

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС  
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»  
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»  
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ**

**Практична робота №5  
з курсу «Комп'ютерні мережі»**

**Виконав: студент 3 курсу  
групи КА-77  
Тарасевич А.А.  
Прийняв: Кухарєв С.О.**

**Київ – 2020р.**

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

Обмен пакетами с gaia.cs.umass.edu [128.119.245.12] с 2000 байтами данных:

Ответ от 128.119.245.12: число байт=2000 время=115мс TTL=50

Ответ от 128.119.245.12: число байт=2000 время=113мс TTL=50

Ответ от 128.119.245.12: число байт=2000 время=115мс TTL=50

Ответ от 128.119.245.12: число байт=2000 время=114мс TTL=50

Статистика Ping для 128.119.245.12:

Пакетов: отправлено = 4, получено = 4, потеряно = 0

(0% потерь)

Приблизительное время приема-передачи в мс:

Минимальное = 113мсек, Максимальное = 115 мсек, Среднее = 114 мсек

Frame 2: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface  
\\Device\NPF\_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0

Ethernet II, Src: CyberTAN\_c2:ea:a9 (60:14:b3:c2:ea:a9), Dst: Fortinet\_dc:64:1d (00:09:0f:dc:64:1d)

Internet Protocol Version 4, Src: 172.16.7.104, 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: 1500

Identification: 0xb42b (46123)

Flags: 0x2000, More fragments

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

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

..1. .... = More fragments: Set

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

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0x37f9 [validation disabled]

[Header checksum status: Unverified]

Source: 172.16.7.104

Destination: 128.119.245.12

Reassembled IPv4 in frame: 3

Data (1480 bytes)

Frame 3: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface  
\\Device\\NPF\_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0

Ethernet II, Src: CyberTAN\_c2:ea:a9 (60:14:b3:c2:ea:a9), Dst: Fortinet\_dc:64:1d (00:09:0f:dc:64:1d)

Internet Protocol Version 4, Src: 172.16.7.104, 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: 0xb42b (46123)

Flags: 0x00b9

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

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

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

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

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0x5af8 [validation disabled]

[Header checksum status: Unverified]

Source: 172.16.7.104

Destination: 128.119.245.12

[2 IPv4 Fragments (2008 bytes): #2(1480), #3(528)]

[Frame: 2, payload: 0-1479 (1480 bytes)]

[Frame: 3, payload: 1480-2007 (528 bytes)]

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 08007b0a0001006d6162636465666768696a6b6c6d6e6f70...]

## Internet Control Message Protocol

Frame 4: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface  
\\Device\\NPF\_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0

Ethernet II, Src: Fortinet\_dc:64:1d (00:09:0f:dc:64:1d), Dst: CyberTAN\_c2:ea:a9 (60:14:b3:c2:ea:a9)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.7.104

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: 1500

Identification: 0xcd18 (52504)

Flags: 0x2000, More fragments

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

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

..1. .... = More fragments: Set

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

Time to live: 50

Protocol: ICMP (1)

Header checksum: 0x6d0c [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 172.16.7.104

Reassembled IPv4 in frame: 5

Data (1480 bytes)

Frame 5: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface  
\\Device\\NPF\_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0

Ethernet II, Src: Fortinet\_dc:64:1d (00:09:0f:dc:64:1d), Dst: CyberTAN\_c2:ea:a9 (60:14:b3:c2:ea:a9)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.7.104

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: 0xcd18 (52504)

Flags: 0x00b9

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

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

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

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

Time to live: 50

Protocol: ICMP (1)

Header checksum: 0x900b [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 172.16.7.104

[2 IPv4 Fragments (2008 bytes): #4(1480), #5(528)]

[Frame: 4, payload: 0-1479 (1480 bytes)]

[Frame: 5, payload: 1480-2007 (528 bytes)]

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 0000830a0001006d6162636465666768696a6b6c6d6e6f70...]

Internet Control Message Protocol

### Контрольні запитання:

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

Моя: 172.16.7.104, цільова: 128.119.245.12

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

1

**3. 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 bytes

Payload:

[2 IPv4 Fragments (2008 bytes): #2(1480), #3(528)]

[Frame: 2, payload: 0-1479 (1480 bytes)]

[Frame: 3, payload: 1480-2007 (528 bytes)]

[Fragment count: 2]

[Reassembled IPv4 length: 2008]

[Reassembled IPv4 data: 08007b0a0001006d6162636465666768696a6b6c6d6e6f70...]

**4. 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, [2 IPv4 Fragments (2008 bytes): #6(1480), #7(528)], Fragment offset: 1480, тож це другий фрагмент

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

More fragments у Flags - 0x01

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

Fragment offset: 0

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

Identification, Header checksum

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

Identification, Header checksum - ці поля повинні змінюватися для того, щоб розрізнявати пакети та перевіряти їх на непошкодженість. Інше - за потребою.

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

Збільшується на один (+1 до старого значення)

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

Identification: 0xb42b (46123), TTL: 128

**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?

Identification змінюється, а TTL - ні, бо за допомогою ідентифікатора визначається той чи інший пакет, а час життя визначається джерелом передачі.

### **Висновки:**

В цій лабораторній роботі я досліджував протокол IP ((IPv4) — протокол мережевого рівня для передавання датаграм між мережами, а також закріпив навички роботи з командою(утилітою) ping командного терміналу Windows