

## Bài thực hành số 5

### Nhóm 5 Học phần: Mạng máy tính

#### BÀI TẬP 14:

**Câu hỏi 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 địa chỉ (port)  
bao nhiêu?**

Trình duyệt web phía Client hoạt động ở port 53138

**o Ứng dụng apache2 của WebServer đang hoạt động ở địa chỉ (port)  
bao nhiêu?**

Ứng dụng apache2 của WebServer đang hoạt động ở địa chỉ 80

**o Xác định giá trị của cờ SYN. Hãy cho biết nhiệm vụ của gói tin TCP (SYN)  
này trong giao thức bắt tay 3 chiều.**

Flag Syn có giá trị bit là 1 để thông báo kích thước màn hình của máy Client đến Server, Sau đó Server sẽ trả về giao diện phù hợp cho màn hình máy Client

Gói tin TCP SYN (Synchronize) được gửi từ Client đến Server để bắt đầu quá trình thiết lập kết nối. Trong giao thức bắt tay ba chiều của TCP, gói tin SYN được gửi từ Client đến Server để yêu cầu bắt đầu kết nối.

**- Chọn khung vật lý TCP tiếp theo (Khung của giao thức TCP thứ 2) và mở  
Transmission Control Protocol Header trong khung này:**

**o Cờ SYN và ACK được bật lên. Hãy cho biết nhiệm vụ của gói tin TCP (SYN,  
ACK) này trong giao thức bắt tay 3 chiều.**

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:**

**o Cờ ACK được bật lên. Hãy cho biết nhiệm vụ của gói tin TCP (ACK) này  
trong giao thức bắt tay 3 chiều.**

ACK :

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

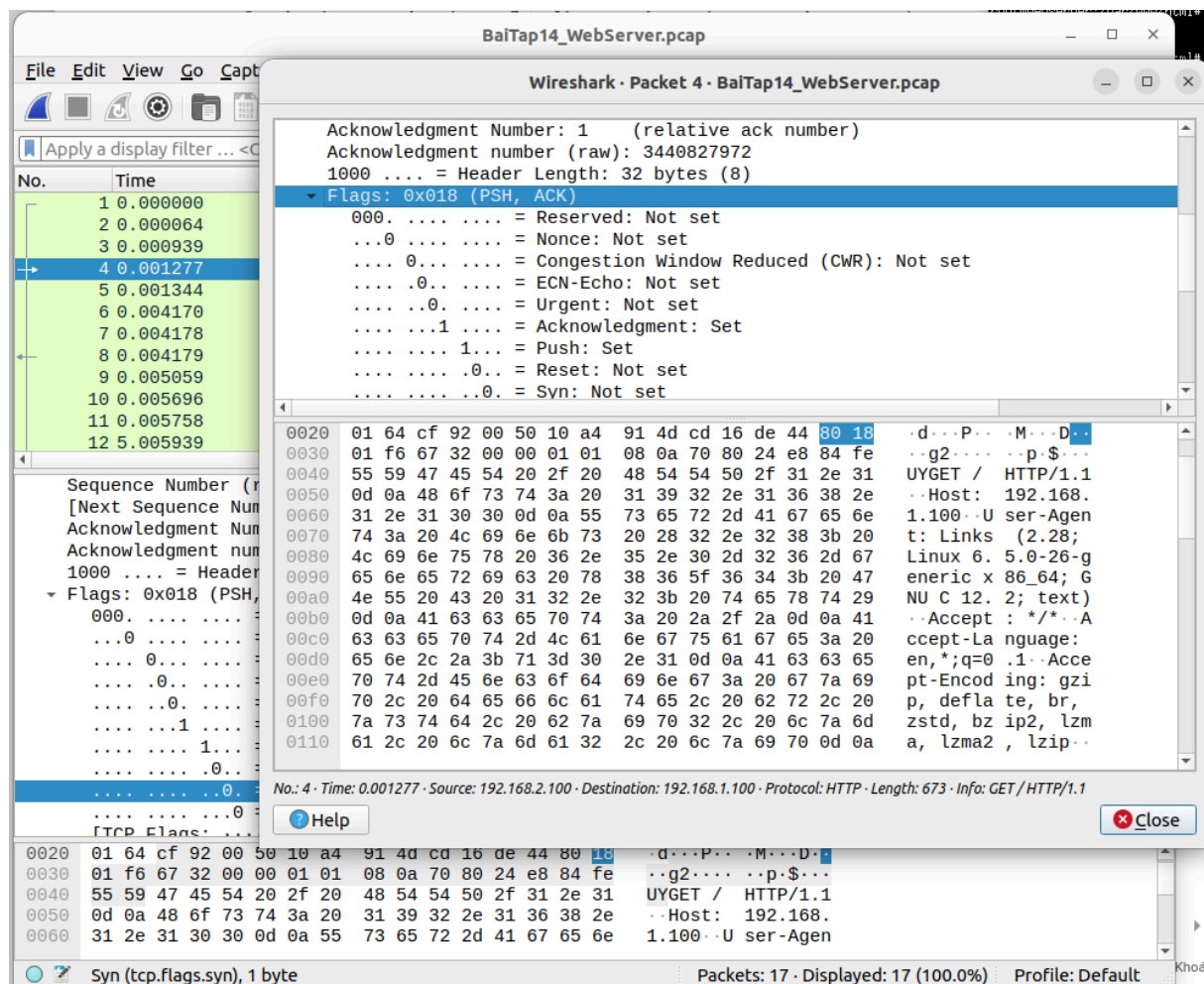
liệu sẽ bắt đầu lưu thông tự do.

⇒ **Kết luận: 03 Khung TCP này dùng để làm gì?**

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:

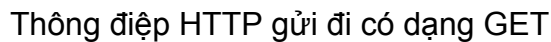
o Cờ PUSH trong Transmission Control Protocol Header có được bật lên không? Cờ này mang ý nghĩa gì?



Cờ PUSH có được bật

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

o Dựa vào thông tin trong HTTP Header, hãy cho biết thông điệp HTTP gửi đi có dạng gì (GET, POST, DELETE...)? Trình duyệt mà phía PC sử dụng là gì? Trình duyệt chạy trên hệ điều hành nào?



## Trình duyệt chạy trên hệ điều hành Linux

Các trường này trong HTTP Header cung cấp thông tin về khả năng của trình duyệt để xử lý các mã hóa, bộ ký tự và ngôn ngữ khác nhau.

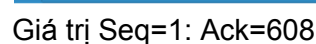
**Accept-Encoding:** Chứa các loại mã hóa (ví dụ: gzip, deflate) mà trình duyệt có thể xử lý cho các nội dung trả về từ máy chủ.

Accept-Charset: Xác định bộ ký tự mà trình duyệt sẽ chấp nhận cho nội dung trả về. Ví dụ: UTF-8.

Accept-Language: Liệt kê các ngôn ngữ mà trình duyệt được ưa thích để nhận dạng nội dung trả về. Ví dụ: en-US (Tiếng Anh Mỹ), vi (Tiếng Việt).

**- Chọn khung vật lý của giao thức TCP tiếp theo (Khung TCP thứ 4):**

**o Giá trị trường Seq và Ack của khung này là bao nhiêu? Có ý nghĩa gì?**



Ý nghĩa

Trường Seq (Sequence Number): Giá trị này là số thứ tự của byte đầu tiên trong phần dữ

liệu của gói tin TCP. Trong trường hợp này, số thứ tự của byte đầu tiên trong phần dữ liệu được gửi từ bên gửi là 1.

Trường Ack (Acknowledgment Number): Giá trị này là số thứ tự của byte tiếp theo mà bên gửi mong muốn nhận được từ bên kia. Trong trường hợp này, bên gửi mong muốn nhận byte tiếp theo có số thứ tự là 608 từ bên nhận.

### - Chọn khung vật lý của giao thức HTTP thứ 2:

o Dựa vào thông tin trong HTTP Header, hãy cho biết thông điệp HTTP trả lời có mã là bao nhiêu (200, 404, 502..)? Thông tin của Web Server? Lần cập nhật cuối cùng nội dung trang web? Sinh viên tự tìm hiểu thêm thông tin về trường Content-Encoding, Content Length, Connection-Type và Connection.

```
▶ Frame 8: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits)
▶ Ethernet II, Src: b6:f1:70:b6:31:8d (b6:f1:70:b6:31:8d), Dst: be:ba:1b:ae:d6:2b (be:ba:1b:ae:d6:2b)
▶ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.2.100
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 53138, Seq: 2897, Ack: 608, Len: 484
▶ [3 Reassembled TCP Segments (3380 bytes): #6(1448), #7(1448), #8(484)]
▼ Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Mon, 08 Apr 2024 07:18:29 GMT\r\n
    Server: Apache/2.4.57 (Debian)\r\n
    Last-Modified: Tue, 26 Sep 2023 08:23:48 GMT\r\n
    ETag: "29cd-6063ecb406d00-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
```

Thông điệp HTTP trả lời có mã là 200

Thông tin của Web Server là Debian

Lần cập nhật cuối cùng nội dung trang web là Mon, 08 Apr 2024

07:18:29 GMT\r\n

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

o Giá trị trường Seq và Ack của khung này là bao nhiêu? Có ý nghĩa gì?

```
▶ Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▶ Ethernet II, Src: b6:f1:70:b6:31:8d (b6:f1:70:b6:31:8d), Dst: be:ba:1b:ae:d6:2b (be:ba:1b:ae:d6:2b)
▶ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.2.100
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 53138, Seq: 1, Ack: 608, Len: 1448
  Source Port: 80
  Destination Port: 53138
  [Stream index: 0]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 1448]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 3440827972
  [Next Sequence Number: 1449 (relative sequence number)]
  Acknowledgment Number: 608 (relative ack number)
```

Giá trị trường Seq là 1 và Ack là 608

Ý nghĩa

Trường Seq (Sequence Number): Giá trị này là số thứ tự của byte đầu tiên trong phần dữ liệu của gói tin TCP. Trong trường hợp này, số thứ tự của byte đầu tiên

trong phần dữ liệu được gửi từ bên gửi là 1.

Trường Ack (Acknowledgment Number): Giá trị này là số thứ tự của byte tiếp theo mà bên gửi mong muốn nhận được từ bên kia. Trong trường hợp này, bên gửi mong muốn nhận byte tiếp theo có số thứ tự là 608 từ bên nhận.

**- Chọn khung vật lý của giao thức TCP tiếp theo (Khung TCP thứ 6):**

**o Nhận thấy rằng cờ FIN được bật lên. Hãy cho biết nhiệm vụ của gói tin TCP (FIN) này trong giao thức giải phóng 3 chiều.**

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.

**- Hãy chỉ ra số thứ tự của các khung còn lại tham gia vào quá trình giải phóng 3 chiều giữa PC và WebServer.**

Chỉ còn khung TCP thứ 8

## **BÀI TẬP 15:**

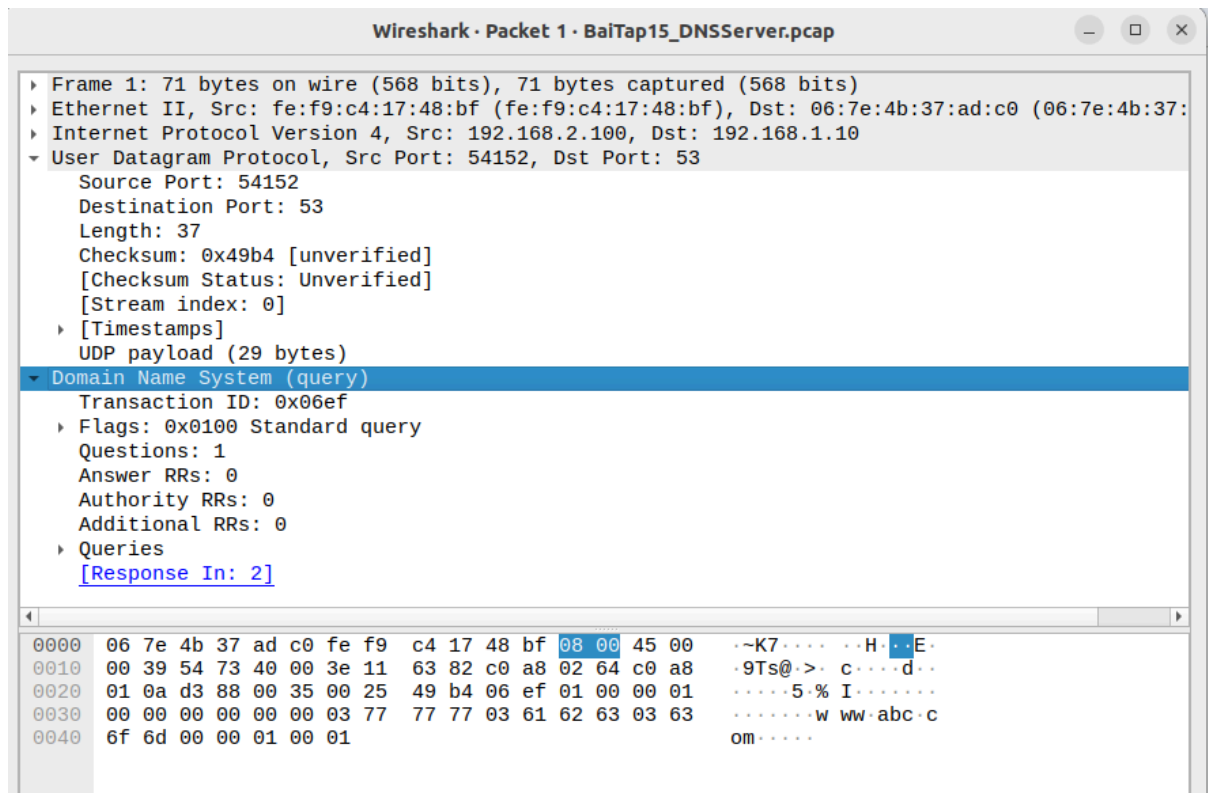
**Câu hỏi 2: kết quả hiển thị mà PC nhận được là gì? có giống ở Bài tập 14 không? Bạn có nhận xét gì?**

Kết quả hiển thị mà PC nhận được là trang default trên webserver

Kết quả hiển thị giống trong Bài tập 14

Nhận xét: Có thể kết luận rằng DNS đã hoạt động thành công và ánh xạ tên miền www.abc.com sang địa chỉ IP của WebServer(192.168.1.100). 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 hỏi 3: - Chọn khung thứ nhất với giao thức DNS và mở User Diagram Protocol Header, trả lời các câu hỏi:**



### o DNS Client trên PC hoạt động ở cổng bao nhiêu?

DNS Client trên PC hoạt động ở cổng 54152

### o Name Server trên DNSServer hoạt động cổng bao nhiêu?

Name Server trên DNSServer hoạt động cổng 53

### o Giá trị của trường Length là bao nhiêu?

Giá trị của trường Length là 37

### o Mở phần Domain Name System (query), nội dung query là gì?

Transaction ID (Mã giao dịch): 0x06ef - Đây là mã giao dịch của gói tin DNS, được sử dụng để đồng bộ hóa giữa truy vấn và phản hồi giữa client và server.

Flags (Cờ): 0x0100 - Đại diện cho các cờ trong gói tin DNS. Trong trường hợp này, 0x0100 cho biết đây là một truy vấn tiêu chuẩn (Standard query).

Questions (Câu hỏi): Trong phần này, có một câu hỏi được đưa ra. Số lượng câu hỏi là 1, cho biết gói tin chứa một truy vấn DNS duy nhất.

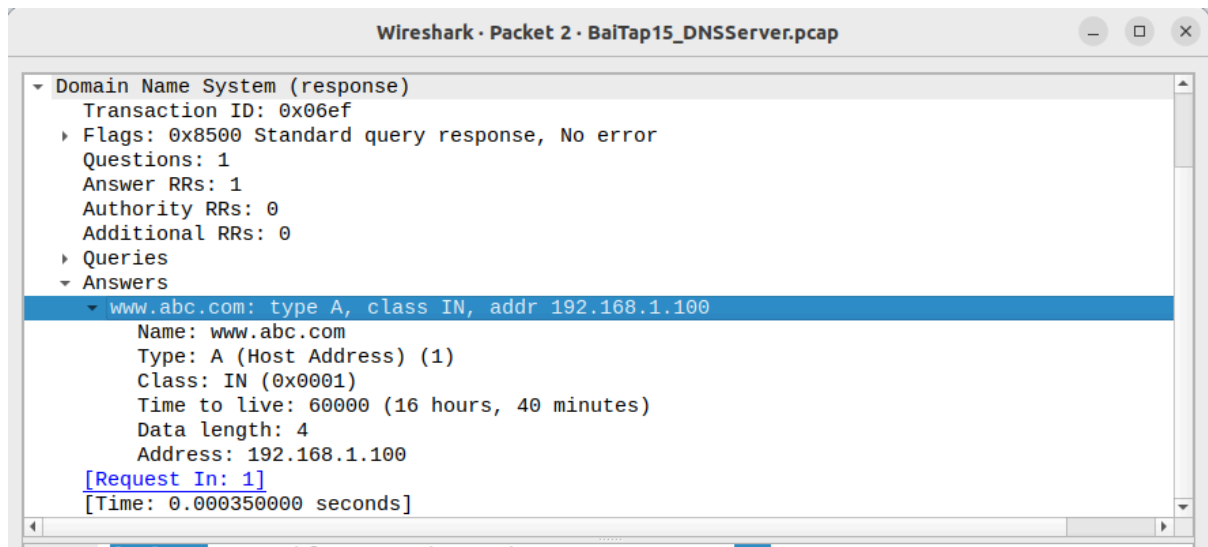
Answer RRs (Số lượng bản ghi câu trả lời): 0 - Cho biết không có bản ghi câu trả lời nào trong gói tin này.

Authority RRs (Số lượng bản ghi quyền lực): 0 - Trong trường hợp này, không có bản ghi quyền lực nào được cung cấp.

Additional RRs (Số lượng bản ghi bổ sung): 0 - Không có bản ghi bổ sung nào được cung cấp.

**- Chọn khung thứ 2 với giao thức DNS và mở Domain Name System (response), trả lời các câu hỏi:**

## o Nội dung phần Answers là gì?



Trong trường hợp này, phần "Answers" cung cấp các thông tin sau:

Tên miền (Name): www.abc.com - Đây là tên miền mà máy tính đã truy vấn.

Loại bản ghi (Type): A (Host Address) - Loại bản ghi này chỉ ra rằng thông tin được cung cấp là địa chỉ IP của máy chủ, cụ thể là IPv4.

Lớp (Class): IN (Internet) - Cho biết rằng loại miền là Internet.

Địa chỉ IP của tên miền (Address): 192.168.1.100 - Địa chỉ IP mà tên miền www.abc.com được ánh xạ tới.

Tóm lại, phần "Answers" trong gói tin DNS cung cấp thông tin cần thiết để máy tính biết được địa chỉ IP tương ứng với tên miền mà nó đã truy vấn. Trong trường hợp này, tên miền www.abc.com được ánh xạ tới địa chỉ IP là 192.168.1.100.

## o Nội dung phần Authoritative Nameservers là gì?

.... .1.. .... = Authoritative: Server is an authority for domain

## Câu hỏi 4: Kết quả hiện thị là gì? Nhận xét?

ping www.abc.com



```
root@pc: /
--- Startup Commands Log
++ ifconfig eth0 192.168.2.100/24 up
++ route add default gw 192.168.2.1
--- End Startup Commands Log
root@pc:/# links
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=0.549 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=2 ttl=62 time=1.43 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=3 ttl=62 time=1.43 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=4 ttl=62 time=1.35 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=5 ttl=62 time=1.30 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=6 ttl=62 time=1.33 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=7 ttl=62 time=1.47 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=8 ttl=62 time=1.50 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=9 ttl=62 time=1.57 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=10 ttl=62 time=1.51 ms
^C
--- www.abc.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 0.549/1.343/1.571/0.277 ms
root@pc:/#
```

ping web.abc.com

```
root@pc: /
root@pc:/# ping web.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=0.884 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=2 ttl=62 time=1.38 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=3 ttl=62 time=1.48 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=4 ttl=62 time=1.38 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=5 ttl=62 time=1.53 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=6 ttl=62 time=1.44 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=7 ttl=62 time=1.47 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=8 ttl=62 time=1.51 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=9 ttl=62 time=1.52 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=10 ttl=62 time=1.51 ms
^C
--- www.abc.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 0.884/1.409/1.531/0.182 ms
root@pc:/#
```



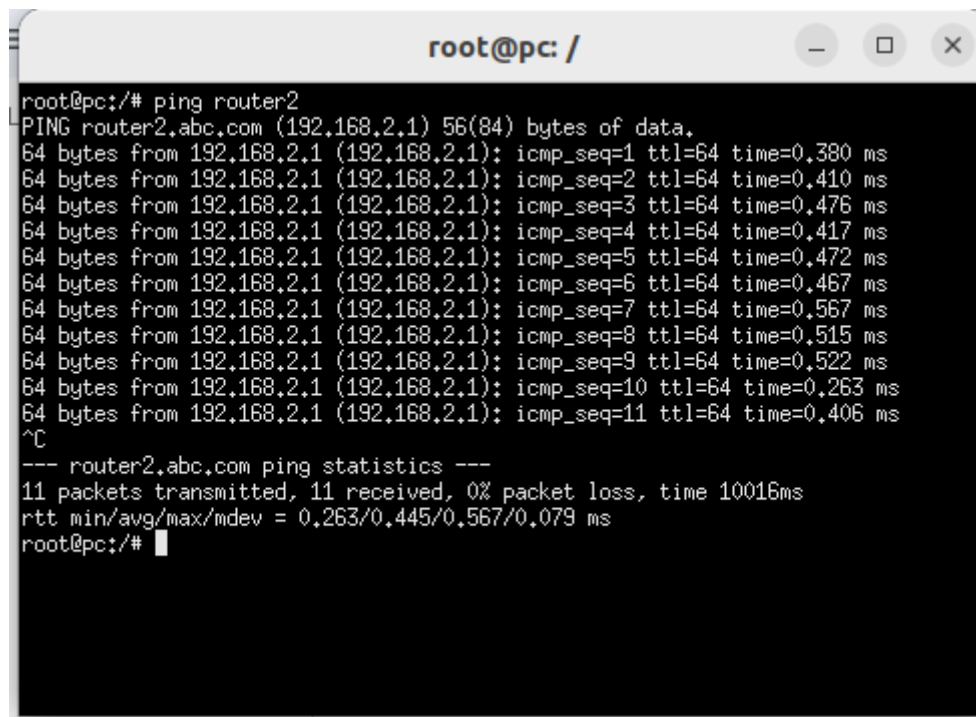
ping dns.abc.com

```
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=1.13 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=2 ttl=62 time=1.45 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=3 ttl=62 time=1.44 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=4 ttl=62 time=1.44 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=5 ttl=62 time=1.40 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=6 ttl=62 time=1.43 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=7 ttl=62 time=1.35 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=8 ttl=62 time=1.40 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=9 ttl=62 time=1.37 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=10 ttl=62 time=1.36 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=11 ttl=62 time=1.39 ms
64 bytes from 192.168.1.10 (192.168.1.10): icmp_seq=12 ttl=62 time=1.39 ms
^C
--- dns.abc.com ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11017ms
rtt min/avg/max/mdev = 1.133/1.379/1.450/0.080 ms
root@pc:/#
```

ping router1

```
root@pc: /
root@pc:/# ping router1
PING router1.abc.com (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1 (192.168.1.1): icmp_seq=1 ttl=63 time=0.691 ms
64 bytes from 192.168.1.1 (192.168.1.1): icmp_seq=2 ttl=63 time=0.928 ms
64 bytes from 192.168.1.1 (192.168.1.1): icmp_seq=3 ttl=63 time=0.761 ms
64 bytes from 192.168.1.1 (192.168.1.1): icmp_seq=4 ttl=63 time=0.968 ms
64 bytes from 192.168.1.1 (192.168.1.1): icmp_seq=5 ttl=63 time=0.946 ms
64 bytes from 192.168.1.1 (192.168.1.1): icmp_seq=6 ttl=63 time=0.920 ms
64 bytes from 192.168.1.1 (192.168.1.1): icmp_seq=7 ttl=63 time=0.954 ms
64 bytes from 192.168.1.1 (192.168.1.1): icmp_seq=8 ttl=63 time=0.980 ms
64 bytes from 192.168.1.1 (192.168.1.1): icmp_seq=9 ttl=63 time=0.969 ms
64 bytes from 192.168.1.1 (192.168.1.1): icmp_seq=10 ttl=63 time=0.995 ms
64 bytes from 192.168.1.1 (192.168.1.1): icmp_seq=11 ttl=63 time=0.950 ms
64 bytes from 192.168.1.1 (192.168.1.1): icmp_seq=12 ttl=63 time=0.932 ms
^C
--- router1.abc.com ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11016ms
rtt min/avg/max/mdev = 0.691/0.916/0.995/0.088 ms
root@pc:/#
```

ping router2:



```
root@pc: /
root@pc:/# ping router2
PING router2.abc.com (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1 (192.168.2.1): icmp_seq=1 ttl=64 time=0.380 ms
64 bytes from 192.168.2.1 (192.168.2.1): icmp_seq=2 ttl=64 time=0.410 ms
64 bytes from 192.168.2.1 (192.168.2.1): icmp_seq=3 ttl=64 time=0.476 ms
64 bytes from 192.168.2.1 (192.168.2.1): icmp_seq=4 ttl=64 time=0.417 ms
64 bytes from 192.168.2.1 (192.168.2.1): icmp_seq=5 ttl=64 time=0.472 ms
64 bytes from 192.168.2.1 (192.168.2.1): icmp_seq=6 ttl=64 time=0.467 ms
64 bytes from 192.168.2.1 (192.168.2.1): icmp_seq=7 ttl=64 time=0.567 ms
64 bytes from 192.168.2.1 (192.168.2.1): icmp_seq=8 ttl=64 time=0.515 ms
64 bytes from 192.168.2.1 (192.168.2.1): icmp_seq=9 ttl=64 time=0.522 ms
64 bytes from 192.168.2.1 (192.168.2.1): icmp_seq=10 ttl=64 time=0.263 ms
64 bytes from 192.168.2.1 (192.168.2.1): icmp_seq=11 ttl=64 time=0.406 ms
^C
--- router2.abc.com ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10016ms
rtt min/avg/max/mdev = 0.263/0.445/0.567/0.079 ms
root@pc:/#
```

## Nhận xét

Qua kết quả ping, ta thấy rằng việc ánh xạ tên miền `www.abc.com` và `dns.abc.com` và `web.abc.com` về địa chỉ IP đã thành công, điều này chỉ ra rằng DNS Server đã hoạt động đúng và các máy trạm PC có thể truy cập vào các dịch vụ trên mạng bằng tên miền.

Sự thành công trong việc ping đến các router và các địa chỉ khác trong mạng cũng cho thấy rằng mạng được cấu hình đúng và các thiết bị mạng hoạt động ổn định.

Tóm lại, việc sử dụng dịch vụ DNS giúp đơn giản hóa việc truy cập vào các dịch vụ trong mạng bằng cách sử dụng tên miền, làm cho quản lý mạng và truy cập dễ dàng hơn đối với người dùng.