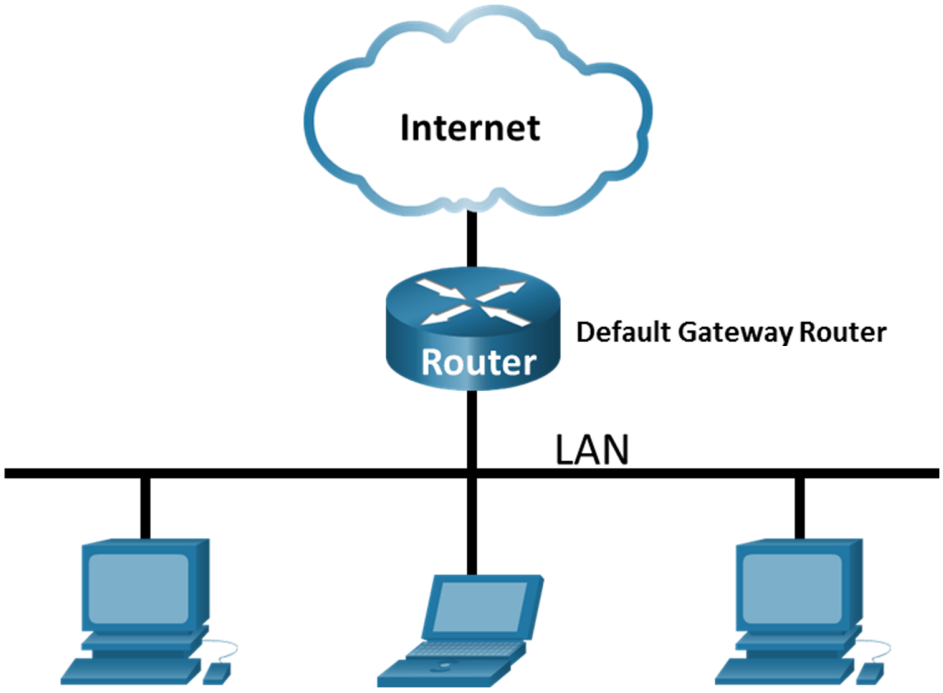
Лабораторна робота - Використання Wireshark для перегляду мережного трафіку

Топологія



Цілі та задачі

Частина 1: Перехоплення та аналіз локальних ICMP-даних за допомогою Wireshark

Частина 2: Перехоплення та аналіз віддалених ICMP-даних за допомогою Wireshark

Довідкова інформація / Сценарій

Wireshark - це програмний аналізатор протоколів або програма "пакетний сніфер", яка використовується для пошуку та усунення несправностей мережі, аналізу повідомлень, розробки програм та протоколів, а також для навчання. Під час передачі даних через мережу, сніфер "захоплює" кожен протокольний блок даних (PDU) і може декодувати та аналізувати його вміст згідно з відповідними RFC або іншими специфікаціями.

Wireshark є корисним інструментом для всіх, хто працює з мережами, і його можна використовувати в більшості лабораторних робіт у курсах CCNA для аналізу даних, пошуку та усунення несправностей У цій лабораторній роботі Ви будете використовувати Wireshark для перехоплення IP-адрес з ICMP-повідомлення та MAC-адрес з Ethernet-кадра.

Необхідні ресурси

- 1 ПК з ОС Windows та доступом до мережі Інтернет
- Додаткові ПК в локальній мережі будуть використовуватись для відповідей на ping-запити.

Інструкції

Частина 1: Перехоплення та аналіз локальних ICMP-даних за допомогою Wireshark

У Частині 1 цієї лабораторної роботи Ви перевірите зв'язок з іншим ПК локальній мережі за допомогою команди ping та перехопите згенеровані ICMP-запити та ICMP-відповіді, використовуючи Wireshark. Ви також розглянете вміст перехоплених кадрів для отримання певної інформації. Цей аналіз має допомогти Вам з'ясувати, як заголовки повідомлень використовуються для транспортування даних до місця призначення.

Крок 1: Визначення адрес мережної плати Вашого ПК.

В цій лабораторній роботі Вам необхідно визначити логічну та фізичну адреси, тобто IP-адресу та MAC-адресу мережної плати/інтерфейсу Вашого ПК.

a. У командному рядку введіть команду **ipconfig /all**, щоб переглянути IP-адресу, MAC-адресу, опис мережної плати Вашого ПК.

```
C:\Users\Student> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-NB48BTC
   Primary Dns Suffix . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . :00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
<output omitted>
```

b. Запитайте члена або членів команди про IP-адресу їх ПК та надайте їм IP-адресу свого ПК. На цьому етапі не повідомляйте їм свою MAC-адресу.

Крок 2: Запуск Wireshark і початок перехоплення даних.

a. Перейдіть до Wireshark. Двічі натисніть на потрібному інтерфейсі, щоб розпочати перехоплення повідомлень. Переконайтеся, що на потрібний інтерфейс надходить трафік.

b. У верхній частині вікна Wireshark рядки даних почнуть прокручуватися донизу. Рядки даних, залежно від протоколу, матимуть різне забарвлення.

   Вони можуть прокручуватися дуже швидко. Швидкість залежатиме від інтенсивності спілкування, яке зараз відбувається між Вашим ПК та іншими вузлами локальної мережі. Для полегшення перегляду даних, які перехоплює Wireshark, та подальшого їх опрацювання можна застосувати фільтри.

   У цій лабораторній роботі нас цікавить відображення лише повідомлень протоколу ICMP (ping). Наберіть **icmp** у полі **Filter** у верхній частині вікна Wireshark і натисніть або **Enter,** або кнопку **Apply** (значок стрілочки), щоб переглядати тільки ICMP-повідомлення.

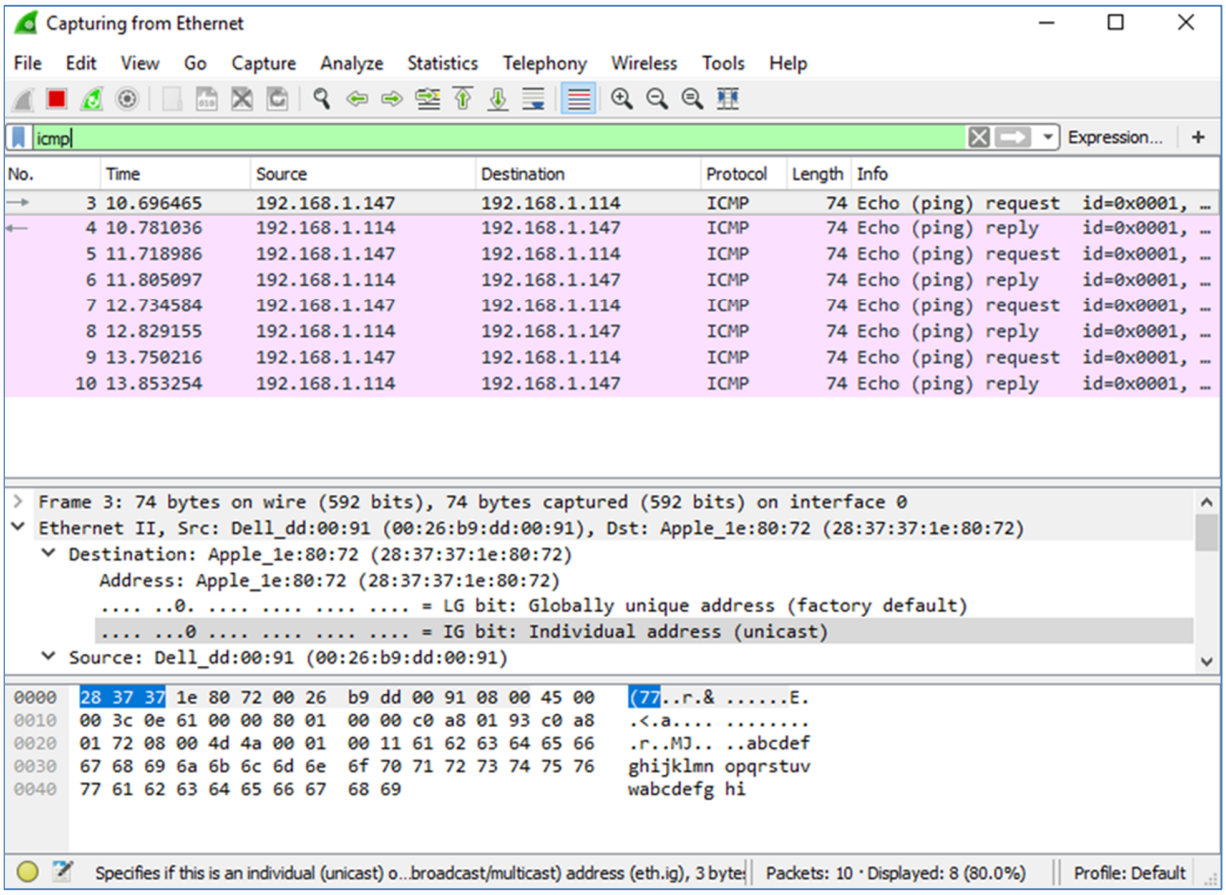
c. Як наслідок застосування цього фільтру всі дані у верхній частині вікна зникнуть, але процес перехоплення трафіку на мережній платі/інтерфейсі продовжується. Перейдіть до вікна командного рядка та пропінгуйте IP-адресу, надану членом Вашої команди.

```
C:\> ping 192.168.1.114

Pinging 192.168.1.114 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Зверніть увагу на те, що дані знову з'являються у верхній частині вікна Wireshark.



Примітка: Якщо ПК члена Вашої команди не відповідає на Ваші ping-запити, причиною може бути блокування цих запитів його міжмережним екраном. Будь ласка, в Додаток А: Дозвіл передачі ICMP-трафіку через міжмережний екран ОС Windows знайдіть і перегляньте інформацію про те, як дозволити передачу ICMP-трафіку через міжмережний екран в ОС Windows.

d. Зупиніть перехоплення даних, натиснувши значок **Stop Capture**.

Крок 3: Дослідження перехоплених даних.

На Кроці 3 виконується перегляд даних, які були згенеровані ping-запитами ПК члена Вашої команди. Дані Wireshark відображаються у трьох секціях: 1) у верхній секції відображається перелік перехоплених кадрів з узагальненням даних IP-пакета; 2) у середній секції відображаються дані кадру, вибраного у верхній частині екрана і перехоплений кадр розділяється на підсекції відповідно до протокольних рівнів; 3) нижня секція відображає необроблені дані кожного рівня. Необроблені дані відображаються як у шістнадцятковій, так і у десятковій формах.

a. У верхній частині вікна Wireshark натисніть на кадр, що містить перший ICMP-запит. Зауважте, що стовпчик **Source** містить IP-адресу Вашого ПК, а стовпчик **Destination** містить IP-адресу ПК Вашого колеги по команді (саме того ПК, який Ви пінгували).

b. Якщо цей кадр все ще вибраний, перейдіть до середньої частини. Натисніть на значок стрілки ліворуч від рядка Ethernet II, щоб переглянути MAC-адреси отримувача та відправника кадру.

Чи співпадає MAC-адреса відправника з MAC-адресою мережної плати/інтерфейсу Вашого ПК?

Чи відповідає у Wireshark MAC-адреса отримувача MAC-адресі ПК Вашого колеги по команді?

Як Ваш ПК отримав MAC-адресу пропінгованого ПК?

Примітка: У попередньому прикладі із перехоплення ICMP-запиту, дані протоколу ICMP інкапсулюються в IPv4-пакет (додається заголовок IPv4), який потім інкапсулюється у кадр Ethernet II (додаються заголовок та трейлер - контрольна сума Ethernet II) для передачі через локальну мережу.

Частина 2: Перехоплення та аналіз віддалених ICMP-даних за допомогою Wireshark

У Частині 2 цієї лабораторної роботи Ви за допомогою команди ping перевірите зв'язок з віддаленими вузлами (вузлами, які не належать до Вашої локальної мережі) та дослідите отримані дані. Потім Ви маєте визначити чим відрізняються ці дані від даних, які досліджувалися у Частині 1.

Крок 1: Початок перехоплення даних на мережній платі/інтерфейсі.

a. Розпочніть перехоплення даних знову.

b. Wireshark запропонує Вам зберегти раніше перехоплені дані перед початком іншого перехоплення. Зберігати ці дані не обов'язково. Натисніть **Continue without Saving**.

c. Після активізації перехоплення у командному рядку Windows виконайте команду ping для таких трьох URL-адрес веб-сайтів:

1) www.yahoo.com
2) www.cisco.com
3) www.google.com

Примітка: Коли Ви пінгуєте перелічені URL-адреси, зауважте, що DNS-сервер транслює ці URL в IP-адреси. Зверніть увагу на IP-адреси, отримані для кожної URL-адреси.

d. Ви можете зупинити перехоплення даних, натиснувши **Stop Capture**.

Крок 2: Дослідіть та проаналізуйте дані з віддалених вузлів.

Перегляньте перехоплені дані в Wireshark та дослідіть IP-адреси та MAC-адреси трьох веб-сайтів, з якими Ви перевіряли зв'язок. Запишіть IP-адреси та MAC-адреси отримувачів для трьох веб-сайтів, з якими Ви перевіряли зв'язок.

IP-адреса для **www.yahoo.com**:

MAC-адреса для **www.yahoo.com**:

IP-адреса для **www.cisco.com**:

MAC-адреса для **www.cisco.com**:

IP-адреса для **www.google.com**:

MAC-адреса для **www.google.com**:

Що важливе в цій інформації?

Чим ця інформація відрізняється від інформації, яку Ви отримали в Частині 1?

Питання для самоперевірки

Чому Wireshark показує реальні MAC-адреси вузлів локальної мережі, але не показує реальні MAC-адреси вузлів віддалених мереж?

Додаток A: Дозвіл передачі ICMP-трафіку через міжмережний екран ОС Windows

Якщо члени Вашої команди не можуть виконати ping-запити до Вашого ПК, ймовірно саме міжмережний екран блокує ці запити. У цьому додатку наведено опис створення правила на міжмережному екрані, яке дозволяє виконання ping-запитів. Також наведено опис відключення створеного ICMP-правила після завершення виконання лабораторної роботи.

Частина 1: Створення нового вхідного правила, яке дозволить ICMP-трафіку пройти через міжмережний екран.

a. Перейдіть до **Control Panel** і натисніть опцію **System and Security** в Category view.

b. У вікні **System and Security**, натисніть **Windows Defender Firewall** або **Windows Firewall**.

c. На лівій панелі **Windows Defender Firewall** або вікна **Windows Firewall** натисніть **Advanced settings**.

d. У вікні **Advanced Security** на лівій бічній панелі виберіть опцію **Inbound Rules** і потім натисніть **New Rule…** на правій бічній панелі.

e. Запустіть **New Inbound Rule Wizard**. У вікні **Rule Type** спочатку натисніть кнопку **Custom**, а потім – кнопку **Next**.

f. На лівій панелі вікна виберіть параметр **Protocol and Ports** і, використовуючи спадне меню **Protocol Type**, виберіть **ICMPv4**, а потім натисніть **Next**.

g. Переконайтесь, що як для локальних так і для віддалених адрес вибрано **Any IP address**. Натисніть **Next**, щоб продовжити.

h. Виберіть **Allow the connection**. Натисніть **Next**, щоб продовжити.

i. За замовчуванням це правило застосовується для всіх профілів ОС. Натисніть **Next**, щоб продовжити.

j. Задайте назву правила **Allow ICMP Requests**. Натисніть **Finish** щоб завершити. Це нове правило дозволить членам Вашої команди отримувати від Вашого ПК відповіді на їх ping-запити.

Частина 2: Вимкнення або видалення ICMP-правила.

Після завершення лабораторної роботи Ви можете вимкнути або навіть видалити правило, створене на Кроці 1. Для вимкнення правила використовуйте параметр **Disable Rule**, це дозволить Вам пізніше увімкнути правило знову. Видалення правила повністю видаляє його зі списку вхідних правил.

a. У вікні **Advanced Security** натисніть **Inbound Rules** на лівій бічній панелі та знайдіть правило, створене Вами раніше.

b. Правою кнопкою миші виберіть ICMP-правило і виберіть **Disable Rule**, якщо Ви вирішили його відключити. Ви також можете вибрати **Delete**, якщо Ви вирішили видалити правило назавжди. Якщо Ви вибрали цей варіант, то потім доведеться знову створювати правило, якщо буде потрібно дозволити надсилати ICMP-відповіді.