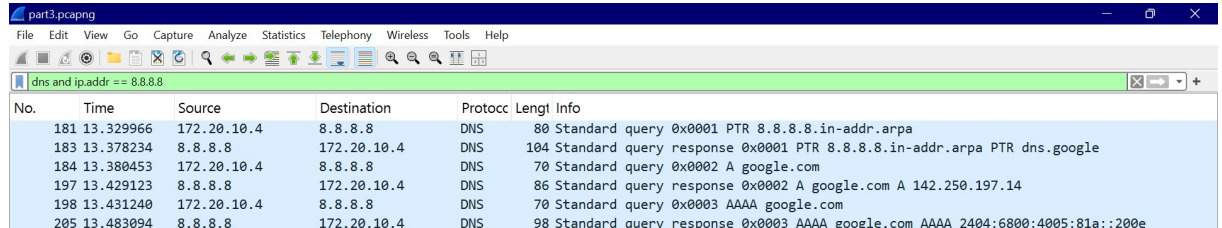


## PART 3. Network and Link Layer Analysis

### 1. Source/Destination IP

Trong gói **DNS Query** gửi tới Google DNS (gói số 181 trong hình):

- **Source IP:** 172.20.10.4 → IP của laptop của bạn (Wi-Fi).
- **Destination IP:** 8.8.8.8 → Google Public DNS.



The screenshot shows a Wireshark packet capture window titled 'part3.pcapng'. The filter bar at the top shows 'dns and ip.addr == 8.8.8.8'. The packet list pane displays several DNS packets. The selected packet (No. 181) is a Standard query from 172.20.10.4 to 8.8.8.8. The packet details pane shows the structure of the DNS query, including the query ID, flags, and the question section.

No.	Time	Source	Destination	Protocol	Length	Info
181	13.329966	172.20.10.4	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
183	13.378234	8.8.8.8	172.20.10.4	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
184	13.380453	172.20.10.4	8.8.8.8	DNS	70	Standard query 0x0002 A google.com
197	13.429123	8.8.8.8	172.20.10.4	DNS	86	Standard query response 0x0002 A google.com A 142.250.197.14
198	13.431240	172.20.10.4	8.8.8.8	DNS	70	Standard query 0x0003 AAAA google.com
205	13.483094	8.8.8.8	172.20.10.4	DNS	98	Standard query response 0x0003 AAAA google.com AAAA 2404:6800:4005:81a::200e

Vì sao 2 IP này “giữ nguyên” khi đi qua Internet?

- Việc địa chỉ IP Nguồn (Source IP Address) và địa chỉ IP Đích (Destination IP Address) không thay đổi khi gói tin (datagram) di chuyển qua Internet đến máy chủ DNS của Google là do **nguyên tắc hoạt động cơ bản của Lớp Mạng (Network Layer) và Giao thức IP (Internet Protocol)**.
- Vai trò của Địa chỉ IP tại Lớp Mạng:
  - Địa chỉ IP được sử dụng để **định danh host**. Cụ thể hơn, địa chỉ IP được gán cho **giao diện** (interface) của host hoặc router.
  - Lớp Mạng có trách nhiệm chính là di chuyển các gói tin lớp mạng, được gọi là **datagram**, từ host gửi đến host nhận.
  - Giao thức IP cung cấp dịch vụ **truyền thông logic giữa các host** (logical communication between hosts).
  - Khi host nguồn tạo một datagram, nó sẽ chèn địa chỉ IP của mình vào trường **Địa chỉ IP Nguồn (Source IP address)** và chèn địa chỉ IP của đích đến cuối cùng (Google DNS server) vào trường **Địa chỉ IP Đích (Destination IP address)** trong header IP.
- Router chỉ thực hiện Chuyển tiếp (Forwarding) dựa trên Địa chỉ Đích
  - Khi datagram di chuyển qua Mạng lõi (Network Core) của Internet, nó sẽ đi qua một chuỗi các **router** (bộ chuyển mạch gói - packet switches).
  - Router, vốn là các thiết bị Lớp 3 (network-layer devices), **chỉ thực hiện chức năng chuyển tiếp (forwarding)**. Chuyển tiếp là hành động cục bộ của router nhằm chuyển gói tin từ giao diện đầu vào sang giao diện đầu ra thích hợp.
  - Router kiểm tra một phần địa chỉ đích của gói tin và sử dụng **bảng chuyển tiếp (forwarding table)** của mình, ánh xạ địa chỉ đích tới các liên kết gửi đi, để xác định liên kết mà gói tin nên được chuyển tiếp tới.
  - **Các router trung gian không can thiệp** vào các trường địa chỉ IP Nguồn và Địa chỉ IP Đích vì chúng chỉ quan tâm đến việc **chuyển gói tin đến host cuối cùng**. Các router hành động chỉ dựa trên các trường lớp mạng của datagram.

- Nói cách khác, IP được thiết kế như một **dịch vụ vận chuyển đầu cuối (end-to-end)**: địa chỉ nguồn và đích được thiết lập tại hai host cuối và duy trì không đổi trong suốt hành trình giữa chúng.
- Vì vậy, địa chỉ IP Nguồn và Đích **đại diện cho các điểm cuối logic** (end-to-end logical endpoints) của phiên truyền thông. Các router chỉ đọc các địa chỉ này để quyết định cách thức **chuyển tiếp** gói tin đến đích, nhưng chúng không được phép thay đổi các định danh host cuối cùng này, đảm bảo gói tin được chuyển giao đến đúng host đích (máy chủ DNS của Google) theo định nghĩa của Giao thức IP.

## 2. TTL trong IP header

- Trường TTL của gói DNS Query được quan sát trong IP header như hình dưới. Gói tin được gửi đi với TTL = 128, là giá trị mặc định của hệ điều hành tại máy nguồn.

```
Internet Protocol Version 4, Src: 172.20.10.4, Dst: 8.8.8.8
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 66
  Identification: 0xc017 (49175)
> 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0xb46b [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.20.10.4
  Destination Address: 8.8.8.8
  [Stream index: 6]
```

### Ý nghĩa TTL ban đầu:

- TTL được thiết lập bởi **host nguồn** khi gói tin IP được tạo ra (ví dụ 64, 128,... tùy hệ điều hành).
- **Mục đích:** TTL được đưa vào để đảm bảo rằng các gói tin **không lưu hành vĩnh viễn** (circulate forever) trong mạng. Tình trạng lưu hành vĩnh viễn có thể xảy ra do các vòng lặp định tuyến (long-lived routing loop) tồn tại.
- **Chức năng:** Giá trị TTL ban đầu được sử dụng để **giới hạn số bước nhảy (hop)** tối đa mà gói tin được phép đi qua trên đường đi từ nguồn đến đích.
- **Cách hoạt động:**
  - Mỗi khi gói tin được xử lý bởi một router, giá trị TTL sẽ **giảm đi một đơn vị** (decremented by one).
  - Nếu trường TTL đạt đến giá trị **0**, router phải **loại bỏ** (dropped) gói tin đó.

### Router/gateway xử lý TTL thế nào?

- Quy trình xử lý trường Time to Live (TTL) của một gói IP tại router/gateway:

- Bước 1: Router/gateway nhận một gói IP tại một giao diện mạng (interface) đầu vào.
- Bước 2: Thiết bị trích xuất và đọc giá trị *Time to Live (TTL)* hiện tại từ tiêu đề IPv4 của gói tin.
- Bước 3: Giảm giá trị TTL theo quy tắc:  $TTL(new) = TTL(old) - 1$  mỗi khi gói tin được xử lý bởi một router. Việc thay đổi giá trị TTL này có một hệ quả trực tiếp đối với router: **Header checksum** (Mã kiểm tra Tiêu đề) phải được **tính toán lại và lưu trữ lại tại mỗi router** bởi vì trường TTL đã thay đổi.
- Bước 4: Kiểm tra điều kiện TTL mới:
  - Nếu  $TTL(new) > 0$  thì Router coi gói tin vẫn còn hợp lệ và **tiếp tục chuyển tiếp (forward)** gói này tới nút kế tiếp (next hop) dựa trên bảng định tuyến.
  - Nếu  $TTL(new) = 0$  thì Router **loại bỏ (drop)** gói tin, đồng thời, trong đa số trường hợp, **phát sinh một thông điệp ICMP “Time Exceeded”** gửi trở lại địa chỉ IP nguồn để thông báo rằng gói tin không thể đến được đích do đã vượt quá giới hạn TTL cho phép.

### 3. MAC Address của router/gateway

- Địa chỉ IP của router sau khi nhập lệnh ipconfig từ command Prompt là 192.168.0.1:

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::e06c:7bb9:7844:c30e%4
IPv4 Address. . . . . : 192.168.0.104
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
```

- Địa chỉ MAC của router/gateway từ Command Prompt sau khi gõ lệnh **arp -a** là 5c-a6-e6-e1-90-01:

```
C:\Users\User>arp -a

Interface: 192.168.0.104 --- 0x4
Internet Address      Physical Address      Type
192.168.0.1           5c-a6-e6-e1-90-01    dynamic
192.168.0.106         64-ff-0a-91-cf-b2    dynamic
192.168.0.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

#### 4. Địa chỉ Source/Destination ở Link Layer vs IP

```
▼ Ethernet II, Src: Intel_be:fe:60 (08:6a:c5:be:fe:60), Dst: 7a:a7:c7:f3:78:64 (7a:a7:c7:f3:78:64)
  > Destination: 7a:a7:c7:f3:78:64 (7a:a7:c7:f3:78:64)
  > Source: Intel_be:fe:60 (08:6a:c5:be:fe:60)
    Type: IPv4 (0x0800)
    [Stream index: 0]
```

Trong header Ethernet (Link Layer) của gói DNS Query, địa chỉ Nguồn và địa chỉ Đích là:

- **Source MAC:** 08-6A-C5-BE-FE-60 → Đây là **địa chỉ MAC cố định** của bộ điều hợp mạng (adapter), trong trường hợp này là card Wi-Fi của laptop.
- **Destination MAC:** 7A-A7-C7-F3-78-64 → Vì DNS server của Google (đích cuối cùng) nằm **ngoài mạng con** (off the subnet) của laptop, gói tin IP phải được gửi đến giao diện của **router bước nhảy đầu tiên** (first-hop router) để được định tuyến ra Internet. Do đó, địa chỉ MAC đích cho khung Ethernet này phải là địa chỉ MAC của giao diện router cục bộ (default gateway).

#### So sánh địa chỉ MAC và địa chỉ IP:

Đặc điểm	Địa chỉ MAC (Lớp Liên kết / Lớp 2)	Địa chỉ IP (Lớp Mạng / Lớp 3)
Phạm vi	Địa chỉ MAC chỉ có ý nghĩa trong <b>mạng cục bộ</b> (LAN segment). Khung (frame) chứa gói tin cần thay đổi Địa chỉ MAC Đích và Nguồn tại <b>mỗi bước nhảy (hop)</b> khi đi qua một router.	Địa chỉ IP được sử dụng trên <b>phạm vi toàn cầu</b> (Internet). Địa chỉ IP Nguồn và Địa chỉ IP Đích được thiết lập tại host gửi và host nhận cuối cùng và <b>không thay đổi</b> trong suốt hành trình (trừ khi có NAT).
Cấp phát	Là <b>địa chỉ vật lý</b> (physical address), được nhà sản xuất gán cho bộ điều hợp mạng (adapter). IEEE quản lý không gian địa chỉ để đảm bảo <b>tính duy nhất</b> trên toàn cầu. Nó có cấu trúc phẳng (flat structure).	Là <b>địa chỉ logic</b> (logical address). Nó có <b>cấu trúc phân cấp</b> (hierarchical structure) (có phần mạng và phần host) và phải được thay đổi nếu host di chuyển sang mạng khác. Địa chỉ thường được cấp phát động thông qua giao thức <b>DHCP</b> .
Định dạng	<b>48 bit</b> , thường được viết dưới dạng 6 nhóm 2 ký tự hệ thập lục phân (Hex), cách nhau bằng dấu gạch ngang hoặc dấu hai chấm (ví dụ: 00:6a:c5:be:fe:60).	<b>32 bit</b> (IPv4) hoặc <b>128 bit</b> (IPv6), thường được viết dưới dạng thập phân có dấu chấm (ví dụ: 172.20.10.4).
Mục đích	Cho phép các thiết bị và bộ điều hợp (adapter) <b>lân cận</b> giao tiếp vật lý trong cùng một liên kết (link) hoặc mạng con (subnet).	Cho phép <b>dịch vụ truyền thông logic giữa các host</b> (logical communication between hosts) trên toàn bộ Internet. Router sử dụng địa chỉ IP Đích để thực hiện <b>chuyển tiếp gói tin</b> (forwarding).

---

## 5. Type field trong Ethernet header

Trong phần **Ethernet II** của gói DNS Query:

- **Type:** 0x0800.

```
√ Ethernet II, Src: Intel_be:fe:60 (08:6a:c5:be:fe:60), Dst: 7a:a7:c7:f3:78:64 (7a:a7:c7:f3:78:64)
  > Destination: 7a:a7:c7:f3:78:64 (7a:a7:c7:f3:78:64)
  > Source: Intel_be:fe:60 (08:6a:c5:be:fe:60)
    Type: IPv4 (0x0800)
    [Stream index: 0]
```

Ý nghĩa:

- Giá trị 0x0800 là một mã chuẩn (**EtherType**) và nó cho thiết bị nhận (router/gateway hoặc thiết bị mạng kế tiếp) biết thông tin quan trọng sau:
  - **Giao thức Tiếp theo:** Nó chỉ ra rằng giao thức được đóng gói (encapsulated) ngay sau tiêu đề Ethernet là **Giao thức Internet phiên bản 4 (IPv4)**.
  - **Chức năng Phân phối:** Sau khi nhận được gói tin, router sẽ nhìn vào giá trị này để biết rằng nó cần chuyển gói dữ liệu này lên **Lớp Mạng (Layer 3)** và xử lý nó bằng cách sử dụng logic của giao thức **IP**.
  - Ví dụ:
    - 0x0800 → IPv4
    - 0x86DD → IPv6
    - 0x0806 → ARP