Lösningsförslag till Tentamen i kurs DVA218

Datakommunikation

2015 03 26

Mälardalens Högskola

Examinator: Elisabeth Uhlemann, IDT, 021-101556 eller 0708-447307.

Tillåtet material:
- Penna, suddgummi och papper

Examination och betygsättning:
- Tentamen består av 8 frågor. Antalen poäng framgår vid varje fråga. Maxpoängen är 40 poäng. För betyg 3 (godkänt) kommer det att krävas ca 20 poäng.
- Motivera alla svar. Avsaknad av motivering kan innebära poängavdrag även om svaret i sig är korrekt.
- Förklara alla eventuella beräkningar tydligt. Om metod och motivering finns på plats så leder inte enkla räknefel automatiskt till poängavdrag.
- Om någon information saknas i en uppgift eller om Du tycker att något är oklart, skriv ner och förklara vilka antaganden Du har gjort för att lösa uppgiften.
- Skriv tydligt. Om jag inte kan läsa eller förstå Ditt svar så är det felaktigt.
- Det går bra att svara både på engelska och på svenska. Om svenska används så går det ändå bra att använda vissa vedertagna engelska begrepp.
- Besvara varje fråga på separat papper. Skriv endast på framsidan av varje papper. Märk varje papper med Din anonymitetskod.

Lycka till!

Uppgift 1. Kortsvarsfrågor (5 poäng)

Kombinera varje begrepp markerat 1-5 med lämplig definition/fras markerade A-K (endast en bokstav per siffra). Rätt delsvar belönas med 1 poäng, fel delsvar ger –1 poäng och obesvarat ger 0 poäng. Den sammanlagda summan på denna uppgift kan dock inte bli mindre än 0 poäng.

1) Token ring = I
2) Bitstuffing ≈ C fast det som beskrivs i C är character stuffing – pga det fick alla alltid rätt på 1.2.
3) Hammingkod = K
4) Network Address Translation (NAT) = E
5) Preemble = G

A) Översättning från IP- till MAC-adress
B) Exponential backoff-mekanism
C) Specialtecknet ESC stoppas in om ett FLAG-tecken uppträder i dataströmmen
D) Ett kollisionsfritt MAC-protokoll
E) En viktig mekanism som minskat behovet av IPv6
F) Krypteringsalgoritm där fasinformation används
G) Behövs för att mottagaren ska komma i takt med sändaren
H) Upptäcker udda antal bitfel
I) En logisk ring skapas över en buss
J) Används i IEEE 802.3 ("Ethernet")
K) Ett exempel på en felrättande kod

Uppgift 2. Tillämpningar (5 poäng)

A) Förklara kort vad som skiljer en klient från en server i en tillämpning som baseras på Klient/Server. (1p)
En klient ber serven om någon typ av service. En server gör inget själv (initierar inget) utan svarar bara på begäran från olika klienter. En server kan serva flera klienter samtidigt.

B) Domain Name System (DNS) är en namnuppslagningstjänst för att översätta namn till adresser, mer specifikt för att översätta domännamn till IP-adresser. Det finns nästan 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. (2 p)
Rent principiellt är DNS en distribuerad databas som är uppdelad i domäner. Varje domän har minst två DNS-servrar som är ansvariga för de poster som är relaterade till domänen. Normalt kontaktas den lokala DNS-servern först, även om förfrågan gäller en helt annan domän. Om denna känner till svaret på förfrågan lämnas detta direkt. I annat fall kan den antingen hänvisa vidare till en annan DNS-server, eller själv kontakta en annan DNS-server och vidarebefordra förfrågan. På så sätt behöver en ändpunkt bara känna till sin egen DNS-server.

C) Olika tillämpningar har olika krav på den underliggande kommunikationen. Traditionellt i Internet har det funnits två kommunikationstjänster att välja på: tillförlitlig byteström (TCP) respektive otillförlitlig paketförmedling (UDP). Strömmande media, exv. video, skulle egentligen vilja ha ett mellanting mellan TCP och UDP. Beskriv vilka av TCP:s egenskaper som är *önskade* vid strömmad video, samt vilka av TCP:s egenskaper som är *oönskade* vid strömmad video. Varför? (2p)
Önskvärt: data kommer fram i rätt ordning
Oönskat: data skickas om – det gör att kraftigt försenade paket kan levereras och störa pågående uppspelning, samt att de stjäl bandbredd från aktuella paket (bättre att kasta försenade paket)

Uppgift 3. Transportskiktet (5 poäng)

Transportskiktet sköter leveransen av data från sändande ändpunkt (process) till mottagande ändpunkt.

A) Ge en kortfattad översikt av de båda ARQ-metoderna Selective Repeat och Go-back-*N*. Följande saker måste tas upp i översikten: skillnader i funktion och prestanda, sekvensnummer, flödeskontroll, buffringskrav, ACK, NAK och timeout. (2p)
Selective Repeat (SR) och Go-back-*N* (GBN) är båda omsändningsmetoder, dvs. man förväntar sig ett ACK eller NACK på varje paket för att veta om något kommit bort eller blivit korrupt och behöver sändas om. Om ACK eller NACK skulle försvinna så kan omsändning ändå ske med hjälp av timeout. SR och GBN har bägge sändfönster som är större än 1, vilket gör att fler paket kan vara aktiva samtidigt (vilket paket som mottagits avgörs med hjälp av sekvensnummer), vilket ger högre överföringshastighet än exv. stop-and-wait, men de kräver en buffert av samma storlek som sändfönstret på sändarsidan. SR skickar bara om de paket som blivit fel, vilket innebär att inga extrapaket skickas om (högre effektiv överföringshastighet), men istället krävs en buffert även på mottagarsidan, så att paket kan levereras i rätt ordning till högre lager. GBN går tillbaka och börjar om med det paketet som blev fel (eller kom bort). Det innebär att paket som har kommit fram korrekt, kastas, vilket leder till onödig trafik, men ingen buffert krävs hos mottagaren.

B) Ett transportprotokoll kan t.ex. använda sig av “sliding window” eller ”stop and wait”. Förklara båda begreppen och beskriv eventuella skillnader/fördelar/nackdelar. (2 p)
Stop and wait (SW) sänder ett paket i taget, väntar på besked (ACK, NACK eller timeout) och sänder sedan om eller går vidare till nästa. Sändfönstret eller sliding window är då 1, vilket gör att en minimal buffert behövs på sändarsidan. SW är inte speciellt effektivt vad gäller överföringshastighet eftersom det stannar och väntar, men å andra sidan skickas inga onödiga paket om (som med GBN). SR och GBN har bägge sliding window, dvs. ett sändfönster som är större än 1, vilket gör att fler paket kan vara aktiva samtidigt. Då krävs en buffert krävs för att hålla koll på vilket paket som ska skickas om. Om det inte finns möjlighet att ha en buffert så får man alltså nöja sig med lägre överföringshastighet.

C) I vilken mån skiljer sig transportskiktets mekanismer för tillförlitlighet (exv. acknowledgements, omsändningar, checksummor) från motsvarande mekanismer på datalänknivå? Förklara varför. (1 p)
På datalänknivå sker omsändningarna över endast en länk (punkt-till-punkt), medan på transportskiktet kan det röra sig om ett eller flera hopp med routing emellan (end-to-end). Detta innebär att kraftigt försenade paket som tagit en annan väg i nätverket plötsligt kan dyka upp igen när omsändningar sker på transportskiktet. Detta kan inte ske på länknivå.

Uppgift 4. TCP (5 poäng)

TCP är Internets stora transportprotokoll och står för mer än 90 % av trafiken på Internet.

A) Stockning (congestion) är något man vill undvika i Internet. Beskriv hur stockning påverkar trafiken i ett nätverk och varför det är ett stort problem. (1p)
Om stockning uppstår så kastar TCP paket för att komma ikapp igen. Då kommer omsändningar så småningom att ske. Dessutom minskas överföringshastigheten (sändtakten) så att allt går långsammare.

B) Alla implementationer av TCP måste innehålla mekanismer för att minska risken för stockning. Beskriv hur stockningskontroll kan implementeras i TCP. (1p)
Överbelastning i nätverket, s.k. stockning, är svårt att exakt förutse eftersom många sessioner pågår samtidigt. TCP använder sig av ett stockningsförnster som en indikator på hur mycket data som kan vara utestående innan förluster sker pga. stockning. När en ny TCP-anslutning upprättas försöker man snabbt få en rimlig uppfattning av stockningsförstrets (cwnd) storlek för att inte ligga på för låg bandbredd, men samtidigt undvika stockning. Med tillståndet slow start är cwnd litet men ökar exponentielltupp till ett tröskelvärde. När cwnd når tröskelvärdets storlek går man över till tillståndet congestion avoidance. I detta tillstånd ökar cwnd långsammare. Alltså, man börjar med ett lågt värde på stockningsfönstret (slow start), för att vara säker på att man inte går ut för hårt, men man ökar det snabbt så länge allt går bra. Sedan när cwnd gått ett rimligt värde så ökas det långsammare för att inte påfresta systemet för mycket. Fönstret minskas på olika sätt beroende på vad som inträffar (timeout eller duplicerade ACKar).

C) TCP:s stockningskontroll får ofta problem när trådlösa länkar används. Varför? (1p)
När trådlösa länkar används så kan förluster som inte beror på stockning ske – men de tolkas ändå som stockning och då sätts motåtgärder in, vilka kan få motsatt effekt för trådlösa länkar.

D) Vilka mekanismer finns för att minska problemen i c) ovan? (1p)
Fast recovery (stockningsfönstret halveras, men man ligger kvar i tillståndet congestion avoidance) och fast retranmsit (en direkt omsändning göra för att undvika en timeout längre fram) minskar problemen.

E) Transport Layer Security/Secure Socket Layer (TLS/SSL) kan användas exempelvis för att autentisera en webbserver. Hur kan man med hjälp av TLS/SSL vara säker på att webbservern verkligen är den som den påstår sig vara? (1p)
TLS/SSL använder certifikat och asymmetrisk kryptering för att autentisera servern så att webbserven och klienten kan förhandla fram en symmetrisk nyckel för sessionen.

Uppgift 5. Nätverksskiktet (5 poäng)

A) Vad innebär Flooding? (1p)
Att ett paket skickas vidare via alla möjliga vägar, dvs. läggs på alla portar förutom den varifrån paketet kom. Flooding är därför en routingalgoritm utan insamlad kunskap. Den belastar närverket oerhört, men kan snabbt hitta rätt väg, så länge nätverket inte kollapsar under belastningen.

B) Vad innebär Hot potato routing? (1p)
Att ett paket skickas vidare så snabbt som möjligt, dvs. läggs på den porten med kortast kö. Flooding är därför en routingalgoritm utan insamlad kunskap. Den belastar inte närverket nämnvärt, men det kan i princip ta oändligt lång tid innan paketet kommer fram.

C) Dijkstras algoritm kallas ibland kortaste-vägenalgoritmen. ”Kortaste” betyder helt enkelt att man har ett mått som man vill minimera vid routingen. Nämn två exempel på mått man kan vilja minimera vid routingen. (1p)

Antal hopp, avstånd mellan sändare och mottagare, fördröjning, …

D) Routing kan ske med eller utan insamlad kunskap. Ge ett exempel på varje, samt beskriv för- och nackdelar med respektive sätt. (2p)

Hot potato routing innebär att ett paket skickas vidare så snabbt som möjligt, dvs. läggs på den porten med kortast kö. Hot potato routing är ett exempel på en routingalgoritm utan insamlad kunskap. Den belastar inte närverket nämnvärt, men det kan i princip ta oändligt lång tid innan paketet kommer fram.

Distance vector skapar routingtabeller genom att berätta allt man vet om hela nätverket för sina grannar (insamlad kunskap). Detta innebär att ett paket som använder routingtabellerna för att välja väg, kommer fram relativt snabbt och säkert. Dock belastar kommunikationen för att samla in kunskap till routingtabellerna nätverket.

Uppgift 6. IP (5 poäng)

Nätverksskiktet i Internet, IP, är förbindelselöst.

A) Jämför styrkor och svagheter med att ha ett förbindelselöst nätskikt kontra att istället ha ett förbindelseorienterat nätskikt. (1p)

Ett förbindelselöst nätskikt tillhandahåller en best-effort-tjänst, dvs. IP ger inga garantier för att datagram kommer fram, eller att de kommer fram i någon viss ordning eller inom någon viss tid. Detta är svagheter. Styrkan är att det krävs lite overhead för att administrera och det är därmed snabbare, eftersom man inte behöver vänta på upp- och nedkoppling eller omsändningar. Det är också svårare att särbehandla vissa paket och att beställa en viss typ av service.

B) Fragmentering kan behöva tillgripas om ett paket är för stort för att komma igenom en länk i nätverket. Beskriv hur fragmentering går till och vilka problem som kan uppstå vid fragmentering. (1p)

Om ett meddelande är för stort för att skickas i sin fullständiga form genom det mellanliggande nätverket måste det fragmenteras, dvs. man styckar upp meddelandet i flera delar, där varje del måste ha en dataidentifierare för att veta vilka delar som hör ihop. Dessutom måste man hålla reda på vilken offset i datamängden som varje meddelande innehåller för att kunna sätta ihop delarna korrekt igen. Om alla fragment inte tas emot korrekt hos mottagaren måste detta hanteras, antingen genom omsändning av saknade fragment, eller genom att genom att kasta fragment som aldrig kommer att kunna återskapas.

C) Beskriv tre viktiga mekanismer/protokoll som har gjort att utnyttjandet av IPv4-adresser har förbättrats (och därmed minskat behovet av införande av IPv6). (2 p)

NAT, CIDR och DHCP (se beskrivning i boken eller på föreläsningsslidsen).

D) På IP-nivå kan avsändaradresser förfalskas, s.k. IP spoofing. Varför är detta ett problem? Kan man göra något åt problemet? (1p)

En spoofingattack är en metod för dataintrång, där angriparen maskerar sig genom att lura ett datasystem eller en användare att tro att anropet kommer från ett annat datasystem än det faktiskt gör. IP spoofing innebär att man använder annan avsändar-IP-adress. För att förhindra IP-spoofing kan varje paket filtreras, exv. med hjälp av en brandvägg, så att IP-adresser som finns internt i nätverket, men som kommer utifrån, blockeras.

Uppgift 7. Datalänk skiktet (5 poäng)

Förklara följande protokoll så kortfattat som möjligt, men ändå så att skillnaderna (inklusive skillnader i prestanda) mellan dem framgår klart och tydligt: Aloha, Slotted aloha, CSMA, CSMA/CD, CSMA/CA. (5p)

Med Aloha skickar varje nod så snart den har något att skicka. Detta ger låg fördröjning, men resulterar i krockar.

Med Slotted Aloha får ingen skicka direkt, utan alla måste vänta tills en slot börjar. Detta ger en minimal fördröjning på max en slotlängd, men minskar antalet krockar något, eftersom delar av paket inte längre krockar (början av ett paket kan inte längre krocka med slutet av ett annat paket).

Med CSMA lyssnar man först om kanalen är ledig, innan man sänder (carrier sense). Om den är upptagen så väntar man tills den blir ledig. Detta gör att det blir en slumpmässigt lång fördröjning som varar så länge kanalen är upptagen, men antalet krockar minskar ytterligare eftersom de endast uppstår om två eller flera noder börjar sända samtidigt.

Med CSMA/CD noterar de sändande noderna även om det har blivit en kollision (collision detection) och meddelar andra noder detta genom att skicka en störsignal. Ett nytt försök görs sedan lite senare. Det resulterar i samma slumpmässigt långa fördröjning som varar så länge kanalen är upptagen, och samma antal krockar, men tiden till dess att omsändning ske kan minskas, eftersom man inte måste vänta på timeout.

CSMA/CA används i trådlösa nätverk för att undvika kollision (collision avoidance), eftersom CSMA/CD inte kan användas (det kräver att man kan sända och lyssna samtidigt, vilket inte går i trådlösa lösningar). Kollision undviks genom att skicka ett mycket kort Request to Send (RTS) paket, och först om mottagaren svarar med Clear to Send (CTS) så skickar man det längre datapaketet. Om andra noder hör ett CTS så väntar de tills kanalen blir ledig igen. Detta resulterar i samma slumpmässigt långa fördröjning som i CSMA, men med något färre antal krockar. Dock lägre effektivitet än med CSMA/CD eftersom extrapaketen RTS och CTS tar tid att skicka.

Uppgift 8. Fysiska skiktet (5 poäng)

A) Ge ett exempel på en felupptäckande kod. Förklara kort hur den fungerar, när den bör användas, när den inte bör användas och vad som krävs för att den ska kunna användas. (2p)

En paritetsbit kan användas för att upptäcka fel. Om jämn paritet används kommer paritetsbiten att vara satt till 1 om det finns ett udda antal ettor i datafältet, och 0 om det finns ett jämt antal ettor i datafältet. En felupptäckande kod bör användas när man kan åtgärda problemet, dvs. antingen kasta den felaktiga informationen, eller begära omsändning av informationen. Om ingen åtgärd görs, är det onödigt med en extra paritetsbit. Om det är ett långt datafält så är en paritetsbit inte så effektiv eftersom det finns stor chans att det har blivit mer än ett fel, och då kan paritetsbiten missa detta. Bättre då att använda en CRC-kod.

B) Ge ett exempel på en felrättande kod. Förklara kort hur den fungerar, när den bör användas, när den inte bör användas och vad som krävs för att den ska kunna användas. (2p)

En Hammingkod är en felrättande kod. Den kan rätta ett fel genom att skapa flera paritetsbitar av olika delar av datagrammet, så att det går att avgöra exakt vilken bit som har blivit fel och ändra denna så den blir rätt. Den bör användas när sannolikheten för max ett bitfel är stor. Om det är mer sannolikt att flera bitar blir fel varje gång något går fel, så är Hammingkoden värdelös eftersom den skickar med flera extrabitar som inte kan användas eftersom den ändå bara kan rätta ett fel.

C) Finns det något tillfälle då man vill använda både en felupptäckande kod och en felrättande kod? Motivera Ditt svar. (1p)

Ja, om det exv. ofta blir ett bitfel men ibland fler, så kan Hammingkoden användas i de flesta fall, men när det blir fler fel så används en felupptäckande CRC-kod för att begära en omsändning.