

Науково-навчальний комплекс
“Інститут прикладного системного аналізу”
Національного технічного університету України "КПІ"
Кафедра математичних методів системного аналізу

Лабораторна робота № 4.
Протокол ІСМР

Виконала
студентка 3-го курсу
групи КА-73
Шаварська М.Ю.

Перевірів
Кухарєв С.О.

Київ-2020

DUMP 1

Microsoft Windows [Version 10.0.18362.778]

(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

C:\Users\User>ping -n 10 www.ust.hk

Обмен пакетами с www.ust.hk [143.89.14.1] с

32 байтами данных: Превышен интервал ожидания для запроса.

Превышен интервал ожидания для запроса. Превышен

интервал ожидания для

запроса. Превышен интервал

ожидания для запроса.

Превышен интервал ожидания

для запроса. Превышен

интервал ожидания для

запроса. Превышен интервал

ожидания для запроса.

Превышен интервал ожидания

для запроса. Превышен

интервал ожидания для

запроса. Превышен интервал

ожидания для запроса.

Статистика Ping для 143.89.14.1:

Пакетов: отправлено = 10, получено =

0, потеряно = 10 (100% потерь)

C:\Users\User>

Контрольні запитання:

1. Які IP адреси вашої та цільової робочих станцій?

Моя: 192.168.43.22 Цільова: 143.89.14.1

2. Чому ICMP пакет не вказує/використовує номери вихідного та цільового портів?

ICMP пакети не мають номери цільового та вихідного портів, тому що вони

були розроблені для обміну інформації на мережевому рівні між хостами та

маршрутизаторами, а не для обміну між процесами на прикладному рівні.

Кожен пакет має поля Тип та Код, комбінація яких визначає кожне конкретне

повідомлення. Оскільки мережеве програмне забезпечення самостійно інтерпретує всі ICMP повідомлення, номери портів не потрібні. Він користується адресами робочих станцій.

3. Дослідіть один з пакетів-запитів ICMP. Які тип та код зазначені у цьому пакеті?

Скільки байтів займають поля контрольної суми, номери послідовності та ідентифікатору?

32 байти 4. Дослідіть відповідний пакет з відповіддю на пакет із пункту 3.

Які тип та код

зазначені у цьому пакеті? Які інші поля має цей пакет? Скільки байтів займають поля

контрольної суми, номери послідовності та ідентифікатору? DUMP 2

C:\Users\User>tracert www.inria.fr

Трассировка маршрута к inria-cms.inria.fr [128.93.162.63]

с максимальным числом прыжков 30:

1 6 ms 4 ms 4 ms 192.168.43.1

2 * * * Превышен интервал ожидания для запроса.

3 45 ms 29 ms 29 ms 88-214-103-193.vf-ua.net [88.214.103.193]

4 23 ms 26 ms 26 ms 88-214-102-192.vf-ua.net [88.214.102.192]

5 24 ms 25 ms 23 ms 172.17.10.1

6 39 ms 69 ms 37 ms ip4.gtt.net [213.254.224.166]

7 40 ms 43 ms 40 ms ae0-1983.cr0-waw3.ip4.gtt.net [213.254.224.165]

8 75 ms 71 ms 67 ms et-3-3-0.cr4-par7.ip4.gtt.net [213.200.119.214]

9 67 ms 67 ms 68 ms renater-gw-ix1.gtt.net [77.67.123.206]

10 70 ms 67 ms 72 ms tel-1-inria-rtr-021.noc.renater.fr [193.51.177.107]

11 70 ms 74 ms 72 ms inria-rocquencourt-tel-4-inria-rtr-021.noc.renater.fr [193.51.184.177]

12 69 ms 69 ms 69 ms unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]

13 72 ms 71 ms 80 ms inria-cms.inria.fr [128.93.162.63]

Трассировка завершена.

C:\Users\User>5. Які IP адреси вашої та цільової робочих станцій?

Моя - 192.168.43.32, цільова - 128.93.162.84

6. Який номер протоколу IP використовується програмою?

Protocol: ICMP (1)

7. Чи відрізняється пакет із запитом програми traceroute від пакету із запитом

програми

ping? Якщо так, наведіть приклади.

Тільки розміром повідомлення.

8. Проаналізуйте пакет ICMP з повідомленням про помилку. Чи є у ньому деякі

додаткові поля, які не зазначаються у повідомленні з підтвердженням.

Якщо є –

які

саме поля і яку інформацію вони вміщують?

Пакет помилки ICMP не такий же, як і пінговий запит. В ньому також знаходяться заголовки IP та 8 байтовий оригінальний пакет помилки ICMP.

9. Проаналізуйте три останні відповіді протоколу ICMP, які отримала ваша

робоча

станція. Як ці пакети відрізняються від пакетів з повідомленням про помилку?

Чому

вони відрізняються? Останні три пакети – це пакети повідомлення, вони мають тип 0 (echo

reply), а не 11 (TTL expired). Це значить, що датаграми дійшли до цільового призначення. Також там є пакет про помилку (Port unreachable), що свідчить про кінець роботи утиліти tracert.

10. Знайдіть етап ретрансляції повідомлень з найбільшою середньою затримкою. Чи є

можливість оцінити географічну відстань між маршрутизаторами на цьому

етапі?

В середньому – найбільша затримка між кроками 5 та 6 (~20 мс). Це є зв'язок між Україною та Францією (2200 км).

Висновки

Були отримані навички захоплення пакетів і аналізу даних, а також аналіз роботи протоколу ICMP.