

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет інформатики та обчислювальної техніки

О.І. Ролік, О.В. Бойко

КОМП'ЮТЕРНІ МЕРЕЖІ

Комп'ютерний практикум

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня бакалавра
за освітньою програмою «Інтегровані інформаційні системи»
за спеціальністю F6 «Інформаційні системи і технології»

Електронне мережне навчальне видання

Київ
КПІ ім. Ігоря Сікорського
2025

УДК 004.7(075.8)

Укладачі: *Ролік Олександр Іванович*, завідувач кафедри інформаційних систем та технологій, технологій, факультету інформатики та обчислювальної техніки, д.т.н., професор

Бойко Олександра Володимирівна, доцент кафедри інформаційних систем та технологій, технологій, факультету інформатики та обчислювальної техніки, к.т.н., доцент.

Рецензент: *Волокита Артем Миколайович*, к.т.н., доцент кафедри обчислювальної техніки, факультету інформатики та обчислювальної техніки.

Відповідальний редактор: *Писаренко Андрій Володимирович*, к.т.н., доцент кафедри інформаційних систем та технологій, факультету інформатики та обчислювальної техніки

*Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол №Сод/04.01.02.01/1097/26 від 17.02.2026 р.)
за поданням Вченої ради факультету/навчально-наукового інституту
(протокол № 5 від 28.12.2025 р.)*

Комп'ютерні мережі. Комп'ютерний практикум. [Електронний ресурс]: навч. посіб. для здобувачів ступеня бакалавра за спеціальністю F6 «Інформаційні системи і технології» / уклад: О.І. Ролік, О.В. Бойко. – Електрон. текст. дані (1 pdf-файл). — Київ: КПІ ім. Ігоря Сікорського, 2025. — 176 с.

Посібник розроблений на основі силабусу навчальної дисципліни «Комп'ютерні мережі», предметом якої є теоретичні та практичні основи побудови та функціонування комп'ютерних мереж. Посібник призначений для якісного виконання комп'ютерного практикуму з відповідної дисципліни здобувачами ступеня бакалавра за спеціальністю F6 «Інформаційні системи і технології» денної та заочної форм навчання.

УДК 004.7(075.8)

Реєстр. № 25/26-149. Обсяг 11,2 авт. арк.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Перемоги, 37, м. Київ, 03056. <https://kpi.ua>

Свідectво про внесення до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

© КПІ ім. Ігоря Сікорського, 2025

© Олександр РОЛІК, 20.12.2025

© Олександра БОЙКО, 20.12.2025

© КПІ ім. Ігоря Сікорського, 2025

ЗМІСТ

ВСТУП	5
КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 1	6
Теоретичні відомості	6
Виконання комп'ютерного практикуму	19
Склад звіту комп'ютерного практикуму	24
КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 2	25
Теоретичні відомості	25
Виконання комп'ютерного практикуму	36
Склад звіту комп'ютерного практикуму	43
КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 3	45
Теоретичні відомості	45
Виконання комп'ютерного практикуму	55
Склад звіту комп'ютерного практикуму	63
КОМП'ЮТЕРНИЙ ПРАКТИКУМ 4	64
Теоретичні відомості	64
Виконання комп'ютерного практикуму	79
Склад звіту комп'ютерного практикуму	83
КОМП'ЮТЕРНИЙ ПРАКТИКУМ 5	85
Теоретичні відомості	85
Виконання комп'ютерного практикуму	112
Склад звіту комп'ютерного практикуму	118
КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 6	120
Теоретичні відомості	120
Виконання комп'ютерного практикуму	127

Склад звіту комп'ютерного практикуму	129
КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 7	130
Теоретичні відомості	130
Виконання комп'ютерного практикуму	143
Склад звіту комп'ютерного практикуму	146
КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 8	148
Теоретичні відомості	148
Виконання комп'ютерного практикуму	156
Склад звіту комп'ютерного практикуму	165
КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 9	166
Теоретичні відомості	166
Виконання комп'ютерного практикуму	172
Склад звіту комп'ютерного практикуму	174
ЛІТЕРАТУРА	176

ВСТУП

Комп'ютерний практикум відповідає робочій програмі навчальної дисципліни «Комп'ютерні мережі» і сприяє формуванню у студентів необхідних знань, навичок і вмінь згідно з вимогами освітньої програми підготовки фахівців за спеціальністю F6 – Інформаційні системи з технології.

Виконання наведених у навчальному посібнику комп'ютерних практикумів дозволить студентам:

- 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 транспортними 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;
- навчитися розрізняти функції концентраторів і комутаторів та базові правила побудови бездротових мереж;
- освоїти команди конфігурації пристрою через командний рядок та зберігати їх файл.

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

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.

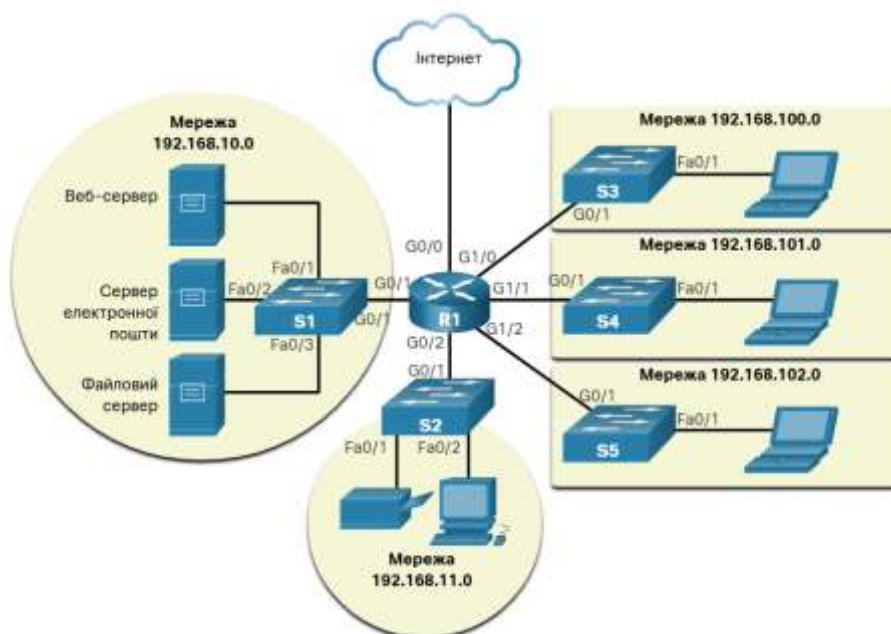


Рисунок 1.4 – Логічна топологія мережі

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

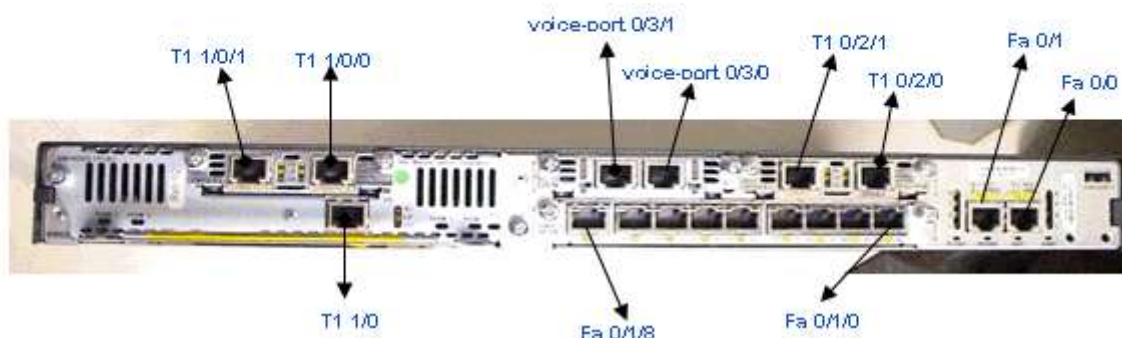


Рисунок 1.5 – Типи та номери інтерфейсів

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.

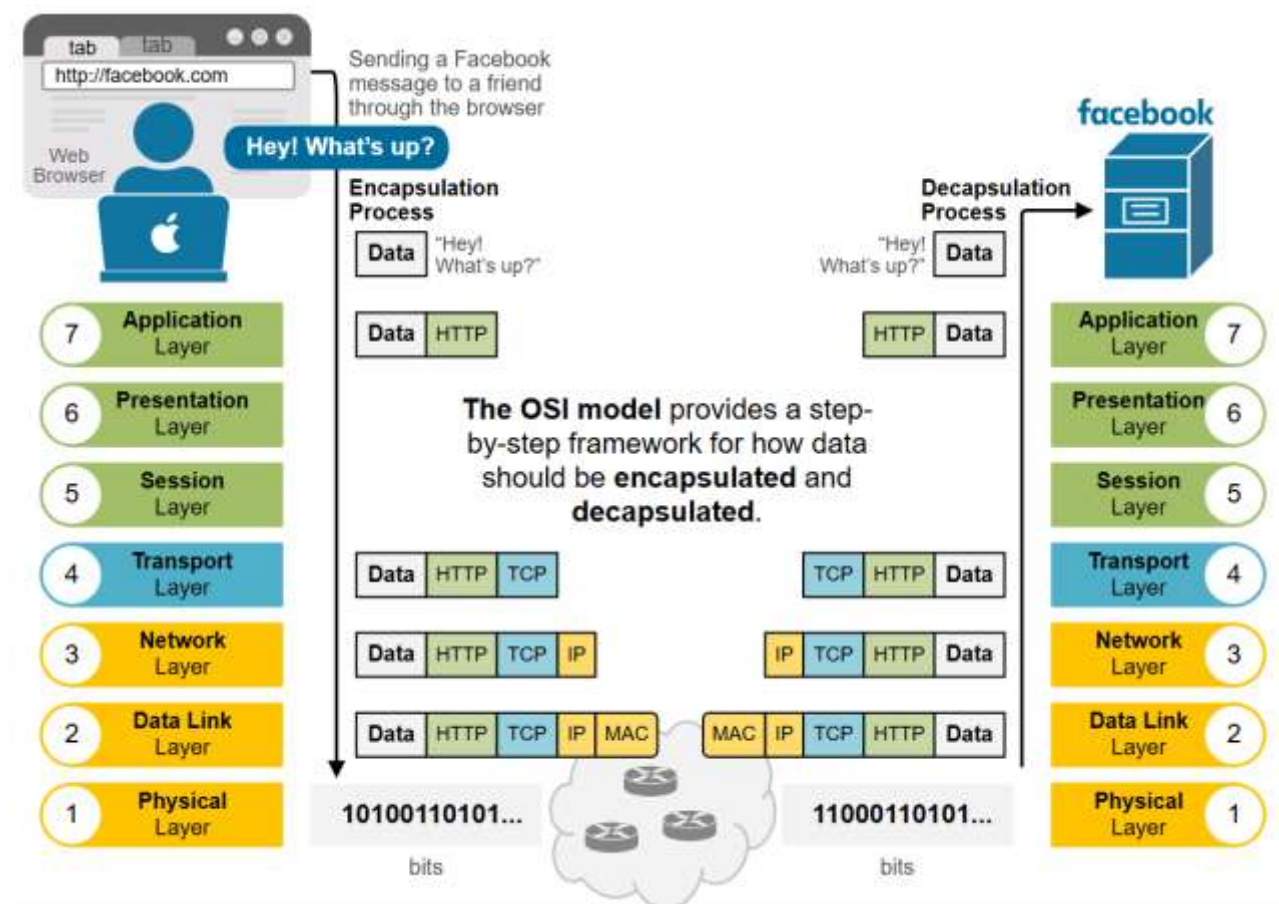


Рисунок 1.6 – Модель OSI

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).

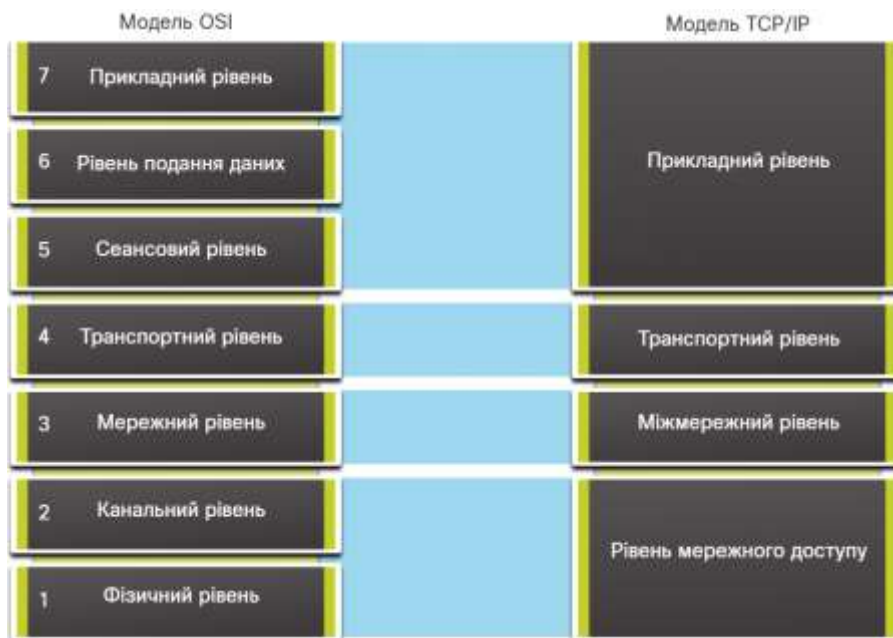


Рисунок 1.7 – Моделі OSI та TCP/IP

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#

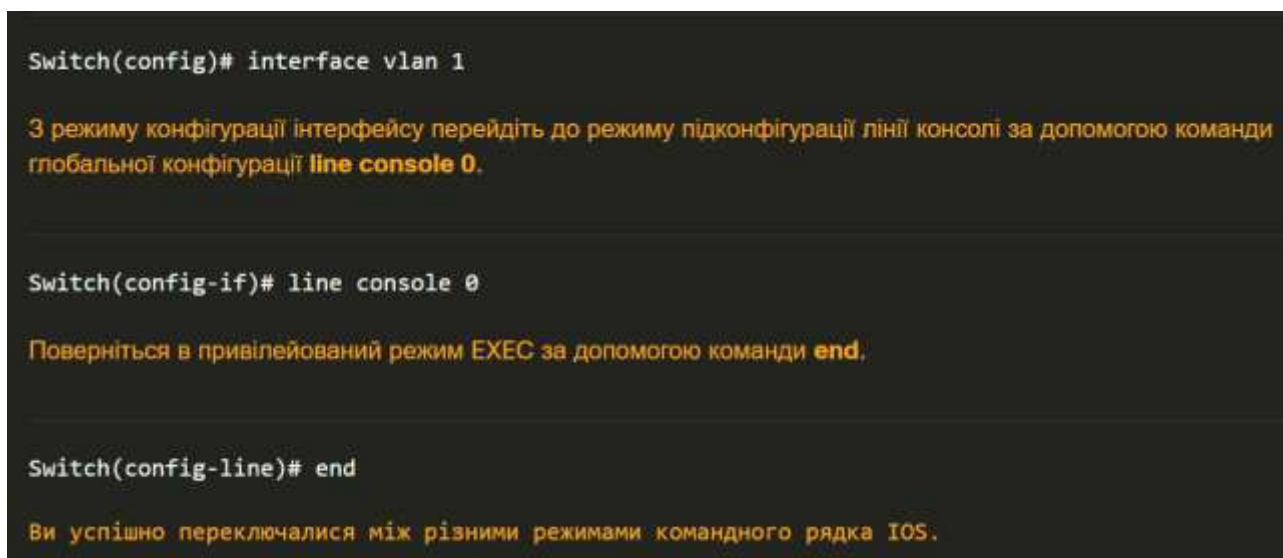
Для переходу між режимами командного рядку використовуються різні команди. Щоб перейти з користувацького режиму EXEC в привілейований, використовується команда `enable`. Для повернення в користувацький режим EXEC використовується команда привілейованого режиму `disable`. Привілейований режим EXEC іноді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

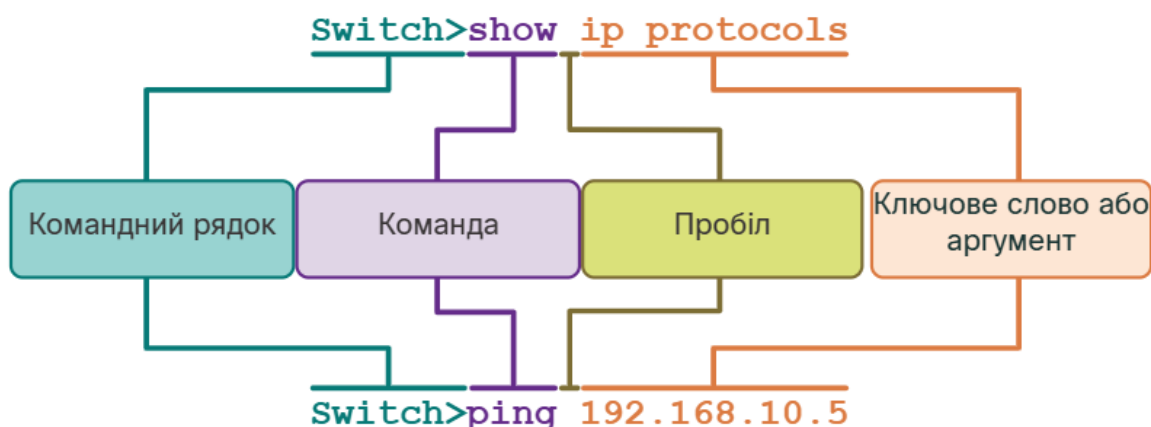


Рисунок 2.2 – Формат команди IOS

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 надсилання 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 ширококомвні пакети рівня MAC. Зазвичай arping спочатку відправляє ширококомвні 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.

Скористайтесь 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 залишаться 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:

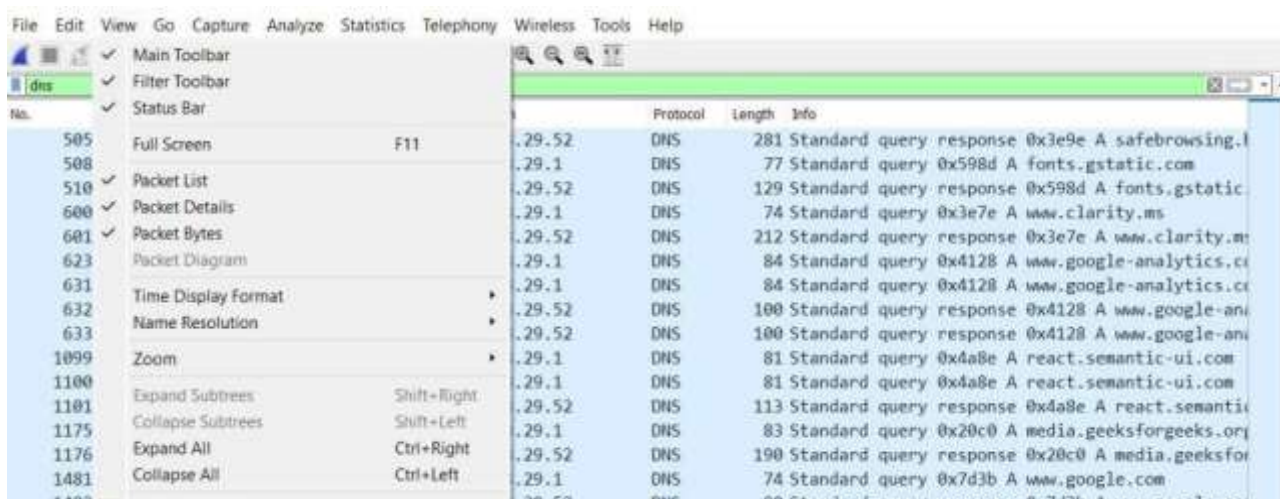


Рисунок 4.1 – Головне вікно програми

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.).

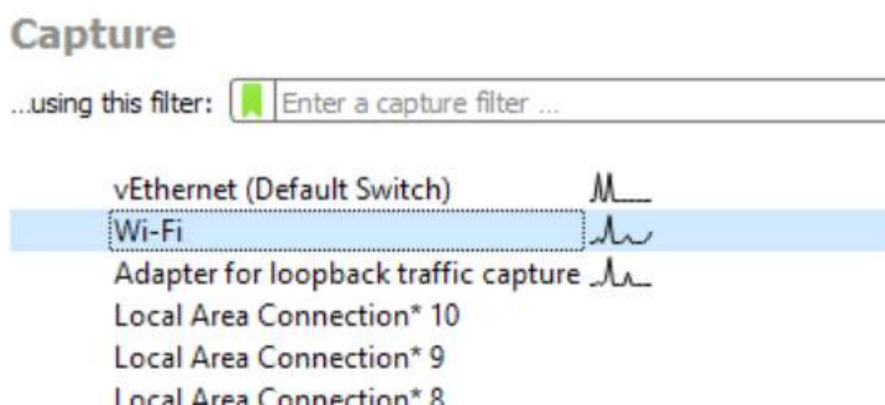


Рисунок 4.2 – Вибір інтерфейсу для аналізу

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.

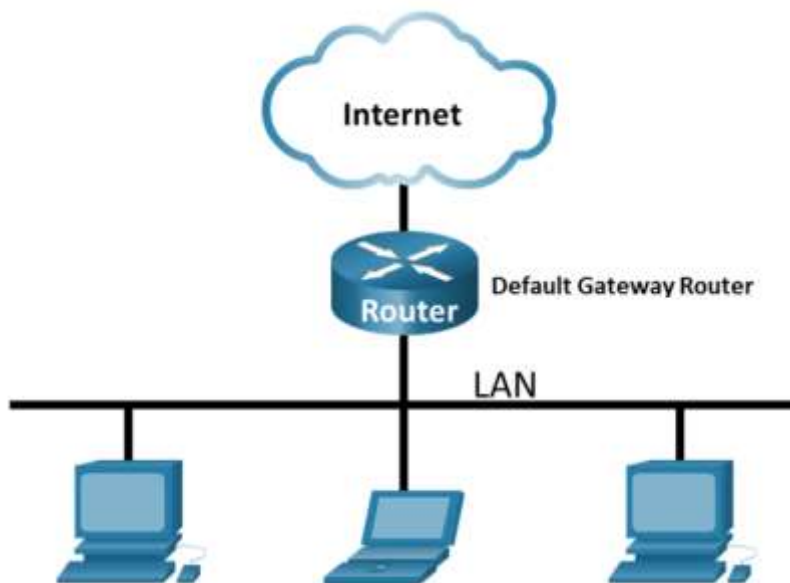


Рисунок 4.3 – Топологія мережі для виконання Завдання 3

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?

КОМП'ЮТЕРНИЙ ПРАКТИКУМ 5

Тема: Базові протоколи та сервіси прикладного та транспортного рівня.

Мета заняття: Ознайомитися з клієнт-серверною взаємодією, UDP і TCP номерами портів та операцій. Прикладний та транспортний рівень. Поняття шлюзу та маршрутизації пакетів.

Теоретичні відомості

Транспортний рівень – це 4-й рівень моделі OSI та 3-й рівень моделі TCP/IP. Його основні функції.

Моніторинг індивідуальних сеансів зв'язку. На транспортному рівні кожен набір даних, що передається між програмою-джерелом і програмою-споживачем, позначається як діалог і обробляється окремо. Цей рівень відповідає за підтримання і відстеження кількох сеансів зв'язку одночасно. Практично в усіх мережах існують обмеження на обсяг даних, що можуть бути передані в рамках одного пакета. Відповідно, дані потрібно розділяти на структури контрольованого розміру.

Сегментація даних і організація порядку доставки сегментів. Транспортний рівень виконує функцію розділення даних програмного забезпечення на блоки визначеного розміру. Залежно від транспортного протоколу ці блоки отримують назву сегментів або дейтаграм. Транспортний рівень забезпечує розподіл інформації на компактні блоки, які є більш керованими та пристосованими для транспортування.

Додавання службової інформації у заголовки. До кожного блоку даних транспортний протокол додає заголовок, що містить ключову службову інформацію, представлену у вигляді двійкових кодів, структурованих у декількох полях. Саме значення цих полів дозволяють різноманітним транспортним протоколам виконувати завдання з управління процесами комунікації. Наприклад, дані заголовка застосовуються вузлом-отримувачем для впорядкування блоків з метою перетворення їх в неперервний потік перед передачею на прикладний рівень. Завдяки цьому транспортний рівень забезпечує

доставку відповідних даних кожній програмі, навіть якщо на пристрої одночасно функціонують кілька додаткових застосунків.

Ідентифікація програмного забезпечення. Важливою функцією транспортного рівня є здатність розділяти діалоги із різними вимогами до передачі даних. Для коректного спрямування потоків інформації до конкретних програм він застосовує механізм ідентифікації за номером порту. Номер порту, показаний на схемі (рисунок 5.1), є унікальним для кожного програмного процесу, що потребує доступу до мережі на конкретному вузлі системи.

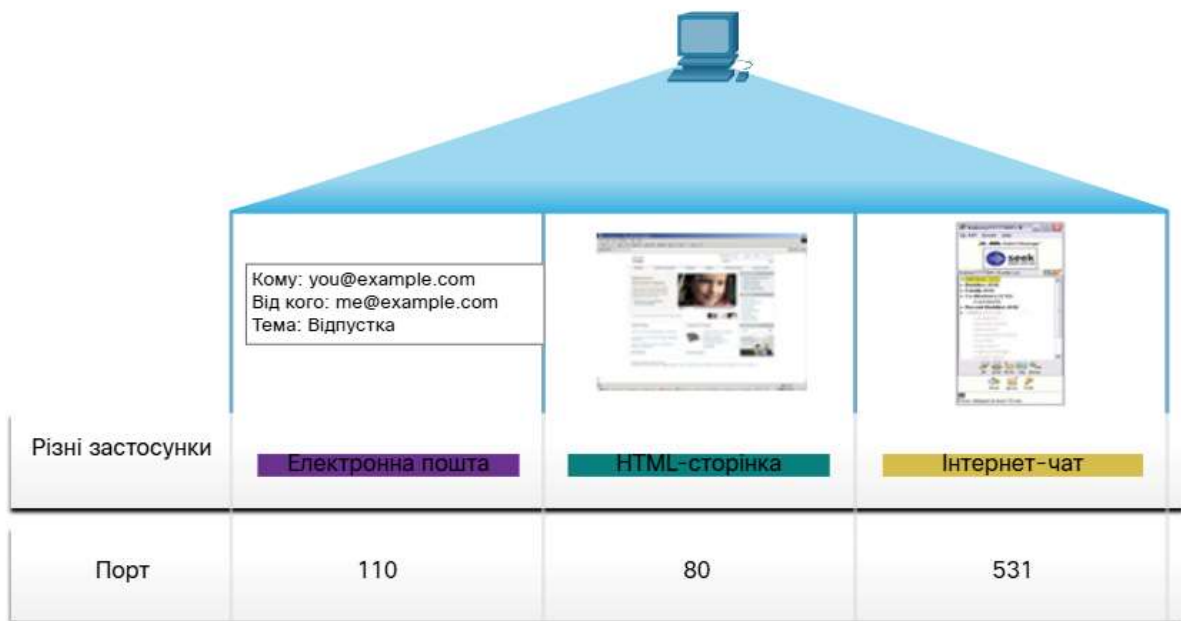


Рисунок 5.1 – Використання портів

Мультиплексування в комунікаційних діалогах відіграє важливу роль у забезпеченні ефективного функціонування мережових взаємодій. Передавання певних видів даних, зокрема потокового відео, у вигляді єдиного безперервного потоку здатне цілковито заповнити доступну пропускну здатність каналу зв'язку. Це, у свою чергу, може спричинити блокування інших паралельно виконуваних процесів передачі даних. Більше того, така організація не лише ускладнює процес відновлення після помилок, але й створює труднощі в реалізації повторної передачі пошкодженої інформації.

Для подолання цих проблем транспортний рівень мережевої моделі застосовує методи сегментації та мультиплексування, як це продемонстровано

на рисунку 5.2. Такі підходи дозволяють поєднувати численні комунікаційні потоки в одній мережі, ефективно розподіляючи ресурси та оптимізуючи їх використання. До того ж, передбачено можливість перевірки сегментів даних на наявність помилок, що забезпечує додатковий рівень надійності під час транспортування, гарантуючи, що інформація залишається незмінною в процесі передачі.

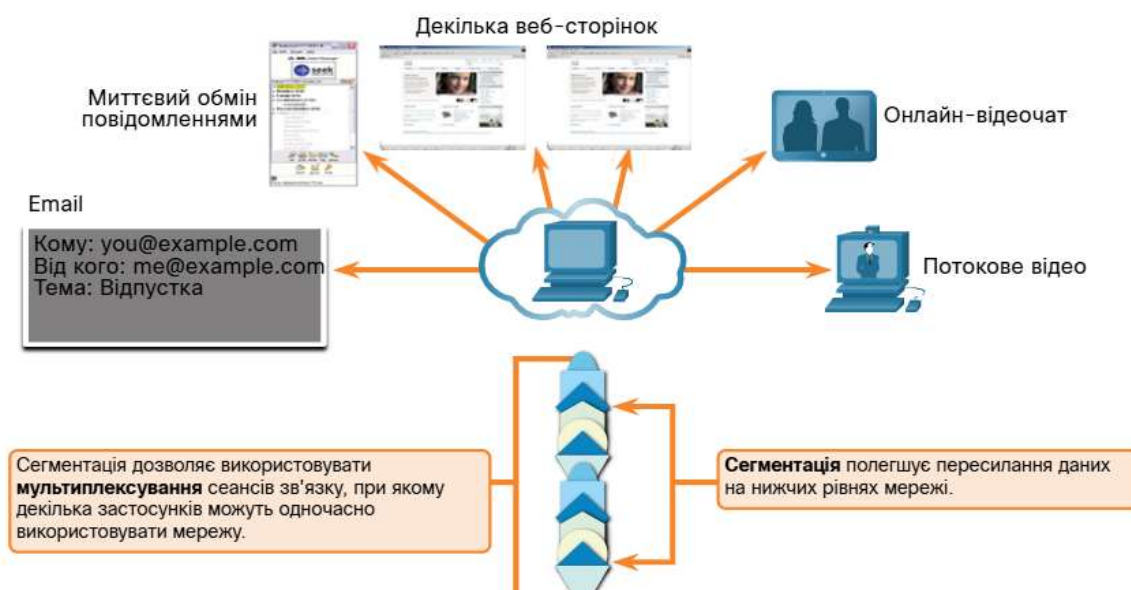


Рисунок 5.2 – Сегментація та мультиплексування на транспортному рівні

Протоколи транспортного рівня визначають спосіб передачі повідомлень між вузлами та відповідають за управління вимогами надійності передачі. На транспортному рівні діють два протоколи – TCP та UDP, що обумовлено різними вимогами щодо надійності послуг транспортного рівня.

Протокол керування передаванням (Transmission Control Protocol, TCP). Цей протокол визнаний надійним і повнофункціональним транспортним протоколом, що забезпечує доставку всіх даних до місця призначення з високим рівнем стабільності та ефективного керування потоком завдяки ключовим механізмам:

- нумерація й моніторинг сегментів даних, переданих певному вузлу з конкретного додатка;
- підтвердження отриманих даних для доведення факту доставки;

- повторна передача даних, які не було підтверджено, через заданий інтервал часу;
- відновлення правильної послідовності сегментів у разі, якщо вони надійшли у неправильному порядку;
- оптимізація швидкості передачі відповідно до спроможностей отримувача.

Окрім підтримки базових функцій, таких як сегментація і забезпечення порядковості передачі, TCP також пропонує розширений набір послуг.

Створення сеансу. TCP є протоколом, орієнтованим на з'єднання, тобто його робота починається з узгодження умов передачі та встановлення стабільного каналу зв'язку (сеансу) між джерелом і отримувачем. Це дозволяє обом сторонам домовитися про обсяг трафіку, який буде передаватися в кожен окремий момент, забезпечуючи максимальний контроль за процесом обміну даними.

Надійна передача. У випадку втрати або пошкодження сегментів під час передачі мережею TCP гарантує їхнє повторне надсилання таким чином, щоб жоден із них не був втрачений у кінцевій точці.

Впорядкована доставка. У мережевому середовищі можуть існувати кілька різних шляхів для пересилання даних, які відрізняються за швидкістю. Це може призводити до того, що сегменти надходять до отримувача у неправильному порядку. Завдяки системі нумерації TCP забезпечує збір даних у їхній правильній послідовності.

Керування потоком. Через обмеженість ресурсів мережевих вузлів (як-от оперативна пам'ять чи обчислювальні можливості), TCP контролює потік даних. Якщо мережевий вузол перевантажений, протокол сигналізує відправнику про необхідність зменшення інтенсивності передачі, тим самим попереджаючи ситуації перевантаження та зайві повторні передачі.

Детальну інформацію про TCP можна знайти у специфікації RFC 793.

Заголовок TCP. TCP – це протокол зі збереженням стану (stateful), який управляє та контролює стан сеансів зв'язку. Для цього TCP реєструє дані,

відправлені раніше, а також отримані для підтвердження передачі інформації. Процес відбувається через двосторонній сеанс, який починається зі встановлення з'єднання для обміну даними і завершується його завершенням.

Під час інкапсуляції даних на прикладному рівні TCP додає до сегмента 20 байтів накладних витрат, що складає 160 бітів. Схематичне зображення полів заголовка TCP представлено на рисунку 5.3.



Рисунку 5.3 – Поля TCP-заголовку

Встановлення з'єднання TCP. Коли пристрій клієнта підключається за протоколом TCP, зв'язок із сервером встановлюється через процес трестороннього рукостискання. Ця процедура дозволяє перевірити, чи доступний вузол призначення для створення з'єднання. Наприклад, як показано на рисунку 5.4, вузол А переконався у доступності вузла В.

Для завершення з'єднання у заголовку сегмента необхідно встановити контрольний біт Finish (FIN) (рисунок 5.5). Процес завершення кожного одностороннього сеансу TCP виконується за допомогою двостороннього рукостискання, яке включає обмін сегментами FIN і підтвердженнями ACK. Таким чином, для завершення одного діалогу, який підтримується TCP, і повного закриття сеансів з обох сторін потрібні чотири обміни. Ініціювати завершення сеансу може як клієнт, так і сервер.

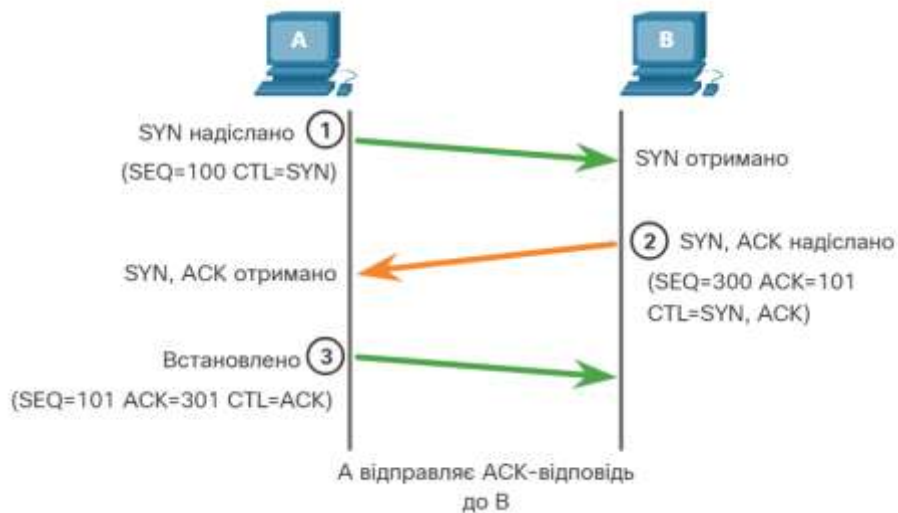


Рисунок 5.4 – Трестороннє рукостискання

У цьому контексті терміни «Клієнт» і «Сервер» використовуються виключно для спрощення. Кожен із двох вузлів, між якими триває відкритий сеанс, здатен розпочати процес завершення.

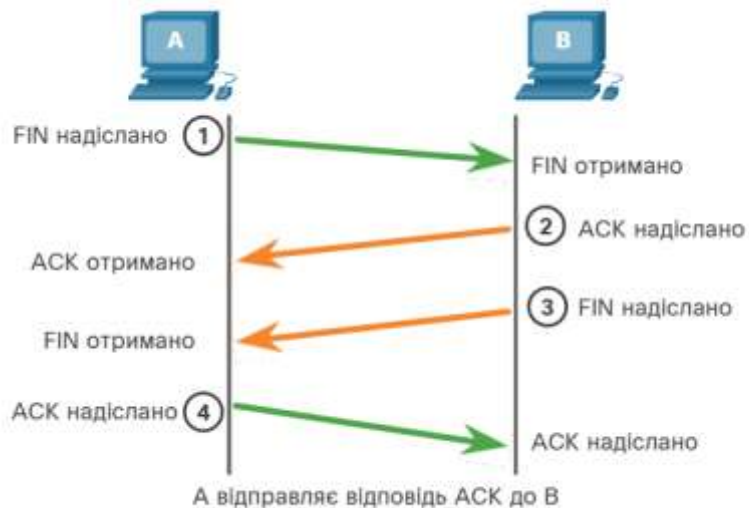


Рисунок 5.5 – Припинення з'єднання

Після завершення підтвердження всіх сегментів, сеанс з'єднання завершується. Протокол TCP є переважним вибором для певних типів застосунків, оскільки, на відміну від UDP, він забезпечує повторне надсилання втрачених пакетів і підтримує їх впорядкування, що гарантує правильну

послідовність доставки даних. Крім того, TCP регулює потік пакетів, запобігаючи перевантаженню пристроїв у мережі.

У практичному використанні нерідко виникають ситуації, коли окремі TCP-сегменти не досягають адресата або доставляються у невірній послідовності. Для того, щоб приймальна сторона могла коректно відновити вихідне повідомлення, необхідно отримати всі передані дані та впорядкувати їх у початковій послідовності. Це забезпечується завдяки вказівці порядкових номерів у заголовку кожного сегмента. Порядковий номер визначає перший байт даних відповідного TCP-сегмента.

З боку отримувача протокол TCP зчитує дані із сегментів та розміщує їх у приймальному буфері. Далі процес передбачає відновлення правильної послідовності сегментів, після чого вони передаються на прикладний рівень для подальшої обробки. Сегменти, які надходять у невідповідній послідовності (з некоректними порядковими номерами), тимчасово зберігаються для подальшої організації. Після отримання всіх відсутніх даних або їхніх фрагментів, протокол формує правильну послідовність сегментів, забезпечуючи цілісність і завершеність повідомлення. (рисунок 5.6.).

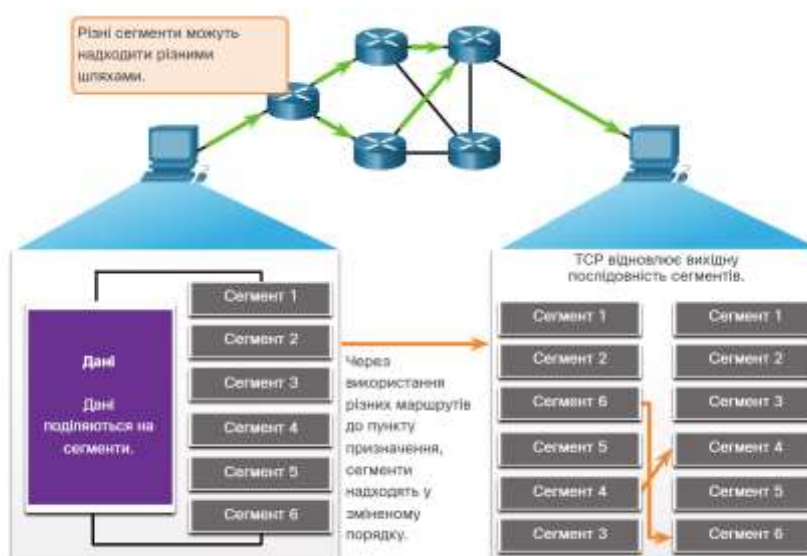


Рисунок 5.6 – Надходження сегментів TCP

Під час встановлення сеансу зв'язку генерується початковий порядковий номер (Initial Sequence Number, ISN), який служить стартовим значенням для

передавання байтів до отримуючого застосунку. У процесі обміну даними в межах одного сеансу цей номер поступово збільшується на величину, що відповідає кількості переданих байтів. Такий механізм нумерації забезпечує точну ідентифікацію та підтвердження кожного сегмента, а також дозволяє виявляти випадки втрати даних. На відміну від простої послідовності з одиниці, ISN є випадково обраним числом, що ефективно мінімізує ризики деяких типів зловмисних атак.

Застосування TCP: веб (HTTP/HTTPS), email (SMTP, IMAP), передача файлів (FTP), SSH

Протокол користувацьких дейтаграм (User Datagram Protocol, UDP).

UDP є транспортним протоколом, який відрізняється простотою в порівнянні з TCP. Основною його особливістю є те, що він не забезпечує надійність передачі даних і контроль потоку, завдяки чому має меншу кількість заголовкових полів. Оскільки UDP не вимагає від відправника та отримувача стеження за надійністю чи потоком даних, обробка UDP-дейтаграм здійснюється більш оперативно, ніж TCP-сегментів. Цей протокол надає базові функції для доставки дейтаграм між застосунками з мінімальними витратами на обробку та перевірку даних. UDP розділяє інформацію на дейтаграми, котрі також часто називають сегментами.

Особливістю UDP є те, що він працює без попереднього встановлення з'єднання. Завдяки цьому немає необхідності в налаштуванні зв'язку перед передачею даних. Крім того, UDP не зберігає стану комунікації між клієнтом і сервером, тому його називають протоколом без стану (stateless). У цьому протоколі немає механізмів, які б повідомляли відправника про успішну доставку даних, що значно спрощує його функціонування.

Роботу UDP можна порівняти зі звичайним поштовим листом без реєстрації. Відправник не отримує підтвердження про те, чи дійшов лист до адресата, а пошта не зобов'язана інформувати про втрату або доставлення листа.

Цей метод передачі даних робить UDP ідеальним вибором для застосунків, де незначна втрата інформації є допустимою, однак будь-які затримки можуть суттєво вплинути на ефективність виконання завдань. Зокрема, протокол широко

використовується в інтеграціях IP-телефонії (VoIP), оскільки дозволяє максимально знизити накладні витрати на мережеву комунікацію. У голосових з'єднаннях повторна передача чи підтвердження отримання даних зменшує швидкість обміну, що суперечить вимогам таких програм.

Основні характеристики UDP:

дані обробляються у порядку їх надходження;

втрачені сегменти повторно не надсилаються;

немає попереднього налаштування сеансу з'єднання;

відправник не інформується про доступність ресурсів з боку одержувача.

Щоб отримати додаткові відомості про UDP, можна скористатися пошуком RFC в інтернеті.

Заголовок UDP. У порівнянні з TCP, заголовок UDP набагато простіший, оскільки містить лише чотири поля і потребує 8 байтів (тобто 64 біти). На рисунку 5.7 показано поля UDP-заголовка.



Рисунок 5.7 – Поля заголовку UDP

Під час передачі UDP-дейтаграм до пункту призначення, як і у випадку з TCP-сегментами, вони можуть слідувати різними маршрутами, через що можуть прибувати в неправильному порядку. Утім, на відміну від TCP, UDP не відстежує порядкові номери сегментів. Як проілюстровано на рисунку 5.8, протокол UDP не забезпечує механізмів для відновлення вихідного порядку дейтаграм, встановленого під час їхнього надсилання.

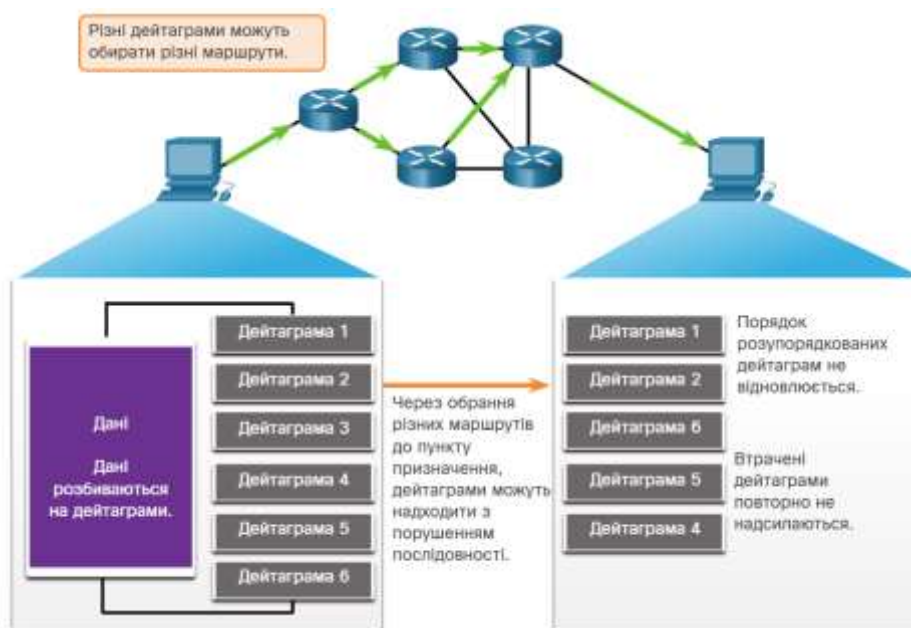


Рисунок 5.8 – Надходження сегментів UDP

Протокол UDP здійснює передачу даних до прикладної програми у хронологічному порядку їх отримання, без гарантування послідовності чи перевірки достовірності. У випадках, коли упорядкування даних є критично важливим для функціонування програми, остання повинна самостійно забезпечити їх правильну послідовність і розробити оптимальні алгоритми обробки.

Щодня через інтернет користувачі взаємодіють з багатьма сервісами, такими як DNS, веб-додатки, електронна пошта, FTP, чати чи VoIP. Використання UDP особливо ефективно у трьох основних категоріях застосунків:

- мультимедійні та відеозастосунки в реальному часі – Ці програми здатні працювати з певними втратами даних, але вимагають мінімальної затримки або її відсутності. До прикладів можна віднести VoIP та потокове відео;

- застосунки типу "запит-відповідь" – Такі програми працюють на основі простих транзакцій, де втрата відповіді на запит не критична. Сюди належать DNS та DHCP;

- додатки, що самостійно забезпечують надійність – Це однонаправлені з'єднання, які не потребують механізмів керування потоком чи перевірки

помилки на транспортному рівні, оскільки за це відповідає сама прикладна програма. Характерними прикладами є протоколи SNMP і TFTP.

UDP також виступає у ролі базового транспортного протоколу для застосунків на базі моделі «запит-відповідь», які надсилають дані невеликими порціями та мають швидкі механізми повторного відправлення. Наприклад, служба доменних імен (DNS) використовує UDP: клієнт надсилає запит серверу DNS для отримання адрес IPv4 або IPv6, а у разі відсутності відповіді протягом заздалегідь визначеного проміжку часу запит просто повторюється.

Однак для прикладних програм, які потребують гарантії доставки та послідовності даних, використовується протокол TCP. Такі програми, як бази даних, веббраузери чи клієнти електронної пошти, залежні від передачі даних у повному обсязі та в початковій послідовності, оскільки будь-яка втрата чи пошкодження інформації можуть зробити її неповною або непридатною для використання. Наприклад, при роботі з високочутливими системами, такими як банківські додатки, критично важливо забезпечити цілісність переданих даних для їх коректного використання.

Таким чином, вибір відповідного транспортного протоколу визначається вимогами конкретного застосунку. Відеоконтент може передаватися і через UDP, і через TCP. Наприклад, збережені аудіо- та відеоматеріали зазвичай передаються через TCP завдяки можливостям буферизації, адаптації до пропускну здатності мережі та управління перевантаженням для забезпечення стабільного користувацького досвіду.

Натомість мультимедійні передачі в реальному часі, такі як відеоконференції чи голосові дзвінки (VoIP), переважно покладаються на UDP з метою мінімізації затримок. Водночас деякі програми можуть використовувати TCP як альтернативний транспортний механізм, наприклад, через обмеження, накладені брандмауерами. Варто зазначити, що програми, які працюють із поточними аудіо- чи відеоматеріалами у записі, переважно застосовують TCP для досягнення кращої якості відтворення.

На рисунку 5.9 підсумовано відмінності між UDP і TCP.

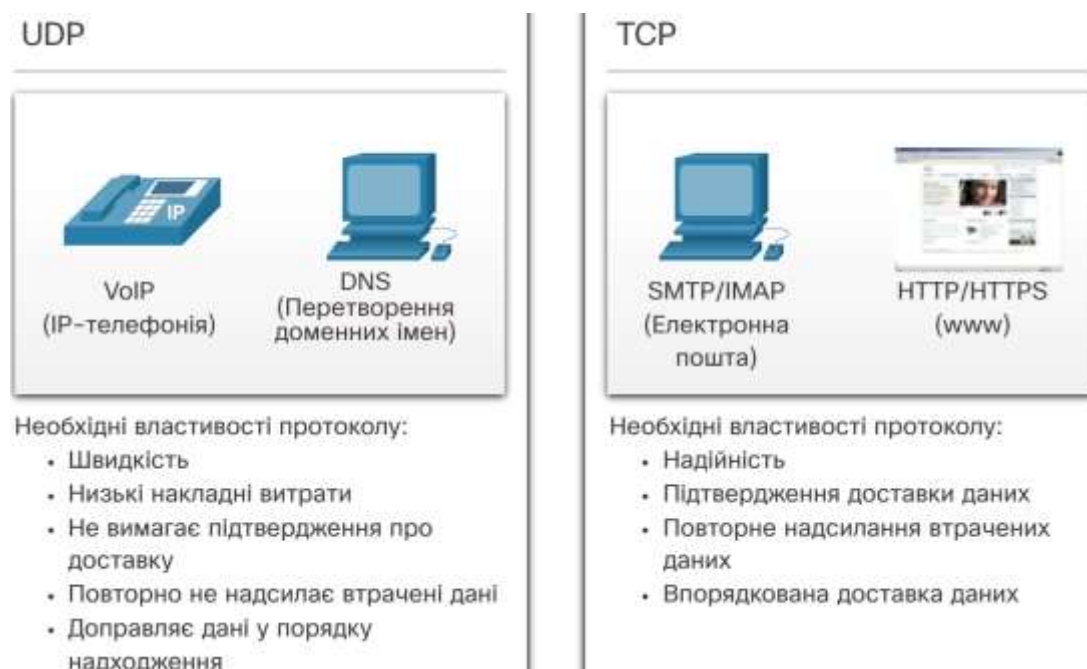


Рисунок 5.9 – Відмінності між UDP і TCP

Порти. Коли повідомлення передаються через TCP чи UDP, запитувані протоколи та служби розпізнаються за допомогою номерів портів, що продемонстровано на схемі. Порт являє собою числовий ідентифікатор, який включається в кожен сегмент даних і дозволяє визначати конкретні зв'язки між клієнтами й серверами. Кожне повідомлення, що надсилається від хоста, містить інформацію про порт джерела та порт призначення.

У комп'ютерних мережах номери портів поділяються на три основні категорії:

1. Добре відомі порти (Well-Known Ports): 0-1023. Ці порти зарезервовані для найпоширеніших системних служб і протоколів. Їх призначення контролюється організацією IANA (Internet Assigned Numbers Authority).

Приклади:

- 20, 21 – FTP (передача файлів)
- 22 – SSH (безпечне підключення)
- 23 – Telnet
- 25 – SMTP (відправка електронної пошти)
- 53 – DNS (система доменних імен)
- 80 – HTTP (веб-трафік)

110 – POP3 (отримання пошти)

143 – IMAP (отримання пошти)

443 – HTTPS (безпечний веб-трафік)

2. Зареєстровані порти (Registered Ports): 1024-49151. Ці порти можуть бути зареєстровані в IANA для конкретних служб, але менш суворо контролюються. Використовуються користувацькими програмами та деякими службами. Приклади:

1433 – Microsoft SQL Server

3306 – MySQL

3389 – Remote Desktop Protocol (RDP)

5432 – PostgreSQL

8080 – Альтернативний HTTP (часто для проксі)

27017 – MongoDB

3. Динамічні або приватні порти охоплюють діапазон від 49152 до 65535. Вони не підлягають реєстрації та застосовуються переважно як тимчасові (ефемерні) порти для клієнтських з'єднань. Їх автоматично призначає операційна система під час ініціації з'єднання додатком. Повний перелік номерів портів та їх відповідностей програмам доступний у реєстрі на офіційному веб-сайті IANA.

Пари сокетів. У сегменті вказуються номери портів джерела та призначення. Після цього ці сегменти інтегруються в IP-пакети, які включають IP-адресу джерела та IP-адресу призначення. Поєднання IP-адреси та номера порту від джерела, або ж адреси і порту призначення, позначають як сокет.

На прикладі, представленому на рисунку 5.10, персональний комп'ютер одночасно здійснює запити до FTP- і веб-служби на сервері призначення.

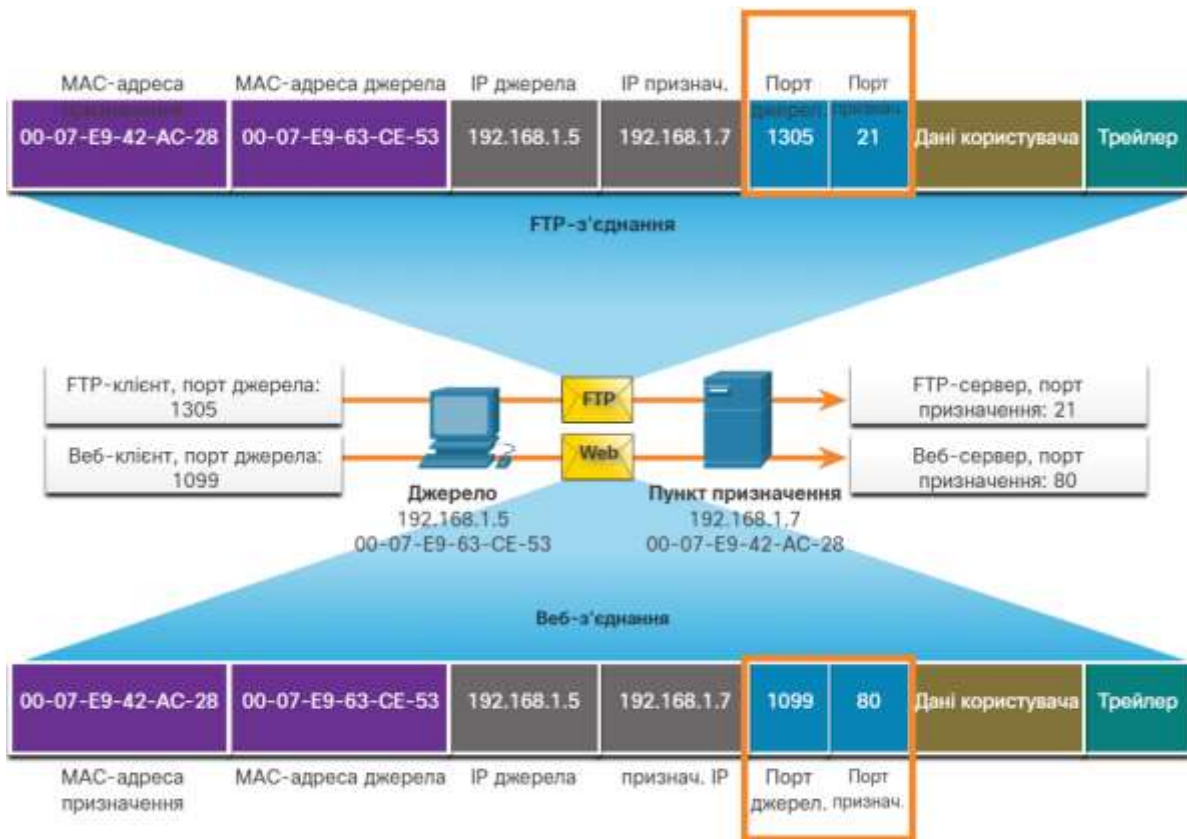


Рисунок 5.10 – Використання портів

У наведеному прикладі FTP-запит, що створюється на комп'ютері, містить MAC-адреси канального рівня (рівень 2) і IP-адреси мережевого рівня (рівень 3). У цьому запиті вказано порт джерела 1305 (динамічно згенерований хостом) і порт призначення, який відповідає FTP-службі — порт 21. Крім того, хост здійснив запит веб-сторінки з сервера, використовуючи ті ж адреси рівнів 2 та 3. При цьому використовується інший порт джерела — 1099 (динамічно обраний хостом), а порт призначення відповідає веб-службі — порт 80.

Сокет застосовується для ідентифікації сервера та його служби за запитом клієнта. Наприклад, клієнтський сокет можна записати як 192.168.1.5:1099, де 1099 позначає порт джерела. Водночас сокет на стороні серверу може виглядати так: 192.168.1.7:80. Разом ці два сокети утворюють сокетну пару: 192.168.1.5:1099 та 192.168.1.7:80.

Сокети дозволяють розмежовувати процеси, які одночасно виконуються на клієнтському комп'ютері, а також забезпечують поділ кількох запитів до єдиного серверного процесу. Номер порту джерела виконує роль зворотної

адреси для застосунку, який відправив запит. Транспортний рівень відстежує цей порт і застосунок, що ініціював запит, щоб правильно скерувати відповідь при її отриманні.

Схожим чином серверні програми, які працюють із UDP, використовують зареєстровані або добре відомі номери портів. Як тільки відповідний процес чи застосунок активовано на сервері, він приймає дані за певним номером порту. У разі отримання дейтаграми, призначеної для такого порту, UDP передає прикладні дані цільовому застосунку, орієнтуючись на номер порту.

Як і у протоколі TCP, взаємодія з використанням UDP починається з ініціативи клієнтського програмного забезпечення, яке здійснює запит до серверного процесу. У цих ситуаціях UDP-клієнт обирає порт джерела динамічно з доступного діапазону та використовує його для передачі даних. Порт отримувача зазвичай є добре відомим чи зареєстрованим номером, що відповідає необхідному серверному процесу.

Після вибору клієнтом портів джерела та призначення вони вказуються у заголовках усіх дейтаграм протягом передачі даних. Коли сервер надсилає відповідь клієнту, номери портів джерела та призначення у заголовку дейтаграми змінюються місцями.

Маршрутизація. Пристрої, які знаходяться за межами локального мережевого сегмента, називають віддаленими хостами. Коли пристрій-джерело передає пакет до віддаленого одержувача, задіюються маршрутизатори, і виконується процес маршрутизації. Маршрутизація передбачає визначення оптимального шляху для передачі пакета до місця призначення.

Маршрутизатор є мережевим пристроєм, який об'єднує кілька IP-мереж третього рівня. На рівні мережевого розподілу маршрутизатори перенаправляють трафік та виконують інші завдання, необхідні для стабільного функціонування мережі. Подібно до комутаторів, маршрутизатори здатні зчитувати та декодувати отримані повідомлення. Однак, на відміну від комутаторів, які здійснюють переадресацію за MAC-адресами рівня 2,

маршрутизатори базуються на IP-адресах третього рівня при прийнятті рішень щодо пересилання даних.

Кожен пакет містить IP-адреси джерела та призначення разом із даними повідомлення, яке необхідно передати між хостами. Маршрутизатор аналізує мережеву частину IP-адреси призначення та обирає найкращу з підключених мереж для подальшої доставки повідомлення до адресата.

Якщо мережеві частини IP-адрес джерела та призначення не збігаються, для передачі повідомлення обов'язково використовується маршрутизатор. Наприклад, якщо хост у мережі 1.1.1.0 бажає надіслати повідомлення до хоста в мережі 4.4.4.0, він перенаправляє повідомлення маршрутизатору. У свою чергу, маршрутизатор приймає повідомлення, розкодовує кадр Ethernet і зчитує IP-адресу призначення в IP-пакеті. Потім він визначає подальший маршрут для передачі даних. Після цього маршрутизатор знову інкапсулює пакет у новий кадр і надсилає його до наступного пункту призначення.

Маршрутизатори забезпечують передачу даних між локальними та віддаленими мережами завдяки таблицям маршрутизації. Ці таблиці не містять адрес окремих хостів, проте зберігають інформацію про доступні мережі та оптимальні шляхи до них. Записи в таблиці маршрутизації можуть створюватися динамічно — на основі даних від інших маршрутизаторів — або вводитися вручну адміністратором мережі. Завдяки цим таблицям маршрутизатор визначає, через який інтерфейс пересилати дані до визначеного місця призначення.

Якщо маршрутизатор не знаходить адресата повідомлення в таблиці маршрутизації, пакет вважається не доставленим і відкидається. Щоб уникнути таких ситуацій, у таблицю додається статичний маршрут за замовчуванням — це шлях, яким маршрутизатор перенаправляє пакети з невідомими адресами мереж призначення. Як правило, цей маршрут веде до іншого маршрутизатора, який може знайти мережу призначення і завершити передачу даних.

Шлюз за замовчуванням. Метод передачі повідомлень, який використовується хостом для зв'язку з пристроєм у віддаленій мережі, суттєво відрізняється від методу, що застосовується для обміну даними в тій самій

локальній мережі (LAN). Коли хост пересилає повідомлення іншому хосту в межах однієї локальної мережі, передача здійснюється безпосередньо. Для цього хост визначає MAC-адресу призначення за допомогою протоколу ARP (Address Resolution Protocol). Після цього IPv4-пакет, що містить адресу призначення, інкапсулюється в Ethernet-кадр, який включає відповідну MAC-адресу як адресу отримувача. Потім цей кадр пересилається в мережу до безпосереднього одержувача.

Коли ж хост намагається надіслати дані до пристрою, розташованого у віддаленій мережі, він залучає маршрутизатор. У цьому випадку хост інкапсулює пакет, залишаючи IP-адресу призначення незмінною, але використовує MAC-адресу маршрутизатора як адресу отримувача кадру. Це дозволяє маршрутизатору отримати кадр і опрацювати його на підставі адресної інформації.

IP-адреса маршрутизатора отримується відповідно до налаштувань шлюзу за замовчуванням. Ця адреса відповідає інтерфейсу маршрутизатора, який підключений до тієї ж локальної мережі, що й хост-надсилач. Усі пристрої в локальній мережі використовують цю адресу шлюзу за замовчуванням для передачі повідомлень до маршрутизатора. Визначивши IP-адресу шлюзу за замовчуванням, хост може за допомогою ARP отримати відповідну MAC-адресу маршрутизатора. Ця MAC-адреса буде використана у кадрі для передачі даних до віддаленої мережі.

Надзвичайно важливо забезпечити належну конфігурацію шлюзу за замовчуванням на кожному хості локальної мережі. Якщо така адреса не налаштована або вказана неправильно, передача даних до пристроїв у віддалених мережах стане неможливою.

У разі, коли в локальній мережі функціонує лише один маршрутизатор, він автоматично стає єдиним шлюзом за замовчуванням. Усі хости й комутатори в цій мережі повинні бути налаштовані відповідним чином. Якщо ж у локальній мережі наявні декілька маршрутизаторів, необхідно обрати один з них для використання як шлюз за замовчуванням. Для забезпечення передачі даних з

кінцевого пристрою вимоги до налаштувань IP-адреси включають правильне визначення адреси шлюзу за замовчуванням. Сам шлюз активується лише при передачі пакетів у напрямку пристроїв, що перебувають у інших мережах. Типово ця адреса є адресою інтерфейсу маршрутизатора, під'єданого до локальної мережі хоста. У такій конфігурації IP-адреси хоста та відповідного інтерфейсу маршрутизатора мають належати до однієї підмережі.

Як приклад розглянемо архітектуру IPv4-мережі, яка складається з маршрутизатора з двома підключеними локальними мережами (рис. 5.11). Інтерфейс G0/0/0 маршрутизатора підключений до мережі 192.168.10.0, у той час як інтерфейс G0/0/1 обслуговує мережу 192.168.11.0. Усі кінцеві пристрої мають налаштовану відповідну адресу шлюзу за замовчуванням, яка співвідноситься з інтерфейсом маршрутизатора.

Наприклад, якщо пристрій PC1 передає пакет на PC2 у межах тієї самої локальної мережі, то шлюз за замовчуванням не буде використовуватися.

Якщо комп'ютер PC1 надішле пакет до комп'ютера PC3 (рисунок 5.12), то PC1 сформує пакет, адресований до IPv4-адреси призначення – PC3. Водночас, маршрутизація здійснюється через шлюз за замовчуванням, який у цьому випадку відповідає інтерфейсу G0/0/0 маршрутизатора R1. Після отримання пакета маршрутизатор R1 аналізує свою таблицю маршрутів, щоб на основі IPv4-адреси призначення встановити, що інтерфейс G0/0/1 є коректною вихідною точкою для подальшої передачі. Маршрутизатор R1 пересилає пакет через вказаний інтерфейс, забезпечуючи доставку даних на PC3.

Комутатор, що забезпечує з'єднання користувацьких комп'ютерів, зазвичай функціонує на Рівні 2 моделі OSI. Для виконання своїх базових функцій комутатору Рівня 2 не потрібно мати IP-адресу. Однак для цілей адміністративного керування можна налаштувати IP-доступ до пристрою, забезпечивши адміністратору можливість віддаленої роботи з комутатором.

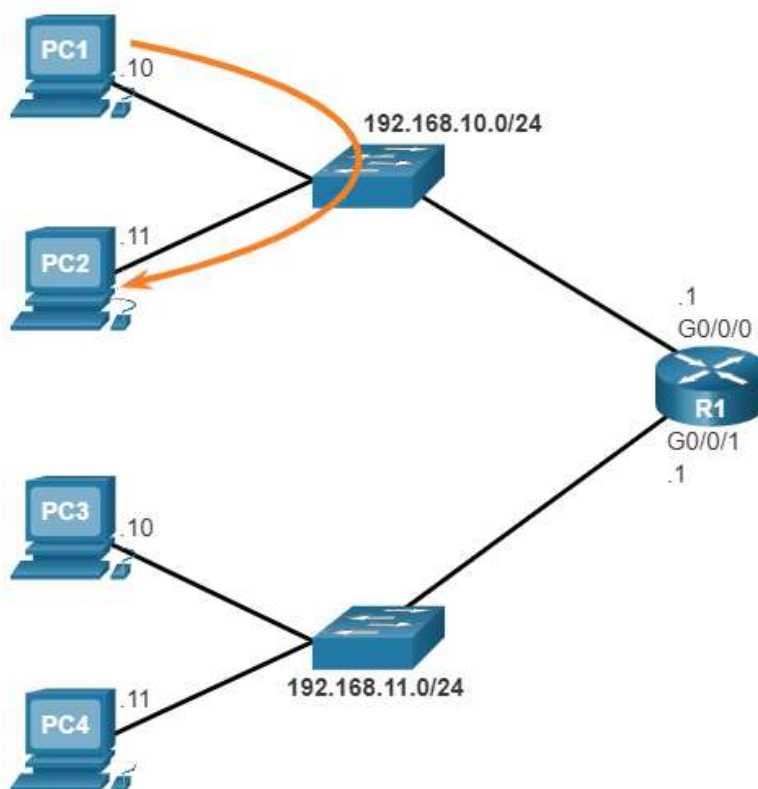


Рисунок 5.11 – Шлюз за замовчуванням

Для організації керування комутатором через локальну IP-мережу необхідно налаштувати його віртуальний інтерфейс (SVI). Конфігурація SVI включає призначення IPv4-адреси та маски підмережі, відповідних параметрам локальної мережі (LAN). Додатково на комутаторі слід зазначити адресу шлюзу за замовчуванням, що забезпечує можливість доступу до комутатора з інших мереж.

Шлюз за замовчуванням вказується на всіх пристроях, які повинні взаємодіяти з мережами за межами своєї локальної підмережі. Для конфігурації IPv4-шлюзу за замовчуванням на комутаторі використовується команда глобального режиму конфігурації `ip default-gateway ip-address`. IP-адреса, яку вводять у команду, повинна відповідати IPv4-адресі інтерфейсу локального маршрутизатора, до якого підключений комутатор (рисунок 5.12).

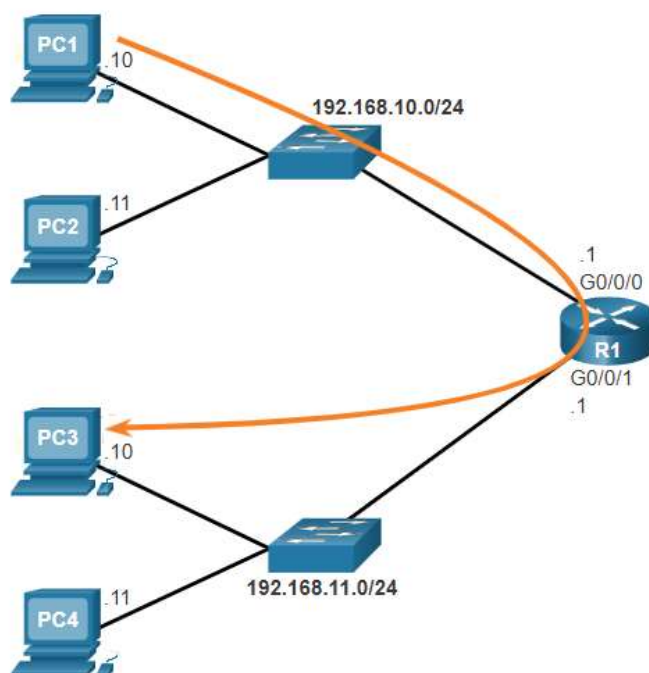


Рисунок 5.12 – Використання шлюзу за замовчуванням

Прикладний рівень (Application Layer) – це сьомий (верхній) рівень моделі OSI та четвертий рівень моделі TCP/IP, основні функції якого включають:

1. Забезпечення взаємодії між користувачем і мережею, що дозволяє додаткам працювати з мережевими службами.
2. Надання мережових сервісів, таких як передача файлів, електронна пошта, перегляд веб-сторінок.
3. Форматування та представлення даних, включаючи кодування, шифрування та стиснення інформації.

Для повного розуміння функцій прикладного рівня важливо враховувати концепцію взаємодії у моделі клієнт-сервер. У такій архітектурі клієнт відповідає за ініціацію запитів і споживання послуг, тоді як сервер виконує функцію обробки запитів та надання необхідних ресурсів чи послуг.

Найпоширеніші сервіси Інтернету, якими постійно користуються користувачі, значною мірою залежать від набору протоколів TCP/IP, що гарантують надійний обмін даними між клієнтами та серверами.

Це основні протоколи прикладного рівня моделі OSI/TCP-IP:

Веб-протоколи:

HTTP (HyperText Transfer Protocol) – передача веб-сторінок, порт 80;

HTTPS (HTTP Secure) – захищена версія HTTP з шифруванням SSL/TLS, порт 443;

WebSocket – двостороння комунікація в реальному часі.

Електронна пошта:

SMTP (Simple Mail Transfer Protocol) – відправка електронної пошти, порт 25, 587;

POP3 (Post Office Protocol v3) – отримання пошти з видаленням з сервера, порт 110;

IMAP (Internet Message Access Protocol) – отримання пошти зі збереженням на сервері, порт 143.

Передача файлів:

FTP (File Transfer Protocol) – передача файлів, порти 20, 21;

SFTP (SSH File Transfer Protocol) – захищена передача файлів через SSH;

TFTP (Trivial File Transfer Protocol) – спрощена передача файлів, порт 69.

Віддалений доступ:

SSH (Secure Shell) – захищений віддалений доступ до терміналу, порт 22;

Telnet – незахищений віддалений доступ, порт 23;

RDP (Remote Desktop Protocol) – віддалений робочий стіл Windows, порт 3389;

VNC (Virtual Network Computing) – віддалений доступ до робочого столу.

Служби імен і адресації:

DNS (Domain Name System) – перетворення доменних імен в IP-адреси, порт 53;

DHCP (Dynamic Host Configuration Protocol) – автоматичне призначення IP-адрес, порти 67, 68;

Обмін даними:

SMB/CIFS (Server Message Block) – спільний доступ до файлів і принтерів у Windows;

NFS (Network File System) – спільний доступ до файлів у Unix/Linux;

LDAP (Lightweight Directory Access Protocol) – доступ до каталогів, порт 389.

Мультимедіа:

RTP/RTSP (Real-time Transport Protocol/Real Time Streaming Protocol) – потокове відео/аудіо;

SIP (Session Initiation Protocol) – VoIP-телефонія.

Управління мережею:

SNMP (Simple Network Management Protocol) – моніторинг мережевого обладнання, порти 161, 162;

NTP (Network Time Protocol) – синхронізація часу, порт 123.

Інші важливі протоколи:

MQTT – протокол для IoT-пристроїв;

CoAP – протокол для обмежених пристроїв;

gRPC – високопродуктивний RPC-фреймворк;

GraphQL – мова запитів для API.

Поняття URI. Веб-ресурси та веб-сервіси визначаються через Уніфікований ідентифікатор ресурсу (URI), який являє собою послідовність символів, що служить для ідентифікації конкретного мережного ресурсу. URI поділяється на два види:

Уніфікована назва ресурсу (URN) призначена для визначення лише простору імен ресурсу, такого як веб-сторінка, документ чи зображення, без вказання протоколу доступу.

Уніфікована адреса ресурсу (URL) використовується для встановлення мережного розташування конкретного об'єкта в онлайн-просторі. Найпоширенішими для роботи в браузері є URL-адреси з протоколами HTTP або HTTPS. Проте існують й інші варіанти, наприклад FTP, SFTP, SSH тощо. Зокрема, URL на основі SFTP може бути представленим у форматі `sftp://sftp.example.com`.

Розглянемо детально, як структурні елементи містить URL на прикладі `https://www.example.com/author/book.html/#page155`:

– протокол або схема – це вказівка на спосіб передачі даних, наприклад HTTPS або інші варіанти протоколів, як FTP, SFTP, mailto чи NNTP;

– назва вузла – це доменне ім'я сервера, в наведеному випадку: `www.example.com`;

– шлях та ім'я файлу – інформація про місцезнаходження ресурсу на сервері: `/author/book.html`;

фрагмент – це додаткова частина для точного визначення певного місця або параметру у файлі: `#page155`.

Розглянемо більш детально де-які протоколи прикладного рівня.

DNS (Domain Name System). Його головне завдання полягає в тому, щоб перетворювати зрозумілі для людей доменні імена (наприклад, `google.com`) у IP-адреси (наприклад, `142.250.185.78`), які комп'ютери використовують для зв'язку між собою. Для роботи застосовуються такі порти: порт 53 UDP – для стандартних DNS-запитів (швидкі та короткі запити), і порт 53 TCP – для обробки великих відповідей (понад 512 байт) або зональних передач.

Ієрархія DNS:

1. Кореневі сервери (Root servers) – 13 груп серверів верхнього рівня
2. TLD сервери (Top-Level Domain) – `.com`, `.org`, `.ua` тощо
3. Авторитетні сервери – зберігають записи для конкретних доменів
4. Рекурсивні резолвери – виконують запити від імені клієнтів

Приклад роботи DNS

1. Користувач вводить: `www.example.com`
2. Запит до локального DNS-резолвера
3. Якщо немає в кеші → запит до кореневого сервера
4. Кореневий сервер → TLD сервер (`.com`)
5. TLD сервер → авторитетний сервер `example.com`
6. Авторитетний сервер повертає IP-адресу
7. Користувач отримує IP і підключається до сайту

До популярних публічних DNS-серверів віднесено: Google: 8.8.8.8, 8.8.4.4, Cloudflare: 1.1.1.1, 1.0.0.1, Quad9: 9.9.9.9

DNS є критично важливою інфраструктурою інтернету, бо без нього довелось б запам'ятовувати IP-адреси всіх сайтів.

Протокол динамічного налаштування вузла Протокол динамічної конфігурації вузлів (Dynamic Host Configuration Protocol, DHCP) для IPv4 забезпечує автоматизацію процесу надання вузлам мережі IPv4-адрес, масок підмереж, шлюзів та інших ключових параметрів мережі. Цей підхід, відомий як динамічна адресація, є протиположним до статичного налаштування мережевих параметрів, яке передбачає ручне введення IP-адрес адміністратором для кожного мережного вузла.

У випадку динамічної адресації, під час підключення до мережі вузол надсилає запит до DHCP-сервера. Сервер вибирає адресу з попередньо визначеного пулу доступних адрес і надає її вузлу на умовах оренди. Такий режим функціонування особливо ефективний для великих мереж або мереж зі змінною кількістю користувачів, оскільки дозволяє оперативно і автоматично забезпечувати нові пристрої або користувачів необхідними IP-адресами.

Однією з важливих характеристик DHCP є можливість налаштування тривалості IP-адреси. Після завершення орендного періоду або отримання сервером спеціального повідомлення від клієнта адреса повертається у пул для повторного використання. Це забезпечує гнучкість та спрощує переміщення користувачів між різними частинами мережі, сприяючи безперешкодному відновленню мережного з'єднання.

У середніх та великих мережах функції DHCP зазвичай виконує локальний сервер на базі виділеного ПК. Важливо зазначити, що багато мереж комбінують використання DHCP та статичної адресації. Наприклад, DHCP звично застосовується для кінцевих користувальницьких пристроїв (ПК, смартфонів тощо), тоді як статична адресація зарезервована для ключових мережних елементів, таких як маршрутизатори-шлюзи, комутатори, сервери чи принтери.

Для відповідності сучасним вимогам також існує версія протоколу DHCP для IPv6—DHCPv6. Хоча вона виконує близькі функції з налаштування параметрів мережного підключення, є суттєва відмінність: DHCPv6 не надає інформацію про шлюз за замовчуванням. Отримання цієї інформації відбувається виключно за допомогою динамічних анонсів маршрутизатора (Router Advertisement, RA), що є власною особливістю IPv6-мереж.

Протокол HTTP (HyperText Transfer Protocol) – це прикладний протокол, призначений для передачі гіпертекстових документів, таких як HTML, зображення, відео тощо, у мережі Інтернет. За замовчуванням працює через порт 80 і функціонує на основі TCP, забезпечуючи надійне з'єднання.

Коли веб-клієнт отримує IP-адресу веб-сервера, браузер користувача використовує цю адресу та порт 80 для створення запиту до веб-служб. Запит відправляється серверу через протокол передачі гіпертекстових даних (HTTP). У свою чергу, сервер, отримуючи запит на порт 80, відповідає клієнту, надаючи йому доступ до веб-сторінки. Вміст веб-сторінки кодується за допомогою спеціальних мов розмітки. Найпоширенішою серед них є мова розмітки HTML, яка визначає, як браузер має формувати сторінку, які графічні елементи або шрифти використовувати.

Протокол HTTP не забезпечує захищеного обміну даними, тому інформацію, яка передається мережею, легко можуть перехопити сторонні особи. Для досягнення більшого рівня безпеки HTTP інтегрується із захищеними транспортними протоколами. У цьому випадку запити надсилаються через порт 443 із використанням HTTPS у адресі сайту замість HTTP.

Інтернет підтримує різноманітні веб-сервери та клієнтські додатки, розроблені різними виробниками. Завдяки стандартам HTTP і HTML ці сервери та клієнти ефективно взаємодіють незалежно від їх походження чи технічних особливостей.

Протокол передавання файлів (FTP) FTP пропонує зручний механізм для передавання файлів між комп'ютерами. Клієнтське програмне забезпечення,

запущене на одному пристрої, може підключатися до FTP-сервера, виконуючи різноманітні дії з файлами, серед яких завантаження та вивантаження інформації.

FTP-сервер забезпечує передавання файлів між різними пристроями та дозволяє дистанційно керувати файлами, наприклад, видаляти чи перейменовувати їх, надсилаючи відповідні команди. Для взаємодії між клієнтом і сервером FTP застосовує два окремі порти. Порт 21 протоколу TCP використовується для встановлення керуючого з'єднання, щоб ініціювати сесію. Після цього для передачі даних сервер задіює порт 20 протоколу TCP.

Сучасні операційні системи та більшість браузерів мають вбудовані FTP-клієнти. Водночас існують спеціалізовані FTP-клієнти з розширеними можливостями, які пропонують графічний інтерфейс для більш зручного керування файлами.

Telnet (Telecommunication Network) – це протокол мережевого рівня прикладного рівня, створений для віддаленого доступу до комп'ютера через командний рядок. Сервери Telnet працюють через TCP-порт 23, приймаючи клієнтські запити. При встановленні з'єднання утворюється сеанс, який часто називають з'єднанням віртуального терміналу (vty). Замість підключення фізичного пристрою Telnet використовує програмне забезпечення для створення віртуального терміналу, що надає ті ж можливості, як і звичайний сеанс з доступом до командного інтерфейсу сервера (CLI).

Варто зазначити, що Telnet не вважається безпечним протоколом. У більшості сучасних середовищ рекомендується використовувати SSH як більш захищену альтернативу. Коли з'єднання Telnet встановлено, користувачі отримують можливість виконувати всі дозволені дії на сервері, наче вони працюють безпосередньо через командний рядок самого пристрою. При наявності відповідних прав можна запускати або зупиняти процеси, змінювати конфігурації пристроїв і навіть вимикати систему.

Однак Telnet має суттєвий недолік — він не підтримує шифрування даних. Хоча система може запитувати логін та пароль, всі передані під час сеансу

відомості пересилаються в мережі у відкритому текстовому форматі. Це створює серйозну вразливість, адже такі дані легко перехопити та прочитати.

Протокол безпечної оболонки (Secure Shell, SSH) пропонує альтернативний та безпечний спосіб доступу до сервера. SSH надає структуру для безпечного віддаленого входу та інших захищених мережних служб. SSH забезпечує надійнішу автентифікацію, ніж Telnet, і підтримує сеанс передавання даних з використанням шифрування. Як найкраща практика, мережні фахівці завжди повинні використовувати SSH замість Telnet, коли це можливо.

Простий протокол передавання електронної пошти (SMTP) використовується клієнтом електронної пошти для надсилання повідомлень на локальний сервер електронної пошти. Тоді локальний сервер вирішує, чи повідомлення призначене для локальної поштової скриньки чи воно адресоване поштової скриньці на іншому сервері.

SMTP також використовується між двома серверами, якщо один сервер повинен відправити повідомлення на інший сервер. SMTP-запити надсилаються до порту 25.

Протокол поштового зв'язку (POP3). Сервер, який підтримує клієнтів POP, отримує та зберігає повідомлення, адресовані своїм користувачам. Коли клієнт приєднується до сервера електронної пошти, повідомлення завантажуються клієнту. За замовчуванням повідомлення не зберігаються на сервері після того, як клієнт отримав доступ до них. Клієнти звертаються до серверів POP3 через порт 110.

Протокол доступу до інтернет-повідомлень (IMAP). Сервер, який підтримує клієнтів IMAP, також отримує та зберігає повідомлення, адресовані своїм користувачам. Однак, на відміну від POP, IMAP зберігає повідомлення в поштових скриньках на сервері, якщо вони не видалені користувачем. Найновішою версією IMAP є IMAP4, яка прослуховує клієнтські запити на порт 143.

Виконання комп'ютерного практикуму

Завдання 1. Відкрити файл Завдання 1_LP5.pka. Треба створити мережевий трафік в режимі моделювання та вивчити функціональності протоколів TCP і UDP.

1. Створення трафіку для заповнення таблиці протоколу визначення адрес (ARP):

- натисніть на MultiServer, оберіть вкладку робочого стола Desktop і перейдіть до режиму командного рядка Command Prompt;

- введіть команду `ping -n 1 192.168.1.255`. Це звернення за широкою адресою клієнтської локальної мережі. Згідно з налаштуваннями команда надсилатиме лише один запит ping, замість звичних чотирьох. За кілька секунд кожен пристрій у мережі відповість на це звернення від MultiServer.

Закрити вікно MultiServer.

2. Створити веб-трафік (HTTP). Для цього:

- перейдіть до режиму моделювання (Simulation mode);
- клацніть на HTTP Client і на робочому столі відкрийте Web Browser;
- у полі URL введіть 192.168.1.254 і натисніть Go. У вікні топології з'являться конверти (PDU).

Згорніть, але не закривайте вікно налаштування HTTP Client.

3. Створити FTP-трафік. Для цього:

- натисніть на FTP Client і відкрийте Command Prompt на робочому столі;
- введіть команду `ftp 192.168.1.254`. У вікні моделювання з'являться відповідні PDU;

- згорніть, але не закривайте вікно налаштування FTP Client.

4. Створити DNS-трафік. Для цього:

- клацніть на DNS Client і відкрийте Command Prompt;
- введіть команду `nslookup multiserver.pt.ptu`. У вікні моделювання з'являться PDU;

- згорніть, але не закривайте вікно налаштування DNS Client.

5. Створити трафік електронної пошти. Для цього:

– натисніть на E-Mail Client і відкрийте інструмент E-Mail на робочому столі;

– натисніть Compose і введіть таку інформацію:

1) To: user@multiserver.pt.ptu

2) Subject: вкажіть тему на власний розсуд

3) E-Mail Body: введіть свій текст Email-повідомлення.

– натисніть Send;

– згорніть, але не закривайте вікно налаштування E-Mail Client.

6. Підтвердити створення трафіку і його готовності до моделювання.

На панелі моделювання повинні з'явитися PDU для кожного з клієнтських комп'ютерів.

7. Вивчити мультиплексування при передаванні трафіку мережею.

Скористайтесь кнопкою Caps/Forward на панелі моделювання для дослідження протоколів, залучених до мережної взаємодії. (Кнопка Caps/Forward '>| ' – це маленька стрілка, що вказує праворуч, з вертикальною рисою поруч).

Один раз натисніть кнопку Capture/Forward. Усі PDU прямують до комутатора.

Натисніть кнопку Capture/Forward шість разів і перегляньте, як PDUs від різних вузлів ширяться мережею. Зверніть увагу, що у заданий момент часу лише одна протокольна одиниця даних може перетинати канал у кожному напрямку.

Завдання 2. Відкрити файл Завдання 2_LP5.pka. Здійснити спостереження за клієнтською взаємодією між сервером і ПК.

1. Перейти до режиму моделювання. Для цього клацніть Simulation Mode, щоб увійти в режим моделювання. Піктограма режиму симуляції знаходиться в правому нижньому куті логічної робочої області.

2. Встановити фільтри списку подій. Для цього:

У розділі Event List Filters натисніть Show All/None, щоб зняти всі прапорці.

Натисніть Edit Filters. На вкладці IPv4 виберіть DNS. На вкладці Різне виберіть HTTP. Після завершення закрийте вікно. Event List Filters показують DNS та HTTP як єдині видимі події.

3. Здійснити запит веб-сторінки з ПК. Для цього

Клацніть PC. Виберіть вкладку Desktop і натисніть на Web Browser.

Відкриється змодельований веб-браузер. Введіть `www.example.com` у поле URL та натисніть кнопку Go, розташовану праворуч. Мінімізуйте вікно ПК.

4. Запустити моделювання. Для цього:

У розділі Play Controls на панелі Simulation Panel, натисніть Play. Обмін між ПК та сервером анімований, а події додаються до Event List.

Коли буфер буде заповнений, клацніть View Previous Event для продовження.

5. Отримати доступ до певного PDU. Для цього

Відновіть змодельоване вікно ПК. Зверніть увагу, що у веб-браузері відображається веб-сторінка. Мінімізуйте змодельоване вікно браузера.

У розділі Simulation Panel Event List останній стовпець містить кольорове поле, яке забезпечує доступ до детальної інформації про подію. Клацніть кольорове поле в першому рядку для першої події. Відкриється вікно PDU Information.

6. Перевірити вміст інформаційного вікна PDU. Перша вкладка інформаційного вікна PDU містить інформацію про вхідний та/або вихідний PDU, що стосується моделі OSI. Натисніть Next Layer >> кілька разів, щоб переходити між вхідними та вихідними рівнями та читати опис у полі під рівнями для отримання інформації про те, як працює обмін.

Перевірте інформацію PDU щодо інших подій, щоб отримати огляд всього процесу обміну.

Завдання 3. Відкрити файл Завдання 3_ЛР5.pka. Переглянути трафік клієнта або сервера, відправленого з ПК на веб-сервер при запиті до веб-служб.

1. Перевірити з'єднання з веб-сервером. Для цього

Натисніть External Client і отримайте доступ до Command Prompt з вкладки Desktop.

Використайте команду ping, щоб отримати URL-адресу ciscolearn.web.com.

```
PC> ping ciscolearn.web.com
```

Зверніть увагу на IP-адресу, що міститься у результаті виконання команди ping. Ця адреса отримана з DNS-сервера та перетворена з доменного імені ciscolearn.web.com. Весь трафік, що пересилається мережею, використовує інформацію про IP-адреси джерела та призначення.

Закрийте вікно командного рядка, однак вікно робочого стола External Client залиште відкритим.

2. Під'єднатися до веб-сервера. Для цього

У вікні робочого столу відкрийте вікно Web Browser.

У рядку URL-адреса, введіть ciscolearn.web.com. Обов'язково прочитайте веб-сторінку, що відображається. Залиште цю сторінку відкритою.

Згорніть вікно External Client, але не закривайте його.

3. Переглянути HTML-код. Для цього

Натисніть сервер ciscolearn.web.com з логічної топології.

Відкрийте вкладку Services > HTTP. Далі поруч з файлом index.html натисніть кнопку (edit).

Порівняйте код розмітки HTML на сервері, який створює сторінку відображення веб-браузера на External Client. Може виникнути потреба повторно розгорнути вікно External Client, якщо воно згорнулось при відкритті вікна сервера.

Закрийте вікна External Client та веб-сервера.

4. Оглянути трафік між клієнтом та веб-сервером. Для цього:

Увійдіть в режим моделювання, натиснувши вкладку Simulation в правому нижньому кутку.

Двічі натисніть Simulation Panel, щоб відкріпити її від вікна Packet Tracer. Це дозволить переміщати Simulation Panel для перегляду всієї мережної топології.

Перегляньте трафік шляхом створення блоку Complex PDU в режимі Simulation.

1) На Simulation Panel, оберіть Edit Filters.

2) Натисніть вкладку Misc, щоб переконатися, що обрані тільки поля для TCP та HTTP.

3) Додайте блок Complex PDU, натиснувши значок відкритого конверту, який розташований над значком режиму Simulation.

4) Натисніть External Client, щоб вказати його як джерело. З'явиться вікно Create Complex PDU.

Вкажіть налаштування створення Complex PDU шляхом зміни наступних параметрів у вікні Complex PDU.

1) У розділі PDU Settings для параметра Select Application має бути встановлено значення HTTP.

2) Виберіть сервер ciscolearn.web.com, щоб вказати його як пристрій призначення. Зверніть увагу, що IP-адреса веб-серверу з'явиться в полі призначення у вікні Complex PDU.

3) У полі Starting Source Port введіть 1000.

4) У розділі Simulation Settings оберіть Periodic Interval 120 секунд.

Створіть PDU, натиснувши кнопку Create PDU у вікні Create Complex PDU.

1) Спостерігайте за потоком трафіку, натиснувши кнопку Play на Simulation Panel. Прискорте анімацію за допомогою повзунка управління відтворенням.

Коли з'явиться вікно Buffer Full, натисніть View Previous Events, щоб закрити вікно.

2) Прокрутіть список подій. Зверніть увагу на кількість пакетів, які передані від джерела до адресата. HTTP – це протокол TCP, який вимагає встановлення з'єднання і підтвердження отримання пакетів, що значно підвищує об'єм трафіку.

Завдання 4. Вивчити перетворення URL-адреси на IP-адресу за допомогою протоколу DNS. Для цього:

1. Відкрийте вікно командного рядка Windows.

2. У командному рядку виконайте ping URL-адреси інтернет-корпорації з призначення імен і номерів (ICANN) за адресою www.icann.org. ICANN координує DNS, IP-адреси, системи керування доменними іменами верхнього рівня та функції керування кореневими серверами. Комп'ютеру потрібно перетворити www.icann.org на IP-адресу, щоб знати, куди надсилати пакети міжмережевого протоколу керуючих повідомлень (Internet Control Message Protocol, ICMP).

Перший рядок виводу відображає виконане за допомогою DNS перетворення www.icann.org на IP-адресу. Результат роботи DNS повинен бути доступний для перегляду, навіть якщо у вашому закладі використовується міжмережний екран, який запобігає пінгуванню, або якщо сервер призначення забороняє звертатися за допомогою ping до свого веб-сервера.

Якщо ім'я домену перетворюється на адресу IPv6, використовуйте команду ping -4 www.icann.org для отримання IPv4-адреси, якщо потрібно.

```
C: > ping www.icann.org
```

```
C:> ping -4 www.icann.org
```

Запишіть IP-адреси для www.icann.org. Закрийте вікно командного рядка.

Замість URL-адреси використайте для звернення у веб-браузері записану адресу IPv4. Введіть <https://192.0.32.7> у веб-браузері. Якщо вдалося отримати IPv6-адресу, її також можна застосувати: [https://\[2620:0:2d0:200::7\]](https://[2620:0:2d0:200::7]).

Завдання 5. Відкрити файл Завдання 5_ЛР5.pka. Виправити неполадки зі шлюзом за замовчуванням. Для цього:

1. Перевірити мережеву документацію та усунути проблеми. В таблиці адресації відсутні деякі дані. Заповнюємо таблицю адресації, вказавши відсутні дані шлюзу за замовчуванням для комутаторів та комп'ютерів.
2. Перевіряємо підключення до пристроїв, що належать до однієї мережі.
3. Перевіряємо підключення до віддалених пристроїв та задокументуємо усі проблеми.
4. Визначаємо оптимальне рішення усунення проблеми.
5. Перевіряємо параметри адресації пристрою, щоб переконатися, що вони відповідають мережевої документації.
6. Впроваджуємо, перевіряємо та документуємо рішення.
7. Використовуємо рішення для усунення проблем підключення.
8. Переконатися, що проблеми вирішено.

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.
- 7) Виконання завдання 4 з відповідними скріншотами.
- 8) Виконання завдання 5 з відповідними скріншотами.
- 9) Висновок.

Контрольні питання:

Яке основне призначення транспортного рівня в моделі OSI?

Які два основні протоколи працюють на транспортному рівні і чим вони відрізняються?

Що таке «портова адресація», і яку роль відіграють номери портів на транспортному рівні?

Поясніть принцип роботи «трестороннього рукошискання» у протоколі TCP.

Який протокол (TCP чи UDP) краще підходить для потокового відео та онлайн-ігор, і чому?

Яким чином транспортний рівень забезпечує надійність доставки даних у TCP?

Що таке сегментація даних, і навіщо вона потрібна на транспортному рівні?

Наведіть приклади відомих номерів портів, які використовуються протоколами прикладного рівня.

Яке основне призначення прикладного рівня в моделі OSI?

Які три рівні моделі OSI об'єднуються в один прикладний рівень моделі TCP/IP?

Назвіть декілька поширених протоколів прикладного рівня.

Яку роль відіграє протокол DNS на прикладному рівні?

КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 6

Тема: Конфігурація мережі на ПК, освоєння: `ifconfig`, `route`, `resolv.conf`, `hosts`, `services`.

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

Теоретичні відомості

Команда `ipconfig /all` надає доступ до детальної інформації, як-от MAC-адреса, IP-шлюз за замовчуванням і налаштування DNS-серверів. Водночас вона повідомляє про активність DHCP-протоколу, а також виводить дані DHCP-сервера, включно з деталями оренди адреси.

У разі динамічного призначення IP-адрес команда `ipconfig /release` дозволяє видалити поточні адреси, закріплені через DHCP. Після цього команда `ipconfig /renew` запитує оновлену конфігурацію з DHCP-сервера. Це може бути надзвичайно корисно, якщо у хоста зберігається некоректна або застаріла IP-інформація, адже просте оновлення часто достатньо для відновлення стабільного підключення.

Однак, якщо після очищення IP-конфігурації хост не отримує нових даних із DHCP-сервера, це може свідчити про відсутність мережевого підключення або проблеми з доступом до DHCP.

Ifconfig (interface configuration) – ця команда призначена для Unix-подібних систем, таких як Linux чи macOS, і є аналогом `ipconfig` у Windows. Вона використовується для перегляду IP-адрес всіх мережевих інтерфейсів, MAC-адрес, стану інтерфейсів (активні чи неактивні), а також для перегляду статистики мережі.

Якщо команда запускається без аргументів, вона відображає інформацію про стан лише активних інтерфейсів. При передачі одного аргументу у вигляді назви інтерфейсу буде показана інформація виключно про цей інтерфейс. Якщо

ж використати аргумент ``-a``, команда надасть дані про всі інтерфейси, включно з відключеними. У разі, якщо подано інші аргументи, команда використовується для конфігурації зазначеного інтерфейсу.

Приклад використання з деякими опціями.

```
#ifconfig interface [[-net|-host] address [parameters]]
```

`interface` – назва інтерфейсу; `address` – IP-адреса, яку потрібно призначити для інтерфейсу. Це може бути або IP адреса в dotted quad форматі, або ім'я, яке `ifconfig` буде шукати в `/etc/hosts` і `/etc/networks`; `-net` і `-host` опції змушують `ifconfig` працювати з адресою як мережевим номером або адресою хоста, відповідно.

Наступний список параметрів використовується `ifconfig` з відповідними назвами прапора, даними в дужках. Детальну інформацію можна отримати за допомогою команди `man ifconfig`.

Route – команда, що відповідає за маршрутизацію, визначає, який мережевий комп'ютер має отримати пакети, щоб вони успішно дійшли до кінцевої точки. Вона відображає таблицю маршрутизації на екрані, де кожен запис містить кілька полів:

`Destination` – IP-адреса кінцевого пункту маршруту;

`Gateway` – IP-адреса або ім'я шлюзу (якщо його немає, то використовується символ `"*"`);

`Genmask` – маска мережі маршруту;

`Flags` – вказівник типу або стану маршруту (може приймати наступні значення: `U` – активний, `H` – хост, `S` – шлюз, `D` – динамічний, `M` – модифікований);

`MSS` – максимальна кількість даних, що передаються за один раз;

`Metric` – число переходів до шлюзу;

`Ref` – кількість звернень до маршруту на певний момент часу;

`Window` – максимальна кількість даних для приймаючої сторони;

`Use` – число пакетів, переданих по маршруту;

`Iface` – тип інтерфейсу.

Щоб додати адресу в таблицю маршрутизації, треба використовувати команду `route` з ключем `add`. При цьому слід врахувати, що якщо відповідний інтерфейс вже сконфігурований за допомогою `ifconfig`, то система сама може отримати відомості про нього. У такому випадку немає сенсу у вживанні специфікаторів – достатньо вказати адресу пункту призначення. Всі інші дані будуть надмірними, а отже, і необов'язковими.

Очевидно, що для роботи в мережі в таблиці маршрутизації повинен бути зроблений хоча б один запис. Пункт призначення за замовчуванням позначається міткою `default`.

Для видалення маршруту треба використовувати команду `route del-net` [IP-адреса пункту призначення].

Приклади використання:

```
# route -n
```

Список локальної таблиці маршрутизації

```
# route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.1.1
```

Додати статичний маршрут в мережу 192.168.0.0/16 через шлюз с ір-адресою 192.168.1.1

```
# route add -net 0/0 gw IP_Gateway
```

Призначити ір-адреса шлюзу за замовчуванням (default gateway) `# route del 0/0 gw IP_gateway`

Видалити ір-адреса шлюзу за замовчуванням (default gateway)

Більш детальну інформацію ви можете отримати за допомогою команди `man route`

Resolv.conf – конфігураційний файл для процедур серверів імен, що є набором підпрограм, які забезпечують доступ до DNS (Domain Name System) – системи доменних імен Інтернету. Цей файл містить налаштування, що в основному використовуються підпрограмами резолвера, котрі викликаються під час роботи будь-яких процесів. Він організований у зрозумілий для людини вигляд із набором ключових слів і відповідних їм значень, які надають резолверу необхідну інформацію.

Всі налаштування файлу читаються процедурами резолвера під час їх першого запуску в межах будь-якого процесу. Файл спеціально розроблений для зручності адміністраторів і представлений у вигляді списку пар «ключове слово – значення». Ці пари забезпечують різнотипну інформацію, необхідну для роботи системи дозволу імен. Кожна пара у конфігураційному файлі має чіткий формат:

ключеве_слово значення

Підтримуються наступні опції конфігурації.

Nameserver адреса. Вказується IP-адреса сервера імен у форматі чисел, розділених точками, на який необхідно перенаправляти всі запити. У конфігураційному файлі `resolv.conf` можна прописувати до MAXNS серверів імен (у даний час — до трьох), кожен у окремому рядку. Якщо зазначено кілька серверів, процеси вирішення імен звертатимуться до них у заданій послідовності. У разі відсутності рядків `nameserver` у файлі, процедури функціонуватимуть через сервер імен на локальній машині.

Процес визначення імен здійснюється за наступною схемою: спочатку відбувається спроба звернутися до першого сервера зі списку. Якщо запит не буде виконано протягом встановленого часу, система переходить до наступного сервера, прописаного у файлі налаштувань, і так далі, доти, поки список серверів не буде повністю опрацьований. У випадку, якщо всі спроби завершаться невдало, процедура знову проходить всі зазначені сервери у межах максимально дозволеної кількості повторних запитів.

Domain ім'я. Локальне доменне ім'я встановлюється як стандартний домен, що дозволяє здійснювати більшість запитів із використанням скорочених імен, асоційованих із локальним доменом. Якщо параметр `domain` не заданий у конфігураційному файлі, домен визначається значенням змінної середовища `LOCALDOMAIN` (якщо вона існує). У разі її відсутності домен визначається шляхом обробки повного доменного імені через метод `gethostname`, вилучаючи перший рівень домену і використовуючи частину імені після першої точки. Якщо

ім'я хоста не містить доменного імені, автоматично використовується кореневий домен.

Search список_пошуку. Список пошукових доменів використовується для визначення імен хостів у процесі розв'язання DNS-запитів. Як правило, цей список налаштовується відповідно до локального домену, який додається за замовчуванням. Проте, за необхідності, його можна змінити шляхом вказівки додаткових доменів, які мають бути включені до пошуку. Доменні імена у цьому списку повинні бути розділені пробілами або символами табуляції.

Процес розв'язання DNS-запитів зазвичай передбачає послідовне використання всіх елементів зазначеного списку до знаходження коректного доменного імені. Втім, цей підхід може виявитися ресурсозатратним, оскільки він здатен спровокувати значне уповільнення роботи через обсяг даних, що передаються мережею. Це, зокрема, стосується ситуацій, коли сервери імен для зазначених доменів розташовані віддалено.

Також слід брати до уваги той факт, що у разі недоступності сервера імен для одного з указаних доменів запит може не бути виконаним протягом встановленого часу очікування. Максимальна кількість записів у списку пошуку обмежена шістьма доменами, а його загальна довжина не повинна перевищувати 256 символів.

Sortlist список_сортування. Викликає сортування адрес, що повертаються функцією `gethostbyname`, відповідно до локальних правил. Список сортування задається у вигляді пар IP-адрес/маска мережі. Маску мережі вказувати не обов'язково – за замовчуванням використовується звичайна маска мережі. У парі IP-адреса та необов'язкова маска мережі розділяються косою рисою. У списку можна вказувати до 10 пар. Наприклад, наступна специфікація вимагає від функції `gethostbyname` () видавати адреси, відповідні мережі 130.155.160.0/255.255.240.0, до адрес мережі 130.155.0.0.

```
sortlist 130.155.160.0/255.255.240.0
```

```
130.155.0.0
```

Options список_опцій. Задає необов'язкові особливості роботи для різних процедур дозволу імен у відповідності із зазначеним списком опцій, кожна з яких еквівалентна внутрішньої змінної процедури вирішення. Опції, встановлені в процесі обробки рядків в локальному файлі `resolv.conf`, можуть бути змінені для кожного процесу шляхом завдання в якості значення змінної середовища `LOCALDOMAIN` списку доменів для пошуку через пробіл.

Опції, встановлені в процесі обробки рядків в локальному файлі `resolv.conf`, можуть бути доповнені для кожного процесу шляхом завдання в якості значення змінної середовища `RES_OPTIONS` списку опцій процедур дозволу імен через кому. Відповідні опції перераховані після ключового слова `options`.

Пари ключове слово-значення повинні задаватися в окремих рядках, причому, ключове слово (наприклад, `nameserver`) повинно починати рядок. Значення або список значень задається після ключового слова, після пробільних символів.

Більш детальну інформацію ви можете отримати за допомогою команди `man resolv.conf`

Hosts – текстовий файл, що містить базу даних доменних імен та використовуваний при їх трансляції в мережеві адреси вузлів. Запит до цього файлу має пріоритет перед зверненням до DNS-серверів. На відміну від DNS, вміст файлу контролюється адміністратором комп'ютера.

Розташування:

`/etc/hosts`

Це простий текстовий файл, який асоціює IP адреси з іменами вузлів, по одній IP адресі в рядку. Для кожного вузла в одному рядку повинен бути представлений запис з наступною інформацією:

IP_адреса каноніческое_імя_узла псевдоніми

Поля запису розділяються пробілами і / або символами табуляції. Текст, що починається з символу `"#"` до кінця рядка вважається коментарем і ігнорується. Імена вузлів можуть містити тільки букви, цифри знак мінус ("`-`") і

крапку ("."). Вони повинні починатися з букви і закінчуватися буквою або цифрою. Псевдоніми надаються для можливості вибору більше одного імені, альтернативної вимови, скорочення імені вузла або для вказівки найбільш загального імені вузла (наприклад, localhost).

DNS сервер Berkeley Internet Name Domain (BIND) реалізує сервер служби імен для UNIX систем. Він розширює або заміщає файл / etc / hosts при операціях пошуку імені вузла, а також звільняє від необхідності підтримувати актуальність та повноту /etc/hosts.

У сучасних системах, навіть задана у файлі / etc / hosts інформація, може бути перекрита інформацією з DNS, це широко використовується для наступних випадків:

Початкове завантаження. Більшість систем мають маленький розмір файлу / etc / hosts, який зазвичай містить імена і адреси найбільш важливих вузлів локальної мережі. Це корисно, коли служба DNS не запущена, наприклад під час завантаження системи.

NIS. Сайти, що використовують NIS, зберігають таблицю вузлів в базі даних вузлів NIS. Але навіть при роботі з NIS залишається можливість використовувати DNS, більшість NIS сайтів також використовують для цілей резервного копіювання і файл / etc / hosts, де розміщуються записи про всі локальні вузли.

Ізольовані вузли. Маленькі сайти, які є ізольованими від мережі, використовують файл / etc / hosts замість DNS. Якщо локальна інформація змінюється рідко і мережа не підключена до інтернету, DNS не дає відчутних переваг.

Приклад

127.0.0.1 localhost

192.168.1.10 foo.mydomain.org foo

192.168.1.13 bar.mydomain.org bar

216.234.231.5 master.debian.org master

205.230.163.103 www.opensource.org

Більш детальну інформацію можна отримати за допомогою команди `man hosts`.

Services. Для конвертації номерів портів в імена сервісів, кожна система зберігає список відповідності. Він зберігається у файлі `/etc/services`. Кожен рядок в цьому файлі має такий формат:

`service port / protocol [aliases]`

Service задає ім'я сервісу, port визначає номер порту, використовуваного цим сервісом, а protocol визначає, яким транспортним протоколом користується сервіс. Є можливість відмінності протоколів `udp` або `tcp`. Сервіс може працювати з різними протоколами, а може бути два сервіси працюють на одному порту, але з різними протоколами. Поле `aliases` дозволяє задавати кілька імен (псевдонімів) для одного сервісу.

Більш детальну інформацію можна отримати за допомогою команди `man services`.

Виконання комп'ютерного практикуму

Завдання 1. Відкрити файл Завдання 1_ЛР6.pka. Використання команди `ipconfig` для виявлення неправильної конфігурації на ПК. Для цього:

Отримайте доступ до Command Prompt на кожному комп'ютері і введіть команду `ipconfig /all`.

Перевірте налаштування IP-адреси, маски підмережі та шлюзу за замовчуванням на кожному ПК. Не забудьте записати IP-конфігурацію кожного ПК, щоб допомогти у виявленні будь-яких ПК, що налаштовані невірно.

Виберіть неправильно налаштований ПК.

Перейдіть на вкладку Desktop > IP Configuration для виправлення конфігурації.

Завдання 2. Використання команди `ifconfig`.

Перегляд налаштувань для мережевого інтерфейсу. Ввести в командному рядку команду `ifconfig`. Переглянути список всіх активних інтерфейсів. Далі

вказіть в якості аргументу ім'я одного з інтерфейсів. З'явиться статистика лише по обраному.

За допомогою аргументу -a отримати відображення всіх інтерфейсів, включаючи вимкнені

Вимкнути один з інтерфейсів (down), потім переглянути статистику по всім інтерфейсам, увімкнути цей інтерфейс (up)

Призначити одному з інтерфейсів нову IP-адресу 192.168.2.2, змінити мережну маску – 255.255.255.0 і бродкаст адресу на 192.168.2.255 однією командою; після цього знову переглянути статистику по всім інтерфейсам

Завдання 3. Команда route.

Вивести на екран таблицю маршрутизації за допомогою аргументу -n

Додати маршрут по локальній мережі через один з інтерфейсів за допомогою аргументу add.

За допомогою del default і add default змінити маршрут за замовчуванням. Переглянути таблицю маршрутизації. Повернути значення для первісного маршруту за замовчуванням (0.0.0.0)

Додати маршрут до мережі 192.57.66.0/24 через шлюз 10.0.0.4, потім переглянути таблицю і видалить маршрут.

Завдання 4. Використання файлу resolv.conf.

Відкрити файл /etc/resolv.conf – ретельно вивчіть вміст файлу і за допомогою інформації в теоретичних відомостях пояснити все, що в ньому зазначено.

Завдання 5. Використання файлу hosts.

Відкрити файл /etc/hosts – ретельно вивчіть вміст файлу і за допомогою інформації в теоретичних відомостях пояснити все, що в ньому зазначено.

Завдання 6. Використання файлу services.

Відкрийте файл /etc/services – ретельно вивчіть вміст файлу і за допомогою інформації в теоретичних відомостях пояснити все, що в ньому зазначено.

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.
- 7) Виконання завдання 4 з відповідними скріншотами та поясненнями.
- 8) Виконання завдання 5 з відповідними скріншотами та поясненнями.
- 8) Виконання завдання 5 з відповідними скріншотами та поясненнями.
- 10) Висновок.

Контрольні питання:

Для чого використовується команда `ifconfig`? Назвіть деякі опції команди.

Що можна побачити при виведенні конфігурацій на екран командою `ifconfig`?

Для чого використовується команда `route`? Назвіть деякі опції команди.

Як додати статичний маршрут в мережу 192.168.0.0/16 через шлюз з ір-адресою 192.168.1.1?

Перерахуйте деякі опції конфігурацій для `resolv.conf` і опишіть їх.

Напишіть приклад вмісту файлу `hosts`. Що в ньому зберігається?

Назви яких двох транспортних протоколів найчастіше можна побачити у файлі `services`? Назвіть відмінність цих двох протоколів.

КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 7

Тема: Мережевий рівень. Адресація та аналіз трафіку в мережі.

Мета заняття: Дізнатися команди для моніторингу мережі, їх призначення. Адресація та типи адрес.

Теоретичні відомості

Протоколи мережного рівня. Третій рівень еталонної моделі OSI, відомий як мережевий рівень, забезпечує функції, завдяки яким кінцеві пристрої можуть здійснювати обмін даними через мережі. Як відображено на рисунку 7.1, ключовими протоколами мережного рівня є інтернет-протоколи IPv4 і IPv6. Додатково до них належать й інші важливі протоколи, наприклад, маршрутизаційні протоколи, такі як OSPF (Протокол відкритого найкоротшого шляху), а також протоколи для обміну службовими повідомленнями, зокрема ICMP (Міжмережний протокол керуючих повідомлень).

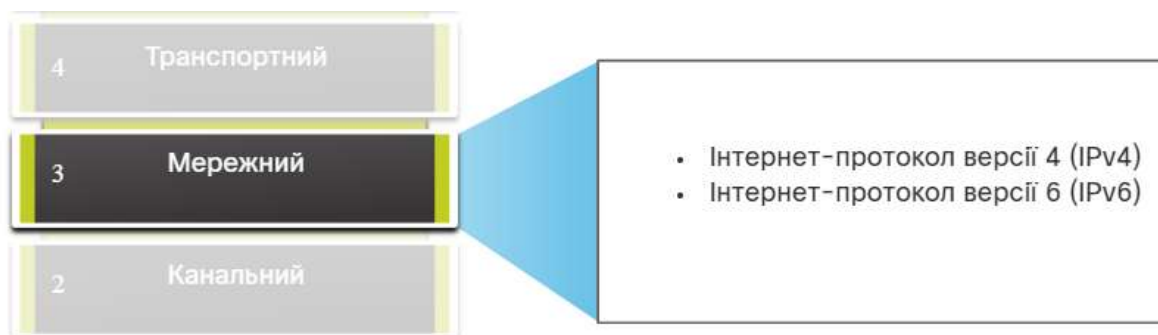


Рисунок 7.1 – Протоколи Мережевого рівня

Для забезпечення можливості наскрізного зв'язку через межі мереж, протоколи Мережевого рівня виконують чотири основні операції:

Адресація кінцевих пристроїв – для ідентифікації в мережі на кінцевих пристроях повинні бути налаштовані унікальні IP-адреси.

Інкапсуляція – на мережевому рівні здійснюється інкапсуляція блоку даних протоколу (PDU) транспортного рівня в мережевий пакет. У ході цього процесу до структури пакета додається інформація, яка міститься в IP-заголовку, зокрема IP-адреси вузлів джерела (відправника) та призначення (отримувача). Весь процес інкапсуляції відбувається на боці джерела IP-пакета.

Маршрутизація – мережевий рівень виконує функцію спрямування пакетів до вузла призначення, який може знаходитися в іншій мережі. Для досягнення іншої мережі пакет потребує обробки маршрутизатором. Основна задача маршрутизатора полягає у виборі найкращого маршруту та передачі пакетів до потрібного вузла. Цей процес називають маршрутизацією. На своєму шляху до вузла призначення пакет може пройти через кілька маршрутизаторів. Кожен маршрутизатор, через який проходить пакет, називається переходом (hop).

Де-інкапсуляція – коли на мережевому рівні вузла призначення отримується пакет, пристрій аналізує його IP-заголовок. Якщо адреса призначення, вказана у заголовку, збігається із власною IP-адресою вузла, заголовок вилучається з пакета. Після завершення процесу деінкапсуляції на мережевому рівні отриманий PDU четвертого рівня передається відповідній службі на транспортному рівні. Це розкриття пакета виконується саме кінцевим вузлом, який є цільовим для IP-пакета.

Транспортний рівень, або четвертий рівень моделі OSI, спеціалізується на керуванні передачею даних між активними процесами на вузлах мережі. Протоколи мережевого рівня, такі як IPv4 та IPv6, орієнтовані на визначення структури пакетів і їх обробку для забезпечення передачі інформації між різними вузлами. Вони функціонують незалежно від типів даних у пакетах, що надає можливість мережевому рівню обробляти передачі для множинних типів зв'язку і різноманітних вузлових інфраструктур.

Пристрої третього рівня, включаючи маршрутизатори і комутатори цього рівня, перевіряють IP-заголовок у процесі переміщення пакета мережею до його кінцевого призначення. Дані про IP-адресацію залишаються незмінними від моменту формування пакета вихідним вузлом до його прибуття на вузол призначення, за винятком випадків, коли пристрої здійснюють трансформацію адрес за допомогою механізму перетворення мережевих адрес (Network Address Translation або NAT) для IPv4.

Маршрутизатори здійснюють функціонування протоколів маршрутизації, забезпечуючи спрямування пакетів між різними мережами. Проміжні пристрої, відповідальні за маршрутизацію, аналізують інформацію адресації на Мережевому рівні, яка міститься в заголовку пакета. У процесі роботи на Мережевому рівні інкапсульовані дані, такі як PDU Транспортного рівня або відповідні інтегровані дані, залишаються незмінними і не зазнають модифікацій.

Характеристики IP. Протокол IP був розроблений як мережевий протокол із мінімальними накладними витратами. Його основна мета полягає в забезпеченні базової функціональності для пересилання пакету даних від джерела до вузла призначення через інтегровану систему мереж. При цьому даний протокол не передбачає механізмів відстеження або управління потоком пакетів. Виконання цих функцій, якщо вони потрібні, делегується іншим протоколам на вищих рівнях мережевої моделі, зокрема протоколу TCP на четвертому рівні.

Таким чином, протокол IP має наступні властивості:

- без орієнтації на з'єднання (Connectionless). Перед початком передачі пакету даних не здійснюється ініціалізація каналу зв'язку з адресатом, що є фундаментальною характеристикою його роботи;
- доставлення на основі найкращих зусиль (Best Effort). Протокол IP характеризується ненадійністю доставки даних, оскільки він не гарантує успішного доставлення кожного пакета до пункту призначення;
- незалежність від середовища передачі даних (Media Independent). Протокол функціонує в незалежності від типу середовища передачі даних, до якого належать мідний кабель, волоконно-оптичний канал або бездротове з'єднання.

Заголовок пакета IPv4. Заголовок пакета IPv4 складається з кількох полів, які містять ключову інформацію про пакет. У цих полях розташовуються двійкові дані, що підлягають аналізу на третьому рівні мережевої моделі. Двійкові значення кожного поля відповідають конкретним параметрам IP-пакета, визначаючи його характеристики. Схеми заголовків протоколів, які

читаються послідовно — зліва направо і зверху вниз, дають наглядне уявлення про структуру та вміст полів протоколу. На рисунку 7.2 представлена схема заголовка протоколу IP, яка детально показує складові пакета IPv4.

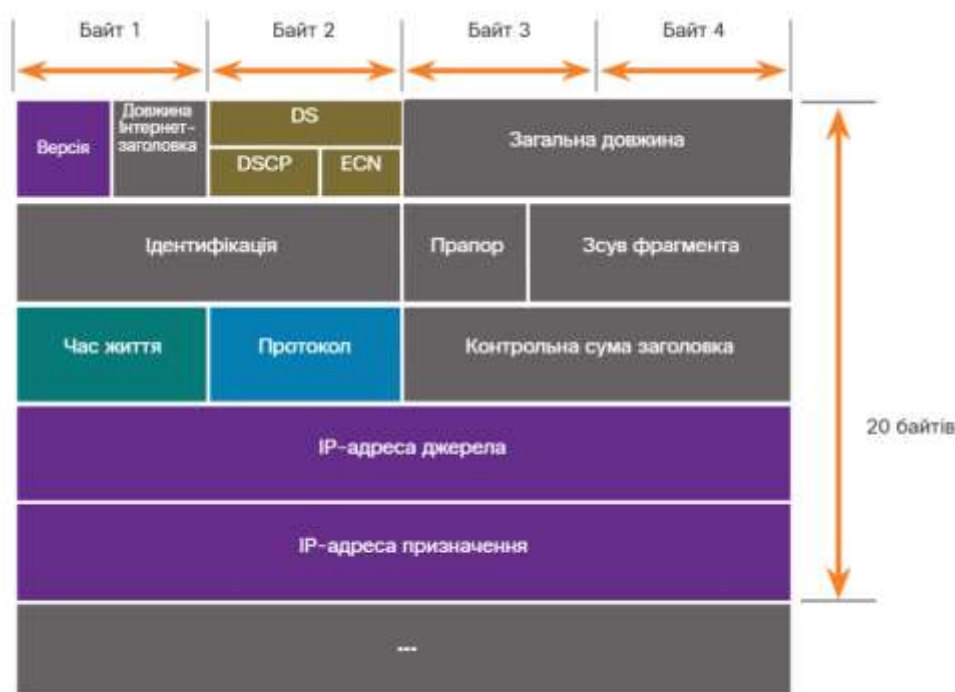


Рисунок 7.2 –Схема заголовка протоколу IP

Основні поля заголовка IPv4 включають наступні важливі елементи.

Поле версії містить 4-бітове двійкове значення, яке завжди встановлене як 0100 і визначає пакет як IPv4.

Поле диференційованих сервісів (DiffServ або DS), яке раніше називалося типом сервісу (Type of Service, ToS), є 8-бітовим параметром, що встановлює пріоритет для кожного пакета. Шість його найбільш значущих бітів формують точку коду диференційованих послуг (Differentiated Services Code Point, DSCP), а решта два біти використовуються для явного повідомлення про перевантаження (Explicit Congestion Notification, ECN).

Елемент «Час життя» (Time to Live, TTL) є 8-бітовим значенням, що визначає максимальний час існування пакета в мережі. Відправник встановлює початкове значення TTL, яке зменшується маршрутизатором на одиницю при кожному проходженні пакета. У випадку, коли TTL досягає нуля,

маршрутизатор відкидає пакет і сповіщає джерело про це через ICMP-повідомлення. При зменшенні TTL маршрутизатор також повторно розраховує контрольну суму заголовка.

Поле протоколу використовується для уточнення типу даних, що містяться в пакеті, та ідентифікації наступного рівня протоколу. Це 8-бітове значення може позначати такі протоколи верхнього рівня, як ICMP (1), TCP (6) чи UDP (17).

Контрольна сума заголовка допомагає визначити пошкодження структури заголовка пакета IPv4.

Адреса джерела IPv4 являє собою 32-бітове двійкове число, яке ідентифікує вихідну адресу пакета. Джерельна адреса завжди є унікальною.

Адреса призначення IPv4 також є 32-бітовим числом, що представляє кінцевий пункт доставки пакета. Вона може бути спрямована на індивідуальну адресу, групу чи ширококомовний пункт.

Найважливішими полями серед заголовка IPv4 вважаються адреси джерела та призначення. Вони вказують на початковий пункт надсилання пакета і його кінцеве місце. Як правило, ці адреси залишаються незмінними у процесі передавання від джерела до отримувача.

Додаткові елементи заголовка, як-от довжина інтернет-заголовка (Internet Header Length, IHL), загальна довжина та контрольна сума заголовка, відповідають за ідентифікацію й коректність пакета під час передачі.

Окремо виділяються поля для роботи з фрагментованими пакетами – ідентифікація, прапор та зміщення фрагмента. Ці параметри допомагають відстежувати частини пакета IPv4 при його передачі. Якщо маршрутизатор стикається з середовищем із меншим розміром MTU, він може бути змушений фрагментувати пакет для належної доставки.

Обмеження IPv4. Розробка IPv6. Вичерпання адресного простору IPv4 є наслідком обмеженого обсягу унікальних публічних адрес у цій версії протоколу. Загальна кількість доступних IPv4-адрес становить приблизно 4 мільярди. Однак стрімке зростання числа пристроїв, що підключаються до мережі, включаючи нові IP-сумісні пристрої та постійно активні пристрої, поряд

із очікуваним розвитком інфраструктури в менш технологічно розвинених регіонах, призвело до більшого попиту на адресний простір.

Однією з ключових проблем IPv4 є обмежені можливості наскрізного підключення. Для подолання цієї проблеми зазвичай застосовується технологія трансляції мережних адрес (Network Address Translation, NAT). Хоча NAT дозволяє групі пристроїв спільно використовувати одну публічну IPv4-адресу, цей механізм призводить до приховування адрес внутрішніх вузлів мережі. Така конфігурація може створювати труднощі для застосунків і технологій, що потребують прямого наскрізного зв'язку між кінцевими точками.

Крім того, впровадження NAT у мережних інфраструктурах супроводжується зростанням складності. Незважаючи на продовження терміну експлуатації IPv4 завдяки використанню NAT, ця технологія замислювалася як тимчасове рішення для перехідного періоду до версії IPv6. Реалізація NAT додає оперативні ускладнення, зокрема погіршення затримок при передачі даних та складність у процесах діагностики та усунення несправностей в мережі.

З огляду на ці проблеми, у 1990-х роках Інженерна група з розвитку інтернету (Internet Engineering Task Force, IETF) ініціювала пошук альтернативи для подолання обмежень IPv4. Наслідком цього стала розробка нового стандарту – IP версії 6 (IPv6). Протокол IPv6 суттєво розширює можливості порівняно з попередником, забезпечуючи функціональність, яка відповідає сучасним і майбутнім вимогам мережних інфраструктур.

IPv6 пропонує низку покращень, серед яких:

- розширений адресний простір. IPv6-адреси побудовані на основі 128-бітної ієрархічної адресації, значно перевершуючи IPv4 із його 32-бітною структурою;
- оптимізована обробка пакетів. Заголовок IPv6 спрощено та містить меншу кількість полів, що підвищує ефективність передачі;
- відсутність необхідності в NAT. Завдяки величезній кількості доступних публічних IPv6-адрес більше немає потреби в NAT для перетворення приватних і публічних IP-адрес, як це відбувається у випадку з IPv4. Це усуває проблеми,

які виникають через NAT, зокрема у програмах, що вимагають прямого з'єднання.

Отже, 32-розрядний адресний простір IPv4 забезпечує приблизно 4 294 967 296 унікальних адрес, а адресний простір IPv6 надає 340 282 366 920 938 463 374 607 431 768 211 456 або 340 ундецильйонів (10^{36}) адрес.

Заголовок пакета IPv6. На рисунку 7.3 показано схему заголовка IP-протоколу, що визначає поля IPv6-пакета.

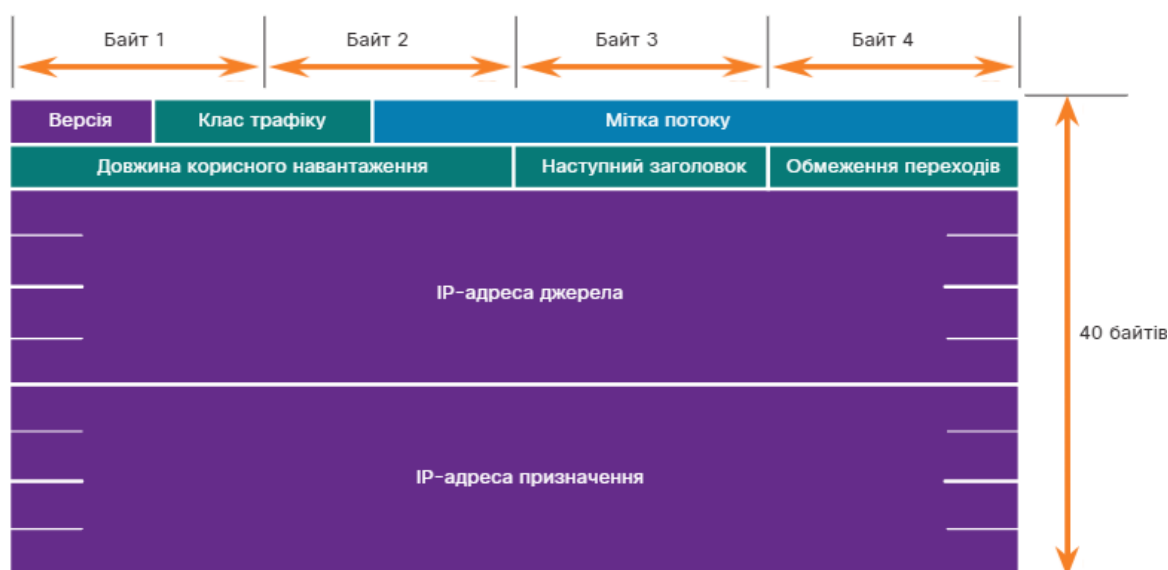


Рисунок 7.3 – Схема заголовка IP-протоколу, що визначає поля IPv6-пакета

Поля заголовка в протоколі IPv6 виконують ключову роль у забезпеченні коректної роботи мережевої передачі даних. Розглянемо основні компоненти заголовка пакета IPv6 з точки зору їх структури та функціонального призначення.

Версія є 4-бітовим полем, значення якого визначено як 0100, що вказує на використання саме шостої версії Інтернет-протоколу.

Поле класу трафіку займає 8 бітів і відповідає полю диференційованих сервісів (Differentiated Services, DS) у протоколі IPv4. Воно забезпечує позначки для класифікації та пріоритезації трафіку.

Мітка потоку представлена 20-бітовим полем, яке слугує для ідентифікації потоків даних, що підлягають однаковій маршрутизації, забезпечуючи однаковий тип обробки пакетів у мережі.

Довжина корисного навантаження відображається у 16-бітовому полі, яке вказує розмір даних у пакеті, виключаючи розмір фіксованого заголовка IPv6, що дорівнює 40 байтам.

Наступний заголовок є 8-бітовим полем, яке еквівалентне полю «Протокол» у заголовку IPv4. Воно дозволяє визначити тип протоколу вищого рівня, для якого передаються дані у пакеті.

Обмеження переходів, що замінює поле "Час життя" (TTL) у протоколі IPv4, також займає 8 бітів. Це поле зменшується на одиницю кожного разу, коли пакет проходить через маршрутизатор. Якщо цей лічильник досягне нульового значення, пакет відкидається, а вузлу-джерелу надсилається повідомлення ICMPv6 про перевищення часу очікування. Крім того, у протоколі IPv6 відсутнє поле «Контрольна сума заголовка», оскільки контрольні суми обробляються як на нижчих (канальних), так і на вищих рівнях моделі OSI. Це рішення підвищує продуктивність мережі, оскільки маршрутизаторам не потрібно щоразу перераховувати контрольну суму після зменшення значення лічильника переходів.

IPv6-адреса джерела є 128-бітовим полем, яке визначає IP-адресу пристрою-відправника. Аналогічно, IPv6-адреса призначення, також розміром 128 бітів, указує місцезнаходження вузла-отримувача.

У складі IPv6-пакету можуть бути присутні розширені заголовки (extension headers, EH), які надають додаткову мережеву інформацію. Розширені заголовки необов'язкові й розташовуються між стандартним заголовком і корисним навантаженням. Вони слугують для реалізації таких функцій, як фрагментація, забезпечення безпеки або підтримка мобільності.

На відміну від IPv4, маршрутизатори в мережах IPv6 не здійснюють фрагментацію пакетів під час їх передачі. Це завдання покладається виключно

на вузли-джерела, які забезпечують відповідність розміру пакету максимальному MTU (Maximum Transmission Unit) у обраному шляху.

IP-адреса (Internet Protocol address) – це унікальний числовий ідентифікатор пристрою в комп'ютерній мережі, яка використовує протокол IP для зв'язку.

Білі (публічні) IP-адреси є унікальними у глобальній мережі Інтернет і забезпечують прямий доступ зі всесвітньої мережі. Вони офіційно присвоюються провайдерами та використовуються для серверів, що мають бути доступні ззовні. Кількість таких адрес, особливо у версії IPv4, є обмеженою.

Сірі (приватні) IP-адреси застосовуються виключно в межах локальних мереж. Вони не маршрутизуються через Інтернет і можуть повторюватися у різних локальних мережах без конфлікту.

Діапазони приватних адрес:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

Пристрої з сірими адресами виходять в інтернет через NAT (Network Address Translation) – технологію, яка перетворює приватні адреси на публічну адресу. Адреса IPv4 шлюзу за замовчуванням використовується для доступу до віддалених мереж, а IPv4-адреса DNS-сервера – для перетворення доменних імен в адреси IPv4.

Маска підмережі – використовується для визначення мережної/вузлової частини IPv4-адреси.

Маска підмережі IPv4 відіграє ключову роль у поділі IPv4-адреси на мережеву та вузлову складові. При призначенні пристрою конкретної IPv4-адреси маска підмережі застосовується для визначення відповідної мережевої адреси цього пристрою. Мережева адреса функціонує як ідентифікатор, що об'єднує всі пристрої в межах однієї мережі. Концептуально маска підмережі являє собою бітову структуру, що складається з послідовності одиничних бітів (1), яка завершується сукупністю нульових бітів (0).

На рисунку 7.4 показано 32-бітну маску підмережі в десятковому і двійковому форматах, в яких крапки використовуються як розділювачі.



Рисунок 7.4 – Поєднання адреси IPv4 з маскою підмережі

Використання десяткового представлення мережеских і вузлових адрес із маскою підмережі, розділеною крапками, може бути незручним та перевантаженим. Тому є альтернативний підхід для визначення маски підмережі, який називається довжиною префікса.

Довжина префікса характеризується числом бітів, значення яких дорівнює одиниці в масці підмережі. Це позначення записується через скісну риску (/) із подальшим зазначенням кількості зазначених бітів.

Наприклад, для вузла з IPv4-адресою 192.168.10.10 і маскою підмережі 255.255.255.0 мережева адреса визначається таким чином: (рисунок 7.5.):

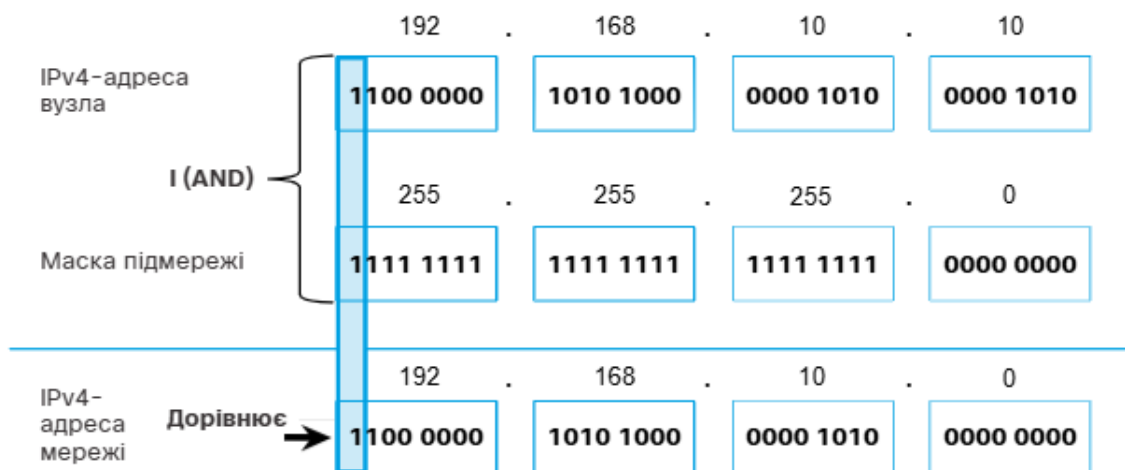


Рисунок 7.5 – Визначення мережевої адреси.

IPv4-адреса вузла (192.168.10.10) – IPv4-адреса вузла в десятковому і двійковому форматах з розділенням крапками.

Маска підмережі (255.255.255.0) – маска підмережі вузла в десятковому і двійковому форматах з розділенням крапками.

Мережева адреса (192.168.10.0) – результатом логічної операції I над IPv4-адресою та маскою підмережі є мережна адреса IPv4, наведена у десятковому і двійковому форматах з розділенням крапками.

Маска підмережі служить для визначення максимальної кількості хостів, які можуть бути присутні в певній мережі. Вона також дає змогу розділити одну мережу на декілька менших підмереж.

Розмір мережі залежить від кількості бітів, відведених для ідентифікації мережі. Чим більше біт виділено для номера мережі, тим менше залишається для ідентифікатора хоста, що відповідно зменшує потенційну кількість хостів у такій мережі.

$$\text{Кількість хостів} = 2^n - 2$$

де n – кількість біт для хостів (нулів у масці).

Віднімаємо 2, бо:

Одна адреса – адреса мережі (всі біти хостів = 0)

Одна адреса – broadcast адреса (всі біти хостів = 1)

Приклади:

Маска 255.255.255.0 (або /24)

Біт для хостів: 8 (останній октет)

Кількість хостів: $2^8 - 2 = 254$ хости

Діапазон: наприклад, 192.168.1.1 – 192.168.1.254

Маска 255.255.255.128 (або /25)

Біт для хостів: 7

Кількість хостів: $2^7 - 2 = 126$ хостів

Приклад розподілу мережі на підмережі. Процес поділу мережі на підмережі простіше пояснити на конкретному прикладі.

На всю мережу нам виділили одну IP-адресу 192.168.0.0/24, яку нам потрібно розділити на 6 підмереж. У двійковому вигляді ця IP-адреса виглядає так: 11000000.10101000.00000000.00000000.

Необхідна кількість вузлів (хостів, в даному випадку комп'ютерів) у кожній підмережі:

Підмережа А – 100 вузлів

Підмережа В – 50 вузлів

Підмережа С – 20 вузлів

Підмережа D – 2 вузли

Підмережа E – 2 вузла

Підмережа F – 2 вузли

Починати процес розподілу мережі треба з мережі з максимальною кількістю вузлів.

"/24" – це префікс маски підмережі (короткий запис маски). Повний запис маски підмережі 255.255.255.0. У двійковому відображенні маска підмережі виглядає так: 11111111.11111111.11111111.00000000 це означає, що нам доступно 8 біт для поділу мережі.

Першій підмережі А потрібно виділити IP-адреси для 100 вузлів. Тобто на адресацію хостів достатньо 7 біт ($01111111 = 127$). 127 разом з нулем за кількістю

дорівнює 128 це повна кількість адрес, що задовольняє вимогам (і навіть залишається кілька адрес про запас).

Отже, замінюємо маску з "/24" на "/25" (у двійковому форматі буде 11111111.11111111.11111111.10000000) та застосовуємо нову маску до нашої мережі та отримаємо 2 підмережі:

1(підмережа А) – 11000000.10101000.00000000.00000000 (мережа 192.168.0.0/25)

2 – 11000000.10101000.00000000.10000000 (мережа 192.168.0.128/25)

У двох нових мережах вузлова частина адреси становить 7 бітів. Далі починаємо розподіл мережі 192.168.0.128/25. Відомо, що для підмережі В потрібно 50 адрес для вузлів. Визначаємо, що вузлова частина для підмережі В має містити 6 біт ($2^6 - 2 = 62$). Маска стає на одиницю більше /26, застосовуємо її до нашої мережі та отримуємо дві нові підмережі

1 (підмережа В) – 11000000.10101000.00000000.10000000 (мережа 192.168.0.128/26)

2 – 11000000.10101000.00000000.11000000 (мережа 192.168.0.192/26)

Так само відокремлюємо ще 1 біт від адреси вузла (00011111 = 31, що більше 20, і отже нам підходить), маска вже /27. Знову дві мережі: 1 – 11000000.10101000.00000000.11000000 (мережа 192.168.0.192/27)

2 – 11000000.10101000.00000000.11100000 (мережа 192.168.0.224/27)

Залишилося нам виділити 3 підмережі по 2 адреси для вузлів. Для адреси вузла достатньо двох бітів (00000011 = 3), $2^2 - 2 = 2$ адреси для двох вузлів.

У свою чергу для трьох, однакових за розміром, підмереж досить теж двох бітів. Всього в IP-адресі 32 біти, віднімаємо необхідні нам 2 і отримуємо 30, отже використовуємо маску /30. Ділимо нашу нову мережу на 3 підмережі:

1 – 11000000.10101000.00000000.11100000 (мережа 192.168.0.224/30).

2 – 11000000.10101000.00000000.11100100 (мережа 192.168.0.228/30).

3 – 11000000.10101000.00000000.11101000 (мережа 192.168.0.232/30).

Отже:

Підмережа А – 192.168.0.0/25

Підмережа В – 192.168.0.128/26

Підмережа С – 192.168.0.192/27

Підмережа D – 192.168.0.224/30

Підмережа Е – 192.168.0.228/30

Підмережа F – 192.168.0.232/30

Виконання комп'ютерного практикуму

Завдання 1. Відкрити файл Завдання 1_LP7.pka. Визначити MAC- та IP-адреси.

Частина 1: Зібрати інформацію про PDU для зв'язку в локальній мережі

Натисніть 172.16.31.5 та відкрийте командний рядок.

Введіть команду ping 172.16.31.2.

Перейдіть у режим моделювання та повторіть команду ping 172.16.31.2.

PDU з'явиться поруч із 172.16.31.5.

Клацніть PDU та зверніть увагу на таку інформацію з вкладок «Модель OSI» та «Шар вихідного PDU»:

MAC-адреса призначення: 000C:85CC:1DA7

MAC-адреса джерела: 00D0:D311:C788

IP-адреса джерела: 172.16.31.5

IP-адреса призначення: 172.16.31.2

На пристрої: 172.16.31.5

Натисніть «Захопити / Переслати» (стрілка праворуч, за якою йде вертикальна смуга), щоб перемістити PDU на наступний пристрій. Зберіть інформацію та повторюйте цей процес, доки PDU не досягне свого призначення. Запишіть зібрану інформацію про PDU в електронну таблицю.

Частина 2: Збір інформації про PDU для зв'язку з віддаленою мережею

1: Зберіть інформацію про PDU, коли пакет передає дані з 172.16.31.5 до 10.10.10.2.

Натисніть 172.16.31.5 та відкрийте командний рядок.

Введіть команду ping 10.10.10.2.

Перейдіть у режим моделювання та повторіть команду ping 10.10.10.2. PDU з'явиться поруч із 172.16.31.5.

Клацніть PDU та зверніть увагу на таку інформацію з вкладки «Вихідний рівень PDU»:

MAC-адреса призначення: 00D0:BA8E:741A

MAC-адреса джерела: 00D0:D311:C788

IP-адреса джерела: 172.16.31.5

IP-адреса призначення: 10.10.10.2

На пристрої: 172.16.31.5

Натисніть «Захопити / Переслати», щоб перемістити PDU на наступний пристрій. Зберіть ту саму інформацію. Повторюйте цей процес, доки PDU не досягне свого призначення. Запишіть інформацію про PDU, яку ви зібрали під час пінгу з 172.16.31.5 на 10.10.10.2, у електронну таблицю.

Завдання 2. Відкрити файл Завдання 2_ЛР7.pka. Розділити мережу на підмережі.

1. Створіть схему підмереж, яка відповідає необхідній кількості підмереж та необхідній кількості адрес хостів.

Перша підмережа – це мережа LAN-A. потрібно щонайменше 50 IP-адрес хостів.

Друга підмережа – це мережа LAN-B. Потрібно щонайменше 40 IP-адрес хостів.

Також потрібно щонайменше дві додаткові невикористані підмережі для майбутнього розширення мережі.

Заповнити таблицю:

Адреса підмережі	Префікс	Маска підмережі

2. Заповніть відсутні IP-адреси в таблиці адресації

Призначте першу підмережу LAN-A.

1) Використовуйте адресу першого хоста для інтерфейсу CustomerRouter, підключеного до комутатора LAN-A.

2) Використовуйте адресу другого хоста для комутатора LAN-A. Обов'язково призначте адресу шлюзу за замовчуванням для комутатора.

3) Використовуйте адресу останнього хоста для ПК-A. Обов'язково призначте адресу шлюзу за замовчуванням для ПК.

Призначте другу підмережу LAN-B.

1) Використовуйте адресу першого хоста для інтерфейсу CustomerRouter, підключеного до комутатора LAN-B.

2) Використовуйте адресу другого хоста для комутатора LAN-B. Обов'язково призначте адресу шлюзу за замовчуванням для комутатора.

3) Використовуйте адресу останнього хоста для ПК-B. Обов'язково призначте адресу шлюзу за замовчуванням для ПК.

Частина 2. Налаштування пристроїв

Налаштуйте основні параметри ПК, комутаторів та маршрутизатора. Зверніться до таблиці адресації для назв пристроїв та інформації про адреси.

1. Налаштуйте CustomerRouter.

Встановіть пароль увімкнення секрету на CustomerRouter на Class123

Встановіть пароль входу в консоль на Cisco123.

Налаштуйте CustomerRouter як ім'я хоста для маршрутизатора.

Налаштуйте інтерфейси G0/0 та G0/1 з IP-адресами та масками підмережі, а потім увімкніть їх.

Збережіть поточну конфігурацію у файлі конфігурації запуску.

2. Налаштуйте два комутатори локальної мережі клієнта. Налаштуйте IP-адреси на інтерфейсі VLAN 1 на двох комутаторах локальної мережі клієнта. Переконайтеся, що ви налаштували правильний шлюз за замовчуванням на кожному комутаторі.

3. Налаштуйте інтерфейси ПК. Налаштуйте IP-адресу, маску підмережі та параметри шлюзу за замовчуванням на ПК А та ПК В.

Частина 3. Тестування та усунення несправностей мережі

Визначте, чи може ПК-А зв'язатися зі своїм шлюзом за замовчуванням. Чи отримуєте ви відповідь?

Визначте, чи може ПК-Б зв'язатися зі своїм шлюзом за замовчуванням. Чи отримуєте ви відповідь?

Визначте, чи може ПК-А зв'язатися з ПК-Б. Чи отримуєте ви відповідь?

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 поясненнями.
- 5) Виконання завдання 2 з відповідними скріншотами, розрахунками, відповідями на запитання.
- 6) Висновок.

Контрольні питання:

Яка основна функція мережевого рівня в моделі OSI?

Що таке IP-адреса і чим вона відрізняється від MAC-адреси (фізичної адреси канального рівня)?

Яку роль відіграють маршрутизатори на мережевому рівні?

Що таке «пакет» (packet) на мережевому рівні і яку інформацію містить його заголовок?

Які існують дві основні версії IP-протоколу і в чому їхні ключові відмінності?

Поясніть різницю між публічними (реальними/білими) та приватними (внутрішніми/сірими) IP-адресами.

Що таке підмережа (subnet) і з якою метою здійснюється розподіл мережі на підмережі?

Що таке маска підмережі (subnet mask) і як вона використовується для визначення мережевої частини та частини хоста в IP-адресі?

Як розрахувати максимальну кількість можливих підмереж та кількість придатних для використання IP-адрес хостів у кожній підмережі, ґрунтуючись на масці підмережі?

Задано IP-адресу 192.168.1.0 з маскою підмережі 255.255.255.192 (/26). Яка адреса мережі (network address) та яка широкомовна адреса (broadcast address) для цієї підмережі?

Як визначити, чи знаходяться два хости з певними IP-адресами в одній підмережі?

Для корпоративної мережі потрібна мінімум 5 підмереж, кожна з яких повинна підтримувати щонайменше 20 хостів. Яку маску підмережі слід використати для задоволення цих вимог, виходячи з вихідної мережі класу C (наприклад, 192.168.1.0/24)?

КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 8

Тема: Протоколи канального рівня ЕМВСС.

Мета заняття: Навчитися розрізняти функції концентраторів і комутаторів та базові правила побудови бездротових мереж.

Теоретичні відомості

Протоколи канального рівня ЕМВСС. Канальний рівень моделі OSI відіграє ключову роль у забезпеченні надійної передачі даних між вузлами, які мають безпосереднє фізичне з'єднання. В рамках цього рівня функціонують кілька основних протоколів, кожен з яких має свої специфічні особливості та застосування.

1. Ethernet (стандарт IEEE 802.3). Це домінуючий протокол у локальних мережах, який використовує MAC-адреси для ідентифікації пристроїв. Ethernet підтримує широкий діапазон швидкостей передачі даних, включаючи 10 Мбіт/с, 100 Мбіт/с, 1 Гбіт/с, 10 Гбіт/с і навіть вищі. Для доступу до середовища передавання він застосовує метод CSMA/CD (множинний доступ з контролем несучої частоти і виявленням колізій), що забезпечує ефективну передачу у середовищах із високим рівнем завантаження.

2. Wi-Fi (стандарт IEEE 802.11). Цей протокол спеціалізується на бездротових локальних мережах і реалізує метод доступу CSMA/CA (множинний доступ з уникненням колізій). Стандарти Wi-Fi охоплюють кілька версій, включаючи 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac та 802.11ax, що дозволяє забезпечувати різні показники продуктивності та функціональності залежно від потреб мережі. Протокол також інтегрує механізми шифрування й автентифікації для безпеки передавання даних, зокрема WPA2 та WPA3.

3. PPP (протокол точка-точка). Цей протокол застосовується для організації прямого з'єднання між двома вузлами. Він набув популярності у таких технологіях, як dial-up-з'єднання та VPN, завдяки своїй універсальності. PPP підтримує функції автентифікації користувачів, стиснення даних для

підвищення ефективності передавання інформації, а також забезпечує роботу з кількома протоколами одночасно.

Таким чином, ці протоколи забезпечують різноманітні можливості для передачі даних на каналному рівні з урахуванням специфічних вимог користувачів і характеру мереж.

Протоколи каналного рівня виконують наступні завдання:

кадрування – упаковка даних у кадри з заголовками та трейлерами;

фізична адресація – використання MAC-адрес;

контроль доступу до середовища – регулювання доступу до спільного каналу;

виявлення помилок – використання контрольних сум (CRC);

управління потоком – запобігання перевантаженню приймача.

Ethernet працює на Канальному та Фізичному рівнях. Це сімейство мережних технологій, які визначені в стандартах IEEE 802.2 та 802.3. Протоколи IEEE 802 LAN/MAN, включно з Ethernet, використовують для роботи наступні два окремі підрівні Канального рівня: підрівень керування логічним зв'язком (Logical Link Control, LLC) та підрівень керування доступом до середовища передавання (Media Access Control, MAC), як показано на рис. 8.1.

На Канальному рівні LLC і MAC виконують важливі функції.

Підрівень LLC відповідає за організацію взаємодії між мережним програмним забезпеченням верхніх рівнів і апаратною частиною пристрою на нижчих рівнях. Згідно зі стандартом IEEE 802.2, цей підрівень вставляє у кадр інформацію, яка визначає, який протокол мережевого рівня застосовується до даного кадру. Завдяки цьому кілька протоколів Рівня 3, таких як IPv4 і IPv6, можуть одночасно використовувати один мережевий інтерфейс та спільне середовище передавання даних.

MAC підрівень, реалізований у апаратному забезпеченні відповідно до стандартів, наприклад IEEE 802.3, IEEE 802.11 або IEEE 802.15, виконує функції інкапсуляції даних та керування доступом до середовища передавання. Він забезпечує адресацію на Канальному рівні і тісно інтегрується з різними

технологіями Фізичного рівня, забезпечуючи стабільну взаємодію між компонентами мережі.



Рисунок 8.1 – Канальний рівень

Підрівень MAC. Підрівень MAC відповідає за інкапсуляцію даних і доступ до середовища передавання даних. Інкапсуляція даних IEEE 802.3 включає наступне:

Кадр Ethernet – це внутрішня структура кадру Ethernet.

Адресацію Ethernet. Кадр Ethernet містить як MAC-адресу джерела, так і MAC-адресу призначення, щоб доставити кадр Ethernet від однієї Ethernet NIC до іншої Ethernet NIC в одній локальній мережі.

Виявлення помилок Ethernet. Кадр Ethernet містить трейлер з послідовністю перевірки кадру (Frame Check Sequence, FCS), яка використовується для виявлення помилок.

Підрівень MAC IEEE 802.3 містить специфікації різних комунікаційних стандартів Ethernet для різних типів середовища передавання даних, включно з міддю і оптоволоконном.

Поля кадру Ethernet. Мінімальний розмір Ethernet-кадру становить 64 байти, а максимальний – 1518 байтів. У цю довжину входять усі байти від

поля MAC-адреси одержувача до поля послідовності перевірки кадру (FCS). Поле Преамбула при обчисленні загальної довжини кадру не враховується.

Кадри, розмір яких менший за 64 байти, класифікуються як «фрагменти», які виникають внаслідок колізій, або як «карликові кадри», і автоматично відкидаються приймаючою станцією. З іншого боку, кадри, довжина яких перевищує 1500 байтів, визначаються як «переповнені» або «гігантські». У випадках, коли розмір переданого кадру виходить за межі встановлених мінімальних чи максимальних значень, приймаючий пристрій також відхиляє такі кадри як некоректні. Найчастіше такі відкинуті кадри є результатом колізій або виникнення небажаних сигналів, через що вони кваліфікуються як недійсні. Проте більшість сучасних комутаторів стандартів Fast Ethernet та Gigabit Ethernet, а також мережевих адаптерів підтримують обробку переповнених кадрів.

На рисунку 8.2 показано всі поля кадру Ethernet. Зверніться до таблиці, щоб отримати додаткові відомості про те, яку функцію виконує кожне поле.

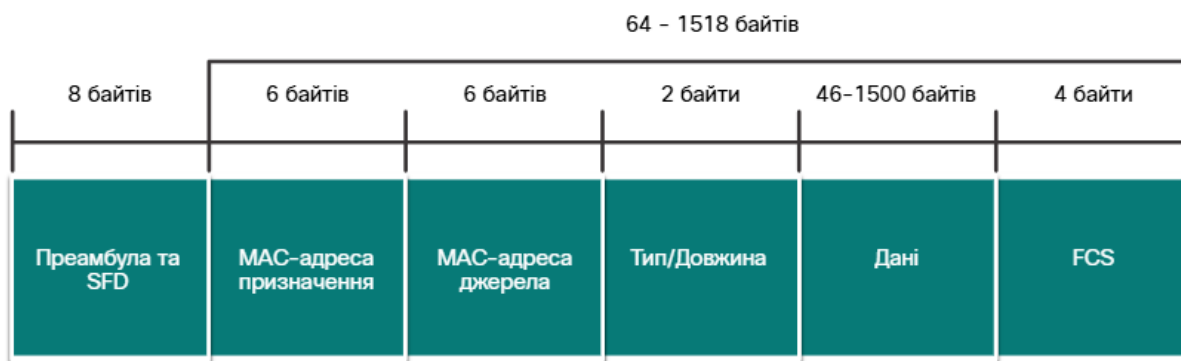


Рисунок 8.2 – Поля кадру Ethernet

В Ethernet для індивідуальної, широкомовної та групової розсилки Рівня 2 використовуються різні MAC-адреси.

Індивідуальна MAC-адреса (unicast) – це унікальна адреса, яка використовується, коли кадр надсилається з одного пристрою-джерела на один пристрій призначення.

Широкомовна адреса – використовується коли кожен пристрій в локальній мережі Ethernet отримує і обробляє широкомовний (broadcast) кадр Ethernet.

Особливості широкомовного кадру Ethernet: має MAC-адресу призначення FF-FF-FF-FF-FF-FF у шістнадцятковому представленні (48 одиниць у двійковому форматі), пересилається на всі порти комутатора Ethernet, окрім вхідного порту, не пересилається маршрутизатором.

У випадку, коли інкапсульовані дані є широкомовним пакетом IPv4, це означає, що адреса призначення IPv4 у такому пакеті складається виключно з одиниць у тій частині, що відповідає за ідентифікацію вузла. Такий формат адресації вказує на те, що пакет буде отриманий і оброблений усіма вузлами, які знаходяться в межах локальної мережі (широкомовного домену).

Групова MAC-адреса. Ethernet-кадр групової (multicast) розсилки отримає і обробить група пристроїв в локальній мережі Ethernet, які належать до однієї групи розсилки.

MAC-адреса призначення 01-00-5E використовується, коли інкапсульовані дані є IPv4-пакетом групової розсилки. MAC-адреса призначення 33-33 використовується, коли інкапсульовані дані є IPv6-пакетом групової розсилки.

Існують інші зарезервовані MAC-адреси для групової розсилки, які використовуються, коли інкапсульовані дані не належать до протоколу IP, а, наприклад, до протоколу Spanning Tree Protocol (STP) або протоколу Link Layer Discovery Protocol (LLDP). Подібний кадр передається через усі порти комутатора Ethernet, за винятком ситуацій, коли комутатор налаштований на обробку групових розсилок через multicast snooping.

Маршрутизатор, у свою чергу, не пересилає подібний кадр, якщо лише він не налаштований на маршрутизацію пакетів групової розсилки. У випадку, якщо інкапсульовані дані є IP-пакетом групової розсилки, пристроям, що входять до такої групи, призначаються IP-адреси з відповідного діапазону. Для IPv4 діапазон адрес групової розсилки становить від 224.0.0.0 до 239.255.255.255. Для IPv6 він починається з ff00::/8. Оскільки адреси групової розсилки представляють сукупність вузлів (іноді їх називають групою вузлів), вони використовуються виключно як адреси призначення в пакеті. Адреса джерела завжди є унікальною.

Як і у випадку з індивідуальними або широкомовними адресами, IP-адреси для групової розсилки потребують відповідних MAC-адрес для доставки кадрів у межах локальної мережі. Групові MAC-адреси пов'язуються з відповідними IPv4- або IPv6-адресами групової розсилки та використовують їхню адресну інформацію.

Основи комутації. Розглянемо, як комутатор використовує MAC-адреси для ефективного пересилання кадрів між пристроями в мережі або їх відкидання. Якщо б комутатор направляв кожен отриманий кадр на всі доступні порти, мережевий трафік був би настільки перевантажений, що функціонування мережі стало б практично неможливим.

Ethernet-комутатор рівня 2 приймає рішення про переадресацію виключно на основі MAC-адрес, не звертаючи уваги на дані всередині кадру або використовуваний протокол, такі як IPv4-пакети, ARP-запити чи ND-пакети IPv6. Всі дії комутатора обмежуються аналізом Ethernet MAC-адрес рівня 2.

Ключовою функцією Ethernet-комутатора є використання таблиці MAC-адрес для визначення, на який порт переслати певний кадр. Це принципово відрізняється від роботи застарілих концентраторів Ethernet, які просто повторювали отримані біти на всі порти, за виключенням того, через який кадр був отриманий.

Вивчення MAC-адрес і переадресація. Комутатор автоматично створює таблицю MAC-адрес, аналізуючи джерела кадрів, які надходять на його порти. Пересилання кадрів здійснюється шляхом перевірки відповідності між MAC-адресою призначення у кадрі та записами в таблиці MAC-адрес.

Фільтрування кадрів. Комутатор, отримуючи кадри від різних пристроїв, здатен автоматично заповнювати таблицю MAC-адрес, аналізуючи MAC-адреси джерела кожного отриманого кадру. У разі, якщо таблиця вже містить MAC-адресу призначення, комутатор може здійснити фільтрацію кадру та передати його через відповідний порт.

Коли пристрій призначення має IP-адресу у віддаленій мережі, передача Ethernet-кадру безпосередньо на цю адресу неможлива. У таких випадках кадр

пересилається за MAC-адресою шлюзу за замовчуванням, тобто маршрутизатора, який виконує роль посередника для подальшого маршруту.

Концентратор (Hub) є пристроєм фізичного рівня (Layer 1), що забезпечує об'єднання кількох мережевих пристроїв у одну Ethernet-мережу. Його дія схожа на багатопортовий повторювач, адже він дублює сигнали, отримані на одному порту, й розподіляє їх по інших портах без розуміння змісту даних.

Натомість комутатор (Switch) – це активний мережевий пристрій канального рівня (Layer 2), який виконує з'єднання пристроїв в локальній мережі з більшою ефективністю та точністю завдяки можливості адресної передачі даних між ними та *інтелектуально пересилає кадри на основі MAC-адрес*. Комутатор є еволюцією концентратора та вирішує його основні проблеми.

Налаштування бездротового зв'язку. На рисунку 8.3 показано інтерфейс базових налаштувань бездротового зв'язку Packet Tracer. На бездротових маршрутизаторах, що використовують стандарти 802.11, потрібно налаштувати декілька параметрів.

Мережевий режим. Протокол 802.11 здатний забезпечити підвищену пропускну здатність у бездротовому мережевому середовищі. Якщо всі пристрої в мережі підключені на основі одного стандарту 802.11, можна досягти максимальних швидкостей для цього стандарту. У випадках, коли точка доступу налаштована виключно на прийом конкретного стандарту 802.11, пристрої, що використовують інші стандарти, не зможуть підключатися до такої точки доступу.

У змішаному режимі бездротова мережа підтримує пристрої з різними стандартами Wi-Fi, надаючи можливість підключення навіть для застарілих пристроїв, які потребують доступу до бездротової мережі, але не сумісні з новими стандартами.

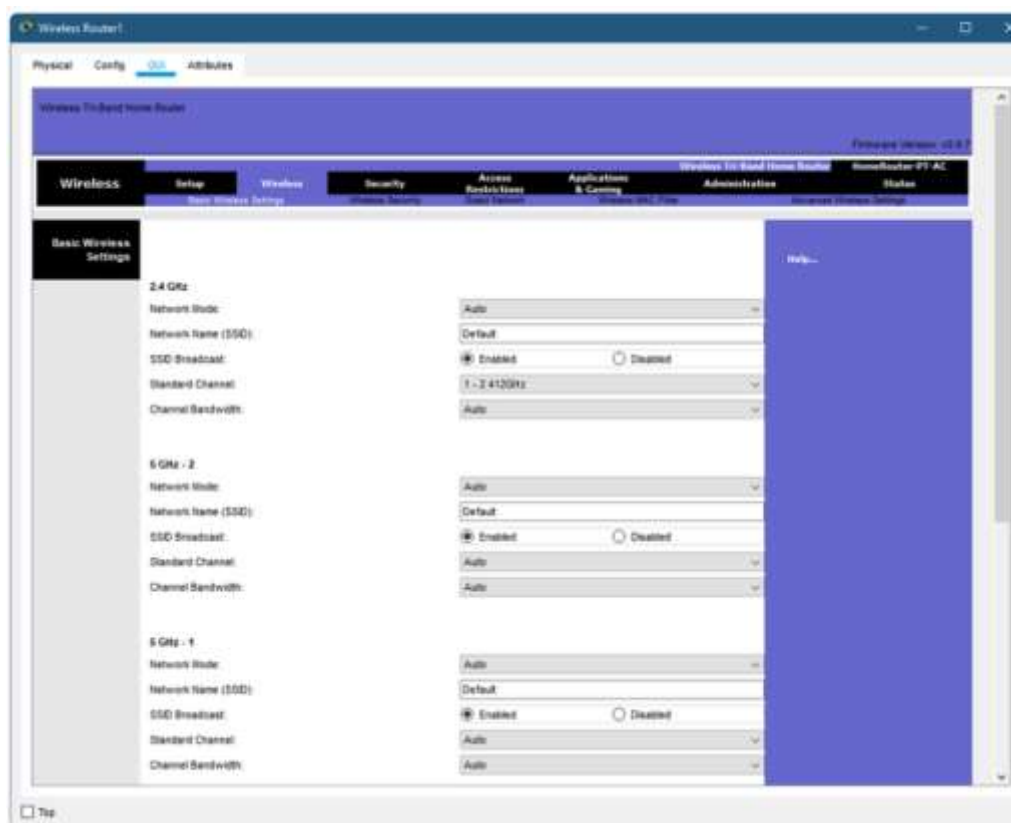


Рисунок 8.3 – Базові налаштування бездротового зв'язку Packet Tracer

Під час створення бездротової мережі важливо, щоб усі компоненти були належним чином підключені до відповідної WLAN-мережі. Для цього застосовується SSID.

SSID є алфавітно-цифровим ідентифікатором довжиною до 32 символів, чутливим до регістру. Цей ідентифікатор передається в заголовках усіх кадрів, що надходять через WLAN-мережу. Він допомагає повідомити бездротовим станціям (STA), до якої мережі вони належать та з якими іншими пристроями можуть обмінюватися даними.

SSID використовується для визначення конкретної бездротової мережі, фактично представляючи її назву. Як правило, маршрутизатори за замовчуванням транслюють свої SSID, дозволяючи пристроям легко знаходити й автоматично визначати ім'я мережі. Якщо ж трансляція SSID вимкнена, користувачам доведеться вводити ідентифікатор вручну.

Відключення трансляції SSID може ускладнити процес підключення для клієнтів, які мають право приєднуватися до мережі. Однак це не є достатнім

заходом для запобігання доступу сторонніх осіб. Для ефективного захисту бездротових мереж необхідно застосовувати максимально надійне шифрування, яке обмежує несанкціонований доступ.

Виконання комп'ютерного практикуму

Завдання 1. Відкрити файл Завдання 1_ЛР8.rka. Здійснити налаштування бездротового маршрутизатора та клієнта.

Частина 1. Під'єднання пристроїв

1. Під'єднайте коаксіальні кабелі. Для цього:

У Network Components натисніть Connections (блискавка).

Знайдіть і клацніть піктограму Coaxial. Це піктограма з блакитним зигзагом.

Клацніть Cable Splitter і виберіть порт Coaxial1.

Натисніть Cable Modem і виберіть Port 0.

Повторіть попередні кроки, щоб приєднати Coaxial2 на Cable Splitter до порту Port 0 на TV.

Клацніть TV, а потім натисніть ON для Status. Якщо ваші з'єднання виконано правильно, на екрані з'явиться зображення, яке відображатиме телевізійну програму.

2. Під'єднайте мережні кабелі.

Клацніть Connections, потім Copper Straight-Through кабель. Він виглядає як суцільна чорна лінія.

Приєднайте Port 1 на Cable Modem до Internet порту Home Wireless Router.

Клацніть Office PC і приєднайте кабель до порту FastEthernet0. Знайдіть Home Wireless Router і клацніть на ньому. Приєднайте інший кінець кабелю до порту GigabitEthernet 1, щоб завершити з'єднання.

Повторіть попередні кроки, щоб приєднати Bedroom PC до порту GigabitEthernet 2 на Home Wireless Router.

Дротова домашня мережа тепер повністю приєднана до інтернету через мережу провайдера кабельного телебачення.

Частина 2: Налаштування бездротового маршрутизатора

1. Доступ до графічного інтерфейсу домашнього бездротового маршрутизатора.

Клацніть Office PC > Desktop, а потім IP Configuration.

Натисніть DHCP. DHCP автоматично налаштує Office PC для роботи в тій самій IP-мережі, що й Home Wireless Router.

Після невеликої затримки значення для IP Configuration мають автоматично оновлюватися. Адреса IPv4 повинна починатися з числа 192. Якщо цього не сталося, клацніть Fast Forward Time під топологією мережі в нижньому лівому куті. Це прискорить симуляцію DHCP.

Занотуйте адресу шлюзу за замовчуванням. Шлюз за замовчуванням – це пристрій, який надає пристроям у домашній мережі доступ до зовнішніх мереж, наприклад інтернету. У цьому випадку адресою шлюзу за замовчуванням буде адреса Home Wireless Router.

У відкритому вікні Office PC, закрийте вікно IP Configuration, а потім клацніть Web Browser. Введіть IP-адресу Home Wireless Router (адреса шлюзу за замовчуванням) у поле URL та натисніть Go.

Щойно встановлені домашні маршрутизатори налаштовані з обліковими даними за замовчуванням. Введіть admin як User Name та Password.

2. Налаштуйте базові параметри.

Знайдіть область Network Setup. Знайдіть поле Maximum Number of Users і введіть 10. Прокрутіть донизу сторінки та натисніть Save Settings. Треба зберігати налаштування на кожній сторінці графічного інтерфейсу користувача, яку змінюєте.

Натисніть вкладку Administration. Введіть і підтвердьте MyPassword1! як новий пароль. Прокрутіть донизу сторінки та натисніть Save Settings.

Буде запропоновано увійти знову. Введіть admin як ім'я користувача та MyPassword1! як новий пароль і натисніть Continue.

3. Налаштувати бездротову локальну мережу.

Прокрутіть назад до верхньої частини вікна, а потім натисніть вкладку Continue.

Для мережі 2,4 ГГц натисніть Enable, щоб активувати мережне радіо.

Змініть ідентифікатор Network Name (SSID) з Default на MyHome. Прокрутіть донизу сторінки та натисніть Save Settings.

Прокрутіть назад до верхньої частини вікна, а потім клацніть Wireless Security на вкладці Wireless.

Натисніть спадне меню для мережі 2,4 ГГц і виберіть WPA2 Personal. Це найнадійніший захист, який пропонує цей маршрутизатор для бездротових мереж.

З'явиться більше налаштувань. Для WPA2 Personal потрібна парольна фраза, яку має ввести кожен, хто хоче приєднатися до бездротової мережі. Введіть MyPassPhrase1! як Passphrase. Зауважте, що використання великих літер є важливим.

Прокрутіть сторінку донизу та клацніть Save Settings, а потім закрийте Web Browser для офісного ПК.

Частина 3. Налаштування IP-адреси та перевірка зв'язку

1. Під'єднайте ноутбук до бездротової мережі.

Натисніть на Laptop, розміщеному у вітальні, далі перейдіть на вкладку Desktop > PC Wireless.

Відкрийте вкладку Connect. Після невеликої затримки бездротова мережа, яку ви налаштували раніше, має з'явитися у списку назв бездротових мереж.

Клацніть назву мережі, яку ви створили, а потім натисніть кнопку Connect.

Введіть парольну фразу, яку раніше налаштували для бездротової мережі, у полі Pre-shared Key, а потім натисніть Connect.

Натисніть вкладку Link Information. Повинно з'явитися повідомлення, що підтверджує успішне під'єднання до точки доступу: You have successfully connected to the access point.

Натисніть кнопку More Information, щоб переглянути докладну інформацію про з'єднання. Якщо IP-адреса не починається з 192, клацніть Fast Forward Time кілька разів, щоб пришвидшити процес.

Закрийте програму PC Wireless та виберіть Web Browser. Переконайтеся, що Laptop тепер може приєднатися до skillsforall.srv, натискаючи Fast Forward Time, доки сторінка не завантажиться. Це підтверджує, що Laptop приєднаний до інтернету.

2. Перевірте під'єднання з офісним ПК.

Перейдіть на вкладку Office PC > Desktop > Web Browser.

Введіть skillsforall.srv і натисніть Go. Після невеликої затримки ви повинні побачити веб-сторінку. Якщо потрібно, клацніть Fast Forward Time кілька разів, щоб прискорити процес.

Під час завантаження зовнішнього веб-сайту перевіряється зв'язок з Інтернетом для Office PC.

3. Налаштуйте комп'ютер, розміщений у спальні.

Для Bedroom PC відкрийте IP Configuration і встановіть значення DHCP. Переконайтеся, що Bedroom PC отримав IP-адресу, яка починається з 192.

Закрийте вікно IP Configuration та відкрийте Web Browser. Переконайтеся, що комп'ютер Bedroom PC тепер може приєднуватися до skillsforall.srv, натискаючи Fast Forward Time, доки сторінка не завантажиться. Це підтверджує, що Bedroom PC має з'єднання з інтернетом.

Завдання 2. Відкрити файл Завдання 2_LP8.pka. Перевірити NAT на бездротовому маршрутизаторі.

1. Перевірка конфігурації для доступу до зовнішньої мережі.

Додайте один ПК і під'єднайте його до бездротового маршрутизатора за допомогою прямого кабелю. Зачекайте, коли всі індикатори стануть зеленими, перш ніж перейти до наступного кроку або натисніть Fast Forward.

На ПК, натисніть Desktop. Виберіть IP Configuration. Натисніть DHCP, щоб кожен пристрій міг отримувати IP-адресу через DHCP на бездротовому маршрутизаторі.

Зверніть увагу на IP-адресу шлюзу за замовчуванням. Закрийте IP Configuration, коли закінчите.

Перейдіть до веббраузера і введіть IP-адресу шлюзу за замовчуванням у полі URL-адреси. Введіть ім'я користувача admin і пароль admin, коли з'явиться відповідний запит.

Натисніть вкладку Status у меню у верхньому правому куті. Після вибору відображається сторінка підменю Router.

Прокрутіть сторінку маршрутизатора донизу до опції підключення до інтернету. Вказана тут IP-адреса – це адреса, призначена провайдером. Якщо IP-адреса відсутня (відображається 0.0.0.0), закрийте вікно, зачекайте декілька секунд і спробуйте ще раз. Бездротовий маршрутизатор перебуває в процесі отримання IP-адреси від ISP DHCP-сервера.

Адреса, яку ми бачимо тут, – це адреса, призначена інтернет-порту бездротового маршрутизатора.

2. Перевірка налаштувань для доступу до внутрішньої мережі.

Натисніть вкладку Local Network в рядку підменю Status.

Прокрутіть донизу, щоб переглянути інформацію про локальну мережу. Це адреса, що призначена внутрішній мережі.

Прокрутіть далі донизу, щоб переглянути інформацію про сервер DHCP та діапазон IP-адрес, які можна призначити підключеним хостам.

Закрийте вікно налаштування бездротового маршрутизатора.

3. Під'єднання трьох ПК до бездротового маршрутизатора.

Додайте ще три ПК та під'єднайте їх до бездротового маршрутизатора за допомогою прямих кабелів. Зачекайте, коли всі індикатори стануть зеленими, перш ніж перейти до наступного кроку або натисніть Fast Forward.

На кожному комп'ютері натисніть Desktop. Виберіть IP Configuration. Натисніть DHCP, щоб кожен пристрій міг отримувати IP-адресу через DHCP на бездротовому маршрутизаторі. Закрийте IP Configuration, коли закінчите.

Натисніть піктограму Command Prompt для того, щоб перевірити на кожному ПК конфігурацію IP, використовуючи команду ipconfig /all.

4. Перегляд функціонування NAT через бездротовий маршрутизатор.

Ввійдіть в режим моделювання, натиснувши вкладку Simulation в правому нижньому кутку. Вкладка Simulation розташована позаду вкладки Realtime та має символ секундоміра.

Перегляньте трафік шляхом створення блоку Complex PDU в режимі Simulation:

На Simulation Panel, натисніть Show All/None, щоб перетворити видимі дії на невидимі. Тепер натисніть Edit Filters і під вкладкою Misc встановіть прапорці для TCP та HTTP. Після завершення закрийте вікно.

Додайте Complex PDU, натиснувши на відкритий конверт, розташований у верхньому меню.

Клацніть на одному з ПК, щоб вказати його як джерело.

Вкажіть параметри комплексного PDU, змінивши наступні у вікні складного PDU:

У розділі PDU Settings для параметра Select Application має бути встановлено значення HTTP.

Натисніть на ciscolearn.nat.com сервер, щоб вказати його як пристрій призначення.

Для Source Port, введіть 1000.

У розділі Simulation Settings виберіть Periodic. Введіть 120 секунд для Interval.

Натисніть Create PDU у вікні Create Complex PDU.

Двічі клацніть на панелі моделювання, щоб розблокувати у вікні PT. Це дозволяє перемістити панель моделювання для перегляду всієї топології мережі.

Спостерігайте за потоком трафіку, натиснувши кнопку Play на панелі моделювання. Пришвидшіть анімацію, пересунувши повзунок керування відтворенням праворуч.

5. Перегляд інформації у заголовках пакетів, які передавалися мережею.

Перевірте заголовки пакетів, що надсилаються між ПК та вебсервером.

На Simulation Panel двічі клацніть третій рядок внизу у списку подій. У робочій області з'явиться конверт, який представляє цю лінію.

Клацніть конверт у вікні робочої області, щоб переглянути інформацію про пакет та заголовки.

Перейдіть на вкладку Inbound PDU details. Ознайомтеся з інформацією про пакет для IP-адреси джерела (SRC) та IP-адреси призначення.

Перейдіть на вкладку Outbound PDU details. Ознайомтеся з інформацією про пакет для IP-адреси джерела (SRC) та IP-адреси призначення.

Зверніть увагу на зміну IP-адреси SRC.

Натискайте інші рядки подій, щоб переглянути ці заголовки протягом усього процесу.

Закінчивши, натисніть Check Results, щоб перевірити свою роботу.

Завдання 3. Відкрити файл Завдання 3_LP8.pka. Здійснити підключення дротової та бездротової локальної мережі.

Частина 1. Підключення до хмари

1. Підключіть хмару до Router0.

Внизу ліворуч натисніть на значок помаранчевої блискавки, щоб відкрити доступні підключення.

Виберіть правильний кабель для підключення Router0 F0/0 до Cloud Eth6. Cloud – це тип комутатора, тому використовуйте мідне пряме з'єднання. Якщо підключили правильний кабель, індикатори з'єднання на кабелі засвітяться зеленим.

2. Підключіть хмару до кабельного модему.

Виберіть правильний кабель для підключення Cloud Coax7 до порту модему 0.

Якщо підключили правильний кабель, індикатори з'єднання на кабелі засвітяться зеленим.

Частина 2. Підключити Router0

1. Підключити Router0 до Router1.

Виберіть правильний кабель для підключення Router0 Ser0/0/0 до Router1 Ser0/0. Використовуйте один із доступних послідовних кабелів.

Якщо ви підключили правильний кабель, індикатори з'єднання на кабелі засвітяться зеленим.

2. Підключити Router0 до netacad.pka.

Виберіть правильний кабель для підключення Router0 F0/1 до netacad.pka F0. Маршрутизатори та комп'ютери традиційно використовують одні й ті ж дроти для передачі (1 та 2) та отримання (3 та 6). Правильний кабель складається з цих перехрещених проводів. Хоча багато мережевих карт тепер можуть автоматично визначати, яка пара використовується для передачі та отримання, Router0 та netacad.pka не мають мережевих карт з автоматичним визначенням.

Якщо ви підключили правильний кабель, індикатори з'єднання на кабелі засвітяться зеленим.

3. Підключити Router0 до терміналу конфігурації.

Виберіть правильний кабель для підключення консолі Router0 до терміналу конфігурації RS232. Цей кабель не забезпечує мережевий доступ до терміналу конфігурації, але дозволяє налаштувати Router0 через його термінал.

Якщо ви підключили правильний кабель, індикатори з'єднання на кабелі засвітяться чорним.

Частина 3. Підключення решти пристроїв

1. Підключіть Router1 до комутатора.

Виберіть правильний кабель для підключення Router1 F1/0 до комутатора F0/1.

Якщо ви підключили правильний кабель, індикатори з'єднання на кабелі засвітяться зеленим. Зачекайте кілька секунд, поки світло перейде з жовтого на зелений.

2. Підключіть кабельний модем до бездротового маршрутизатора.

Виберіть правильний кабель для підключення порту 1 кабельного модему до інтернет-порту бездротового маршрутизатора.

Якщо підключили правильний кабель, індикатори з'єднання на кабелі засвітяться зеленим.

3. Підключить бездротовий маршрутизатор до сімейного ПК.

Виберіть правильний кабель для підключення бездротового маршрутизатора Ethernet 1 до сімейного ПК.

Якщо підключили правильний кабель, індикатори з'єднання на кабелі засвітяться зеленим.

Частина 4. Перевірка з'єднань

1. Перевірте з'єднання від сімейного ПК до netacad.pka.

Відкрийте командний рядок сімейного ПК та виконайте команду `ping netacad.pka`.

Відкрийте веб-браузер та веб-адресу `http://netacad.pka`.

2. Перевірте комутатор командою `ping` з домашнього ПК.

Відкрийте командний рядок домашнього ПК та перевірте IP-адресу комутатора командою `ping`, щоб перевірити з'єднання.

3. Відкрийте Router0 з терміналу конфігурації.

Відкрийте термінал терміналу конфігурації та прийміть налаштування за замовчуванням.

Натисніть Enter, щоб переглянути командний рядок Router0.

Введіть `show ip interface brief`, щоб переглянути стани інтерфейсу.

Частина 5. Перевірка фізичної топології

1: Перевірка хмари. Перейдіть на вкладку «Фізичний робочий простір» або натисніть Shift+P та Shift+L, щоб перемикатися між логічним та фізичним робочими просторами.

Натисніть значок «Домашнє місто».

Натисніть значок «Хмара».

2. Перевірте основну мережу. Натисніть значок «Основна мережа». Наведіть курсор миші на різні кабелі.

Натисніть «Назад», щоб повернутися до розділу «Домашнє місто».

3. Перевірте вторинну мережу. Натисніть значок вторинної мережі. Наведіть курсор миші на різні кабелі. Натисніть «Назад», щоб повернутися до розділу «Домашнє місто».

4. Перевірте домашню мережу. Натисніть значок домашньої мережі. Натисніть вкладку «Логічний робочий простір», щоб повернутися до логічної топології.

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.
- 6) Виконання завдання 2 з відповідними скріншотами.
- 6) Виконання завдання 3 з відповідними скріншотами.
- 7) Висновок.

Контрольні питання:

Яка основна функція канального рівня в моделі OSI?

Яку назву мають одиниці даних (PDU) на канальному рівні?

Які дві основні підрівні складають канальний рівень згідно зі стандартом IEEE 802, і за що відповідає кожен з них?

У чому полягає процес інкапсуляції на канальному рівні? Які елементи додаються до пакету мережевого рівня?

Який протокол використовується для перетворення IP-адреси в MAC-адресу в локальній мережі?

Які обмеження має канальний рівень у порівнянні з мережевим рівнем?

Назвіть поширені протоколи канального рівня та опишіть їх основні сфери застосування.

Який пристрій працює на канальному рівні та використовує MAC-адреси для пересилання кадрів у межах локальної мережі?

КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 9

Тема: Робота з командним рядком та конфігураційними файлами

Мета заняття: Освоїти команди конфігурації пристрою через командний рядок та їх збереження у файл.

Теоретичні відомості

За допомогою командного інтерфейсу Cisco IOS можна налаштовувати пристрій і переглядати поточний стан його роботи. Більшість мережевих пристроїв Cisco мають подібний інтерфейс, що забезпечує однаковий користувацький досвід. Після завершення процесу завантаження маршрутизатора і появи запиту Router> у командному рядку доступний ввід команд Cisco IOS. Для управління функціями пристрою Cisco IOS пропонує два окремі режими роботи з командами.

Перший – це користувацький режим EXEC (User EXEC), який обмежений у своїх можливостях, але підходить для виконання базових операцій. У цьому режимі можна використовувати лише основні команди для моніторингу, тоді як внесення змін до конфігурації пристрою недоступне. Користувацький режим EXEC можна розпізнати за символом >, що завершує командний рядок.

Другий режим – привілейований EXEC (Privileged EXEC), який необхідний для виконання більш складних адміністративних команд, включаючи налаштування конфігурації. Доступ до привілейованого режиму є обов'язковим для мережевих адміністраторів, оскільки тільки через цей рівень можна отримати доступ до інших режимів, таких як глобальна конфігурація. Привілейований режим EXEC відрізняється закінченням командного рядка символом #.

Основні етапи налаштування комутатора. Перед підключенням до мережі, комутатор Cisco слід попередньо налаштувати, забезпечивши базові параметри безпеки. До ключових елементів конфігурації комутатора локальної мережі зазвичай входять призначення імені хоста, встановлення IP-адреси для управління, налаштування паролів і внесення описової інформації.

Ім'я хоста комутатора – це налаштоване ім'я пристрою. Подібно до того, як кожному комп'ютеру чи принтеру присвоюється назва, для мережевого обладнання також необхідно задавати унікальне ім'я з описом. Дуже зручно, якщо в назві пристрою зазначено місце його розташування. Наприклад: SW_Room_155.

IP-адреса управління необхідна, якщо планується налаштовувати або керувати комутатором через внутрішньосмугове з'єднання в мережі. Вона дає змогу отримати доступ до пристрою за допомогою протоколів Telnet, SSH або HTTP. Для цього на комутаторі слід налаштувати параметри IP-адресації, аналогічні до тих, що використовуються на комп'ютері: IP-адреса, маска підмережі та шлюз за замовчуванням. Щоб гарантувати безпеку комутатора Cisco у локальній мережі, важливо встановити паролі для кожного способу доступу до командного рядка. Мінімально рекомендовано задати паролі для таких методів віддаленого підключення, як Telnet, SSH, а також для консольного доступу.

Як правило, процес налаштуванням комутатора наступний (рисунок 9.1).

Налаштуйте назву пристрою.

```
hostname name
```

Захистіть доступ до користувацького режиму EXEC.

```
line con 0
```

```
password password
```

```
login
```

Захистіть віддалений доступ до Telnet / SSH.

```
line vty 0 15
```

```
password password
```

```
login
```

Захистіть доступ до привілейованого режиму EXEC.

```
enable secret password
```

Захистіть усі паролі у файлі конфігурації.

service password-encryption

Встановіть банер з попередженням щодо обмеженого доступу.

banner motd delimiter message delimiter

Налаштуйте управління SVI.

interface vlan 1

ip address ip-address subnet-mask

no shutdown

Збережіть налаштування.

copy running-config startup-config

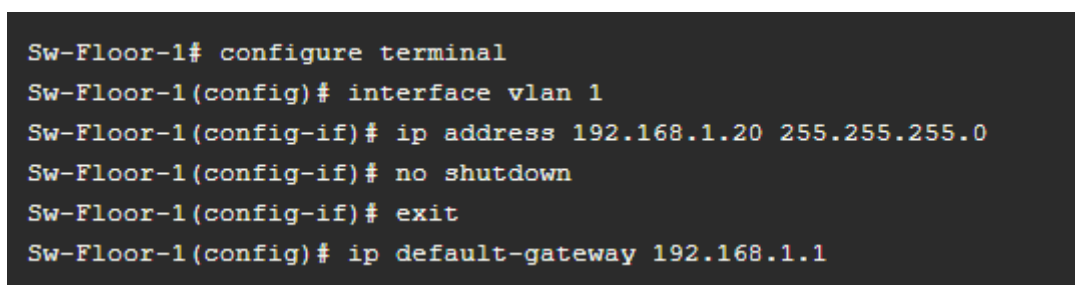
```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# enable secret class
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)# service password-encryption
S1(config)# banner motd #No unauthorized access allowed!#
S1(config)# interface vlan1
S1(config-if)# ip address 192.168.1.20 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Рисунок 9.1 – Налаштування комутатора

Налаштування віртуального інтерфейсу комутатора. Для забезпечення віддаленого доступу до комутатора необхідно налаштувати IP-адресу та маску підмережі на його віртуальному інтерфейсі (SVI). Для цього використовується команда глобального режиму конфігурації `interface vlan 1`. Важливо зазначити,

що VLAN 1 є віртуальним, а не фізичним інтерфейсом. Після цього потрібно призначити адресу IPv4 за допомогою команди конфігурації інтерфейсу `ip address ip-address subnet-mask`. Завершальним кроком є активація віртуального інтерфейсу через команду конфігурації `no shutdown`. Застосувавши ці команди, комутатор отримує всі необхідні налаштування для роботи з IPv4 у межах локальної мережі.

Як і у випадку з операційною системою Windows, комутатори із здатною IP-адресою часто вимагають визначення шлюзу за замовчуванням. У цих умовах використовується команда глобальної конфігурації `ip default-gateway ip-address`, де `ip-address` є IP-адресою локального маршрутизатора, що є шлюзом у мережі, як показано на рисуюнок 9.2.



```

Sw-Floor-1# configure terminal
Sw-Floor-1(config)# interface vlan 1
Sw-Floor-1(config-if)# ip address 192.168.1.20 255.255.255.0
Sw-Floor-1(config-if)# no shutdown
Sw-Floor-1(config-if)# exit
Sw-Floor-1(config)# ip default-gateway 192.168.1.1

```

Рисуюнок 9.2 – Команда глобальної конфігурації `ip default-gateway`

Основні етапи налаштування маршрутизатора. Процес встановлення початкових налаштувань на маршрутизаторі.

1. Налаштування назви пристрою.

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

2. Захист доступу до привілейованого режиму EXEC.

```
Router(config)# enable secret password
```

3. Захист доступу до користувацького режиму EXEC.

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

```
Router(config-line)# password password
```

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

4. Захист віддаленого доступу до Telnet / SSH.

```
Router(config-line)# line vty 0 4
```

```
Router(config-line)# password password
```

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

```
Router(config-line)# transport input {ssh | telnet | none | all}
```

5. Захистіть усі паролі у файлі конфігурації.

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

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

6. Налаштування попередження щодо обмеженого доступу.

```
Router(config)# banner motd delimiter message delimiter
```

7. Збережіть налаштування.

Усі методи доступу до маршрутизатора мають бути належним чином захищені, оскільки вони є ключовими точками входу для управління пристроєм. Режим привілеїв EXEC забезпечує користувачу повний контроль над маршрутизатором, включаючи можливість змінювати його конфігурацію, у зв'язку з чим цей рівень доступу потребує особливої уваги в забезпеченні безпеки.

Для захисту доступу до режимів користувача та привілеїв EXEC, віддалених підключень через Telnet та SSH, а також для шифрування всіх відкритих паролів (як для консолі, так і для ліній VTY), слід використовувати команди, наведені на рисунок 9.3. Особливо важливо обрати складний і надійний пароль для захисту привілейованого режиму EXEC, оскільки компрометація цього рівня доступу може призвести до несанкціонованого втручання у конфігурацію пристрою.

```

R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#

```

Рисунок 9.3 – Захистити доступу до привілейованого і користувацького режимів EXEC

Банерне сповіщення попереджає користувачів про те, що до пристрою мають доступ лише уповноважені користувачі. Банер з попередженням щодо обмеженого доступу налаштовується наступним чином (рис. 9.4):

```

R1(config)# banner motd #
Enter TEXT message. End with the character '#'.
*****
WARNING: Unauthorized access is prohibited!
*****
R1(config)#

```

Рис. 9.4. Налаштування банеру з попередженням

Якщо маршрутизатор було налаштовано за допомогою попередніх команд і він випадково втратив живлення, конфігурація маршрутизатора буде втрачена. Тому важливо зберегти конфігурацію при впровадженні змін. Наступна команда зберігає конфігурацію у NVRAM (рисунок 9.5):

```

R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

```

Рисунок 9.5 –Збереження конфігурації в файл

Виконання комп'ютерного практикуму

Завдання 1. Відкрити файл Завдання 1_ЛР9.pka. Здійснити налаштування пристроїв в мережі, записати конфігурацію в файл.

1. Визначення схеми IP-адресації.

Розробіть схему адресації IPv4 та заповніть таблицю адресації на основі наступних вимог.

Розділіть мережу 192.168.1.0/24 на підмережу, щоб забезпечити 30 адрес хостів на підмережу, витрачаючи при цьому найменшу кількість адрес.

Призначте четверту підмережу локальній мережі першого поверху.

Призначте останню адресу хоста мережі (найвищу) у цій підмережі інтерфейсу G0/0 у будівлі 1.

Починаючи з п'ятої підмережі, знову розділіть мережу на підмережу, щоб нові підмережі надавали 14 адрес хостів на підмережу, витрачаючи при цьому найменшу кількість адрес.

Призначте другу з цих нових підмереж із 14 хостами локальній мережі другого поверху.

Призначте останню адресу хоста мережі (найвищу) у підмережі локальної мережі другого поверху інтерфейсу G0/1 маршрутизатора будівлі 1.

Призначте передостанню адресу (другу за величиною) у цій підмережі інтерфейсу VLAN 1 комутатора другого поверху.

Налаштуйте адреси на хостах, використовуючи будь-які з решти адрес у відповідних підмережах.

2. Налаштування адресації хостів

Використовуйте адресацію IPv4 з кроку 1 та значення адресації IPv6, надані в таблиці адресації, щоб налаштувати всі хост-ПК з правильною адресацією.

Використовуйте локальну адресу інтерфейсу маршрутизатора як шлюзи IPv6 за замовчуванням на хостах.

Завершіть налаштування сервера, використовуючи значення адресації IPv4 з кроку 1 та значення в таблиці адресації.

3. Налаштуйте маршрутизатор Building-1.

Налаштуйте маршрутизатор Building-1 з усіма початковими конфігураціями, які ви вивчили у роботі:

Налаштуйте ім'я хоста маршрутизатора: Building-1

Захистіть конфігурації пристроїв від несанкціонованого доступу за допомогою зашифрованого привілейованого пароля exes.

Захистіть усі лінії доступу до маршрутизатора, використовуючи методи, розглянуті в комп'ютерних практикумах.

Введені паролі мають мати мінімальну довжину 10 символів.

Запобігти перегляду всіх паролів у відкритому тексті у файлах конфігурації пристрою.

Налаштувати маршрутизатор на прийняття лише внутрішньосмугових підключень керування через протокол, який є безпечнішим за Telnet. Використовуйте значення 1024 для надійності ключа шифрування.

Налаштувати локальну автентифікацію користувача для внутрішньосмугових підключень керування. Створити користувача з іменем netadmin та секретним паролем Cisco_CCNA7.

Налаштувати два інтерфейси Gigabit Ethernet, використовуючи розраховані вами значення адресації IPv4 та значення IPv6, надані в таблиці адресації.

Переналаштувати локальні адреси з'єднання на значення, показане в таблиці.

Зберегти файл конфігурації.

4. Налаштування комутатора другого поверху.

Налаштування комутатора другого поверху для віддаленого керування через Telnet.

Налаштувати VLAN 1 як SVI.

Налаштуйте адресацію IPv4 відповідно до вашої роботи, виконаної на кроці 1.

Переконайтеся, що комутатор може приймати з'єднання від хостів в інших мережах.

Перевірить функціональність мережі після налаштування пристроїв.

Надайте всі проведені розрахунки.

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, розрахунками, командами та поясненнями.

7) Висновок.

Контрольні питання:

Які існують основні режими роботи в Cisco IOS, і як між ними переміщуватися?

Яка команда використовується для перегляду поточної активної конфігурації пристрою?

Яка команда використовується для збереження поточної конфігурації в енергонезалежну пам'ять (NVRAM) після внесення змін?

Опишіть послідовність команд для налаштування IP-адреси та маски підмережі на інтерфейсі маршрутизатора (наприклад, GigabitEthernet 0/1) та його активації.

Які команди потрібні для створення нової VLAN (наприклад, VLAN 10) на комутаторі та присвоєння їй імені?

Яка команда використовується для перегляду поточної конфігурації VLAN на комутаторі? Яка команда використовується для налаштування статичного маршруту до віддаленої мережі?

Яка команда використовується для перегляду таблиці маршрутизації маршрутизатора Cisco?

Опишіть команди, необхідні для налаштування віддаленого доступу до пристрою через SSH (безпечніше, ніж Telnet).

ЛІТЕРАТУРА

1. Комп'ютерні мережі. Частина 1 Навчальний посібник. [Електронний ресурс]: навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології», спеціалізації «Інженерія програмного забезпечення інформаційно управляючих систем» та «Інформаційне забезпечення робототехнічних систем»/ Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 8,6 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.
2. Ролік О.І. Моделювання управління потоками даних в корпоративних ІР-мережах/ О.І. Ролік, Ю.М. Пошак, М.А. Никоненко, А.В. Мельник // Адаптивні системи автоматичного управління. Міжвідомчий наук.-техн. зб. – Дніпропетровськ: Системні технології, 2011.– Вип.18(38).– С. 94–103.
3. Теленик С.Ф., Ролік О.І., Ясочка М.В., Голоднов К.О. Аналіз підходів до визначення впливу неполадок елементів мережі доступу на якість обслуговування клієнтів // Вісник Вінницького політехнічного інституту. – 2011. – №3. – С. 69–83.
4. O. Rolik, V. Kolesnik, and V. Barna. “Network traffic monitoring system for the quality of service control” in Proc. of the International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). – Odessa, Ukraine. – 2017. – pp. 1–6.
5. O. Rolik, E. Zharikov, M. Yasochka, M. Butenko “The Method Of Impact Analysis For Access Networks With RIP And OSPF Protocols” 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), 10-14 Sept. 2018. — Odessa, Ukraine. – 2018. – pp. 1–7.
6. Learning Path: CCNA Enterprise Infrastructure (200-301) CCNAv1.1. URL: <https://www.networkacademy.io/ccna>
7. CCNA: Introduction to Networks. URL: <https://www.netacad.com/courses/ccna-introduction-networks>