1. HTTP och Webb 6p

1a)

När en webbklient hämtar klart html-basfilen för en webbsida, kommer basfilen vanligtvis innehålla referenser till ett antal tillhörande objekt (bilder, ikoner, ..) som webbklienten skall använda för att hämta objekten från samma webbserver.

- Förklara tydligt vad menas med att webbklienten hämtar ett antal av dessa refererade objekt:
  - Parallellt
  - Seriellt

- Förklara ditt svar i samband med **HTTP**-meddelanden vid s.k. ”persistent” dvs. beständiga anslutningar.

- Kombinera dina svar med hjälp av rum-tids överföringsdiagram i båda fallen (parallellt **och** seriellt).

- Hur kan man praktiskt identifiera att hämtningen sker parallellt eller seriellt?

(4p)

Se avsnitt 2.2.2 i kursboken och Wireshark-labb (HTTP)

FÖRKLARING:

Beständigt ”persistent” HTTP innebär att webbklienten först skapar en TCP-anslutning för att hämta HTML-filen och servern behåller denna anslutning öppen (Connection: Keep-Alive) tills klienten har hämtat de tillhörande objekten. Detta medför att klienten slipper skapa en TCP-anslutning för att hämta varje objekt. På detta sätt minskar man den totala hämtningstiden och de allokerade resurserna.

Parallell hämtning: klienten hämtar klart HTML-filen och sedan begär objekten ”back-to-back” dvs. klienten behöver **inte** vänta på svar **OK-respons** om ett objekt från servern innan den begär nästa med GET-meddelande. Klienten tillåts att begära fler objekt samtidigt (parallellt) men **oberoende** av varandra för att hämta de tillhörande objekten på webbsidan och på detta sätt snabba på svarstiden från servern.

Om man fångar HTTP-trafiken med Wireshark kan det identifieras att **GET-meddelande** för varje refererat objekt skickas nästan samtidigt utan att behöva vänta på **OK-respons** från servern på varje objekt

Seriell hämtning: klienten hämtar klart HTML-filen och sedan begär objekten **ett efter ett** dvs. klienten **väntar på svar OK-respons** om ett objekt från servern innan den begär nästa med GET-meddelande.

På samma sätt som tidigare, när man fångar HTTP-trafiken med Wireshark kan det identifieras att ett **GET-meddelande** för ett av de refererade objekten skickas först och klienten väntar på **OK-respons** från servern innan den begär nästa objekt.

*För mer förklaring se **slide 21-22** i Kapitel_2 föreläsningsbilder.*

1b) Varför har många kända hemsidor (webbservrar) flera IP-adresser för samma namn? Förklara hur det kan vara praktiskt möjligt och motiverat.

(2p)

För att tillmötesgå den stora efterfrågan från stort antal webbklienter skapas ett kluster av maskiner med olika IP-adresser som har samma DNS-namn och med samma innehåll på webbplatsen (replika). DNS-auktoritativa namnservern skall rotera adresserna (round robin) i sina svar om typ-A RRs för hostnamnet på servern för att sprida belastningen mellan flera maskiner.

2. Transportprotokollen 8p

2a) Vad är syftet med att transportprotokollen TCP och UDP använder två nummer (anges i 2 st. 16-bitars header-fält i de sända segmenten)? Ditt svar skall klargöra för användningen av dessa nummer vid transport av data mellan klient och server.

(2p)

Dessa nummer är sändar-portnummer och mottagar-portnummer och används av både TCP och UDP för att identifiera vilket socket (applikation) som segmentets data kom ifrån på en host och till vilket socket (applikation) på den andra hosten skall data levereras. På server-sida är portnummret allmänt känt (0-1023) för en specifik applikation, medan på klient-sidan ofta slumpas numret från ett interval (49152–65535).

2b) Vilket eller vilka av de följande meddelandena **måste** använda UDP och inte TCP? Förklara **specifikt** varför. *(3p)*

- DNS-meddelande mellan klient och server
- *ICMP-meddelande om fel-rapportering*
- DHCP-meddelande om IP-konfiguration
- *HTTP-meddelande med metoden HEAD*
- RIP-uppdateringsmeddelande

- **DNS-meddelande mellan klient och server**
  Se avsnitt 3.3 i kursboken

  DNS-meddelanden mellan klient och server består av en enda DNS-förfråga från klienten följt av ett enda DNS-svar från servern. Dessutom är DNS-meddelandet kompakt och kort dvs innehåller data på ett antal fördefinerade fält som vanligen inte överstiger 512 byte.

  DNS använder UDP för att transportera förfrågningar och svaren. Att använda UDP är snabbare och att det kommer att vara minimal overhead för att få svar. På så sätt kan servern hantera enkelt fler förfrågningar utan att behöva hantera onödvändiga TCP-anslutningar.

- **DHCP-meddelande om IP-konfiguration**
  Se avsnitt 3.3 i kursboken

  DHCP är ett applikation-protokoll (klient/server förhållande) för bootstrap och **använder UDP** för att transportera meddelanden i IP-paket till **broadcast**-adressen som mottagaradress. Dessutom kan TCP-anslutningen inte skapas från en klient som **saknar IP-konfiguration**.

- **RIP-uppdateringsmeddelande**
  Se avsnitt 4.6.1 i kursboken

  RIP är ett applikation-protokoll för att skicka **regelbundna** routing-uppdateringar till routerns grannroutrar oavsett hur många och därför **använder UDP** för att transportera meddelanden i IP-paket till **multicast**-adressen som mottagaradress.

  Dessutom är ett RIP-meddelande **aktuellt just nu**, så är det opraktiskt och meaningslöst med att använda TCP för att försöka rätta till eventuella fel eller förlust, det kommer att uppdateras ändå av ett senare meddelande.

2c) *(3p)*

- Beskriv med tekniska termer hur TCP implementerar stockningskontroll.
- Förklara hur denna kontroll hjälper att lösa problem med stockning på Internet.
- Beskriv de algoritmer som TCP tillämpar i de vanliga implementationerna.

Se avsnitt 3.7 i kursboken

Det är TCP-protokollet på varje sändare (varje TCP/IP-värd) som kontrollerar stockningen på end-to-end basis. Det är kollektivt ansvar för alla Internet-anslutna TCP/IP värdar, till skillnad från en nätverksbaserad stockningskontroll.

Genom att varje TCP-sändare håller en variabel kallas för ”Congestion Window” CongWin som anger hur mycket data (t.ex. i antal segment) som sändaren får skicka i väg på en gång utan att behöva vänta på ACK på varje segment.

Syftet med stockningskontroll är att förhindra TCP-sändaren from att överbelasta nätverket dvs. de mellan-liggande **routrarna** med paket som dem inte hinner med att vidarebefordra vilket leder till långa köer och evenuellt paketförlust.

”Slow Start” är det då sändar-TCP börjar försiktigt genom att sända bara ett segment först och sedan ökar sändingshastighet genom att fördubbla antalet segment i CongWin efter varje RTT dvs. exponentiell ökning (om det får ACK på alla tidigare sända segmenten) tills det når en tröskel. Vid början av sändningen sätts tröskelen till ett default värde.

”Congestion Avoidance” är det då sändar-TCP har nått tröskeln och börjar öka CongWin med ett segment i taget efter varje RTT dvs. linjär ökning (om det får ACK på alla tidigare sända segmenten) för att undvika stockningen.

Händer det timeout när sändar-TCP väntar på ett ACK återgår TCP i alla fall till ”Slow Start” med ett nytt tröskelvärde, men om ett trippel duplikat ACK tas emot för ett och samma segment, indikerar detta en kortvarig stockning. Detta innebär att ett tidigare segment bland de sända segmenten är förlorat. TCP övergår till ”Congestion Avoidance” efter ”Fast Recovery” dvs. sända om segmentet. Nya värdet på tröskeln anger storleken i antal segment på halva “Congestion Window” vid senaste händelse.

3. DNS 4p

En student använder en dator som är ansluten till Internet via Chalmers nätverk. Studenten vill testa om det går att ta reda på en viss DNS-information genom att skicka DNS-förfrågan direkt till någon av de kända Chalmers namnservrarna. Studenten gör två försök genom att köra kommandot **nslookup** två gånger. Resultaten visas nedan.

```
C:\>nslookup -type=mx hv.se ns1.chalmers.se
Server:  ns1.chalmers.se
Address:  129.16.2.40

*** ns1.chalmers.se can't find hv.se: Query refused

C:\>nslookup -type=mx hv.se res1.chalmers.se
Server:  res1.chalmers.se
Address:  129.16.1.53

Non-authoritative answer:
hv.se   MX preference = 0, mail exchanger = lmail02.server.hv.se
hv.se   MX preference = 10, mail exchanger = lmail01.server.hv.se

hv.se   nameserver = ns2.hv.se
hv.se   nameserver = ns1.hv.se

ns1.hv.se       internet address = 193.10.198.34
ns2.hv.se       internet address = 193.10.199.95
```

Viktigt: I dina svar på de nedanstående delfrågorna skall du använda **DNS-termer** såsom; RR (Resource Record), domän, rekursivt**,** iterativt, lokal eller auktoritativ namnserver, TLD-server, .. m.m.

3a) Vilken DNS-information har studenten frågat om? Ditt svar skall förklara utförligt kommandots syntax som studenten använder. *(1p)*

Studenten har frågat om namnen på email-servrarna för domänen **hv.se**. Studenten har angett RR-typ MX: Mail eXchanger i kommandot.

3b) Varför är resultaten som visas, helt olika trots att studenten kör kommandot nästan på samma sätt? Vad är den DNS-tekniska orsaken till skillnaden?

Observera att:
*”Det räcker **inte** med att svara att skillnaden ligger i att **ns1** och **res1** är olika namn”.*

I ditt svar skall du också:

- Förklara innebörden i resultatet av att köra det **första** kommandot genom att klargöra för **varför** det står ”*ns1.chalmers.se can't find hv.se: Query refused*”.

- Beskriva med egna ord (***inte kopia av vad som visas***) de olika delarna i resultatet av att köra det **andra** kommandot samt klargör för **varför** det står ”*Non-authoritative answer:*” i detta fall.

(3p)

Resultaten är helt olika pga att i första kommandot skickas DNS-förfrågan till Chalmers auktoritativa namnservern **ns1.chalmers.se** som har ansvar om Chalmers-domän och inte om andra domäner, med andra ord denna server erbjuder inte rekursivt svar för klienter utan svarar på förfrågor om RR som finns i sin databas. Därför svarar denna server inte på förfrågan utan ”Query refused”.

I andra kommandot anges annan nanmnserver **res1.chalmers.e** som är cache-only server och erbjuder rekursivt svar för Chalmers-anslutna datorer och deras DNS-klienter. Resultatet består av:

- namnet på denna server och dess IP-adress. Eftersom denna server inte har hand om domänen **hv.se** utan att den är cache-server på Chalmers och söker DNS-informationen inom DNS-hierarkin iterativt för att leverera rekursivt svar för Chalmers-klienter från sin cache, indikerar den att svaret är icke-auktoritativt.

- själva DNS-svaret i form av två st. MX-RR typ-MX för namnen på email-servrarna på **hv.se**.

- två st. RR typ-NS för namnen på två auktoritativa namnservrar för domänen **hv.se.**

- extra information i form av två st. RR typ-A för IP-adresser på namnservrarna.

4. Ethernet & Trådlöst LAN 10p

4a) Ponera att en användare vid en värddator **A** startar webbläsaren för att hämta en webbsida från en extern webbserver **X** (med redan-känd IP-adress). Värddatorn **A** tillsammans med två andra värddatorer **B** och **C** har anslutning till Internet via en Ethernet-switch och en access-router **R**. Alla enheter är direkt-anslutna till var sin switch-port. Anta att ARP-tabellen hos värddatorn **A** är tom vid initiering av kommunikationen. Anta också att switch-tabellen är tom i början. *(5p)*

Tips: för att lättare svara på de följande uppgifterna, använd beteckningen med enhetens adresser, t.ex. **A**-IP, **A**-MAC, osv.

- **Redovisa** för hur och varför värddatorn startar med att använda ARP (Address Resolution Protocol) innan den kan sända paketen till servern.

- **Beskriv** i detalj de steg som värddatorn skall utföra med hjälp av protokollen (ARP, MAC, IP) för att kunna börja hämtningen.

- **Förklara** tydligt, steg för steg, hur Ethernet-switchen hanterar vidarebefordringen av Ethernet-ramarna mellan enheterna i detta fall. Beskriv också den tabell som används och hur den skapas av switchen.

Se avsnitt 5.4.3 i kursboken
Förklaring:

Switchen är en flerport brygga som kontrollerar Ethernet-ramarnas MAC-adresser innan de skickas vidare. Switchen skapar och uppdaterar sin MAC-adress-tabell (dynamiskt) med självlärning. Vid varje inkommande ram på en switchport läser switchen av **sändarens MAC-adress** i ramens header för att spara **den** i MAC-adress-tabellen för denna port. Switchen använder denna tabell för att avgöra till vilken port skall en ram skickas vidare om mottagares MAC-adress finns (är lärt finnas) i portens MAC-adress-tabell. Switchen skickar vidare en ram till den port där **mottagarens MAC-adress** finns med i MAC-adress-tabellen

Om en ram kommer in till switchen via en port och skall till en mottagare med MAC-adress som **inte** finns i adress-tabellen **vidarebeforas kopia av ramen** till alla andra portar utom den port som ramen kommit ifrån.

- Värddatorn **A** börjar med att genomföra AND-operation mellan serverns IP-adress och subnätmasken och konstaterar att den tillhör inte samma subnät .

- Värddatorn **A** är konfigurerad med IP-adress för access-routern **R** som default gateway för att skicka paket utanför sitt eget subnät. IP-paket skall kapslas in i Ethernet-ramar inför överföringen inom det lokal nätverket . Då behöver värddatorn **A** veta **R**-MAC adress och med hjälp av **ARP** skickas en broadcast-förfråga så att den som har **R**-IP adress skall svara med sin **R**-MAC adress.

- När ramen innehållande ARP-förfrågan kommer till switchen via porten **A** där värddatorn **A** är ansluten, sparar switchen sändarens MAC-adress dvs **A**-**MAC** i sin tabell mappat till port **A** och eftersom mottagar-adressen är broadcast (FF-FF-FF-FF-FF-FF) kommer switchen att vidarebefordra kopia av ramen till alla andra porter (port **B**, port **C** och port **R**) utom port **A**.

Kopior av ramen når **B** och **C** som läser av IP-adressen i **ARP**-meddelandet och konstaterar att det inte är sin egen och inget görs. Samtidigt får **R** en kopia av ramen via sin switchport och läser av IP-adressen i ARP-meddelandet och konstaterar att det är sin egen. Då skickar **R** sin MAC-adress i ett ARP-svar inkapslat i en unicast-ram på det lokala nätverket, adresserat till **A-MAC**.

När ramen innehållande ARP-svar kommer till switchen via porten **R** där access-routern **R** är ansluten, sparar switchen sändarens MAC-adress dvs **R-MAC** i sin tabell mappat till port **R**. Mottagar-adressen **A-MAC** finns ju redan i switchens tabell och därmed vidarebefordrar switchen ramen endast till port **A**.

Värddatorn **A** tar emot ARP-svaret och sparar **R-MAC** i ARP-tabellen mappat till **R-IP**. Nu kan värddatorn **A** skicka IP-paket (innehållande TCP-segment) som är adresserade till serverns IP-adress genom att kapsla dessa paket i Ethernet-ramar adresserade till **R-MAC**. Access-routern **R** använder sedan sin routingtabell för vidareleverans av dessa paket över Internet. Switchen kommer att vidarebefordra ramarna direkt mellan port **A** och port **R**.

4b) Beskriv **utförligt** hur protokollet CSMA/CA (Collision Avoidance) hanterar och undviker kollisioner vid kontrollen av accessen till radiokanalen. Förklara hur det kan genomföras och hur kollisioner kan undvikas när det är två eller fler associerade trådlösa enheter som försöker **samtidigt** försöker sända *normala* dataramar ”frames” till accesspunkten AP. Redovisa de steg som varje nätverkskort skall följa enligt standarden IEEE 802.11 i minst **tre** olika möjliga situationer (ex. om kanalen ledig eller inte, kollision, ..).

(3p)

Se avsnitt 6.3.2 i kursboken

FÖRKLARING:

I **WLAN** tillämpas **CSMA/CA** mekanismer kollektivt (Multiple Access) så att en trådlös station STA som vill sända en ram med *normal* storlek, skall först lyssna på radiokanalen (Carrier Sense) och se om det är ledig.

Är kanalen ledig, väntar STA en förbestämd tid **DIFS**, sända **hela ramen** om kanalen är fortfarande ledig och sedan väntar STA på **ACK** från mottagaren (som i detta fall är den associerade accesspunkten AP). Om ramen tagits emot felfitt skickas ACK av AP efter att ha tillämpat samma regler som ovan men med en kortare väntetid **SIFS**.

En positiv bekräftelse ”ACK” används av CSMA/CA för att informera sändaren om lyckad överföring över radiolänken. ACK är nödvändigt med anledningen av att radiolänken är mer utsatt för störningar, brus och interferens så att de sända ramarna kan lätt drabbas av bitfel och även **kollisioner** kan, trots dessa mekanismer, inträffas.

Är kanalen upptagen, backar STA och först **när kanalen blir ledig startar stationen nedräkningen** av en slumpmässigt vald tid (**back-off time)**. Med olika valda tider undviker man kollisioner (Collision Avoidance) när två eller fler associerade trådlösa enheter försöker **samtidigt** sända och väntar på att kanalen blir ledig. Utebliven ACK är en indikation för sändaren om att försöka sända om samma ram och därför **ökas väntetiden** (**back-off time)** av sändaren **inför** nästa sändningsförsök.

4c) Vid mycket vanliga infrastruktur-installationer som består av ett antal BSS (Basic Service Set); baserade på IEEE 802.11 WLAN, arbetar accesspunkten (AP) som en MAC-brygga. Beskriv **varför** och **hur** accesspunkten genomför denna funktion. *(2p)*

Se avsnitt 6.3 i kursboken
Förklaring:

Brygga (bridge):
En lager-2 enhet innebär att datatrafiken inom enheten hanteras med ett länk-protokoll, vanligen MAC. Detta medför att enheten tar emot ramar på inkommande interface, bearbetar de olika fälten i header (och eventuellt trailer) för att skicka (eller vidarebefordra) innehållet i datafältet (ofta IP-paket) i en ram på ett utgående interface.

En lager-2 enhet brukar kallas för brygga (bridge) och arbetar inom ett lokalt nätverk, för att jämföra med lager-3 enhet som är IP-router på Internet.

WLAN-AP:

AP har förutom **trådlöst interface,** ett **Ethernet-interface** anslutet till en switch. AP:ens uppgift vid en sådan installation, är att förmedla all trafik mellan stationerna oavsett MAC-typen (802.3 eller 802.11) och omvandlar ramarna från ena sidan till den andra.

AP:en utför sina arbetsuppgifter genom att hantera innehållet i headerfälten på ramarna enligt ett MAC-protokoll som utför funktioner på länklagret (lager-2). AP arbetar aktivt och deltar i kommunikationen på länk-lagret genom att vara mottagare/sändare för 802.11 MAC-ramarna på radiolänken.

Kommunikationen mellan de associerade stationerna (STAs) över radiolänken går via AP som en lager-2 mellanhandsenhet och som har MAC-adress (BSSID) för sitt trådlösa interfacet.

Om AP tar emot 802.11 MAC ram från en trådlös station STA som skall till annan i samma BSS kommer AP att bearbeta om MAC-headers olika fält och beräknar om trailer innan den skickar till mottagar-STA. AP behöver inte (förutom listan på de associerade STAs) ha MAC-adress-tabell liksom den som switchen skapar dynamiskt .

Vid infrastruktur-installationer agerar accesspunkten AP som en MAC-brygga mellan den trådlösa (WLAN 802.11) och den trådbundna (Ethernet 802.3) delarna av LANet. AP har förutom **trådlöst interface,** ett **Ethernet-interface** anslutet till en switch. Vid en sådan installation har AP för uppgift att förmedla all trafik mellan stationerna oavsett MAC-typen (802.3 eller 802.11) och omvandlar ramarna från ena sidan till den andra.

När AP får en Ethernet-ram med mottagare-MAC-adress som tillhör en av de associerade trådlösa STAs inom sitt täckningsområde, extraherar accesspunkten datafältet, skapar en ny .11-ram som adresseras med användning av adresserna i Ethernet-ramen och AP sänder ramen över den trådlösa radiolänken.

Omvänt om AP får en .11 ram från en associerad STA och med mottagare-adress som **inte** tillhör annan STA, extraherar accesspunkten datafältet, skapar en ny .3 ram som adresseras med användning av adresserna i .11-ramen och sedan skickas ramen över Ethernet till switchen den är kopplad till.

4: Adresser och subnetting 7p

5a) Ett nätverk har tilldelats prefixet **33.22.11.0/25**. Nätverket skall bestå av tre subnät som sammankopplas med en enda intern router. Ett av subnäten skall ha utrymme för **minst dubbelt** så många IP-adresser som vart och ett av de andra lika stora två subnäten. Hela adress-utrymmet i prefixet skall användas optimalt (fullt ut) för dessa tre subnät. *(4p)*

i. Beräkna subnäten enligt ovan. Ange adress och subnätsmask för varje subnät i **decimal** form.
Det stora: 33.22.11.0/26 255.255.255.192
Det första mindre: 33.22.11.64/27 255.255.255.224
Det andra mindre: 33.22.11.96/27 255.255.255.224

ii. Hur många giltiga host-adresser har varje subnät utrymme för?
62, 30, 30

iii. Om du skulle konfigurera (eller rekommendera), vilken default gateway (standard-router) kommer värddatorerna att ha i varje subnät?
33.22.11.1
33.22.11.65
33.22.11.97

iv. Till vilket subnät tillhör följande adress **33.22.11.95**? Kan den användas som IP-adress för en värddator? Varför eller varför inte?
33.22.11.95 är det riktade broadcast-adressen för det första mindre subnätet 33.22.11.64/27 och därför kan den inte användas som unicast för en värddator.

5b)

i. Vad är skillnaden mellan privata och globala IPv4-adresser med avseende på routing inom Internet? *(1p)*
De privata adresserna kan endast användas och återanvändas i privata nätverk. Paket med privata adresser (sändare /mottagare) får absolut inte routas till det globala Internet. Routrarna ser till att blockera vidarebefordring av sådana paket till Internet eller översätta adresserna till globala adresser med användning av NAT (se nästa delfrågan).

ii. De flesta Internet-anslutna hemnätverken använder privata adresser. Hur fungerar det med att fler enheter får access till Internet? *(2p)*

Hemnätverkets enheter tilldelas IP-adresser från ett privat **CIDR** adressblock (t.ex. 192.168.0.0/24). Hemroutern reserverar den första tillgängliga adressen för eget interface mot det lokala nätverket och därmed blir detta en intern ”default gateway”. Hemdatorerna kommunicerar direkt med detta interface för att skicka och ta emot IP-paket till och från Internet.
Hemroutern har vanligtvis tilldelats en global adress på det andra interfacet som är anslutet till ISP mot Internet.
Hemroutern använder NAT-funktionen för att ersätta den privata sändaradressen i varje utgående paket med sin globala adress samt ersätta sändarens portnummer med ett annat portnummer. Denna ersättning upprepas för alla paket som kommer från en och samma sändaradress med samma portnummer. NAT-funkionen sparar denna information (sändaradress och sändarportnummer + NAT-portnummer) och skapar en tabell för dessa ersättningar för att användas också i motsats riktning när inkommande paket adresserat till hemroutern (som egentligen skall till datorerna på hemnätverket) omadresseras och vidarebefordras till det lokala nätet. Med fler portnummer kan NAT översätta paket från fler enheter samtidigt.

6. Traceroute 5p

En student kör programmet ”**tracert**” på en värddator ansluten till Internet genom nätverket Nomad. Studenten vill spåra vägen till webbservern för ”Norges teknisk-naturvitenskapelige universitet”. Undersök noggrant resultatet som visas nedan och sedan svara på delfrågorna.

C:\>tracert www.ntnu.no

Tracing route to semper26.itea.ntnu.no [129.241.56.116] over a maximum of 30 hops:

1	3 ms	1 ms	1 ms	nomad-radio3-joh.nomad.chalmers.se [129.16.232.23]
2	34 ms	40 ms	2 ms	wlan-nomad-gw.chalmers.se [129.16.6.113]
3	3 ms	2 ms	1 ms	core2-wlan-gw.chalmers.se [129.16.2.154]
4	2 ms	2 ms	1 ms	optosunet-lr2-core2-gw.chalmers.se [129.16.2.201]
5	3 ms	4 ms	2 ms	cth-br1.sunet.se [193.11.0.13]
6	10 ms	10 ms	9 ms	m1fre-xe-7-2-1.sunet.se [130.242.85.97]
7	11 ms	10 ms	10 ms	se-fre.nordu.net [109.105.102.9]
8	10 ms	9 ms	9 ms	se-tug.nordu.net [109.105.97.2]
9	16 ms	16 ms	16 ms	oslo-gw1.uninett.no [109.105.102.22]
10	24 ms	24 ms	24 ms	trd-gw.uninett.no [128.39.255.46]
11	24 ms	24 ms	25 ms	ntnu-gw.nettel.ntnu.no [158.38.0.222]
12	26 ms	24 ms	24 ms	dc-gsw2.nettel.ntnu.no [129.241.1.19]
13	24 ms	24 ms	23 ms	semper26.itea.ntnu.no [129.241.56.116]

6a) Beskriv **tydligt** hur programmet fungerar när man kör det på en Internet-ansluten värddator. I ditt svar skall framgå vilka TCP/IP-protokoll och meddelande som används i samband med att köra programmet, från start till slut. *(2p)*

Se avsnitt 4.4.3 i kursboken samt labbarna

Tracert skickar IP-paket som innehåller ICMP-echo request meddelande upprepade gånger och samtliga är adresserade till måldatorn.

I första omgång sätts TTL-värdet i IP-paket till 1 och sedan ökas det med 1 vid nästa omgång osv.

Varje omgång upprepas tre gånger med samma TTL-värde. När dessa paket skall routas på Internet, passeras ett antal routrar på vägen till måldatorn. Varje router minskar TTLvärdet i paketet med 1 innan den vidarebefordrar det till nästa hopp. Ett paket med TTL = 0 kastas bort av routern och sändaren informeras av denna router genom ett skicka ICMP-meddelandet ”TTL exceeded”. Värddator (som kör tracert) använder informationen i dessa ICMP-meddelanden för att sammanställa en lista på de routrarna på vägen samt ett mättvärde för RTT till varje router tre gånger. Sista omgång når IP-paketen måldatorn som svarar med ICMP- echo reply meddelande.

6b) Förklara **hur** varje del av informationen, som visas **vid varje hopp**, har hittats av programmet. Välj hopp 7 som ett exempel för ditt svar. *(1p)*

Vid varje hopp visas:
- hopp-nummer som motsvarar värdet på TTL i de skickade IP-paketen,
- 3 uppmätta RTT-tider för varje omgång (hopp).
- måldatorns eller routerns DNS-hostnamnet ”CNAME” vilket DNS-klienten på värddatorn (som kör tracert) tar reda på med DNS-fråga om typ-PTR,

- måldatorns eller routerns IP-adress vilken hittas som sändaradress i paket innehållande retur ICMP-meddelande, och

6c) Enligt resultatet som visas är det uppenbart att det angivna namnet ***www.ntnu.no*** för måldatorn skiljer sig från ***semper26.itea.ntnu.no*** vid slutet av tracet. Förklara först hur du kan bekräfta att spårningen har nått måldatorn. Förklara sedan varför måldatorn har två olika namn? *(1p)*

JA, paketen nått måldatorn vid slutet därför att sista omgången visar IP-adressen 129.241.56.116 vilken är detsamma som värddatorn har tagit reda på från början:
" Tracing route to semper26.itea.ntnu.no [129.241.56.116]" .
www.ntnu.no är aliasnamn till **semper26.itea.ntnu.no** som är CNAME.

6d) Hur många **och** vilka routrar som tillhör den norska **TLD**-domänen, är det på vägen till måldatorn enligt detta trace? *(1p)*
4 routrar

oslo-gw1.uninett.no [109.105.102.22]
trd-gw.uninett.no [128.39.255.46]
ntnu-gw.nettel.ntnu.no [158.38.0.222]
dc-gsw2.nettel.ntnu.no [129.241.1.19]

****

Lycka Till!