4

Lab

Giao thức ICMP, địa chỉ IP và kỹ thuật chia mạng con

ICMP Protocol, IP Address and Subnetting

Thực hành Nhập môn Mạng máy tính

GVTH: Nguyễn Thanh Hòa

Tháng 11/2017

Lưu hành nội bộ

A. TỔNG QUAN

1. Mục tiêu

- Tìm hiểu về hoạt động của giao thức ICMP tại tầng Network
- Phân tích các thông điệp của chương trình Ping và Traceroute
- Tìm hiểu về địa chỉ IP và kỹ thuật chia mạng con (FLSM, VLSM)

2. Môi trường & công cụ

- Máy tính Windows *có kết nối Internet*
- Trình duyệt **Chrome/Firefox**
- Phần mềm **Wireshark**

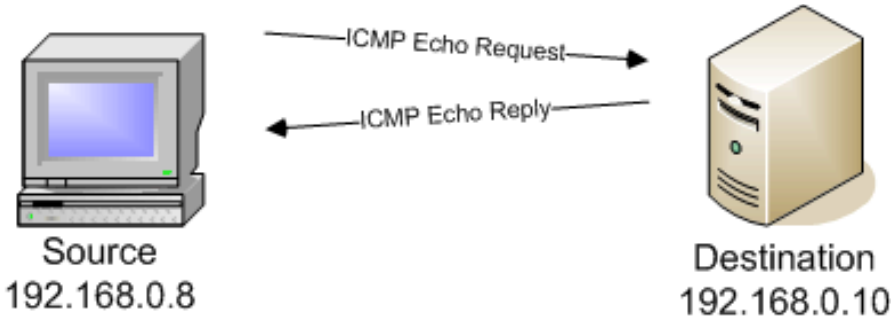
3. Kiến thức cơ bản

- Giao thức ICMP *(Internet Control Message Protocol):* được sử dụng bởi các máy tính và bộ định tuyến để trao đổi thông tin tầng Mạng với nhau, chủ yếu để kiểm tra mạng và báo lỗi.
- Giao thức IP và phân mảnh gói tin IP khi gửi qua mạng.
- Địa chỉ IP và các kỹ thuật chia mạng con.

B. THỰC HÀNH

1. Giao thức ICMP & lệnh Ping

ping *(Packet InterNet Groper)* là 1 chương trình chạy trên dòng lệnh dùng để kiểm tra 2 thiết bị trong mạng có thể kết nối với nhau hay không. Ping còn được dùng để đo thời gian trễ của gói tin trong mạng.



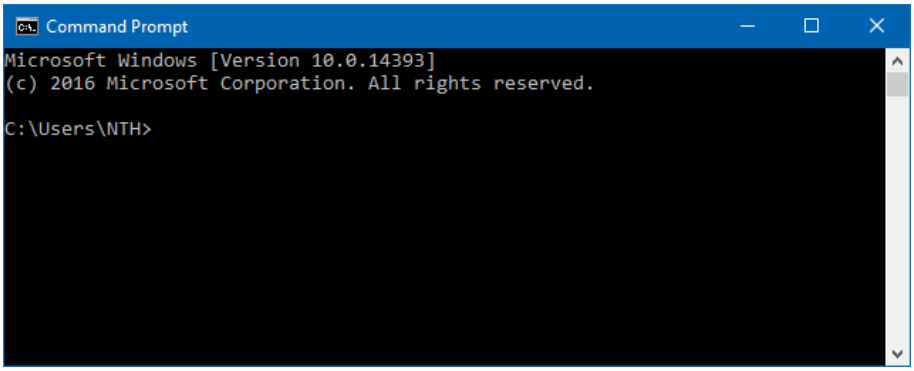
Hình 1. Ví dụ về quá trình Ping giữa 2 máy

Chương trình ping ở Host nguồn gửi một gói tin ICMP Echo Request tới địa chỉ IP đích. Nếu Host đích còn hoạt động và có kể kết nối đến thì Host đích sẽ trả lời bằng

cách gửi một gói tin ICMP Echo Reply trở lại Host nguồn. Cả 2 loại gói tin được dùng trong quá trình Ping này đều là các gói tin dùng giao thức **ICMP**.

Thực hiện các bước sau khi có kết nối Internet:

- **Bước 1:** Mở chương trình Command Prompt (CMD) trong Windows



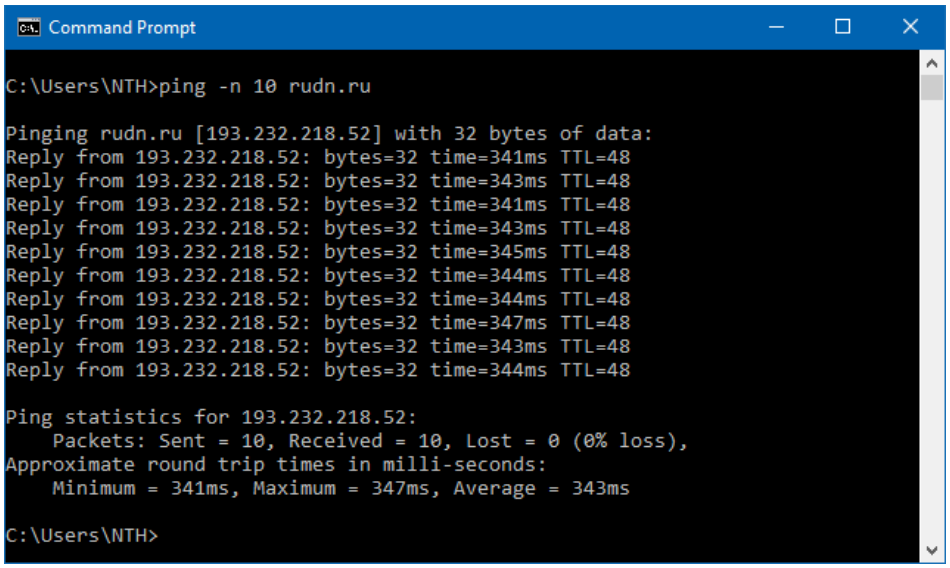
*Hình 2. Vào Start > Run > gõ **cmd** hoặc tìm ứng dụng tên **Command Prompt***

- **Bước 2:** Mở phần mềm Wireshark và bắt đầu bắt gói tin trên card mạng đang sử dụng kết nối Internet.
- **Bước 3:** Trong Command Prompt, thực hiện lệnh với cú pháp như sau:

ping -n 10 *hostname*

Trong đó:

- **hostname** là một địa chỉ (tên miền) của 1 website do sinh viên chọn.
- **-n 10** là 10 gói tin ping sẽ được gửi đi *(mặc định nếu không có tham số này, ping trên Windows sẽ chỉ gửi 4 gói)*

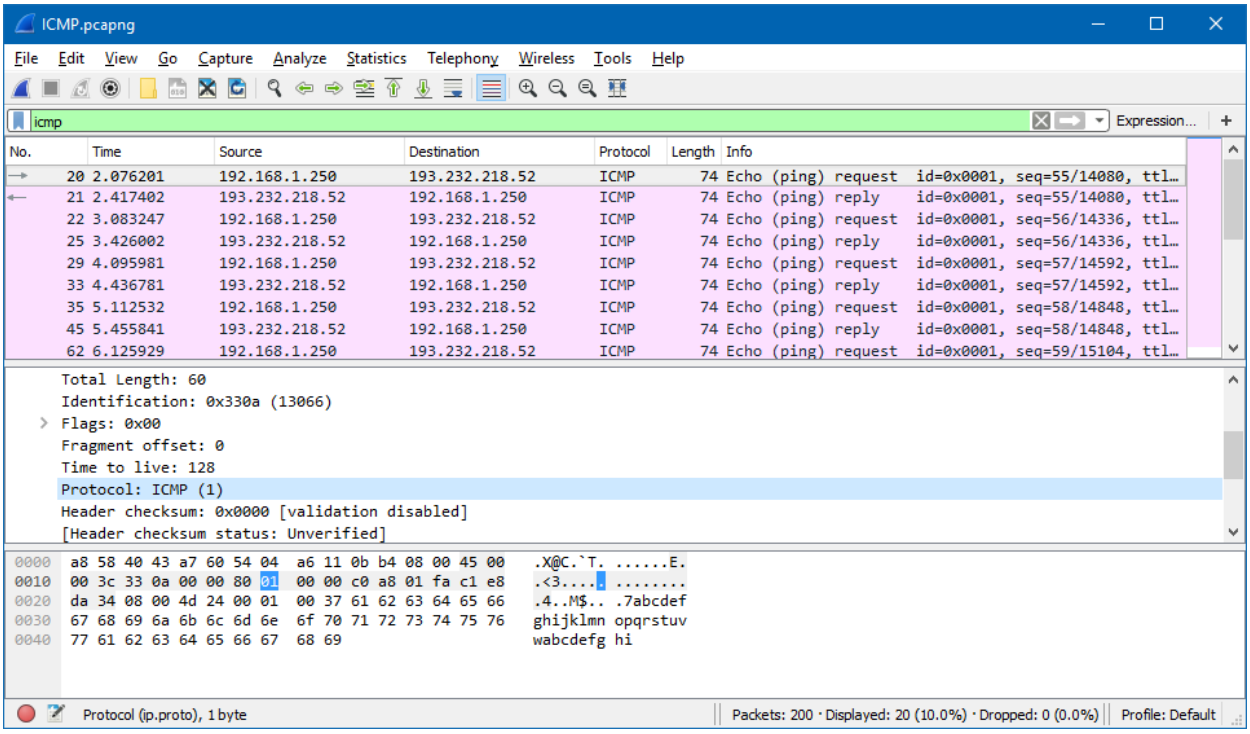


Hình 3. Ví dụ ping đến website Đại học RUDN - Nga

Sau khi thực hiện các bước trên, cửa sổ Command Prompt sẽ như hình 2. Trong ví dụ này, chương trình ping nguồn ở Việt Nam và host đích ở Nga. Từ cửa sổ này chúng ta thấy rằng chương trình Ping ở địa chỉ nguồn gửi 10 gói tin truy vấn và nhận được 10 gói tin trả lời.

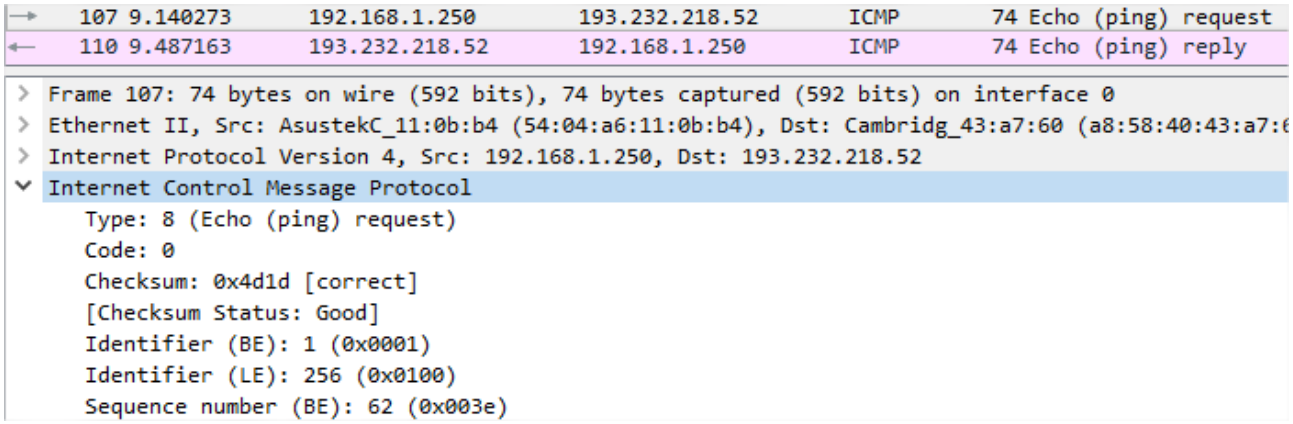
Với mỗi thông điệp trả lời, chương trình Ping nguồn sẽ tính thời gian của chu trình (***Round-Trip Time – RTT***), với 10 gói tin thì thời gian chu trình trung bình vào khoảng 344 mili-giây.

- **Bước 4:** Dừng bắt gói tin ở Wireshark sau khi ping xong và lưu thành file có tên *Ping-MSSV.pcapng* nộp kèm báo cáo.
- **Bước 5:** Gõ "**icmp**" vào bộ lọc của Wireshark để hiển thị tất cả các gói tin ICMP.



Hình 4. Lọc các gói tin ICMP bắt được

Ở hình 3 là cửa sổ của chương trình Wireshark sau khi lọc các gói ICMP. Chú ý rằng cửa sổ liệt kê 20 gói tin gồm: 10 gói tin truy vấn được gửi bởi host nguồn và 10 gói tin phản hồi mà host nguồn nhận được. Cũng chú ý thêm rằng địa chỉ IP nguồn là một địa chỉ tĩnh ở định dạng 192.168.x.x, và địa chỉ IP đích là của web server ở Nga. Ở gói tin đầu tiên trong ví dụ bên dưới thì vùng cửa sổ về nội dung gói tin cung cấp thông tin về gói tin này. Chúng ta thấy rằng phần địa chỉ IP của gói tin này có giao thức số 1 cũng là số giao thức của giao thức ICMP.



Hình 5. Tập trung kiểm tra các thông tin trong phần ICMP

Kiểm tra thông tin trong phần ICMP (*Internet Control Message Protocol*). Ta quan sát 1 gói tin như hình 4 thấy rằng gói tin ICMP thuộc Type 8 và Code 0, một dạng gói tin gọi là ICMP 'Echo Request'.

Cũng chú ý rằng gói tin ICMP này chứa một Checksum, một định danh, và một số thứ tự (Sequence Number).

Sinh viên tự chọn 1 website nước ngoài để ping, thực hiện bắt gói tin, quan sát các gói tin đã lọc và trả lời các câu hỏi sau:

Lưu ý: *Thực hiện ping bằng Command Prompt và báo cáo ảnh màn hình kết quả đã ping. Mỗi câu trả lời cần kèm theo minh chứng cụ thể là ảnh chụp màn hình của khu vực tìm thấy dữ liệu để suy ra đáp án trong gói tin (có thể dùng công cụ Snipping Tool hoặc phần mềm PrtScr - http://www.fiastarta.com/PrtScr đã được giới thiệu)*

1. Cho biết địa chỉ IP của máy tính mà sinh viên đang dùng và địa chỉ IP của Host đích đã chọn? Tại sao một gói tin ICMP không có số cổng (port number) của Host nguồn và đích?
2. Xem xét chi tiết thông tin (*quan sát trong phần Internet Control Message Protocol - ICMP*) của 1 gói tin Ping Request được gửi bởi Host mà SV đang dùng và 1 gói tin Ping Reply tương ứng:

   So sánh thông tin về ICMP Type và các Code Number của 2 gói tin trên. Gói tin ICMP có các trường thông tin nào khác? Các trường thông tin Checksum, Sequence Number và định danh có bao nhiêu byte?

3. Tìm hiểu và thử nghiệm, cho biết khi sử dụng lệnh ping thì có thể có những loại kết quả trả về nào?

   Giải thích ý nghĩa từng loại kết quả trả về và cho ví dụ minh họa.

   Tiến hành ping đến website uit.edu.vn và kiểm tra, giải thích kết quả.

4. *(Mở rộng) **Tìm hiểu các thông số mở rộng của lệnh ping và thử nghiệm:**

   Mở CMD, dùng lệnh **ping /?** để xem các thông số mở rộng của lệnh ping:

```
C:\Users\NTH>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

Hình 6. Các thông số mở rộng của lệnh Ping.

- *Tìm hiểu và giải thích ý nghĩa của ít nhất 3 thông số (như -t,-l,-I,w,…). Thử nghiệm lệnh ping mở rộng với các thông số này và cho ví dụ minh họa.*
- *Công cụ **ping** có thể dùng để thực hiện Tấn công từ chối dịch vụ (DoS) không? Nếu có hãy tìm hiểu và trình bày về loại tấn công này.*

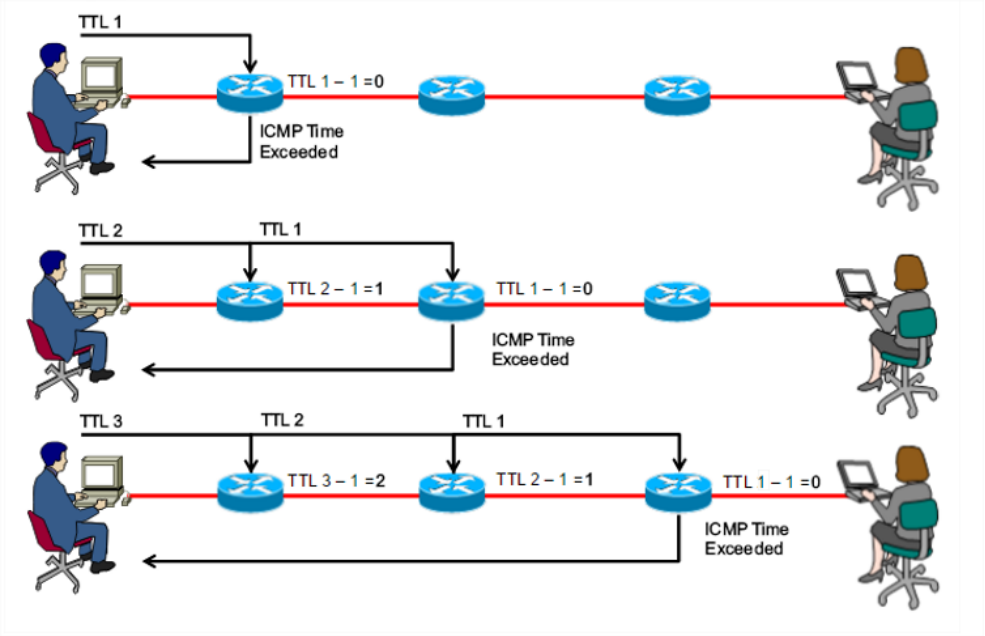
2. Giao thức ICMP và công cụ tracert (traceroute)

Ở phần này sẽ tiến hành bắt các gói tin ICMP tạo bởi chương trình Traceroute. ***Traceroute*** *(hay còn gọi là* ***Tracert*** *trên Windows) là chương trình được dùng để truy vết/hiển thị đường đi của một gói tin từ nguồn đến đích.*

Traceroute được hiện thực theo nhiều cách khác nhau trong Linux/MacOS và trong Windows. Trong Unix/Linux, Host nguồn gửi một chuỗi các gói tin UDP tới địa chỉ đích sử dụng số cổng đích (destination port number).

Trong Windows, nguồn gửi một chuỗi các gói tin ICMP tới địa chỉ đích.

Quá trình traceroute (tracert) trên Windows có thể được mô tả như sau:



Hình 7. Quá trình Traceroute

- Đầu tiên, máy tính sẽ gửi 3 gói ICMP request với TTL=1 để đi qua các Router và tìm đến đích.
- Khi gói tin qua 1 router/bộ định tuyến thì giá trị TTL sẽ được giảm 1. Khi một gói dữ liệu có TTL = 0 có nghĩa là gói tin đó đã hết hạn, bộ định tuyến sẽ bỏ gói tin này và gửi trả về 1 thông điệp báo lỗi ICMP *(Type 11, Code 0 – Time-to-live Exceeded)*
- Khi chưa có gói tin đến đích, máy tính sẽ tiếp tục gửi 3 gói tin ICMP có TTL tăng thêm 1 và quá trình trên sẽ được lặp lại cho đến khi gói tin đến được địa chỉ đích.

- Khi gói tin ICMP Request đã đến được đích, lúc đó máy tính sẽ nhận được 3 gói ICMP reply thành công, đồng thời dựa vào giá trị TTL lúc đó, ta cũng có thể xác định cần phải qua bao nhiêu router/bộ định tuyến (hops) và cần qua những hop nào để gói tin có thể di chuyển từ nguồn đến đích cũng như xác định có hop nào đang gặp sự cố giữa 2 điểm hay không.

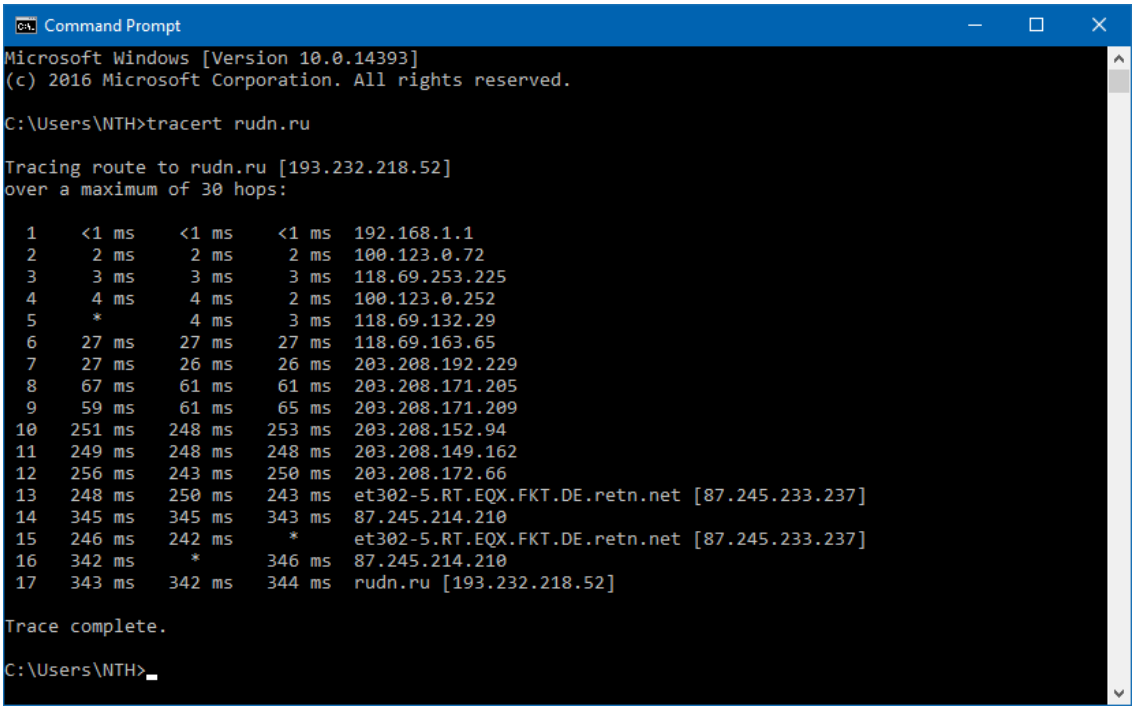
Thực hiện các bước sau khi có kết nối Internet:

- **Bước 1:** Mở chương trình Command Prompt (CMD) trong Windows
- **Bước 2:** Mở phần mềm Wireshark và bắt đầu bắt gói tin trên card mạng đang sử dụng kết nối Internet.
- **Bước 3:** Trong Command Prompt, thực hiện lệnh với cú pháp như sau:

tracert *hostname*

Trong đó:

- **hostname** là một địa chỉ (tên miền) của 1 ***website nước ngoài*** do sinh viên chọn (khác trang ví dụ).



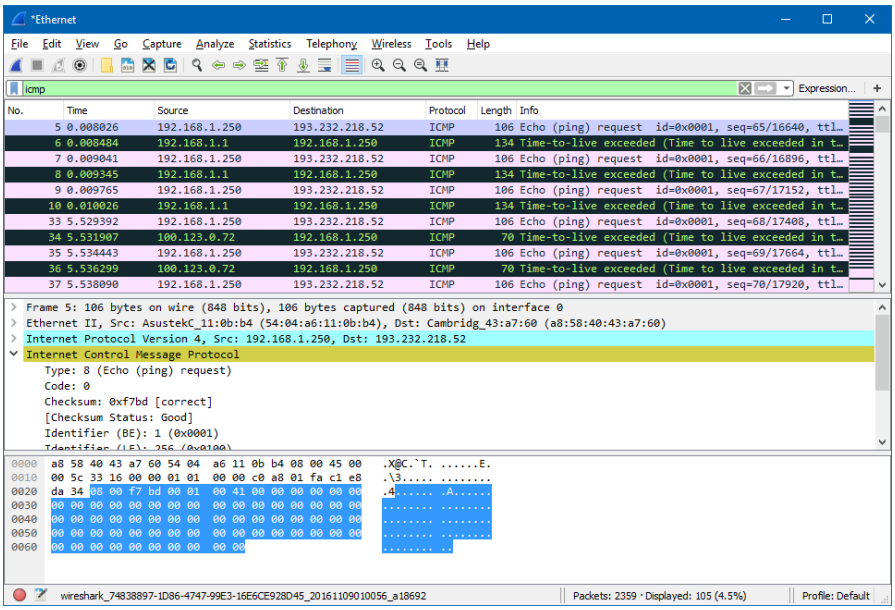
Hình 8. Ví dụ tracert đến website Đại học RUDN – Nga

- **Bước 4:** Khi Traceroute kết thúc, ngưng việc bắt gói tin trong Wireshark.

Sau khi chạy tracert thì cửa sổ Command Prompt tương tự như hình 7. Trong hình này, chương trình Traceroute khách là ở Việt Nam và đích đến là ở Nga. Từ hình này

chúng ta thấy rằng với mỗi giá trị TTL, chương trình nguồn gửi 3 gói tin tham dò. Traceroute hiển thị RTT cho mỗi gói tin thăm dò, cũng như địa chỉ IP (có thể có thêm tên) của Router.

- **Bước 5:** Dừng bắt gói tin trên Wireshark và lưu thành file ***Tracert-MSSV.pcapng***
- **Bước 6:** Gõ "**icmp**" vào bộ lọc của Wireshark để hiển thị tất cả các gói tin ICMP.



Hình 9. Lọc và quan sát các gói ICMP

Quan sát các gói tin đã lọc và trả lời các câu hỏi sau:

Lưu ý: *Thực hiện ping bằng Command Prompt và báo cáo ảnh màn hình kết quả đã tracert. Mỗi câu trả lời cần kèm theo minh chứng cụ thể là ảnh chụp màn hình của khu vực tìm thấy dữ liệu để suy ra đáp án trong gói tin (có thể dùng công cụ Snipping Tool hoặc phần mềm PrtScr - http://www.fiastarta.com/PrtScr đã được giới thiệu)*

1. Cho biết địa chỉ IP của máy tính đang sử dụng? Địa chỉ IP của Host đích mà sinh viên đã chọn?
2. Giá trị Time-To-Live (TTL) có ý nghĩa gì? TTL với website đã tracert bằng bao nhiêu? Khi dùng lệnh Ping thì giá trị TTL tương ứng bằng bao nhiêu? Giải thích sự khác biệt.
3. Liệt kê IP của các router và phân tích đường đi của gói tin từ nguồn đến đích thông qua lệnh tracert.

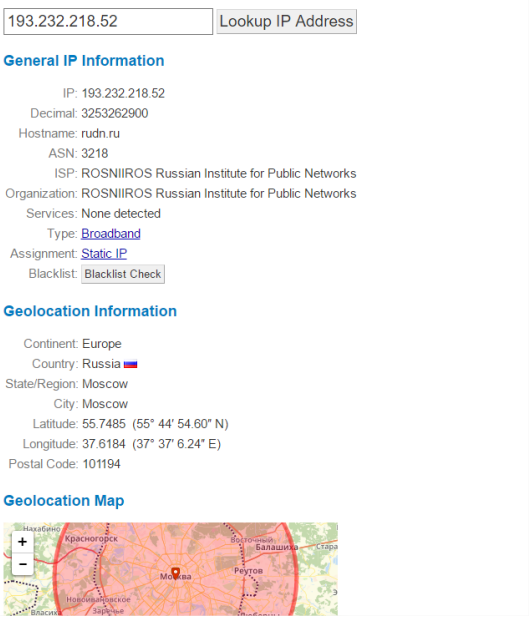
4. Xem chi tiết 1 cặp gói tin ICMP Request và Reply thành công khi thực hiện **tracert** và so sánh với 1 cặp gói ICMP Request và Reply khi thực hiện **ping** ở bài 1, cặp gói tin này có khác gì nhau không? Nếu có, hãy giải thích?
5. Xem chi tiết 1 gói tin ICMP lỗi (*Time-to-live Exceeded*) trong kết quả Wireshark, nó có nhiều trường thông tin hơn gói tin ICMP Reply thông thường. Những trường thông tin này bao gồm những gì và kích thước của chúng thế nào?
6. Trong quá trình **Tracert**, có đường liên kết (link) nào mà có thời gian trễ dài hơn đáng kể so với các link khác hay không?

   Căn cứ vào các tên Router có thể đoán biết được vị trí của 2 Router ở điểm kết thúc ở link này hay không?

   Nếu không thể đoán được, có thể dựa vào IP để tìm vị trí của 2 điểm đó.

   Gợi ý: *Ví dụ có thể xem lại hình 7 khi tracert đến website rudn.ru, tại điểm số 9 và 10 thì RTT thay đổi đáng kể so với các vị trí khác (từ ~59 đến 250).*

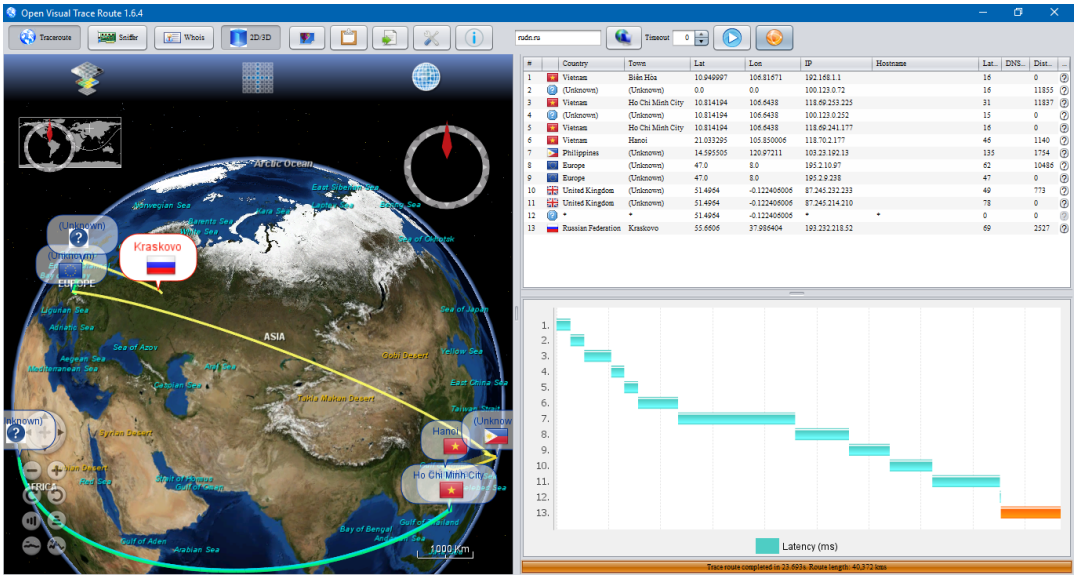
   Sinh viên có thể dùng trang http://whatismyipaddress.com/ để xác định vị trí 1 máy tính dựa vào IP.



Hình 10. Như ví dụ trên, dựa vào IP có thể xác định server đặt tại Moscow – Nga

7. ** **Mở rộng:** Sinh viên có thể dùng phần mềm Open Visual Trace (OVT) để có thể theo dõi quá trình Traceroute trực quan được thể hiện qua các vị trí địa lý trên bản đồ.*

OVT được cung cấp miễn phí tại *https://sourceforge.net/projects/openvisualtrace*



Hình 11. Traceroute với OVT

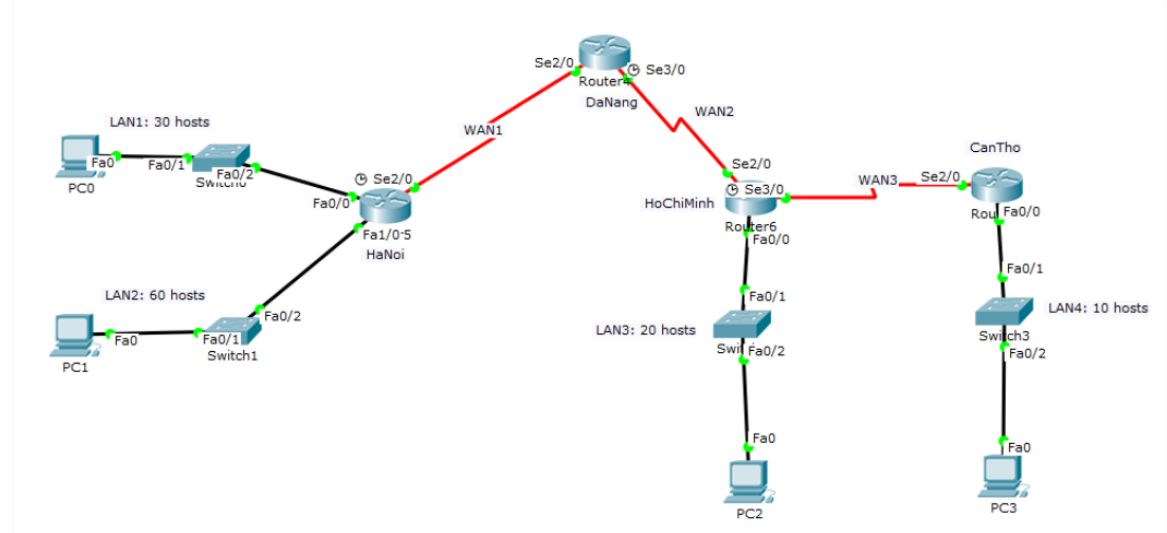
3. Địa chỉ IP và Chia mạng con (subnet)

Trước khi thực hành phần 3, trả lời các câu hỏi sau:

1. Địa chỉ IP dùng để làm gì? IP Private và IP Public là gì và được sử dụng trong trường hợp nào? Liệt kê các dãy IP Private.
2. Mạng con (subnet) là gì? Tại sao cần phải chia mạng con?
3. Subnet Mask là gì? Địa chỉ Broadcast là gì?

- **Bước 1:** Mỗi sinh viên sẽ được cấp địa chỉ IP ban đầu là 172.X.0.0/16 để chia mạng con. Trong đó X = 16 + (2 số cuối Mã số sinh viên % 16).

Áp dụng kiến thức về chia địa chỉ mạng con đã học để thực hiện chia mạng con phục vụ cho mô hình mạng như sau:



Ví dụ: Nếu có MSSV = 16520**01** → được cấp IP là 172.17.0.0/16 (X = 16 + 1%16)

Trong mô hình trên, yêu cầu chia thành 7 mạng con gồm:

- LAN1: 30 host
- LAN2: 60 host
- LAN3: 20 host
- LAN4: 10 host
- WAN1: 2 host
- WAN2: 2 host
- WAN3: 2 host

• **Bước 2:** Sử dụng kỹ thuật **FLSM** (*Fixed Length Subnet Mask – các mạng con có Subnet Mask giống nhau, chia mạng dựa trên số lượng mạng con*) hoặc **VLSM** (*Variable Length Subnet Mask – các mạng con có thể có Subnet Mask khác nhau, chia mạng dựa trên số lượng host của từng mạng con*) hoặc **cả 2 kỹ thuật**, tiến hành chia mạng con và **mô tả chi tiết cách thực hiện** và điền kết quả tổng hợp vào bảng sau:

Subnet	IP Address	Subnet Mask	IP khả dụng đầu tiên	IP khả dụng cuối cùng
LAN1				
LAN2				
LAN3				
LAN4				
WAN1				
WAN2				
WAN3				

C. YÊU CẦU

1. Yêu cầu

- Sinh viên tìm hiểu và thực hành theo hướng dẫn. Thực hiện **cá nhân.**
- Sinh viên báo cáo kết quả thực hiện và nộp bài bằng file. Trong đó:
  - Trình bày trong file Word (.docx) hoặc PDF theo mẫu có sẵn tại website môn học.
  - Đính kèm các file ***pcapng*** từ Wireshark kết quả bắt được.

Nén tất cả các file và đặt tên file theo định dạng theo mẫu: **[Mã lớp viết tắt]-LabX_MSSV-Họ Tên SV.** *Ví dụ: [I16.1]-Lab1_14520000-NguyenVietNam*

  - Nộp báo cáo trên theo thời gian đã thống nhất tại website môn học.

2. Đánh giá:

- Sinh viên hiểu và tự thực hiện được bài thực hành, đóng góp tích cực tại lớp.
- Báo cáo trình bày chi tiết, giải thích các bước thực hiện, chứng minh được do sinh viên tự thực hiện.

Kết quả thực hành cũng được đánh giá bằng kiểm tra trực tiếp tại lớp ngẫu nhiên vào cuối buổi thực hành hoặc vào buổi thực hành thứ 5.

Lưu ý: *Bài sao chép từ bạn khác, từ internet, nộp trễ sẽ bị xử lý tùy theo mức độ (-30% đến -90% số điểm)*

D. THAM KHẢO

[1] Giáo trình Mạng máy tính – Chương 4 – Tầng Network (ICMP, IP)

HẾT