TRƯỜNG ĐẠI HỌC CẦN THƠ **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
KHOA CÔNG NGHỆ THÔNG TIN & TT **Độc lập – Tự do – Hạnh phúc**

ĐỀ CƯƠNG CHI TIẾT

Môn học: Thực hành Mạng máy tính

Mã môn học: CT112, số tín chỉ: 3

Học kỳ áp dụng: Học kỳ II, năm học 2016-2017

Số tiết: 30 tiết (5 buổi), thi Thực hành vào buổi thứ 6

A. NỘI DUNG VÀ MỤC TIÊU MÔN HỌC

Phần thực hành Mạng máy tính hướng đến mục tiêu xây dựng các bài tập thực hành theo từng chủ đề liên quan đến các kiến thức đã được giới thiệu trong phần Lý thuyết. Thông qua các bài tập này, sinh viên thiết kế và phân tích được các hệ thống mạng khác nhau, các giao thức khác nhau, cách thức truyền tải dữ liệu khác nhau….

Phần thực hành Mạng máy tính chia làm 5 buổi với nội dung các buổi như sau:

- Buổi 1: Làm quen Netkit Emulator, công cụ xây dựng hệ thống mạng ảo. Làm quen Wireshark, công cụ bắt gói tin và phân tích dữ liệu trên gói tin bắt được.
- Buổi 2: Xây dựng hệ thống mạng sử dụng phương pháp vạch đường tĩnh, minh hoạ giao thức ARP kết hợp với sử dụng Wireshark để phân tích gói dữ liệu.
- Buổi 3: Xây dựng hệ thống mạng sử dụng giao thức vạch đường động (RIPv2 và OSPFv2). Phân tích dữ liệu với Wireshark để nhận biết khuôn dạng dữ liệu trao đổi, cập nhật bảng vạch đường của các router...
- Buổi 4: Sử dụng Wireshark để làm rõ giao thức bắt tay 3 chiều của TCP và UDP trên tầng vận chuyển. Khảo sát cơ chế điều khiển thông lượng.
- Buổi 5: Xây dựng hệ thống mạng minh hoạ cho hệ thống phân giải tên miền DNS và WebMail server.

B. PHƯƠNG PHÁP GIẢNG DẠY

- Sinh viên cần đọc trước nội dung của buổi thực hành và các kiến thức liên quan.
- Sinh viên cần hoàn thành các bài tập về nhà của buổi thực hành.
- Sinh viên chuẩn bị 1 USB để lưu trữ bài thực hành vào cuối buổi.
- Sinh viên vắng thực hành 1 buổi sẽ bị CẤM THI phần thực hành.
- Sinh viên nên thực hành trước ở nhà và đặt câu hỏi cho giáo viên khi lên lớp.

C. TÀI LIỆU THAM KHẢO

1. [Ngô Bá Hùng, Phạm Thế Phi], Giáo trình Mạng máy tính, NXB Đại học Cần Thơ, 2014.
2. [J.F.Kurose, K.W.Ross], Supplements: Wireshark Labs – Computer Networking: A Top to Down Approach 6th, Protocols and Practice, Saylor Foundation, 2014
3. [Netkit Community], Labs Official: http://wiki.netkit.org/index.php/Labs_Official
4. [Massimo Rimondini], Emulating Computer Networks with Netkit, 4th International Workshop on Internet Performance, Simulation, Monitoring and Mesurement.

BUỔI THỰC HÀNH 2

Mục đích:

- Làm quen với công cụ phân tích gói tin Wireshark.
- Phân tích định dạng khung của: ***IEEE 802.3, Ethernet II*** và ***Wifi 802.11*** trên tầng liên kết dữ liệu
- Phân tích định dạng khung của các giao thức TCP và UDP trên tầng vận chuyển
- Xây dựng mô hình mạng ảo và phân tích dữ liệu trao đổi sử dụng Wireshark.

I. Wireshark

1. Giới thiệu

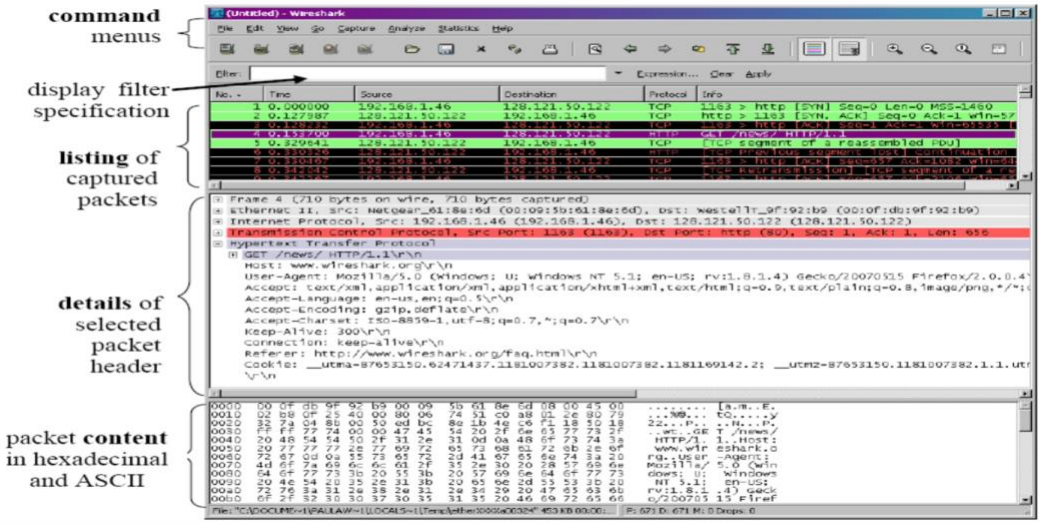
Wireshark là một công cụ mã nguồn mở sử dụng phổ biến trên nhiều hệ điều hành khác nhau. Wireshark cho phép quan sát và phân tích các thành phần trong gói dữ liệu bắt được theo thời gian thực.

Wireshark cung cấp giao diện thân thiện và thuận lợi cho việc phân tích chi tiết các gói dữ liệu.

Trong phần thực hành Mạng máy tinh, Wireshark sẽ được dùng như sau:

- ***Bước 1***: Sử dụng lệnh tcpdump ghi nhận thông tin trao đổi trong mạng ảo và ghi ra file ***.pcap***
- ***Bước 2:*** Sử dùng Wireshark trên máy thực (host) để mở file ***.pcap*** và thực hiện phân tích các thông tin trong file này để hiểu rõ về định dạng dữ liệu và giao thức truyền tải ở mỗi tầng.

2. Giao diện tương tác với Wireshark



- ***Thanh menu lệnh***: chứa các lựa chọn để tương tác với file đang được mở.
- ***Bộ lọc*****:** lọc và hiển thị dữ liệu tương ứng.
- ***Giao diện liệt kê các gói dữ liệu*****:** thể hiện thông tin chi tiết của các gói dữ liệu bắt được như: protocol, source, destination,…
- ***Giao diện thể hiện thông tin của dữ liệu:*** số thứ tự frame, chiều dài frame, khuôn dạng frame, khuôn dạng gói tin IP, giao thức tầng ứng dụng…
- ***Giao diện thể hiện nội dung của dữ liệu bằng mã HEX và mã ASCII***

II. Phân tích dữ liệu với Wireshark

Bài tập 5: Phân tích dữ liệu cơ bản

❖ ***Bước 1:*** Mở file ***wireshark_exa.pcap*** bằng Wireshark.

❖ ***Bước 2:*** Khảo sát thông tin cơ bản hiển thị trên Wireshark

- Các gói tin màu xanh lá cây, màu xanh dương, màu xanh dương nhạt lần lượt đại diện cho các giao thức nào? Trên file này còn có những gói tin có màu khác nữa không? Nếu có, thì các gói tin với màu sắc khác thể hiện các thông tin gì?
- Chọn gói tin thứ 100, gói tin này có kiểu giao thức sử dụng để truyền tải là gì?
- Chọn gói tin thứ 104, 105 và 106, các gói tin này có kiểu giao thức sử dụng để truyền tải là gì?
- Chọn gói tin 106, phần ***Data*** của gói tin thể hiện thông tin gì? Click chuột phải lên gói tin 106 và chọn *Follow TCP Stream*, nhận xét về kết quả thu được?

Bài tập 6: Phân tích ***Ethernet II Header***

❖ ***Bước 1:*** Mở file ***ethernet2.pcap*** bằng Wireshark. File này chứa các gói tin được trao đổi từ một máy tính (client) đến một server chứa website ***gaia.cs.umass.edu***.

❖ ***Bước 2:*** Khảo sát các thông tin trong Ethernet II Header

Chọn gói tin số 10. Đây là gói tin chứa thông điệp GET/HTTP của Client đến Server để lấy nội dung trang ***gaia.cs.umass.edu***. Trả lời các câu hỏi sau:

- Địa chỉ MAC của máy gửi đi thông điệp GET/HTTP?
- Địa chỉ đích (destination) trong khung Ethernet II có phải là địa chỉ MAC của server chứa website ***gaia.cs.umass.edu*** hay không? Nếu không, đây là địa chỉ của ai?
- Giao thức mà tầng mạng sử dụng là giao thức gì? Giá trị HEX bằng bao nhiêu?
- Từ vị trí bắt đầu khung cho đến khi ký tự G của lệnh GET trong giao thức HTTP có bao nhiêu trường (field) thông tin? Mỗi trường gồm bao nhiêu byte dữ liệu và thể hiện nội dung gì?

Bài tập 7: Phân tích ***IEEE 802.3 Header***

❖ ***Bước 1:*** Mở file ***802ieee.pcap*** bằng Wireshark

❖ ***Bước 2:*** Khảo sát sự khác biệt giữa khung IEEE 802.3 và khung Ethernet II

Chọn gói tin số 20 và trả lời các câu hỏi sau:

- Hãy cho biết giao thức tầng mạng đang sử dụng là giao thức gì? Nếu không tìm thấy thông tin thể hiện cho giao thức tầng mạng, cho biết thông tin đó đã được thay thế bằng thông tin mới tên gì?
- Thông tin mới này có ý nghĩa gì trong việc phân biệt cấu trúc của 2 khung Ethernet II và 802.3?
- Hãy cho biết các trường hợp mà khung IEEE 802.3 và khung Ethernet II được sử dụng.

Bài tập 8: Phân tích ***Wifi 802.11 Header***

❖ ***Bước 1:*** Mở file ***wlan-trace-1.pcap*** bằng Wireshark.

❖ ***Bước 2:*** Khảo sát các thông tin trong Wifi 802.11 Header

- Chọn 1 gói dữ liệu bất kỳ và cho biết ý nghĩa tổng quát của các thông tin sau: ***Frame, Radiotap, IEEE 802.11, Data*** *(nếu có)*
- Nhập lệnh sau vào bộ lọc: *wlan.fc.type==n* với n có các giá trị 0, 1, 2.
  Giải thích lệnh và nhận xét kết quả lọc khi n lần lượt bằng 1,2 và 3.
- Nhập lệnh sau vào bộ lọc: *wlan.fc.type==2 && wlan.fc.retry==0*
  Giải thích lệnh và nhận xét kết quả lọc dữ liệu hiển thị?

Bài tập 9: Phân tích ***UDP Header***

❖ ***Bước 1:*** Mở file ***http-ethereal-trace-5.pcap*** bằng Wireshark.

❖ ***Bước 2:*** Khảo sát các thông tin trong UDP Header

- Nhập lệnh sau vào bộ lọc: *snmp*
  Lệnh này lọc các dữ liệu là thông điệp trong giao thức SNMP – Simple Network Management Protocol.
- Trong các gói tin này có sử dụng UDP Header hay không? Nếu có, chọn 1 gói tin bất kỳ.
- Có bao nhiêu trường (field) trong UDP Header của gói tin? Mỗi trường có độ dài là bao nhiêu bytes?
- Giá trị của trường ***Length*** trong UDP Header bằng bao nhiêu và thể hiện thông tin gì? Cách tính giá trị của trường Length này?
- Tìm hiểu về cách tính ***Checksum*** của UDP Header. Gợi ý: tham khảo cách tính trên wiki: https://en.wikipedia.org/wiki/User_Datagram_Protocol
- Dựa trên kiến thức đã tìm hiểu được hãy trình bày lại cách tính ra ***Checksum*** của UDP Header của một gói tin bất kỳ. Gợi ý: ***Checksum*** được tính bằng phương pháp nào, các toán hạng nào tham gia, giá trị của các toán hạng được lấy ở đâu trong gói tin...

Bài tập 10: Phân tích ***TCP Header***

❖ ***Bước 1:*** Mở file ***tcp-ethereal-trace-1.pcap*** bằng Wireshark.

❖ ***Bước 2:*** Khảo sát các thông tin trong TCP Header

- Nhập lệnh sau vào bộ lọc: *tcp*
  Lệnh này lọc các dữ liệu là thông điệp trong giao thức TCP
- Cho biết ***Sequence Number*** của *TCP SYN segment* để khởi tạo kết nối giữa client-server? Thành phần (field) nào trong segment này chỉ ra đây là *TCP SYN segment*?
- Cho biết ***Sequence Number*** của *TCP SYN ACK segment* để trả lời từ server cho client? Thành phần (field) nào trong segment này chỉ ra đây là *TCP SYN ACK segment*?
- Giá trị của trường ***Acknowledgement*** trong *SYN ACK segment* là gì? Giá trị này được xác định như thế nào?
- Tìm gói tin có chứa dữ liệu là thông điệp *POST/HTTP*. Cho biết ***Sequence Number*** của gói tin này là bao nhiêu? Gói tin tiếp theo sau sẽ có ***Sequence Number*** bằng bao nhiêu? Giải thích vì sao có giá trị này?
- Lập bảng sau cho 6 TCP segment chứa các dữ liệu đầu tiên được gửi từ client sang server và điền vào các giá trị quan sát được trên Wireshark vào bảng.

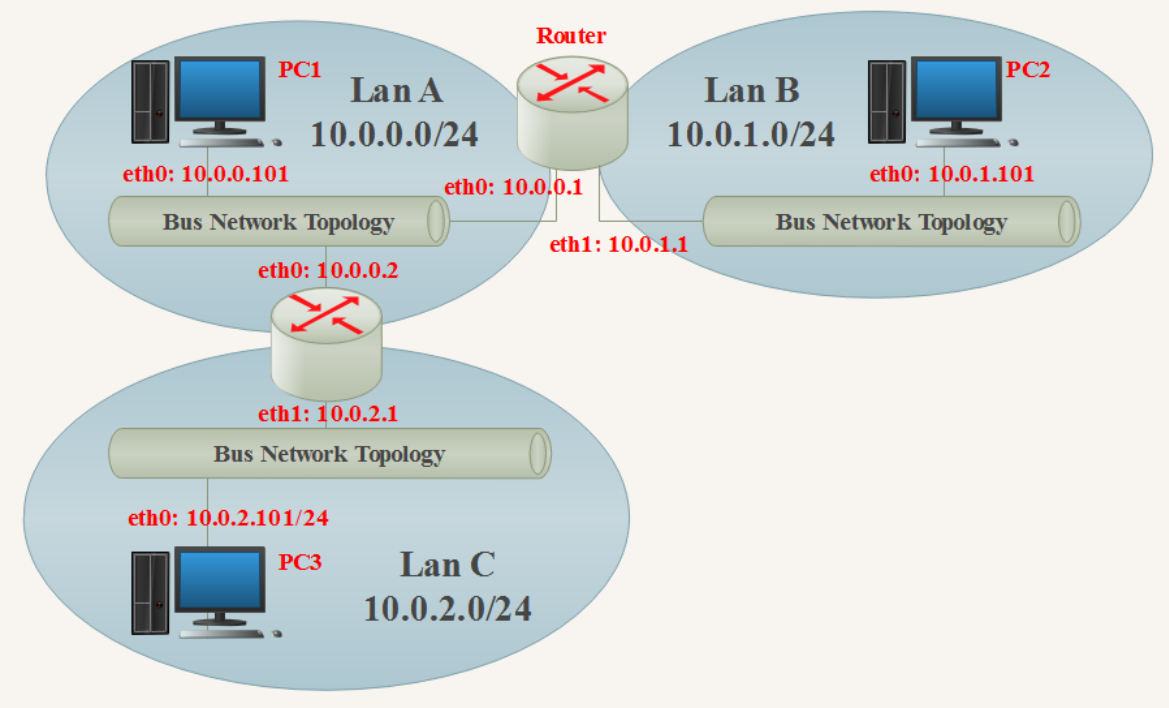
Segment	Packet Number	Sequence Number	Length	Time Sent	Time ACK received	Round Trip Time
1	4	1	565	0.026477	0.053937	0.02746
2						
3						
4						
5						
6						

- Giá trị nhỏ nhất của ***buffer space (receiver window)*** mà Server quảng bá (advertised) cho Client? Sau bao lâu thì kích thước của buffer space đạt giá trị tối đa, và bằng bao nhiêu?
- Trong quá trình truyền dữ liệu, Client có truyền tải lại segment nào không. Gợi ý: Chọn ***Statistics***, chọn tiếp ***TCP Steam Graph,*** chọn ***Time Sequence (Stevens)***, ta nhận được 1 đồ thị theo *sequence number* và *time*. Dựa vào đồ thị để trả lời.

Bài tập 11: Phân tích dữ liệu thu được trên mô hình mạng ảo Netkit

Mở rộng mô hình mạng đã xây dựng thành công ở bài tập 3 bằng cách thêm vào 1 LAN C và 1 máy pc3 trong LAN C.

Mục tiêu: xây dựng thành công mạng ảo, đảm bảo truyền tải dữ liệu giữa các máy ảo là thông suốt và thực hiện khảo sát dữ liệu với Wireshark.



Lệnh mới cần sử dụng:

route add -net <Network Address> gw <Gateway Interface Address> [dev <Name Of Interface>]

Ví dụ: để thêm thông tin vạch đường cho pc1 đến mạng LAN C, sử dụng lệnh:

route add -net 10.0.2.0/24 gw 10.0.0.2

Giải thích: Lệnh này cho phép pc1 có thể đi đến được LAN C nhờ vào giao diện eth0 của Router R2.

Gợi ý việc khảo sát dữ liệu với Wireshark:

❖ ***Bước 1:*** Trên pc2 thực hiện lệnh *tcpdump* để bắt gói tin truyền tải đến. Trên pc3 *ping* đến pc2, các gói tin bắt được sẽ hiển thị trên terminal của pc2.

❖ ***Bước 2:*** Thực hiện lại lệnh *ping* trên pc3, lần này sử dụng lệnh

tcpdump –w /hosthome/pc2.pcap trên máy ảo pc2
tcpdump –w /hosthome/R1.pcap trên máy ảo router R1
tcpdump –w /hosthome/R2.pcap trên máy ảo router R2

để ghi thông tin lắng nghe được khi dữ liệu đi qua R2, R1 và pc2 ra file ***.pcap***

Thư mục ***/hosthome*** là thư mục để chia sẻ các tài nguyên (file, folder…) giữa máy host và máy ảo.

❖ ***Bước 3:*** Trên máy host, dùng Wireshark mở các file ***pc2.pcap, R1.pcap, R2.pcap*** đã ghi lại được. Quan sát các gói tin bắt được, kiểm tra và đối chiếu kiến thức lý thuyết đã học ***về khuôn dạng của dữ liệu*** với kết quả thu được.