**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС**

**«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»**

**НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ**

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

**КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ**

**Практична робота №5**

**з курсу «Комп'ютерні мережі»**

**Виконав студент 3 курсу**

**групи КА-72**

**Бойко Павло**

**Прийняв Кухарєв С.О.**

**Київ – 2020 р.**

**Контрольні запитання:**

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

Моя - 192.168.0.110, 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.**

Head Load = 20 байт

Total Length =576 байт

Payload = 576 -20 = 556

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 (1980 bytes): #98(1480), #99(500)

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

Reassembled IPv4 in frame: 102

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

Тільки назва фрейму та Upper Layer Protocol

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)
* Time to live

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

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

Інкрементується на 1

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

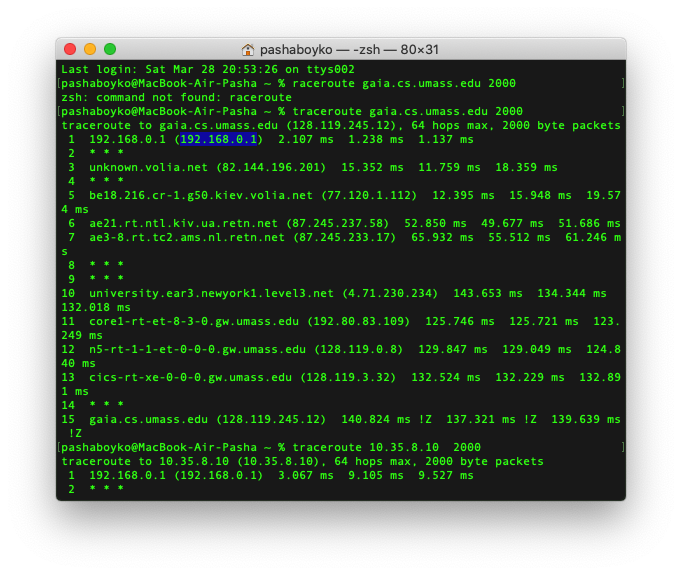
Time to live: 2 Identification: 0xe63d (58941)

1. **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?**

Time to live: не змінюється

Identification : змінюєтся щоб розрізняти фрагменти (Якщо дві або більше IP датаграми мають однаковий Identification, то це означає, що вони є фрагментами однієї великої IP датаграми.)

**Висновки:** при виконанні роботи я познайомився з протоколом IP. Ознайомився з деякими принципами фрагментації та як вони виражаються у запитах.



No. Time Source Destination Protocol Length Info

100 17.058010 192.168.0.1 192.168.0.110 ICMP 590 Time-to-live exceeded (Time to live exceeded in transit)

Frame 100: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface en0, id 0

Ethernet II, Src: Tp-LinkT\_52:65:b6 (f4:f2:6d:52:65:b6), Dst: Apple\_12:88:12 (14:c2:13:12:88:12)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.110

0100 .... = Version: 4

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

Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)

Total Length: 576

Identification: 0xff98 (65432)

Flags: 0x0000

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64

Protocol: ICMP (1)

Header checksum: 0xf6a4 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.1

Destination: 192.168.0.110

Internet Control Message Protocol

No. Time Source Destination Protocol Length Info

101 17.058142 192.168.0.110 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=e63b) [Reassembled in #102]

Frame 101: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0

Ethernet II, Src: Apple\_12:88:12 (14:c2:13:12:88:12), Dst: Tp-LinkT\_52:65:b6 (f4:f2:6d:52:65:b6)

Internet Protocol Version 4, Src: 192.168.0.110, Dst: 128.119.245.12

0100 .... = Version: 4

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

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

Total Length: 1500

Identification: 0xe63b (58939)

Flags: 0x2000, More fragments

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 1

[Expert Info (Note/Sequence): "Time To Live" only 1]

Protocol: UDP (17)

Header checksum: 0x773b [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.110

Destination: 128.119.245.12

Reassembled IPv4 in frame: 102

Data (1480 bytes)

No. Time Source Destination Protocol Length Info

102 17.058143 192.168.0.110 128.119.245.12 UDP 534 58936 → 33437 Len=1972

Frame 102: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface en0, id 0

Ethernet II, Src: Apple\_12:88:12 (14:c2:13:12:88:12), Dst: Tp-LinkT\_52:65:b6 (f4:f2:6d:52:65:b6)

Internet Protocol Version 4, Src: 192.168.0.110, Dst: 128.119.245.12

0100 .... = Version: 4

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

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

Total Length: 520

Identification: 0xe63b (58939)

Flags: 0x00b9

...0 0101 1100 1000 = Fragment offset: 1480

Time to live: 1

[Expert Info (Note/Sequence): "Time To Live" only 1]

Protocol: UDP (17)

Header checksum: 0x9a56 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.110

Destination: 128.119.245.12

[2 IPv4 Fragments (1980 bytes): #101(1480), #102(500)]

User Datagram Protocol, Src Port: 58936, Dst Port: 33437

Data (1972 bytes)