Lab 3

Phân tích hoạt động giao thức TCP - UDP

TCP/UDP Protocol

Môn học: Nhập môn Mạng máy tính

Tháng 03/2024

Lưu hành nội bộ

A. TỔNG QUAN

1. Mục tiêu

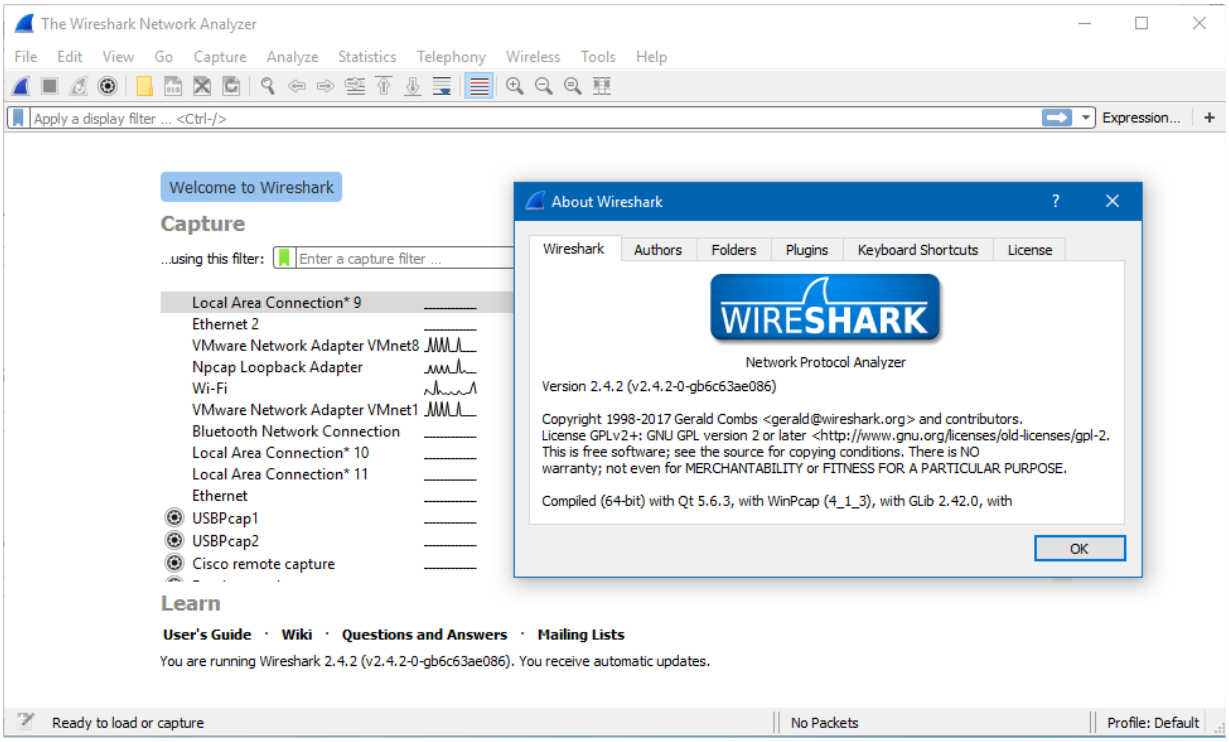
- Tìm hiểu cách thực hiện một truy vấn DNS và các đặc điểm của giao thức UDP.
- Sử dụng Wireshark để bắt các gói tin khi truy vấn DNS và truy cập website http để tiến hành phân tích các đặc điểm của gói tin UDP và TCP.
- Tìm hiểu việc TCP sử dụng sequence number và acknowledgement number để có thể truyền dữ liệu tin cậy.

2. Kiến thức tổng quan

- Kiến thức về giao thức TCP – UDP của chương Transport.

3. Môi trường & công cụ thực hành

- Một máy tính có kết nối Internet sử dụng hệ điều hành Windows/Linux.
- Phần mềm **Wireshark:** *Sinh viên có thể tải về miễn phí phiên bản mới nhất theo hướng dẫn tại https://www.wireshark.org/download.html*



Hình 1. Giao diện chính của phần mềm Wireshark 2.4.2

B. THỰC HÀNH

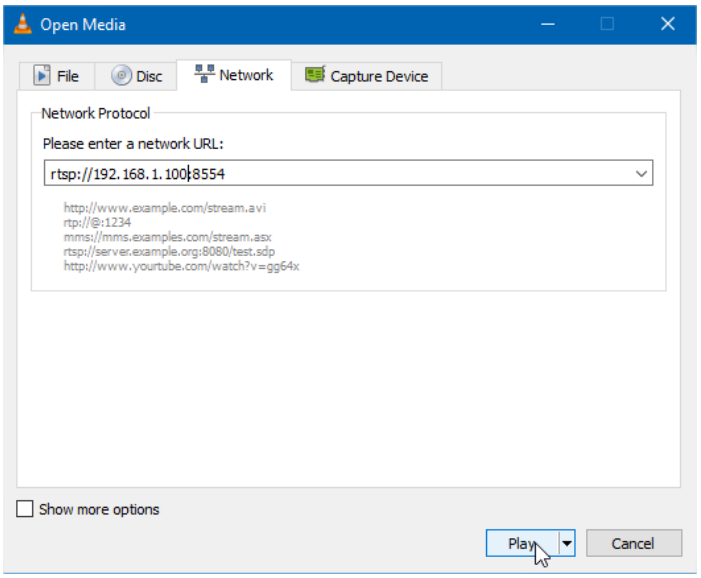
1. Task 1: Phân tích tổng quan giao thức TCP và UDP

1.1 Phân tích, bắt gói tin khi xem streaming video lần 1

- **Bước 1:** Mở Wireshark và bắt đầu bắt gói tin.
- **Bước 2:** Truy cập để xem video từ 1 máy server bằng cách mở phần mềm VLC » Chọn Open network stream.

  Nhập địa chỉ theo định dạng **rtsp://[địa chỉ IP server]:8554/**

  Ví dụ khi IP của server là **192.168.1.100**:
  *Địa chỉ IP của server sẽ được cung cấp trên lớp.



Hình 2. Chọn Play để bắt đầu xem video đang được streaming từ Server

- **Bước 3:** Quan sát Video được hiển thị.
- **Bước 4:** Kết thúc bắt gói tin bằng Wireshark.

1.2 Phân tích kết quả thu được lần 1

Tìm hiểu 1: Mô tả kết quả quan sát được khi xem Video khi xem streaming từ Server?

Tìm hiểu 2: Tìm trong file Wireshark thu được, quá trình streaming ở kịch bản này sử dụng giao thức UDP hay TCP?

1.3 Phân tích, bắt gói tin khi xem streaming video lần 2

- **Bước 1:** Mở Wireshark và bắt đầu bắt gói tin.

- **Bước 2:** Truy cập để xem video từ 1 máy server bằng cách mở phần mềm VLC » Chọn Open network stream.

  Nhập địa chỉ theo định dạng **http://[địa chỉ IP server]:8080/**
- **Bước 3:** Quan sát Video được hiển thị.
- **Bước 4:** Kết thúc bắt gói tin bằng Wireshark.

1.4 Phân tích kết quả thu được lần 2

Tìm hiểu 3: Mô tả kết quả quan sát được khi xem Video khi xem streaming từ Server?

Tìm hiểu 4: Tìm trong file Wireshark thu được, quá trình streaming ở kịch bản này sử dụng giao thức UDP hay TCP?

Tìm hiểu 5: Phân tích sự khác nhau giữa 2 lần xem streaming Video.

2. Task 2: Phân tích hoạt động giao thức UDP

2.1 Thực hiện truy vấn DNS và bắt các gói tin UDP

DNS là một trong những giao thức tầng ứng dụng sử dụng cả **UDP** và **TCP** ở Tầng Vận chuyển (Transport). **DNS** là viết tắt của cụm từ Domain Name System, mang ý nghĩa đầy đủ là hệ thống phân giải tên miền. Hiểu một cách ngắn gọn nhất, DNS cơ bản là một hệ thống chuyển đổi các tên miền website mà chúng ta đang sử dụng, ở dạng *www.tenmien.com* sang một địa chỉ IP dạng số tương ứng với tên miền đó và ngược lại.

➲ *Sinh viên ghi lại thông tin cấu hình IP của PC:*

Sử dụng lệnh **ipconfig /all** trong giao diện Command Prompt để tìm và ghi lại các thông tin sau vào bảng bên dưới:

Bảng 1. Ví dụ về các thông tin địa chỉ của PC

IPv4 Link-local IPv6 address	192.168.1.8 fe80::4923:18cd:8c3f:afbe
MAC address	14-DD-A9-BF-48-AB
Default gateway	fe80::1 192.168.1.1

DNS Servers	fe80::1 8.8.8.8

- **Địa chỉ MAC** (Physical Address) và **IP** (IPv4 và Link-local IPv6 Address) của card mạng mà sinh viên sử dụng để giao tiếp qua mạng (NIC).
- **Địa chỉ IP của các cổng mặc định** được chỉ định (Default gateway).
- **Địa chỉ IP của các máy chủ DNS** được chỉ định cho PC.

Tìm hiểu 6: Sinh viên tìm và điền vào bảng như mẫu ở trên.

➲ *Thực hiện bắt gói tin truy vấn và phản hồi của DNS:*

- **Bước 1:** Mở Command Prompt.
- **Bước 2:** Đảm bảo xóa DNS Cache bằng cách gõ lệnh **ipconfig /flushdns**
- **Bước 3:** Mở Wireshark và bắt đầu bắt gói tin.
- **Bước 4:** Từ Command Line, gõ **nslookup type=A uit.edu.vn** (hoặc 1 domain nào khác).
- **Bước 5:** Sau khi kết quả được hiển thị, ngưng bắt gói tin bằng Wireshark và lưu file với tên theo định dạng MSSV-**UDP.pcapng** *(sẽ nộp kèm báo cáo).*

1. Thông qua hướng dẫn, tìm hiểu và trình bày lại về sự khác nhau cơ bản, ưu điểm, nhược điểm của UDP và TCP. Thông qua việc xem streaming Video, tìm hiểu và trình bày Tìm hiểu 1, 2, 3, 4, 5. Tìm và thực hiện Tìm hiểu 6 để sử dụng làm thông tin, góp phần hiểu rõ hơn các nội dung về DNS và TCP ở bên dưới.

2.2 Phân tích hoạt động giao thức UDP

Mở file Wireshark đã bắt được ở Task 2 ở trên, lọc các gói "dns" và trả lời các câu hỏi sau:

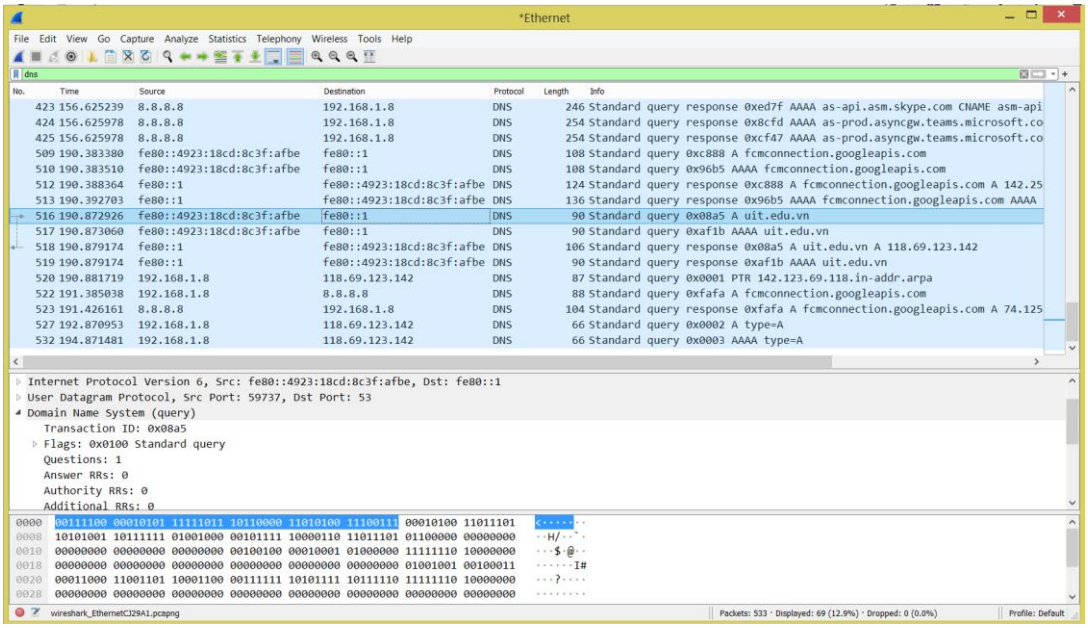
2. Tại danh sách các gói tin bắt được, tìm gói tin truy vấn domain **uit.edu.vn** (hoặc domain đã chọn ở Task 2, bước 4 ở trên).

   Gợi ý: chứa "*standard query*" và "*A uit.edu.vn*".

3. Xác định gói tin phản hồi của truy vấn trên? Từ thông điệp phản hồi, ghi lại **địa chỉ IP** của domain **uit.edu.vn**
4. Chọn một gói tin UDP, xác định các trường (*field*) có trong UDP header và giải thích ý nghĩa của mỗi trường đó? **Gợi ý**: Xem tại phần User Datagram Protocol.
5. Qua thông tin hiển thị của Wireshark, xác định độ dài (*tính theo byte*) của mỗi trường trong UDP header?
6. Giá trị của trường **Length** trong UDP header là độ dài của gì? Chứng minh nhận định này?
7. Số bytes lớn nhất mà **payload** *(phần chứa dữ liệu gốc, không tính UDP header và IP header)* của UDP có thể chứa?

   Gợi ý: Dựa vào kích thước của trường Length trong UDP header và giá trị lớn nhất có thể thể hiện.
8. Giá trị lớn nhất có thể có của port nguồn *(Source port)?*
9. Quan sát 2 gói tin tìm được ở câu 2 và 3, mô tả mối quan hệ giữa các địa chỉ IP và các port của 2 gói tin này.

   Gợi ý: Quan sát **Source (IP, Port)** và **Destination (IP, Port)** của 2 gói tin trên.
10. Chọn 1 gói tin UDP, dựa trên các thông tin của gói tin này và tính UDP Checksum. So sánh kết quả tự tính toán và trường Checksum của gói tin UDP. Giải thích cách tính.



Hình 3. Ví dụ về phân tích gói tin UDP

3. Task 3: Phân tích hoạt động giao thức TCP

3.1 Truy cập website và bắt các gói tin TCP

- **Bước 1:** Xóa Cache của trình duyệt sử dụng.
- **Bước 2:** Mở Wireshark và bắt đầu bắt gói tin.
- **Bước 3:** Sử dụng trình duyệt, truy cập đến địa chỉ sau: http://www.celuit.edu.vn/
- **Bước 4:** Sau khi website đã hiển thị đầy đủ, ngưng bắt gói tin bằng Wireshark và lưu file với tên theo định dạng MSSV-**TCP.pcapng**. *(sẽ nộp kèm báo cáo).*

3.2 Phân tích hoạt động giao thức TCP

Mở file Wireshark đã bắt được trong Task 3 ở trên, lọc các gói "tcp" và trả lời các câu hỏi sau:

11. Tìm địa chỉ IP và TCP port của máy Client?
12. Tìm địa chỉ IP của Server? Nó sử dụng port nào để nhận các **segments**?
13. Tìm TCP SYN segment *(gói tin TCP có cờ SYN)* 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.

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

    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?

15. Chỉ ra 6 segment đầu tiên mà server gửi cho Client *(dựa vào Số thứ tự gói – No)*

    - Tìm sequence number của 6 segments đầu tiên đó?
    - Xác định thời gian mà mỗi segment được gửi, thời gian ACK cho mỗi segment được nhận?
    - Đưa ra sự khác nhau giữa thời gian mà mỗi segment được gửi và thời gian ACK cho mỗi segment được nhận bằng cách tính RTT *(Round Trip Time)* cho 6 segments này?

> ***Round-trip time (RTT)*** *là khoảng thời gian tính từ lúc máy tính bắt đầu gửi segment cho đến khi nó nhận được ACK trả về tương ứng. Xem thêm tại Slide Chương Transport.*

Lưu ý: *Lập bảng thống kê và tính các giá trị thời gian trên theo dạng:*

STT	Thời gian	RTT	SEQ number	ACK number	Phân loại
					Gói tin Gửi / Nhận ACK

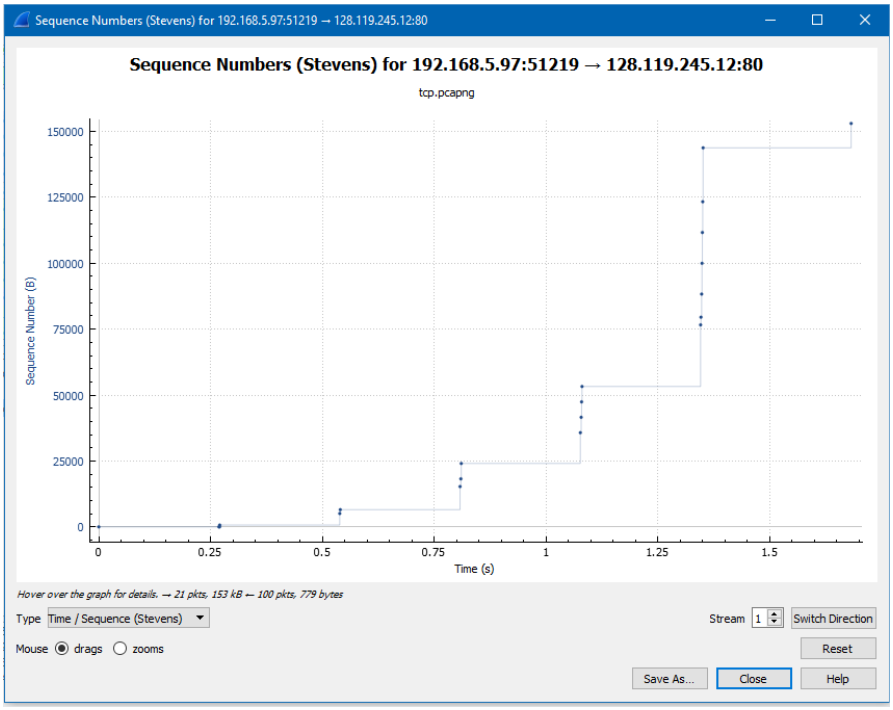
**Cần minh chứng rõ ràng bằng hình ảnh, xác định bằng các gói tin thu thập được.*

16. Có segment nào được gửi lại hay không? Thông tin nào trong quá trình truyền tin cho chúng ta biết điều đó? Giải thích.

Gợi ý: *Để kiểm tra lượng dữ liệu được truyền trong một đơn vị thời gian, thay vì phải tự tính toán trực tiếp từ dữ liệu của các gói tin, ta sử dụng một tính năng của Wireshark – Time – Sequence – Graph (Steven)*

Chọn một segment bất kỳ trong phần danh sách các gói tin. Chọn ***Statistics » TCP Stream Graph » Time-Sequence-Graph(Steven).***

Ta sẽ thấy một biểu đồ tương tự như sau:



Hình 4. Ví dụ về biểu đồ Sequence Number (Stevens)

Mỗi chấm trong biểu đồ tượng trưng cho một TCP segment có sequence number tương ứng với thời gian segment đó được gửi đi. Lưu ý là một chồng các dấu chấm tương ứng với một chuỗi các gói tin được gửi liên tiếp nhau.

C. YÊU CẦU & ĐÁNH GIÁ

1. Yêu cầu

- Sinh viên tìm hiểu và thực hành theo hướng dẫn. Thực hiện **cá nhân.**
- Sinh viên báo cáo kết quả thực hiện và nộp bài bằng file. Trong đó:
  - Trình bày chi tiết quá trình thực hành của mình ở phần a,b và trả lời các câu hỏi ở 2 phần TCP và UDP *(kèm theo các ảnh chụp màn hình tương ứng).*

- Đính kèm các file *pcapng* từ Wireshark kết quả bắt được.
- Nộp báo cáo trên theo thời gian đã thống nhất tại website môn học.

Đặt tên file báo cáo theo định dạng như mẫu: **Mã lớp-LabX_MSSV** *Ví dụ: IT005.X11.1-Lab03_25520001* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

- Chi tiết các quy định, quy tắc đặt tên sinh viên xem lại mẫu báo cáo thực hành trên website môn học.

2. Đánh giá:

Sinh viên hiểu và tự thực hiện được bài thực hành, trả lời đầy đủ các yêu cầu đặt ra, khuyến khích trình bày báo cáo chi tiết, rõ ràng.

HẾT

Chúc các em hoàn thành tốt