Uppsamlingstentamen

DATATEKNIK B, DATORKOMMUNIKATION OCH NÄT (DT2017-0100)

och

DATATEKNIK B, TILLÄMPAD DATAVETENSKAP, DELKURS II: DATORKOMMUNIKATION OCH NÄT (DT2022-0220)

2013-08-23

Hjälpmedel: papper, penna (ej med röd skrift) och miniräknare

Tid: 4 timmar

Maximal poängsumma: 50

Betygsgränser för SDT2 och TDVB
För betyget **G** krävs 25 poäng.
För betyget **VG** krävs 37 poäng.

Betygsgränser för D2
För betyget **3** krävs 25 poäng.
För betyget **4** krävs 35 poäng.
För betyget **5** krävs 43 poäng.

---

1. Datornät och Internet

   a. Vilken organisation skapar standarder för Internet och vad kallas dess dokument över sådana standarder? Det går bra att svara med förkortningar. **1p**

   b. Vad är Internet Service Provider (ISP)?

      Förklara ISP-hierarkin.

      Vad är Internet backbone? **3p**

c. Låt *L* vara paketstorleken (bitar), *a* vara medelhastigheten för paket som anländer till en kö med enheten (paket/s) och *R* vara bithastigheten (bps).

Hur stor bli då trafikintensiteten?

Vilken gyllene regel gäller för denna? **1p**

d. Vad bidrar till total nodfördröjning (router och länk)? (Vilka är orsakerna?) **2p**

e. I vilken situation kan en router orsaka paketförlust (packet loss) i Internet? **0,5p**

---

2. Applikationsskiktet

a. Vad definierar Hyper-Text Transfer Protocol (HTTP)?

När tappar webbklienten och webbservern kontroll över meddelanden som de skickar?

Varför kan man säga att HTTP är ett tillståndslöst protokoll (stateless protocol)?

Ger versionen HTTP/1.0 respektive versionen HTTP/1.1 flyktiga (nonpersistent) eller varaktiga (persistent) uppkopplingar? **3p**

b. Vilken är huvuduppgiften för Domain Name System (DNS)?

DNS består av två huvuddelar. Vilka är dessa?

Beskriv hur Hyper-Text Transfer Protocol (HTTP) arbetar för att ta sig till en Uniform Resource Locator (URL).

Vad innebär host aliasing, kanoniskt värdnamn (canonical hostname) och mail server aliasing? **4p**

---

3. Transportskiktet

   a. Vad är innebörden av att transportprotokollen ger logisk förbindelse? **1p**

   b. Till en värd anländer ett UDP-datagram (User Datagram Protocol). Tänk dig att det endast består av följande fyra data och en checksumma (längst ned):

      0101010101010101
      1111000011110000
      1100110011001100
      1111111011101110
      1010111000000000 (checksumman)

      Visa om överföringen har givit bitfel eller ej.

      (I verkliga UDP-datagram ingår betydligt fler data. Alla beräkningar ska redovisas. Använd den metod som beskriv i bokens tredje upplaga, dvs. wrap around.) **3p**

   c. Vilken är den stora skillnaden mellan Go-Back-N (GBN) och den version av GBN som används av Transmission Control Protocol (TCP)?

      Vilket är syftet med flödeskontroll i TCP?

      Vilket fält i TCP-segmentet överför mottagningsfönstret till den andra parten?

      Är mottagningsfönstret nödvändigtvis konstant under en TCP-förbindelse?

      Vilket intervall har (generellt, inte för TCP) sekvensnummer som skrivs med *k* bitar? **3,5p**

---

4. Nätverksskiktet

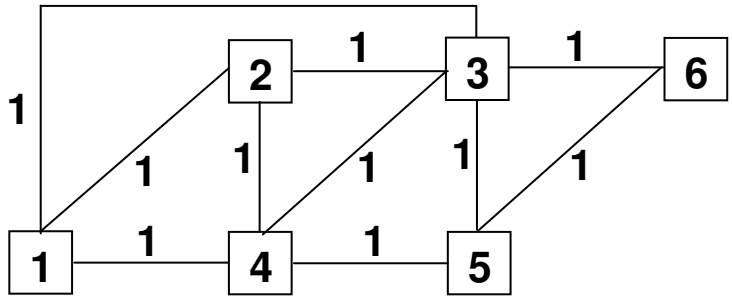
   a. Vilka är de tre komponenterna (huvuddelarna, bl.a. protokoll) i Internet-skiktet (nätverksskiktet) och vad gör dessa? **5,5p**

b. Gör Link state routing (LS) med Dijkstras algoritm för router 1 (nod 1).

Svara genom att rita nätet steg för steg.

Redovisa mängden av färdiga noder i varje steg och stoppvilkoret för att visa algoritmens funktion.

Kostnaden antas vara lika åt bägge hållen (symmetrisk) för varje väg (länk). **3p**



---

5. Länkskiktet, lokala nät, trådlösa och mobila nät

a. Förklara (kort) grunden för kanaluppdelning TDM respektive FDM. **2p**

b. Beskriv ett Bluetooth-pikonät (enligt IEEE 802.15) med enhetstyper och det som är typiskt för respektive enhetstyp. (En tidig version av Bluetooth beskrivs i IEEE 802.15.1.) **3p**

---

6. Multimedia

a. Vad avses med "interactive" i real-time interactive audio and video? **1p**

b. Vad innebär best-effort service för Internet Protocol (IP)?

För Internet-telefoni och real-time interactive voice/video talas om ”packet jitter”. Vad avses med detta? **2p**

c. Beskriv återskapandet av paket med piggybacking (en FEC-mekanism, Forward Error Correction) av redundant information av låg kvalitet (låg samplingsfrekvens, lågt antal bitar). Metoden kan användas på paketströmmar. **2p**

d. Vad avses med Rspec och Tspec?

Varför behöver dessa bestämmas i Intserv-arkitekturen? **2,5p**

---

7. Datasäkerhet och management

a. Vad innebär en man-in-the-middle attack (bucket-brigade attack) då det gäller autenticitet? (Beskriv hur en attack går till.) **4p**

b. Var placeras vanligtvis en paketfiltrerande brandvägg?

Ge exempel på fyra vanligt förekommande filterparametrar. **3p**

Lösningar

1. Datornät och Internet
   a. IETF (Internet Engineering Task Force) tar fram RFC:er (Request for Comments).
   b. ISPs ger access till Internet. Egentligen är det fråga om en hierarki av ISPs som ger access till olika nivåer av Internet. Tier-1 ISPs är kopplade till varandra, ger access till/från tier-2 ISPs och ger internationell täckning. Det är tier-1 ISPs som kallas Internet backbone (ryggraden). Tier-2 ger typiskt regional eller nationell täckning. På den lägsta nivån återfinns tier-3 ISPs.
   c. Trafikintensiteten är La/R.
      Den gyllene regeln: Designa ditt system så att trafikintensiteten inte blir större än 1.
   d. Den totala nodfördröjningen hos en router och tillhörande länk är summan av tiden för att behandla (processa) ett paket i routern, väntetiden inne i routrens köer, sändningstiden och utbredningstiden till nästa router.
   e. Om kön i en inport är full, uppstår paketförlust för fler inkommande paket på samma port.

2. Applikationsskiktet
   a. HTTP definierar strukturen hos meddelanden som utbyts mellan server- och klientprogram. Vidare definierar det hur klienten (webbläsaren, bläddraren) begär webbsidor från servern (webbservern) och hur den senare svarar. När HTTP överlämnar meddelandet till transportskiktet, tappar HTTP kontrollen över hanteringen av meddelandet. (Transportprotokollet övertar hanteringen.) HTTP är tillståndslöst eftersom servrar inte hanterar information om klienters tillstånd. HTTP/1.0 ger alltid flyktiga uppkopplingar medan HTTP/1.1 har varaktiga uppkopplingar (default). Det senare kan ställas om till att ge flyktiga uppkopplingar.
   b. DNS översätter från värdnamn till IP-adresser. (1) DNS är en distribuerad (utspridd på flera datorer) databas i en hierarki av DNS-servrar och (2) ett applikationsprotokoll som tillåter att värdar och DNS-servrar kan kommunicera. Användaren skriver in ett värdnamn (t.ex. www.oru.se) i webbläsaren (HTTP-klienten) som med hjälp av DNS-klienten skickar en fråga till en bestämd DNS-server. (Det är vanligtvis en lokal DNS-server men den behöver nödvändigtvis inte vara lokal.) Den senare svarar genom att skicka tillbaka motsvarande IP-adress (t.ex. 130.243.97.140) till det aktuella värdnamnet. Om DNS-servern inte har det aktuella värdnamnet i sin databas, skickas frågan vidare till nästa DNS-server i hierarkin. Frågan skickas tills någon DNS-server kan ge svar. Detta svar skickas tillbaka till den frågande DNS-klienten. På så sätt får webbläsaren en IP-adress att skicka paket till. En DNS-server håller också redan på alias för värdnamn. Detta kallas host aliasing. Något av värdnamnen som går till samma värd är kanoniskt, dvs. det riktiga värdnamnet. DNS översätter också från e-postadresser till IP-adresser. Värddelen i en e-postadress kan vara ett alias för det verkliga värdnamnet. Sådana håller DNS också reda på. Detta kallas mail server aliasing.

3. Transportskiktet
   a. Ur applikationernas synvinklar verkar det som att värdarna (datorerna) som kör processserna är direkt hopkopplade. I verkligheten kan det finnas många routrar och länkar mellan dessa.
   b. Addering av data inklusive checksumman ger följande (enligt den korrekta metoden som beskrivs i boken tredje upplaga):

```
  0101010101010101
+ 1111000011110000
(1)0100011001000101

(wrap around)
  0100011001000101
+ 0000000000000001
  0100011001000110

  0100011001000110
+ 1100110011001100
(1)0001001100010010

(wrap around)
  0001001100010010
+ 0000000000000001
  0001001100010011

  0001001100010011
+ 1111111011101110
(1)0001001000000001

(wrap around)
  0001001000000001
+ 0000000000000001
  0001001000000010

  0001001000000010
+ 1010111000000000
  1100000000000010
```

   Eftersom adderingen ger ett tal som inte är lika med 1111111111111111 så har överföringen orsakat fel.

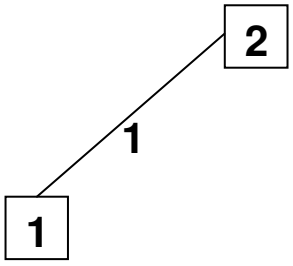
   c. Under sändning av en serie av TCP-segment blir det fel i överföringen av ett mellanliggande segment. Då sänder TCP om endast det felaktiga segmentet. Med äkta GBN skulle alla segment från och med det felaktiga sändas på nytt. Syftet med flödeskontroll i TCP är att mottagaren ska kunna ta emot alla segment som sänds utan att behöva kasta bort segment som kommer fram, dvs. skydda mot överfull mottagarbuffert. (Indirekt besparar flödeskontrollen på så sätt onödiga omsändningar, dvs. reducerar trafiken på nätet.) Det är fältet receive window i TCP-segmentet som

överför mottagningsfönstret. Storleken på mottagningsfönstret bestäms av fritt utrymme i mottagningsbufferten som varierar med tiden. Om sekvensnummer skrivs (generellt) med k bitar, ger det intervallet 0 till $2^k - 1$, t.ex. $k = 3$ ger intervallet 0 till 7.

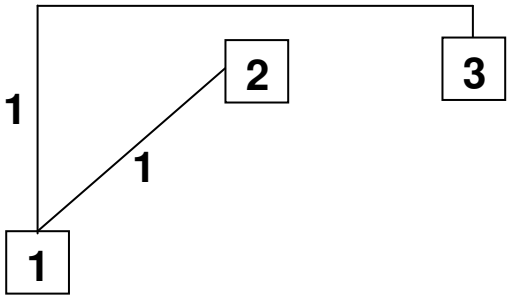
4. Nätverksskiktet
   a. Internet Protocol (IP), routing protocol inklusive forwarding table (routingtabell) och Internet Control Message Protocol (ICMP) är de tre huvuddelarna i Internet-skiktet. IP används för adressering, paketformat och pakethantering. Routing protocol som t.ex. RIP, OSPF och BGP används i routrarna för att bestämma bästa väg. ICMP används för felrapportering och routermeddelanden (routersignalering).
   b. Lösningen kan framställas på olika sätt eftersom det finns flera alternativa steg. Den lösning som presenteras här bygger på principen att noden (routern) med lägsta nummer väljs om det finns två eller flera alternativa vägar (länkar) som har lika kostnad.

Initialt: 

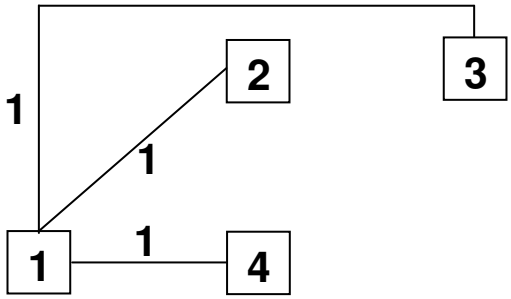
{1}

Steg 1: 

{1, 2}

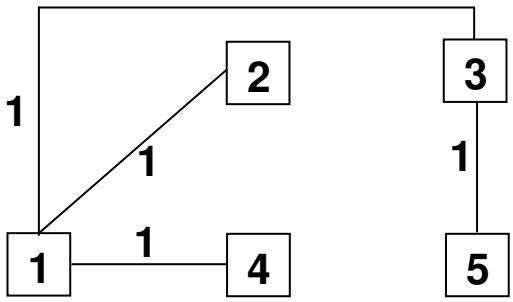
Steg 2: 

{1, 2, 3}

Steg 3: 

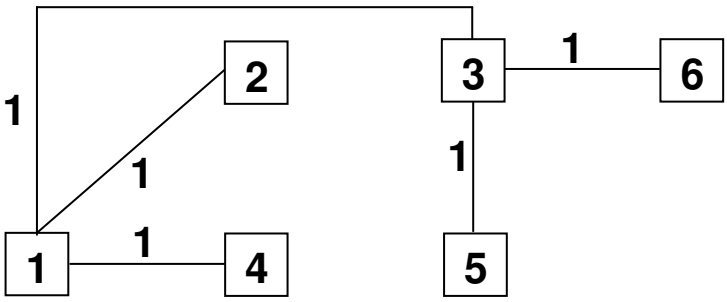
{1, 2, 3, 4}

Steg 4:



{1, 2, 3, 4, 5}

Steg 5:



{1, 2, 3, 4, 5, 6} = {ALLA}
=> STOPP!

5. Länkskiktet, lokala nät, trådlösa och mobila nät
   a. TDM (TDMA) står för ”time” som innebär att sändningstiden delas upp för fleråtkomst (multiaccess). Vanligtvis delas sändningstiden upp i tidsluckors (slots) som upprepas efter ett bestämt mönster så att varje station för möjlighet att sända i egna tidsluckor.
      FDM (FDMA) står för ”frequency” som innebär att stationerna sänder på egna bärvågsfrekvenser (i Hz). För att inte störa varandra finns det reserverad banddredd (i Hz) kring varje bärvåg.
      (Det förekommer också kombinationer av TMA och FDM. Så fungerar exempelvis GSM.)
   b. Pikonätet består aktiva enheter (master och slavar) och inaktiva enheter som sägs vara ”parkerade”.
      Masterenheten: Bestämmer tiden. Kan sända i alla tidsluckor med udda nr.
      Slavenheter: Någon/några. Kan endast sända efter anrop från masterenheten. Kan endast sända till masterenheten.
      Parkerade enheter: Det kan finnas maximalt 255 parkerade (inaktiva) enheter.

6. Multimedia
   a. Real-time interactive audio and video avser kommunikation i ljud och bild över Internet mellan klienter. (Interactive audio kallas Internet-telefoni eftersom det ur användarens synvinkel liknar ett traditionellt telefonsamtal.)
   b. Best-effort innerbär att IP flyttar varje paket från sändare till mottagare så snabbt som möjligt, men IP ger inga garantier om fördröjningen från ände till ände för enskilda paket. Packet jitter har med det senare att göra. Begreppet används för Internet-telefoni och real-time interactive voice/video. Då gäller det variationen för paketens fördröjning inom samma paketström.
   c. Det kan åstadkommas genom att från originalet (audio stream) skapa en motsvarande kopia med låg samplingsfrekvens och lågt antal bitar, dvs. en lågkvalitetskopia. Ett stycke (chunk) anpassas efter paketstorleken så att även en lågkvalitetskopia för plats. I paket n finns stycket n tillsammans med lågkvalitetskopian $n - 1$. (Givetvis finns det ingen lågkvalitetskopia i det första paketet.) På så sätt kan man vid paketförlust ersätta stycket n med lågkvalitetskopian n som kommer fram till mottagaren i paket $n + 1$.
   d. Rspec står för reservation, dvs. den specifika QoS som en uppkoppling erfordrar. Tspec står för trafiken, dvs. trafiken som sändaren kommer att åstadkomma i nätverket eller som mottagaren kommer att få från nätverket. En router i Intserv-arkitekturen avgör med dessa parametrar om den har tillräckligt med resurser för att möta QoS-kraven.

7. Datasäkerhet och management
   a. En inkräktare fångar upp meddelanden från en sändare A och skickar meddelanden vidare till den rätta mottagaren B.
   Inkräktaren fångar upp B's temporära testmeddelande, s.k. nonce, och skickar tillbaka en krypterad version detta. Krypteringen görs med inkräktarens privata nyckel.
   På begäran skickar inkräktaren sin publika nyckel till B.
   Inkräktaren skickar B's temporära testmeddelande, s.k. nonce, vidare till A och fångar på detta sätt upp A's publika nyckel.
   Efter detta kan inkräktaren dekryptera meddelanden från B, läsa meddelanden och kryptera meddelanden för att sända vidare till A.
   b. Paketfilter är ett program som placeras (eller redan finns) i en standardgateway (default gateway, routern för trafik in och ut). (Paketfiltrerande brandväggar förekommer också som separat enheter, dvs. som komplement till standardgateways, speciellt i stora nät.) Det filtrerar med avseende på t.ex. IP-adresser (sändare/mottagare), TCP/UDP-portnummer (sändare/mottagare), ICMP-typ och användandet av TCP-SYN eller TCP-ACK.