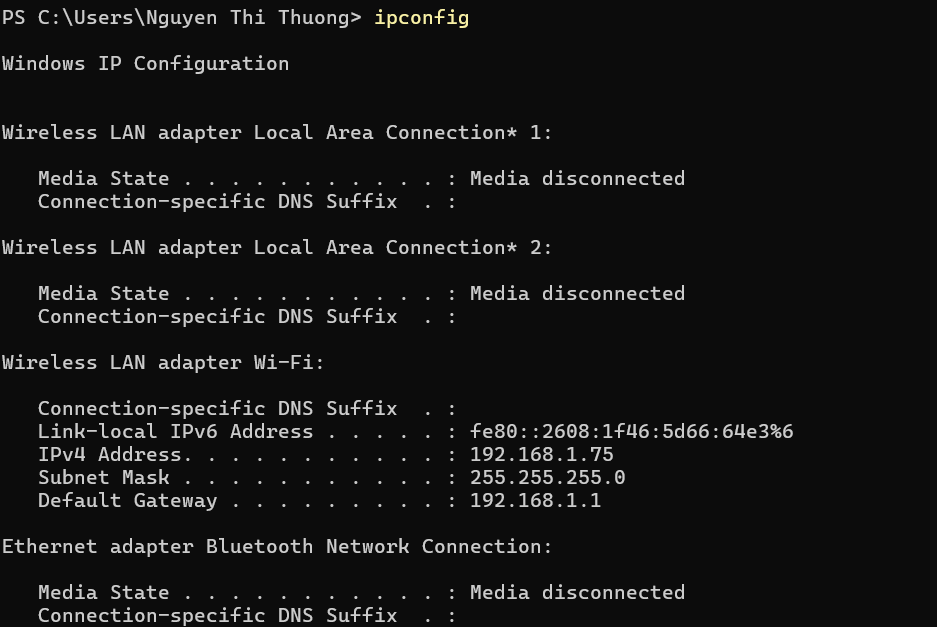
TÌM HIỂU CÁC LỆNH CƠ BẢN VỀ MẠNG

1. Lệnh **ipconfig**

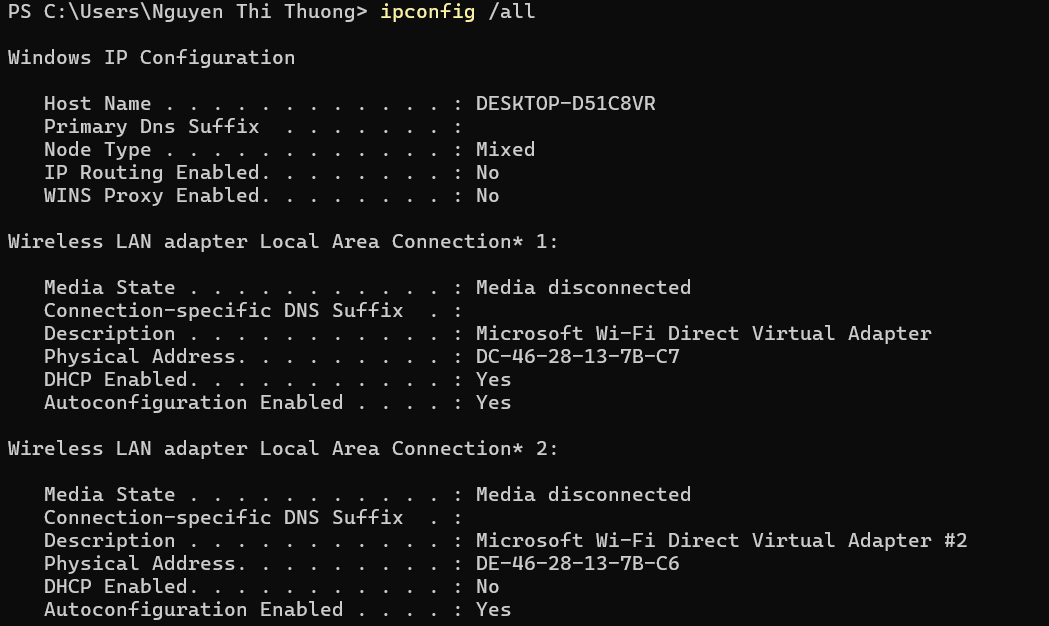
* Chức năng: Lệnh ipconfig trong Windows được sử dụng để hiển thị thông tin về cấu hình IP của các adapter mạng trên máy tính. Nó cung cấp thông tin về địa chỉ IP, subnet mask, gateway mặc định, địa chỉ IPv6, và trạng thái kết nối của từng adapter mạng.
* Cú pháp:ipconfig
* Kết quả thực hiện (hình ảnh):

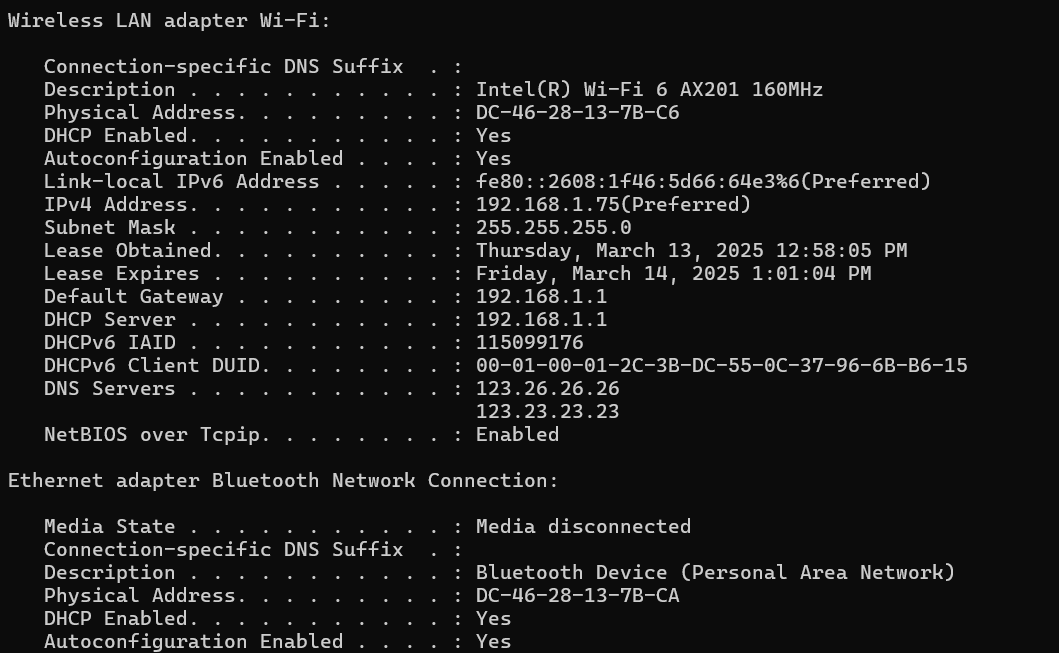


* Phân tích kết quả:
* *Wireless LAN adapter Local Area Connection 1 & 2:*\*
* Trạng thái: Media disconnected → Hai adapter mạng này không được kết nối.
* **Wireless LAN adapter Wi-Fi:**
* IPv4 Address: 192.168.1.75 → Địa chỉ IP nội bộ của máy tính trong mạng.
* Subnet Mask: 255.255.255.0 → Địa chỉ lớp mạng C, giới hạn trong phạm vi 192.168.1.x.
* Default Gateway: 192.168.1.1 → Địa chỉ IP của router/gateway giúp kết nối với mạng khác hoặc internet.
* Link-local IPv6 Address: fe80::2608:1f46:5d66:64e3%6 → Địa chỉ IPv6 cục bộ, chỉ có hiệu lực trong mạng nội bộ.
* **Ethernet adapter Bluetooth Network Connection:**
* Trạng thái: Media disconnected → Không có kết nối qua Bluetooth.

1. **ipconfig /all**

* Chức năng:
* Lệnh ipconfig /all được sử dụng để hiển thị thông tin chi tiết về tất cả các bộ điều hợp mạng (network adapter) trên máy tính, bao gồm:
* Địa chỉ IPv4 và IPv6
* Địa chỉ MAC (Physical Address)
* Máy chủ DHCP, DNS
* Gateway mặc định
* Trạng thái DHCP
* Lease Time (thời gian cấp phát IP)
* Lệnh này thường được dùng để kiểm tra kết nối mạng, xác định địa chỉ IP, khắc phục sự cố mạng hoặc cấu hình lại hệ thống mạng.
* Cú pháp: ipconfig /all
* Kết quả thực hiện (hình ảnh):

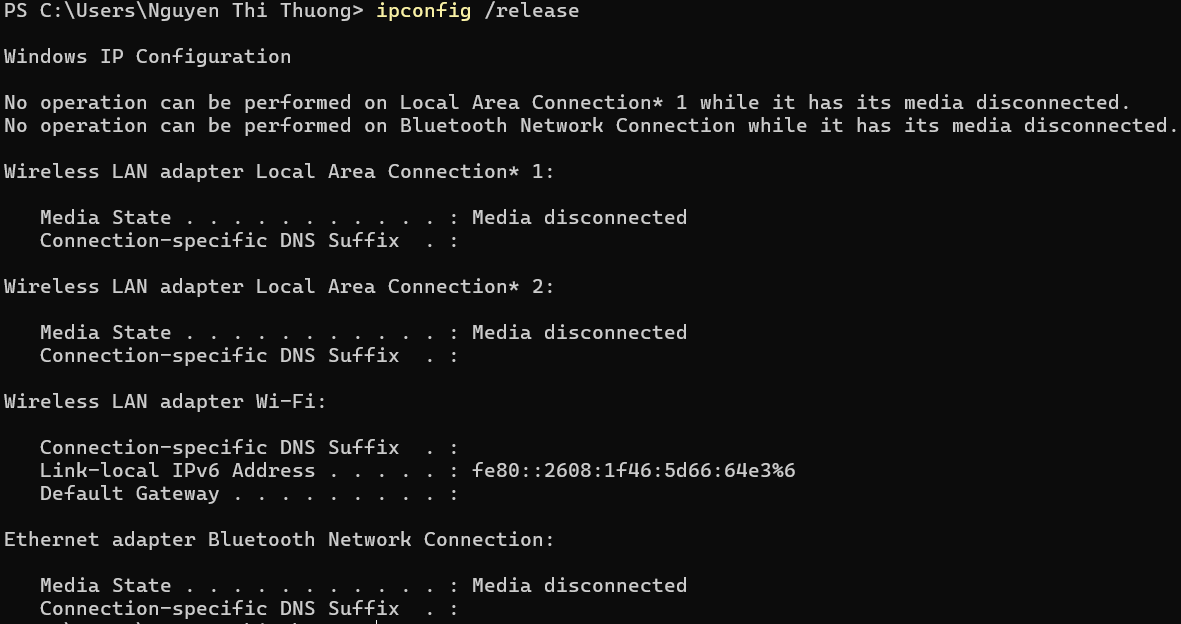




* Phân tích kết quả:
* **Thông tin chung về Windows IP Configuration**
* Host Name: DESKTOP-D51C8VR (Tên máy tính)
* Node Type: Mixed
* IP Routing Enabled: No (Không bật định tuyến IP)
* WINS Proxy Enabled: No
* **Thông tin bộ điều hợp mạng không dây (Wi-Fi Adapter)**
* **Mô tả (Description):** Intel(R) Wi-Fi 6 AX201 160MHz
* **Địa chỉ vật lý (MAC Address):** DC-46-28-13-7B-C6
* **DHCP Enabled:** Yes (Được cấp phát IP động)
* **IPv4 Address:** 192.168.1.75 (Địa chỉ IP nội bộ)
* **Subnet Mask:** 255.255.255.0
* **Default Gateway:** 192.168.1.1 (Cổng ra mạng)
* **DNS Servers:** 123.26.26.26, 123.23.23.23
* **Lease Obtained:** March 13, 2025 12:58:05 PM
* **Lease Expires:** March 14, 2025 1:01:04 PM
* **Thông tin bộ điều hợp Bluetooth (Bluetooth Network Connection)**
* Trạng thái: Media Disconnected (Không kết nối)
* **Các bộ điều hợp mạng ảo (Wi-Fi Direct Virtual Adapter)**
* Local Area Connection\* 1 & Local Area Connection\* 2
* Media State: `Media Dis

1. **ipconfig /release**

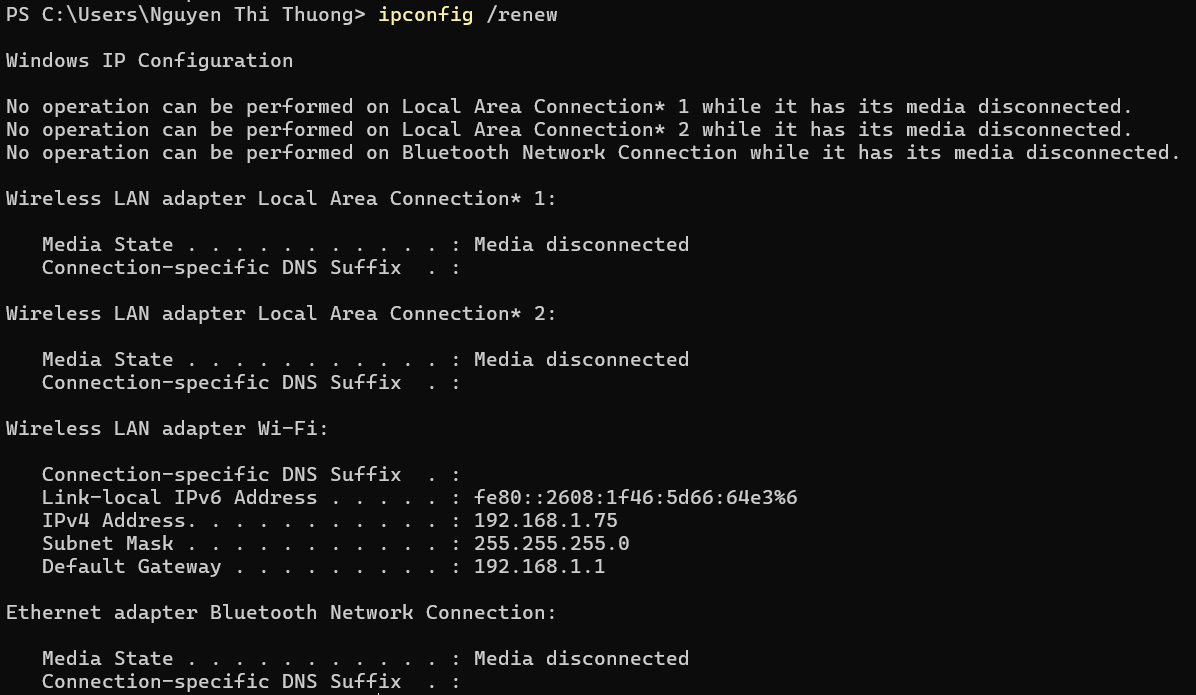
* Chức năng: Lệnh ipconfig /release được sử dụng để giải phóng (release) địa chỉ IP hiện tại mà bộ điều hợp mạng (network adapter) đã nhận từ DHCP server. Khi thực hiện lệnh này, máy tính sẽ mất kết nối với mạng cho đến khi nhận lại địa chỉ IP mới.
* Cú pháp: ipconfig /release
* Kết quả thực hiện (hình ảnh):



* Phân tích kết quả:
* *Wireless LAN adapter Local Area Connection 1:*\*
* **Trạng thái Media:** Media disconnected (không có kết nối)
* *Wireless LAN adapter Local Area Connection 2:*\*
* **Trạng thái Media:** Media disconnected
* **Wireless LAN adapter Wi-Fi:**
* **IPv6 Address:** fe80::2608:1f46:5d66:64e3%6 (địa chỉ link-local)
* **Default Gateway:** Không hiển thị (đã mất kết nối)
* **Ethernet adapter Bluetooth Network Connection:**
* **Trạng thái Media:** Media disconnected
* **Các bộ điều hợp mạng có trạng thái "Media disconnected"** → Không có kết nối vật lý hoặc không có địa chỉ IP hợp lệ.
* **Wi-Fi adapter bị mất Default Gateway** → Địa chỉ IP đã bị giải phóng, không thể kết nối Internet cho đến khi thực hiện ipconfig /renew.
* **Không có IPv4 Address** → Chứng tỏ máy đã mất IP do lệnh release.

1. **ipconfig /renew**

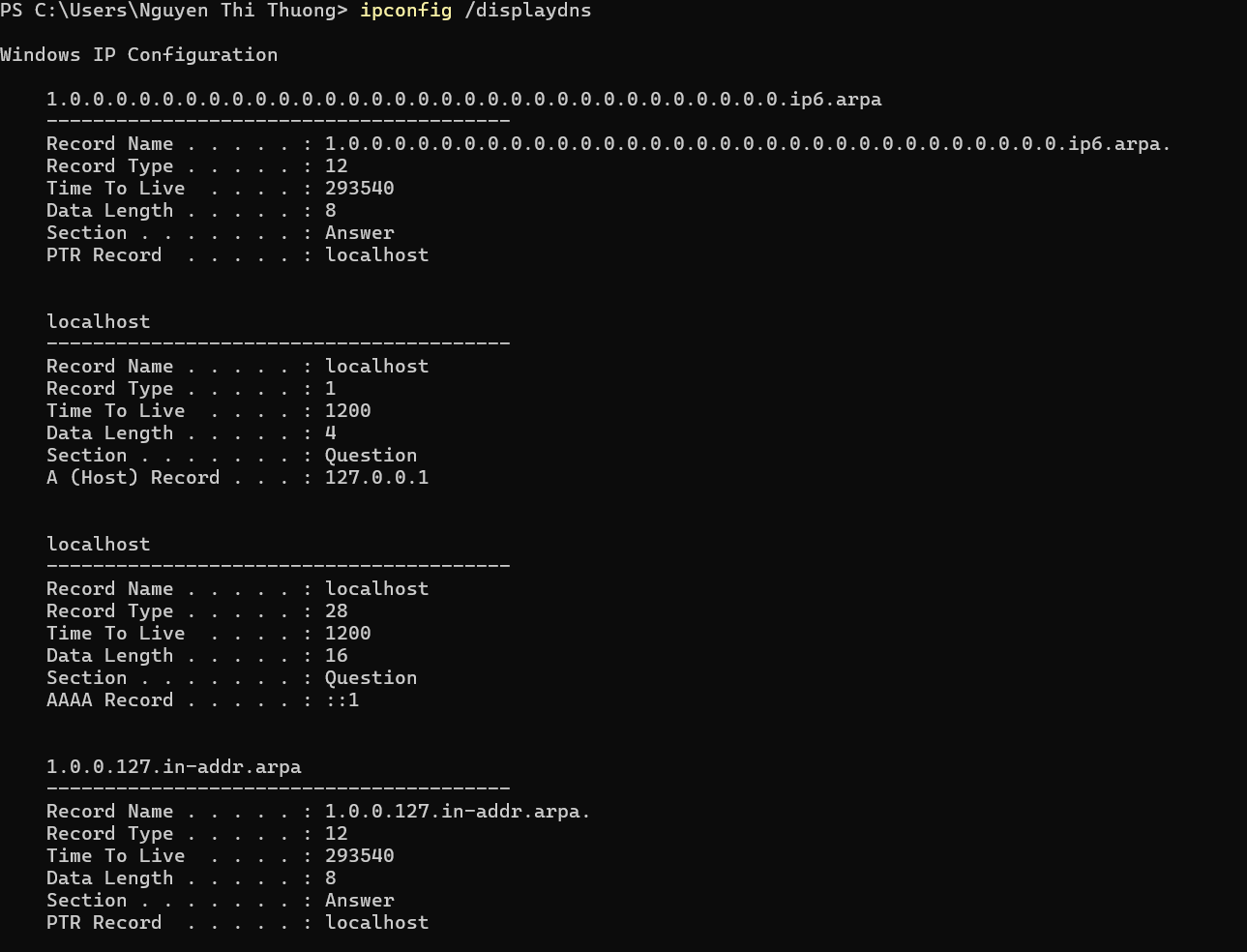
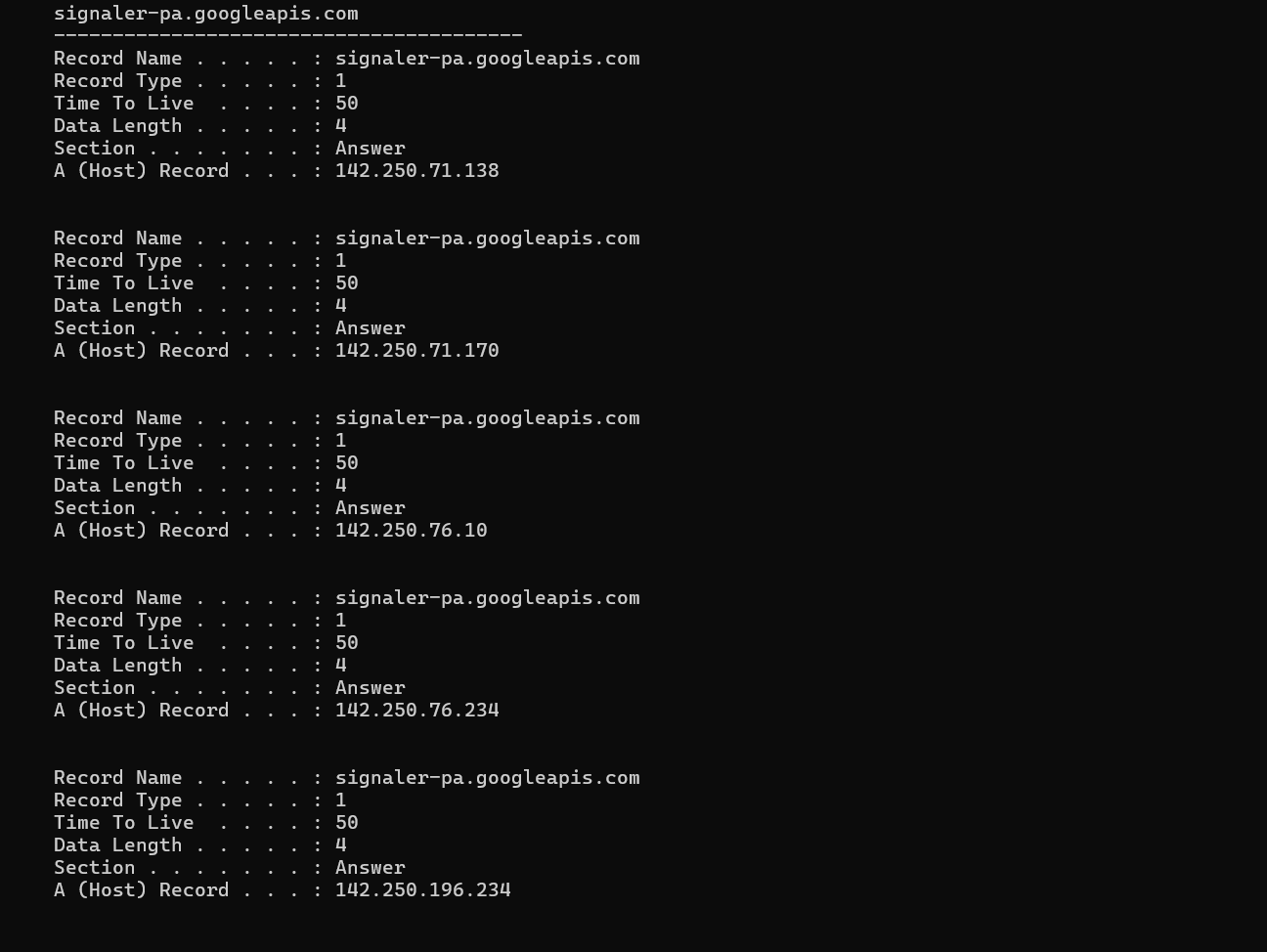
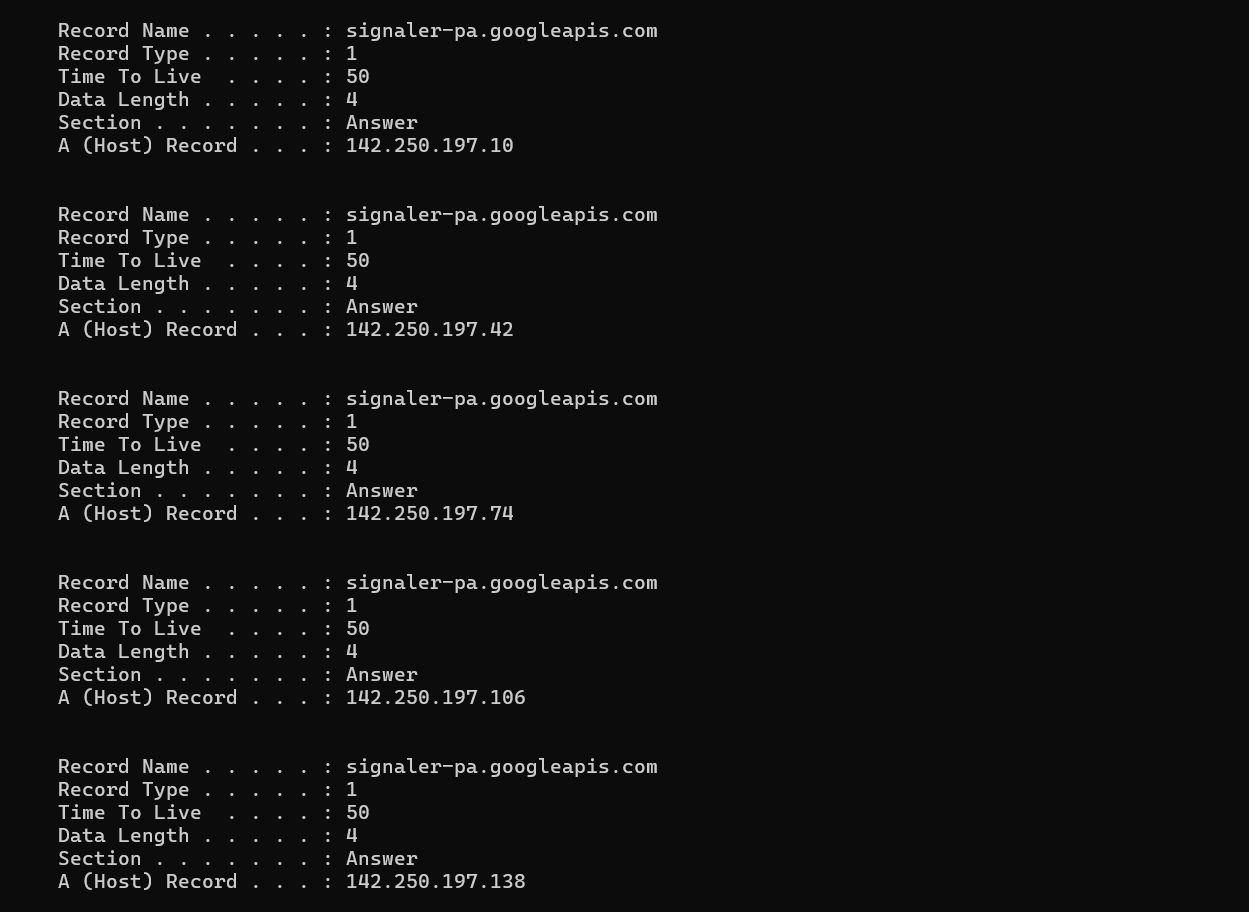
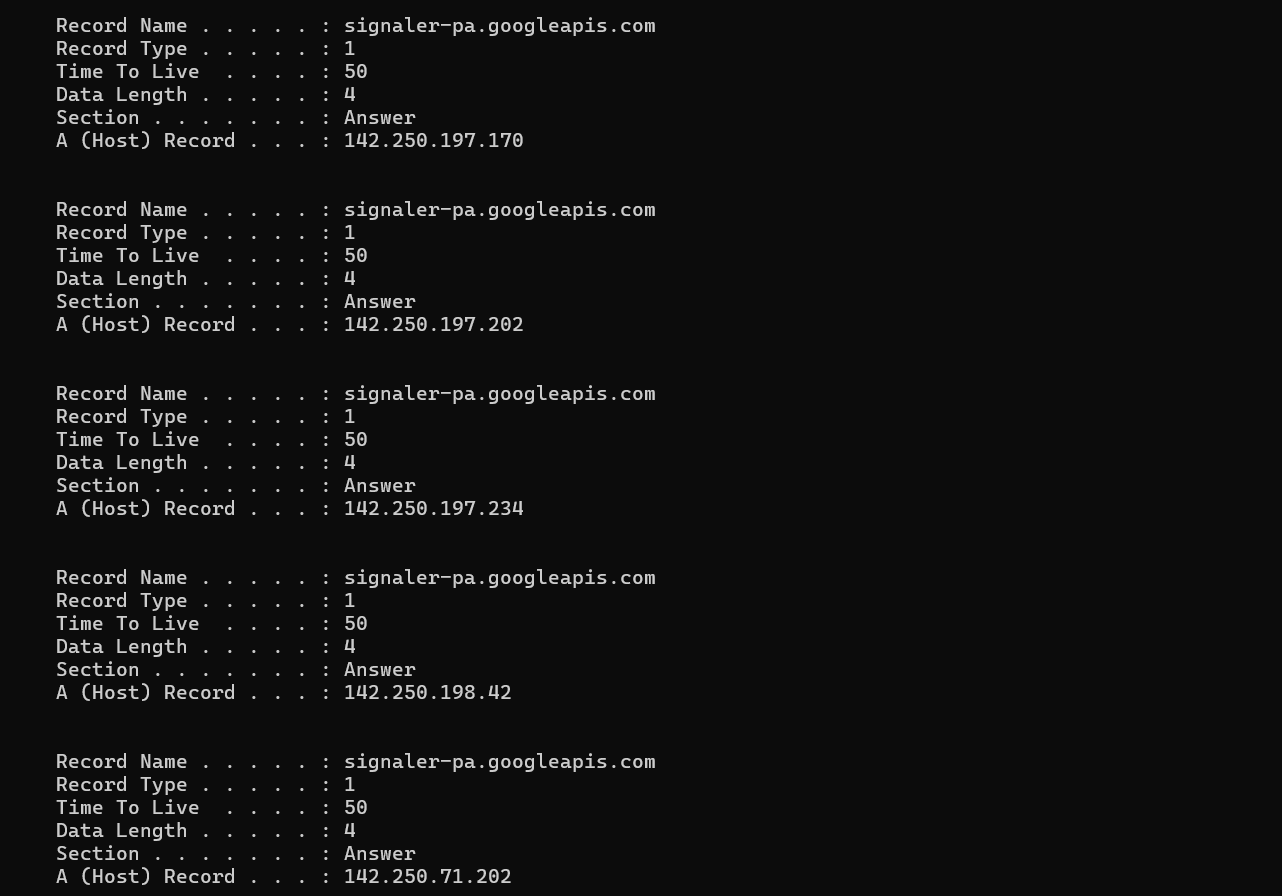
* Chức năng: Lệnh ipconfig /renew được sử dụng để yêu cầu DHCP cấp lại địa chỉ IP mới cho các bộ điều hợp mạng (network adapter) sau khi đã bị giải phóng bởi lệnh ipconfig /release.
* Cú pháp: ipconfig /renew
* Kết quả thực hiện (hình ảnh)



* Phân tích kết quả:
* **Các adapter không kết nối (Media disconnected):**
* Local Area Connection\* 1
* Local Area Connection\* 2
* Bluetooth Network Connection
* Các adapter này không kết nối hoặc không có cáp mạng cắm vào.
* **Wireless LAN adapter Wi-Fi (Đang hoạt động):**
* **Địa chỉ IPv6:** fe80::2608:1f46:5d66:64e3%6
* **Địa chỉ IPv4:** 192.168.1.75 (được cấp bởi DHCP từ router).
* **Subnet Mask:** 255.255.255.0 (mạng nội bộ chuẩn).
* **Default Gateway:** 192.168.1.1 (địa chỉ router, dùng để truy cập Internet).

1. **ipconfig /displaydns**

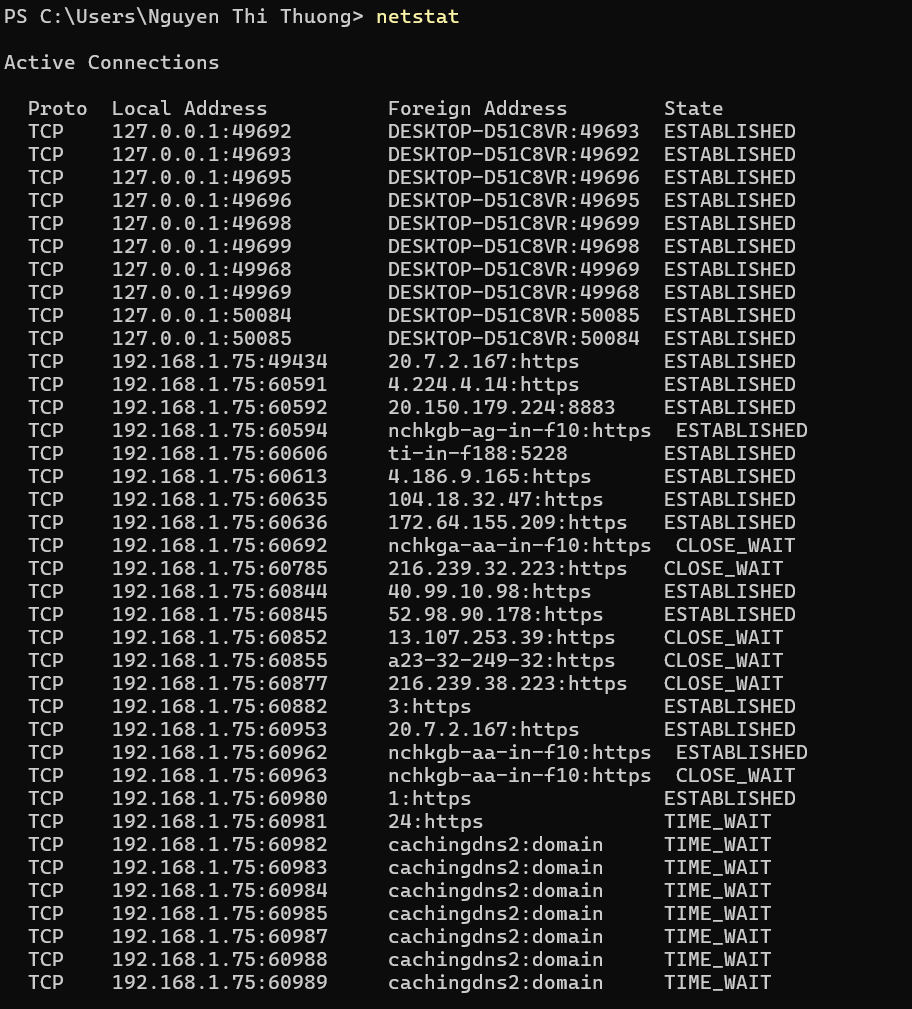
* Chức năng: Lệnh ipconfig /displaydns trong Windows được sử dụng để hiển thị bộ nhớ cache DNS (DNS Resolver Cache) của hệ thống. Bộ nhớ cache này lưu trữ các bản ghi DNS đã được phân giải trước đó để tăng tốc độ truy cập internet và giảm độ trễ khi truy vấn các tên miền.
* Cú pháp: ipconfig /displaydns
* Kết quả thực hiện (hình ảnh):

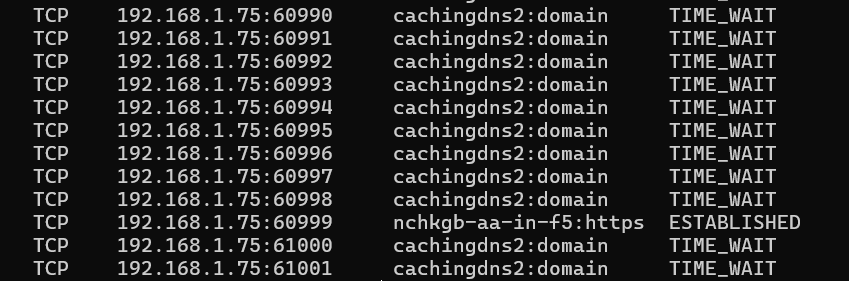
    

* Phân tích kết quả:
* localhost:
* **localhost** → 127.0.0.1 (IPv4) và ::1 (IPv6) → Đây là địa chỉ loopback, dùng để giao tiếp nội bộ.
* **1.0.0.127.in-addr.arpa** và **ip6.arpa** → Bản ghi DNS ngược (PTR) trỏ về localhost.
* Google API:
* **signaler-pa.googleapis.com** có nhiều bản ghi A trỏ đến các IP như:
* 142.250.71.138, 142.250.71.170, 142.250.76.234, 142.250.196.234, 142.250.197.10, 142.250.197.42 , 142.250.197.74, 142.250.197.106, 142.250.197.138, 142.250.71.234
* Đây là máy chủ của Google, có thể liên quan đến dịch vụ Firebase hoặc Google Cloud.

1. Lệnh **netstat**

* Chức năng: Lệnh netstat được sử dụng để hiển thị các kết nối mạng (cả đến và đi) hiện tại, bảng định tuyến và một số thống kê giao diện mạng.
* Cú pháp: netstat
* Kết quả thực hiện (hình ảnh):

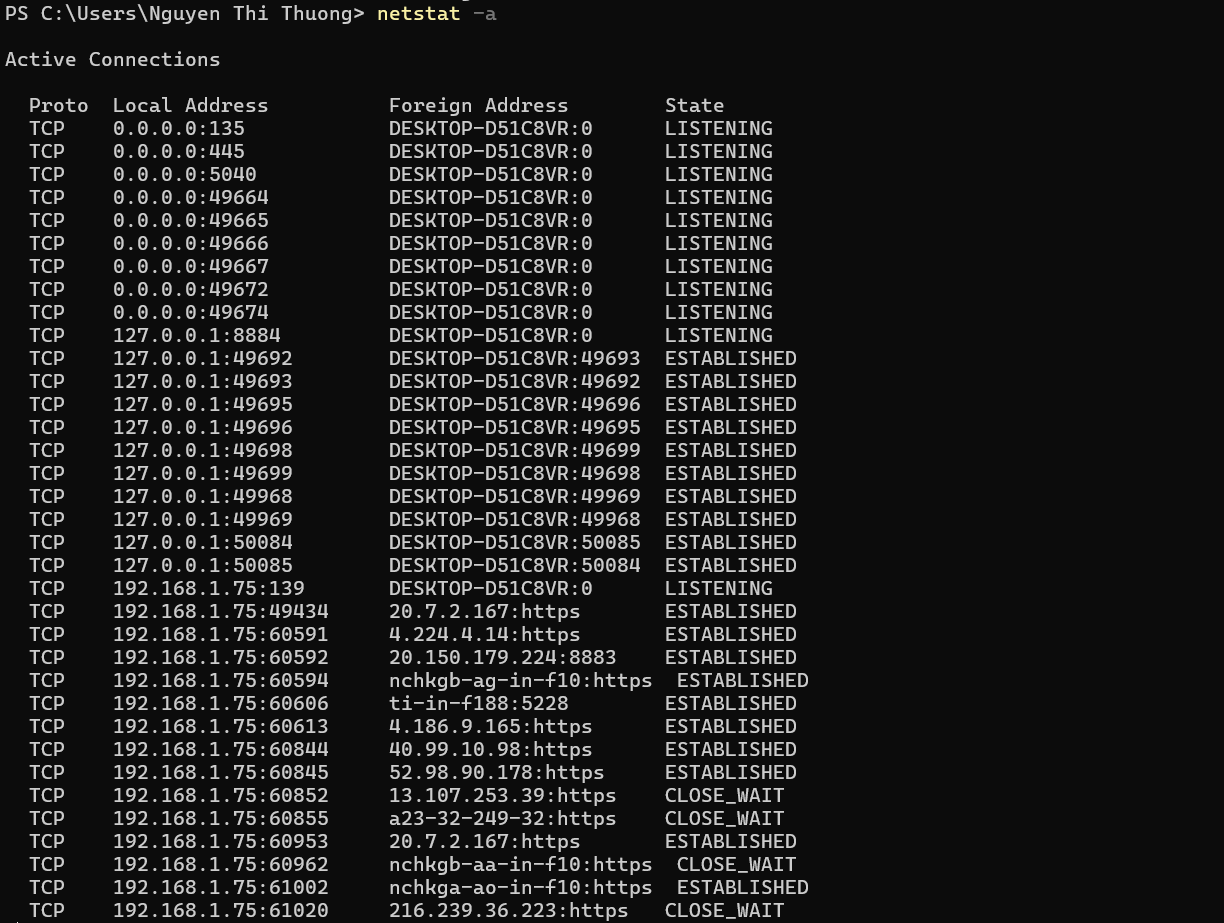


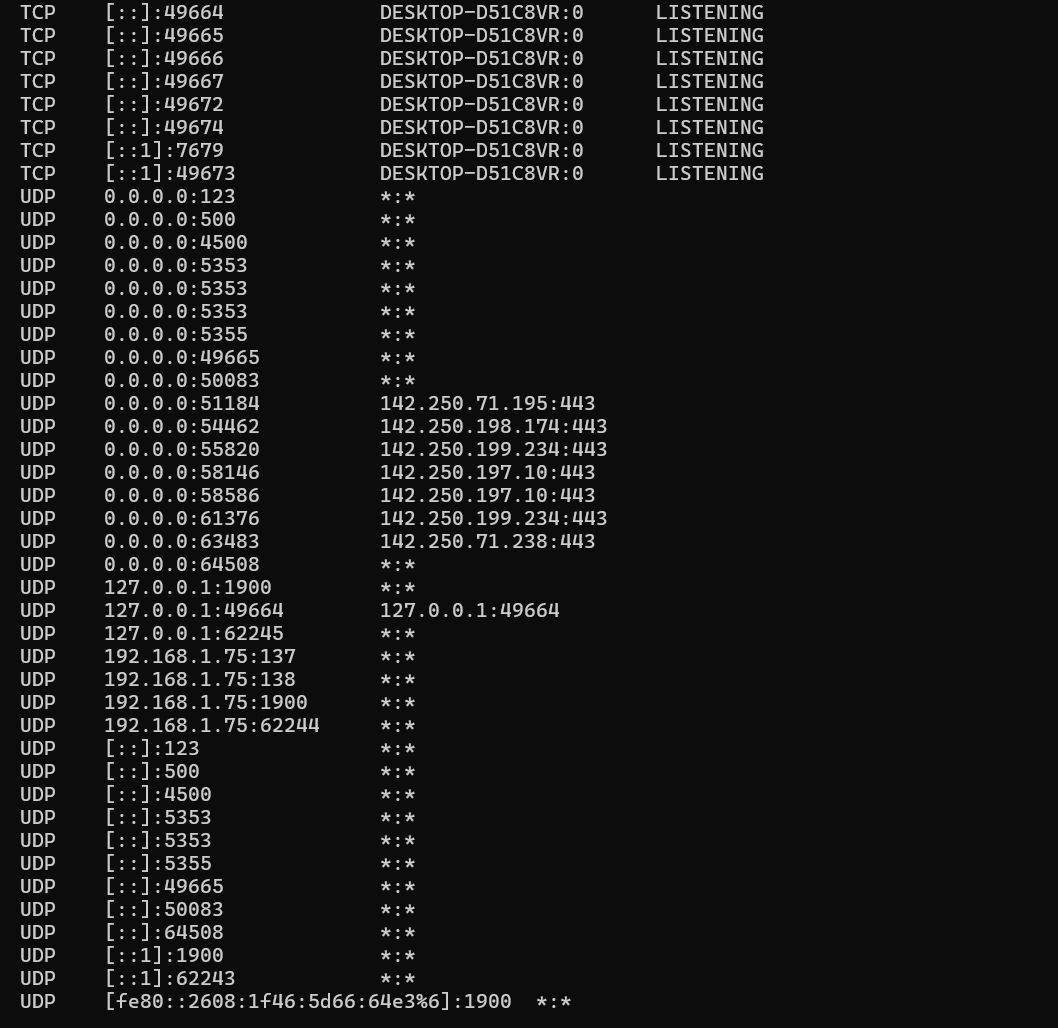


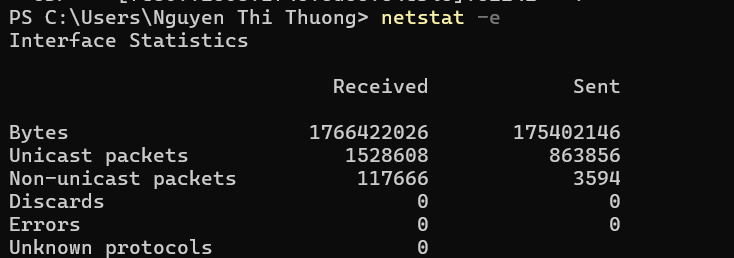
* Phân tích kết quả:
* **Kết nối nội bộ:** Nhiều kết nối TCP đang hoạt động giữa máy tính và chính nó (127.0.0.1), thường là do các ứng dụng trên cùng máy giao tiếp.
* **Kết nối HTTPS:** Máy tính đang kết nối với nhiều máy chủ từ xa qua cổng HTTPS (443), cho thấy hoạt động duyệt web và các dịch vụ trực tuyến.
* **Trạng thái kết nối:**
* **ESTABLISHED:** Kết nối đang hoạt động.
* **CLOSE\_WAIT:** Máy chủ từ xa đã đóng kết nối, máy tính vẫn chờ đóng hoàn toàn.
* **TIME\_WAIT:** Máy tính đã đóng kết nối, đang chờ xử lý gói tin còn sót lại.
* **Tên máy chủ:** Một số kết nối có tên máy chủ rõ ràng (ví dụ: cachingdns2, nchkgb-ag-in-f10), giúp xác định dịch vụ hoặc ứng dụng liên quan.
* **Cổng không chuẩn:** Một số kết nối sử dụng các cổng không chuẩn (ví dụ: 8883, 5228), có thể liên quan đến các ứng dụng đặc biệt.
* **Nhiều kết nối TIME\_WAIT**: Hàng loạt kết nối TCP từ địa chỉ 192.168.1.75 đến cachingdns2:domain ở trạng thái TIME\_WAIT. Điều này cho thấy máy tính đã chủ động đóng các kết nối này, nhưng vẫn đang chờ các gói tin còn sót lại trước khi giải phóng hoàn toàn cổng.
* **Một kết nối ESTABLISHED**: Một kết nối TCP từ 192.168.1.75 đến nchkgb-aa-in-f5:https ở trạng thái ESTABLISHED. Đây là kết nối đang hoạt động, có thể là kết nối HTTPS đến một máy chủ web hoặc dịch vụ nào đó.
* **Cổng dịch vụ DNS (domain)**: Các kết nối đến cachingdns2:domain cho thấy máy tính đang sử dụng dịch vụ phân giải tên miền (DNS) từ máy chủ cachingdns2.
* **Cổng HTTPS**: Kết nối đến nchkgb-aa-in-f5:https cho thấy máy tính đang truy cập một dịch vụ web an toàn.
* **Dải cổng cao**: Các kết nối sử dụng các cổng có số hiệu cao (60990, 60991, v.v.), thường là các cổng động được hệ điều hành gán cho các kết nối tạm thời.

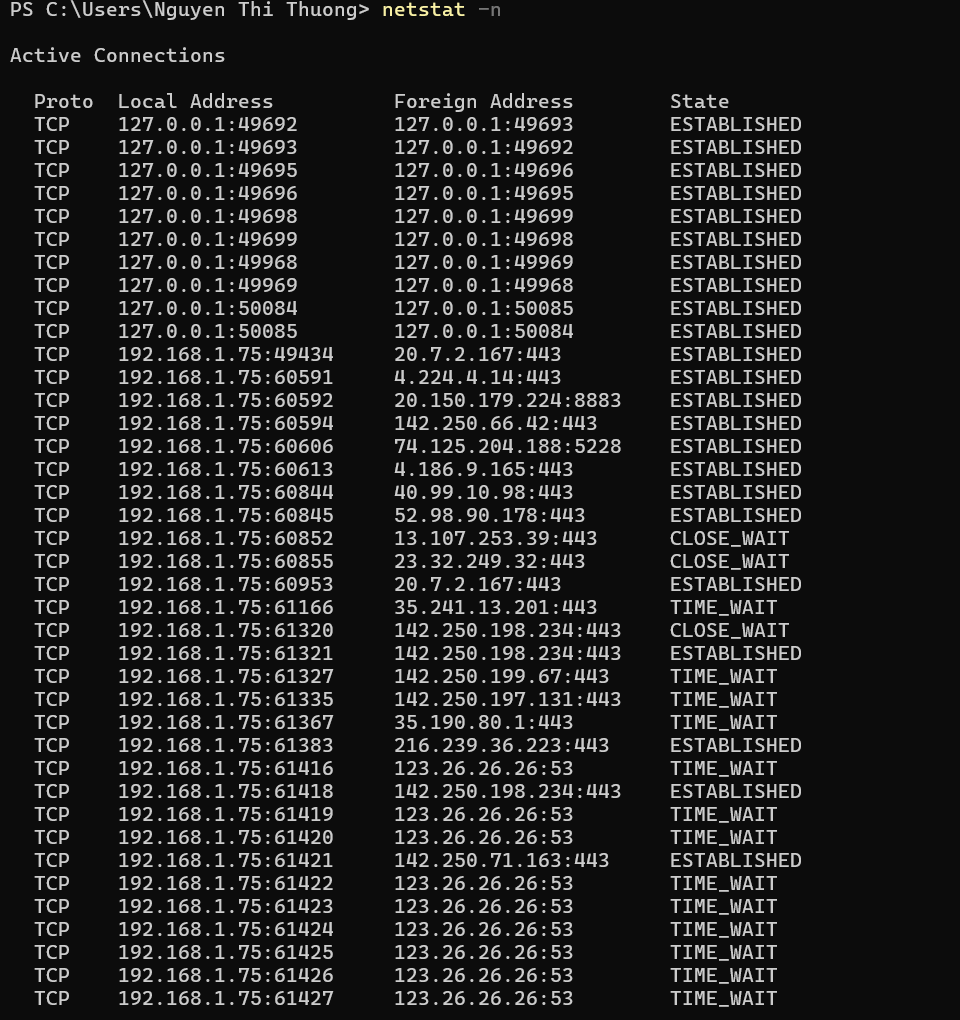
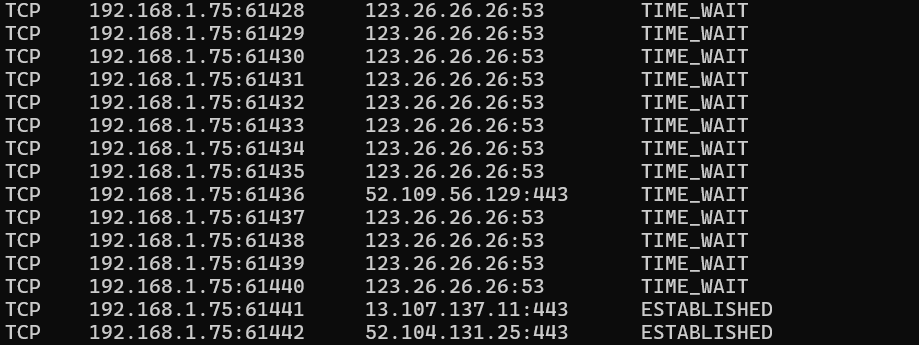
Thực hiện tương tự lệnh **netstat** kèm với các tham số **[-a], [-e], [-n], [-o], [-p protocol], [-r], [-s]**

* 1. **netstat** kèm với các tham số **[-a]**
* Chức năng: Lệnh netstat -a hiển thị tất cả các kết nối mạng đang hoạt động (active connections) và các cổng đang lắng nghe (listening ports) trên máy tính.
* Cú pháp: netstat -a
* Kết quả thực hiện (hình ảnh):

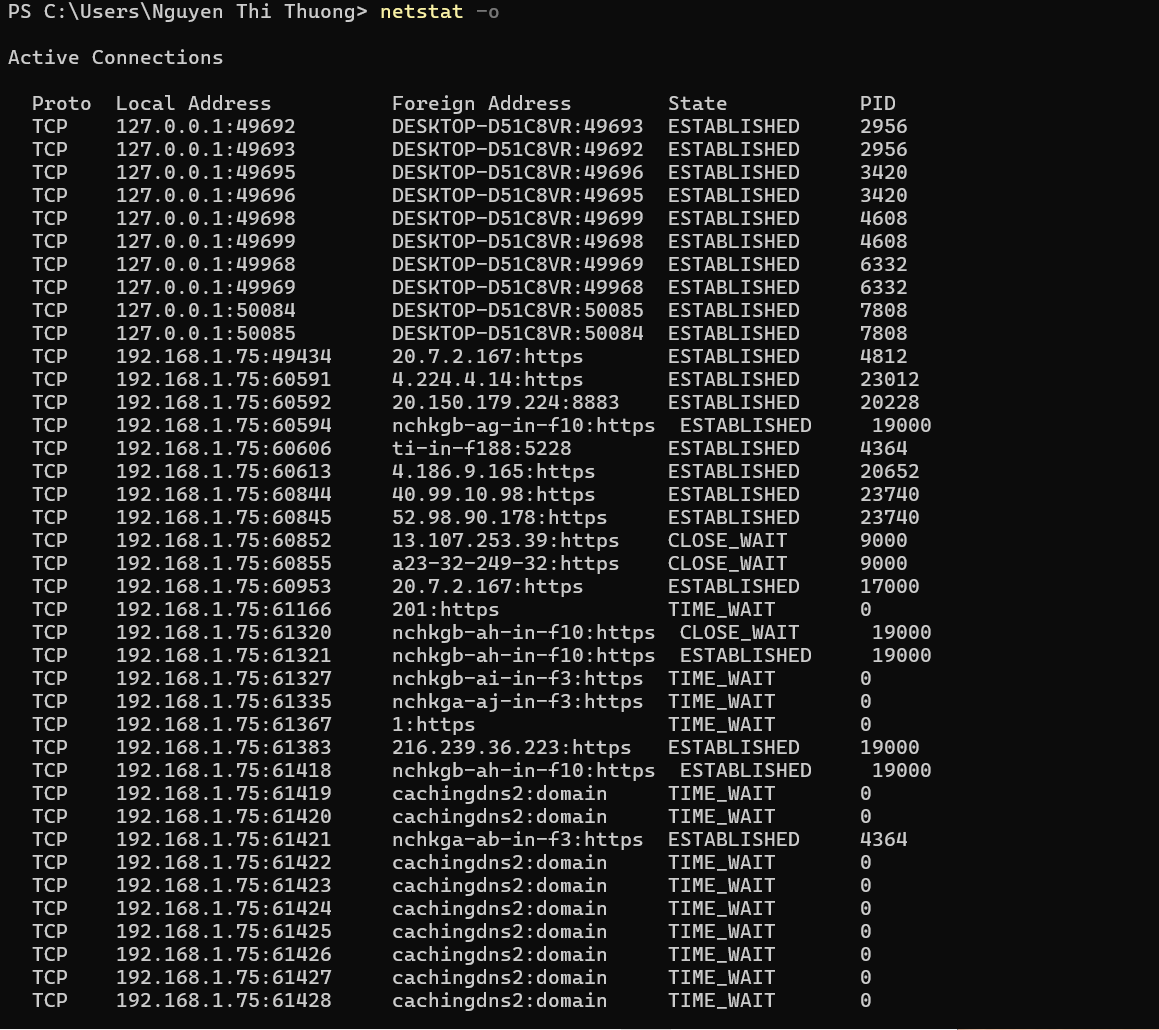


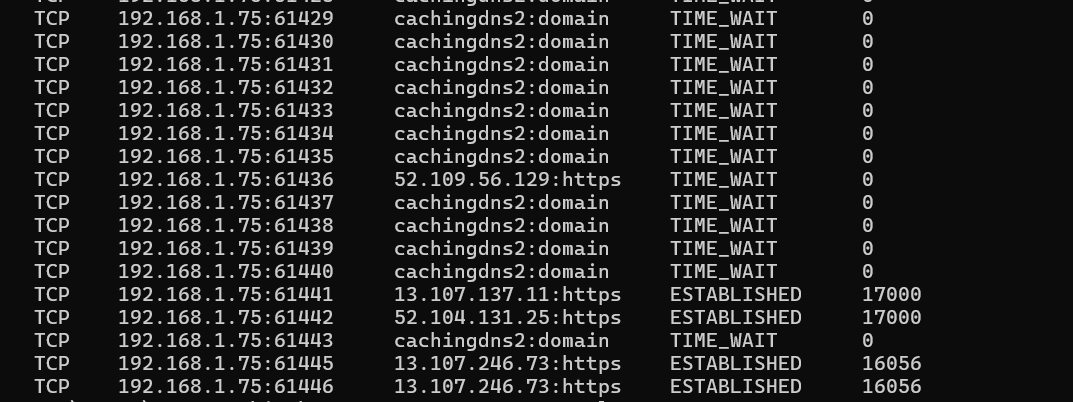


* Phân tích kết quả:
* **Proto (Giao thức)**: Cột này cho biết giao thức được sử dụng cho kết nối, trong trường hợp này là TCP.
* **Local Address (Địa chỉ cục bộ)**: Địa chỉ IP và số cổng mà máy tính đang sử dụng cho kết nối.
* 0.0.0.0: Nghĩa là cổng này đang lắng nghe trên tất cả các giao diện mạng của máy tính.
* 127.0.0.1: Địa chỉ loopback, chỉ máy tính hiện tại có thể truy cập được.
* 192.168.1.75: Địa chỉ IP cục bộ của máy tính trong mạng LAN.
* **Foreign Address (Địa chỉ từ xa)**: Địa chỉ IP và số cổng của máy tính từ xa mà máy tính đang kết nối đến.
* DESKTOP-D51C8VR:0: Cho biết cổng đang lắng nghe và không có kết nối từ xa.
* Các địa chỉ IP và cổng cụ thể cho thấy máy tính đang kết nối đến các máy chủ khác nhau trên Internet.
* **State (Trạng thái)**: Trạng thái của kết nối.
* LISTENING: Cổng đang lắng nghe các kết nối đến.
* ESTABLISHED: Kết nối đã được thiết lập và đang hoạt động.
* CLOSE\_WAIT: Máy tính từ xa đã đóng kết nối, nhưng máy tính cục bộ vẫn chưa đóng.
* **Kết nối TCP (Transmission Control Protocol):**
* **Cổng đang lắng nghe:** Máy tính đang lắng nghe trên nhiều cổng TCP, bao gồm các cổng động (49664, 49665, v.v.) và cổng loopback (7679). Điều này cho thấy các dịch vụ hoặc ứng dụng đang chạy trên máy tính đang chờ kết nối đến.
* **Địa chỉ IPv6:** Một số cổng đang lắng nghe trên địa chỉ IPv6 ([::]), cho thấy máy tính hỗ trợ giao thức IPv6.
* **Địa chỉ IPv4:** Một số cổng đang lắng nghe trên địa chỉ IPv4 (0.0.0.0), cho thấy máy tính đang lắng nghe trên tất cả các giao diện mạng.
  + **Kết nối UDP (User Datagram Protocol):**
* **Nhiều cổng UDP đang mở:** Máy tính có nhiều cổng UDP đang mở, bao gồm các cổng hệ thống (123, 500, 4500, 5353, 5355) và các cổng động.
* **Kết nối đến Google:** Một số kết nối UDP đang kết nối đến các máy chủ của Google (142.250.x.x:443), cho thấy máy tính đang sử dụng các dịch vụ của Google.
* **Địa chỉ loopback và LAN:** Một số kết nối UDP sử dụng địa chỉ loopback (127.0.0.1) và địa chỉ LAN (192.168.1.75), cho thấy các ứng dụng trên máy tính đang giao tiếp với nhau hoặc với các thiết bị trong mạng LAN.
* **Địa chỉ IPv6:** Tương tự như TCP, một số cổng UDP cũng đang mở trên địa chỉ IPv6.
  1. **netstat** kèm với các tham số **[-e]**
* Chức năng:
* Cú pháp:
* Kết quả thực hiện (hình ảnh): 
* Phân tích kết quả
  1. **netstat** kèm với các tham số **[-n]**
* Chức năng:
* Cú pháp:
* Kết quả thực hiện (hình ảnh): \

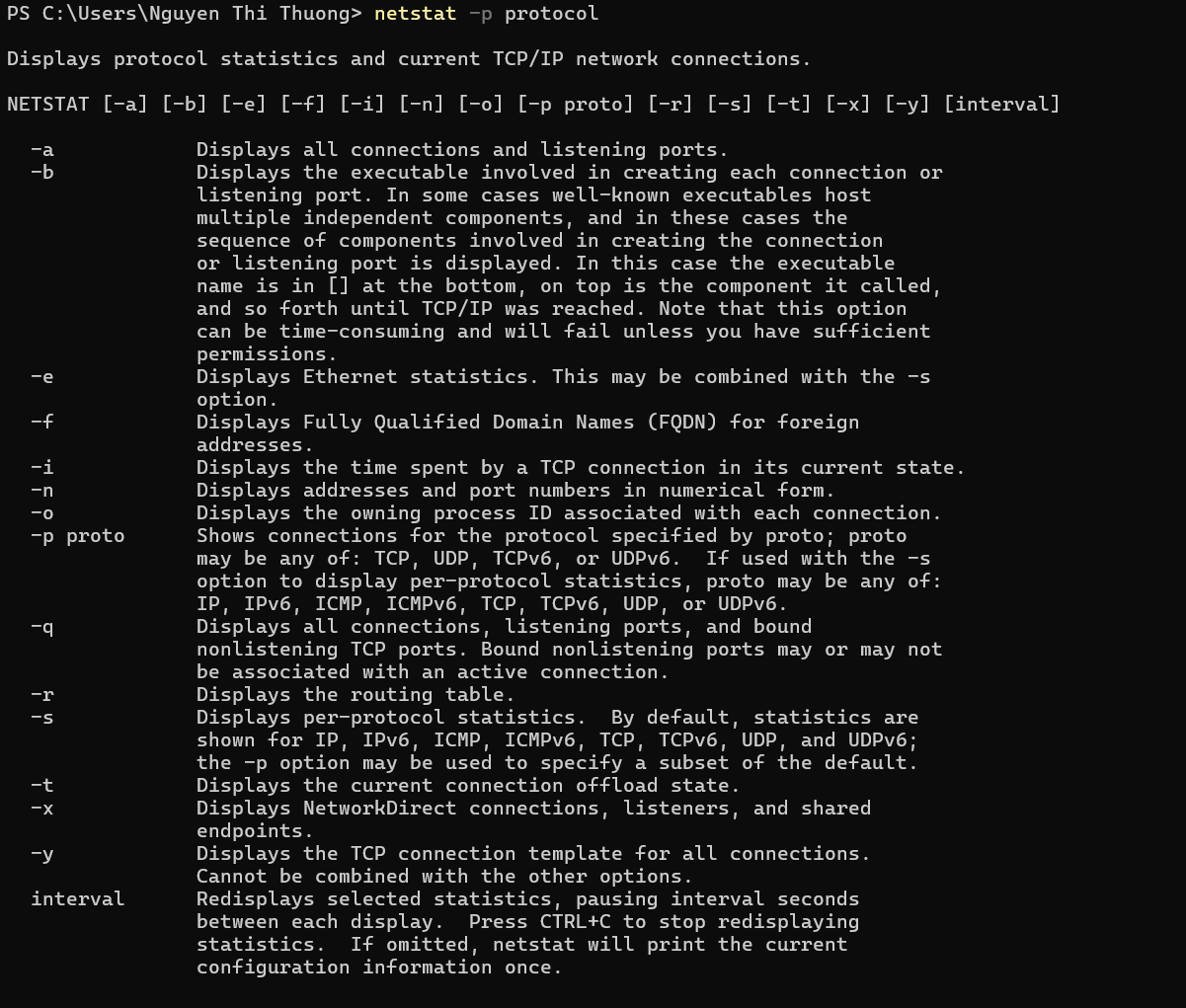
 

* Phân tích kết quả
  1. **netstat** kèm với các tham số **[-o]**
* Chức năng:
* Cú pháp:
* Kết quả thực hiện (hình ảnh):

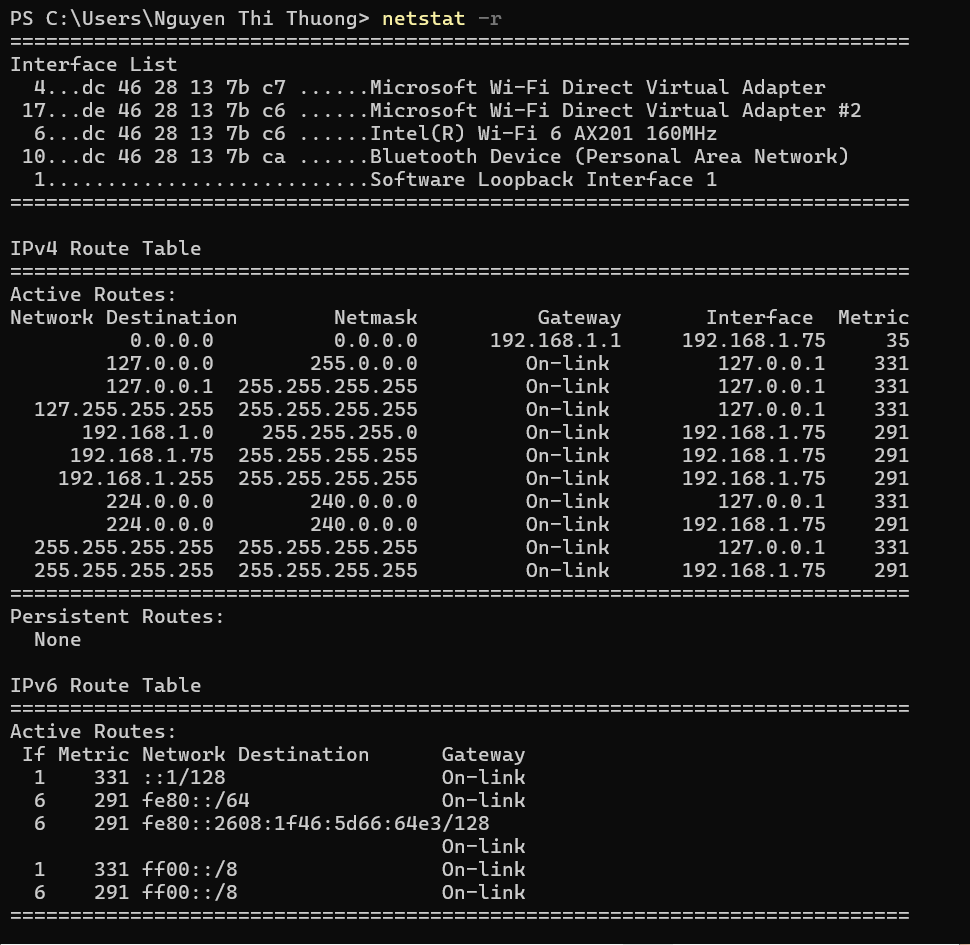




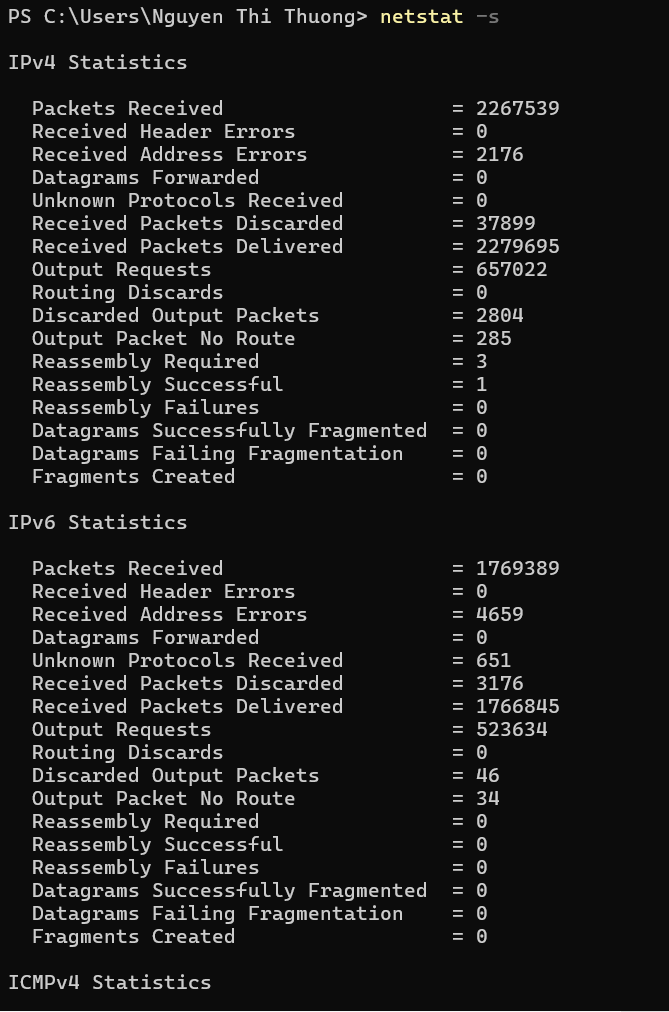
* Phân tích kết quả
  1. **netstat** kèm với các tham số **[-protocol]**
* Chức năng:
* Cú pháp:
* Kết quả thực hiện (hình ảnh):

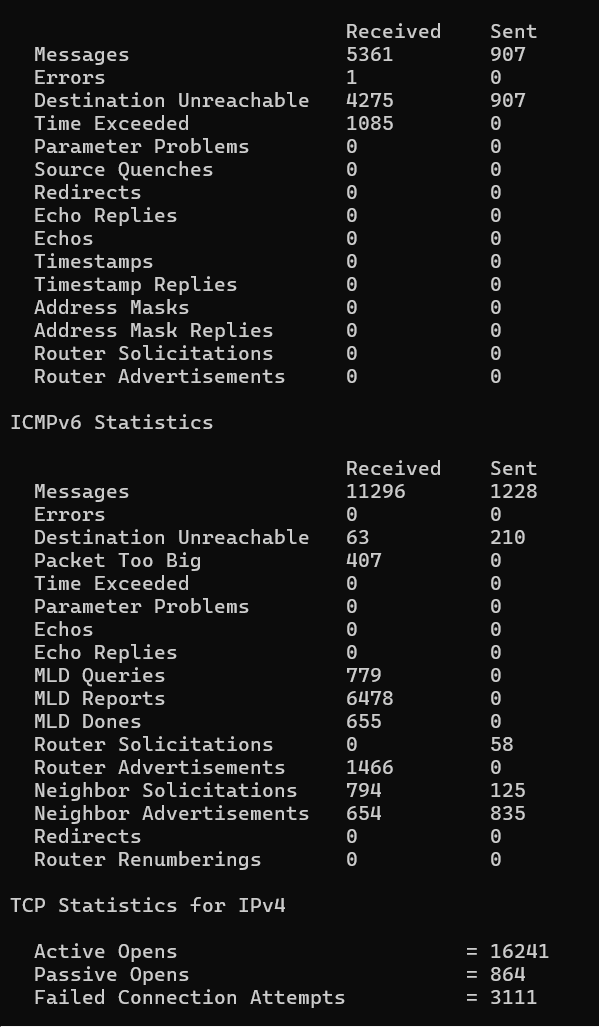
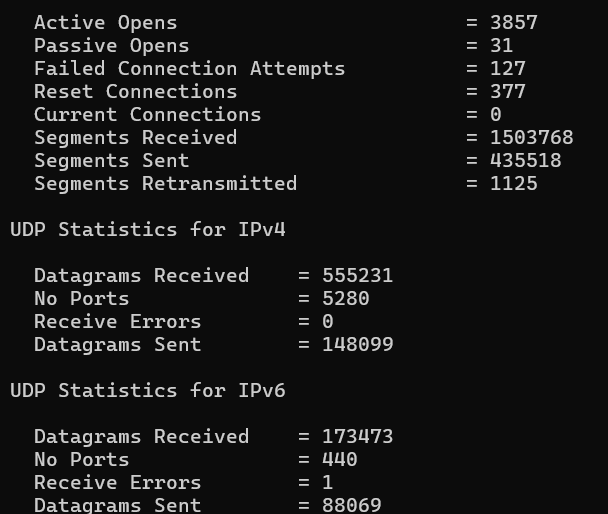


* Phân tích kết quả
  1. **netstat** kèm với các tham số **[-r]**
* Chức năng:
* Cú pháp:
* Kết quả thực hiện (hình ảnh):



* Phân tích kết quả
  1. **netstat** kèm với các tham số **[-s]**
* Chức năng:
* Cú pháp:
* Kết quả thực hiện (hình ảnh):



* Phân tích kết quả

1. Lệnh **tracert**

Chức năng:

Cú pháp:

Kết quả thực hiện (hình ảnh):

Phân tích kết quả: .

Thực hiện tương tự lệnh **tracert** kèm với các tham số **[-d], [-h MaximumHops], [-j HostList], [-w Timeout]**

1. Lệnh **route**

Chức năng:

Cú pháp:

Kết quả thực hiện (hình ảnh):

Phân tích kết quả: .

Tìm hiểu lệnh **route** kèm với các tham số **[-f], [-p], [-4|-6] command [destination], [MASK netmask], [gateway], [METRIC metric], [IF interface]**

Cho biết kết quả của lệnh **route PRINT**

1. Lệnh **ping**

Chức năng:

Cú pháp:

Kết quả thực hiện (hình ảnh):

Phân tích kết quả:

Thực hiện tương tự lệnh **ping** kèm với các tham số **[/t], [/a], [/l], [/n]**

Giải thích các thông báo lỗi sau khi sử dụng lệnh **ping**:

|  |  |
| --- | --- |
| **Thông báo lỗi kết nối** | **Giải thích** |
| Request time out |  |
| Destination host unreachable |  |

1. Lệnh **nslookup**

Chức năng:

Cú pháp:

Kết quả thực hiện (hình ảnh):

Phân tích kết quả:

Giải thích các thông báo lỗi sau khi sử dụng lệnh **nslookup**:

|  |  |
| --- | --- |
| **Thông báo lỗi** | **Giải thích** |
| timed out |  |
| No response from server |  |
| Nonexistent domain |  |
| Network is unreachable |  |
| Refused |  |