**Họ Tên SV: Le Quang Sang**

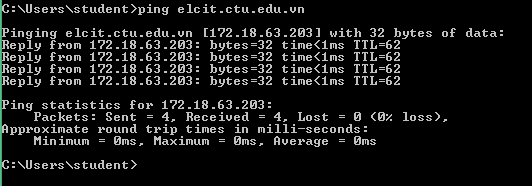
**MSSV: B1606927**

**Buổi 1:**

**AN TOÀN HỆ THỐNG**

Bài 1: Thăm dò hệ thống bằng Footprinting

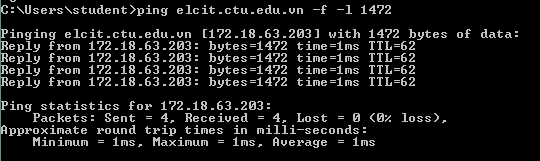
Bước 1: **ping elcit.ctu.edu.vn Địa chỉ IP: 172.18.63.203**



Bước 2: Xác định định số khung tải tối đa

**ping elcit.ctu.edu.vn -f -l [Kích thước]**

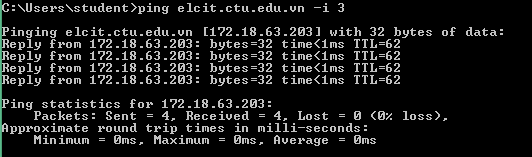
**Maximum frame size: 1472**



Bước 3: Xác định số bước nhảy:

**ping elcit.ctu.edu.vn –i [Số bước nhảy]**

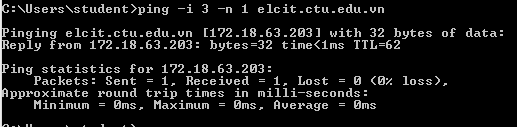
**Số bước nhảy: 3**



Bước 4: Sử dụng tham số trả về -n 1

**ping –i 3 –n 1 elcit.ctu.edu.vn**

ping đến 1 lần cho 1 kết quả trả về:



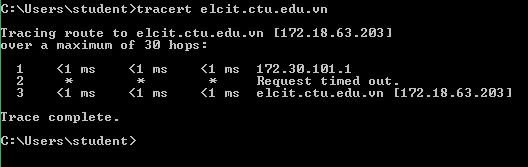
**Bảng Kết quả:**

|  |  |
| --- | --- |
| **Tool/Utility** | **Information Collected/Objectives Achieved** |
| **ping** | **IP Address:** 172.18.63.30 |
| **Packet Statistics:**  ■ Packets Sent — 4  ■ Packets Received — 4  ■ Packets Lost — 0  ■ Approximate Round Trip Time — 0ms |
| **Maximum Frame Size:** 1472 |
| **TTL Response:** 3 hops |

**Trả lời Câu hỏi:**

**Q1:**

**tracert www.ctu.edu.vn**



Tiện ích chẩn đoán TRACERT xác định đường đến một đích bằng cách gửi gói echo Giao thức Thông báo Điều khiển Internet (ICMP) đến đích. Trong các gói này, TRACERT sử dụng các giá trị Thời gian Tồn tại (TTL) IP liên tục thay đổi. Vì mỗi bộ định tuyến theo đường dẫn phải giảm TTL của gói tối thiểu 1 trước khi chuyển tiếp gói nên TTL là một bộ đếm bước nhảy hiệu quả. Khi TTL trên một gói đạt đến không (0), bộ định tuyến sẽ gửi một thông báo "Đã quá Thời gian" ICMP lại cho máy tính nguồn. TRACERT gửi gói echo đầu tiên với TTL bằng 1 và tăng TTL thêm 1 trên mỗi lần chuyển tiếp theo, cho đến khi đích đáp ứng hoặc đạt đến TTL tối đa. Thông báo "Quá Thời gian" ICMP mà bộ định tuyến trung gian gửi lại hiển thị đường

**Q2:** Chung ta cũng có thể nhận được số packet tùy ý chúng ta muốn. và một số ví dụ chúng ta có thê tìm kiếm trong option ping --help

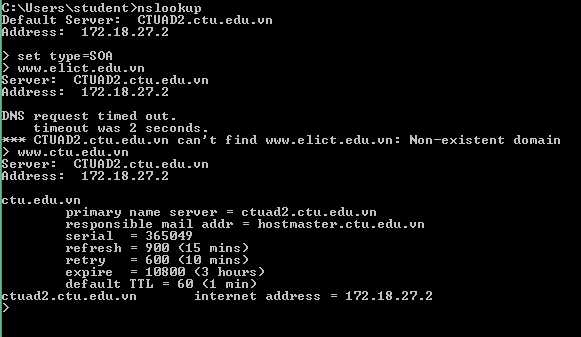
**Q3:**

* Request timed out: 2.
* Packet needs to be fragmented but DF set: 1473
* Reply from XXX.XXX.XXX.XX: TTL: Thời gian sống của gói tinh (time to live)
* ICMP : Internet control message protocal là giao thức của gói tinh internet cho các router chỉ ra các dịch vụ có tổn tại hay không.

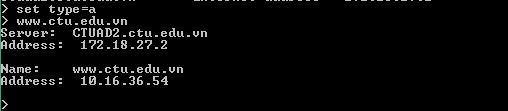
**Q4:** Do nghẽn mạng nên bộ vạch đường của router cho ra các đường đi khác nhau để đảm bảo gói tin đến dích và nhanh nhất.

Bài 2: Thăm dò hệ thống bằng Nslookup

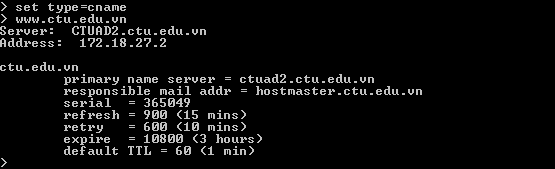
Bước 1:Xác định tên miền chính (set type=SOA)



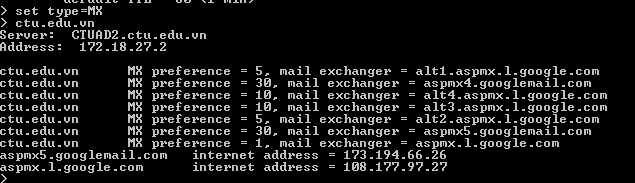
Bước 2:Xác định IP host của www.ctu.edu.vn (set type=a)



Bước 3: Cung cấp tên (set type=CNAME)



Bước 4: Mail server của www.ctu.edu.vn (set type=MX)



**Bảng Kết quả:**

|  |  |
| --- | --- |
| **Tool/Utility** | **Information Collected/Objectives Achieved** |
| **nslookup** | **DNS Server Name:** 172.18.27.2 |
| **Non-Authoritative Answer:** |
| **CNAME (Canonical Name of an alias)**  ■ **Alias:** ctu.edu.vn  ■ **Canonical name:** ctuad2.ctu.edu.vn |
| **MX (Mail Exchanger):**  + alt1.aspmx.1.google.com  + aspmx4.googlemail.com  + alt4.aspmx.1.google.com  + alt3.aspmx.1.google.com  + alt2.aspmx.1.google.com  + aspmx5.googlemail.com  +aspmx.1.google.com |

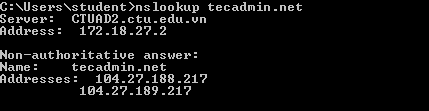
**Trả lời Câu hỏi:**

**Q1:**

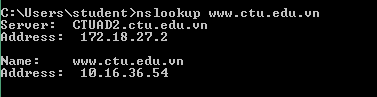
* **SOA:** Xác định DNS Server có nhiệm vụ thông tin miền.
* **NS:** Xác định Name Server khác cho miền.
* **A**: Ánh xạ hostname tới địa chỉ IP.
* **PTR**: Ánh xạ địa chỉ IP thành tên máy chủ.
* **CNAME**: Cung cấp tên hay bí danh cho mẫu tin địa chỉ.
* **MX**: Xác định mail server cho miền.
* **SRV**: Xác định những dịch vụ như dịch vụ thư mục.

**Q2:**

**Non-Authoritative DNS Server:** là server không chứa các tập tin gốc của server chính. Phản hồi được coi là server không xác thực



**Authoritative DNS Server:** là máy chủ phân giải tên miền có chứa các tập tin gốc của tên miền.



**Q3:** chúng ta nhận được thông báo request time out khi chúng ta yêu cầu phân giải tên miền mà không được phản hồi.