ЛАБОРАТОРНА РОБОТА 2

Тема: Аналізатор мережевих пакетів Wireshark. Захват та аналіз мережевих кадрів

Мета: За допомогою аналізатора вивчити структуру та типи кадрів у комп’ютерній мережі

1. Теоретична частина

Аналізатори мережевих протоколів (англ. – sniffer) відносяться до категорії засобів, які є необхідними адміністратору мережі для визначення та аналізу подій, що відбуваються в мережі. Робота аналізаторів базується на використанні так званого "нерозбірливого" (promiscuous) режиму роботи адаптеру мережевого інтерфейсу. У цьому режимі кадри, які пересилаються мережею, буферизуються мережевим адаптером і, незалежно від MAC-адреси призначення, аналізуються. Крім цієї основної функції аналізатори збирають та визначають у реальному часі завантаження мережі та окремих робочих станцій, ведуть статистику використання мережевих протоколів, визначають розподіл кадрів та пакетів за розміром тощо.

Одним з найпопулярніших аналізаторів кадрів та пакетів у комп’ютерній мережі є Wireshark. Аналізатор Wireshark дозволяє виконувати захват кадрів з мережі, до якої комп’ютер підключено та проводити детальний аналіз його вмісту. Як правило аналізатор використовується:

- для рішення проблем із мережею;
- для оцінки рівня мережної безпеки;
- для вивчення мережевих протоколів та виявлення хибного їх використання;
- для діагностування роботи мережевого програмного забезпечення, що розробляється;
- для виявлення типів протоколів, що використовуються в локальній мережі;
- для виявлення прихованого мережевого трафіку.

Основними відмінностями Wireshark є:

кросплатформова реалізація;
захоплення кадрів та пакетів, що надходять до мережевого адаптеру;
повна деталізація інформації про протоколи, що використано у пакетах;
збереження даних пакету, який було захоплено, та можливість подальшого аналізу цих даних;
імпортування та експортування пакетів у різні відомі формати для інших програм-аналізаторів;
фільтрування пакетів за багатьма критеріями;
пошук пакетів за багатьма критеріями;

забарвлення рядків із захопленими пакетами відповідно до фільтрів;
створення різноманітних статистик;
та інше.

Захоплення кадрів можна виконати через меню Capture–Options або за допомогою команд Capture-Start та Capture-Stop. Через вкладку Options можна зробити додаткові налаштування, щодо процесу захоплення та показу захоплених даних під час його виконання.

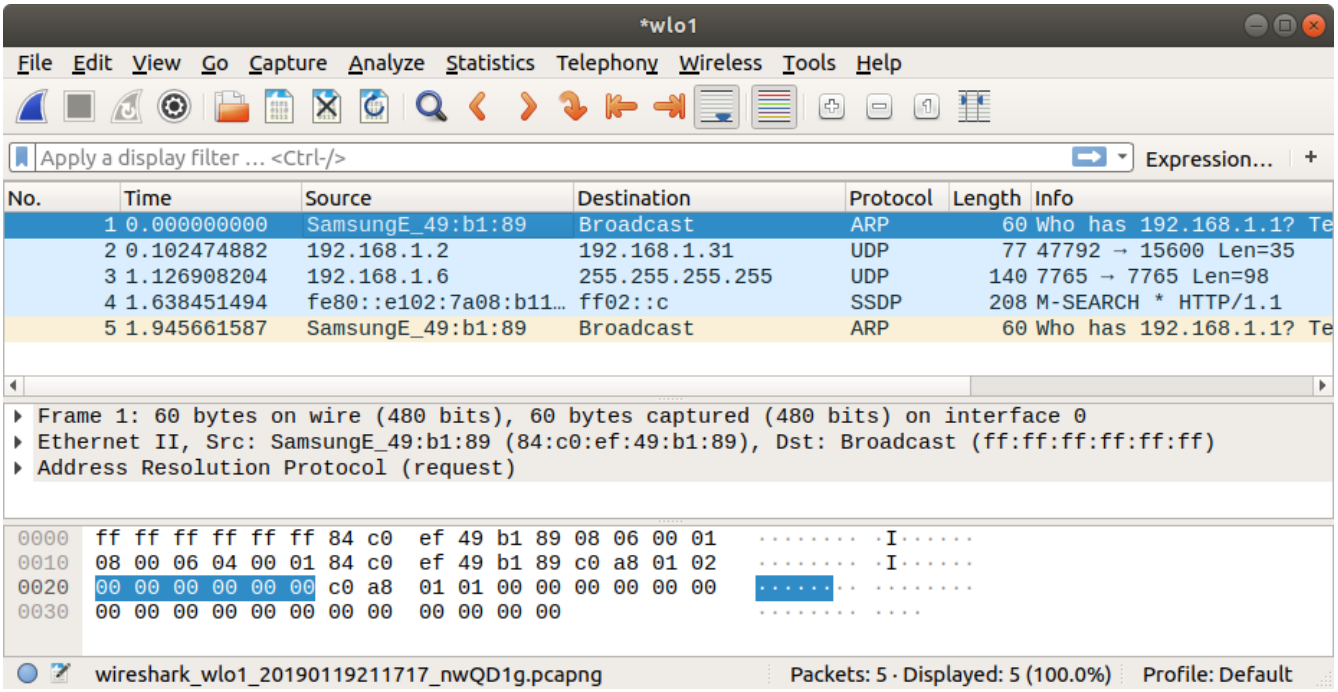


Рис. 1. Wireshark дозволяє захопити мережевий кадр та виконати аналіз його вмісту

У верхній частині вікна аналізатору Wireshark показуються захоплені кадри з мережі з вказівкою їх основних параметрів: мережевої адреси відправника та отримувача, типу кадру, довжини у байтах, часу отримання після початку процесу захоплення. У центральній частині показується ієрархічна структура мережевих протоколів, що використовуються на відповідних рівнях передавання даних. Якщо розгорнути певний рівень, то можна побачити опис полів його заголовку. У нижній частині вікна - шістнадцятирічний дамп кадру (байти кадру, які представлено у шістнадцятирічному форматі).

Адреса відправника та отримувача у кадрі Ethernet зазвичай мають довжину 6 байтів. У MAC-адресі молодший біт першого байту є ознакою індивідуальної або групової адреси: 0 - вказує на певну станцію, 1 - вказує на групову адресу декількох станцій мережі. При широкомовній адресації усі біти адреси встановлюються в 1. Адреса отримувача може бути як індивідуальною, так і груповою або широкомовною. Відправник може мати лише індивідуальну адресу, тобто молодший біт першого байта його адреси завжди має значення 0. Другий біт

вказує на унікальність адреси у глобальному сенсі: 0 — унікальний глобально; 1 — унікальний у межах локальної мережі. Перші 3 байти (за порядком їх передавання у мережі та традиційному запису MAC-адреси) є унікальним ідентифікатором організації (OUI), які реєстраційна адміністрація IEEE надає виробникам мережевого обладнання. Останні 3 байти (на рис.1 це 4, 5 та 6 байти) призначаються виробником для кожного виготовленого екземпляру пристрою і тому забезпечують повну унікальність усієї MAC-адреси.

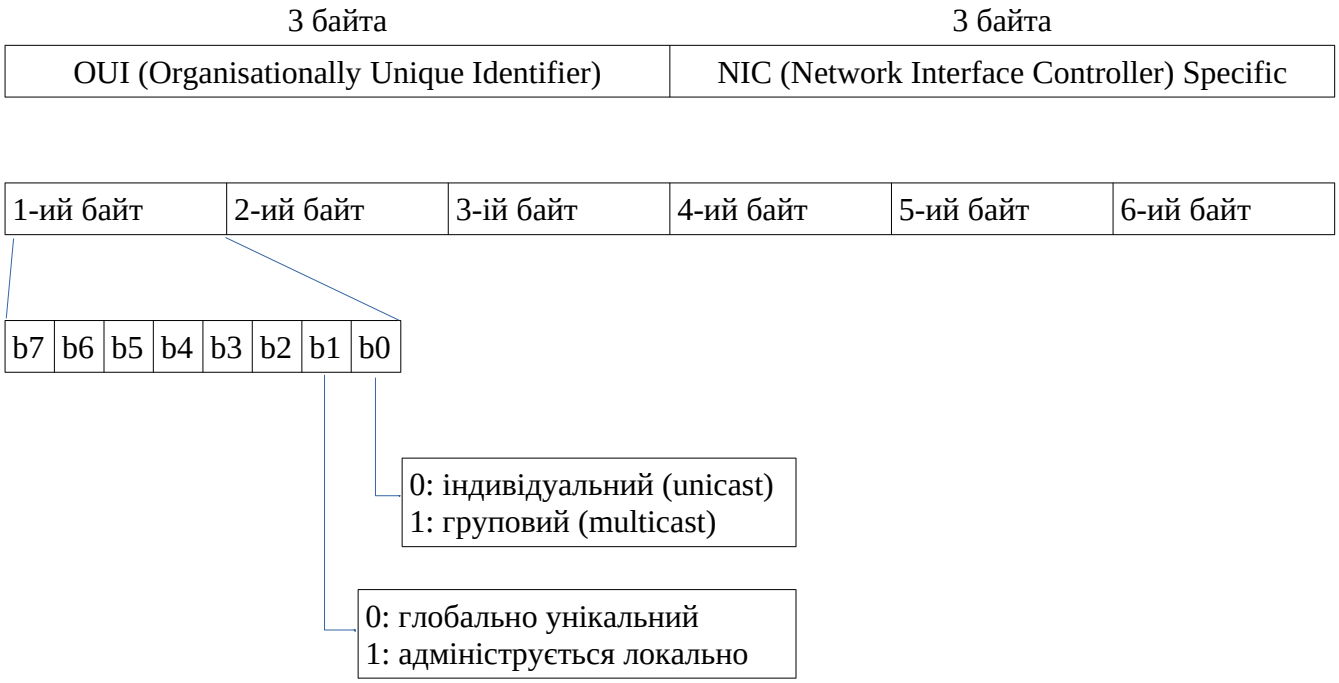


Рис.1. Структура MAC-адреси у канонічному форматі

На практиці у комп’ютерній мережі на канальному рівні зустрічаються 4 типи кадрів Ethernet (рис.2), що обумовлено тривалою історією розвитку технологій до прийняття стандартів IEEE 802. Практично усе мережеве обладнання вміє може працювати з цими форматами кадрів.

Кадр **Ethernet DIX** (або кадр Ethernet II) визначає наступні поля заголовку:

− адреса отримувача - 6 байтів (MAC-адреса отримувача);

− адреса відправника - 6 байтів (MAC-адреса мережевого інтерфейсу, з якого відправлено кадр);

− тип протоколу (поле Type), що вказує на мережевий протокол верхнього рівня, який використовує поле даних кадру для передачі свого пакету. Для позначення типу протоколу використовуються значення, що перевищують значення максимальної довжини поля даних кадру (1500 байт) для забезпечення відмінності кадрів Ethernet DIX від інших типів;

− кадр може вміщувати не більше 1500 байт даних, але якщо даних передається менш 46 байт, то поле даних заповнюється байтами з 0 значенням до

мінімально припустимої довжини. Загальна довжина мінімального за розміром кадру складає 7+1+6+6+2+46+4=72 байта = 576 біт. Такий мінімальний розмір був вимушений для забезпечення коректної роботи механізму виявлення колізій на початку розвитку технологій Ethernet;

− поле контрольної суми (4 байти) має значення, що обчислюється за алгоритмом CRC-32 та призначене для виявлення цільності кадру на стороні отримувача. Якщо значення цього поля переданого кадру не буде збігатись з обчисленим на стороні отримувача, то такий кадр буде проігноровано, якщо не задано іншого механізму.

Кадр 802.3/LLC (або кадр 802.3/802.2) має заголовок, який є результатом поєднання заголовків кадрів, визначених стандартами 802.3 та 802.2. Відповідно до стандарту 802.2 в поле даних кадру 802.3 (MAC-підревнь) вкладається кадр підрівня LLC з видаленими прапорцями початку та кінця кадру. Поля DSAP та SSAP дозволяють вказати на сервіс верхнього рівня, що пересилає данні за допомогою цього кадру. Зазвичай ці поля мають одинакові значення. Поле управління використовується для позначення типу кадру даних — інформаційний, кадр управління або ненумерований (зазвичай в Ethernet використовуються ненумеровані кадри). На відмінність від формату Ethernet DIX двобайтове поле довжини вказує довжину поля даних, яке не може перевищувати 1500 байтів. Тому що кадр LLC додає до заголовку 3 байти, то максимальний розмір поля даних зменшується до 1497 байт.

Кадр 802.3

6	6	2	46-1500	4
DA	SA	L	Data	FCS

Кадр 802.3/LLC

6	6	2	1	1	1	43-1497	4
DA	SA	L	DSAP	SSAP	Control	Data	FCS
			Заголовок LLC				

Кадр Ethernet DIX (II)

6	6	2	46-1500	4
DA	SA	T	Data	FCS

Кадр Ethernet SNAP

6	6	2	1	1	1	3	2	38-1492	4
DA	SA	L	DSAP	SSAP	Control	OUI	T	Data	FCS
			AAh	AAh	03h	000000			
			Заголовок LLC			Заголовок SNAP			

Рис. 2. Формати кадрів Ethernet. DA – MAC-адреса отримувача, SA – MAC-адреса відправника, T – поле, що вказує тип протоколу верхнього рівня, L – довжина полю даних, FCS – поле контрольної суми (CRC-код).

Кадр **Raw 802.3** (або кадр Novell 802.3). У ранніх версіях операційної системи NetWare її розробник фірма Novell проігнорувала вимогу щодо розміщення LLC кадру у кадр 802.3. Безпосередньо за заголовком кадру 802.3 вони розташовували IPX-пакет, який починається з FFFFh ідентифікатору кадру цього типу. Novell тривалий час не використовувала службові поля кадру LLC у своїй операційній системі NetWare, тому що в цьому не було необхідності - у полі даних знаходився пакет протоколу IPX. Операційна система NetWare сьогодні практично не використовується, фірма Novell вже втратила свою самостійність, а підтримка протоколу IPX у світі майже не здійснюється.

Кадр **Ethernet SNAP** (SNAP - SubNetwork Access Protocol, протокол доступу до підмереж). Кадр Ethernet SNAP визначено стандартом 802.2H і він є розширенням кадру 802.3/LLC завдяки введенню додаткового поля ідентифікатора організації OUI, яке також може використовуватись для обмеження доступу до мережі комп'ютерів інших організацій. Додатковий заголовок SNAP використовується для надання більшої впорядкованості при позначені типу протоколу, який розміщує свою інформацію у полі даних кадру LLC. Стандарт 802.2 використовує для цього однобайтові поля DSAP та SSAP (масксимально 256 протоколів). У версії протоколу Ethernet, яку запропонували разом компанії Digital, Intel та Xerox (версія Ethernet DIX), для позначення типу протоколу у полі даних кадру використовується двобайтове поле Type. Для позначення протоколів мережевого рівня використовуються значення вище 05DCh (шістнадцятковий формат), наприклад, 0800 використовується для позначення протоколу IP. Заголовок SNAP також вміщує двобайтове поле Type, призначення та формат якого такі самі як і у поля Type кадру Ethernet DIX. Трьохбайтовий код організації (OUI) використовується для позначення тієї організації по стандартизації, яка відповідає за числові значення поля Type. Так, числові значення поля Type для заголовку SNAP у випадку використання його у кадрі Ethernet визначає комітет 802.3 IEEE, код якого 00 00 00. Для інших протоколів канального рівня значення кодів поля Type визначають інші організації по стандартизації. Таким чином, при використанні додаткового заголовку SNAP досягається сумісність кадрів 802.3 з кадрами Ethernet DIX за методом кодування пакетів протоколів верхнього рівня, які передаються у полі даних. Поля DSAP та SSAP, при використанні заголовку SNAP, отримують значення $170_{(10)}$ = AAh, що вказує на те, що у полі даних кадру LLC знаходиться заголовок SNAP. Поле управління зазвичай має значення 03h, яке вказує на відсутність попереднього з'єднання на канальному рівні.

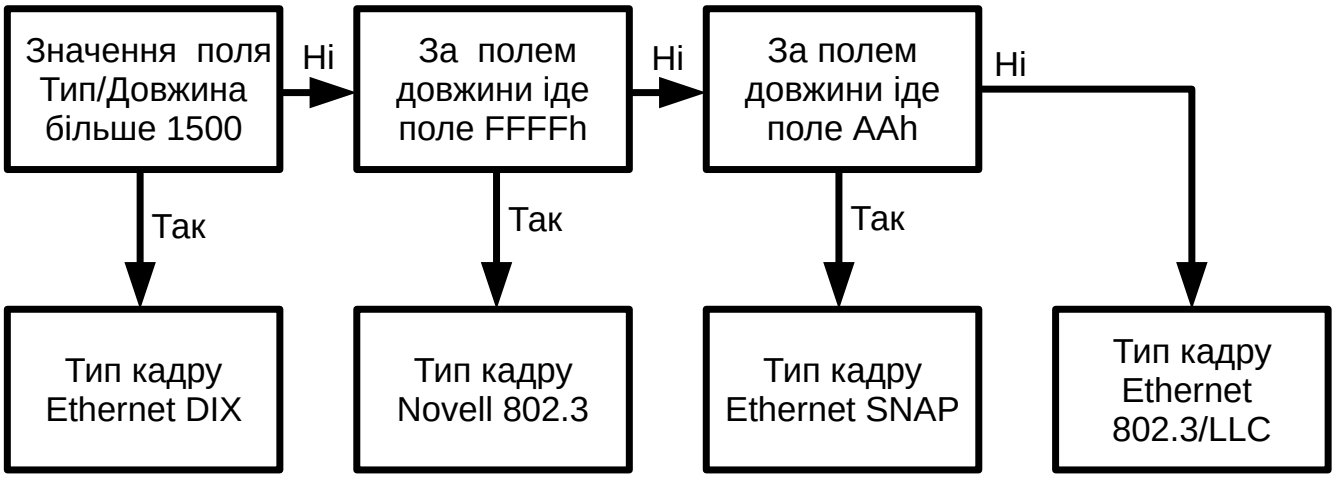
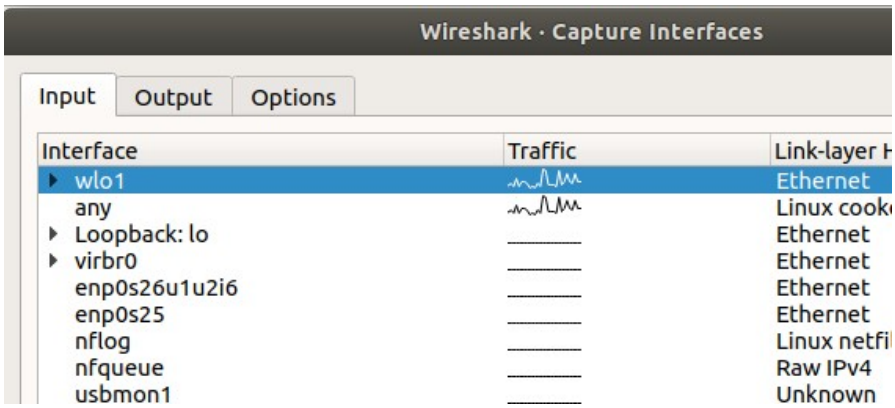


Рис. 3. Алгоритм визначення типу кадру Ethernet

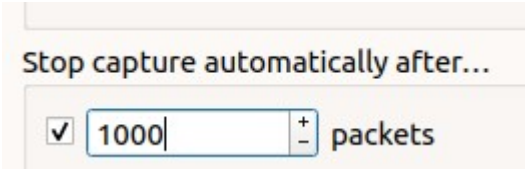
Сучасне мережеве обладнання підтримує усі 4 типи кадрів Ethernet.

Завдання до роботи

1. Запустіть аналізатор Wireshark. Через панель меню оберіть (Capture → Options) або натисніть Ctrl+K.



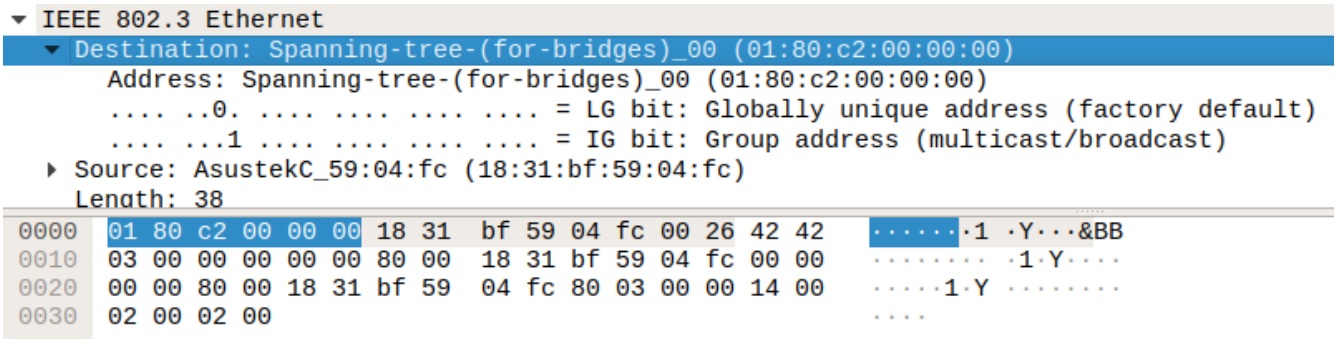
Оберіть вкладку “Options” та задайте автоматичну зупинку захоплення після 1000 кадрів. Натисніть “Start”.



Дочекайтесь захоплення 1000 кадрів і автоматичної зупинки цього процесу.

2. Виконайте статистичний аналіз захоплених кадрів за типом протоколів: Statistics → Protocol Hierarchy. Визначте кількість кадрів за типами: Ethernet DIX; 802.3/LLC; Novell 802.3; Ethernet SNAP.

3. Серед захоплених кадрів знайдіть один кадр Ethernet DIX та один 802.3/LLC. Наведіть для кожного з них бінарний вміст та відповідний до нього аналіз. Для цього використовуйте переміщення у вікнах аналізатору



Аналізатор показує бінарний вміст кадру та відповідне призначення цього поля. Зробіть повний аналіз кожного із двох обраних кадрів, визначте призначення кожного поля та його вміст.

4. На прикладі кадрів з пункту 3 покажіть, що за алгоритмом на рис.3 дійсно можна визначити тип цих кадрів.
5. Визначте які типи MAC-адрес використано у цих кадрах: індивідуальні, групові, широкомовні. Надайте пояснення.
6. Серед захоплених кадрів знайдіть кадр з ARP-пакетом. Наведіть його бінарний вміст та за допомогою аналізатора визначте призначення та вміст кожного його поля. Наведіть, скільки серед захоплених 1000 кадрів вміщувало пакети ARP.
7. Наведіть розподіл кадрів за довжиною. Кадрів якої довжини найбільше? Скільки відсотків кадрів максимальної довжини?
8. Підготуйте звіт, в який внесіть результати 2-7 пунктів.

Контрольні запитання

1. Що позначається терміном sniffer ?
2. До якого типу програмних засобів відноситься Wireshark?
3. У чому особливість режиму роботи “promiscuous” мережевого адаптеру?
4. Які функції виконує аналізатор Wireshark?
5. Яка довжина та структура MAC-адреси?
6. Яку максимальну і яку мінімальну довжину можуть мати Ethernet кадри?
7. Що таке преамбула та який вона має вміст?
8. Скільки і які типи кадрів Ethernet? Чим вони відрізняються?
9. З яких полів складається кадр Ethernet DIX?
10. З яких полів складається кадр Ethernet 802.3/LLC?