PHỤ LỤC 4

**HƯỚNG DẪN KIỂM TRA TÌNH TRẠNG KẾT NỐI**

**Mục tiêu:**

Bài này được thiết kế với mục tiêu cung cấp cho sinh viên các kỹ năng cơ bản để sử dụng các công cụ để hiển thị và kiểm tra tình trạng kết nối của mạng:

* Kiểm tra tình trạng kết nối của mạng với công cụ ping
* Hiển thị các chặng trên đường đi trong mạng với công cụ traceroute
* Sử dụng Wireshark phân tích hoạt động của các công cụ ping và traceroute

**Môi trường:** Hệ điều hành Ubuntu 18.04

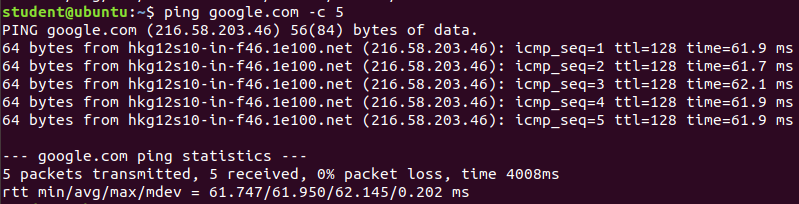
**Nội dung**

***Lưu ý: Trước khi thực hiện các nội dung thực hành sau đây, nên tắt các ứng dụng mạng đang sử dụng***

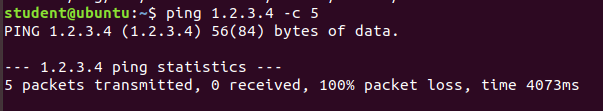
**1. Sử dụng công cụ ping**

*Lưu ý: Những hình ảnh dưới đây mang tính chất ví dụ minh họa. Kết quả thực hiện trên máy sinh viên có thể sẽ khác.*

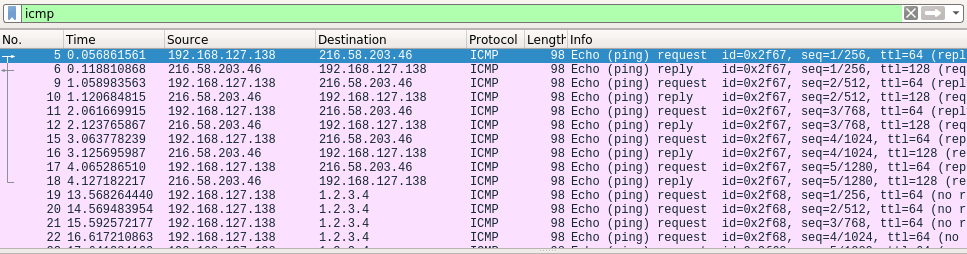
* **Bước 1**: Mở Wireshark bằng lệnh **sudo wireshark** trên cửa sổ Terminal thứ nhất
* **Bước 2**:Trên cửa sổ Terminal thứ hai thực hiện lệnh ping như dưới đây:



* **Bước 3**: Sau khi lệnh ping ở trên kết thúc, thực hiện lệnh ping lần 2 như sau:



* **Bước 4**: Ngừng bắt gói tin trên Wireshark
* **Bước 5**: Trên Wireshark điền xâu icmp vào bộ lọc để lọc lấy các gói tin ICMP. Kết quả nhận được sẽ tương tự như sau:



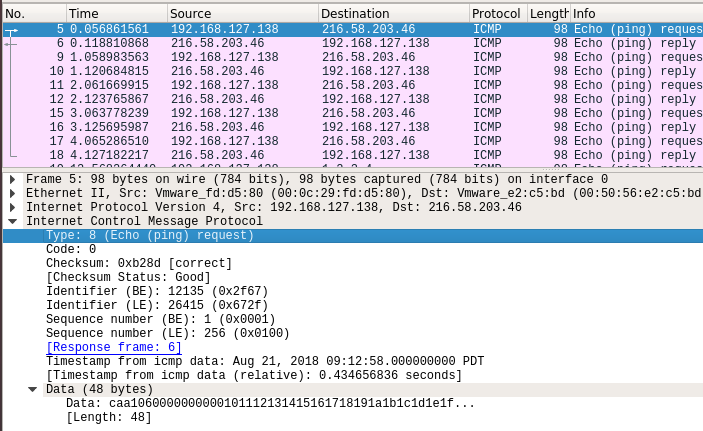
**Phân tích kết quả:**

**-** Kết quả của lệnh ping ở bước 2 cho thấy kết nối tới máy chủ google.com là bình thường. Từ kết quả này, ta còn thu được một số thông tin sau:

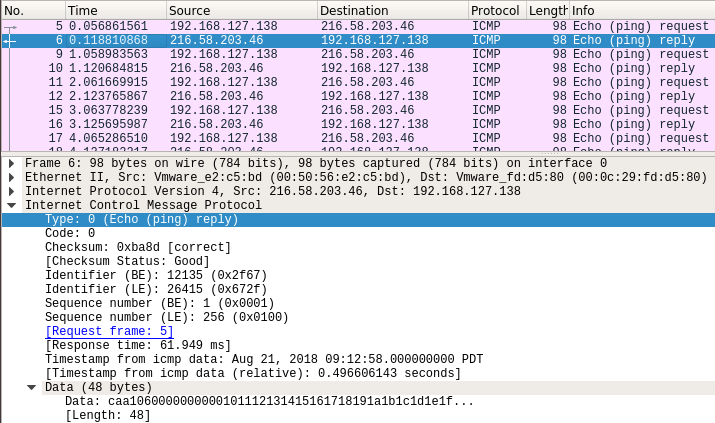
* Địa chỉ IP của máy chủ google.com: 216.58.203.46
* Tên khác của máy chủ: hkg12s10-in-f46.1e100.net
* Kích thước mỗi gói tin: 64 byte
* Số gói gửi: 5; số gói nhận: 5; tỉ lệ mất gói tin (packet loss): 0%
* (Trễ nhỏ nhất/trung bình/lớn nhất/độ lệch)rtt min/avg/max/mdev = 61.747/61.950/62.145/0.202 ms
* Thời gian thực hiện lệnh (time): 4008 ms

- Kết quả của lệnh ping ở bước 3 cho thấy kết nối tới máy có địa chỉ 1.2.3.4 là có lỗi, khi có 5 gửi đi thăm dò nhưng không nhận được gói trả lời nào (tỉ lệ mất gói tin là 100%)

- Mở rộng phần tiêu đề của gói tin Echo (ping) request bất kỳ ta thấy trường Type là 8 cho thấy gói tin là ICMP Echo Request



- Mở rộng phần tiêu đề của gói tin Echo (ping) reply của gói trên ta thấy trường Type là 0 cho thấy gói tin này là ICMP Echo Reply. Hơn nữa, ta có thế thấy nội dung phần Data(48 bytes) giống với gói tin ICMP Eco Request ở trên

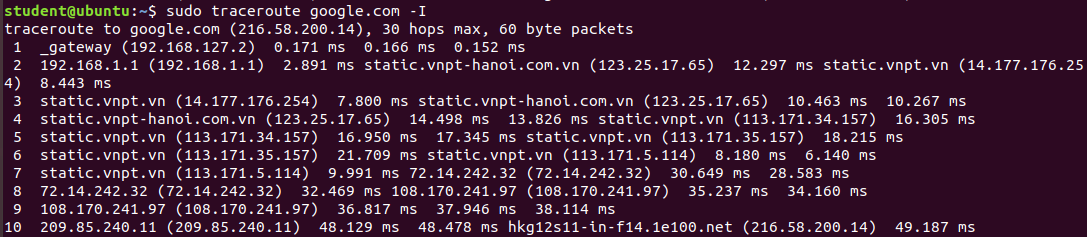


**2. Sử dụng công cụ traceroute**

*Công cụ traceroute đã được cài đặt mặc định trên Ubuntu 18.04, nhưng vì một lý do nào đó không có công cụ này, bạn có thể cài đặt bằng lệnh đơn giản sau trước khi thực hiện nội dung thực hành này:*

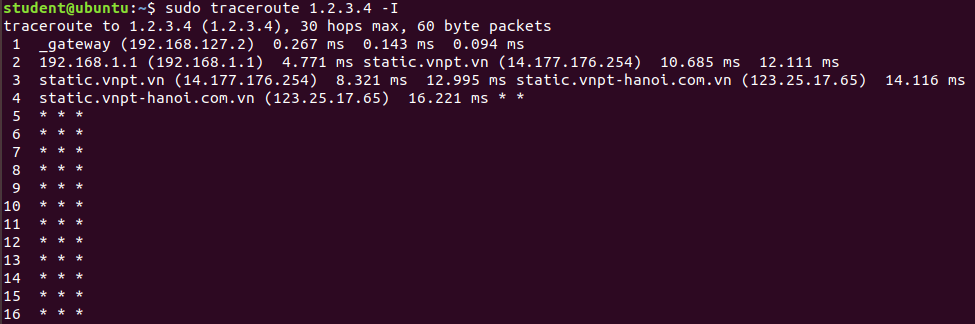
**sudo apt-get install traceroute**

* **Bước 1**: Mở Wireshark bằng lệnh trên cửa sổ Terminal thứ nhất
* **Bước 2**:Trên cửa sổ Terminal thứ hai thực hiện lệnh traceroute như dưới đây:

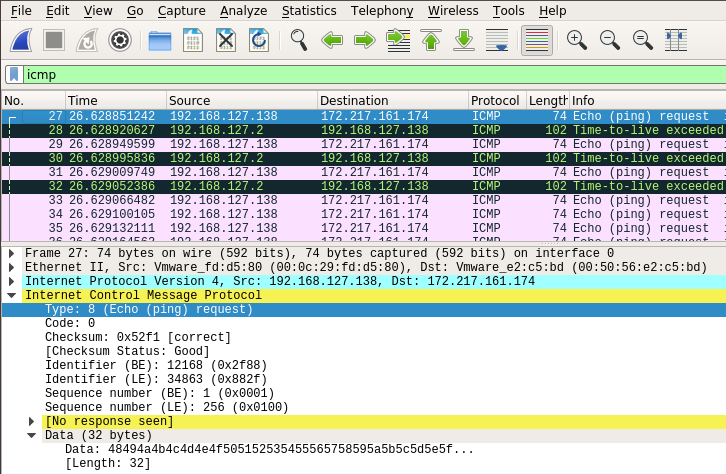


*Lưu ý: Với tùy chọn -I lệnh này sẽ gửi đi các gói tin ICMP Echo Request thay vì dùng các gói tin UDP theo mặc định*

* **Bước 3**: Sau khi lệnh traceroute ở trên kết thúc, thực hiện lệnh traceroute lần 2 như sau:



* **Bước 4**: Ngừng bắt gói tin trên Wireshark
* **Bước 5**: Trên Wireshark điền xâu icmp vào bộ lọc để lọc lấy các gói tin ICMP. Kết quả nhận được sẽ tương tự như sau:

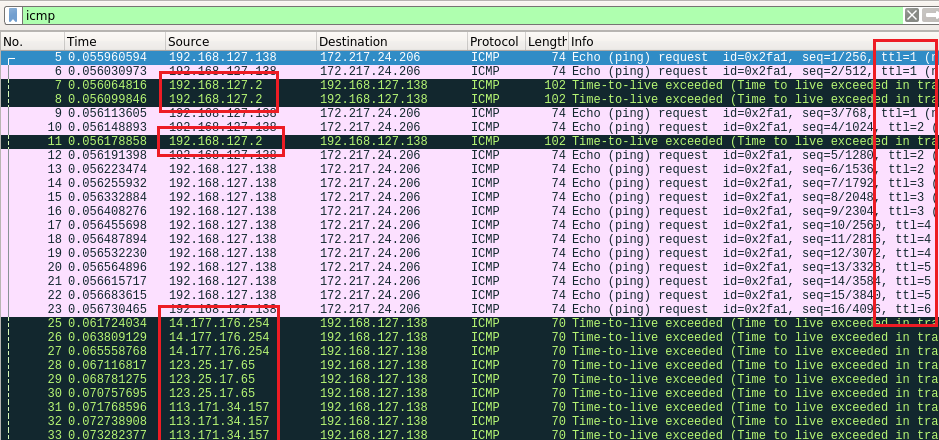


**Phân tích kết quả:**

**-** Kết quả của lệnh traceroute ở bước 2 cho thấy từ máy tính thực hiện tới máy chủ google.com có 10 chặng đi qua với địa chỉ IP của mỗi chặng đã được liệt kê.

- Kết quả của lệnh traceroute ở bước 3 cho thấy bắt đầu từ chặng thứ 5, lệnh này không phân tích được địa chỉ. Như vậy, có thể phán đoán, kết nối của máy tính thực hiện lệnh tới máy 1.2.3.4 bắt đầu có lỗi từ bước này.

- Trên kết quả bắt gói tin của Wireshark, chúng ta có thể thấy các nhóm 3 gói tin ICMP được gửi đi. Sau khi gửi xong một nhóm, giá trị TTL của nhóm tiếp theo tăng thêm 1. Địa chỉ nguồn của các gói tin báo lỗi ICMP Time to live exceeded chính là địa chỉ các chặng.



**Kết luận**

Với nội dung mà các bạn vừa thực hiện, các bạn đã làm quen được với cách thức sử dụng một số công cụ để kiểm tra tình trạng kết nối và phán đoán vị trí lỗi. Bên cạnh đó, chúng ta cũng đã sử dụng Wireshark để phân tích hoạt động của các công cụ này. Các bạn tham khảo thêm cách thức sử dụng các công cụ trên tại địa chỉ sau:

* ping: <http://manpages.ubuntu.com/manpages/bionic/man1/ping.1.html>
* tracecoute: <http://manpages.ubuntu.com/manpages/bionic/man1/traceroute.db.1.html>