Лабораторна робота 10
ДОСЛІДЖЕННЯ ПРАВИЛ ТА ПРОТОКОЛІВ УСТАНОВЛЕННЯ ВІДПОВІДНОСТЕЙ МІЖ ЛОГІЧНИМИ І ФІЗИЧНИМИ АДРЕСАМИ В IP-МЕРЕЖАХ

Мета заняття: ознайомитися з основними правилами та протоколами встановлення відповідностей між логічними і фізичними адресами в IP-мережах; ознайомитися з правилами встановлення відповідностей для групових та широкомовних адрес; ознайомитися з деталями організації та функціонування протоколу ARP; отримати практичні навички побудови локальної мережі на базі комутатора Ethernet та навички моніторингу, діагностики та керування процесами встановлення відповідностей між логічними і фізичними адресами в IP-мережах для вузлів ОС Windows, ОС Linux та комунікаційних пристроїв Cisco; дослідити процеси встановлення відповідностей між логічними і фізичними адресами та процеси передачі повідомлень протоколу ARP у побудованій мережі.

Теоретичні відомості

Загальні відомості про встановлення відповідностей між фізичними та логічними адресами в IP-мережах

Для забезпечення передачі повідомлень між вузлами IP-мережі необхідно, щоб вузли володіли інформацією як про власні фізичні і логічні адреси, так і про фізичні і логічні адреси решти вузлів. Це пов'язано з тим, що вузлові під час формування пакета необхідно зазначати логічні адреси відправника й отримувача, а під час формування кадру – фізичні адреси відправника й отримувача. Інформацію про власні адреси вузол/пристрій отримує з налаштувань мережних адаптерів/інтерфейсів системи. Інформацію про адреси решти вузлів мережі – за допомогою спеціальних правил та протоколів. Важливими є питання як установлення, так і дотримання коректних відповідностей між логічними і фізичними адресами у процесі функціонування вузлів. Для різних мережних технологій та протокольних стеків існують свої правила та протоколи встановлення відповідностей між логічними і фізичними адресами.

Найпоширенішим сучасним варіантом побудови локальних, регіональних, а часто і глобальних мереж є використання технологій Ethernet (стандарт IEEE 802.3) та Wi-Fi (стандарт IEEE 802.11) у поєднанні з протокольним стеком TCP/IP за умови застосування протоколу IP версії 4. Зазначені технології є технологіями широкомовних мереж із множинним доступом (BMA, Broadcast Multiple Access). У мережах типу BMA передбачається підключення вузлів до загального середовища передачі даних, у якому можлива передача унікальних (Unicast), групових (Multicast) та широкомовних (Broadcast) повідомлень (Messages) канального рівня моделі OSI – кадрів (Frames). Часто таке середовище носить назву ,,широкомовний домен" (Broadcast Domain). У протоколі IP версії 4 також застосовуються унікальні, групові та широкомовні повідомлення мережного рівня моделі OSI/рівня міжмережної взаємодії стеку TCP/IP – IP-пакети (IP-Packets). Тип повідомлення для наведених випадків визначається адресою отримувача, яка зазначається у повідомленні (кадрі або пакеті). Адреса відправника повідомлення завжди залишається унікальною.

Встановлення і дотримання відповідностей між логічними і фізичними адресами, тобто між IP-адресами версії 4 і MAC-адресами, у широкомовних мережах з множинним доступом здійснюється із застосуванням таким правил та протоколів:

– правило формування групових MAC-адрес на основі групових IP-адрес (і навпаки);

– правило формування широкомовних MAC-адрес на основі широкомовних IP-адрес;

– протокол визначення унікальних MAC-адрес на основі унікальних IP-адрес ARP (Address Resolution Protocol);

– протокол визначення унікальних IP-адрес на основі унікальних MAC-адрес RARP (Reverse Address Resolution Protocol).

У деяких випадках застосовується ручне встановлення відповідностей між IP-адресами версії 4 і MAC-адресами. Якщо у мережі застосовується протокол IP версії 6, то встановлення відповідностей між логічними і фізичними адресами здійснюється за правилами, що передбачені цим протоколом.

Блок-схему узагальненого алгоритму застосування зазначених правил формування групових та широкомовних MAC-адрес на основі відповідних IP-адрес версії 4, а також застосування протоколу ARP наведено на рис. 1.

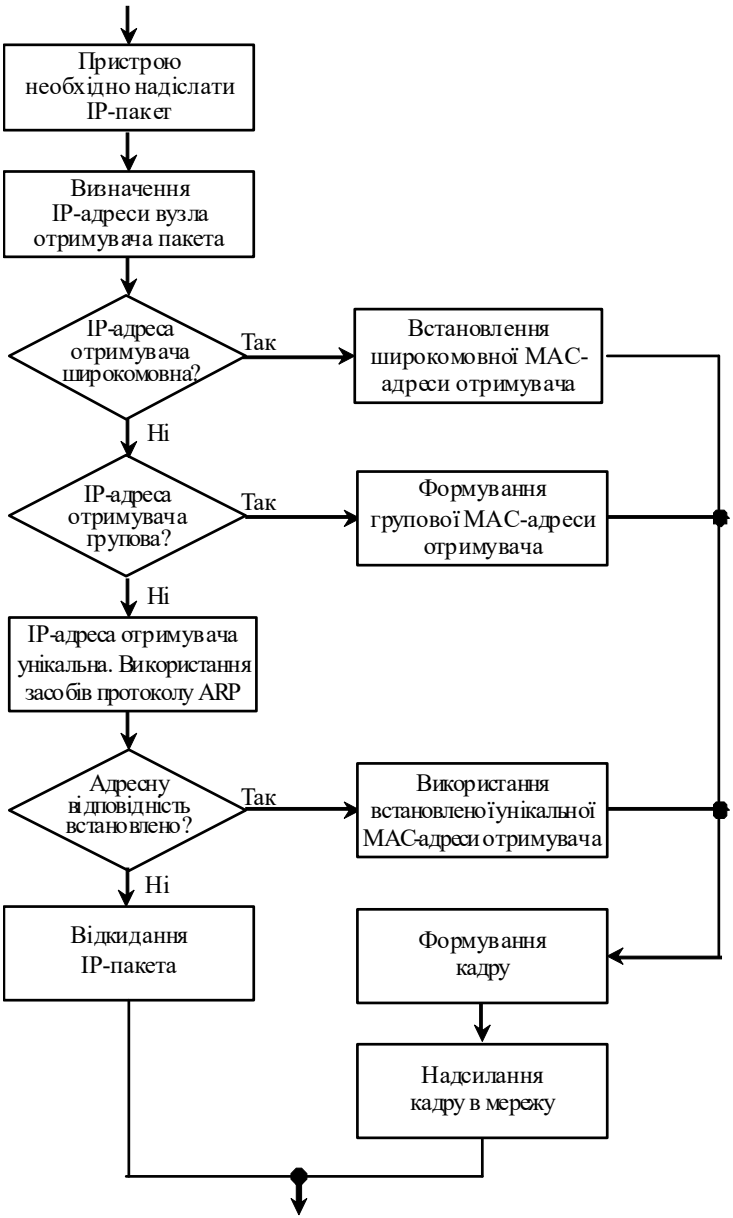


Рис. 1. Блок-схема узагальненого алгоритму застосування правил та протоколів установлення відповідностей між IP-адресами версії 4 та MAC-адресами

Правила формування групових та широкомовних MAC-адрес на основі групових та широкомовних IP-адрес версії 4

Для передачі групових повідомлень (IP-пакетів) у стеку TCP/IP у разі застосування IP-адресації версії 4 передбачено окремий клас IP-адрес – клас D. До цього класу належать адреси з діапазону 224.0.0.0 – 239.255.255.255. Для передавання повідомлень багатьох мережних протоколів стеку TCP/IP застосовуються зарезервовані групові IP-адреси. Детальну інформацію стосовно переліку протоколів та зарезервованих адрес можна знайти на Web-сайті IANA за посиланням http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml. Загальновживані зарезервовані групові IP-адреси версії 4 та відповідні їм мережні протоколи наведено у табл. 1.

Таблиця 1

Зарезервовані групові IP-адреси

Групова адреса	Призначення/Протокол	Документ
224.0.0.0	Базова адреса (зарезервовано)	RFC 1112
224.0.0.1	Всі системи даної підмережі	RFC 1112
224.0.0.2	Всі маршрутизатори даної підмережі	
224.0.0.4	Всі маршрутизатори DVMRP	RFC 1075
224.0.0.5	Всі маршрутизатори OSPF	RFC 2328
224.0.0.6	Призначені маршрутизатори OSPF	RFC 2328
224.0.0.7	Призначені маршрутизатори	RFC 1190
224.0.0.8	Призначені вузли	RFC 1190
224.0.0.9	Маршрутизатори RIP2	RFC 1723
224.0.0.10	Маршрутизатори IGRP/EIGRP	
224.0.0.11	Доступ до мережі мобільного зв’язку (Mobile Agents)	
224.0.0.12	Сервер DHCP/Агент ретрансляції	RFC 1184
224.0.0.18	Протокол VRRP (Virtual Router Redundancy Protocol)	
224.0.0.22	Протокол IGMP v3 (Internet Group Management Protocol)	
224.0.0.102	Протокол HSRP v2 (Hot Standby Router Protocol)	
224.0.0.251	Адреси Multicast DNS	
224.0.1.1	Протокол NTP (Network Time Protocol)	

Групова розсилка повідомлень може застосовуватися у мережах різних типів, але найчастіше застосовується у широкомовних мережах з множинним доступом (мережах типу BMA), таких як мережі Ethernet та Wi-Fi. І саме для мереж Ethernet та Wi-Fi сформульовані правила встановлення відповідностей між груповими і широкомовними логічними і фізичними адресами.

Груповий IP-пакет інкапсулюється у груповий кадр відповідної технології. Під час формування групового кадру необхідно як MAC-адресу призначення вказати групову MAC-адресу. Формування групової MAC-адреси для групового IP-пакета здійснюється таким чином (рис. 2). Частина MAC-адреси, яка містить ідентифікатор виробника для групових MAC-адрес (24 біти), у шістнадцятковій формі запису завжди дорівнює 01-00-5E (у двійковій – 00000001-00000000-01011110). Частина MAC-адреси, яка містить ідентифікатор пристрою (24 біти), ділиться на окремі частини – старший біт завжди дорівнює 0, решта 23 біти містять ідентифікатор групи. Ідентифікатор групи може набувати значень від 00-00-00 до 7F:FF:FF (00000000-00000000-00000000 до 01111111-11111111-11111111). Цей ідентифікатор формується за рахунок перенесення 23 молодших бітів IP-адреси. Решта 9 бітів ігноруються.

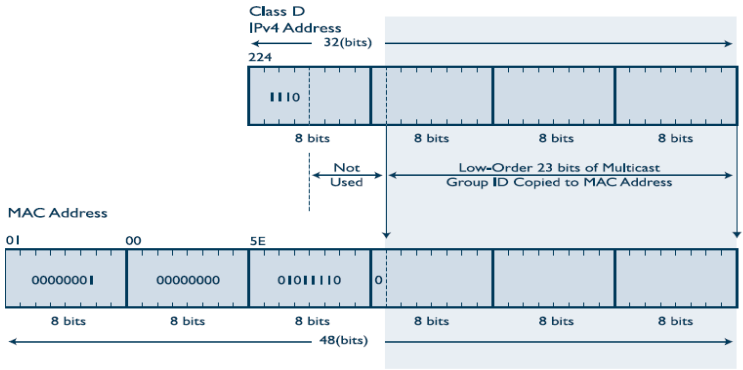


Рис. 2. Формування групової MAC-адреси на основі групової IP-адреси

Для передачі широкомовних повідомлень (IP-пакетів) у стеку TCP/IP у разі використання IP-адресації версії 4 передбачено, що у кожній IP-мережі остання із можливих IP-адрес застосовується саме як широкомовна IP-адреса. У широкомовних мережах із множинним доступом (мережах типу BMA), таких як мережі Ethernet або Wi-Fi, широкомовний IP-пакет інкапсулюється у широкомовний кадр відповідної технології. Для формування широкомовного кадру необхідно як MAC-адресу призначення вказати широкомовну MAC-адресу. Як правило, такою адресою є MAC-адреса FF-FF-FF-FF-FF-FF.

Приклад 1.

Для заданої IP-адреси 224.0.0.22 визначити MAC-адресу групової розсилки. За можливості визначити, повідомлення якого протоколу передається за допомогою даної адреси.

Розв'язання.

Для розв'язання даного прикладу переводимо задану IP-адресу 224.0.0.22 з десяткової у двійкову систему числення:

11100000.0**0000000.00000000.00010110**

Для формування ідентифікатора групи використовуються 23 молодших біти вихідної IP-адреси. У даному випадку це біти:

0000000.00000000.00010110

Додаємо до цієї послідовності ліворуч старший 24-й біт зі значенням 0. Отримаємо бітову послідовність:

00000000.00000000.00010110

У шістнадцятковому вигляді як частина MAC-адреси ця бітова послідовність записується так:

00-00-16

Результуюча групова MAC-адреса має вигляд:

01-00-5E-00-00-16

Групова IP-адреса 224.0.0.22 у поєднанні з груповою MAC-адресою 01-00-5E-00-00-16 у стеку TCP/IP застосовуються для передачі повідомлень протоколу керування груповою передачею IGMP v3.

Приклад 2.

Для заданої MAC-адреси групової розсилки 01-00-5E-00-00-12 визначити IP-адресу (можливі IP-адреси) групової розсилки. За можливості, визначити, повідомлення якого протоколу передається у кадрі з такою адресою.

Розв'язання.

У загальному записі у двійковій формі числення групова IP-адреса версії 4 має вигляд:

1110xxxx.xmmmmmmm.mmmmmmmm.mmmmmmmm

Старші 4 біти (1110) є однаковими для всіх групових IP-адрес версії 4. Наступні 5 бітів (xxxxx) – це біти, які відкидаються під час формування групової MAC-адреси. Решта 23 біти (m…m) – біти, які використовуються для формування ідентифікатора групи у груповій

MAC-адресі. Для формування повного ідентифікатора групи (24 біти) перед цими бітами додається ще один біт – 0.

Визначення групової IP-адреси версії 4 на основі групової MAC-адреси по суті передбачає формування вказаних вище бітових послідовностей. Особливістю формування є те, що неможливо точно відновити 5 бітів (xxxxx), які відкидалися. Як правило, їх відновлюють у вигляді послідовності із 5 нулів.

Для розв'язання даної задачі необхідно задану групову MAC-адресу 01-00-5E-00-00-12 перевести у двійкову форму. Результат має вигляд:

00000001-00000000-01011110-0**0000000-00000000-00010010**

Повний ідентифікатор групи для цієї адреси має вигляд:

0000000-00000000-00010010

Молодші 23 біти, що будуть використані для формування групової IP-адреси, – це біти:

0000000-00000000-00010010

Результуюча групова IP-адреса у двійковій формі має вигляд:

1110xxxx.x0000000.00000000.00010010

За умови, що бітова послідовність xxxxx є нульовою, ця адреса матиме вигляд:

1110**0000**.**0**0000000.00000000.00010010

У десятковій формі відповідно:

224.0.0.18

Визначена групова IP-адреса є адресою групової розсилки протоколу динамічного резервування шлюзу VRRP.

Необхідно зазначити, що в п'яти бітах послідовності xxxxx можна записати 32 різних значення від 00000 до 11111. Відповідно будь-якій одній груповій MAC-адресі можуть відповідати 32 різних групових IP-адреси.

Для нашого випадку це адреси:

224.0.0.18
224.128.0.18
225.0.0.18
225.128.0.18
…
239.0.0.18
239.128.0.18

Приклад 3.

Ethernet-вузол, мережному інтерфейсу якого призначена IP-адреса 198.13.1.6/28, розсилає широкомовне повідомлення решті вузлів мережі. Визначити логічну та фізичну адреси призначення, що будуть застосовуватися для формування повідомлень.

Розв'язання.

Для розв'язання даної задачі переводимо IP-адресу 198.15.1.6 з десяткової у двійкову систему числення:

11000110.00001111.00000001.00000110

На основі відомого префікса мережі /28 формуємо пряму маску як послідовність одиниць (їх кількість – префікс показує кількість бітів, які використовуються для адресації (номера) мережі) та нулів (решта бітів, які використовуються для адресації (номера) вузла):

11111111.11111111.11111111.11110000

Результат у десятковій системі числення має вигляд:

255.255.255.240

IP-адреса мережі визначається шляхом накладання прямої маски на вихідну IP-адресу, тобто виконання логічної операції кон'юнкції (логічне AND) між відповідними бітами вихідної IP-адреси та прямої маски:

11000110.00001111.00000001.00000110
11111111.11111111.11111111.11110000
11000110.00001111.00000001.00000000

Результат виконання кон'юнкції між відповідними бітами вихідної IP-адреси та прямої маски у двійковій системі числення має вигляд:

11000110.00001111.00000001.00000000

Результат у десятковій системі числення має вигляд:

198.15.1.0

Для отримання широкомовної IP-адреси необхідно інвертувати біти частини IP-адреси мережі, що виділяються на номер вузла. У нашому випадку це останні 4 біти. Результат інверсії має вигляд:

11000110.00001111.00000001.0000**1111**

Широкомовна логічна адреса мережі 198.15.1.0 у десятковій системі числення – це IP-адреса:

198.15.1.15

Цій широкомовній IP-адресі відповідає загальноприйнята широкомовна фізична адреса – MAC-адреса FF-FF-FF-FF-FF-FF.

Загальні відомості про протоколи ARP/RARP

Протокол ARP призначений для динамічного визначення MAC-адреси віддаленого вузла за відомою його IP-адресою версії 4. Протокол RARP виконує зворотну процедуру. Частіше поряд із терміном ,,визначення адрес" застосовують терміни ,,встановлення" або ,,перетворення адрес". Спочатку протоколи ARP/RARP були розроблені як універсальні протоколи для мереж різних технологій та різних протокольних стеків, сьогодні, у першу чергу, вони застосовуються у мережах Ethernet та Wi-Fi у поєднанні з протокольним стеком TCP/IP за умови застосування IP версії 4.

Основним стандартом протоколу ARP є прийнятий у 1982 р. стандарт RFC-826 ,,An Ethernet Address Resolution Protocol (or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware)". Основним стандартом протоколу RARP є прийнятий у 1984 р. стандарт RFC-903 ,,A Reverse Address Resolution Protocol". Протоколи ARP та RARP належать до базових протоколів стеку TCP/IP, тому стандарти, у яких вони описані, також позначають як STD-37 та STD-38 відповідно. На сьогодні існують два стандарти, пов'язані з протоколом ARP, які мають статус Proposed Standard. Це стандарти RFC-5227 ,,IPv4 Address Conflict Detection" та RFC-5494 ,,IANA Allocation Guidelines for the Address Resolution Protocol (ARP)". Зазначені стандарти орієнтовані на розширення функціональності протоколу ARP.

Стосовно моделі OSI протоколи ARP/RARP належать до мережного рівня. Але у багатьох випадках їх позиціонують як протоколи, що знаходяться між канальним і мережним рівнями. Таке позиціонування пов'язане з тим, що протоколи ARP/RARP не застосовують повідомлення мережного рівня для передачі власної службової інформації, а формують власні повідомлення, які надалі інкапсулюються у кадри технології канального рівня.

Слід зазначити, що протокол ARP орієнтований на функціонування у межах одного канального сегмента (широкомовного домену). За необхідності передачі ARP-повідомлень між різними канальними сегментами, об'єднаними за допомогою маршрутизаторів/багаторівневих комутаторів, застосовується спеціально розроблений механізм Proxy-ARP.

Обмін інформацією між вузлами мережі для формування адресних відповідностей між IP-адресами і MAC-адресами у протоколі ARP здійснюється із застосуванням механізму „запит-відповідь" (Request-Reply). Результати обміну зберігаються у таблиці, що називається ARP-таблицею/ARP-кешем (ARP-Table/ARP-Cache). ARP-таблиця після завантаження вузла є порожньою і заповнюється ARP-записами динамічно у процесі інформаційного обміну. Джерелами заповнення ARP-таблиці поточного вузла є: ARP-відповіді на власні ARP-запити; ARP-запити інших вузлів. Для кожного ARP-запису створюється таймер (тайм-аут) існування запису. Таймер щосекундно декрементується, і якщо його значення досягає нуля, то ARP-запис з ARP-таблиці видаляється. Якщо вузол повторно отримує ARP-повідомлення з адресною інформацією, яка відповідає наявному у ARP-таблиці ARP-запису, то значення таймера цього запису оновлюється до максимального значення. Загальні вимоги до встановлення максимальних значень тайм-аутів існування ARP-записів відсутні, тому виробники мережного обладнання та ОС встановлюють їх на свій розсуд. Наприклад, для ОС Windows тайм-аут становить 10 хв, для ОС Linux – 1 хв, для комунікаційних пристроїв Cisco – 4 год. Описаний варіант керування записами в ARP-таблиці є спрощеним варіантом, насправді керування здійснюється за більш складними механізмом, який описаний у стандарті RFC-826. Слід зазначити, що у більшості систем та пристроїв наявна можливість статичного формування ARP-записів, що зберігаються в ARP-таблиці.

Повідомлення протоколів ARP/RARP є однаковими за структурою та інкапсулюються у кадри канального рівня відповідної технології. Для ідентифікації ARP-повідомлення у відповідному полі кадру зазначається код протоколу 806h, а для RARP-повідомлення – код протоколу 8035h. Згідно зі стандартом ARP-запити інкапсулюються у широкомовні кадри, а ARP-відповіді – в унікальні кадри.

Структуру повідомлення протоколу ARP для стеку TCP/IP за умови інкапсуляції ARP-повідомлень у кадри технологій Ethernet/Wi-Fi наведено на рис. 3. Для інших технологій можуть існувати розбіжності у довжинах полів, що містять фізичні і логічні адреси вузлів.

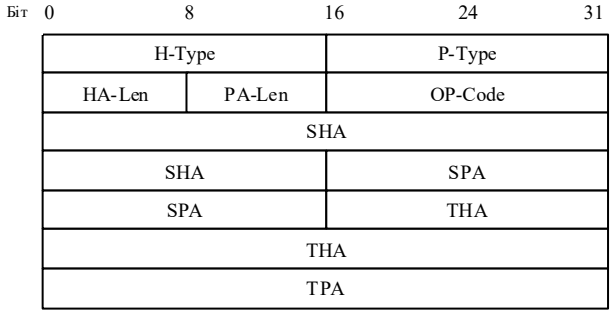


Рис. 3. Структура повідомлення протоколу ARP

Поле H-Type (Hardware Type) містить значення типу мережного інтерфейсу/адаптера, для якого відправник встановлює відповідність адрес (для мереж Ethernet дорівнює 0001h). Поле P-Type (Protocol Type) містить код мережного протоколу, для якого відправник встановлює відповідність адрес (для протоколу IP версії 4 – цей код дорівнює 0800h). Поле HA-Len (Hardware Address Length) містить довжину апаратної адреси (у байтах, для MAC-адреси HA-Len дорівнює 06h). Поле PA-Len (Protocol Address Length) містить довжину протокольної адреси (у байтах, для IP-адреси версії 4 поле PA-Len дорівнює 04h). Поле OP-Code (Operation Code) містить код операції, може набувати значень: 01h – ARP-запит; 02h – ARP-відповідь; 03h – RARP-запит; 04h – RARP-відповідь; решта значень пов'язані з маловживаними протоколами). Поля SHA (Sender Hardware Address) та SPA (Sender Protocol Address) містять відповідно фізичну та логічну адреси відправника ARP-повідомлення. Поля THA (Target Hardware Address) та TPA (Target Protocol Address) – фізичну та логічну адреси отримувача ARP-повідомлення. Для технологій Ethernet/Wi-Fi та протоколу IP версії 4 поля SHA та THA – це MAC-адреси, а поля SPA та TPA – це IP-адреси. Необхідно зазначити, що у коректно сформованому ARP-запиті поле THA містить значення 000000000000h.

Блок-схему узагальненого алгоритму роботи протоколу ARP для випадку пересилання ARP-запиту наведено на рис. 4. Блок-схему узагальненого алгоритму роботи протоколу ARP для випадку отримання ARP-повідомлення наведено на рис. 5.

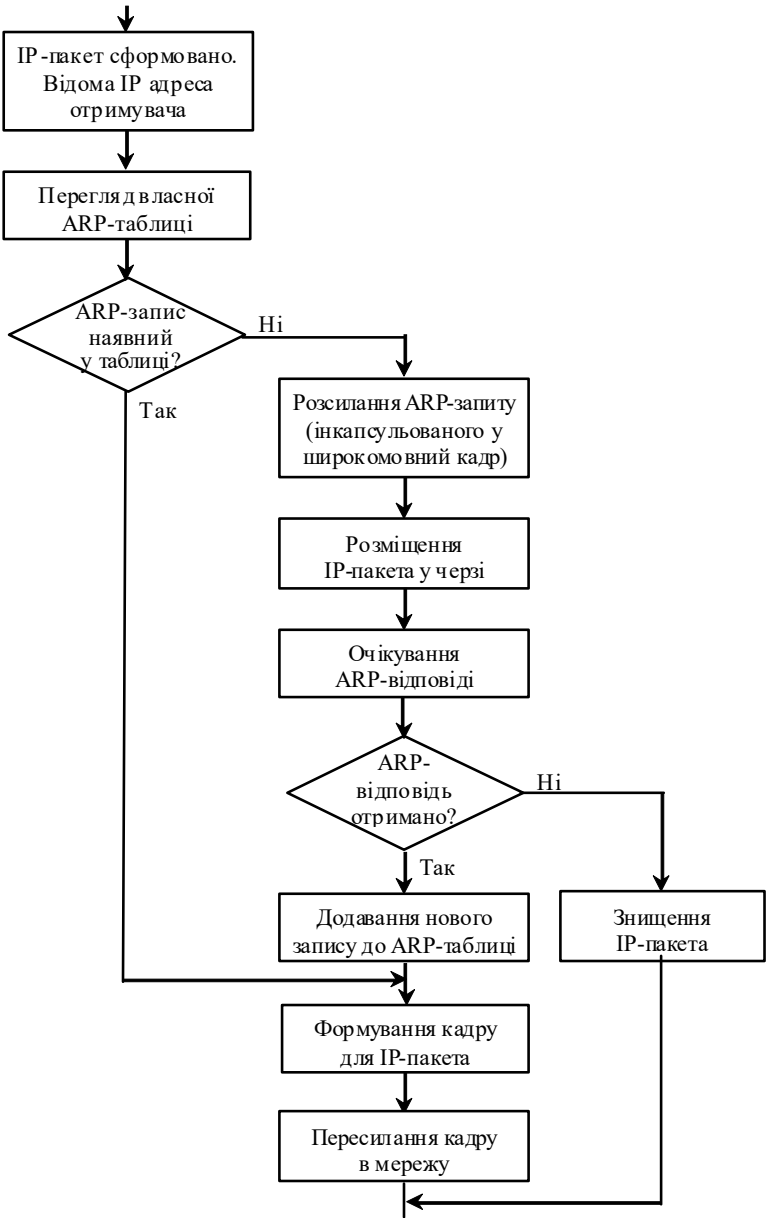


Рис. 4. Блок-схема алгоритму роботи протоколу ARP для випадку пересилання ARP-запиту

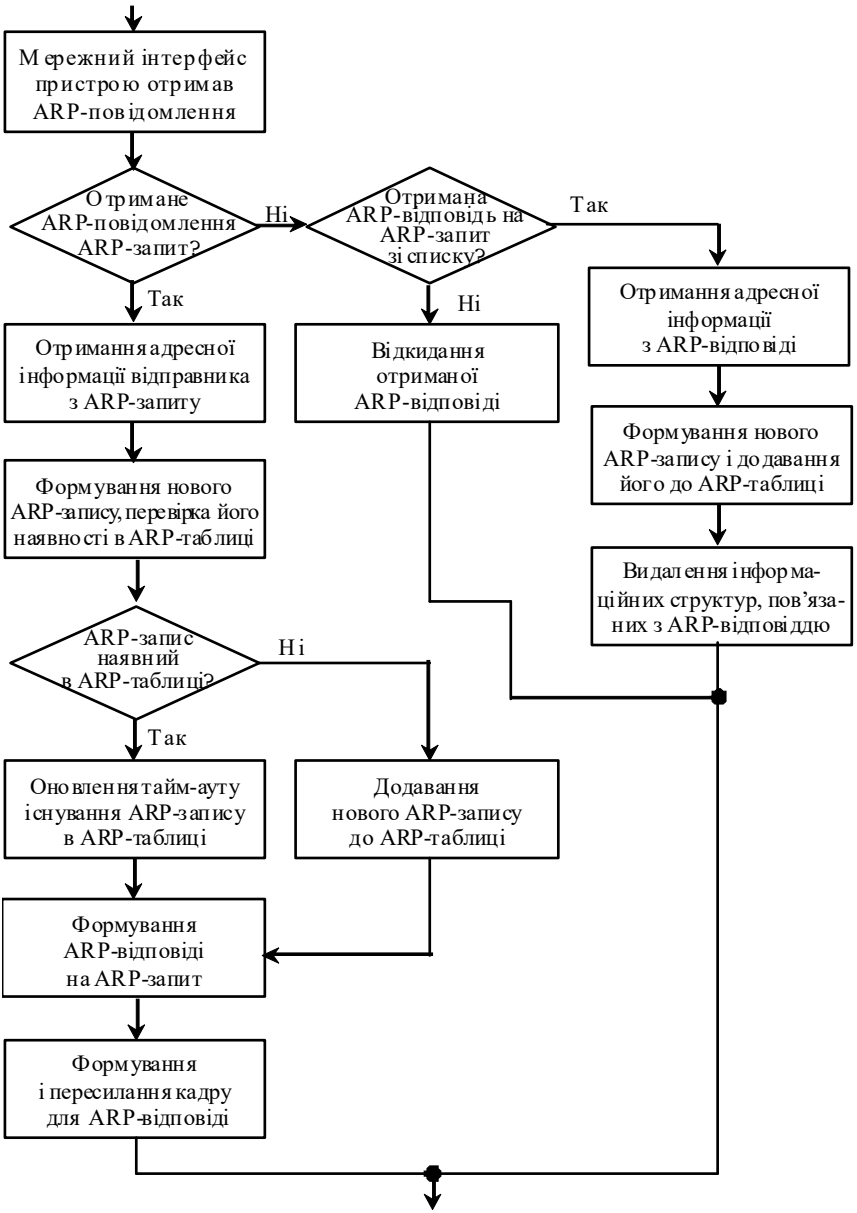


Рис. 5. Блок-схема алгоритму роботи протоколу ARP
для випадку отримання ARP-повідомлення

Приклад 4.

Вузлові А, який знаходиться у IP-мережі 195.10.1.0/24 і мережному Ethernet-інтерфейсу якого призначені MAC-адреса 00-60-5C-16-8B-30 та IP-адреса 195.10.1.1/24, необхідно переслати IP-пакет вузлові В, що знаходиться у цій же мережі і мережному Ethernet-інтерфейсу якого призначені MAC-адреса 00-10-11-49-ED-09 та IP-адреса 195.10.1.3/24. ARP-таблиця вузла А є порожньою. Сформувати ARP-запит вузла А та отриману від вузла В ARP-відповідь. Сформовані ARP-повідомлення показати інкапсульованими у кадри канального рівня. Результати показати у шістнадцятковій формі.

Розв'язання.

ARP-запит формується за загальною структурою ARP-повідомлення. Оскільки вузол А належить мережі Ethernet, у якій застосовується протокол IP версії 4, то всі поля ARP-запиту формуються з урахуванням цих параметрів. Тобто, поле H-Type дорівнює 0001h, а поле P-Type – 0800h. Поля HA-Len та PA-Len відповідно дорівнюють 06h та 04h. Оскільки формується ARP-запит, то поле OP-Code дорівнює 0001h. Поля SHA та SPA формуються на основі MAC-адреси 00-60-5C-16-8B-30 і IP-адреси 195.10.1.1 відправника (вузла А) і відповідно дорівнюють 00605C168B30h та 3C0A0101h. В ARP-запиті поле THA за замовчуванням дорівнює 000000000000h, поле TPA формується на основі IP-адреси 195.10.1.3 отримувача (вузла В) і дорівнює 3C0A0103h.

Побудований ARP-запит має вигляд:

```
000108000604000100605C168B30
3C0A0101000000000000003C0A0103
```

ARP-відповідь також формується за загальною структурою ARP-повідомлення для мереж Ethernet із застосуванням протоколу IP версії 4. Тобто поле H-Type дорівнює 0001h, а поле P-Type – 0800h, поле HA-Len – 06h, поле PA-Len – 04h. Оскільки формується ARP-відповідь, то поле OP-Code дорівнює 0002h. Поля SHA та SPA формуються на основі MAC-адреси 00-10-11-49-ED-09 і IP-адреси 195.10.1.3 відправника (вузла В) і відповідно дорівнюють 00101149ED09h та 3C0A0103h. Поля THA та TPA формуються на основі MAC-адреси 00-60-5C-16-8B-30 і IP-адреси 195.10.1.1 отримувача (вузла А) і відповідно дорівнюють 00605C168B30h та 3C0A0101h.

Побудована ARP-відповідь має вигляд:

```
000108000604000200101149ED09
3C0A010300605C168B303C0A0101
```

Загальна довжина ARP-повідомлення у разі застосування технології Ethernet та протоколу IP версії 4 є фіксованою і становить 28 байтів. Така довжина повідомлення дає змогу для інкапсуляції застосовувати Ethernet-кадри мінімальної довжини (64 байти), у яких поле даних (Data) дорівнює 46 байтів. Таке поєднання призводить до необхідності доповнення ARP-повідомлення до 46 байтів заповнювачем – довільною послідовністю довжиною 18 байтів. Як правило, поле заповнювача (Padding) – це послідовність із байтів зі значенням 00h.

ARP-запит інкапсулюються у широкомовний кадр відповідної технології. Для побудованого ARP-запиту вузла A поля заголовка Ethernet-кадру DA-MAC, SA-MAC, Type/Length містять значення відповідно FFFFFFFFFFFFh, 00605C168B30h та 0806h.

ARP-відповідь інкапсулюються в унікальний кадр відповідної технології. Для побудованої ARP-відповіді вузла B поля заголовка Ethernet-кадру DA-MAC, SA-MAC, Type/Length містять значення відповідно 00605C168B30h, 00101149ED09h та 0806h.

Результуючий Ethernet-кадр з інкапсульованим ARP-запитом має вигляд

```
FFFFFFFFFFFF00605C168B300806
00010800060400010060 5C168B30
3C0A0101000000000003C0A0103
00000000000000000000000000000000000000
XXXXXXXX
```

Результуючий Ethernet-кадр з інкапсульованою ARP-відповіддю має вигляд

```
00605C168B3000101149ED090806
00010800060400020010 1149ED09
3C0A010300605C168B303C0A0101
00000000000000000000000000000000000000
XXXXXXXX
```

Для побудованих Ethernet-кадрів контрольні суми (поле FCS) не розраховувалися, замість них записана умовна 4-байтова послідовність XXXXXXXX. У реальному житті контрольні суми розраховуються для всіх полів кадру (крім FCS) за алгоритмом CRC-32 як у разі надсилання кадру в мережу, так і отримання кадру з мережі.

Команди моніторингу стану та операцій з ARP-таблицями вузлів ОС Windows та ОС Linux

Для моніторингу та операцій із записами ARP-таблиць у більшості сучасних ОС реалізовано однойменну команду (утиліту) **arp**. За допомогою цієї команди можна здійснювати як перегляд вмісту, так і видалення та додавання записів до ARP-таблиці. Набір параметрів команди **arp** є досить універсальним, близьким за записом і функціоналом для різних ОС. Це пов'язано з тим фактом, що спочатку команду, як і весь стек TCP/IP, було розроблено для ОС Unix, і пізніше перенесено в інші ОС. Перелік параметрів команди **arp**, що застосовуються в ОС Windows XP/7/8/10, ОС Linux MicroCore, ОС Linux Debian, наведено відповідно на рис. 6 – 8.

```
C:\>arp

Отображение и изменение таблиц преобразования IP-адресов в Физические,
используемые протоколом разрешения адресов <ARP>.

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]
  -a            Отображает текущие ARP-записи, опрашивая текущие данные
                протокола. Если задан inet_addr, то будут отображены IP и
                физический адреса только для заданного компьютера. Если
                ARP используют более одного сетевого интерфейса, то будут
                отображаться записи для каждой таблицы.
  -g            То же, что и параметр -a.
  -v            Отображает текущие ARP-записи в режиме подробного
                протоколирования. Все недопустимые записи и записи в
                интерфейсе обратной связи будут отображаться.
  inet_addr     Определяет IP-адрес.
  -N if_addr    Отображает ARP-записи для заданного в if_addr сетевого
                интерфейса.
  -d            Удаляет узел, задаваемый inet_addr. Параметр inet_addr может
                содержать знак шаблона * для удаления всех узлов.
  -s            Добавляет узел и связывает адрес в Интернете inet_addr
                с Физическим адресом eth_addr. Физический адрес задается
                6 байтами (в шестнадцатеричном виде), разделенных дефисом.
                Эта связь является постоянной
  eth_addr      Определяет физический адрес.
  if_addr       Если параметр задан, он определяет адрес интерфейса в
                Интернете, чья таблица преобразования адресов должна
                измениться. Если параметр не задан, будет использован
                первый доступный интерфейс.
Пример:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .. Добавляет статическую запись.
  > arp -a                                    .. Выводит ARP-таблицу.
C:\>
```

Рис. 6. Перелік параметрів утиліти **arp** (ОС Windows XP/7)

```
root@box:~# arp

BusyBox v1.19.0 (2011-08-14 21:05:38 UTC) multi-call binary.

Usage: arp

[-vn]   [-H HWTYPE] [-i IF] -a [HOSTNAME]
[-v]                [-i IF] -d HOSTNAME [pub]
[-v]    [-H HWTYPE] [-i IF] -s HOSTNAME HWADDR [temp]
[-v]    [-H HWTYPE] [-i IF] -s HOSTNAME HWADDR [netmask MASK] pub
[-v]    [-H HWTYPE] [-i IF] -Ds HOSTNAME IFACE [netmask MASK] pub

Manipulate ARP cache
        -a              Display (all) hosts
        -s              Set new ARP entry
        -d              Delete a specified entry
        -v              Verbose
        -n              Don't resolve names
        -i IF           Network interface
        -D              Read <hwaddr> from given device
        -A,-p AF        Protocol family
        -H HWTYPE        Hardware address type
root@box:~#
```

Рис. 7. Перелік параметрів утиліти **arp** (ОС Linux MicroCore)

```
root@debian8-3~: # arp

Usage:

  arp [-vn]  [<HW>] [-i <if>] [-a] [<hostname>]             <-Display ARP cache
  arp [-v]          [-i <if>] -d  <host> [pub]               <-Delete ARP entry
  arp [-vnD] [<HW>] [-i <if>] -f  [<filename>]            <-Add entry from file
  arp [-v]   [<HW>] [-i <if>] -s  <host> <hwaddr> [temp]           <-Add entry
  arp [-v]   [<HW>] [-i <if>] -Ds <host> <if> [netmask <nm>] pub          <-''-

        -a                      display (all) hosts in alternative (BSD) style
        -s, --set               set a new ARP entry
        -d, --delete            delete a specified entry
        -v, --verbose           be verbose
        -n, --numeric           do n't resolve names
        -i, --device            specify network interface (e.g. eth0)
        -D, --use-device        read <hwaddr> from given device
        -A, -p, --protocol      specify protocol family
        -f, --file              read new entries from file or from /etc/ethers

  <HW>=Use '-H <hw>' to specify hardware address type. Default: ether
  List of possible hardware types (which support ARP) :
    ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) rose (AMPR ROSE) arcnet (ARCnet)
    dlci (Frame Relay DLCI) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
    irda (IrLAP) x25 (generic X.25) eui64 (Generic EUI-64)

root@debian8-3~: #
```

Рис. 8. Перелік параметрів утиліти **arp** (ОС Linux Debian)

Налагодження параметрів функціонування протоколу ARP на вузлах ОС Windows та ОС Linux

Механізм керування часовими параметрами функціонування протоколу ARP, зокрема і ARP-таблицею, детально описаний у стандарті RFC-826 „An Ethernet Address Resolution Protocol (or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware)". Кожен з виробників ОС має свою програмну реалізацію цього механізму. Типово часові параметри протоколу ARP зберігаються у конфігураційних файлах систем і пристроїв. Відповідно налагодження параметрів, у першу чергу тайм-ауту утримання записів у ARP-таблиці, передбачає внесення змін у зазначені файли.

В ОС Windows XP часові параметри протоколу ARP зберігаються у реєстрі системи. З цією метою у розділі реєстру HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\ Parametrs створені два параметри – ArpCacheLife та ArpCacheMinReferenceLife. Їх значення зазначаються в секундах. У параметрі ArpCacheLife міститься час існування ARP-записів, що не використовуються. За замовчуванням його значення дорівнює 2 хв. У параметрі ArpCacheMinReferenceLife – час існування ARP-записів, до яких звернення здійснюються часто. За замовчуванням його значення дорівнює 10 хв. В останніх версіях ОС Windows ці параметри усунуті із реєстру та застосовується інший, складніший механізм керування вмістом ARP-таблиці. Детальний опис механізму та його реалізації для ОС Windows можна отримати з документації, розміщеної на Web-сайті виробника.

В ОС Linux базові параметри керування ARP-таблицею, що необхідні для функціонування протоколу ARP згідно RFC-826, зберігаються у кількох конфігураційних файлах, що містяться у шаблонному каталозі /proc/sys/net/ipv4/neigh/default/. Зокрема, початковий тайм-аут існування записів у ARP-таблиці міститься у файлі /proc/sys/net/ipv4/ neigh/default/gc_stale_time і за замовчування його значення дорівнює 60 с. Для кожного з мережних інтерфейсів на етапі встановлення ОС на базі шаблонного каталога створюється власний конфігураційний каталог /proc/sys/net/ipv4/neigh/if-name/ та власні конфігураційні файли, які надалі можна редагувати.

Команди моніторингу стану та операцій з ARP-таблицями комунікаційних пристроїв Cisco

Моніторинг стану ARP-таблиць комунікаційних пристроїв Cisco здійснюється за допомогою команди **show arp** та похідних від неї команд **show arp detail**, **show arp dynamic**, **show arp static**, **show arp summary**, **show arp interface** тощо. Видалення записів з ARP-таблиць здійснюється за допомогою команди **clear arp** та похідних від неї команд. Додавання записів до ARP-таблиць здійснюється за допомогою команди **arp**.

Перелік основних команд **show arp**, **clear arp** та їх призначення наведено у табл. 2. Синтаксис команди **arp** для випадку застосування протоколу IP версії 4 наведено нижче.

Таблиця 2

Перелік основних команд show arp та **clear arp** комунікаційних пристроїв Cisco

Команда	Призначення
Команди **show arp**	
show arp	Виведення загальної ARP-таблиці пристрою
show arp detail	Виведення ARP-таблиці пристрою у деталізованому вигляді
show arp dynamic	Виведення інформації про динамічні ARP-записи, що містяться у таблиці
show arp static	Виведення інформації про статичні ARP-записи, що містяться у таблиці
show arp summary	Виведення сумарної інформації про роботу протоколу ARP на пристрої
show arp interface ***interface_type interface_id***	Виведення ARP-таблиці у розрізі окремого фізичного або логічного інтерфейсу
show arp ***IP_address***	Виведення ARP-таблиці для окремої IP-адреси або окремої IP-мережі
show arp ethernet ***interface-id***	Виведення ARP-таблиці у розрізі окремого інтерфейсу Ethernet
Команди **clear arp**	
clear arp	Повне очищення (видалення всіх ARP-записів) ARP-таблиці пристрою
clear arp ***IP_address***	Видалення окремого (за IP-адресою) ARP-запису з ARP-таблиці пристрою
clear arp ***interface_type interface_id***	Видалення ARP-записів з ARP-таблиці пристрою, які пов’язані із зазначеним інтерфейсом

Синтаксис команди **arp** (режим глобального конфігурування):

arp ***IP_address hw_address*** **arpa** ***interface_type interface_id***,

де ***IP_address*** – IP-адреса віддаленого вузла у десятковому записі;

hw_address – MAC-адреса віддаленого вузла у вигляді HHHH.HHHH.HHHH; кожне число HHHH має довжину 2 байти і записується в шістнадцятковій формі.

arpa – службова конструкція, за допомогою якої на пристрої зазначається встановлення відповідностей між IP-адресами і MAC-адресами;

interface_type – тип інтерфейсу (порту), може набувати значень **Ethernet**, **FastEthernet**, **GigabitEthernet**, **Port-channel**, **Vlan** тощо;

interface_id – ідентифікатор інтерфейсу (порту), може мати одночислове позначення ***number*** (номер порту), або двочислове позначення ***module/number*** (номер модуля/номер порту).

Налагодження параметрів функціонування протоколу ARP на комунікаційних пристроях Cisco

Налагодження параметрів функціонування протоколу ARP на комунікаційних пристроях Cisco передбачає встановлення певних загальних параметрів (наприклад, тайм-ауту утримання записів в ARP-таблиці) та набору спеціалізованих параметрів (наприклад, параметрів розсилки повідомлень ARP-Probe). Основною командою, від якої походить решта команд для налагодження параметрів та засобів протоколу ARP у Cisco IOS, є команда **arp**. До переліку похідних від цієї команди належать такі команди, як: **arp arpa**, **arp authorized**, **arp frame-relay**, **arp log threshold entries**, **arp probe interval**, **arp snap**, **arp timeout**. Призначення та синтаксис вищезгаданих команд наведено нижче.

Команди **arp arpa** та **arp snap** застосовуються для зазначення протоколу інкапсуляції у кадри канального рівня; **arp arpa** – звичайна інкапсуляція, **arp snap** – інкапсуляція із застосуванням заголовків кадрів SNAP. Команда **arp authorized** дозволяє застосовувати лише внутрішні авторизовані записи. Команда **arp frame-relay** активує застосування протоколу ARP для інтерфейсів технології Frame Relay. Команда **arp log threshold entries** призначена для налагодження параметрів підсистеми журналювання, які стосуються протоколу ARP. За допомогою команди **arp probe interval** здійснюється налагодження механізму ARP-

Probe. Команда **arp timeout** застосовується для встановлення тайм-ауту утримання ARP-записів в ARP-таблиці пристрою.

Синтаксис команди **arp arpa** (режим конфігурування інтерфейсу):

arp arpa.

Команда не має параметрів.

Синтаксис команди **arp authorized** (режим конфігурування інтерфейсу):

arp authorized.

Команда не має параметрів.

Синтаксис команди **arp frame-relay** (режим конфігурування інтерфейсу):

arp frame-relay.

Команда не має параметрів.

Синтаксис команди **arp log threshold entries** (режим конфігурування інтерфейсу):

arp log threshold entries ***threshold_value***,

де ***threshold_value*** – кількість записів, може змінюватися у діапазоні від 1 до 2147483647.

Синтаксис команди **arp probe interval** (режим конфігурування інтерфейсу):

arp probe interval ***probe_int_value*** **count** ***count_value***,

де ***probe_int_value*** – тривалість інтервалу для розсилки повідомлень ARP-Probe; зазначається у секундах, може змінюватися у діапазоні від 1 до 10 с;

count – службова конструкція, за допомогою якої зазначається кількість повідомлень, що посилаються у послідовності повідомлень ARP-Probe;

count_value – кількість повідомлень у послідовності ARP-Probe; може змінюватися у діапазоні від 1 до 60;

Синтаксис команди **arp snap** (режим конфігурування інтерфейсу):

arp snap.

Команда не має параметрів.

Синтаксис команди **arp timeout** (режим конфігурування інтерфейсу):

arp timeout ***arp_timeout_value***,

де ***arp_timeout_value*** – тривалість тайм-ауту протоколу ARP; зазначається у секундах, може змінюватися у діапазоні від 0 до 2147483; за замовчуванням дорівнює 14400 с (4 год).

Програмні розробки на базі протоколу ARP

На базі протоколу ARP розроблено утиліту **arping**, яка за функціоналом є подібною до утиліти **ping**. Проте її застосування обмежене лише канальним сегментом (широкомовним доменом), до якого належить вузол. Найуживанішим випадком застосування утиліти **arping** є перевірка доступності вузлів, на яких налагоджено блокування відповідей на ICMP-запити утиліти **ping**. Автором утиліти **arping** є Томас Хабетс (Thomas Habets). На основі його розробки реалізовано кілька відмітних за функціоналом варіантів утиліти. Проте найбільш функціональним варіантом є саме варіант автора. Зокрема, авторський варіант дає змогу перевіряти доступність вузла і за MAC-адресою.

Спочатку утиліту **arping** було розроблено лише для ОС Unix/Linux, нині наявні варіанти і для ОС Windows. У деяких ОС Linux (наприклад, ОС Linux Microcore) цю утиліту встановлено за замовчуванням, в інших (наприклад, ОС Linux Debian) – її можна встановити з репозиторію ОС. Актуальна інформація стосовно стану розробки утиліти **arping** знаходиться на Web-сторінці її автора за адресою http://www.habets.pp.se/synscan/programs.php?prog=arping.

Перелік параметрів для спрощеного варіанта утиліти **arping**, що застосовується в ОС Linux Microcore, наведено на рис. 9. Перелік параметрів авторського варіанта утиліти, що реалізований в ОС Linux Debian, наведено на рис. 10.

```
root@box:~# arping
BusyBox v1.19.0 (2011-08-14 21:05:38 UTC) multi-call binary.
Usage: arping [-fqbDUA] [-c CNT] [-w TIMEOUT] [-I IFACE] [-s SRC_IP] DST_IP
Send ARP requests/replies
        -f              Quit on first ARP reply
        -q              Quiet
        -b              Keep broadcasting, don't go unicast
        -D              Duplicated address detection mode
        -U              Unsolicited ARP mode, update your neighbors
        -A              ARP answer mode, update your neighbors
        -c N            Stop after sending N ARP requests
        -w TIMEOUT      Time to wait for ARP reply, seconds
        -I IFACE        Interface to use (default eth0)
        -s SRC_IP       Sender IP address
        DST_IP          Target IP address
root@box:~#
```

Рис. 9. Перелік параметрів утиліти arping (ОС Linux Microcore)

```
root@debian8-3:~# arping
ARPing 2.14, by Thomas Habets <thomas@habets.se>
usage: arping [ -0aAbdDeFpPqrRuUv ] [ -w <us> ] [ -W <sec> ] [ -S <host/ip> ]
              [ -T <host/ip ] [ -s <MAC> ] [ -t <MAC> ] [ -c <count> ]
              [ -C <count> ][ -i <interface> ] <host/ip/MAC | -B>
For complete usage info, use —help or check the manpage.
```

```
root@debian8-3:~#
```

Рис. 10. Перелік параметрів утиліти arping (ОС Linux Debian)

Модельний приклад дослідження функціонування протоколу ARP в локальній комп'ютерній мережі

Розглянемо специфіку налагодження вузлів (робочих станцій) ОС Windows та ОС Linux для локальної комп'ютерної мережі, схему якої наведено на рис. 11.

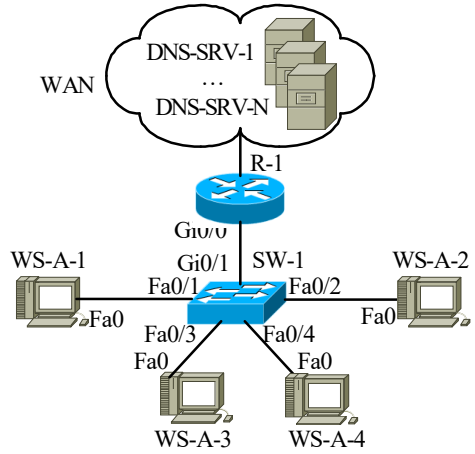


Рис. 11. Приклад мережі

Під час побудови даної мережі для з'єднання пристроїв використано дані табл. 3. Для налагодження параметрів адресації вузлів та комунікаційних пристроїв мережі використано дані табл. 4.

Таблиця 3

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R-1	Gi0/1	WAN	WAN Interface
	Gi0/0	Комутатор SW-1	Gi0/1
Комутатор SW-1	Fa0/1	Робоча станція WS-A-1	Fa0
	Fa0/2	Робоча станція WS-A-2	Fa0
	Fa0/3	Робоча станція WS-A-3	Fa0
	Fa0/4	Робоча станція WS-A-4	Fa0
	Gi0/1	Маршрутизатор R-1	Gi0/0
WAN	WAN Interface	Маршрутизатор R-1	Gi0/1
Робоча станція WS-A-1	Fa0	Комутатор SW-1	Fa0/1
Робоча станція WS-A-2	Fa0		Fa0/2
Робоча станція WS-A-3	Fa0		Fa0/3
Робоча станція WS-A-4	Fa0		Fa0/4

Таблиця 4

Параметри адресації мережі для прикладу

Мережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	MAC-адреса	IP-адреса	Маска	Префікс
Мережа А	–	–	195.10.1.0	255.255.255.0	/24
Маршрутизатор R-1	Інтерфейс Gi0/0	CA-01-07-FE-00-08	195.10.1.254	255.255.255.0	/24
	Інтерфейс Gi0/1	*	*	*	*
Комутатор SW-1	Інтерфейс Vlan 1	00-D0-B1-E1-14-11	195.10.1.252	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–
Робоча станція WS-A1 (Windows XP)	Мережний адаптер	00-60-5C-16-8B-30	195.10.1.1	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–
	Альтернат. DNS-сервер 1	–	8.8.8.8		–
	Альтернат. DNS-сервер 2	–	8.8.4.4	–	–
Робоча станція WS-A2 (Windows 7)	Мережний адаптер	00-10-43-2C-BD-BB	195.10.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–
	Альтернат. DNS-сервер 1	–	8.8.8.8		–
	Альтернат. DNS-сервер 2	–	8.8.4.4	–	–
Робоча станція WS-A3 (Linux Debian)	Мережний адаптер	00-10-11-49-ED-09	195.10.1.3	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–
	Альтернат. DNS-сервер 1	–	8.8.8.8		–
	Альтернат. DNS-сервер 2	–	8.8.4.4	–	–
Робоча станція WS-A4 (Linux CentOS)	Мережний адаптер	00-00-27-32-F9-E7	195.10.1.4	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–
	Альтернат. DNS-сервер 1	–	8.8.8.8		–
	Альтернат. DNS-сервер 2	–	8.8.4.4	–	–

Примітка: * – параметри адресації не зазначені.

Сценарій налагодження параметрів функціонування маршрутизатора мережі R-1 наведено нижче.

```
…
Router>enable
Router#configure terminal
Router(config)#hostname R-1
R-1(config)#interface GigabitEthernet 0/0
R-1(config-if)#description LAN-A(LINK_TO_SW-1)
R-1(config-if)#ip address 195.10.1.254 255.255.255.0
R-1(config-if)#arp timeout 600
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#exit
R-1#
…
```

Сценарій налагодження параметрів функціонування комутатора мережі SW-1 наведено нижче.

```
…
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-1
SW-1(config)#interface vlan 1
SW-1(config-if)#ip address 195.10.1.252 255.255.255.0
SW-1(config-if)#mac-address 00D0.B1E1.1411
SW-1(config-if)#arp timeout 600
SW-1(config-if)#no shutdown
SW-1(config-if)#exit
SW-1(config)#ip default-gateway 195.10.1.254
SW-1(config)#ip name-server 195.10.1.254
SW-1(config)#ip domain-name MY.NET
SW-1(config)#no ip domain-lookup
SW-1(config)#exit
SW-1#
…
```

Сценарій налагодження параметрів IP-адресації (IP-адреси, маски, IP-адреси основного шлюзу, IP-адрес DNS-серверів) робочої станції WS-A-1 (ОС Windows XP) наведено нижче.

1. Через ,,Панель управления" запустити на виконання додаток ,,Сетевые подключения".

2. Серед переліку наявних мережних підключень обрати необхідне підключення.

3. Для обраного мережного підключення натиснути кнопку ,,Свойства" для виведення переліку його компонентів.

4. Обрати компонент ,,Протокол Интернета (TCP/IP)" та натиснути кнопку ,,Свойства".

5. Ввести у відповідні поля параметри IP-адресації (IP-адресу, маску, IP-адресу основного шлюзу, IP-адреси основного та додаткового DNS-серверів).

6. Натиснути кнопку ,,Дополнительно" та за допомогою відповідних засобів увести додаткові параметри IP-адресації.

7. Активувати налагоджені параметри.

Сценарій налагодження параметрів IP-адресації (IP-адреси, маски, IP-адреси основного шлюзу, IP-адрес DNS-серверів) робочої станції WS-A-2 (ОС Windows 7) наведено нижче.

1. Через ,,Панель управления" запустити на виконання додаток ,,Центр управления сетями и общим доступом".

2. Для виведення переліку наявних мережних підключень обрати вкладку ,,Изменение параметров адаптера".

2. Серед переліку наявних мережних підключень обрати необхідне підключення.

3. Для обраного мережного підключення натиснути кнопку ,,Свойства" для виведення переліку його компонентів.

4. Обрати компонент ,,Протокол Интернета версии 4 (TCP/IPv4)" та натиснути кнопку ,,Свойства".

5. Ввести у відповідні поля параметри IP-адресації (IP-адресу, маску, IP-адресу основного шлюзу, IP-адреси основного та додаткового DNS-серверів).

6. Натиснути кнопку ,,Дополнительно" та за допомогою відповідних засобів увести додаткові параметри IP-адресації.

7. Активувати налагоджені параметри.

Сценарій налагодження параметрів адресації (IP-адреси, маски, IP-адреси шлюзу за замовчуванням) робочої станції WS-A-3 (ОС Linux Debian) за допомогою команд наведено нижче.

```
…
root@debian8-3:~# hostname WS-A-3
root@debian8-3:~# ifconfig eth0 down
root@debian8-3:~# ifconfig eth0 195.10.1.3 netmask 255.255.255.0
root@debian8-3:~# ifconfig eth0 up
root@debian8-3:~# route add default gw 195.10.1.254
root@debian8-3:~#
…
```

Сценарій налагодження параметрів адресації (IP-адреси, маски, IP-адреси шлюзу за замовчуванням) робочої станції WS-A-4 (ОС Linux CentOS) за допомогою команд **ip** наведено нижче.

```
…
root@centos:~#hostname WS-A-4
root@WS-A-4:~#ip link set enp0s3 down
root@WS-A-4:~#ip addr add 195.10.1.4/24 dev enp0s3
root@WS-A-4:~#ip route add default via 195.10.1.254
root@WS-A-4:~#ip link set enp0s3 up
root@WS-A-4:~#
…
```

Результати виконання команд моніторингу встановлених відповідностей між фізичними і логічними адресами для розглянутого прикладу

З метою перегляду інформації про налагоджені параметри фізичної і логічної адресації мережних адаптерів/інтерфейсів робочих станцій мережі для розглянутого прикладу використано команди ОС Windows **ipconfig** та ОС Linux **ifconfig**, **ip addr show**, для комутатора та маршрутизатора Cisco – команду Cisco IOS **show interfaces**. Для перевірки зв'язку між вузлами використано команди **ping** та **arping**. З метою перегляду встановлених відповідностей між логічними і фізичними адресами на вузлах ОС Windows та ОС Linux використано команду **arp**, на комутаторі та маршрутизаторі – команду Cisco IOS **show arp**. Результати роботи цих команд для робочих станцій WS-A-1 – WS-A-3, комутатора SW-1 та маршрутизатора R-1 наведено відповідно на рис. 12–22.

Для перехоплення трафіка протоколу ARP на робочій станції WS-A-1 встановлено та використано відкритий кросплатформний програмний аналізатор трафіка (сніфер) WireShark (http://www.wireshark.org). Уміст перехопленого ARP-запиту від робочої станції WS-A-1 до робочої станції WS-A-2 наведено на рис. 23, а. Вміст ARP-відповіді робочої станції WS-A-2 на отриманий запит наведено на рис. 23, б.

```
C:\>ipconfig /all

Настройка протокола IP для Windows
        Имя компьтера . . . . . . . . . . : WS-A-1
        Основной DNS-суффикс  . . . . . . :
        Тип узла. . . . . . . . . . . . . : неизвестный
        IP-маршрутизация включена . . . . : нет
        WINS-прокси включен . . . . . . . : нет

Подключение по локальной сети – Ethernet адаптер:
        DNS-суффикс этого подключения . . :
        Описание  . . . . . . . . . . . . : AMD PCNET Family Ethernet Adapter (PCI)
        Физический адрес. . . . . . . . . : 00-60-5C-16-8B-30
        DHCP включен. . . . . . . . . . . : да
        Автонастройка включена  . . . . . : да
        IP- адрес . . . . . . . . . . . . : 195.10.1.1
        Маска подсети . . . . . . . . . . : 255.255.255.0
        Основной шлюз . . . . . . . . . . : 195.10.1.254
        DNS-серверы . . . . . . . . . . . : 195.10.1.254
                                            8.8.8.8
                                            8.8.4.4
C:\>
```

Рис. 12. Результат виконання команди **ipconfig /all** на робочій станції WS-A-1

```
C:\>ipconfig /all

Настройка протокола IP для Windows
        Имя компьтера . . . . . . . . . . : WS-A-2
        Основной DNS-суффикс  . . . . . . :
        Тип узла. . . . . . . . . . . . . : Гибридный
        IP-маршрутизация включена . . . . : Нет
        WINS-прокси включен . . . . . . . : Нет

Ethernet адаптер Подключение по локальной сети:
        DNS-суффикс подключения . . . . . :
        Описание  . . . . . . . . . . . . : AMD PCNET Family Ethernet Adapter (PCI)
        Физический адрес. . . . . . . . . : 00-10-43-2C-BD-BB
        DHCP включен. . . . . . . . . . . : Нет
        Автонастройка включена  . . . . . : Да
        IPv4-адрес. . . . . . . . . . . . : 195.10.1.2<Основной>
        Маска подсети . . . . . . . . . . : 255.255.255.0
        Основной шлюз . . . . . . . . . . : 195.10.1.254
        DNS-серверы . . . . . . . . . . . : 195.10.1.254
                                            8.8.8.8
                                            8.8.4.4
        NetBIOS через TCP/IP              : включен
...
C:\>
```

Рис. 13. Результат виконання команди **ipconfig /all** на робочій станції WS-A-2

```
root@debian8-3:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:10:11:49:ed:09
          inet addr:195.10.1.3  Bcast:195.10.1.255  Mask:255.255.255.0
          inet6 addr: fe80::210:11ff:fe49:ed09/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:26368 (25.7 KiB)  TX bytes:4014 (3.9KiB)
root@debian8-3:~#
```

Рис. 14. Результат виконання команди **ifconfig eth0** на робочій станції WS-A-3

```
[root@localhost /]# ip addr show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP, LOWER_UP> mtu 1500 qdisc pfofo_fast state UP
qlen 1000
    Link/ether 00:00:27:32:f9:e7 brd ff:ff:ff:ff:ff:ff
    inet 195.10.1.3/24 scope global enp0s3
       valid_lft firever prefferes_lft forever
    Inet6 fe80::200:27ff:fe32:f9e7/64 scope link
       valid_lft firever prefferes_lft forever
[root@localhost /]#
```

Рис. 15. Результат виконання команди **ip addr show enp0s3** на робочій станції WS-A-4

```
SW-1#show interfaces vlan 1
Vlan1 is up, line protocol is up
  Hardware is Ethernet SVI, address is 00d0.b1e1.1411 (bia aabb.cc80.0100)
  Internet address is 195.10.1.252/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 00:10:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
...
SW-1#
```

Рис. 16. Результат виконання команди **show interfaces vlan 1** на комутаторі SW-1

```
R-1#show interfaces GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is i82543 (Livengood), address is ca01.07fe.0008 (bia ca01.07fe.0008)
  Description: LAN-A(LINK_TO_SW-1)
  Internet address is 195.10.1.254/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, link type is autonegotiation, media type is SX
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 00:10:00
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     35 packets input, 4611 bytes, 0 no buffer
     Received 38 broadcasts, 0 runts, 0 giants, 0 throttles
...
R-1#
```

Рис. 17. Результат виконання команди **show interfaces GigabitEthernet 0/0** на маршрутизаторі R-1

```
SW-1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  195.10.1.1             2   0060.5c16.8b30  ARPA   Vlan1
Internet  195.10.1.2             0   0010.432c.bdbb  ARPA   Vlan1
Internet  195.10.1.3             2   0010.1149.ed09  ARPA   Vlan1
Internet  195.10.1.4             2   0000.2732.f9e7  ARPA   Vlan1
Internet  195.10.1.252           -   00d0.b1e1.1411  ARPA   Vlan1
Internet  195.10.1.244           2   ca01.07fe.0008  ARPA   Vlan1
SW-1#
```

Рис. 18. Результат виконання команди **show arp** на комутаторі SW-1

```
C:\>arp –a
Интерфейс: 195.10.1.1 --- 0x2
  Адрес IP             Физический адрес          Тип
  195.10.1.2           00-10-43-2c-bd-bb       динамический
  195.10.1.3           00-10-11-49-ed-09       динамический
  195.10.1.4           00-00-27-32-f9-e7       динамический
  195.10.1.252         00-d0-bl-el-14-ll       динамический
  195.10.1.254         ca-01-07-fe-00-08       динамический
C:\>
```

Рис. 19. Результат виконання команди **arp -a** на робочій станції WS-A-1

```
C:\>arp –a
Интерфейс: 195.10.1.2 --- 0xb
  адрес в Интернете      Физический адрес        Тип
  195.10.1.1           00-60-5c-16-8b-30       динамический
  195.10.1.3           00-10-11-49-ed-09       динамический
  195.10.1.4           00-00-27-32-f9-e7       динамический
  195.10.1.252         00-d0-bl-el-14-ll       динамический
  195.10.1.254         ca-01-07-fe-00-08       динамический
  195.10.1.255         ff-ff-ff-ff-ff-ff       статический
  224.0.0.22           01-00-5e-00-00-16       статический
  224.0.0.252          01-00-5e-00-00-fc       статический
  255.255.255.255      ff-ff-ff-ff-ff-ff       статический
C:\>
```

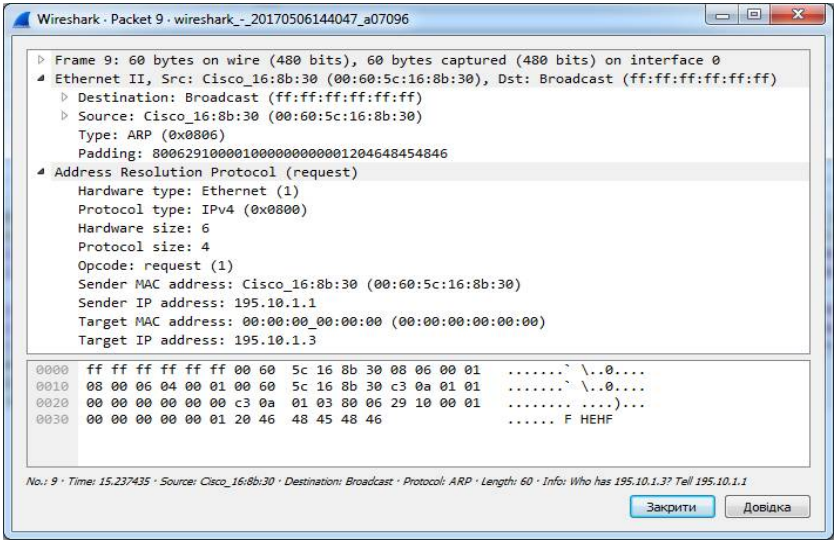
Рис. 20. Результат виконання команди **arp -a** на робочій станції WS-A-2

```
root@debian8-3:~# arp -a
? (195.10.1.252)  at  00:d0:b1:e1:14:11  [ether]  on eth0
? (195.10.1.1)  at  00:60:5c:16:8b:30  [ether]  on eth0
? (195.10.1.2)  at  00:10:43:2c:bd:bb  [ether]  on eth0
? (195.10.1.3)  at  00:10:11:49:ed:09  [ether]  on eth0
? (195.10.1.4)  at  00:00:27:32:f9:e7  [ether]  on eth0
? (195.10.1.252)  at  00:d0:bl:el:14:ll  [ether]  on eth0
? (195.10.1.254)  at  ca:01:07:fe:00:08  [ether]  on eth0
root@debian8-3:~#
```

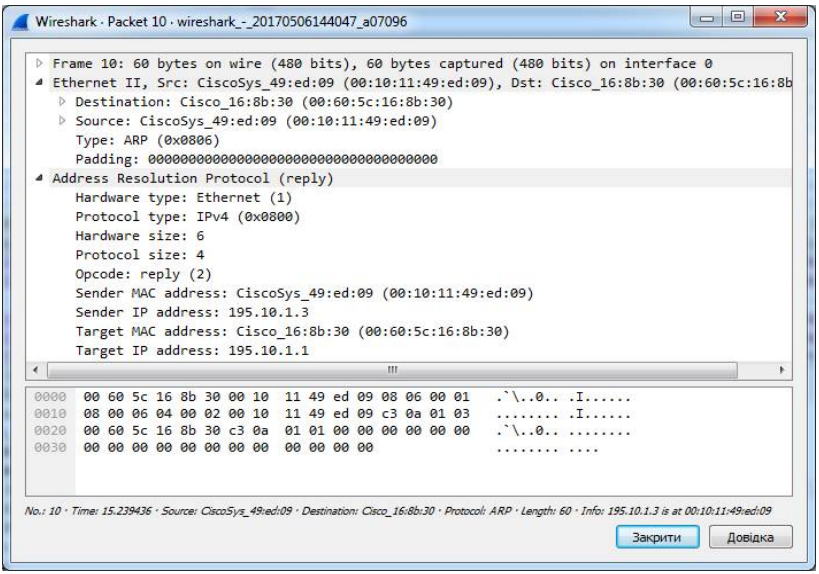
Рис. 21. Результат виконання команди **arp -a** на робочій станції WS-A-3

```
root@debian8-3:~# arping -C 5 195.10.1.1
ARPING 195.10.1.1
60 bytes from 00:60:5c:16:8b:30 (195.10.1.1): index=0 time=1.001 sec
60 bytes from 00:60:5c:16:8b:30 (195.10.1.1): index=1 time=1.002 sec
60 bytes from 00:60:5c:16:8b:30 (195.10.1.1): index=2 time=1.001 sec
60 bytes from 00:60:5c:16:8b:30 (195.10.1.1): index=3 time=1.001 sec
60 bytes from 00:60:5c:16:8b:30 (195.10.1.1): index=4 time=1.002 sec
--- 195.10.1.1 statistics ---
5 packets transmitted, 5 packets received,   0% unanswered (0 extra)
rtt min/avg/max/std-dev = 1001.226/1001.487/1001.837/0.202 ms
root@debian8-3:~#
```

Рис. 22. Результат виконання команди **arping** на робочій станції WS-A-3



а



б

Рис. 23. Вміст перехоплених на робочій станції WS-A-1
повідомлень протоколу ARP: а – ARP-запит; б – ARP-відповідь

Завдання на лабораторну роботу

1. У середовищі програмного емулятора/симулятора створити проект локальної комп'ютерної мережі (рис. 24). Для побудованої мережі заповнити описову таблицю, аналогічну табл. 3.

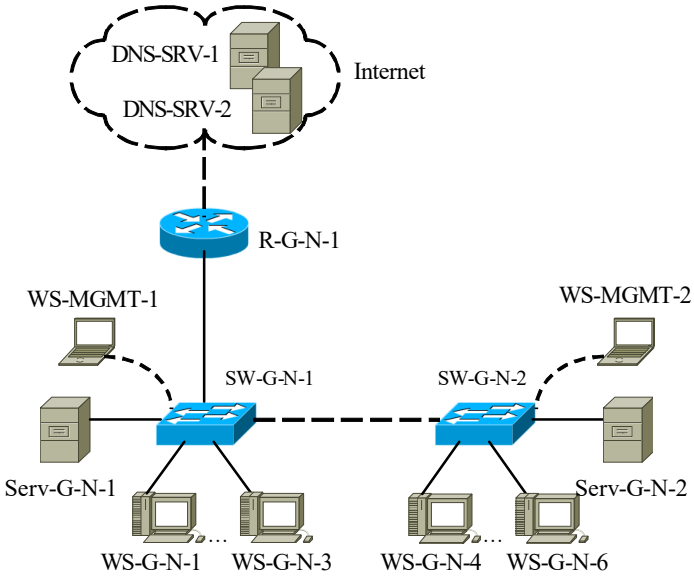


Рис. 24. Проект мережі

2. Розробити схему адресації пристроїв (як кінцевих вузлів, так і комунікаційних пристроїв) мережі. Для цього скористатися даними табл. 5, 6. Під час розрахунку враховувати, що комутатору та інтерфейсу маршрутизатора мережі також виділяється по одній IP-адресі. Результати навести у вигляді таблиці, аналогічної табл. 4.

Таблиця 5

Параметри для розрахунку п. 2

№ варі-анта	IP-адреса мережі A	Префікс	IP-адреса шлюзу за замовчуванням/ IP-адреса DNS-сервера
1	191.G.N.0	/24	Перша IP-адреса діапазону
2	192.G.N.0	/25	Остання IP-адреса діапазону
3	193.G.N.0	/26	Перша IP-адреса діапазону
4	194.G.N.0	/27	Остання IP-адреса діапазону
5	195.G.N.0	/28	Перша IP-адреса діапазону
6	196.G.N.0	/24	Остання IP-адреса діапазону
7	197.G.N.0	/25	Перша IP-адреса діапазону
8	198.G.N.0	/26	Остання IP-адреса діапазону
9	199.G.N.0	/27	Перша IP-адреса діапазону
10	200.G.N.0	/28	Остання IP-адреса діапазону
11	201.G.N.0	/24	Перша IP-адреса діапазону
12	202.G.N.0	/25	Остання IP-адреса діапазону
13	203.G.N.0	/26	Перша IP-адреса діапазону
14	204.G.N.0	/27	Остання IP-адреса діапазону
15	205.G.N.0	/28	Перша IP-адреса діапазону
16	206.G.N.0	/24	Остання IP-адреса діапазону
17	207.G.N.0	/25	Перша IP-адреса діапазону
18	208.G.N.0	/26	Остання IP-адреса діапазону
19	209.G.N.0	/27	Перша IP-адреса діапазону
20	210.G.N.0	/28	Остання IP-адреса діапазону
21	211.G.N.0	/24	Перша IP-адреса діапазону
22	212.G.N.0	/25	Остання IP-адреса діапазону
23	213.G.N.0	/26	Перша IP-адреса діапазону
24	214.G.N.0	/27	Остання IP-адреса діапазону
25	215.G.N.0	/28	Перша IP-адреса діапазону
26	216.G.N.0	/24	Остання IP-адреса діапазону
27	217.G.N.0	/25	Перша IP-адреса діапазону
28	218.G.N.0	/26	Остання IP-адреса діапазону
29	219.G.N.0	/27	Перша IP-адреса діапазону
30	220.G.N.0	/28	Остання IP-адреса діапазону
31	221.G.N.0	/24	Перша IP-адреса діапазону
32	222.G.N.0	/25	Остання IP-адреса діапазону
33	223.G.N.0	/26	Перша IP-адреса діапазону

Таблиця 6

Дані для визначення параметрів адресації мережі

№ варіанта	IP-адреса альтернативного DNS-сервера 1	IP-адреса альтернативного DNS-сервера 2
1	Level3 Communications	Level3 Communications
2	Google	Google
3	OpenDNS Home	OpenDNS Home
4	Securly	Securly
5	Comodo Secure DNS	Comodo Secure DNS
6	DNS Advantage	DNS Advantage
7	Norton ConnectSafe	Norton ConnectSafe
8	SafeDNS	SafeDNS
9	OpenNIC	OpenNIC
10	Public-Root	Public-Root
11	Level3 Com-ns	Level3 Com-ns
12	Google	Google
13	OpenDNS Home	OpenDNS Home
14	Securly	Securly
15	Comodo Secure DNS	Comodo Secure DNS
16	DNS Advantage	DNS Advantage
17	Norton ConnectSafe	Norton ConnectSafe
18	SafeDNS	SafeDNS
19	OpenNIC	OpenNIC
20	Public-Root	Public-Root
21	Level3 Com-ns	Level3 Com-ns
22	Google	Google
23	OpenDNS Home	OpenDNS Home
24	Securly	Securly
25	Comodo Secure DNS	Comodo Secure DNS
26	DNS Advantage	DNS Advantage
27	Norton ConnectSafe	Norton ConnectSafe
28	SafeDNS	SafeDNS
29	OpenNIC	OpenNIC
30	Public-Root	Public-Root
31	AdGuard DNS	AdGuard DNS
32	Fourth Estate	Fourth Estate
33	CenturyLink (Level3)	CenturyLink (Level3)

3. Сформувати повідомлення ARP-запити, що надсилаються з робочої станції (табл. 8) до комутатора, маршрутизатора та одного з серверів мережі для формування адресних відповідностей. Сформувати повідомлення ARP-відповіді, що надходять від вузлів-відповідачів. ARP-запити та ARP-відповіді показати як такі, що інкапсульовані у кадри Ethernet. Побудувати ARP-таблицю робочої станції після надходження ARP-відповідей.

4. Провести налагодження параметрів іменування та параметрів IP-адресації мережних адаптерів/інтерфейсів пристроїв мережі згідно з даними п. 1, 2. При налагодженні врахувати, що налагодження альтернативного DNS-сервера не завжди є можливим.

Таблиця 8

Параметри для виконання п. 3

№ варіанта	Робоча станція	№ варіанта	Робоча станція	№ варіанта	Робоча станція
1	WS-G-N-1	12	WS-G-N-6	23	WS-G-N-5
2	WS-G-N-2	13	WS-G-N-1	24	WS-G-N-6
3	WS-G-N-3	14	WS-G-N-2	25	WS-G-N-1
4	WS-G-N-4	15	WS-G-N-3	26	WS-G-N-2
5	WS-G-N-5	16	WS-G-N-4	27	WS-G-N-3
6	WS-G-N-6	17	WS-G-N-5	28	WS-G-N-4
7	WS-G-N-1	18	WS-G-N-6	29	WS-G-N-5
8	WS-G-N-2	19	WS-G-N-1	30	WS-G-N-6
9	WS-G-N-3	20	WS-G-N-2	31	WS-G-N-1
10	WS-G-N-4	21	WS-G-N-3	32	WS-G-N-2
11	WS-G-N-5	22	WS-G-N-4	33	WS-G-N-3

5. Провести налагодження тайм-ауту утримання ARP-записів в ARP-таблицях пристроїв мережі. Для вибору значення тайм-ауту скористатися даними табл. 9 (необов’язково).

Таблиця 9

Параметри для виконання п. 5

№ варіанта	Тайм-аут, хв	№ варіанта	Тайм-аут, хв	№ варіанта	Тайм-аут, хв
1	5	12	5	23	20

2	10	13	8	24	3
3	15	14	10	25	5
4	20	15	12	26	7
5	6	16	15	27	9
6	11	17	20	28	11
7	16	18	25	29	13
8	21	19	4	30	15
9	7	20	8	31	5
10	12	21	12	32	10
11	3	22	16	33	15

6. Перевірити можливість інформаційного обміну між робочою станцією (табл. 8) та рештою робочих станцій та комунікаційних пристроїв мережі за допомогою команд **ping** та **arping** (за можливості).

7. Вивести ARP-таблицю робочої станції (табл. 8) та порівняти її з отриманою у п. 3. Вивести ARP-таблиці решти пристроїв мережі.

8. Очистити ARP-таблиці всіх вузлів мережі. На робочій станції (табл. 8) запустити програмний аналізатор трафіка, здійснити інформаційний обмін та провести перехоплення ARP-повідомлень, що передаються між цією станцією і рештою пристроїв мережі під час обміну.

9. Дослідити перехоплені програмним аналізатором трафіка ARP-повідомлення та порівняти їх із сформованими у п. 3.

10. Очистити ARP-таблиці всіх робочих станцій та комунікаційних пристроїв мережі. Внести статичні ARP-записи у ARP-таблиці серверів мережі та комунікаційних пристроїв мережі.

11. На робочій станції (табл. 8) повторно запустити програмний аналізатор трафіка, здійснити інформаційний обмін та дослідити процес функціонування засобів протоколу ARP на робочій станції за умови застосування статичних ARP-записів.

12. Для заданої IP-адреси версії 4 (табл. 10) визначити MAC-адресу групової розсилки. За можливості визначити, повідомлення якого протоколу передається за допомогою даної адреси.

13. Для заданої MAC-адреси групової розсилки (табл. 11) визначити IP-адресу (можливі IP-адреси) групової розсилки. За можливості визначити, повідомлення якого протоколу передається у кадрі з такою адресою.

Таблиця 10

Параметри для розрахунку п. 12

№ варіанта	IP-адреса	№ варіанта	IP-адреса
1	224.0.0.1	16	224.0.0.10
2	224.0.0.2	17	224.15.0.65
3	224.20.75.25	18	224.0.0.11
4	224.0.0.4	19	224.35.0.85
5	224.40.115.45	20	224.0.0.12
6	224.0.0.5	21	224.0.0.13
7	224.60.155.85	22	224.0.0.18
8	224.0.0.6	23	224.75.20.135
9	224.80.195.125	24	224.0.0.22
10	224.0.0.7	25	224.95.40.155
11	224.100.0.5	26	224.0.0.102
12	224.0.0.8	27	224.215.60.165
13	224.0.0.107	28	224.0.0.251
14	224.0.0.9	29	224.235.80.185
15	224.140.0.45	30	224.0.1.1

Таблиця 11

Параметри для розрахунку п. 13

№ варіанта	MAC-адреса	№ варіанта	MAC-адреса
1	01-00-5E-00-AF-B1	16	01-00-5E-10-CC-B2
2	01-00-5E-01-AE-B3	17	01-00-5E-11-CB-B4
3	01-00-5E-02-AD-B7	18	01-00-5E-12-CA-B6
4	01-00-5E-03-AC-B9	19	01-00-5E-13-DF-B8
5	01-00-5E-04-AB-BB	20	01-00-5E-14-DE-BA
6	01-00-5E-05-AA-BE	21	01-00-5E-15-DD-BC
7	01-00-5E-06-BF-BF	22	01-00-5E-16-DC-BE
8	01-00-5E-07-BE-A1	23	01-00-5E-17-DB-A2
9	01-00-5E-08-BD-A3	24	01-00-5E-18-DA-A4
10	01-00-5E-09-BC-A5	25	01-00-5E-19-EF-A6
11	01-00-5E-0A-BB-A7	26	01-00-5E-1A-EE-A8
12	01-00-5E-0B-BA-A9	27	01-00-5E-1B-ED-AA
13	01-00-5E-0C-CF-AB	28	01-00-5E-1C-EC-AC
14	01-00-5E-0D-CE-AE	29	01-00-5E-1D-EB-AF
15	01-00-5E-0E-CD-AF	30	01-00-5E-1E-EA-FF

Контрольні питання

1. Протоколи та правила встановлення відповідностей між фізичними і логічними адресами в IP-мережах за умови застосування IP-адрес версії 4.
2. Правило формування групових MAC-адрес на основі групових IP-адрес версії 4.
3. Правило формування широкомовних MAC-адрес на основі широкомовних IP-адрес версії 4.
4. Загальна характеристика протоколу ARP.
5. Стандартизація протоколу ARP.
6. Характеристики протоколу ARP стосовно моделі OSI та стеку TCP/IP.
7. Структура повідомлення протоколу ARP.
8. Види повідомлень протоколу ARP.
9. Структура ARP-таблиці.
10. Джерела заповнення ARP-таблиці.
11. Алгоритми роботи протоколу ARP.
12. Призначення та синтаксис команди **arp**.
13. Призначення та синтаксис команди **arping**.
14. Команди моніторингу стану ARP-таблиць комунікаційних пристроїв Cisco.
15. Команди операцій з ARP-таблицями комунікаційних пристроїв Cisco.