 22?
  - -i 4|6 - toon alleen welke IPv4 of IPv6 open files
  - -i:22 -a -i 4 - logische combinaties
  - -p PID: welke files heeft PID open?
  - -u *user*: welke files heeft *user* open?
  - -u^root - list niet-root open files
  - *file*: list all open files voor *file*
  - -t: toon alleen PID (voor gebruik met kill)

Note 1: combinatie van -i:port en -p goed voor troubleshoot welke files (logfiles?) gebruikt worden.

Note 2: een file opruimen wat nog in gebruik is (“open”) door een proces levert geen diskruimte op!

Tooling - handige debug met nc

- nc
  - -l *port*: listen (“simulate a service”)
  - host: cat to host
  - -zv: eenvoudige port-scanning (maar er is ook nmap)

Tooling - Wat gaat er over de lijn?

- tcpdump [option]... expression
  - -v: verbose (-vv)
  - -A: data in ascii
  - -i interface
  - -n: geen naam-*lookup*
  - -s *bytes*
  - -w *file*

- wireshark *file*
- tshark -r *file*

expressions:

- host *hostname*
- host a and \(b or c \)
- tcp port 80
- …

Bier?