Kursen Introduktion till datakommunikation
Laboration 3:

Skapad av
Douglas Howie
Högskolan i Gävle (HiG)
2011-02-14
2013-02-14 revision 1

Analys av Ethernet ramar och TCP segment

Syfte

Efter genomförandet av denna laboration ska studenten ha grundläggande kunskaper om tillförlitlig dataöverföring i datornät, om det förbindelseorienterade protokollet TCP (Transport Control Protocol) och hur portnummer används i TCP.

Anvisningar

Denna laboration är avsedd att utföras i en PC-sal på HiG (inte på studentens egen PC). Operativsystemet är av typen MS Windows. Börja med att klipp-och-klistra hela detta dokument in i ett ordbehandlingsprogram. Skriv in dina svar efter varje fråga nedan (markerad med frågenummer **). Glöm inte att skriva ditt namn, födelseår och e-postadress i början av redovisningen!

Du behöver läroboken ”Internet” av Maria Kihl och Jens Andersson för att kunna besvara en del av frågorna i denna laboration. Om en annan informationskälla används ska denna anges i din redovisning.

Laboration 3 täcker den delen av kursen som motsvaras av kapitel 3, 5 och 10 i läroboken Internet version 2008 av Maria Kihl och Jens A. Andersson.

---
1 Analys av Ethernet II ramar i ett LAN

Du kan köra igång Wireshark (WS) genom att dubbelklicka på en .cap- eller .trace-fil om WS är installerad på din Windows-PC.

I annat fall kan du söka i Windows efter Wireshark-ikonen och dubbelklicka på den. WS är en nätverksanalysator som kan fånga upp och tolka paket i ett datornät. WS tolkar bitarna i paketen och visar upp i ett grafiskt gränssnitt innehållet i paketets huvud, data och svans. Det går att köra WS mot ett datornät under drift eller mot en s.k. "trace file". I denna laboration kommer du att köra WS mot två olika trace-filer. Båda filerna är hämtade från WS-webbplatsen på Internet (http://www.wireshark.org/).

Öppna trace-filen som heter tcpshake.cap. (Ett alternativ är att klicka på ikonen "Open a capture file…" som är sjätte ikonen från vänster räknat). Översta fönstret i WS innehåller en rad för varje paket i trace-filen (bara tre stycken i fallet tcpshake). När man klickar på en av raderna öppnas en avkodning eller beskrivning av paketet i mittersta fönstret. Fönstret längs ner visar det binära innehållet av paketet dels i hexadecimala form dels som ASCII text.

1.1 **Vad är IP nummer på de två datorerna som kommunicerar med varann? Vad är IP nummer på datorn som initierar dialogen?

1.2 **Hela dialogen mellan datorerna i denna trace-fil består av tre ramar. Hur stor är varje ram i bytes räknat? Hur många bytes skickas totalt under hela dialogen?

1.3 **Hur många millisekunder tar hela proceduren? Räkna även ut överföringshastigheten i bitar per sekund.

Länkprotokollet som används i denna dialog heter Ethernet II. Varje Ethernet II ram består av huvud, data och svans. Klick på raden i mittersta fönstret som börjar med ”Ethernet II” och titta sedan i nedersta fönstret.

1.4 **Hur många bytes finns i varje rams huvud respektive svans?

1.5 **Det finns tre fält i Ethernet II huvudet. Beskriv innehållet i dessa fält och hur många bytes som finns i varje fält.

1.6 **Vad finns det i ramens datadel?

1.7 **Finns det någon nedre eller övre gräns för Ethernet II ramens storlek? I så fall vad? Tips: prova med sökbegrepp ”ethernet II” i din favorit sökmotor.

”Det fysiska skiktet levererar en bitström och för att särskilja olika ramar används ofta så kallade flaggor, som är en bitsekvens med ett speciellt mönster” (citat från sidan 41 i kursboken). Bitsekvensen som signalerar ramens slut kallas för svans.

1.8 **Är svansarna (Trailers) i Ethernet II ramarna i denna trace-fil alltid lika stora? Förklara!

1.9 **Anta att en ethernet ram som är 72 bytes lång skickas mellan två datorer i ett 100 Mbps LAN. Kabeln mellan datorerna är 100 meter lång och signalerna går med 2/3-delar av ljusets hastighet i vakuum. Hur lång tid tar det från tidpunkten då första biten skickas från sändande datorns adapterkort till tidpunkten då sista biten kommer till mottagande datorns adapterkort? Visa dina beräkningar!

---

2 Handskakning i det förbindelseorienterade protokollet TCP

Som framgår av beskrivningen i läroboken på sidan 78 finns det 3 steg i TCP uppkopplingsfasen. Denna "3-way handshake" eller handskakningsprocedur består av följande steg: 1) initierande dator skickar ett TCP-segment till svarande dator, 2)svarande dator accepterar eller nekar till att en logisk förbindelse upprättas, 3) initierande dator fastställer upprättandet av förbindelsen och skickar första datablocket till svarande dator.

Under uppkopplingsfasen bestäms det maximala storleken på TCP segment som skickas mellan datorerna på den logiska förbindelsen.

2.1 **Vad är den maximala mängd data som tas med i ett TCP-segment på förbindelsen som upprättas i trace-filen som heter tcpshake.cap? (Tips: läs sidan 80 i läroboken)

2.2 **Är det den initierande eller svarande dator som bestämmer den maximala storleken?

Det finns två viktiga kontrollflaggor i TCP-headern som heter SYN och ACK. (se sidan 77 i läroboken)

2.3 **Beskriv värdet på SYN- och ACK-flaggorna för varje steg i TCP handskakningsproceduren.

---

3 TCP: Seq (sequence number), Ack (acknowledgement), MSS (Maximum Segment Size)

Öppna WS capture filen med namnet tcp-ethereal-file1.trace. Denna WS capture-fil består av 220 stycken Ethernet II ramar. En kort beskrivning av händelseförloppet följer.

I ram nummer 3 tar dator 167 (131.212.31.167) kontakt med dator 12 (128.119.245.12). TCP handskakning sker mellan datorerna i ramarna 3-5. Observera att applikationen på dator 167 använder portnummer 2096. Applikationen på dator 12 svarar från en port som heter http (d.v.s. port 80). Då kan vi anta att användaren på dator 167 kör en webbläsare mot en webbserver på dator 12. Vi använder därför beteckningen klient-167 och server-12 i resten av denna beskrivning.

Läs om TCP i läroboken av Kihl sidorna 81-84. Om exemplet i figur 5.8 på sidan 82 jämförs med innehållet i filen tcp-ethereal-file1.trace kan man säga att Sändare motsvarar klient-167 och Mottagare motsvarar server-12.

Klick på rubriken "Source" i WS för att sortera ramarna efter källans IP-nummer. Nu kan du lättare se all datatrafik som kommer från server-12 eller klient-167. Observera att Ack-fältet från server-12 har värdet "1" i ram 4 och ökar successivt för varje ny ram som skickas till klient-167.

3.1 **Hur många bytes har server-12 tagit emot när den skickar Ack till klient-167 i ram 16? Beskriv vad värdet i Ack-fältet egentligen betyder.

Lite längre ner i den sorterade WS-filen ser man trafiken från klient-167. Första Ack-fältet från klient-167 till server-12 kommer i ram nummer 5. Titta nu på värdet i Ack-fältet i ramarna 6, 7, 9, 11, 12 o.s.v. genom att öppna TCP-huvudet i varje ram. Det står t.ex. "Acknowledgement number: XXX (relativ ack number)".

3.2 **Vad är värdet på Ack i TCP-huvudet som finns i ramarna som skickas från klient-167? Förklara det som du har observerat.

3.3 **Vad är det maximala antalet bytes som kan skickas i datafältet av en Ethernet II ram? Detta kallas även för MTU (Maximum Transfer Unit, se sidan 55 i läroboken).

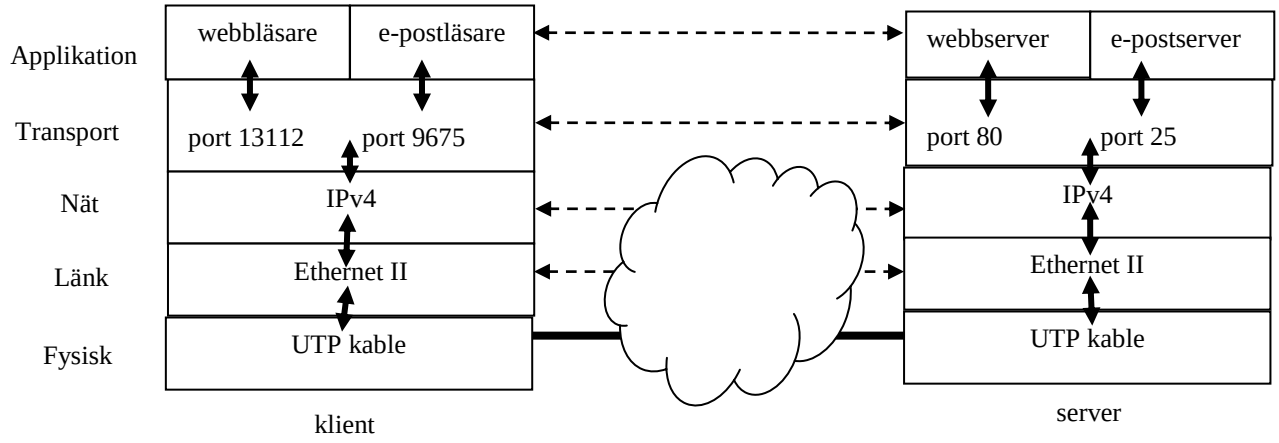
3.4 **Med tanke på MTU i Ethernet II och längden på IP- och TCP-huvuden kan du förklara varför server-12 ställer MSS (Maximum Segment Size) till 1460 i ram nummer 4?

3.5 **Titta på innehållet i ram nummer 216 och förklara det som händer när server-12 tar emot den.

3.6 **Räkna ut dataöverföringshastigheten i bps när filen överförs från klient-167 till server-12 (d.v.s. från ram 6 till ram 216). Visa dina bräkningar.

---
4 TCP portar

Varje applikation som vill kommunicera med andra applikationer via nätverket måste ansluta sig till en portadress i transportskiktet. Se Figur 1 nedan.



Figur 1 Jämför med Figur 5.1 i läroboken!

Figur 1 visar hur en webbläsare kan användas samtidigt som en e-postläsare i klientdatorn t.v. för att kommunicera med en webbserver och e-postserver i serverdatorn t.h. Ethernet II-huvuden och IP-huvuden mellan dessa två datorer ser likadana ut oavsett om det är ett webb TCP-segment eller ett e-post TCP-segment som transporteras. Det är bara portadresserna i TCP-huvuden som skiljer segmenterna åt.

Öppna ett cmd-fönster på din Windows PC. Läs om netstat-kommandot med följande kommando:

```
netstat ?
```

4.1 **Testa följande kommando och beskriv med dina egna ord vad kommandot gör och hur utskriften från kommandot skall tolkas (tips: den andra varianten lägger upp netstat-utskriften i en textfil som du kan klistra in i din laborationsredovisning).

```
 netstat -a -n -p tcp
(netstat -a -n -p tcp > netstat-nummer.txt)
```

4.2 **Kör nu kommandot "netstat -a -p tcp" och jämför resultatet med "netstat -a -n -p tcp". Vad är skillnaden?

4.3 **Välj ut tre olika portnummer och ange vad porttjänsten heter i klartext.