

ЗАТВЕРДЖУЮ
Директор ЗПО «ДПТК»
31.08.2026 р.
Олександр СТРИЛЕЦЬ
ПОГОДЖЕНО
Заступник директора з навчально-методичної
роботи ЗПО «ДПТК»
31.08.2026 р.
Сергій ГОРДІЄНКО

ВСТУП

Комп'ютерний практикум відповідає робочій програмі навчальної дисципліни «Комп'ютерні мережі в електроніці» і сприяє формуванню у здобувачів освіти необхідних знань, навичок і вмінь згідно з вимогами освітньо-професійної програми підготовки фахівців за спеціальністю G5 – Електроніка, електронні комунікації, приладобудування та радіотехніка.

Виконання наведених у навчальному посібнику комп'ютерних практикумів дозволить здобувачам освіти:

ознайомитися з топологіями та інструментарієм моделювання невеликих комп'ютерних мереж, використовувати TCP/IP протоколи та модель OSI, використовувати Packet Tracer для перегляду протокольних блоків даних;

навчитися користуватися командами IOS та знаходити помилки в конфігурації мережевих пристроїв;

ознайомитись з програмними засобами діагностики мереж, освоївши при цьому `arp`, `arping`, `ping`, `tracert`, `mtr`;

ознайомитися і навчитися працювати з такими мережевими сніферами, як `tcpdump` та `Wireshark`; освоїти аналізатори мережевого трафіку, отримати навички написання фільтрів для аналізаторів та ознайомитися зі стеком мережевих протоколів;

ознайомитися з клієнт-серверною взаємодією, UDP і TCP номерами портів та операцій, прикладним та транспортним рівнями; поняття шлюзу та маршрутизація пакетів;

ознайомитися з методами конфігурації ПК, освоївши при цьому роботу з командами `ifconfig` та `route`, а також вивчивши файли `resolv.conf`, `hosts` і `services`;

дізнатися команди для моніторингу мережі, їх призначення; адресація та типи адрес.

КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 1

Тема: Топології мереж, освоєння Packet Tracer.

Мета заняття: Ознайомитися з топологіями та інструментарієм моделювання невеликих комп'ютерних мереж. Використання TCP/IP протоколів та моделі OSI. Використання Packet Tracer для перегляду протокольних блоків даних (Protocol Data Units – PDU).

Теоретичні відомості

Cisco Packet Tracer (CPT) – це безкоштовний, високоякісний симулятор комп'ютерних мереж, розроблений компанією Cisco Systems — провідним світовим виробником мережевого обладнання для маршрутизації, комутації, віддаленого доступу, забезпечення безпеки, управління мережами зберігання даних тощо. Програма створена для навчання та практичного засвоєння навичок у сфері мережевих технологій.

Інструмент дозволяє виконувати такі завдання: проектування мережевої топології з використанням функції drag-and-drop, віртуальні практичні заняття без необхідності фізичного обладнання, тестування конфігурацій і виправлення проблем, а також моделювання передачі даних у реальному часі. Програмне забезпечення сумісне з Windows, Linux і MacOS, завантажити його можна за посиланням: <https://www.netacad.com/resources/lab-downloads> (рисунок 1.1).



Рисунок 1.1 – Інструкція щодо встановлення Cisco Packet Tracer

Інтерфейс Packet Tracer дозволяє інтуїтивно працювати з ним та складається з кількох основних областей (рисунок 1.2.).

1. Головне меню та панель інструментів (зверху). Пункти меню: File, Edit, Options, View, Tools, Extensions, Help. Швидкі кнопки: New, Open, Save, Print, Zoom тощо.

2. Панель вибору пристроїв (знизу зліва). Містить категорії обладнання: Routers (маршрутизатори), Switches (комутатори), End Devices (кінцеві пристрої: ПК, ноутбуки, принтери), Wireless Devices (бездротові пристрої), Connections (кабелі та з'єднання), Security (міжмережеві екрани), IoT (пристрої інтернету речей), Multiuser Connection (багатокористувацьке підключення).

3. Робоча область (центр екрану). Можливе перемикання між областями Логічна топологія (де користувач розміщує та з'єднує пристрої) та Фізична топологія (3D-вид мережі).

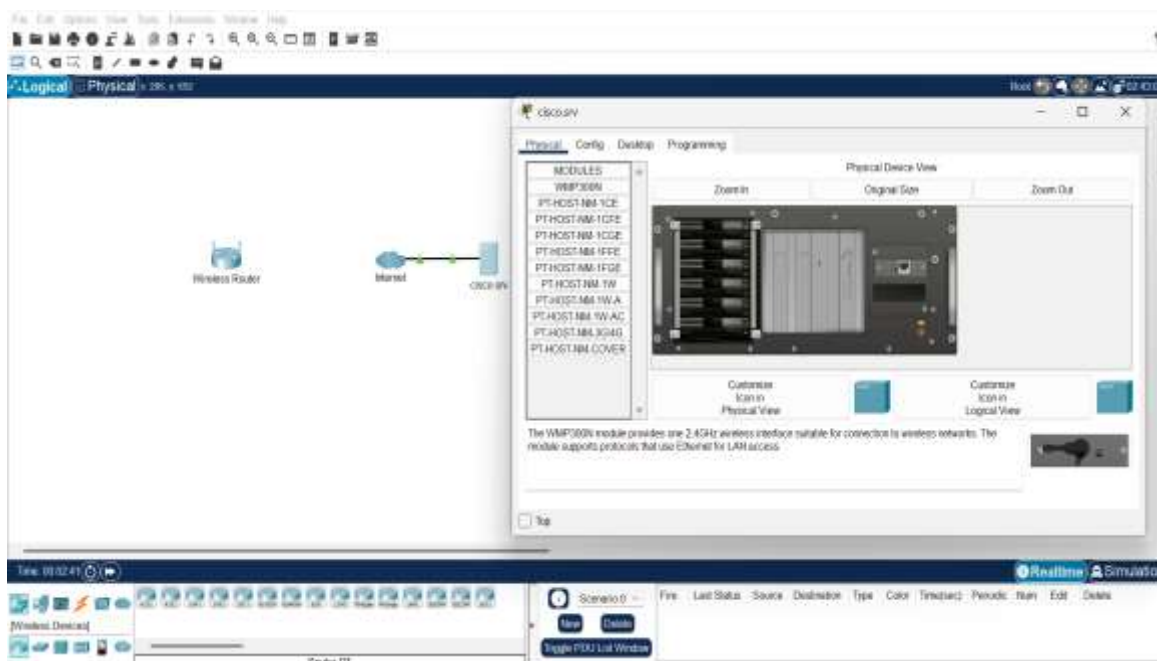


Рисунок 1.2 – Інтерфейс Packet Tracer

4. Панель режимів роботи (праворуч знизу). Режим Realtime (реальний час) – це дослідження роботи мережі в реальному часі. Режим Simulation (симуляція) – це дослідження покрокової передачі пакетів для навчання.

5. Вікно конфігурації пристрою, яке відкривається при кліку на будь-який пристрій та містить наступні вкладки: Physical (фізичний вигляд, додавання модулів), Config (графічний інтерфейс для конфігурації), CLI (командний рядок як на реальному обладнанні Cisco), Desktop (для кінцевих пристроїв: IP-конфігурація, браузер, CMD), Services (сервіси для серверів: DHCP, DNS, HTTP), тощо.

6. Панель фільтрів подій (у режимі Simulation), яка показує передачу пакетів та за допомогою якої можна фільтрувати за протоколами (ICMP, HTTP, DNS тощо) та покроково відстежувати рух даних.

Для подання різних пристроїв та з'єднань на мережних схемах в CPT часто використовуються наступні позначення (рисунок 1.3).



Рисунок 1.3 – Позначення на мережних схемах

Схема у простий спосіб зображає те, як зв'язані пристрої у мережі. Така схема називається топологією. Здатність розуміти логічне представлення фізичних компонентів мережі має ключове значення для аналізу її побудови та функціонування. У схемах логічних топологій зображуються пристрої, порти та адресація мережі. Завдяки цим схемам можна чітко визначити, до яких проміжних пристроїв підключені кінцеві пристрої та яке середовище

використовується для цього. Приклад логічної топології представлено на рисунок 1.4.

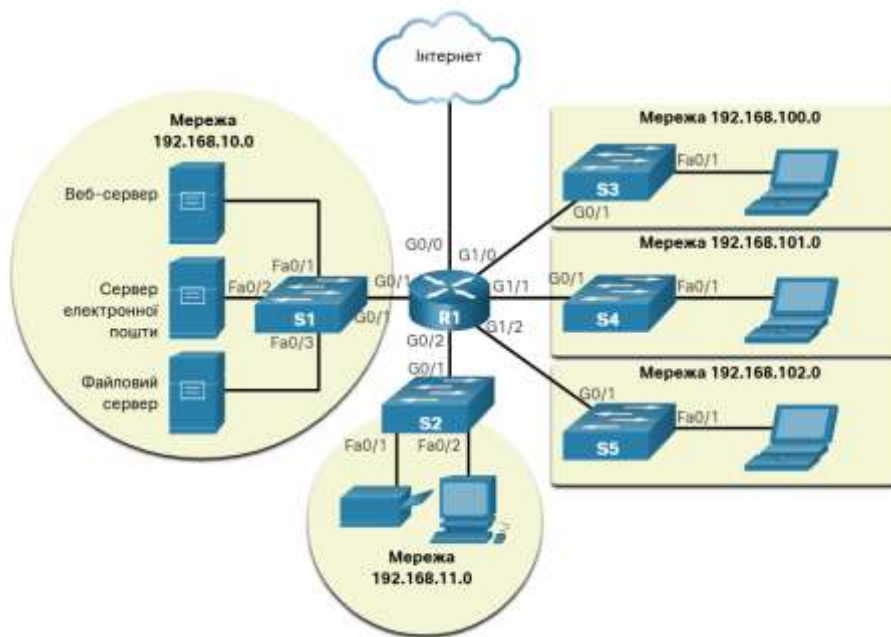


Рисунок 1.4 – Логічна топологія мережі

Для розуміння логічної топології мережі необхідно опанувати наступні визначення.

Мережеві пристрої:

Мережевий концентратор (хаб) – це мережевий пристрій, який об'єднує кілька комп'ютерів чи інших пристроїв у локальну мережу, передаючи дані на всі підключені порти одночасно. Поеднує пристрої в мережу, створюючи топологію «зірка», де всі комп'ютери підключені до центральної точки.

Комутатор (або Switch) – це мережевий пристрій, який з'єднує кілька комп'ютерних пристроїв (комп'ютери, принтери, інші комутатори) в одну локальну мережу (LAN), передаючи дані безпосередньо між пристроєм-відправником та пристроєм-одержувачем, а не всім пристроям одночасно, як це робить концентратор. Комутатор отримує пакет даних від одного з пристроїв, підключених до нього, аналізує пакет – визначає MAC-адресу отримувача, після чого пересилає пакет безпосередньо до пристрою-одержувача, використовуючи

відповідний порт. Отже комутатор оптимізує мережевий трафік, підвищуючи продуктивність мережі та забезпечуючи її безпеку.

Маршрутизатор (або *роутер*) – це мережевий пристрій, який з'єднує дві або більше мережі, керує передачею даних (пакетів) між ними та дозволяє кільком пристроям у локальній мережі спільно використовувати одне підключення до інтернету. Використовує IP-адреси для прийняття рішень. Основне завдання маршрутизатора – пересилання даних за допомогою таблиць маршрутизації, що визначають раціональний шлях для їх доставлення.

Ідентифікація мережевих інтерфейсів. На пристроях Cisco (комутаторах, маршрутизаторах тощо) для ідентифікації мережевих інтерфейсів використовують наступний формат:

Тип інтерфейсу Модуль/Порт

Наприклад, FastEthernet 0/1 або Fa 0/1

Далі наведено приклади де-яких інтерфейсів.

Таблиця. Ethernet інтерфейси (за швидкістю)

Повна назва	Швидкість	Скорочення
Ethernet	10 Мбіт/с	E
FastEthernet	100 Мбіт/с	Fa
GigabitEthernet	1 Гбіт/с	Gi, G
TenGigabitEthernet	10 Гбіт/с	Te
FortyGigabitEthernet	40 Гбіт/с	Fo
HundredGigE	100 Гбіт/с	Hu

Розшифровка G 0/1 наступна:

G = GigabitEthernet (тип інтерфейсу), відповідно швидкість: 1 Гбіт/с (1000 Мбіт/с);

0 = Номер модуля/слота, відповідно вказує на фізичний слот або модуль у пристрої. 0 = перший слот;

1 = Номер порту, відповідно конкретний порт модуля. 1 = другий порт (нумерація починається з 0).

Наприклад, на комутаторах можуть бути десятки портів:

Fa0/1 до Fa0/24 (24 порти FastEthernet);

G0/1 до G0/2 (2 порти GigabitEthernet для аплінків).

Також може використовуватися розширений формат (для модульних пристроїв):

Тип інтерфейсу Слот/Модуль/Порт

Наприклад, GigabitEthernet 1/0/1 – слот 1, модуль 0, порт 1

На рисунку 1.5 показано нумерацію

Figure 1 – Interface Numbering on Cisco 2811 Platform

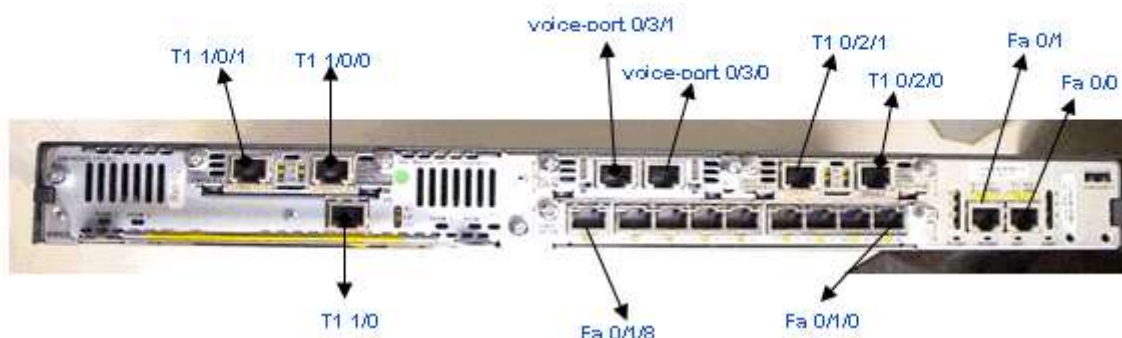


Рисунок 1.5 – Типи та номери інтерфейсів

Кожен інтерфейс позначено стрілкою з відповідною назвою, що вказує на його тип і розташування.

T1 1/0/0, T1 1/0/1, T1 1/0: Інтерфейси T1.

voice-port 0/3/1, voice-port 0/3/0: Голосові порти.

T1 0/2/1, T1 0/2/0: Інтерфейси T1.

Fa 0/1, Fa 0/0, Fa 0/1/8, Fa 0/1/0: Інтерфейси Fast Ethernet (Fa).

Адресація пристроїв.

Існує дві основні адреси, призначені пристрою в локальній мережі Ethernet – фізична та логічна адреси.

Фізична адреса (MAC-адреса) – використовується для комунікації між мережними інтерфейсними картами (NIC) в одній мережі. Це унікальна адреса

кожного пристрою у світі, яка призначається виробником та складається з 48 біт (6 байт). Її формат це 12 шістнадцяткових цифр (наприклад, 00:1E:2D:3C:4B:5A або 00-1E-2D-3C-4B-5A). Де перші 3 байти (OUI) – ідентифікатор виробника, а останні три байти – унікальний номер пристрою. Саме MAC-адреси використовують комутатори для визначення отримувача кадру.

Логічна адреса (IP-адреса) – використовується для надсилання пакета від пристрою-джерела до пристрою-одержувача. IP-адреса призначення може бути в тій самій IP-мережі, що й джерело, або у віддаленій мережі. Маршрутизатори працюють саме з IP-адресами. Використовуються IPv4 та IPv6. Адреса IPv4 – це логічна мережева адреса, яка ідентифікує конкретний хост. Вона має бути належним чином налаштована та унікальна в локальній мережі для локального спілкування. Вона також повинна бути належним чином налаштована та унікальна у світі для віддаленого зв'язку. IPv4-адреса призначається мережному інтерфейсу для хоста. Зазвичай це мережева карта інтерфейсу (NIC), встановлена в пристрої. Приклади пристроїв кінцевих користувачів з мережевими інтерфейсами включають робочі станції, сервери, мережеві принтери та IP-телефони. Деякі сервери можуть мати більше одного NIC, і кожен з них має свою IPv4 адресу. Інтерфейси маршрутизатора, які забезпечують з'єднання з мережею IP, також матимуть IPv4 адресу. IPv4-адреси мають довжину 32 біти. Це приклад адреси IPv4 у двійковому форматі та у десятково-крапковому представленні:

11010001101001011100100000000001 та 209.165.200.1

Нестача адресного простору Ipv4 у зв'язку з лавиноподібним розвитком комп'ютерних мереж стала мотиваційним фактором для переходу на IPv6. Точної дати для переходу на IPv6 поки немає. Як IPv4, так і IPv6 будуть співіснувати найближчим часом, і перехід триватиме кілька років. Фахівці IETF створили різні протоколи та інструменти, які допомагають мережевим адміністраторам поступово здійснити перехід своїх мереж на IPv6. Адреси IPv6 мають довжину 128 бітів і записуються у вигляді рядка шістнадцяткових значень. Кожні чотири біти представлено однією шістнадцятковою цифрою. Наприклад,

2001:0cb8:85b3:0000:0000:8a2c:0370:7334 або у стислому вигляді 2001:0cb8:85b3::8a2c:0370:7334.

Маска мережі. IP-адреса складається з двох основних частин: номера мережі та номера вузла (хоста). Номер мережі ідентифікує мережу, до якої підключено пристрій, це спільна частина IP-адреси для всіх пристроїв в одній локальній мережі. Номер вузла (хоста) ідентифікує конкретний пристрій у межах цієї мережі. Маска мережі – це 32-бітне число, яке використовується разом з IP-адресою для визначення, яка її частина є номером мережі, а яка – номером пристрою (хоста) в цій мережі. Маска складається з одиниць (частина, де стоять одиниці, відповідає частині IP-адреси, що є адресою мережі) і нулів (частина, де стоять нулі, відповідає частині IP-адреси, що є адресою хоста). Наприклад, маска 255.255.255.0 в двійковій системі має такий вигляд 11111111.11111111.11111111.00000000. Це означає, що перші 24 біти IP-адреси є адресою мережі, а останні 8 бітів – адресою хоста. Також цю маску можна записати у вигляді “/24”.

Таблиця. Порівняння MAC та IP-адрес

Параметр	MAC-адреса (Фізична)	IP-адреса (Логічна)
Рівень OSI	2 (канальний)	3 (мережевий)
Призначення	Виробник	Адміністратор/DHCP
Зміна	Постійна	Може змінюватися
Область дії	Локальна мережа	Глобальна (інтернет)
Пристрій	Комутатор	Маршрутизатор
Приклад	00:1A:2B:3C:4D:5E	192.168.1.100

Протоколи передачі даних. Протокол передачі даних – це набір правил і стандартів, які визначають, як дані передаються між пристроями в комп'ютерній мережі. Протоколи містять вимоги до формату повідомлення, розміру

повідомлення, синхронізації, кодування, інкапсуляції, шаблонів повідомлень тощо.

Формат повідомлення. Для надсилання повідомлення від відправника до одержувача необхідно, щоб воно було сформовано відповідно до певного формату або структури. Формати повідомлень залежать від типу повідомлення і каналу, який використовується для його доставлення.

Розмір повідомлення. Існують чіткі правила, які регулюють розмір частин даних, які передаються у мережі. Розмір залежить від типу протоколів або від каналу, який використовується. Якщо з одного хоста на інший через мережу надсилається довге повідомлення, то може виникнути необхідність в розділенні повідомлення на менші частини, щоб забезпечити ефективне доставлення повідомлення.

Синхронізація. Багато функцій мережових підключень залежать від синхронізації у часі. Синхронізація визначає швидкість передавання бітів даних у мережі. Вона також впливає на те, коли окремий вузол може відправляти дані, і на загальний обсяг даних, що може бути переданий однією операцією взаємодії.

Кодування. Повідомлення, що надсилаються мережею, спочатку перетворюються в біти або групи бітів (при багатопозиційному кодуванні) вузлом-відправником. Кожен біт/група бітів кодується у вигляді звуків, світлових хвиль або електричних імпульсів, залежно від мережевого середовища, яким передаються біти/групи бітів. Вузол призначення отримує і декодує сигнали, щоб інтерпретувати повідомлення.

Інкапсуляція. У кожному повідомленні, що передається мережею, має бути заголовок, який містить адресну інформацію, що ідентифікує вузол відправлення та вузол призначення. Інкапсуляція – це процес додавання цієї інформації до фрагментів даних, з яких складається повідомлення. Крім адреси, в заголовку може міститися інша інформація, яка гарантує, що повідомлення буде доставлено правильній програмі на вузлі призначення.

Шаблони повідомлень. В деяких випадках перед надсиланням наступного повідомлення необхідно підтвердити попереднє повідомлення. Цей тип шаблону запиту/відповіді є загальним компонентом багатьох мережних протоколів.

Існує два ключові типи моделей, які застосовуються для опису функцій, необхідних для успішного інформаційного обміну в мережі: модель протоколів та еталонні моделі.

Модель протоколів тісно пов'язана зі структурою певного стеку протоколів. Стек протоколів об'єднує кілька взаємозалежних протоколів, що зазвичай виконують всі функції, потрібні для взаємодії користувачів із мережею передачі даних. Модель TCP/IP є прикладом моделі протоколів, оскільки вона визначає функції, які виконуються на кожному рівні стеку протоколів TCP/IP.

Еталонна модель, у свою чергу, описує функції, що повинні виконуватися на конкретному рівні, але не встановлює чіткого способу їх реалізації. Вона не забезпечує достатньо деталей для точного визначення роботи кожного протоколу на всіх рівнях. Головна задача еталонної моделі полягає у сприянні кращому розумінню функцій і процесів, необхідних для передачі даних у мережі.

Модель OSI. Найвідоміша еталонна модель міжмережної взаємодії була створена Міжнародною організацією зі стандартизації (ISO) в рамках проекту Взаємодія відкритих систем (Open Systems Interconnection, OSI). Вона використовується для проектування мереж передавання даних, визначення технічних вимог до операцій, а також для пошуку і усунення неполадок. Вона складається з 7 рівнів, кожен з яких виконує специфічні функції. Найнижчий – це 1 рівень (фізичний), найвищий – 7 рівень (прикладний).

7 рівень. Прикладний рівень містить протоколи, які використовуються для обміну даними між процесами та людьми.

6 рівень. Рівень представлення даних забезпечує загальне представлення даних, які передаються між службами прикладного рівня.

5 рівень. Сеансовий рівень надає послуги рівню представлення даних для організації його діалогу та керування обміном даними.

4 рівень. Транспортний рівень визначає послуги сегментування, надійного та економічно ефективного передавання, відновлення послідовності даних для індивідуального зв'язку між кінцевими пристроями та виконання інших функцій.

3 рівень. Мережний рівень надає послуги для обміну окремими частинами даних через підмережі між визначеними кінцевими пристроями.

2 рівень. Канальний рівень. Протоколи цього рівня визначають методи обміну кадрами даних між пристроями через спільне середовище передавання даних.

1 рівень. Фізичний рівень. Протоколи цього рівня описують електричні, механічні, функціональні та процедурні засоби для активації, обслуговування та деактивації фізичних з'єднань для передавання бітів пристроєм до лінії зв'язку та прийняття бітів пристроєм з лінії зв'язку.

Робота моделі представлено на рисунку 1.6. Коли дані передаються, вони проходять **зверху вниз** (від рівня 7 до рівня 1) у відправника, де кожен рівень додає свої заголовки (інкапсуляція). У приймача дані проходять **знизу вгору** (від рівня 1 до рівня 7), де кожен рівень обробляє та видаляє свої заголовки (декапсуляція). Основною метою моделі OSI є встановлення стандартної та незалежної від постачальника системи інкапсуляції даних. Вона допомагає різним пристроям і системам працювати разом, дотримуючись одного й того ж набору правил і стандартів. що загалом різні мережеві пристрої працюють на різних рівнях моделі OSI. Причому мережевий пристрій дбає лише про заголовки до певного рівня і не дбає про решту заголовків у повідомленні. Наприклад, комутатор дбає лише про заголовок каналу передачі даних (рівень 2), який складається з MAC-адрес джерела та призначення. Маршрутизатор дбає лише про заголовки рівнів 2 та 3 тощо. Також слід звернути увагу, що кожному рівні моделі OSI дані називаються різними термінами. Наприклад, на рівні 4 TCP-повідомлення називаються сегментом, на рівні 3 – пакетом, а на рівні 2 – кадром.

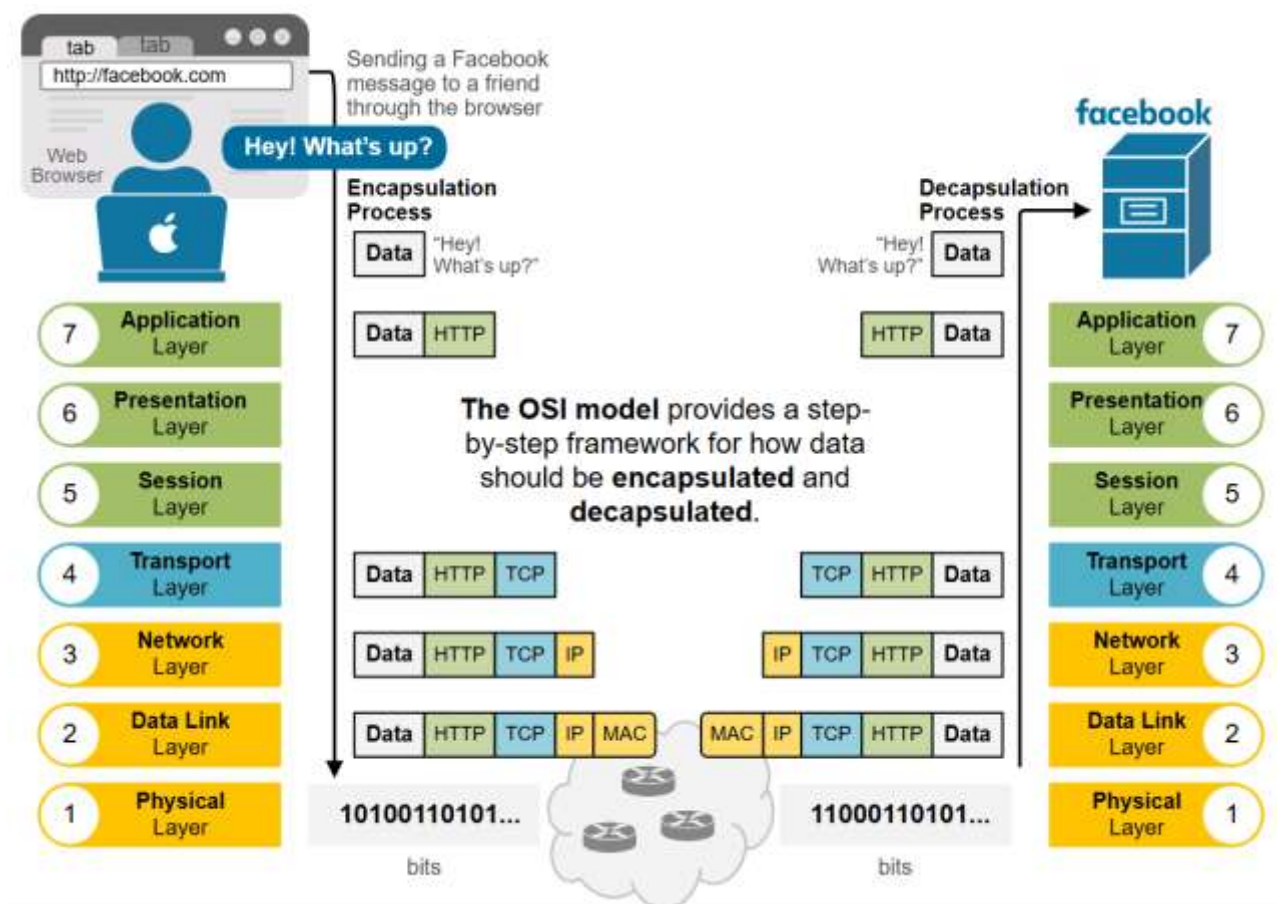


Рисунок 1.6 – Модель OSI

Стек протоколів TCP/IP – це набір комунікаційних протоколів, які використовуються для передачі даних в інтернеті.

Модель TCP/IP визначає як дані передаються від одного комп'ютера до іншого. Модель TCP/IP має 4 рівні, а саме:

Рівень застосунків – відображає дані для користувача, а також забезпечує кодування/шифрування та керування сеансами зв'язку.

Транспортний рівень – підтримує зв'язок між різними пристроями в різних мережах.

Рівень міжмережевої взаємодії (міжмережевий рівень) – визначає найкращий маршрут передавання даних через мережу.

Рівень доступу до мережі (рівень мережевого доступу) – керує фізичними пристроями та середовищем передавання даних, з яких складається мережа.

Модель TCP/IP – це метод візуалізації взаємодій різних протоколів, що складають стек протоколів TCP/IP. Він не описує загальні функції, необхідні для

всіх мережних комунікацій, а описує мережні функції, що притаманні тим протоколам, які використовуються в стеці протоколів TCP/IP.

Стек протоколів TCP/IP можна описати в термінах еталонної моделі OSI. Функції, які в моделі TCP/IP реалізуються на міжмережевому рівні, в моделі OSI містяться на мережному рівні, як показано на рисунку 1.7. Функції транспортного рівня однакові для обох моделей. Однак рівень мережного доступу і прикладний рівень моделі TCP/IP розділені в моделі OSI на додаткові рівні, щоб визначити функції, які повинні виконуватися на цих рівнях (рисунок 1.7).

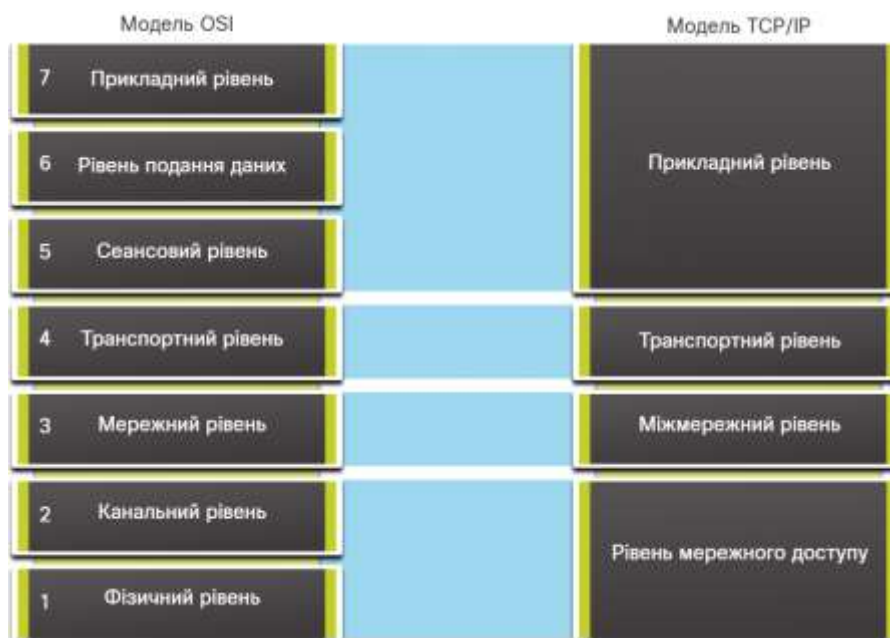


Рисунок 1.7 – Моделі OSI та TCP/IP

Блок даних протоколу (Protocol Data Unit, PDU). На кожному рівні використовується свій інформаційний пакет, який називається блоком даних протоколу (PDU), що містить специфічні для відповідного протоколу керуючу інформацію протоколу та дані користувача. Під час проходження через рівні інформація додається або видаляється і кожний рівень формує власний PDU.

Так, наприклад, на каналному рівні це буде MAC-адреси джерела та призначення, Поле типу/довжини, Корисне навантаження даних, послідовність перевірки кадру (FCS). На мережному рівні – «Версія та довжина заголовка»,

«Тип послуги», «Загальна довжина», «Ідентифікація», прапорці та зміщення фрагмента, «Час життя» (TTL).

Для протоколів, наприклад, TCP, UDP – Контрольна сума заголовка, IP-адреси джерела та призначення, Параметри (якщо є), Корисне навантаження даних.

На транспортному рівні для протокол керування передачею – «Номери портів» джерела та призначення, «Номери послідовності» та підтвердження, «Зміщення даних», прапорці керування, «Розмір вікна», «Контрольна сума», «Вказівник терміновості» (якщо є) тощо.

Тобто кожен рівень додає певні заголовки до корисного навантаження даних під час проходження мережею. Перегляд цих заголовків є одним з методів діагностики роботи мережі.

Виконання комп'ютерного практикуму

Завдання 1. Відкрити файл Завдання1_LP1.pka. Побудувати просту мережу в Логічному робочому просторі Packet Tracer, налаштувати пристрої і перевірити з'єднання. Для цього необхідно зробити наступне:

1. Додати мережеві пристрої до робочого простору (PC, ноутбук та cable modem). Використовуючи область вибору пристроїв, додайте ці пристрої до робочого простору.

Категорії та підкатегорії, в яких розташовані пристрої, перелічені нижче:

PC: End Devices > End Devices > PC

Laptop: End Devices > End Devices > Laptop

Cable Modem: Network Devices > WAN Emulation > Cable Modem.

2. Змінити назви, які відображаються під мережними пристроями. Для цього:

- клацніть піктограму пристрою в Логічному просторі;
- виберіть вкладку Config у вікні налаштування пристрою;
- введіть нове ім'я пристрою в полі Display Name для всіх нещодавно доданих пристроїв: PC, ноутбука, та кабельного модему.

3. Додати фізичні кабельні з'єднання між пристроями в робочому просторі.

Треба використати область вибору пристроїв для додавання фізичних кабельних з'єднань між пристроями в робочому просторі:

- мідний прямий кабель для з'єднання PC з бездротовим маршрутизатором.

В області вибору пристроїв натисніть Connections (піктограма з блискавкою). Виберіть мідний прямий кабель в області вибору пристроїв і приєднайте його до FastEthernet 0 інтерфейсу на PC і до Ethernet 1 інтерфейсу на бездротовому маршрутизаторі;

- мідний прямий кабель для з'єднання бездротового маршрутизатора з кабельним модемом. Виберіть мідний прямий кабель в області вибору пристроїв та приєднайте до інтернет-інтерфейсу на бездротовому маршрутизаторі та до інтерфейсу Port 1 кабельного модему;

- коаксіальний кабель для з'єднання кабельного модему з інтернет-хмарою. Виберіть коаксіальний кабель в області вибору пристроїв та приєднайте до інтерфейсу Port 0 кабельного модему та до інтерфейсу Coaxial 7 інтернет-хмари.

4. Налаштувати PC для роботи в дротовій мережі. Для цього:

- натиснути на пристрій PC. На вкладці Desktop виберіть IP Configuration, щоб перевірити, що DHCP дозволено і PC отримав IP-адресу;

- вибрати DHCP одразу під заголовком IP Configuration, якщо ви не бачите IP-адресу в полі IPv4 Address. Спостерігайте за процесом, як PC отримує IP-адресу від сервера DHCP. DHCP (Dynamic Host Configuration Protocol) – це протокол динамічної конфігурації вузла. Цей протокол призначає IP-адреси пристроям динамічно. В цій простій мережі бездротовий маршрутизатор налаштований, щоб призначати IP-адреси пристроям, які їх запитують. Якщо DHCP вимкнено, потрібно призначити IP-адресу та налаштувати всю іншу необхідну інформацію вручну, щоб мати зв'язок з іншими пристроями в мережі та в інтернеті;

- закрити вікно IP Configuration. На вкладці Desktop виберіть Command Prompt.

В командному рядку введіть `ipconfig /all` щоб переглянути IPv4-адресну інформацію, отриману з DHCP-сервера. Комп'ютер мав отримати IPv4-адресу в діапазоні 192.168.0.x.

Для перевірки зв'язку між PC та `cisco.srv` з командного рядку виконати команду `ping cisco.srv`. Для отримання відповіді на `ping` може знадобитися кілька секунд.

5. Налаштувати ноутбук. Для цього:

- натиснути на Laptop, і виберіть вкладку Physical;
- на вкладці Physical необхідно видалити модуль для мідного Ethernet і замінити його на модуль Wireless WPC300N;
- вимкнути живлення Laptop натиснувши на кнопку живлення на бічній панелі ноутбука;
- видалити поточний модуль для мідного Ethernet, клацнувши на модулі з боку ноутбука та протягнувши його на панель MODULES ліворуч від вікна з ноутбуком;
- встановити бездротовий модуль WPC300N, клацнув на ньому на панелі MODULES і а перетягнув до порожнього порту модуля з боку ноутбук;
- увімкнути Laptop знову натиснувши кнопку живлення ноутбука;
- після встановлення бездротового модуля підключить ноутбук до бездротової мережі. Перейдіть на вкладку Desktop і виберіть PC Wireless;
- вибрати вкладку Connect. Після невеликої затримки в списку бездротових мереж з'явиться HomeNetwork. Якщо це необхідно, натисніть Refresh, щоб отримати перелік доступних мереж. Виберіть HomeNetwork. Натисніть кнопку Connect;
- закрити PC Wireless. Виберіть Web Browser на вкладці Desktop;
- у Web-браузері перейдіть до `cisco.srv`.

Завдання 2. Відкрити файл Завдання2_ЛР1.pka. Дослідити моделі TCP/IP та OSI в дії та переглянути PDU.

1. Перейти з режиму реального часу в режим моделювання. Для цього:

- клацнути значок режиму Simulation (Моделювання), щоб переключитися з режиму Realtime (Режим реального часу) в режим Simulation (Моделювання);
- вибрати пункт HTTP у списку Event List Filters (Фільтри списку подій).

2. Згенерувати веб-трафік (HTTP). Для цього необхідно зробити наступне:

- клацнути Web Client (Веб-клієнт) на крайній лівій панелі;
- клацнути вкладку Desktop (Робочий стіл), потім клацнули значок Web Browser, щоб відкрити веб-браузер;
- у полі URL ввести адресу `www.osi.local` і натиснути кнопку Go;
- натиснути кнопку Capture/Forward чотири рази. У списку подій з'явиться чотири події. Веб-сторінку повернуто з веб-сервера;
- клацнути перший кольоровий квадрат у стовпці під Event List (Список подій) > Type column (Тип стовпця).

Має відкритися вікно PDU Information at Device: Web Client (Інформація про PDU на пристрої: веб-клієнт);

- переконатися в тому, що обрано вкладку OSI Model tab.

Надати відповіді на запитання:

1) Яка інформація перерахована в пронумерованих кроках безпосередньо під полями In Layers (Вхідні рівні) та Out Layers (Вихідні рівні)?

2) Яке значення Dst порту на рівні 4 під стовпцем “Out Layers”?
Яке значення має параметр Dest?

3) Значення IP для рівня 3 в стовпці “Out Layers”?

4) Яка інформація відображається на рівні 2 у стовпці “Out Layers”?

Клацнути вкладку Outbound PDU Details (Відомості про вихідну PDU).

Надати відповіді на запитання:

1) Якщо порівняти відомості в розділі IP вкладки PDU Details з відомостями на вкладці OSI Model, яка інформація для них є спільною?

2) До якого рівня вона належить?

3) Якщо порівняти відомості в розділі TCP вкладки PDU Details з відомостями на вкладці OSI Model, яка інформація є для них загальною і до якого рівня вона відноситься?

4) Який хост, зазначений у розділі HTTP вкладки PDU Details?

5) З яким рівнем будуть пов'язані ці відомості на вкладці OSI Model?

Клацнути перший кольоровий квадрат у стовпці Type списку подій Event List.

Перейти до наступного поля HTTP Type у списку подій Event List і клацнути кольоровий квадрат. У цьому вікні є два стовпці: In Layers і Out Layers.

Надати відповіді на запитання. Порівняти дані в стовпці In Layers з даними в стовпці Out Layers і скажіть, у чому полягає основна відмінність між ними.

Відкрити вкладку Inbound PDU Details (Відомості про вхідну PDU). Переглянути відомості про PDU. Скільки вкладок відображається з цією подією?

3. Відобразити елементи сімейства протоколів TCP/IP та переглянули додаткові події. Для цього:

- зачинити всі вікна з відомостями про PDU;

- у розділі Event List Filters > Visible Events (Фільтри списку подій > Видимі події) натиснути кнопку Show All/None та відповісти на запитання «Які додаткові типи подій показано?»;

- клацнути першу подію DNS у стовпці Type. Переглянули вкладки OSI Model і PDU Detail;

- клацнути вкладку Outbound PDU Details (Відомості про вихідну PDU) та відповісти на запитання «Які відомості відображаються в полі NAME та у розділі DNS QUERY?»;

- клацнути останній кольоровий квадрат DNS Info у списку подій та відповісти на запитання «На якому пристрої було захоплено PDU? Яке значення показано поряд з полем ADDRESS: у розділі DNS ANSWER на вкладці Inbound PDU Details?»;

- знайти першу подію HTTP у списку і клацнули кольоровий квадрат події TCP відразу після цієї події. Відповісти на запитання «Які відомості

відображаються під пунктами 4 та 5 у пронумерованому списку безпосередньо під стовпцями In Layers та Out Layers?».

Склад звіту комп'ютерного практикуму

В звіті повинно бути відображено:

- 1) Тема роботи.
- 2) Мета роботи.
- 3) Постановка задачі.
- 4) Виконання завдання 1 з відповідними скріншотами.
- 5) Виконання завдання 2 з відповідними скріншотами та відповідями на запитання.
- 6) Висновок.

Контрольні питання:

Що таке Cisco Packet Tracer і для чого він призначений?

Які основні режими роботи існують у Packet Tracer?

Що таке Logical та Physical режими перегляду?

Що таке IP-адреса та маска підмережі?

Скільки рівнів містить модель OSI та яка основна мета її створення?

Які основні функції виконує фізичний рівень (Physical Layer) моделі OSI?

У чому полягає різниця між канальним рівнем (Data Link Layer) та мережевим рівнем (Network Layer)?

Що таке інкапсуляція даних у моделі OSI?

Які функції виконує сесійний рівень (Session Layer)?

У чому полягає роль рівня представлення (Presentation Layer)?

Яка різниця між моделлю OSI та стеком протоколів TCP/IP?

КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 2

Тема: Команди IOS та тестування мережі за допомогою команд IOS.

Мета заняття: Навчитися користуватися командами IOS та знаходити помилки в конфігурації мережевих пристроїв.

Теоретичні відомості

Сімейство мережних операційних систем, що використовуються на багатьох пристроях Cisco, називається Cisco Internetwork Operating System (IOS). Cisco IOS використовується на багатьох маршрутизаторах і комутаторах Cisco незалежно від типу або розміру пристрою. Мережні операційні системи схожі на операційну систему ПК. Через GUI операційна система ПК дозволяє користувачеві виконати такі задачі:

- Використовувати мишку для вибору та запуску програм.

- Вводити текст та текстові команди.

- Переглядати результат на моніторі.

Мережна операційна система на основі CLI (наприклад, Cisco IOS на комутаторі або маршрутизаторі) дозволяє мережному спеціалісту:

- Використовувати клавіатуру для запуску мережевих програм на базі CLI.

- Використовувати клавіатуру для введення тексту та текстових команд.

- Переглядати результат на моніторі. Мережні пристрої Cisco працюють під керуванням певних версій Cisco IOS. Версія IOS залежить від типу пристрою, який використовується, та необхідних функцій.

З міркувань безпеки Cisco IOS використовує два окремих командних режими для доступу до адміністративних функцій:

Користувацький режим EXEC (User EXEC) володіє обмеженим функціоналом, але є корисним для виконання базових операцій. У цьому режимі доступний лише невеликий набір основних команд для моніторингу, при цьому неможливо виконувати команди, що змінюють конфігурацію пристрою. Користувацький режим EXEC визначається за допомогою запиту CLI, який завершується спеціальним символом >.

Приклад:

Switch>

Router>

Привілейований режим EXEC (Privileged EXEC) – для виконання команд конфігурації адміністратор мережі повинен отримати доступ до привілейованого режиму EXEC. Режими конфігурації більш високого рівня, як, наприклад, режим глобальної конфігурації, можуть бути доступні лише з привілейованого режиму EXEC. Привілейований режим EXEC може бути визначений підказкою, що закінчується символом # .

Приклад:

Switch#

Router#

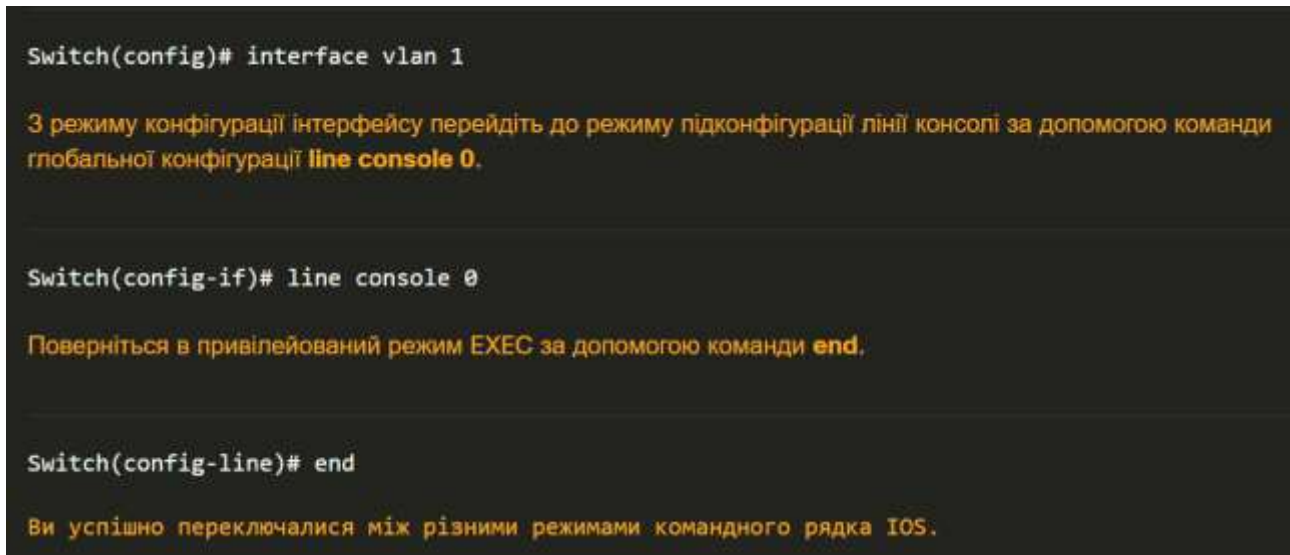
Для переходу між режимами командного рядку використовуються різні команди. Щоб перейти з користувацького режиму EXEC в привілейований, використовується команда `enable`. Для повернення в користувацький режим EXEC використовується команда привілейованого режиму `disable`. Привілейований режим EXEC іноді називається режимом `enable`.

Щоб перейти в режим глобальної конфігурації і вийти з нього, використовується команда `configure terminal` привілейованого режиму EXEC. Щоб повернутися до привілейованого режиму EXEC, треба ввести команду `exit` режиму глобальної конфігурації.

Існує багато різних підрежимів конфігурації. Наприклад, для входу в підрежим конфігурації лінії треба ввести команду `line`, за якою слідує тип і номер лінії керування, до якої треба отримати доступ. Для виходу з підрежиму конфігурації та повернення в режим глобальної конфігурації використовується команда `exit`.

Щоб перейти з будь-якого підрежиму конфігурації в рамках режиму глобальної конфігурації на один рівень вище в ієрархії режимів, треба ввести команду `exit`. Приклад наведено на рисунку 2.1

Щоб перейти з будь-якого підрежиму конфігурації в привілейований режим EXEC, треба ввести команду `end` або застосувати комбінацію клавіш `Ctrl+Z`. Зверніть увагу, що після вибору інтерфейсу командний рядок змінюється з `(config-line)#` на `(config-if)#`.



```
Switch(config)# interface vlan 1
З режиму конфігурації інтерфейсу перейдіть до режиму підконфігурації лінії консолі за допомогою команди
глобальної конфігурації line console 0.

Switch(config-if)# line console 0
Поверніться в привілейований режим EXEC за допомогою команди end.

Switch(config-line)# end
Ви успішно переключалися між різними режимами командного рядка IOS.
```

Рисунок 2.1 – Перехід між режимами командного рядку

Кожна команда IOS має певний формат або синтаксис і може виконуватися лише у відповідному режимі (рисунок 2.2). Загальний синтаксис команди, показаний на рисунку, – це команда, за якою слідують всі відповідні ключові слова і аргументи.

Ключове слово (Keyword) – це особливий параметр, визначений в операційній системі (на рисунку, `ip protocols`).

Аргумент (Argument) – не є наперед заданим; це значення або змінну визначає користувач (на рисунку, `192.168.10.5`).

Після введення повної команди, що включає всі необхідні ключові слова та аргументи, натискайте клавішу `Enter`. Команда може містити один або кілька аргументів. Щоб зрозуміти, які ключові слова та аргументи потрібні для певної команди, зверніться до її синтаксису. Синтаксис визначає шаблон або формат, за яким слід вводити команду.

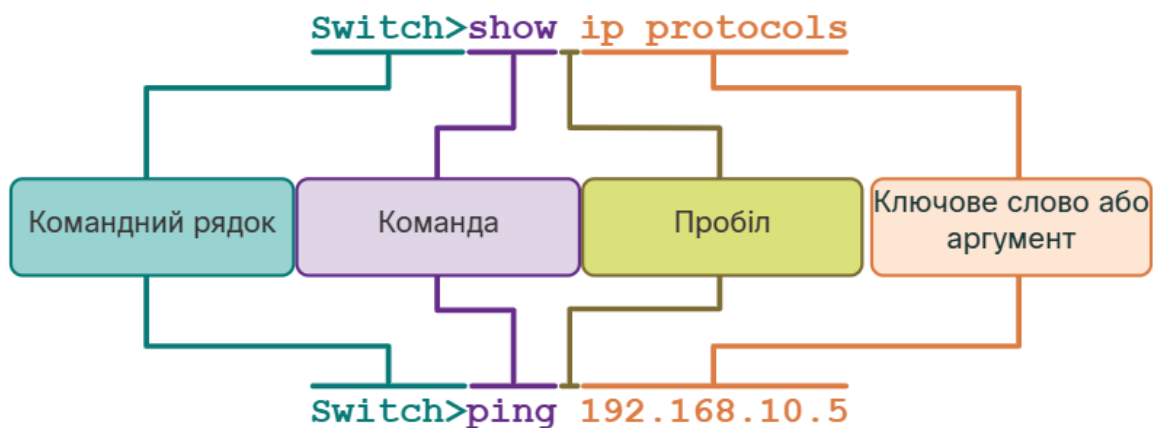


Рисунок 2.2 – Формат команди IOS

Наприклад, для використання команди `description` необхідно використовувати наступний синтаксис `description string`. Аргумент – це рядкове значення, надане користувачем. Команда `description` зазвичай використовується для визначення призначення інтерфейсу, тобто для додавання текстового опису до інтерфейсу мережевого пристрою, що допомагає ідентифікувати його призначення. Опис призначений для адміністраторів і не впливає на функціонування мережі. Наприклад, `description Connects to the main headquarter office switch`, де `Connects to the main headquarter office switch` – це аргумент.

Нижче представлені приклади умовних позначень для документування та використання команд IOS:

`ping ip-address` – виконується команда `ping`, а аргумент `ip-address`, визначений користувачем, є IP-адресою пристрою призначення. Наприклад, `ping 10.10.10.4`.

`traceroute ip-address` – виконується команда `traceroute`, а аргумент `ip-address`, визначений користувачем, є IP-адресою пристрою призначення. Наприклад, `traceroute 192.168.254.252`.

Якщо команда складна, з кількома аргументами, її можна представити таким чином:

```
Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}
```

Зазвичай команда супроводжується детальним описом команди і кожного аргументу в довіднику команд Cisco IOS.

Розглянемо детально кілька команд IOS щодо базової конфігурації пристрою.

Встановлення імені пристрою. Першою командою налаштування на будь-якому пристрої має бути присвоєння йому унікального імені пристрою або імені вузла. Всім пристроям присвоєне заводське ім'я за замовчуванням. Наприклад, для комутаторів Cisco IOS це "Switch", яке рекомендується змінити. Основні принципи створення імен вузлів передбачають: починати з літери; уникати пробілів; завершувати літерою або цифрою; використовувати лише літери, цифри та тире; обмежувати довжину до 64 символів.

Щоб змінити ім'я пристрою, необхідно перейти до режиму глобальної конфігурації, виконавши відповідну команду `configure terminal` та ввести команду `hostname`, а потім ім'я комутатора та натисніть Enter. Наприклад:

```
Router(config)# hostname R1
```

```
R1(config)#
```

Щоб повернути комутатор до запрошення за замовчуванням, використовуйте команду глобальної конфігурації `no hostname`.

Налаштування паролів. Використання слабких або легко вгадуваних паролів залишається однією з найсерйозніших проблем безпеки організацій. Для забезпечення захищеності, мережні пристрої, зокрема домашні бездротові маршрутизатори, завжди повинні бути налаштовані з використанням пароля, який обмежує адміністративний доступ. Усі пристрої повинні забезпечувати захищений паролем доступ до привілейованого та користувацького EXEC режимів, а також до віддаленого доступу через Telnet. Крім того, усі паролі мають бути зашифровані, а сповіщення про обмеження доступу повинно бути активоване. Під час першого під'єднання до пристрою зазвичай здійснюється вхід у користувацький режим EXEC. Щоб убезпечити доступ у цьому режимі, необхідно увійти в консольну лінію в режимі конфігурації, використовуючи відповідну команду глобальної конфігурації `line console 0`, як показано в

прикладі. Нуль використовується для представлення першого (і в більшості випадків єдиного) консольного інтерфейсу. Далі встановіть пароль користувачького режиму EXEC, використовуючи команду `password`. Активуйте доступ до користувачького режиму EXEC, використовуючи команду `login`.

Приклад.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Використання слабких або легко передбачуваних паролів залишається однією з найсерйозніших проблем безпеки для організацій. Для забезпечення захисту мережеві пристрої, зокрема домашні бездротові маршрутизатори, обов'язково слід налаштовувати із надійними паролями, що обмежують адміністративний доступ. Усі пристрої мережі мають бути захищені шляхом встановлення паролів для обмеження доступу до привілейованого та користувачького режимів EXEC, а також для віддалених каналів, таких як Telnet. Додатково, усі паролі мають бути зашифровані, а пристрої – налаштовані на видачу сповіщень про обмеження доступу.

При первинному підключенні до пристрою користувач потрапляє в користувачький режим EXEC. Щоб забезпечити безпеку цього режиму, гарантувати захищений адміністративний доступ та уникнути потенційних ризиків необхідно перейти в режим конфігурації консольної лінії через команду глобальної конфігурації `enable secret password`, як показано в прикладі.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Налаштування віддаленого доступу (Telnet/SSH). Лінії віртуального терміналу (VTY) забезпечують віддалений доступ до пристрою за допомогою Telnet або SSH. Багато комутаторів Cisco підтримують до 16 ліній VTY, які пронумеровані від 0 до 15.

Щоб захистити лінії VTY, увійдіть у режим лінії VTY за допомогою команди глобальної конфігурації `line vty 0 15`. Далі вкажіть пароль VTY за допомогою команди `password password`. Нарешті, активуйте доступ до VTY, використовуючи команду `login`.

Нижче наведено приклад захисту ліній VTY на комутаторі.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Шифрування паролів. Файли `startup-config` і `running-config` зберігають значну частину паролів у незашифрованому вигляді, що становить серйозну загрозу безпеці. У разі доступу до цих файлів сторонні особи можуть легко побачити всі відкриті паролі. Щоб усунути цю проблему та зашифрувати весь текст паролів, слід скористатися командою глобальної конфігурації `service password-encryption`, як показано в прикладі.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)#
```

Команда використовує простий алгоритм шифрування для обробки незашифрованих паролів, які зберігаються у файлі конфігурації. Важливо зазначити, що це шифрування поширюється виключно на паролі в самому файлі конфігурації й не стосується їх передачі через мережу. Основна мета – завадити стороннім особам отримати доступ до незашифрованих паролів у

конфігураційному файлі. Використовуйте команду `show running-config`, щоб перевірити, що паролі тепер зашифровані.

```
Sw-Floor-1(config)# end
```

```
Sw-Floor-1# show running-config
```

Створення Banner (повідомлення при вході). Щоб створити банерне повідомлення на мережному пристрої, використовуйте команду глобальної конфігурації `banner motd # the message of the day #`. Символ "#" у синтаксисі команд називається символом розмежування. Він вводиться до і після повідомлення. Символом-роздільником може бути будь-який символ, якщо він не присутній в повідомленні. З цієї причини часто використовуються такі символи, як #. Після виконання команди банер буде відображатися при всіх наступних спробах доступу до пристрою, поки не буде видалений.

Наступний приклад показує кроки налаштування банера на Sw-Floor-1.

```
Sw-Floor-1# configure terminal
```

```
Sw-Floor-1(config)# banner motd #Authorized Access Only#
```

Файли конфігурації. Існує два важливих системних файли, які відповідають за збереження конфігурації пристрою:

`Startup-config` – це файл конфігурації, який постійно зберігається у пам'яті типу NVRAM. У ньому містяться усі команди, необхідні для роботи пристрою під час його запуску або перезавантаження. Вміст цього файлу залишається незмінним навіть після вимкнення обладнання, оскільки флеш-пам'ять не залежить від електроживлення.

`Running-config` – файл, що містить поточну конфігурацію пристрою та розташовується в оперативній пам'яті (RAM). У ньому зберігаються всі внесені зміни, які одразу впливають на роботу пристрою Cisco. Оперативна пам'ять є енергозалежною, тому її вміст повністю стирається після вимкнення живлення чи перезавантаження пристрою.

Команда привілейованого режиму `EXEC show running-config` використовується для перегляду поточної конфігурації. Щоб переглянути файл

стартової конфігурації, використовуйте команду привілейованого режиму EXEC `show startup-config`.

У разі втрати живлення пристрою або його перезавантаження всі зміни в налаштуваннях будуть втрачені, якщо їх попередньо не було збережено. Щоб зафіксувати внесені зміни в поточних налаштуваннях у файлі стартової конфігурації, необхідно скористатися командою привілейованого режиму EXEC `copy running-config startup-config`.

Суттєвим недоліком використання команди `reload` для видалення незбереженої робочої конфігурації є той факт, що пристрій певний час перебуває в автономному режимі, що може спричинити тимчасове простоювання мережі. Під час ініціації перезавантаження операційна система IOS виявляє наявність незбережених змін у поточному файлі конфігурації, які не були перенесені у стартовий файл конфігурації, і пропонує користувачеві можливість зберегти ці зміни. Для відмови від збереження змін необхідно виконати введення **n** або **no**.

У разі збереження небажаних змін у конфігурації запуску може виникнути потреба у повному очищенні налаштувань. Для цього необхідно видалити стартову конфігурацію та виконати перезапуск пристрою. Видалення стартової конфігурації здійснюється через використання команди в привілейованому режимі EXEC `erase startup-config`. Після виконання команди комутатор запросить підтвердження. Натисніть Enter для підтвердження.

Перегляд поточної інформації. Команди `show` використовуються для перегляду інформації про стан пристрою, конфігурацію та роботу мережі.

Найпоширеніші команди `show` представлено в таблиці.

Таблиця. Команди `show`.

Команда	Призначення
<code>show version #</code>	Версія IOS, модель, час роботи, конфігураційний реєстр
<code>show running-config #</code>	Поточна активна конфігурація (в RAM)
<code>show startup-config #</code>	Збережена конфігурація (в NVRAM)

Команда	Призначення
show flash #	Вміст флеш-пам'яті
show tech-support #	Повна технічна інформація для діагностики
show ip interface brief #	Короткий статус всіх інтерфейсів (IP, статус)
show interfaces #	Детальна інформація про всі інтерфейси
show interfaces gi0/0 #	Інформація про конкретний інтерфейс
show interfaces status #	Статус портів (для комутаторів)
show interfaces trunk #	Інформація про trunk-порти
show interfaces description #	Описи інтерфейсів
show ip route #	Таблиця маршрутизації
show ip route summary #	Підсумок таблиці маршрутизації
show ip protocols #	Активні протоколи маршрутизації
show ip ospf neighbor #	OSPF сусіди
show ip eigrp neighbors #	EIGRP сусіди
show ip bgp summary #	BGP підсумок
show vlan #	Інформація про всі VLAN
show vlan brief #	Короткий список VLAN
show vlan id 10 #	Інформація про конкретний VLAN
show interfaces switchport #	Режим роботи портів (access/trunk)
show spanning-tree #	Інформація про STP
show mac address-table #	Таблиця MAC-адрес
show mac address-table dynamic #	Тільки динамічні записи
show mac address-table count #	Кількість MAC-адрес
show arp #	Таблиця ARP
show users #	Активні користувачі

Команда	Призначення
\show sessions #	Активні Telnet/SSH сесії
show line #	Статус консолі та VTY ліній
show access-lists #	Списки контролю доступу (ACL)
show ip access-lists #	IP ACL
show port-security #	Налаштування безпеки портів
show processes cpu #	Завантаження CPU
show memory #	Використання пам'яті
show log #	Системні логи
show logging #	Конфігурація логування
show cdp neighbors #	Сусідні Cisco пристрої (CDP)
show cdp neighbors detail #	Детальна інформація про сусідів
show lldp neighbors #	Сусідні пристрої (LLDP)
show ip dhcp binding #	DHCP оренди
show ip dhcp pool #	DHCP пули
show ip nat translations #	Таблиця NAT перекладів
show ip nat statistics #	Статистика NAT
show crypto ipsec sa #	IPSec Security Associations
show ntp status #	Статус NTP
show controllers #	Стан контролерів інтерфейсів
show environment #	Температура, живлення, вентилятори
show inventory #	Інвентарна інформація про модулі
show diag #	Діагностична інформація

Виконання комп'ютерного практикуму

Завдання 1. Відкрити файл Завдання1_LP2.pka. Створити основні підключення та отримати доступ до інтерфейсу командного рядка (CLI) та вивчити режими EXEC.

Частина 1. Створення основних підключень, доступ до командного інтерфейсу, рядки (CLI) та вивчення довідки.

1. Підключіть PC1 до S1 за допомогою консольного кабелю. Для цього:

- натисніть піктограму Connections (Підключення) (у вигляді блискавки) у нижньому лівому куті вікна Packet Tracer;

- виберіть світло-блакитний консольний кабель, клацнувши по ньому;

- натисніть PC1. У вікні буде показано варіант підключення RS-232.

Підключіть кабель до порту RS-232;

- перетягніть інший кінець консольного підключення до комутатора S1 і клацніть комутатор, щоб відкрити список з'єднань;

- виберіть Console (Консольний), щоб завершити з'єднання.

2. Встановіть діалоговий сеанс з комутатором S1. Для цього:

- натисніть PC1 і перейдіть на вкладку Desktop (Робочий стіл);

- натисніть піктограму Terminal (Термінал). Перевірте правильність параметрів конфігурації портів, заданих за промовчанням;

- натисніть кнопку OK.

3. Вивчіть довідку по IOS. В IOS доступна довідка по командах, залежно від рівня роботи. В даний момент відображається запрошення User EXEC (Користувацький режим EXEC) та пристрій очікує на введення команди. Найпростіший спосіб виклику довідки – ввести запитальний знак (?) у командному рядку, щоб отримати список команд. Тому:

У командному рядку введіть t із знаком питання в кінці (?).

S1> t?

У командному рядку введіть te із знаком питання в кінці (?).

S1> te?

Довідка такого виду називається контекстною. Чим докладніше вводяться команди, тим більше відомостей може надати довідка.

Частина 2. Вивчення режимів EXEC.

1. Увійдіть у привілейований режим EXEC. Для цього:

У командному рядку введіть знак запитання (?).

```
S1>?
```

Введіть `en` і натисніть клавішу `TAB`.

```
S1> en<Tab>
```

Введіть команду `enable` та натисніть клавішу введення.

Введіть у рядку знак запитання (?).

```
S1#?
```

2. Увійдіть у режим глобального налаштування. Для цього:

У привілейованому режимі EXEC одна з команд, що починаються з літери «с», `configure`. Введіть або команду повністю, або стільки символів, скільки буде потрібно для унікального визначення команди. Натисніть `<Tab>`, щоб виконати команду та натисніть клавішу введення.

```
S1# configure
```

Натисніть клавішу введення, щоб прийняти параметр за замовчуванням, що міститься в квадратні дужки, – `[terminal]`.

А тепер поверніться до привілейований режим EXEC, ввівши команду `end` або `exit` або натиснувши клавіші `Ctrl+Z`.

```
S1(config)# exit
```

```
S1#
```

Частина 3. Налаштування годинника.

1. Використовуйте команду `clock`, щоб детальніше вивчити довідку та синтаксис команди. Введіть `show clock` у привілейованому режимі EXEC.

```
S1# show clock
```

Використовуйте контекстну довідку та команду `clock`, щоб встановити поточний час на комутаторі. Введіть `clock` і натисніть клавішу введення.

S1# clock<ENTER>

Налаштуйте час за допомогою clock set. Продовжуйте виконувати команду поетапно.

S1# clock set?

Взявши за основу відомості, запрошені за допомогою clock set?, введіть час 15:00 у 24-годинному форматі (15:00:00). Перевірте, чи потрібні додаткові параметри.

Спробуйте встановити дату 31 січня 2035, використовуючи запитаний формат.

2. Вивчіть додаткові командні повідомлення.

Введіть наступну команду та запишіть повідомлення.

S1# cl<tab>

S1# clock

S1# clock set 25:00:00

S1# clock set 15:00:00 32

Завдання 2. Відкрити файл Завдання2_ЛР2.pka. Налаштувати початкові параметри комутатора.

Частина 1. Перевірка конфігурації комутатора за умовчанням.

Увійдіть у привілейований режим EXEC. Для цього:

Натисніть S1 і відкрийте вкладку CLI. Натисніть клавішу введення.

Перейдіть до привілейованого режиму EXEC, виконавши команду enable.

Відкрийте вікно конфігурації на S1

Switch> enable

Switch#

Зверніть увагу, що командний рядок змінився, вказуючи на привілейований режим EXEC.

2. Вивчіть поточну конфігурацію комутатора.

Введіть show running-config.

Switch # show running-config

Частина 2. Налаштування основних параметрів комутатора

1. Надайте комутатору ім'я. Для налаштування параметрів комутатора, можливо, потрібно перемикатися між режимами налаштування. Тому забезпечте безпечний доступ до консолі. Для цього:

Перейдіть до режиму config-line і встановіть для консолі пароль letmein.

```
S1# configure terminal
```

Введіть рядкові команди налаштування. Наприкінці натисніть CTRL+Z.

```
S1(config)# line console 0
```

```
S1(config-line)# password letmein
```

```
S1(config-line)# login
```

```
S1(config-line)# exit
```

```
S1(config)# exit
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
S1#
```

3. Переконайтеся, що доступ до консолі захищено. Вийдіть з привілейованого режиму, щоб переконатися, що для консольного порту встановлено пароль.

```
S1# exit
```

```
Switch con0 is now available
```

```
Press RETURN to get started.
```

```
User Access Verification
```

```
Password:
```

```
S1>
```

Примітка. Якщо комутатор не виводить запит на введення пароля, ви не налаштували параметр login у кроці 2.

4. Забезпечте безпечний доступ до привілейованого режиму. Встановіть пароль enable c1\$c0. Цей пароль обмежує доступ до привілейованого режиму.

```
S1> enable
```

```
S1# configure terminal
```

```
S1(config)# enable password c1$c0
```

```
S1(config)# exit
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
S1#
```

5. Переконайтеся, що доступ до привілейованого режиму захищено.

Виконайте команду `exit` ще раз, щоб вийти з комутатора. та натисніть <клавішу введення>, після чого вам буде запропоновано ввести пароль.

User Access Verification

Password:

Перший пароль – це пароль для консолі, який було встановлено для `line con 0`. Введіть цей пароль, щоб повернутися до режиму користувача EXEC.

Введіть команду, щоб отримати доступ до привілейованого режиму.

Введіть другий пароль, який було встановлено для обмеження доступу до привілейованого режиму EXEC.

Перевірте конфігурацію, вивчивши вміст файлу `running-configuration`:

```
S1# show running-config
```

Налаштуйте зашифрований пароль для доступу до привілейованого режиму.

Пароль для `enable` потрібно замінити на новий зашифрований пароль за допомогою команди `enable secret`. Встановіть для `enable secret` пароль `itsasecret`.

```
S1# config t
```

```
S1(config)# enable secret itsasecret
```

```
S1(config)# exit
```

```
S1#
```

7. Переконайтеся, що пароль `enable secret` додано до конфігураційного файлу. Введіть команду `show running-config` ще раз, щоб перевірити новий пароль `enable secret`.

```
S1# show run
```

8. Зашифруйте паролі enable та console за допомогою команди service password-encryption.

```
S1# config t
```

```
S1(config)# service password-encryption
```

```
S1(config)# exit
```

Частина 3. Налаштування банера MOTD (повідомлення дня).

```
S1# config t
```

```
S1(config)# banner motd «Це є безпечна система. Authorized Access Only!»
```

```
S1(config)# exit
```

```
%SYS-5-CONFIG_: Configured from console by console
```

```
S1#
```

Частина 4. Збережіть та перевірте файли конфігурації на NVRAM.

1. Перевірте правильність конфігурації за допомогою команди show run.

2. Виконайте резервне копіювання файлу конфігурації в NVRAM і переконайтеся, що внесені зміни не були втрачені під час перезавантаження системи або відключення живлення.

```
S1# copy running-config startup-config
```

```
Destination filename [startup-config]?[Enter]
```

```
Building configuration...
```

```
[OK]
```

Закрийте вікно налаштування S1

Чи всі внесені зміни були записані у файл?

Частина 5. Налаштування комутатора S2. Налаштуйте для комутатора S2 такі параметри.

Відкрийте вікно конфігурації на S2

Ім'я пристрою: S2

Захистить доступ до консолі паролем letmein.

Встановіть як пароль enable c1\$c0, а як пароль enable secret – itsasecret.

Налаштуйте відповідне повідомлення для тих, хто увійшов до комутатора.

Зашифруйте всі відкриті паролі.

Перевірте правильність конфігурації.

Збережіть файл конфігурації, щоб запобігти його втраті у разі вимкнення живлення комутатора.

Завдання 3. Відкрити файл Завдання3_ЛР2.pka. Використання команд show Cisco IOS на маршрутизаторі, що знаходиться у провайдера інтернет послуг (ISP).

1: Підключіться до маршрутизатора провайдера Cisco 4321.Для цього:

Натисніть ISP PC.

Натисніть вкладку Desktop. Виберіть Terminal. Перегляньте конфігурацію терміналу і натисніть кнопку ОК щоб продовжити.

Рядок ISPRouter > вказує, що Ви перебуваєте в режимі користувача EXEC. Натисніть Enter, якщо запит не відображається.

2: Ознайомтеся з командами show. Дослідить роботу команд show у користувацькому режимі EXEC. Для цього:

Введіть show ? у командному рядку.

Введіть show arp у командному рядку. Запишіть вказану MAC-адресу та IP-адресу.

c. Введіть show flash у командному рядку. та запишіть вказаний образ IOS:

d. Введіть show ip route у командному рядку. Скільки маршрутів вказано в таблиці?

Введіть show interfaces у командному рядку. Який інтерфейс запущений та працює?

Введіть show ip interface у командному рядку.

Введіть show version у командному рядку. Який пакет технологій увімкнено у маршрутизаторі?

Введіть show protocols у командному рядку. Які протоколи зараз увімкнено на маршрутизаторі?

Введіть show running-config у командному рядку. Який результат?

Крок 2: Дослідить роботу команд show у привілейованому режимі EXEC.

Для цього:

Введіть enable у командному рядку, щоб перейти у привілейований режим EXEC.

Введіть show running-config у командному рядку. Який результат?

Склад звіту комп'ютерного практикуму

В звіті повинно бути відображено:

- 1) Тема роботи.
- 2) Мета роботи.
- 3) Постановка задачі.
- 4) Виконання завдання 1 з відповідними скріншотами.
- 5) Виконання завдання 2 з відповідними скріншотами.
- 6) Виконання завдання 3 з відповідними скріншотами та відповідями на запитання.
- 7) Висновок.

Контрольні питання:

Які існують основні режими командного рядка (CLI) Cisco IOS і як між ними перемикаються?

Якою командою можна перейти з режиму користувача в привілейований режим?

Якою командою можна переглянути поточну активну конфігурацію пристрою, що зберігається в оперативній пам'яті (RAM), і якою — конфігурацію, збережену в енергонезалежній пам'яті (NVRAM)?

Як налаштувати на маршрутизаторі або комутаторі Cisco банер, який відображатиметься всім користувачам під час входу в систему?

Як зберегти поточну конфігурацію з RAM в NVRAM, щоб вона не була втрачена після перезавантаження пристрою?

Як забезпечити базовий захист доступу до привілейованого режиму за допомогою пароля, який зберігається в зашифрованому вигляді?

Як забезпечити базовий захист доступу до привілейованого режиму за допомогою пароля, який зберігається в зашифрованому вигляді?

Яка команда дозволяє переглянути інформацію про версію програмного забезпечення Cisco IOS, модель пристрою та обсяг пам'яті?

Яка команда використовується для перегляду детальної інформації про інтерфейси пристрою, включаючи статистику трафіку та помилки?

Яка команда дозволяє переглянути MAC-адресну таблицю на комутаторі Cisco?

КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 3

Тема: Програмні засоби діагностики мереж, освоєння: – arp, arping, ping, traceroute, mtr.

Мета: Ознайомитись з програмними засобами діагностики мереж, освоївши при цьому arp, arping, ping, traceroute, mtr

Теоретичні відомості

ARP (англ. *Address Resolution Protocol* – протокол визначення адреси) – протокол канального рівня, призначений для визначення MAC-адреси за відомою IP-адресою.

Коли пакет передається на канальний рівень для інкапсуляції в Ethernet-кадр, пристрій звертається до таблиці в оперативній пам'яті, щоб визначити MAC-адресу, пов'язану з певною адресою IPv4. Ця таблиця, яка тимчасово зберігається у пам'яті, називається ARP-таблицею, або ARP-кешем. Відправник спершу переглядає ARP-таблицю в пошуках MAC-адреси, що відповідає адресі IPv4 призначення.

Якщо IPv4-адреса призначення пакета належить тій самій мережі, що й адреса джерела, пристрій здійснює пошук у ARP-таблиці запису для зазначеної адреси. У випадку, якщо IPv4-адреса призначення знаходиться за межами локальної мережі, тобто в іншій мережі, пристрій звертається до ARP-таблиці для отримання IPv4-адреси шлюзу за замовчуванням.

У кожній із цих ситуацій здійснюється пошук відповідного значення MAC-адреси для визначеної IPv4-адреси. Якщо запис існує, його MAC-адреса використовується як адреса призначення у кадрі Ethernet. Якщо ж запис відсутній, пристрій ініціює відправлення ARP-запиту. Запит передається у вигляді Ethernet-кадру з урахуванням інформації, зазначеної в заголовку.

MAC-адреса призначення – це адреса широкомовної розсилки FF-FF-FF-FF-FF-FF, яка вимагає, щоб всі мережні адаптери Ethernet у локальній мережі приймали та обробляли ARP-запит.

MAC-адреса джерела – це MAC-адреса відправника ARP-запиту.

Поле «Тип» для ARP-повідомлень має значення 0x806. Завдяки цьому мережний адаптер отримує вказівку передати дані з відповідного кадру в ARP-процес. ARP-запити, будучи широкомовними, поширюються через усі порти комутатора, за винятком порту, з якого запит надійшов. Усі Ethernet-адаптери в локальній мережі обробляють такі кадри та передають ARP-запит операційній системі для перевірки.

Кожний пристрій у мережі аналізує ARP-запит, звіряючи цільову IPv4-адресу із власною. Широкомовні кадри не перенаправляються між інтерфейсами маршрутизатора. Тільки один пристрій у мережі матиме IPv4-адресу, яка збігається з цільовою адресою у запиті ARP, тоді як решта не відповідатиме.

Пристрій зі співпадаючою IPv4-адресою формує ARP-відповідь. Відповідь інкапсулюється в Ethernet-кадр із наступними параметрами заголовка: MAC-адреса призначення вказує на MAC-адресу відправника запиту, а MAC-адреса джерела — це MAC пристрою, який відповідає. Поле «Тип» для ARP-повідомлень залишається зі значенням 0x806, щоб мережний адаптер передавав його прямо в ARP-процес запитувача.

Тільки пристрій-ініціатор отримує одноадресну ARP-відповідь. Після її отримання він додає пару IPv4-адреса та її відповідну MAC-адресу до своєї таблиці ARP. Це дозволяє надсилати пакети до відповідної IPv4-адреси, інкапсулюючи їх у кадри Ethernet із визначеною MAC-адресою.

Якщо ARP-запит залишається без відповіді, доставка пакета стає неможливою, і він відкидається через неспроможність створити Ethernet-кадр. Записи в таблиці ARP мають обмежений строк дії, і якщо пристрій не приймає кадри від певного джерела до завершення цього терміну, відповідна інформація видаляється з таблиці.

До ARP-таблиці також можна додавати статичні зіставлення, проте це трапляється досить рідко. Такий вид записів не має автоматичного терміну закінчення і їх необхідно видаляти вручну. У протоколі IPv6 замість ARP використовується процес виявлення сусідів (ND, Neighbor Discovery), оснований на ICMPv6. Цей механізм виконує функції, подібні до процесу ARP у IPv4,

застосовуючи повідомлення про запит сусіда (NS, Neighbor Solicitation) та його анонсування (NA, Neighbor Advertisement), що нагадують ARP-запити та відповіді у протоколі IPv4.

Якщо IPv4-адреса одержувача належить до іншої мережі, пристрій-відправник надсилає кадр до шлюзу за замовчуванням, тобто до інтерфейсу локального маршрутизатора. У кожному випадку, коли пристрій передає пакет до IPv4-адреси з іншої мережі, відбувається інкапсуляція пакета з використанням MAC-адреси маршрутизатора.

Конфігурація хостів IPv4 містить інформацію про адресу шлюзу за замовчуванням. Коли вузол створює пакет для передачі, він проводить порівняння між IPv4-адресою одержувача та власною IPv4-адресою. Це дозволяє визначити, чи знаходяться обидві адреси в одній підмережі рівня 3. Якщо адресу призначення розташовано в іншій мережі, пристрій-відправник звертається до таблиці ARP у пошуках запису з адресою шлюзу за замовчуванням. У разі відсутності такого запису запускається процес ARP для отримання MAC-адреси шлюзу.

На кожному пристрої існує таймер для кешу ARP, який автоматично видаляє записи з таблиці ARP після певного часу неактивності. Тривалість цього періоду варіюється залежно від операційної системи: наприклад, у сучасних версіях Windows записи можуть зберігатися від 15 до 45 секунд.

Доступні також команди для ручного видалення окремих або всіх записів з таблиці ARP. Після такого очищення для того, щоб додати нове зіставлення, процедура надсилення ARP-запиту та отримання відповіді повторюється.

На маршрутизаторах Cisco для перегляду вмісту ARP-таблиці використовується спеціальна команда `show ip arp`, як показано на рисунку 3.1.

```

R1# show ip arp
Protocol    Address          Age (min)  Hardware Addr  Type   Interface
Internet    192.168.10.1      -          a0e0.af0d.e140 ARPA    GigabitEthernet0/0/0
Internet    209.165.200.225   -          a0e0.af0d.e141 ARPA    GigabitEthernet0/0/1
Internet    209.165.200.226   1          a03d.6fe1.9d91 ARPA    GigabitEthernet0/0/1
R1#

```

Рисунок 3.1 – Команда show ip arp

На ПК під керуванням ОС Windows 10 для відображення таблиці ARP використовується команда arp -a.

Параметри:

arp -a [IP- адреса] [-N <адреса_інтерфейсу>]

arp -d < IP- адреса > [адреса_інтерфейсу]

arp -s < IP- адреса > <MAC- адреса > [адреса_інтерфейсу]

Таблиця. Параметри команди arp

Параметр	Використання
-a	Відображає відповідність адреси IP адресі MAC, яке зберігається в локальному кеші ARP
-d	Видаляє запис кешу ARP для вказаної адреси IP
-s	Додає статичний (постійний) запис у Кеш ARP
<адрес IP>	Призводить до відображення інформації тільки для цієї IP-адреси

Параметр	Використання
<адрес_інтерфейса>	Для систем з декількома мережевими адаптерами цей параметр використовується для вказівки адрес MAC локального мережевого адаптера, для якого виконується команда <code>arp</code> , в іншому випадку команда <code>arp</code> виконується по відношенню до першого ж мережевому адаптеру в порядку прив'язки до мережі
<адрес_MAC>	Використовується для вказівки адреси MAC, для якого створюється статичний запис кеші ARP

Приклади.

Щоб вивести таблиці кешу ARP для всіх інтерфейсів, введіть:

```
arp -a
```

Щоб вивести таблицю кешу ARP для інтерфейсу, якому призначено IP-адресу 10.0.0.99, введіть:

```
arp -a -N 10.0.0.99
```

Щоб додати статичний запис кешу ARP, який зіставляє IP-адресу 10.0.0.80 з фізичною адресою 00-AA-00-4F-2A-9C, введіть:

```
arp -s 10.0.0.80 00-AA-00-4F-2A-9C
```

PING – утиліта для перевірки з'єднань в мережах на основі TCP/IP, а також повсякденне найменування самого запиту.

Утиліта відправляє запити (ICMP Echo-Request) протоколу ICMP зазначеному вузлу мережі й фіксує відповіді, що надходять (ICMP Echo-Reply). Час між відправленням запиту й одержанням відповіді (RTT, від англ. Round Trip Time) дозволяє визначати двосторонні затримки (RTT) за маршрутом і частоту

втрати пакетів, тобто побічно визначати завантаженість на каналах передачі даних і проміжних пристроях.

У розмовній мові пінгом називають також час, витрачений на передачу пакету інформації в комп'ютерних мережах від клієнта до сервера і назад від сервера до клієнта.

Повна відсутність ICMP-відповідей може також означати, що віддалений вузол (або який-небудь з проміжних маршрутизаторів) блокує ICMP Echo-Reply або ігнорує ICMP Echo-Request.

Практичне використання. Можна дізнатися:

- IP-адресу за доменним ім'ям;
- чи працює сервер;
- чи є зв'язок з сервером;
- якість каналу, подивившись, скільки відповідей не прийшло.

Для оцінки якості каналу можна звернути увагу на кількість втрачених відповідей під час пінгування. Цей підхід також є корисним при вирішенні проблем у мережі, як з дротовими, так і з бездротовими з'єднаннями. Використовуючи метод «поділай і володарюй», можна ізолювати джерело несправностей, визначивши, чи вони виникають у дротовій або бездротовій мережі. Для цього слід виконати наступні кроки:

- провести пінгування бездротового клієнта до шлюзу за замовчуванням. Це допоможе перевірити, чи відповідає з'єднання бездротового пристрою заданим налаштуванням;

- провести пінгування дротового клієнта до шлюзу за замовчуванням. Цей тест дозволяє впевнитися, що параметри з'єднання дротового пристрою налаштовані коректно;

- реалізувати пінгування від бездротового клієнта до дротового. Даний тест покаже, чи правильно функціонує бездротовий маршрутизатор та чи є між пристроями належний зв'язок.

Завдяки цим діям можна швидко визначити та усунути проблеми в роботі мережі.

Після команди `ping` може вказуватися IP-адреса або ім'я хоста призначення. Якщо в команді `ping` вказана IP-адреса, на неї по мережі буде відправлений пакет ехо-запиту. При отриманні ехо-запиту пристрій-відповідач надсилає у відповідь пакет із ехо-відповіддю. У ситуації, коли джерело отримує ехо-відповідь, це підтверджує факт успішного встановлення зв'язку з конкретною IP-адресою. Якщо ехо-запит завершується невдало, система може інформувати про це через такі повідомлення, як "час запиту минув" або "загальна помилка".

Типова команда `ping` зазвичай формує чотири ехо-запити, очікуючи відповідь на кожен з них. Утім, її функціональність можна зробити більш гнучкою та ефективною завдяки додатковим параметрам. Параметри, представлені на рисунку 3.2, дозволяють користувачеві отримати доступ до розширених можливостей цієї команди.

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
          [-4] [-6] target_name

Options:
  -t          Ping the specified host until stopped.
              To see statistics and continue - type Control-Break;
              To stop - type Control-C.
  -a          Resolve addresses to hostnames.
  -n count    Number of echo requests to send.
  -l size     Send buffer size.
  -f          Set Don't Fragment flag in packet (IPv4-only).
  -i TTL      Time To Live.
  -v TOS      Type Of Service (IPv4-only. This setting has been deprecated
              and has no effect on the type of service field in the IP
              Header).
  -r count    Record route for count hops (IPv4-only).
  -s count    Timestamp for count hops (IPv4-only).
  -j host-list Loose source route along host-list (IPv4-only).
  -k host-list Strict source route along host-list (IPv4-only).
  -w timeout  Timeout in milliseconds to wait for each reply.
  -R          Use routing header to test reverse route also (IPv6-only).
              Per RFC 5095 the use of this routing header has been
              deprecated. Some systems may drop echo requests if
              deprecated. Some systems may drop echo requests if
  -S srcaddr  Source address to use.
  -c compartment Routing compartment identifier.
  -p          Ping a Hyper-V Network Virtualization provider address.
  -4          Force using IPv4.
  -6          Force using IPv6.
```

Рисунок 3.2 – Параметри команди `ping`

ARPING – це утиліта для відправки ARP-запитів на рівні канального рівня (Layer 2). На відміну від звичайного ping (ICMP), arping працює з MAC-адресами. Її основне призначення:

- перевірка доступності хоста на рівні Data Link;
- визначення MAC-адреси за IP-адресою;
- виявлення дублікатів IP-адрес;
- тестування ARP-відповідей;
- перевірка з'єднання, коли ICMP заблоковано.

Таблиця. Параметри утиліти

Параметр	Використання
-U	Надає вміст кешу ARP для поновлення ARP кешей сусідніх систем. Відповіді не очікуються
-A	Аналогічно -U, але використовуються пакети ARP REPLY замість ARP REQUEST
-b	Відправляє тільки широкомовні пакети рівня MAC. Зазвичай arping спочатку відправляє широкомовні пакети, а після прийому відповіді – тільки адресату.
-c <лічильник>	Додає статичний (постійний) запис у Кеш ARP
-D	Режим дубльованого виявлення адреси. Повертає 0, якщо дубльоване визначення адреси пройшло успішно, тобто відповіді не прийняті
-f	Завершує роботу після першого прийому відповіді
-I <інтерфейс>	Найменування мережевого пристрою (інтерфейсу), через який відправляються пакети ARP REQUEST. Вказівка інтерфейсу для цієї опції обов'язкова
-h	Відображає сторінку допомоги і завершує роботу
-q	Вивід не відображається

Параметр	Використання
-s <відправник>	IP адреса відправника, що використовується в ARP пакетах. Якщо ця опція не вказана, використовується наступна адреса відправника: * У режимі дубльованого визначення адреси (з опцією-D) – 0.0.0.0. * У звичайному ARP-режимі (з опцією-U або-A) використовується адресат. * В інших випадках адресу обчислюється по таблиці маршрутизації
-V	Показує номер версії програми і завершує роботу
-w <дедлайн>	Вказує таймаут в секундах перед тим, як arping завершить роботу і відобразить скільки пакетів було відправлено або прийнято. У цьому випадку arping не зупиняється після відправки лічильник пакетів, він очікує поки дедлайн закінчиться або поки не буде прийнято лічильник відповідей

Приклад: ARPING 192.168.39.120 from 192.168.39.1 eth0

TRACEROUTE – це службова комп'ютерна програма, призначена для визначення маршрутів прямування даних в мережах TCP/IP. Traceroute входить в поставку більшості сучасних мережевих операційних систем. У системах Microsoft Windows ця програма носить назву tracert, а в системах GNU/Linux, Cisco IOS і MacOS – traceroute.

Traceroute може використовувати різні протоколи передачі даних в залежності від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE. Комп'ютери зі встановленою операційною системою Windows використовують ICMP-протокол, при цьому операційні системи Linux і маршрутизатори Cisco – протокол UDP. Traceroute показує всі хости, через які проходить пакет по шляху до кінцевого призначення.

Утиліта `tracert` надає інформацію про з'єднання, шлях, який проходить пакет, щоб дістатися до пункту призначення, а також про кожен маршрутизатор (хоп) на цьому шляху. Також вказується, скільки часу потрібно пакету, щоб дістатися від джерела до кожного хопу і назад (час в обидва боки). Утиліта `tracert` допомагає встановити місця втрати та затримки пакетів через обмеження пропускної здатності або уповільнення трафіку в мережі. Параметри утиліти зображено на рис. 3.3.

```
C:\> tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d                Do not resolve addresses to hostnames.
  -h maximum_hops   Maximum number of hops to search for target.
  -j host-list       Loose source route along host-list (IPv4-only).
  -w timeout         Wait timeout milliseconds for each reply.
  -R                Trace round-trip path (IPv6-only).
  -S srcaddr         Source address to use (IPv6-only).
  -4                Force using IPv4.
  -6                Force using IPv6.
```

Рис. 3.3. Параметри утиліти `tracert`

MTR – інтерактивна програма, здатна постійно виводити оновлену статистику по трасі. Те ж що і `traceroute`, тільки вона працює поки не зупинити і постійно показує відомості про маршрут, втрати, мінімальні та максимальні затримки. За допомогою `mtr` можна дізнаватися де в мережі відбуваються втрати, затримки і обривається зв'язок.

Таблиця. Параметри програми.

Параметр	Використання
-U	Надає вміст кешу ARP для поновлення ARP кешей сусідніх систем. Відповіді не очікуються
-A	Аналогічно -U, але використовуються пакети ARP REPLY замість ARP REQUEST

Параметр	Використання
-h, -help	Вивід довідкової інформації
-v, -version	Версія програми
-r, -report	Поміщає mtr в режим звіту. У цьому режимі, mtr обробить кількість циклів, визначених опцією -c, потім відобразить статистику і завершить роботу. Цей режим корисний для генерації статистики про якість мережі
-c COUNT	Встановити кількість циклів, після яких mtr завершить роботу
-s BYTES	Розмір пакетів, що посилаються
-n	Не використовувати DNS. Відображати IP-адреси і не намагатися отримати їх хостнейми
-o fields order	Використовуйте цю опцію, щоб визначити відображувані поля, наприклад -o "LSD NBAW"

Наприклад, `mtr google.com`

Виконання комп'ютерного практикуму

Завдання 1. Відкрити файл Завдання1_ЛР3.рка. Здійснити вивчення ARP-запиту, таблиці MAC-адрес комутатора та процесу ARP у випадку віддаленого зв'язку.

Частина 1. Вивчення ARP-запиту. Для цього:

1. Генеруйте ARP-запити, надсилаючи запит ping на 172.16.31.3 з вузла 172.16.31.2.

Натисніть 172.16.31.2 і відкрийте Command Prompt.

Введіть команду `arp -d` для очищення ARP-таблиці.

Увійдіть в режим моделювання Simulation і введіть команду `ping 172.16.31.3`. Буде створено два PDU. Команда ping не може відправити ICMP-пакет, не знаючи MAC-адресу призначення. Тому комп'ютер відправляє широкомовну розсилку кадру ARP, щоб знайти MAC-адресу призначення.

Натисніть Capture/Forward один раз. PDU ARP переміщується на комутатор Switch1, а ICMP PDU зникає, чекаючи на ARP-відповідь. Відкрийте PDU і запишіть MAC-адресу призначення.

Натисніть кнопку Capture/Forward, щоб перемістити PDU до наступного пристрою. Яка IP-адреса пристрою, що прийняв PDU?

Відкрийте PDU і перегляньте Рівень 2.

Що сталося з MAC-адресами джерела та призначення?

Натискати кнопку Capture/Forward, доки PDU не повернеться до 172.16.31.2.

Скільки копій PDU зробив комутатор під час ARP-відповіді?

2. Вивчіть ARP-таблицю. Для цього:

- відкрийте PDU і погляньте на MAC-адреси;
- поверніться до режиму реального часу Realtime, і пінгування завершиться;

- натисніть 172.16.31.2 і введіть команду `arp -a`.

Якій IP-адресі відповідає запис MAC-адреси?

Частина 2. Вивчення таблиці MAC-адрес комутатора.

1. Створіть додатковий трафік для наповнення таблиці MAC-адрес комутатора. Для цього:

- натисніть 172.16.31.2 і введіть команду `ping 172.16.31.4`;
- натисніть 10.10.10.2 і відкрийте командний рядок Command Prompt;
- введіть команду `ping 10.10.10.3`.

Скільки відповідей було надіслано та отримано?

2. Вивчіть таблицю MAC-адрес на комутаторах.

Натисніть Switch1, а потім вкладку CLI. Введіть команду `show mac-address-table`.

Чи відповідають записи тим, що в таблиці вище? Чому дві MAC-адреси пов'язані з одним портом?

Частина 3. Вивчення процесу ARP у випадку віддаленого зв'язку.

1. Генеруйте трафік для створення ARP-трафіку.

Натисніть 172.16.31.2 і відкрийте Command Prompt.

Введіть команду `ping 10.10.10.1`.

Введіть `arp -a`. Яка IP-адреса нового запису ARP-таблиці?

Введіть `arp -d`, щоб очистити ARP-таблицю, і перейдіть в режим моделювання Simulation.

Повторіть команду `ping` для 10.10.10.1.

Скільки PDU відображається?

Натисніть Capture/Forward. Натисніть PDU, який зараз знаходиться у Switch1.

Яка цільова IP-адреса призначення ARP-запиту? IP-адреса призначення не 10.10.10.1. Чому?

2. Вивчіть ARP-таблицю маршрутизатора Router1.

Перейдіть в режим реального часу Realtime. Натисніть Router1, а потім перейдіть на вкладку CLI.

Увійдіть в привілейований режим EXEC, а потім введіть команду `show mac-address-table`.

Скільки MAC-адрес в таблиці? Чому?

Введіть команду `show arp`.

Чи є запис для 172.16.31.2?

Завдання 2. Відкрити файл Завдання2_ЛР3.pka. Перевірити мережеве з'єднання за допомогою утиліт `ping` і `tracert`.

Частина 1. Перевірка та відновлення IPv4-з'єднання.

1. Використайте команди `ipconfig` та `ping` для перевірки з'єднання. Для цього:

– натисніть на PC1 та відкрийте Command Prompt;

- введіть команду `ipconfig /all` для збору даних про IPv4. Доповніть Таблицю адресації вказавши IPv4-адресу, маску підмережі та шлюз за замовчуванням;

- натисніть на PC3 та відкрийте Command Prompt;

- введіть команду `ipconfig /all` для збору даних про IPv4. Доповніть Таблицю адресації вказавши IPv4-адресу, маску підмережі та шлюз за замовчуванням;

- використайте команду `ping` для перевірки з'єднання між PC1 і PC3. Запит `ping` повинен завершитися помилкою.

2. Знайдіть джерело збою з'єднання.

На PC1 введіть команду для трасування маршруту до PC3. Яка остання успішна IPv4 адреса була досягнута?

Трасування припиниться після 30 спроб. Щоб зупинити трасування передчасно до 30 спроб, натисніть `Ctrl+C`.

На PC3 ввести команду для трасування маршруту до PC1.

Яка остання успішна IPv4 адреса була досягнута?

Щоб зупинити трасування передчасно до 30 спроб, натисніть `Ctrl+C`.

Натисніть на R1. Натисніть `ENTER` та увійдіть до системи маршрутизатора.

Введіть команду `show ip interface brief`, щоб вивести список інтерфейсів і їхній статус.

Введіть команду `show ip route`, щоб відобразити список мереж під'єднаних до маршрутизатора. Зверніть увагу, що до інтерфейсу `Serial0/0/1` під'єднано дві мережі. Які вони?

Повторіть дії на R3 та запишіть свої відповіді.

Натисніть R2. Натисніть `ENTER` та увійдіть до системи маршрутизатора.

Введіть команду `show ip interface brief` та запишіть адреси.

Виконайте додаткові перевірки, якщо це допоможе виявити проблему. Доступний режим симуляції.

3. Запропонуйте вирішення проблеми.

Порівняйте отримані відповіді на кроці 2 з наявною документацією про мережу.

Яке рішення ви б запропонували для даної проблеми?

4. Реалізуйте запропоноване рішення.

5. Перевірте чи з'єднання відновлено.

З PC1 перевірте з'єднання до PC3.

Частина 2. Перевірка та відновлення IPv6-з'єднання

1. Використайте команду `ipv6config` та `ping` для перевірки з'єднання. Для цього:

- натисніть на PC2 та відкрийте Command Prompt;

- введіть команду `ipv6config /all` для збору даних про IPv6. Доповніть Таблицю адресації вказавши IPv6-адресу, префікс підмережі та шлюз за замовчуванням;

- натисніть на PC4 та відкрийте Command Prompt;

- введіть команду `ipv6config /all` для збору даних про IPv6. Доповніть Таблицю адресації вказавши IPv6-адресу, префікс підмережі та шлюз за замовчуванням;

- перевірте з'єднання між PC2 і PC4. Запит `ping` не повинен спрацювати;

- знайдіть джерело збою з'єднання.

З PC2 введіть необхідну команду для трасування маршруту до PC4. Яка остання IPv6-адреса успішно досягнута?

Трасування припиниться після 30 спроб. Щоб зупинити трасування передчасно до 30 спроб, натисніть `Ctrl+C`.

З PC4 введіть необхідну команду для трасування маршруту до PC2. Яка остання IPv6-адреса успішно досягнута?

Щоб зупинити трасування натисніть `Ctrl+C`.

Натисніть на R3. Натисніть `ENTER` та увійдіть до системи маршрутизатора.

Введіть команду `show ipv6 interface brief`, щоб показати список інтерфейсів та їх статус. На маршрутизаторі є дві адреси IPv6. Одна повинна відповідати адресі шлюзу за замовчуванням, отриманому на Кроці 1.

Виконайте додаткові перевірки, якщо це допоможе виявити проблему. Доступний режим симуляції.

3. Запропонуйте вирішення проблеми. Порівняйте отримані відповіді на кроці 2 з наявною документацією про мережу.

Крок 4. Реалізуйте запропоноване рішення.

Крок 5. Перевірте чи з'єднання відновлено.

З PC2 перевірте з'єднання до PC4.

З PC4 перевірте з'єднання до PC2. Чи вдалося усунути проблему?

Завдання 3. Відкрити файл Завдання3_ЛР3.pka. Виконайте дослідження потоків трафіку в маршрутизованій мережі.

Частина 1. Дослідження потоків трафіку в немаршрутизованій локальній мережі.

Мережа XYZ складається з приблизно 150 пристроїв, підключених до LAN. LAN налаштовано на єдину підмережу IPv4. Вузли в різних відділах підключаються до комутаторів, які потім з'єднуються з маршрутизатором Edge. Маршрутизатор лише переадресовує трафік між LAN та Інтернетом, представленим хмарою ISP. Оскільки в LAN використовується лише одна підмережа, усі відділи знаходяться в одній мережі.

Топологія Packet Tracer спрощена. Тут показано лише деякі відділи та вузли.

Очистіть ARP-кеш на хості Sales

1. Наведіть курсор миші на вузол Sales 1, щоб побачити його IP-адресу. Запишіть її. Натисніть Sales 1 > вкладка Desktop > Command Prompt, а потім введіть команду `arp -a`. У ARP-кеші не повинно бути MAC-адрес. Якщо в ARP-кеші є записи, видаліть їх за допомогою команди `arp -d`.

2. Дослідить трафік у мережі.

Натисніть кнопку Simulation в правому нижньому куті вікна PT, щоб перемкнутися з режиму Realtime на режим Simulation.

Відкрийте Command Prompt для Sales 2, а потім виконайте команду ping для IP-адреси Sales 1.

Скористайтеся кнопкою Capture then Forward (трикутник, спрямований вправо з вертикальною смужкою) в Play Controls на Simulation Panel, щоб розпочати виконання команди ping. Поруч із Sales 2 з'явиться піктограма кольорового конверта. Це PDU. Натисніть кнопку Capture then Forward, щоб перемістити PDU до першого пристрою на шляху до цільового пристрою. Натисніть на конверт PDU, щоб переглянути його вміст. Які MAC- та IP-адреси джерела та призначення мають кадр та пакет? Чому MAC-адреса призначення є широкомовною адресою?

Просувajte PDU мережею, доки в Sales 2 не буде створено новий PDU (іншого кольору).

У Sales 2 з'явився новий PDU іншого кольору. Натисніть новий PDU та поверніться до режиму Realtime.

Частина 2. Переналаштування мережі для маршрутизації між локальними мережами.

1. Змініть підключення пристроїв.

Три комутатори з'єднані один з одним мідними прямими кабелями.

Для кабелю, який з'єднує маршрутизатор Accounting з маршрутизатором Finance, натисніть збоку зелений трикутник на маршрутизаторі Accounting на стороні з'єднання.

Перетягніть цей кінець кабелю до маршрутизатора Edge і під'єднайте його до порту GigabitEthernet 1/0.

Повторіть цей крок для встановлення з'єднання між Finance і Sales. Під'єднайтеся до вільного порту GigabitEthernet.

2. Налаштуйте вузли з адресами у нових локальних мережах.

Кожен інтерфейс маршрутизатора Edge був попередньо налаштований так, щоб кожний відділ працював у власній мережі IPv4. Вузли отримують свої нові IP-адреси від маршрутизатора. Однак, для того, щоб вузли в мережах Finance та Sales отримали нові IP-адреси, знадобиться певний час. (Вузли в мережі Accounting залишаються на 192.168.1.0/24.)

Щоб пришвидшити процес отримання нових IP-адрес, відкрийте Command Prompt на кожному з чотирьох пристроїв у мережах Finance та Sales.

Введіть команду `ipconfig /renew`. Це змусить вузол запросити нову IP-адресу у DHCP-сервера, який працює на Edge маршрутизаторі. Треба отримати підтвердження нової IP-адреси.

Яка підмережа призначена для мережі Finance?

Яка підмережа призначена для мережі Sales?

Частина 3: Дослідження потоків трафіку в маршрутизованій мережі.

1. Перейдіть до Sales 1 із Sales 2.

Поверніться до Command Prompt для Sales 2 і переконайтеся, що його ARP-кеш порожній. Якщо це не так, видаліть всі записи.

Перейдіть до режиму Simulation.

Виконайте `ping` з Sales 2 до Sales 1.

Скористайтесь кнопкою Capture then Forward, щоб покроково переглянути PDUs у мережі. Зверніть увагу, як цього разу повідомлення ARP-запиту передається через мережу. Які пристрої отримують широкомовні повідомлення ARP цього разу?

2. Виконайте ping інших хостів.

Повторіть `ping`, перевіривши інші вузли та інтернет-сервер. Зверніть увагу на потік PDU ARP-запитів. Яку перевагу надає використання декількох мереж або підмереж на підприємстві?

Склад звіту комп'ютерного практикуму

В звіті повинно бути відображено:

1) Тема роботи.

2) Мета роботи.

3) Постановка задачі.

4) Виконання завдання 1 з відповідними скріншотами та відповідями на запитання.

5) Виконання завдання 2 з відповідними скріншотами та відповідями на запитання.

6) Виконання завдання 3 з відповідними скріншотами та відповідями на запитання.

7) Висновок.

Контрольні питання:

Яке основне призначення протоколу ARP?

На якому рівні моделі OSI працює ARP і чому ARP-запит є широкомовним (broadcast)?

Що таке ARP-кеш (ARP cache) і чому записи в ньому мають обмежений час життя (TTL)?

Чи можна застосувати arping для перевірки, чи не використовується вже бажана IP-адреса іншим пристроєм у локальному широкомовному домені, що допомагає запобігти конфліктам IP-адрес?

Яке основне призначення команди ping?

Що таке traceroute і яка її основна мета?

У чому основна різниця між командами traceroute і tracert?

Що таке MTR і чим він відрізняється від традиційних команд ping та traceroute?

Яку основну інформацію надає MTR, окрім послідовності вузлів (хопів)?

КОМП'ЮТЕРНИЙ ПРАКТИКУМ 4

Тема: Мережеві сніфери – tcpdump, wireshark.

Мета заняття: Ознайомитися і навчитися працювати з такими мережевими сніферами, як tcpdump та wireshark. Освоєння аналізаторів мережевого трафіку, отримання навичок написання фільтрів для аналізаторів та ознайомлення зі стеком мережевих протоколів.

Теоретичні відомості

Мережевий сніфер (*network sniffer*) – це програма або пристрій, який перехоплює та аналізує мережевий трафік, що проходить через комп'ютерну мережу. Мережеві сніфери дозволяють здійснювати діагностику мережевих проблем, аналізувати продуктивності мережі, розуміти та досліджувати протоколи, тестувати безпеку власних систем. До основних функції мережевих сніферів віднесено:

- захоплення пакетів даних, що передаються мережею;
- аналіз протоколів (HTTP, TCP, UDP, DNS тощо);
- моніторинг мережевої активності;
- виявлення проблем з мережею.

Найпопулярнішими сніферами є Wireshark – найвідоміший безкоштовний сніфер з графічним інтерфейсом та Tcpdump – консольний інструмент для Linux/Unix.

Мережеві сніфери здебільшого функціонують на канальному рівні (Data Link Layer, рівень 2) моделі OSI, проте вони також здатні проводити аналіз даних з кількох рівнів одночасно. Канальний рівень є найнижчим рівнем, на якому можливе перехоплення даних ще до фільтрування їх мережевою картою. Це дозволяє відображати увесь трафік у рамках локального сегмента мережі. У процесі роботи сніфер переводить мережевий адаптер у неселективний режим (*promiscuous mode*), завдяки чому адаптер збирає всі пакети в межах мережевого сегмента, а не лише ті, що адресовані конкретно йому. Після захоплення аналізуються Ethernet-кадри та MAC-адреси. Крім цього, захоплений трафік на

канальному рівні може бути розшифрований і підданий подальшому аналізу на інших рівнях, таких як:

- рівень 3 (Мережевий) – IP-адреси, маршрутизація;
- рівень 4 (Транспортний) – TCP/UDP порти, з'єднання;
- рівень 7 (Прикладний) – HTTP, FTP, DNS, протоколи додатків.

Таким чином, сніфери працюють на рівні 2, але аналізують дані всіх рівнів OSI від 2 до 7.

Існує кілька основних способів перехоплення мережевого трафіку:

1. Використання «прослуховування» мережевого інтерфейсу. Цей метод особливо ефективний у сегментах мереж, де використано концентратори (хаби) замість комутаторів (світчів). У випадку застосування комутаторів він менш дієвий, адже на сніфер потрапляють лише окремі кадри даних.

2. Підключення сніфера безпосередньо в розрив каналу зв'язку.

3. Відгалуження трафіку, яке може бути реалізоване програмно або апаратно. При цьому копія трафіку перенаправляється на сніфер для аналізу.

4. Аналіз побічних електромагнітних випромінювань, що виникають під час передавання даних. За допомогою цього методу можна відновлювати прослуховуваний трафік.

5. Проведення атак на канальному (MAC-spoofing) або мережевому рівні (IP-spoofing). Такі дії призводять до перенаправлення трафіку жертви або навіть всього сегменту мережі на сніфер, після чого трафік повертається до адресата, так, ніби атаки не було.

Сніфери застосовуються як в позитивних, так і в деструктивних цілях, а саме:

– виявити паразитний, вірусний і закільцьований трафік, наявність якого збільшує завантаження мережного устаткування і каналів зв'язку (сніфери тут малоефективні; як правило, для цих цілей використовують збір різноманітної статистики серверами і активним мережним устаткуванням і її подальший аналіз);

- виявити в мережі шкідливе і несанкціоноване ПЗ, наприклад, мережеві сканери, флудери, троянські програми, клієнти пірінгових мереж та інші (це зазвичай роблять за допомогою спеціалізованих сніфер моніторів мережевої активності);

- перехопити будь-який незашифрований (а деколи і зашифрований) трафік користувача з метою отримання паролів і іншої інформації;

- локалізувати несправність мережі або помилку конфігурації мережних агентів (для цієї мети сніфери часто застосовуються системними адміністраторами)

Також треба пам'ятати, що для запобігання перехоплення зловмисниками конфіденційної інформації (паролів, даних банківських карток) важливо використовувати засоби шифрування, наприклад HTTPS, VPN та інші засоби.

Tcpdump – як вже було зазначено, це потужний та універсальний мережевий сніфер, що використовує інтерфейс командного рядка, завдяки чому, він ідеально підходить для запуску та, відповідно, для збору даних, які можна проаналізувати пізніше, на віддалених серверах або пристроях для яких немає графічного інтерфейсу користувача. Також його можна запускати у фоновому режимі або як заплановане завдання.

Встановлення на Linux. Tcpdump входить до складу кількох дистрибутивів Linux, тому, ймовірно, його вже встановлено. Якщо tcpdump не встановлено, можна встановити його за допомогою dnf менеджера пакетів:

```
dnf install tcpdump
```

Tcpdump вимагає libpcap бібліотеки для захоплення мережних пакетів. Якщо вона не встановлена, вона автоматично додається.

```
TcpDump [ -adeflnNOpqStvx ] [ -c count ] [ -F file ] [ -i interface ] [ -r file ]  
[ -s snaplen ] [ -T type ] [ -w file ] [ expression ]
```

Таблиця. Параметри tcpdump

Параметр	Використання
-a	Дозволяє конвертувати числові IP-адреси у доменні імена, а номерів портів – у назви служб
-c	Вихід після обробки count пакетів
-d	Виводить вміст пакету у зрозумілому людині вигляді
-dd	Виводить вміст пакету як фрагмент C-програми
-ddd	Виводить вміст пакету в десятковому вигляді
-e	Виводить заголовки канального рівня в кожній новій рядку
-f	Виводить адреси віддалених і локального хостів без перетворення в імена
-F	Використовувати file з описом параметрів фільтрації (додаткові вирази в командному рядку ігноруються)
-i	Використовувати інтерфейс interface для трасування. Якщо не визначений, tcpdump знаходить активний мережевий інтерфейс з найменшим номером (виключаючи loopback)
-l	Використовує буферизований вивід на stdout. Корисним може виявитися конструкція вигляду "tcpdump-l tee dat" or " tcpdump-l> dat &tail-f dat"

Параметр	Використання
-n	Не перетворювати адреси (тобто, адресу хоста, номер порту і т.п.) в імена
-N	Не друкувати доменне ім'я в імені хоста. Тобто, якщо використаний даний прапорець, tcpdump надрукує "nic" замість "nic.ddn.mil"
-O	Не запускати оптимізатор пакетів
-p	Не переводити мережевий інтерфейс в "promiscuous mode"
-q	Виводить інформацію в скороченому вигляді
-r	Читає пакети з файлу file (які створені за допомогою опції -w). Якщо ви хочете використовувати в якості введення консоль, то file це "-"
-s	Видає snaplen байт кожного пакета (в SunOS'овському NIT мінімальна кількість 96). 68 байт достатньо для протоколів IP, ICMP, TCP і UDP, проте обрізає інформацію з більш високих рівнів, скажімо, DNS і NFS пакетів

Параметр	Використання
-T	Примусова інтерпретація пакетів по типу type відповідних масці "expression". На даний момент відомі наступні типи: rpc (Remote Procedure Call), rtp (Real-Time Applications protocol), rtcp (Real-Time Applications control protocol), vat (Visual Audio Tool), i wb (distributed White Board)
-S	Виводить абсолютний номер TCP-пакету
-t	Не виводить час в кожному рядку
-tt	Виводить неформатований час в кожному рядку
-v	Детальний вивід. Наприклад, час життя пакетів та тип сервісу
-vv	Більш детальний вивід. Наприклад, вивід додаткових полів NFS reply packets
-w	Записує raw-пакети в file, які ви зможете надалі розшифрувати з використанням опції-r. Якщо ви хочете використовувати в якості виводу консоль, то file це "-"
-X	Виводить кожен пакет в шістнадцятковому вигляді (без заголовка). На вивід буде відправлено snaplen байт

Якщо tcpdump запустити без параметрів, то буде надаватися інформація про всі мережеві пакети. За допомогою параметра -i можна вказати мережевий інтерфейс, з якого слід приймати дані:

```
# tcpdump -i eth2
```

Щоб дізнатися отримані або відправлені пакети від певного хоста, необхідно його ім'я або IP-адресу вказати після ключового слова host:

```
# tcpdump host nameofserver
```

Щоб дізнатися про пакети якими обмінюються nameofserverA та nameofserverB:

```
# tcpdump host nameofserverA and nameofserverB
```

Для відстеження тільки вихідних пакетів від якогось вузла потрібно вказати наступне:

```
# tcpdump src host nameofserver
```

Тільки вхідні пакети:

```
# tcpdump dst host nameofserver
```

Порт відправника і порт одержувача відповідно:

```
# tcpdump dst port 80
```

```
# tcpdump src port 22
```

Щоб відстежувати один з протоколів TCP, UDP, ICMP, його назву слід вказати в команді. Використання операторів and (&&), or (||) і not (!) Дозволяє задавати фільтри будь-якої складності. Приклад фільтра, що відслідковує тільки UDP-пакети, що приходять з зовнішньої мережі:

```
# tcpdump udp and not src net localnet
```

Приклади використання tcpdump як фільтра:

Видача всіх вхідних та вихідних пакетів від sundown:

```
#tcpdump host sundown
```

Видача трафіку між helios і одним з двох hot або ace:

```
#tcpdump host helios and \(hot or ace \)
```

Видача всіх пакетів між ace та іншими хостами, виключаючи helios:

```
#tcpdump ip host ace and not helios
```

Видача трафіку між машиною і машиною, що знаходиться в Berkeley:

```
#tcpdump net ucb-ether
```

Видача ftp трафіку через шлюз snup:

```
#tcpdump 'gateway snup and (port ftp or ftp-data)'
```

Видача трафіку машинам, що не належать локальній мережі (якщо ваша машина – шлюз в іншу мережу, tcpdump не зможе видати трафік вашої локальної мережі).

```
#tcpdump ip and not net localnet
```

Видача старт і стоп пакетів (SYN і FIN пакети), які не належать до локальної мережі.

```
#tcpdump 'tcp[13] & 3!= 0 and not src and dst net localnet'
```

Видача IP пакетів довжиною більше 576 байт, переданих через шлюз snup:

```
#tcpdump 'gateway snup and ip[2:2] > 576'
```

Видача IP broadcast або multicast пакетів, які не посилаються через Ethernet broadcast або multicast:

```
#tcpdump 'ether[0] & 1 = 0 and ip[16] >= 224'
```

Видача всіх ICMP пакетів, які не є запитами-відлуннями / відповідями (тобто, не ping пакети):

```
#tcpdump 'icmp[0]!= 8 and icmp[0]!= 0'
```

Нижче наведено приклади застосування.

Захопіть усі пакети в будь-якому інтерфейсі:

```
tcpdump --interface any
```

Щоб обмежити кількість захоплених пакетів і зупинити tcpdump, використовують опцію -c (для count). У цьому випадку захоплення буде зупинено після захоплення п'яти пакетів. Це корисно в різних сценаріях, наприклад, для усунення несправності з'єднання і тоді достатньо захопити кілька початкових пакетів.

```
tcpdump -i any -c 5
```

За замовчуванням tcpdump перетворює IP-адреси та порти на імена. Під діагностики для усунення несправностей мережі простіше використовувати IP-адреси та номери портів; вимикання розпізнавання імен –це опція -n, а розпізнавання портів відбувається за допомогою -nn:

```
tcpdump -i any -c5 -nn
```

Для перехоплення лише ICMP-пакети, можна скористатися командою:

```
tcpdump -i any -c5 icmp
```

Для обмеження захоплення лише пакетів, пов'язаних з певним хостом, за допомогою host фільтра використовується команда:

```
$ sudo tcpdump -i any -c5 -nn host 54.204.39.132
```

Для перехоплення пакетів, пов'язані з веб-службою (HTTP), можна скористатися port фільтром та командою. (Порт 80 – це стандартний порт для протоколу HTTP (Hypertext Transfer Protocol), який використовується для передачі веб-сторінок в інтернеті) :

```
$ sudo tcpdump -i any -c5 -nn port 80
```

Примітка: Порт – це логічний ідентифікатор, який визначає конкретний процес або службу на комп'ютері, що приймає або передає дані. IP-адреса доставляє пакет до потрібного комп'ютера, а порт направляє його до конкретної програми. Діапазон портів : від 0 до 65535 (16-бітне число). Існують:

- загальновідомі порти (0-1023). Серед них є зарезервовані для стандартних служб. Наприклад, 80 (HTTP), 443 (HTTPS), 22 (SSH), 25 (SMTP);
- зареєстровані порти (1024-49151), що використовуються спеціальними програмами. Наприклад, 3306 (MySQL), 5432 (PostgreSQL);
- динамічні/приватні порти (49152-65535). Їх використовують як тимчасові порти для клієнтських з'єднань.

Для фільтрації пакетів лише з IP-адреси джерела 192.168.122.98 та HTTP-адреси служби, використовують команду:

```
tcpdump -i any -c5 -nn src 192.168.122.98 and port 80
```

Можна групувати filter за допомогою дужок. У цьому випадку треба взяти візьміть весь вираз filter у лапки, щоб сніфер не плував їх з виразами сніфера. Фільтрація пакетів лише для HTTP-сервісу (порт 80) та вихідних IP-адрес 192.168.122.98 або 54.204.39.132:

```
$ sudo tcpdump -i any -c5 -nn "port 80 and (src 192.168.122.98 or src 54.204.39.132)"
```

У попередніх прикладах перевірялися лише заголовки пакетів на наявність такої інформації, як джерело, пункти призначення, порти тощо. Іноді цього достатньо для усунення проблем із підключенням до мережі. Тому треба перевірити вміст пакета, щоб переконатися, що повідомлення, яке надсилається, містить те, що потрібно, тобто отримана відповідь задовольняє очікувань. Щоб переглянути вміст пакета, tcpdump надає два додаткові прапорці: -X для друку вмісту в шістнадцятковому форматі та ASCII або -A для друку вмісту в ASCII.

Наприклад, перевірити HTTP-вміст веб-запиту можна за допомогою:

```
tcpdump -i any -c10 -nn -A port 80
```

Для збереження пакетів у файл для подальшого детального аналізу, а не відображення їх на екрані, використовується опція -w (для write):

```
tcpdump -i any -c10 -nn -w webserver.pcap port 80
```

Основні найбільш використовувані команди можна знайти за посиланням <https://www.packetlevel.ch/workshop/drahthai/tcpdump.pdf>

Wireshark (*раніше – Ethereal*) – програма-аналізатор трафіку для комп'ютерних мереж Ethernet і деяких інших. Має графічний користувацький інтерфейс. У червні 2006 року проект був перейменований в Wireshark через проблеми з торговою маркою. Функціональність, яку надає Wireshark, дуже схожа з можливостями програми tcpdump, проте Wireshark має графічний користувацький інтерфейс і більше можливостей із сортування і фільтрації інформації. Wireshark збирає дані з мережевих інтерфейсів (таких як Ethernet, Wi-Fi та VPN) та відображає необроблений трафік у зручному для читання форматі. Користувачі можуть застосовувати фільтри для перегляду певних потоків даних або аналізу того, як різні пристрої взаємодіють. Існують

версії для більшості типів UNIX, в тому числі Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, а також для Windows. Wireshark можна безкоштовно завантажити з офіційного вебсайту <https://www.wireshark.org/>

Інструкція для користувача знаходиться за посиланням: https://www.wireshark.org/docs/wsug_html/

Вікно програми має вигляд та містить наступні пункти меню:

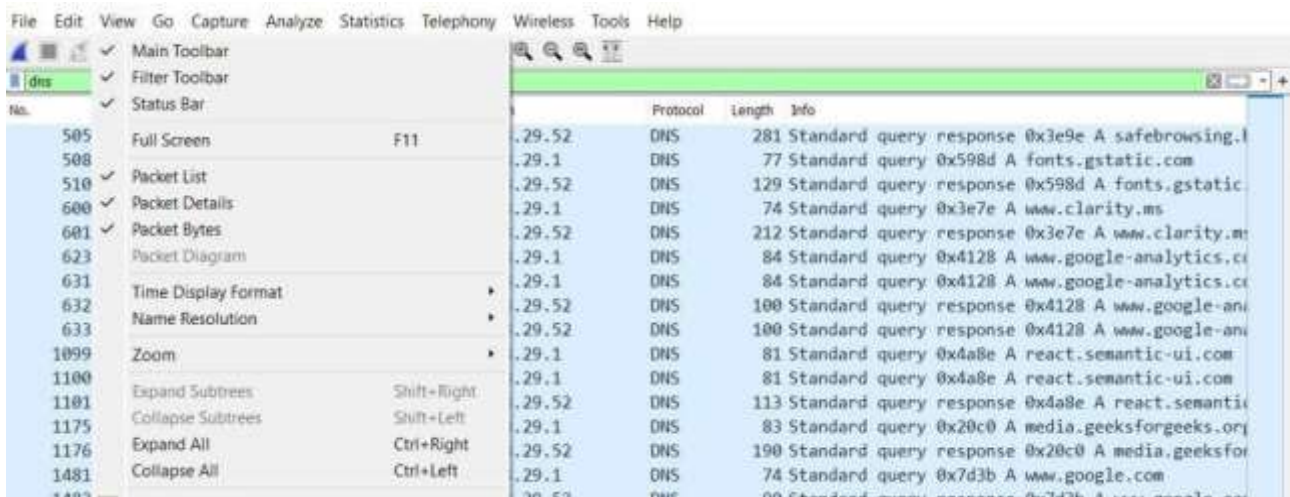


Рисунок 4.1 – Головне вікно програми

File (Файл)

Робота з файлами захоплення:

Open – відкрити збережений файл захоплення (.pcap, .pcapng)

Open Recent – нещодавно відкриті файли

Merge – об'єднати кілька файлів захоплення

Import from Hex Dump – імпорт з hex-файлу

Close – закрити поточний файл

Збереження:

Save / Save As – зберегти захоплення

Export Specified Packets – експорт вибраних пакетів

Export Packet Dissections – експорт у текстовому форматі (CSV, JSON, XML)

Export Objects – витягти об'єкти (HTTP, SMB, TFTP файли)

Друк:

Print – друк пакетів

Quit – вихід з програми

Edit (Редагування)

Copy – копіювання інформації про пакети

Find Packet (Ctrl+F) – пошук пакетів

Find Next / Previous – наступний/попередній результат пошуку

Mark/Unmark Packet – позначити пакет для відстеження

Mark All Displayed – позначити всі видимі

Time Reference – встановити часову мітку відліку

Configuration Profiles – профілі налаштувань

Preferences – основні налаштування Wireshark

View (Вигляд)

Масштабування:

Zoom In/Out – збільшити/зменшити

Normal Size – нормальний розмір

Панелі:

Main Toolbar – головна панель інструментів

Filter Toolbar – панель фільтрів

Wireless Toolbar – панель бездротових мереж

Status Bar – рядок стану

Колонки:

Time Display Format – формат відображення часу

Name Resolution – розв'язання імен (MAC, IP, порти)

Colorize Packet List – кольорове виділення пакетів

Auto Scroll in Live Capture – автопрокрутка при захопленні

Розширення/згортання:

Expand Subtrees – розгорнути деталі пакету

Collapse All – згорнути всі деталі

Режими:

Reload – перезавантажити файл

Go (Перехід)

Навігація по пакетах:

Back / Forward – назад/вперед по історії

Go to Packet (Ctrl+G) – перейти до пакету за номером

Go to Corresponding Packet – до відповідного пакету

Previous/Next Packet – попередній/наступний

First/Last Packet – перший/останній пакет

Previous/Next Packet in Conversation – у межах діалогу

Capture (Захоплення)

Управління захопленням:

Interfaces – вибір мережових інтерфейсів

Options – налаштування параметрів захоплення

Start – почати захоплення

Stop – зупинити

Restart – перезапустити

Capture Filters – фільтри захоплення (BPF синтаксис)

Refresh Interfaces – оновити список інтерфейсів

Analyze (Аналіз)

Аналіз пакетів:

Display Filters – керування фільтрами відображення

Display Filter Macros – макроси фільтрів

Apply as Filter – застосувати як фільтр

Prepare as Filter – підготувати фільтр

Enabled Protocols – увімкнені протоколи

Decode As – декодувати як інший протокол

User Specified Decodes – користувацьке декодування

Follow – відстежити потік (TCP/UDP/HTTP/TLS Stream)

Expert Information – експертна інформація (помилки, попередження)

Conversation Filter – фільтр діалогів

Protocol Hierarchy – ієрархія протоколів

Statistics (Статистика)

Аналіз трафіку:

Capture File Properties – властивості файлу

Protocol Hierarchy – статистика протоколів

Conversations – діалоги між хостами

Endpoints – кінцеві точки (IP-адреси)

Packet Lengths – розподіл довжини пакетів

I/O Graph – графік вхідного/вихідного трафіку

Service Response Time – час відгуку служб

Flow Graph – графік послідовності пакетів

Протоколи:

HTTP – статистика HTTP (запити, коди відповідей)

DNS – статистика DNS

TCP Stream Graphs – графіки TCP-потоків

Telephony (Телефонія)

VoIP і телефонні протоколи:

RTP – аналіз RTP-потоків

SIP – SIP-дзвінки

VoIP Calls – список VoIP-дзвінків

Wireless (Бездротові мережі)

Для Wi-Fi аналізу:

WLAN Traffic – статистика Wi-Fi трафіку

Tools (Інструменти)

Firewall ACL Rules – генерація правил файрволу

Credentials – знайдені облікові дані (паролі)

Lua – виконання Lua-скриптів

Help (Допомога)

Contents – довідка

Manual Pages – сторінки посібника

Website – офіційний сайт

Wiki – wiki Wireshark

About Wireshark – інформація про версію

Після запуску Wireshark в головному вікні програми буде список мережевих інтерфейсів (Ethernet, Wi-Fi, VPN мають теж окремий інтерфейс). Необхідно обрати потрібний інтерфейс, через який проходить потрібний для аналізу трафік (рис.4.2.).

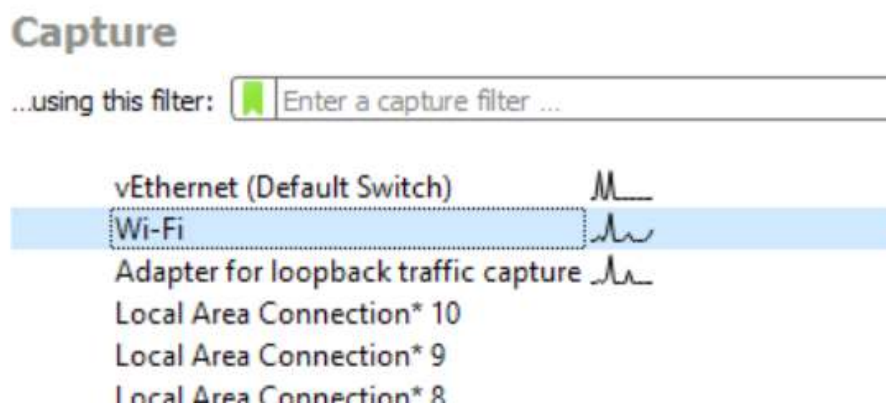


Рисунок 4.2 – Вибір інтерфейсу для аналізу

Для фільтрації трафіку можна використовувати фільтри захоплення (Capture filter) та фільтри відображення (Display filter).

Фільтр відображення захоплює весь трафік з мережевої карти та відображає/ фільтрує, що потрібно. Фільтр захоплення захоплює і зберігає лише той трафік, який прописаний у фільтрі. Фільтр захоплення можна прописати відразу при виборі інтерфейсу Capture ...using this filter). Найпопулярніші фільтри це фільтр за хостом (host www.nbuv.gov.ua) та фільтр за протоколом та портом (tcp port 35170). Список всіх фільтрів можна переглянути за посиланням <https://wiki.wireshark.org/CaptureFilter>. Фільтри відображення можна змінювати під час захоплення трафіку. Список фільтрів відображення можна переглянути за посиланням <https://wiki.wireshark.org/DisplayFilters>. Також можливе використання операторів (==, !=, <, >, <=, >=, contains, matches) та об'єднання

фільтрів за допомогою логічних операцій: `&&` , `||`. Наприклад, `ip.addr == 10.20.7.192 && tcp.port == 1250`.

Виконання комп'ютерного практикуму

Завдання 1. З використанням програмного забезпечення `tcpdump` виконати наступні завдання.

1. Переглянути, який трафік проходить через основний мережевий інтерфейс.

Команда: `tcpdump -i <ім'я_інтерфейсу>`. Наприклад: `tcpdump -i eth0` (замініть `eth0` на ім'я вашого інтерфейсу, наприклад, `enp3s0`). Треба зайти на довільний сайт, щоб побачити, які пакети надсилаються та приймаються.

2. Відфільтрувати трафік за IP-адресою. Треба переглянути тільки трафік, пов'язаний з конкретною віддаленою IP-адресою. Наприклад, `tcpdump host 8.8.8.8` (це покаже весь трафік або від сервера Google DNS). Треба вказати іншу віддалену IP-адресу.

3. Відфільтрувати трафік по порту. Для цього переглянути весь трафік, що йде на певний порт або з нього. Команда: `tcpdump port <номер_порту>` Наприклад: `tcpdump port 80` (покаже весь HTTP-трафік) або `tcpdump port 443` (покаже весь HTTPS-трафік). Зверніть увагу, що для незахищених протоколів (як HTTP) можна побачити вміст пакетів, а HTTPS-трафік буде зашифрований

4. Записати трафік у файл. Для цього зберегти захоплені пакети у файл для подальшого аналізу. Наприклад, `tcpdump -i eth0 -w mycapture.pcap` (захоплює трафік з `eth0` та записує його у файл `mycapture.pcap`). Збережений файл можна аналізувати за допомогою `tcpdump` (команда `sudo tcpdump -r mycapture.pcap`) або інших інструментів, таких як Wireshark.

5. Обмежити кількість пакетів. Для цього захопити невелику кількість пакетів, щоб не перевантажувати термінал і уникнути надто великого файлу. Наприклад, `tcpdump -i eth0 -c 10` (захопить лише 10 пакетів).

Завдання 2. Завантажити та встановити Wireshark.

1. Завантаження Wireshark. Wireshark можна завантажити з сайту www.wireshark.org. Для цього оберіть необхідну версію програмного продукту, враховуючи архітектуру та операційну систему вашого комп'ютера. Щойно вибір зроблено, завантаження має розпочатися. Розташування завантаженого файлу залежить від використовуваного браузера та операційної системи. Для користувачів Windows за замовчуванням використовується папка Downloads.

2. Встановлення Wireshark. Завантажений файл має назву Wireshark-win64-x.x.x.exe, де x – це номер версії. Двічі натисніть на значку файла, щоб розпочати процес встановлення. Відповідайте на будь-які повідомлення безпеки, які можуть відображатися на екрані. Якщо копія Wireshark вже встановлена то буде запропоновано видалити стару версію перед встановленням нової версії. Перед встановленням іншої версії рекомендується видалити стару версію Wireshark. Натисніть Yes, щоб видалити попередню версію Wireshark. Якщо встановлюється Wireshark вперше або після завершення процесу видалення попередньої версії, здійснюється перехід до Wireshark Setup Wizard. Для захоплення даних в реальному часі на комп'ютері повинен бути встановлений Npcap. Якщо на комп'ютері Npcap вже встановлено, опція Встановити не буде зазначена. Якщо встановлена версія Npcap старіша ніж версія, яка йде в комплекті з Wireshark, рекомендується встановити нову версію, вибравши опцію Install Npcap x.x.x (номер версії). НЕ встановлюйте USBPcap для захоплення звичайного трафіку. НЕ обирайте опцію Встановити USBPcap. USBPcap є експериментальним, і це може спричинити проблеми з використанням USB на ПК. Натисніть Install , щоб продовжити. Wireshark починає встановлювати свої файли та відображати стан встановлення. В окремому вікні прийміть ліцензійні умови в Npcap Setup Wizard, якщо встановлюєте Npcap. Закінчить встановлення та перезавантажте комп'ютер, якщо це необхідно.

Завдання 3. Відкрити файл Завдання3_ЛР.pka та за допомогою Wireshark здійснити перегляд мережного трафіку.

Для виконання завдання використовуйте реальну мережу, яка має наступну топологію.

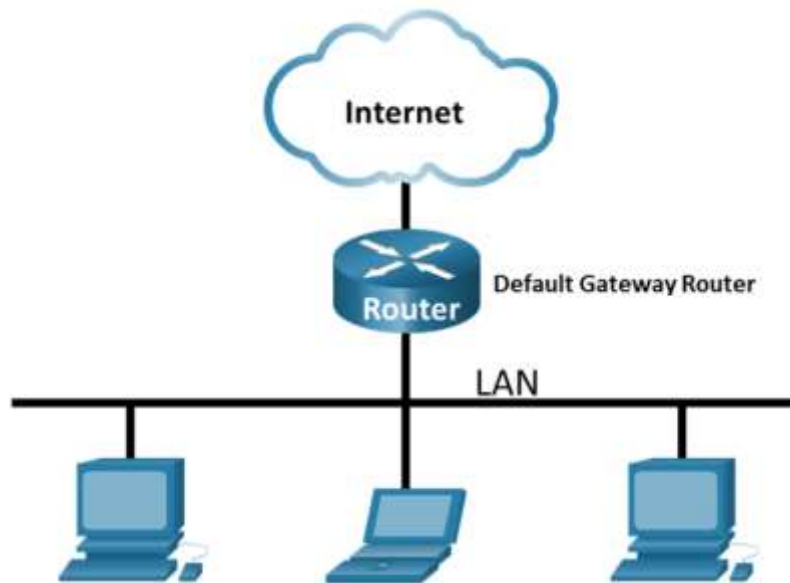


Рисунок 4.3 – Топологія мережі для виконання Завдання 3

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

1. Визначення адрес мережевої плати ПК.

Відкрийте вікно командного рядка Windows.

У командному рядку введіть команду `ipconfig /all`, щоб переглянути IP-адресу, MAC-адресу, опис мережевої плати вашого ПК.

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

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

2. Запуск Wireshark і початок перехоплення даних.

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

У верхній частині вікна Wireshark рядки даних почнуть прокручуватися донизу. Рядки даних, залежно від протоколу, матимуть різне забарвлення. Вони можуть прокручуватися дуже швидко. Швидкість залежатиме від інтенсивності

спілкування, яке зараз відбувається між Вашим ПК та іншими вузлами локальної мережі. Для полегшення перегляду даних, які перехоплює Wireshark, та подальшого їх опрацювання можна застосувати фільтри.

Наберіть `icmp` у полі Filter у верхній частині вікна Wireshark і натисніть або Enter, або кнопку Apply (значок стрілочки), щоб переглядати тільки ICMP-повідомлення.

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

```
C:\> ping 192.168.1.114
```

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

Зупиніть перехоплення даних, натиснувши значок Stop Capture.

3. Дослідження перехоплених даних.

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

Якщо цей кадр все ще вибраний, перейдіть до середньої частини. Натисніть на значок стрілки ліворуч від рядка Ethernet II, щоб переглянути MAC-адреси отримувача та відправника кадру. Чи співпадає MAC-адреса відправника з MAC-адресою мережної плати/інтерфейсу вашого ПК?

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

1. Початок перехоплення даних на мережевій платі/інтерфейсі.

Розпочніть перехоплення даних знову.

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

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

Відкрийте вікно командного рядка Windows

1) www.yahoo.com

2) www.cisco.com

3) www.google.com.

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

IP-адреса для www.yahoo.com:

MAC-адреса для www.yahoo.com:

IP-адреса для www.cisco.com:

MAC-адреса для www.cisco.com:

IP-адреса для www.google.com:

MAC-адреса для www.google.com:

Склад звіту комп'ютерного практикуму

В звіті повинно бути відображено:

1) Тема роботи.

2) Мета роботи.

3) Постановка задачі.

4) Виконання завдання 1 з відповідними скріншотами.

5) Виконання завдання 2 з відповідними скріншотами.

6) Виконання завдання 3 з відповідними скріншотами та відповідями на запитання.

7) Висновок.

Контрольні питання:

У чому головна відмінність між tcpdump і Wireshark.

Два хоста обмінюються пакетами між собою, як за допомогою утиліти `tcpdump` можна подивитися їх трафік?

Що буде, якщо в поле фільтра після сеансу захоплення мережевого трафіку Wireshark ввести «`ftp || ftp-data`»?

Яким чином можна подивитися статистику по протоколам після аналогічного сеансу Wireshark?

Чи можна за допомогою Wireshark перехопити паролі або текстові повідомлення, призначені іншому користувачеві? Що для цього потрібно?