

VERSION 2.0
SEPTEMBER 29, 2021



[PRAKTIKUM KOMUNIKASI DATA]

MODUL 1 TUGAS– BASIC NETWORK CONNECTIVITY AND COMMUNICATIONS

DISUSUN OLEH :

SALSABILA AULIA RAMADHAN
WAHYU BUDI UTOMO

DIAUDIT OLEH :

MAHAR FAIQURAHMAN, S.KOM., M.T.
FAUZI DWI SETIAWAN SUMADI, S.T., M.CompSc.

PRESENTED BY: TIM LAB-IT

UNIVERSITAS MUHAMMADIYAH MALANG

[PRAKTIKUM KOMUNIKASI DATA]

PERSIAPAN MATERI

Praktikan diharapkan mempelajari Group Exam Modules 1-3 : Basic Network Connectivity and Communications Exam yang terdiri dari beberapa chapter berikut :

1. Networking Today (Chapter 1)
2. Basic Switch and End Perangkat Configuration (Chapter 2)
3. Protocols and Models (Chapter 3)

TUJUAN PRAKTIKUM

1. Bagian 1: Capture and Analyze Local ICMP Data in Wireshark
2. Bagian 2: Capture and Analyze Remote ICMP Data in Wireshark

PERSIAPAN SOFTWARE/APLIKASI

- Komputer/Laptop
- Sistem operasi Windows/Linux/Max OS
- Packet Tracer v8.01 <https://www.packettracernetwork.com/download/download-packet-tracer.html>

MATERI TUGAS**Bagian 1: Capture and Analyze Local ICMP Data in Wireshark**

Pada Bagian ini, kita akan melakukan ping ke Perangkat lain dalam satu jaringan LAN dan menangkap serta membalas ICMP request dengan menggunakan Wireshark. Analisis ini akan membantu memperjelas bagaimana packet headers melakukan transport data ke destinationnya.

Sebagai catatan karena praktikum kali ini menggunakan setidaknya minimal 2 ip address, maka kalian bisa menggunakan metode dual Perangkat pc/laptop. Jika memang tidak bisa, alternatifnya adalah dengan menggunakan smartphone. Dan pastikan terhubung dalam satu jaringan local.

1. Mendapatkan Informasi Interface Address Dari PC.

Kita catat terlebih dahulu ip address dan network interface card (NIC) atau MAC pada Perangkat kita melalui command dari command prompt.

- Buka command prompt dari pc/laptop kalian dan masukkan command **ipconfig /all**
- Fokus pada jenis jaringan yang terhubung dengan Perangkat kalian. Sebagai contoh seperti berikut:

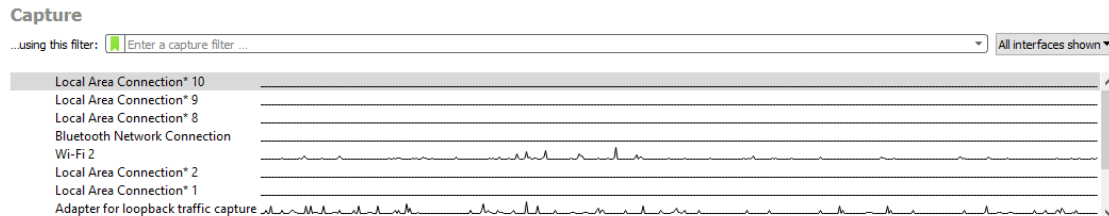
```
Wireless LAN adapter Wi-Fi 2:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Dual Band Wireless-AC 8265
Physical Address. . . . . : 8E-BB-4C-89-CC-CD
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4d17:5db9:a852:65b1%17(Preferred)
IPv4 Address. . . . . : 192.168.43.221(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Jumat, 24 September 2021 14.06.26
Lease Expires . . . . . : Jumat, 24 September 2021 15.36.26
Default Gateway . . . . . : 192.168.43.1
DHCP Server . . . . . : 192.168.43.1
DHCPv6 IAID . . . . . : 294566732
DHCPv6 Client DUID. . . . . : 00-03-00-01-8E-BB-4C-89-CC-CD
DNS Servers . . . . . : 192.168.43.1
NetBIOS over Tcpip. . . . . : Enabled
```

- Lakukan juga untuk Perangkat yang satunya dan catat nilai ip addressnya. Jika kalian menggunakan smartphone, silahkan cari ip address dari smartphone kalian di setting.

2. Menjalankan Wireshark dan Memulai Capture Data

- Buka wireshark, pada halaman awal akan muncul beberapa jaringan pada menu **Capture**. Kalian pilih jaringan yang kalian gunakan dengan cara double click. Pada dasarnya jaringan yang memiliki traffic akan terlihat ada grafik seperti berikut. Disini saya menggunakan Wi-Fi 2.



- Setelah double click jaringan yang dipilih, akan muncul semua proses yang terjadi dalam jaringan local tersebut pada wireshark dengan sangat cepat. Kita juga bisa memfilter berdasarkan protokolnya. Pada praktikum kali ini kita hanya memfilter protocol **ICMP** saja.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	31.13.95.60	192.168.43.221	TLSv1.2	726	Application Data
2	0.042423	192.168.43.221	31.13.95.60	TCP	54	62784 → 443 [ACK] Seq=1 Ack=673 Win=258 Len=0
3	0.361146	193.29.63.133	192.168.43.221	TCP	54	1688 → 50799 [FIN, ACK] Seq=1 Ack=1 Win=27872 Len=0
4	0.361378	192.168.43.221	193.29.63.133	TCP	54	50799 → 1688 [ACK] Seq=1 Ack=2 Win=63776 Len=0
5	0.361541	192.168.43.221	193.29.63.133	TCP	54	50799 → 1688 [FIN, ACK] Seq=1 Ack=2 Win=63776 Len=0
6	0.650954	193.29.63.133	192.168.43.221	TCP	54	1688 → 50799 [RST] Seq=2 Win=0 Len=0
7	1.954888	192.168.43.221	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
8	1.995931	23.108.101.68	192.168.43.221	TCP	54	80 → 58692 [ACK] Seq=1 Ack=1 Win=501 Len=0
9	1.996005	192.168.43.221	23.108.101.68	TCP	54	[TCP ACKED unseen segment] 58692 → 80 [ACK] Seq=1 Ack=2 Win=257 Len=0
10	2.167295	192.168.43.221	91.108.56.149	SSL	351	Continuation Data
11	2.315654	91.108.56.149	192.168.43.221	TCP	54	443 → 49300 [ACK] Seq=1 Ack=298 Win=29619 Len=0

- Pada field filter diatas, masukkan **ICMP** dan tekan ENTER pada keyboard
- Pada list event seharusnya kosong karena kita belum melakukan kegiatan yang melibatkan protocol ICMP

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

- Untuk berikutnya buka lagi command prompt untuk melakukan ping namun dengan ip address dari Perangkat yang berbeda.

```
C:\Users\WINDOWS 10>ping 10.223.218.117

Pinging 10.223.218.117 with 32 bytes of data:
Reply from 10.223.218.117: bytes=32 time=1ms TTL=64
Reply from 10.223.218.117: bytes=32 time=4ms TTL=64
Reply from 10.223.218.117: bytes=32 time=5ms TTL=64
Reply from 10.223.218.117: bytes=32 time=2ms TTL=64

Ping statistics for 10.223.218.117:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 3ms
```

- Seperti pada gambar diatas, ip address dari Perangkat kedua saya adalah 10.223.218.117. Pastikan menulis ip address dengan benar. Apabila terjadi kendala error alternatifnya adalah matikan firewall pada pc/laptop kalian.
- Setelah melakukan ping dari Perangkat yang berbeda. Coba cek kembali ke wireshark, maka akan muncul beberapa event baru dari protocol ICMP

No.	Time	Source	Destination	Protocol	Length	Info
4028	203.749730	192.168.43.221	10.223.218.117	ICMP	74	Echo (ping) request id=0x0001, seq=108/27648, ttl=128 (reply in 4029)
4029	203.751447	10.223.218.117	192.168.43.221	ICMP	74	Echo (ping) reply id=0x0001, seq=108/27648, ttl=64 (request in 4028)
4032	204.767794	192.168.43.221	10.223.218.117	ICMP	74	Echo (ping) request id=0x0001, seq=109/27904, ttl=128 (reply in 4033)
4033	204.771899	10.223.218.117	192.168.43.221	ICMP	74	Echo (ping) reply id=0x0001, seq=109/27904, ttl=64 (request in 4032)
4034	205.796117	192.168.43.221	10.223.218.117	ICMP	74	Echo (ping) request id=0x0001, seq=110/28160, ttl=128 (reply in 4035)
4035	205.801122	10.223.218.117	192.168.43.221	ICMP	74	Echo (ping) reply id=0x0001, seq=110/28160, ttl=64 (request in 4034)
4038	206.810160	192.168.43.221	10.223.218.117	ICMP	74	Echo (ping) request id=0x0001, seq=111/28416, ttl=128 (reply in 4039)
4039	206.812840	10.223.218.117	192.168.43.221	ICMP	74	Echo (ping) reply id=0x0001, seq=111/28416, ttl=64 (request in 4038)

- Klik stop capture apabila sudah berhasil.

3. Menganalisis data yang telah di-capture

- Perhatikan bahwa kolom source adalah ip address kalian sedangkan pada kolom destination adalah ip tujuan yang didapat dari ip address Perangkat kedua.
- Klik salah satu ICMP Request PDU yang ada pada di section atas wireshark.
- Akan muncul tab baru, double klik Ethernet II untuk melihat destination dan source MAC

Catatan: dari contoh sebelumnya dari permintaan ICMP yang telah ditangkap, data ICMP dienkapsulasi di dalam IPv4 packet PDU (header IPv4) yang kemudian dienkapsulasi dalam tab PDU Ethernet II (header Ethernet II) untuk ditransmisikan ke LAN.

Bagian 2: Melakukan Capture dan Analisis Pada Remote ICMP Data di dalam Wireshark

Pada Bagian ini kita akan melakukan ping ke host jarak jauh dan memeriksa data yang dihasilkan dari ping tersebut. Kita kemudian akan menentukan data apa yang berbeda dari data pada Bagian 1.

1. Memulai capture data pada interface

- Tekan CTRL + W pada wireshark untuk menutup data sebelumnya.
- Lakukan capture data lagi, pada halaman awal akan muncul beberapa jaringan pada menu **Capture**. Kalian pilih jaringan yang kalian gunakan dengan cara double click
- Kita lakukan ping ketiga URL situs web berikut ke command prompt
 - www.yahoo.com
 - www.cisco.com
 - www.google.com

```
C:\Users\WINDOWS 10>ping www.yahoo.com

Pinging new-fp-shed.wg1.b.yahoo.com [202.165.107.48] with 32 bytes of data:
Reply from 202.165.107.48: bytes=32 time=55ms TTL=52
Reply from 202.165.107.48: bytes=32 time=68ms TTL=52
Reply from 202.165.107.48: bytes=32 time=61ms TTL=52
Reply from 202.165.107.48: bytes=32 time=68ms TTL=52

Ping statistics for 202.165.107.48:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 55ms, Maximum = 68ms, Average = 63ms
```

```

C:\Users\WINDOWS 10>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [23.15.104.32] with 32 bytes of data:
Reply from 23.15.104.32: bytes=32 time=50ms TTL=54
Reply from 23.15.104.32: bytes=32 time=81ms TTL=54
Reply from 23.15.104.32: bytes=32 time=47ms TTL=54
Reply from 23.15.104.32: bytes=32 time=63ms TTL=54

Ping statistics for 23.15.104.32:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 47ms, Maximum = 81ms, Average = 60ms

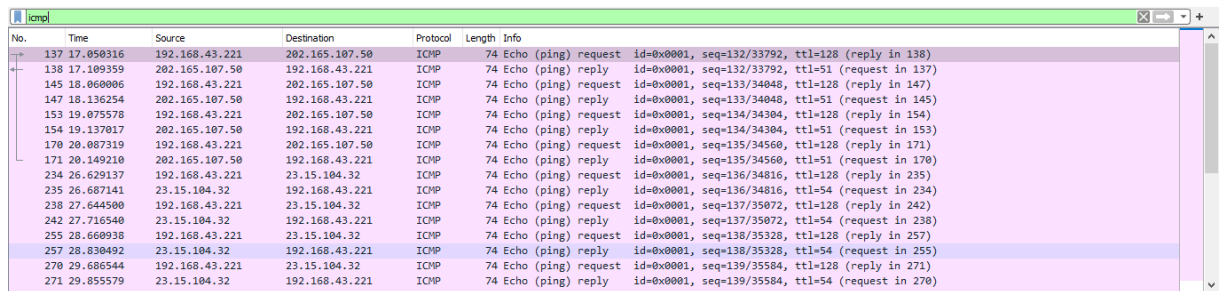
C:\Users\WINDOWS 10>ping www.google.com

Pinging forcesafesearch.google.com [216.239.38.120] with 32 bytes of data:
Reply from 216.239.38.120: bytes=32 time=220ms TTL=115
Reply from 216.239.38.120: bytes=32 time=63ms TTL=115
Reply from 216.239.38.120: bytes=32 time=77ms TTL=115
Reply from 216.239.38.120: bytes=32 time=63ms TTL=115

Ping statistics for 216.239.38.120:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 63ms, Maximum = 220ms, Average = 105ms

```

- d. Saat kalian melakukan ping ke URL tersebut, lihat pada wireshark untuk melihat proses capturing.



No.	Time	Source	Destination	Protocol	Length	Info
137	17.050316	192.168.43.221	202.165.107.50	ICMP	74	Echo (ping) request id=0x0001, seq=132/33792, ttl=128 (reply in 138)
138	17.109359	202.165.107.50	192.168.43.221	ICMP	74	Echo (ping) reply id=0x0001, seq=132/33792, ttl=51 (request in 137)
145	18.060006	192.168.43.221	202.165.107.50	ICMP	74	Echo (ping) request id=0x0001, seq=133/34048, ttl=128 (reply in 147)
147	18.136254	202.165.107.50	192.168.43.221	ICMP	74	Echo (ping) reply id=0x0001, seq=133/34048, ttl=51 (request in 145)
153	19.075578	192.168.43.221	202.165.107.50	ICMP	74	Echo (ping) request id=0x0001, seq=134/34304, ttl=128 (reply in 154)
154	19.137017	202.165.107.50	192.168.43.221	ICMP	74	Echo (ping) reply id=0x0001, seq=134/34304, ttl=51 (request in 153)
170	20.087319	192.168.43.221	202.165.107.50	ICMP	74	Echo (ping) request id=0x0001, seq=135/34560, ttl=128 (reply in 171)
171	20.149210	202.165.107.50	192.168.43.221	ICMP	74	Echo (ping) reply id=0x0001, seq=135/34560, ttl=51 (request in 170)
234	26.629137	192.168.43.221	23.15.104.32	ICMP	74	Echo (ping) request id=0x0001, seq=136/34816, ttl=128 (reply in 235)
235	26.687141	23.15.104.32	192.168.43.221	ICMP	74	Echo (ping) reply id=0x0001, seq=136/34816, ttl=54 (request in 234)
238	27.644500	192.168.43.221	23.15.104.32	ICMP	74	Echo (ping) request id=0x0001, seq=137/35072, ttl=128 (reply in 242)
242	27.716540	23.15.104.32	192.168.43.221	ICMP	74	Echo (ping) reply id=0x0001, seq=137/35072, ttl=54 (request in 238)
255	28.660938	192.168.43.221	23.15.104.32	ICMP	74	Echo (ping) request id=0x0001, seq=138/35328, ttl=128 (reply in 257)
257	28.830492	23.15.104.32	192.168.43.221	ICMP	74	Echo (ping) reply id=0x0001, seq=138/35328, ttl=54 (request in 255)
270	29.686544	192.168.43.221	23.15.104.32	ICMP	74	Echo (ping) request id=0x0001, seq=139/35584, ttl=128 (reply in 271)
271	29.855579	23.15.104.32	192.168.43.221	ICMP	74	Echo (ping) reply id=0x0001, seq=139/35584, ttl=54 (request in 270)

Catatan: saat kalian melakukan ping ke URL diatas, perhatikan bahwa Domain Name Server (DNS) menerjemahkan URL ke ip address. Perhatikan ip address yang diterima untuk setiap URL. Kalian dapat stop capturing data dengan mengklik ikon Stop Capture.

PERTANYAAN TUGAS

1. Lakukan analisa data dari remote host. Lalu tentukan ip address dan MAC dari ketiga URL diatas.
2. Bagaimana informasinya bisa berbeda dari informasi ping lokal yang kalian terima di Bagian 1. Jelaskan?
3. Mengapa Wireshark menunjukkan alamat MAC sebenarnya dari local host, namun bukan alamat MAC sebenarnya untuk remote host?
4. Simpan hasil kerja wireshark kalian untuk yang local host dan remote host dalam 1 folder

CATATAN TUGAS

Tugas :

Batas maksimal dikerjakan H-1 praktikum dan dikumpulkan di i-Lab dengan format [Nama_Nim_Modul1] .rar

Batas maksimal pengerjaan netacad adalah 1 minggu setelah jadwal praktikum

KRITERIA PENILAIAN TUGAS

>81 : Praktikan mampu mengerjakan serta menjelaskan tugas yang ada di materi tugas dengan benar

70 – 40 : Praktikan mampu mengerjakan serta menjelaskan tugas yang ada di materi tugas namun kurang maksimal.

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

TUGAS	20%
PRAKTEK	80%