

TECHNICAL REPORT

PRAKTIKUM JARINGAN KOMPUTER

MODUL 4



Disusun Oleh :

TGL. PRAKTIKUM	: 8 April 2021
NAMA	: Achmad Farid Alfa Waid
NIM	: 190411100073
KELOMPOK	: 1
DOSEN	: Yoga Dwitya Pramudita, S.Kom
ASPRAK	: Rizal Abdul Fata



LABORATORIUM COMMON COMPUTING
JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS TRUNOJOYO MADURA

2020

I. Latihan 1

1. Langkah 1: Review Deskripsi 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

Preamble:

8 bit ini mengandung bit-bit sinkronisasi, diproses oleh hardware NIC.

Destination Address:

6 byte adalah Destination Mac Address dari tujuan data. Disinilah Mac Address digunakan komputer untuk berkomunikasi. jadi, sebelum sampai ke target yang dituju, sebaiknya adalah untuk mengetahui Mac Addressnya terlebih dahulu, agar mempermudah ketika berkomunikasi menggunakan ethernet. Mac Address tujuan data juga dapat di isi dengan (ff:ff:ff:ff:ff:ff). ini berfungsi untuk membroadcast data. jadi seluruh pc akan membaca dari pesan dengan mac address tujuan seperti tersebut.

Source Address:

6 byte adalah Mac Address dari pengirim. perangkat jaringannya pasti telah terdapat Mac Addressnya. Contoh value: Netgear_99:c5:72 (30:46:9a:99:c5:72). 6 angka heksa pertama menunjukkan kode network interface card (NIC), 6 angka heksa terakhir merupakan nomor seri dari NIC tersebut.

Frame Type:

2 byte digunakan untuk type komunikasi. 2 byte ini maka di isi dengan 08 06 kalau untuk valuenya sendiri maka akan terlihat seperti ini (0x0806). Untuk frame Ethernet II, field ini mengandung suatu nilai hexadecimal yang digunakan untuk menunjukkan jenis protokol upperlayer dalam data field.

Data:

Data 46 – 1500 byte ini merupakan protokol upper-level yang terenkapsulasi dan memiliki panjang tampungan dari interval 46 byte hingga 1500 byte.

FCS(Frame Check Sequence):

Dilihat dari banyaknya byte(4 byte) kemungkinan frame ini merupakan CRC32.

2. Langkah 2: Memeriksa konfigurasi jaringan dari PC

```
Command Prompt

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : Realtek RTL8723DE 802.11b/g/n PCIe Adapter
Physical Address. . . . . : 80-91-33-F8-87-D9
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4dc:738d:7e2f:b28f%15(Preferred)
IPv4 Address. . . . . : 192.168.0.105(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Jumat, 07 Mei 2021 12.26.46
Lease Expires . . . . . : Sabtu, 08 Mei 2021 20.57.48
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 226529587
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-21-BD-53-00-68-EB-3B-21-64
DNS Servers . . . . . : 192.168.0.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 80-91-33-F8-87-D8
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Pada PC saya memiliki IP Address **192.168.0.105** dan default gateway **192.168.0.1**

3. Langkah 3: Memeriksa frame Ethernet dalam tangkapan Wireshark

Dikarenakan saya menggunakan jaringan wifi maka untuk capture jaringanya saya memilih wifi. berikut merupakan rincian frame untuk suatu request ARP or ICMP.

Wireshark interface showing a capture on the Wi-Fi interface. The packet list pane displays several ARP requests. Packet 5854 is selected, showing details of an ARP request from TendaTec_6e:96:40 to Broadcast.

No.	Time	Source	Destination	Protocol	Length	Info
5854	0.000000	TendaTec_6e:96:40	Broadcast	ARP	42	Who has 192.168.0.101? Tell 192.168.0.1
5942	38.036046	TendaTec_6e:96:40	Broadcast	ARP	42	Who has 192.168.0.101? Tell 192.168.0.1
5962	38.436754	TendaTec_6e:96:40	Broadcast	ARP	42	Who has 192.168.0.101? Tell 192.168.0.1
6299	55.640030	TendaTec_6e:96:40	Broadcast	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
6304	60.965218	TendaTec_6e:96:40	Broadcast	ARP	42	Who has 192.168.0.105? Tell 192.168.0.1
6305	60.965248	AzureNav_f8:87:d9	TendaTec_6e:96:40	ARP	42	192.168.0.105 is at 80:91:33:f8:87:d9

Packet 5854 details:

- Frame 5854: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{CDA18B8F-150A-4215-8ABA-44414310020B}, id 0
- Ethernet II, Src: TendaTec_6e:96:40 (cc:2d:21:6e:96:40), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (request)

Packet bytes:

Offset	Hex	ASCII
0000	ff ff ff ff ff cc 2d 21 6e 96 40 08 06 00 01In. @----
0010	08 00 06 04 00 01 cc 2d 21 6e 96 40 c0 a8 00 01In. @----
0020	00 00 00 00 00 00 c0 a8 00 65e

berikut merupakan rincian frame untuk balsan ARP (ARP reply)

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
5854	37.310330	TendaTec_6e:96:40	Broadcast	ARP	42	Who has 192.168.0.101? Tell 192.168.0.1
5942	38.036046	TendaTec_6e:96:40	Broadcast	ARP	42	Who has 192.168.0.101? Tell 192.168.0.1
5962	38.436754	TendaTec_6e:96:40	Broadcast	ARP	42	Who has 192.168.0.101? Tell 192.168.0.1
6299	55.640030	TendaTec_6e:96:40	Broadcast	ARP	42	Who has 192.168.0.100? Tell 192.168.0.1
6304	60.965218	TendaTec_6e:96:40	Broadcast	ARP	42	Who has 192.168.0.105? Tell 192.168.0.1
6305	60.965248	AzureWav_f8:87:d9	TendaTec_6e:96:40	ARP	42	192.168.0.105 is at 80:91:33:f8:87:d9

> Frame 6305: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{CDA18B8F-150A-4215-8ABA-44414310020B}, id 0

> Ethernet II, Src: AzureWav_f8:87:d9 (80:91:33:f8:87:d9), Dst: TendaTec_6e:96:40 (cc:2d:21:6e:96:40)

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: AzureWav_f8:87:d9 (80:91:33:f8:87:d9)

Sender IP address: 192.168.0.105

Target MAC address: TendaTec_6e:96:40 (cc:2d:21:6e:96:40)

Target IP address: 192.168.0.1

```

0000  cc 2d 21 6e 96 40 80 91 33 f8 87 d9 08 06 00 01  --In @.. 3-----
0010  08 00 06 04 00 02 80 91 33 f8 87 d9 c0 a8 00 69  .... 3-----i
0020  cc 2d 21 6e 96 40 c0 a8 00 01  --In @.. ..

```

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

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	AzureWav_f8:87:d9 (80:91:33:f8:87:d9)	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 upperlayer 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).

A. Soal dalam modul

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!

Jawaban :

1. Field Destination Address adalah sebuah field yang memiliki panjang 6 byte yang menandakan alamat tujuan ke mana frame yang bersangkutan akan dikirimkan. Alamat tujuan ini bisa berupa alamat unicast Ethernet, alamat multicast Ethernet, atau alamat broadcast Ethernet. Jika tidak ada alamat pada field destination address, maka tidak akan ada yang dituju.
2. untuk meminta Mac Address dari host dengan alamat IP yang terdapat dalam ARP. MAC Address tersebut nantinya akan digunakan untuk alamat yang akan dituju.
3. 80:91:33:f8:87:d9
4. Azure Wave
5. 3 octet pertama dari alamat Mac menunjukkan OUI.
6. f8:87:d9

II. Latihan 2

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

```
Command Prompt

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : 
Description . . . . . : Realtek RTL8723DE 802.11b/g/n PCIe Adapter
Physical Address. . . . . : 80-91-33-F8-87-D9
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4dc:738d:7e2f:b28f%15(Preferred)
IPv4 Address. . . . . : 192.168.0.105(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Jumat, 07 Mei 2021 12.26.46
Lease Expires . . . . . : Sabtu, 08 Mei 2021 20.57.48
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 226529587
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-21-BD-53-00-68-EB-3B-21-64
DNS Servers . . . . . : 192.168.0.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 80-91-33-F8-87-D8
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Pada PC saya memiliki IP Address **192.168.0.105** dan default gateway **192.168.0.1**

2. Langkah 2: Mulai menangkap trafik pada NIC PC

Saya menggunakan wifi untuk capture jaringan.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
10	1.072040	192.168.0.105	35.186.224.25	TCP	54	51580 → 443 [ACK] Seq=196 Ack=332 Win=255 Len=0
11	1.072149	35.186.224.25	192.168.0.105	TLSv1.2	272	Application Data
12	1.078388	35.186.224.25	192.168.0.105	TLSv1.2	96	Application Data
13	1.078459	192.168.0.105	35.186.224.25	TCP	54	51580 → 443 [ACK] Seq=196 Ack=589 Win=254 Len=0
14	1.078634	192.168.0.105	35.186.224.25	TLSv1.2	93	Application Data
15	1.108075	35.186.224.25	192.168.0.105	TCP	56	443 → 51580 [ACK] Seq=589 Ack=235 Win=2430 Len=0
16	3.533054	192.168.0.105	35.186.224.46	TLSv1.2	97	Application Data
17	3.568336	35.186.224.46	192.168.0.105	TCP	56	443 → 51214 [ACK] Seq=1 Ack=44 Win=269 Len=0
18	3.620165	35.186.224.46	192.168.0.105	TLSv1.2	96	Application Data
19	3.662899	192.168.0.105	35.186.224.46	TCP	54	51214 → 443 [ACK] Seq=44 Ack=41 Win=255 Len=0
20	4.697446	192.168.0.105	36.91.234.48	TCP	55	51955 → 443 [ACK] Seq=1 Ack=1 Win=8519 Len=1 [TCP segment of a reassembled PDU]
21	4.748154	36.91.234.48	192.168.0.105	TCP	68	443 → 51955 [ACK] Seq=1 Ack=2 Win=245 Len=0 SLE=1 SRE=2

> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{CDA18B8F-150A-4215-8ABA-444143100208}, id 0
> Ethernet II, Src: AzureWav_f8:87:d9 (80:91:33:f8:87:d9), Dst: TendaTec_6e:96:40 (cc:2d:21:6e:96:40)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 74.125.200.188
> Transmission Control Protocol, Src Port: 50983, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
> Data (1 byte)

```
0000  cc 2d 21 6e 96 40 80 91 33 f8 87 d9 08 00 45 00  ..In@...3....E-
0010  00 29 55 89 40 00 80 06 d0 fa c0 a8 00 69 4a 7d  ..)U_@... ..13}
0020  c8 bc c7 27 14 6c 25 d0 cd fe 8d 21 12 b2 50 10  ...'.1%...|.P.
0030  01 00 6b 52 00 00 00      ..kR...
```

3. Langkah 3: Menfilter Wireshark untuk menampilkan hanya trafik ICMP

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

icmp

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

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

```
Command Prompt
Microsoft Windows [Version 10.0.19042.928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hp>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64

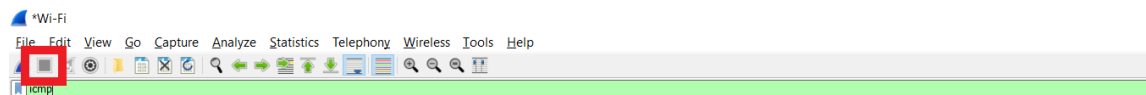
Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\Users\hp>
```

5. Langkah 5: Hentikan penangkapan trafik pada NIC

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



No.	Time	Source	Destination	Protocol	Length	Info
1257	123.928365	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 1256)
1274	124.938486	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 1275)
1275	124.940604	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 1274)
1277	125.952553	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 1278)
1278	125.954952	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 1277)
1285	126.965304	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 1286)
1286	126.967572	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 1285)

> Frame 1256: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CDA18B8F-150A-4215-8ABA-44414310020B}, id 0
> Ethernet II, Src: AzureWav_f8:87:d9 (80:91:33:f8:87:d9), Dst: TendaTec_6e:96:40 (cc:2d:21:6e:96:40)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.1
> Internet Control Message Protocol

0000 cc 2d 21 6e 96 40 80 91 33 f8 87 d9 08 00 45 00 --ln @ 3E-
0010 00 3c 41 1e 00 00 80 01 77 e8 c0 a8 00 69 c0 a8 -<A.... w....i..
0020 00 01 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66 ...MZ... abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

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

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1256	123.926396	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 1257)
1257	123.928365	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 1256)
1274	124.938486	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 1275)
1275	124.940604	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 1274)
1277	125.952553	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 1278)
1278	125.954952	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 1277)
1285	126.965304	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 1286)
1286	126.967572	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 1285)

> Frame 1256: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CDA18B8F-150A-4215-8ABA-44414310020B}, id 0
 > Ethernet II, Src: AzureWav_f8:87:d9 (80:91:33:f8:87:d9), Dst: TendaTec_6e:96:40 (cc:2d:21:6e:96:40)
 > Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.1
 > Internet Control Message Protocol

```

0000  cc 2d 21 6e 96 40 80 91 33 f8 87 d9 08 00 45 00  --In-@... 3-----E-
0010  00 3c 41 1e 00 00 80 01 77 e8 c0 a8 00 69 c0 a8  .<A-----w....i..
0020  00 01 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66  ....MZ...-abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                  wabcdefg hi

```

A. Soal dalam modul

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?
5. 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?
6. 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.
7. Sebutkan device dan MAC address yang ditampilkan sebagai destination address!

Jawaban :

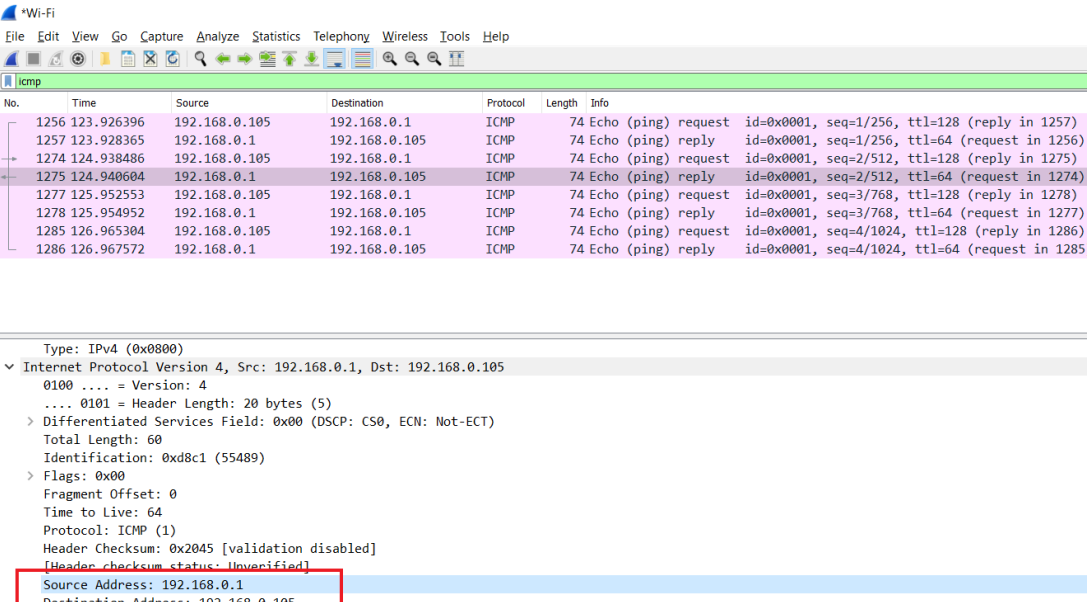
1. 80:91:33:f8:87:d9
2. cc:2d:21:6e:96:40

3.
 - ▼ Ethernet II, Src: AzureWav_f8:87:d9 (80:91:33:f8:87:d9), Dst: TendaTec_6e:96:40 (cc:2d:21:6e:96:40)
 - > Destination: TendaTec_6e:96:40 (cc:2d:21:6e:96:40)
 - > Source: AzureWav_f8:87:d9 (80:91:33:f8:87:d9)
 - Type: IPv4 (0x0800)
 - ▼ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.1
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 60
 - Identification: 0x411e (16670)
 - > Flags: 0x00
 - Fragment Offset: 0
 - Time to Live: 128
 - Protocol: ICMP (1)
 - Header Checksum: 0x77e8 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.0.105
 - Destination Address: 192.168.0.1
- 4.

Ip Address : 192.168.0.105

Destination Address: 192.168.0.1

5.
 - ▼ Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0x4d5a [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence Number (BE): 1 (0x0001)
 - Sequence Number (LE): 256 (0x0100)
 - [\[Response frame: 1257\]](#)
 - > Data (32 bytes)

6. 

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1256	123.926396	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 1257)
1257	123.928365	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 1256)
1274	124.938486	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 1275)
1275	124.940604	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 1274)
1277	125.952553	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 1278)
1278	125.954952	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 1277)
1285	126.965304	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 1286)
1286	126.967572	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 1285)

Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0xd8c1 (55489)

> Flags: 0x00

Fragment Offset: 0

Time to Live: 64

Protocol: ICMP (1)

Header Checksum: 0x2045 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.0.1

Destination Address: 192.168.0.105

Terbalik

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1256	123.926396	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 1257)
1257	123.928365	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 1256)
1274	124.938486	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 1275)
1275	124.940604	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 1274)
1277	125.952553	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 1278)
1278	125.954952	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 1277)
1285	126.965304	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 1286)
1286	126.967572	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 1285)

> Frame 1275: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CDA18B8F-150A-4215-8ABA-44414310020B}, id 0

> Ethernet II, Src: TendaTec_6e:96:40 (cc:2d:21:6e:96:40), Dst: AzureWav_f8:87:d9 (80:91:33:f8:87:d9)

> Destination: AzureWav_f8:87:d9 (80:91:33:f8:87:d9)

> Address: AzureWav_f8:87:d9 (80:91:33:f8:87:d9)

> ..0. = LG bit: Globally unique address (factory default)

>0. = IG bit: Individual address (unicast)

> Source: TendaTec_6e:96:40 (cc:2d:21:6e:96:40)

> Type: IPv4 (0x0800)

7.

Azure Wave

7. Langkah 7: Menangkap paket host jauh

Quit without saving

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1256	123.926396	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 1257)
1257	123.928365	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 1256)
1274	124.938486	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 1275)
1275	124.940604	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 1274)
1277	125.952553	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 1278)
1278	125.954952	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 1277)
1285	126.965304	192.168.0.105	192.168.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 1286)
1286	126.967572	192.168.0.1	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 1285)

> Frame 1275: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CDA18B8F-150A-4215-8ABA-44414310020B}, id 0

> Ethernet II, Src: TendaTec_6e:96:40 (cc:2d:21:6e:96:40), Dst: AzureWav_f8:87:d9 (80:91:33:f8:87:d9)

> Destination: AzureWav_f8:87:d9 (80:91:33:f8:87:d9)

> Address: AzureWav_f8:87:d9 (80:91:33:f8:87:d9)

> ..0. = LG bit: Globally unique address (factory default)

>0. = IG bit: Individual address (unicast)

> Source: TendaTec_6e:96:40 (cc:2d:21:6e:96:40)

> Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105

> Internet Control Message Protocol

Unsaved packets...

Do you want to save the captured packets before quitting?

Your captured packets will be lost if you don't save them.

Save Quit without Saving Cancel

0000 80 91 33 f8 87 d9 cc 2d 21 6e 96 40 00 00 45 00 ...3... In @ . E-

0010 00 3c d8 c1 00 00 00 01 20 45 c0 a8 00 01 c0 a8 ...<...@: E-----

0020 00 69 00 00 55 59 00 01 00 02 61 62 63 64 65 66 ...i..UY... abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ...ghijklm opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 ...wabcdfgh i

Source Address (p.prc), 4 byte(s)

Packets: 1469 - Displayed: 8 (0.5%) - Dropped: 0 (0.0%)

Profile: Default

Ping ke www.cisco.com

Command Prompt

Microsoft Windows [Version 10.0.19042.928]

(c) Microsoft Corporation. All rights reserved.

C:\Users\hp>cd..

C:\Users>cd..

C:\>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [104.93.97.215] with 32 bytes of data:

Reply from 104.93.97.215: bytes=32 time=15ms TTL=59

Reply from 104.93.97.215: bytes=32 time=15ms TTL=59

Reply from 104.93.97.215: bytes=32 time=15ms TTL=59

Reply from 104.93.97.215: bytes=32 time=30ms TTL=59

Ping statistics for 104.93.97.215:

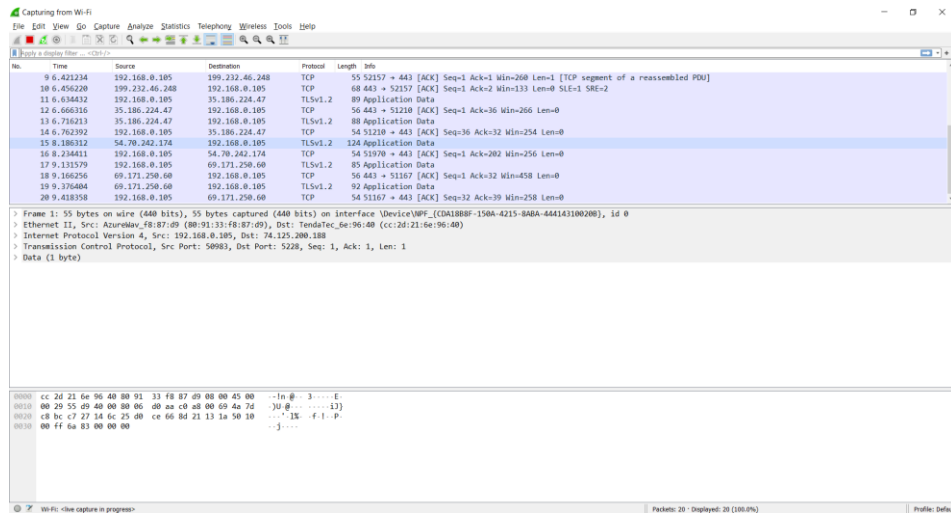
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 15ms, Maximum = 30ms, Average = 18ms

C:\>

Capture whreshark baru



B. Soal dalam modul

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

Source:

Destination:

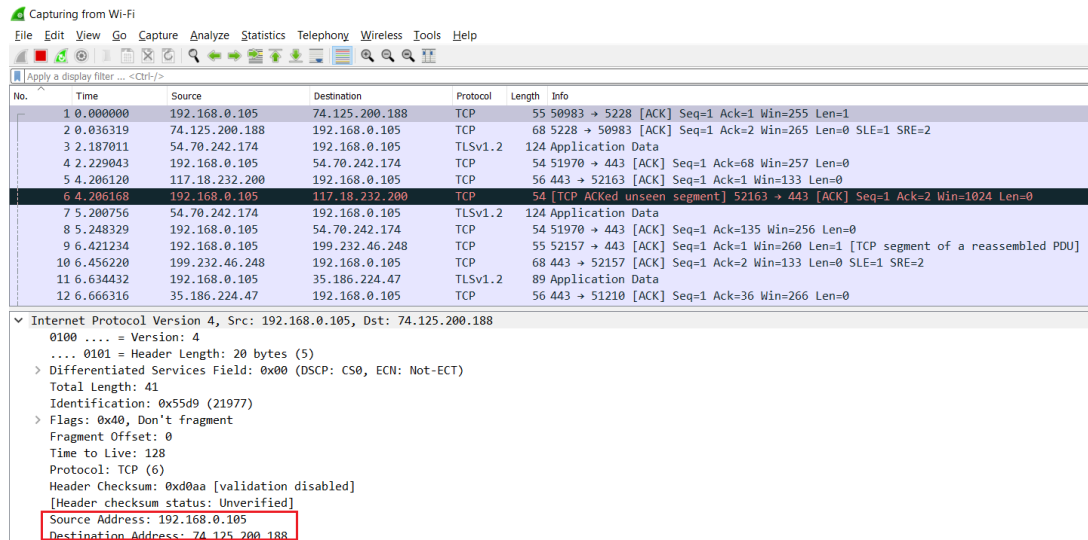
2. Sebutkan IP address source dan destination yang terkandung di dalam field data dari frame!

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?

Jawaban :



1.

Source: 192.168.0.105

Destination: 74.125.200.188

2. **Source: 192.168.0.105**

Destination: 74.125.200.188

3. Langkah 6:

Source: 192.168.0.105

Destination: 192.168.0.1

Langkah 7:

Source: 192.168.0.105

Destination: 74.125.200.188

Karena frame layer 2 tidak pernah meninggalkan LAN. Ketika ping dikeluarkan ke host jarak jauh, sumber akan menggunakan alamat MAC Gateway Default untuk tujuan bingkai. Default Gateway menerima paket, menghapus informasi frame Layer 2 dari paket dan kemudian membuat header frame baru dengan alamat MAC hop berikutnya. Proses ini berlanjut dari router ke router hingga paket mencapai alamat IP tujuannya.

4. Field Preamble berisi tujuh oktet dari urutan 1010 bergantian, dan satu oktet yang menandakan awal frame, 10101011.