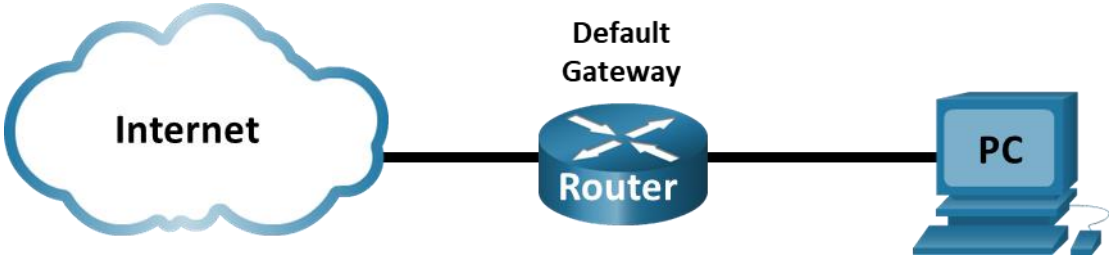
4. Wireshark: Memeriksa Frame Ethernet

Topologi



Tujuan

- Latihan 1: Memeriksa header dalam frame Ethernet II
- Latihan 2: Menangkap dan menganalisis frame Ethernet dengan Wireshark

Skenario

Pada saat protokol-protokol layer lebih atas saling berkomunikasi, data mengalir menuruni layer-layer *Open Systems Interconnection* (OSI) dan dienkapsulasi ke dalam suatu frame Layer 2. Komposisi frame tersebut tergantung pada jenis *media access*. Sebagai contoh, jika protokol layer lebih atas adalah TCP dan IP dan media accessnya adalah Ethernet, maka enkapsulasi frame Layer 2 akan berupa Ethernet II. Ini merupakan tipikal untuk lingkungan LAN.

Ketika belajar mengenai konsep Layer 2, sangat berguna untuk menganalisis informasi header frame. Dalam Latihan 1 dari praktikum kali ini, Anda akan mereview field-field yang terkandung di dalam suatu frame Ethernet II. Dalam Latihan 2, anda akan menggunakan Wireshark untuk meng-capture dan menganalisis field-field header frame Ethernet II untuk trafik lokal dan jauh.

Kebutuhan Perangkat

1 PC (Windows dengan akses Internet dan Wireshark yang telah terinstal)

Latihan 1: Memeriksa Header Frame Ethernet II

Dalam latihan 1, anda akan memeriksa field-field header dan isi dalam suatu frame Ethernet II. Suatu tangkapan Wireshark akan digunakan untuk mengetahui isi di dalam field-field tersebut.

Langkah 1: Review Deskrpsi dan Panjang Header Ethernet II.

Preamble	Destination Address	Source Address	Frame Type	Data	FCS
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 – 1500 Bytes	4 Bytes

Langkah 2: Memeriksa konfigurasi jaringan dari PC.

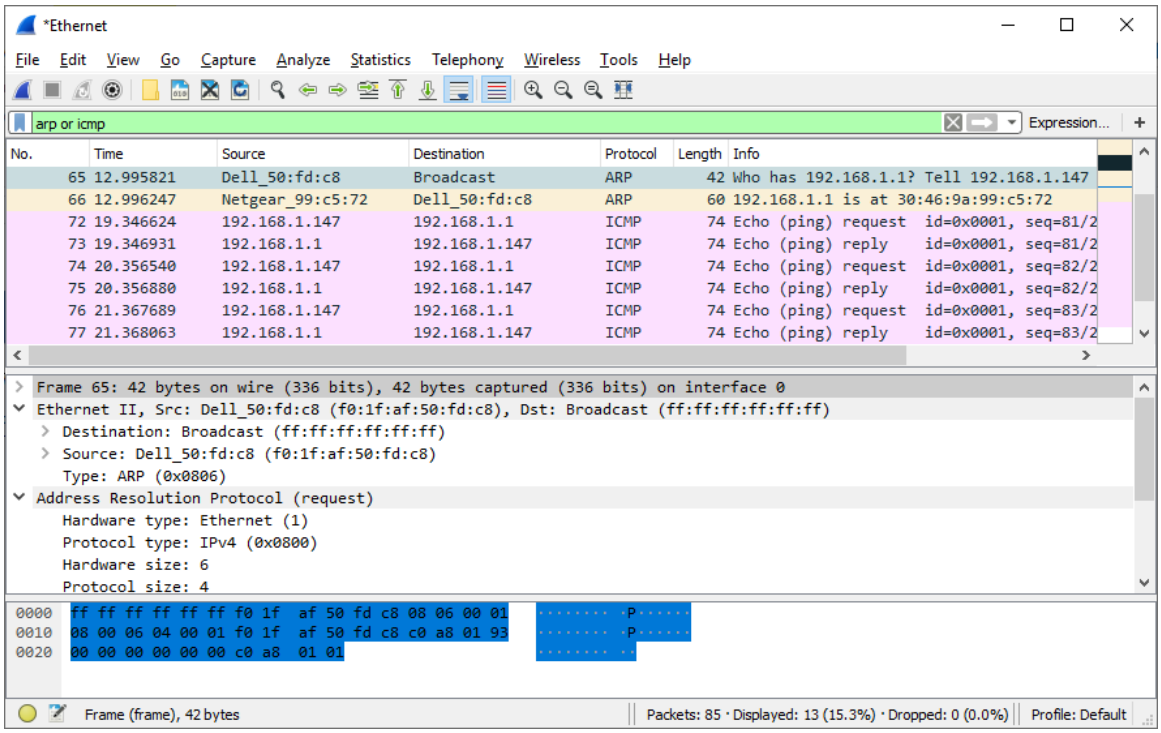
Dalam contoh di bawah, host PC ini mempunyai IP address 192.168.1.147 dan default gatewaynya mempunyai IP address 192.168.1.1.

```
C:\> ipconfig /all

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connection
   Physical Address. . . . . . . . . : F0-1F-AF-50-FD-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::58c5:45f2:7e5e:29c2%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, September 6, 2019 11:08:36 AM
   Lease Expires . . . . . . . . . . : Saturday, September 7, 2019 11:08:36 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
<output omitted>
```

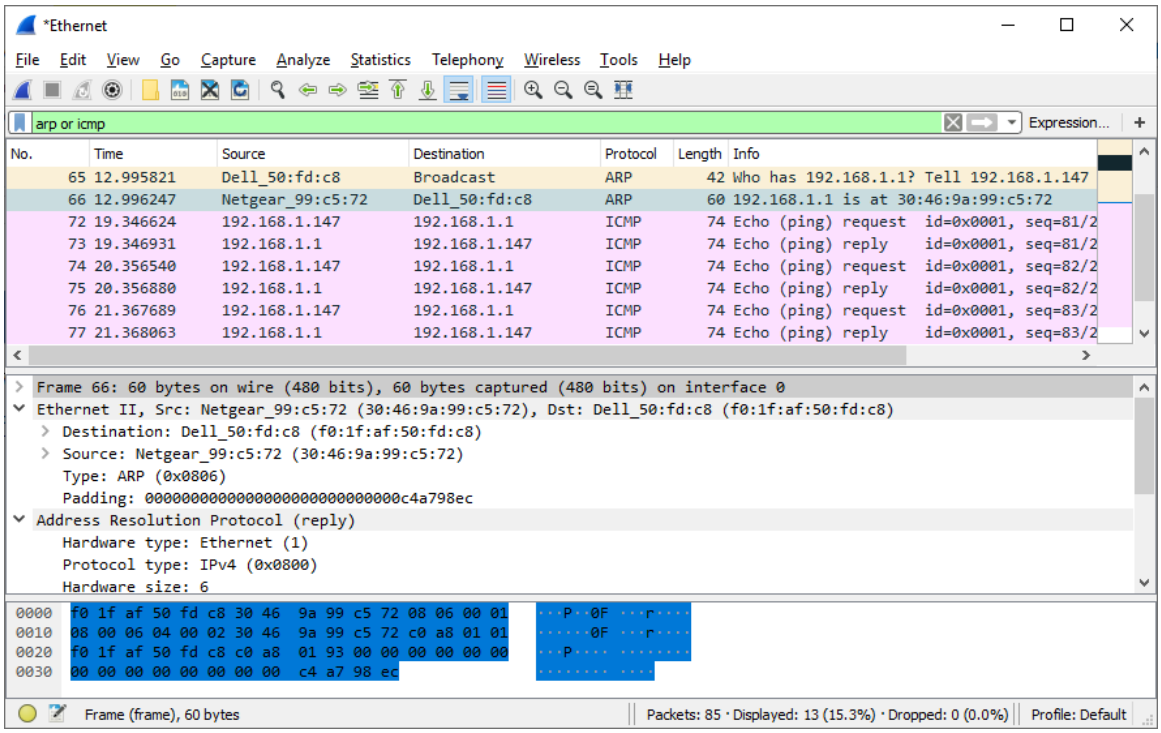
Langkah 3: Memeriksa frame Ethernet dalam tangkapan Wireshark.

Tangkapan layar dari tangkapan Wireshark di bawah memperlihatkan paket-paket yang dibangkitkan oleh suatu ping yang dijalankan dari host PC ke gateway defaultnya. Suatu filter telah diberlakukan terhadap Wireshark untuk menampilkan hanya protokol ARP dan ICMP. ARP merupakan singkatan bagi *address resolution protocol*. ARP adalah protokol komunikasi yang digunakan untuk memperoleh MAC address yang diasosiasikan dengan IP address tertentu. Sesinya dimulai dengan suatu query ARP dan jawaban untuk MAC address dari gateway router, diikuti oleh empat request dan jawaban ping.

Tampilkan ini menyoroti rincian frame untuk suatu request ARP.



Screenshot ini menyorot rincian frame untuk balasan ARP (ARP *reply*).



Langkah 4: Memeriksa isi header Ethernet II dari Request ARP.

Tabel berikut ini memperlihatkan frame pertama dalam tangkapan Wireshark dan menampilkan data di dalam field header Ethernet II.

Field	Value	Description
Preamble	Tidak terlihat dalam tangkapan	Field ini mengandung bit-bit sinkronisasi, diproses oleh hardware NIC.
Destination Address	Broadcast (ff:ff:ff:ff:ff:ff)	Alamat Layer 2 untuk frame tersebut. Setiap address panjangnya 48 bit atau 6 octet, diekspresikan sebagai 12 digit hexadecimal, 0-9,A-F. Format umumnya 12:34:56:78:9A:BC.
Source Address	Netgear_99:c5:72 (30:46:9a:99:c5:72)	6 angka heksa pertama menunjukkan kode pabrik *network interface card* (NIC), 6 angka heksa terakhir merupakan nomor seri dari NIC tersebut. Destination Address dapat berupa alamat broadcast yang berisi semua alamat atau unicast. Source address selalu unicast.
Frame Type	0x0806	Untuk frame Ethernet II, field ini mengandung suatu nilai hexadecimal yang digunakan untuk menunjukkan jenis protokol upper-layer dalam data field. Ada banyak protokol upper-layer yang didukung oleh Ethernet II. Dua jenis frame yang umum adalah Nilai Deskripsi 0x0800 IPv4 Protocol 0x0806 Address Resolution Protocol (ARP)
Data	ARP	Mengandung protokol upper-level yang terenkapsulasi. Data field antara 46 – 1,500 byte.
FCS	Tidak terlihat dalam tangkapan	Frame Check Sequence, digunakan oleh NIC untuk mengidentifikasi error selama transmisi. Nilai ini dihitung oleh perangkat yang mengirimkan, mencakup jenis, field data dan alamat frame. Ini diverifikasi oleh penerima (receiver).

Pertanyaan

1. Apa yang penting mengenai isi dari field *destination address*?
2. Mengapa PC mengirimkan suatu broadcast ARP sebelum mengirimkan request ping yang pertama?
3. Sebutkan MAC address dari source dalam frame pertama?
4. Sebutkan Vendor ID (OUI) dari Source NIC dalam balasan ARP?
5. Bagian mana dari MAC address yang merupakan OUI?
6. Sebutkan nomor seri NIC dari source!

Latihan 2: Wireshark: Menangkap & Menganalisis Frame Ethernet

Dalam latihan 2, anda akan menggunakan Wireshark untuk meng*capture* frame Ethernet lokal dan remote. Anda kemudian akan memeriksa informasi yang terkandung di dalam filed-field header frame tersebut.

Langkah 1: Mengetahui IP address dari default gateway pada PC anda.

1. Bukan jendela command prompt dan jalankan perintah **ipconfig**.
2. Tuliskan IP address dari default gateway!

Langkah 2: Mulai menangkap trafik pada NIC PC.

1. Buka Wireshark dan mulailah menangkap data.
2. Amati trafik yang muncul di dalam jendela daftar paket.

Langkah 3: Menfilter Wireshark untuk menampilkan hanya trafik ICMP.

Anda dapat menggunakan filter dalam Wireshark untuk memblok visibilitas dari trafik yang tidak diinginkan. Filter ini tidak memblok capture data yang tak diiinginkan; hanya menyaring apa yang ingin ditampilkan pada layar. Saat ini, hanya trafik ICMP yang ditampilkan.

Dalam kotak **Filter** Wireshark, ketik **icmp**. Kotak tersebut akan menjadi hijau (green) jika anda memasukkan filter dengan benar. Jika kotak sudah hijau, klik **Apply** (panah kanan) untuk memberlakukan filternya.

Langkah 4: Dari jendela command prompt, ping default gateway dari PC.

Dari jendela command, ping terhadap default gateway menggunakan IP address yang telah anda rekam dalam Langkah 1.

Langkah 5: Hentikan penangkapan trafik pada NIC.

Klik ikon **Stop Capturing Packets** untuk menghentikan penangkapan trafik.

Langkah 6: Periksa request Echo (ping) pertama dalam Wireshark.

Jendela utama Wireshark dibagi ke dalam tiga bagian: panel daftar paket (atas), panel **Packet Details** (tengah), dan panel **Packet Bytes** (bawah). Jika anda memilih interface yang tepat untuk penangkapan paket sebelumnya, Wireshark akan menampilkan informasi ICMP dalam panel daftar paket Wireshark.

- Dalam panel daftar paket (bagian atas), klik frame pertama. Anda akan melihat **Echo (ping) request** di bawah judul **Info**. Baris tersebut menjadi tersorot.
- Periksa baris pertama dalam panel rincian paket (bagian tengah). Baris ini menampilkan panjang dari frame.
- Baris kedua dalam panel rincian paket menunjukkan bahwa itu merupakan frame Ethernet II. MAC address dari source dan destination juga ditampilkan.

Pertanyaan

1. Apa MAC address dari NIC PC?
2. Apa MAC address dari default gateway?
3. Anda dapat klik tanda lebih dari (>) pada awal baris kedua untuk memperoleh informasi lanjutan dari frame Ethernet II.

   Jenis frame apa yang ditampilkan?
4. Dua baris terakhir ditampilkan dalam bagian tengah menyediakan informasi mengenai field data dari frame. Ingatlah bahwa data mengandung informasi IPv4 address source dan destination.

   Mana IP address dari source?

   Mana IP address dari destination?
3. Anda dapat klik baris manapun dalam bagian tengah untuk menyorot bagian itu dari frame (hex dan ASCII) dalam panel **Packet Bytes** (bagian bawah). Klik baris **Internet Control Message Protocol** dalam bagian tengah dan periksa apa yang disorot dalam panel **Packet Bytes**.

   Bagaimana mengeja dua oktet terakhir yang disorot?

4. Klik frame selanjutnya di dalam bagian atas dan periksalah frame Echo reply. Ingatlah bahwa MAC address dari source dan destination sudah terbalik, karena frame ini dikirimkan dari router default gateway sebagai balasan terhadap ping yang pertama.
5. Sebutkan device dan MAC address yang ditampilkan sebagai destination address!

Langkah 7: Menangkap paket host jauh.

1. Klik ikon **Start Capture** untuk memulai suatu tangkapan Wireshark baru. Anda akan menerima jendela popup menanyakan apakah akan menyimpan paket tangkapan sebelumnya ke suatu file sebelum memulai tangkapan baru. Klik **Continue without Saving**.

   Buka suatu jendela command prompt.
2. Dalam jendela prompt window, silakan ping ke www.cisco.com.

   Tututp jendeka command prompt.
3. Hentikan penangkapan paket.
4. Periksa paket baru dalam panel daftar paket dari Wireshark.

Pertanyaan

1. Dalam frame request echo (ping) pertama, mana yang merupakan MAC address source dan destination?

   Source:

   Destination:

2. Sebtukan IP address source dan destination yang terkandung di dalam field data dari frame!

   Source:

   Destination:

3. Bandingkan address ini dengan address yang diterima pada Langkah 6. Address yang berubah hanyalah IP address destination. Mengapa IP address destination berubah, sedangkan MAC address destination tersebut masih tetap sama?

4. Wireshark tidak menampilkan field *preamble* dari suatu header frame. Apa yang terkandung dalam *preamble*?