TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN - ĐHQG-HCM
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG
FACULTY OF COMPUTER NETWORK AND COMMUNICATION

**MÔN HỌC:** NHẬP MÔN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 3

# GIAO THỨC UDP & TCP

## LAB 3 - UDP & TCP PROTOCOL

Tháng 10 năm 2018

# Lab 1 – UDP & TCP Protocol

## 1 TỔNG QUAN

### 1.1 Mục tiêu

- Bắt và phân tích các đặc điểm của các gói tin của giao thức UDP.
- Bắt và phân tích các đặc điểm của các gói tin của giao thức TCP

### 1.2 Môi trường thực hành

- Máy tính cá nhân có kết nối Internet
- Công cụ bắt gói tin Wireshark https://www.wireshark.org/

## 2 THỰC HÀNH VỚI WIRESHARK

### 2.1 Tìm hiểu giao thức UDP

Tầng vận chuyển (Transport) cung cấp 2 giao thức cơ bản là **UDP** và **TCP** – được sử dụng trong hầu hết các ứng dụng về Mạng.

**UDP (User Datagram Protocol)** là loại giao thức phi kết nối, không đảm bảo tính tin cậy khi truyền dữ liệu và không có cơ chế phục hồi dữ liệu

#### 2.1.1 Ghi lại thông tin cấu hình IP của PC

Sử dụng lệnh **ipconfig / all** trong giao diện Command line của bạn để tìm và ghi lại các thông tin sau:

+ Địa chỉ MAC và IP của card mạng mà sinh viên sử dụng để giao tiếp qua mạng (NIC)

+ Địa chỉ IP của cổng mặc định được chỉ định (Default gateway)

+ Địa chỉ IP máy chủ DNS được chỉ định cho PC

Ghi lại thông tin này trong bảng được cung cấp. Thông tin này sẽ được sử dụng trong các phần sau của bài lab này để phân tích các gói tin.

# Lab 1 – UDP & TCP Protocol

| | |
|---|---|
| IP address | 192.168.222.186 |
| MAC address | |
| Default gateway IP address | fe80::1a0f:76ff:fe92:f408%16<br>192.168.222.1 |
| DNS server IP address | |

### 2.1.2 Sử dụng Wireshark, bắt các gói tin truy vấn và phản hồi của DNS

***Bước 1.*** Khởi động phần mềm Wireshark

***Bước 2.*** Chọn capture từ Interface đã ghi lại trong phần 1

***Bước 3.*** Từ Command Line, gõ **nslookup google.com** (hoặc 1 domain nào khác)

***Bước 4.*** Dừng bắt gói tin

***Bước 5.*** Lưu file capture lại dưới dạng **MSSV-UDP.pcapng** (sẽ nộp kèm báo cáo)

### 2.1.3 Phân tích các gói tin UDP hoặc DNS đã bắt

Trong phần này, bạn sẽ quan sát các gói tin UDP được tạo ra khi giao tiếp với 1 DNS Server để truy vấn địa chỉ IP cho domain **google.com**.

***Bước 1.*** Mở lại file capture ở trên

***Bước 2.*** Trong cửa sổ chính Wireshark, gõ **dns** trong vùng nhập của Bộ lọc Filter. Nhấp vào **Áp dụng** hoặc nhấn Enter.

Trả lời các câu hỏi sau:

# Lab 1 – UDP & TCP Protocol

**Câu 1.** Điền thông tin vào bảng sau

| | |
|---|---|
| IP address | |
| MAC address | |
| Default gateway IP address | |
| DNS server IP address | |

**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**".

**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

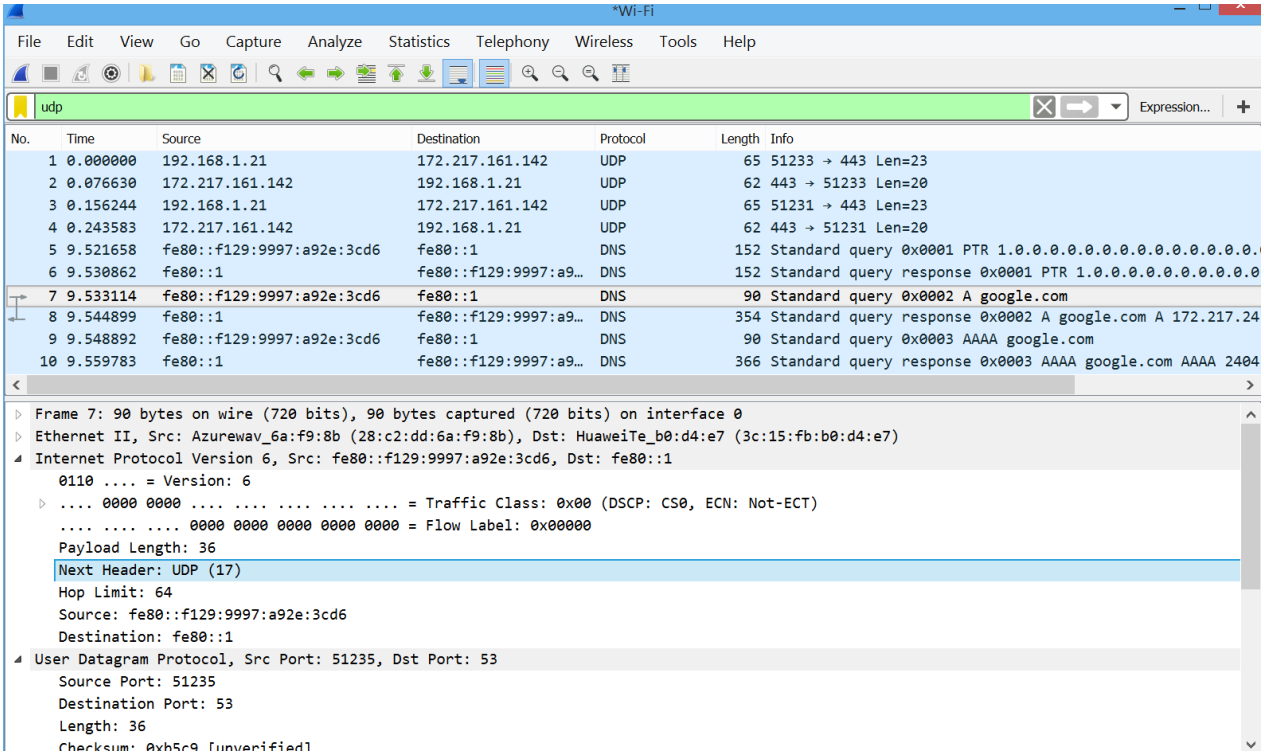
**Câu 4.** Chọn một gói tin DNS, xác định các trường (field) có trong UDP header và giải thích ý nghĩa của mỗi trường đó? ***Gợi ý:*** *Xem tại phần User Datagram Protocol*

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

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

**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.

# Lab 1 – UDP & TCP Protocol




***Hình 1. Ví dụ về phân tích gói tin truy vấn DNS***

## 2.2 Tìm hiểu giao thức TCP

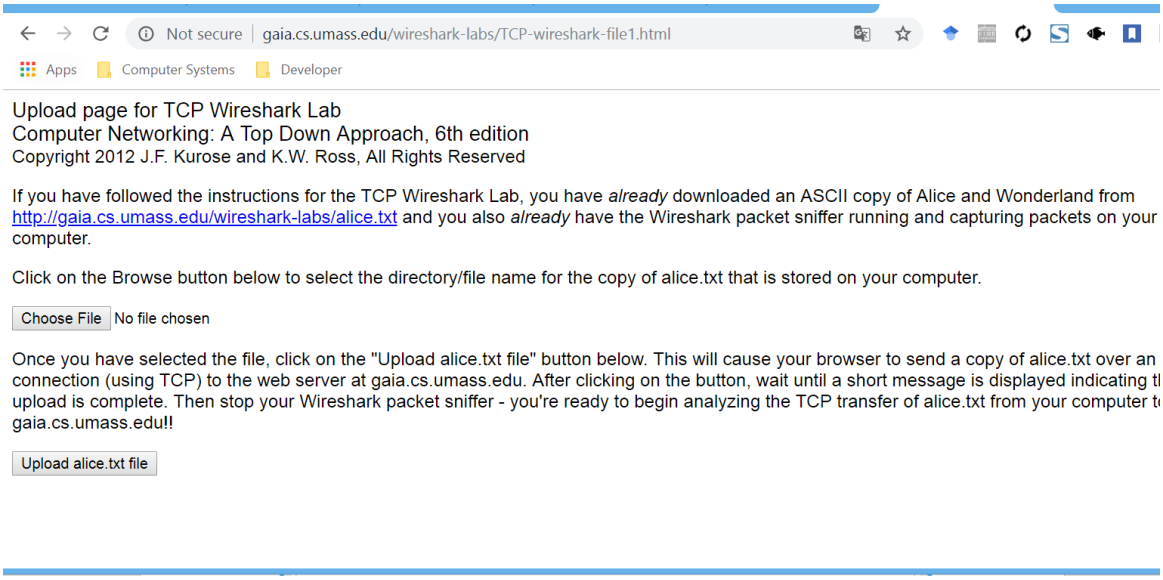
### 2.2.1 Upload file thông qua Web Browser (HTTP) và bắt các gói tin TCP

Thực hiện các bước sau

***Bước 1.*** Khởi động Web browser (Có thể lựa chọn bất kỳ Browser như Google, Firefox, Safari, IE, Edge, …)

***Bước 2.*** Truy cập http://gaia.cs.umass.edu/wireshark-labs/alice.txt và lấy bản sao ASCII của Alice in Wonderland. Lưu trữ tệp này trên máy tính của bạn

***Bước 3.*** Tiếp theo, truy cập http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html. Giao diện như hình bên dưới




***Hình 2: Giao diện Upload file (sử dụng TCP)***

***Bước 4.*** Sử dụng nút **Browse/Choose File** trong trang web để chọn file alice.txt vừa download. Lưu ý: Chưa nhấn nút Upload alice.txt file

***Bước 5.*** Mở phần mềm Wireshark và bắt đầu bắt gói tin trên card mạng đang sử dụng kết nối Internet.

***Bước 6.*** Quay lại trình duyệt, nhấn nút Upload alice.txt file để upload file lên server. Khi file đã được upload, một tin nhắn chúc mừng sẽ xuất hiện trên trình duyệt.

***Bước 7.*** Dừng bắt gói tin ở Wireshark và lưu thành file với tên theo dạng *MSSV-TCP.pcapng* (sẽ nộp kèm báo cáo).

### 2.2.2 Phân tích các gói tin TCP đã bắt được

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

***Câu 8.*** Xác định IP và TCP port của client sử dụng để chuyển tệp sang gaia.cs.umass.edu là gì? **Gợi ý**: *Chọn một thông điệp HTTP và khám phá các chi*

*tiết của gói tin TCP được sử dụng để mang thông điệp HTTP này*

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

***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.

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

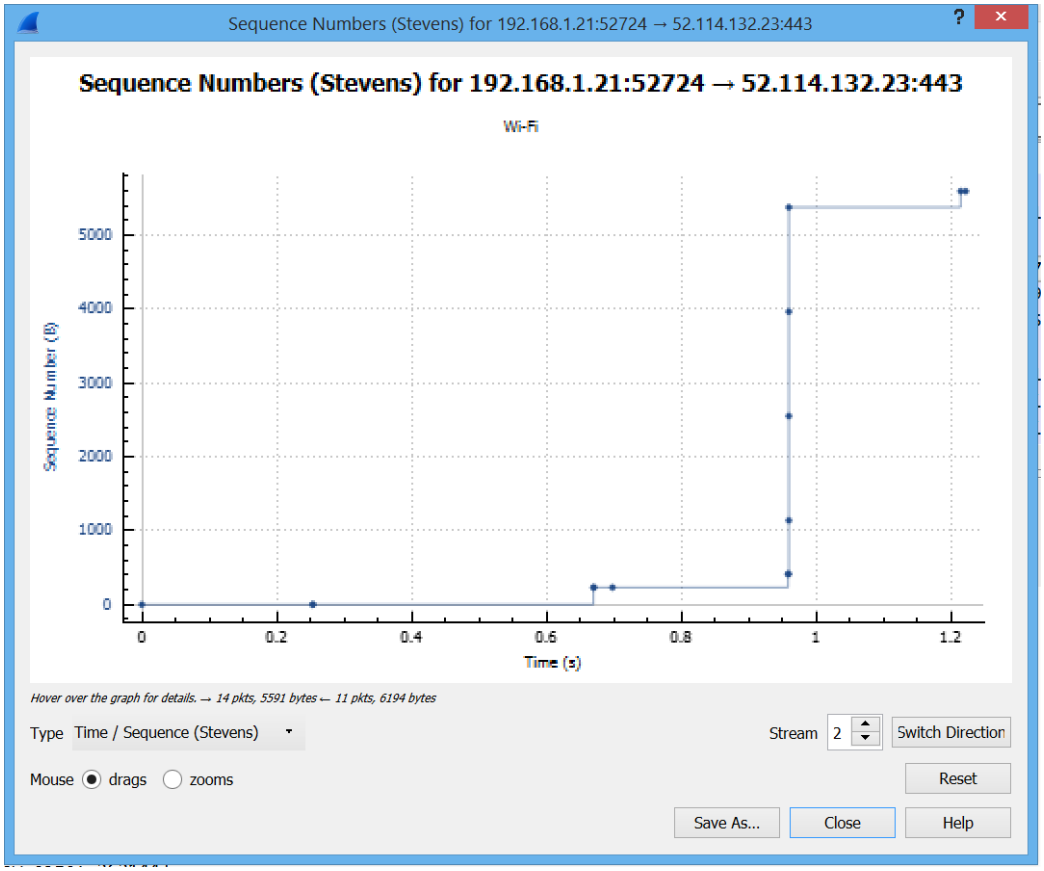
***Câu 13.*** Tìm độ dài của từng segment trong bộ 6 segments đầu tiên trên? Tìm lượng buffer còn trống nhỏ nhất mà bên nhận thông báo cho bên gửi trong suốt truyền tin? ***Gợi ý:*** Buffer còn trống = giá trị Calculated window size (Win) trong các gói ACK mà server báo về bên gửi. Kiểm tra trong tất cả các gói chứa ACK từ server trả về máy tính để xác định giá trị nhỏ nhất. Có thể chỉ lọc các gói từ server bằng cách thêm điều kiện filter "*tcp and ip.src==IP của server*"

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

*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 3. 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*

***Câu 15.*** Tính thông lượng (throughput – byte/s) của kết nối TCP? Giải thích cách tính thông lượng.

*Gợi ý (tham khảo Slide môn học)*

| |
|---|
| Thông lượng trung bình của 1 kết nối = **(0,75*W)/RTT** |
| **W**: windown size (bytes) = Tổng dữ liệu được truyền |
| **RTT**: round trip time (seconds) = Thời gian truyền |

# 3 NỘP BÀI

Sinh viên thực hiện Bài thực hành, viết báo cáo quá trình, và trả lời các câu hỏi, tất cả lưu vào 1 File Báo cáo.

Nộp bài theo hình thức **cá nhân**

Kết quả nộp lại:

- File báo cáo
- File capture. pcapng

Lưu ý: Đặt tất cả vào 1 folder, nén lại và đặt tên theo định dạng như mẫu:

Mã lớp_MSSV_HoTen_LabX

Ví dụ: Lop1_17521006_NguyenVanA_Lab3