

Họ tên: Nguyễn Tấn Tài
MSSV: B1906342

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:

Trình duyệt web phía Client đang hoạt động ở địa chỉ (port) bao nhiêu?
43360

Ứng dụng apache2 của WebServer đang hoạt động ở địa chỉ (port) bao nhiêu?
80

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.

Nhiệm vụ của gói tin TCP (SYN) trong giao thức bắt tay 3 chiều (Three-way Handshake) là bắt đầu quá trình thiết lập kết nối giữa hai máy tính trên mạng. Gói tin SYN được gửi từ máy khởi tạo (client) đến máy chấp nhận (server) để yêu cầu bắt đầu một kết nối TCP. Khi máy chấp nhận nhận được gói tin SYN, nó sẽ trả lời bằng một gói tin SYN-ACK để xác nhận và đồng ý với yêu cầu thiết lập kết nối. Sau đó, máy khởi tạo sẽ gửi một gói tin ACK để xác nhận việc kết nối đã được thiết lập. Qua đó, quá trình bắt tay 3 chiều hoàn tất và kết nối TCP được thiết lập thành công.

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

- Gói tin SYN, ACK là phản hồi của máy chủ (server) đến máy khởi tạo (client) sau khi nhận được gói tin SYN từ máy khởi tạo. Gói tin này chứa cờ SYN và cờ ACK được đặt.
- Trong quá trình bắt tay 3 chiều, sau khi máy chủ đã nhận được gói tin SYN từ máy khởi tạo và đồng ý thiết lập kết nối TCP, nó sẽ gửi lại một gói tin SYN, ACK để xác nhận việc thiết lập kết nối và yêu cầu máy khởi tạo xác nhận (ACK) lại.
- Gói tin SYN, ACK này thường chứa thông tin về các cài đặt cần thiết để máy khởi tạo xác nhận lại kết nối, bao gồm cửa sổ TCP (TCP window size) và các thông số khác. Sau khi máy khởi tạo nhận được gói tin này, nó sẽ gửi một gói tin ACK để xác nhận việc thiết lập kết nối.

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

- Nhiệm vụ của gói tin TCP (ACK) trong giao thức bắt tay 3 chiều (Three-way Handshake) là:
- Gói tin ACK là phản hồi cuối cùng trong quá trình bắt tay 3 chiều. Sau khi máy chủ (server) đã gửi gói tin SYN, ACK cho máy khởi tạo (client), và máy khởi tạo đã xác nhận gói tin SYN, ACK bằng cách gửi lại một gói tin ACK, kết nối TCP được thiết lập hoàn toàn.
- Gói tin ACK xác nhận rằng quá trình thiết lập kết nối đã hoàn tất và cả hai bên (client và server) đều đã sẵn sàng truyền dữ liệu. Sau khi gửi gói tin ACK này, quá trình bắt tay 3 chiều kết thúc và kết nối TCP đã sẵn sàng để truyền dữ liệu hai chiều giữa client và server.

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

- Khung 1 (Gửi SYN): Khung này được gửi từ máy khởi tạo (client) đến máy chấp nhận (server) để bắt đầu quá trình thiết lập kết nối TCP. Trong khung này, cờ SYN được đặt để yêu cầu máy chấp nhận thiết lập kết nối mới.
- Khung 2 (Gửi SYN, ACK): Khung này là phản hồi từ máy chấp nhận (server) đến máy khởi tạo (client) sau khi nhận được khung 1. Trong khung này, cờ SYN và cờ ACK đều được đặt. Nó xác nhận yêu cầu thiết lập kết nối từ máy khởi tạo và đồng ý với việc thiết lập kết nối.
- Khung 3 (Gửi ACK): Khung này là phản hồi cuối cùng từ máy khởi tạo (client) đến máy chấp nhận (server). Trong khung này, chỉ có cờ ACK được đặt. Nó xác nhận việc máy khởi tạo đã nhận được phản hồi từ máy chấp nhận và xác nhận việc thiết lập kết nối. Sau khi gửi khung này, quá trình bắt tay 3 chiều kết thúc và kết nối TCP đã được thiết lập.

Vì vậy, tổng cộng ba khung TCP này được sử dụng để thiết lập một kết nối TCP an toàn và đảm bảo giữa máy khởi tạo và máy chấp nhận.

- Chọn khung vật lý của giao thức HTTP đầu tiên: Cờ PUSH trong Transmission Control Protocol Header có được bật lên không? Cờ này mang ý nghĩa gì?

Có, cờ PUSH có bật lên và có nghĩa là gói tin này chứa dữ liệu mà máy nhận (receiver) yêu cầu để được "đẩy" đến ứng dụng ngay lập tức mà không cần chờ đợi cho đến khi có đủ dữ liệu hoặc đến khi có thời gian chờ (timeout) kết thúc. Cờ PUSH thường được sử dụng để đảm bảo dữ liệu được gửi một cách nhanh chóng và không phải chờ đợi đến khi một cửa sổ TCP đầy đủ được xác định.

Dựa vào thông tin trong HTTP Header, hãy cho biết thông điệp HTTP gửi đi có dạng gì (GET, POST, DELETE...)?

GET

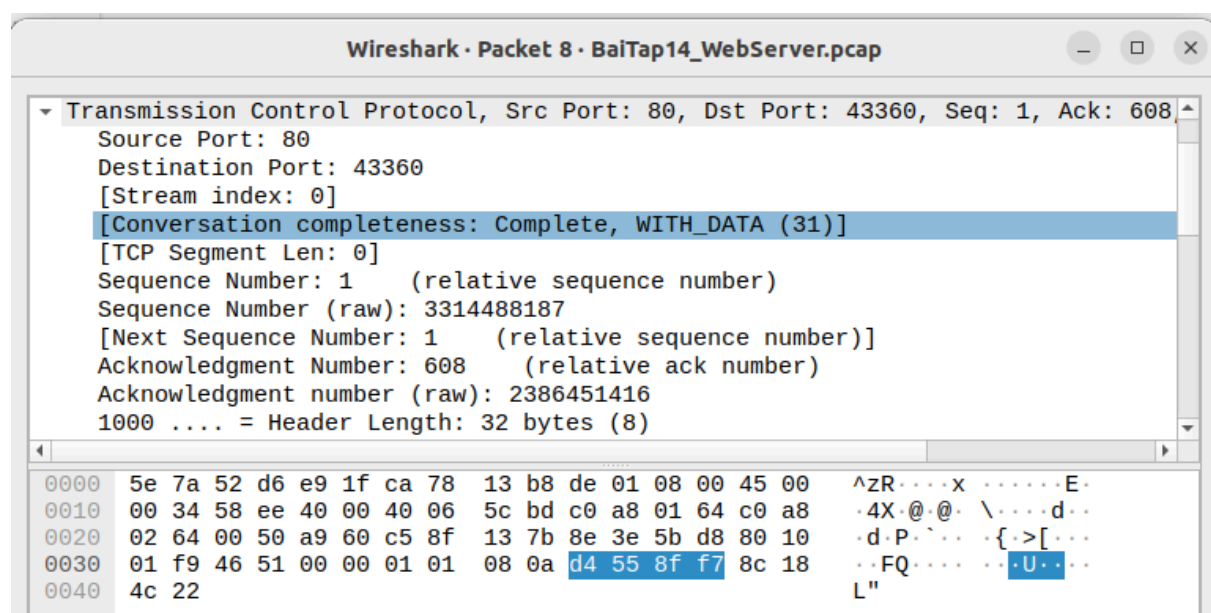
Trình duyệt mà phía PC sử dụng là gì?

Links

Trình duyệt chạy trên hệ điều hành nào?

Linux

- Chọn khung vật lý của giao thức TCP tiếp theo (Khung TCP thứ 4): Giá trị trường Seq và Ack của khung này là bao nhiêu? Có ý nghĩa gì?



Trong khung vật lý của giao thức TCP thứ tư, giá trị của trường Seq (Sequence Number) là 1 và giá trị của trường Ack (Acknowledgment Number) là 608.

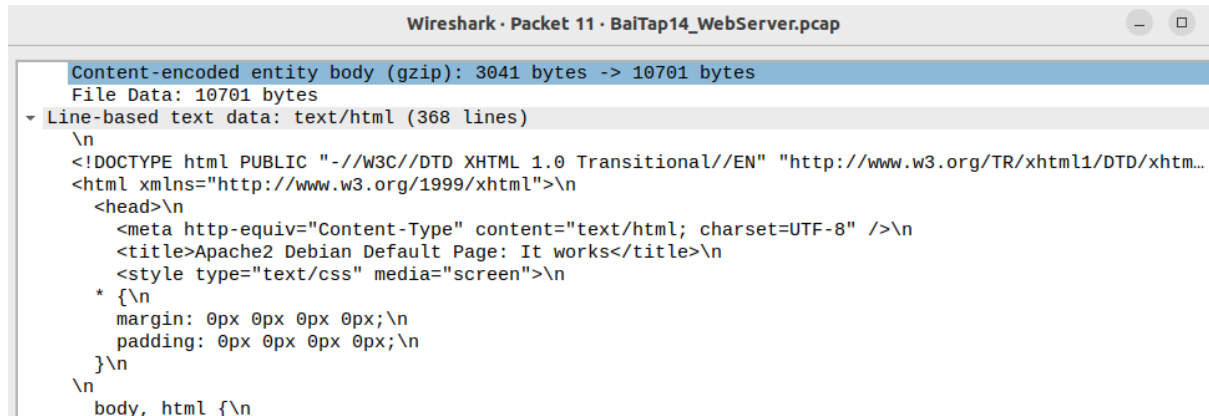
Ý nghĩa của các giá trị này như sau:

- Trường Seq (Sequence Number): Giá trị này đại diện cho số thứ tự của dữ liệu trong gói tin. Trong trường hợp này, giá trị Seq là 1, tức là gói tin này chứa dữ liệu có số thứ tự bắt đầu từ 1.
- Trường Ack (Acknowledgment Number): Giá trị này đại diện cho số thứ tự của gói tin mà bên nhận mong muốn nhận được từ bên gửi. Trong trường hợp này, giá trị Ack là 608, tức là bên nhận mong muốn nhận gói tin có số thứ tự là 608.

Tổng quát, các giá trị Seq và Ack trong khung TCP này xác định vị trí của dữ liệu được gửi và nhận trong quá trình truyền tải thông tin giữa các bên trong kết nối TCP. Điều này giúp đảm bảo dữ liệu được gửi và nhận theo đúng thứ tự và không bị mất mát.

- Chọn khung vật lý của giao thức HTTP thứ 2: Dựa vào thông tin trong HTTP Header, hãy cho biết thông điệp HTTP trả lời có mã là bao nhiêu (200, 404, 502..)?
200

Thông tin của Web Server?

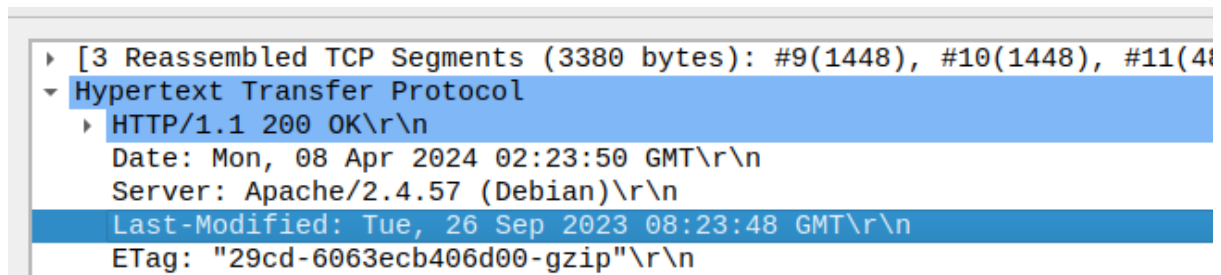


Wireshark · Packet 11 · BaiTap14_WebServer.pcap

```
Content-encoded entity body (gzip): 3041 bytes -> 10701 bytes
File Data: 10701 bytes
Line-based text data: text/html (368 lines)
  \n
  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml...
  <html xmlns="http://www.w3.org/1999/xhtml">\n
  <head>\n
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /\n
    <title>Apache2 Debian Default Page: It works</title>\n
    <style type="text/css" media="screen">\n
      * {\n
        margin: 0px 0px 0px 0px;\n
        padding: 0px 0px 0px 0px;\n
      }\n
    \n
  \n
  body, html {\n
```

Lần cập nhật cuối cùng nội dung trang web?

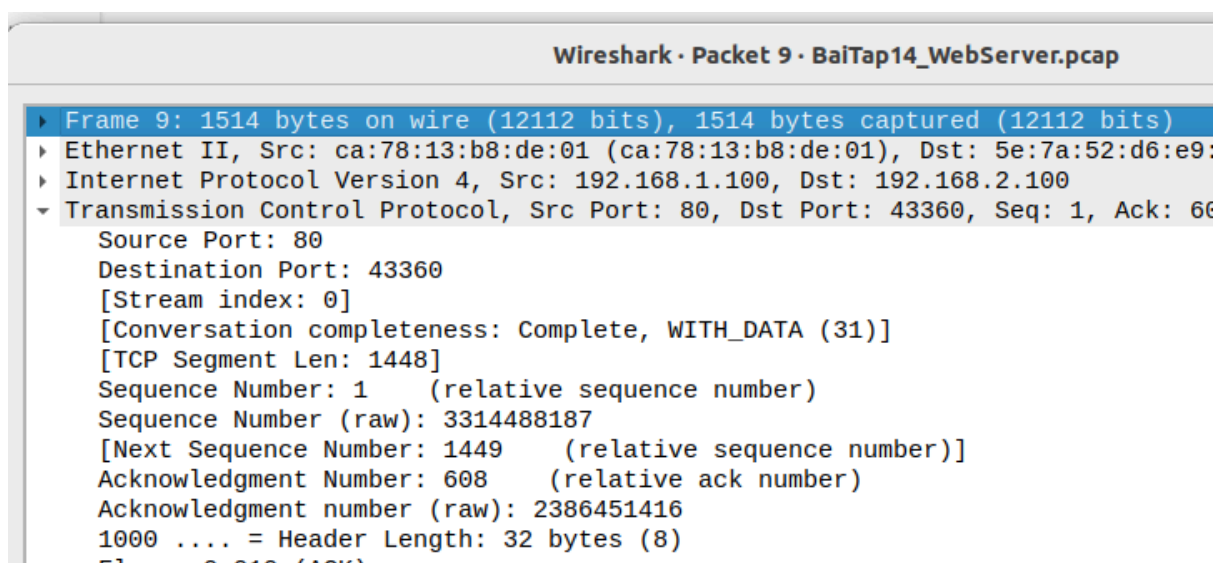
Tue, 26 Sep 2023 08:23:48 GMT



[3 Reassembled TCP Segments (3380 bytes): #9(1448), #10(1448), #11(488)]

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Mon, 08 Apr 2024 02:23:50 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
```

- Chọn khung vật lý của giao thức TCP tiếp theo (Khung TCP thứ 5): Giá trị trường Seq và Ack của khung này là bao nhiêu? Có ý nghĩa gì?



Wireshark · Packet 9 · BaiTap14_WebServer.pcap

```
Frame 9: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: ca:78:13:b8:de:01 (ca:78:13:b8:de:01), Dst: 5e:7a:52:d6:e9:00 (5e:7a:52:d6:e9:00)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.2.100
Transmission Control Protocol, Src Port: 80, Dst Port: 43360, Seq: 1, Ack: 608
  Source Port: 80
  Destination Port: 43360
  [Stream index: 0]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 1448]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 3314488187
  [Next Sequence Number: 1449 (relative sequence number)]
  Acknowledgment Number: 608 (relative ack number)
  Acknowledgment number (raw): 2386451416
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x010 (ACK)
```

Trong khung vật lý của giao thức TCP thứ năm, giá trị của trường Seq (Sequence Number) là 1 và giá trị của trường Ack (Acknowledgment Number) là 608.

Ý nghĩa của các giá trị này như sau:

- Trường Seq (Sequence Number): Giá trị này đại diện cho số thứ tự của dữ liệu trong gói tin. Trong trường hợp này, giá trị Seq là 1, tức là gói tin này chứa dữ liệu có số thứ tự bắt đầu từ 1.
- Trường Ack (Acknowledgment Number): Giá trị này đại diện cho số thứ tự của gói tin mà bên nhận mong muốn nhận được từ bên gửi. Trong trường hợp này, giá trị Ack là 608, tức là bên nhận mong muốn nhận gói tin có số thứ tự là 608.

Tổng quát, các giá trị Seq và Ack trong khung TCP này xác định vị trí của dữ liệu được gửi và nhận trong quá trình truyền tải thông tin giữa các bên trong kết nối TCP. Điều này giúp đảm bảo dữ liệu được gửi và nhận theo đúng thứ tự và không bị mất mát.

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

Gói tin TCP với cờ FIN (Finish) được sử dụng để kết thúc một kết nối TCP giữa hai máy tính. Cụ thể, gói tin này được gửi từ một bên (thông thường là bên gửi dữ liệu cuối cùng) đến bên kia để yêu cầu kết thúc kết nối TCP.

Quá trình giải phóng 3 chiều thường diễn ra như sau:

Bước 1 - Gửi FIN: Bên muốn kết thúc kết nối gửi một gói tin TCP với cờ FIN đến bên kia.

Bước 2 - Xác nhận FIN: Bên kia nhận được gói tin FIN và xác nhận nó bằng cách gửi lại một gói tin ACK. Gói tin ACK này thường có số thứ tự (sequence number) là số thứ tự của gói tin FIN cộng với 1.

Bước 3 - Gửi FIN và ACK: Sau khi xác nhận FIN, bên kia cũng muốn kết thúc kết nối, do đó nó gửi một gói tin TCP mới, có cờ FIN và cờ ACK được đặt. Điều này là để xác nhận việc đã nhận được FIN từ bên kia và đồng ý kết thúc kết nối.

Hoàn tất kết nối: Sau khi cả hai bên đều đã gửi và nhận gói tin FIN và ACK, kết nối TCP được coi là đã được kết thúc và các tài nguyên liên quan có thể được giải phóng.

Vậy nhiệm vụ của gói tin TCP (FIN) trong giao thức giải phóng 3 chiều là báo hiệu cho bên kia biết rằng bên gửi muốn kết thúc kết nối và bắt đầu quá trình đóng kết nối TCP.

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

1. Khung gửi FIN từ PC đến WebServer.
2. Khung ACK xác nhận FIN từ WebServer đến PC.
3. Khung gửi FIN và ACK từ WebServer đến PC.

4. Khung ACK xác nhận FIN từ PC đến WebServer.

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 giống bài tập 14

Câu hỏi 3:

Chọn khung thứ nhất với giao thức DNS và mở User Diagram Protocol Header, trả lời các câu hỏi:

DNS Client trên PC hoạt động ở cổng bao nhiêu?

33538

Name Server trên DNSServer hoạt động cổng bao nhiêu?

53

Giá trị của trường Length là bao nhiêu?

37

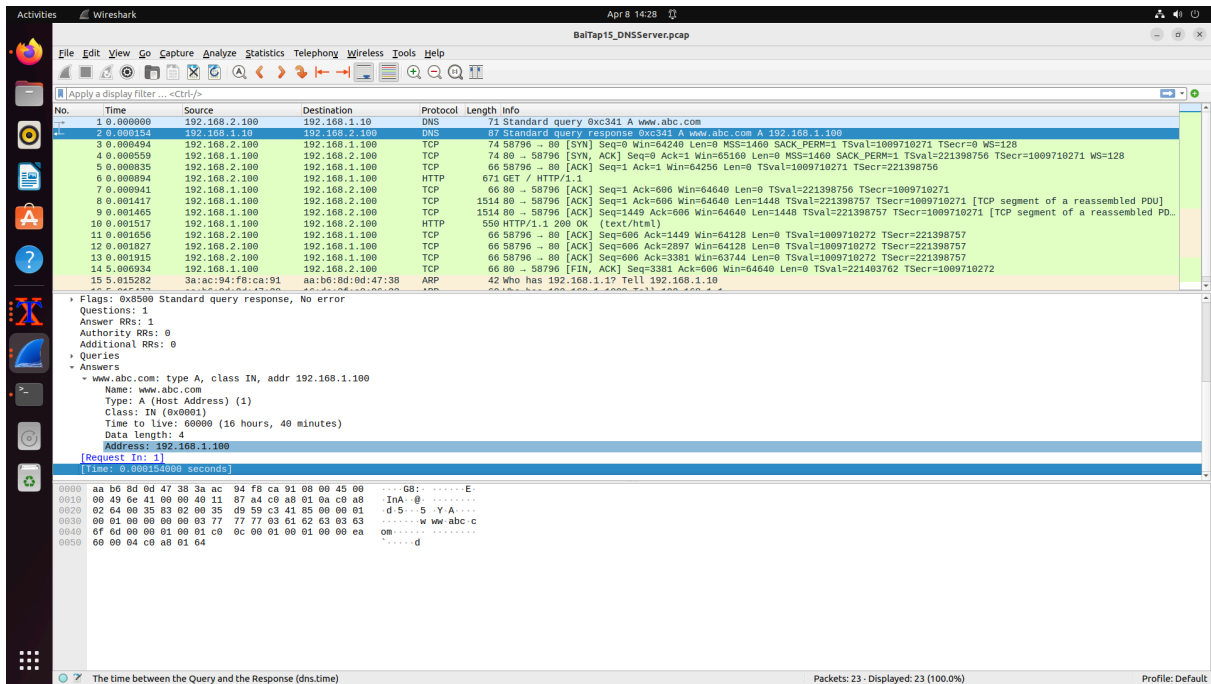
Mở phần Domain Name System (query), nội dung query là gì?

Query có thông tin truy vấn www.abc.com có các thông tin như type là A, Chiều dài tên là 12, Label Coun là 3

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

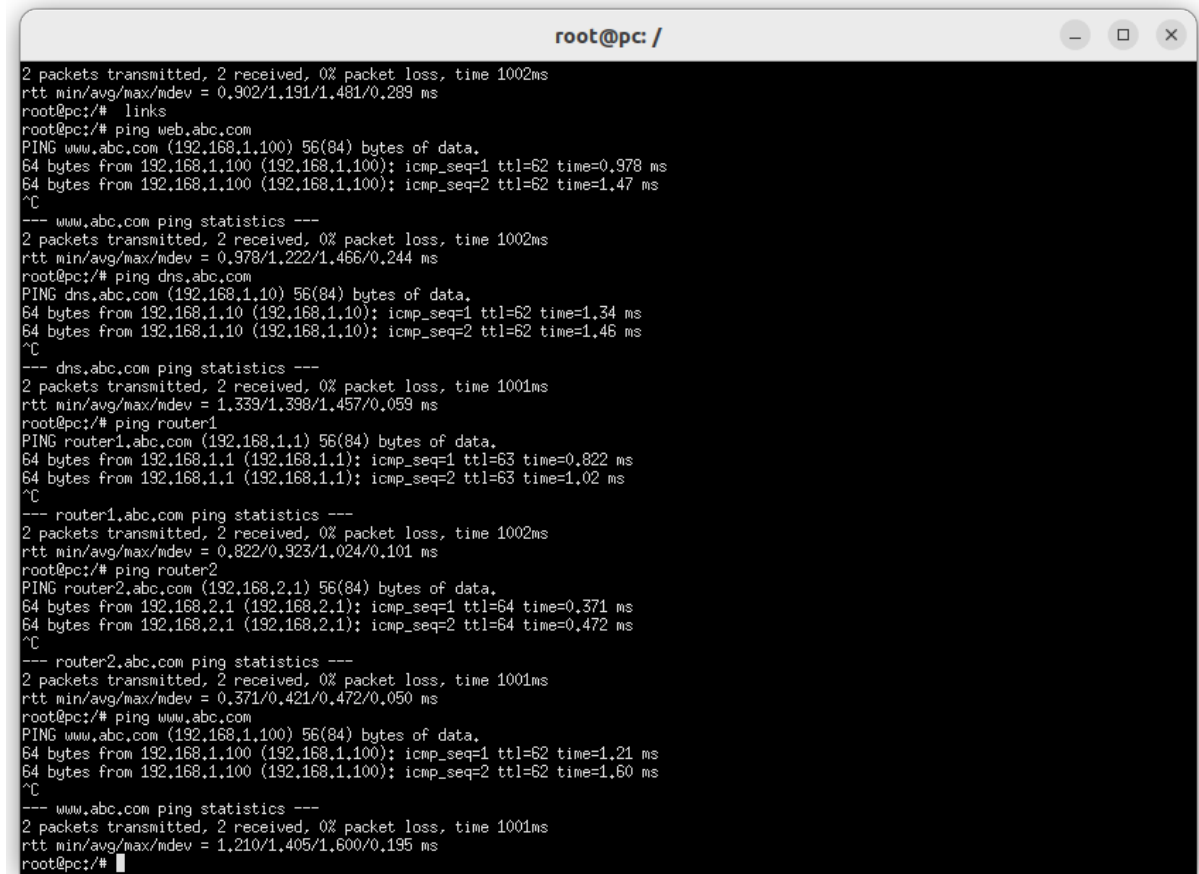
Nội dung phần Answers là gì?

Được trả lời từ server có ip là 192.168.1.100, có type A và thời gian sống 16 giờ, 40 phút và có Data length là 4, có request in là 1 (đây là request của DNS đầu tiên), có thời gian thực thi là 0.000154000 giây



Nội dung phần Authoritative Nameservers là gì?

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



Kết quả đều nhận được reply của các router và tên miền của webserver, điều này chứng tỏ các cấu hình đều hoạt động tốt