

ĐỒ ÁN THỰC HÀNH

WIRESHARK

MÔN MẠNG MÁY TÍNH

1. Quy định chung

- Đồ án được làm theo nhóm: mỗi nhóm tối đa **2** sinh viên, sinh viên tự chọn nhóm.
- Các bài làm giống nhau sẽ đều bị điểm 0 toàn bộ phần thực hành (dù có điểm các bài tập, đồ án thực hành khác).
- Môi trường: Sử dụng công cụ Wireshark

2. Cách thức nộp bài

Nộp bài trực tiếp trên Website môn học, không chấp nhận nộp bài qua email hay hình thức khác.

Tên file: **MSSV1_MSSV2.zip** (Với MSSV1 < MSSV2)

Ví dụ: Nhóm gồm 2 sinh viên: 1912001 và 1912002 làm đề 1, tên file nộp: **1912001_1912002.zip**

Cấu trúc file nộp gồm:

1. **Report.pdf**: chứa báo cáo về bài làm
2. **Packets**: thư mục chứa pcap file (*bai2.pcapng, bai3.pcapng, bai4.pcapng*)

Nhóm nào không nộp pcap file bài 2, bài 3 và bài 4 thì không được chấm bài đó.

Lưu ý: Cần thực hiện đúng các yêu cầu trên, nếu không, bài làm sẽ không được chấm.

3. Hình thức chấm bài

GV chấm dựa trên bài làm được nộp tại Moodle

4. Tiêu chí đánh giá

Về báo cáo:

- Thông tin của nhóm.

- Đánh giá mức độ hoàn thành từ 0 – 100% (Chú thích rõ những mục làm được, chưa làm được và còn bị lỗi)
- Trả lời các câu hỏi mà đề án đưa ra
- Chụp hình để minh chứng cho câu trả lời (có tô đậm/ khoanh vùng cụ thể)
- Bảng phân công công việc và cho biết rõ ràng ai làm việc gì cách rõ ràng. Không ghi chia đều công việc hay cùng làm mọi việc.
- Các nguồn tài liệu tham khảo.

5. Thang điểm chi tiết

Mỗi câu trả lời, nếu có hình ảnh để trả lời, thì bắt buộc phải chèn hình ảnh và highlight nội dung trả lời, đồng thời kèm theo giải thích chi tiết về câu trả lời đó nếu có.

Bài	Câu	Ghi chú	Điểm
1			
	1,2,3,4		0.375
	5		0.5
		Tổng	2đ
2	1,2,...,13	Mỗi phần trả lời là 0.2	0.2
	14		0.4
		Tổng: 14 câu nhỏ	3đ
3			
	1	Bắt được gói tin yêu cầu	0.5
	2, 3, 4, 5	Mỗi phần nhỏ trả lời là	0.3125
		Tổng: câu 1 + 8 câu trả lời nhỏ	3đ
4			
	1,2,3,4		0.5
		Tổng	2đ
Báo cáo		Đầy đủ nội dung yêu cầu, trình bày đẹp	

Giới thiệu:

Wireshark là công cụ cho phép giám sát gửi/nhận gói tin trên card mạng. Có 2 modes hoạt động: Open và Capture. Capture mode cho phép người dùng có thể xem trực tiếp các gói tin hiện tại đang ra/vào card mạng, và có thể lưu trữ lại với định dạng pcap file. Open mode cho phép người dùng đọc gói tin pcap file có sẵn.

Nội dung:

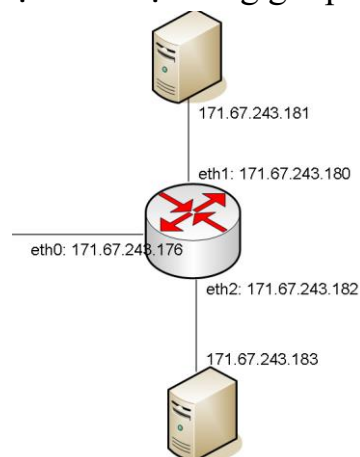
Bài 01: Ping (2đ)

Mở *ping.pcapng* file, nội dung của file pcap là thông tin các gói tin gửi từ một máy sang một máy khác bằng lệnh ping. Trả lời các câu hỏi sau:

1. Cho biết địa chỉ IP của host ping và host được ping?
2. Cho biết port được sử dụng là bao nhiêu? Nếu không có port thì giải thích tại sao?
3. Với gói tin ICMP request, cho biết kích thước (bytes) của từng phần trong diagram. (Chú ý: Kích thước tổng của gói tin là 98 bytes)

?	?	?	?
ICMP data	ICMP header	IP header	Ethernet header

4. Tại sao lại có 2 gói ARP?
5. Hãy vẽ sơ đồ mạng logic dựa trên nội dung gói pcap đó. Ví dụ:



Bài 02: HTTP (3đ)

Xóa cache browser trước khi truy cập trang web hoặc dùng ẩn danh. Dùng wireshark để bắt gói tin khi truy cập vào trang web: <http://example.com> và trả lời các câu hỏi sau:

1. Chụp hình kết quả bắt gói tin từ lúc bắt đầu DNS đến lúc gửi HTTP request (thấy được những gói tin liên quan)
2. Cho biết IP của host
3. Cho biết IP của router (default gateway) (nếu không thấy được thì trả lời không có và giải thích tại sao)
4. Cho biết địa chỉ MAC của host?
5. Cho biết địa chỉ MAC của router (default gateway)
6. Protocol nào được sử dụng để phân giải tên miền của trang web
7. Cho biết IP của HTTP server
8. Cho biết Protocol của tầng Transport được sử dụng bởi DNS
9. Cho biết port sử dụng khi truy vấn DNS server
10. Bao lâu thì quá trình bắt tay 3 bước (3-way handshake) hoàn thành
11. Cho biết host machine của website đang truy cập (Application)
12. Version HTTP mà trình duyệt web (browser) đang sử dụng (Application)
13. Trong cái mục filter, nhập câu query sau đây: **udp.dstport==53** và click apply. Hãy cho biết chức năng và kết quả của câu query vừa thực hiện?
14. Trình bày quá trình gửi data (Sequence number, Acknowledgement number) từ khi kết nối đến khi kết thúc nhận data HTTP server

Bài 03: Traceroute (3đ)

Nếu bạn dùng Window thì dùng lệnh **tracert**, nếu bạn dùng Linux/iOS thì bạn dùng lệnh **traceroute**. Lưu ý kết quả bắt gói tin trên Window và Linux/iOS sẽ khác nhau, vì vậy câu trả lời phụ thuộc bạn dùng OS nào.

Bật wireshark để bắt gói tin lệnh traceroute từ máy của mình (có thể dùng máy ảo) đến www.fit.hcmus.edu.vn (FIT). Trả lời những câu hỏi sau:

1. Chụp hình kết quả bắt gói tin sau khi traceroute hoặc tracert (thấy được những gói tin liên quan)
2. Cho biết traceroute/tracert dùng để làm gì?
3. Cho biết địa chỉ IP của máy gửi request?

4. Cho biết cách máy tính xác định được địa chỉ IP của FIT
5. Sau khi xác định được IP của `www.fit.hcmus.edu.vn`, máy sẽ bắt đầu gửi gói tin đến FIT
 - a. Protocol được sử dụng của những gói tin sau đó là gì?
 - b. Có bao nhiêu gói tin được gửi đi (**request**) trước khi nhận được **response đầu tiên trả lời** cho những request? (Hay nói một cách khác là: lệnh `trace*` sẽ gửi request message đi, và nhận về response. Vậy có bao nhiêu gói tin request đã gửi đi đến khi nhận được gói tin response đầu tiên?)
 - c. Cho biết **TTL của gói tin cuối cùng** được gửi trước khi nhận được gói tin **response đầu tiên trả lời** cho những gói tin request?
 - d. Bạn có thấy thông tin **port** trong các gói tin gửi đi? Nếu có bạn nhận thấy port nguồn/đích của gói tin có gì đặc biệt? Nếu không thấy thông tin port, hãy giải thích nguyên nhân?
 - e. Gói tin **response đầu tiên** là trả lời cho **gói tin request thứ mấy**? (No.)

Bài 04: DHCP (2đ)

Sử dụng lệnh **ipconfig /release** (xóa ip), và **ipconfig /renew** (xin lại ip mới) và bắt gói tin DHCP trong quá trình release và renew. Trả lời những câu hỏi sau:

1. Chụp hình kết quả sau sau khi bắt được gói tin (thấy những gói tin DHCP trong quá trình release, renew)
2. DHCP message dùng UDP hay TCP tại tầng transport? Tại sao?
3. Mục đích của DHCP release message là gì? DHCP Server có đảm bảo lúc nào cũng nhận được ACK message từ Client? Chuyện gì xảy ra nếu DHCP release message của Client bị mất?
4. Một người cấu hình DHCP server cho modem của một quán cafe với thời gian cấp là 8 tiếng, và cấp IP thuộc đường mạng **192.168.1.0/24** với **range IP từ 192.168.1.10 đến 192.168.1.100**. Giả sử bắt đầu ngày mới và modem này được mở lên vào lúc 7:00 AM. Người uống cafe đến uống, ai cũng truy cập vào mạng wifi để truy cập Internet. Lượng khách cứ đi vào ra liên tục từ 7:00 AM đến 11:00 AM. Khi đến 11:00 AM, thì quán đón vị khách thứ 92 (và trong quán chỉ còn 20 khách đang uống và truy cập Internet) và người

này không thể nào truy cập được Internet mặc dù đã nhập đúng pass Wifi.
Hỏi:

- a. Chuyện gì đã xảy ra mà vị khách thứ 92 không thể truy cập được Internet
- b. Vậy những vị khách tiếp theo 93, 94,có truy cập được hay không? và có thể truy cập vào thời điểm nào?
- c. Chủ quán cafe nên làm gì để vị khách thứ 90 có thể truy cập được Internet và hướng giải quyết để khắc phục tình trạng này về sau là gì?