



# [PRAKTIKUM KOMUNIKASI DATA]

## MODUL 2 TUGAS – ETHERNET CONCEPTS

**DISUSUN OLEH :**

FAIZAL QADRI TRIANTO

RIFKI RAMADANY MAJID

**DIAUDIT OLEH :**

LUQMAN HAKIM, S.KOM., M.KOM

PRESENTED BY: TIM LAB-IT  
UNIVERSITAS MUHAMMADIYAH MALANG

## [PRAKTIKUM KOMUNIKASI DATA]

---

### PERSIAPAN MATERI

Praktikan diharapkan mempelajari Group Exam Modules 4 - 7: Ethernet Concepts Exam yang terdiri dari beberapa chapter berikut :

1. Physical Layer (Chapter 4)
  2. Number Systems (Chapter 5)
  3. Data Link Layer (Chapter 6)
  4. Ethernet Switching (Chapter 7)
- 

### TUJUAN PRAKTIKUM

1. Bagian 1: Memeriksa Header dalam Frame Ethernet II
  2. Bagian 2: Menggunakan Wireshark untuk mengambil dan menganalisis Frame Ethernet
- 

### PERSIAPAN SOFTWARE/APLIKASI

1. Perangkat : Komputer/Laptop
  2. Sistem Operasi: Windows/Linux/Mac OS
  3. Aplikasi :
    - Packet Tracer 8.2.2 <https://skillsforall.com/resources/lab-downloads?courseLang=en-US>
    - Wireshark 4.2.6 <https://www.wireshark.org/download.html>
- 

### MATERI TUGAS

#### **Bagian 1: Memeriksa Header dalam Frame Ethernet II**

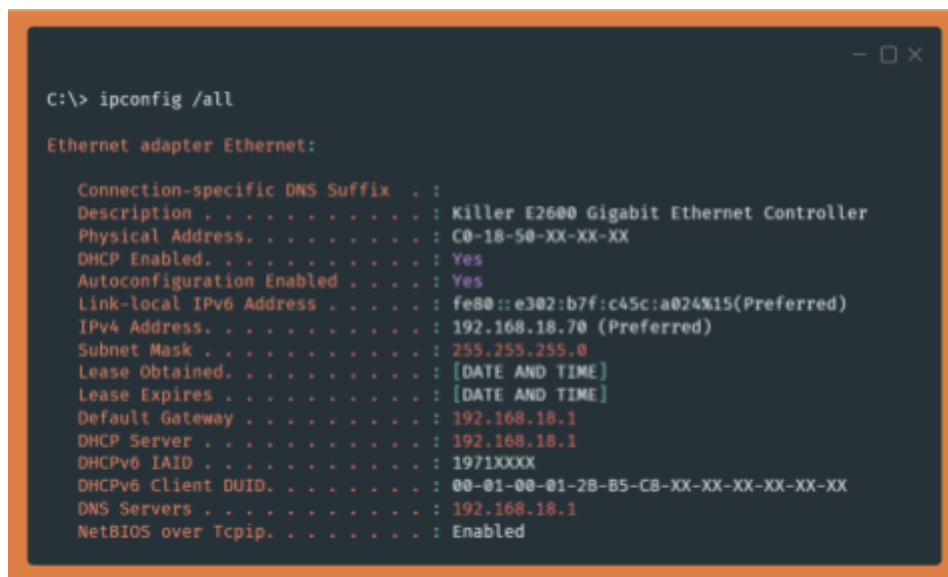
1. Meninjau deskripsi dan panjang pada Header Ethernet II

Frame Ethernet II terdiri dari beberapa field yang masing-masing memiliki fungsi penting dalam proses transmisi data. Setiap field memiliki panjang yang telah ditentukan dan berisi informasi spesifik yang digunakan untuk memastikan data dikirim dan diterima dengan benar. Berikut adalah deskripsi singkat dari masing-masing field dalam header Ethernet II beserta panjangnya:

Field	Length	Description
Preamble	8 Bytes	Berisi bit-bit sinkronisasi untuk mengatur waktu penerima sebelum data yang sebenarnya diterima.
Destination Address	6 Bytes	Alamat MAC dari perangkat tujuan. Setiap alamat MAC adalah unik untuk setiap perangkat jaringan.
Source Address	6 Bytes	Alamat MAC dari perangkat sumber.
Frame Type	2 Bytes	Menunjukkan tipe protokol layer atas yang dibawa oleh frame ini.
Data	46 – 1500 Bytes	Berisi data atau payload yang dikirimkan. Jika data kurang dari 46 byte, padding akan ditambahkan.
FCS	4 Bytes	Frame Check Sequence, digunakan untuk mendeteksi kesalahan selama transmisi data.

## 2. Memeriksa konfigurasi jaringan pada PC

Pada aktivitas ini, Anda akan memeriksa konfigurasi jaringan pada PC untuk memastikan pengaturan jaringan telah diatur dengan benar. Langkah ini melibatkan penggunaan Command Prompt untuk menjalankan perintah **ipconfig /all**, yang akan menampilkan informasi penting tentang koneksi jaringan Anda, termasuk alamat IP, gateway, dan server DNS.



```

C:\> ipconfig /all

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Killer E2600 Gigabit Ethernet Controller
    Physical Address. . . . . : C0-18-50-XX-XX-XX
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::e302:b7f:c45c:a024%15(Preferred)
    IPv4 Address. . . . . : 192.168.18.70 (Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : [DATE AND TIME]
    Lease Expires . . . . . : [DATE AND TIME]
    Default Gateway . . . . . : 192.168.18.1
    DHCP Server . . . . . : 192.168.18.1
    DHCPv6 IAID . . . . . : 1971XXXX
    DHCPv6 Client DUID. . . . . : 00-01-00-01-28-B5-C8-XX-XX-XX-XX-XX
    DNS Servers . . . . . : 192.168.18.1
    NetBIOS over Tcpip. . . . . : Enabled
  
```

Berdasarkan informasi di atas, dapat kita ketahui bahwa alamat IP host PC Anda saat ini

adalah **192.168.18.70**. Ini adalah alamat unik yang digunakan untuk mengidentifikasi perangkat Anda di jaringan. Default gateway yang digunakan adalah **192.168.18.1**, yang berfungsi sebagai gerbang penghubung untuk perangkat Anda ke jaringan lain.

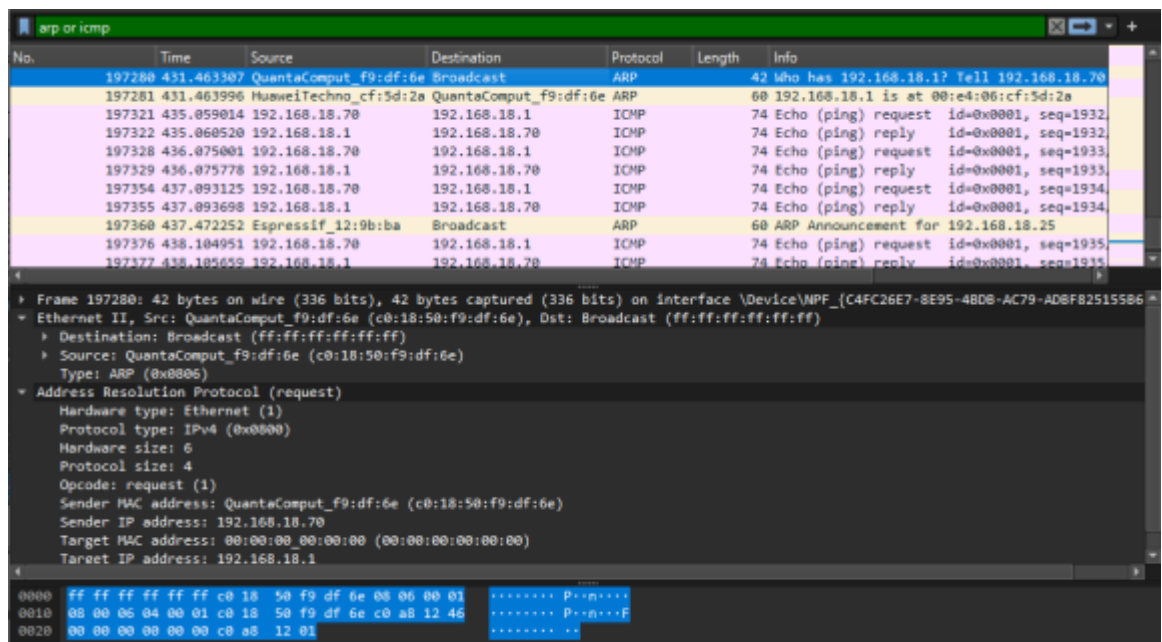
### 3. Memeriksa frame Ethernet dalam sebuah Wireshark.

Dalam aktivitas ini, Anda akan menggunakan Wireshark untuk memeriksa frame Ethernet yang dihasilkan saat Anda melakukan ping dari host PC ke default gateway. Ini akan membantu Anda memahami bagaimana data dikirim dan diterima dalam jaringan.

- Menggunakan Wireshark untuk Memeriksa Paket:

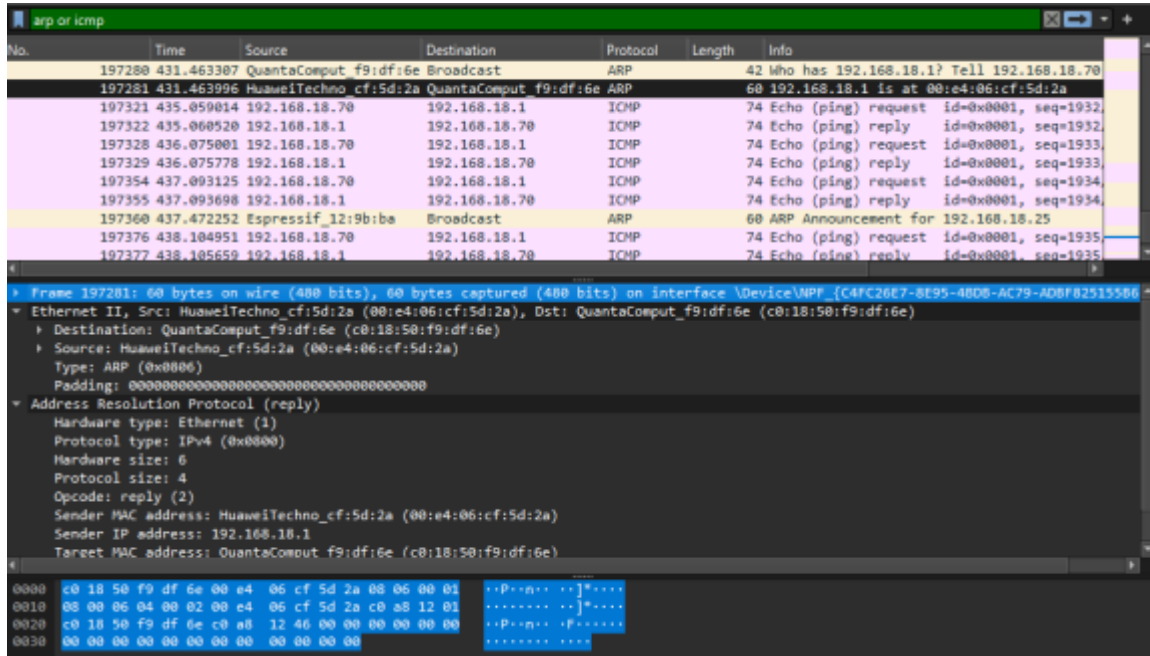
Buka Wireshark, mulai penangkapan lalu lintas jaringan, lakukan ping dari host PC ke default gateway (misalnya ke alamat **IP 192.168.18.1**), dan hentikan penangkapan setelah ping selesai untuk menganalisis paket dalam Wireshark.

- **Permintaan ARP (Address Resolution Protocol):**



Wireshark akan menampilkan permintaan ARP yang dibuat oleh host PC Anda untuk mencari tahu alamat MAC dari default gateway dengan pertanyaan "Siapa yang memiliki alamat IP 192.168.18.1? Beritahu saya alamat MAC Anda."

- **Balasan ARP:**



Sebagai respons, default gateway akan mengirim balasan ARP yang menyatakan alamat MAC-nya dengan informasi "Saya memiliki alamat IP 192.168.18.1, dan alamat MAC saya adalah XX:XX:XX:XX."

4. Memeriksa konten header Ethernet 2 dari permintaan ARP.

Pada bagian ini, kita akan memeriksa konten header Ethernet II dari permintaan ARP yang ditangkap oleh Wireshark. Header Ethernet berisi informasi penting tentang bagaimana data dikirim melalui jaringan. Tabel berikut menjelaskan field-field utama dalam header Ethernet yang relevan dengan permintaan ARP.

Field	Value	Description
Preamble	Not shown in capture	Berisi bit-bit sinkronisasi untuk mengatur waktu penerima sebelum data yang sebenarnya diterima.

Destination Address	Broadcast (ff:ff:ff:ff:ff:ff)	Alamat Layer 2 untuk frame. Setiap alamat sepanjang 48 bit, atau 6 oktet, dinyatakan sebagai 12 digit heksadesimal, 0-9, A-F. Alamat tujuan mungkin berupa broadcast, yang berisi semua satuan, atau unicast. Alamat sumber selalu unicast.
Source Address	QuantaComput_f9:df:6e (c0:18:50:f9:df:6e)	Enam angka heksadesimal pertama menunjukkan pabrikan dari kartu jaringan (NIC), enam angka heksadesimal terakhir adalah nomor seri dari NIC tersebut.
Frame Type	0x0806	Untuk frame Ethernet II, field ini berisi nilai heksadesimal yang digunakan untuk menunjukkan tipe protokol lapisan atas dalam data field. Ada banyak protokol lapisan atas yang didukung oleh Ethernet II. Dua tipe frame umum adalah: - Nilai 0x0800 (Protokol IPv4, dan - 0x0806 (Protokol Resolusi Alamat - ARP).
Data	ARP	Berisi protokol lapisan atas yang dienkapsulasi. Field data ini berukuran antara 46 hingga 1.500 byte.
FCS	4 Bytes	Frame Check Sequence, digunakan oleh NIC untuk mengidentifikasi kesalahan selama transmisi. Nilai ini dihitung oleh perangkat pengirim, mencakup alamat frame, tipe, dan field data. Diverifikasi oleh penerima.

## Bagian 2: Menggunakan Wireshark untuk Mengambil dan Menganalisis Frame Ethernet

1. Tentukan alamat IP dari gateway default pada PC.
  - a. Pastikan menggunakan model Realtime.
  - b. Buka Command Prompt pada tab Desktop.
  - c. Masukkan perintah **ipconfig**.

```

C:\Windows\System32>ping 192.168.18.1

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

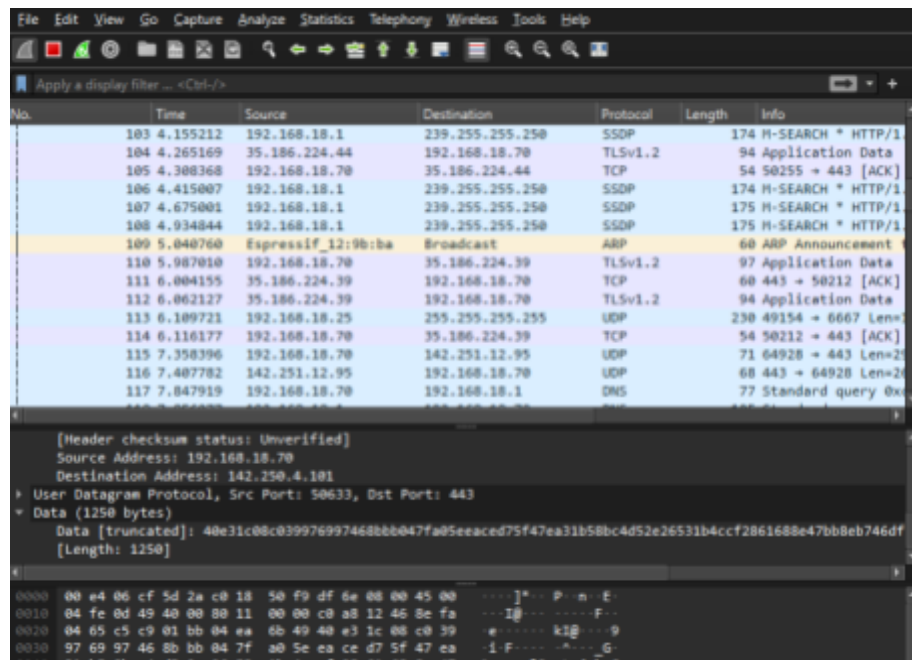
    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::e302:b7f:c45c:a024%15
    IPv4 Address. . . . . : 192.168.18.70
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.18.1

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::5d94:461d:dd94:1d29%16
    IPv4 Address. . . . . : 192.168.1.108
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

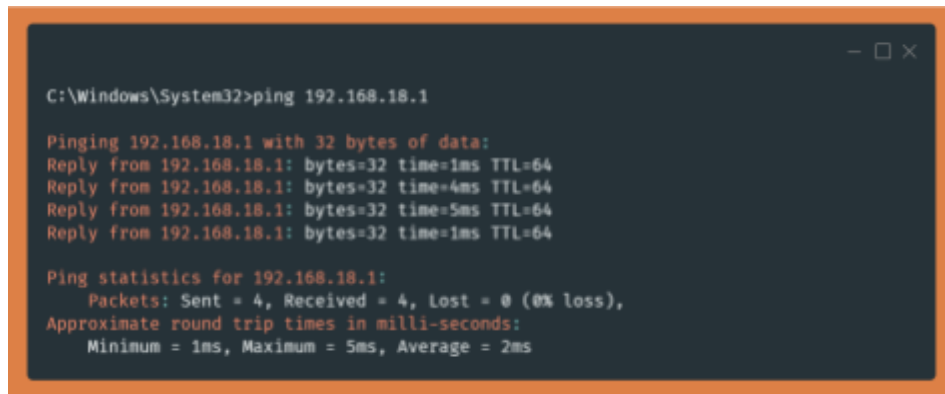
```

2. Lakukan pengambilan data lalu lintas di NIC PC.
  - a. Buka Wireshark untuk melakukan pengambilan data.
  - b. Klik "Start Capture" untuk memulai pengambilan data.
  - c. Amati lalu lintas yang muncul pada daftar paket.



3. Lakukan ping ke gateway default PC pada Command Prompt.

- a. Lakukan ping ke gateway default menggunakan alamat IP Bagian 1.



```

C:\Windows\System32>ping 192.168.18.1

Pinging 192.168.18.1 with 32 bytes of data:
Reply from 192.168.18.1: bytes=32 time=1ms TTL=64
Reply from 192.168.18.1: bytes=32 time=4ms TTL=64
Reply from 192.168.18.1: bytes=32 time=5ms TTL=64
Reply from 192.168.18.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.18.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
  
```

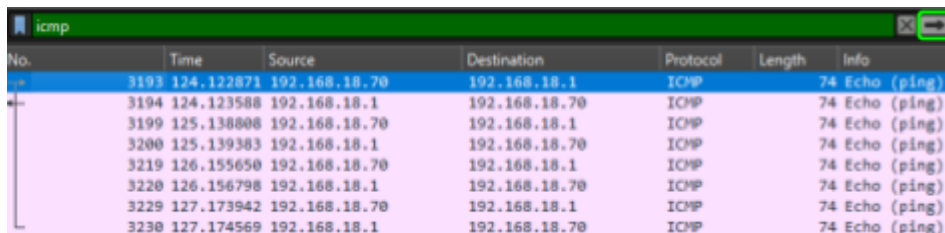
4. Lakukan pemberhentian pengambilan data lalu lintas di NIC.

- a. Klik ikon "Stop Capturing Packets" untuk berhenti.



5. Lakukan filtering Wireshark agar menampilkan lalu lintas ICMP saja.

- Gunakan filter di Wireshark untuk memblokir visibilitas lalu lintas yang tidak diinginkan.
- Agar hanya lalu lintas ICMP yang muncul, ketik "ICMP" pada kotak filter Wireshark.
- Kotak akan berubah menjadi warna hijau jika sudah difilter dengan benar.
- Klik "Terapkan" (panah kanan) untuk menerapkan filter.



No.	Time	Source	Destination	Protocol	Length	Info
3193	124.122871	192.168.18.70	192.168.18.1	ICMP	74	Echo (ping)
3194	124.123508	192.168.18.1	192.168.18.70	ICMP	74	Echo (ping)
3199	125.138808	192.168.18.70	192.168.18.1	ICMP	74	Echo (ping)
3200	125.139383	192.168.18.1	192.168.18.70	ICMP	74	Echo (ping)
3219	126.155650	192.168.18.70	192.168.18.1	ICMP	74	Echo (ping)
3220	126.156798	192.168.18.1	192.168.18.70	ICMP	74	Echo (ping)
3229	127.173942	192.168.18.70	192.168.18.1	ICMP	74	Echo (ping)
3230	127.174569	192.168.18.1	192.168.18.70	ICMP	74	Echo (ping)

6. Periksa permintaan Echo (ping) pertama di Wireshark.

- Pada panel bagian atas, klik frame pertama yang terdaftar. Akan muncul permintaan Echo (ping) di bawah judul Info.
- Periksa baris pertama di bagian tengah. Baris ini menampilkan panjang dari frame.
- Baris kedua di panel detail paket menunjukkan Frame Ethernet 2. Alamat MAC sumber dan tujuan juga ditampilkan.
- Klik tanda (>) di awal baris kedua untuk informasi tentang Frame Ethernet 2.



```

> Frame 3194: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C4FC26E7-8E9...
- Ethernet II, Src: HuaweiTechno_cf:5d:2a (00:e4:06:cf:5d:2a), Dst: QuantaComput_f9:df:6e (c0:18:50:f9:df:6e)
  > Destination: QuantaComput_f9:df:6e (c0:18:50:f9:df:6e)
  > Source: HuaweiTechno_cf:5d:2a (00:e4:06:cf:5d:2a)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.18.1, Dst: 192.168.18.70
> Internet Control Message Protocol

```

- e. Dua baris terakhir yang ditampilkan di bagian tengah memberikan informasi tentang bidang data. Perhatikan bahwa data berisi informasi alamat IPv4 sumber dan tujuan.
- f. Pilih garis mana saja di bagian tengah untuk menyorot bagian frame tersebut (hex dan ASCII) di panel Packet Bytes (bagian bawah). Klik baris Internet Control Message Protocol di bagian tengah dan periksa apa yang disorot di panel Packet Bytes.

```

> Frame 3194: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C4FC26E7-8E9...
- Ethernet II, Src: HuaweiTechno_cf:5d:2a (00:e4:06:cf:5d:2a), Dst: QuantaComput_f9:df:6e (c0:18:50:f9:df:6e)
  > Destination: QuantaComput_f9:df:6e (c0:18:50:f9:df:6e)
  > Source: HuaweiTechno_cf:5d:2a (00:e4:06:cf:5d:2a)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.18.1, Dst: 192.168.18.70
- Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x4cbe [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 2205 (0x089d)
  Sequence Number (LE): 40200 (0x9d08)
  [Request frame: 3193]
  [Response time: 0,717 ms]
- Data (32 bytes)

```

- g. Klik frame berikutnya di bagian atas dan periksa balasan Echo. Perhatikan bahwa alamat MAC sumber dan tujuan telah dibalik, karena frame ini dikirim dari router gateway default sebagai balasan untuk ping pertama.

```

> Frame 3199: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C4FC26E7-8E9...
- Ethernet II, Src: QuantaComput_f9:df:6e (c0:18:50:f9:df:6e), Dst: HuaweiTechno_cf:5d:2a (00:e4:06:cf:5d:2a)
  > Destination: HuaweiTechno_cf:5d:2a (00:e4:06:cf:5d:2a)
  > Source: QuantaComput_f9:df:6e (c0:18:50:f9:df:6e)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.18.70, Dst: 192.168.18.1
> Internet Control Message Protocol

```

7. Pengambilan paket untuk host jarak jauh.
  - a. Klik "**Start Capture**" untuk memulai pengambilan Wireshark baru. Anda akan menerima sebuah pop-up yang menanyakan apakah ingin menyimpan paket yang diambil sebelumnya ke file sebelum memulai pengambilan baru. Klik "**Continue without Saving.**"
  - b. Pada Command Prompt, ping [www.tokopedia.com](http://www.tokopedia.com).

```

C:\Windows\System32>ping www.tokopedia.com

Pinging a1136.w7.akamai.net [202.169.45.225] with 32 bytes of data:
Reply from 202.169.45.225: bytes=32 time=23ms TTL=56
Reply from 202.169.45.225: bytes=32 time=22ms TTL=56
Reply from 202.169.45.225: bytes=32 time=22ms TTL=56
Reply from 202.169.45.225: bytes=32 time=22ms TTL=56

Ping statistics for 202.169.45.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 23ms, Average = 22ms

```

- c. Hentikan pengambilan paket.
- d. Periksa data baru di panel daftar paket Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
265	19.194456	192.168.18.70	202.169.45.225	ICMP	74	Echo (ping) request id=0x0001, seq=2209/41224, ttl=128 (reply i
266	19.217294	202.169.45.225	192.168.18.70	ICMP	74	Echo (ping) reply id=0x0001, seq=2209/41224, ttl=56 (request
267	20.204927	192.168.18.70	202.169.45.225	ICMP	74	Echo (ping) request id=0x0001, seq=2210/41480, ttl=128 (reply i
268	20.227354	202.169.45.225	192.168.18.70	ICMP	74	Echo (ping) reply id=0x0001, seq=2210/41480, ttl=56 (request
276	21.214955	192.168.18.70	202.169.45.225	ICMP	74	Echo (ping) request id=0x0001, seq=2211/41736, ttl=128 (reply i
277	21.237129	202.169.45.225	192.168.18.70	ICMP	74	Echo (ping) reply id=0x0001, seq=2211/41736, ttl=56 (request
279	22.223909	192.168.18.70	202.169.45.225	ICMP	74	Echo (ping) request id=0x0001, seq=2212/41992, ttl=128 (reply i
280	22.246298	202.169.45.225	192.168.18.70	ICMP	74	Echo (ping) reply id=0x0001, seq=2212/41992, ttl=56 (request

<p>Frame 265: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C4FC26E7-8E95-480B-AC79-ADB825155B6}, id 0</p> <p>Ethernet II, Src: QuantaComput_f9:df:6e (c0:18:50:f9:df:6e), Dst: HuaweiTechno_cf:5d:2a (00:e4:06:cf:5d:2a)</p> <p>Destination: HuaweiTechno_cf:5d:2a (00:e4:06:cf:5d:2a)</p> <p>Source: QuantaComput_f9:df:6e (c0:18:50:f9:df:6e)</p> <p>Type: IPv4 (0x0800)</p> <p>Internet Protocol Version 4, Src: 192.168.18.70, Dst: 202.169.45.225</p> <p>Internet Control Message Protocol</p>
--

---

## PERTANYAAN TUGAS

- a. Apa tipe protokol yang digunakan dalam frame Ethernet saat melakukan ping dari host PC ke default gateway? Jelaskan bagaimana Anda menemukannya menggunakan Wireshark.
- b. Deskripsikan informasi yang dapat ditemukan dalam frame pertama yang ditangkap oleh Wireshark ketika Anda melakukan ping ke default gateway.
- c. Bandingkan alamat MAC dari frame permintaan ICMP pertama dengan alamat MAC yang diterima di frame balasan ICMP. Jelaskan perubahan yang terjadi.
- d. Bagaimana proses resolusi alamat bekerja ketika sebuah perangkat di jaringan ingin berkomunikasi dengan perangkat lain yang alamat IP-nya diketahui namun alamat MAC-nya tidak diketahui?
- e. Apa alamat IP dari PC yang Anda gunakan dalam pengujian ini? Jelaskan langkah-langkah untuk menemukannya menggunakan Command Prompt.
- f. Mengapa frame Ethernet yang dikirim dari PC Anda saat melakukan ping menggunakan alamat MAC broadcast? Jelaskan proses dan tujuannya.

---

### CATATAN PRAKTEK

1. Batas maksimal dikerjakan H-1 praktikum dan dikumpulkan di i-Lab dengan format:  
**[Nama\_Nim\_Modul2].rar**
  2. Batas maksimal pengerjaan di NetAcad adalah 1 minggu setelah jadwal praktikum.
  3. Semoga Beruntung ! 😊
- 

### KRITERIA PENILAIAN TUGAS

- > 81 : Praktikan mampu mengerjakan serta menjelaskan tugas yang ada di materi tugas dengan benar.
  - 70 – 80 : Praktikan mampu mengerjakan serta menjelaskan tugas yang ada di materi tugas namun kurang maksimal.
  - 55 - 69 : Praktikan memiliki pemahaman yang terbatas tentang materi tugas dan perlu meningkatkan kemampuan dalam mengerjakan serta menjelaskan tugas.
  - < 55 : Praktikan tidak memahami, menjawab, dan memahami materi modul tugas.
- 

### KRITERIA PENILAIAN PRAKTEK

- > 81 : Praktikan mampu memahami, menjawab, dan menjelaskan materi praktek kepada asisten.
  - 70 – 80 : Praktikan mampu memahami, menjawab, dan menjelaskan materi praktek kepada asisten namun kurang maksimal.
  - 55 - 69 : Praktikan mampu menjawab soal yang ada di materi praktek kepada asisten namun tidak bisa menjelaskan proses yang terjadi.
  - < 55 : Praktikan tidak memahami, menjawab, dan menjelaskan materi praktek kepada asisten.
- 

### DETAIL PENILAIAN PRAKTIKUM

ASPEK PENILAIAN	POIN
TUGAS	30
PRAKTEK	70