Tentamen Datakommunikation, DVA218

Datum: 2022-05-31
Hjälpmedel: Penna, papper, radergummi.
Maxpoäng 30 poäng. Gränsen för godkänt kommer att ligga vid 15 poäng.
Ansvarig lärare: Mats Björkman, 021-10 70 37. Skulle det inte gå att nå mig, gör egna antaganden och notera det i svaret.

Lycka till!

Uppgift 1 (3 p) – Tillämpningar: DNS
Domain Name System (DNS) är en namnuppslagningstjänst på Internet, där ett antal namnservrar används för att översätta namn till adresser, närmare bestämt för att översätta domännamn till IP-adresser.

a) Varför vill man ha en namnuppslagningstjänst som DNS? Vad vore alternativet? (1 p)

b) Det finns över en miljard datorer på Internet. Beskriv hur DNS är designat för att inte alla namnservrar skall behöva känna till adressen till alla datorer på Internet. (1 p)

c) DNS håller också reda på så kallade MX-records, IP-adresser till den mailserver dit man skall skicka e-mail om mottagaren finns i en viss domän. Varför vill man skilja denna uppslagning från den vanliga adressuppslagningen? (1 p)

Uppgift 2 (5 p) – Transportskiktet: Fönster
Transportskiktet sköter dataleveransen från sändare till mottagare.

a) Ett transportprotokoll kan t.ex. använda sig av "sliding window" eller "stop and wait". Förklara båda begreppen och beskriv vilka skillnader/fördelar/nackdelar som finns. (2 p)

b) När man använder sliding window är det viktigt att man använder sekvensnummer på paketen. Varför? (1 p)

c) Varje protokoll som använder sekvensnummer har fält i protokollheadern för sekvensnummer. Antalet bitar i detta fält gör att det blir en maxstorlek på talet som används för att ange sekvensnummer. Denna storlek begränsar i sin tur hur stort fönstret i sliding window maximalt kan vara. Varför begränsar maxstorleken på sekvensnumret maxstorleken på fönstret, och hur begränsas fönsterstorleken? (1 p)

d) TCP har problem med att den ursprungliga maximala fönsterstorleken på 64 kB inte räcker till i dagens nätverk. Förklara vad i dagens nätverk som gör att en fönsterstorlek på 64 kB inte är tillräcklig. Hur kan TCP komma runt problemet? (1 p)

Uppgift 3 (3 p) – Transportskiktet: Interaktiv media
Det är vanligt att koppla upp interaktiva röst- och videosamtal. System som till exempel Zoom och Skype använder UDP över IP för kommunikationen mellan sändare och mottagare.

a) Varför använder Zoom (och många andra system för interaktiv media över Internet) UDP istället för TCP som transportprotokoll? (1 p)

b) Vilka av TCP:s tillförlitlighetsmekanismer vore trots allt bra för ett protokoll för interaktiv media som Zoom att använda? (1 p)

c) Att IP är förbindelselöst ställer till problem för Zoom och andra protokoll med interaktiva media när det blir överlast (stockning, congestion) i nätverket. Varför? Kan man göra något åt det? (1 p)

Uppgift 4 (5 p) – Transportskiktet: TCP
TCP är Internets vanligaste transportprotokoll. Över 90% av datatrafiken över Internet använder TCP som transportprotokoll.

a) TCP försöker skatta Round Trip Time, dvs. tiden från det att ett segment sänds, till dess att ett ACK på detta segment kommer åter till sändaren. Detta görs för att kunna sätta timeouttiden för omsändningar till ett bra värde. Vad händer om timeouttiden är för kort? Varför? Vad händer om timeouttiden är för lång? Varför? (2 p)

b) Alla implementationer av TCP måste innehålla mekanismer för att minska risken för stockning. Vanligast (exv. i TCP Reno) är att man för stockningskontroll implementerar ett extra fönster på sändarsidan, congestion window. Detta fönster minskas när sändaren tar emot duplicerade ACK:ar. Varför? Vad har hänt om sändaren tar emot duplicerade ACK:ar? (1 p)

c) Fast retransmit används i TCP Reno för att slippa vänta på timeout. Beskriv hur Fast retransmit fungerar och varför det sparar tid. (1 p)

d) Vad gör PAWS (Protection Against Wrapped-Around Sequence numbers)? Varför måste man skydda sig mot wrapped-around sequence numbers? (1 p)

Uppgift 5 (5 p) – Prestanda
Antag att sändaren S och mottagaren M är direkt sammankopplade med en länk, exv. en Ethernet-kabel.

a) Två viktiga faktorer som påverkar tiden det tar att skicka en ram av storlek R (bitar) mellan S och M är datatakten (signaleringshastigheten) D (bitar per sekund), och utbredningstiden U (sekunder) för signalen mellan S och M. Beskriv hur överföringstiden Ö från S till M beror av ramstorleken R, datatakten D och utbredningstiden U. (Bortse från övriga faktorer, exv. tiden som går åt inne i de båda datorsystemen.) (2 p)

b) Hur påverkas överföringstiden Ö om ramstorleken R fördubblas? (1 p)

c) Hur påverkas överföringstiden Ö om istället datatakten D fördubblas? (1 p)

d) Utgå från situationen i a). Nu delar vi kabeln på mitten och kopplar in en switch där. Switchen har samma datatakt D på båda länkarna och arbetar enligt store-and forward, d.v.s. den tar emot hela ramen innan den skickar den vidare. Hur förändras överföringstiden Ö relativt situationen i a) ? (1 p)

Uppgift 6 (5 p) – Datalänkskiktet
Datalänkskiktet ser till att data kommer från en nod till nästa.
a) Carrier Sense, Multiple Access (CSMA) är en klass av datalänkprotokoll som ofta används i lokala nät. Beskriv hur ett CSMA-protokoll fungerar. (1 p)

b) Vissa CSMA-protokoll har s.k. Collision Detect (CD). På vilket sätt förbättrar detta utnyttjandet av länken? (1 p)

c) Ethernet (IEEE 802.3) är ett väldigt vanligt CSMA/CD-protokoll. I Ethernet finns en backoffmekanism som anpassar sig till trafiken på länken. Beskriv Ethernets backoffmekanism och förklara varför man vill anpassa sig till länkens trafik. (2 p)

d) På en trådlös länk är det inte säkert att alla stationer kan höra varandra. Detta ger upphov till (minst) två problem: Vilka? Hur kan de två problemen lösas? (1 p)

Uppgift 7 (4 p) – Säkerhet
a) Symmetriska krypton för nätsäkerhet bygger på en delad hemlighet (en delad nyckel). Beskriv två olika sätt som Alice och Bob kan använda för att kunna dela en nyckel om de inte har en delad nyckel från början. (1 p)

b) Asymmetriska krypton för nätsäkerhet bygger på att en nyckel är hemlig medan den andra nyckeln kan vara publik. Beskriv hur Alice kan säkerställa att det verkligen är Bobs publika nyckel hon använder och ingen annans. (1 p)

c) För att åstadkomma säkerhet i Internet-stacken finns det dels protokoll som arbetar på transportnivå (exv. Transport Layer Security, TLS), del sådana som arbeta på nätverksnivå (exv. IP sec). Beskriv hur det skiljer sig åt att hantera säkerhet i respektive skikt, och vilka som är för respektive nackdelarna med de olika alternativen. (2 p)