Oppgave 1. Pakkelogger (maks 100 ord pr. deloppgave)

På hjemmesiden er det lagt ut tekstfiler med informasjon fra 5 forskjellige datapakker som er logget med biblioteket pcap og analysert i programmet Wireshark. Denne oppgaven går ut på å si litt om hver pakke basert på innholdet av loggen.

a) Pakke 1:

Generelt om pakken: dette er en DHCP discover pakke, ref DHCP i forelesningene / boken.

Hva er MAC-adressen til avsenderen av denne pakken?
00:0b:82:01:fc:42
Hva er MAC-adressen til mottakeren av denne pakken?
ff:ff:ff:ff:ff:ff (broadcast)

Hvilken transportlagsprotokoll brukes i pakken?
UDP

Hva er portnummeret til sender og mottager i denne pakken?
Sender: 68 (Bootstrap Protocol Client)
Mottager: 67 (Bootstrap Protocol Server)
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=2

Hva er funksjonen til denne pakken i nettverket?
Sende forespørsel om å få tildelt en IP-adresse via DHCP, sendes til alle maskiner på LAN i håp om at en av dem kjører en DHCP-tjener.

Hva slags pakke kan man forvente som svar på denne forespørselen?
Et DHCP-offer fra DHCP tjeneren

Fra hva slags tjener/enhet vil dette svaret komme?
En maskin (evt router eller annen enhet) som kjører en DHCP-tjener.

Hva betyr det om det ikke kommer noe svar på denne pakken?
At det ikke er noen korrekt kjørende DHCP-tjener på nettverket.

b) Pakke 2:

Hvilken transportlagsprotokoll brukes i pakken?
TCP

Hva er portnummeret til sender og mottager i denne pakken?
Sender: 25
Mottager: 1470

Hva slags tjeneste på avsendermaskinen har sendt denne pakken?
En SMTP (Simple Mail Transfer Protocol) tjener.

Hva slags henvendelse er denne pakken et svar på?
En forespørsel om autentisering.

Hvor mange bytes har blitt sendt i denne forbindelsen frem til denne pakken ble mottatt?
Her må man se på det relative sekvensnummeret til pakken som er 355. Dette er antall bytes som er sendt i forbindelsen til nå. Om denne pakken blir levert korrekt, vil sekvensnummeret være lik 355+TCP Segment Len (30) = 385, som oppgis i feltet "Next sequence number"

c) Pakke 3:

Hva er IP-adressen til sender?
fe80::a00:27ff:fefe:8f95 (eller fe80:0000:0000:0000:0a00:27ff:fefe:8f95)

Hva er IP-adressen til mottaker?
ff02::1:2 (eller ff02:0000:0000:0000:0000:0000:0001:0002) - Dette er en multicastadresse som bare rutes på det lokale LANet, noe som ikke er pensum, men for alle praktiske formål har den samme funksjon som en broadcastadresse på LANet.

Hvilken transportlagsprotokoll brukes i pakken?
UDP

Hva er formålet med pakken?
Dette er også en DHCP-request pakke, men for IPv6.

d) Pakke 4:

Hvilken transportlagsprotokoll brukes i pakken?
TCP

Hva er formålet med denne pakken? (hint, se på flagg i transportlagsprotokollen)
SYN-flagget (Flags: 0x002 (SYN)) viser at dette er den første pakken i 3-veis håndtrykket på en ny forbindelse.

Hva slags forespørsel kommer mest sannsynlig litt etter denne pakken?
Etter dette vil mottakeren sende en SYN,ACK pakke, etterfulgt av en pakke som inneholder ACK-flagget. Siden mottakerporten er 80 (HTTP), kan man forvente en HTTP GET-forespørsel som første applikasjonslagsdata når forbindelsen er satt opp.

Har det blitt utvekslet noe data i samme forbindelse i forkant av at denne pakken ble sendt?
Nei - dette er tydelig, både pga SYN-flagget og sekvensnummeret som er 0 (Sequence number: 0 (relative sequence number))

e) Pakke 5:

Hvilken nettverkslagsprotokoll brukes i pakken?
I prinsippet ingen, siden ARP gjerne klassifiseres som en linklagsprotokoll, men om de svarer ARP på denne, er det for så vidt greit, siden ARP opererer i overgangen mellom nettverkslag og linklag.

Hvilken transportlagsprotokoll brukes i pakken?
Ingen transportlagsprotokoll i denne pakken.

Hva er hensikten med pakken?
ARP brukes til å koble linklagsadresse (MAC-adresse) med IP-adresse. Dette er en ARP-reply pakke som oppgir hvilken IP-adresse og MAC adresse avsenderen har.

Hva er IP-adressen som korresponderer med MAC-adresse 80:fb:06:f0:45:d7?
10.251.23.1

Hva er IP-adressen som korresponderer med MAC-adresse e0:a1:d7:18:c2:72?
10.251.23.139

Oppgave 2 subnetting (maks 500 ord i innleveringen)

I denne oppgaven er det en viss frihet når det gjelder valg, så mye av poenget blir å vise at det ligger noe refleksjon/kunnskap bak valgene.

I denne oppgaven legges det vekt på forståelse for valgene involvert når man må sette opp et nett og forståelse av tjenestene som kreves i et LAN som skal snakke med Internett. Prøv å svare kort og konsist.

Du skal hjelpe det lokale bakeriet med å sette opp et nettverk til bruk for kundene, slik at de kan ha Internettforbindelse via trådløst nettverk. De forventer å ha opp mot 50 kunder av gangen. De har fått tildelt én global internettadresse fra sin ISP.

a) Hvilke enheter og tjenester må nettverket minimum ha for å fungere.
Enheter: En router som sørger for at trafikken kan nå Internett. Denne routeren må implementere NAT, siden det oppgis at bakeriet har fått tildelt kun én IP-adresse fra sin ISP. Det må også finnes et trådløst aksesspunkt, siden det oppgis at kundene skal kunne bruke trådløst nettverk. Dette må gjerne være i samme enhet som routeren, men det bør komme tydelig frem at det er forståelse for at dette er to forskjellige tjenester/funksjoner. Om noen velger å liste opp netteverkskabler osv, er ikke det noe negativt. Om de sier at de ønsker å plassere f.eks DHCP og DNS på dedikerte tjenere, er ikke dette noe problem. Det er heller ikke noe problem at alt plasseres i en WiFi router (noe som er det mest vanlige i et lite nettverk som dette).
Tjenester: utover NAT som nevnes over, er det viktigste DNS og DHCP. Om de velger å ikke bruke dette, bør de ha skrevet hva slags konsekvenser dette vil by på for

klientene. F.eks at mangel på DHCP vil bety at de må tildele brukerne IP-adresser manuelt.
DNS kan f.eks være gitt av en ekstern tjeneste, men da må DHCP-tjeneren forsyne klientene med riktig DNS-adresse gjennom en DHCP-opsjon. Om de velger å si noe om WiFi kryptering (f.eks WPA) er dette bare positivt, men ikke kritisk for bestått.

b) Spesifiser hvordan subnettet kan se ut, og diskuter valgene. Spesifiser subnettadresse, nettverksmaske, kringkastingsadresse.

Her tenkes det mest på å velge en subnettmaske som gir et passe antall vertsadresser for bruken. En 24 bits maske gir 254 vertsadresser, noe som bør være mer enn nok. Om de velger en nettverksmaske med mindre enn 24 bits, bør de ha en refleksjon rundt at det er et stort kringkastingsdomene, og om det er hensiktsmessig. Det bør også være valgt et subnett som bruker private IP-adresser, fortrinnsvis 192.168.x.x (16-bit blokk). Subnettadresse, nettverksmaske, kringkastingsadresse må passe med valgene de har tatt.

c) Gitt valgene deres i a) og b), hvor mange enheter kan være tilkoblet samtidig?
Her bør de vite hvor mange vertsadresser deres valg av nettverksmaske gir, samt at de må huske at hver av enhetene de har sagt at de plasserer tjenester på (f.eks WiFi router, aksesspunkt eller tjenere) må ha IP-adresser som trekkes fra de tilgjengelige adressene for bakeriets kunder. Siden spørsmålet er litt utydelig formulert når det gjelder dette, bør det allikevel godkjennes om de bare oppgir antall mulige vertsadresser innenfor den gitte nettverksmasken.

d) Bakeriet ønsker å montere et webkamera på utsiden av lokalene, som skal være offentlig tilgjengelig fra utsiden av nettverket. Hva må gjøres på det lokale nettverket/routeren for at dette skal virke?
Her tenkes det på at det må settes opp videresending på porter utenfor routeren til webkameraet på innsiden. Dette kan f.eks. gjøres med demilitarized zone (DMZ), videresending av porter, eller UPnP.