

Laporan Tugas Komunikasi Data

Nama: Dino Alfian Zamri

Nim: 202310370311329

Mata Kuliah: Komunikasi Data

Tugas yang dilakukan yaitu mengerjakan Praktikum Komunikasi Data.

Bagian 1: Capture and Analyze Local ICMP Data in Wireshark

1. Mendapatkan Informasi Alamat Jaringan dari PC:

- Memasukkan perintah ipconfig/all
- Mencatat alamat IP serta MAC Address yang tertera di 2 perangkat (Laptop & Smartphone)

```
Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : umm.ac.id
    Description . . . . . : Realtek RTL8822CE 802.11ac PCIe A
dapter
    Physical Address. . . . . : 34-6F-24-71-CB-A5
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::4c30:a6a8:8ac2:3fc6%19(Pref
erred)
    IPv4 Address. . . . . : 172.16.58.218(Preferred)
    Subnet Mask . . . . . : 255.255.252.0
    Lease Obtained. . . . . : 29 September 2024 00:06:03
    Lease Expires . . . . . : 29 September 2024 00:16:03
    Default Gateway . . . . . : 172.16.56.1
    DHCP Server . . . . . : 10.18.21.10
    DHCPv6 IAID . . . . . : 338980644
    DHCPv6 Client DUID. . . . . : 00-01-00-01-29-1C-8E-C5-C8-5A-CF-
75-28-F6
    DNS Servers . . . . . : 8.8.8.0
                           8.8.4.4
    NetBIOS over Tcpip. . . . . : Enabled
```

2. Menjalankan Wireshark dan Memulai Capture Data:

- Buka Wireshark.
- Pilih jaringan yang digunakan dengan cara double-click. Menggunakan Wifi.
- Memfilter protokol ICMP.

- Buka kembali Command Prompt untuk melakukan ping dengan menggunakan IP Address dari perangkat Smartphone.

```
C:\Users\HP>ping 172.16.58.214

Pinging 172.16.58.214 with 32 bytes of data:
Reply from 172.16.58.214: bytes=32 time=994ms TTL=64
Reply from 172.16.58.214: bytes=32 time=12ms TTL=64
Reply from 172.16.58.214: bytes=32 time=77ms TTL=64
Reply from 172.16.58.214: bytes=32 time=70ms TTL=64

Ping statistics for 172.16.58.214:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 994ms, Average = 288ms
```

- Setelah melakukan ping dari perangkat lain, periksa kembali Wireshark. Klik Stop Capture jika sudah berhasil

No.	Time	Source	Destination	Protocol	Length	Info
194	186.893576	172.16.58.218	172.16.58.214	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 195)
195	186.898080	172.16.58.214	172.16.58.218	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 194)
196	186.924888	172.16.58.218	172.16.58.214	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 197)
197	186.937320	172.16.58.214	172.16.58.218	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 196)
198	187.940293	172.16.58.218	172.16.58.214	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 199)
199	188.017685	172.16.58.214	172.16.58.218	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 198)
200	188.962737	172.16.58.218	172.16.58.214	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 201)
201	189.032860	172.16.58.214	172.16.58.218	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 200)

> Frame 194: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{...}	0000	ca 6b 07 75 15 d0	34 f6	24 71 cb a5 08 00 45 00	40 50 40 \$g...
> Ethernet II, Src: AzureWaveTec_71:cb:a5 (34:6f:24:71:cb:a5), Dst: ca:6b:07:75:15:d0 (ca:6b:07:75:15:d0)	0010	00 3c c9 f6 00 00 00 01	a2 f9 ac 10 3a da ac 10		...
> Internet Protocol Version 4, Src: 172.16.58.218, Dst: 172.16.58.214	0020	3a d6 08 00 4d 5a 00 01	00 01 61 62 63 64 65 66		...MZ... abcdef
> Internet Control Message Protocol	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		wabcedfg hi

3. Menganalisis Data yang Telah Di-capture:

Memperhatikan bahwa kolom Source menunjukkan IP Address pengirim, sedangkan kolom Destination menunjukkan IP tujuan yang didapat dari IP Address perangkat kedua. Mengklik salah satu ICMP Request PDU yang ada di bagian atas Wireshark. Dan akan muncul tab baru, double-click pada Ethernet II untuk melihat destination dan source MAC Address.

> Frame 194: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{FD65F81D-1C4F-49BA-8883-D6595706B8CC}, id 0
✓ Ethernet II, Src: AzureWaveTec_71:cb:a5 (34:6f:24:71:cb:a5), Dst: ca:6b:07:75:15:d0 (ca:6b:07:75:15:d0)
> Destination: ca:6b:07:75:15:d0 (ca:6b:07:75:15:d0)
> Source: AzureWaveTec_71:cb:a5 (34:6f:24:71:cb:a5)
Type: IPv4 (0x0800)
[Stream index: 24]
> Internet Protocol Version 4, Src: 172.16.58.218, Dst: 172.16.58.214
> Internet Control Message Protocol

Bagian 2: Capture and Analyze Remote ICMP Data in Wireshark

Di bagian ini, Saya akan melakukan ping ke host jarak jauh dan memeriksa data yang dihasilkan dari ping tersebut. Saya kemudian akan menentukan perbedaan data ini dibandingkan dengan data dari Bagian 1.

1. Menganalisis Data yang Telah Di-capture: Tekan CTRL + W pada Wireshark untuk menutup data capture sebelumnya. Lakukan capture data lagi. Pada halaman awal, pilih jaringan yang digunakan dengan cara double-click. Melakukan ping ke tiga URL situs web berikut melalui Command Prompt:

- Ping www.tokopedia.com

```
C:\Users\HP>ping www.tokopedia.com

Pinging a1136.w7.akamai.net [114.10.52.219] with 32 bytes of data:
Reply from 114.10.52.219: bytes=32 time=18ms TTL=59
Reply from 114.10.52.219: bytes=32 time=16ms TTL=59
Reply from 114.10.52.219: bytes=32 time=16ms TTL=59
Reply from 114.10.52.219: bytes=32 time=17ms TTL=59

Ping statistics for 114.10.52.219:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 16ms
```

- Ping www.cisco.com

```
C:\Users\HP>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [23.3.76.99] with 32 bytes of data:
Reply from 23.3.76.99: bytes=32 time=18ms TTL=59
Reply from 23.3.76.99: bytes=32 time=17ms TTL=59
Reply from 23.3.76.99: bytes=32 time=18ms TTL=59
Reply from 23.3.76.99: bytes=32 time=17ms TTL=59

Ping statistics for 23.3.76.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 18ms, Average = 17ms
```

- Ping www.instagram.com

```
C:\Users\HP>ping www.instagram.com

Pinging z-p42-instagram.c10r.instagram.com [157.240.235.174] with 32 bytes of data:
Reply from 157.240.235.174: bytes=32 time=26ms TTL=53
Reply from 157.240.235.174: bytes=32 time=26ms TTL=53
Reply from 157.240.235.174: bytes=32 time=26ms TTL=53
Reply from 157.240.235.174: bytes=32 time=26ms TTL=53

Ping statistics for 157.240.235.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 26ms, Average = 26ms
```

- Saat melakukan ping ke URL tersebut, saya memperhatikan Wireshark untuk melihat proses capturing.

No.	Time	Source	Destination	Protocol	Length	Info
47	21.619325	172.16.58.218	114.10.52.193	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=128 (reply in 48)
48	21.638670	114.10.52.193	172.16.58.218	ICMP	74	Echo (ping) reply id=0x0001, seq=17/4352, ttl=59 (request in 47)
49	22.638323	172.16.58.218	114.10.52.193	ICMP	74	Echo (ping) request id=0x0001, seq=18/4608, ttl=128 (reply in 50)
50	22.658380	114.10.52.193	172.16.58.218	ICMP	74	Echo (ping) reply id=0x0001, seq=18/4608, ttl=59 (request in 49)
60	23.643040	172.16.58.218	114.10.52.193	ICMP	74	Echo (ping) request id=0x0001, seq=19/4864, ttl=128 (reply in 62)
62	23.664519	114.10.52.193	172.16.58.218	ICMP	74	Echo (ping) reply id=0x0001, seq=19/4864, ttl=59 (request in 60)
87	24.656258	172.16.58.218	114.10.52.193	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=128 (reply in 88)
88	24.675263	114.10.52.193	172.16.58.218	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=59 (request in 87)
144	34.477664	172.16.58.218	23.3.76.99	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 145)
145	34.495076	23.3.76.99	172.16.58.218	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=59 (request in 144)
146	35.492302	172.16.58.218	23.3.76.99	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 147)
147	35.509454	23.3.76.99	172.16.58.218	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=59 (request in 146)
148	36.509619	172.16.58.218	23.3.76.99	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 149)
149	36.527036	23.3.76.99	172.16.58.218	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=59 (request in 148)
150	37.525742	172.16.58.218	23.3.76.99	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 151)
151	37.543490	23.3.76.99	172.16.58.218	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=59 (request in 150)

> Frame 47: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F065F81D-1C4F-49BA-8883-D659570688CC}, id 0		0000	38 45 3b 3a f9 96 34 6f 24 71 cb
> Ethernet II, Src: AzureWaveTec_71:cb:a5 (34:6f:24:71:cb:a5), Dst: RuckusWirele_3a:f9:96 (38:45:3b:3a:f9:96)		0010	00 3c 43 1a 00 00 00 01 69 f1 ac
> Destination: RuckusWirele_3a:f9:96 (38:45:3b:3a:f9:96)		0020	34 c1 08 00 4d 4a 00 01 00 11 61
> Source: AzureWaveTec_71:cb:a5 (34:6f:24:71:cb:a5)		0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71
> Type: IPv4 (0x0800)		0040	77 61 62 63 64 65 66 67 68 69
[Stream index: 0]			
> Internet Protocol Version 4, Src: 172.16.58.218, Dst: 114.10.52.193			
> Internet Control Message Protocol			

Pertanyaan Tugas

Berdasarkan informasi yang diperiksa selama penangkapan Packet Tracer tentukan:

- a. Apakah MAC Address dari perangkat Anda berubah ketika Anda terhubung ke jaringan yang berbeda? Berikan penjelasan rinci dan contoh tentang bagaimana MAC Address berperilaku di jaringan yang berbeda

Jawaban : Perubahan MAC Address bisa terjadi karena fitur MAC Address Randomization, yang ada pada banyak perangkat modern (terutama smartphone) untuk meningkatkan privasi. Fitur ini membuat perangkat menggunakan MAC Address yang berbeda setiap kali terhubung ke jaringan baru, sehingga lebih sulit untuk dilacak.

Contoh situasi: Jika saya terhubung ke Wi-Fi di kos-an, MAC Address bisa menjadi 0e:e8:90:de:a3:10. Saat saya berpindah ke jaringan Wi-Fi di kampus, MAC Address bisa berubah menjadi ca:6b:07:75:15::d0.

- b. Mengapa MAC Address penting dalam jaringan komputer? Diskusikan bagaimana MAC Address digunakan dalam proses pengiriman data dan identifikasi perangkat.

Jawaban :

- MAC Address (Media Access Control Address) adalah identifikasi unik yang ditetapkan pada setiap Network Interface Card (NIC) yang ada di perangkat seperti laptop, PC, smartphone, maupun router. MAC Address digunakan dalam jaringan untuk memastikan pengiriman data yang benar dari sumber ke tujuan.
- Ketika sebuah perangkat mengirimkan paket data ke perangkat lain dalam jaringan, proses yang terjadi adalah Perangkat pengirim menyiapkan data yang akan dikirim, kemudian menambahkan header MAC Address pada Lapisan Data Link.
Header ini mencakup:
Source MAC Address: MAC Address dari perangkat pengirim.
Destination MAC Address: MAC Address dari perangkat penerima.

Perangkat penerima memeriksa Destination MAC Address untuk melihat apakah paket tersebut ditujukan untuknya. Jika Destination MAC Address cocok, perangkat tersebut menerima data dan memprosesnya. Jika tidak cocok, perangkat akan mengabaikan paket data tersebut.

- c. Setelah melakukan ping ke ketiga URL, gunakan Wireshark untuk mengidentifikasi IP Address dari setiap host tersebut. Bagaimana proses pengambilan data ini berbeda dari pengambilan data lokal yang dilakukan sebelumnya?

Jawaban :

Hasil IP Address dari Masing-Masing Host:

- www.tokopedia.com : 210.210.145.145
- www.cisco.com : 23.54.48.102
- www.instagram.com : 57.144.100.34

Memeriksa IP Address di Wireshark:

Saat paket ping dikirim dan diterima, di kolom Destination pada Wireshark. Akan terlihat Source IP Address dari perangkat saya dan Destination IP Address yang merupakan IP dari host tujuan.

Mengklik pada salah satu paket ICMP dan memeriksa detailnya di bagian Internet Protocol Version 4. Di sini akan terlihat:

www.tokopedia.com

Source IP Address : 192.168.1.16

Destination Address : 210.210.145.145

www.cisco.com

Source IP Address : 23.54.48.102

Destination Address : 192.168.1.16

www.instagram.com

Source IP Address : 57.144.100.34

Destination Address : 192.168.1.16

Perbedaan Proses Pengambilan Data:

Pada ping lokal (ke perangkat di jaringan yang sama), proses lebih cepat dan sederhana karena perangkat berada di satu jaringan LAN.

Pada ping remote (ke URL eksternal), paket harus melewati beberapa router dan jaringan publik, sehingga waktu dan jalur pengiriman lebih kompleks.

- d. Jelaskan bagaimana Anda dapat memastikan bahwa PC/Laptop Anda dapat terhubung ke ketiga URL tersebut. Langkah apa yang diambil untuk mengatasi masalah koneksi yang mungkin terjadi?

Jawaban :

1. Memeriksa koneksi internet (Memastikan perangkat terhubung ke internet dengan cara mencoba akses situs seperti www.google.com)
 2. Mengecek IP Address dan DNS (Menggunakan ipconfig di CMD untuk melihat IP Address. Jika IP invalid, maka perbaiki koneksi atau atur ulang DNS).
 3. Melakukan Ping URL (Ketik ping www.tokopedia.com di CMD. Jika mendapat Reply maka koneksi berhasil). Jika ping gagal, maka coba nonaktifkan firewall atau antivirus dulu yang kemungkinan memblokir koneksi.)
- e. Apa perbedaan utama yang Anda temukan antara hasil ping lokal dan ping remote? Gunakan pemahaman Anda tentang jaringan untuk menjelaskan mengapa perbedaan ini terjadi.

Jawaban :

1. Ping Lokal:

- Defini: Hanya dalam jaringan yang sama (LAN)
- Kecepatan: Lebih cepat, karena perangkat berada dalam satu jaringan yang sama dan tidak perlu melewati router eksternal.
- Jumlah Hop: Hanya melalui satu hop (switch atau router lokal).
- Waktu Respon: Rendah, rata-rata nya di bawah 1 ms hingga 5 ms.
- Contoh: Ping ke IP Address (192.168.1.16)

2. Ping Remote:

- Definisi: Mengirimkan *ping* ke perangkat atau server yang ada di luar jaringan lokal, seperti situs web.
- Kecepatan: Lebih lambat, karena data harus melewati beberapa router dan jaringan publik (Internet).
- Jumlah Hop: Bisa melalui banyak hop (beberapa router di Internet).
- Waktu Respon: Lebih tinggi, bisa berkisar antara 20 ms hingga 200 ms, tergantung jarak geografis.
- Contoh: Ping ke www.tokopedia.com yang menghasilkan respon dari IP server tujuan.

