**BÁO CÁO THỰC HÀNH ATHT**

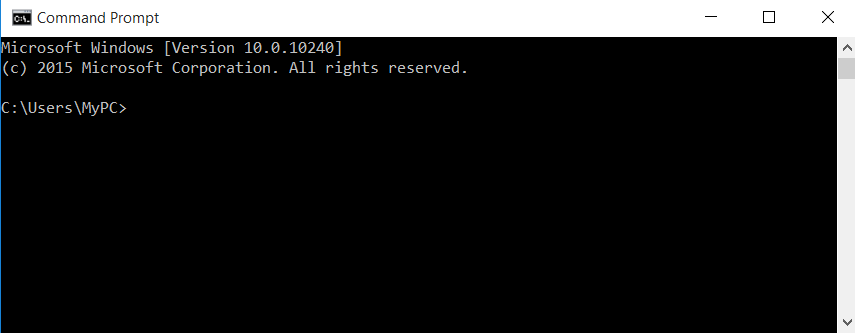
**BÀI 02**

MSSV: B1809365

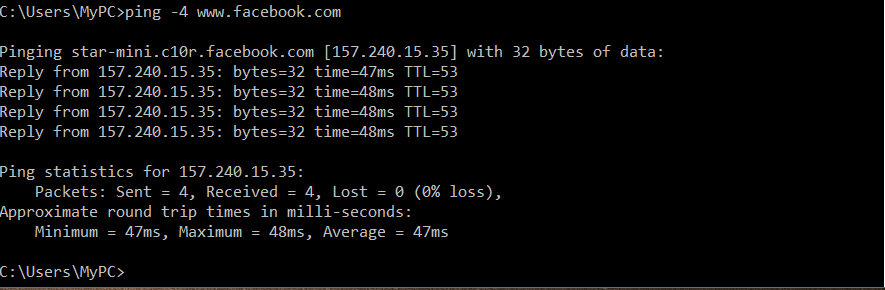
Họ Tên: Phạm Thị Hồng Linh

1. **Lab01 – Sử dụng lệnh ping để thăm dò hệ thống**

* Chọn [www.facebook.com](http://www.facebool.com) làm mục tiêu
* Mở Command Prompt



* Dùng lệnh **ping** [**www.facebook.com**](http://www.facebool.com)



* Website [www.facebook.com](http://www.facebool.com) có địa chỉ IP **157.240.15.35**
* Thông tin về số liệu thống kê trên lệnh Ping
* Gói gửi = 4
* Gói nhận = 4
* Gói bị mất = 0
* Kích thước mỗi gói là 32 bytes
* Thời gian sống của gói tin (TTL) là 53
* Approximate round trip times (Khoảng thời gian khứ hồi)

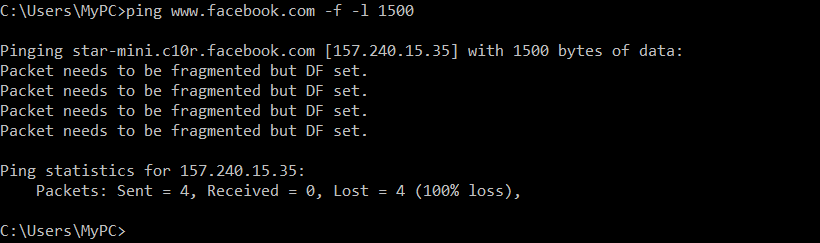
+ Nhỏ nhất = 47ms

+ Lớn nhất = 48ms

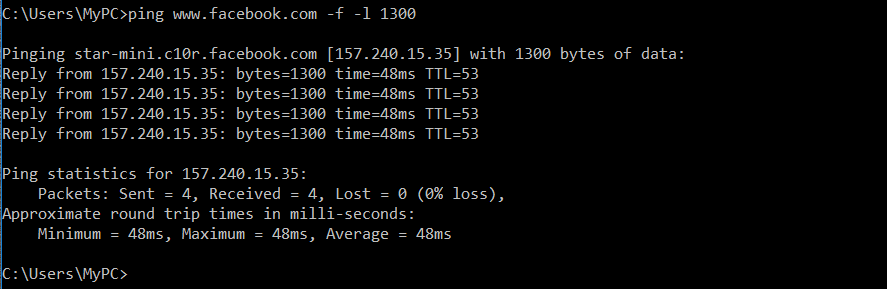
+ Trung bình = 47ms

* Dùng lệnh để xem số lượng bytes tối đa cho phép trên đường truyền:

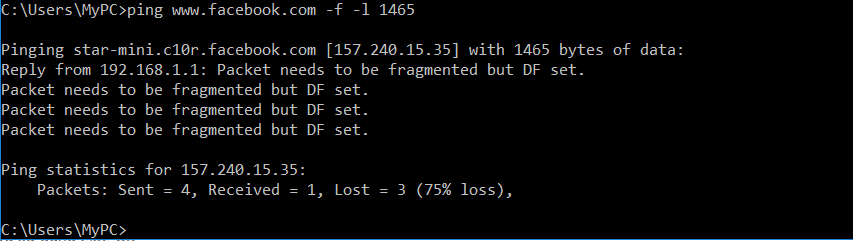
**ping** [**www.facebook.com**](http://www.facebool.com) **–f –l 1500**

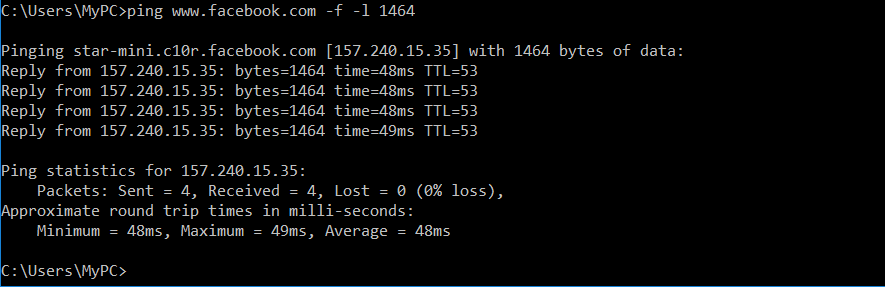


* Gói hiển thị cần được phân mảnh nhưng DF đặt có nghĩa là khung quá lớn để có trên mạng và cần được phân mảnh. Vì đã sử dụng -f với lệnh ping, gói tin không gửi được và lệnh ping trả về lỗi.
* Dùng lệnh **ping** [**www.facebook.com**](http://www.facebool.com) **–f –l 1300**

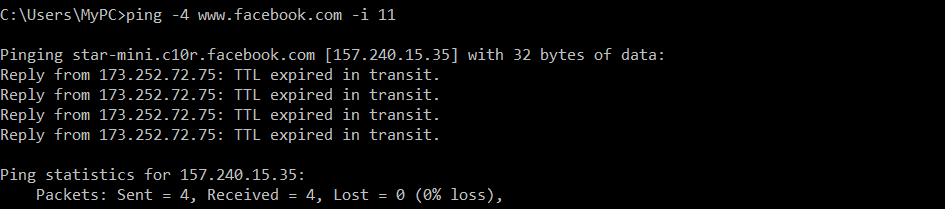


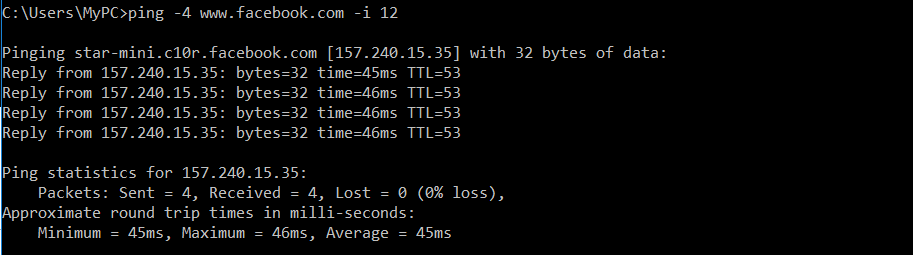
* Tiếp tục kiểm tra kích thước gói tin lớn nhất có thể truyền từ 1300 đến dưới 1500bytes
* Số lượng byte tối đa có thể truyền là: **1464** byte





* Tìm số nút trung gian đi qua bằng lệnh **ping -4** [**www.facebook.com**](http://www.facebool.com) **–i 11**

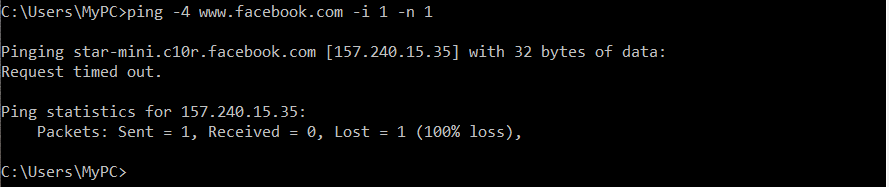


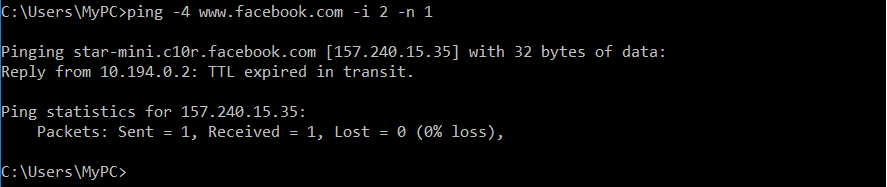


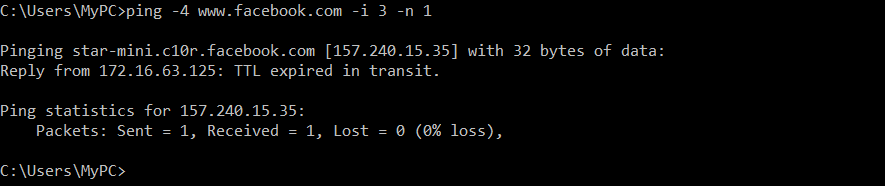
* Số nút trung gian đi qua là 12 nút.
* Dùng lệnh **tracert -4** [**www.facebook.com**](http://www.facebool.com)**.** Tracert là công cụ dòng lệnh nền tảng Windows dùng để xác định đường đi từ nguồn tới đích của một gói Giao thức mạng Internet (IP - Internet Protocol)

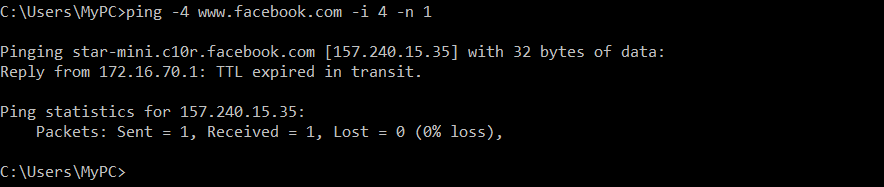


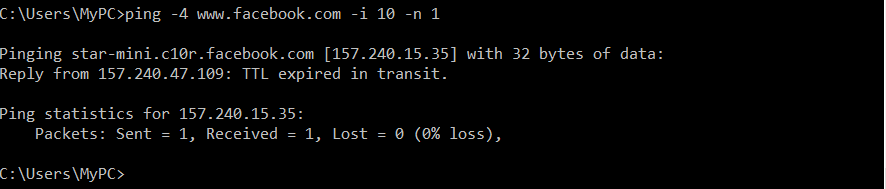
* Tìm số lượng router trung gian khi kết nối tới [www.facebook.com](http://www.facebook.com), giới hạn số lượng gói tin đi qua là 1, bằng lệnh: “**ping** [**www.facebook.com**](http://www.facebook.com) **–i 1 –n 1**” và tăng dần tham số -i

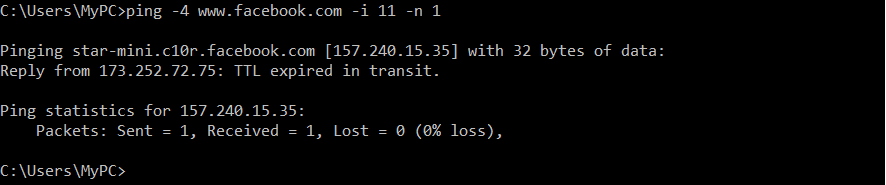




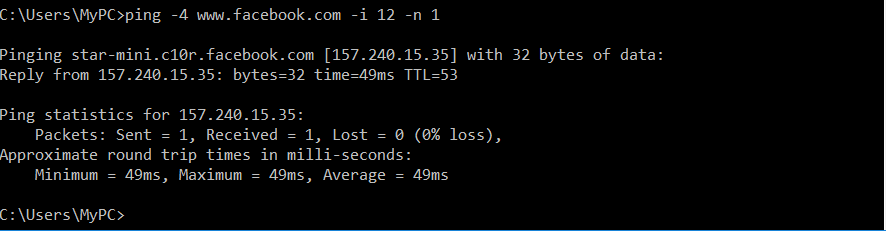








* Với i 11 thì địa chỉ IP 173.252.72.75 tương ứng với route thứ 11 của lệnh tracert



* Với tham số -i 12 thì ping tới [www.facebook.com](http://www.facebook.com) với địa chỉ IP: **157.240.15.35** tương ứng với route thứ 12 của lệnh tracert



* **Lab Analysis**

|  |  |
| --- | --- |
| **Tool/Utility** | **Information Collected/Objectives Achieved** |
| Ping | **IP Address:** 157.240.15.35 |
| **Packet Statistics:**   * Packets Sent – 4 * Packets Received – 4 * Packets Lost – 0 * Approximate Round Trip Time – 47ms |
| **Maximum Frame Size:** 1464 |
| **TTL Response:** 12 hops |

* **Question**

1. How does tracert (trace route) find the route that the trace packets are (probably) using?



**Answer:**

* **Tracert** tìm đường tới đích bằng cách gửi các thông báo Echo Request (yêu cầu báo hiệu lại) Internet Control Message Protocol (ICMP) tới từng đích. Sau mỗi lần gặp một đích, giá trị Time to Live (TTL), tức thời gian cần để gửi đi sẽ được tăng lên cho tới khi gặp đúng đích cần đến. Đường đi được xác định từ quá trình này

1. Is there any other answer ping could give us (except those few we saw before)?

**Answer:**

ping –r count,…

1. We saw before:

* Request timed out
* Packet needs to be fragmented but DF set
* Reply from XXX.XXX.XXX.XX: TLL expired 111 transit

What ICMP type and code are used for the ICMP Echo request?

**Answer:**

* Type 8: Echo Request (Ping Request, used with Type 0, Ping Reply)

1. Why does traceroute give different results on different networks (and

sometimes on the same network)?

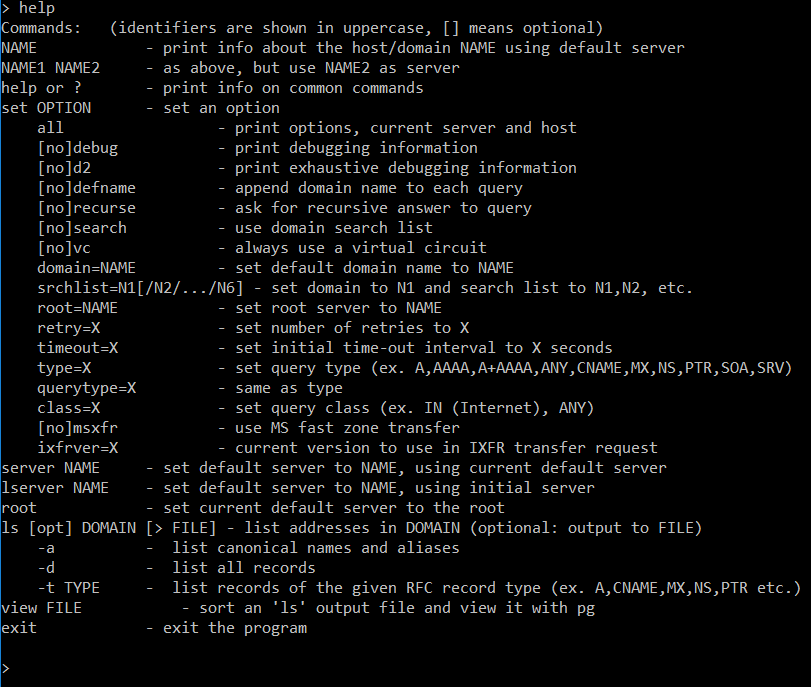
**Answer:**

* Do các bộ định tuyến các gói tin khác nhau.

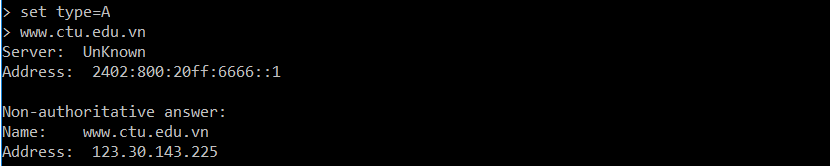
1. **Lab02 – Sử dụng lệnh nslookup để thăm dò hệ thống**
2. Mục tiêu: <www.ctu.edu.vn>
3. Mở Command Prompt
4. Gõ lệnh **nslookup**



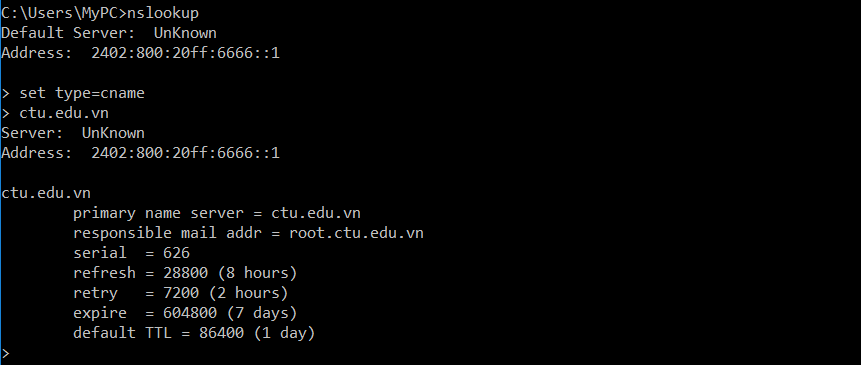
1. Gõ lệnh **help**



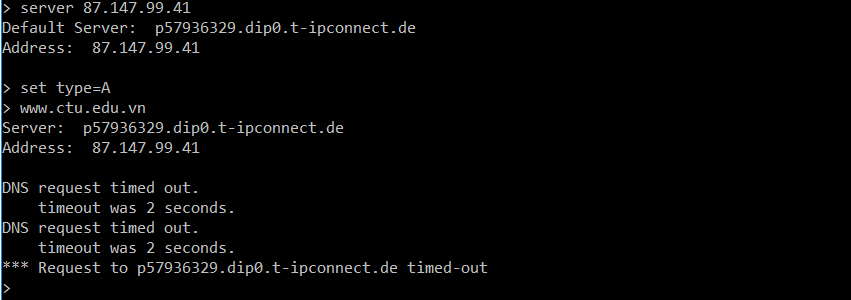
1. Thiết lập các loại mẫu tin DNS:
2. Loại A (Address): Ánh xạ hostname tới địa chỉ IP:



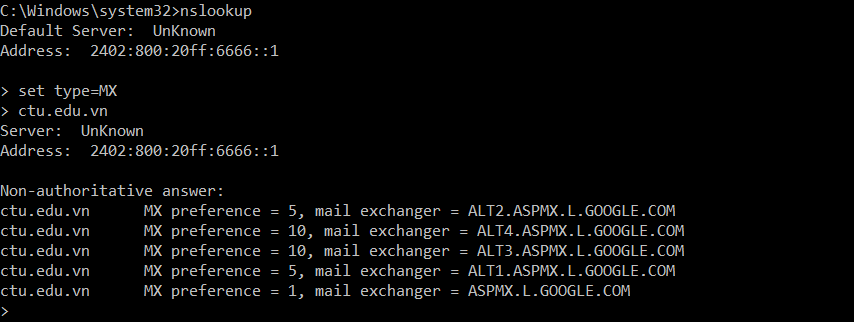
1. Câu trả lời không chính chủ: Non-authoritative answer
2. Loại CNAME (Canonical Name): Cung cấp tên hay bí danh cho mẫu tin địa chỉ



1. Gõ lệnh “server 87.147.99.41” một địa chỉ IP bất kỳ, và “set type=A”



1. Kết quả nhận *DNS request timed out* do tường lửa đã ngăn chặn kết nối DNS bên ngoài mạng LAN
2. Gõ set type=MX -> (Mail Exchange): Xác định mail server cho miền



* Lab Analysis

|  |  |
| --- | --- |
| **Tool/Utility** | **Information Collected/Objectives Achieved** |
| nslookup | **DNS Server Name: 2402:800:20ff:6666::1 (địa chỉ MAC)** |
| **Non-Authoritative Answer:** 123.30.143.225 |
| **CNAME (Canonial Name of an alias):**   * **Alias:** ctu.edu.vn * **Canonial Name:** Unknown |
| **MX (Mail Exchanger):**   * ASPMX.L.GOOGLE.COM * ALT1.ASPMX.L.GOOGLE.COM * ALT2.ASPMX.L.GOOGLE.COM * ALT3.ASPMX.L.GOOGLE.COM * ALT4.ASPMX.L.GOOGLE.COM |

* **Question**

1. Analyze and determine each of the following DNS resource records:

* SOA (Start of Authoriy): Xác định DNS Server có nhiệm vụ thông tin miền.
* A (Address): Ánh xạ hostname tới địa chỉ IP:
* PTR (Pointer): Ánh xạ địa chỉ IP thành tên máy chủ
* CNAME (Canonical Name): Cung cấp tên hay bí danh cho mẫu tin địa chỉ
* MX (Mail Exchange): Xác định mail server cho miền
* SRV (Pointer): Ánh xạ địa chỉ IP thành tên máy chủ

1. Evaluate the difference between an authoritative and non-audioritative answer

* Authoritative: Máy chủ DNS có thẩm quyền chịu trách nhiệm ánh xạ các bản ghi thích hợp và phản hồi lại các máy chủ đệ quy với thông tin quan trọng cho mỗi trang web, chẳng hạn như; địa chỉ IP tương ứng và các bản ghi DNS cần thiết khác. Truy vấn đã được cấu hình từ trước trong source nguồn, có thể là master hoặc slave
* Non-audioritative: Máy chủ định danh không có thẩm quyền không chứa các tệp vùng gốc. Chúng có thể có bộ nhớ cache với các bản ghi DNS được yêu cầu trước đó từ tất cả các lần tra cứu DNS đã thực hiện trước đó. Nếu máy chủ DNS phản hồi một truy vấn DNS không có tệp vùng, thì đó là câu trả lời không có thẩm quyền. Truy vấn được lấy từ authoritative server

1. Determine when you will receive request time out in nslookup.

* Do máy chủ gặp sự cố hay tường lửa chặn DNS khi truy cập bằng máy tính công cộng Do máy chủ gặp sự cố hay tường lửa chặn DNS khi truy cập bằng máy tính công cộng.

*--Hết--*