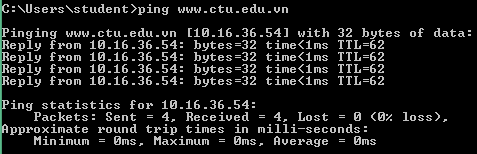
BÀI THỰC HÀNH AN TOÀN HỆ THỐNG BUỔI 1

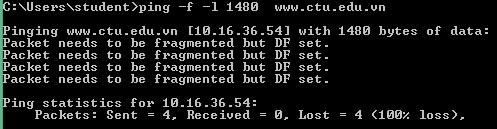
Nguyễn Phước Thành

B1610669

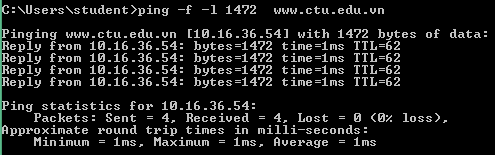
**PING**

1. Ping địa chỉ tìm IP của trang [www.ctu.edu.vn](http://www.ctu.edu.vn)



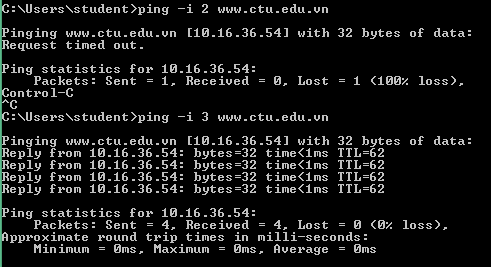
1. Kích thước khung tối đa của trang [www.ctu.edu.vn](http://www.ctu.edu.vn) 





Kích thước khung tối đa chỉ ra giữa 1300byte và 1472byte đều là khung tối đa trên máy thiếc mạng.

1. Tìm số bước nhảy đến [www.ctu.edu.vn](http://www.ctu.edu.vn)



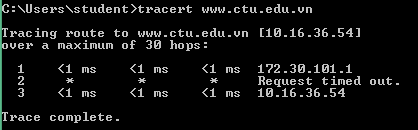
Điền tất cả địa chỉ IP, trả lời địa chỉ IP theo yêu cầu và TTLs:

|  |  |
| --- | --- |
| Tool/Utility | Information Collected/Objective Achieved |
| **Ping** | **IP Address**: 10.16.36.54 |
| **Packet Statistics**:   * Packets Sent – 3 * Packets Received – 3 * Packets Lost – 0 * Approximate Round Trip Time – 0ms |
| **Maximum Frame Size**: 1472 |
| **TTL Response**: 3 hops |

Question:

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

(probably) using?



Bằng cách gửi một gói echo Giao thức Thông báo Điều khiển Internet(ICMP) đến đích. Trong cách gói này, TRACERT sử dụng các giá trị Thời gian Tồn tại (TTL) IP liên tục thay đổi. Khi qua mỗi Router giá trị của TTL giảm đi 1, nên khi đạt giá trị 0 bộ định tuyễn sẽ gửi thông báo “Request timed out” ICMP về source để hiện thị lại đường.

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

- Giao thức ICMP (Internet Control Message Protocol).

3. We saw before:

י Request timed out

י Packet needs to be fragmented but DF set

י Reply from XXX.XXX.XXX.XX: TI L expired 111 transit

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

* Có 2 loại và mã sử dụng cho ICMP Echo:

Type 0: Echo Reply, Code: 0.

Type 0: Echo Request, Code: 0.

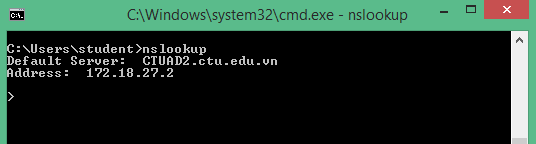
4. Why does traceroute give different results on different networks (and

sometimes on the same network)?

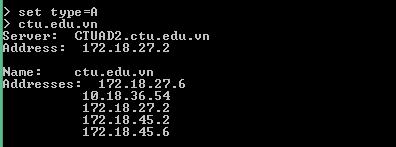
* Do các bộ định tuyến các gói tin khác nhau.

**Nslookup**

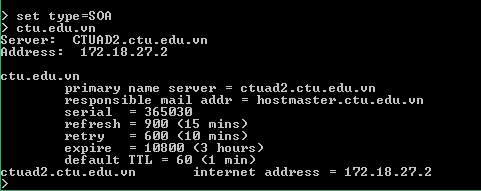
1. Tra cứu tên máy chủ



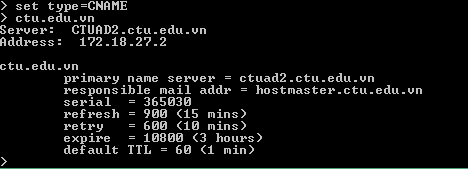
1. Các loại mẫu tin DNS
   * Loại A



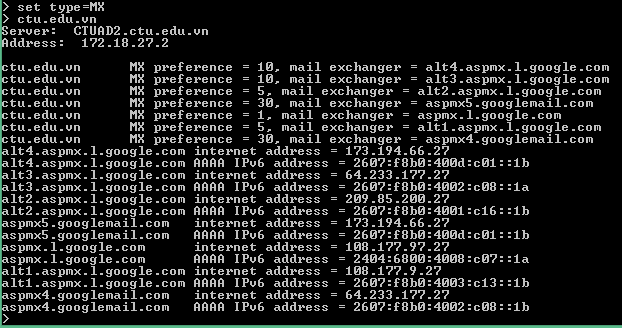
* + Loại SOA



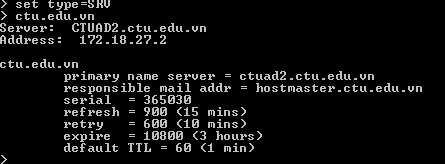
* + Loại CNAME



* + Loại MX



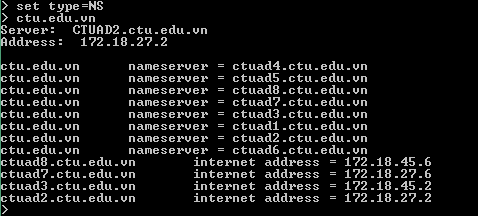
* + Loại SRV



* + Loại PTR



* + Loại NS



|  |  |
| --- | --- |
| Tool/Utility | Information Collected/Objective Achieved |
| **Nslookup** | **DNS Server Name:** 172.18.27.2 |
| **Non-Authoritative Answer:**   * 172.18.27.6 * 10.18.36.54 * 172.18.27.2 * 172.18.45.2 * 172.18.45.6 |
| **CNAME (Canonical Name of an alias):**   * **Alias:** ctu.edu.vn * **Canonical name:** CTUAD2.ctu.edu.vn |
| **MX (Mail Exchanger):**   * aspmx5.googlemail.com * aspmx.l.google.com * alt1.aspmx.l.google.com * aspmx4.googlemail.com * alt4.aspmx.l.google.com * alt3.aspmx.l.google.com * alt2.aspmx.l.google.com |

Question:

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

■ SOA: Xác định DNS Server có nhiệm vụ thông tin miền.

■ NS: Xác định Name Sever 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.

2. Evaluate the difference between an authoritative and non-authoritative

answer.

|  |  |
| --- | --- |
| Authoritative | Non-Authoriatative |
| * Truy vẫn đã được cấu hình từ trước trong source nguồn. * Bản thân có thể là master hoặc slave. * Kết quả nhận được đến từ một truy vẫn đã được cấu hình | * Truy vẫn được lấy từ authoritative server * Trả lời từ lookup trước được lấy ra từ cache * Kết quả nhận được không phải đến từ một authoritative server |

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

DNS đã hết thời gian yêu cầu có nghĩa là nslookup đã gửi truy vấn nhưng không nhận được phản hồi, cũng có thể do máy chủ DNS gặp sự cố hoặc lỗi mạng.