

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»**

**КАФЕДРА ММСА**

**Лабораторна робота № 5**

**З дисципліни: Комп’ютерні мережі**

***Основи захоплення та аналізу пакетів***

**Виконаd:**

**Студент ІII курсу**

**Групи КА-74**

**Таровський Б. Є.**

**Перевірив: Кухарєв С. О.**

**Київ 2020**

**C:\Users\Roman>ping -l 2000 gaia.cs.umass.edu**

**Pinging gaia.cs.umass.edu [128.119.245.12] with 2000 bytes of data:**

**Reply from 128.119.245.12: bytes=2000 time=128ms TTL=47**

**Reply from 128.119.245.12: bytes=2000 time=132ms TTL=47**

**Reply from 128.119.245.12: bytes=2000 time=130ms TTL=47**

**Reply from 128.119.245.12: bytes=2000 time=129ms TTL=47**

**Ping statistics for 128.119.245.12:**

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

**Approximate round trip times in milli-seconds:**

**Minimum = 128ms, Maximum = 132ms, Average = 129ms**

No. Time Source Destination Protocol Length Info

29 2.792995 192.168.0.103 128.119.245.12 ICMP 562 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 31)

Frame 29: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface 0

Ethernet II, Src: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13), Dst: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 128.119.245.12

0100 .... = Version: 4

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

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

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 548

Identification: 0x1474 (5236)

Flags: 0x00b9

0... .... .... .... = Reserved bit: Not set

.0.. .... .... .... = Don't fragment: Not set

..0. .... .... .... = More fragments: Not set

...0 0000 1011 1001 = Fragment offset: 185

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0xed18 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.103

Destination: 128.119.245.12

[2 IPv4 Fragments (2008 bytes): #28(1480), #29(528)]

[Frame: 28, payload: 0-1479 (1480 bytes)]

[Frame: 29, payload: 1480-2007 (528 bytes)]

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 08007b71000100066162636465666768696a6b6c6d6e6f70...]

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x7b71 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 6 (0x0006)

Sequence number (LE): 1536 (0x0600)

[Response frame: 31]

Data (2000 bytes)

No. Time Source Destination Protocol Length Info

31 2.926689 128.119.245.12 192.168.0.103 ICMP 562 Echo (ping) reply id=0x0001, seq=6/1536, ttl=47 (request in 29)

Frame 31: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface 0

Ethernet II, Src: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a), Dst: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.103

0100 .... = Version: 4

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

Differentiated Services Field: 0x04 (DSCP: Unknown, ECN: Not-ECT)

0000 01.. = Differentiated Services Codepoint: Unknown (1)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 548

Identification: 0x6ed5 (28373)

Flags: 0x00b9

0... .... .... .... = Reserved bit: Not set

.0.. .... .... .... = Don't fragment: Not set

..0. .... .... .... = More fragments: Not set

...0 0000 1011 1001 = Fragment offset: 185

Time to live: 47

Protocol: ICMP (1)

Header checksum: 0xe3b3 [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.0.103

[2 IPv4 Fragments (2008 bytes): #30(1480), #31(528)]

[Frame: 30, payload: 0-1479 (1480 bytes)]

[Frame: 31, payload: 1480-2007 (528 bytes)]

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 00008371000100066162636465666768696a6b6c6d6e6f70...]

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x8371 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 6 (0x0006)

Sequence number (LE): 1536 (0x0600)

[Request frame: 29]

[Response time: 133.694 ms]

Data (2000 bytes)

No. Time Source Destination Protocol Length Info

33 3.798443 192.168.0.103 128.119.245.12 ICMP 562 Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 43)

Frame 33: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface 0

Ethernet II, Src: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13), Dst: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 128.119.245.12

0100 .... = Version: 4

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

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

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 548

Identification: 0x1475 (5237)

Flags: 0x00b9

0... .... .... .... = Reserved bit: Not set

.0.. .... .... .... = Don't fragment: Not set

..0. .... .... .... = More fragments: Not set

...0 0000 1011 1001 = Fragment offset: 185

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0xed17 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.103

Destination: 128.119.245.12

[2 IPv4 Fragments (2008 bytes): #32(1480), #33(528)]

[Frame: 32, payload: 0-1479 (1480 bytes)]

[Frame: 33, payload: 1480-2007 (528 bytes)]

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 08007b70000100076162636465666768696a6b6c6d6e6f70...]

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x7b70 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 7 (0x0007)

Sequence number (LE): 1792 (0x0700)

[Response frame: 43]

Data (2000 bytes)

No. Time Source Destination Protocol Length Info

43 3.932783 128.119.245.12 192.168.0.103 ICMP 562 Echo (ping) reply id=0x0001, seq=7/1792, ttl=47 (request in 33)

Frame 43: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface 0

Ethernet II, Src: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a), Dst: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.103

0100 .... = Version: 4

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

Differentiated Services Field: 0x04 (DSCP: Unknown, ECN: Not-ECT)

0000 01.. = Differentiated Services Codepoint: Unknown (1)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 548

Identification: 0x713e (28990)

Flags: 0x00b9

0... .... .... .... = Reserved bit: Not set

.0.. .... .... .... = Don't fragment: Not set

..0. .... .... .... = More fragments: Not set

...0 0000 1011 1001 = Fragment offset: 185

Time to live: 47

Protocol: ICMP (1)

Header checksum: 0xe14a [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.0.103

[2 IPv4 Fragments (2008 bytes): #42(1480), #43(528)]

[Frame: 42, payload: 0-1479 (1480 bytes)]

[Frame: 43, payload: 1480-2007 (528 bytes)]

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 00008370000100076162636465666768696a6b6c6d6e6f70...]

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x8370 [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 7 (0x0007)

Sequence number (LE): 1792 (0x0700)

[Request frame: 33]

[Response time: 134.340 ms]

Data (2000 bytes)

No. Time Source Destination Protocol Length Info

48 4.812858 192.168.0.103 128.119.245.12 ICMP 562 Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 50)

Frame 48: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface 0

Ethernet II, Src: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13), Dst: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 128.119.245.12

0100 .... = Version: 4

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

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

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 548

Identification: 0x1476 (5238)

Flags: 0x00b9

0... .... .... .... = Reserved bit: Not set

.0.. .... .... .... = Don't fragment: Not set

..0. .... .... .... = More fragments: Not set

...0 0000 1011 1001 = Fragment offset: 185

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0xed16 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.103

Destination: 128.119.245.12

[2 IPv4 Fragments (2008 bytes): #47(1480), #48(528)]

[Frame: 47, payload: 0-1479 (1480 bytes)]

[Frame: 48, payload: 1480-2007 (528 bytes)]

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 08007b6f000100086162636465666768696a6b6c6d6e6f70...]

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x7b6f [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 8 (0x0008)

Sequence number (LE): 2048 (0x0800)

[Response frame: 50]

Data (2000 bytes)

No. Time Source Destination Protocol Length Info

50 4.947327 128.119.245.12 192.168.0.103 ICMP 562 Echo (ping) reply id=0x0001, seq=8/2048, ttl=47 (request in 48)

Frame 50: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface 0

Ethernet II, Src: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a), Dst: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.103

0100 .... = Version: 4

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

Differentiated Services Field: 0x04 (DSCP: Unknown, ECN: Not-ECT)

0000 01.. = Differentiated Services Codepoint: Unknown (1)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 548

Identification: 0x741b (29723)

Flags: 0x00b9

0... .... .... .... = Reserved bit: Not set

.0.. .... .... .... = Don't fragment: Not set

..0. .... .... .... = More fragments: Not set

...0 0000 1011 1001 = Fragment offset: 185

Time to live: 47

Protocol: ICMP (1)

Header checksum: 0xde6d [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.0.103

[2 IPv4 Fragments (2008 bytes): #49(1480), #50(528)]

[Frame: 49, payload: 0-1479 (1480 bytes)]

[Frame: 50, payload: 1480-2007 (528 bytes)]

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 0000836f000100086162636465666768696a6b6c6d6e6f70...]

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x836f [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 8 (0x0008)

Sequence number (LE): 2048 (0x0800)

[Request frame: 48]

[Response time: 134.469 ms]

Data (2000 bytes)

No. Time Source Destination Protocol Length Info

52 5.827698 192.168.0.103 128.119.245.12 ICMP 562 Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 56)

Frame 52: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface 0

Ethernet II, Src: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13), Dst: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 128.119.245.12

0100 .... = Version: 4

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

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

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 548

Identification: 0x1477 (5239)

Flags: 0x00b9

0... .... .... .... = Reserved bit: Not set

.0.. .... .... .... = Don't fragment: Not set

..0. .... .... .... = More fragments: Not set

...0 0000 1011 1001 = Fragment offset: 185

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0xed15 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.103

Destination: 128.119.245.12

[2 IPv4 Fragments (2008 bytes): #51(1480), #52(528)]

[Frame: 51, payload: 0-1479 (1480 bytes)]

[Frame: 52, payload: 1480-2007 (528 bytes)]

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 08007b6e000100096162636465666768696a6b6c6d6e6f70...]

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x7b6e [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 9 (0x0009)

Sequence number (LE): 2304 (0x0900)

[Response frame: 56]

Data (2000 bytes)

No. Time Source Destination Protocol Length Info

56 5.964349 128.119.245.12 192.168.0.103 ICMP 562 Echo (ping) reply id=0x0001, seq=9/2304, ttl=47 (request in 52)

Frame 56: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface 0

Ethernet II, Src: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a), Dst: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.103

0100 .... = Version: 4

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

Differentiated Services Field: 0x04 (DSCP: Unknown, ECN: Not-ECT)

0000 01.. = Differentiated Services Codepoint: Unknown (1)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 548

Identification: 0x76c8 (30408)

Flags: 0x00b9

0... .... .... .... = Reserved bit: Not set

.0.. .... .... .... = Don't fragment: Not set

..0. .... .... .... = More fragments: Not set

...0 0000 1011 1001 = Fragment offset: 185

Time to live: 47

Protocol: ICMP (1)

Header checksum: 0xdbc0 [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.0.103

[2 IPv4 Fragments (2008 bytes): #55(1480), #56(528)]

[Frame: 55, payload: 0-1479 (1480 bytes)]

[Frame: 56, payload: 1480-2007 (528 bytes)]

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 0000836e000100096162636465666768696a6b6c6d6e6f70...]

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x836e [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 9 (0x0009)

Sequence number (LE): 2304 (0x0900)

[Request frame: 52]

[Response time: 136.651 ms]

Data (2000 bytes)

**Контрольні питання**

1. **Визначте IP адреси вашої та цільової робочих станцій.**

Моя – 192.168.0.103, цільова – 128.119.245.12.

1. **Яке значення в полі номера протоколу вищого рівня в заголовку IP першого пакету із запитом ICMP?**

Protocol: ICMP (1)

1. **Скільки байт займає заголовок IP першого пакету із запитом ICMP? Скільки байт займає корисна інформація (payload) пакету? Поясніть як ви встановили кількість байт корисної інформації.**

20 байт, 2008 байт = 1480 + 528

**[2 IPv4 Fragments (2008 bytes): #28(1480), #29(528)]**

**[Frame: 28, payload: 0-1479 (1480 bytes)]**

**[Frame: 29, payload: 1480-2007 (528 bytes)]**

**[Fragment count: 2]**

**[Reassembled IPv4 length: 2008]**

**[Reassembled IPv4 data: 08007b71000100066162636465666768696a6b6c6d6e6f70...]**

1. **Дослідіть пакет із пунктів 2/3. Чи фрагментований цей пакет? Поясніть як ви встановили фрагментацію пакету. Як можна встановити номер фрагменту, що передається у пакеті?**

Так, фрагментований. По номеру фрейма.

**[2 IPv4 Fragments (2008 bytes): #28(1480), #29(528)]**

1. **Знайдіть наступний фрагмент датаграми IP. Яка інформація дозволяє встановити наявність наступних фрагментів, що мають слідувати за другим фрагментом?**

Flags: 0x00b9

0... .... .... .... = Reserved bit: Not set

.0.. .... .... .... = Don't fragment: Not set

..0. .... .... .... = More fragments: Not set

...0 0000 1011 1001 = Fragment offset: 185

1. **Які поля протоколу IP відрізняють перший фрагмент від другого?**

Тільки назва фрейму та Upper Layer Protocol, Fragment offset.

1. **Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Які поля заголовку IP завжди змінюються?**

Identification та Header checksum.

1. **Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Які поля заголовку IP мають зберігати свої значення? Які поля мають змінюватися? Чому?**

Поля, які зберігають свої значення:

* Version (ми використовуємо IPv4 для всіх пакетів)
* header length (всі пакети – ICMP)
* source IP, destination IP (Ми пінгуємо одну і ту ж адресу)
* Differentiated Services (всі ICMP пакети одного службового типу)
* TTL

Поля, які змінюють свої значення:

* Upper Layer Protocol (всі загаловки ICMP мають унікальні поля, що змінюються)
* Identification (IP пакети мають мати різні id)
* Header checksum (оскільки заголовки змінюються, то контрольна сума теж)

**9. Розгляньте послідовність пакетів IP із запитами ICMP вашої робочої станції. Опишіть закономірність зміни значень поля Identification рівня IP.**

Інкремент на 1.

**10. Розгляньте послідовність пакетів IP із повідомленнями TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL?**

Таких повідомлень не було, оскільки утиліта ping на Windows не змінює TTL для різних запитів.

**11. Розгляньте послідовність пакетів IP із повідомленнями TTL-exceeded від найближчого маршрутизатора. Які значення встановлені у полях Identification та TTL? Чи змінюються ці значення для різних пакетів у послідовності? Чому?**

Поле Identification має змінюватись для кожної ICMP TTL-exceeded відповіді. Якщо дві або більше IP датаграми мають однаковий Identification, то це означає, що вони є фрагментами однієї великої IP датаграми. Поле TTL завжди однакове, бо у найближчого маршрутизатора він завжди однаковий.