

Nguyễn Văn Nhật

B2012122

THỰC HÀNH BUỔI 5

Bài 14

Câu 1

- Chọn khung vật lý của giao thức TCP đầu tiên và mở Transmission Control Protocol Header trong khung này:
 - o Trình duyệt web phía Client đang hoạt động ở port 39620
 - o Ứng dụng apache2 của WebServer đang hoạt động ở port 80
 - o Giá trị cờ SYN:

The image shows a Wireshark packet capture of a SYN packet. The packet list on the left shows 'Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)'. The packet details pane shows the following information:

- Ethernet II, Src: 82:81:35:27:34:fb (82:81:35:27:34:fb), Dst: 22:d1:c2:e0:98:5b (22:d1:c2:e0:98:5b)
- Internet Protocol Version 4, Src: 192.168.2.100, Dst: 192.168.1.100
- Transmission Control Protocol, Src Port: 39620, Dst Port: 80, Seq: 0, Len: 0
 - Source Port: 39620
 - Destination Port: 80
 - [Stream index: 0]
 - [TCP Segment Len: 0]
 - Sequence Number: 0 (relative sequence number)
 - Sequence Number (raw): 1453422543
 - [Next Sequence Number: 1 (relative sequence number)]
 - Acknowledgment Number: 0
 - Acknowledgment number (raw): 0
 - 1010 = Header Length: 40 bytes (10)
 - Flags: 0x002 (SYN)
 - 000. = Reserved: Not set

The packet bytes pane shows the raw data of the packet, with the flag field (0000) highlighted in blue.

Nhiệm vụ của gói tin TCP (SYN): dùng để bắt đầu một connection

- Chọn khung vật lý TCP tiếp theo (Khung của giao thức TCP thứ 2) và mở Transmission Control Protocol Header trong khung này:
 - o Nhiệm vụ gói tin TCP (SYN, ACK): Cờ ACK được sử dụng để xác nhận việc nhận thành công các gói tin. Khi client gửi yêu cầu kết nối trong đó có cờ syn, Sau khi server nhận được cờ syn rồi thì sẽ phản hồi lại cho client 1 gói tin gồm có cờ syn và 1 cờ ACK đi sau nó để báo là đã nhận gói dữ liệu vừa nhận được.
- Chọn khung vật lý TCP tiếp theo (Khung của giao thức TCP thứ 3) và mở Transmission Control Protocol Header trong khung này và trả lời:

- Nhiệm vụ gói tin TCP (ACK): Packet này được gửi với mục đích duy báo cho máy chủ biết rằng client đã nhận được SYN/ACK packet và lúc này connection đã được thiết lập và dữ liệu sẽ bắt đầu lưu thông tự do.

Kết luận: 3 khung này dùng để cho dữ liệu có thể lưu thông tự do giữa máy Client và Server trong giao thức TCP

- Chọn khung vật lý của giao thức HTTP đầu tiên:
 - Cờ PUSH trong Transmission Control Protocol Header được bật lên, nó tồn tại để đảm bảo rằng các dữ liệu được ưu tiên và được xử lý tại nơi gửi hoặc nơi nhận. Cờ này cụ thể được sử dụng khá thường xuyên ở đầu và cuối của việc truyền dữ liệu, ảnh hưởng đến cách dữ liệu được xử lý ở cả 2 đầu. Khi sử dụng, cờ PUSH làm cho các Segment chắc chắn được xử lý 1 cách chính xác và ưu tiên thích hợp ở cả 2 đầu của kết nối.
 - Thông điệp HTTP gửi đi có dạng GET, trình duyệt phía PC sử dụng là Links, hệ điều hành Linux
- Chọn khung vật lý của giao thức TCP tiếp theo (Khung TCP thứ 4):

```

▶ Ethernet II, Src: 22:d1:c2:e0:98:5b (22:d1:c2:e0:98:5b), Dst: 82:81:35:27:34:fb (82:81:35:27:34:fb)
▶ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.2.100
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 39620, Seq: 1, Ack: 592, Len: 0
  Source Port: 80
  Destination Port: 39620
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 224189603
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 592 (relative ack number)
  Acknowledgment number (raw): 1453423135
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x010 (ACK)
  Window: 505
  [Calculated window size: 64640]
  0000  82 81 35 27 34 fb 22 d1 c2 e0 98 5b 08 00 45 00  ..5'4."...[..E.
  0010  00 34 02 26 40 00 40 06 b3 85 c0 a8 01 64 c0 a8  .4.&@. @. ....d..
  0020  02 64 00 50 9a c4 0d 5c dc a3 56 a1 7a 1f 80 10  .d.P... \..V.z...
  0030  01 f9 85 3f 00 00 01 01 08 0a f4 b1 47 93 37 18  ...?.....G.7.
  0040  0f fa
  
```

Sequence Number (tcp.seq), 4 bytes Packets: 31 · Displayed: 31 (100.0%) Profile: Default

- **Sequence number** Trường này có 2 nhiệm vụ. Nếu cờ SYN bật thì nó là số thứ tự gói ban đầu và byte đầu tiên được gửi có số thứ tự này cộng thêm 1. Nếu không có cờ SYN thì đây là số thứ tự của byte đầu tiên
- **Acknowledgement number** Nếu cờ ACK bật thì giá trị của trường chính là số thứ tự gói tin tiếp theo mà bên nhận cần.
- Chọn khung vật lý của giao thức HTTP thứ 2:
 - Thông điệp HTTP trả lời có mã là 200,
 - Thông tin Web Server:

```

- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Date: Sun, 21 Nov 2021 08:50:36 GMT\r\n
    Server: Apache/2.4.25 (Debian)\r\n
    Last-Modified: Mon, 11 Oct 2021 10:49:31 GMT\r\n
    ETag: "29cd-5ce117bd6e4c0-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n

```

○ Lần cập nhật cuối:

```

- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Date: Sun, 21 Nov 2021 08:50:36 GMT\r\n
    Server: Apache/2.4.25 (Debian)\r\n
    Last-Modified: Mon, 11 Oct 2021 10:49:31 GMT\r\n
    ETag: "29cd-5ce117bd6e4c0-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n

```

- Chọn khung vật lý của giao thức TCP tiếp theo (Khung TCP thứ 5):

```

Sequence Number: 592 (relative sequence number)
Sequence Number (raw): 1453423135
[Next Sequence Number: 592 (relative sequence number)]
Acknowledgment Number: 3381 (relative ack number)
Acknowledgment number (raw): 224192983

```

- **Sequence number** Trường này có 2 nhiệm vụ. Nếu cờ SYN bật thì nó là số thứ tự gói ban đầu và byte đầu tiên được gửi có số thứ tự này cộng thêm 1. Nếu không có cờ SYN thì đây là số thứ tự của byte đầu tiên
- **Acknowledgement number** Nếu cờ ACK bật thì giá trị của trường chính là số thứ tự gói tin tiếp theo mà bên nhận cần.
- Chọn khung vật lý của giao thức TCP tiếp theo (Khung TCP thứ 6):
 - Nhiệm vụ gói tin TCP (FIN) trong giao thức giải phóng 3 chiều: dùng để ngắt một connection, Cờ này luôn xuất hiện khi các gói dữ liệu cuối cùng được trao đổi giữa 1 kết nối.
- Số thứ tự của các khung còn lại tham gia vào quá trình giải phóng 3 chiều giữa PC và WebServer:

No.	Time	Source	Destination	Protocol	Length	Info
13	25.881210	192.168.1.100	192.168.2.100	TCP	66	80 → 39620 [FIN, ACK]
14	25.923500	192.168.2.100	192.168.1.100	TCP	66	39620 → 80 [ACK] Seq=
15	29.911147	fe80::6c08:bfff:fe9...	ff02::2	ICMPv6	70	Router Solicitation f
16	31.105486	192.168.2.100	192.168.1.100	TCP	66	39620 → 80 [FIN, ACK]
17	31.105501	192.168.1.100	192.168.2.100	TCP	66	80 → 39620 [ACK] Seq=
18	31.105792	192.168.2.100	192.168.1.100	TCP	74	39622 → 80 [SYN] Seq=
19	31.105815	192.168.1.100	192.168.2.100	TCP	74	80 → 39622 [SYN, ACK]
20	31.106065	192.168.2.100	192.168.1.100	TCP	66	39622 → 80 [ACK] Seq=
21	31.106669	192.168.2.100	192.168.1.100	HTTP	710	GET /icons/openlogo-7
22	31.107032	192.168.1.100	192.168.2.100	TCP	66	80 → 39622 [ACK] Seq=

23	31.147715	192.168.1.100	192.168.2.100	HTTP	6107 HTTP/1.1 200 OK (PNG
24	31.147798	192.168.2.100	192.168.1.100	TCP	66 39622 → 80 [ACK] Seq=
25	32.024408	fe80::6c08:bfff:fe9...	ff02::fb	MDNS	203 Standard query 0x0000
26	36.051822	192.168.1.100	192.168.2.100	TCP	66 80 → 39622 [FIN, ACK]
27	36.095799	192.168.2.100	192.168.1.100	TCP	66 39622 → 80 [ACK] Seq=
28	38.785058	fe80::1c4b:2dff:fe5...	ff02::fb	MDNS	203 Standard query 0x0000
29	40.151069	fe80::1c4b:2dff:fe5...	ff02::2	ICMPv6	70 Router Solicitation f
30	40.449802	192.168.2.100	192.168.1.100	TCP	66 39622 → 80 [FIN, ACK]
31	40.449813	192.168.1.100	192.168.2.100	TCP	66 80 → 39622 [ACK] Seq=

Bài 15

Câu 2

```

root@pc: /
Apache2 Debian Default Page: It works (p1 of 4)
Debian Logo Apache2 Debian Default Page
It works!

This is the default welcome page used to test the correct operation of the
Apache2 server after installation on Debian systems. If you can read this
page, it means that the Apache HTTP server installed at this site is
working properly. You should replace this file (located at
/var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is
about, this probably means that the site is currently unavailable due to
maintenance. If the problem persists, please contact the site's
administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream
default configuration, and split into several files optimized for
interaction with Debian tools. The configuration system is fully
documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for
the full documentation. Documentation for the web server itself can be
found by accessing the manual if the apache2-doc package was installed on
Image http://www.abc.com/icons/openlogo-75.png

```

Kết quả này giống với kết quả bài tập 14, ta thấy giao thức DNS giúp ta phân giải địa chỉ IP thành tên miền (Domain name) => Giúp ích trong quá trình ghi nhớ các địa chỉ, thân thiện hơn với người dùng

Câu 3

- Chọn khung thứ nhất với giao thức DNS và mở User Diagram Protocol Header:
 - o DNS Client trên PC hoạt động ở cổng : 53363
 - o Name Server trên DNSServer hoạt động cổng: 53
 - o Giá trị trường Length: 37
 - o Domain Name System (query):

Domain Name System (query)

Transaction ID: 0x0f53

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

[Response In: 8]

0000	ce 13 39 77 14 6f fe 53 be 16 eb 9b 08 00 45 00	..9w.o.SE.
0010	00 39 5d de 40 00 3e 11 5a 17 c0 a8 02 64 c0 a8	.9].@.>.Z....d..
0020	01 0a d0 73 00 35 00 25 84 f5 0f 53 01 00 00 01	...s.5.% ...S...
0030	00 00 00 00 00 00 03 77 77 77 03 61 62 63 03 63w ww.abc.c
0040	6f 6d 00 00 01 00 01	om.....

Domain Name System (dns), 29 bytes

Packets: 25 · Displayed: 25 (100.0%) Profile: Default

- Chọn khung thứ 2 với giao thức DNS và mở Domain Name System (response):
 - o Nội dung phần Answers:

Answers

- www.abc.com: type A, class IN, addr 192.168.1.100
 - Name: www.abc.com
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 60000 (16 hours, 40 minutes)
 - Data length: 4
 - Address: 192.168.1.100
- Authoritative nameservers
- Additional records
- [Request In: 7]

0010	00 6b 7a e1 00 00 40 11	7a e2 c0 a8 01 0a c0 a8	.kz...@. z.....
0020	02 64 00 35 d0 73 00 57	85 27 0f 53 85 00 00 01	.d.5.s.w .'.S....
0030	00 01 00 01 00 01 03 77	77 77 03 61 62 63 03 63w ww.abc.c
0040	6f 6d 00 00 01 00 01 c0	0c 00 01 00 01 00 00 ea	om.....
0050	60 00 04 c0 a8 01 64 c0	10 00 02 00 01 00 00 ead.....
0060	60 00 06 03 64 6e 73 c0	10 c0 39 00 01 00 01 00	...dns...9.....
0070	00 ea 60 00 04 c0 a8 01	0a

Text item (text), 16 bytes Packets: 25 · Displayed: 25 (100.0%) Profile: Default

- o Nội dung phần Authoritative Nameservers:

Authoritative nameservers

- abc.com: type NS, class IN, ns dns.abc.com
 - Name: abc.com
 - Type: NS (authoritative Name Server) (2)
 - Class: IN (0x0001)
 - Time to live: 60000 (16 hours, 40 minutes)
 - Data length: 6
 - Name Server: dns.abc.com
- Additional records
- [Request In: 7]
- [Time: 0.000318000 seconds]

0010	00 6b 7a e1 00 00 40 11	7a e2 c0 a8 01 0a c0 a8	.kz...@. z.....
0020	02 64 00 35 d0 73 00 57	85 27 0f 53 85 00 00 01	.d.5.s.w .'.S....
0030	00 01 00 01 00 01 03 77	77 77 03 61 62 63 03 63w ww.abc.c
0040	6f 6d 00 00 01 00 01 c0	0c 00 01 00 01 00 00 ea	om.....
0050	60 00 04 c0 a8 01 64 c0	10 00 02 00 01 00 00 ead.....
0060	60 00 06 03 64 6e 73 c0	10 c0 39 00 01 00 01 00	...dns...9.....
0070	00 ea 60 00 04 c0 a8 01	0a

Text item (text), 18 bytes Packets: 25 · Displayed: 25 (100.0%) Profile: Default

Câu 4:

```

root@pc:/# ping www.abc.com
PING www.abc.com (192.168.1.100) 56(84) bytes of data:
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=1 ttl=62 time=1.33 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=2 ttl=62 time=0.157 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=3 ttl=62 time=0.206 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=4 ttl=62 time=0.194 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=5 ttl=62 time=0.205 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=6 ttl=62 time=0.096 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=7 ttl=62 time=0.216 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=8 ttl=62 time=0.146 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=9 ttl=62 time=0.137 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=10 ttl=62 time=0.273 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=11 ttl=62 time=0.138 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=12 ttl=62 time=0.211 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=13 ttl=62 time=0.201 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=14 ttl=62 time=0.222 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=15 ttl=62 time=0.222 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=16 ttl=62 time=0.171 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=17 ttl=62 time=0.315 ms
^C
--- www.abc.com ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16366ms
rtt min/avg/max/mdev = 0.096/0.261/1.330/0.272 ms
root@pc:/#

```

```

root@pc:/# ping dns.abc.com
PING dns.abc.com (192.168.1.10) 56(84) bytes of data:
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=1 ttl=62 time=0.171 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=2 ttl=62 time=0.218 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=3 ttl=62 time=0.200 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=4 ttl=62 time=0.205 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=5 ttl=62 time=0.138 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=6 ttl=62 time=0.135 ms
^C
--- dns.abc.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5097ms
rtt min/avg/max/mdev = 0.135/0.177/0.218/0.036 ms
root@pc:/#

```

```

root@pc:/# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data:
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=0.158 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.085 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.077 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=0.083 ms
64 bytes from 192.168.2.1: icmp_seq=5 ttl=64 time=0.080 ms
64 bytes from 192.168.2.1: icmp_seq=6 ttl=64 time=0.175 ms
64 bytes from 192.168.2.1: icmp_seq=7 ttl=64 time=0.097 ms
64 bytes from 192.168.2.1: icmp_seq=8 ttl=64 time=0.133 ms
64 bytes from 192.168.2.1: icmp_seq=9 ttl=64 time=0.077 ms
64 bytes from 192.168.2.1: icmp_seq=10 ttl=64 time=0.097 ms
^C
--- 192.168.2.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 920ms
rtt min/avg/max/mdev = 0.077/0.106/0.175/0.034 ms
root@pc:/#

```

```

root@pc:/# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data:
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=0.221 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=0.413 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=63 time=0.194 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=63 time=0.151 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=63 time=0.117 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=63 time=0.145 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=63 time=0.207 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=63 time=0.103 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=63 time=0.097 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=63 time=0.102 ms
^C
--- 192.168.1.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 922ms
rtt min/avg/max/mdev = 0.097/0.175/0.413/0.090 ms
root@pc:/#

```

⇒ Nhận xét: Có thể gửi dữ liệu trực tiếp đến các tên miền thông qua lệnh Ping, khi ta gửi dữ liệu đến các tên miền được cấu hình sẵn thì các web server và dns server sẽ trả lời lại máy gửi như 1 thiết bị bình thường

