

Nät - Protokoll för Internet och Ethernet

I denna laboration undersöktes olika protokoll med hjälp av programmet Wireshark i operativsystemet Linux med distributionen Ubuntu.

Undersökta protokoll var bland annat HTTP, Ethernet, ARP ...

Kurs: Datorkommunikation och nät (DT2017-0200/DT2022-0222)

Härmed försäkrar jag/vi att jag/vi utan att ha erhållit eller lämnat någon hjälp utfört detta arbete.

Datum: 2015-09-20 (Kompletterad 2015-10-22)

Underskrift:

Özgun Mirtchev

Namn: Özgun Mirtchev
Personnr: 920321-2379
E-post: ozziee@gmail.com
Program: Dataingenjörsprogrammet

Lärarens anteckningar

Table of Contents

Bakgrund	2
Resultat.....	3
HTTP	3
Upp och nedkoppling med TCP	3
GET-metoden	4
Villkorlig GET-metod	5
Långa HTML-filer	5
HTML-filer med inbäddade objekt	6
Autentisering med HTTP	6
Ethernet	7
Ethernet II.....	7
ARP	8
ARP för Ethernet II	8

Bakgrund

I dagens samhälle präglas all sorts teknik med någon sorts trådlös eller trådbunden kommunikation. Alla denna kommunikation sköts om automatiskt med hjälp av olika algoritmer och avancerade program som körs i bakgrunden utan att användaren märker av det själv.

Många av dessa kommunikationer (om inte alla) sköts om av olika protokoller som har blivit utvecklade från olika tekniska företag och även viktiga departement som har hand om världskommunikationen. Internet och hela intranätet är fortfarande ganska ungt, då det har funnits i lite mer än 20 år. Även om det är så ungt så utvecklas det enormt varje år och nya protokoll och sätt att koppla ihop system i olika delar av världen utvecklas i en oerhörd takt.

Vad är då protokoller? Protokoller är i själva verket de program och de hårdvaror som gör så att intranätet och kommunikationen mellan alla routrar och servrar fungerar. Det har utvecklats mycket inom detta och det kommer nya protokoller och de befintliga utvecklas mer och mer. I denna laboration kommer HTTP att undersökas tillsammans med Ethernet och ARP, som alla är olika protokoller och som håller koll på olika saker i kommunikationen mellan klient och server.

Först fanns HTTP 1.0 (1990-talet), sedan kom HTTP 1.1 (2000-talet) som används i många sidor nu, men fortfarande finns det sidor som använder HTTP 1.0. Just nu utvecklas även en ny version av protokollet som kallas HTTP 2.0 (som främst är utvecklad av Google), men dock är den inte lika utbredd, endast runt 1 % av alla webbsidor använder HTTP 2.0 just nu. Skillnaderna mellan de olika protokoll-versionerna kan vara att de är mer säkra och kan hantera fler kopplingar på samma gång osv.

Laborationen utgår på att man kan vissa begrepp inom protokollernas värld och kan teorin runt deras funktionalitet. Först kommer att kopplingar inom HTTP att gås igenom, sedan Ethernet och till sist ARP. Utförandet skedde på så sätt att frågorna besvarades direkt från Labb-PM, den krävs för att man ska kunna förstå vilka frågor det handlar om. Dessutom beskrivs vissa frågor med tillhörande bilder/pilar och förklarande text.

Resultat

HTTP

Upp och nedkoppling med TCP

1.

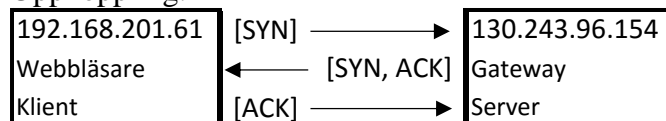
Upp och nedkopplingar sker i ett samspel mellan klienten och servern. Där klienten skickar en request och servern svarar med en reply.

I detta fall skulle sekvensen av en uppkoppling mot en server undersökas med TCP-segment som är flaggade, som klienten och servern skickar mellan varandra för att bekräfta mottagning och sändning. Klientens IP-adress i detta fall var 192.168.201.61, och serverns IP-adress var 130.243.96.154.

Flaggorna är olika för uppkoppling och nedkoppling. Flaggornas begrepp kan hittas i bilaga 1. Nedan syns ordningen för sekvensen av TCP-flaggorna vid uppkoppling och nedkoppling med tillhörande bild från laborationen.

A.

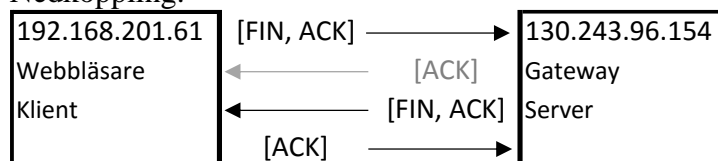
Uppkoppling:



10	5.776958000	192.168.201.61	130.243.96.154	TCP	74 37088 > http-alt [SYN] Seq=0
11	5.777440000	130.243.96.154	192.168.201.61	TCP	74 http-alt > 37088 [SYN, ACK]
12	5.777474000	192.168.201.61	130.243.96.154	TCP	66 37088 > http-alt [ACK] Seq=1

B.

Nedkoppling:




Den andra flaggan[ACK] i nedkoppling, som är från server till klient, är svår att upptäcka (varför den är färgad grå) men det kan hända att den syns på listan ändå. I detta fall lyckades laboranten att få fram den, som syns i nedanstående bild på steg 100.

99	4.246603000	192.168.201.61	130.243.96.154	TCP	66 37196 > http-alt [FIN, ACK] S
100	4.247030000	130.243.96.154	192.168.201.61	TCP	66 http-alt > 37197 [ACK] Seq=58
101	4.247352000	130.243.96.154	192.168.201.61	TCP	66 http-alt > 37201 [FIN, ACK] S
102	4.247367000	192.168.201.61	130.243.96.154	TCP	66 37201 > http-alt [ACK] Seq=2

GET-metoden


2A. Webbbläsaren använder HTTP-version 1.1

```
▼Hypertext Transfer Protocol
▼GET http://basen.oru.se/datorkom/enkel.html HTTP/1.1\r\n
▶[Expert Info (Chat/Sequence): GET http://basen.oru.se/datorkom/enkel.html HTTP/1.1\r\n]
Request Method: GET
Request URI: http://basen.oru.se/datorkom/enkel.html
Request Version: HTTP/1.1
```



2B. Webbservern använder HTTP-version 1.0

```
▼Hypertext Transfer Protocol
▼HTTP/1.0 200 OK\r\n
▶[Expert Info (Chat/Sequence): HTTP/1.0 200 OK\r\n]
Request Version: HTTP/1.0
Status Code: 200
Response Phrase: OK
Last-Modified: Fri, 13 Feb 2015 12:55:14 GMT\r\n
```



3A. Accept-Language: en-US, en;q=0,5

3B. Accept-Encoding: gzip, deflate

4A. 192.168.201.61

4B. 130.243.96.154

5A. Status Code: 200

5B. Response Phrase: OK

6A. Thu, 17 sep 2015 12:55:29 GMT

6B. Last Modified: Fri, 13 Feb 2015 12:55:14 GMT

7A. 273 (Ingen komprimering)

8. Ingen favicon.ico skickades till webbläsaren eftersom svaret från servern till GET <http://basen.oru.se/favicon.ico> blev "404 Not Found".

9.

HTML-koden för sidan:

```
<html>
  <head></head>
  <body link="#330000" vlink="#666633" bgcolor="#D2FFFA">
    <p><br></p>
    <center><h1>Enkel sida</h1><br></center>
    <p><font> size="5">
      Gratulerar! Du har överfört den första testsidan för laborationen!.
    </font></p>
  </body>
</html>
```

Villkorlig GET-metod

10. If-Modified-Since syns inte eftersom att cachén rensades precis innan GET skickades. Webbplatsen finns alltså inte lagrad i cachén för att jämföras.

11A. Status Code: 200

11B. Response Phrase: OK

12. If-Modified-Since: Fri, 13 Feb 2015 12:55:48 GMT

13A. Status Code: 304

13B. Response Phrase: Not Modified

Långa HTML-filer

14A. Bara en.

5	1.146283000	192.168.201.61	130.243.96.154	HTTP	437 GET http://basen.oru.se/datorkom/dataterm.html HTTP/1.1	←
7	1.148297000	130.243.96.154	192.168.201.61	HTTP	1997 HTTP/1.0 200 OK (text/html)	

14B. Gzip och Deflate

15A. Två TCP-segment

192.168.201.61	130.243.96.154	HTTP	437 GET http://basen.oru.se/datorkom/dataterm.html HTTP/1.1	
130.243.96.154	192.168.201.61	TCP	66 http-alt > 37258 [ACK] Seq=1 Ack=372 Win=2332 Len=0 TSv	
130.243.96.154	192.168.201.61	TCP	1514 [TCP segment of a reassembled PDU]	←
130.243.96.154	192.168.201.61	HTTP	557 HTTP/1.0 200 OK (text/html)	
192.168.201.61	130.243.96.154	TCP	66 37258 > http-alt [ACK] Seq=372 Ack=1940 Win=315 Len=0 TS	
192.168.201.61	130.243.96.154	HTTP	396 GET http://basen.oru.se/favicon.ico HTTP/1.1	
130.243.96.154	192.168.201.61	HTTP	573 HTTP/1.0 404 Not Found (text/plain)	
192.168.201.61	130.243.96.154	HTTP	426 GET http://basen.oru.se/favicon.ico HTTP/1.1	
130.243.96.154	192.168.201.61	TCP	561 [TCP segment of a reassembled PDU]	←
130.243.96.154	192.168.201.61	HTTP	78 HTTP/1.0 404 Not Found (text/plain)	

15B. 7773 byte

15C. 1397 byte

15D. Gzip

HTML-filer med inbäddade objekt

16A. Fyra HTTP-GET skickades.

16B. <http://basen.oru.se/datorkom/japan.html>
<http://basen.oru.se/datorkom/hjarta.png>
<http://basen.oru.se/datorkom/favicon.ico>
<http://basen.oru.se/datorkom/favicon.ico>

17A. Accept: image/png, image/*;q=0.8, */*;q=0.5

17B. Tre stycken (2 + 1 segment = 3)

6	1.033380000	192.168.201.61	130.243.96.154	HTTP	454 GET http://basen.oru.se/datorkom/hjarta.png HTTP/1.1	
7	1.035235000	130.243.96.154	192.168.201.61	TCP	1514 [TCP segment of a reassembled PDU]	←
8	1.035257000	130.243.96.154	192.168.201.61	TCP	1514 [TCP segment of a reassembled PDU]	←
9	1.035265000	192.168.201.61	130.243.96.154	TCP	66 37267 > http-alt [ACK] Seq=757 Ack=4252 Win=308 Len=0 TSval=146359083 TSecr=3294492556	←
10	1.035269000	130.243.96.154	192.168.201.61	HTTP	206 HTTP/1.0 200 OK (PNG)	

18A. HTTP 1.1

18B. Default-läget för HTTP 1.1 är att alla kopplingar är varaktiga

18C. Eftersom kopplingarna mellan GET requesten och inte kopplades ned så dras slutsatsen att det var en varaktig koppling.

Autentisering med HTTP

19. **Statuscode:** 401
Response Phrase: Unauthorized

3	2.340839000	192.168.201.61	130.243.96.154	HTTP	394 GET http://dkn.com.li.com/auktorisering.php HTTP/1.1
5	2.643955000	130.243.96.154	192.168.201.61	HTTP	541 HTTP/1.0 401 Unauthorized (text/html)
17	13.620685000	192.168.201.61	130.243.96.154	HTTP	429 GET http://dkn.com.li.com/auktorisering.php HTTP/1.1
22	13.913502000	130.243.96.154	192.168.201.61	HTTP	445 HTTP/1.0 200 OK (text/html)
24	13.969298000	192.168.201.61	130.243.96.154	HTTP	419 GET http://stats.hosting24.com/count.php HTTP/1.1
28	14.230442000	130.243.96.154	192.168.201.61	HTTP	464 HTTP/1.0 200 OK

20A. Authorization

20B. Basic b2xl0nBpenph

20C. Credentials: ole:pizza

Ethernet

Ethernet II

Rad 7 = GET

Rad 9 = TCP

Rad 11 = OK

4	4.481037000	Hewlett-_79:0e:d1	Hewlett-_e3:c8:da	0x0800	74 IP
5	4.481555000	Hewlett-_e3:c8:da	Hewlett-_79:0e:d1	0x0800	74 IP
6	4.481578000	Hewlett-_79:0e:d1	Hewlett-_e3:c8:da	0x0800	66 IP
7	4.481650000	Hewlett-_79:0e:d1	Hewlett-_e3:c8:da	0x0800	437 IP ←
8	4.482116000	Hewlett-_e3:c8:da	Hewlett-_79:0e:d1	0x0800	66 IP
9	4.483055000	Hewlett-_e3:c8:da	Hewlett-_79:0e:d1	0x0800	1514 IP ←
10	4.483065000	Hewlett-_79:0e:d1	Hewlett-_e3:c8:da	0x0800	66 IP
11	4.483074000	Hewlett-_e3:c8:da	Hewlett-_79:0e:d1	0x0800	556 IP ←
12	4.483082000	Hewlett-_79:0e:d1	Hewlett-_e3:c8:da	0x0800	66 IP

21A. 0x00:1B:78:E3:C8:DA

21B. Standard Gateway

22. 0xD8:D3:85:79:0E:D1

23A. Två (2)

23B. Fyra (4)

23C. 0x0800

23D. IP

24. (Hittad i innehållsfönstret)

25. 542 bytes

26A. 1500 bytes är den största från TCP 9

26B. 1500 bytes enligt figur 5.

ARP

ARP för Ethernet II

27A.

```
t002-client ubuntu@drone ~ > arp
```

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.201.53	ether	d8:d3:85:77:36:a0	C		eth1
192.168.201.1	ether	00:1b:78:e3:c8:da	C		eth1

IP-adress	MAC-adress	Funktion i nätet
192.168.201.53	D8:D3:85:77:36:A0	Värd
192.168.201.1	00:1B:78:E3:C8:DA	Standard-Gateway

27B.

Hewlett- 77:36:a0	Hewlett- 77:36:94	ARP	Who has 192.168.201.60? Tell 192.168.201.53
Hewlett- 77:36:94	Hewlett- 77:36:a0	ARP	192.168.201.60 is at d8:d3:85:77:36:94

Från min värd till Standard-Gateway:

Who has 192.168.201.60? Tell 192.168.201.53

Svar från Standard-Gateway till värd:

192.168.201.60 is at D8:D3:85:77:36:94

28. Data-fältet, eftersom ARP blir transporterad i "payloaden".

29. Type: ARP(0x0806)

Ethernet II

Preamble (8 B)
Destination address (2 el. 6 B)
Source address (2 el. 6 B)
Type (2 B)
Data (0–1500 B)
Pad (0–46 B)
FCS (4 B)

Tack för en lärorik laboration!