# **Øving til forelesning uke 2 – Lagmodell og Wireshark**

Hensikten med øvingen er å bli kjent med Lagmodellen (forenklet 5-lag OSI) ved å analysere pakkefangst med Wireshark (WS).

**0. Få en hensiktsmessig pakkefangst**

Pakkefangst med Wireshark viser at det går en overveldende mengde pakker med mange ulike protokoller over trådløsnettet på campus, og sikkert også på hjemmenettet. Vi skal avgrense denne første undersøkelsen til en usikret HTTP-webside.

a. Start fangst i Wireshark: Når du starter Wireshark vises mange nettverkskort på din pc. Dobbeltklikk på nettverkskortet hvor det er aktivitet, mest sannsynlig Wi-Fi kortet.

b. Gjør oppslag på *datakom.no* eller annen webside som bruker usikret HTTP (ikke kryptert overføring HTTPS)

c. Sett display-filter i Wireshark ved å skrive HTTP. Feltet skifter farge til grønt når det er skrevet et lovlig filter. Nå skal bare et fåtall pakker vises, og hvis det er slik kan du stoppe videre pakkefangst.

**1. Undersøk protokollene i pakkene**

Wireshark viser ett pakkehode per linje for den pakken man studerer. Detaljene i pakkehodet vises ved å åpne denne linjen (>).

Når man markerer en protokoll-linje (pakkehode) viser Wireshark hvor stort pakkehodet er. Verdien kan leses nederst til venstre «på bunnlinjen».

* Hvilke protokoller brukes i pakkene?
* Hvor hører disse protokollene til i Forenklet 5-lags OSI-modell?
* Hvor stort er pakkehodet for hver protokoll?

|  |  |  |  |
| --- | --- | --- | --- |
| **Protokoll** | **Lagets navn** | **Lag nummer i lagmodell** | **Størrelsen på pakke-header (ant. byte)** |
| WiFi, fiber, coax (fysiske overføringsmedier) | Fysisk lag | 5 | 595 |
| Ethernet (f.eks. 802.11n) | Lenkelag | 4 | 14 |
| IPv4 | Nettverkslag | 3 | 20 |
| TCP | Transportlag | 2 | 32 |
| HTTP | Applikasjonslag | 1 | 529 |

\*) TCP-Syn pakken har noen «options» som gjør dette pakkehodet noe større. SYN-pakkene inneholder ikke meldingsdata  
\*\*) HTTP-meldingens størrelse avhenger av hvilken pakke man ser på

**3. Hvordan vet mottaker hvilken protokoll (prosess) på laget over som er mottaker av nyttelasten i pakken?**

Når en pakke kommer til mottaker skjer det motsatte av innpakking, pakkehodene blir skrelt av og innholdet (nyttelasten) sendt opp til laget over. Det kan være mange aktuelle protokoller på laget over så derfor har avsender for enkelhets skyld lagt inn beskjed om hvilken protokoll som er mottaker. «Har lagt inn» betyr at det er et felt i pakkehodet hvor denne informasjonen ligger.

* Hva heter dette protokollfeltet på de ulike lagene og hvilken verdi har det?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lag | Gjeldende  Protokoll | Datafelt navn | Datafelt Verdi | Mottaker  protokoll |
| Lenkelag | Ethernet | Type | IPv4 (0x0800) | ? |
| Nettverkslag | IPv4 | Protocol | TCP (6) | ? |
| Transportlag | TCP | Destination Port | http (80) | ? |

\*) sender og mottaker bruker forskjellige Portnummer, webtjener lytter på port 80

**4. Hvilken protokoll bruker navnetjenesten DNS på transportlaget?**

DNS (applikasjonlaget) kan velge blant to typer tjenester på transportlaget, enten pålitelig overføring med TCP eller upålitelig (best effort) med UDP.

Start Wireshark og sett display-filter «DNS». Vent til det dukker opp noen DNS-pakker, f.eks etter bruk av Nettleseren.

* Hvilke tjenester og tilhørende protokoller kan DNS benytte på transportlaget?

*DNS kan bruke tjenestene TCP og UDP. UDP kan forespørre HTTPS, A, AAAA, PTR protokollene.*

**5. Adresser**

Pakker går mellom likestilte lag som kan befinne seg på ulike maskiner. Man må kunne identifisere kilde/avsender og destinasjon/mottaker på de ulike lagene.

🡪 Man finner setting for egen PC slik: *Windows: kjør Ledetekst (eller CMD)*

* *>ipconfig* som viser IP-info for nettverkslaget
* *>ipconfig /all* for mer detaljer, blant annet MAC-adresser

**Hvilken konfigurering har egen PC?**

|  |  |
| --- | --- |
| **Adressefelt** | **Verdi** |
| MAC-adresse | 5c:e9:1e:97:7a:e9 |
| IPv4 | 192.168.0.75 |
| Default gateway IPv4 | 192.168.0.1 |
| Nettmaske | 255.255.255.0 |

Senere i kurset vil vi også spørre om nettverksadressen for denne enheten, denne finnes med en logisk OG-operasjon mellom nettverkmasken og IP-adressen.

🡪 Man kan bruke Wireshark for å finne mottakeradresser (dst) i pakkene som sendes. Adressene kan f.eks. finnes med et ping på en ekstern webadresse. Når man pinger på en webadresse vil det gjøres et DNS-oppslag. Da kan man undersøke DNS-protokollen også 😊

* Finn mottakeradresser (dst) i pakker som sendes. For enkelhets skyld kan undersøkelsen avgrenses til IPv4, vi venter med IPv6.

**Hvilke mottakeradresser brukes i pakker som sendes fra din PC?**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lag** | **Feltnavn i pakkehodet** | **Verdi** | **Tilhører enhet** |
| Lenkelaget | Dst MAC | 00:22:07:72:c1:cc | Ruter (IP-adr. er default gateway) |
| Nettverkslaget | Dst IPv4 | 20.100.42.130 | Mottakers datamaskin (fordi IPv4-adressen er datamaskinens internett-adresse) |

**\*) Hvilken enhet har MAC-adressen som man fant her?**

For å finne/verifisere svaret kan man undersøke ARP-tabell på egen PC. Denne tabellen viser en oversikt som knytter MAC-adresser til aktuelle IP-adresser. Her vil det vises en IP-adresse som også er kjent fra undersøkelsen av egen PCs konfigurering og som har denne MAC-adressen. Slik søker man egen ARP-tabell

* Cmd>arp -a