BÁO CÁO THỰC HÀNH

**Môn học: Nhập môn mạng máy tính**

**Tên chủ đề:** **Làm quen với Wireshark**

*GVHD: Tô Trọng Nghĩa*

1. **THÔNG TIN CHUNG:**

Lớp: IT005.O119.2

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 1 | Nguyễn Trọng Nhân | 22521005 | 22521005@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung | Tình trạng | Trang |
| 1 | Mở đầu về mạng máy tính | 100% | 1 - 2 |
| 2 | Làm quen với Wireshark và thử nghiệm bắt gói tin trong mạng | 100% | 2 - 6 |
| Điểm tự đánh giá | | | **9.5/10** |

BÁO CÁO CHI TIẾT

## Mở đầu về Mạng máy tính

Trước khi bắt đầu thực hành, sinh viên hãy trả lời các câu hỏi sau:

- Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng (kèm ảnh minh họa).

Trả lời:

Router



Switch



- Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút?

Trả lời: Nếu không có internet trong 5 phút, mọi hoạt động cần mạng bị trì trệ bao gồm liên lạc, các dịch vụ ngân hàng, giải trí,…

- Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn là gì?

Trả lời: Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của em là biết và hiểu rõ cách hoạt động của mạng Internet, có khả năng hiểu và triển khai được các hệ thống mạng phục vụ cho việc đi làm sau này.

## Làm quen với Wireshark và thử nghiệm bắt gói tin trong mạng

* 1. Giới thiệu và làm quen với Wireshark
  2. Thử nghiệm bắt gói tin với Wireshark

Sinh viên thực hành theo các bước sau tại môi trường đã chuẩn bị:

* 1. Phân tích kết quả bắt gói tin từ Wireshark

Sinh viên tự thực hiện các bước thực hành như hướng dẫn tại phần 2.2 để có được 2 file kết quả pcapng từ Wireshark. Lần lượt mở từng file tương ứng với 2 website trên và trả lời các câu hỏi sau:

1. Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu?

Trả lời:

Tổng thời gian và số gói tin trang gaia.cs.umass.edu lần lượt là 6.231973 giây và 1173 gói



Tổng thời gian và số gói tin trang http://www.testingmcafeesites.com/index.html lần lượt là 6.263038 giây và 140 gói



1. Liệt kê ít nhất 5 giao thức khác nhau xuất hiện trong cột giao thức (Protocol) khi không áp dụng bộ lọc “http” khi truy cập 2 website. Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.











5 giao thức khác nhau xuất hiện trong cột giao thức gồm:

-HTTP: HTTP là từ viết tắt của Hyper Text Transfer Protocol nghĩa là Giao thức Truyền tải Siêu Văn Bản được sử dụng trong www. HTTP là 1 giao thức cho phép tìm nạp tài nguyên, chẳng hạn như HTML doc.

-TCP: là một trong các giao thức cốt lõi của bộ giao thức TCP/IP. Sử dụng TCP, các ứng dụng trên các máy chủ được nối mạng có thể tạo các "kết nối" với nhau, mà qua đó chúng có thể trao đổi dữ liệu hoặc các gói tin. Giao thức này đảm bảo chuyển giao dữ liệu tới nơi nhận một cách đáng tin cậy và đúng thứ tự. TCP còn phân biệt giữa dữ liệu của nhiều ứng dụng đồng thời chạy trên cùng một máy chủ.

-DNS: Hệ thống phân giải tên miền (DNS) về căn bản là một hệ thống giúp cho việc chuyển đổi các tên miền mà con người dễ ghi nhớ sang địa chỉ IP vật lý tương ứng của tên miền đó. DNS giúp liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị trên Internet.

-ICMPv6: là phiên bản được biến đổi và nâng cấp của Internet Control Message Protocol (ICMP) cho giao thức liên mạng thế hệ 6 (IPv6). ICMPv6 được định nghĩa trong RFC 4443. ICMPv6 là một phần gắn liền với IPv6 và thực hiện thông báo lỗi mạng và chức năng chẩn đoán (ví dụ, ping), và có một khuôn khổ cho các phần mở rộng để thực hiện những thay đổi trong tương lai.

-TLSv1.2: là giao thức mật mã được thiết kế để cung cấp truyền thông an toàn qua một mạng máy tính. Một số phiên bản của các giao thức này được sử dụng rộng rãi trong các ứng dụng như trình duyệt Web, thư điện tử, tin nhắn nhanh, và VoIP.

1. Mất bao lâu từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận đối với mỗi website đã thử nghiệm. (mặc định, giá trị của cột thời gian (Time) trong packet-listing window là khoảng thời gian tính bằng giây kể từ khi chương trình Wireshark bắt đầu bắt gói tin)

Mất 0.26545s cho gaia.cs.umass.edu

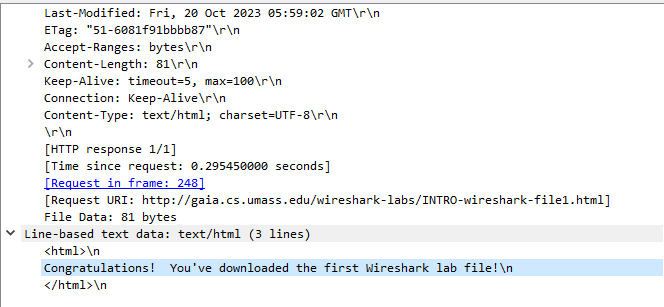


Mất 0.261628s cho http://www.testingmcafeesites.com/index.html



1. Nội dung hiển thị trên trang web gaia.cs.umass.edu “Congratulations! You've downloaded the first Wireshark lab file!” có nằm trong các gói tin HTTP bắt được hay không? Nếu có, hãy tìm và xác định vị trí của nội dung này trong các gói tin bắt được.

Có. Vị trí ở phần cuối gói tin bắt được từ server.



1. Địa chỉ IP của gaia.cs.umass.edu và website đã chọn ở bước 10 là gì? Địa chỉ IP của máy tính đang sử dụng là gì?

Địa chỉ IP của gaia.cs.umass.edu là 128.119.245.12



Địa chỉ IP của <http://www.testingmcafeesites.com/index.html> là 34.218.221.118



Địa chỉ máy đang sử dụng là 192.168.11.198

1. Qua ví dụ bắt gói tin trên và kết quả bắt gói tin từ Wireshark, hãy mô tả ngắn gọn diễn biến xảy ra khi bắt đầu truy cập vào một đường dẫn đến một trang web cho đến lúc xem được các nội dung trên trang web đó.

Trả lời:

-Trình duyệt gửi request tới server DNS biên dịch url thành địa chỉ IP





-Trình duyệt sẽ sử dụng địa chi IP đó để yêu cầu HTTP gọi tới Server lưu trữ trang web đó



-Trình duyệt gửi gói ACK đã nhận được gói tin thông qua TCP



-Server chấp nhận, gửi lại thông báo "200 OK". Và sau đó trình duyệt sẽ truy xuất mã HTML của trang web cụ thể được yêu cầu.



Mở rộng:

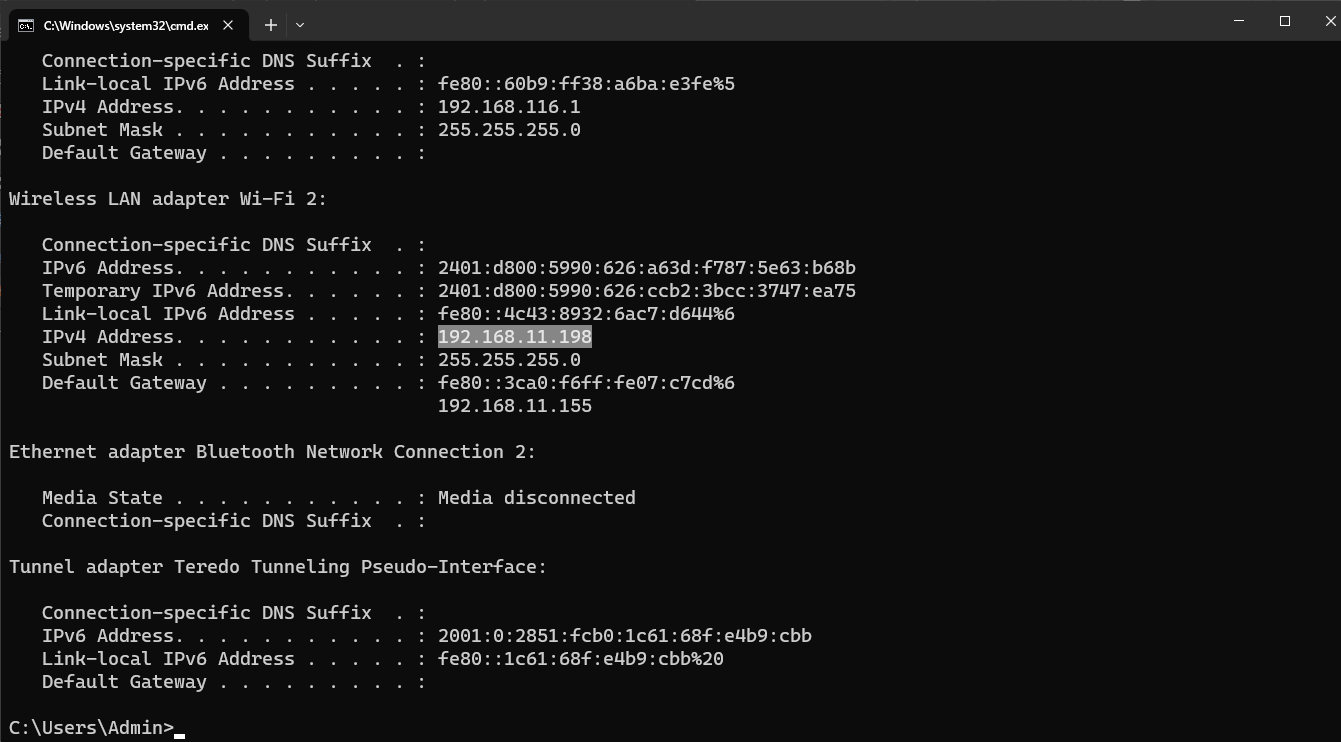
-Địa chỉ IP dùng để nhận diện và liên lạc với nhau trên mạng máy tính bằng cách sử dụng giao thức Internet.

Cách xem IP máy:

-Mở Command promt

-Nhập ipconfig, enter

-Tìm IP trong phần mạng không dây hoặc Ethernet dựa theo mạng đang sử dụng

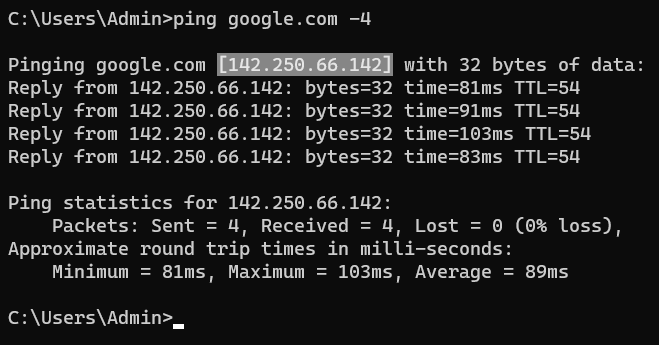


Cách xem ip website:

-Mở Command promt

-Nhập ping <url> (-4 cho IPv4 hoặc -6 cho IPv6), enter

-Địa chỉ IP sẽ hiện sau url



1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)