1

Lab

**BÁO CÁO BÀI THỰC HÀNH SỐ 1**

**Làm quen với Wireshark**

Wireshark Getting Started

**Môn học: Nhập môn Mạng máy tính**

|  |  |
| --- | --- |
| **Sinh viên thực hiện** | Dương Thuận Trí (22521517) |
| **Thời gian thực hiện** | 25/10/2023 – 1/11/2023 |
| **Tự chấm điểm** | 10/10 |

**TRẢ LỜI CÁC CÂU HỎI**

**Câu 1:**

|  |  |
| --- | --- |
| IP address | 192.168.222.186 |
| MAC address | 98-FA-9B-12-13-EC |
| Default gateway IP address | fe80::1a0f:76ff:fe92:f408%16  192.168.222.1 |
| DNS server IP address | 192.168.54.4  192.168.20.4 |

**Câu 2: Tại danh sách các gói tin bắt được, định vị gói tin truy vấn domain google.com. Gợi ý: chứa “standard query” và “A** [**www.google.com**](http://www.google.com)**”**

* Trả lời: Gói tin truy vấn domain google.com là gói tin số 346 có Source là 192.168.222.186 ( IP address của máy) và Destination là 192.168.54.4 ( IP address của DNS server)



**Câu 3: Định vị gói tin phản hồi của truy vấn trên? Từ thông điệp trả lời, ghi lại địa chỉ IP của domain google.com**

* Gói tin phản hồi của truy vấn trên là gói tin số 347, chứa thông điệp trả lời (Answers).



* A screenshot of a computer

  Description automatically generatedĐịa chỉ IP của domain google.com là 142.251.220.14

**Câu 4: Chọn một gói tin DNS, xác định các trường (field) có trong UDP header và giải thích ý nghĩa của mỗi trường đó?**

A screenshot of a computer

Description automatically generated

* Các trường có trong UDP header là Source Port, Destination Port, Length, Checksum:

+ Sources Port: cổng của người gửi thông tin

+ Destination Port: cổng nhận thông tin

+ Length: chiều dài của toàn bộ datagram (header và dữ liệu)

+ Checksum: dùng để kiểm tra lỗi của header và dữ liệu.

**Câu 5: Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của mỗi trường trong UDP header?**

* Sources Port: 2 bytes
* Destination Port: 2 bytes
* Length: 2 bytes
* A screenshot of a computer

  Description automatically generatedChecksum: 2 bytes.

**Câu 6: Giá trị của trường Length trong UDP header là độ dài của gì? Chứng minh nhận định này**

* A screenshot of a computer

  Description automatically generatedGiá trị của trường Length trong UDP header là độ dài của toàn bộ datagram, bao gồm: phần header và dữ liệu

**Câu 7: Quan sát 2 gói tin tìm được ở Câu 1 và 2, mô tả mối quan hệ giữa các địa chỉ IP và port number của 2 gói tin này.**

* Gói tin truy vấn domain có địa chỉ IP đích là địa chỉ IP của DNS server, và gói tin phản hồi được gửi từ DNS server có địa chỉ IP đích là máy tính đang sử dụng.
* A screenshot of a computer

  Description automatically generatedPort number cũng tương tự: Source port của gói tin truy vấn domain là 49735, Destination Port là 53 ( 53 chính là port number của DNS server), ở gói tin phản hồi, Destination Port mà DNS server gửi tới chính là port number của máy tính đã gửi truy vấn.

A screenshot of a computer

Description automatically generated

**Câu 8: Xác định IP và TCP port của client sử dụng để chuyển tệp sang gai.cs.umass.edu là gì?**

* IP: 192.168.222.186
* A screenshot of a computer

  Description automatically generatedTCP port: 51445

**Câu 9: Địa chỉ của gaia.cs.umass.edu là gì? Trên số cổng nào nó gửi và nhận các segment TCP cho kết nối này?**

* Địa chỉ của gais.cs.umass.edu là 128.119.245.12
* gais.cs.umass.edu có số cổng gửi là 51445, số cổng nhận là 80.A screenshot of a computer

  Description automatically generated

**Câu 10: TCP SYN segment (gói tin TCP có cờ SYN) sử dụng sequence number nào để khởi tạo kết nối TCP giữa client và server? Thành phần nào trong segment cho ta biết segment đó là TCP SYN segment? Gợi ý: quan sát trường Flags**

* TCP SYN segment sử dụng sequence number 0 để khởi tạo kết nối TCP giữa client và server.
* Kế bên trường Flags, tên segment được đề cập là SYN. ( và trường SYN được bật trong Flags)

A screenshot of a computer

Description automatically generated

**Câu 11: Tìm sequence number của gói tin SYN/ACK segment được gửi bởi server đến client để trả lời cho SYN segment?**

* Sequence number của gói tin SYN/ACK segment là 0 ( cùng sequence number với SYN segment)

**Câu 12: Tìm giá trị của Acknowledgement trong SYN/ACK segment? Làm sao server có thể xác định giá trị đó? Thành phần nào trong segment cho ta biết segment đó là SYN/ACK segment?**

* Giá trị của của Acknowledgement trong SYN/ACK segment là 1.
* Server lấy Sequence number cộng thêm 1 để xác định giá trị ACK.
* A screenshot of a computer

  Description automatically generatedKế bên trường Flags, tên segment được đề cập là SYN/ACK segment.

**Câu 13: Tìm độ dài của từng segment trong bộ 6 segments đầu tiên trên? Tìm lượng buffer còn trống nhỏ nhất mà bên nhận thông báo cho bên gửi**

* A screenshot of a computer

  Description automatically generated6 segments đầu tiên đều có độ dài là 54
* A screenshot of a computer

  Description automatically generatedLượng buffer trống nhỏ nhất bên nhận thông báo cho bên gửi là 229

**Câu 14: Có segment nào được gửi lại hay không? Thông tin nào trong quá trình truyền tin cho chúng ta biết điều đó?**

* Có, khi kiểm tra trong Time-Sequence-Graph(Steven), biểu đồ cho thấy có nhiều gói tin cùng một Sequence Number nhưng được gửi nhiều lần.
* A screenshot of a computer

  Description automatically generated