

Sieci komputerowe I – laboratorium

Wiktor Opieliński 157198 Stanowisko: K2

Informatyka, Niestacjonarnie semestr 4, Grupa 1

Warstwa międzysieciowa

Zadanie 1

1. Zaloguj ruch przy pomocy programu wireshark. Jakie

zazwyczaj są ustawione flagi w pakietach?

2376	160.732556	192.168.0.21	142.250.180.69	TCP	1466	62611 → 443 [ACK] Seq=3890 Ack=1 Win=131072 Len=1412 [TCP PDU reassembled in 2377]
2377	160.732556	192.168.0.21	142.250.180.69	TLSv1.3	1263	Application Data
2379	160.735469	162.159.130.234	192.168.0.21	TLSv1.2	138	Application Data
2380	160.759302	142.250.180.69	192.168.0.21	TCP	60	443 → 62611 [ACK] Seq=1 Ack=1413 Win=268288 Len=0
2381	160.759856	142.250.180.69	192.168.0.21	TCP	60	[TCP Dup ACK 2380#1] 443 → 62611 [ACK] Seq=1 Ack=1413 Win=268288 Len=0
2382	160.759856	142.250.180.69	192.168.0.21	TCP	60	443 → 62611 [ACK] Seq=1 Ack=2472 Win=267264 Len=0
2383	160.765960	142.250.180.69	192.168.0.21	TCP	60	443 → 62611 [ACK] Seq=1 Ack=2478 Win=267264 Len=0
2384	160.766535	142.250.180.69	192.168.0.21	TCP	60	443 → 62611 [ACK] Seq=1 Ack=3890 Win=265984 Len=0
2385	160.766535	142.250.180.69	192.168.0.21	TCP	60	443 → 62611 [ACK] Seq=1 Ack=5302 Win=264704 Len=0
2386	160.766535	142.250.180.69	192.168.0.21	TCP	60	443 → 62611 [ACK] Seq=1 Ack=6511 Win=263680 Len=0
2387	160.769477	142.250.180.69	192.168.0.21	TLSv1.3	1466	Server Hello, Change Cipher Spec, Application Data
2388	160.770053	192.168.0.21	142.250.180.69	TLSv1.3	138	Application Data, Application Data

> Frame 2380: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{5298A11C-0424-4C8D-8FA1-0034ECAB932}	0000	90 e8 68 42 a2 31 60 3d 26
> Ethernet II, Src: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6), Dst: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31)	0010	00 28 5b 95 00 00 75 06 e6
> Internet Protocol Version 4, Src: 142.250.180.69, Dst: 192.168.0.21	0020	00 15 01 bb f4 93 9e 9b 51
> 0100 = Version: 4	0030	04 18 c4 ea 00 00 00 00
> ... 0101 = Header Length: 20 bytes (5)		
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)		
> Total Length: 40		
> Identification: 0x5b95 (23445)		
> 000. Flags: 0x0		
> ...0 0000 0000 0000 = Fragment Offset: 0		
> Time to Live: 117		
> Protocol: TCP (6)		
> Header Checksum: 0xe63d [validation disabled]		
> [Header checksum status: Unverified]		
> Source Address: 142.250.180.69		
> Destination Address: 192.168.0.21		
> [Stream index: 18]		
> Transmission Control Protocol, Src Port: 443, Dst Port: 62611, Seq: 1, Ack: 1413, Len: 0		

Po przeanalizowaniu pakietów, zazwyczaj flagi są ustawione na 0x0.

- Bit zarezerwowany nie jest ustawiony.
- Pakiet może być fragmentowany, jeśli zajdzie taka potrzeba
- Pakiet nie jest częścią większego pakietu, czyli nie został zfragmentowany
- Fragment Offset: 0 – wskazuje, że jest to pierwszy (i jedyny) fragment pakietu.

Jest to typowe zachowanie dla niewielkich pakietów, które mieszczą się w jednej ramce sieciowej.

2. Powtórzyć ćwiczenie otwierając w międzyczasie jakąś stronę internetową przy użyciu protokołu https.

7562	39.557294	192.168.0.21	199.232.81.140	TLSv1.3	1113	Application Data
7563	39.633018	142.250.147.84	192.168.0.21	TCP	66 443 → 62702	[SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
7564	39.633073	192.168.0.21	142.250.147.84	TCP	54 62702 → 443	[ACK] Seq=1 Ack=1 Win=131072 Len=0
7565	39.633983	192.168.0.21	142.250.147.84	TCP	1466 62702 → 443	[ACK] Seq=1 Ack=1 Win=131072 Len=1412 [TCP PDU reassembled in 7566]
7566	39.633983	192.168.0.21	142.250.147.84	TLSv1.3	1117	Client Hello (SNI=accounts.google.com)
7567	39.634102	192.168.0.21	142.250.147.84	TLSv1.3	60	Change Cipher Spec
7568	39.634118	192.168.0.21	142.250.147.84	TLSv1.3	146	Application Data
7569	39.652796	199.232.81.140	192.168.0.21	TCP	66 443 → 62701	[SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
7570	39.652841	192.168.0.21	199.232.81.140	TCP	54 62701 → 443	[ACK] Seq=1 Ack=1 Win=131328 Len=0
7571	39.653290	192.168.0.21	199.232.81.140	TCP	1514 62701 → 443	[ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP PDU reassembled in 7572]
7572	39.653290	192.168.0.21	199.232.81.140	TLSv1.3	501	Client Hello (SNI=styles.redditmedia.com)
7573	39.657219	199.232.81.140	192.168.0.21	TCP	66 443 → 62699	[SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
7574	39.657219	199.232.81.140	192.168.0.21	TCP	66 443 → 62700	[SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
7575	39.657219	199.232.81.140	192.168.0.21	TCP	60 443 → 62679	[ACK] Seq=140920 Ack=28024 Win=215552 Len=0
7576	39.657219	199.232.81.140	192.168.0.21	TCP	60 443 → 62679	[ACK] Seq=140920 Ack=28469 Win=217088 Len=0

> Frame 7566: 1117 bytes on wire (8936 bits), 1117 bytes captured (8936 bits) on interface \Device\NPF_{5298A11C-0424-4C8D-8FA1-0034E8C00000} (0.0.0.0) on 0.0.0.0
> Ethernet II, Src: AzureIaveTec_42:a2:31 (90:e8:68:42:a2:31), Dst: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)
▼ Internet Protocol Version 4, Src: 192.168.0.21, Dst: 142.250.147.84
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 1103
 Identification: 0x52f1 (21233)
 > 010. = Flags: 0x2, Don't fragment
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 128
 Protocol: TCP (6)
 Header Checksum: 0xc0ab [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.0.21
 Destination Address: 142.250.147.84
 [Stream index: 26]
 > Transmission Control Protocol, Src Port: 62702, Dst Port: 443, Seq: 1413, Ack: 1, Len: 1063
 > [2 Reassembled TCP Segments (2475 bytes): #7565(1412), #7566(1063)]
 > Transport Layer Security

0000 60 3d 26 8e 3d b6 90 e8 68 42 a2 31 08 00 45
0010 04 4f 52 f1 40 00 80 06 c0 ab c0 a0 00 15 8e
0020 93 54 f4 ee 01 bb 98 c1 cb dc 97 fc 89 63 50
0030 02 00 a9 16 00 00 fd 3b 12 83 69 ba 5f 86 33
0040 c5 1d 32 e2 cb 53 30 c9 5f 2d 1b 84 f3 d7 86
0050 39 b2 6a f7 2c a2 2e 20 ba b9 08 16 00 1d 00
0060 5f 86 33 66 c5 1d 32 e2 cb 53 30 c9 5f 2d 1b
0070 f3 d7 86 9a 39 b2 6a f7 2c a2 2e 20 ba b9 08
0080 00 17 00 41 04 f3 83 ca 49 03 eb e5 6a 48 1f
0090 47 1e 70 f6 1e ea c6 c2 af f6 66 d5 89 4f f8
00a0 be b3 60 94 ce 0d 7c ad 9d ea cf 2a b0 df 0e
00b0 58 ed 5c 02 a2 bf af 0f 3d 41 07 f4 a4 78 43
00c0 08 bc 26 83 1b 00 2a 00 00 00 2b 00 05 04 03
00d0 03 03 00 0d 00 18 00 16 04 03 05 03 06 03 08
00e0 08 05 08 06 04 01 05 01 06 01 02 03 02 01 00
00f0 00 02 01 01 00 1c 00 02 40 01 00 1b 00 07 06
0100 01 00 02 00 03 fe 0d 02 39 00 00 01 00 03 11
0110 20 e9 95 d0 f5 ac dd 99 51 0f 58 ad 66 f4 14
0120 18 63 ef 67 86 77 13 ef 07 a1 ea 4d 96 fe 15
0130 1b 02 0f ff 1d ef 1e 30 d7 c1 37 b0 da 0a c8
0140 df 71 38 56 19 de e5 08 26 b7 51 99 23 d3 49
0150 8c c6 5b 8a 69 ca 6d e0 05 d4 25 85 29 8c 34
0160 77 b8 88 27 5d 5c 9c bb e6 7c 15 a2 4f a2 42
0170 51 6c 6f 07 90 76 57 7c e0 f3 8e 53 19 9e 39
0180 09 ce eb 71 1e 19 bd 0e 25 12 ab e7 16 1a eb
0190 2d a6 f9 4a 14 ed ce 60 d8 df 66 46 23 57 60
01a0 ef 43 aa 8b 4a 90 13 2a da 06 e2 f1 8d e9 2f
01b0 d3 ef 10 78 8c 81 e8 17 ce 50 f2 2e 5d 31 6c

Frame (1117 bytes) | Reassembled TCP (2475 bytes)

Flaga ustawiona jest na 0x2, oznacza to, że tym razem w porównaniu z poprzednim ćwiczeniem pakiet nie może być fragmentowany. Jest to standardowe zachowanie dla współczesnych sieci, gdzie fragmentacja jest niepożądana z powodu bezpieczeństwa i wydajności.

Zamiast fragmentacji protokół TCP z ustawioną flagą 0x2 wykorzystuje Path MTU Discovery, czyli:

- Ustawia DF = 1 i wysyła coraz większe pakiety.
- Gdy pakiet jest za duży, router odrzuca go i odsyła błąd ICMP „Fragmentation needed”.

Dzięki temu nadawca dowiaduje się maksymalnego MTU na trasie i dopasowuje rozmiar.

HTTPS korzysta z tego mechanizmu, aby dobrać optymalny rozmiar segmentów bez fragmentacji.

3.Powtórz ćwiczenie w międzyczasie wykonując polecenie

ping -s 4000 na wybrany adres IP.

W celu przeanalizowania fragmentacji pakietów IP wykonano polecenie:

ping -s 4000 8.8.8.8

Polecenie to generuje pakiet ICMP o długości 4000 bajtów, który przekracza domyślną wartość MTU (1500 bajtów) dla sieci Ethernet. W efekcie system dzieli pakiet IP na mniejsze fragmenty, które są widoczne w przechwyty Wiresharka.

Fragment 1

No.	Time	Source	Destination	Protocol	Length	Info
963	100.473790	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2276) [Reassembled in #965]
964	100.473790	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2276) [Reassembled in #965]
965	100.473790	192.168.0.21	8.8.8.8	ICMP	1082	Echo (ping) request id=0x0001, seq=144/36864, ttl=128 (no response found!)
969	105.426164	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2277) [Reassembled in #971]
970	105.426164	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2277) [Reassembled in #971]
971	105.426164	192.168.0.21	8.8.8.8	ICMP	1082	Echo (ping) request id=0x0001, seq=145/37120, ttl=128 (no response found!)
991	110.422269	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2278) [Reassembled in #993]
992	110.422269	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2278) [Reassembled in #993]
993	110.422269	192.168.0.21	8.8.8.8	ICMP	1082	Echo (ping) request id=0x0001, seq=146/37376, ttl=128 (no response found!)
1032	115.428203	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2279) [Reassembled in #1034]
1033	115.428203	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2279) [Reassembled in #1034]
1034	115.428203	192.168.0.21	8.8.8.8	ICMP	1082	Echo (ping) request id=0x0001, seq=147/37632, ttl=128 (no response found!)
3623	289.865789	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2279a) [Reassembled in #3625]
> Frame 963: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{5298A11C-0424-4C8D-8FA1-003...}						
✓ Ethernet II, Src: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31), Dst: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)						
> Destination: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)						
> Source: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31)						
Type: IPv4 (0x0800)						
[Stream index: 0]						
✓ Internet Protocol Version 4, Src: 192.168.0.21, Dst: 8.8.8.8						
0100 = Version: 4						
... 0101 = Header Length: 20 bytes (5)						
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 1500						
Identification: 0x2276 (8822)						
> 001. = Flags: 0x1, More fragments						
...0 0000 0000 0000 = Fragment Offset: 0						
Time to Live: 128						
Protocol: ICMP (1)						
Header Checksum: 0x21de [validation disabled]						
[Header checksum status: Unverified]						
Source Address: 192.168.0.21						
Destination Address: 8.8.8.8						
[Reassembled IPv4 in frame: 965]						
[Stream index: 25]						
> Data (1480 bytes)						
						0000 60 3d 26 8e 3d b6
						0010 05 dc 22 76 20 00
						0020 08 08 08 00 f2 e6
						0030 67 68 69 6a 6b 6e
						0040 77 61 62 63 64 6e
						0050 70 71 72 73 74 77
						0060 69 6a 6b 6c 6d 6e
						0070 62 63 64 65 66 6e
						0080 72 73 74 75 76 77
						0090 6b 6c 6d 6e 6f 70
						00a0 64 65 66 67 68 6e
						00b0 74 75 76 77 78 79
						00c0 6d 6e 6f 70 71 72
						00d0 66 67 68 69 6a 6b
						00e0 76 77 78 79 7a 7b
						00f0 6f 70 71 72 73 74
						0100 68 69 6a 6b 6c 6d
						0110 61 62 63 64 65 66
						0120 71 72 73 74 75 76
						0130 6a 6b 6c 6d 6e 6f
						0140 63 64 65 66 67 68
						0150 73 74 75 76 77 78
						0160 6c 6d 6e 6f 70 71
						0170 65 66 67 68 69 6a
						0180 75 76 77 78 79 7a
						0190 6e 6f 70 71 72 73
						01a0 67 68 69 6a 6b 6c
						01b0 77 61 62 63 64 6e
						01c0 70 71 72 73 74 77
						01d0 69 6a 6b 6c 6d 6e
						01e0 62 63 64 65 66 6e
						01f0 72 73 74 75 76 77
						0200 6b 6c 6d 6e 6f 70
						0210 64 65 66 67 68 69

Fragment Offset: 0

Flaga MF (More Fragments): 1

Długość (Total Length): 1500

Zawartość: początek nagłówka IP + fragment danych ICMP

Fragment 2

No.	Time	Source	Destination	Protocol	Length	Info
963	100.473790	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2276) [Reassembled in #965]
964	100.473790	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2276) [Reassembled in #965]
965	100.473790	192.168.0.21	8.8.8.8	ICMP	1082	Echo (ping) request id=0x0001, seq=144/36864, ttl=128 (no response found!)
969	105.426164	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2277) [Reassembled in #971]
970	105.426164	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2277) [Reassembled in #971]
971	105.426164	192.168.0.21	8.8.8.8	ICMP	1082	Echo (ping) request id=0x0001, seq=145/37120, ttl=128 (no response found!)
991	110.422269	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2278) [Reassembled in #993]
992	110.422269	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2278) [Reassembled in #993]
993	110.422269	192.168.0.21	8.8.8.8	ICMP	1082	Echo (ping) request id=0x0001, seq=146/37376, ttl=128 (no response found!)
1032	115.428203	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2279) [Reassembled in #1034]
1033	115.428203	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2279) [Reassembled in #1034]
1034	115.428203	192.168.0.21	8.8.8.8	ICMP	1082	Echo (ping) request id=0x0001, seq=147/37632, ttl=128 (no response found!)
3623	289.865789	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=227a) [Reassembled in #3625]

Frame 964: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{5298A11C-0424-4C8D-8FA1-0034}

Ethernet II, Src: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31), Dst: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)

> Destination: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)

> Source: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31)

Type: IPv4 (0x0800)

[Stream index: 0]

Internet Protocol Version 4, Src: 192.168.0.21, Dst: 8.8.8.8

0100 = Version: 4

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

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

Total Length: 1500

Identification: 0x2276 (8822)

> 001. = Flags: 0x1, More fragments

...0 0000 1011 1001 = Fragment Offset: 1480

Time to Live: 128

Protocol: ICMP (1)

Header Checksum: 0x2125 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.0.21

Destination Address: 8.8.8.8

[Reassembled IPv4 in frame: 965]

[Stream index: 25]

Data (1480 bytes)

0000 60 3d 26 8e 3d

0010 05 dc 22 76 20

0020 08 08 61 62 63

0030 6f 70 71 72 73

0040 68 69 6a 6b 6c

0050 61 62 63 64 65

0060 71 72 73 74 75

0070 6a 6b 6c 6d 6e

0080 63 64 65 66 67

0090 73 74 75 76 77

00a0 6c 6d 6e 6f 70

00b0 65 66 67 68 69

00c0 75 76 77 61 62

00d0 6e 6f 70 71 72

00e0 67 68 69 6a 6b

00f0 77 61 62 63 64

0100 70 71 72 73 74

0110 69 6a 6b 6c 6d

0120 62 63 64 65 66

0130 72 73 74 75 76

0140 6b 6c 6d 6e 6f

0150 64 65 66 67 68

0160 74 75 76 77 61

0170 6d 6e 6f 70 71

0180 66 67 68 69 6a

0190 76 77 61 62 63

01a0 6f 70 71 72 73

01b0 68 69 6a 6b 6c

01c0 61 62 63 64 65

01d0 71 72 73 74 75

01e0 6a 6b 6c 6d 6e

01f0 63 64 65 66 67

0200 73 74 75 76 77

0210 6c 6d 6e 6f 70

0220 65 66 67 68 69

Fragment Offset: 1480

Flaga MF: 1

Długość: 1500

Zawiera kolejną porcję danych ICMP.

Fragment 3 (ostatni)

965	100.473790	192.168.0.21	8.8.8.8	ICMP	1082 Echo (ping) request id=0x0001, seq=144/36864, ttl=128 (no response found!)
969	105.426164	192.168.0.21	8.8.8.8	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2277) [Reassembled in #971]
970	105.426164	192.168.0.21	8.8.8.8	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2277) [Reassembled in #971]
971	105.426164	192.168.0.21	8.8.8.8	ICMP	1082 Echo (ping) request id=0x0001, seq=145/37120, ttl=128 (no response found!)
991	110.422269	192.168.0.21	8.8.8.8	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2278) [Reassembled in #993]
992	110.422269	192.168.0.21	8.8.8.8	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2278) [Reassembled in #993]
993	110.422269	192.168.0.21	8.8.8.8	ICMP	1082 Echo (ping) request id=0x0001, seq=146/37376, ttl=128 (no response found!)
1032	115.428203	192.168.0.21	8.8.8.8	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2279) [Reassembled in #1034]
1033	115.428203	192.168.0.21	8.8.8.8	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2279) [Reassembled in #1034]
1034	115.428203	192.168.0.21	8.8.8.8	ICMP	1082 Echo (ping) request id=0x0001, seq=147/37632, ttl=128 (no response found!)
3623	289.865789	192.168.0.21	8.8.8.8	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=227a) [Reassembled in #3625]
> Frame 965: 1082 bytes on wire (8656 bits), 1082 bytes captured (8656 bits) on interface \Device\NPF_{5298A11C-0424-4C8D-8FA1-0034E...}					
Ethernet II, Src: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31), Dst: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)					
> Destination: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)					
> Source: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31)					
Type: IPv4 (0x8000)					
[Stream index: 0]					
Internet Protocol Version 4, Src: 192.168.0.21, Dst: 8.8.8.8					
0100 = Version: 4					
.... 0101 = Header Length: 20 bytes (5)					
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 1068					
Identification: 0x2276 (8822)					
> 0000. = Flags: 0x0					
...0 0001 0111 0010 = Fragment Offset: 2960					
Time to Live: 128					
Protocol: ICMP (1)					
Header Checksum: 0x421c [validation disabled]					
[Header checksum status: Unverified]					
Source Address: 192.168.0.21					
Destination Address: 8.8.8.8					
> [3 IPv4 Fragments (4008 bytes): #963(1480), #964(1480), #965(1048)]					
[Stream index: 25]					
Internet Control Message Protocol					
Type: 8 (Echo (ping) request)					
Code: 0					
Checksum: 0xf26a [correct]					
[Checksum Status: Good]					
Identifier (BE): 1 (0x0001)					
Identifier (LE): 256 (0x0100)					
Sequence Number (BE): 144 (0x0090)					
Sequence Number (LE): 36864 (0x9000)					
> [No response seen]					
> Data (4000 bytes)					

Fragment Offset: 2960

Flaga MF: 0 (czyli brak — Flags: 0x0)

Długość: 1048

Wireshark scala wszystkie fragmenty i pokazuje je jako pełen pakiet ICMP w ramce końcowej.

Zadanie 2

1. Jak działa program traceroute (ewentualnie skorzystaj z

opcji **-I** lub **-T**)?

student@lab-sec-2:~> traceroute 1.1.1.1

traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets

- 1 150.254.32.65 (150.254.32.65) 0.480 ms 0.503 ms 0.599 ms
- 2 150.254.30.129 (150.254.30.129) 0.579 ms 0.676 ms 0.668 ms
- 3 hellfire.put.poznan.pl (150.254.6.36) 1.352 ms 1.216 ms 1.208 ms
- 4 PUTNET-BGP-P.put.poznan.pl (150.254.4.66) 2.116 ms 1.970 ms 2.493 ms
- 5 237.14.119.185-rev.hti.pl (185.119.14.237) 1.954 ms 1.823 ms 1.691 ms
- 6 088156078001.p2p.business.static.vectranet.pl (88.156.78.1) 7.906 ms 7.652 ms 7.480 ms
- 7 172.17.64.10 (172.17.64.10) 9.951 ms 9.393 ms 9.437 ms

```
8 172.17.64.10 (172.17.64.10) 8.852 ms 9.170 ms 9.161 ms
9 162.158.100.12 (162.158.100.12) 7.899 ms 7.825 ms 8.149 ms
10 162.158.100.17 (162.158.100.17) 8.139 ms 162.158.100.7 (162.158.100.7) 12.670 ms
12.661 ms
11 one.one.one.one (1.1.1.1) 7.402 ms 7.403 ms 7.119 ms
```

Polecenie traceroute służy do śledzenia trasy pakietów IP od źródła (nasz komputer) do hosta docelowego (tu: 1.1.1.1).

Traceroute wykorzystuje mechanizm TTL (Time to Live) w nagłówku IP:

TTL to liczba skoków, jaką pakiet może wykonać.

Każdy router zmniejsza TTL o 1.

Gdy TTL = 0, router odrzuca pakiet i odsyła odpowiedź ICMP Time Exceeded.

Traceroute wysyła pakiety z TTL od 1 w górę, po 3 pakiety dla każdego skoku.

W ten sposób:

- Pakiety z TTL = 1 docierają tylko do pierwszego routera → dostajemy odpowiedź od niego.
- TTL = 2 → odpowiedź od drugiego routera.
- ... i tak dalej, aż do hosta docelowego (który odpowiada inaczej – np. ICMP Echo Reply).

2. Zaloguj ruch przy pomocy programu wireshark i zbadaj nagłówki pakietów generowanych przez program traceroute.

-Traceroute wysyła pakiety z kolejnymi wartościami TTL.

-Każdy router pośredni odrzuca pakiet z TTL = 0 i wysyła ICMP Time Exceeded.

-Dzięki temu traceroute zbiera adresy wszystkich routerów na drodze.

-Ostateczny host może odpowiedzieć Echo Reply (przy ICMP) – tak jak w tym przypadku lub Unreachable (w przypadku UDP).

TTL = 1

Wireshark packet capture showing ICMP Echo (ping) requests. The packet list shows several ping requests from 192.168.0.21 to 8.8.8.8, all of which failed with "Time-to-live exceeded" or "no response found". The packet details pane shows the structure of an ICMP Echo request, including the header and data fields.

ICMP Time Exceeded

Wireshark packet capture showing ICMP Time Exceeded messages. The packet list shows several ICMP Time Exceeded messages from 8.8.8.8 to 192.168.0.21, indicating that the TTL of the original ping request was exceeded. The packet details pane shows the structure of an ICMP Time Exceeded message, including the header and data fields.

TTL = 2

Wireshark packet capture showing network traffic. The packet list shows various protocols including TLSv1.2, TCP, NBNS, UDP/XML, and ICMP. The packet details pane shows the structure of an Internet Protocol Version 4 packet and an Internet Control Message Protocol (ICMP) Echo (ping) request. The packet bytes pane shows the raw data in hexadecimal and ASCII.

TTL = 3

Wireshark packet capture showing network traffic. The packet list shows various protocols including UDP/XML, NBNS, TLSv1.2, TCP, and ICMP. The packet details pane shows the structure of an Internet Protocol Version 4 packet and an Internet Control Message Protocol (ICMP) Echo (ping) request. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Echo reply od celu

288	52.092905	192.168.0.21	8.8.8.8	ICMP	106 Echo (ping) request	id=0x0001, seq=141/36096, ttl=12 (reply in 288)
289	52.092905	8.8.8.8	192.168.0.21	ICMP	106 Echo (ping) reply	id=0x0001, seq=141/36096, ttl=113 (request in 288)
290	52.093439	192.168.0.21	8.8.8.8	ICMP	106 Echo (ping) request	id=0x0001, seq=142/36352, ttl=12 (reply in 291)
291	52.110616	8.8.8.8	192.168.0.21	ICMP	106 Echo (ping) reply	id=0x0001, seq=142/36352, ttl=113 (request in 290)
292	52.111141	192.168.0.21	8.8.8.8	ICMP	106 Echo (ping) request	id=0x0001, seq=143/36608, ttl=12 (reply in 293)
293	52.128268	8.8.8.8	192.168.0.21	ICMP	106 Echo (ping) reply	id=0x0001, seq=143/36608, ttl=113 (request in 292)
294	52.751402	192.168.0.21	35.186.224.44	TLSv1.2	89 Application Data	
295	52.771026	35.186.224.44	192.168.0.21	TCP	60 443 → 61537 [ACK] Seq=1 Ack=71 Win=1051 Len=0	

Frame 293: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{5298A11C-0424-4C8D-8FA1-0034ECAB92}	0000	90 e8 68 42 a2 31 60 3d 2f
Ethernet II, Src: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6), Dst: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31)	0010	00 5c 00 00 00 71 01 7e
> Destination: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31)	0020	00 15 00 00 ff 6f 00 01 0e
> Source: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)	0030	00 00 00 00 00 00 00 00 0e
Type: IPv4 (0x0800)	0040	00 00 00 00 00 00 00 00 0e
[Stream index: 0]	0050	00 00 00 00 00 00 00 00 0e
	0060	00 00 00 00 00 00 00 00 0e

Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.0.21
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0x0000 (0)
> 000. = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 113
Protocol: ICMP (1)
Header Checksum: 0x78d4 [validation disabled]
[Header checksum status: Unverified]
Source Address: 8.8.8.8
Destination Address: 192.168.0.21
[Stream index: 3]

Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0xffff [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 143 (0x008f)
Sequence Number (LE): 36608 (0x8f00)
[Request frame: 292]
[Response time: 17.127 ms]
> Data (64 bytes)

Zadanie 3

1.Podłącz swój komputer (poprzez port p4p1) do koncentratora (na zapleczu).

2. Skonfiguruj interfejs p4p1, tak by wszystkie komputery w rzędzie działały w jednej sieci (unikalne sieci między rzędami).

student@lab-sec-2:~> arp

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.1.4	ether	00:10:18:aa:a8:b8	C		p4p1
lab-sec-61.cs.put.pozna	ether	00:25:64:3b:c1:d0	C		br0
192.168.1.3	ether	00:10:18:b4:e3:7c	C		p4p1
lab-sec-1.cs.put.poznan	ether	e4:54:e8:a5:98:c6	C		br0
150.254.32.65	ether	00:04:96:9b:9b:f0	C		br0
192.168.1.1	ether	e4:54:e8:a5:98:c6	C		br0
lindev.cs.put.poznan.pl	ether	52:54:00:7d:97:53	C		br0
lab-sec-9.cs.put.poznan	ether	e4:54:e8:a5:98:f0	C		br0

3. Zbadaj jak zmienia się tablica ARP, gdy uruchamiasz program

ping z argumentami będącymi adresami IP komputerów z

Twojej sieci i adresami komputerów w innych rzędach

(należących do innych sieci).

```
student@lab-sec-2:~> ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=0.503 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.544 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=0.542 ms
^C
--- 192.168.1.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2048ms
rtt min/avg/max/mdev = 0.503/0.529/0.544/0.018 ms
student@lab-sec-2:~> arp
Address          HWtype HWaddress      Flags Mask        Iface
192.168.1.4      (incomplete)          p4p1
lab-sec-61.cs.put.pozna ether 00:25:64:3b:c1:d0 C          br0
192.168.1.3      ether 00:10:18:b4:e3:7c C          p4p1
lab-sec-1.cs.put.poznan ether e4:54:e8:a5:98:c6 C          br0
192.168.1.1      ether 00:10:18:aa:bd:7c C          p4p1
150.254.32.65    ether 00:04:96:9b:9b:f0 C          br0
192.168.1.1      ether e4:54:e8:a5:98:c6 C          br0
lindev.cs.put.poznan.pl ether 52:54:00:7d:97:53 C          br0
lab-sec-9.cs.put.poznan ether e4:54:e8:a5:98:f0 C          br0
```

Po nadaniu adresu IP, włączeniu interfejsu oraz wykonaniu poleceń ping do komputerów w sieci 192.168.1.0 (2 wiersz), do tablicy ARP zostają dodane powiązania adresów IP z odpowiadającymi im adresami MAC.

Komputery o adresach 192.168.1.1 oraz 192.168.1.3 zostały uwzględnione w poniższej tablicy, natomiast komputer o adresie 192.168.1.4 nie odpowiedział poprawnie – wpis ARP pozostał w stanie incomplete, co może oznaczać, że komputer jest wyłączony, nieosiągalny lub interfejs sieciowy nie działa.