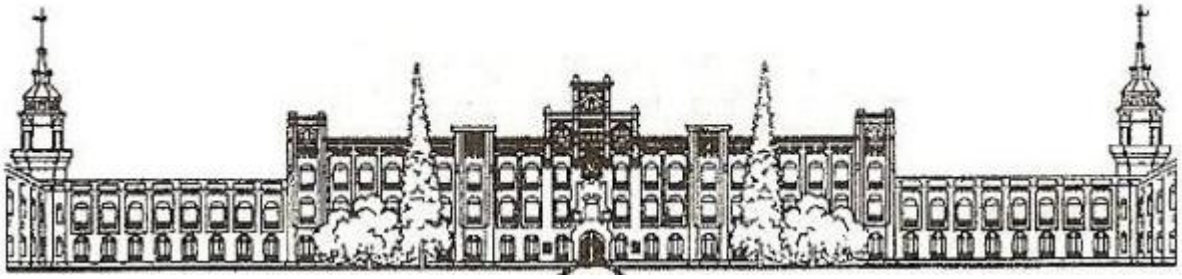

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

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

КАФЕДРА ММСА

Лабораторна робота № 5

З дисципліни: Комп'ютерні мережі

Протоколи IP

Виконав:

Студент III курсу

Групи КА-72

Братцев Антін

Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу IP.

Хід виконання роботи

No. Time Source Destination Protocol Length Info

144 58.618840 192.168.1.2 128.119.245.12 ICMP 562 Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (reply in 146)

Frame 144: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{04A418C6-E72D-4DC5-8B1A-21EC1CC49F79}, id 0

Ethernet II, Src: Chongqin_d9:c0:f7 (ac:d5:64:d9:c0:f7), Dst: ASUSTekC_dc:ce:a0 (e0:cb:4e:dc:ce:a0)

Internet Protocol Version 4, Src: 192.168.1.2, 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: 548

Identification: 0x6838 (26680)

Flags: 0x00b9

Fragment offset: 1480

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0x98b9 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.2

Destination: 128.119.245.12

[2 IPv4 Fragments (2008 bytes): #143(1480), #144(528)]

Internet Control Message Protocol

No. Time Source Destination Protocol Length Info

146 58.791908 128.119.245.12 192.168.1.2 ICMP 562 Echo (ping) reply id=0x0001, seq=48/12288, ttl=49 (request in 144)

Frame 146: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{04A418C6-E72D-4DC5-8B1A-21EC1CC49F79}, id 0

Ethernet II, Src: ASUSTekC_dc:ce:a0 (e0:cb:4e:dc:ce:a0), Dst: Chongqin_d9:c0:f7 (ac:d5:64:d9:c0:f7)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.2

0100 .... = Version: 4

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

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

Total Length: 548

Identification: 0x0a6a (2666)

Flags: 0x00b9

Fragment offset: 1480

Time to live: 49

Protocol: ICMP (1)

Header checksum: 0x4588 [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.1.2

[2 IPv4 Fragments (2008 bytes): #145(1480), #146(528)]

Internet Control Message Protocol

No. Time Source Destination Protocol Length Info

157 59.629941 192.168.1.2 128.119.245.12 ICMP 562 Echo (ping) request id=0x0001, seq=49/12544, ttl=128 (reply in 160)

Frame 157: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{04A418C6-E72D-4DC5-8B1A-21EC1CC49F79}, id 0

Ethernet II, Src: Chongqin_d9:c0:f7 (ac:d5:64:d9:c0:f7), Dst: ASUSTekC_dc:ce:a0 (e0:cb:4e:dc:ce:a0)

Internet Protocol Version 4, Src: 192.168.1.2, 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: 548

Identification: 0x6839 (26681)

Flags: 0x00b9

Fragment offset: 1480

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0x98b8 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.2

Destination: 128.119.245.12

[2 IPv4 Fragments (2008 bytes): #156(1480), #157(528)]

Internet Control Message Protocol

No. Time Source Destination Protocol Length Info

160 59.756698 128.119.245.12 192.168.1.2 ICMP 562 Echo (ping) reply id=0x0001, seq=49/12544, ttl=49 (request in 157)

Frame 160: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{04A418C6-E72D-4DC5-8B1A-21EC1CC49F79}, id 0

Ethernet II, Src: ASUSTekC_dc:ce:a0 (e0:cb:4e:dc:ce:a0), Dst: Chongqin_d9:c0:f7 (ac:d5:64:d9:c0:f7)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.2

0100 .... = Version: 4

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

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

Total Length: 548

Identification: 0x0d15 (3349)

Flags: 0x00b9

Fragment offset: 1480

Time to live: 49

Protocol: ICMP (1)

Header checksum: 0x42dd [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.1.2

[2 IPv4 Fragments (2008 bytes): #159(1480), #160(528)]

Internet Control Message Protocol

No. Time Source Destination Protocol Length Info

165 60.639876 192.168.1.2 128.119.245.12 ICMP 562 Echo (ping) request id=0x0001, seq=50/12800, ttl=128 (reply in 167)

Frame 165: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{04A418C6-E72D-4DC5-8B1A-21EC1CC49F79}, id 0

Ethernet II, Src: Chongqin_d9:c0:f7 (ac:d5:64:d9:c0:f7), Dst: ASUSTekC_dc:ce:a0 (e0:cb:4e:dc:ce:a0)

Internet Protocol Version 4, Src: 192.168.1.2, 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: 548

Identification: 0x683a (26682)

Flags: 0x00b9

Fragment offset: 1480

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0x98b7 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.2

Destination: 128.119.245.12

[2 IPv4 Fragments (2008 bytes): #164(1480), #165(528)]

Internet Control Message Protocol

No. Time Source Destination Protocol Length Info

167 60.770032 128.119.245.12 192.168.1.2 ICMP 562 Echo (ping) reply id=0x0001, seq=50/12800, ttl=49 (request in 165)

Frame 167: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{04A418C6-E72D-4DC5-8B1A-21EC1CC49F79}, id 0

Ethernet II, Src: ASUSTekC_dc:ce:a0 (e0:cb:4e:dc:ce:a0), Dst: Chongqin_d9:c0:f7 (ac:d5:64:d9:c0:f7)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.2

0100 .... = Version: 4

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

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

Total Length: 548

Identification: 0x0ddb (3547)

Flags: 0x00b9

Fragment offset: 1480

Time to live: 49

Protocol: ICMP (1)

Header checksum: 0x4217 [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.1.2

[2 IPv4 Fragments (2008 bytes): #166(1480), #167(528)]

Internet Control Message Protocol

No. Time Source Destination Protocol Length Info

172 61.650410 192.168.1.2 128.119.245.12 ICMP 562 Echo (ping) request id=0x0001, seq=51/13056, ttl=128 (reply in 174)

Frame 172: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{04A418C6-E72D-4DC5-8B1A-21EC1CC49F79}, id 0

Ethernet II, Src: Chongqin_d9:c0:f7 (ac:d5:64:d9:c0:f7), Dst: ASUSTekC_dc:ce:a0 (e0:cb:4e:dc:ce:a0)

Internet Protocol Version 4, Src: 192.168.1.2, 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: 548

Identification: 0x683b (26683)

Flags: 0x00b9

Fragment offset: 1480

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0x98b6 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.2

Destination: 128.119.245.12

[2 IPv4 Fragments (2008 bytes): #171(1480), #172(528)]

Internet Control Message Protocol

No. Time Source Destination Protocol Length Info

174 61.776216 128.119.245.12 192.168.1.2 ICMP 562 Echo (ping) reply id=0x0001, seq=51/13056, ttl=49 (request in 172)

Frame 174: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{04A418C6-E72D-4DC5-8B1A-21EC1CC49F79}, id 0

Ethernet II, Src: ASUSTekC_dc:ce:a0 (e0:cb:4e:dc:ce:a0), Dst: Chongqin_d9:c0:f7 (ac:d5:64:d9:c0:f7)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.2

0100 .... = Version: 4

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

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

Total Length: 548

Identification: 0x0e3a (3642)

Flags: 0x00b9

Fragment offset: 1480

Time to live: 49

Protocol: ICMP (1)

Header checksum: 0x41b8 [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 192.168.1.2

[2 IPv4 Fragments (2008 bytes): #173(1480), #174(528)]

Internet Control Message Protocol

Контрольні запитання:

1. Визначте IP адреси вашої та цільової робочих станцій.

IP адреси:
Моя: 192.168.1.2
Цільова: 128.119.245.12.

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

144

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
2008 bytes – payload.

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?

[2 IPv4 Fragments (2008 bytes): #143(1480), #144(528)]
Fragmen offset: 1480
2 фрагмент

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

Flags: More Fragments

6. Як поля протоколу IP відрізняють перший фрагмент від другого?

Фрагменти відрізняються Flags- у кожного фрагменту він різний.

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

Завжди змінюється поле Identification.

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

Щоб розрізняти пакети

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

Кожного разу додається одиниця

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

Id = 0x6838
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?

Id змінюється, ttl ні

Висновок

В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи IP та було проведено аналіз деталей роботи даних протоколів.