**ĐỒ ÁN THỰC HÀNH**

**PHÂN TÍCH GÓI TIN VỚI WIRESHARK**

**MÔN MẠNG MÁY TÍNH**

# **Quy định chung**

- Đồ án được làm theo nhóm: mỗi nhóm tối đa 3 sinh viên, tối thiểu 2 sinh viên (theo nhóm TH đã đăng ký).

- 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

# **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\_MSSV3.zip** (Với MSSV1 < MSSV2 < MSSV3)

Ví dụ: Nhóm gồm 3 sinh viên: 2312001, 2312002 và 2312003 tên file nộp: **2312001\_2312002\_2312003.zip**

**Cấu trúc file nộp gồm:**

Thư mục **MSSV1\_MSSV2\_MSSV3** chứa tập tin, thư mục con:

1. **Report.pdf:** chứa báo cáo về bài làm
2. **Packets**: thư mục chứa pcap file (***bai2.pcapng***,**icmp**[5\_1, 5\_2, ,6,7,8].***pcapng***)

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

# **Hình thức chấm bài**

GV chấm dựa trên bài làm được nộp tại Moodle

# **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 đồ 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.

# **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 | mỗi câu 0.375 | **1.5** |
|  | 5,6 | mỗi câu 0.5 | **1** |
|  | 7 | a, b, c: mỗi câu 0.25 | **0.75** |
|  |  | d | **0.75** |
|  |  | **Tổng** | **4** |
| 2 |  |  |  |
|  | 1,...,8 | mỗi câu 0.5 | **4** |
|  |  | **Tổng** | **4** |
| 3 |  |  |  |
|  | 1,2,3,4 | mỗi câu 0.1875 | **0.75** |
|  | 5,6,7,8 | mỗi câu 0.3125 | **1.25** |
|  |  | **Tổng** | **2** |
| Báo cáo |  | Đầy đủ nội dung yêu cầu, trình bày tốt  Không có báo cáo: 0 điểm đồ án 2 |  |

## **Bài 01: HTTP (4đ)**

Dùng phần mềm "Wireshark" để mở gói tin "01.pcap". Bạn sẽ thấy có tổng cộng 176 gói tin khi truy cập web. Mỗi phần trả lời đều phải **chụp hình và highlight** vào phần trả lời của mình.

1. Nhìn vào những gói đầu tiên, máy client đang truy vấn IP của một tên miền. Cho biết tên miền của website là gì**?** Cho biết hai địa chỉ IPs của website này**?**
2. Có bao nhiêu gói tin (packets) mà Server đã gửi cho máy client tính từ lúc bắt đầu đến khi nhận được trang web (chỉ tính kết quả của yêu cầu HTTP GET đầu tiên)**?**
3. Trang web này (server) có sử dụng gzip để nén dữ liệu khi gửi đi không**?** Nó có ghi cookie không**?** Để trả lời câu hỏi này, bạn cần xem phần header của gói dữ liệu được tái tạo lại. Nó là gói cuối cùng từ câu hỏi số 2 ở trên. Kiểm tra xem nó có “Content-Encoding” được đặt là gzip không, còn có ghi cookie không, thì các bạn tự tìm hiểu.
4. Gói tin số 26 và 27 đang muốn làm gì**?** Theo bạn, tại sao lại phát sinh gói 26 và 27**?**.
5. Tại gói tin thứ 37 là một gói tin DNS query khác, cho domain là us.i1.yimg.com. Tại sao client lại cần hỏi địa chỉ IP cho domain này**?** trong khi gói tin số 26 đã làm việc này rồi phải không?
6. Tại gói 42, bạn sẽ thấy một câu lệnh HTTP “Get”, và trong gói 48 là một câu lệnh HTTP “Get” mới. Tại sao hệ thống không cần một yêu cầu DNS khác trước câu lệnh get thứ hai**?** (Nhấp vào gói 42 và nhìn vào cửa sổ giữa. Mở rộng dòng có tiêu đề “Hypertext Transfer Protocol” và đọc dòng “Host:”. So sánh dòng đó với dòng “Host:” của gói 48)
7. Nhấp chuột phải lên gói tin thứ 31 => Follow => TCP Stream.
   1. Cho biết có bao nhiêu HTTP request từ client gửi đi**?**
   2. Cho biết IP của máy client**?**
   3. Cho biết loại HTTP connections là gì**?** (Non-persistent HTTP hay Persistent HTTP), tại sao**?**
   4. Vẽ hình quá trình trao đổi gói tin giữa client và máy chủ bắt đầu từ gói tin TCP SYN đến khi kết thúc tcp stream filter. Hình vẽ thể hiện được seq number, SYN, ACK, ack number, lượng data (bytes) gửi đi .... (không sử dụng chức năng Statistics/Flow Graph của Wireshark)

## **Bài 02: DHCP (4đ)**

Chuẩn bị:

1. Khởi chạy terminal/ command prompt, gõ lệnh ipconfig /release
2. Khởi chạy wireshark, kiểm tra và bắt gói tin trên card mạng thật của máy tính
3. Khởi chạy terminal/ command prompt, gõ lệnh ipconfig /renew
4. Sau khi nhận được cấu hình IP, thực hiện lại bước 1 và 3 một lần nữa
5. Dừng quá trình bắt gói tin

Yêu cầu:

1. Lọc các gói tin theo giao thức DHCP
2. Gói tin DHCP sử dụng giao thức nào tại tầng transport
3. Hãy cho biết địa chỉ tại tầng link của host được cấp IP
4. Cho biết thông tin IP nguồn, Port nguồn và IP đích, Port đích của 4 gói tin (Discover/Offer/Request/ACK) trong đợt xin cấp IP đầu tiên
5. Chỉ ra điểm khác biệt giữa các giá trị trong gói tin DHCP Discover và DHCP Request
6. Cho biết giá trị Transaction-ID của 4 gói tin (Discover/Offer/Request/ACK) trong đợt xin cấp IP đầu tiên, giá trị Transaction-ID của 2 gói tin (Request/ACK) trong đợt xin cấp IP lần hai.

Mục đích sử dụng của transaction-ID là gì?

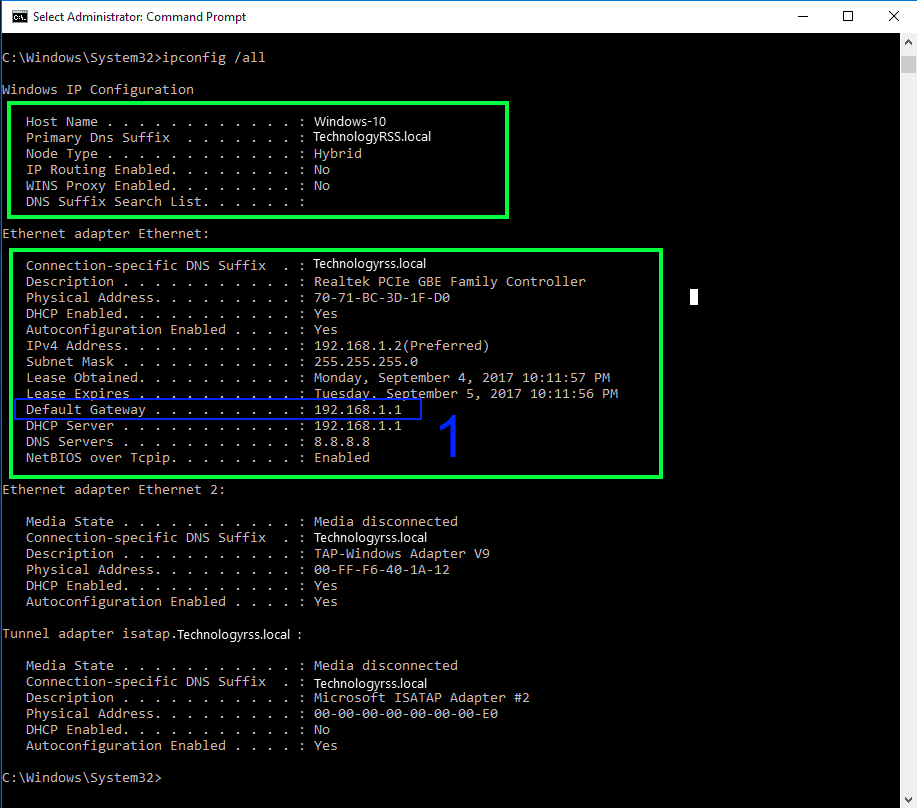
1. Cho biết ý nghĩa trường thông tin lease-time, giá trị của trường này trong gói tin bắt được là bao nhiêu?
2. Trong gói tin DHCP bắt được, hãy chỉ ra trường giá trị cho biết có thông tin DHCP relay agent hay không? Nếu có hãy cho biết IP của DHCP relay agent.

**Bài 03: ICMP (2đ)**

1. Cho biết MSS (maximum segment size) là gì? có liên quan gì đến MTU (maximum transmission unit)?
2. Cho biết MTU trên card mạng kết nối internet của máy bạn là bao nhiêu (có chụp hình)?
3. Kích thước MTU là 1500, cho biết kích thước của các phần của gói ICMP tại tầng mạng cơ bản (network) là bao nhiêu? (cho biết cách tính toán của bạn để có kết quả của từng phần)
4. Kích thước MTU là 1500, cho biết kích thước của các phần của gói ICMP tại tầng Data Link cơ bản là bao nhiêu? (cho biết cách tính toán của bạn để có kết quả của từng phần)

Chuẩn bị trên máy Windows:

Mở "Command Prompt" trên Windows, và gõ lệnh "ipconfig /all". Bạn sẽ thấy được địa chỉ IP của "Default Gateway" (số 1 trong hình bên dưới)



Bạn sẽ ping địa chỉ IP này và bắt gói tin

1. "> ping -i 5 <ip của default gateway>"

Vd: **ping -i 5 192.168.1.1** và bắt gói tin lưu lại với tên file "icmp5\_1.pcap". Cho biết lượng data trong ICMP (ICMP payload) là bao nhiêu? TTL (Time to live) là bao nhiêu?

"> ping -l 33 <ip của default gateway>"

Vd: **ping -l 33 192.168.1.1** và bắt gói tin lưu lại với tên file "icmp5\_2.pcap". Cho biết lượng data trong ICMP (ICMP payload) là bao nhiêu**?** TTL (Time to live) là bao nhiêu**?**

1. "> ping -l 1472 <ip của default gateway>"

Vd: **ping -l 1472 192.168.1.1** và bắt gói tin lưu lại với tên file "icmp6.pcap". Cho biết lượng data trong ICMP (ICMP payload) là bao nhiêu**?**

1. "> ping -l 1475 <ip của default gateway>"

Vd: **ping -l 1475 192.168.1.1** và bắt gói tin lưu lại với tên file "icmp7.pcap". Cho biết lượng data trong ICMP (ICMP payload) là bao nhiêu**?** Gói tin khác gì so với câu 6 bạn đã bắt ở trên và giải thích sự khác nhau đó**?**

1. "> ping -f -l 1475 <ip của default gateway>"

Vd: **ping -f -l 1475 192.168.1.1** và bắt gói tin lưu lại với tên file "icmp8.pcap". Sau khi bắt gói tin bạn thấy vấn đề gì và giải thích kết quả mà bạn có được**?**

**HẾT**