Institutt for datateknologi og informatikk

**Eksamensoppgave i TDAT2004 - Datakommunikasjon med nettverksprogrammering**

**SENSORVEILEDNING**

Faglig kontakt under eksamen:

Olav Skundberg     - tlf.: 95 12 66 50

Eksamensdato: 01.06.2019

Eksamenstid (fra-til): 09:00-12:00

Hjelpemiddelkode/Tillatte hjelpemidler: Ingen

Annen informasjon:

Merk! Studenter finner sensur i Studentweb. Har du spørsmål om din sensur må du kontakte instituttet ditt. Eksamenskontoret vil ikke kunne svare på slike spørsmål.

**1. Lagmodellen**

1. List opp lagene i forenklet OSI-modell. Gi eksempler på tilhørende protokoller og adressering.
2. Beskriv hovedtrekk for adressering på relevante lag og gi eksempler på adresser.
3. Hvilken organisasjon har ansvaret for å standardisering av TCP/IP, og hvordan utvikles disse standardene?

*Svar 1.1*

|  |  |  |
| --- | --- | --- |
| ***Lag*** | ***Protokoller*** | ***Adresser*** |
| *Applikasjonslaget* | *HTTP, SMTP* |  |
| *Transportlaget* | *TCP, UDP* | *Port: 80* |
| *Nett(verks)laget* | *IP* | *IPv4: 158.38.50.20* |
| *Lenkelaget* | *ARP, ETHERNET, 802.11X* | *MAC: 1A:2B:3C:4D:5:E:6F* |
| *Fysisk lag* | *-* |  |

*Svar 1.2*

*Applikasjonslaget: Ikke involvert i pakkeadressering i nettverket, bare ende-ende kommunikasjon. (Kan nevne bruk av URL/DNS uten at det gjør noe)*

*Transportlaget: Porter*

*16 bit / 64 k adresser. Grupperes i velkjente/systemporter (-1024), Bruker/registrerte porter (-49151) og dynamiske/private (resten, -65535).*

*Eks: 80 (HTTP)*

*Nettlaget: IP-adresser (IPv4 og IPv6)*

*IPv4: 32 bit. Grupperes i nummerserier for særskilt bruk. Må nevnte private og offentlige serier. Inneholder både nettadresse og nodeadresse som skilles med nettmasken.*

*Eks: 158.38.50.20 (offentlig), 192.168.0.3 (privat)*

*IPv6: 128 bit. Først og fremst utvidet adresserom. Har fjernet fragmentering og sjekksum som brukes i IPv4. har lagt til felt for flyt.*

*Eks: 2001:0db8:0000:0042:0000:8a2e:0370:7334 (regler for å forkorte skriveformen)*

*Lenkelaget: Mac-adresser/fysiske adresser*

*48 bit, grupperer 24 bit til produsent og 24 bit unik for kretskortet.*

*Eks: 1A:2B:3C:4D:5E:6F (6 posisjoner \* 8 bit = 48 bit)*

*FF:FF:FF:FF:FF:FF kringkastingsadresse, leses inn av alle nettverkskort*

*Svar 1.3*

*TCP/IP (transport- og lenkelag) utvikles av IETF (Internet Engineering Task Force). Basert på frivillig medlemskap. Utvikler RFC-standarder (Request for Comment)*

**2. Webtjenesten**

1. Hvordan er formatet på en request-melding og på en headerlinje?
2. Beskriv hvordan webtjenesten bruker mellomlager på PC for å oppnå bedre ytelse.

*Svar 2.1*

*Request-melding: 3 hovedseksjoner*

* *Request-linje (protokoll og versjon, metoder som GET, POST ... )*
* *Headerfelter: angir egenskaper og ønsket funksjonalitet*
* *Body: eventuelle data*

Headerfelter: *kolonseparerte navn-verdi par, eks Host:datakom.no*

*Svar 2.2*

*Mellomlager (lokal cache) hos klient (egen PC) har kopi av nedlastede objekter/filer. Dersom disse kan benyttes om igjen, uten å måtte laste ned på nytt, sparer det tid og båndbredde.*

*Klient:  
Sender en GET-melding og legger samtidig til en headerlinje i forespørselen:* ***If-modified since: dato og tidspunkt*** *(som viser når fila ble laget, ikke når den sist ble lastet ned)*

*Tjener: svarer enten*

1. *Fila er endret:* ***Status 200 (OK)****, sender hele objektet på nytt*
2. *Fila er* ikke *endret:* ***Status 304 «Not modified»*** *(betyr bruk kopi du har)*

**3. Navnetjenesten**

1. Hvordan jobber en lokal navnetjener?
2. Hva er formålet med å ulike *typer* navnerecords (RR)? Gi noen eksempler på typebetegnelser.

*Svar 3.1*

*Jobber rekursivt. Betyr å finne svar på DNS-oppslaget på vegne av klient. Kan ha oppslag lagret i eget cache (levetid), hvis ikke spørres rottjener først. Rottjener henviser videre (gir ikke svaret), så lokal navnetjener må spørre videre (derav rekursjon). Toppnivå-tjener, mellomtjenere, til slutt autoritativ tjener (hvis ingen har mellomlagret)*

*Lokal navnetjener kan være plassert i egen virksomhet, hos ISP eller egentlig hvor som helst i nettet, men bør være nærmest mulig (færrest hopp) for å ha rask responstid.*

*Svar 3.2.*

*Et domenenavn (ntnu.no) er knyttet til flere typer tjenester (web, epost..). For å kunne plassere tjenestene på ulike maskiner av driftsmessige hensyn trengs ulike IP-grensesnitt (ulike IP-adresser). Da må DNS vite hvilken tjeneste man spør om for domenenavnet. Angis med type-feltet:*

*Eks: A (web IPv4), AAAA (IPv6), MX (mailtjener), NS (Navnetjener)…*

*Type-feltet kan også bruke CNAME for å skille Maskinnavn og Alias. (alias: ntnu.no kan ha maskinnavn: mx.mail.it2.whatever.idi) Hvis man får et nytt domenenavn til svar må man gjøre et nytt oppslag for å finne tilhørende IP-adresse til dette navnet)*

**4. Transportlaget**

1. Beskriv etablering av en TCP-forbindelse.
2. Hvordan sikres en fortløpende pålitelig dataoverføring?

*Svar 4.1*

*TCP er pålitelig og bruker kvitteringer. Er tilstandsfull (må kople opp før overføring). Stikkord er 3WHS (three way handshake)*

*Part A: oppretter sende- og mottakerbuffer. Sender en pakke med SYN-flagget satt og sekvensnummer= ISN (Initial Sequence Number, relativt 0). 🡪* ***SYN***

*Part B: Oppretter sende- og mottakerbuffer, aksepterer ved å returnere en pakke med ACK-flagget satt og kvitteringsnummer = 1.   
Men vi ønsker å etablere forbindelse begge veier. Derfor setter part B også SYN-flagget i svarpakken samt eget ISN.****🡨 SYN-ACK***

*Part A: Svarer med ACK-flagget satt og kvitteringsnummer=1 for å vise at pakken er mottatt.****🡪 ACK***

*Svar 4.2*

*(Fokus på sekvensnummer og kvitteringsnummer. Kandidaten må vise forståelse av begrepene, helst med utregnignseksempel. Glidende vindu omtales i neste oppgave, selv om ordet «fortløpende» er gitt i oppgaven her.)*

* *Sekvensnummer: Startposisjon til første byte i nyttelasten for hver eneste pakke (mange forveksler med bit-nummer og pakke/segmentnummer)*
* *Kvitteringsnummer: Summen av sekvensnummer + nyttelast på siste mottatte pakke. Alle pakker med gyldig kvitteringsnummer har satt ACK-flagget=1.*

*Part A: Den første pakken har sekvensnummer=1, og f.eks nyttelast 100*

*Part B: Sender kvittering med kvitteringsnummer 101. Dette viser da forventede sekvensnummer i neste mottatte pakke.*

*TCP kan kvittere på flere pakker i slengen ved å kvittere sist mottatte gyldige pakke, kalles akkumulativ kvittering. Pakker på transportlaget kalles segmenter.*

**5. Transportlaget**

1. Hva er formål og virkemåte for glidende vindu?
2. Hva skjer dersom en pakke går tapt i denne sammenhengen?

*Svar 5.1*

*Formål: Effektivisere kommunikasjon ved å kutte ned ventetid på kvitteringer*

*Virkemåte: Sendebuffer og mottakerbuffer. Sender data fortløpende inntil maks størrelse på sendevindu. Sendevindu regulerer hvor mye data man kan ha utestående før kvitteringer (kvitteringsnummer på sist mottatte byte) mottas. Etter hvert som kvitteringer mottas vil sendevindu «gli» videre til data som venter på å bli sendt.*

*Sendevindu størrelse påvirkes av RTT, flytkontroll og metningskontroll*

*Svar 5.2*

*Feil indikeres gjennom uteblitte kvitteringer (timeout) eller dobbeltkvittering. Må sende pakker på nytt. Retransmisjon to metoder go-back-n eller selective repeat. (TCP kan håndtere begge, SACK avtales i 3WHS)*

**6. Nettlaget**

1. Hva kjennetegner et IP-nett?
2. Hva kjennetegner et autonomt system (AS) på Internett?
3. Hva bruker en PC nettmasken til, og hvordan?

*Svar 6.1*

*Et IP-nett er definert av sin nettadresse. Alle noder i et IP-nett har samme nettadresse (og derfor også samme nettmaske). Kan kommunisere direkte med hverandre uten å gå via ruter. Felles kringskastingsdomene.   
(Private nettadresser og NAT endrer ikke kjennetegn av IP-nett, man kan absolutt opprette IP-nett hvor alle noder får tildelt offentlige IP-adresser)*

*Svar 6.2*

*Dette spørsmålet er gjentatt også neste oppgave, vurderes der.*

*Svar 6.3*

*En PC bruker nettmasken for å finne ut om mottaker er i eget IP-nett (kan sende direkte) eller om mottaker er i annet IP-nett (må sende via ruter).*

*Bruker logisk OG mellom nettmaske og IP-adresser for sender (egen) og mottaker for å se om nettadressene er like eller ikke.*

*Eksempel: 192.168.0.13* ***OG*** *255.255.255.0 viser nettadressen som 192.168.0.0. (Bonus: CIDR omtale)*

**7. Nettlaget**

1. Hva kjennetegner autonome systemer (AS), og hvordan er de koplet sammen?
2. Forklar virkemåten til Traceroute

*Svar 7.1*

*AS er samling av rutere og overføringslinjer som en organisasjon (ISP/Internettoperatør) eier og drifter. Alle rutere i AS må kjøre samme protokoll for oppdatering av rutingtabeller.*

*AS-er er sammenkoplet i samtrafikkpunkter. Dette er svitsjer (plassert sentrale plasser i landet) hvor Border Gateways (kantrutere) kommuniserer seg imellom. BG snakker sammen (oppdaterer sine rutingstabeller) med protokollen BGP. Om en BG faller ut kan interne brukere kommunisere med hverandre med ikke utenfor ISP-området. Et AS er tildelt adresseområder (som andre AS kjenner til) og som ISP tildeler videre til sine kunder.*

Svar 7.2

*IP-protokoll pakkeheader TTL telles ned for hvert hopp mellom rutere. Hvis 0, vil ruter forkaste pakken og bruker ICMP til å sende feilmelding om dette tilbake til avsender.*

*TR utnytter dette ved systematisk å sette TTL=1 og økende. Da vil hver ruter i kjeden «tvinges» til å sende en feilmelding, og dermed også vise sin avsender-IP.*

**8. Lenkelaget**

1. Beskriv aksessmekanismen på delt Ethernet
2. Hva kjennetegner et ESS (Extended Service Sets)?

*Svar 8.1*

*Gjelder altså kablet LAN uten svitsj. Kalles CSMA/CD, carrier sense multiple access. Konkurransemetode.*

* *Lytter om mediet er ledig. Hvis opptatt, vent tilfeldig tid før nytt forsøk*
* *Hvis ledig, send.*
* *Hvis kollisjon, avbryt. Vent tilfeldig tid og begynn å lytte igjen*

*Bonus: Kan nevne at svitsjet LAN benyttter kabel alene og ikke bruker CSMA/CD.*

*Svar 8.1*

*Et BSS (Basic Service Set) brukes for trådløs kommunikasjon (lenkelaget) og består av ett AP (aksesspunkt) samt et antall noder. AP er koplet til ruter i bakkant. Dette utgjør ett* ***IP-nett*** *og med felles kanal/frekvens for å kommunisere (kollisjonsdomene)*

*Et ESS er bygd opp av flere BSS; og gir mulighet for roaming (forflytning). Det skjer ved at BSS-ene blir koplet sammen «i bakkant» til ruter, slik at grupperingen av BSS-er til sammen fortsatt utgjør ett IP-nett. Det medfører at ESS er et kringkastingsdomene, i motsetning til BSS som er et kollisjonsdomene*

**9. Funksjoner**

1. Beskriv formål og virkemåte for ARP (Address Resolution Protocol)
2. Beskriv formål og virkemåte for DHCP (Dynamic Host Configuration Protocol)

*Svar 9.1*

*Formål: ARP brukes for å finne MAC-adressen til en gitt IP-adresse (på eget IP-nett). Alle noder er konfigurert med en IP men man trenger MAC-adressen for å sende en pakke til rett nettverkskort.*

*Virkemåte: Sender MAC-broadcast på eget IP-nett «hvem har IP nn». Alle nettverkskort tar imot broadcast, men bare node med rett IP svarer. I svaret ligger MAC-adressen (avsender-feltet i MAC-header). ARP brukes også for å finne MAC til egen ruter (hvis mottaker er på eksternt IP-nett)*

*PC bygger opp egen ARP-tabell for å slippe å spørre for hver pakkesending.*

*Svar 9.2*

*Formål: DHCP gir automatisk konfigurering av innstillinger på PC som koples opp i et IP-nett. (Minimum IP-adresse, Nettmaske, DNS og ruteradresse). Slippe brukerkonfigurering av eget utstyr!*

*Virkemåte: DORA*

1. *Klient Discover: PC sender UDP-forespørsel adressert til IP-broadcast 255.255.255.255 og DHCP-port 67. Egen IP settes til 0.0.0.0*
2. *Tjener Offer: Tjener tilbyr minimum 4 nevnte parametere (DHCP kan «huske» MAC-adresse og tilby samme IP som sist)*
3. *Klient Request: PC ber om å få beholde denne konfig*
4. *Accept: Tjener bekrefter at det er i orden og notert (slik at samme IP ikke dels til andre)*

*(DHCP-tjener kan vare plassert i eget IP-nett, i egen ruter (typisk hjemmenett), eller ruter kan fange opp og videresende til DHCP-tjener utenfor eget IP-nett)*

**10. TLS/SSL**

1. Hvordan kontrolleres et digitalt sertifikat?
2. Hvordan etableres en HTTPS-forbindelse?

*Svar 10.1*

*Kontrolleres for gyldighet og ekthet*

*Gyldighet: sjekker felter for gyldighetsdato, bruksområde og ikke trukket tilbake*

*Ekthet: Sertifikatet inneholder et digitalt fingeravtrykk som er kryptert med utsteders private nøkkel. Avtrykket dekrypteres med utsteders offentlige nøkkel (Som man finner i utsteders sertifikat, forhåndsinstallert i nettleser). Da har vi en pålitelig hash-verdi for opprinnelig utstedt sertifikat.*

*Deretter regner man selv ut en hash-verdi for sertifikatet. Dersom denne er lik avtrykket (som vi har dekryptert) har vi garanti for at sertifikatet vi undersøker er identisk med opprinnelig utstedt sertifikat.*

*Svar 10.2*

*Nettleser ber om oppkopling (kan være til vanlig HTTP port 80, men blir omdirigert til port 443 HTTPS)*

*Webtjener svarer med sitt digitale sertifikat*

*Nettleser genererer en symmetrisk nøkkel, krypterer denne med websertifikatets offentlige nøkkel og sender denne krypterte verdien tilbake*

*Webtjener dekrypterer med sin private nøkkel (som bare tjener har!)*

*Videre kommunikasjon skjer med symmetrisk kryptering (begge parter har nå samme symmetriske nøkkel)*

Merknad 1: Sesjonsnøkkelen (Den felles, symmetriske nøkkelen) genereres i TLS-sesjon etter forhandlinger om bruk av algoritmer OBS, men det kreves ikke detaljer om dette.

Merknad 2: Kreves ikke at klient har eget sertifikat installert!