ЛАБОРАТОРНА РОБОТА № 4

Тема: Дослідження Ethernet та ARP.

Мета: Дослідити протоколи Ethernet та ARP, використовуючи можливості програми Wireshark.

Час виконання: 2 год.

ХІД РОБОТИ

Теоретичні відомості

Перед тим, як розпочати, перегляньте інформацію про технологію Ethernet, адресацію канального рівня та ARP (частково її подано в дод. 1). RFC 826 (http://www.faqs.org/rfcs/rfc826.html) містить достатньо інформації про протокол ARP, що використовується протоколом IP для визначення MAC адреси віддаленого інтерфейсу, IP адреса якого відома.

Зверніть увагу, що протокол ARP на вашому комп'ютері зазвичай кешує дані трансляції IP адреси в MAC (Ethernet) адресу. Команда **arp** (як у Windows, так і у Linux / Unix) використовується для перегляду і управління вмістом цього кеша. Оскільки команда **arp** і протокол ARP мають одне і те ж ім'я, їх легко переплутати. Але майте на увазі, що вони різні – arp використовується для перегляду та керування вмістом ARP кеша, в той час як протокол ARP визначає формат і зміст повідомлень, що відправляються і одержуються, а також визначає заходи з передачі повідомлень та їх отримання.

Виконувані файли для команди **arp** розміщені:
Windows: `C:\Windows\system32` або `C:\Windows\system32\arp`.
Linux / Unix: виконуваний файл може бути в різних місцях. Популярні місця `/sbin/arp` (для Linux) і `/usr/sbin/arp` (для деяких варіантів Unix).

Щоб дослідити відправлення і отримання повідомлень ARP, ми повинні очистити ARP кеш, оскільки в іншому випадку комп'ютер може знайти потрібні IP-Ethernet адреси в своєму кеші і, отже, не буде надсилати ARP запити. Команда **`arp -d *`** очистить кеш ARP. Прапорець **`-d`** вказує на операцію видалення, а зірочка (**`*`**) є шаблоном, що говорить; видалити всі записи в таблиці. У Linux / Unix для виконання команда **`arp -d *`** потрібно мати права привілейованого користувача (root або входити в число sudoers).

Завдання

Перехоплення і аналіз кадрів Ethernet

Розпочнемо перехоплення кадрів Ethernet. Виконайте таке:

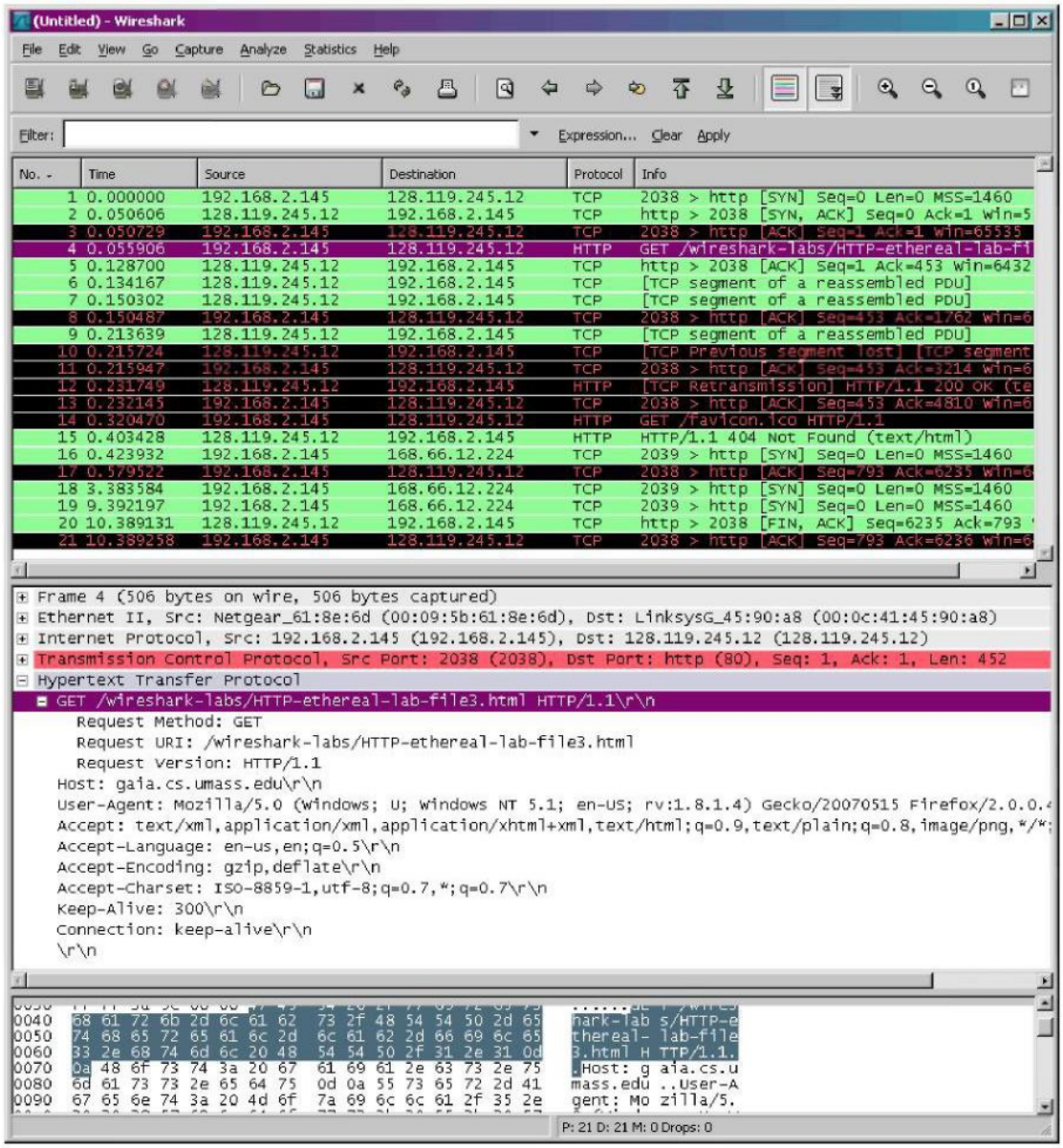
1. Впевніться, шо кеш вашого браузера пустий.
   Firefox: Приватність і безпека → Куки і дані сайтів → Стерти дані...

Chrome: Розширені → Конфіденційність і безпека → Очистити дані веб-перегляду

2. Запустіть Wireshark і розпочніть захоплення пакетів.

3. Введіть наступний URL в вашому браузері: `http://10.25.0.1/`

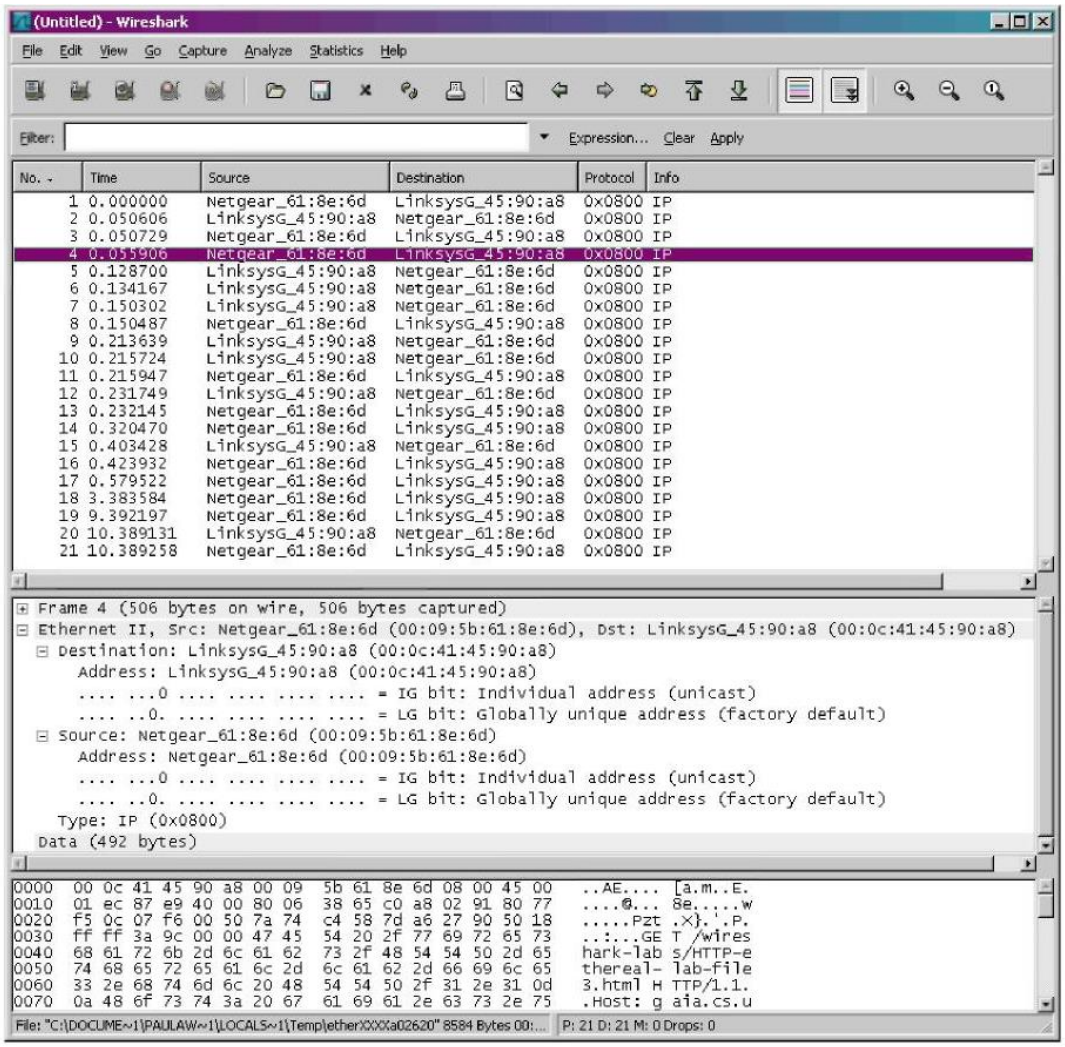
4. Зупиніть перехоплення пакетів. Спочатку знайдіть номери пакетів запитів HTTP GET, що були надіслані з вашого комп'ютера на 10.25.0.1, потім HTTP повідомлення-відповіді, що були надіслані на ваш комп'ютер сервером 10.25.0.1. Ви маєте побачити щось схоже на рисунок нижче (пакет 4 на скріншоті містить повідомлення HTTP GET)



5. Оскільки ми досліджуємо Ethernet і ARP, ми не будемо аналізувати IP та протоколи верхніх рівнів. Тому треба змінити фільтр перехоплених пакетів так, щоб він показував інформацію лише протоколів нижчих по відношенню до IP рівнів. Для цього виберіть Analyze → Enabled Protocols. Потім зніміть прапорець з IP і натисніть OK. Тепер ви повинні побачити

вікно Wireshark, що виглядає приблизно так, як на рисунку 16 (конкретний зміст рядків у вікні залежить від типів і моделей мережних адаптерів і мережного обладнання).

6. Виберіть Ethernet кадр, що містить повідомлення HTTP GET. Розкрийте інформацію Ethernet в головному вікні. Зверніть увагу, що вміст кадру Ethernet (заголовок, а також дані кадру) відображаються у вікні змісту пакета.



Нагадаємо, що у відповідності до моделі взаємодії відкритих систем і стеку TCP/IP повідомлення HTTP GET міститься всередині сегмента TCP, який розміщений в дейтаграмі IP, яка в свою чергу перебуває всередині кадру Ethernet.

7. Проаналізуйте дані пакету. Дайте відповідь на контрольні запитання 1 – 5, які базуються на перехоплених кадрах Ethernet, що містять **повідомлення HTTP GET**. (Корисно буде скористатися можливістю Wireshark друкувати пакети. Для цього в File → Print оберіть Selected packet only).

8. Далі дайте відповіді на контрольні запитання 6 – 10, що базуються на даних кадрів Ethernet, які містять **HTTP відповіді**.

Спостереження за ARP в дії

Тепер ми будемо розглядати протокол ARP.

1. Виконайте команду **arp**.

2. Запишіть вміст ARP-кешу комп'ютера. У чому полягає значення кожного стовпця?

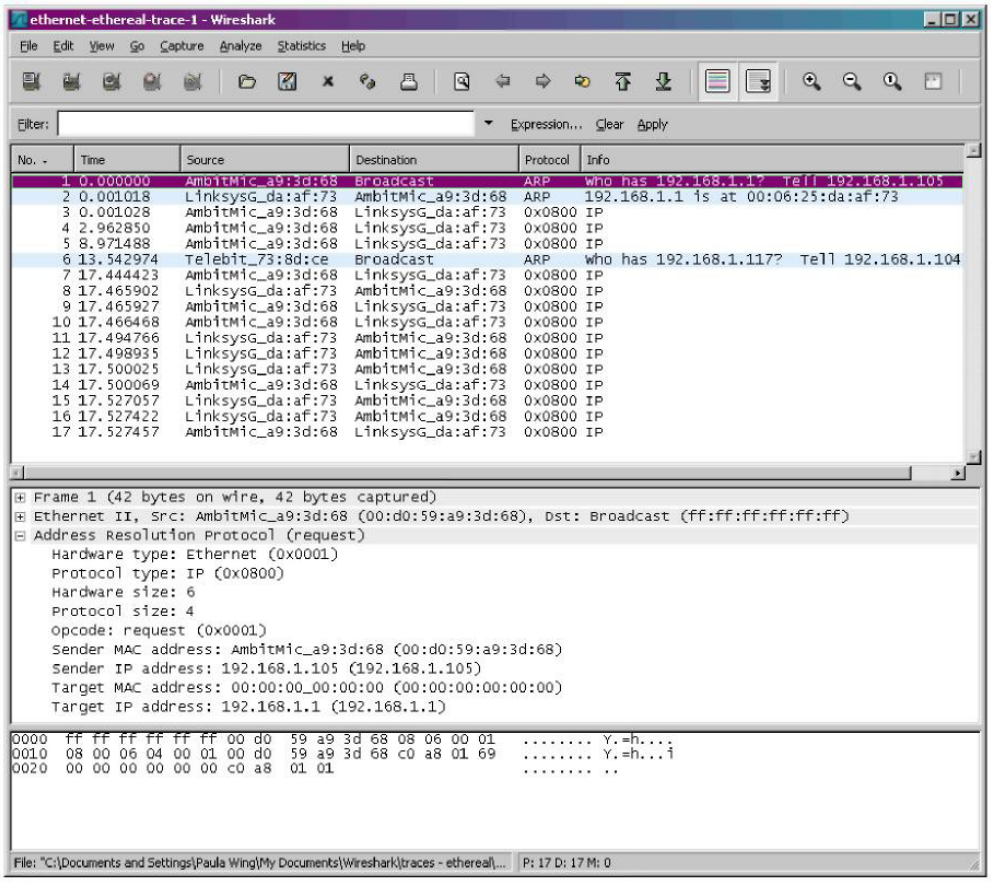
3. Очистіть кеш ARP, як описано вище.

4. Переконайтеся, що кеш браузера порожній.

5. Запустіть сніфер пакетів Wireshark

6. Введіть наступний URL в рядок адрес браузера: `http://10.25.0.1`

7. Зупиніть перехоплення пакетів. Зараз ми не зацікавлені в аналізі заголовків IP та інших протоколів верхніх рівнів, тому відповідно до цього змініть налаштування Wireshark, як ми це вже робили раніше.



У прикладі, наведеному на рисунку, перші два кадри містять ARP повідомлення.

8. Дослідіть захоплені пакети ARP. Дайте відповіді на контрольні запитання 11 – 14.

Контрольні запитання

1. Якою є 48-бітна MAC-адреса Вашого комп'ютера?
2. Якою є 48-бітна MAC-адреса отримувача Ethernet кадру? Чи є ця адреса адресою сервера 10.25.0.1? Якщо ні, то який пристрій має цю Ethernet адресу?
3. Дайте шістнадцяткове представлення двохбайтового поля типу кадру Ethernet.
4. Який відступ в кадрі Ethernet має літера "G" в "GET"?
5. Яке шістнадцяткове значення має поле CRC в цьому кадрі? Що це за поле?
6. Якою є адреса відправника кадру? Чи є це адреса вашого комп'ютера або адреса 10.25.0.1.
7. Якою є 48-бітна адреса отримувача Ethernet кадру? Чи є це адреса вашого комп'ютера? Якщо ні, то який пристрій має цю Ethernet адресу?
8. Дайте шістнадцяткове представлення двохбайтового поля типу кадру Ethernet. Що означає біт(и), які дорівнюють 1?
9. Який відступ в кадрі Ethernet має літера"O" в "OK"?
10. Яке шістнадцяткове значення має поле CRC в цьому кадрі? Що це за поле?
11. Які шістнадцяткові значення мають адреса відправника і адреса одержувача в кадрах Ethernet, що містить повідомлення ARP?
12. Дайте шістнадцяткове представлення поля типу кадру Ethernet. Що значать біти, значення яких дорівнюють 1?
13. Чи містить ARP повідомлення IP адресу відправника?
14. Знайдіть повідомлення ARP, що було надіслано у відповідь на запит ARP.

Додаток 1.

Мережева технологія Ethernet і формати кадрів даних

Ethernet являє собою пакетну технологію передачі даних, що працює на фізичному і канальному рівнях моделі OSI в основному в локальних комп'ютерних мережах. Стандарти Ethernet розробляє комітет 802.3 Міжнародного професійного співтовариства – Інституту інженерів електротехніки та електроніки (*Institute of Electrical and Electronics Engineers – IEEE*). На сьогодні найпоширенішими версіями технології є *Fast Ethernet* зі швидкістю передачі даних 100 Мбіт/с (стандарт IEEE 802.3u (оптика / вита пара) і *Gigabit Ethernet* зі швидкістю передачі даних 1 Гбіт/с (стандарт IEEE 802.3z – оптика / 802.3ab – вита пара). У той же час все більша частина мережевих пристроїв і серверів вже випускається з підтримкою технології *10 Gigabit Ethernet* (або *10GbE*) зі швидкістю передачі даних 10 Гбіт/с (стандарти 802.3ae – оптика / 802.3an – вита пара). У червні 2010 р остаточно затверджений стандарт 802.3ba (тільки оптика) для наступних поколінь Ethernet – *40 Gigabit Ethernet* (або *40GbE*) і *100 Gigabit Ethernet* (або *100GbE*) зі швидкістю передачі даних 40 і 100 Гбіт/с, відповідно. Наступною межею Ethernet повинна стати розробка технології *Terabit Ethernet*, що дає змогу передавати дані зі швидкістю 1Тбіт/с. Найбільш поширеними середовищами передачі технології Ethernet є вита пара і оптоволоконний кабель.

Інформація, передана технологією Ethernet, розміщується в структурах даних, які називають кадрами (*frame*) Ethernet. Ці структури мають заголовок (*Header*) зі службовою інформацією, поле даних (*Data*) і завершення з контрольною сумою (*Frame Check Sequence – FCS*) (рис. 1). Розмір кадрів може варіюватися в межах 64 – 1518 байтів.

Першими двома полями заголовка кадру є 6-байтові поля «Адреса одержувача» (*Destination Address – DA*) і «Адреса відправника» (*Source Address – SA*). Решта полів можуть варіюватися в різних типах кадрів. Завершення кадру містить чотирибайтове значення контрольної суми (*Frame Check Sequence – FCS*), обчисленої з використанням алгоритму CRC-32 (*Cyclic Redundancy Code* – циклічний надлишковий код).

14-22 байт	46-1500 байт	4 байти
Заголовок	**Поле даних**	**FCS**

Рис. 1. Узагальнений формат кадру Ethernet

Контрольна сума являє собою деяке значення, яке відправник розрахував за певним алгоритмом з послідовності переданих даних і помістив у поле кадру. Це значення одержувач використовує для перевірки правильності передачі даних, провівши розрахунок з послідовності отриманих даних за тим же алгоритмом і порівнявши отриманий результат зі значенням контрольної суми, переданої в кадрі.

Як адресу технологія Ethernet використовує 6-байтові MAC-адреси, які визначають для підрівня доступу до середовища передачі (*Media Access Control – MAC*) канального рівня виробники мережевих інтерфейсів. Ці адреси вважаються жорстко прив'язаними до конкретного інтерфейсу, хоча й існує можливість їх перевизначити в додаткових налаштуваннях драйвера мережевого адаптера. MAC-адресу мережевого адаптера комп'ютера можна побачити командою `ipconfig /all` для Windows або `ifconfig` для Linux / Unix.

На рис. 2 наведено формат 48-бітної MAC-адреси.

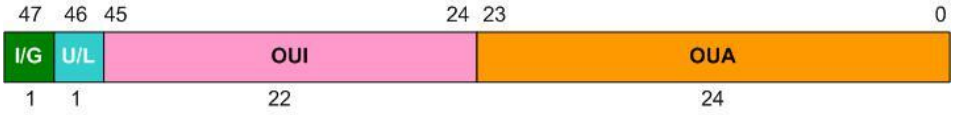


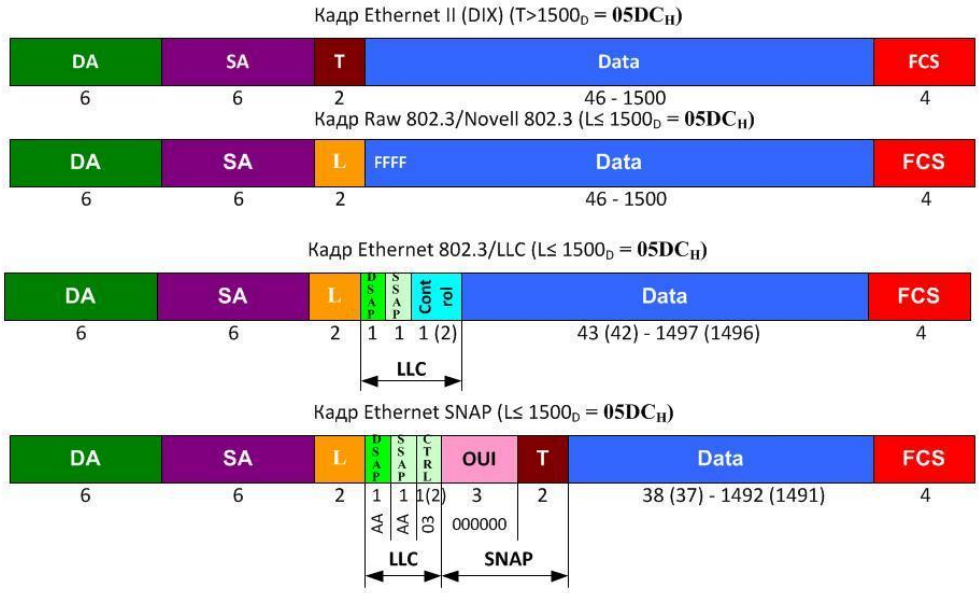
Рис. 2. Формат MAC-адреси

Старші 3 байти MAC-адреси являють собою так званий організаційно унікальний ідентифікатор (*Organizationally Unique Identifier – OUI*). IEEE виділяє такі унікальні ідентифікатори для виробників мережевого устаткування. На сайті IEEE за адресою http://standards.ieee.org/regauth/oui/index.shtml організовано можливість пошуку інформації про виробника за значенням OUI. Молодші 3 байти представляють собою організаційно унікальну адресу (*Organizationally Unique Address – OUA*), яку виробник призначає кожному випущеному контролеру мережевого інтерфейсу. Таким чином, унікальність MAC-адреси забезпечується, з одного боку, IEEE – не існує двох однакових значень OUI, виділених різними виробникам. З іншого боку виробник задає унікальні значення OUA контролерам мережевих інтерфейсів, які він виробляє. В результаті можна гарантувати унікальність значення будь-якої MAC-адреси, записаної в конфігураційну інформацію контролера мережевого інтерфейсу.

Існують три типи MAC-адрес: індивідуальні або однопунктовий (*Unicast*), групові (*Multicast*) і широкомовні (*Broadcast*). Індивідуальна (однопунктова) адреса визначає одну конкретну робочу станцію мережі, це адреса, що трапляється в кадрах Ethernet найчастіше. Іноді необхідно розіслати інформацію всім комп'ютерам локальної мережі. Наприклад, при включенні робочої станції вона висилає всім учасниками мережі своє ім'я мережі і адресну інформацію (після чого її ім'я відображається, наприклад, в розділі ***Мережа***). MAC-адреса, що вказується в цьому випадку в поле адреси одержувача, є широкомовною. Широкомовна адреса являє собою 48 одиничних бітів, які в шістнадцятковій системі виглядають як FF-FF-FF-FF-FF-FFh. У разі, коли одержувачів кадру має бути більше одного, але менше, ніж всі комп'ютери локальної мережі, використовують групові MAC-адреси. Такі адреси використовують, наприклад, у випадку потокової передачі аудіо та відео тим комп'ютерам, користувачі яких підписалися на ці передачі. Ознакою індивідуальної (однопунктової) адреси є встановлений в нуль старший біт (47-й) MAC-адреси (I/G). Відповідно, якщо старший біт встановлений в одиницю,

адреса є груповою (рис. 3). Слід зазначити, що адреса відправника може бути тільки індивідуальною (однопунктовою). А 46-й біт MAC-адреси (U/L) вказує, чи є ця адреса унікальною в глобальному сенсі (біт дорівнює 0), чи в межах локальної мережі в разі, якщо вона перевизначена адміністратором (біт дорівнює 1). З урахуванням характерного для Ethernet порядку передачі бітів першими передаються молодші біти байту, значення старшого байту групової адреси можуть дорівнювати або 01h (для унікальної в глобальному сенсі адреси), або 03h (для унікальної в межах локальної мережі адреси).

У мережах Ethernet на канальному рівні можуть використовувати заголовки чотирьох типів (рис. 3). Їхнє існування пов'язане з тривалою (за мірками інформаційних технологій) історією розвитку технології Ethernet. Практично все мережеве обладнання вміє працювати з усіма форматами кадрів технології Ethernet.



DA – Destination Address – адреса отримувача
SA – Source Address – адреса відправника
T – Type – тип протоколу мережевого рівня
L – Length – довжина поля даних кадру (Data)
DSAP – Destination Service Access Point – тип протоколу мережевого рівня отримувача
SSAP – Source Service Access Point – тип протоколу мережевого рівня відправника
Control – поле керування (визначає тип LLC-кадру тощо)
Data – поле даних (містить пакет мережевого рівня)
FCS – Frame Check Sequence – контрольна сума (CRC-32)

Рис. 5. Формати кадрів Ethernet

Історично першим типом кадру є так званий кадр Ethernet II або Ethernet DIX (де DIX – перші літери назв фірм DEC, Intel і Xerox, які розробили цей формат). Формат цього кадру визначає наступні поля:

- *Адреса одержувача* (DA) – шестибайтова MAC-адреса одержувача.
- *Адреса відправника* (SA) – шестибайтова MAC-адреса відправника.
- *Тип протоколу* (Type – T) – двобайтове поле, призначене для вказання ідентифікатора протоколу, що вклав свій пакет в поле даних кадру Ethernet. Ідентифікатори протоколів, які використовують кадри Ethernet в

якості транспорту, визначено IEEE, вони являють собою двобайтові значення, що перевищують значення максимальної довжини поля даних кадру, яка дорівнює 1500 байтів (05DCh в шістнадцятковій системі), наприклад 0800h – для протоколу IP, 0806h – для протоколу ARP і т.д.

- *Поле даних* (Data) може містити від 46 до 1500 байтів, якщо довжина поля менша від 46 байтів, то використовується заповнення нульовими байтами (00h), щоб доповнити кадр до мінімально допустимої довжини.
- *Поле контрольної суми* (FCS) – 4 байти, містять значення, яке обчислюється за алгоритмом CRC-32.

Описаний тип кадру з'явився під час появи і розвитку Інтернет, очевидно, тому і на сьогодні він використовується для перенесення в локальних мережах пакетів протоколу IP та інших протоколів стеку TCP/IP.

Формат Ethernet II (DIX) має один недолік: якщо передача кадру раптово перервалася, то одержувач такого незавершеного кадру буде приймати його як цілий і знайде помилку тільки після повного його прийому і розрахунку контрольної суми. Очевидно, що в цьому випадку досить багато комп'ютерного часу буде витрачено даремно. Інженери фірми Novell, котра є першою фірмою, яка розробила системне програмне забезпечення для роботи в локальних комп'ютерних мережах Netware, запропонували інший формат кадру, так званий Novell 802.3 або Raw 802.3 (англ. – сирий, необроблений), в якому замість типу протоколу відправника містилася довжина поля даних (Length – L). Одержувач встановлював лічильник байтів у це значення і декрементував його з отриманням кожного байту поля даних. Очевидно, що занулення лічильника свідчило про закінчення поля даних. Якщо дані закінчувалися до занулення лічильника, то такий кадр був незавершеним і його можна було відкинути без необхідності розрахунку контрольної суми. Мотивацією для заміни типу протоколу лічильником довжини був той факт, що на початку 1980-х рр. для локальних мереж, де працює технологія Ethernet, крім стеку протоколів IPX/SPX операційної системи Novell Netware, альтернатив не було, а значить, не було необхідності ідентифікації протоколів, що використовують Ethernet.

Природно, що така позиція легко піддається критиці, і таке рішення не могло бути довговічним. Тому IEEE розробив третій формат кадру Ethernet 802.3/LLC, в якому додав так званий підзаголовок LLC з ідентифікаторами протоколів верхніх рівнів на боці одержувача і на боці відправника. Ці ідентифікатори, також визначені IEEE, розміщуються в полі точки доступу до послуг одержувача (Destination Service Access Point – DSAP) і в полі точки доступу до послуг відправника (Source Service Access Point – SSAP). Зазвичай ці поля мають однакові значення, наприклад, для протоколу IPX вони рівні E0h, для протоколу NetBIOS – F0h, для протоколу STP BPDU – 42h. Поле управління (Control) підзаголовка LLC використовується для позначення типу кадру даних – інформаційний, керуючий або ненумерований (зазвичай в Ethernet використовуються ненумеровані кадри, в цьому випадку значення поля

рівне 03h). Оскільки кадр LLC має заголовок довжиною 3 (4) байти, то максимальний розмір поля даних зменшується до 1497 (1496) байтів. Кадри цього формату використовуються як транспорт у випадку встановлення в операційній системі стеків мережевих протоколів IPX/SPX і NetBIOS.

Поява четвертого типу кадру Ethernet SNAP (SNAP – SubNetwork Access Protocol – протокол доступу до підмереж), швидше за все, зобов'язана прорахункові розробників IEEE, які виділили для ідентифікації протоколів верхніх рівнів однобайтові поля DSAP і SSAP, в які можна записати не більше 256 унікальних ідентифікаторів. Як тільки кількість протоколів стало наближатися до цієї цифри, виникла необхідність розробки нового формату кадру. Кадр Ethernet SNAP визначено в стандарті 802.2H і являє собою розширення кадру 802.3/LLC введенням додаткового підзаголовка SNAP, в якому розміщено поле типу протоколу (Type – T), що має розмір два байти. При цьому двобайтові ідентифікатори протоколів збігаються з ідентифікаторами протоколів для формату Ethernet II (DIX). Крім типу протоколу, в підзаголовку SNAP вказується ідентифікатор організації (OUI), котра визначає ідентифікатори протоколів, які вказують в полі типу протоколу. Прикладами кодів OUI, які використовуються в SNAP є: код IEEE = 00 00 00h, код Cisco Systems = 00 00 0Ch. В поля DSAP і SSAP, якщо використано заголовок SNAP, поміщаються значення AAh, які вказують, що в поле даних кадру LLC вкладено заголовок SNAP. Оскільки підзаголовок SNAP "забирає" ще п'ять байтів у поля даних, останнє зменшується до розмірів 38 (37) – 1491 (1492) байтів.