МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

КОМП'ЮТЕРНІ МЕРЕЖІ

Частина 2

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДЛЯ ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

Житомир
2023

УДК 681.324
К63

Рекомендовано до друку науково-методичною радою
Державного університету «Житомирська політехніка»
(протокол № 12 від 25 грудня 2023 року)

Рецензенти:
Ю.М. Россінський – кандидат технічних наук, доцент
О. С. Головня – кандидат педагогічних наук, доцент

Комп'ютерні мережі : методичні рекомендації для виконання
К63 лабораторних робіт. Ч. 2 / підг. В.В. Воротніков,
А. А. Єфіменко, О.Ю. Дячук, М.С. Колощук. – Житомир :
Житомирська політехніка, 2023. – 236 с.

Методичні рекомендації містять теоретичний матеріал, приклади та вказівки для виконання лабораторних робіт, пов'язаних із вивченням питань адресації кінцевих вузлів.

Методичні рекомендації призначені для студентів, які навчаються за спеціальностями 123 „Комп'ютерна інженерія" галузі знань 12 „Інформаційні технології".

Підготували: доктор технічних наук, доцент **В.В. Воротніков**, кандидат технічних наук, доцент **А. А. Єфіменко, О.Ю. Дячук, М.С. Колощук**.

УДК 681.324

ЗМІСТ

ВСТУП

Дані методичні рекомендації розроблені для студентів, які навчаються за спеціальностями 123 ,,Комп'ютерна інженерія", галузі знань 12 ,,Інформаційні технології", для вивчення відповідного змістового модуля навчальної дисципліни ,,Комп'ютерні мережі". Зазначена дисципліна згідно з освітньою програмою та навчальними планами підготовки бакалаврів належить до нормативної частини циклу дисциплін професійної і практичної підготовки.

Основним призначенням даного видання є: поглиблення теоретичних знань, отриманих студентами під час вивчення змістового модуля; набуття практичних навичок із налагодження, моніторингу та діагностики роботи кінцевих вузлів та комунікаційних пристроїв; набуття навичок дослідження процесів передачі даних у локальних мережах під час використання різних мережних технологій, а також набуття навичок усунення проблем у ході роботи мережних пристроїв.

Для проведення лабораторних робіт, залежно від можливостей навчальних лабораторій, передбачається два альтернативних варіанти. Перший варіант – використання реального обладнання, другий – використання спеціалізованих програмних комплексів із комп'ютерної симуляції/емуляції роботи мережних вузлів і пристроїв та мереж у цілому. Вибір варіанта, обладнання та програмних комплексів покладається на викладача. Не виключається поєднання двох варіантів.

Особливістю даних методичних рекомендацій є: наявність у кожній лабораторній роботі необхідних теоретичних відомостей, пов'язаних із вивченням певної технології чи протоколу; наявність достатньо деталізованої довідкової інформації з питань налагодження та діагностики роботи мережних пристроїв, технологій та протоколів, а також наявність готових прикладів налагоджень пристроїв. Слід зазначити, що роботи виконуються індивідуально за варіантами. Вибір номера варіанта проводиться за списком групи. Під час іменування комунікаційних пристроїв, кінцевих вузлів, розрахунку параметрів та розподілу IP-адрес також використовується індивідуалізований підхід. Він полягає у тому, що у назвах пристроїв, IP-адресах мереж використовуються дві останні цифри номера групи (G) та дві цифри номера варіанта (N). Наприклад, IP-адреса

мережі 192.G.N.0/24 для 312-ї групи та 25-го номера варіанта виглядатиме як 192.12.25.0/24. Додаткові параметри налагоджень також обираються відповідно до варіанта.

Повне виконання лабораторної роботи передбачає виконання таких етапів: ознайомлення з теоретичними відомостями; аналіз прикладу (сценарію) розрахунків та налагоджень; аналіз індивідуального варіанта завдання; підготовка інформації для налагодження пристроїв та з'єднань; виконання, за потреби, теоретичних розрахунків; проведення налагоджень мережних пристроїв та кінцевих вузлів; діагностика роботи побудованої мережі; визначення проблем у взаємодії вузлів та їх усунення; дослідження процесів передачі даних у побудованій мережі; формування висновків по роботі; оформлення та захист звіту; підготовка до подальших контрольних заходів.

Звіт із лабораторної роботи оформлюється згідно з вимогами Державного стандарту України ДСТУ 3008-95 ,,Документація. Звіти у сфері науки і техніки. Структура і правила оформлення", міжнародних стандартів ISO 5966:1982, ГОСТ 19.404 ЕСПД ,,Пояснительная записка. Требования к содержанию и оформлению" і повинен містити такі складові: номер роботи; тема роботи; мета роботи; розділ, у якому описано хід виконання роботи відповідно до пунктів завдання; висновки; додаток із лістингами налагоджень усіх комунікаційних пристроїв (за необхідності), рукописні відповіді на контрольні питання. Звіт виконується в електронному вигляді, роздруковується, доповнюється відповідями на контрольні питання і здається на кафедру для перевірки та захисту.

Під час оформлення звіту необхідно дотримуватися таких вимог: звіт оформлюється на аркушах формату А4 з рамками (перша сторінка – з кутовим штампом форми 2, решта сторінок – форми 2а за ГОСТ 2.104-68 ЕСКД. ,,Основные надписи"). Штампи заповнюються згідно з вимогами. Нумерація сторінок наскрізна в межах роботи. Поля для тексту: ліве – 25 мм, праве – 10 мм, верхнє – 20 мм від краю аркуша, нижнє – 10 мм від верхнього краю штампа. Текст роботи оформлюється шрифтом Times New Roman 14-го розміру, міжрядковий інтервал 1 – 1,5. Абзацний відступ 5 символів. Тексти сценаріїв налагоджень, лістингів конфігураційних файлів та інших

елементів рекомендується оформлювати шрифтом Curier New, 10–12-го розміру, міжрядковий інтервал 1. Рекомендується у текстах сценаріїв та лістингів видаляти інформацію, яка не є значущою для виконання завдання або роботи. Ілюстрації та таблиці повинні розміщуватися безпосередньо після тексту, де вони зустрічаються.

Ілюстрації (креслення, рисунки, схеми тощо) позначаються таким чином: ,,Рисунок № – Назва рисунка" (вирівнювання по центру, без абзацного відступу). Позначення ілюстрації виконується під ілюстрацією. Якщо кількість ілюстрацій значна і вони однотипні та невеликі за розміром, то їх рекомендується групувати в одну ілюстрацію, позначати літерами *а*), *б*) ... і підписувати їх як одну ілюстрацію.

Таблиці позначаються таким чином: ,,Таблиця № – Назва таблиці" (вирівнювання по лівому краю, без абзацного відступу). Їх нумерація здійснюється окремо і наскрізно у межах роботи. Позначення таблиці виконується над таблицею. Текст таблиць рекомендується оформлювати шрифтом New Roman 12-го розміру, міжрядковий інтервал 1. Якщо таблиця займає понад одну сторінку, то на другій і наступних сторінках ставиться позначення ,,Продовження табл. №". Головка таблиці повторюється в усіх її частинах.

У тексті звіту можна використовувати переліки (списки в термінології текстових редакторів). Перед перерахуванням ставиться двокрапка. Перед кожною позицією переліку можна ставити тире, малу літеру українського алвафіту з дужкою, арабські цифри з дужкою. Елементи переліку пишуться з маленької літери, наприкінці ставиться крапка з комою, для останнього елемента – крапка.

Для оформлення додатка до роботи, який містить лістинги налагоджень комунікаційних пристроїв, допускається подання інформації у колонки. Слід звернути увагу на те, що лістинги налагоджень окремих пристроїв повинні бути підписані і відокремлені один від одного. Відповіді на контрольні питання оформлюються акуратно, чітким почерком, літерами достатнього для нормального сприйняття розміру. Їх оформлення слід починати з нового аркуша.

Важливо, щоб контрольні питання, які наводяться після кожної лабораторної роботи, були ретельно відпрацьованими студентом

самостійно з метою підготовки до контрольних заходів, таких як тестування та вирішення практичних завдань.

Лабораторна робота 1
ОСНОВИ РОБОТИ З КЕРОВАНИМИ КОМУТАТОРАМИ CISCO ТА МЕРЕЖНОЮ ОПЕРАЦІЙНОЮ СИСТЕМОЮ CISCO IOS

Мета заняття: ознайомитися із загальною будовою керованого комутатора Cisco; ознайомитися з основними можливостями мережної операційної системи Cisco IOS та розглянути особливості її застосування на керованих комутаторах Cisco; дослідити можливості Cisco IOS з налагодження та діагностування основних параметрів функціонування керованих комутаторів Cisco.

Теоретичні відомості

Будова керованого комутатора Cisco

Фірма Cisco займається розробкою і виробництвом комутаторів понад 20 років. За цей період проектувальники та інженери Cisco додали до базового функціоналу комутатора Ethernet велику кількість нових функцій, реалізували підтримку багатьох мережних протоколів, спеціалізованих технологій, архітектурних та технологічних рішень. Багато розробок були включені до стандарту IEEE 802.3 або стали новими стандартами.

Типова структурна схема комутатора Ethernet фірми Cisco наведена на рис. 1. Основними складовими комутатора є:

– центральний процесор (CPU, Central Processing Unit);

– блок комутації (Switch Fabric);

– блок постійної пам'яті (OnBoard ROM, Read-Only Memory);

– блок оперативної пам'яті (OnBoard RAM, Random Access Memory типу DRAM, Dynamic RAM або SDRAM, Synchronous DRAM);

– блок постійної перезаписуваної пам'яті (OnBoard Flash);

– блок змінної перезаписуваної пам'яті (Removable Flash);

– блок енергонезалежної пам'яті (NVRAM, Non-Volatile Random Access Memory);

– блоки керування інтерфейсами/портами Ethernet (Port ASICs);

– блоки фізичного рівня, трансивери Ethernet (PHYs, Physical Layer Devices);

– блоки фізичного рівня для формування стеку (Stack Port PHYs);

– блоки керування інтерфейсів/портів для підключення робочих станцій керування (Management Interfaces).

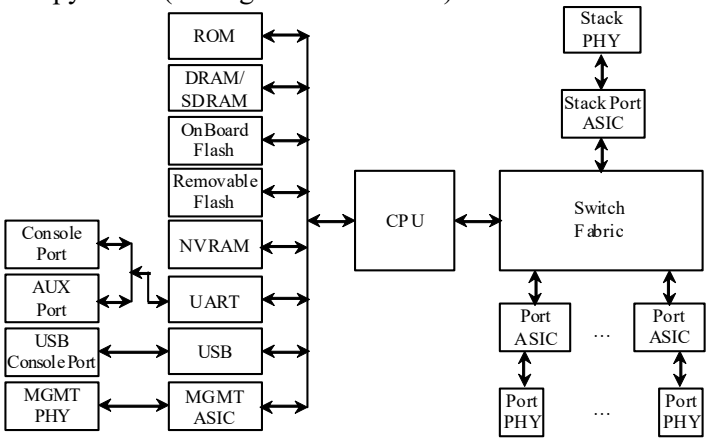


Рис. 1. Типова структурна схема комутатора Ethernet фірми Cisco

Центральний процесор (CPU) забезпечує керування комутатором та координацію роботи його складових, а також забезпечує актуальність основної таблиці комутації. Блок комутації (Switch Fabric) виконує такі функції: забезпечує передачу трафіка між портами, надає якість обслуговування, забезпечує відмовостійкість. Цей блок може бути реалізований у вигляді однієї спеціалізованої мікросхеми великого ступеня інтеграції або кількох спеціальним способом поєднаних мікросхем. Блок комутації характеризується пропускною здатністю (Switch Fabric Capacity, Forwarding Bandwidth), що вимірюється у Гбіт/с. До блока комутації підключені блоки керування інтерфейсами/портами Ethernet та відповідних стекових технологій. Один такий блок може забезпечувати функціонування кількох портів Ethernet або кількох стекових портів. До блоків керування інтерфейсами підключені відповідні блоки фізичного рівня (трансивери) Ethernet та блоки фізичного рівня відповідних технологій стекування.

У постійній пам’яті (OnBoard ROM) комутатора містяться процедура початкового самотестування пристрою POST (Power-On Self-Test) та програма початкового завантаження Boot Loader. Блок оперативної пам’яті (OnBoard RAM) виконує функції, що аналогічні такому ж блоку персонального комп’ютера. В оперативній пам’яті

після завантаження розміщується Cisco IOS, ця пам'ять також використовується для забезпечення процесу передачі кадрів між портами. Блок постійної перезаписуваної пам'яті (OnBoard Flash) виконує функції накопичувача пристрою. Він містить файл образу Cisco IOS та деякі конфігураційні файли, які створюються у процесі налагодження та використовуються у процесі роботи комутатора. Файлів образів у перезаписуваній пам'яті може міститися кілька. Можливості постійної перезаписуваної пам'яті можуть бути розширені за рахунок застосування блока змінної перезаписуваної пам'яті (Removable Flash). Блок енергонезалежної пам'яті (NVRAM) застосовується для збереження конфігурації комутатора.

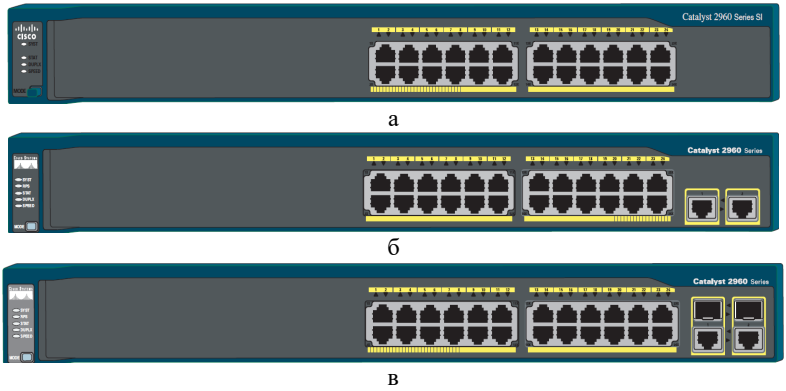
Для забезпечення налагодження та керування комутатором наявні блоки керування інтерфейсів/портів для підключення робочих станцій керування, що підтримують застосування різних фізичних інтерфейсів: послідовного інтерфейсу, інтерфейсу USB, інтерфейсу Ethernet. Для забезпечення функціонування послідовних інтерфейсів (основного – Console Port, допоміжного – AUX Port) застосовується блок, що базується на мікросхемі UART. Для забезпечення функціонування інтерфейсу USB (USB Console Port) – відповідний блок USB. Для підключення робочих станцій керування із застосуванням технологій Ethernet через інтерфейс керування MGMT – блок, який аналогічний за функціями блока керування портом Ethernet. У деяких моделях комутаторів блок інтерфейсу USB також підтримує можливість підключення зовнішніх змінних USB-носіїв або пристроїв.

Зовнішній вигляд комутаторів Cisco серії 2960 наведено на рис. 2. На передній панелі комутатора Cisco розміщуються мережні інтерфейси/порти, кнопка переключення режимів світлодіодних індикаторів (Mode), світлодіодні індикатори (LEDs), що призначені для відображення стану комутатора в цілому. Кожен порт Ethernet також має власний індикатор, який відображає його стан.

На задній панелі комутатора Cisco типово розміщуються консольний порт, гніздо для підключення кабелю основного живлення, спеціальний слот для підключення системи резервного живлення та консольний порт. У деяких спеціалізованих моделях на задній панелі також містяться слоти для об'єднання комутаторів у стек.

Варто зазначити, що у деяких моделях комутаторів на передній панелі також розміщуються консольний порт (порти), спеціалізований порт Ethernet мережного керування, інтерфейс(и) USB для підключення зовнішніх носіїв. Більшість із них також мають власні світлодіодні індикатори.

Загальні правила розуміння свічення індикаторів є такими. Якщо індикатор не світиться (Off) – це свідчить про відключення або непрацездатність пристрою в цілому, певного його блока, підсистеми або каналу зв'язку. Якщо індикатор світиться зеленим кольором (Green) або мерехтить зеленим кольором (Blinking Green) – це свідчить про нормальний режим роботи, якщо ж індикатор світиться жовтим кольором (Amber) або мерехтить жовтим кольором (Blinking Amber) – це свідчить про те, що виникла певна проблема.



а

б

в

Рис. 2. Передня панель комутатора Cisco серії Catalyst 2960:
а – модель 2960-24-S; б – модель 2960-24TT-L; в – модель 2960-Plus 24PC-S

Підключення до керованого комутатора Cisco

Налагодження та керування керованим комутатором може здійснюватися з використанням таких видів підключень:

1. Консольне підключення (Console Connection).
2. Допоміжне підключення (Auxiliary Connection).
3. Мережне керуюче підключення (Network Management Connection).
4. Мережне підключення (Network Connection).

Термін ,,підключення" (Connection) охоплює як фізичну (пряме кабельне з'єднання чи з'єднання через наявну мережну інфраструктуру), так і програмну складові (програму – термінальний клієнт). Для пристроїв Cisco поряд із терміном ,,підключення" застовується термін-синонім ,,лінія" (Line).

Консольне підключення (Console Connection) – це пряме підключення послідовного порту комп'ютера до консольного порту комутатора за допомогою спеціального консольного кабелю (рис. 3). Це підключення також позначається як Console Out-of-Band Connection. Консольне підключення є основним типом підключення для початкового налагодження комутатора. На схемах консольне підключення позначається лінією з коротких штрихів (рис. 4, а).

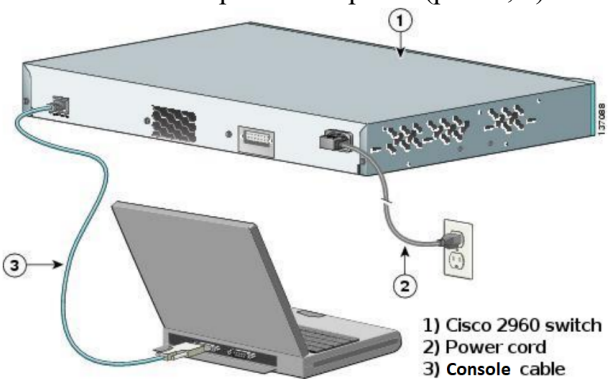


Рис. 3. Консольне підключення до комутатора Cisco

Допоміжне підключення (Auxiliary Connection) – це підключення послідовного порту комп'ютера до допоміжного порту комутатора за допомогою модемів через телефонну мережу загального користування (PSTN, Public Switched Telephone Network чи POTS, Plain Old Telephone Service) (рис. 4, б). Часто це підключення позначається як POTS Out-of-Band Connection. Таке підключення налагоджується з метою забезпечення функціонування резервного комутованого каналу керування для випадку, коли мережне підключення виходить із ладу і необхідно провести налагодження віддаленого пристрою. Порти для здійснення допоміжних підключень реалізовувалися лише в перших моделях комутаторів Cisco.

Мережне керуюче підключення (Network Management Connection) – це пряме підключення мережного адаптера Ethernet комп'ютера до спеціалізованого Ethernet-порту керування (In-Band Ethernet Management Interface) комутатора за допомогою звичайного (прямого) Ethernet кабелю (рис. 4, в). Таке підключення застосовується у випадку, коли основні параметри комутатора є заздалегідь налагодженими (наприклад, виробником) і наявна можливість для виконання підключення. Також таке підключення застосовується у разі, коли необхідно мати ізольований від решти портів комутатора, а отже і вузлів мережі, канал зв'язку для налагодження пристрою. Порти для здійснення мережного керуючого підключення реалізовують лише на деяких сучасних моделях комутаторів Cisco.

Основним типом підключення для поточного налагодження, керування та діагностування процесів роботи комутатора є мережне підключення (Network Connection) – підключення через наявну мережну інфраструктуру (рис. 4, г). Це підключення також позначається як Network In-Band Connection.

У всіх випадках підключень використовуються спеціальні термінальні програмні додатки, що мають засоби забезпечення функціонування як прямих підключень, так і мережних підключень, що формуються з використанням протоколів віддаленого доступу.

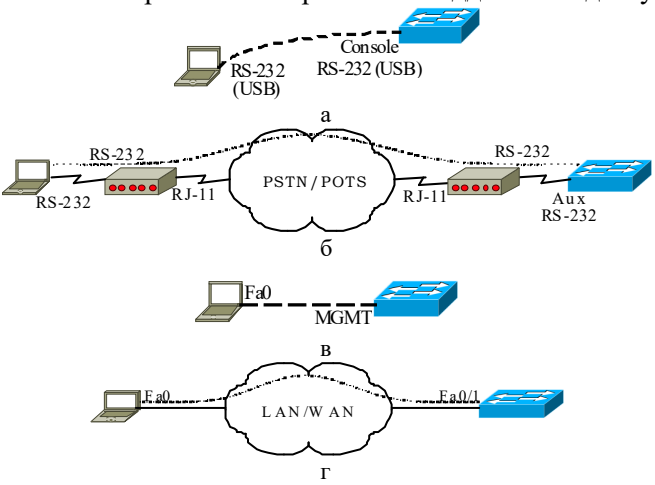
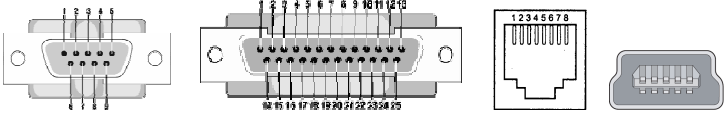


Рис. 4. Підключення до керованого комутатора:
а – консольне підключення; б – допоміжне підключення;
в – мережне керуюче підключення; г – мережне підключення

Консольне підключення реалізовується з використанням або послідовних інтерфейсів RS-232 (EIA/TIA-232), або інтерфейсу USB. Для інтерфейсу RS-232 можуть застосовуватися розніми DB-9 (стандарт EIA/TIA-574), DB-25 (стандарт EIA/TIA-232/RS-232-E), RJ-45 (стандарт EIA/TIA-561). Для інтерфейсу USB застосовуються розніми USB Type A, USB Type B (5 pin mini-Type B). У більшості сучасних моделей комутаторів Cisco для консольного підключення наявні або одне гніздо рознімy RJ-45 (8P8C), або два гнізда – рознімy RJ-45 і рознімy USB 5 pin mini-Type B одночасно. Слід зазначити, що у певний момент часу активним може бути лише один консольний порт. Перевага надається порту USB. У разі підключення кабелю до цього порту, порт RJ-45 автоматично відключається, при відключенні кабелю – активується. У старіших моделях комутаторів Cisco та на пристроях Cisco інших типів можуть застосовуватися розніми DB-9, DB-25. Більшість виробників мережного обладнання у своїх пристроях застосовують аналогічні розніми. Консольний порт може розміщуватися як на передній, так і на задній панелях комутатора. Для моніторингу функціонування консольного порту, які і решти портів, застосовуються світлодіодні індикатори.

Зображення гнізд рознімів DB-9, DB-25, RJ-45, USB 5 pin mini-Type B та нумерація їх контактів наведені на рис. 5, а, б, в, г відповідно. Позначення та опис інформаційних сигналів для вищезгаданих рознімів наведені відповідно у табл. 3, 4, 5, 6.



а б в г

Рис. 5. Нумерація контактів рознімів:
а – DB-9; б – DB-25; в – RJ-45; г – USB 5 pin mini-Type B

Таблиця 3

Сигнали інтерфейсу RS-232 для рознімy DB-9 (стандарт EIA/TIA-574)

Контакт	Сигнал
1	Детектування несучої (Data Carrier Detect, CD, DCD)
2	Приймання даних (Received Data, RxD)
3	Передача даних (Transmitted Data, TxD)
4	Готовність терміналу (Data Terminal Ready, DTR)

5	Сигнальна „земля” (Signal Ground, SG)
6	Готовність даних (Data Set Ready, DSR)
7	Запит на передачу (Request to Send, RTS)
8	Готовність до передачі (Clear to Send, CTS)
9	Індикатор виклику (Ring Indicator, RI)

Таблиця 4

Сигнали інтерфейсу USB для розніму USB 5 pin mini-Type B

Контакт	Сигнал
1	Живлення +5 В (VCC)
2	Дані– (Data–, D–)
3	Дані+ (Data+, D+)
4	Індикатор (Indicator, ID)
5	„Земля” (Ground, GND)

Таблиця 5

Сигнали інтерфейсу RS-232 для розніму DB-25 (стандарт EIA/TIA-232)

Контакт	Сигнал
1	Корпус (PG)
2	Передача даних (Transmitted Data, TxD)
3	Приймання даних (Received Data, RxD)
4	Запит на передачу (Request to Send, RTS)
5	Готовність до передачі (Clear to Send, CTS)
6	Готовність даних (Data Set Ready, DSR)
7	Сигнальна „земля” (Signal Ground/Common Return, SG)
8	Детектування несучої (Rcvd. Line Signal Detector, CD, DCD)
9	Тестова напруга (+)
10	Тестова напруга (–)
11	Не використовується
12	Детектування несучої, повернення (Rcvd. Line Signal Detector, DCD2/SF2)
13	Готовність до передачі, повернення (Secondary Clear to Send, CTS2)
14	Передача, повернення (Secondary Transmitted Data, TxD2)
15	Тактування передачі (Transmitted Signal Element Timing, TSET, ETxC)
16	Приймання, повернення (Secondary Received Data, RxD2)
17	Тактування приймання (Receiver Signal Element Timing, RSET, RxC)
18	Локальний шлейф (LL)
19	Запит на передачу, повернення (Secondary Request to Send, RTS2)
20	Готовність терміналу (Data Terminal Ready, DTR)
21	Детектування якості сигналу (Sig. Quality Detector, SQ)
22	Індикатор виклику (Ring Indicator, RI)
23	Вибір швидкості (Data Sig. Rate Selector, SF)
24	Тактування передачі (Tramsmitter Sig. Element Timing, TSET, TxC)
25	Не використовується

Таблиця 6

Сигнали інтерфейсу RS-232 для розніму RJ-45 (стандарт EIA/TIA-561)

Контакт	Сигнал
1	Запит на передачу (Request to Send, RTS)
2	Готовність терміналу (Data Terminal Ready, DTR)
3	Передача даних (Transmitted Data, TxD)
4	Сигнальна „земля” (Signal Ground, SG)
5	Сигнальна „земля” (Signal Ground, SG)
6	Приймання даних (Received Data, RxD)
7	Готовність даних (Data Set Ready, DSR)
8	Готовність до передачі (Clear to Send, CTS)

Інтерфейс RS-232 початково був розроблений для з’єднання пристрою типу DTE з пристроєм типу DCE. Типовим прикладом з’єднання DTE–DCE є з’єднання комп’ютер-модем або комутатор-модем. Кабель, який застосовується для формування такого з’єднання, називається модемним кабелем (Modem Cable). Схема модемного кабелю, побудованого з використанням рознімів DB-9–DB-9 наведена на рис. 6. Для кабелів, що побудовані з використанням рознімів DB-25–DB-25 або DB-9–DB-25, схеми є аналогічними.

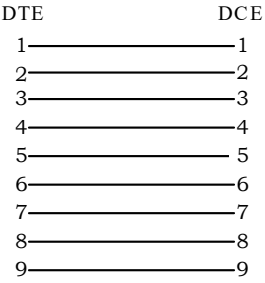


Рис. 6. Схема модемного кабелю DB-9–DB-9

Пряме з’єднання на базі інтерфейсу RS-232 між двома пристроями типу DTE (зокрема, між комп’ютером і комутатором) вимагає застосування спеціального кабелю, який називається нуль-модемним кабелем (Null-Modem Cable). Залежно від того, які рознімі застосовуються, нуль-модемні кабелі можуть мати такі власні назви:

1. Null-Modem Cable (DB-9–DB-9, DB-9–DB-25, DB-25–DB-25).
2. Cisco Rollover Cable (RJ-45–RJ-45).
3. Cisco Console Cable (DB-9–RJ-45, DB-25–RJ-45).

Повна і спрощена схеми нуль-модемного кабелю, побудованого з використанням рознімів DB-9–DB-9, наведені на рис. 7, а та 7, б відповідно. Максимальна довжина кабелю у даному випадку – 30 м.

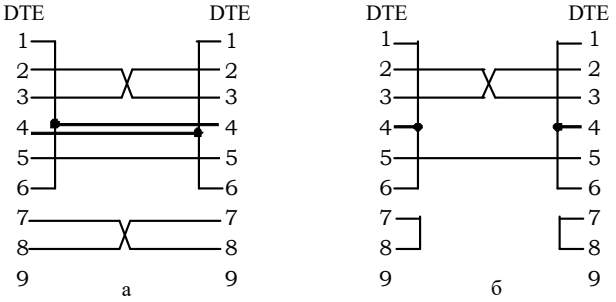


Рис. 7. Схеми нуль-модемного кабелю DB-9–DB-9: а – повна; б – спрощена

Консольний кабель на базі інтерфейсу USB – Cisco USB Console Cable може мати реалізації з використанням рознімів USB Type A – RJ-45 та USB Type A – USB 5 pin mini-Type B. У першому варіанті до складу кабелю входить мікросхема-конвертор інтерфейсів USB–RS-232, яка забезпечує перетворення сигналів інтерфейсу USB комп'ютера в сигнали інтерфейсу RS-232 комутатора і навпаки. У другому варіанті кабель забезпечує передачу сигналів інтерфейсу USB. У цьому випадку комутатор повинен мати модуль USB для підтримки функціонування даного інтерфейсу.

Підключення з використанням інтерфейсу RS-232, як правило, не вимагає встановлення додаткового ПЗ на комп'ютері адміністратора, оскільки драйвер наявний в ОС. Підключення з використанням інтерфейсу USB передбачає встановлення додаткового драйвера. Цей драйвер, як правило, можна завантажити із сайта виробника кабелю або пристрою.

Слід зазначити, що деякі виробники мережного обладнання (зокрема, Zyxel, D-Link, Allied Telesis) на своїх комутаторах встановлюють мікросхеми інтерфейсу RS-232, що забезпечують їх функціонування як пристроїв типу DCE. У таких випадках підключення здійснюються з використанням звичайних модемних кабелів і формально теж називаються консольними підключеннями.

Виробниками кабелів розроблено великий набір спеціальних модульних адаптерів-перехідників, які дають змогу „перетворити" один кабель в інший. Серед них слід згадати такі:

- DB-9–DB-25 Adapter (DB-25–DB-9 Adapter).
- Rollover Adapter.
- Null-Modem Adapter.
- RJ-45–DB-9 Adapter (RJ-45–DB-25 Adapter).
- USB–RS-232 Adapter.

DB-9–DB-25 Adapter дає змогу застосовувати модемний кабель DB-9–DB-9 для забезпечення підключення до розніму DB-25, а DB-25–DB-9 Adapter – навпаки, модемний кабель DB-25–DB-25 – до розніму DB-9. Rollover Adapter у поєднанні зі звичайним прямим кабелем Ethernet (що застосовується для підключення мережного адаптера комп'ютера до звичайного порту комутатора) дає змогу здійснити підключення, яке аналогічне підключенню із застосуванням кабелю Cisco Rollover Cable. Null-Modem Adapter у поєднанні зі звичайним модемним кабелем дає змогу здійснити підключення, яке аналогічне підключенню із застосуванням кабелю Null-Modem Cable. RJ-45–DB-9 Adapter (рис. 8) у поєднанні з Cisco Rollover Cable дає змогу здійснити підключення, яке аналогічне підключенню із застосуванням кабелю Cisco Console Cable DB-9–RJ-45. USB–RS-232 Adapter у поєднанні з Cisco Console Cable DB-9–RJ-45 дає змогу здійснити підключення, яке аналогічне підключенню із застосуванням кабелю Cisco USB–RJ-45 Console Cable.

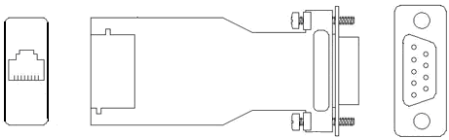


Рис. 8. RJ-45–DB-9 Adapter

Програмні засоби забезпечення підключень

Налагодження та керування функціонуванням комутатора Cisco може здійснюватися з використанням різних підходів та засобів. З метою налагодження комутатора з використанням консольного та допоміжного підключень на комп'ютері адміністратора необхідно застосовувати спеціальні програми емулятори терміналу (термінальні додатки). Найбільш відомими термінальними додатками є Hyper Terminal,

PuTTY, Tera Term, SecureCRT, Minicom, ZTerm Pro. Інтерфейс Windows-додатка Hyper Terminal за умови створення з'єднання наведений на рис. 9.

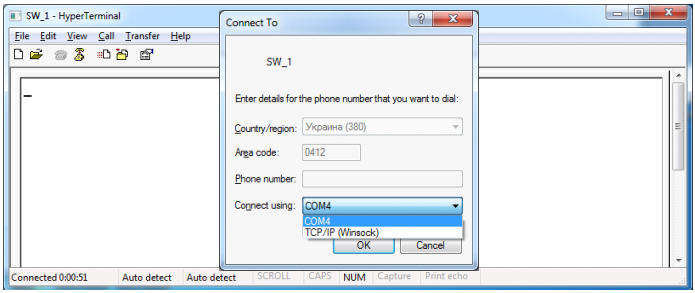


Рис. 9. Інтерфейс термінального додатка HyperTerminal

Для налагодження комутатора за допомогою мережного керуючого підключення або мережного підключення необхідно застосовувати засоби, що забезпечують можливість віддаленого доступу на базі мережних протоколів Telnet, SSH, HTTP, SNMP тощо. Вищезгадані термінальні додатки теж підтримують цю можливість.

Фірмою Cisco розроблено ряд спеціалізованих програмних додатків, які дають змогу проводити віддалене налагодження та керування комунікаційними пристроями. Серед них слід згадати такі: Cisco Network Assistant; Cisco Device Manager; CiscoWorks LAN Management Solution (LMS); CiscoView Application; Cisco Configuration Engine; SNMP Network Management Application; Cisco Security Manager; Catalyst Smart Operations. Ці засоби, як правило, мають графічний інтерфейс та використовують для обміну даними між пристроями протоколи прикладного рівня (HTTP, HTTPs, SNMP). У багатьох випадках їх застосування передбачає початкове налагодження пристрою за допомогою консольного підключення.

Програмне забезпечення сучасних комутаторів

Функціонування сучасного комутатора Ethernet забезпечується за рахунок поєднання можливостей його апаратної та програмної складових. Простіші моделі комутаторів реалізуються повністю апаратно. Більш складні моделі комутаторів є програмно-апаратними засобами, тобто частина функцій цих пристроїв виконується апаратно, а частина – програмно. Зручність такого підходу полягає в тому, що можна відносно оперативно змінювати програ-

мну складову системи у разі появи нових версій чи варіантів системи з розширеними та покращеними можливостями. Окрім того, використання програмної складової дає можливість налагоджувати комутатори для специфічних умов функціонування та керувати процесом їх роботи. Останнім часом провідні виробники комутаторів все більшу частину функцій пристрою перекладають на програмну складову, залишаючи на апаратному рівні лише необхідний для функціонування пристрою мінімум.

Програмна складова комутатора може бути реалізована як у вигляді мікропрограми, так і у вигляді повноцінної мережної ОС. Мікропрограма (FirmWare) – це системне ПЗ, яке є вбудованим („прошитим") у пристрої і зберігається в його енергонезалежній пам'яті. Основною відмітністю ОС від FirmWare є наявність файлової системи, яка забезпечує можливість виконання різних операцій над файлами. Як правило, і FirmWare, і ОС комутатора є монолітними, тобто поставляються у вигляді одного бінарного файла-образу, зміни в який вносити неможливо. Цей файл-образ зберігається у флеш-пам'яті пристрою. Заміна FirmWare або ОС здійснюється шляхом заміни файла-образу. Для комутаторів, які використовують FirmWare, налагодження пристрою зберігаються у вигляді бітової послідовності у спеціально відведеній області енергонезалежної пам'яті. У комутаторах, які використовують мережну ОС, як правило, збереження конфігурації здійснюється у вигляді структурованого текстового файла.

Оскільки комутатори є досить спеціалізованими комунікаційними пристроями, то під час розробки їх програмних складових застосовується модельно-орієнтований підхід – FirmWare та ОС розробляються з урахуванням апаратної складової та призначення пристроїв.

Мережна операційна система Cisco IOS

Для забезпечення функціонування мережних пристроїв фірмою Cisco розробляються як різні варіанти FirmWare, так і спеціалізовані мережні ОС. Використання Cisco FirmWare характерне для точок доступу та безпровідних маршрутизаторів, деяких моделей комутаторів. Більшість моделей комутаторів та маршрутизаторів Cisco використовують спеціалізовані мережні ОС.

Основними мережними ОС Cisco є:

- Cisco IOS (Cisco Internetwork Operating System);
- Cisco NX-OS (NeXt-generation OS, Nexus OS);
- Cisco IOS XR;
- Cisco IOS XE.

У сучасних комутаторах та маршрутизаторах Cisco найчастіше використовується спеціалізована мережна ОС Cisco IOS. У старих моделях комутаторів використовувалася CatOS (Catalyst Operating System), але її рекомендується замінювати на більш сучасну IOS. Для спеціалізованих комутаторів серій Nexus (технології Ethernet) та MDS (технології Fibre Channel), які використовуються в центрах обробки та збереження даних, Cisco розроблено мережну ОС Cisco NX-OS. Для сучасних високопродуктивних маршрутизаторів розроблено ОС, відому як Cisco IOS XR. Також розроблена і широко впроваджується для використання в комутаторах, маршрутизаторах та інших пристроях ОС наступного покоління Cisco IOS XE. Всі зазначені ОС мають різні архітектурни, особливості внутрішної реалізації, кодову базу, відмінності у інтерфейсі тощо. Варто зазначити, що для ОС Cisco IOS та Cisco IOS XE для зручності роботи збережений однаковий інтерфейс командного рядка.

Cisco IOS є багатозадачною ОС, яка виконує функції мережної організації, комутації, маршрутизації та передачі даних. Ядро цієї ОС є монолітним, це означає, що всі елементи системи розміщені в одному образі і всі процеси запускаються в одному адресному просторі. У Cisco IOS немає міжпроцесного захисту пам'яті, це означає, що крах одного процесу може викликати крах або перезавантаження всієї системи.

Cisco IOS поставляється у вигляді монолітного образу, який орієнтований на конкретну модель пристрою. Образи можуть мати певні набори властивостей та версії. Конкретний образ IOS ідентифікується трьома параметрами:

апаратна платформа (серія) пристрою, для якої він призначений;

набір можливостей (Feature Set, Packages),

версія ОС.

Узагальнена структура взаємозв'язків між наборами можливостей Cisco IOS наведена на рис. 10. Кожен із наборів можливостей забезпе-

чує використання певних технологій та наборів протоколів. Для керованих комутаторів Cisco більш простих моделей характерне використання наборів Layer 2 Base та LAN Base. Набір можливостей Layer 2 Base забезпечує функціонування як базових компонентів технології Ethernet згідно зі стандартом IEEE 802.3, так і додаткових стандартизованих протоколів та технологій чи спеціалізованих функцій. Зокрема це: 802.1D, 802.1x, 802.1s/w (RSTP), 802.3ad Etherchannel, Port Security, SSHv2 та ін. Набір властивостей LAN Base включає всі можливості Layer 2 Base і розширені можливості з налагодження комутатора та обробки трафіка, такі як Cisco AutoSecure, Cisco AutoQoS, Advanced 802.1x, Advanced Access Lists, Advanced QoS.

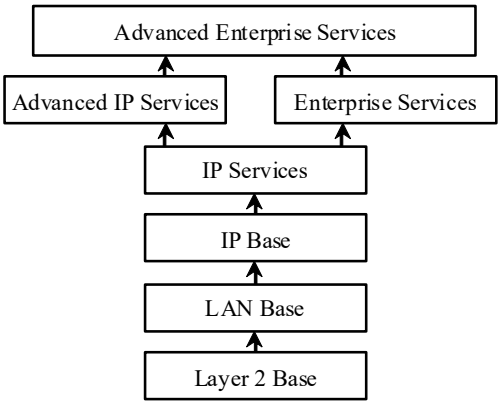


Рис. 10. Узагальнена структура взаємозв'язків між наборами можливостей Cisco IOS

На сьогодні найбільш поширеними у використанні є версії Cisco IOS з номерами 12.x. та 15.x. У практиці зустрічаються пристрої, на яких використовуються і попередні версії. Це, як правило, пристрої, життєвий цикл підтримки яких вже закінчився, і нові версії Cisco IOS для яких не розроблені або неможливо встановити з технічних причин. Для більшості сучасних пристроїв наявні образи як 12, так і 15 версій.

Приклади запису назв файлів образів для комутаторів серії 2960: c2960-lanbasek9-mz.122-58.SE2.bin, c2960-lanbasek9-mz.150-2.SE.bin. Додаткову інформацію Cisco IOS можна отримати з довідників, які містять деталізовані розшифровки скорочень, що використовуються у назвах файлів образів.

Порядок завантаження Cisco IOS на комутаторі Cisco

Після включення живлення на комутаторі Cisco виконується визначений набір дій, які забезпечують тестування функціонування складових комутатора і завантаження Cisco IOS. Цей набір також називають ,,завантажувальною послідовністю" (Boot Sequence). Дана послідовність включає 6 етапів (рис. 11).

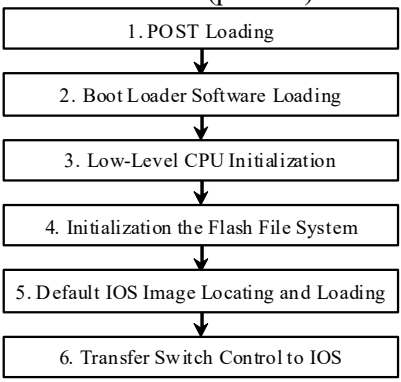


Рис. 11. Етапи завантаження комутатора Cisco

На першому етапі здійснюється завантаження процедури початкового самотестування пристрою POST, що зберігається в постійній пам'яті (OnBoard ROM) комутатора. У процесі роботи цієї процедури здійснюється перевірка функціонування підсистеми CPU, яка включає тестування процесора, оперативної пам'яті (OnBoard RAM) та частини флеш-пам'яті, яка містить файлову систему. На другому етапі здійснюється завантаження в оперативну пам'ять програми початкового завантаження Boot Loader, яка також зберігається в постійній пам'яті пристрою. На третьому етапі Boot Loader виконує низькорівневу ініціалізацію CPU, яка включає ініціалізацію регістрів, що контролюють доступ до фізичної пам'яті, її об'єм та швидкість. На четвертому етапі Boot Loader ініціалізує файлову систему, що міститься у флеш-пам'яті системної плати. На п'ятому етапі Boot Loader знаходить образ Cisco IOS за замовчуванням і завантажує його в оперативну пам'ять. Після завантаження образу Cisco IOS на шостому етапі керування комутатором передається Cisco IOS. Надалі система здійснює пошук файла конфігурації або запускає режим початкового конфігурування комутатора.

Інтерфейс командного рядка Cisco IOS

Налагодження пристроїв Cisco можливе як із використанням інтерфейсу командного рядка, так і з використанням спеціалізованих графічних додатків. Інтерфейс командного рядка є гнучкішим і ефективнішим інструментом. У деяких випадках без нього неможливо виконати налагодження пристрою, зокрема: створити початкову конфігурацію, відновити втрачені паролі, створити нестандартні конфігурації, активувати приховані можливості, перевірити правильність налагодження, відлагодити процеси обміну даними тощо.

Інтерфейс командного рядка має великий набір можливостей для редагування команд та їх параметрів. Важливими властивостями командного рядка Cisco IOS є:

а) надання допомоги, яка полягає у виведенні списку команд (та їх коротких описів), що доступні у відповідному режимі, та довідки за параметрами окремої команди Cisco IOS (див. рис. 12, 13);

б) можливість використання скороченого запису команд, яка полягає в тому, що система розпізнає команди за їх скороченим записом і для виконання здійснює операцію внутрішнього доповнення, наприклад, записи команд **configure terminal**, **conf term** та **conf t** для системи є ідентичними;

в) можливість виведення списку команд (параметрів команди), початкові літери яких збігаються (див. рис. 14);

г) функція автодоповнення поточної команди, робота якої полягає ось у чому: вводиться скорочений запис команди (чи її параметра), натискається клавіша <Tab> і в новому рядку з'являється повна команда.

```
SW_01>?
Exec commands:
  <1-99>      Session number to resume
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
```

Рис. 12. Перелік команд, які доступні у режимі користувача

```
SW_01#copy ?
  flash:          Copy from flash: file system
  ftp:            Copy from ftp: file system
  running-config  Copy from current system configuration
  startup-config  Copy from startup configuration
  tftp:           Copy from tftp: file system
SW_01#copy
```

Рис. 13. Виведення довідки за параметрами команди **copy**

```
SW_01#co?
configure  connect  copy
SW_01#co
...
SW-1(config)#e?
enable  end  exit
SW-1(config)#e
```

Рис. 14. Приклади переліків команд, початкові літери яких збігаються

Перелік комбінацій клавіш, які можна використовувати для редагування командного рядка, наведено у табл. 7.

Таблиця 7

Клавіші редагування командного рядка Cisco IOS

Клавіша/ Комбінація клавіш	Виконувані дії
Ctrl+A	Переміщення курсора на початок рядка
Ctrl+B	Переміщення курсора на один символ назад (аналог клавіші ←)
Ctrl+D	Видалення символу ліворуч від курсора
Ctrl+E	Переміщення курсора на кінець рядка
Ctrl+F	Переміщення курсора вперед на один символ (аналог клавіші →)
Ctrl+K	Видалення всіх символів від поточної позиції курсора до кінця рядка
Ctrl+N	Перехід на наступну в історії сеансу команду (аналог клавіші ↓)
Ctrl+P	Перехід на попередню в історії сеансу команду (аналог клавіші ↑)
Ctrl+T	Міняє місцями поточний символ і символ ліворуч від курсора
Ctrl+R	Перерисовує або заново виводить поточний рядок
Ctrl+U	Очищення рядка
Ctrl+W	Видалення слова ліворуч від курсора
Ctrl+X	Видалення символів від поточної позиції курсора і до початку рядка

Продовження таблиці 7

Ctrl+Y	Вставка символів, що видалені останніми, на місце, яке відповідає поточній позиції курсора
Ctrl+Z	Вихід із поточного режиму налагодження і перехід у привілейований режим
Tab	Доповнення поточної команди
↑	Перехід на попередній запис у списку „історії команд”
↓	Перехід на наступний запис у списку „історії команд”
←	Переміщення курсора ліворуч
→	Переміщення курсора праворуч
Ctrl +^, X	Відміна послідовності. Переривання виконання будь-якої виконуваної команди

Режими роботи комутатора Cisco

Керований комутатор Cisco, який працює під керуванням Cisco IOS, має три основних та кілька додаткових командних режими функціонування (рис. 15).

Основними режимами є:

- режим користувача (User Mode, User EXEC Mode);
- привілейований режим (Privilege Mode, Privilege EXEC Mode);
- режим глобального конфігурування (Global Configuration Mode).
- Додатковими режимами є:
- режим конфігурування інтерфейсу (Interface Configuration Mode);
- режим конфігурування групи інтерфейсів (Interface-range Configuration Mode);
- режим конфігурування лінії (Line Configuration Mode);
- режим конфігурування віртуальної локальної мережі (Config-VLAN Mode);
- режим конфігурування параметрів бази даних віртуальної локальної мережі (VLAN Configuration Mode).

Кожен із режимів надає певні функціональні можливості з діагностування та налагодження роботи комутатора. У кожному режимі користувачеві надається певний набір команд. Переходи між режимами також здійснюються за допомогою відповідних команд (рис. 15). Певні моделі комутаторів, окрім зазначених режимів, надають можливість використання й інших режимів. Номенклатура режимів пристрою також визначається набором можливостей та версією Cisco IOS.

Після завантаження налагоджений комутатор Cisco перебуває, якщо не передбачений парольний захист, у режимі користувача. Для переходу до привілейованого режиму використовується команда **enable**. Для повернення – або **disable**, або **exit**, або **logout**. Для переходу до режиму глобального конфігурування використовується команда **configure terminal**, для виходу – або команда **end**, або команда **exit**. Для переходів до інших режимів (конфігурування інтерфейсу/групи інтерфейсів, конфігурування лінії, конфігурування vlan і т.д.) використовуються відповідні команди. Можливе пряме повернення з будь-якого нижчого режиму до привілейованого режим командою **end** або натисненням комбінації клавіш **<Ctrl>+<Z>**.

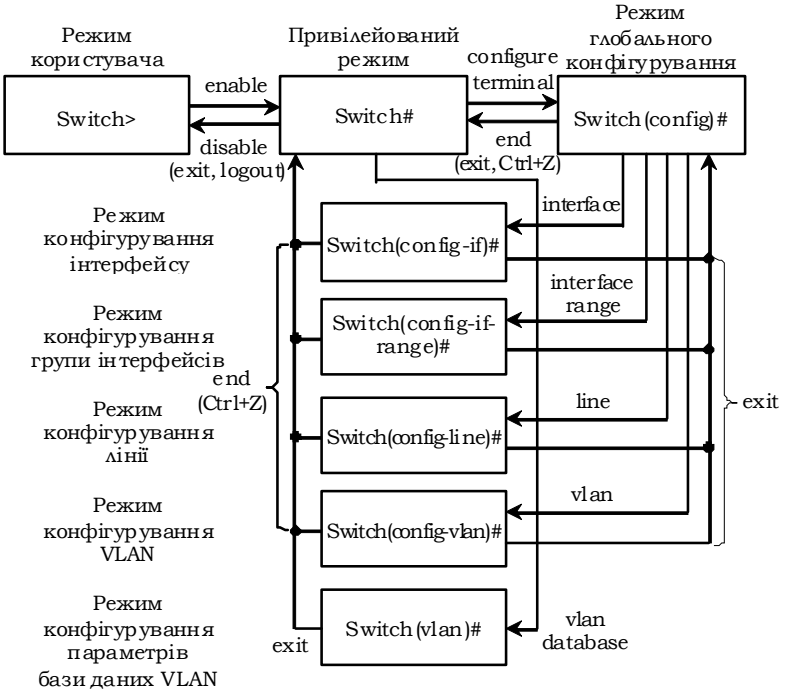


Рис. 15. Командні режими комутатора Cisco та команди переходів між режимами

Початкове конфігурування комутатора Cisco

У Cisco IOS наявні два основних методи створення початкової конфігурації пристрою:

– режим початкового конфігурування (Setup Mode);

– режим глобального конфігурування (Global Configuration Mode).

Режим початкового конфігурування реалізовано у вигляді діалогу, у якому IOS інтерактивно запитує у системного адміністратора базові параметри налагодження пристрою. Цей режим активується IOS після завантаження у разі, коли відсутня попередньо сформована конфігурація (наприклад, у новому пристрої). Іноді є потреба перейти у режим діалогу примусово, тоді необхідно виконати команду **setup** у привілейованому режимі. На рис. 16 наведено блок-схему спрощеного алгоритму завантаження комутатора із зазначенням ситуації, у якій використовується режим початкового конфігурування.

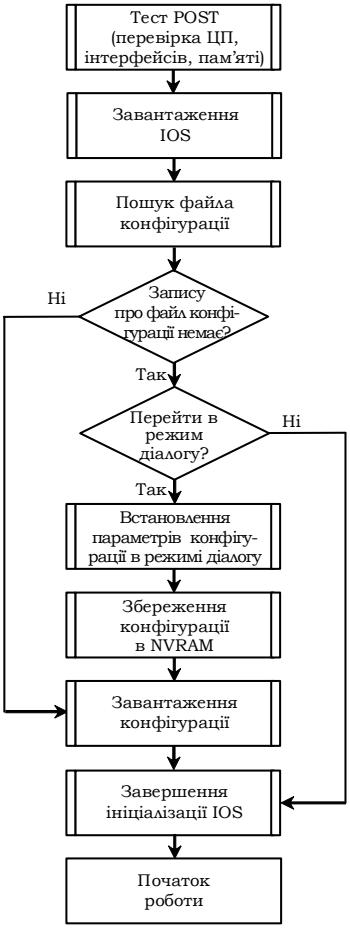


Рис. 16. Блок-схема спрощеного алгоритму завантаження комутатора Cisco

Команди базового налагодження керованого комутатора Cisco

Конфігурування керованого комутатора Cisco передбачає налагодження: параметрів іменування, системного годинника, параметрів консольного підключення, параметрів термінального вікна, часових періодів (тайм-аутів) сеансу, системних повідомлень, безпечного доступу до пристрою, параметрів IP-адресації та багато ін.

Іменування пристроїв у Cisco IOS використовується:

– для ідентифікації пристрою під час підключення (як за консольного підключення, так і в разі мережних термінальних підключень за допомогою протоколів віддаленого доступу Telnet чи SSH);

– під час розсилки інформації про пристрій іншим пристроям (наприклад, за допомогою протоколів виявлення пристроїв LLDP чи CDP);

– для генерації ключів у разі використання криптографічних засобів (наприклад, у протоколі SSH).

Для зміни імені пристрою призначена команда **hostname**. Повернення імені пристрою за замовчуванням – **no hostname**. За замовчуванням заводське ім'я комутатора **Switch**.

Операційна система Cisco IOS на пристроях Cisco забезпечує функціонування системного (програмного) годинника/календаря. У деяких моделях пристроїв також наявний і апаратний годинник/календар. Відповідно існують механізми обміну даними між ними. Параметри системних часу (та дати) пристрою можуть встановлюватися як за допомогою команд локального застосування, так і з використанням мережного джерела часу. У першому випадку за умови відсутності апаратного годинника параметри системного часу не зберігаються у конфігураційному файлі і є актуальними лише на період роботи пристрою. Після перезавантаження їх необхідно встановлювати заново. У другому випадку системний час після завантаження пристрою синхронізується з часом сервера часу за протоколом NTP. Надалі операція синхронізації виконується періодично. Звичайно, що це потребує певних специфічних налагоджень.

Встановлення системного часу здійснюється за допомогою команди **clock set**, встановлення часового поясу – за допомогою команди **clock timezone**. Для активації переходу на літній час застосовується команда **clock summertime**. Для виведення параметрів часу та дати апаратного годинника пристрою у ручному режимі застосовується команда **clock read-calendar**. Для налагодження використання апаратного годинника пристрою як авторитетного джерела мережного часу застосовується команда **clock calendar-valid**. Для одноразової ручної синхронізації параметрів часу апаратного годинника з параметрами часу програмного годинника пристрою застосовується команда **clock update-calendar**. Синтаксис розглянутих команд наведено нижче.

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

hostname ***device-name***,

де ***device-name*** – текстове ім'я пристрою; теоретично може містити до 63 символів (літер, цифр, спец. символів), рекомендується задавати ім'я довжиною до 10 символів, оскільки в більшості систем існує обмеження на довжину службової частини командного рядка.

Синтаксис команди **clock set** (привілейований режим):

clock set ***hh*:*mm*:*ss dd month yyyy***,

де ***hh*:*mm*:*ss*** – години (у 24-годинному форматі), хвилини, секунди;

dd – день, значення у діапазоні від 1 до 31;

month – місяць, назва місяця англійською мовою;

yyyy – рік, чотирицифрове значення в діапазоні від 1993 до 2035.

Синтаксис команди **clock timezone** (режим глобального конфігурування):

clock timezone ***time-zone hh*[*mm*]**,

де ***time-zone*** – часовий пояс (текстове значення вигляду WET – Western European Time, CET –Central European Time, EET – Eastern European Time, EEST – Eastern European Summer Time і т.д.), за замовчуванням установлено універсальний глобальний час (UTC, Coordinated Universal Time);

hh – години, зсув від UTC, ціле число в діапазоні від – 23 до 23;

mm – хвилини, зсув від UTC, ціле число в діапазоні від – 59 до 59.

Синтаксис команди **clock summertime** (режим глобального конфігурування):

clock summertime ***time-zone*** **date** [***b_day, b_month, b_year, b_hh:mm e_day, e_month, e_year, e_hh:mm***] [***shift***]

clock summertime ***time-zone*** **reccuring** [***b_week, b_day, b_month, b_hh:mm e_week, e_day, e_month, e_hh:mm***] [***shift***],

де ***time-zone*** – часовий пояс;

date – службова конструкція, за допомогою якої зазначається початкова і кінцева дати літнього часу;

reccuring – службова конструкція, яка зазначає, що перехід на літній час повинен здійснюватися щороку;

b_day, e_day – день початку і закінчення дії літнього часу, решта параметрів трактуються подібним чином;

shift – кількість хвилин, які необхідно додати у момент переходу на літній час, за замовчуванням – 60 хв.

Синтаксис команди **clock read-calendar** (режим глобального конфігурування):

clock read-calendar.

Команда не має параметрів.

Синтаксис команди **clock calendar-valid** (режим глобального конфігурування):

clock calendar-valid.

Команда не має параметрів.

Синтаксис команди **clock update-calendar** (режим глобального конфігурування):

clock update-calendar.

Команда не має параметрів.

Основні команди налагодження консольного підключення до пристроїв Cisco

Для консольного підключення (а також і для підключень по інших термінальних лініях) використовуються спеціальні програми-емулятори терміналу, які мають можливість працювати з послідовними портами комп'ютера. Це можуть бути як вбудовані в систему програмні продукти, так і розробки сторонніх виробників. Як приклади можна навести вбудовану в ОС Windows програму HyperTerminal та широковживані відкриті кросплатформені розробки PuTTY, SecureCRT.

Для термінальної програми, за допомогою якої здійснюється консольне підключення до пристрою (комутатора чи маршрутизатора), можна налагодити такі параметри взаємодії, як:

швидкість (приймання і передавання даних для лінії, біт/с);

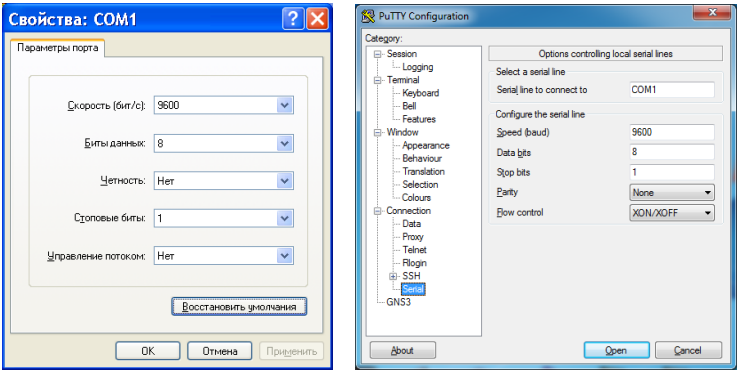
біти даних (кількість бітів даних на символ, яку розуміє і генерує апаратне забезпечення);

парність (біт парності для асинхронної послідовної лінії зв'язку, фактично це сума бітів даних, яка показує, що дані містять або не містять парну чи непарну кількість одиничних бітів);

стопові біти (стопові розряди, які передаються для кожного байта);

керування потоком (керування потоком даних між пристроями, які підключені через послідовну лінію зв'язку).

Параметри за замовчуванням на прикладі програм HyperTerminal та PuTTY наведені на рис. 17, а та рис. 17, б відповідно.



а б

Рис. 17. Параметри за замовчуванням для консольного підключення за допомогою програм: а – HyperTerminal; б – PuTTY

Вибір лінії консольного підключення для налагодження здійснюється командою **line console 0** (режим глобального конфігурування). Для налагодження параметрів лінії на стороні комутатора (чи іншого пристрою Cisco) використовуються команди **speed, databits, parity, stopbits, flowcontrol** відповідно. Повернення до стандартних значень параметрів здійснюється з використанням службового слова **no** з відповідною командою (наприклад, **no speed).** Також можна використати команду **default** (наприклад, **default speed).** Синтаксис указаних команд наведено нижче.

Синтаксис команди **speed** (режим конфігурування лінії):

speed *value*,

де ***value*** – значення швидкості у біт/с, число з діапазону 0…4294967295. Як правило, задається з набору стандартних значень 110, 300, 1200, 2400, 4800, 9600, 19200 і т.д. Верхня межа залежить від мікросхеми UART, на якій реалізовано послідовний порт консолі. За замовчуванням встановлюється швидкість 9600 біт/с.

Синтаксис команди **databits** (режим конфігурування лінії):

databits *value*,

де ***value*** – кількість бітів даних на символ, набуває значень 5, 6, 7, 8. За замовчуванням становить 8 бітів.

Синтаксис команди **parity** (режим конфігурування лінії):

parity *value*,

де ***value*** – параметр, який може набувати значень **even**, **mark**, **none**, **odd**, **space**; за замовчуванням значення не визначене;

none – біт парності відсутній і не передається;

even – біт парності дорівнює 0, якщо у переданому символі парна кількість одиничних бітів;

mark – біт парності завжди дорівнює 1;

odd – біт парності дорівнює 0, якщо у переданому символі непарна кількість одиничних бітів;

space – біт парності завжди дорівнює 0;

Синтаксис команди **stopbits** (режим конфігурування лінії):

stopbits *value*,

де ***value*** – параметр, який може набувати значень 1; 1.5; 2. За замовчуванням – 2.

Синтаксис команди **flowcontrol** (режим конфігурування лінії):

flowcontrol *value* [lock] [in | out],

де ***value*** – параметр, який може набувати значень **none**, **hardware**, **software**, за замовчуванням керування потоком даних відсутнє;

none – параметр вимикання режиму керування потоком даних;

hardware – параметр вмикання режиму апаратного керування потоком даних;

software – параметр вмикання режиму програмного керування потоком даних;

lock – службова конструкція, яка забороняє вимикання режиму керування потоком даних, застосовується лише для параметра **software**;

in – параметр, який вказує на встановлення контролю потоку на вхід лінії;

out – параметр, який вказує на встановлення контролю потоку на вихід лінії;

Якщо не вказаний жоден із параметрів **in** або **out**, то вважається, що контроль потоку здійснюється в обох напрямках.

Синтаксис команди **default** (режим конфігурування лінії):

default *value*,

де ***value*** – параметр, який може набувати значень **speed, databits, parity, stopbits, flowcontrol, history size**

Для інших ліній можуть здійснюватися налагодження, подібні до тих, що здійснюються для консольної лінії.

Для зручності відображення інформації під час налагодження пристрою доцільно встановити параметри термінального вікна, у якому вводяться команди та виводяться їх результати. Правильний підбір параметрів допомагає розв'язати проблему занадто довгих рядків або їх великої кількості. Для налагодження ширини та висоти використовуються команди **width** та **length**. Повернення до стандартних розмірів здійснюється командами **no width** та **no length** відповідно.

Синтаксис команди **width** (режим конфігурування лінії):

width *columns*,

де ***columns*** – кількість стовпчиків вікна термінальної програми, за замовчуванням – 80.

Синтаксис команди **length** (режим конфігурування лінії):

length *lines*,

де ***lines*** – кількість рядків термінальної програми (може змінюватися в діапазоні від 0 до 512), за замовчуванням – 24.

У пристроях Cisco наявна можливість використовувати попередньо введені в сеансі роботи команди. Ця можливість називається ,,історія команд". Її можна використовувати як для пристрою в цілому, так і для окремих ліній. Включення і відключення режиму історії команд у цілому для пристрою здійснюється командами **history**, **no history.** Для встановлення кількості команд, які вводилися останніми і зберігаються у пам'яті пристрою, використовується команда **history size.** Налагодження даної команди зберігаються у конфігурації пристрою і застосовуються до всіх сеансів користувачів. Результати роботи команди переглядаються командою **show history**.

Синтаксис команди **history size** (режим конфігурування лінії):

history size *value*,

де ***value*** – кількість команд, про які повинен пам'ятати пристрій, може змінюватися в діапазоні від 0 до 255, за замовчуванням становить 10 команд.

Для поточного сеансу використовуються подібні команди: **terminal width**, **terminal length**, **terminal history**, **terminal history size**. Їх синтаксис аналогічний попередньо розглянутим командам.

Для поточного сеансу зв'язку по лінії існує можливість встановити певні часові періоди (тайм-аути) та режими його роботи, наприклад, інтервал часу, протягом якого сеанс може залишатися відкритим, інтервал часу, протягом якого сеанс зв'язку може бути неактивним, активацію виведення повідомлення у разі виходу із системи тощо. З цією метою використовуються команди **absolute-timeout**, **session-timeout**, **exec-timeout**, **logout-warning**, **logging synchronous** тощо.

Команда **absolute-timeout** встановлює чіткий інтервал часу до того моменту, коли сеанс буде закрито. На відміну від інших періодів, цей інтервал не залежить від періоду простою, тобто сеанс буде закрито через зазначений час, незалежно від того, активно використовується сеанс чи ні. Відміна дії команди **no absolute-timeout** або **absolute-timeout 0**. Команда **session-timeout** встановлює інтервал часу, протягом якого пристрій очікує передавання даних перед тим, як закрити сеанс, тобто інтервал простою для лінії. Відміна дії команди **no session-timeout** або **session-timeout 0**. Команда **exec-timeout** встановлює інтервал часу, протягом якого пристрій очікує введення даних в активному сеансі привілейованого режиму. Після закінчення даного інтервалу здійснюється перехід у попередній режим. Відміна дії команди **no exec-timeout** або **exec-timeout 0**.

Команда **logout-warning** активізує виведення попередження у разі виходу із системи. Це попередження інформує користувача, що найближчим часом відбудеться примусовий вихід із сеансу. Відміна дії команди **no logout-warning**. Команда **logging synchronous** керує виведенням журнальних повідомлень на термінал користувача. За замовчуванням повідомлення можуть виводитися у будь-який момент, часто перериваючи виконання поточної команди користувача. За допомогою команди **logging synchronous** можна примусити пристрій очікувати завершення поточної команди і виведення її результатів і лише після цього відображати журнальні повідомлення. Відміна дії команди **no logging synchronous**.

Синтаксис команди **absolute-timeout** (режим конфігурування лінії):

absolute-timeout *minutes*,

де ***minutes*** – тривалість періоду, протягом якого сеанс може залишатися відкритим, зазначається у хвилинах, може змінюватися у діапазоні від 0 до 10000; за замовчуванням значення дорівнює 0, тобто не визначене.

Синтаксис команди **session-timeout** (режим конфігурування лінії):

session-timeout *minutes* [output],

де ***minutes*** – тривалість періоду до моменту, як сеанс буде припинено за тайм-аутом; зазначається у хвилинах, може змінюватися у діапазоні від 0 до 35791; за замовчуванням дорівнює 0, тобто не визначено;

output – службова конструкція, яка примушує пристрій враховувати у разі обнулення лічильників як вхідний, так і вихідний трафік, якщо вона відсутня, то лише вхідний трафік викликає обнулення лічильника.

Синтаксис команди **exec-timeout** (режим конфігурування лінії):

exec-timeout *minutes*,

де ***minutes*** – тривалість періоду, протягом якого сеанс зв'язку може бути неактивним; зазначається у хвилинах, може змінюватися у діапазоні від 0 до 35791, за замовчуванням становить 10 хвилин; не рекомендується налаштовувати цей період занадто коротким, оскільки існує ймовірність втратити можливість контролю над пристроєм.

Синтаксис команди **logout-warning** (режим конфігурування лінії):

logout-warning *seconds*,

де ***seconds*** – тривалість періоду до завершення сеансу, може змінюватися в діапазоні від 0 до 4294967295; за замовчуванням значення не визначене.

Синтаксис команди **logging synchronous** (режим конфігурування лінії):

logging synchronous [level *importance* | all] [limit *number_of_messages*],

де **level** – службова конструкція, яка вказує на зміну рівня важливості команди;

importance – значення рівня важливості, змінюється від 0 до 7, за замовчуванням у разі активації команди без параметрів дорівнює 2; всі повідомлення даного і більш низького рівнів (із номерами біль-

ше даного) відправляються синхронно (тобто після того, як користувач завершить поточну команду, а пристрій виведе результат);

all – параметр, який вказує, що всі повідомлення відправляються синхронно;

limit – службова конструкція, яка вказує, що використовуються обмеження щодо кількості повідомлень;

number_of_messages – кількість повідомлень, які можуть бути розміщені в черзі доставки, максимальна – 20.

Системні повідомлення пристроїв Cisco

У пристроях Cisco передбачено кілька стандартних системних повідомлень (банерів) для користувачів. Як правило, ці повідомлення асоціюються з процесом входу в систему або виходу з неї. Виведення того чи іншого повідомлення (чи кількох почергово) залежить від налагоджень пристрою. У пристроях Cisco використовуються такі повідомлення:

Повідомлення дня (Motd Banner, Message of the Day).

Повідомлення входу в систему (Login Banner).

Повідомлення виконання (Exec Banner).

Повідомлення вхідного термінального з'єднання (Incoming Banner).

Повідомлення тайм-ауту входу в систему (Promt-Timeout Banner).

Повідомлення для протоколів SLIP/PPP.

Приклад використання кількох повідомлень-банерів може бути таким. При вході користувача виводиться повідомлення дня, після нього йде повідомлення входу в систему, а далі саме запрошення входу. Після успішної реєстрації на екрані виводиться повідомлення виконання. Для встановлення повідомлень-банерів використовується команда **banner**. Відключення виведення повідомлення здійснюється командою **no banner.**

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

banner ***btype*** **#** ***banner-text*** **#**,

де ***btype*** вказує тип банера і може набувати значень:

LINE – текстове повідомлення;

exec – повідомлення виконання;

incoming – повідомлення вхідного термінального з'єднання;

login – повідомлення входу в систему;

motd – повідомлення дня;

promt-timeout – повідомлення тайм-ауту входу в систему;

slip-ppp – повідомлення для протоколів SLIP/PPP;

banner-text # – текст повідомлення, **#** – знак початку і кінця повідомлення, замість цього знака можуть використовуватися будь-які символи, які не зустрічаються у тексті повідомлення.

Як правило, якщо повідомлення-банери встановлені, то вони виводяться на екран. Відключити виведення більшості повідомлень-банерів неможливо, їх можна лише видалити. Повідомлення виконання та повідомлення дня можна відключити чи включити, скориставшися командами **no exec-banner**, **no motd-banner** та **exec-banner**, **motd-banner**. Відключення повідомлення виконання призводить до відключення повідомлення дня, а відключення повідомлення дня не впливає на повідомлення виконання.

Типи паролів Cisco IOS

На пристроях Cisco існує можливість налагодити безпечний доступ для всіх видів підключень та певних режимів Cisco IOS із використанням парольного захисту. Для забезпечення парольного захисту на пристроях Cisco передбачено такі паролі:

Пароль ліній (пароль для входу в режим користувача).

Пароль входу у привілейований режим.

Паролі користувачів.

Перші два паролі встановлюються на пристрій у цілому й обмежують вхід до відповідних режимів. Паролі для користувачів можуть мати різний рівень привілеїв щодо виконання команд. Інформація про паролі та користувачів зберігається у конфігураційному файлі пристрою.

Для пристроїв Cisco використовуються три типи паролів:

Звичайний пароль (Plain-text password).

Пароль типу 7 (Type 7 password).

Пароль типу 5 (MD5 hash password).

Звичайні паролі встановлюються за замовчуванням і зберігаються у конфігураційному файлі пристрою у відкритому вигляді, що є загрозою безпеці. Паролі типу 7 для підвищення рівня безпеки використовують шифрування за алгоритмом Віженера (Vigenere). Паролі даного типу доволі легко розшифровуються, тому рекомен-

дується використовувати паролі типу 5, які мають найвищий рівень безпеки.

Налагодження парольного доступу на пристроях Cisco

Для налагодження доступу по лініях до пристрою Cisco використовуються команди **password** та **login**. Застосування цих команд передбачає те, що паролі є звичайними (відкритими). Для налагодження парольного доступу до привілейованого режиму у пристроях Cisco передбачено команду **enable password**. Якщо цю команду використати без параметрів, то пароль буде теж звичайним відкритим. Існує можливість використання цієї команди із встановленням шифрованого пароля типу 7. Для шифрування всіх паролів відразу (встановлення паролів типу 7) використовується команда **service password-encryption**. Оскільки пароль даного типу вважається слабким, використовувати дану команду не рекомендується. Замість неї рекомендується використовувати команду **enable secret**, яка активує використання шифрованих паролів типу 5. Існує можливість створення окремих користувачів із різними привілеями входу в різні режими на пристроях Cisco. Для цього використовується команда **username**. Відміна дії всіх розглянутих команд здійснюється за допомогою службової конструкції **no**.

Синтаксис команди **password** (режим конфігурування лінії):

password ***password-string***,

де ***password-string*** – текстовий рядок пароля довжиною до 80 символів, який повинен починатися з літери.

Синтаксис команди **login** (режим конфігурування лінії):

login {local},

де **local** – службова конструкція, яка вказує, що для входу необхідно використовувати імена створених користувачів та їх паролі.

Синтаксис команди **enable password** (режим глобального конфігурування):

enable password [level ***level-value*****]** **{*password-string* | [*encryption-type*] *encrypted-password-string*}**,

де **level** – службова конструкція, яка зазначає рівень привілеїв пароля.

level-value – значення рівня, число в межах від 0 до 15;

password-string – текстовий рядок пароля;

encryption-type – тип шифрування;

encrypted-password-string – зашифрований пароль, отриманий з іншого джерела шифрування.

Синтаксис команди **enable secret** (режим глобального конфігурування):

enable secret [level *level-value*] { *password-string* | [*encryption-type*] *encrypted-password-string* }.

Параметри команди аналогічні параметрам попередньої команди.

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

username *name* {nopassword | password *password-string* | password *encryption-type encrypted-password-string*},

де ***name*** – текстове ім'я користувача;

nopassword – службова конструкція, яка вказує на те, що не потрібно використовувати пароль;

password – службова конструкція, яка вказує на використання пароля;

password-string – текстовий рядок пароля;

encryption-type – тип шифрування.

encrypted-password-string – зашифрований пароль, отриманий з іншого джерела шифрування.

Основні команди діагностики параметрів роботи комутатора Cisco

Для виведення діагностичної інформації про фізичні параметри комутатора, результати налагоджень, результати роботи комутатора, стан комутатора тощо використовується команда **show**. Вона є доступною як із режиму користувача, так і з привілейованого режиму. Залежно від режиму дана команда може мати різні параметри. Частина параметрів є однаковими і доступними в обох режимах. Часто команда **show** із певним параметром уважається окремою командою. Перелік основних команд **show** та їх призначення наведені у табл. 8.

Таблиця 8

Перелік основних команд show

Команда	Призначення
show version	Виведення технічної інформації про пристрій
show tech-support	Виведення розширеної технічної інформації про пристрій
show flash	Виведення вмісту Flash-пам'яті
show boot	Виведення параметрів завантаження
show processes	Виведення інформації про стан процесів, що запущені в

	системі
show terminal	Виведення параметрів роботи термінала
show clock	Виведення параметрів системного часу
show history	Виведення історії команд
show running-config	Виведення поточної конфігурації комутатора
show startup-config	Виведення стартової конфігурації комутатора

Основні команди роботи з конфігураціями

Важливим питанням налагодження комутатора Cisco є перегляд та збереження його конфігурацій. Як уже зазначалося, для перегляду стартової конфігурації використовується команда **show startup-config,** а для перегляду поточної конфігурації – команда **show running-config**. Обов'язковим є збереження налагоджень поточної конфігурації у стартовій. Для цього використовується команда **copy running-config startup-config**. Існує можливість копіювання конфігурації на зовнішні сервери або із зовнішніх серверів. Це можуть бути традиційні FTP/TFTP або менш уживані SCP чи RCP-сервери.

Синтаксис команди **copy** (привілейований режим):

copy *source destination*,

де ***source***, ***destination*** – джерело та приймач даних відповідно.

Основні комбінації параметрів команди **copy** наведені у табл. 9.

Таблиця 9

Можливі комбінації параметрів команди *copy*

Джерело	Приймач				
	running-config	**startup-config**	**flash**	**ftp:**	**tftp:**
running-config	–	+	+	+	+
startup-config	+	–	+	+	+
flash	+	+	–	+	+
ftp:	+	+	+	–	–
tftp:	+	+	+	–	–

Для видалення стартової конфігурації використовується команда **erase startup-config**. Для перезавантаження пристрою використовується команда **reload**. Окрім зазначених команд для роботи з образами ОС та конфігураціями застосовуються команди **dir**, **more** та інші.

Також для роботи з поточною конфігурацією може використовуватися команда **write**. Вона вважається застарілою, і замість неї рекомендується використовувати команди **copy**, **show**, **erase**.

Синтаксис команди **write** (привілейований режим):

write { erase | memory | network | terminal },

де **erase** – параметр, який указує, що необхідно видалити стартову конфігурацію пристрою;

memory – параметр, який указує, що необхідно зберегти поточну конфігурацію пристрою;

network – параметр, який указує, що необхідно зберегти поточну конфігурацію на TFTP-сервері;

terminal – параметр, який указує, що необхідно вивести поточну конфігурацію на екран.

Відповідності застарілих команд **write** сучасним командам наведені у табл. 10.

Таблиця 10

Команди *write* та їх сучасні еквіваленти

Команда ***write***	Сучасний еквівалент
write erase	**erase startup-config**
write memory	**copy running-config startup-config**
write network	**copy running-config tftp**
write terminal	**show running-config**

Модельні приклади базового налагодження керованого комутатора Cisco

Розглянемо специфіку базового налагодження параметрів функціонування комутатора Cisco моделі WS-C2960-24TT-L за допомогою консольного підключення (рис. 18) із використанням Cisco Console Cable (Cisco USB Console Cable) та термінального додатка HyperTerminal. Слід зазначити, що параметри консольного підключення у разі першого підключення до нового пристрою Cisco (пристрою без конфігурації) зазначаються за замовчуванням. Результат такого підключення до нового комутатора Cisco (комутатора без конфігурації) наведено на рис. 19.

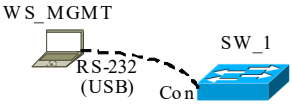


Рис. 18. Приклад консольного підключення

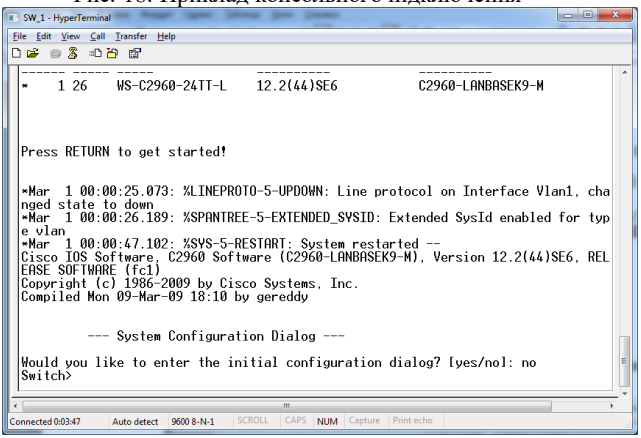


Рис. 19. Результат підключення до нового комутатора

Для налагодження основних параметрів комутатора та параметрів консольного підключення до комутатора використано дані табл. 11.

Таблиця 11

Параметри налагодження комутатора для прикладу

Параметр	**Значення**
Основні параметри	
Назва комутатора	SW-1
Повідомлення дня	1 рядок, текст – Switch SW-1 / Location – 101v
Параметри часу	
Системний час	Поточний (включає поточні час та дату)
Часовий пояс	Східноєвропейський (EET, Eastern European Time)
Перехід на літній час	Україна
Параметри консольного підключення	
Швидкість, біт/с	19200
Біти даних	7

Парність	Парні
Стопові біти	2
Керування потоком	Апаратне
Параметри термінального сеансу	
Історія команд, шт.	100
Тайм-аут виходу, с	30
Виведення журнальних повідомлень	Так

Сценарій налагодження основних параметрів комутатора (імені, повідовлення дня) наведений нижче. У цьому сценарії виконано збереження конфігурації та перезавантаження.

...

Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-1
SW-1(config)#banner motd #Switch SW-1 / Location – 101v#
SW-1(config)#exit
SW-1#copy running-config startup-config
SW-1#reload

...

Результат виконання даного сценарію у разі повторного підключення до комутатора наведений на рис. 20.

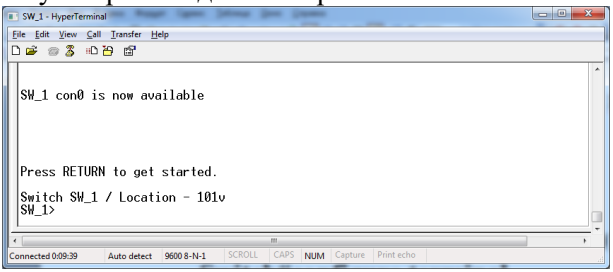


Рис. 20. Результат підключення до комутатора SW-1 після базового налагодження

Сценарій налагодження часових параметрів комутатора (часового поясу та поточного часу) наведений нижче. Слід зазначити, якщо має місце перезавантаження комутатора, то системний час потрібно встановити повторно, оскільки для моделі комутатора WS-C2960-24TT-L він не зберігається в апаратному годиннику.

...

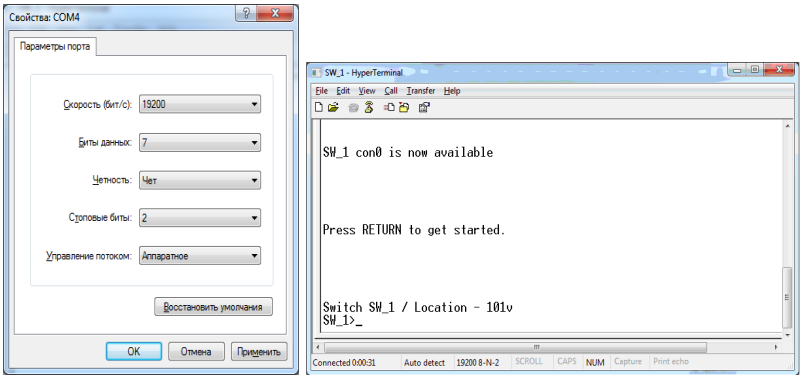
SW-1>enable
SW-1#configure terminal
SW-1(config)#clock timezone EET 2
SW-1(config)#exit

SW-1#clock set 8:00:00 01 may 2016
SW-1#copy running-config startup-config
SW-1#exit
SW-1>
...

Сценарій налагодження параметрів консольного підключення (лінії) до комутатора та термінального сеансу наведений нижче.

...
SW-1>enable
SW-1#configure terminal
SW-1(config)#line console 0
SW-1(config-line)#speed 19200
SW-1(config-line)#databits 7
SW-1(config-line)#parity even
SW-1(config-line)#stopbits 2
SW-1(config-line)#flowcontrol hardware
SW-1(config-line)#logging synchronous
SW-1(config-line)#history size 100
SW-1(config-line)#exec-timeout 30
SW-1(config-line)#end
SW-1#copy running-config startup-config
SW-1#exit
SW-1>
...

Для перевірки налагоджених за даним сценарієм параметрів консольного підключення необхідно перезапустити термінальний додаток, у якому встановити необхідні значення параметрів підключення. Результати налагодження параметрів для Windows-додатка HyperTerminal та результат виконання підключення наведено відповідно на рис. 21, а, б.



а б

Рис. 21. Результат налагодження:
а – параметрів підключення для Windows-додатка HyperTerminal;
б – консольного підключення до комутатора SW-1 та термінального сеансу

Сценарій налагодження доступу до комутатора з використанням механізму паролів наведено нижче (встановлюється пароль на вхід для консольного підключення та пароль на перехід до привілейованого режиму). Паролі зберігаються у файлі конфігурації у відкритому вигляді.

```
...
SW-1>enable
SW-1#configure terminal
SW-1(config)#line console 0
SW-1(config-line)#password mypass1
SW-1(config-line)#login
SW-1(config-line)#exit
SW-1(config)#enable password mypass2
SW-1(config)#exit
SW-1#exit
SW-1>
...
```

Файл конфігурації, що створений як результат виконання попередніх трьох сценаріїв, і виведений за допомогою команди **show running-config** наведений на рис. 22 (частину файла, яка містить несуттєву інформацію, вилучено; жирним шрифтом виділено додані за останнім сценарієм рядки конфігурації).

```
Building configuration...

Current configuration : 1288 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW-1
!
enable password mypass2
!
clock timezone EET 2
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
...
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^C Switch SW-1
Location - 101v^C
!
!
line con 0
 password mypass1
 logging synchronous
 login
 history size 100
 exec-timeout 30 0
 speed 19200
 databits 7
 parity even
 stopbits 2
 flowcontrol hardware
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

Рис. 22. Файл конфігурації комутатора SW-1 для модельного прикладу з використанням відкритих паролів

Сценарій налагодження доступу до комутатора з використанням механізму користувачів та паролів типу 7 наведено нижче (; встановлюється пароль на вхід у привілейований режим; створюються користувач User1 із рівнем привілеїв 1 (за замовчуванням) та користувач Admin із максимальним рівнем привілеїв 15; відключається пароль на вхід для консольного підключення; активується застосування механізму користувачів для консольного підключення; здійснюється операція шифрування звичайних відкритих паролів із метою отримання паролів типу 7).

...
SW-1#configure terminal
SW-1(config)#enable password mypass2
SW-1(config)#username User1 password mypass3
SW-1(config)#username Admin privilege 15 password mypass4
SW-1(config)#line console 0
SW-1(config-line)#no password
SW-1(config-line)#login local
SW-1(config-line)#exit
SW-1(config)#service password-encryption
SW-1(config)#exit
SW-1#
...

Файл конфігурації, що створений як результат виконання цього сценарію, наведено на рис. 23 (частину файла, яка містить несуттєву інформацію, вилучено; жирним шрифтом виділено модифіковані та додані рядки конфігурації).

```
Building configuration...

Current configuration : 1442 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SW-1
!
enable password 082C555E080A1645
!
clock timezone EET 2
!
username Admin privilege 15 password 7 082C555E080A1643
username User1 privilege 1 password 7 082C555E080A1644
!
spanning-tree mode pvst
```

```
!
interface FastEthernet0/1
!
...
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
banner motd ^CSwitch SW-1
Location - 101v^C
!
line con 0
 logging synchronous
 login local
 history size 100
 exec-timeout 30 0
 speed 19200
 databits 7
 parity even
 stopbits 2
 flowcontrol hardware
!
line vty 0 4
 login
line vty 5 15
 login
end
```

Рис. 23. Файл конфігурації комутатора SW-1 для модельного прикладу з використанням механізму користувачів та шифрованих паролів типу 7

Для підвищення рівня безпеки комутатора рекомендується замість паролів типу 7 застосовувати паролі типу 5. У такому разі краще застосовувати наведений нижче модифікований сценарій налагодження доступу до комутатора.

```
...
SW-1#configure terminal
SW-1(config)#no enable password
SW-1(config)#enable secret mypass2
SW-1(config)#no username User1
SW-1(config)#no username Admin
SW-1(config)#username User1 secret mypass3
SW-1(config)#username Admin privilege 15 secret mypass4
SW-1(config)#line console 0
SW-1(config-line)#login local
SW-1(config-line)#exit
SW-1(config)#
```

...

Результати виконання команд моніторингу та діагностики роботи комутатора для розглянутого модельного прикладу

З метою перегляду інформації про налагоджені параметри системного часу для розглянутого прикладу виконано команду **show clock**. Із метою визначення параметрів консольного підключення та термінального вікна виконано команду **show terminal**. Із метою визначення імені користувача, що здійснив підключення до пристрою, та рівня його привілеїв виконано команди **show users** та **show privilege**. Результати роботи зазначених команд наведено відповідно на рис. 24 – 26.

```
SW-1#show clock
11:17:37.780 EET Sun May 1 2016
SW-1#
```

Рис. 24. Результати виконання команди **show clock** на комутаторі SW-1

```
SW-1#show terminal
Line 0, Location: , Type:
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 19200/19200, even parity, 2 stopbits, 7 databits
Status: PSI Enabled, Ready, Active, Automore On
Capabilities: none
Modem state: Ready
Modem hardware state: CTS* noDSR DTR RTS
Special Chars: Escape  Hold  Stop  Start  Disconnect Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer Session   Dispatch
               00:10:00        never                  none     not set
                            Idle Session Disconnect Warning
                              never
                            Login-sequence User Response
                             00:00:30
                            Autoselect Initial Wait
                              not set
Modem type is unknown.
Session limit is not set.
Time since activation: 00:03:04
Editing is enabled.
History is enabled, history size is 100.
DNS resolution in show commands is enabled
Full user help is disabled
Allowed input transports are All.
Allowed output transports are pad telnet rlogin.
Preferred transport is telnet.
No output characters are padded
No special data dispatching characters
```

Рис. 25. Результати виконання команди **show terminal** на комутаторі SW-1

```
SW-1#show users
    Line         User        Host(s)       Idle          Location
*  0 con 0       Admin       idle          00:00:00
   Interface     User        Mode          Idle        Peer Address
SW-1#show privilege
Current privilege level is 15
```

Рис. 26. Результати виконання команди **show users** та **show privilege** на комутаторі SW-1

Завдання на лабораторну роботу

1. Розглянути та скласти повну і спрощену схеми нуль-модемного кабелю, побудованого з використанням двох рознімів DB-9. На схемах зазначити відповідні сигнали для відповідних контактів.

2. На основі схем з'єднань п. 1 та відповідних таблиць сигналів, наведених у теоретичних відомостях, скласти повну і спрощену схеми нуль-модемного кабелю, побудованого з використанням двох рознімів DB-25.

3. На основі схем з'єднань п. 1 та відповідних таблиць сигналів, наведених у теоретичних відомостях, скласти повну і спрощену схеми нуль-модемного кабелю, побудованого з використанням рознімів DB-9 та DB-25.

4. На основі схем з'єднань п. 1 та відповідних таблиць сигналів, наведених у теоретичних відомостях, скласти повну і спрощену схеми кабелю Cisco Rollover Cable, побудованого з використанням двох рознімів RJ-45.

5. На основі схем з'єднань п. 1 та відповідних таблиць сигналів, наведених у теоретичних відомостях, скласти повну і спрощену схеми кабелю Cisco Console Cable, побудованого з використанням рознімів DB-9 та RJ-45. На схемах зазначити відповідні сигнали для відповідних контактів.

6. На основі схем з'єднань п. 1 та відповідних таблиць сигналів, наведених у теоретичних відомостях, скласти повну і спрощену схеми кабелю Cisco Console Cable, побудованого з використанням рознімів DB-25 та RJ-45.

7. У середовищі програмного симулятора/емулятора створити проект мережі, у якому здійснити фізичне підключення робочої станції до комутатора за допомогою консольного кабелю (рис. 27). Виконати підключення з робочої станції до комутатора за допомогою термінальної програми. Визначити основні параметри комутатора та занотувати їх у вигляді табл. 12.

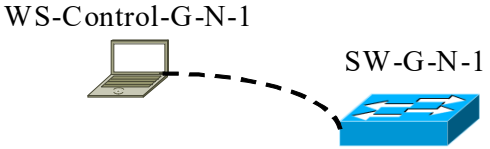


Рис. 27. Схема підключення

Таблиця 12

Параметри комутатора

Параметр	Значення
Модель комутатора	
Модель та номер процесора	
Об'єм пам'яті (RAM, Flash, NVRAM)	
Кількість інтерфейсів Ethetnet/Fast Ethernet	
Кількість інтерфейсів Gigabit Ethernet	
Серійний номер системи	
Серійний номер материнської плати	
Серійний номер блока живлення	
Базова MAC адреса блока управління	
Конфігураційний регістр	
Версія IOS	
Образ IOS	
Розмір файла образу IOS	

8. Провести налагодження параметрів іменування, системного часу (за даними табл. 13), системних повідомлень-банерів, консольного підключення та термінального сеансу (за даними табл. 14). Зберегти налагодження. Перезавантажити комутатор та перевірити можливість підключення за допомогою термінальної програми з налагодженими параметрами, вивести параметри налагоджень поточного термінального сеансу.

9. Провести налагодження парольного доступу до комутатора (його режимів користувача та привілейованого режиму) із використанням відкритих паролів. Зберегти налагодження. Перезавантажити комутатор та перевірити виконані налагодження. Зашифрувати паролі за типом 7 та перевірити результати шифрування.

10. Провести налагодження доступу до комутатора з використанням механізму користувачів. Для цього створити трьох користувачів (два користувачі з мінімальним рівнем привілеїв 0 – Technic-G-N-X, один – із максимальним рівнем привілеїв 15 – Admin-G-N-1). Зберегти налагодження. Перезавантажити комутатор та перевірити виконані налагодження. Дослідити відмітності у можливостях для користувачів із різними рівнями привілеїв.

11. Вивести та проаналізувати файл конфігурації комутатора.

Таблиця 13

Параметри налагодження системного часу

№ варіанта	Часовий пояс	Години	Хвилини	Перехід на літній час
1	GMT	0	00	+
2	BST	+1	00	+
3	IST	+1	00	+
4	WET	0	00	+
5	WEST	+1	00	+
6	CET	+1	00	+
7	CEST	+2	00	+
8	EET	+2	00	+
9	EEST	+3	00	+
10	MSK	+4	00	+
11	GMT	0	30	+
12	BST	+1	30	+
13	IST	+1	30	+
14	WET	0	30	+
15	WEST	+1	30	+
16	CET	+1	30	+
17	CEST	+2	30	+
18	EET	+2	30	+
19	EEST	+3	30	+
20	MSK	+4	30	+
21	GMT	0	00	+
22	BST	+1	00	+
23	IST	+1	00	+
24	WET	0	00	+
25	WEST	+1	00	+
26	CET	+1	30	+
27	CEST	+2	30	+
28	EET	+2	30	+
29	EEST	+3	30	+
30	MSK	+4	30	+

Примітка: GMT, Greenwich Mean Time (UTC); BST, British Summer Time (UTC + 1 год.); IST, Irish Standard Time (UTC + 1 год.); WET, Western European Time (UTC); WEST, Western European Summer Time (UTC + 1 год.); CET, Central European Time (UTC + 1 год.); CEST, Central European Summer Time (UTC + 2 год.); EET, Eastern European Time (UTC + 2 год.); EEST, Eastern European Summer Time (UTC + 3 год.); MSK, Moscow Standard Time (UTC + 4 год.).

Таблиця 14

Параметри налагодження консольного підключення та сеансу

№ варіанта	Speed, біт/с	Databits	Parity	Stopbits	Flow-control	History size	Width, стовпчиків	Length, рядків	Exec-timeout, хв	Logout-warning, с	Logging synchronous
1	1200	7	even	1	None	20	80	24	20	20	+
2	115200	8	odd	2	Software	50	75	24	60	30	+
3	2400	7	none	1	Hardware	25	70	24	30	40	+
4	115200	8	mark	2	None	45	65	24	40	40	+
5	4800	7	space	1	Hardware	30	60	24	50	30	+
6	57600	8	mark	2	Software	35	80	22	60	30	+
7	9600	7	none	1	Software	15	75	22	15	20	+
8	38400	8	odd	2	None	65	70	22	55	20	+
9	19200	7	even	1	Hardware	20	65	22	20	20	+
10	2400	8	odd	2	Software	60	60	22	50	30	+
11	57600	7	mark	1	Hardware	25	80	20	25	20	+
12	1200	8	even	2	None	55	75	20	45	30	+
13	115200	7	none	1	Hardware	30	70	20	30	30	+
14	9600	8	space	2	Software	50	65	20	40	30	+
15	19200	7	even	1	None	35	60	20	35	30	+
16	4800	8	none	2	Hardware	45	60	24	50	40	+
17	38400	7	space	1	None	40	65	24	10	20	+
18	4800	8	odd	2	Software	10	70	24	45	30	+
19	38400	7	mark	1	None	50	75	24	15	20	+
20	1200	8	even	2	Software	15	80	24	40	20	+
21	115200	7	odd	1	Hardware	45	60	22	20	20	+
22	9600	8	mark	2	None	20	65	22	35	30	+

23	19200	7	space	1	Hardware	40	70	22	25	20	+
24	2400	8	none	2	Software	25	75	22	30	30	+
25	57600	7	even	1	Software	35	80	22	60	60	+
26	19200	8	mark	2	None	30	60	20	35	30	+
27	57600	7	odd	1	Hardware	60	65	20	55	60	+
28	9600	8	none	2	Software	80	70	20	40	40	+
29	38400	7	space	1	Hardware	65	75	20	50	60	+
30	115200	8	none	2	None	75	80	20	45	40	+

Примітки: 1) Параметр Software, який налаштовується на пристроях Cisco, відповідає параметру Xon/Xoff термінальних програм.

2) Налаштовані значення, які збігаються із тими, що передбачені за замовчуванням, у конфігураційному файлі не відображаються.

Контрольні питання

1. Типова структурна схема комутатора Ethernet фірми Cisco.
2. Кабельні підключення, що застосовуються з метою налагодження та керування комутатором Cisco.
3. Наведіть повну і спрощену схеми кабелю Cisco Rollover Cable.
4. Наведіть повну і спрощену схеми кабелю Cisco Console Cable.
5. Програмне забезпечення сучасних комутаторів Ethernet.
6. Загальна характеристика Cisco IOS. Платформи, набори можливостей та версії Cisco IOS, які використовуються для комутаторів Cisco.
7. Командні режими Cisco IOS для комутаторів Cisco. Команди переходів між командними режимами Cisco IOS для комутаторів.
8. Особливості отримання довідкової інформації у командному рядку Cisco IOS.
9. Наведіть перелік та поясніть призначення основних команд налагодження системного часу в комутаторах Cisco.
10. Наведіть перелік та поясніть призначення команд іменування пристроїв та створення системних повідомлень для пристроїв Cisco.
11. Наведіть перелік та поясніть призначення основних команд налагодження консольного підключення для пристроїв Cisco.
12. Наведіть перелік та поясніть призначення основних команд налагодження часових тайм-аутів та команд термінального виведення для пристроїв Cisco.
13. Наведіть перелік та поясніть призначення основних команд, що стосуються роботи з конфігураціями пристроїв Cisco.
14. Парольний доступ до пристроїв Cisco.

15. Наведіть перелік та поясніть призначення основних команд налагодження парольного доступу до пристроїв Cisco.

Лабораторна робота 2
НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ МЕРЕЖНИХ З'ЄДНАНЬ ETHERNET, ПОБУДОВАНИХ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: розглянути засоби організації мережних з'єднань між кінцевими та проміжними пристроями мережі Ethernet; ознайомитися з можливостями керованих комутаторів Cisco та мережної операційної системи Cisco IOS щодо налагодження мережних інтерфейсів та мережних з'єднань Ethernet; отримати практичні навички налагодження, моніторингу та діагностування роботи мережних інтерфейсів та мережних з'єднань Ethernet кінцевих вузлів, керованих комутаторів та маршрутизаторів Cisco.

Теоретичні відомості

Мережні інтерфейси та кабельні з'єднання Ethernet

Мережний інтерфейс (Network Interface) – фізичний (або віртуальний) пристрій, призначений для передавання даних у мережу та приймання даних із мережі. Мережний інтерфейс Ethernet – це фізичний пристрій, який є складовою кінцевого або проміжного вузла мережі. Цей інтерфейс забезпечує фізичне підключення вузла до середовища передачі даних та проводить інформаційний обмін з іншими вузлами мережі. Мережний інтерфейс Ethernet є пристроєм, що виконує фунції фізичного і канального (MAC-підрівень) рівнів моделі OSI. Стосовно стеку TCP/IP мережний інтерфейс Ethernet є пристроєм, що виконує фунції рівня мережних інтерфейсів. Прикладами мережних інтерфесів Ethernet є мережні адаптери/плати робочих станцій та серверів, порти комутаторів або точок доступу, мережні інтерфейси, плати та модулі маршрутизаторів тощо.

Відповідно до функцій рівнів моделі OSI мережний інтерфейс Ethernet фактично розглядається як сукупність фізичного і логічного інтерфейсів. Фізичний інтерфейс забезпечує фізичне підключення до середовища передачі даних та вирішує питання передавання/приймання сигналів. Логічний інтерфейс забезпечує опрацювання сукупності сигналів як повідомлень певного формату.

Згідно зі стандартом (ISO/IEC/IEEE 8802-3:2014 „Standard for Ethernet") для побудови кабельних з'єднань мереж Ethernet можуть застосовуватися такі фізичні середовища передачі даних, як коаксі-

альний кабель, вита пара, волоконно-оптичний кабель. У сучасній практиці побудови мереж коаксіальний кабель є застарілим середовищем і майже не застосовується. Вита пара є основним середовищем, що застосовується для підключень пристроїв, які знаходяться на невеликих відстанях (до 100 м) один від одного. У сучасних мережах застосовується вита пара категорії 5е і вище. Волоконно-оптичний кабель є основним середовищем, що застосовується для підключень на великі відстані (сотні метрів і більше). У сучасних мережах застосовується як одномодовий, так і багатомодовий волоконно-оптичний кабель.

Для технологій Ethernet, які як середовище передачі даних застосовують 8-провідникову виту пару (Ethernet 10Base-T, Fast Ethernet 100Base-TX, Gigabit Ethernet 1000Base-T тощо) основним фізичним рознімом є 8-контактний рознім, відомий під назвою RJ-45 (Registered Jack). У деяких джерелах замість позначення RJ-45 рекомендується застосовувати більш коректне позначення 8P8C (8 Position 8 Contact). Зовнішній вигляд 8-позиційних модульної вилки та гнізда рознімy RJ–45 наведено на рис. 1.

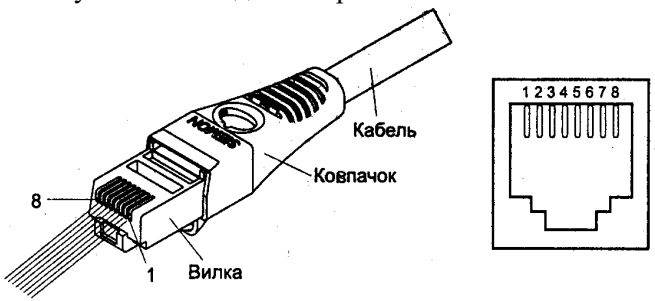


Рис. 1. Модульна вилка та гніздо рознімy RJ–45

Слід зазначити, що гнізда рознімy RJ–45 мережних адаптерів та комунікаційних пристроїв для забезпечення коректного використання полярності сигналів поділяються на два види:

– гнізда RJ–45 MDI (Media Dependent Interface);

– гнізда RJ–45 MDIX (Media Dependent Interface Xover= Crossover).

Призначення контактів та сигналів рознімy RJ–45 технологій Ethernet 10Base-T, Fast Ethernet 100Base-TX та Gigabit Ethernet 1000Base-T для гнізд MDI/MDIX наведено у табл. 1. Типові гнізда

розніму RJ–45 найпоширеніших мережних пристроїв Ethernet наведені у табл. 2.

Таблиця 1

Контакти та сигнали розніму RJ–45

Контакт	Технології 10Base-T/100Base-TX		Технологія 1000Base-T	
	MDI	MDIX	MDI	MDIX
1	Tx+ (Передавання+)	Rx+ (Приймання+)	BI_DA+	BI_DB+
2	Tx– (Передавання–)	Rx– (Приймання–)	BI_DA–	BI_DB–
3	Rx+ (Приймання+)	Tx+ (Передавання+)	BI_DB+	BI_DA+
4	Не задіяний	Не задіяний	BI_DC+	BI_DD+
5	Не задіяний	Не задіяний	BI_DC–	BI_DD–
6	Rx– (Приймання–)	Tx– (Передавання–)	BI_DB–	BI_DA–
7	Не задіяний	Не задіяний	BI_DD+	BI_DC+
8	Не задіяний	Не задіяний	BI_DD–	BI_DC–

Таблиця 2

Типові гнізда пристроїв технологій Ethernet для розніму RJ-45

Пристрій	Гніздо	Пристрій	Гніздо
Мережний адаптер (NIC)	MDI	Повторювач (Repeater)	MDIX
Маршрутизатор (Router)	MDI	Концентратор (Hub)	MDIX
Точка доступу (Access Point)	MDI	Міст (Bridge)	MDIX
IP-Телефон (IP-Phone)	MDI	Комутатор (Switch)	MDIX
VoIP шлюз (VoIP Gateway)	MDI	DSL-модем (DSL-Modem)	MDIX
Мережний принтер (Network Printer)	MDI	Кабельний модем (TV Cable Modem)	MDIX

У багатьох моделях концентраторів та комутаторів наявні додаткові порти RJ–45 ,,Up-Link", що призначені для з'єднання пристроїв між собою, підключення концентратора чи комутатора до маршрутизатора тощо. Порти ,,Up-Link" типово є портами MDI. У деяких старих моделях концентраторів та комутаторів один із звичайних портів RJ-45 (зазвичай перший або останній) також може бути портом ,,Up-Link", у цьому разі переключення між MDI/MDIX для порту здійснюється фізично за допомогою перемикача.

У варіантах технології Ethernet 10Base-T та Fast Ethernet 100Base-TX для забезпечення передачі даних застосовуються дві з наявних чотирьох пар провідників. Кожна з пар є окремим симплексним каналом передачі. По одній із пар передача здійснюється в одному напрямку, по іншій – у протилежному. Разом вони фор-

мують дуплексний канал передачі. У технології Gigabit Ethernet 1000Base-T застосовуються всі чотири пари провідників. По кожній парі передача здійснюється у двох напрямках одночасно.

З метою з'єднання порту MDI одного пристрою з портом MDIX іншого пристрою застосовується прямий кабель Ethernet (Ethernet Straight-Through Cable). З метою з'єднання двох пристроїв, які мають однакові порти (MDI–MDI чи MDIX–MDIX), застосовується перехресний кабель Ethernet (Ethernet Crossover Cable). Схеми з'єднання контактів розніму RJ-45 прямого та перехресного кабелів для технологій Ethernet 10Base-T та Fast Ethernet 100Base-TX наведені на рис. 2, а та рис. 2, б відповідно. Мінімальна рекомендована стандартом довжина кабелю Ethernet – 0,5 м. Максимальна можлива довжина – 100 м. Допускається використання кабелів більшої довжини (на 10–15%), при цьому необхідно контролювати якість та втрати сигналу. Для зручності підключення до пристроїв із метою адміністрування розроблено модульний адаптер-перехідник (Ethernet Crossover Adapter), який дає змогу ,,перетворити" прямий кабель Ethernet у перехресний.

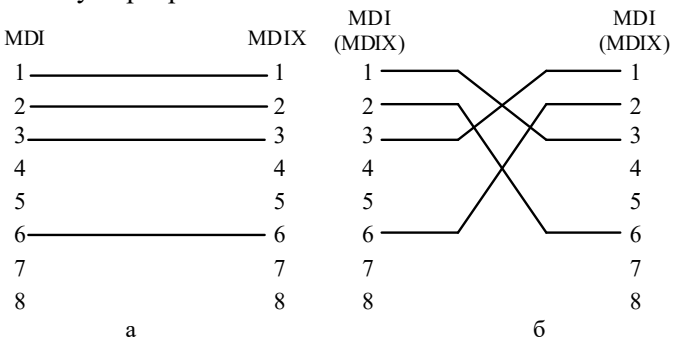


Рис. 2. Схеми кабелів Ethernet 10BaseT/ Fast Ethernet 100Base-TX:
а – прямий кабель; б – перехресний кабель

Вибір провідника витої пари за кольором для відповідного контакту вилки RJ-45 прямого чи перехресного кабелю Ethernet визначається вимогами стандарту побудови структурованих кабельних мереж у комерційних будівлях TIA-568 ,,Commercial Building Telecommunications Cabling Standard Set". У цьому стандарті описано два варіанти використання кольорів – так звані монтажні схеми

(таблиці, ,,розкладки") T568A та T568B. Параметри цих схем наведені у табл. 3. Найпоширенішою сьогодні є монтажна схема T568B.

Таблиця 3

Параметри монтажних схем T568A та T568B

Контакт	Монтажна схема T568A		Монтажна схема T568B	
	Колір: основний/смужки	Номер пари	Колір: основний/смужки	Номер пари
1	Білий/зелений	3 (Tip – прямий)	Білий/помаранчевий	2 (Tip – прямий)
2	Зелений	3 (Ring – зворотний)	Помаранчевий	2 (Ring – зворотний)
3	Білий/помаранчевий	2 (Tip)	Білий/зелений	3 (Tip)
4	Помаранчевий	1 (Ring)	Синій	1 (Ring)
5	Білий/синій	1 (Tip)	Білий/синій	1 (Tip)
6	Синій	2 (Ring)	Зелений	3 (Ring)
7	Білий/коричневий	4 (Tip)	Білий/коричневий	4 (Tip)
8	Коричневий	4 (Ring)	Коричневий	4 (Ring)

У багатьох сучасних мережних адаптерах, комутаторах та маршрутизаторах Ethernet на інтерфейсах RJ-45 підтримується функція автоматичного визначення полярності сигналів, що передаються по витій парі, відома як Auto-MDI. Функція Auto-MDI, залежно від того, прямий чи перехресний кабель Ethernet використано для підключення пристрою до комутатора, забезпечує автоматичне переведення інтерфейсу з MDI у MDIX і навпаки. У деяких моделях комутаторів реалізація функції Auto-MDI є ще більш інтелектуальною – дає змогу коректно передавати дані через кабелі, які мають некоректне з'єднання контактів.

Необхідно зазначити, що мережні інтерфейси технологій Ethernet 10Base-T, Fast Ethernet 100Base-TX, Gigabit Ethernet 1000Base-T, окрім підтримки автоматичного визначення полярності сигналів за допомогою функції Auto-MDI, також забезпечують автоматичне узгодження швидкостей і режимів передачі за допомогою функції Auto-Negotiation.

Для технологій Ethernet, які як середовище передачі даних використовують волоконно-оптичний кабель (Fast Ethernet 100Base-FX Gigabit Ethernet 1000Base-SX, 1000Base-LX тощо), застосовуються фізичні рознімі SC (Subscriber Connector), LC (Lucent Connector), ST (Straight Tip), FC (Ferrule Connector), MTRJ (Mechanical Transfer Registered Jack). Найбільш уживаними у практиці є рознімі SC та LC. Рознімі ST та FC застосовуються рідше. Рознім MTRJ є застарілим, застосовується лише у тих випадках, коли йому немає сучасної альтернативи. Загальна інформація та зовнішній вигляд модульних вилок основних оптичних рознімів наведені у табл. 4.

Для передачі даних у волоконно-оптичному каналі може застосовуватися як два, так і одне волокно. У випадку застосування двох волокон кожне оптичне волокно є окремим симплексним каналом передачі. Два волокна, по яких дані передаються у протилежних напрямках, разом формують дуплексний канал. Нині набули поширення варіанти технології, які дають змогу організувати дуплексну передачу по одному оптичному волокну.

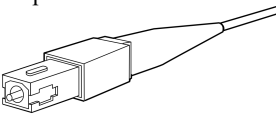
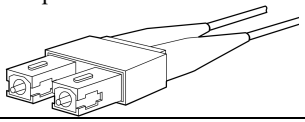
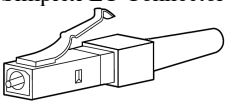
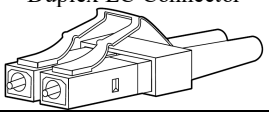
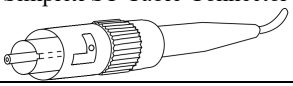
У сучасних пристроях Ethernet (мережних адаптерах, портах комутаторів тощо) фіксовані рознімі для підключення пристроїв за допомогою волоконно-оптичного кабелю застосовуються досить рідко. У більшості пристроїв замість фіксованих оптичних інтерфейсів застосовуються інтерфейсні слоти для змінних мережних інтерфейсних модулів (трансиверів), які дають змогу здійснювати підключення пристроїв різних технологій Ethernet. Іноді ці модулі називають ,,медіаконверторами" (MediaConvertors). Деякі моделі модулів дають змогу підключати і пристрої інших технологій, зокрема, Fibre Channel, SONET/SDH.

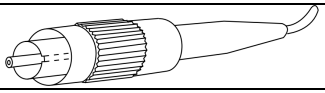
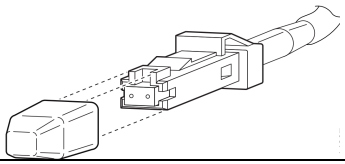
Стандартизацією змінних інтерфейсних модулів займається комітет SFF (Small Form Factor Committee). Першим стандартом, який описував вимоги до модулів GBIC, є стандарт INF-8053i ,,Specification for GBIC (Gigabit Interface Converter)", що з'явився у 2000 році. Через рік було розроблено стандарт для модулів SPF INF-8074i ,,Specification for SFP (Small Form Factor Pluggable) Transceiver". Пізніше були розроблені стандарти для модулів SFP+, XFP, CFP, QSFP, QSFP+, XENPAK, XPAK, X2. Зовнішній вигляд

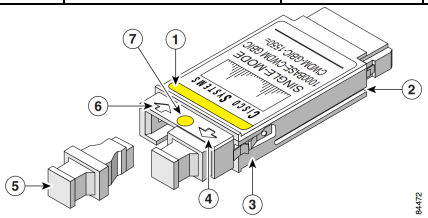
найпоширеніших мережних інтерфейсних модулів наведено на рис. 3 – 9.

Таблиця 4

Модульні вилки оптичних рознімів

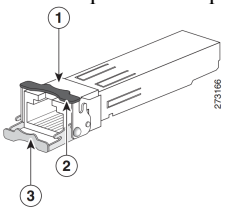
Скорочена назва	Повна назва	Стандарт	Зображення рознiму
SC	Subscriber Connector / Square Connector / Standard Connector	IEC 61754-4	Simplex SC Cable Connector  Duplex SC Cable Connector 
LC	Lucent Connector / Little Connector / Local Connector	IEC 61754-20	Simplex LC Connector  Duplex LC Connector 
ST/BFOC	Straight Tip / Bayonet Fiber Optic Connector	IEC 61754-2	Simplex ST Cable Connector 
FC	Ferrule Connector / Fiber Channel	IEC 61754-13	Simplex FC Cable Connector

			
MTRJ	Mechanical Transfer Registered Jack / Media Termination - Recommended Jack	IEC 61754-18	MTRJ Cable Connector 



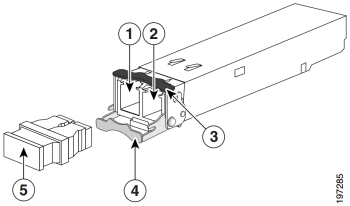
1 – кольорова смужка
2 – направляюча канавка
3 – пружинний фіксатор
4 – оптичний канал передавання
5 – захисна протипилова заглушка
6 – оптичний канал приймання
7 – кольорова точка

Рис. 3. Мережний інтерфейсний модуль GBIC (рознім SC)



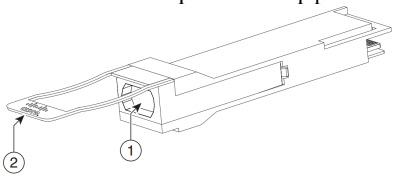
1 – гніздо рознімy RJ-45
2 – фіксатор у закритому стані
3 – фіксатор у відкритому стані

Рис. 4. Мережний інтерфейсний модуль SFP (рознім RJ-45)



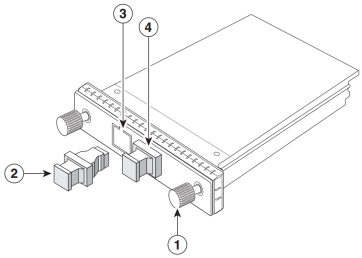
1 – оптичний канал приймання
2 – оптичний канал передавання
3 – фіксатор у закритому стані
4 – фіксатор у відкритому стані
5 – захисна протипилова заглушка

Рис. 5. Мережний інтерфейсний модуль SFP+ (рознім LC)



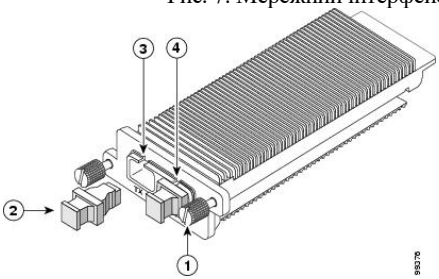
1 – оптичний канал
2 – „язичковий” фіксатор

Рис. 6. Мережний інтерфейсний модуль QSFP+



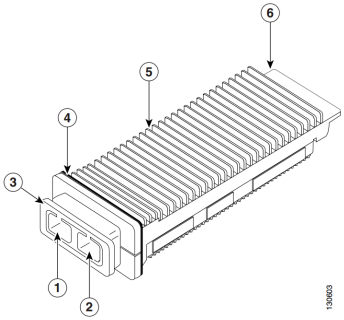
1 – кріпильний гвинт
2 – захисна протипилова заглушка
3 – оптичний канал передавання
4 – оптичний канал приймання

Рис. 7. Мережний інтерфейсний модуль CFP



1 – кріпильний гвинт
2 – захисна протипилова заглушка
3 – оптичний канал передавання
4 – оптичний канал приймання

Рис. 8. Мережний інтерфейсний модуль XENPAK



1 – оптичний канал передавання
2 – оптичний канал приймання
3 – механізм фіксації
4 – прокладка EMI
5 – тепловідвідний радіатор
6 – рознім

Рис. 9. Мережний інтерфейсний модуль X2

Мережні інтерфейсні модулі реалізовуються як для підключення пристроїв за допомогою витої пари, так і за допомогою волоконно-оптичного кабелю. У першому випадку застосовується рознім RJ-45. У другому випадку, як правило, розніми SC, LC. Варіанти використання рознімів для найуживаніших нині інтерфейсних модулів наведено у табл. 5.

Таблиця 5

Мережні інтерфейсні модулі та їх параметри

Скорочена назва	Повна назва	Основний стандарт	Рознім		
			RJ-45	SC	LC

GBIC	GigaBit Interface Converter	INF-8053i	+	+	
SFP	Small Form-factor Pluggable	INF-8074i	+	+	+
SFP+	Enhanced Small Form-factor Pluggable	SFF-8431	+	+	+
XFP	10 GE Small Form-factor Pluggable	INF-8077i		+*	+
CFP	C (Centrum, 100 GE) Form-factor Pluggable			+*	+
QSFP, QSFP+	Quad (4-Channel) Small Form-factor Pluggable	INF-8438i		+*	+
XENPAK	XENPAK	INF-8474i		+*	+
XPAK	XPAK	INF-8475i		+*	+
X2	X2	INF-8476i		+*	+

* застосовується рідко

Мережні адаптери Ethernet

Мережний адаптер (Network Adapter), мережна плата/контролер Ethernet (NIC, Network Interface Card/Controller) – є різновидом мережних інтерфейсів Ethernet, що орієнтовані на застосування у робочих станціях та серверах. Відповідно він забезпечує основні функції мережного інтерфейсу – передавання даних у середовище і приймання даних з середовища.

Типову структурну схему мережного адаптера Ethernet наведено на рис. 10. Основними його складовими є:

– фізичний рознім (MDI, Media Dependent Interface);

– блок фізичного рівня, трансивер Ethernet (Ethernet PHY, Ethernet Physical Layer Device, Ethernet PHY Tranciever/Reciever);

– блок MAC (MAC ASIC);

– блок керування автопереговорами (Auto-Negotiation Control);

– блок керування світлодіодними індикаторами (LED Control);

– мікросхема завантаження з мережі (Boot ROM);

– блок перезаписуваної пам’яті (EEPROM);

– інтерфейс підключення до комп’ютера (PCI, PCI-x, PCI Express тощо).

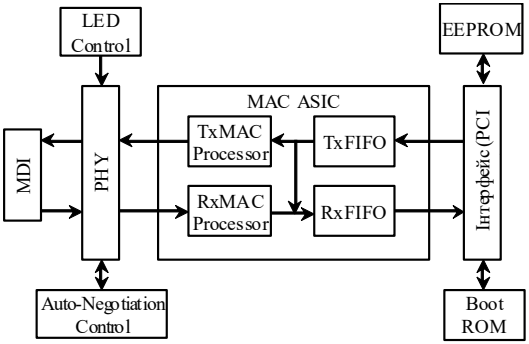


Рис. 10. Типова структурна схема мережного адаптера Ethernet

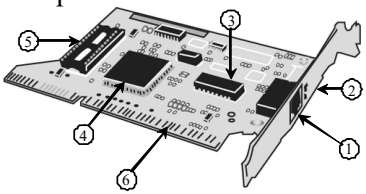
Для загального позначення рознімів мережних адаптерів Ethernet застосовується скорочення MDI, Media Dependent Interface, яке перекладається як ,,залежний від середовища інтерфейс". MDI забезпечує безпосереднє підключення адаптера до фізичного середовища передачі даних. Блок фізичного рівня PHY забезпечує приймання фізичних сигналів із середовища, перетворення їх у бітові послідовності та передачу цих послідовностей для подальшого опрацювання MAC ACIS. Блок PHY також виконує зворотні дії: отримує дані від MAC ACIS, формує бітові послідовності і забезпечує передачу цих послідовностей у вигляді фізичних сигналів у середовище. До блока PHY зазвичай підключаються блоки Auto-Negotiation Control та LED Control. Блок Auto-Negotiation Control забезпечує автоматичне виконання процесу переговорів про швидкість і режим передачі між пристроями. Блок LED Control керує свіченням світлодіодних індикаторів, які показують наявність фізичного з'єдання, швидкість та режим передачі.

Основним блоком мережного адаптера є блок MAC ASIC. Як правило, він реалізовується у вигляді однієї мікросхеми. Ця мікросхема вирішує всі основні питання, пов'язані з опрацюванням кадрів Ethernet. До її складу входить кілька функціональних блоків, основними з яких є блоки передавання та приймання даних TxMAC Processor і RxMAC Processor та блоки вихідних і вхідних буферів TxFIFO та RxFIFO. Блок TxMAC Processor забезпечує опрацювання та передачу попередньо розміщених у буфері TxFIFO даних до пристрою PHY. Блок RxMAC Processor забезпечує приймання даних

від пристрою PHY, їх опрацювання і подальше розміщення у буфері RxFIFO. Підключення мережного адаптера до комп'ютера здійснюється через відповідний інтерфейс. Це може бути як внутрішній інтерфейс (PCI, PCI-x, PCI Express тощо) так і зовнішній інтерфейс (USB тощо). До складу мережного адаптера входить блок енергонезалежної перезаписуваної пам'яті EEPROM, який містить вбудоване програмне забезпечення („Firmware") мережного адаптера. Також до складу мережного адаптера може входити блок Boot ROM, який забезпечує завантаження ОС комп'ютера з спеціального сервера мережі.

Слід зазначити, що мережний адаптер Ethernet є пристроєм, який забезпечує функції фізичного і канального рівнів моделі OSI. Функції фізичного рівня і MAC-підрівня реалізовуються апаратно, функціє LLC-підрівня – програмно, за рахунок драйвера. Досить часто на драйвер покладається виконання частини функцій MAC-підрівня.

Зовнішній вигляд звичайного мережного адаптера Ethernet наведено на рис. 11.



1 – гніздо розніму RJ-45
2 – світлодіодні індикатори
3 – пристрій PHY
4 – MAC ASIC
5 – Boot ROM
6 – інтерфейс

Рис. 11. Зовнішній вигляд мережного адаптера Ethernet

Залежно від призначення мережні адаптери Ethernet поділяють на адаптери робочих станцій/клієнтів та серверні адаптери. Сучасні адаптери робочих станцій є адаптерами або технології Fast Ethernet 100Base-TX, або технології Gigabit Ethernet 1000Base-T. Такі адаптери типово мають один фізичний рознім RJ-45. Серверні адаптери реалізовуються для різних як за швидкостями передачі (1 Гбіт і вище), так і за середовищами передачі (вита пара, волоконно-оптичний кабель) технологій Ethernet. Сучасні серверні адаптери можуть мати кілька фізичних рознімів або інтерфейсних слотів (2, 4, 8) для формування агрегованих каналів. Вбудовані оптичні рознімі у сучасних адаптерах застосовуються досить рідко, замість них застосовуються змінні інтерфейсні модулі.

Інтерфейси/порти комутаторів Cisco

Переважна більшість сучасних комутаторів Cisco є комутаторами, які орієнтовані на побудову мереж Ethernet різного масштабу, починаючи від локальних мереж невеликого розміру і закінчуючи регіональними і глобальними мережами. Лише деякі моделі комутаторів Cisco орієнтовані на використання інших технологій. Як правило, це комутатори технології Fibre Channel, яка застосовується для побудови мереж збереження даних.

Комутатори Cisco забезпечують можливість підключення до мережі кінцевих та проміжних вузлів із використанням різних середовищ передачі даних та різних швидкостей. Найбільш поширеними на сьогодні є підключення на основі витої пари та волоконно-оптичного кабелю. Для підключень на основі витої пари типово забезпечуються швидкості 100 Мбіт/с та 1 Гбіт/с. Підключення на швидкості 10 Гбіт/с для витої пари зустрічаються досить рідко. Для підключень на основі волоконно-оптичного кабелю типово забезпечуються швидкості 1 Гбіт/с, 10 Гбіт/с, 40 Гбіт/с та 100 Гбіт/с. Підключення на основі витої пари 10 Мбіт/с та оптичні підключення на швидкості 100 Мбіт/с є застарілими і нині зустрічаються досить рідко. Ведуться розробки підключень на швидкостях вище 100 Гбіт/с.

З появою високошвидкісних мереж Wi-Fi (стандарти IEEE 802.11ac та IEEE 802.11ad), які функціонують зі швидкостями вище 1 Гбіт/с, з метою підключення точок доступу Wi-Fi до проводової мережі фірмою Cisco були розроблені власні технології, що отримали загальну назву mGig (MultiGigabit Ethernet). Найбільш відомими варіантами mGig є варіанти, що функціонують на швидкостях 2,5 та 5 Гбіт/с. Особливістю цих технологій є можливість використання наявної кабельної інфраструктури технологій 100Base-TX та 1000Base-T.

Підключення за допомогою витої пари частіше застосовується для побудови мереж доступу, рідше – мереж розподілу і дуже рідко – мережі ядра. Таке застосування витої пари зумовлене граничними обмеженнями на відстань передачі даних і, певною мірою, швидкостями передачі по витій парі. Підключення за допомогою волоконно-оптичного кабелю частіше застосовується для побудови мереж розподілу та мережі ядра, де необхідно забезпечити більші

відстані та вищі швидкості передачі. Описаний підхід стосується як локальних, так і кампусних, регіональних та глобальних мереж.

Перелік технологій Ethernet, які підтримуються комутаторами Cisco, та їх основні параметри наведені у табл. 6.

Таблиця 6

Параметри технологій Ethernet

Назва технології	Швидкість	Середовище	Кількість провідників	Максимальна відстань передачі
Технології Ethernet на основі звитої пари				
10Base-T	10 Мбіт/с	Звита пара кат. 3 і вище	2 пари	100 м
100Base-TX	100 Мбіт/с	Звита пара кат. 5 і вище	2 пари	100 м
1000Base-T	1 Гбіт/с	Звита пара кат. 5е і вище	4 пари	100 м
mGig	2,5/5 Гбіт/с	Звита пара кат. 5е і вище	4 пари	50-70 м
10G Base-T	10 Гбіт/с	Звита пара кат. 6 і вище	4 пари	100 м
Технології Ethernet на основі волоконно-оптичного кабелю				
100Base-BX	100 Мбіт/с	SMF	1 волокно	10 км
100Base-FX	100 Мбіт/с	MMF	2 волокна	2 км
100Base-LX	100 Мбіт/с	SMF	2 волокна	10 км
100Base-SX	100 Мбіт/с	MMF	2 волокна	300 м
100Base-LX10	100 Мбіт/с	SMF	2 волокна	10 км
100Base-BX10	100 Мбіт/с	SMF	1 волокно	10 км
1000Base-BX	1 Гбіт/с	SMF	1 волокно	10 км
1000Base-SX	1 Гбіт/с	MMF	2 волокна	220, 275, 500, 550 м
1000Base-LX	1 Гбіт/с	MMF, SMF	2 волокна	550 м, 10 км
1000Base-LH	1 Гбіт/с	MMF, SMF	2 волокна	550 м, 10 км
1000Base-ZX	1 Гбіт/с	SMF	2 волокна	70–100 км
1000Base-EX	1 Гбіт/с	SMF	2 волокна	120 км
1000Base-BX10	1 Гбіт/с	SMF	1 волокно	10 км
1000Base-LX10	1 Гбіт/с	MMF, SMF	2 волокна	550 м, 10 км
10G Base-LR	10 Гбіт/с	SMF	2 волокна	10 км
10G Base-ER	10 Гбіт/с	SMF	2 волокна	40 км
10G Base-SR	10 Гбіт/с	MMF	2 волокна	26 м, 300 м
10G Base-ZR	10 Гбіт/с	SMF	2 волокна	80 км
10G Base-LRM	10 Гбіт/с	MMF	2 волокна	100, 220 м

Якщо вести мову про сучасні комутатори Cisco, то слід зазначити, що застосування фіксованих оптичних інтерфейсів у них не передбачено. Замість фіксованих оптичних інтерфейсів застосовуються інтерфейсні слоти для змінних мережних інтерфейсних модулів. Це забезпечує можливість гнучко змінювати конфігурацію комутатора з метою підключення сегментів мереж Ethernet різних середовищ і різних швидкостей передачі.

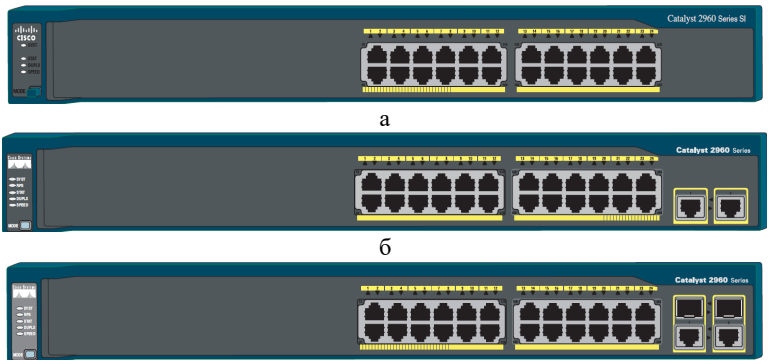
Загальний опис комутатора Cisco

Фірмою Cisco розроблено велику кількість моделей комутаторів Ethernet, які відрізняються своїм функціоналом та можливостями. Частина моделей орієнтовані на використання у невеликих локальних мережах із неінтенсивним інформаційним обміном – домашніх мережах або мережах малих офісів. Частина моделей орієнтована на використання у високошвидкісних локальних, кампусних або глобальних мережах. Як правило, моделі комутаторів, що застосовуються для побудови невеликих локальних мереж та мереж доступу, забезпечують підключення пристроїв технологій Ethetnet/Fast Ethetnet. Моделі комутаторів, що застосовуються для побудови великих локальних мереж, мереж розподілу та магістральних мереж, забезпечують підключення пристроїв електричних або оптичних варіантів технологій Gigabit Ethernet, 10 Gigabit Ethernet і вище.

Найвідомішими серіями комутаторів фірми Cisco є сучасні серії Catalyst 2950, 2960, 3560, 3650, 3750, 3850. Однією з найбільш вживаних нині серій є серія 2960.

Типово комутатор Cisco має фіксований набір з 8, 16, 24, 48 інтерфейсів/портів Ethernet 10/100/1000 Мбіт/с для підключення кінцевих вузлів за допомогою витої пари. Іноді такі порти називають лінійними портами, або ,,Down-Link Ports". Зовнішній вигляд передньої панелі 24-портового комутатора Catalyst 2960 наведений на рис. 12, а. У багатьох моделях комутаторів Cisco наявні додаткові один, два або чотири порти 1000 Мбіт/с. Ці високошвидкісні порти призначені для: підключення серверів, з'єднання комутаторів між собою, підключення комутатора до маршрутизатора тощо. Часто ці порти називають магістральними портами, або ,,Up-Link Ports". Порти ,,Up-Link" можуть бути фіксованими (рис. 12, б), як правило, вони орієнтовані на підключення за допомогою звитої пари, та змінними (рис. 12, в) – у цьому разі вони орієнтовані на підключення або за допомогою витої пари, або за допомогою волоконно-оптичного кабелю. Для підключення використовуються спеціальні змінні модулі (SFP, SFP+ тощо), які встановлюються у відповідні слоти комутатора. Існують серії комутаторів Cisco, орієнтовані на використання виключно портів 1000 Мбіт/с або комбінацій портів 1000 Мбіт/с та 10 Гбіт/с.

Для позначення кількості інтерфейсів/портів як комутаторів Cisco, так і комутаторів інших виробників, уведено поняття щільності портів (Port Density). У більшості випадків щільність портів комутатора можна дізнатися з назви його моделі. Наприклад, комутатор Cisco Catalyst 2960-24-S має 24 порти Ethernet 10/100 Мбіт/с для підключення пристроїв за допомогою витої пари. Наявність портів „Up-Link", їх кількість та тип можна визначити з символьного позначення, що записується після кількості основних портів у назві моделі пристрою. Більш детальна інформація стосовно цих портів міститься у технічній документації.



а

б

в

Рис. 12. Передня панель комутатора Cisco серії Catalyst 2960:
а – модель 2960-24-S; б – модель 2960-24TT-L; в – модель 2960-Plus 24PC-S

На передній панелі комутатора Cisco також розміщуються кнопка переключення режимів світлодіодних індикаторів (Mode) та світлодіодні індикатори (LEDs), що призначені для відображення стану комутатора в цілому (рис. 13). Кожен порт Ethernet також має власний індикатор, який відображає його стан.

У деяких моделях комутаторів на передній панелі також розміщуються консольний порт (порти), спеціалізований порт Ethernet мережного керування, інтерфейс(и) USB для підключення зовнішніх носіїв. Більшість із них також мають власні світлодіодні індикатори.

Загальні правила розуміння свічення індикаторів є такими. Якщо індикатор не світиться (Off) – це свідчить про відключення або непрацездатність пристрою в цілому, певного його блока, підсистеми або каналу зв'язку. Якщо індикатор світиться зеленим кольором (Green)

або мерехтить зеленим кольором (Blinking Green) – це свідчить про нормальний режим роботи, якщо ж індикатор світиться жовтим кольором (Amber) або мерехтить жовтим кольором (Blinking Amber) – це свідчить про те, що виникла певна проблема.

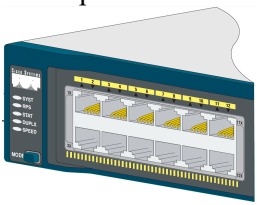


Рис. 13. Індикатори та лінійні порти комутатора Cisco серії Catalyst 2960

Позначення та короткий опис основних і додаткових світлодіодних індикаторів та світлодіодних індикаторів окремих портів комутаторів Cisco серії Catalyst 2960 наведені у табл. 7.

Таблиця 7

Світлодіодні індикатори комутатора Cisco

№	Позначення	Повна назва	Опис
Основні світлодіодні індикатори			
1	SYST	System LED	Індикатор загального стану системи
2	RPS (XPS)	Redundant Power Supply (eXpandable Power System) LED	Індикатор стану системи резервного живлення
3	STAT	Status LED	Індикатор стану портів (режим за замовчуванням)
4	DUPLX	Duplex LED	Індикатор напівдуплексної/дуплексної передачі портів
5	SPEED	Speed LED	Індикатор швидкості передачі портів
Додаткові світлодіодні індикатори			
6	PoE	Power over Ethernet LED	Індикатор живлення підключених вузлів через з'єднання Ethernet.
7	MSTR	Master Switch LED	Індикатор головного комутатора стеку
8	STCK	Stack Switch LED	Індикатор комутатора – члена стеку
9	S-PWR	Stack Power LED	Індикатор живлення стеку
10	ACTV	Active LED	Індикатор активності комутатора
Світлодіодні індикатори звичайних портів та портів (інтерфейсів) керування			
11	*N*X[1]	Port LED	Індикатори окремих портів Ethernet 10/100/1000 Мбіт/с
12	Console	Console LED	Індикатор консольного порту
13	MGMT	Managament LED	Індикатор спеціалізованого порту керування 10/100 Мбіт/с

Примітка: 1 – *N* це номер відповідного порту Ethernet.

Опис станів основних світлодіодних індикаторів та індикаторів звичайних портів Ethernet і портів керування комутатора Cisco наведено

у табл. 2. Необхідно зазначити, що порт Ethernet комутатора Cisco має лише один індикатор, який може працювати або у режимі відображення стану порту STAT (активований за замовчуванням), або у режимі відображення напівдуплексної/дуплексної передачі DUPLX, або у режимі відображення швидкості SPEED. Переключення між цими трьома режимами здійснюється циклічно кнопкою MODE. Режим встановлюється для всіх портів одночасно. Для відображення обраного режиму призначені індикатори режимів STAT, DUPLX, SPEED. Опис станів додаткових індикаторів міститься у технічній документації.

Таблиця 8

Стани основних світлодіодних індикаторів комутатора Cisco

№	Свічення індикатора	Опис
Системний індикатор SYST		
1	Off	Живлення комутатора не ввімкнено
2	Green	Живлення ввімкнене, ОС завантажилася і комутатор функціонує коректно
3	Amber	Живлення ввімкнене, але ОС функціонує некоректно
Індикатор системи резервного живлення RPS		
1	Off	Система вимкнена або некоректно підключена
2	Green	Система підключена і готова подати живлення за потреби
3	Blinking Green	Система підключена, але не може подати живлення, бо забезпечує роботу іншого пристрою
4	Amber	Система знаходиться у режимі резервування або несправна
5	Blinking Amber	Внутрішній блок живлення комутатора вийшов з ладу і система забезпечує живлення пристрою
Індикатор STAT		
1	Off	Канал зв'язку не функціонує або відключений
2	Green	Канал зв'язку функціонує нормально, але через інтерфейс дані не передаються
3	Blinking Green	Канал зв'язку функціонує і через нього передаються дані
4	Blinking Amber	Порт адміністративно вимкнений (або заблокований)
Індикатор DUPLX		
1	Off	Порт функціонує у напівдуплексному режимі передачі
2	Green	Порт функціонує у дуплексному режимі передачі
Індикатор SPEED		
1	Off	Порт функціонує на швидкості 10 Мбіт/с
2	Green	Порт функціонує на швидкості 100 Мбіт/с
3	Blinking Green	Порт функціонує на швидкості 1000 Мбіт/с

Продовження таблиці 8

Індикатор Console		
1	Off	Консольний кабель не підключено або функціонує некоректно
2	Green	Консольний кабель підключено і порт функціонує коректно
Індикатор MGMT		
1	Off	Порт функціонує на швидкості 10 Мбіт/с
2	Green	Порт функціонує на швидкості 100 Мбіт/с

На задній панелі комутатора Cisco типово розміщуються гніздо для підключення кабелю основного живлення, спеціальний слот для підключення системи резервного живлення та консольний порт. У деяких спеціалізованих моделях на задній панелі також містяться слоти для об'єднання комутаторів у стек.

Налагодження параметрів мережних адаптерів Ethernet вузлів ОС Windows та ОС Linux

Мережні адаптери Ethernet, що застосовуються у сучасних серверах та робочих станціях мають набір параметрів, зміна значень яких дає змогу підвищити продуктивність та ефективність інформаційного обміну. До цього набору входять такі параметри як:

– швидкість і режим передачі адаптера (Speed&Duplex);

– функція ,,Пробудження через локальну мережу" (WoL, Wake-on-LAN);

– функція забезпечення якості обслуговування (IEEE 802.1q QoS, QoS, Quality of Service);

– розмір буфера передавання даних (Transmit Buffer);

– розмір буфера приймання даних (Receive Buffer);

– розмір оброблюваних кадрів великих розмірів (Large Frames);

– MAC-адреса адаптера (Network Address, Locally Administrated Address);

– ідентифікатор віртуальної локальної мережі (VLAN Identifier);

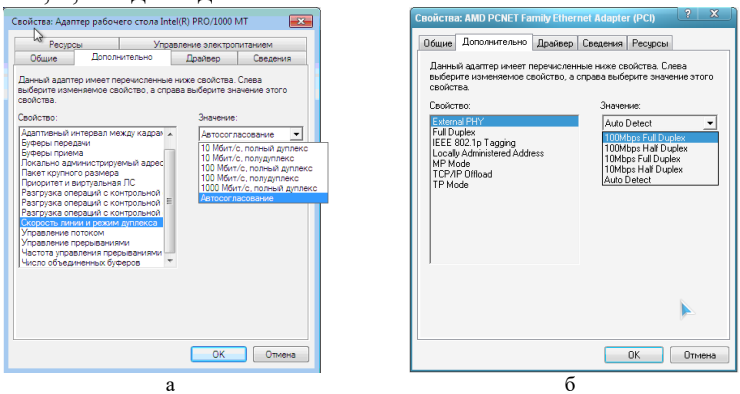
– пріоритет трафіку (IEEE 802.1p Tagging,Traffic Priority);

– режим енергозбереження адаптера (Energy Efficient Ethernet) тощо.

Перелік параметрів може відрізнятися для мережних адаптерів різних технологій та різних моделей мережних адаптерів однієї технології. Деякі параметри, наприклад, швидкість і режим передачі, можуть налагоджуватися лише для адаптерів, що як середовище застосовують звиту пару, інші, наприклад, MAC-адреса можуть налагоджуватися для будь-яких технологій Ethernet.

Значення параметрів встановлюються за замовчуванням на етапі встановлення ОС і зберігаються або у реєстрі для вузлів ОС Windows, або у конфігураційних файлах для вузлів ОС Linux/Unix. У більшості клієнтських та серверних мережних ОС наявні як вбудовані, так і додаткові засоби перегляду та налагодження параметрів функціонування мережних адаптерів.

Зміна параметрів мережного адаптера Ethernet в ОС Windows здійснюється шляхом налагодження параметрів його драйвера. Для зміни параметрів необхідно за допомогою додатку „Система" запустити додаток „Диспетчер устройств", надалі з переліку мережних адаптерів обрати необхідний адаптер. У вікні властивостей адаптера перейти на вкладку „Дополнительно", обрати відповідний параметр і встановити необхідне значення цього параметра. Приклади вибору швидкості і режиму роботи мережного адаптера технології Gigabit Ethernet моделі Intel (R) PRO/1000 MT для ОС Windows 7 та для мережного адаптера технології Fast Ethernet моделі AMD PCNET Family Ethernet Adapter (PCI) для ОС Windows XP наведено на рис. 14, а, б відповідно.



а б

Рис. 14. Приклад вибору швидкості і режиму роботи мережного адаптера:
а – моделі Intel (R) PRO/1000 MT (ОС Windows 7);
б – моделі AMD PCNET Family Ethernet Adapter (PCI) (ОС Windows XP)

Для перегляду або зміни параметрів мережного адаптера Ethernet в ОС Linux розроблено команду (утиліту) **ethtool**. За її допомогою можна і діагностувати, і змінювати певні параметри функціонування адаптера. Зокрема, ця утиліта надає можливість іден-

тифікувати адаптер, отримати статистичну інформацію щодо певних параметрів його роботи, змінювати параметри швидкості чи режиму передачі, активувати/деактивувати функцію автопереговорів, виконувати оновлення „прошивки" пристрою.

Утиліта **ethtool** у більшості систем Linux не встановлюється автоматично, її необхідно встановити з відповідного репозиторію у ручному режимі командою **apt-get install ethtool**. Перелік можливих варіантів застосування утиліти можна отримати виконавши **ethtool -h**. Приклади отримання інформації про драйвер та діагностики параметрів мережного адаптера технології Gigabit Ethernet моделі Intel PRO/1000 MT за допомогою утиліти **ethtool** для ОС Linux Debian наведено на рис. 15 та 16 відповідно.

```
root@debian8-3:~# ethtool –i eth0
driver: e1000
version: 7.3.21-k8-NAPI
firmware-version:
bus-info: 0000:00:03.
supports-statistics: yes
supports-test: yes
supports-eeprom-access: yes
supports-register-dump: yes
supports-priv-flags: no
```

Рис. 15. Приклад виконання утиліти **ethtool** з метою отримання інформації про драйвер для ОС Linux Debian

```
root@debian8-3:~# ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: No
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: Yes
        Speed: 1000Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 0
        Transceiver: internal
        Auto-negotiation: on
        MDI-X: off (auto)
        Supports Wake-on: umbg
        Wake-on: d
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes
```

Рис. 16. Приклад виконання утиліти **ethtool** з метою діагностики параметрів мережного адаптера для ОС Linux Debian

Зміна параметрів мережного адаптера за домогою команди **ethtool** можлива як тимчасово, так і на постійній основі. Для тимчасової зміни достатньо виконати команду з відповідними ключами. Наприклад, для встановлення швидкості 100 Мбіт/с, дуплексного режиму роботи та відключення автопереговорів необхідно виконати таку команду:

ethtool -s eth0 speed 100 duplex full autoneg off

Для постійної зміни параметрів адаптера необхідно внести зміни у відповідні конфігураційні файли. Для ОС Linux Debian/Ubuntu необхідно внести зміни у файл **/etc/network/interfaces**, для ОС Linux CentOS/Red Hat/Oracle/Fedora – у файл **/etc/sysconfig/network-scripts/ifcfg-<*if-name*>**, де ***if-name*** – назва мережного інтерфейсу (наприклад, **eth0**).

Приклади структури конфігураційних файлів **/etc/network/interfaces** та **/etc/sysconfig/network-scripts/ifcfg-enp0s3** за умови встановлення постійних параметрів швидкості 100 Мбіт/с, дуплексного режиму роботи та відключення автопереговорів наведено на рис. 17 та 18 відповідно.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
Source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
allow-hotplug eth0
iface eth0 inet static
   address 195.10.1.1
   netmask 255.255.255.128
   broadcast 195.10.1.127
   gateway 195.10.1.126
   dns-domain example.com
   dns-nameservers 195.10.1.126 8.8.8.8
   post-up ethtool -s eth0 speed 100 duplex full autoneg off
...
```

Рис. 17. Структура файла **/etc/network/interfaces** ОС Linux Debian

```
DEVICE=enp0s3
ETHTOOL_OPTS="speed 100 duplex full autoneg off"
HWADDR=00:21:70:10:7E:CD
NM_CONTROLLED=no
ONBOOT=yes
BOOTPROTO=static
IPADDR=195.10.1.1
```

```
NETMASK=255.255.255.128
#the GATEWAY is sometimes in: /etc/sysconfig/network
GATEWAY=195.10.1.126
```

Рис. 18. Структура файла **/etc/sysconfig/network-scripts/ifcfg-enp0s3** ОС Linux CentOS

Слід зазначити, що змінені параметри конфігураційних файлів активуються або після перезавантаження адаптера, або після повного перезавантаження системи.

Основні команди налагодження параметрів інтерфейсів/портів комутатора Cisco

Інтерфейси комутатора Cisco з погляду адміністрування можна розділити на дві групи: фізичні інтерфейси та логічні (віртуальні) інтерфейси. Фізичні інтерфейси – це інтерфейси/порти відповідних технологій Ethernet. Логічні інтерфейси – це інтерфейси, які автоматично створені операційною системою Cisco IOS для виконання певних функцій, або інтерфейси, які створюються адміністратором із певною метою. Позначення і, в багатьох аспектах, налагодження фізичних інтерфейсів не залежить від того, чи є вони електричними, чи оптичними. Слід зазначити, що фізичні інтерфейси комутатора Cisco за замовчуванням є активними. Позначення інтерфейсів комутатора Cisco наведені у табл. 9.

Таблиця 9

Інтерфейси (порти) комутаторів Cisco

Назва інтерфейсу	Опис інтерфейсу
Фізичні інтерфейси	
Ethernet	Класичний Ethernet, 10 Мбіт/с
FastEthernet	Fast Ethernet, 100 Мбіт/с
GigabitEthernet	Gigabit Ethernet, 1 Гбіт/с
TenGigabitEthernet	10 Gigabit Ethernet, 10 Гбіт/с
Логічні інтерфейси	
Vlan, SVI (Switched Virtual Interface)	Інтерфейс VLAN (Virtual LAN), на комутаторах автоматично створено vlan 1. До цієї VLAN за замовчуванням входять усі фізичні інтерфейси.
PortChannel	Інтерфейс агрегованого каналу зв’язку EtherChannel

Вибір інтерфейсу для налагодження здійснюється командою **interface**. Налагодження інтерфейсу комутатора передбачає зміну як фізичних параметрів роботи інтерфейсу (середовища, типу кабелю, швидкості, режиму), так і зміну параметрів фунціонування певних мережних протоколів. Основними командами налагодження пара-

метрів інтерфейсу є **description**, **media-type**, **mdix auto**, **duplex**, **speed**, **mac-address**, **shutdown** та деякі інші.

Команда **description** застосовується для зазначення текстового опису інтерфейсу. Цей опис полегшує аналіз конфігураційного файла пристрою та аналіз результатів виведення діагностичної інформації певного інтерфейсу. За допомогою команди **media-type** здійснюється вибір типу середовища передачі. Команда **mdix auto** активує режим автоматичного визначення типу (прямий чи перехресний) Ethernet-кабелю, що застосовується для підключення пристрою, та переключення у відповідний режим. За замовчуванням ця команда активована. Для того, щоб команда **mdix auto** працювала коректно, необхідно також, щоб швидкість і режим інтерфейсу визначалися автоматично. За допомогою команд **duplex** та **speed** можна змінити режим та швидкість передачі даних інтерфейсу. За замовчуванням встановлено автоматичне визначення цих параметрів. Команда **mac-address** застосовується для примусового призначення MAC-адреси інтерфейсу комутатора. Відключення інтерфейсу здійснюється за допомогою команди **shutdown**. Відміна дії вищезгаданих команд – використання форми **no**. Синтаксис розглянутих команд та режими їх застосування наведено нижче.

Можливе одночасне налагодження групи інтерфейсів. Для цього застосовується команда **interface range**. Для зручності роботи із групами інтерфейсів можливе застосування макросів. Створення макросу виконується командою **define interface-range.** Видалення – командою **no define interface-range**.

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

interface ***interface_type interface_id***,

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

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

Синтаксис команди **interface range** (режим глобального конфігурування):

interface range { ***port_range*** **| macro** ***macro_name*** **}**,

де ***port_range*** – діапазон ідентифікаторів інтерфейсів (портів), що може формуватися як і з неперервної послідовності ідентифікаторів інтерфейсів, так і з окремих ідентифікаторів. Наприклад, FastEthernet 0/1 – 0/10, FastEthernet 1/1, FastEthernet 2/1;

macro – службова конструкція, за допомогою якої зазначається необхідність використання макросу;

macro_name – текстова назва макросу.

Синтаксис команди **define interface-range** (режим глобального конфігурування):

define interface-range *macro_name port_range*,

де ***macro_name*** – текстова назва макросу;

port_range – діапазон ідентифікаторів інтерфейсів (портів).

Синтаксис команди **description** (режим конфігурування інтерфейсу):

description *text_line*,

де ***text_line*** – тестовий рядок опису інтерфейсу (до 240 символів).

Синтаксис команди **duplex** (режим конфігурування інтерфейсу):

duplex { auto | full | half },

де **auto** – службова конструкція, за допомогою якої встановлюється автоматичний вибір режиму передачі;

full – службова конструкція, за допомогою якої встановлюється повнодуплексний режим передачі;

half – службова конструкція, за допомогою якої встановлюється напівдуплексний режим передачі.

Синтаксис команди **speed** (режим конфігурування інтерфейсу):

speed { 10 | 100 | 1000 | auto [10 | 100 | 1000] | nonegotiate },

де **10**, **100**, **1000** – фіксовані значення швидкості (Мбіт/с);

auto – службова конструкція, за допомогою якої встановлюється автоматичний вибір швидкості; якщо використовується форма **auto 10** (**auto 100, auto 1000**), порт веде переговори лише на цій швидкості;

nonegotiate – службова конструкція, за допомогою якої відключається режим автопереговорів про швидкість передачі.

Синтаксис команди **media-type** (режим конфігурування інтерфейсу):

media-type {**auto-select** | **rj45** | **sfp**},

де **auto-select** – службова конструкція, за допомогою якої активується вибір середовища передачі (змінного інтерфейсного модуля); автоматичний вибір встановлений за замовчуванням;

rj45 – службова конструкція, за допомогою якої зазначається застосування змінного інтерфейсного модуля RJ-45;

sfp – службова конструкція, за допомогою якої зазначається застосування змінного інтерфейсного модуля SFP.

Синтаксис команди **mdix** (режим конфігурування інтерфейсу):

mdix auto.

Команда не має параметрів.

Синтаксис команди **mac-address** (режим конфігурування інтерфейсу):

mac-address *hw_address*,

де ***hw_address*** – MAC-адреса інтерфейсу у вигляді HHHH.HHHH.HHHH; кожне число HHHH має довжину 2 байти і записується у шістнадцятковій формі□

Основні команди діагностики параметрів інтерфейсів, параметрів адресації та процесу роботи комутатора Cisco

Для виведення діагностичної інформації про параметри фізичних та логічних інтерфейсів, результати налагоджень, уміст службових таблиць, процес роботи комутатора використовуються різні варіанти команд **show**. Перелік команд та їх призначення наведено у табл. 10.

Таблиця 10

Перелік команд show, необхідних для діагностики процесу роботи комутатора Cisco

Команда	Призначення
show interfaces	Виведення деталізованої інформації про всі фізичні і логічні інтерфейси комутатора
show interface *interface-type interface-id*	Виведення деталізованої інформації про конкретний інтерфейс комутатора
show controllers ethernet-controller *interface-type interface-id*	Виведення деталізованої інформації про стан контролера конкретного інтерфейсу Ethernet
show controllers utilization	Виведення інформації про завантаження комутатора в цілому або окремого його порту
show version	Виведення інформації про фізичні параметри пристрою та параметри IOS

Модельний приклад налагодження функціонування мережних з'єднань локальної комп'ютерної мережі, побудованої на базі керованого комутатора Cisco

Розглянемо специфіку налагодження роботи комутатора Cisco моделі WS-C2960-24TT-L та маршрутизатора моделі Cisco 1841 для локальної комп'ютерної мережі, схему якої наведено на рис. 19.

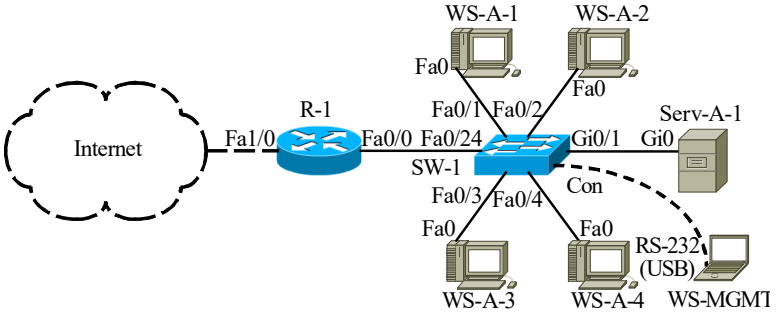


Рис. 19. Приклад мережі

Під час побудови даної мережі для з'єднання пристроїв використано дані табл. 11. Для налагодження параметрів окремих Ethernet-каналів зв'язку між пристроями використано дані табл. 12. Для налагодження параметрів адресації пристроїв використано дані табл. 13.

Таблиця 11

Параметри інтерфейсів пристроїв для прикладу

Пристрій	**Інтерфейс**	**Підключення до пристрою**	**Підключення до інтерфейсу**
Маршрутизатор R_1 (Cisco 1841)	Fa0/1	Internet	Internet_Interface
	Fa0/0	Комутатор SW-1	Fa0/24
Комутатор SW-1 (Cisco 2960-24TT-L)	Con	Робоча станція WS-MGMT	RS-232 (USB)
	Gi0/1	Сервер Serv-A-1	Gi0
	Fa0/1	Робоча станція WS-A-1	Fa0
	Fa0/2	Робоча станція WS-A-2	Fa0
	Fa0/3	Робоча станція WS-A-3	Fa0
	Fa0/4	Робоча станція WS-A-4	Fa0
	…	…	…
	Fa0/24	Маршрутизатор R_1	Fa0/0
Робоча станція WS-MGMT	RS-232 (USB)	Комутатор SW-1	Con
Сервер Serv-A-1	Gi0		Gi0/1
Робоча станція WS-A-1	Fa0		Fa0/1
Робоча станція WS-A-2	Fa0		Fa0/2
Робоча станція WS-A-3	Fa0		Fa0/3
Робоча станція WS-A-4	Fa0		Fa0/4

Таблиця 12

Параметри Ethernet-каналів зв'язку між пристроями для прикладу

Канал між пристроями	Технологія	Тип кабелю	Режим	Швидкість, Мбіт/с
R-1 – SW-1	100Base-TX	Прямий	Автовибір	Автовибір
Serv-A-1 – SW-1	1000Base-T	Прямий	Дуплексний	1000
WS-A-1 – SW-1	100Base-TX	Прямий	Дуплексний	100
WS-A-2 – SW-1	100Base-TX	Прямий	Дуплексний	100
WS-A-3 – SW-1	100Base-TX	Прямий	Дуплексний	100
WS-A-4 – SW-1	100Base-TX	Прямий	Дуплексний	100

Таблиця 13

Параметри адресації мережі для прикладу

Мережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	MAC-адреса	IP-адреса	Маска	Префікс
Мережа A	–	–	195.10.1.0	255.255.255.0	/24
Маршрутизатор R_1	Інтерфейс Fa0/0	CA-01-07-FE-00-08	195.10.1.254	255.255.255.0	/24
	Інтерфейс Fa1/0	*	*	*	*
Комутатор SW-1	Інтерфейс Vlan 1	00-D0-BA-E4-0D-9B	195.10.1.252	255.255.255.0	/24
	Шлюз за замовчуванням				
	Основний DNS-сервер	–	195.10.1.254	–	–
Сервер Serv-A-1	Мережний адаптер	00-05-5E-26-8A-1C	195.10.1.250	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–
Робоча станція WS-A-1 (Linux)	Мережний адаптер	00-60-5C-16-8B-30	195.10.1.1	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–
Робоча станція WS-A-2 (Windows)	Мережний адаптер	00-10-43-2C-BD-BB	195.10.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–

Продовження таблиці 13

Робоча станція WS-A-3 (Windows)	Мережний адаптер	00-10-11-49-ED-09	195.10.1.3	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–
Робоча станція WS-A-4 (Windows)	Мережний адаптер	00-E0-8F-00-51-96	195.10.1.4	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–

Примітка: * – параметри адресації не зазначені.

Сценарій налагодження параметрів іменування наведено нижче.

```
…
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-1
SW-1(config)#no ip domain-lookup
SW -1(config)#exit
SW-1#copy running-config startup-config
SW-1#
…
```

Сценарії налагодження параметрів інтерфейсів комутатора мережі SW-1 наведено нижче. Їх особливістями є налагодження Ethernet-каналів зв'язку з такими параметрами: швидкість передачі – максимальна, режим передачі – дуплексний. Варто зазначити, що автоматичний вибір Ethernet-кабелю для портів комутатора Cisco 2960-24TT-L встановлено за замовчуванням.

Сценарій налагодження Ethernet каналу між комутатором SW-1 і сервером SERV-A-1.

```
…
SW-1#configure terminal
SW-1(config)#interface GigabitEthernet 0/1
SW-1(config-if)#description LINK-TO-SERV-A-1
SW-1(config-if)#duplex full
SW-1(config-if)#speed 1000
SW-1(config-if)#exit
SW-1(config)#exit
SW-1#copy running-config startup-config
SW-1#
…
```

Сценарій налагодження каналу між комутатором SW-1 і робочими станціями WS-A-1 – WS-A-4. У сценарії наведено команди налагодження каналів до робочих станцій WS-A-1 та WS-A-4, до станцій WS-A-2 та WS-A-3 дії аналогічні.

```
…
SW-1#configure terminal
SW-1(config)#interface FastEthernet 0/1
```

SW-1(config-if)#description LINK-TO-WS-A-1
SW-1(config-if)#duplex full
SW-1(config-if)#speed 100
SW-1(config-if)#exit
SW-1(config)#interface FastEthernet 0/4
SW-1(config-if)#description LINK-TO-WS-A-4
SW-1(config-if)#duplex full
SW-1(config-if)#speed 100
SW-1(config-if)#exit
SW-1(config)#exit
SW-1#copy running-config startup-config
…

Сценарій налагодження налагодження групи інтерфейсів комутатора SW-1 наведено нижче. У цьому сценарії зазначається однаковий опис для всіх інтерфейсів та здійснюється їх відключення/деактивація.

…
SW-1#configure terminal
SW-1(config)#interface range FastEthernet 0/5-23, GigabitEthernet 0/2
SW-1(config-if-range)#description UNUSED-PORT
SW-1(config-if-range)#shutdown
SW-1(config-if-range)#exit
SW-1(config)#exit
SW-1#copy running-config startup-config
…

Сценарій параметрів іменування пристрою, активації та налагодження інтерфейсу FastEthernet 0/0 для маршрутизатора R-1 наведено нижче. Для виконання цього сценарію необхідно відключити консольний кабель від комутатора SW-1 та підключити до маршрутизатора R-1.

…
Router>enable
Router#configure terminal
Router(config)#hostname R-1
R-1(config)#no ip domain-lookup
R-1(config)#interface FastEthernet 0/0
R-1(config-if)#description LINK-TO-LAN-A

R-1(config-if)#ip address 195.10.1.254 255.255.255.0
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#ip domain-name MY.NET
R-1(config)#exit
R-1#copy running-config startup-config
…

Налаштування параметрів мережних адапетрів робочих станцій та серверві здійснюється засобами відповідних операційних систем.

Результати виконання команд моніторингу та діагностики роботи інтерфейсів комутатора для розглянутого модельного прикладу

З метою перегляду інформації про налагодження інтерфейсів комутатора для розглянутого прикладу застосовано команду **show interface**. Результати роботи зазначених команд наведено відповідно на рис. 20 та 21.

З метою перевірки досяжності сервера та решти робочих станцій мережі з робочих станцій WS-A-1 та WS-A-2 застосовано команду **ping**. За допомогою цієї ж команди виконано перевірку досяжності всіх вузлів мережі з комутатора SW-1. Частину результатів цих перевірок наведено на рис. 22 та 23.

Файл конфігурації, що створений за сценарієм модельного прикладу, наведено на рис. 24 (частину несуттєвої інформації вилучено).

```
SW-1#show interfaces FastEthernet 0/1
  FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.5c23.b801 (bia 0060.5c23.b801)
  Description: LINK-TO-WS-A-1
  BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    2357 packets output, 263570 bytes, 0 underruns
    0 output errors, 0 collisions, 10 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

Рис. 20. Результати виконання команди **show interfaces FastEthernet 0/1** на комутаторі SW-1

```
SW-1#show interfaces GigabitEthernet 0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.5c23.b819 (bia 0060.5c23.b819)
  Description: LINK-TO-SERV-A-1
 BW 1000000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
SW-1#
```

Рис. 21. Результати виконання команди **show interfaces GigabitEthernet 0/1** на комутаторі SW-1

```
root@WS-A-1~#ping 195.10.1.2
PING 195.10.1.2 (195.10.1.2): 56 data bytes
64 bytes from 195.10.1.2: seq=0 ttl=255 time=12.064 ms
64 bytes from 195.10.1.2: seq=1 ttl=255 time=5.239 ms
64 bytes from 195.10.1.2: seq=2 ttl=255 time=13.561 ms
64 bytes from 195.10.1.2: seq=3 ttl=255 time=10.502 ms
^C
--- 195.10.1.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 5.239/10.341/13.561 ms
root@WS-A-1~#
```

Рис. 22. Результат виконання команди **ping** на робочій станції WS-A-1

```
C:\>ping 195.10.1.250
Обмен пакетами с 195.10.1.250 по 32 байт:
```

```
Ответ от 195.10.1.250: число байт=32 время 21мс TTL=255
Ответ от 195.10.1.250: число байт=32 время 4мс TTL=255
Ответ от 195.10.1.250: число байт=32 время 2мс TTL=255
Ответ от 195.10.1.250: число байт=32 время 6мс TTL=255
Статистика Ping для 195.10.1.250:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 <0% потерь>,
Приблизительное время приема-передачи в мс:
    Минимальное = 2 мсек, Максимальное 21 мсек, Среднее = 8 мсек
C:\>
```

Рис. 23. Результат виконання команди **ping** на робочій станції WS-A-2

```
Building configuration...
Current configuration : 1771 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW-1
!
no ip domain-lookup
!
interface FastEthernet0/1
description LINK-TO-WS-A-1
duplex full
speed 100
!
interface FastEthernet0/2
description LINK-TO-WS-A-2
duplex full
speed 100
!
interface FastEthernet0/3
description LINK-TO-WS-A-3
duplex full
speed 100
!
interface FastEthernet0/4
description LINK-TO-WS-A-4
duplex full
speed 100
!
interface FastEthernet0/5
description UNUSED-PORT
shutdown
!
...
!
interface GigabitEthernet0/1
description LINK-TO-SERV-A-1
duplex full
speed 1000
!
interface GigabitEthernet0/2
description UNUSED-PORT
shutdown
!
interface Vlan1
no ip address
```

```
shutdown
!
...
end
```

Рис. 24. Файл конфігурації комутатора SW-1 для модельного прикладу

Завдання на лабораторну роботу

1. Навести схеми прямих кабелів для технологій Ethernet 10Base-T/FastEthernet 100Base-TX та Gigabit Ethernet 1000Base-T. Побудувати схеми перехресних кабелів для цих же технологій. Для побудови скористатися інформацією, наведеною у теоретичних відомостях.

2. Визначити, який тип кабелю (прямий чи перехресний) застосовуються для з'єднання мережних інтерфейсів/адаптерів/портів Ethernet кінцевих вузлів та мережних пристроїв. Для побудови скористатися інформацією щодо типів інтерфейсів/адаптерів/портів Ethernet (MDI/MDIX), наведеною у теоретичних відомостях. Результати подати у вигляді табл. 14.

Таблиця 14

З'єднання основних Ethernet-пристроїв

Пристрій	Комп'ютер	Концентратор	Комутатор	Маршрутизатор	Точка доступу
Комп'ютер					
Концентратор					
Комутатор					
Маршрутизатор					
Точка доступу					

3. У середовищі програмного симулятора/емулятора створити проект локальної мережі (рис. 25). Під час побудови звернути увагу на вибір моделей комутаторів, мережних модулів та адаптерів, а також мережних з'єднань. Для цього використовувати дані табл. 15. Для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 9. (Заповнення описовоої таблиці – необов'язкове).

4. Розробити схему адресації пристроїв мережі. Для цього скористатися даними табл. 17. Результати навести у вигляді таблиці, яка аналогічна табл. 13.

5. Провести налагодження параметрів мережних адаптерів/інтерфейсів маршрутизатора, комутаторів, робочих станцій та серверів відповідно до даних, які наведені у табл. 16. Під час налагодження звернути увагу на те, що для оптичних інтерфейсів значення режиму передачі і швидкості змінити не можна.

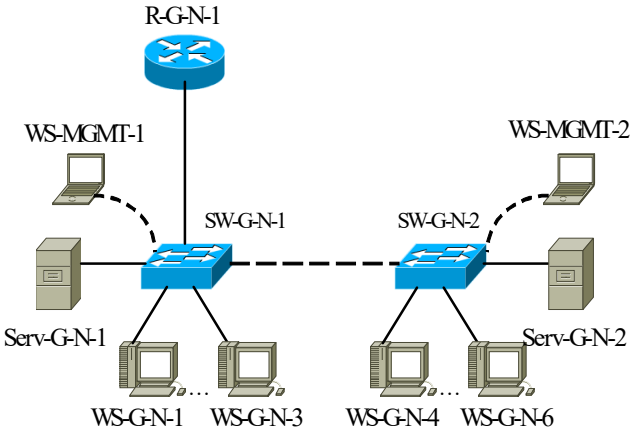


Рис. 25. Проект мережі

6. Для одного із з'єднань FastEthernet 100Base-TX або Gigabit Ethernet 1000Base-T дослідити застосування функції Auto-MDI шляхом заміни прямого Ethernet-кабелю на перехресний (чи навпаки) та виконанням відповідного налагодження інтерфейсу/порту комутатора. При виконанні цього завдання можна додати до мережі інші інші пристроями.

7. Провести налагодження параметрів IP-адресації пристроїв мережі згідно з даними п. 4.

8. Провести перевірку зв'язку між однією з робочих станцій та рештою вузлів мережі (комутаторами, серверами, робочими станціями). У випадку виявлення проблем – визначити та усунити їх причини.

Таблиця 15

Вихідні дані для побудови мережі

№ варіанта	Канал R-G-N-1 – SW-G-N-1	Канал Serv-G-N-1 – SW-G-N-1	Канал Serv-G-N-2 – SW-G-N-2	Канал SW-G-N-1 – SW-G-N-2	Канали підключення робочих станцій
1	1000Base-T	1000Base-T	1000Base-T	1000Base-T	100Base-TX
2	1000Base-T	1000Base-T	1000Base-T	100Base-TX	100Base-TX

3	1000Base-T	1000Base-T	100Base-TX	1000Base-T	100Base-TX
4	100Base-TX	100Base-TX	1000Base-T	1000Base-T	100Base-TX
5	1000Base-T	1000Base-T	100Base-TX	100Base-TX	100Base-TX
6	100Base-TX	100Base-TX	1000Base-T	100Base-TX	100Base-TX
7	100Base-TX	100Base-TX	100Base-TX	1000Base-T	100Base-TX
8	100Base-TX	100Base-TX	100Base-TX	100Base-TX	100Base-TX
9	1000Base-FX	1000Base-FX	1000Base-T	1000Base-T	100Base-TX
10	1000Base-T	1000Base-T	1000Base-FX	1000Base-T	100Base-TX
11	1000Base-FX	1000Base-FX	1000Base-T	100Base-TX	100Base-TX
12	1000Base-FX	1000Base-FX	100Base-TX	1000Base-T	100Base-TX
13	1000Base-FX	1000Base-FX	100Base-TX	100Base-TX	100Base-TX
14	100Base-TX	100Base-TX	1000Base-FX	100Base-TX	100Base-TX
15	100Base-FX	100Base-FX	1000Base-T	1000Base-T	100Base-TX
16	1000Base-T	1000Base-T	100Base-FX	1000Base-T	100Base-TX
17	100Base-FX	100Base-FX	1000Base-T	100Base-TX	100Base-TX
18	100Base-FX	100Base-FX	100Base-TX	1000Base-T	100Base-TX
19	100Base-FX	100Base-FX	100Base-TX	100Base-TX	100Base-TX
20	100Base-TX	100Base-TX	100Base-FX	100Base-TX	100Base-TX
21	1000Base-T	1000Base-T	1000Base-T	1000Base-T	100Base-TX
22	1000Base-T	1000Base-T	1000Base-T	100Base-TX	100Base-TX
23	1000Base-T	1000Base-T	100Base-TX	1000Base-T	100Base-TX
24	100Base-TX	100Base-TX	1000Base-T	1000Base-T	100Base-TX
25	1000Base-T	1000Base-T	100Base-TX	100Base-TX	100Base-TX

Продовження таблиці 15

26	100Base-TX	100Base-TX	1000Base-T	100Base-TX	100Base-TX
27	100Base-TX	100Base-TX	100Base-TX	1000Base-T	100Base-TX
28	100Base-TX	100Base-TX	100Base-TX	100Base-TX	100Base-TX
29	1000Base-FX	1000Base-FX	1000Base-T	1000Base-T	100Base-TX
30	1000Base-T	1000Base-T	1000Base-FX	1000Base-T	100Base-TX
31	1000Base-T	1000Base-T	1000Base-T	1000Base-T	100Base-TX
32	1000Base-T	1000Base-T	1000Base-T	100Base-TX	100Base-TX
33	1000Base-T	1000Base-T	100Base-TX	1000Base-T	100Base-TX

Примітка: Технології 10BaseT, 100BaseTX та 1000Base-T як середовище передавання даних використовують мідну звиту пару (Cooper Twisted Pair), а технології 100Base-FX та 1000Base-FX – волоконно-оптичний кабель (Fiber Cable). Для волоконно-оптичного кабеля існую і інші варіанти позначення – 1000Base-SX, 1000Base-LH, 10G Base-LR тощо

Таблиця 16

Вихідні дані для налагодження параметрів інтерфейсів пристроїв

№ варіанта	Канал Serv-G-N-1 –	Канал Serv-G-N-2 –	Канал SW-G-N-1 –	Канали підключення

	SW-G-N-1		SW-G-N-2		SW-G-N-2		робочих станцій	
	Швидкість, Мбіт/с	Режим	Швидкість, Мбіт/с	Режим	Швидкість, Мбіт/с	Режим	Швидкість, Мбіт/с	Режим
1	1000	Full	1000	Full	1000	Full	100	Full
2	1000	Full	1000	Full	100	Full	100	Full
3	1000	Full	100	Full	100	Full	100	Half
4	100	Full	100	Full	100	Full	100	Half
5	100	Full	100	Full	100	Full	100	Full
6	100	Full	1000	Full	100	Full	100	Half
7	100	Full	100	Full	100	Full	100	Half
8	100	Full	100	Full	100	Full	100	Half
9	1000	Full	1000	Full	1000	Full	100	Full
10	1000	Full	1000	Full	1000	Full	100	Half
11	1000	Full	1000	Full	100	Full	100	Half
12	1000	Full	100	Full	100	Full	100	Half
13	1000	Full	100	Full	100	Full	100	Full
14	100	Full	1000	Full	100	Full	100	Full
15	100	Full	1000	Full	1000	Full	100	Full
16	1000	Full	100	Full	1000	Full	100	Half
17	100	Full	1000	Full	100	Full	100	Half
18	100	Full	100	Full	1000	Full	100	Half
19	100	Full	100	Full	100	Full	100	Half
20	100	Full	100	Full	100	Full	100	Full
21	1000	Full	1000	Full	1000	Full	100	Half
22	1000	Full	1000	Full	100	Full	100	Full
23	1000	Full	100	Full	1000	Full	100	Half
24	100	Full	1000	Full	1000	Full	100	Half
25	1000	Full	100	Full	100	Full	100	Half

Продовження таблиці 16

26	100	Full	1000	Full	100	Full	100	Full
27	100	Full	100	Full	1000	Full	100	Full
28	100	Full	100	Full	100	Full	100	Half
29	1000	Full	1000	Full	1000	Full	100	Half
30	1000	Full	1000	Full	1000	Full	100	Half
31	1000	Full	1000	Full	1000	Full	100	Full
32	1000	Full	1000	Full	100	Full	100	Full
33	1000	Full	100	Full	100	Full	100	Half

Таблиця 17

Параметри IP-адресації мережі

№ варіанта	IP-адреса мережі A	Префікс	IP-адреса шлюзу за замовчуванням/ IP-адреса DNS-сервера
1	191.G.N.0	/24	Перша IP-адреса діапазону

2	192.G.N.0	/25	Остання IP-адреса діапазону
3	193.G.N.0	/26	Перша IP-адреса діапазону
4	194.G.N.0	/27	Остання IP-адреса діапазону
5	195.G.N.0	/28	Перша IP-адреса діапазону
6	196.G.N.0	/24	Остання IP-адреса діапазону
7	197.G.N.0	/25	Перша IP-адреса діапазону
8	198.G.N.0	/26	Остання IP-адреса діапазону
9	199.G.N.0	/27	Перша IP-адреса діапазону
10	200.G.N.0	/28	Остання IP-адреса діапазону
11	201.G.N.0	/24	Перша IP-адреса діапазону
12	202.G.N.0	/25	Остання IP-адреса діапазону
13	203.G.N.0	/26	Перша IP-адреса діапазону
14	204.G.N.0	/27	Остання IP-адреса діапазону
15	205.G.N.0	/28	Перша IP-адреса діапазону
16	206.G.N.0	/24	Остання IP-адреса діапазону
17	207.G.N.0	/25	Перша IP-адреса діапазону
18	208.G.N.0	/26	Остання IP-адреса діапазону
19	209.G.N.0	/27	Перша IP-адреса діапазону
20	210.G.N.0	/28	Остання IP-адреса діапазону
21	211.G.N.0	/24	Перша IP-адреса діапазону
22	212.G.N.0	/25	Остання IP-адреса діапазону
23	213.G.N.0	/26	Перша IP-адреса діапазону
24	214.G.N.0	/27	Остання IP-адреса діапазону
25	215.G.N.0	/28	Перша IP-адреса діапазону
26	216.G.N.0	/24	Остання IP-адреса діапазону
27	217.G.N.0	/25	Перша IP-адреса діапазону
28	218.G.N.0	/26	Остання IP-адреса діапазону
29	219.G.N.0	/27	Перша IP-адреса діапазону

Продовження таблиці 17

30	220.G.N.0	/28	Остання IP-адреса діапазону
31	221.G.N.0	/24	Перша IP-адреса діапазону
32	222.G.N.0	/25	Остання IP-адреса діапазону
33	223.G.N.0	/26	Перша IP-адреса діапазону

Контрольні питання

1. Середовища передачі даних мереж Ethernet.
2. Рознім для звитої пари.
3. Рознімі для волоконно-оптичного кабеля.
4. Мережні адаптери Ethernet.
5. Інтерфейси комутаторів Ethernet.
6. Змінні інтерфейсні модулі для мережних адаптерів, маршрутизаторів та комутаторів Ethernet.

7. Наведіть пояснення понять MDI/MDIX та призначення функції Auto-MDI.
8. Схеми прямих Ethernet-кабелів для технологій Ethernet 10 Base-T/Fast Ethernet 100Base-TX та технології Gigabit Ethernet 1000 BaseT.
9. Схеми перехресних Ethernet-кабелів для технологій Ethernet 10 Base-T/Fast Ethernet 100Base-TX та технології Gigabit Ethernet 1000 BaseT.
10. Наведіть таблицю з'єднань основних Ethernet-пристроїв. Зазначте, який кабель використовується.
11. Основні параметри фізичних інтерфейсів комутатора Cisco.
12. Фізичні і логічні інтерфейси комутаторів Cisco.
13. Наведіть перелік та поясніть призначення команд для операцій з інтерфейсом, групою інтерфейсів комутатора Cisco.
14. Наведіть перелік та поясніть призначення команд для налагодження параметрів фізичних інтерфейсів комутатора Cisco.
15. Наведіть перелік та поясніть призначення основних команд моніторингу роботи інтерфейсів комутатора Cisco.

Лабораторна робота 3
НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ КОМУТАТОРІВ ETHERNET

Мета заняття: ознайомитися алгоритмом роботи комутатора Ethernet; ознайомитися з можливостями керованих комутаторів Cisco та можливостями мережної операційної системи Cisco IOS стосовно налагодження комутаторів; отримати практичні навички налагодження, моніторингу та діагностування роботи комутаторів керованих комутаторів Cisco у локальній мережі; дослідити процеси роботи керованих комутаторів Cisco та процеси передачі даних у побудованій мережі.

Теоретичні відомості

Структурна схема та алгоритм роботи комутатора Ethernet

Основним пристроєм для побудови сучасних мереж Ethernet є комутатор, який використовує «алгоритм прозорого моста», що розроблявся власне для мостів – пристроїв попередників комутаторів. Цей алгоритм описаний у стандарті IEEE 802.1D. Оскільки стандарт був розроблений задовго до появи комутатора, то в ньому використовується термін міст. Структурна схема моста наведена на рис. 1.

Прозорий міст непомітний для мережевих адаптерів кінцевих вузлів, тобто мережеві адаптери при його використанні не виконують ніяких додаткових дій для того, щоб кадр пройшов через міст. Прозорий міст сам будує свою адресну таблицю на основі пасивного спостереження за трафіком, який передається у підключених до його портів сегментах. При цьому враховуються адреси джерел кадрів даних, які поступають на порти моста. За адресою джерела кадру міст робить висновок про приналежність вузла тому чи іншому сегменту мережі. На основі адресної таблиці приймаються рішення передавати кадри в інший сегмент чи ні.

Алгоритм роботи прозорого моста наведений на рис. 2

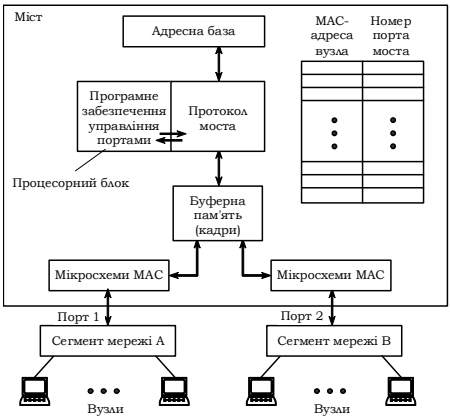


Рис. 1. Структура моста

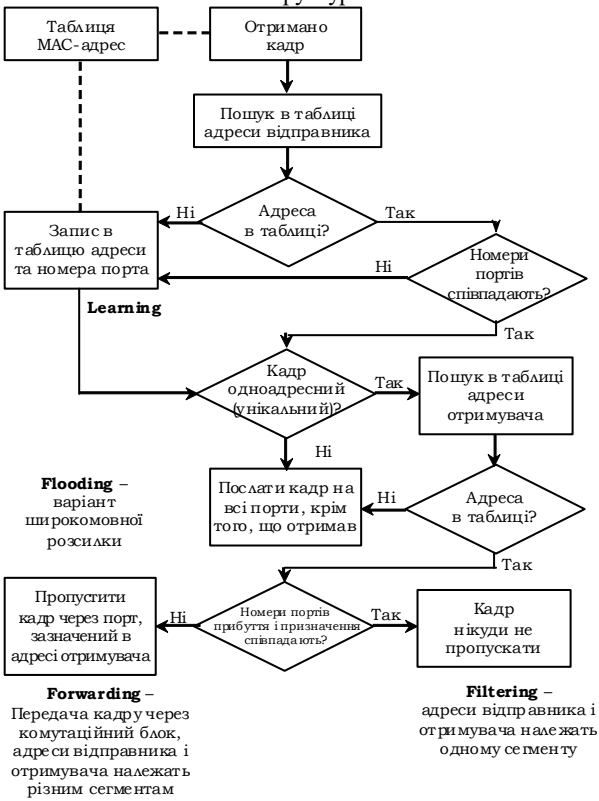


Рис. 2. Блок-схема алгоритму роботи прозорого моста

Основні команди налагодження параметрів мережної адресації комутатора Cisco

Питання призначення IP-адрес мережним пристроям є досить важливим. Наявність IP-адреси дає змогу перевірити доступність пристрою, а подальші активація та налагодження засобів віддаленого доступу дають змогу здійснювати підключення до пристрою за відповідною IP-адресою та виконувати операції його налагодження та керування процесом роботи.

Для налагодження параметрів адресації комутатора Cisco використовуються такі команди: **ip address**, **ip default-gateway**, **ip name-server**, **ip host** та деякі інші Для відміни дії вищезгаданих команд використовують форму **no**.

Команда **ip address** застосовується для призначення комутатору IP-адреси, що застосовується для виконання операцій налагодження та керування роботою пристрою. Особливістю її застосування є те, що IP-адреса призначається логічному інтерфейсу VLAN. За замовчуванням на комутаторі створено логічний інтерфейс Vlan 1. Наявна можливість створювати нові інтерфейси VLAN і призначати їм відповідні IP-адреси. Команда **ip default-gateway** застосовується для призначення IP-адреси шлюзу за замовчуванням комутатора. На комутаторі налагоджується лише один шлюз за замовчуванням. Команда **ip name-server** призначена для встановлення IP-адреси DNS-сервера (таких адрес може бути декілька).

Також для адресації використовуються команди **ip domain-name** – зазначення текстового імені домену, **ip host** – встановлення локальної відповідності між текстовими іменами вузлів та їх IP-адресами (принцип, аналогічний використанню файла відповідностей на робочій станції, наприклад: файл /etc/hosts в ОС Unix). Особливим є застосування команди **ip domain-lookup**. Ця команда активує функцію пошуку в системі DNS. Рекомендується відключати цю функцію командою **no ip domain-lookup**, оскільки пристрій не повинен намагатися шукати в DNS кожне слово, яке введено у командному рядку, і якщо воно не збігається зі стандартною командою – пересилати запит на сервер. Замість команди **ip domain-name** можна застосовувати команду, аналогічну команді **ip domain name**, а

замість команди **ip domain-lookup** – команду **ip domain lookup**. Синтаксис усіх розглянутих команд наведено нижче.

Синтаксис команди **ip address** (режим конфігурування інтерфейсу VLAN):

ip address { *IP_address network_mask* } | dhcp,

де ***IP_address*** – IP-адреса в десятковому записі;

network_mask – маска мережі, записана у звичайній формі;

dhcp – службова конструкція, за допомогою якої зазначається, що IP-адресу необхідно отримати автоматично за протоколом DHCP.

Синтаксис команди **ip default-gateway** (режим глобального конфігурування):

ip default-gateway *IP_address*,

де ***IP_address*** – IP-адреса шлюзу за замовчуванням у десятковому записі.

Синтаксис команди **ip name-server** (режим глобального конфігурування):

ip name-server *IP_address* [*IP_address*],

де ***IP_address*** – IP-адреса (адреси) DNS-сервера (серверів), можна зазначити до шести включно DNS-серверів.

Синтаксис команди **ip domain-name** (режим глобального конфігурування):

ip domain-name *domain_name*,

де ***domain_name*** – текстове ім'я домену.

Синтаксис команди **ip domain name** (режим глобального конфігурування):

ip domain name *domain_name*,

де ***domain_name*** – текстове ім'я домену.

Синтаксис команди **ip domain-lookup** (режим глобального конфігурування):

ip domain-lookup.

Команда не має параметрів.

Синтаксис команди **ip domain lookup** (режим глобального конфігурування):

ip domain lookup.

Команда не має параметрів.

Синтаксис команди **ip host** (режим глобального конфігурування):

ip host *name* [*tcp-port*] *IP_address* [*IP_address*],

де ***name*** – ім'я вузла;

tcp-port – номер TCP-порту, необов'язковий аргумент. Порт вузла, до якого здійснюється підключення за протоколом telnet.

IP_address – IP-адреса у десятковому записі, з кожним іменем вузла може бути пов'язано до восьми IP-адрес.

Основні команди роботи з таблицею комутації комутатора Cisco

Основними діями в ході роботи з таблицею комутації комутатора Cisco є перегляд таблиці комутації, додавання та вилучення записів у таблицю, встановлення часових параметрів для записів. Для цього використовуються такі команди, як: **mac-address-table, mac-address-table static, mac-address-table dynamic, mac-address-table secure, mac-address-table aging-time, mac-address-table notification, clear mac-address-table, show mac-address-table** та ін. Найбільш узагальненою командою для формування записів таблиці комутації є команда **mac-address-table**. У багатьох випадках використовують її спрощений варіант **mac-address-table static**. Відміна дії більшості команд виконується з використанням службового слова **no**. Для перегляду таблиці комутації та її параметрів використовується команда **show mac-address-table** і її модифікації **show mac-address-table static, show mac-address-table dynamic, show mac-address-table aging-time** та ін. Повне очищення таблиці комутації або видалення окремих її записів здійснюється за допомогою команди **clear mac-address-table.**

Синтаксис команди **mac-address-table** (режим глобального конфігурування):

mac-address-table { dynamic | static | secure } ***hw-address*** **{ vlan** ***vlan_id*** **} { interface** ***interface_type1 interface-id1*** **[...** ***interface_typeN interface_idN*** **] [protocol { ip | ipx | assigned }]**,

де **dynamic** – службова конструкція, за допомогою якої зазначається, що запис є динамічним (тобто застаріває і після спливання виділеного часу видаляється з таблиці комутації);

static – службова конструкція, за допомогою якої зазначається, що запис є статичним (тобто не застаріває і знаходиться у таблиці комутації постійно);

secure – службова конструкція, за допомогою якої зазначається, що запис є захищеним записом типу (тобто може існувати лише на одному порту);

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

vlan – службова конструкція, за допомогою якої зазначається належність запису до певної VLAN;

vlan_id – номер VLAN в діапазоні від 1 до 1005, якщо використовується стандартний образ IOS, у разі використання образу з розширеними можливостями – у діапазоні від 1 до 4094;

interface – службова конструкція, за допомогою якої зазначається порт для формування запису;

interface_type – тип інтерфейсу (порту), може набувати значень Ethernet, FastEthernet, GigabitEthernet та ін.;

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

protocol – службова конструкція, за допомогою якої зазначається протокол, для якого формуються записи (використовується у спеціальних версіях IOS для високопродуктивних комутаторів), якщо протокол не задається, то запис формується для всіх протоколів;

ip – службова конструкція, за допомогою якої зазначається протокол IP стеку TCP/IP;

ipx – службова конструкція, за допомогою якої зазначається протокол IPX стеку IPX/SPX;

assigned – службова конструкція, за допомогою якої зазначаються інші протоколи (DECnet, Appletalk).

Синтаксис команди **mac-address-table static** (режим глобального конфігурування):

mac-address-table static ***hw_address*** **vlan** ***vlan_id*** **interface** ***interface_type interface_id***.

Параметри команди аналогічні параметрам команди **mac-address-table**.

Синтаксис команди **mac-address-table aging-time** (режим глобального конфігурування):

mac-address-table aging-time ***seconds*** **[vlan** ***vlan_id*** **]**,

де ***seconds*** – інтервал часу існування динамічного запису в таблиці комутації комутатора від моменту його появи або оновлення (може набувати значення 0 або змінюватися в діапазоні від 10 до 1000000), за замовчуванням 300. Значення 0 виключає застарівання запису;

vlan – службова конструкція, за допомогою якої зазначається належність запису до певної VLAN; якщо параметр **vlan** не вказано, то команда застосовується для всіх VLAN;

vlan_id – номер VLAN.

Синтаксис команди **mac-address-table notification** (режим глобального конфігурування):

mac-address-table notification [history-size ***size_value*** **| interval** ***interval_value*** **]**,

де **history-size** – службова конструкція, за допомогою якої зазначається небхідність ведення історії оновлень MAC-адрес пристрою;

size_value – значення максимальної кількості записів у таблиці оновлень MAC-адрес пристрою, може змінюватися у діапазоні від 0 до 500;

interval – службова конструкція, за допомогою якої зазначається інтервал оновлень записів;

interval_value – значення інтервалу оновлення записів (с), може змінюватися у діапазоні від 0 до 2147483647, за замовчуванням становить 1 с.

Синтаксис команди **clear mac-address-table** (привілейований режим):

clear mac-address-table {dynamic [address ***hw-address*** **| interface** ***interface-type interface-id*** **| vlan** ***vlan-id*****] | notification}**.

Параметри команди аналогічні параметрам інших команд керування таблицею комутації.

Синтаксис команди **show mac-address-table** (привілейований режим):

show mac-address-table [aging-time | count | dynamic | static] [address ***hw_address*** **] [interface** ***interface_type interface_id*** **] [vlan** ***vlan_id*** **]**.

Параметри команди аналогічні параметрам попередньо розглянутих команд.

Основні команди діагностики параметрів адресації та процесу роботи комутатора Cisco

Для виведення діагностичної інформації про параметри фізичних та логічних інтерфейсів, результати налагоджень, уміст службових таблиць, процес роботи комутатора використовуються різні варіанти команд **show**. Перелік команд та їх призначення наведено у табл. 1.

Таблиця 1

Перелік команд show, необхідних для діагностики процесу роботи комутатора Cisco

Команда	Призначення
show ip interface	Виведення інформації про IP-інтерфейси пристрою
show ip interface brief	Виведення інформації про IP-інтерфейси пристрою у чкороченому вигляді
show hosts	Виведення інформації про встановлені відповідності між IP-адресами та текстовими адресами
show mac-address-table	Виведення інформації про стан таблиці комутації
show mac address-table address	Виведення таблиці комутації для вказаної MAC-адреси
show mac address-table aging-time	Виведення часу старіння для певного запису таблиці комутації, для всіх записів таблиці комутації для певної VLAN або для всіх записів таблиці комутації всіх VLAN
show mac address-table count	Виведення кількості адрес, які наявні у всіх VLAN або у певній VLAN
show mac address-table dynamic	Виведення інформації лише про динамічні записи таблиці комутації
show mac address-table static	Виведення інформації лише про статичні записи таблиці комутації
show mac address-table interface ***interface-type interface-id***	Виведення інформації про записи в таблиці комутації, які пов'язані з певним інтерфейсом у певній VLAN
show mac address-table vlan	Виведення інформації з таблиці комутації для певної VLAN
show mac address-table notification	Виведення інформації про установки оновлень таблиці комутації для всіх інтерфейсів або певного інтерфейсу.

Модельний приклад налагодження функціонування локальної комп'ютерної мережі, побудованої на базі керованого комутатора Cisco

Розглянемо специфіку налагодження роботи комутатора Cisco моделі WS-C2960-24TT-L та маршрутизатора моделі Cisco 1841 для локальної комп'ютерної мережі, схему якої наведено на рис. 17.

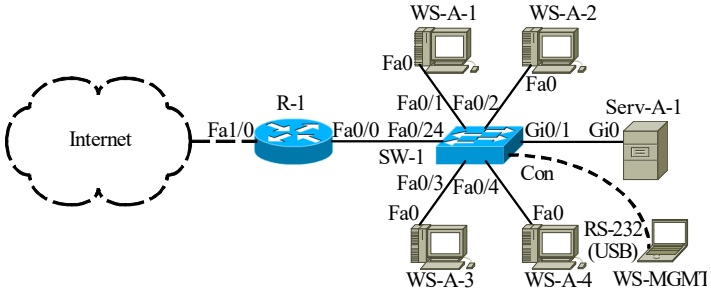


Рис. 17. Приклад мережі

Під час побудови даної мережі для з'єднання пристроїв використано дані табл. 2. Для налагодження параметрів окремих Ethernet-каналів зв'язку між пристроями використано дані табл. 3. Для налагодження параметрів адресації пристроїв використано дані табл. 4.

Таблиця 2

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R_1 (Cis-	Fa0/1	Internet	Internet_Interface

со 1841)	Fa0/0	Комутатор SW-1	Fa0/24
Комутатор SW-1 (Cisco 2960-24TT-L)	Con	Робоча станція WS-MGMT	RS-232 (USB)
	Gi0/1	Сервер Serv-A-1	Gi0
	Fa0/1	Робоча станція WS-A-1	Fa0
	Fa0/2	Робоча станція WS-A-2	Fa0
	Fa0/3	Робоча станція WS-A-3	Fa0
	Fa0/4	Робоча станція WS-A-4	Fa0
	…	…	…
	Fa0/24	Маршрутизатор R_1	Fa0/0
Internet	Internet Interface	Маршрутизатор R_1	Fa1/0
Робоча станція WS-MGMT	RS-232 (USB)	Комутатор SW-1	Con
Сервер Serv-A-1	Gi0		Gi0/1
Робоча станція WS-A-1	Fa0		Fa0/1
Робоча станція WS-A-2	Fa0		Fa0/2
Робоча станція WS-A-3	Fa0		Fa0/3
Робоча станція WS-A-4	Fa0		Fa0/4

Таблиця 3

Параметри Ethernet-каналів зв'язку між пристроями для прикладу

Канал між пристроями	Технологія	Тип кабелю	Режим	Швидкість, Мбіт/с
R-1 – SW-1	100Base-TX	Прямий	Автовибір	Автовибір
Serv-A-1 – SW-1	1000Base-T	Прямий	Дуплексний	1000
WS-A-1 – SW-1	100Base-TX	Прямий	Дуплексний	100
WS-A-2 – SW-1	100Base-TX	Прямий	Дуплексний	100
WS-A-3 – SW-1	100Base-TX	Прямий	Дуплексний	100
WS-A-4 – SW-1	100Base-TX	Прямий	Дуплексний	100

Таблиця 4

Параметри адресації мережі для прикладу

Мережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	MAC-адреса	IP-адреса	Маска	Префікс
Мережа A	–	–	195.10.1.0	255.255.255.0	/24
Маршрутизатор R_1	Інтерфейс Fa0/0	CA-01-07-FE-00-08	195.10.1.254	255.255.255.0	/24
Комутатор SW-1	Інтерфейс Vlan 1	00-D0-BA-E4-0D-9B	195.10.1.252	255.255.255.0	/24
	Шлюз за замовчуванням				
	Основний DNS-сервер	–	195.10.1.254	–	–
Сервер Serv-A-1	Мережний адаптер	00-05-5E-26-8A-1C	195.10.1.250	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–
Робоча станція WS-A-1 (Linux)	Мережний адаптер	00-60-5C-16-8B-30	195.10.1.1	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–

Робоча станція WS-A-2 (Windows)	Мережний адаптер	00-10-43-2C-BD-BB	195.10.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–
Робоча станція WS-A-3 (Windows)	Мережний адаптер	00-10-11-49-ED-09	195.10.1.3	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–
Робоча станція WS-A-4 (Windows)	Мережний адаптер	00-E0-8F-00-51-96	195.10.1.4	255.255.255.0	/24
	Шлюз за замовчуванням	–	195.10.1.254	–	–
	Основний DNS-сервер	–	195.10.1.254	–	–

Примітка: * – параметри адресації не зазначені.

Сценарій налагодження параметрів іменування та IP-адресації комутатора мережі SW-1 наведено нижче.

```
…
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-1
SW-1(config)#interface vlan 1
SW-1(config-if)#description SW-1-MANAGEMENT-IP-ADDRESS
SW-1(config-if)#ip address 195.10.1.252 255.255.255.0
SW-1(config-if)#no shutdown
SW-1(config-if)#exit
SW-1(config)#ip default-gateway 195.10.1.254
SW-1(config)#ip name-server 195.10.1.254
SW-1(config)#ip domain-name MY.NET
SW-1(config)#no ip domain-lookup
SW-1(config)#exit
SW-1#
…
```

Сценарій параметрів іменування пристрою, активації та налагодження інтерфейсу FastEthernet 0/0 для маршрутизатора R-1 наведено нижче. Для виконання цього сценарію необхідно відключити консольний кабель від комутатора SW-1 та підключити до маршрутизатора R-1.

…
Router>enable
Router#configure terminal
Router(config)#hostname R-1
R-1(config)#interface FastEthernet 0/0
R-1(config-if)#description LINK-TO-LAN-A
R-1(config-if)#ip address 195.10.1.254 255.255.255.0
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#ip domain-name MY.NET
R-1(config)#no ip domain-lookup
R-1(config)#exit
R-1#
…

Сценарій налагодження локальних відповідностей між назвами кінцевих вузлів та комунікаційних пристроїв та їх IP-адресами для комутатора SW-1 наведено нижче.

…
SW-1>enable
SW-1#configure terminal
SW-1(config)#ip host SERV-A-1 195.10.1.250
SW-1(config)#ip host WS-A-1 195.10.1.1
SW-1(config)#ip host WS-A-2 195.10.1.2
SW-1(config)#ip host WS-A-3 195.10.1.3
SW-1(config)#ip host WS-A-4 195.10.1.4
SW-1(config)#ip host SW-1 195.10.1.252
SW-1(config)#ip host R-1 195.10.1.254
SW-1(config)#exit
SW-1#
…

Сценарій внесення статичного запису, що містить відповідність MAC-адреси мережного адаптера сервера Serv-A-1 CA-01-07-FE-00-08) та інтерфейсу GigabitEthernet 0/1 комутатора SW-1, до таблиці комутації комутатора SW-1 наведено нижче.

…
SW-1#configure terminal
SW-1(config)#mac-address-table static CA01.07FE.0008 vlan 1 interface GigabitEthernet 0/1
SW-1(config)#exit

SW-1#

…

Результати виконання команд моніторингу та діагностики роботи комутатора для розглянутого модельного прикладу

З метою перевірки досяжності сервера та решти робочих станцій мережі з робочих станцій WS-A-1 та WS-A-2 застосовано команду **ping**. За допомогою цієї ж команди виконано перевірку досяжності всіх вузлів мережі з комутатора SW-1. Частину результатів цих перевірок наведено на рис. 18 – 20. З метою перегляду інформації про налагодження інтерфейсів комутатора та маршрутизатора для розглянутого прикладу застосовано команди **show interfaces** та **show ip interfaces brief**. Для отримання інформації про MAC-адресу блока керування комутатора можта також скористатися командами **show version** або **show tech-support.** З метою перевірки встановлених локальних відповідностей між текстовими іменами вузлів та їх IP-адресами застосовано команду **show hosts**. Для перегляду таблиці комутації комутатора застосовано команду **show mac-address-table**. Результати роботи зазначених команд наведено відповідно на рис. 21 – 26.

```
root@WS-A-1~#ping 195.10.1.2
PING 195.10.1.2 (195.10.1.2): 56 data bytes
64 bytes from 195.10.1.2: seq=0 ttl=255 time=12.064 ms
64 bytes from 195.10.1.2: seq=1 ttl=255 time=5.239 ms
64 bytes from 195.10.1.2: seq=2 ttl=255 time=13.561 ms
64 bytes from 195.10.1.2: seq=3 ttl=255 time=10.502 ms
^C
--- 195.10.1.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 5.239/10.341/13.561 ms
```

Рис. 18. Результат виконання команди **ping** на робочій станції WS-A-1

```
C:\>ping 195.10.1.250
Обмен пакетами с 195.10.1.250 по 32 байт:
Ответ от 195.10.1.250: число байт=32 время 21мс TTL=255
Ответ от 195.10.1.250: число байт=32 время 4мс TTL=255
Ответ от 195.10.1.250: число байт=32 время 2мс TTL=255
Ответ от 195.10.1.250: число байт=32 время 6мс TTL=255
Статистика Ping для 195.10.1.250:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 <0% потерь>,
Приблизительное время приема-передачи в мс:
    Минимальное = 2 мсек, Максимальное 21 мсек, Среднее = 8 мсек
```

Рис. 19. Результат виконання команди **ping** на робочій станції WS-A-2

```
SW-1#ping SERV-A-1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.10.1.250, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

Рис. 20. Результат виконання команди **ping** на комутаторі SW-1

```
SW-1#show interfaces Vlan 1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 00d0.bae4.0d9b (bia 00d0.bae4.0d9b)
  Description: SW-1-MANAGEMENT-IP-ADDRESS
  Internet address is 195.10.1.252/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
```

Рис. 21. Результати виконання команди **show interfaces Vlan 1** на комутаторі SW-1

```
R-1#show interfaces FastEthernet 0/0
FastEthernet0/0 is up, line protocol is up (connected)
Hardware is Lance, address is ca01.07fe.0008 (bia ca01.07fe.0008)
Description: LINK-TO-LAN-A
Internet address is 195.10.1.254/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Full-duplex, 100Mb/s, media type is RJ45
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
R-1#
```

Рис. 22. Результати виконання команди **show interfaces GigabitEthernet 0/1** на маршрутизаторі R-1

```
SW-1>show ip interface brief
Interface              IP-Address      OK? Method Status           Protocol
FastEthernet0/1        unassigned      YES manual up                   up
FastEthernet0/2        unassigned      YES manual up                   up
FastEthernet0/3        unassigned      YES manual up                   up
FastEthernet0/4        unassigned      YES manual up                   up
FastEthernet0/5        unassigned      YES manual down                 down
...
FastEthernet0/23       unassigned      YES manual down                 down
```

```
FastEthernet0/24       unassigned      YES manual up                    up
GigabitEthernet0/1     unassigned      YES manual up                    up
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  195.1.1.100     YES manual up                    up
SW-1>
```

Рис. 23. Результати виконання команди **show ip interfaces brief** на комутаторі SW-1

```
R-1#show ip interface brief
Interface              IP-Address      OK? Method Status           Protocol
FastEthernet0/0        195.10.1.254    YES manual up                   up
FastEthernet0/1        unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
R-1#
```

Рис. 24. Результати виконання команди **show ip interfaces brief** на маршрутизаторі R-1

```
SW-1#show hosts
Default Domain is MY.NET
Name/address lookup uses domain service
Name servers are 195.10.1.254
Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
temp - temporary, perm - permanent
NA - Not Applicable None - Not defined
Host                 Port Flags      Age Type Address(es)
SERV-A-1             None (perm, OK)  0   IP    195.10.1.250
WS-A-1               None (perm, OK)  0   IP    195.10.1.1
WS-A-2               None (perm, OK)  0   IP    195.10.1.2
WS-A-3               None (perm, OK)  0   IP    195.10.1.3
WS-A-4               None (perm, OK)  0   IP    195.10.1.4
SW-1                 None (perm, OK)  0   IP    195.10.1.252
R-1                  None (perm, OK)  0   IP    195.10.1.254
SW-1#
```

Рис. 25. Результати виконання команди **show hosts** на комутаторі SW-1

```
SW-1#show mac-address-table
Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0010.432c.bdbb    DYNAMIC     Fa0/2
   1    0005.5e26.8a1c    DYNAMIC     Gig0/1
   1    0010.1149.ed09    DYNAMIC     Fa0/3
   1    0060.5c16.8b30    DYNAMIC     Fa0/1
   1    00e0.8f00.5196    DYNAMIC     Fa0/4
SW-1#
```

Рис. 26. Результати виконання команди **show mac-address-table** на комутаторі SW-1

Файл конфігурації, що створений за сценарієм модельного прикладу, наведено на рис. 27 (частину несуттєвої інформації вилучено).

```
Building configuration...
Current configuration : 1771 bytes
!
version 12.2
```

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW-1
!
no ip domain-lookup
ip domain-name MY.NET
ip host SERV-A-1 195.10.1.250
ip host WS-A-1 195.10.1.1
ip host WS-A-2 195.10.1.2
ip host WS-A-3 195.10.1.3
ip host WS-A-4 195.10.1.4
ip host SW-1 195.10.1.252
ip host R-1 195.10.1.254

ip name-server 195.10.1.254
!
spanning-tree mode pvst
!
interface FastEthernet0/1
description LINK_TO_WS-A-1
duplex full
speed 100
!
interface FastEthernet0/2
description LINK_TO_WS-A-2
duplex full
speed 100
!
interface FastEthernet0/3
description LINK_TO_WS-A-3
duplex full
speed 100
!
...
!
interface GigabitEthernet0/1
description LINK_TO_SERV-A-1
duplex full
speed 1000
!
...
!
interface Vlan1
description SW-1-MANAGEMENT-IP-ADDRESS
ip address 195.10.1.252 255.255.255.0

!
ip default-gateway 195.10.1.254
!
...
!
end
```

Рис. 27. Файл конфігурації комутатора SW-1 для модельного прикладу

Завдання на лабораторну роботу

1. У середовищі програмного симулятора/емулятора створити проект локальної мережі (рис. 28). Під час побудови звернути увагу на вибір моделей комутаторів, мережних модулів та адаптерів, а також мережних з'єднань. Для цього використовувати дані табл. 5. Для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 9.

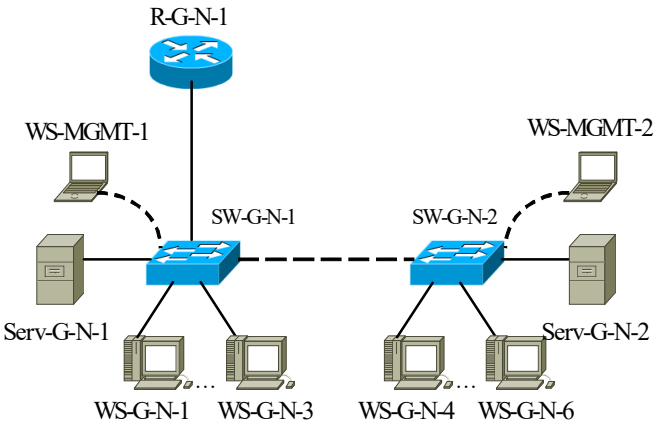


Рис. 28. Проект мережі

2. Визначити MAC-адреси мережних адаптерів робочих станцій та серверів мережі, MAC-адресу інтерфейса маршрутизатора, до якого підключена локальна мережа, базові MAC-адреси блоків керування (Base Ethernet MAC Address) комутаторів, MAC-адреси ін-

терфесів VLAN 1 комутаторів. Результати навести у вигляді таблиці, яка аналогічна табл. 4.

3. Розробити схему IP-адресації пристроїв мережі. Для цього скористатися даними табл. 6. Результати навести у вигляді таблиці, яка аналогічна табл. 4.

3. Провести налагодження параметрів IP-адресації пристроїв мережі згідно з даними п. 3. На кожному комутаторі та на маршрутизаторі для всіх вузлів встановити локальні відповідності між текстовими іменами та IP-адресами вузлів мережі.

5. Провести обмін даними між однією з робочих станцій та рештою вузлів мережі (комутаторами, серверами, робочими станціями). Дослідити процес формування та використання таблиць комутації на обох комутаторах мережі під час проведення обміну даними між пристроями.

6. Очистити таблиці комутації комутаторів.

7. На кожному комутаторі у таблицях комутації встановити статичні відповідності для фізичних адрес серверів, комутаторів та інтерфейса маршрутизатора. Дослідити процес використання таблиць комутації на обох комутаторах мережі для даних налагоджень під час проведення обміну даними між пристроями.

Таблиця 5

Вихідні дані для побудови мережі

№ варіанта	Канал R-G-N-1 – SW-G-N-1	Канал Serv-G-N-1 – SW-G-N-1	Канал Serv-G-N-2 – SW-G-N-2	Канал SW-G-N-1 – SW-G-N-2	Канали підключення робочих станцій
1	1000Base-T	1000Base-T	1000Base-T	1000Base-T	100Base-TX
2	1000Base-T	1000Base-T	1000Base-T	100Base-TX	100Base-TX
3	1000Base-T	1000Base-T	100Base-TX	1000Base-T	100Base-TX
4	100Base-TX	100Base-TX	1000Base-T	1000Base-T	100Base-TX
5	1000Base-T	1000Base-T	100Base-TX	100Base-TX	100Base-TX
6	100Base-TX	100Base-TX	1000Base-T	100Base-TX	100Base-TX
7	100Base-TX	100Base-TX	100Base-TX	1000Base-T	100Base-TX
8	100Base-TX	100Base-TX	100Base-TX	100Base-TX	100Base-TX
9	1000Base-FX	1000Base-FX	1000Base-T	1000Base-T	100Base-TX
10	1000Base-T	1000Base-T	1000Base-FX	1000Base-T	100Base-TX
11	1000Base-FX	1000Base-FX	1000Base-T	100Base-TX	100Base-TX
12	1000Base-FX	1000Base-FX	100Base-TX	1000Base-T	100Base-TX
13	1000Base-FX	1000Base-FX	100Base-TX	100Base-TX	100Base-TX
14	100Base-TX	100Base-TX	1000Base-FX	100Base-TX	100Base-TX
15	100Base-FX	100Base-FX	1000Base-T	1000Base-T	100Base-TX
16	1000Base-T	1000Base-T	100Base-FX	1000Base-T	100Base-TX

17	100Base-FX	100Base-FX	1000Base-T	100Base-TX	100Base-TX
18	100Base-FX	100Base-FX	100Base-TX	1000Base-T	100Base-TX
19	100Base-FX	100Base-FX	100Base-TX	100Base-TX	100Base-TX
20	100Base-TX	100Base-TX	100Base-FX	100Base-TX	100Base-TX
21	1000Base-T	1000Base-T	1000Base-T	1000Base-T	100Base-TX
22	1000Base-T	1000Base-T	1000Base-T	100Base-TX	100Base-TX
23	1000Base-T	1000Base-T	100Base-TX	1000Base-T	100Base-TX
24	100Base-TX	100Base-TX	1000Base-T	1000Base-T	100Base-TX
25	1000Base-T	1000Base-T	100Base-TX	100Base-TX	100Base-TX
26	100Base-TX	100Base-TX	1000Base-T	100Base-TX	100Base-TX
27	100Base-TX	100Base-TX	100Base-TX	1000Base-T	100Base-TX
28	100Base-TX	100Base-TX	100Base-TX	100Base-TX	100Base-TX
29	1000Base-FX	1000Base-FX	1000Base-T	1000Base-T	100Base-TX
30	1000Base-T	1000Base-T	1000Base-FX	1000Base-T	100Base-TX
31	1000Base-T	1000Base-T	1000Base-T	1000Base-T	100Base-TX
32	1000Base-T	1000Base-T	1000Base-T	100Base-TX	100Base-TX
33	1000Base-T	1000Base-T	100Base-TX	1000Base-T	100Base-TX

Таблиця 6

Параметри IP-адресації мережі

№ варіанта	IP-адреса мережі A	Префікс	IP-адреса шлюзу за замовчуванням/ IP-адреса DNS-сервера
1	191.G.N.0	/24	Перша IP-адреса діапазону
2	192.G.N.0	/25	Остання IP-адреса діапазону
3	193.G.N.0	/26	Перша IP-адреса діапазону
4	194.G.N.0	/27	Остання IP-адреса діапазону
5	195.G.N.0	/28	Перша IP-адреса діапазону
6	196.G.N.0	/24	Остання IP-адреса діапазону
7	197.G.N.0	/25	Перша IP-адреса діапазону
8	198.G.N.0	/26	Остання IP-адреса діапазону
9	199.G.N.0	/27	Перша IP-адреса діапазону
10	200.G.N.0	/28	Остання IP-адреса діапазону
11	201.G.N.0	/24	Перша IP-адреса діапазону
12	202.G.N.0	/25	Остання IP-адреса діапазону
13	203.G.N.0	/26	Перша IP-адреса діапазону
14	204.G.N.0	/27	Остання IP-адреса діапазону
15	205.G.N.0	/28	Перша IP-адреса діапазону
16	206.G.N.0	/24	Остання IP-адреса діапазону
17	207.G.N.0	/25	Перша IP-адреса діапазону
18	208.G.N.0	/26	Остання IP-адреса діапазону
19	209.G.N.0	/27	Перша IP-адреса діапазону
20	210.G.N.0	/28	Остання IP-адреса діапазону
21	211.G.N.0	/24	Перша IP-адреса діапазону

22	212.G.N.0	/25	Остання IP-адреса діапазону
23	213.G.N.0	/26	Перша IP-адреса діапазону
24	214.G.N.0	/27	Остання IP-адреса діапазону
25	215.G.N.0	/28	Перша IP-адреса діапазону
26	216.G.N.0	/24	Остання IP-адреса діапазону
27	217.G.N.0	/25	Перша IP-адреса діапазону
28	218.G.N.0	/26	Остання IP-адреса діапазону
29	219.G.N.0	/27	Перша IP-адреса діапазону
30	220.G.N.0	/28	Остання IP-адреса діапазону
31	221.G.N.0	/24	Перша IP-адреса діапазону
32	222.G.N.0	/25	Остання IP-адреса діапазону
33	223.G.N.0	/26	Перша IP-адреса діапазону

Контрольні питання

1. Наведість короткий опис структура прозорого моста.
2. Наведіть структуру таблиці комутації.
3. Наведіть основні складові алгоритму роботи прозорого моста.
4. Поясніть призначення режиму «Learning» в алгоритмі роботи прозорого моста.
5. Поясніть призначення режиму «Flooding» в алгоритмі роботи прозорого моста.
6. Поясніть призначення режиму «Forwarding» в алгоритмі роботи прозорого моста.
7. Поясніть призначення режиму «Filtering» в алгоритмі роботи прозорого моста.
8. Параметри фізичної адресації комутатора Cisco.
9. Параметри логічної адресації комутатора Cisco.
10. Наведіть перелік та поясніть призначення команд за допомогою яких можна визначити фізичні адреси комутатора Cisco.
11. Наведіть перелік та поясніть призначення команд за допомогою яких можна визначити параметри IP-адресації комутатора Cisco.
12. Наведіть перелік та поясніть призначення команд для налагодження параметрів IP-адресації комутатора Cisco.
13. Наведіть перелік та поясніть призначення основних команд моніторингу таблиці комутації комутатора Cisco.
14. Наведіть перелік та поясніть призначення команд очистки таблиці комутації комутатора Cisco.

15. Наведіть перелік та поясніть призначення команд додавання статичних записів до таблиці комутації комутатора Cisco.

Лабораторна робота 4
ДОСЛІДЖЕННЯ ПРАВИЛ ТА ПРОТОКОЛІВ УСТАНОВЛЕННЯ ВІДПОВІДНОСТЕЙ МІЖ ЛОГІЧНИМИ І ФІЗИЧНИМИ АДРЕСАМИ В IP-МЕРЕЖАХ

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

Теоретичні відомості

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

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

Найпоширенішим сучасним варіантом побудови локальних, регіональних, а часто і глобальних мереж є використання технологій

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

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

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

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

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

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

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

Блок-схему узагальненого алгоритму застосування зазначених правил формування групових та широкомовних MAC-адрес на ос-

нові відповідних IP-адрес версії 4, а також застосування протоколу ARP наведено на рис. 1.

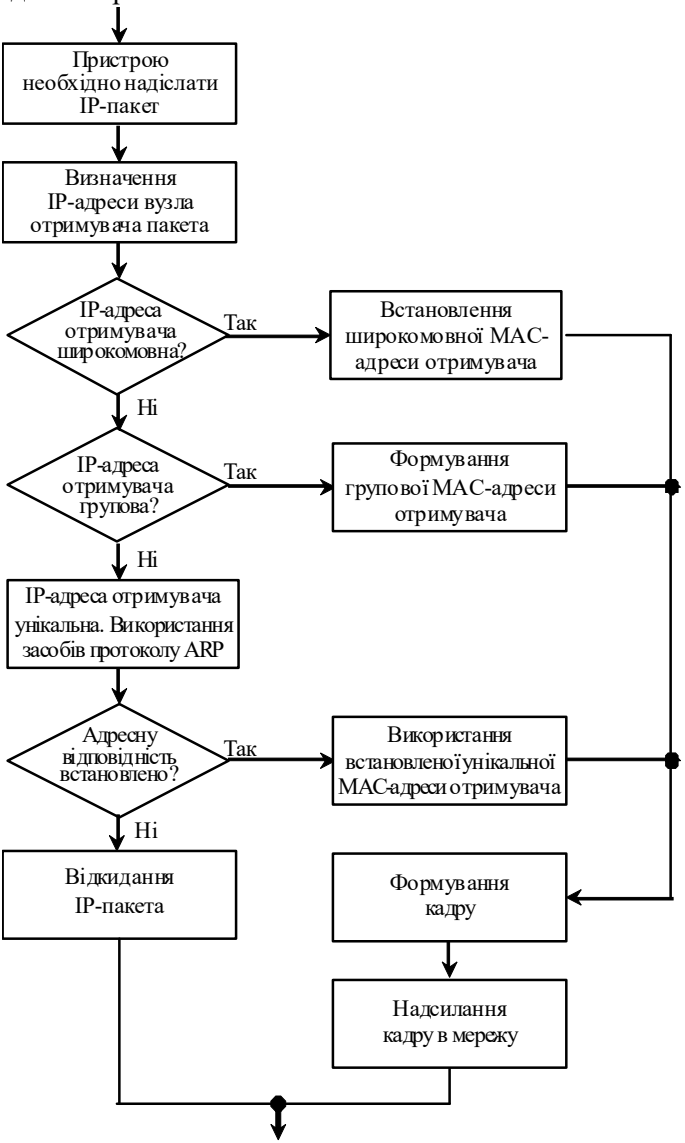


Рис. 1. Блок-схема узагальненого алгоритму застосування правил та протоколів установлення відповідностей між IP-адресами версії 4 та MAC-адресами

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

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

Таблиця 1

Зарезервовані групові IP-адреси

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

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

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

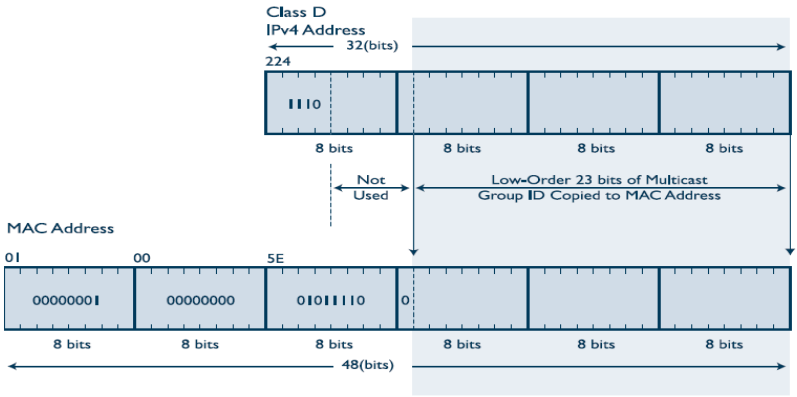


Рис. 2. Формування групової MAC-адреси на основі групової IP-адреси

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

Приклад 1.

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

Розв'язання.

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

11100000.0**0000000.00000000.00010110**

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

0000000.00000000.00010110

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

00000000.00000000.00010110

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

00-00-16

Результуюча групова MAC-адреса має вигляд:

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

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

Приклад 2.

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

Розв'язання.

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

1110xxxx.xmmmmmmm.mmmmmmmm.mmmmmmmm

Старші 4 біти (1110) є однаковими для всіх групових IP-адрес версії 4. Наступні 5 бітів (xxxxx) – це біти, які відкидаються під час

формування групової MAC-адреси. Решта 23 біти (m…m) – біти, які використовуються для формування ідентифікатора групи у груповій MAC-адресі. Для формування повного ідентифікатора групи (24 біти) перед цими бітами додається ще один біт – 0.

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

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

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

Повний ідентифікатор групи для цієї адреси має вигляд:

0**0000000-00000000-00010010**

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

0000000-00000000-00010010

Результуюча групова IP-адреса у двійковій формі має вигляд:

1110хххх.х0000000.00000000.00010010

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

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

У десятковій формі відповідно:

224.0.0.18

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

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

Для нашого випадку це адреси:

224.0.0.18

224.128.0.18

225.0.0.18

225.128.0.18

…
239.0.0.18
239.128.0.18

Приклад 3.

Ethernet-вузол, мережному інтерфейсу якого призначена IP-адреса 198.15.1.6/28, розсилає широкомовне повідомлення решті вузлів мережі. Визначити логічну та фізичну адреси призначення, що будуть застосовуватися для формування повідомлень.

Розв'язання.

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

11000110.00001111.00000001.00000110

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

11111111.11111111.11111111.11110000

Результат у десятковій системі числення має вигляд:

255.255.255.240

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

11000110.00001111.00000001.00000110

11111111.11111111.11111111.11110000

11000110.00001111.00000001.00000000

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

11000110.00001111.00000001.00000000

Результат у десятковій системі числення має вигляд:

198.15.1.0

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

11000110.00001111.00000001.0000**1111**

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

198.15.1.15

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

Загальні відомості про протоколи ARP/RARP

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

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

Стосовно моделі OSI протоколи ARP/RARP належать до мережного рівня. Але у багатьох випадках їх позиціонують як протоколи, що знаходяться між канальним і мережним рівнями. Таке позиціо-

нування пов'язане з тим, що протоколи ARP/RARP не застосовують повідомлення мережного рівня для передачі власної службової інформації, а формують власні повідомлення, які надалі інкапсулюються у кадри технології канального рівня.

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

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

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

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

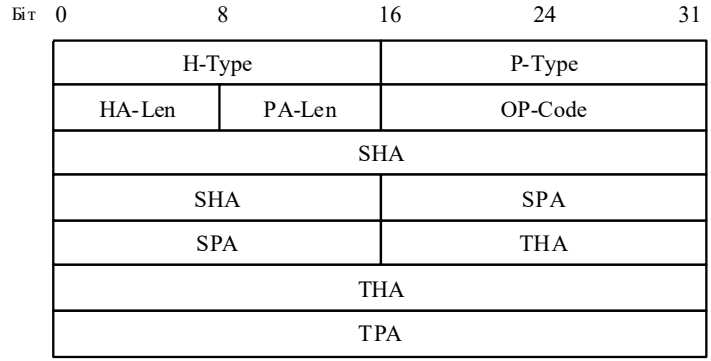


Рис. 3. Структура повідомлення протоколу ARP

Поле H-Type (Hardware Type) містить значення типу мережного інтерфейсу/адаптера, для якого відправник встановлює відповідність адрес (для мереж Ethernet дорівнює 0001h). Поле P-Type (Protocol Type) містить код мережного протоколу, для якого відправник встановлює відповідність адрес (для протоколу IP версії 4 – цей код дорівнює 0800h). Поле HA-Len (Hardware Address Length) містить довжину апаратної адреси (у байтах, для MAC-адреси HA-Len дорівнює 06h). Поле PA-Len (Protocol Address Length) містить довжину протокольної адреси (у байтах, для IP-адреси версії 4 поле PA-Len дорівнює 04h). Поле OP-Code (Operation Code) містить код операції, може набувати значень: 01h – ARP-запит; 02h – ARP-відповідь; 03h – RARP-запит; 04h – RARP-відповідь; решта значень пов’язані з маловживаними протоколами). Поля SHA (Sender

Hardware Address) та SPA (Sender Protocol Address) містять відповідно фізичну та логічну адреси відправника ARP-повідомлення. Поля THA (Target Hardware Address) та TPA (Target Protocol Address) – фізичну та логічну адреси отримувача ARP-повідомлення. Для технологій Ethernet/Wi-Fi та протоколу IP версії 4 поля SHA та THA – це MAC-адреси, а поля SPA та TPA – це IP-адреси. Необхідно зазначити, що у коректно сформованому ARP-запиті поле THA містить значення 000000000000h.

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

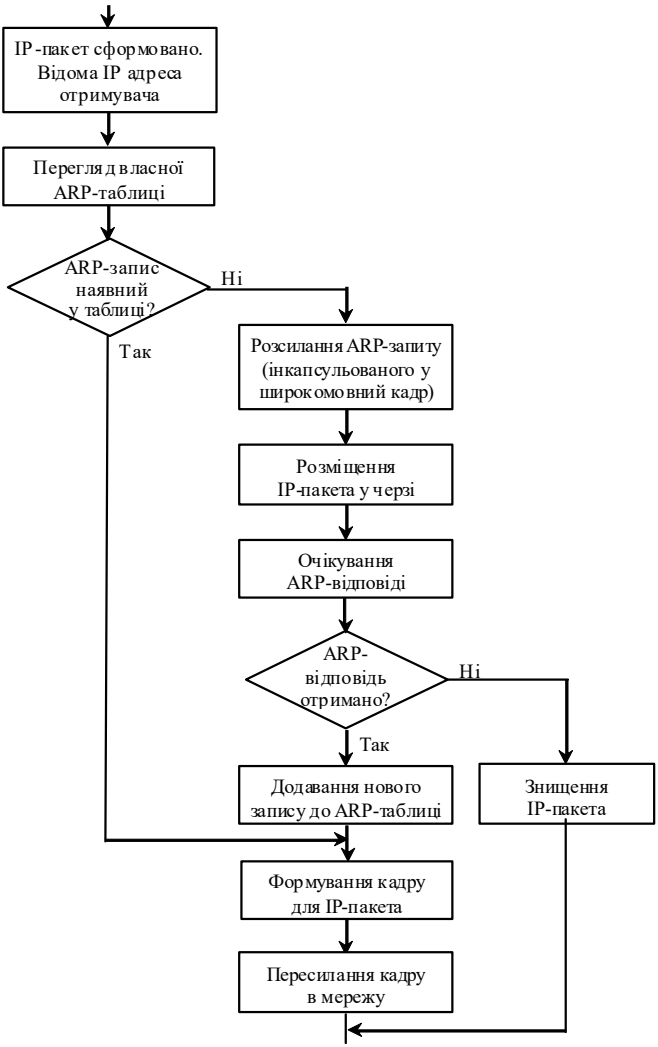


Рис. 4. Блок-схема алгоритму роботи протоколу ARP для випадку пересилання ARP-запиту

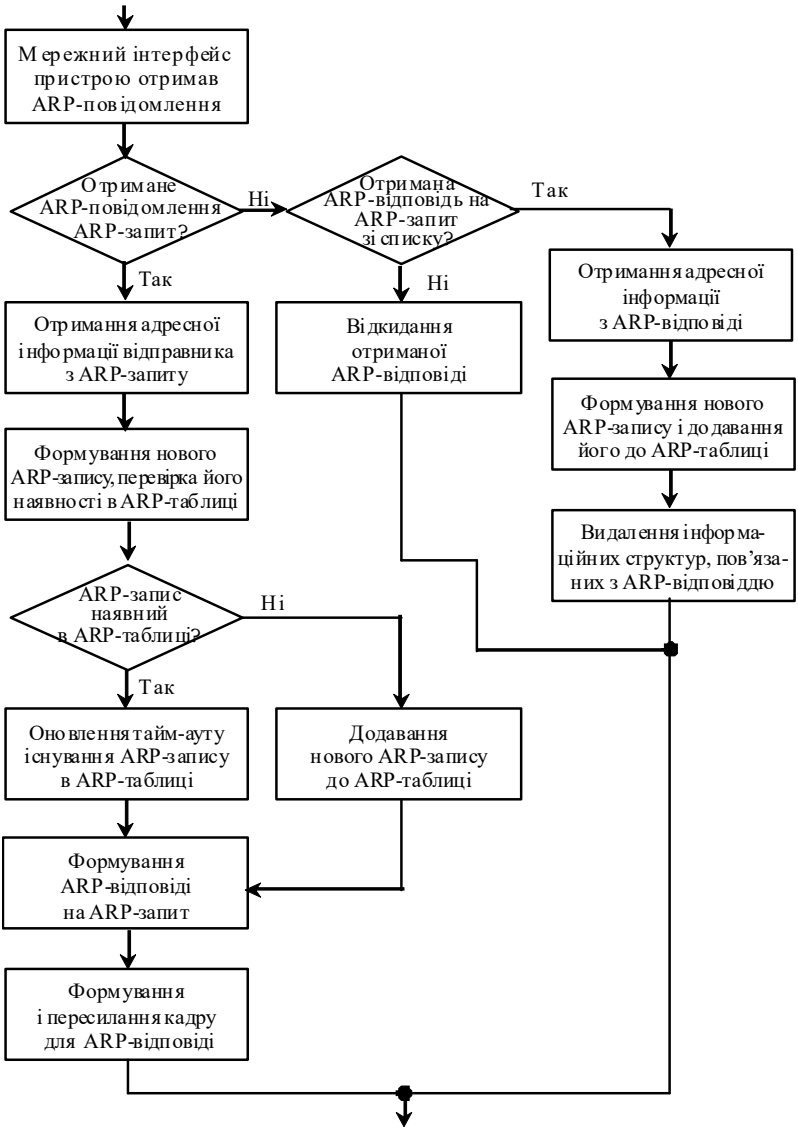


Рис. 5. Блок-схема алгоритму роботи протоколу ARP для випадку отримання ARP-повідомлення

Приклад 4.

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

Розв'язання.

ARP-запит формується за загальною структурою ARP-повідомлення. Оскільки вузол А належить мережі Ethernet, у якій застосовується протокол IP версії 4, то всі поля ARP-запиту формуються з урахуванням цих параметрів. Тобто, поле H-Type дорівнює 0001h, а поле P-Type – 0800h. Поля HA-Len та PA-Len відповідно дорівнюють 06h та 04h. Оскільки формується ARP-запит, то поле OP-Code дорівнює 0001h. Поля SHA та SPA формуються на основі MAC-адреси 00-60-5C-16-8B-30 і IP-адреси 195.10.1.1 відправника (вузла А) і відповідно дорівнюють 00605C168B30h та 3C0A0101h. В ARP-запиті поле THA за замовчуванням дорівнює 000000000000h, поле TPA формується на основі IP-адреси 195.10.1.3 отримувача (вузла В) і дорівнює C30A0103h.

Побудований ARP-запит має вигляд:

```
000108000604000100605C168B30
C30A0101000000000000C30A0103
```

ARP-відповідь також формується за загальною структурою ARP-повідомлення для мереж Ethernet із застосуванням протоколу IP версії 4. Тобто поле H-Type дорівнює 0001h, а поле P-Type – 0800h, поле HA-Len – 06h, поле PA-Len – 04h. Оскільки формується ARP-відповідь, то поле OP-Code дорівнює 0002h. Поля SHA та SPA формуються на основі MAC-адреси 00-10-11-49-ED-09 і IP-адреси 195.10.1.3 відправника (вузла В) і відповідно дорівнюють 00101149ED09h та C30A0103h. Поля THA та TPA формуються на основі MAC-адреси 00-60-5C-16-8B-30 і IP-адреси 195.10.1.1 отримувача (вузла А) і відповідно дорівнюють 00605C168B30h та C30A0101h.

Побудована ARP-відповідь має вигляд:

```
0001080006040002001011 49ED09
C30A010300605C168B303C0A0101
```

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

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

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

Результуючий Ethernet-кадр з інкапсульованим ARP-запитом має вигляд

```
FFFFFFFFFFFF00605C168B300806
0001080006040001006 05C168B30
C30A0101000000000000C30A0103
00000000000000000000000000000000000000
XXXXXXXX
```

Результуючий Ethernet-кадр з інкапсульованою ARP-відповіддю має вигляд

```
00605C168B3000101149ED090806
0001080006040002001011 49ED09
C30A010300605C168B30C30A0101
00000000000000000000000000000000000000
XXXXXXXX
```

Для побудованих Ethernet-кадрів контрольні суми (поле FCS) не розраховувалися, замість них записана умовна 4-байтова послідовність XXXXXXXX. У реальному житті контрольні суми розрахову-

ються для всіх полів кадру (крім FCS) за алгоритмом CRC-32 як у разі надсилання кадру в мережу, так і отримання кадру з мережі.

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

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

```
C:\>arp

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

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

```
      > arp -s 157.55.85.212       00-aa-00-62-c6-09  .. Добавляет статическую за-
пись.
      > arp -a                                    .. Выводит ARP-таблицу.
```

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

```
root@box:~# arp

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

Usage: arp

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

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

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

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

Usage:

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

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

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

root@debian8-3~: #
```

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

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

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

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

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

власний конфігураційний каталог /proc/sys/net/ipv4/neigh/if-name/ та власні конфігураційні файли, які надалі можна редагувати.

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

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

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

Таблиця 2

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

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

	з ARP-таблиці пристрою
clear arp ***interface_type interface_id***	Видалення ARP-записів з ARP-таблиці пристрою, які пов'язані із зазначеним інтерфейсом

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

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

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

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

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

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

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

Налагодження параметрів функціонування протоколу ARP на комунікаційних пристроях Cisco

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

Команди **arp arpa** та **arp snap** застосовуються для зазначення протоколу інкапсуляції у кадри канального рівня; **arp arpa** – звичайна інкапсуляція, **arp snap** – інкапсуляція із застосуванням заголовків кадрів SNAP. Команда **arp authorized** дозволяє застосовувати лише внутрішні авторизовані записи. Команда **arp frame-relay** активує застосування протоколу ARP для інтерфейсів технології Frame Relay. Команда **arp**

log threshold entries призначена для налагодження параметрів підсистеми журналювання, які стосуються протоколу ARP. За допомогою команди **arp probe interval** здійснюється налагодження механізму ARP-Probe. Команда **arp timeout** застосовується для встановлення тайм-ауту утримання ARP-записів в ARP-таблиці пристрою.

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

arp arpa.

Команда не має параметрів.

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

arp authorized.

Команда не має параметрів.

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

arp frame-relay.

Команда не має параметрів.

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

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

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

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

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

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

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

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

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

arp snap.

Команда не має параметрів.

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

arp timeout ***arp_timeout_value***,

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

Програмні розробки на базі протоколу ARP

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

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

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

```
BusyBox v1.19.0 (2011-08-14 21:05:38 UTC) multi-call binary.
Usage: arping [-fqbDUA] [-c CNT] [-w TIMEOUT] [-I IFACE] [-s SRC_IP] DST_IP
Send ARP requests/replies
        -f              Quit on first ARP reply
        -q              Quiet
        -b              Keep broadcasting, don't go unicast
```

```
-D              Duplicated address detection mode
-U              Unsolicited ARP mode, update your neighbors
-A              ARP answer mode, update your neighbors
-c N            Stop after sending N ARP requests
-w TIMEOUT      Time to wait for ARP reply, seconds
-I IFACE        Interface to use (default eth0)
-s SRC_IP       Sender IP address
DST_IP          Target IP address
```

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

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

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

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

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

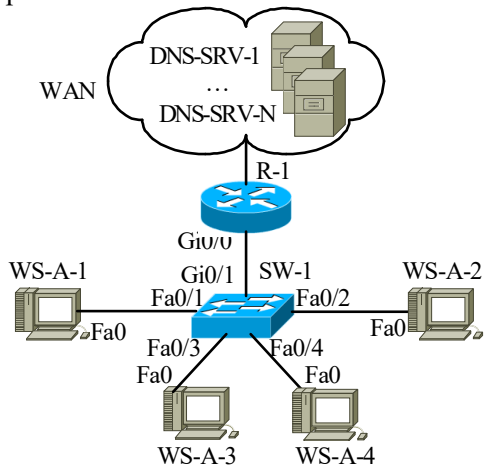


Рис. 11. Приклад мережі

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

Таблиця 3

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу

Маршрутизатор R-1	Gi0/1	WAN	WAN Interface
	Gi0/0	Комутатор SW-1	Gi0/1
Комутатор SW-1	Fa0/1	Робоча станція WS-A-1	Fa0
	Fa0/2	Робоча станція WS-A-2	Fa0
	Fa0/3	Робоча станція WS-A-3	Fa0
	Fa0/4	Робоча станція WS-A-4	Fa0
	Gi0/1	Маршрутизатор R-1	Gi0/0
WAN	WAN Interface	Маршрутизатор R-1	Gi0/1
Робоча станція WS-A-1	Fa0	Комутатор SW-1	Fa0/1
Робоча станція WS-A-2	Fa0		Fa0/2
Робоча станція WS-A-3	Fa0		Fa0/3
Робоча станція WS-A-4	Fa0		Fa0/4

Таблиця 4

Параметри адресації мережі для прикладу

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

	Альтернат. DNS-сервер 2	–	8.8.4.4	–	–

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

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

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

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

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

1. Через „Панель управления” запустити на виконання додаток „Сетевые подключения”.

2. Серед переліку наявних мережних підключень обрати необхідне підключення.

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

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

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

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

7. Активувати налагоджені параметри.

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

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

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

2. Серед переліку наявних мережних підключень обрати необхідне підключення.

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

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

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

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

7. Активувати налагоджені параметри.

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

…

root@debian8-3:~# hostname WS-A-3

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

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

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

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

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

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

23, а. Вміст ARP-відповіді робочої станції WS-A-2 на отриманий запит наведено на рис. 23, б.

```
C:\>ipconfig /all
Настройка протокола IP для Windows
        Имя компьтера . . . . . . . . . . : WS-A-1
        Основной DNS-суффикс  . . . . . . :
        Тип узла. . . . . . . . . . . . . : неизвестный
        IP-маршрутизация включена . . . . : нет
        WINS-прокси включен . . . . . . . : нет
Подключение по локальной сети – Ethernet адаптер:
        DNS-суффикс этого подключения . . :
        Описание  . . . . . . . . . . . . : AMD PCNET Family Ethernet Adapter
(PCI)
        Физический адрес. . . . . . . . . : 00-60-5C-16-8B-30
        DHCP включен. . . . . . . . . . . : да
        Автонастройка включена  . . . . . : да
        IP- адрес . . . . . . . . . . . . : 195.10.1.1
        Маска подсети . . . . . . . . . . : 255.255.255.0
        Основной шлюз . . . . . . . . . . : 195.10.1.254
        DNS-серверы . . . . . . . . . . . : 195.10.1.254
                                            8.8.8.8
                                            8.8.4.4
C:\>
```

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

```
C:\>ipconfig /all
Настройка протокола IP для Windows
        Имя компьтера . . . . . . . . . . : WS-A-2
        Основной DNS-суффикс  . . . . . . :
        Тип узла. . . . . . . . . . . . . : Гибридный
        IP-маршрутизация включена . . . . : Нет
        WINS-прокси включен . . . . . . . : Нет
Ethernet адаптер Подключение по локальной сети:
        DNS-суффикс подключения . . . . . :
        Описание  . . . . . . . . . . . . : AMD PCNET Family Ethernet Adapter
(PCI)
        Физический адрес. . . . . . . . . : 00-10-43-2C-BD-BB
        DHCP включен. . . . . . . . . . . : Нет
        Автонастройка включена  . . . . . : Да
        IPv4-адрес. . . . . . . . . . . . : 195.10.1.2<Основной>
        Маска подсети . . . . . . . . . . : 255.255.255.0
        Основной шлюз . . . . . . . . . . : 195.10.1.254
        DNS-серверы . . . . . . . . . . . : 195.10.1.254
                                            8.8.8.8
                                            8.8.4.4
        NetBIOS через TCP/IP              : включен
...
C:\>
```

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

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

```
          RX bytes:26368 (25.7 KiB)  TX bytes:4014 (3.9KiB)
root@debian8-3:~#
```

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

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

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

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

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

```
R-1#show interfaces GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is i82543 (Livengood), address is ca01.07fe.0008 (bia
ca01.07fe.0008)
  Description: LAN-A(LINK_TO_SW-1)
  Internet address is 195.10.1.254/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, link type is autonegotiation, media type is SX
  output flow-control is XON, input flow-control is XON
```

```
  ARP type: ARPA, ARP Timeout 00:10:00
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     35 packets input, 4611 bytes, 0 no buffer
     Received 38 broadcasts, 0 runts, 0 giants, 0 throttles
...
```

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

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

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

```
C:\>arp -a
Интерфейс: 195.10.1.1 --- 0x2
  Адрес IP             Физический адрес      Тип
  195.10.1.2           00-10-43-2c-bd-bb     динамический
  195.10.1.3           00-10-11-49-ed-09     динамический
  195.10.1.4           00-00-27-32-f9-e7     динамический
  195.10.1.252         00-d0-b1-e1-14-11     динамический
  195.10.1.254         ca-01-07-fe-00-08     динамический
C:\>
```

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

```
C:\>arp -a
Интерфейс: 195.10.1.2 --- 0xb
  адрес в Интернете      Физический адрес      Тип
  195.10.1.1           00-60-5c-16-8b-30     динамический
  195.10.1.3           00-10-11-49-ed-09     динамический
  195.10.1.4           00-00-27-32-f9-e7     динамический
  195.10.1.252         00-d0-b1-e1-14-11     динамический
  195.10.1.254         ca-01-07-fe-00-08     динамический
  195.10.1.255         ff-ff-ff-ff-ff-ff     статический
  224.0.0.22           01-00-5e-00-00-16     статический
  224.0.0.252          01-00-5e-00-00-fc     статический
  255.255.255.255      ff-ff-ff-ff-ff-ff     статический
C:\>
```

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

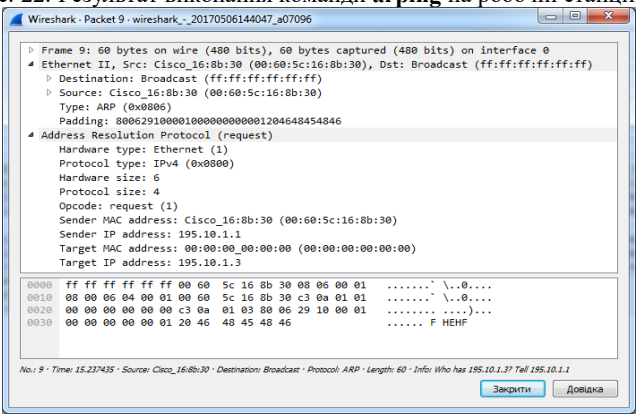
```
root@debian8-3:~# arp -a
? (195.10.1.252)  at  00:d0:b1:e1:14:11  [ether]  on eth0
? (195.10.1.1)  at  00:60:5c:16:8b:30  [ether]  on eth0
? (195.10.1.2)  at  00:10:43:2c:bd:bb  [ether]  on eth0
? (195.10.1.3)  at  00:10:11:49:ed:09  [ether]  on eth0
? (195.10.1.4)  at  00:00:27:32:f9:e7  [ether]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

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

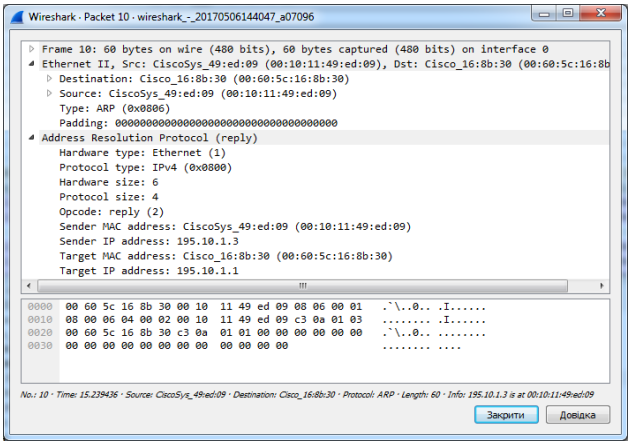
Рис. 21. Результат виконання команди **arp -a** на робочій станції WS-A-3

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

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



а



б

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

Завдання на лабораторну роботу

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

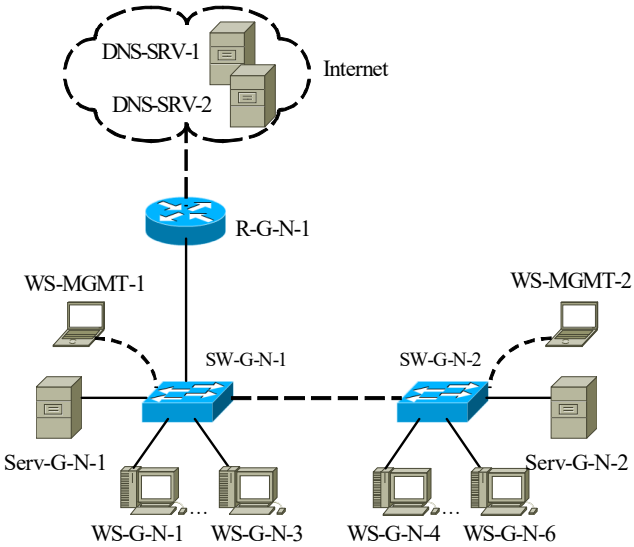


Рис. 24. Проект мережі

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

Таблиця 5

Параметри для розрахунку п. 2

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

28	218.G.N.0	/26	Остання IP-адреса діапазону
29	219.G.N.0	/27	Перша IP-адреса діапазону
30	220.G.N.0	/28	Остання IP-адреса діапазону
31	221.G.N.0	/24	Перша IP-адреса діапазону
32	222.G.N.0	/25	Остання IP-адреса діапазону
33	223.G.N.0	/26	Перша IP-адреса діапазону

Таблиця 6

Дані для визначення параметрів адресації мережі

№ варіанта	IP-адреса альтернативного DNS-сервера 1	IP-адреса альтернативного DNS-сервера 2
1	Level3 Communications	Level3 Communications
2	Google	Google
3	OpenDNS Home	OpenDNS Home
4	Securly	Securly
5	Comodo Secure DNS	Comodo Secure DNS
6	DNS Advantage	DNS Advantage
7	Norton ConnectSafe	Norton ConnectSafe
8	SafeDNS	SafeDNS
9	OpenNIC	OpenNIC
10	Public-Root	Public-Root
11	Level3 Com-ns	Level3 Com-ns
12	Google	Google
13	OpenDNS Home	OpenDNS Home
14	Securly	Securly
15	Comodo Secure DNS	Comodo Secure DNS
16	DNS Advantage	DNS Advantage
17	Norton ConnectSafe	Norton ConnectSafe
18	SafeDNS	SafeDNS
19	OpenNIC	OpenNIC
20	Public-Root	Public-Root
21	Level3 Com-ns	Level3 Com-ns
22	Google	Google
23	OpenDNS Home	OpenDNS Home
24	Securly	Securly
25	Comodo Secure DNS	Comodo Secure DNS

26	DNS Advantage	DNS Advantage
27	Norton ConnectSafe	Norton ConnectSafe
28	SafeDNS	SafeDNS
29	OpenNIC	OpenNIC
30	Public-Root	Public-Root
31	AdGuard DNS	AdGuard DNS
32	Fourth Estate	Fourth Estate
33	CenturyLink (Level3)	CenturyLink (Level3)

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

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

Таблиця 8

Параметри для виконання п. 3

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

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

Таблиця 9

Параметри для виконання п. 5

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

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

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

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

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

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

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

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

Таблиця 10

Параметри для розрахунку п. 12

№ варіанта	IP-адреса	№ варіанта	IP-адреса

1	224.0.0.1	18	224.0.0.11
2	224.0.0.2	19	224.35.0.85
3	224.20.75.25	20	224.0.0.12
4	224.0.0.4	21	224.0.0.13
5	224.40.115.45	22	224.0.0.18
6	224.0.0.5	23	224.75.20.135
7	224.60.155.85	24	224.0.0.22
8	224.0.0.6	25	224.95.40.155
9	224.80.195.125	26	224.0.0.102
10	224.0.0.7	27	224.215.60.165
11	224.100.0.5	28	224.0.0.251
12	224.0.0.8	29	224.235.80.185
13	224.0.0.107	30	224.0.1.1
14	224.0.0.9	31	224.0.0.4
15	224.140.0.45	32	224.0.0.6
16	224.0.0.10	33	224.0.0.9
17	224.15.0.65	34	224.0.0.102

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

Таблиця 11

Параметри для розрахунку п. 13

№ варіанта	MAC-адреса	№ варіанта	MAC-адреса
1	01-00-5E-00-AF-B1	18	01-00-5E-12-CA-B6
2	01-00-5E-01-AE-B3	19	01-00-5E-13-DF-B8
3	01-00-5E-02-AD-B7	20	01-00-5E-14-DE-BA
4	01-00-5E-03-AC-B9	21	01-00-5E-15-DD-BC
5	01-00-5E-04-AB-BB	22	01-00-5E-16-DC-BE
6	01-00-5E-05-AA-BE	23	01-00-5E-17-DB-A2
7	01-00-5E-06-BF-BF	24	01-00-5E-18-DA-A4
8	01-00-5E-07-BE-A1	25	01-00-5E-19-EF-A6
9	01-00-5E-08-BD-A3	26	01-00-5E-1A-EE-A8
10	01-00-5E-09-BC-A5	27	01-00-5E-1B-ED-AA
11	01-00-5E-0A-BB-A7	28	01-00-5E-1C-EC-AC
12	01-00-5E-0B-BA-A9	29	01-00-5E-1D-EB-AF
13	01-00-5E-0C-CF-AB	30	01-00-5E-1E-EA-FF
14	01-00-5E-0D-CE-AE	31	01-00-5E-1E-E0-FD
15	01-00-5E-0E-CD-AF	32	01-00-5E-1E-3F-23
16	01-00-5E-10-CC-B2	33	01-00-5E-1E-0A-F1
17	01-00-5E-11-CB-B4	34	01-00-5E-1E-AA-F2

Контрольні питання

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

Лабораторна робота № 5
ОСНОВИ РОБОТИ З МАРШРУТИЗАТОРАМИ CISCO ТА МЕРЕЖЕВОЮ ОПЕРАЦІЙНОЮ СИСТЕМОЮ CISCO IOS

Мета заняття: ознайомитися з загальною будовою маршрутизатора Cisco; ознайомитися з основними можливостями мережної операційної системи Cisco IOS для маршрутизаторів та розглянути особливості її застосування на маршрутизаторах Cisco; дослідити можливості Cisco IOS з налагодження та діагностування основних параметрів функціонування маршрутизаторів Cisco.

Теоретичні відомості

Будова маршрутизатора Cisco

Спеціалізовані пристрої, відомі як IMP (Interface Message Processors), що функціонально були подібними до сучасних маршрутизаторів, з'явилися і набули застосування ще на перших етапах розвитку мережі ARPAnet. Пізніше, з появою стеку TCP/IP, IMP були замінені міні-комп'ютерами загального призначення, для яких розроблялися спеціальні програмні модулі з забезпечення підтримки маршрутизації. Перші прототипи спеціалізованих багатопротокольних маршрутизаторів були розроблені у 1981 році незалежно у Стенфордському університеті та Масачусетському технологічному інституті. І саме розробки програмного коду Стенфордського університету були ліцензовані і стали основою для побудови маршрутизаторів фірми Cisco, відомих як Cisco AGS Multi-Protocol Router (Cisco Advanced Gateway Server Multi-Protocol Router). Маршрутизатори Cisco AGS (1986 р.) та їх подальші модифікації Cisco AGS+, Cisco MGS стали першими світовими масовими комерційно успішними маршрутизаторами.

З дня заснування науковці та інженери Cisco займаються впровадженням інновацій у сфері мережних технологій, мережних операційних систем, спеціалізованого мережного програмного забезпечення. Фахівці Cisco постійно беруть участь у розробці нових технологій, протоколів, архітектурних і технологічних рішень. Велика кількість як відкритих стандартів (зокрема, стандартів IEEE та RFC), так і закритих стандартів була розроблена саме за їх участі. Сьогодні фірма Cisco залишається світовим лідером у розробці і ви-

робництві маршрутизаторів різного призначення – від домашніх маршрутизаторів до маршрутизаторів ядра мережі Інтернет.

Залежно від призначення маршрутизатори Cisco будуються за різними архітектурними схемами. Типова структурна схема маршрутизатора Cisco, орієнтованого на забезпечення підключення локальної мережі до глобальної через один або кілька каналів зв'язку наведена на рис. 1.

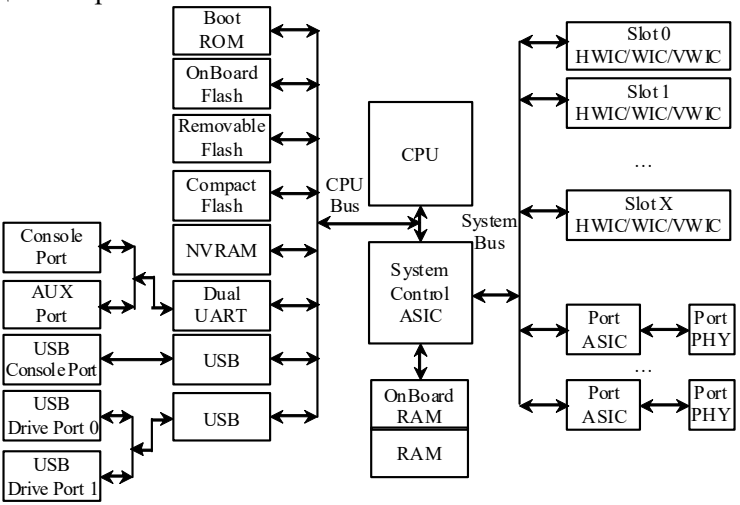


Рис. 1. Типова структурна схема маршрутизатора Cisco

Основними складовими маршрутизатора є:

– центральний процесор (CPU, Central Processing Unit);

– блок керування системою (System Control ASIC)

– блок постійної пам'яті (OnBoard Boot ROM, Read-Only Memory);

– блок постійної перезаписуваної пам'яті (OnBoard Flash);

– блок змінної перезаписуваної пам'яті (Removable Flash);

– блок енергонезалежної пам'яті (NVRAM, Non-Volatile Random Access Memory);

– блок оперативної пам'яті (RAM, OnBoard RAM, Random Access Memory типу DRAM, Dynamic RAM або SDRAM, Synchronous DRAM);

– блок керування послідовним інтерфейсом UART;

– блоки керування інтерфейсами USB;

– блоки керування вбудованими інтерфейсами/портами Ethernet/Fast Ethernet/Gigabit Ethernet, Wi-Fi тощо (Port ASICs);

– блоки фізичного рівня, трансивери Ethernet/Fast Ethernet/Gigabit Ethernet, Wi-Fi тощо (PHYs, Physical Layer Devices);

– блоки підключення змінних плат/модулів розширення (Slot X).

Основними функціями центрального процесора (CPU) маршрутизатора є: пересилання пакетів між інтерфейсами; визначення оптимальних маршрутів (підтримка функціонування протоколів маршрутизації, побудова та підтримка таблиць маршрутизації); керування та обслуговування маршрутизатора (забезпечення підтримки інтерфейсу командного рядка, забезпечення журналювання подій системи тощо). Координацію роботи складових маршрутизатора забезпечує блок керування системою (System Control ASIC). Фірма Cisco не орієнтована на використання процесорів та блоків керування системою одного виробника, а тісно співпрацює з більшістю провідних розробників і виробників. Серед них варто згадати Intel, Motorolla, IDT, Cavium. Для різних моделей маршрутизаторів Cisco, залежно від їх призначення, застосовуються центральні процесори різних архітектур. Це можуть бути CISC або RISC-процесори, процесори архітектур x86, PowerPC, MIPS, ARM тощо.

У перших моделях маршрутизаторів Cisco часто застосовувалися центральні процесори загального призначення. Наприклад, у маршрутизаторах моделі Cisco 2600 – процесор Motorola PowerPC860, у маршрутизаторах моделей Cisco 3600 та 7200 – процесор IDT MIPS R4700. У сучасних моделях маршрутизаторів, як правило, застосовуються спеціалізовані високопродуктивні захищені процесори, наприклад, у маршрутизаторах моделі Cisco 1941 – процесор Cavium Octeon Plus. Високопродуктивні магістральні маршрутизатори Cisco у своєму складі містять кілька процесорів або процесорних блоків: для ретрансляції пакетів застосовуються спеціальні інтерфейсні процесори, а для визначення маршрутів та обслуговування маршрутизатора – основний центральний процесор.

У постійній енергонезалежній пам’яті (OnBoard Boot ROM) маршрутизатора містяться процедура початкового самотестування пристрою POST (Power-On Self-Test) та програма початкового завантаження Bootstrap (Bootstrap Program). Також у цій пам’яті знахо-

диться дві спеціальні утиліти, які є обмеженими версіями мережної ОС Cisco IOS: утиліта ROMMON та утиліта mini-IOS. Завантаження пристрою у режимі ROMMON (ROM Monitor Mode) здійснюється для виконання різних діагностичних процедур та тестів, а також для відновлення адміністративного доступу до пристрою при втраті паролів. Завантаження Cisco mini-IOS (RXBOOT Mode) відбувається у тому випадку, коли маршрутизатор через технічний збій не може завантажити повний варіант Cisco IOS.

Блок постійної перезаписуваної пам'яті (OnBoard Flash) виконує функції накопичувача маршрутизатора. Він містить файл образу Cisco IOS та деякі конфігураційні файли, які створюються у процесі налагодження та використовуються у процесі роботи пристрою. Файлів образів у перезаписуваній пам'яті може міститися кілька. Можливості постійної перезаписуваної пам'яті можуть бути розширені за рахунок застосування блока змінної перезаписуваної пам'яті (Removable Flash). Блок енергонезалежної пам'яті (NVRAM) застосовується для збереження конфігурації маршрутизатора.

Блок оперативної пам'яті (RAM/OnBoard RAM) виконує функції, що аналогічні такому ж блоку звичайного комп'ютера. Оперативна пам'ять маршрутизатора логічно поділяється на дві частини: основну процесорну пам'ять (Main Processor Memory) та пам'ять вводу-виводу (Shared Input-Output Memory). В основну пам'ять завантажується Cisco IOS, у ній також розміщуються поточна конфігурація пристрою та різні таблиці (таблиці маршрутизації, ARP-таблиці, CDP-таблиці тощо). У пам'яті вводу-виводу містяться вхідні та вихідні буфери інтерфейсів, у яких розміщуються пакети, що маршрутизуються. У багатьох маршрутизаторах наявна можливість нарощення об'єму вбудованої оперативної пам'яті (OnBoard RAM) за рахунок додавання нових модулів.

Взаємозв'язок блоків пам'яті маршрутизатора Cisco наведено на рис. 2.

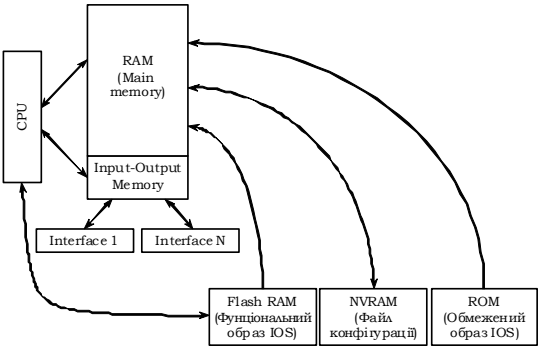


Рис. 2. Організація пам'яті у маршрутизаторах Cisco

Конфігураційний регістр маршрутизатора Cisco

В енергонезалежній пам'яті пристрою Cisco виділена окрема ділянка (2 байти), яка носить назву конфігураційний регістр (Configuration Register). За його допомогою пристрій визначає, які параметри повинні використовуватися для початкового завантаження. Конфігураційний регістр є аналогом CMOS для BIOS в ПК. Вміст конфігураційного регістра відображається у вигляді чотирьох шістнадцяткових цифр. За замовчуванням конфігураційний регістр маршрутизатора Cisco містить значення 0x2102 (комутатора Cisco – значення 0xF). Нумерація розрядів конфігураційного регістра та його бітові значення за замовчуванням наведені у табл. 1

Таблиця 1

Нумерація розрядів конфігураційного регістра

Номер розряду	15 14 13 12	11 10 9 8	7 6 5 4	3 2 1 0
Двійковий код (за замовчуванням)	0 0 1 0	0 0 0 1	0 0 0 0	0 0 1 0
Шістнадцятковий код (за замовчуванням)	**2**	**1**	**0**	**2**

Змінюючи значення конфігураційного регістра можна змінити спосіб запуску і джерела завантаження маршрутизатора, зокрема:

– встановити завантаження системи у режимі ROMMON;

– зазначити джерело завантаження і назву завантажувального файлу за замовчуванням;

– дозволити або заборонити можливість переривання процесу завантаження;

– керувати адресою широкомовної розсилки;

– встановити швидкість обміну для консольного підключення;

– завантажити ПЗ з ROM;

– дозволити заватаження Cisco IOS з TFTP-сервера.

Групування бітів конфігураційного регістру та особливості їх використання наведені у табл 2.

Таблиця 2

Групування бітів конфігураційного регістру та їх використання

Біти	Діапазон	Призначення
00-03	0x0000-0x000F	Ознаки встановлення способу завантаження Cisco IOS: 000 – виконати початкове завантаження у режимі ROMMON; 001 – завантаження з Boot Helper Image; 010 – завантажити перший образ Cisco IOS (як системний образ) з флеш-пам'яті; решта значень – наступні образи Cisco IOS з флеш-пам'яті
4		Зарезервований

Продовження таблиці 2

5	0x0020	Ознака визначення швидкості передачі консольного підключення (пов'язаний з бітами 11 та 12). За замовчуванням дорівнює 0 .
6	0x0040	Ознака використання конфігураційного файлу. Якщо цей біт дорівнює 1, то при перезавантаженні пристрою це є ознакою того, що необхідно ігнорувати конфігураційний файл в NVRAM (вважати, що маршрутизатор не є налагодженим). За замовчуванням біт дорівнює 0.
7	0x0080	Ознака включення/відключення виведення повідомлень Bootstrap при завантаженні пристрою.
8	0x0100	Ознака переривання процесу завантаження Cisco IOS і переходу в режим ROMMON. За замовчування біт дорівнює 1. Це означає, що сигнал переривання Break працює тільки перші 60 с процесу завантаження Cisco IOS. Якщо біт дорівнює 0, це означає, що подача сигналу Break викличе перехід у режим ROMMON у будь-який момент роботи системи.
9	0x0200	Ознака використання вторинного bootstrap. За замовчуванням біт дорівнює 0 і не використовується.
10	0x0400	Ознака керування октетом, який відповідає за вузли в широкомовній IP-адресі. Якщо біт дорівнює 1, це означає, що в октеті вузла будуть використовуватися нулі. Біт пов'язаний з бітом 14.
11-12	0x0800 0x1000 0x1800	Ознаки визначення швидкості передачі консольного підключення (пов'язані з бітом 5). За замовчуванням обидва біти дорівнюють 0 – встановлена швидкість 9600 біт/с.
13	0x2000	Ознака завантаження після збоїв (Load Rom After Netboot Fails). Служить встановлення кількості спроб виконання команди Boot System. Якщо біт дорівнює 1, то маршрутизатор один раз здійснює спробу завантажитися по команді Boot System. Якщо спроба невдала – відразу ж переходить до наступної такої команди. Якщо біт дорівнює 0, то маршрутизатор намагається виконати команду Boot System п'ять разів (через 2, 4, 16, 256, 300) і лише після п'ятої спроби переходить до наступної

		команди. За замовчуванням біт дорівнює 1.
14	0x4000 0x1000 0x1800	Ознака керування октетом, який відповідає за мережу і підмережу в широкомовній IP-адресі. За замовчуванням дорівнює 0.
15	0x8000 0x1000 0x1800	Ознака включення виведення діагностичних повідомлень і ігнорування вмісту NVRAM. За замовчуванням дорівнює 0.

Комбінації бітів, які відповідають за швидкість консольного підключення наведені у табл. 3.

Таблиця 3

Комбінації бітів встановлення швидкості консольного підключення

Швидкість, біт/с	Біт 5	Біт 11	Біт 12
115200	1	1	1
57600	1	0	1
38400	1	1	0
19200	1	0	0
9600	0	0	0
4800	0	1	0
2400	0	1	1
1200	0	0	1

Комбінації бітів, які відповідають за управління широкомовною розсилкою наведені у табл. 4.

Таблиця 4

Комбінації бітів управління широкомовною розсилкою

Біт 14	Біт 10	Address (<Мережа ><Вузол>)
0	0	<Одиниці><Одиниці>
0	1	<Нулі>< Одиниці >
1	1	<Мережа><Нулі>
1	0	< Мережа >< Одиниці >

Існують програмні рішення, які полегшують формування значення конфігураційного регістра за рахунок візуалізації процесу та його результатів. Серед них варто відмітити програму Config

Register Calculator, розроблений фірмою Boson Software (www.boson.com). Інтерфейс даного продукту наведений на рис. 3.

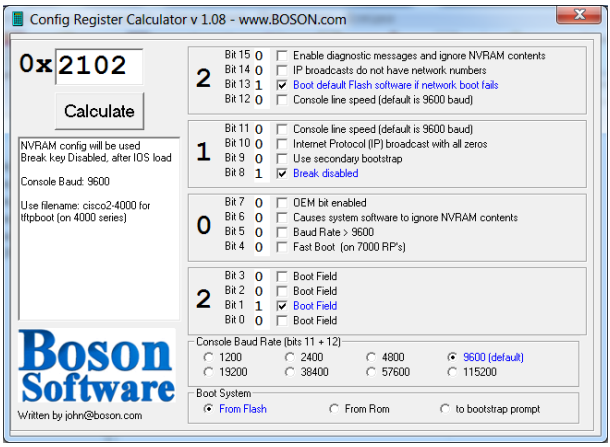


Рис. 3. Інтерфейс додатку Config Register Calculator

Для забезпечення налагодження та керування комутатором наявні блоки керування інтерфейсами/портами для підключення робочих станцій керування, що підтримують застосування різних фізичних інтерфейсів: послідовного інтерфейсу, інтерфейсу USB. Для забезпечення функціонування послідовних інтерфейсів (основного – Console Port, допоміжного – AUX Port, Auxiliary Port) застосовується блок, що базується на мікросхемі UART. Для забезпечення функціонування інтерфейсу USB (USB Console Port) – відповідний блок USB. У деяких моделях маршрутизаторів для підключення робочих станцій керування передбачено спеціальний мережний інтерфейс керування (MGMT Interface, Out-of-Band Ethernet Management Interface) – блок, який аналогічний за функціями блоку керування портом Ethernet/Fast Ethernet/Gigabit Ethernet. У певних моделях комутаторів блок інтерфейсу USB також підтримує можливість підключення зовнішніх змінних USB-носіїв або пристроїв.

Підключення маршрутизатора до мережі здійснюється з використанням різних мережних технологій. Типово застосовуються канали всіх варіантів технологій Ethernet та Wi-Fi, послідовні (Serial) виділені канали зв'язку, канали стандартів 3G/4G, рідше – послідовні комутовані канали, канали технологій ATM, POS тощо. Інтер-

фейсні блоки, що забезпечують різні мережі підключення, можуть бути і вбудованими (у більшості сучасних маршрутизаторів Cisco це інтерфейсні блоки технологій FastEthernet/Gigabit Ethernet), і додатковими. Додаткові блоки реалізують як змінні плати та модулі розширення відповідних технологій.

Фірмою Cisco розроблено велику кількість моделей маршрутизаторів, які відрізняються своїм функціоналом та можливостями. Частина розроблених моделей орієнтовані на забезпечення доступу до мережі Інтернет невеликих локальних мереж з відносно інтенсивним інформаційним обміном – домашніх мереж або мереж малих офісів. Такі маршрутизатори часто називають домашніми маршрутизаторами/маршрутизаторами малих офісів (SOHO Routers, Small Office Home Office Routers). Сучасні моделі SOHO Routers мають вбудовані інтерфейси та інтерфейсні блоки. Як правило, це: WAN Interface – один інтерфейс технології Fast Ethetnet/Gigabit Ethetnet для підключення до глобальної мережі, LAN Interfaces – інтерфейсний блок комутатора Fast Ethetnet/Gigabit Ethetnet, WLAN Interface – інтерфейсний блок технології Wi-Fi. У деяких моделях наявні інтерфейсні блоки послідовних (Serial) каналів зв'язку, блоки технологій 3G/4G LTE. Прикладами таких маршрутизаторів є сучасні маршрутизатори Cisco серії 800, зокрема моделі 819, 829.

Для підключення до глобальної мережі великих локальних мереж, кампусних мереж тощо застосовуються спеціалізовані маршрутизатори Cisco. Як правило, такі маршрутизатори мають більшу номенклатуру підтримуваних технологій, інтерфейсів, протоколів. Прикладами таких маршрутизаторів є сучасні маршрутизатори Cisco серій 1900, 2600, 2900, 3900, 4000 тощо. Побудова високошвидкісних каналів зв'язку у глобальних мережах передбачає застосування глибоко спеціалізованих маршрутизаторів. Серед них варто згадати маршрутизатори Cisco серій 7200, 7600, 12000, CRS-1, CRS-3 тощо.

Зовнішній вигляд передньої та задньої панелей маршрутизатора серії 1900 наведений на рис. 4, а, б.

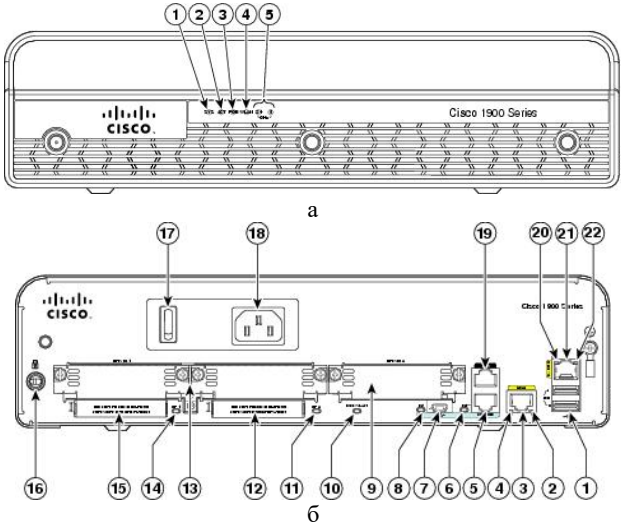


Рис. 4. Маршрутизатор Cisco серії 1900: а – передня панель; б – задня панель

Типово на передній панелі маршутизатора розміщуються світлодіодні індикатори (LEDs), які відображають стан пристрою в цілому та стан деяких його підсистем. Кількість індикаторів залежить від моделі маршрутизатора. На задній панелі маршрутизатора розміщуються вимикач живлення, вбудовані інтерфейси технологій Fast Ethernet/Gigabit Ethernet, гнізда для встановлення модулів та плат розширення, консольний порт/порти (Console Ports), допоміжний порт (Auxiliary Port), спеціалізований порт Ethernet мережного керування (MGMT Out-of-Band Ethernet Management Interface), інтерфейс(и) USB для підключення зовнішніх носіїв, гнізда для встановлення додаткових карт пам'яті та інших додаткових блоків. Більшість із них також мають власні світлодіодні індикатори.

Загальні правила розуміння свічення індикаторів є такими. Якщо індикатор не світиться (Off) – це свідчить про відключення або непрацездатність пристрою в цілому, певного його блоку, підсистеми або каналу зв'язку. Якщо індикатор світиться зеленим кольором (Green) або мерехтить зеленим кольором (Blinking Green) – це свідчить про нормальний режим роботи, якщо ж індикатор світиться жовтим кольором (Amber) або мерехтить жовтим кольором (Blinking Amber) – це свідчить про те, що виникла певна проблема.

Позначення та короткий опис основних і додаткових світлодіодних індикаторів та світлодіодних індикаторів окремих інтерфейсів маршрутизатора Cisco наведені у табл. 5. Опис станів основних світлодіодних індикаторів та індикаторів інтерфейсів і портів керування маршрутизатора Cisco наведено у табл. 6.

Таблиця 5

Світлодіодні індикатори маршрутизатора Cisco

№	Позначення	Повна назва	Опис
Основні світлодіодні індикатори			
1	SYS PWR	System Power	Індикатор загального стану системи
2	ACT (SYS ACT)	System Activity	Індикатор активності процесів передачі або процесів моніторингу стану системи
3	EN	Enable	Індикатор(и) консольного порта RJ-45/USB
4	CF	Compact Flash	Індикатор функціонування карти пам'яті
5	CF 0	Compact Flash 0	Індикатор функціонування карти пам'яті 0
6	CF 1	Compact Flash 1	Індикатор функціонування карти пам'яті 1
Вбудовані інтерфейси Fast Ethernet (RJ-45)			
7	FDX	Full Duplex	Індикатор режиму передачі інтерфейсу
8	100	100	Індикатор швидкості передачі інтерфейсу
9	Link	Link	Індикатор активності каналу зв'язку
Вбудовані інтерфейси Gigabit Ethernet (RJ-45)			
10	S	Speed	Індикатор швидкості передачі інтерфейсу
11	L	Link	Індикатор активності каналу зв'язку
Додаткові світлодіодні індикатори			
12	PoE	Power over Ethernet	Індикатор живлення підключених вузлів через з'єднання Ethernet.
13	WLAN x	Wireless LAN	Індикатор(и) функціонування безпровідної мережі

Таблиця 6

Стани основних світлодіодних індикаторів маршрутизатора Cisco

№	Свічення індикатора	Опис
Системний індикатор SYS PWR		
1	Off	Живлення маршрутизатора не ввімкнено або системна плата пристрою несправна
2	Amber	Живлення пристрою ввімкнене, але виникла помилка системи
3	Blinking Amber	Операційна система Cisco IOS пристрою завантажується або пристрій знаходиться у спеціальному режимі ROMMON
4	Green	Живлення ввімкнене, операційна система Cisco IOS завантажилася і пристрій функціонує коректно
Системний індикатор SYS ACT		
1	Green	Індикація активності процесів передачі повідомлень або процесів моніторингу стану системи
2	Blinking Green	
Індикатор швидкості передачі інтерфейсу Fast Ethernet 100		

1	Off	Інтерфейс функціонує на швидкості 10 Мбіт/с
2	Green	Інтерфейс функціонує на швидкості 100 Мбіт/с
Індикатор режиму передачі інтерфейсу Fast Ethernet FDX		
1	Off	Інтерфейс функціонує у напівдуплексному режимі передачі
2	Green	Інтерфейс функціонує у дуплексному режимі передачі
Індикатор активності каналу зв'язку Fast Ethernet		
1	Off	Канал зв'язку не активовано (підключено не той тип кабелю, інтерфейс вимкнено, встановлено некоректні параметри, проблеми з каналом зв'язку)
2	Green	Канал зв'язку не активовано (підключено коректний тип кабелю, інтерфейс активовано, встановлено коректні параметри)
Індикатор швидкості передачі інтерфейсу Gigabit Ethernet S (Speed)		
1	1 Blink + Pause	Інтерфейс функціонує на швидкості 10 Мбіт/с
2	2 Blink + Pause	Інтерфейс функціонує на швидкості 100 Мбіт/с
3	3 Blink + Pause	Інтерфейс функціонує на швидкості 1000 Мбіт/с
Індикатор активності каналу зв'язку Gigabit Ethernet L (Link)		
1	Off	Канал зв'язку не активовано (підключено не той тип кабелю, інтерфейс вимкнено, встановлено некоректні параметри, проблеми з каналом зв'язку)
2	Green	Канал зв'язку активовано (підключено коректний тип кабелю, інтерфейс активовано, встановлено коректні параметри)
Індикатори консольних портів EN		
1	Off	Консольний кабель не підключено або функціонує некоректно
2	Green	Консольний кабель підключено, порт функціонує коректно
Індикатор функціонування карти пам'яті CF		
1	Green	Карта пам'яті використовується у процесі роботи (вилучення заборонене)
2	Amber	Карта пам'яті активована з помилкою
3	Blinking Green (Then Turn Off)	Карта пам'яті готова до вилучення

Інтерфейси маршрутизаторів Cisco

Маршрутизатори Cisco забезпечують можливість організації з'єднань з використанням різних мережних стандартів, технологій та протоколів. Найбільш поширеним є застосування з'єднань на базі технологій стандарту Ethernet (стандарт ISO/IEC/IEEE 8802-3:2014 „Standard for Ethernet"), послідовних (Serial) каналів зв'язку (стандарти ITU-T Recommendation V.35 „Data transmission at 48 kbit/s using 60-108 kHz group band circuits", ANSI/EIA/TIA-530 „High Speed 25-position Interface For Data Terminal Equipment And Data Circuit-terminating Equipment, Including Alternative 26-position Connector" тощо), каналів технологій PDH/SDH/SONET (стандарт ITU-T Recommendation G.709 „Interfaces for the Optical Transport Network (OTN) " та ін.) тощо.

Найпоширенішим варіантом організації з'єднань між маршрутизаторами є застосування з'єднань стандарту Ethernet на основі витої пари та волоконно-оптичного кабелю. Для підключень на основі витої пари типово забезпечуються швидкості 100 Мбіт/с та 1 Гбіт/с. Підключення на швидкості 10 Гбіт/с для витої пари зустрічаються досить рідко. Для підключення сучасних безпровідних точок доступу розроблені підключення на швидкості 2,5 Гбіт/с та 5 Гбіт/с. Для підключень на основі волоконно-оптичного кабелю типово забезпечуються швидкості 1 Гбіт/с, 10 Гбіт/с, 40 Гбіт/с та 100 Гбіт/с. Підключення на швидкості 10 Мбіт/с є застарілими і нині зустрічаються досить рідко. Наявні розробки підключень зі швидкістю 400 Гбіт/с. Ведуться розробки підключень на швидкостях 1 Тбіт/с і вище. Підключення за допомогою витої пари частіше застосовується для підключення до маршрутизаторів локальних мереж. Підключення до кампусних, регіональних, глобальних мереж типово здійснюється за допомогою волоконно-оптичного кабелю.

Для підключення пристроїв за допомогою витої пари майже у кожному маршрутизаторі Cisco наявні фіксовані інтерфейси RJ-45 технологій 100Base-TX/1000-Base-T. Інтерфейс RJ-45 маршрутизатора типово є інтерфейсом виду MDI. Тому при підключенні мережного пристрою (комутатора, маршрутизатора, комп'ютера) до такого інтерфейсу потрібно визначати вид інтерфейсу пристрою та обирати правильний тип Ethernet-кабелю (прямий чи перехресний). У деяких старих моделях маршрутизаторів можливе виставлення режимів MDI/MDIX перемикачами. Інтерфейси RJ-45 більшості сучасних маршрутизаторів підтримують функцію Auto-MDI.

У деяких старих моделях маршрутизаторів Cisco реалізуються фіксовані інтерфейси оптичних варіантів технологій Ethernet. Найчастіше застосовуються розніми SC, ST, FC, LC. У більшості сучасних маршрутизаторів Cisco застосовуються інтерфейсні слоти для змінних мережних інтерфейсних модулів (трансиверів), які дають змогу здійснювати підключення пристроїв різних технологій Ethernet. Як правило, у сучасних маршрутизаторах застосовуються модулі SPF, SFP+, XFP, CFP, QSFP, QSFP+.

Окрім інтерфейсів стандарту Ethernet у маршрутизаторах Cisco досить часто реалізуються послідовні (Serial) інтерфейси, які можуть підтримувати різні стандарти передачі даних та різні мережні технології. Послідовні інтерфейси забезпечують підключення маршрутизатора до мережевого пристрою провайдера послуг (маршрутизатора чи спеціалізованого комутатора глобальної мережі). Також часто використовуються пряме двоточкове з'єднання маршрутизаторів між собою. Такий варіант може реалізуватися за допомогою пристроїв CSU/DSU (56к, T1/E1 і т.д.) – рис. 5, а або за допомогою спеціальних нуль-модемних кабелів – рис. 5, б.

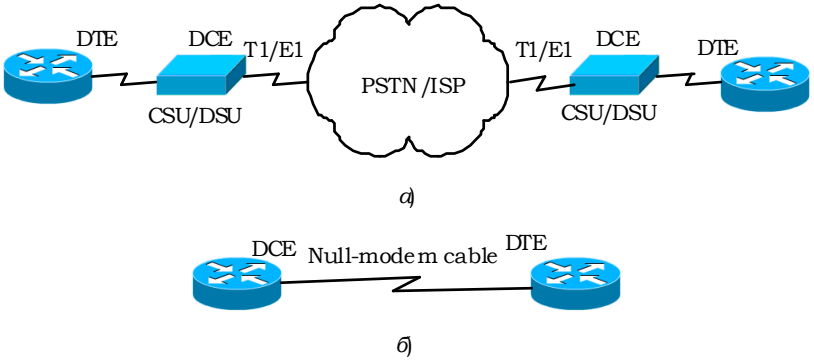
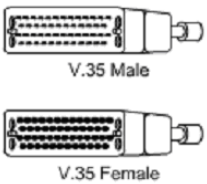


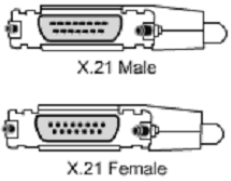
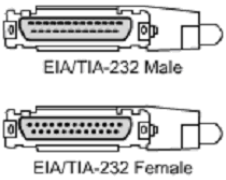
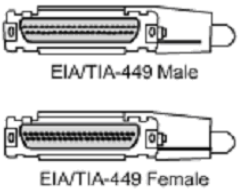
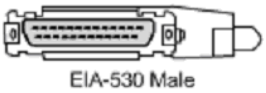
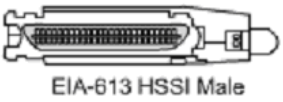
Рис. 5. Підключення за допомогою послідовних інтерфейсів

Перелік стандартів та рознімів, що застосовуються для побудови послідовних каналів зв'язку наведено у табл. 7. Для вибору необхідного типу з'єднувального кабелю для підключення за допомогою пристрою CSU/DSU або за допомогою нуль-модемного кабелю рекомендується скористатися документацією на пристрої та кабелі.

Таблиця 7

Стандарти та розніми послідовних інтерфейсів

Назва рознімy	**Стандарт**	**Зображення рознімy**
34-pin Rectangular Connector	V.35 (ITU-T V.35)	 V.35 Male V.35 Female

15-pin D-Connector	X.21bis	
25-pin D-connector	EIA/TIA-232 (RS-232, ITU-T V.24)	
37-pin D-Connector	EIA/TIA-449 (RS-449)	
25-pin D-Connector	EIA/TIA-530, EIA/TIA-530A, (RS-422&RS-423)	
50-pin D-Connector	EIA/TIA-612/613 (HSSI, High-Speed Serial Interface)	

Маршрутизатори Cisco залежно від моделі реалізуються монолітно (з певною кількістю інтерфейсів) або модульно. В останньому випадку передбачається встановлення модулів та плат розширення, які містять певну кількість інтерфейсів тієї чи іншої мережної технології. Загальне позначення модулів і плат розширення маршрутизаторів Cisco наведено у табл. 8.

Таблиця 8

Позначення модулів і плат розширення для маршрутизаторів Cisco

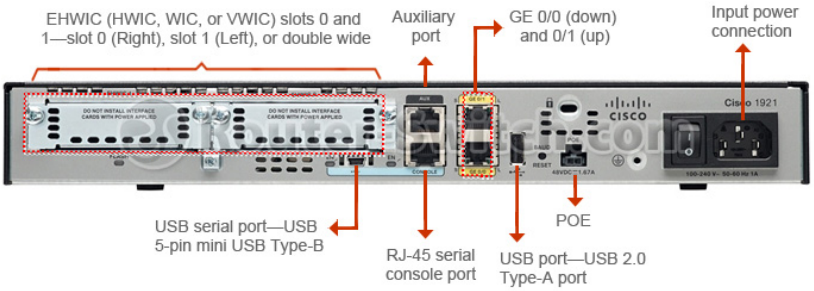
Позначення	Розшифровка
Інтерфейсні модулі	
NM, NME	Network Module, single-wide Network Module
NME-X	eXtended single-wide Network Module
NMD	Double-wide Network Module

NME-XD	eXtended Double-wide Network Module
SM	Service Module
SPE	Services Performance Engine
PVDM	Packet Voice Data Module
ISM	Internal Services Module
AIM	Advanced Integration Module
Інтерфейсні плати	
WIC	WAN Interface Card
VIC	Voice Interface Card
HWIC	High-Speed WIC
VWIC	Voice WIC
EHWIC	Enchanced High-Speed WIC
DW-HWIC	Double-Wide HWIC
DW-EHWIC	Double-Wide EHWIC

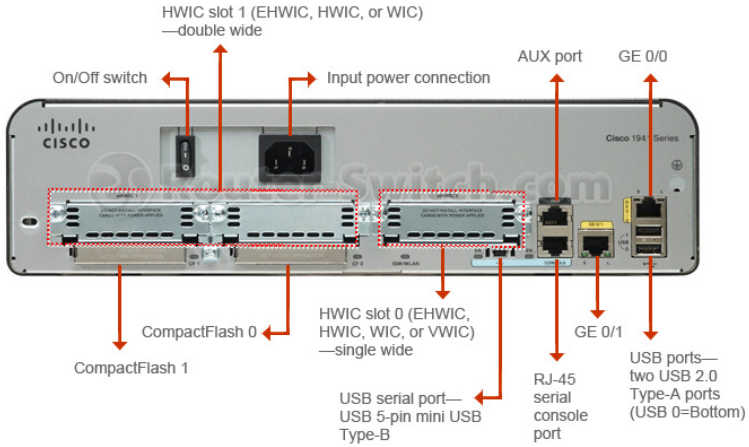
Нумерація інтерфейсів маршрутизатора проводиться починаючи з нуля. Наприклад Ethernet 0, Ethernet 1, …; Serial 0, Serial 1, …; FastEthernet 0, FastEthernet 1, … У разі використання модулів та/або плат розширення вказуються номери модулів та/або номери плат. Наприклад, Ethernet 0/0, Fast Ethernet 0/1/1, Serial 0/0, Serial 0/1/0. Можна використовувати скорочення. Наприклад, e0; fa0/0; s0/1/0 і т.д.

Зовнішній вигляд панелей маршрутизаторів Cisco моделей 1841, 1921 та 1941 на яких розміщені інтерфейси та гнізда розширення для модулів та плат розширення наведено на рис. 6, а, б, в відповідно. Зовнішній вигляд різних плат розширення наведено на рис. 7.

а

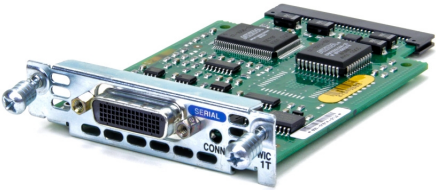


б



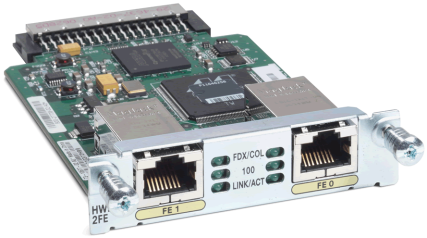
в

Рис. 6. Зовнішній вигляд панелей маршрутизаторів

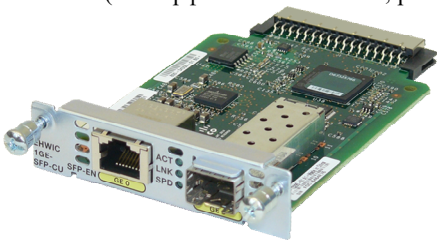


а) Cisco WIC-1T (послідовний інтерфейс, рознім V.35)

б) Cisco HWIC-1T1/E1 (послідовний інтерфейс, рознім RJ-48)



в) Cisco HWIC-2FE (2 інтерфейси Fast Ethernet, рознім RJ-45)



г) Cisco EHWIC-1GE-SFP-CU (1 інтерфейс Gigabit Ethernet, рознім RJ-45, 1 інтерфейс Gigabit Ethernet для змінного модуля SFP)

д) Cisco HWIC-4ESW (4 інтерфейси Fast Ethernet, рознім RJ-45)

Рис. 7. Зовнішній вигляд модулів і плат розширення

Операційні системи маршрутизаторів Cisco

Необхідно відмітити, що сучасний маршрутизатор – це цілісна сукупність апаратної платформи та спеціалізованої мережної операційної системи. У маршрутизаторах Cisco застосовуються такі мережні ОС як Cisco IOS, Cisco IOS XR, Cisco IOS XE. З точки зору внутрішньої архітектури ці ОС відрізняються між собою. З точки

зору налагодження та адміністрування вони мають багато спільних рис. Як правило, Cisco IOS XR та Cisco IOS XE застосовуються у високошвидкісних та високопродуктивних магістральних маршрутизаторах, Cisco IOS у простіших маршрутизаторах мереж розподілу та доступу.

Порядок завантаження маршрутизатора Cisco

Після включення живлення на маршрутизаторі Cisco виконується визначений набір дій, які забезпечують тестування функціонування складових пристрою і завантаження Cisco IOS. Цей набір також називають „завантажувальною послідовністю" (Boot Sequence). Ця послідовність містить 4 основних етапи (рис. 8, а). У деяких випадках етапи 3 та 4 розбивають на частини і тоді загальна кількість етапів зростає до шести (рис. 8, б).

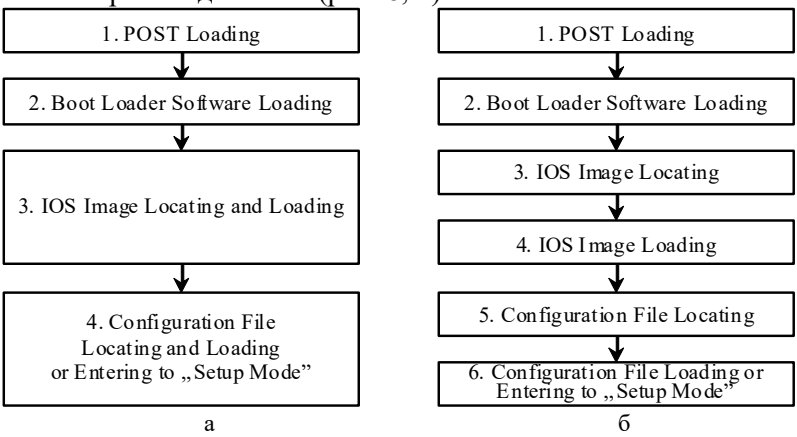


Рис. 8. Етапи завантаження маршрутизатора Cisco

На першому етапі здійснюється завантаження процедури початкового самотестування пристрою POST, що зберігається в постійній пам'яті маршрутизатора. Під час виконання цієї процедури здійснюється перевірка функціонування основних блоків та підсистем пристрою, яка включає тестування процесора, оперативної пам'яті, флеш-пам'яті, NVRAM. На другому етапі здійснюється завантаження з постійної пам'яті в оперативну пам'ять програми початкового завантаження Boot Loader. На цьому етапі здійснюється підготовка до визначення місця розташування образу Cisco IOS. На третьому етапі здійснюється визначення місця розташування образу

Cisco IOS та завантаження його в оперативну пам'ять. Якщо образ Cisco IOS не знайдено, то здійснюється завантаження обмеженого образу операційної системи – Cisco mini-IOS (перехід до режиму RXBOOT Mode). На четвертому етапі здійснюється визначення місця розташування файла конфігурації маршрутизатора та завантаження його оперативну пам'ять. Якщо ж файл конфігурації не знайдено, то здійснюється запуск процедури початкового конфігурування пристрою (перехід до режиму Setup Mode/System Configuration Dialog).

Блок-схема алгоритму завантаження маршрутизатора Cisco, у якій наведено різні варіанти завантаження образу Cisco IOS та файлу конфігурації наведена на рис. 9. Варіанти завантаження образу системи та конфігураційного файлу встановлюються за рахунок зміни значень конфігураційного регістра пристрою.

У випадку нормального завантаження маршрутизатора на екран термінальної програми виводиться повідомлення, подібне до наведеного на рис. 10.

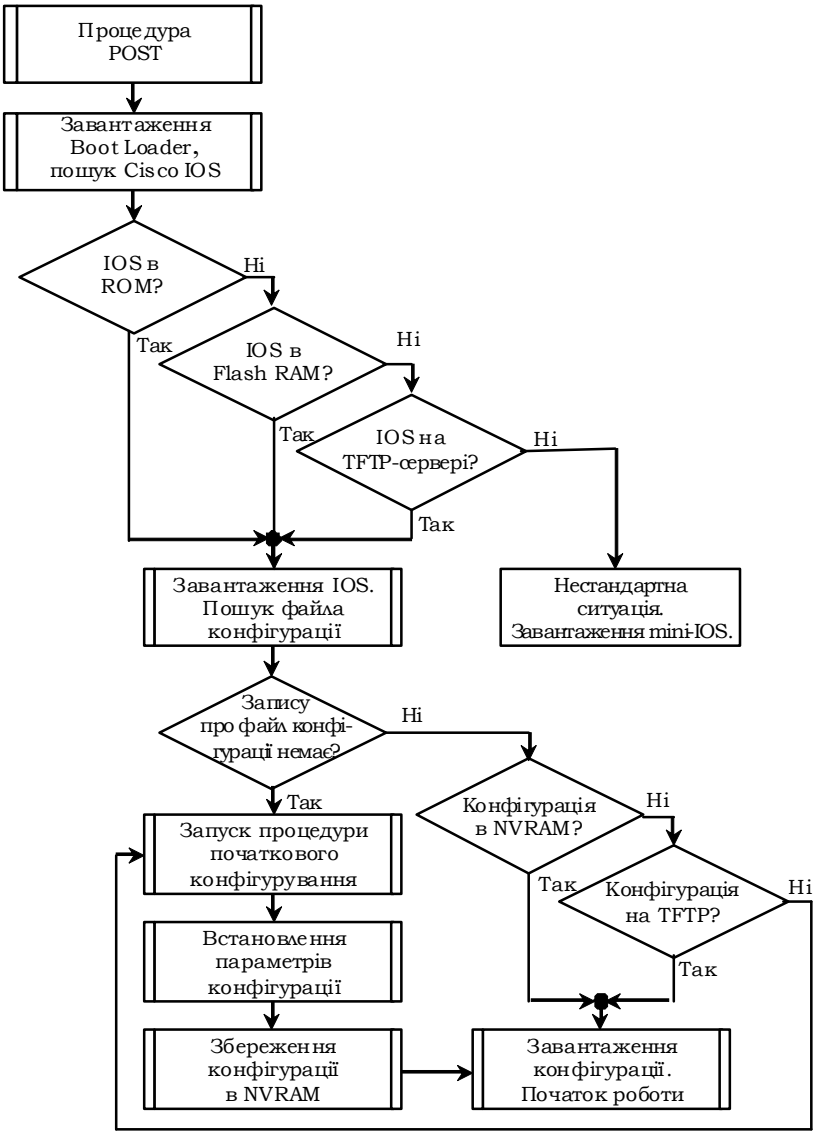


Рис. 9. Блок-схема алгоритму завантаження маршрутизатора Cisco

```
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled
Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340
IOS Image Load Test
_____
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
######################### [OK]
Smart Init is enabled
smart init is sizing iomem
TYPE MEMORY_REQ
Onboard devices &
buffer pools 0x01E8F000
-----------------------------------------------
TOTAL: 0x01E8F000
Rounded IOMEM up to: 32Mb.
Using 6 percent iomem. [32Mb/512Mb]
Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
R-1>
```

Рис. 10. Повідомлення при нормальному завантаженні маршрутизатора

Режими роботи маршрутизатора Cisco

Як і решта пристроїв Cisco, маршрутизатор Cisco, який працює під керуванням Cisco IOS, має основні та додаткові командних режими функціонування (рис. 10). На відміну від комутатора, який має обмежену кількість додаткових режимів, у маршрутизатора Cisco їх достатньо багато. Кожен із режимів надає певні функціональні можливості з діагностування та налагодження роботи маршрутизатора. У кожному режимі користувачеві надається певний набір команд. Переходи між режимами також здійснюються за допомогою відповідних команд (рис. 10). Номенклатура режимів маршрутизатора визначається набором можливостей та версією Cisco IOS.

Основними режимами є:

- режим користувача (User Mode, User EXEC Mode);
- привілейований режим (Privilege Mode, Privilege EXEC Mode);
- режим глобального конфігурування (Global Configuration Mode).

У режимі користувача надається обмежений доступ до маршрутизатора, дозволяється переглядати (але не змінювати) деякі параметри конфігурації. У привілейованому режимі дозволяється детально аналізувати стан маршрутизатора. Адміністраторові надається можливість виконати велику кількість команд. У цьому режимі можливе налагодження певних параметрів і їх збереження для подальшої роботи. У режимі глобального конфігурування, що активується тільки з привілейованого режиму, надається повний доступ до набору команд налагодження маршрутизатора та доступ до додаткових режимів.

Найбільш вживаними додатковими режимами є:

режим конфігурування інтерфейсу (Interface Configuration Mode);

режим конфігурування підінтерфейсу (Subinterface Configuration Mode);

режим конфігурування лінії (Line Configuration Mode);

режим конфігурування протоколу маршрутизації (Router Configuration Mode);

режим конфігурування DHCP-сервера (DHCP Configuration Mode);

режим конфігурування стандартного списку доступу (Standard ACL Configuration Mode);

режим конфігурування розширеного списку доступу (Extended ACL Configuration Mode).

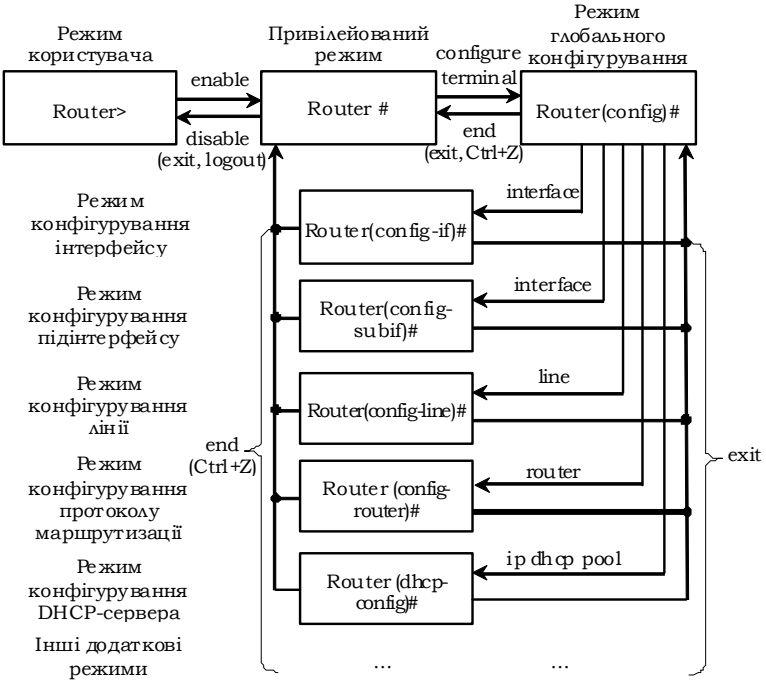


Рис. 10. Командні режими маршрутизатора Cisco та команди переходів між режимами

Після завантаження маршрутизатор Cisco перебуває у режимі користувача. Для переходу до привілейованого режиму використовується команда **enable**. Для повернення до режиму користувача – одна з команд **disable**, **logout** або **exit**. Для переходу до режиму глобального конфігурування – команда **configure terminal**, для повернення до попереднього режиму – одна з команд **end** або **exit**. Перехід з режиму глобального конфігурування до додаткових режимів здійснюється за допомогою відповідних команд. Повернення до режиму глобального конфігурування – за допомогою команди **exit**. Можливий прямий перехід і з будь-якого додаткового режиму до привілейованого режиму. З цією метою застосовується або команда **end**, або натиснення комбінації клавіш **<Ctrl>+<Z>**.

Інтерфейси маршрутизатора Cisco

Інтерфейси маршрутизатора Cisco з точки зору адміністрування можна розділити на дві групи: фізичні інтерфейси та логічні інтерфейси. Фізичні інтерфейси – це інтерфейси відповідних мережних технологій. Логічні інтерфейси – це інтерфейси, які автоматично створені операційною системою Cisco IOS для виконання певних функцій, або інтерфейси, які створюються адміністратором із певною метою. Позначення і, в багатьох аспектах, налагодження фізичних інтерфейсів не залежить від того, чи є вони електричними, чи оптичними. Слід зазначити, що фізичні інтерфейси маршрутизатора Cisco за замовчуванням є неактивними. Активність логічного інтерфейсів залежить від їх видів та зв'язків з фізичними інтерфейсами. Перелік та опис основних фізичних і логічних інтерфейсів маршрутизатора Cisco наведені у табл. 9.

Таблиця 9

Інтерфейси маршрутизаторів Cisco

Назва інтерфейсу	Опис інтерфейсу
Фізичні інтерфейси	
Ethernet	Інтерфейс класичного Ethernet, 10 Мбіт/с
FastEthernet	Інтерфейс FastEthernet, 100 Мбіт/с
GigabitEthernet	Інтерфейс GigabitEthernet, 1 Гбіт/с
TenGigabitEthernet	Інтерфейс 10 GigabitEthernet, 10 Гбіт/с
Dot11radio	Інтерфейс Wi-Fi
Serial	Послідовний інтерфейс
POS	Інтерфейс Packet over SONET
ATM	Інтерфейс технології ATM (сюди ж відносяться DSL-зєднання)
Async	Асинхронний інтерфейс
BRI	Інтерфейс BRI мереж технології ISDN (служба 2B+D)
Tokenring	Інтерфейс Token Ring
FDDI	Інтерфейс FDDI
Hub	Вбудований концентратор (вважається інтерфейсом)
HSSI	Високошвидкісний (до 52 Мбіт/с) послідовний інтерфейс
Логічні інтерфейси (як правило, створюються адміністратором)	
Null	Інтерфейс бітоприймача. Будь-які дані, відіслані на даний інтерфейс, видаляються. Використовується для простої фільтрації маршрутів.
PortChannel	Інтерфейс агрегованого каналу (L3 EtherChannel)
Tunnel	Інтерфейс віртуального GRE/IP Security тунелю
Loopback	Віртуальний інтерфейс маршрутизатора (не плутати з Loopback/Localhost/127.0.0.1 звичайного комп'ютера)
Dialer	Інтерфейс маршрутизації викликів за запитом.
Virtual-Template	Інтерфейс віртуального тунелю IP-Security
Multilink	Інтерфейс агрегованого за протоколом MLPPP каналу (канал склада-

	ється з кількох фізичних послідовних каналів).
BVI	Інтерфейс віртуального моста
Group-Async	Логічна група асинхронних інтерфейсів.
VLAN	Інтерфейс VLAN. На деяких маршрутизаторах автоматично створено інтерфейс vlan 1 за замовчуванням.

Порядок налаштування інтерфейсів маршрутизатора Cisco

Специфіка налагодження певного інтерфейсу маршрутизатора Cisco зумовлена специфікою використання відповідної мережної технології чи з'єднання. Наприклад, для маршрутизатора інтерфейс Ethernet одночасно є і DTE, і DCE-пристроєм, тому не виникає потреби в деталізації функцій інтерфейсу. Послідовне з'єднання в одних випадках при використанні певного типу кабелю передбачає виділення ролі DTE-пристрою для одного маршрутизатора та DCE для іншого, в інших випадках – ні.

Порядок налаштування Ethernet інтерфейса на маршрутизаторах Cisco є наступним згідно з рекомендаціями виробника є наступним:

1. Вибір інтерфейсу (обов'язково).
2. Присвоєння IP-адреси та маски підмережі (обов'язково).
3. Активація інтерфейсу(обов'язково).
4. Налаштування додаткових параметрів: пропускної здатності, затримки, опису і т.п. (необов'язково).

Порядок налаштування послідовного інтерфейсу при використання прямого з'єднання нуль-модемним кабелем на маршрутизаторах Cisco згідно з рекомендаціями виробника є наступним:

1. Вибір інтерфейсу (обов'язково).
2. Налаштування на одному з двох інтерфейсів ролі інтерфейсу DCE (обов'язково).
3. Присвоєння IP-адреси та маски підмережі (обов'язково).
4. Активація інтерфейсу(обов'язково).
5. Налаштування додаткових параметрів: пропускної здатності, затримки, опису і т.п. (необов'язково).

Основні команди налагодження параметрів інтерфейсів маршрутизатора Cisco

Вибір інтерфейсу маршрутизатора для налагодження виконується командою **interface**. Можливе одночасне налагодження групи інтерфейсів. Для цього використовується команда **interface range**. Слід нагадати, що за замовчуванням фізичні інтерфейси маршрутизатора знаходяться у відключеному стані, а логічні інтерфейси залежно від типу можуть знаходитися як у відключеному, так і включеному станах. Відключення інтерфейсу виконується командою **shutdown**, включення – командою **no shutdown**. Для налагодження параметрів інтерфейсів маршрутизатора, залежно від їх типу використовується достатньо великий набір команд. Більшість команд є загальними для всіх інтерфейсів, частина – характерними лише для інтерфейсів певних технологій.

Основними командами налаштування параметрів фізичного і канального рівня для інтерфейсів маршрутизатора є команди: **arp**, **bandwidth**, **clock rate, delay**, **description**, **duplex**, **encapsulation**, **keepalive**, **ip**, **mac-address**, **mtu**, **speed.** Відміна дії команд – використання форми **no**, або команда **default**.

Команда **arp** та її модифікації служать для обробки ARP-запитів та їх параметрів на інтерфейсі. Команда **bandwidth** служить для встановлення значення пропускної здатності, що використовується при обчисленні метрик маршрутів у протоколах маршрутизації, не встановлює швидкість передачі даних інтерфейсу і не впливає на фактичну швидкість передачі даних по каналу зв'язку. Команда **clock rate** служить для налаштування частоти тактових імпульсів на одному з пари інтерфейсів (типу DCE), що формують прямий двоточковий послідовний канал між двама маршрутизаторами (з'єднання типу нуль-модем). При підключенні маршрутизатора через DCE-пристрій (наприклад, CSU/DSU) команда не задається, оскільки синхронізація здійснюється провайдером послуг. Команда **delay** служить для встановлення значення затримки на інтерфейсі, це значення використовується при обчисленні метрик у деяких протоколах маршрутизації, команда не визначає параметрів інтерфейса. Команда **description** служить для опису інтерфейсу, використову-

ється з метою полегшення аналізу результатів виводу команд при адмініструванні. Команда **duplex** (та її модифікації **duplex-full, duplex-half**) служать для зазначення режиму передачі даних на інтерфейсі. Команда **encapsulation** служить для налаштування типу інкапсуляції на інтерфейсі. Часто використовується на послідовних інтерфейсах для зазначення протоколу або технології канального рівня, на інтерфейсах Ethernet використовується для тегування VLAN (як 802.1Q, так і ISL). Команда **keepalive** служить для зазначення інтервалу, протягом якого маршрутизатор буде очікувати перед тим, як відправити через інтерфейс повідомлення про перевірку зв'язку для визначення чи працює інтерфейс на іншому кінці послідовного каналу. На Ethernet-інтерфейсах маршрутизатор пересилає повідомлення самому собі. Команда **mtu** служить для зазначення MTU інтерфейса, це значення варто змінювати для оптимізації продуктивності мережі, наприклад, для каналів з великими втратами його варто зменшувати.

Синтаксис команди **interface** (режим глобального конфігурування).

interface *interface-type interface-id.subinterface-id* [{point-to-point | multipoint}]

де ***interface-type*** – тип інтерфейса, може приймати значення **Ethernet**, **FastEthernet**, **Serial**, **ATM**, **Loopback**, **Tunnel**, **Vlan** та ін.;

interface-id – ідентифікатор інтерфейса, може мати одночислове позначення ***number*** (номер інтерфейса), двочислове позначення ***module/number*** (номер модуля (адаптера)/номер інтерфейса), тричислове позначення ***slot/module/number*** (номер слота/номер модуля(адаптера)/ номер інтерфейса);

subinterface-id **–** ідентифікатор підінтерфейса, може приймати значення від 0 до 4294967295, за замовчуванням інтерфейс не містить підінтерфейсів, вони створюються у процесі виконання команди **interface**; підінтерфейси використовуються дла забезпечення роботи протоколу 802.1Q та технологій Frame Relay і ATM;

point-to-point – службова конструкція, яка зазначає, що підінтерфейс логічно з'єднаний з одним віддаленим вузлом;

multipoint – службова конструкція, яка зазначає, що підінтерфейс логічно з'єднаний з кількома віддаленими вузлами;

Параметри **point-to-point** та **multipoint**, як правило, зазначаються при роботі з інтерфейсами Frame Relay і ATM.

Синтаксис команди **arp** (режим конфігурування інтерфейсу).

arp {arpa | frame-relay | probe | snap }

де **arpa** – інкапсуляція для мереж Ethernet, встановлюється за замовчуванням;

frame-relay – інкапсуляція для мереж Frame Relay;

probe – інкапсуляція для протоколу HP Probe;

snap – інкапсуляція для SNAP (згідно RFC 1042);

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

arp timeout ***seconds***

де ***seconds*** – час життя ARP-запису в ARP-таблиці (с), за замовчуванням дорівнює 14400.

Синтаксис команди **bandwidth** (режим конфігурування інтерфейсу).

bandwidth ***value***

де ***value*** – значення пропускної здатності в Кбіт/с, за замовчуванням залежить від типу інтерфейсу.

Синтаксис команди **clock rate** (режим конфігурування інтерфейсу).

clock rate ***bps***

де ***bps*** – значення частоти тактових імпульсів (біт/с), може приймати значення 1200, 2400, 4800, 9600, 19 200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, 4000000; за замовчуванням не зазначається.

Синтаксис команди **delay** (режим конфігурування інтерфейсу).

delay ***value***

де ***value*** – значення затримки на інтерфейсі в десятках мілісекунд, за замовчуванням залежить від типу інтерфейсу.

Синтаксис команди **description** (режим конфігурування інтерфейсу).

description ***text-line***

де ***text-line*** – тестовий рядок опису інтерфейсу (до 240 символів).

Синтаксис команди **duplex** (режим конфігурування інтерфейсу).

duplex {auto | full | half}

де **auto** – автоматичний вибір режиму;

full – повнодуплексний режим;

half – напівдуплексний режим.

Синтаксис команди **encapsulation** (режим конфігурування інтерфейсу/підінтерфейсу).

encapsulation { ppp | hdlc | frame-relay [cisco | ietf] | dotlq *vlan-id* … }

ppp – службова конструкція, яка вказує, що інкапсуляцію здійснювати згідно стандартів протоколу PPP;

hdlc – службова конструкція, яка вказує, що інкапсуляцію здійснювати згідно стандартів протоколу HDLC;

frame-relay – службова конструкція, яка вказує, що інкапсуляцію здійснювати згідно стандартів технології Frame Relay;

cisco – фірмовий спосіб інкапсуляції Cisco для Frame Relay;

ietf – стандартний спосіб інкапсуляції IETF;

dotlq – інкапсуляція по протоколу 802.1Q;

vlan-id – номер VLAN в діапазоні від 1 до 1005 при використанні стандартного образу IOS, при використанні образу з розширеними можливостями – в діапазоні від 1 до 4094.

Синтаксис команди **keepalive** (режим конфігурування інтерфейсу).

keepalive *seconds*

де ***seconds*** – значення інтервалу часу очікування, яке задається в секундах, за замовчуванням становить 10 с.

Синтаксис команди **ip** (режим конфігурування інтерфейса/підінтерфейса).

Синтаксис команди **ip address** (режим конфігурування інтерфейса)**.**

ip address {*address network_mask*} | dhcp

де ***address*** – IP-адреса в десятковому записі;

network_mask – маска мережі, записана у звичайній формі;

dhcp – службова конструкція, яка вказує, що IP-адресу необхідно отримати автоматично по протоколу DHCP.

Синтаксис команди **mac-address** (режим конфігурування інтерфейсу).

mac-address *hw-address*

де ***hw-address*** – MAC-адреса інтерфейсу у вигляді HHHH.HHHH.HHHH, кожне число HHHH має довжину 2 байти і записується в шістнадцятковій формі.

Синтаксис команди **mtu** (режим конфігурування інтерфейсу).

mtu *value*

де ***value*** – значення MTU в байтах, значення за замовчуванням залежить від технології або протоколу канального рівня.

Синтаксис команди **speed** (режим конфігурування інтерфейсу).

speed {10 | 100 | 1000 | auto [10 | 100 | 1000] | nonegotiate}

де **10**, **100**, **1000** – значення швидкості в Мбіт/с,

auto – службова конструкція, яка вказує автоматичний вибір швидкості; якщо використовується форма **auto 10** (**auto 100, auto 1000**) інтерфейс веде переговори лише на цій швидкості;

nonegotiate – службова конструкція, яка відключає режим автопереговорів про швидкість.

Синтаксис команди **config-register** (режим глобального конфігурування):

config-register *conf_reg_value*

де ***conf_reg_value*** – значення конфігураційного регістру, число з діапазону 0x0000 ... 0xFFFF; за замовчуванням становить 0x2102.

Основні команди Cisco IOS для базової діагностики роботи маршрутизатора Cisco

Для виведення діагностичної інформації про фізичні параметри маршрутизатора чи його інтерфейсів, стан маршрутизатора, результати налагоджень або результати роботи маршрутизатора тощо використовується команда **show**. Вона є доступною як із режиму користувача, так і з привілейованого режиму. Залежно від режиму дана команда може мати різні параметри. Частина параметрів є однаковими і доступними в обох режимах. Часто команда **show** із певним параметром уважається окремою командою. Перелік основних команд **show** та їх призначення наведені у табл. 10.

Таблиця 10

Перелік основних параметрів команди show

Команда	Призначення
show version	Виведення поточної інформації про апаратне і програмне забезпечення
show tech-support	Виведення системної інформації для технічної підтримки
show flash	Перегляд вмісту флеш-пам'яті
show file systems	Виведення про файлову систему
show memory	Виведення інформації про використання пам'яті
show processes	Виведення інформації про процеси, запущені на пристрої
show processes cpu	Виведення деталізованої інформації про завантаження процесора
show processes memory	Виведення інформації про завантаження процесами оперативної пам'яті

show controllers	Виведення деталізованої інформації про роботу контролера інтерфейса
show interfaces	Виведення деталізованої інформації про інтерфейси маршрутизатора та їх стан
show ip interface	Виведення інформації про функціонування протоколу IP версії 4 та суміжних протоколів
show ip interface brief	Виведення інформації про функціонування протоколу IP версії 4 на інтерфейсі у скороченеому вигляді
show ipv6 interface	Виведення інформації про функціонування протоколу IP версії 6 та суміжних протоколів
show ipv6 interface brief	Виведення інформації про функціонування протоколу IP версії 6 на інтерфейсі у скороченеому вигляді
show route	Виведення таблиці маршрутизації протоколу IP версії 4
Show ipv6 route	Виведення таблиці маршрутизації протоколу IP версії 6
show protocols	Виведення глобальної та інтерфейсно-залежної інформації про протоколи 3-го рівня, що функціонують на маршрутизаторі
show startup-config	Перегляд стартової конфігурації пристрою
show running-config	Перегляд поточної конфігурації пристрою
show history	Перегляд списку останніх виконаних команд (за замовчуванням 10 рядків)
show clock	Виведення часу, встановленого на маршрутизаторі

Модельний приклад налагодження параметрів каналу зв'язку технології Fast Ethernet, побудованого між маршрутизаторами Cisco

Розглянемо специфіку налагодження параметрів каналу зв'язку технології Fast Ethernet між маршрутизаторами Cisco для з'єднання, схема якої наведена на рис. 11.

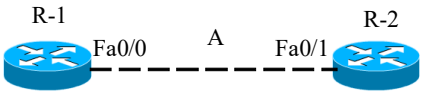


Рис. 11. Приклад мережі

Під час побудови каналу зв'язку для з'єднання пристроїв використано дані табл. 11. Для налагодження параметрів адресації інтерфейсів пристроїв використано дані табл. 12.

Таблиця 11

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R-1	Fa0/0	Маршрутизатор R-2	Fa0/1
Маршрутизатор R-2	Fa0/1	Маршрутизатор R-1	Fa0/0

Таблиця 12

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс

Підмережа А	–	195.1.1.0	255.255.255.252	/30
Маршрутизатор R-1	Інтерфейс Fa0/0	195.1.1.1	255.255.255.252	/30
Маршрутизатор R-2	Інтерфейс Fa0/1	195.1.1.2	255.255.255.252	/30

Сценарії налагодження параметрів інтерфейсів технології Fast Ethernet (швидкість, режим роботи, MAC-адреса) та параметрів IP-адресації для маршрутизаторів R-1, R-2 наведені нижче.

```
…
Router>enable
Router#configure terminal
Router(config)#hostname R-1
R-1(config)#interface FastEthernet 0/0
R-1(config-if)#description LINK-TO-R-2
R-1(config-if)#speed 100
R-1(config-if)#duplex full
R-1(config-if)#mac-address 00aa.00ad.0001
R-1(config-if)#ip address 195.1.1.1 255.255.255.252
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#exit
R-1#
…
…
Router>enable
Router#configure terminal
Router(config)#hostname R-2
R-2(config)#interface FastEthernet 0/1
R-2(config-if)#description LINK-TO-R-1
R-2(config-if)#speed 100
R-2(config-if)#duplex full
R-2(config-if)#mac-address 00aa.00ad.0002
R-2(config-if)#ip address 195.1.1.2 255.255.255.252
R-2(config-if)#no shutdown
R-2(config-if)#exit
R-2(config)#exit
R-2#
…
```

Результати виконання команд моніторингу та діагностики роботи інтерфейсів маршрутизаторів для розглянутого прикладу

З метою перегляду інформації про функціонування інтерфейсів маршрутизаторів для розглянутого прикладу використано команди **show interfaces, show ip interface brief**. Перевірка зв'язку між маршрутизаторами здійснена за допомогою команди **ping**. Результати роботи цих команд для маршрутизаторів R-1 та R-2 наведено відповідно на рис. 12–16.

```
R-1#show interfaces FastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 00aa.00ad.0001 (bia c403.0755.0000)
  Description: LINK-TO-R-2
  Internet address is 195.1.1.1/30
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:30, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     24 packets input, 4536 bytes
     Received 13 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     66 packets output, 7056 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Рис. 12. Результат виконання команди **show interfaces FastEthernet 0/0** на маршрутизаторі R-1

```
R-2#show interfaces FastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Gt96k FE, address is 00aa.00ad.0002 (bia c404.0764.0001)
  Description: LINK-TO-R-1
  Internet address is 195.1.1.2/30
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:36, output 00:00:06, output hang never
```

```
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   20 packets input, 3716 bytes
   Received 8 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog
   0 input packets with dribble condition detected
   69 packets output, 7526 bytes, 0 underruns
   0 output errors, 0 collisions, 3 interface resets
   0 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   0 output buffer failures, 0 output buffers swapped out
```

Рис. 13. Результат виконання команди **show interfaces FastEthernet 0/1** на маршрутизаторі R-2

```
R-1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0          196.1.1.1       YES NVRAM  up                    up
FastEthernet0/1         unassigned      YES NVRAM  administratively down down
FastEthernet1/0         unassigned      YES NVRAM  administratively down down
R-1#
```

Рис. 14. Результат виконання команди **show ip interface brief** на маршрутизаторі R-1

```
R-2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0         unassigned      YES NVRAM  administratively down down
FastEthernet0/1         196.1.1.2       YES NVRAM  up                    up
FastEthernet1/0         unassigned      YES NVRAM  administratively down down
R-2#
```

Рис. 15. Результат виконання команди **show ip interface brief** на маршрутизаторі R-2

```
R-1#ping 195.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/36/84 ms
R-1#
```

Рис. 16. Результат виконання команди **ping** на маршрутизаторі R-1

Модельний приклад налагодження параметрів послідовного каналу зв'язку, побудованого між маршрутизаторами Cisco

Розглянемо специфіку налагодження послідовних інтерфейсів маршрутизаторів Cisco у ході організації двоточкового послідовного каналу зв'язку, що зображений на рис. 17.

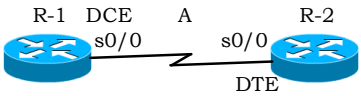


Рис. 17. Приклад мережі

Під час побудови даного каналу для з'єднання пристроїв використано дані табл. 13. Для налаштування параметрів адресації пристроїв використано дані табл. 14.

Таблиця 13

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R-1	Se0/0 (DCE)	Маршрутизатор R-2	Se0/0 (DTE)
Маршрутизатор R-2	Se0/0 (DTE)	Маршрутизатор R-1	Se0/0 (DCE)

Таблиця 14

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа А	–	196.1.1.0	255.255.255.252	/30
Маршрутизатор R-1	Інтерфейс Se0/0	196.1.1.1	255.255.255.252	/30
Маршрутизатор R-2	Інтерфейс Se0/0	196.1.1.2	255.255.255.252	/30

Сценарії налагодження параметрів послідовних інтерфейсів та параметрів адресації для маршрутизаторів R-1 та R-2 за умови використання встановленого за замовчуванням канального протоколу HDLC наведені нижче.

```
...
R-1>enable
R-1#configure terminal
R-1(config)#interface Serial 0/0
R-1(config-if)#description LINK-TO-R-2
R-1(config-if)#clock rate 64000
R-1(config-if)#ip address 196.1.1.1 255.255.255.252
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#exit
R-1#
…
…
R-2>enable
R-2#configure terminal
R-2(config)#interface Serial 0/0
R-2(config-if)#description LINK-TO-R-1
R-2(config-if)#ip address 196.1.1.2 255.255.255.252
```

```
R-2(config-if)#no shutdown
R-2(config-if)#exit
R-2(config)#exit
R-2#
…
```

Результати виконання команд моніторингу та діагностики роботи інтерфейсів маршрутизаторів для розглянутого прикладу

З метою перегляду інформації про функціонування інтерфейсів маршрутизаторів для розглянутого прикладу використано команди **show controllers**, **show interfaces**. Перевірка зв'язку між маршрутизаторами здійснена за допомогою команди **ping**. Результати роботи цих команд для маршрутизаторів R-1 та R-2 наведено відповідно на рис. 18–22.

```
R-1#show controllers serial 0/0
Interface Serial0/0
Hardware is GT96K
DCE 530, clock rate 64000
idb at 0x6570905C, driver data structure at 0x65710780
wic_info 0x65710D84
Physical Port 1, SCC Num 1
...
```

Рис. 18. Результати виконання команди **show controllers Serial 0/0** на маршрутизаторі R-1

```
R-2#show controllers serial 0/0
Interface Serial0/0
Hardware is GT96K
DTE 530 serial cable attached
idb at 0x6570905C, driver data structure at 0x65710780
wic_info 0x65710D84
Physical Port 1, SCC Num 1
...
```

Рис. 19. Результати виконання команди **show controllers Serial 0/0** на маршрутизаторі R-2

```
R-1#show interfaces Serial 0/0
Serial0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: LINK-TO-R-2
  Internet address is 196.1.1.1/30
  MTU 1492 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (5 sec)
  Restart-Delay is 3 secs
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```
     6 packets input, 1038 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     56 packets output, 3123 bytes, 0 underruns
     0 output errors, 0 collisions, 78 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
R-1#
```

Рис. 20. Результати виконання команди **show interface Serial 0/0** на маршрутизаторі R-1

```
R-2#show interfaces Serial 0/0
Serial0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: LINK-TO-R-1
  Internet address is 196.1.1.2/30
  MTU 1492 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (5 sec)
  Restart-Delay is 3 secs
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     100 packets input, 5073 bytes, 0 no buffer
     Received 100 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     50 packets output, 2988 bytes, 0 underruns
     0 output errors, 0 collisions, 6 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
R-2#
```

Рис. 21. Результати виконання команди **show interface Serial 0/0** на маршрутизаторі R-2

```
R-1#ping 196.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 196.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/36/84 ms
R-1#
```

Рис. 22. Результат виконання команди **ping** на маршрутизаторі R-1

Модельний приклад налагодження параметрів агрегованого каналу технології Gigabit Ethernet, побудованого між маршрутизаторами Cisco

Розглянемо специфіку налагодження параметрів агрегованого каналу зв'язку технології Gigabit Ethernet між маршрутизаторами Cisco для з'єднання, схема якої наведена на рис. 23.

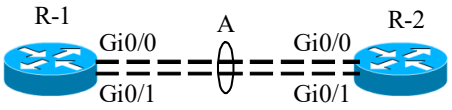


Рис. 23. Приклад мережі

Під час побудови каналу зв'язку для з'єднання пристроїв використано дані табл. 15. Для налагодження параметрів адресації інтерфейсів пристроїв використано дані табл. 16.

Таблиця 15

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R-1	Gi0/0	Маршрутизатор R-2	Gi0/0
	Gi0/1		Gi0/1
Маршрутизатор R-2	Gi0/0	Маршрутизатор R-1	Gi0/0
	Gi0/1		Gi0/1

Таблиця 16

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	–	197.1.1.0	255.255.255.252	/30
Маршрутизатор R-1	Інтерфейс Port-Channel 1	197.1.1.1	255.255.255.252	/30
Маршрутизатор R-2	Інтерфейс Port-Channel 1	197.1.1.2	255.255.255.252	/30

Сценарії налагодження параметрів агрегованого каналу технології Gigabit Ethernet та параметрів адресації для маршрутизаторів R-1, R-2 наведені нижче.

```
…
Router>enable
Router#configure terminal
Router(config)#hostname R-1
R-1(config)#interface port-channel 1
R-1(config-if)#description AGGREGATED_LINK-TO-R-2
```

```
R-1(config-if)#ip address 197.1.1.1 255.255.255.0
R-1(config-if)#exit
R-1(config)#interface GigabitEthernet 0/0
R-1(config-if)#channel-group 1
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#interface GigabitEthernet 0/1
R-1(config-if)#channel-group 1
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#exit
R-1#
…
```

```
…
Router>enable
Router#configure terminal
Router(config)#hostname R-2
R-2(config)#interface Port-Channel 1
R-2(config-if)#description AGGREGATED_LINK-TO-R-1
R-2(config-if)#ip address 197.1.1.2 255.255.255.0
R-2(config-if)#exit
R-2(config)#interface GigabitEthernet 0/0
R-2(config-if)#channel-group 1
R-2(config-if)#no shutdown
R-2(config-if)#exit
R-2(config)#interface GigabitEthernet 0/1
R-2(config-if)#channel-group 1
R-2(config-if)#no shutdown
R-2(config-if)#exit
R-2#
…
```

Результати виконання команд моніторингу та діагностики роботи інтерфейсів маршрутизаторів для розглянутого прикладу

З метою перегляду інформації про функціонування інтерфейсів маршрутизаторів для розглянутого прикладу використано команди **show interfaces**. Перевірка зв'язку між маршрутизаторами здійснена

за допомогою команди **ping**. Результати роботи цих команд для маршрутизаторів R-1 та R-2 наведено відповідно на рис. 24–26.

```
R-1#show interfaces port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is GEChannel, address is ca01.0645.0008 (bia ca01.0645.0006)
  Description: AGGREGATED_LINK-TO-R-2
  Internet address is 197.1.1.1/30
  MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Unknown duplex, Unknown Speed, media type is unknown media type
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 2
        Member 0 : GigabitEthernet0/0 , Full-duplex, 1000Mb/s
        Member 1 : GigabitEthernet1/0 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
    No. of PF_JUMBO supported members in this channel : 0
  Last input 00:01:54, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/150/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/80 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 516 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     6 packets output, 576 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
R-1#
```

Рис. 24. Результати виконання команди **show interface port-channel 1** на маршрутизаторі R-1

```
R-2#show interfaces port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is GEChannel, address is ca02.0720.0008 (bia ca02.0720.0006)
  Description: AGGREGATED_LINK-TO-R-1
  Internet address is 197.1.1.2/30
  MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Unknown duplex, Unknown Speed, media type is unknown media type
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 2
        Member 0 : GigabitEthernet0/0 , Full-duplex, 1000Mb/s
        Member 1 : GigabitEthernet1/0 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
    No. of PF_JUMBO supported members in this channel : 0
  Last input 00:02:59, output never, output hang never
  Last clearing of "show interface" counters never
```

```
  Input queue: 0/150/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/80 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

R-2#
```

Рис. 25. Результати виконання команди **show interface port-channel 1** на маршрутизаторі R-2

```
R-1#ping 197.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 197.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/28/60 ms
R-1#
```

Рис. 26. Результати виконання команди **ping** на маршрутизаторі R-1

Завдання на лабораторну роботу

1. У середовищі програмного симулятора/емулятора створити проект мережі (рис. 27). При побудові звернути увагу на вибір моделей маршрутизаторів, мережних модулів та плат, а також мережних з'єднань. На схемі канали зв'язку підмереж показані у загальному вигляді, при побудові підмережі вибирати потрібний тип кабелю для відповідної технології. Для цього використовувати дані табл. 6. Для побудованої мережі заповнити описову таблицю.

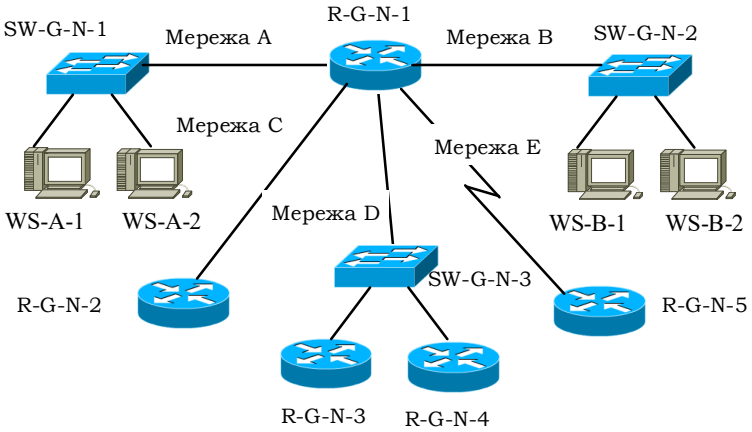


Рис. 27. Проект мережі

2. Провести базове налаштування маршрутизаторів, мережних інтерфейсів та з'єднань. Для цього використовувати дані табл. 17. На маршрутизаторі R-G-N-1 створити віртуальні інтерфейси Loopback N та Tunnel N, які відповідають мережам F та G.

3. Розробити схему адресації пристроїв мережі на основі даних, які наведені у табл. 18-19. Результати навести у вигляді таблиці.

4. Провести налаштування параметрів IP-адресації пристроїв мережі у відповідності до даних п. 3. Перевірити наявність зв'язку між парами пристроїв мережі.

5. Визначити основні параметри апаратної частини маршрутизаторів та інформацію про встановлені на маршрутизаторах Cisco IOS. Результати навести у вигляді таблиці табл. 19.

6. Визначити параметри фізичних і логічних інтерфейсів маршрутизатора R-G-N-1. Результати навести у вигляді таблиці, що аналогічна табл. 21.

Таблиця 17

Параметри каналів зв'язку підмереж

№ варіанта	Підмережа A	Підмережа B	Підмережі C, D	Підмережа E	
				Clock rate, біт/с	Bandwidth, Кбіт/с
1	10BaseT	100BaseTX	1000BaseT	9600	64
2	10BaseT	100BaseTX	1000BaseFX	1000000	128
3	10BaseT	100BaseFX	1000BaseT	38400	192

4	10BaseT	100BaseFX	1000BaseFX	250000	256
5	100BaseTX	100BaseTX	1000BaseT	64000	320
6	100BaseTX	100BaseTX	1000BaseFX	128000	384
7	100BaseTX	100BaseFX	1000BaseT	125000	448
8	100BaseTX	100BaseFX	1000BaseFX	128000	512
9	100BaseFX	100BaseTX	1000BaseT	148000	576
10	100BaseFX	100BaseTX	1000BaseFX	250000	640
11	100BaseFX	100BaseFX	1000BaseT	500000	704
12	100BaseFX	100BaseFX	1000BaseFX	800000	768
13	1000BaseT	100BaseTX	1000BaseT	1000000	832
14	1000BaseT	100BaseTX	1000BaseFX	1300000	896
15	1000BaseT	100BaseFX	1000BaseT	2000000	960
16	1000BaseT	100BaseFX	1000BaseFX	1000000	1024
17	100BaseFX	100BaseTX	1000BaseT	19200	1088
18	100BaseFX	100BaseTX	1000BaseFX	2000000	1152
19	100BaseFX	100BaseFX	1000BaseT	56000	1216
20	100BaseFX	100BaseFX	1000BaseFX	19200	1280
21	1000BaseFX	100BaseTX	1000BaseT	72000	32
22	1000BaseFX	100BaseTX	1000BaseFX	500000	64
23	1000BaseFX	100BaseFX	1000BaseT	64000	96
24	1000BaseFX	100BaseFX	1000BaseFX	128000	128
25	10BaseT	100BaseFX	1000BaseT	250000	160
26	100BaseFX	10BaseT	1000BaseT	800000	192
27	1000BaseFX	1000BaseT	10BaseT	128000	128
28	1000BaseFX	1000BaseT	10BaseT	19200	256
29	100BaseFX	10BaseT	1000BaseT	2000000	256
30	10BaseT	100BaseFX	1000BaseT	1000000	512
31	10BaseT	100BaseTX	1000BaseT	9600	64
32	10BaseT	100BaseTX	1000BaseFX	1000000	128
33	10BaseT	100BaseFX	1000BaseT	38400	192

Таблиця 18

Параметри IP-адресації підмереж

Мережа	Адреса мережі	Префікс
A	193.G.N.0	/25
B	194.G.N.0	/26
C	195.G.N.0	/30

D	196.G.N.0	/28
E	197.G.N.0	/30
F	198.G.N.0	/30
G	199.G.N.0	/30

Таблиця 19

Дані для визначення параметрів адресації мережі

№ варіанта	IP-адреса шлюзу за замовчуванням, IP-адреса основного DNS-сервера	IP-адреса альтернативного DNS-сервера 1	IP-адреса альтернативного DNS-сервера 2
1	Перша IP-адреса діапазону	Level3 Communications	Level3 Communications
2	Остання IP-адреса діапазону	Google	Google
3	Перша IP-адреса діапазону	OpenDNS Home	OpenDNS Home
4	Остання IP-адреса діапазону	Securly	Securly
5	Перша IP-адреса діапазону	Comodo Secure DNS	Comodo Secure DNS
6	Остання IP-адреса діапазону	DNS Advantage	DNS Advantage
7	Перша IP-адреса діапазону	Norton ConnectSafe	Norton ConnectSafe
8	Остання IP-адреса діапазону	SafeDNS	SafeDNS
9	Перша IP-адреса діапазону	OpenNIC	OpenNIC
10	Остання IP-адреса діапазону	Public-Root	Public-Root
11	Перша IP-адреса діапазону	Level3 Com-ns	Level3 Com-ns
12	Остання IP-адреса діапазону	Google	Google
13	Перша IP-адреса діапазону	OpenDNS Home	OpenDNS Home
14	Остання IP-адреса діапазону	Securly	Securly
15	Перша IP-адреса діапазону	Comodo Secure DNS	Comodo Secure DNS
16	Остання IP-адреса діапазону	DNS Advantage	DNS Advantage
17	Перша IP-адреса діапазону	Norton ConnectSafe	Norton ConnectSafe
18	Остання IP-адреса діапазону	SafeDNS	SafeDNS
19	Перша IP-адреса діапазону	OpenNIC	OpenNIC
20	Остання IP-адреса діапазону	Public-Root	Public-Root
21	Перша IP-адреса діапазону	Level3 Com-ns	Level3 Com-ns
22	Остання IP-адреса діапазону	Google	Google
23	Перша IP-адреса діапазону	OpenDNS Home	OpenDNS Home
24	Остання IP-адреса діапазону	Securly	Securly
25	Перша IP-адреса діапазону	Comodo Secure DNS	Comodo Secure DNS
26	Остання IP-адреса діапазону	DNS Advantage	DNS Advantage
27	Перша IP-адреса діапазону	Norton ConnectSafe	Norton ConnectSafe
28	Остання IP-адреса діапазону	SafeDNS	SafeDNS

Продовження таблиці 19

29	Перша IP-адреса діапазону	OpenNIC	OpenNIC
30	Остання IP-адреса діапазону	Public-Root	Public-Root
31	Перша IP-адреса діапазону	Level3 Communications	Level3 Communications

32	Остання IP-адреса діапазону	Google	Google
33	Перша IP-адреса діапазону	OpenDNS Home	OpenDNS Home

Таблиця 20

Основні публічні DNS-сервери

№ з/п	Провайдер	IP-адреса основного (первинного) DNS-сервера	IP-адреса альтернативного (вторинного) DNS-сервера
1	Level3 Communications	209.244.0.3	209.244.0.4
2	Verisign	64.6.64.6	64.6.65.6
3	Google	8.8.8.8	8.8.4.4
4	DNS.WATCH	84.200.69.80	84.200.70.40
5	Comodo Secure DNS	8.26.56.26	8.20.247.20
6	OpenDNS Home	208.67.222.222	208.67.220.220
7	DNS Advantage	156.154.70.1	156.154.71.1
8	Norton ConnectSafe	198.153.192.40	198.153.194.40
9	SafeDNS	195.46.39.39	195.46.39.40
10	OpenNIC	74.207.247.4	64.0.55.201
11	Securly	184.169.143.224	184.169.161.155
12	SmartViper	208.76.50.50	208.76.51.51
13	Dyn	216.146.35.35	216.146.36.36
14	FreeDNS	37.235.1.174	37.235.1.177
15	Public-Root	199.5.157.131	208.71.35.137
16	Alternate DNS	198.101.242.72	23.253.163.53
17	UncensoredDNS	91.239.100.100	89.233.43.71
18	censurfridns.dk	89.233.43.71	89.104.194.142
19	ScrubIt	67.138.54.100	207.225.209.66
20	Quad9	9.9.9.9	149.112.112.112
21	Neustar	156.154.70.1	156.154.71.1
22	Claudflare DNS	1.1.1.1	1.0.0.1

Таблиця 21

Параметри маршрутизаторів мережі

Параметр	R-G-N-1	. . .	…	…	R-G-N-5
Модель маршрутизатора					
Модель та номер процесора					
Об’єм пам’яті RAM, Мб					
Об’єм пам’яті NVRAM, Мб					
Об’єм Flash: – всього, Мб – зайнято, Мб – вільно, Мб					
Конфігураційний регістр					
Кількість інтерфейсів: – Ethernet – Fast Ethernet – Gigabit Ethernet – Serial – Loopback – Tunnel – Vlan					
Версія IOS					
Образ IOS					
Розмір файла образа IOS					
Системний час					

Таблиця 20

Параметри інтерфейсів маршрутизатора R-G-N-1

Параметр	Значення
Інтерфейс	
Адміністративний (фізичний) стан	
Стан лінійного протоколу	
Виробник, модель чіпсета	
Тип (для послідовних інтерфейсів DTE/DCE)	
Апаратна адреса	
Логічна адреса	
Затримка, мс	
Пропускна здатність, Кбіт/с (Мбіт/с, Гбіт/с)	
MTU, байт	
Протокол інкапсуляції	

Контрольні питання

1. Типова структурна схема маршрутизатора фірми Cisco.
2. Блоки пам’яті маршрутизатора Cisco та їх призначення.
3. Інтерфейси маршрутизаторів Cisco.
4. Модулі та плати розширення маршрутизаторів Cisco.
5. Змінні інтерфейсні модулі маршрутизаторів Ethernet.
6. Кабельні з’єднання Ethernet та Serial інтерфейсів маршрутизаторів Cisco.
7. Кабельні підключення, що застосовуються з метою налагодження та керування маршрутизатором Cisco.
8. Фізичні і логічні інтерфейси маршрутизаторів Cisco.
9. Загальна характеристика Cisco IOS. Платформи, набори можливостей та версії Cisco IOS, які використовуються для маршрутизаторів Cisco.
10. Джерела завантаження образу Cisco IOS та конфігурації маршрутизатора Cisco.
11. Командні режими Cisco IOS для маршрутизаторів Cisco. Команди переходів між командними режимами Cisco IOS для маршрутизаторів.
12. Команди діагностики апаратних складових маршрутизатора Cisco.
13. Команди діагностики функціонування інтерфейсів маршрутизатора Cisco.
14. Порядок та основні команди налагодження Ethernet-інтерфейсу маршрутизатора Cisco.
15. Порядок та основні команди налагодження послідовного інтерфейсу маршрутизатора Cisco.

ЛАБОРАТОРНА РОБОТА № 6
НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ВІДДАЛЕНОГО ДОСТУПУ ТА АДМІНІСТРУВАННЯ

Мета заняття: ознайомитися з особливостями функціонування протоколів та засобів віддаленого доступу та адміністрування; отримати практичні навички налагодження, моніторингу та діагностування засобів віддаленого доступу та адміністрування сучасних ОС; дослідити можливості ОС Windows, Linux, Cisco IOS з організації, налагодження та функціонування незахищених та захищених віддалених мережних підключень на базі протоколів Telnet та SSH.

Теоретичні відомості

Протоколи віддаленого доступу

Надзвичайно важливим питанням системного та мережного адміністрування є забезпечення постійного доступу до комунікаційних пристроїв та кінцевих вузлів мережі. Виконання цього завдання у сучасних мережах забезпечують так звані протоколи віддаленого доступу. Протокол віддаленого доступу забезпечує доступ адміністратора/користувача з одного вузла до іншого через існуючу мережну інфраструктуру. Як правило, такі протоколи побудовані за клієнт-серверною схемою. До протоколів віддаленого доступу належать протоколи:

– Telnet, TELecommunication NETwork;
– SSH, Secure SHell;
– RLOGIN, Remote LOGIN;
– RDP, Remote Desktop Protocol;
– RFB, Remote FrameBuffer.

Для цих протоколів розроблено ряд інструментальних засобів для реалізації віддаленого доступу – програм-серверів та програм термінальних клієнтів. У багатьох ОС термінальні клієнти є вбудованими. Більшість із вищеперерахованих протоколів (зокрема, Telnet та SSH) орієнтовані на використання інтерфейсу командного рядка, лише деякі (зокрема, RDP) – на використання графічних засобів. Найбільш поширеними протоколами сьогодні є протоколи віддаленого доступу Telnet та SSH. Протокол Telnet є недостатньо захищеним, тому у практиці адміністрування рекомендується застосовувати засоби, які базуються на протоколі SSH.

Протокол віддаленого доступу Telnet

Telnet (англ. TELecommunication NETwork, телекомунікаційна мережа) – протокол, який був розроблений одним із перших у стеку TCP/IP. Перші згадки про нього наявні у стандарті RFC-15 „Network Subsystem for Time Sharing Hosts", що був випущений у 1969 р. До 1983 р., коли було випущено основну специфікацію протоколу RFC-854 „Telnet Protocol Specification", розроблено й опубліковано понад 20 стандартів RFC, які покращували і розширювали можливості протоколу. Останній стандарт, який має відношення до протоколу Telnet, –це стандарт RFC-5198 „Unicode Format for Network Interchange", випущений у 2008 р.

Необхідність розробки протоколу Telnet була зумовлена потребою спрощення підключення до віддалених вузлів та пристроїв різних типів. У повсякденній діяльності використовується велика кількість різнотипних комп'ютерів, кожен із яких потребує сумісного обладнання для введення-виведення інформації (рис. 1, *а*), і це є проблемою.

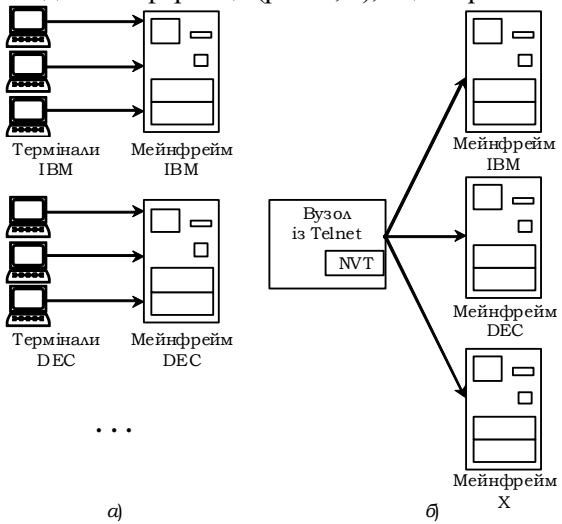


Рис. 1. Концепція віртуального термінала

Ситуацію ускладнює і те, що на цих комп'ютерах використовуються різні ОС, різні таблиці кодування та різне програмне забезпечення. Тому виникла потреба у службі емуляції термінала, яка б за-

мінила спеціалізовані пристрої та програми однією службою. Це було реалізовано за рахунок концепції віртуального термінала (NVT, Network Virtual Terminal) (див. рис. 1, *б*). Віртуальний термінал отримує дані, які вводяться у клієнтській системі, і перекладає їх на „універсальну мову". Отримані дані перекладаються з „універсальної мови" на спеціалізовану мову, яка сприймається вузлом. Це дає змогу будь-якому спеціалізованому клієнтові взаємодіяти з будь-яким спеціалізованим сервером.

Telnet є клієнт-серверним протоколом. Належить цей протокол до прикладного рівня моделі OSI та прикладного рівня стеку TCP/IP. Для передачі своїх повідомлень Telnet використовує засоби надійного транспортного протоколу TCP. Саме TCP забезпечує стабільний і надійний зв'язок. За замовчуванням сервер Telnet застосовує порт 23. Клієнт Telnet для організації обміну обирає вільний порт із діапазону динамічних портів системи.

Клієнт Telnet може бути налагоджений на підключення до іншого порту сервера, на якому працює інша служба. Це дозволяє використовувати клієнт Telnet для передачі команд та отримання відповідей на команди конкретним службам додатків та для потреб діагностики.

Telnet може працювати у таких режимах:

- напівдуплексний режим;
- посимвольний режим;
- рядковий режим;
- локальний режим.

Напівдуплексний режим уважається застарілим і у сучасних системах не застосовується. У посимвольному режимі кожен уведений символ відразу ж передається вузлу для обробки, а потім повертається клієнтові. У низькошвидкісних мережах це створює затримки. У багатьох реалізаціях згаданий режим застосовується за замовчуванням. У рядковому режимі текст команди спочатку виводиться на екран, і лише закінчені рядки передаються віддаленому вузлу для обробки. У локальному режимі обробка символів проводиться у локальній системі під контролем віддаленої системи.

Протокол віддаленого доступу SSH

Протокол SSH (англ. Secure SHell, ,,безпечна оболонка") – це мережний протокол віддаленого доступу, який дає змогу здійснювати віддалене управління операційною системою будь-якого мережного пристрою і безпечно передавати у незахищеному середовищі повідомлення будь-якого іншого мережного протоколу (наприклад, здійснювати тунелювання TCP-з'єднань для передачі файлів). За функціональністю схожий на протоколи Telnet, rlogin, rsh, але на відміну від них, шифрує увесь трафік, що передається, зокрема і паролі. Окрім шифрування може також здійснювати стиснення даних. Протокол SSH, як і решта протоколів віддаленого управління, побудований із використанням клієнт-серверного підходу. SSH-клієнти та SSH-сервери доступні для більшості мережних операційних систем.

Протокол SSH належить до прикладного рівня моделі OSI та прикладного рівня стеку TCP/IP. Для організації інформаційного обміну SSH-сервер використовує порт 22 TCP. Існує дві версії протоколу: SSH-1 (1995 р.) та SSH-2 (1996 р.). Версія SSH-2 є більш безпечною у порівнянні з SSH-1, тому набула більшого поширення. На сьогодні, коли йде мова про протокол SSH, то мається на увазі саме SSH-2.

Як стандарт мереж TCP/IP протокол SSH був затверджений IETF у 2000 р. Спочатку SSH був описаний у таких стандартах: RFC-4250 ,,The Secure Shell (SSH) Protocol Assigned Numbers", RFC-4251 ,,The Secure Shell (SSH) Protocol Architecture", RFC-4252 ,,The Secure Shell (SSH) Authentication Protocol", RFC-4253 ,,The Secure Shell (SSH) Transport Layer Protocol", RFC-4254 ,,The Secure Shell (SSH) Connection Protocol", RFC-4255 ,,Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints", RFC-4256 ,,Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)", RFC-4335 ,,The Secure Shell (SSH) Session Channel Break Extension", RFC-4344 ,,The Secure Shell (SSH) Transport Layer Encryption Modes", RFC-4345 ,,Improved Arcfour Modes for the Secure Shell (SSH) Transport Layer Protocol".

На сьогодні наведений перелік доповнено стандартами, що пов'язані з криптографічним захистом: RFC-4419 ,,Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol",

RFC-4432 „RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol", RFC-4462 „Generic Security Service Application Program Interface (GSS-API) Authentication and Key Exchange for the Secure Shell (SSH) Protocol", RFC-4716 „The Secure Shell (SSH) Public Key File Format", RFC-5656 „Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer".

Архітектурно у протоколі SSH виділяють три рівні:

– транспортний рівень (Transport Layer);

– рівень аутентифікації користувача (Authentication Layer);

– рівень з'єднання (Connection Layer).

Протокол транспортного рівня забезпечує аутентифікацію сервера, конфіденційність і цілісність даних з гарною естафетною передачею. Додатково може підтримуватися стиснення даних. Протокол аутентифікації користувача дає змогу серверу аутентифікувати клієнта. Протокол з'єднання мультиплексує шифрований тунель, створюючи в ньому кілька логічних каналів.

Для аутентифікації сервера у SSH використовується протокол аутентифікації сторін на основі алгоритмів електронно-цифрового підпису RSA або DSA. Для аутентифікації клієнта також може використуватися ЕЦП RSA або DSA, але допускається також аутентифікація за допомогою пароля (режим зворотної сумісності з Telnet) і навіть за IP-адресою вузла (режим зворотної сумісності з rlogin). Аутентифікація за паролем найбільш поширена і безпечна, оскільки пароль передається по зашифрованому віртуальному каналу. Аутентифікація за IP-адресою небезпечна, цю можливість, як правило, відключають. Для створення загального секрету (сеансового ключа) використовується алгоритм Діффі-Хеллмана. Для шифрування переданих даних використовується симетричне шифрування, алгоритми IDEA, AES, Blowfish, DES або 3DES. Цілісність передачі даних перевіряється за допомогою CRC32 у протоколі SSH версії 1 та за допомогою HMAC-SHA1/HMAC-MD5 у протоколі SSH версії 2. У протоколі SSH також можливе застосовування функції стиснення даних, що передаються. З цією метою використовується алгоритм LempelZiv (LZ77), який забезпечує рівень стиснення, аналогічний архіватору ZIP. Стиснення у SSH активується лише за запитом клієнта і на практиці застосовується досить рідко.

На базі протоколу SSH розроблено і функціонує ряд інших протоколів. Зокрема, SFTP (SSH File Transfer Protocol), SCP (Secure CoPy), FISH (Files Transferred over Shell Protocol), Rsync.

Широкого використання протокол SSH набув для віддаленого доступу та адміністрування мережних пристроїв. Більшість виробників мережного обладнання (в т.ч. Cisco, Juniper, Vyatta, Huawei та ін.) включають реалізації SSH-серверів та клієнтів у мережні операційні системи комутаторів, маршрутизаторів та інших пристроїв і саме цей протокол рекомендують використовувати.

Рекомендації щодо підвищення рівня захищеності віддалених мережних підключень на базі протоколів Telnet та SSH

Багатьма виробниками обладнання розроблені базові рекомендації, що стосуються підвищення рівня захищеності віддалених мережних підключень до комунікаційних пристроїв на базі протоколів Telnet та SSH. Часто ці рекомендації поєднуються з рекомендаціями щодо політик застосування засобів аутентифікації (парольного доступу).

Базові рекомендації щодо застосування засобів аутентифікації є такими:

1. Забезпечувати формування та дотримання політики стійких до зламу паролів.
2. Забезпечувати застосування аутентифікації з використанням механізму користувачів із зазначенням відповідного рівня привілеїв.
3. Вилучити/відключити облікові записи адміністраторів/користувачів, що створені за замовчуванням.
4. Змінити паролі, що створені за замовчуванням.
5. Надавати користувачам доступ до пристроїв/ресурсів (авторизувати користувачів) із мінімально необхідним рівнем привілеїв.
6. Забезпечити періодичну зміну паролів користувачів.
7. Обмежено застосовувати засоби протоколу SNMP (та інших подібних протоколів), у повідомленнях яких здійснюється передача паролів адмінстраторів.
8. Забезпечити контроль параметрів, що встановлені на пристроях для виконання процедур відновлення паролів.

Загальні рекомендації щодо захисту віддалених підключень є такими:

1. Забезпечити, за можливості, застосування засобів віддаленого доступу та адміністрування, які базуються на захищених протоколах, зокрема: SSH, SCP, SSL, OTP тощо.

2. Забезпечити застосування засобів віддаленого доступу та адміністрування, що базуються на незахищених протоколах Telnet, Rlogin (та інших незахищених протоколах: Syslog, SNMP, FTP, TFTP тощо), лише на мережних керуючих підключеннях (OOB-підключеннях, що, як правило, забезпечують підключення лише легітимних користувачів/адміністраторів).

3. Використовувати як VLAN керування пристроєм нестандартну VLAN (будь-яку VLAN, окрім Default VLAN – VLAN 1, що створюється за замовчуванням).

4. Обмежити можливості віддалених підключень за допомогою списків доступу, зокрема у випадках, якщо застосування мережних керуючих підключень (OOB) неможливе.

Рекомендації щодо застосування засобів протоколу SSH є такими:

1. Заборонити віддалений доступ під паролем основного адміністратора (root-доступ).

2. Заборонити підключення з пустим паролем або відключення входу за паролем.

3. Встановити нестандартний порт для SSH-сервера.

4. Забезпечити використання довгих SSH версії 2 RSA-ключів (як мінімум 1024, бажано 2048 біт і більше).

5. Сформувати та застосувати список IP-адрес, із яких дозволений доступ.

6. Заборонити доступ із потенційно небезпечних IP-адрес.

7. Відмовитися від використання поширених або широковідомих системних логінів для віддалених підключень.

8. Забезпечити регулярний перегляд та аналіз повідомлень про спроби та помилки аутентифікації.

9. Встановити та забезпечити фунціонування систем виявлення і попередження втручань.

10. Забезпечити використання засобів-пасток, які підроблюють SSH-сервіс (HoneyPots).

Серверні та клієнтські засоби організації віддаленого доступу до мережних пристроїв із використанням протоколів Telnet та SSH

Як відомо, протокол віддаленого доступу Telnet працює з використанням клієнт-серверного підходу. У більшості сучасних ОС наявні серверні та клієнтські програмні модулі, які забезпечують роботу цього протоколу. У деяких ОС згадані модулі є невід'ємними їх частинами та активуються за замовчуванням під час початкового встановлення системи, в інших ОС – потрібне виконання певних додаткових дій щодо їх встановлення та активації. У більшості ОС існує можливість встановлення і використання Telnet-серверів та Telnet-клієнтів сторонніх виробників. Як правило, і серверні, і клієнтські додатки протоколу Telnet використовують інтерфейс командного рядка.

Під час розробки протоколу Telnet проблемам захисту інформації не приділяли достатньої уваги, тому сеанси інформаційного обміну, які організовані за даним протоколом, не є захищеними від дій зловмисників. З метою підвищення рівня інформаційної безпеки засобами даного протоколу не рекомендується користуватися у відкритих (незахищених) мережних середовищах. Як виняток, можливе використання Telnet у захищених сегментах мереж.

Основною альтернативою використанню протоколу Telnet, яка забезпечує високий рівень захисту інформаційного обміну в ході організації віддаленого доступу як у відкритих, так і у захищених мережних середовищах, сьогодні є протокол SSH. Цей протокол, як і протокол Telnet, працює з використанням клієнт-серверного підходу. На жаль, у багатьох мережних ОС відсутні вбудовані програмні модулі, які забезпечують його роботу.

На ринку програмного забезпечення наявна велика кількість як комерційних, так і вільнорозповсюджуваних SSH-серверів та SSH-клієнтів для різних ОС. Деякі з них орієнтовані на використання лише в певних ОС, деякі є кросплатформними. Найбільш поширеними SSH-серверами є OpenSSH, Bitvise SSH Server (WinSSHD), CopSSH, Dropbear, freeSSHd SSH Server, GoAnywhere Services, lsh,

MobaSSH SSH Server, Pragma Fortress SSH Server, Tectia SSH Serve. Найбільш поширеними SSH-клієнтами є OpenSSH, PuTTY, SecureCRT та інші.

Узагальнена інформація про вбудовані серверні та клієнтські засоби організації віддаленого доступу сучасних мережних ОС наведена у табл. 1.

Таблиця 1

Вбудовані серверні та клієнтські засоби організації віддаленого доступу

ОС	Telnet		SSH	
	Сервер	Клієнт	Сервер	Клієнт
Windows XP	+	+	–	–
Windows 7/8/10	+*	+*	–	–
Linux	+	+	+	+
Cisco IOS	+	+	+	+
Juniper JunOS	+	+	+	+

* необхідні додаткові дії щодо встановлення та активації сервера та клієнта в системі

Встановлення та використання серверних та клієнтських додатків протоколів Telnet та SSH в ОС Windows

В ОС Windows XP сервер та клієнт протоколу Telnet встановлюються автоматично під час початкового встановлення системи. В ОС Windows 7/8/10 необхідно виконати додаткові дії щодо їх встановлення. У Windows 7 інсталяція Telnet-сервера та Telnet-клієнта проводиться через „Панель управления” → „Программы и компоненты” → „Включение или отключение компонентов Windows” → „Telnet-сервер” („Telnet-клиент”). В ОС Windows запуск (або зупинка) Telnet-сервера здійснюється через „Панель управления” → „Администрирование” → „Службы” (запускається додаток **tlntsvr**). Альтернативним способом запуску/зупинки Telnet-сервера є використання мережних команд **net start tlntsvr** та **net stop tlntsvr** відповідно.

Для адміністрування Telnet-сервера в ОС Windows передбачено використання специфічного текстового додатка **tlntadmn.exe**. Запущений без ключів додаток (рис. 2) показує налагоджені за замовчуванням параметри роботи сервера. Для зміни параметрів цей додаток може використовуватися з відповідними ключами (рис. 3).

Telnet-клієнти ОС Windows реалізуються у вигляді текстових та графічних утиліт. Серед вбудованих в ОС графічних Telnet-клієнтів

можна відмітити Microsoft Telnet (ОС Windows 9x) та Hyper Terminal (усі версії Windows). У багатьох випадках адміністратори використовують багатофункціональні термінальні клієнти сторонніх виробників, які дають змогу здійснювати віддалені мережні підключення не лише за протоколом Telnet, а й за іншими протоколами (зокрема, SSH та rlogin). Часто такі клієнти забезпечують роботу і консольних підключень. Найбільш відомими термінальними клієнтами для ОС Windows є Putty (www.putty.org) та SecureCRT (www.vandyke.com).

```
C:\>tlntadmn
Параметры localhost
Клавиша Alt переназначена на сочетание 'CTRL+A':        YES
Таймаут простоя сеанса                          :        1 часов
Максимум подключений                            :        2
Порт Telnet                                     :        23
Максимальное число попыток входа в систему      :        3
Действия при отключении                         :        YES
Режим работы                                    :        Console
Способ проверки подлинности                     :        NTLM, Password
Домен по умолчанию                              :        WS_01
Состояние                                       :        Работает
```

Рис. 2. Налагоджені за замовчуванням параметри роботи Telnet-сервера в ОС Windows

```
C:\>tlntadmn /?
Использование: tlntadmn [имя компьютера] [общие_параметры] start | stop |
pause
| continue | -s | -k | -m | config параметры_настройки
                                Для работы со всеми сеансами используйте
                                значение 'all'.
    -s код_сеанса               Вывод сведений о сеансе.
    -k код_сеанса               Прекращение сеанса.
    -m код_сеанса               Отправка сообщения сеансу.
    config                      Настройка параметров сервера telnet.
общие_параметры:
    -u пользователь             Пользователь, чьи учетные данные будут
                                использоваться
    -p пароль                   Пароль пользователя
параметры_настройки:
    dom = домен                 Домен по умолчанию для имен пользователей
    ctrlakeymap = yes|no        Сопоставление клавиши ALT
    timeout = чч:мм:сс          Таймаут для простаивающего сеанса
    timeoutactive = yes|no      Включение таймаута простаивающего сеанса.
    maxfail = число_попыток     Максимальное число неудачных попыток входа
                                до отключения.
    maxconn = число_подключений Максимальное число подключений.
    port = число                Задает порт telnet.
    sec = [+/-]NTLM [+/-]passwd Задает механизм проверки подлинности
    mode = console|stream       Задает режим работы.
C:\>
```

Рис. 3. Ключі для налагодження параметрів роботи Telnet-сервера в ОС Windows

Запуск вбудованого в ОС Windows Telnet-клієнта проводиться за допомогою командного рядка. Для безпосереднього зазначення параметрів підключення можуть використовуватися відповідні ключі (рис. 4). Слід зазначити, що для різних версій ОС Windows можуть бути наявні відмітності у переліку та використанні ключів.

Якщо додаток запускається без ключів, то адміністратор потрапляє у командний рядок Telnet-клієнта. У цьому разі параметри мережного підключення налагоджуються за допомогою відповідних команд (рис. 5). Слід звернути уваги на особливості налагодження параметрів Telnet-з'єднання за допомогою команди **set** (рис. 6).

```
C:\>telnet /?
telnet [-a][-e Символ][-f Файл_входа][-l Имя][-t Тип][Узел [Порт]]
 -l      Имя пользователя для входа в удаленную систему при условии, что
         поддерживается параметр TELNET ENVIRON.
 -a      Попытка автоматического входа в систему. Как и ключ -l, но исполь-
зует
         текущее имя пользователя, под которым выполнен вход в систему.
 -e      Служебный символ переключения режима ввода в окне telnet-клиента.
 -f      Имя файла со стороны клиента для выполнения входа в систему.
 -t      Тип telnet-терминала.
         Поддерживаются только 4 типа терминалов: vt100, vt52, ansi и vtnt.
 Узел    Имя узла или IP-адрес удаленного компьютера, к которому выполняе-
тся
         подключение.
 Порт    Номер порта или имя службы.
C:\>
```

Рис. 4. Ключі для налагодження параметрів підключення Telnet-клієнта в ОС Windows 7

```
Добро пожаловать в программу-клиент Microsoft Telnet
Символ переключения режима: 'CTRL+]'
Microsoft Telnet> ?
Команды могут быть сокращены. Поддерживаемыми командами являются:
c    - close                закрыть текущее подключение
d    - display              отобразить параметры операции
o    - open имя_узла [Порт] подключиться к сайту (по умолчанию, Порт = 23)
q    - quit                 выйти из telnet
set  - set                   установить параметры (,,set ?,, для вывода их спи-
ска)
sen  - send                 отправить строки на сервер
```

```
    st   - status               вывести сведения о текущем состоянии
    u    - unset                сбросить параметры (,,unset ?,, для вывода их спи-
ска)
    ?/h  - help                 вывести справку
    Microsoft Telnet>
```

Рис. 5. Команди Telnet-клієнта ОС Windows 7

```
    Microsoft Telnet> set ?
    bsasdel     символ <BackSpace> будет отправляться как символ <Delete>
    crlf        режим возврата каретки; приводит к отправке символов CR & LF
    delasbs     символ <Delete> будет отправляться как символ <BackSpace>
    escape x    где x - символ переключения в режим telnet-терминала и обратно
    localecho   включение локального эха.
    logfile x   где x - файл входа текущего клиента в систему
    logging     выполнение входа в систему
    mode x      где x - консоль или поток
    ntlm        включение проверки подлинности NTLM.
    term x      где x - ansi, vt100, vt52, или vtnt
    Microsoft Telnet>
```

Рис. 6. Параметри команди **set** Telnet-клієнта ОС Windows 7

Встановлення та використання серверних та клієнтських додатків протоколів віддаленого доступу Telnet та SSH в ОС Linux/Unix

Більшість Linux/Unix-подібних ОС у своєму складі мають засоби забезпечення роботи протоколу віддаленого доступу Telnet. У деяких з них Telnet-сервер та Telnet-клієнт Telnet встановлюються і активуються автоматично при початковому встановленні системи. Через проблеми безпеки протоколу у більшості сучасних ОС не виконується встановлення та активація роботи Telnet-сервера, а виконується лише встановлення Telnet-клієнта.

Для запуску Telnet-сервера використовується системна служба (демон) **telnetd**. Запуск може здійснюватися як в автоматичному, так і у ручному режимі. Додаток Telnet-клієнта встановлюється автоматично у більшості ОС Linux/Unix. Його запуск проводиться за допомогою командного рядка. За допомогою відповідних ключів існує можливість налагодити відповідні параметри підключення. Перелік ключів для запуску Telnet-клієнта ОС Linux Microcore наведено на рис. 7.

```
    tc@box:~$ telnet
    BusyBox v1.19.0 (2011-08-14 21:05:38 UTC) multi-call binary.
    Usage: telnet [-a] [-l USER] HOST [PORT]
    Connect to telnet server
            -a      Automatic login with $USER variable
            -l USER Automatic login as USER
```

```
tc@box:~$
```

Рис. 7. Ключі для налагодження параметрів підключення Telnet-клієнта в ОС Linux Microcore

Як безпечна альтернатива протоколу Telnet в Linux/Unix-системах широко використовується протокол віддаленого доступу SSH. На ринку програмних додатків існує досить багато відкритих розробок протоколу SSH. Найбільш поширеною і такою, що динамічно розвивається, є реалізація відома як OpenBSD Secure Shell або OpenSSH (www.openssh.org). У більшості сучаних Linux/Unix-подібних ОС SSH-сервер та SSH-клієнт встановлюються та активуються автоматично під час початкового встановлення системи. У багатьох ОС користувач має можливість керувати процесом встановлення SSH-сервера та SSH-клієнта у діалоговому режимі.

Сценарій налагодження та активації OpenSSH сервера в ОС Linux Microcore наведений нижче.

```
    root@box:#ls                                /mnt/hda1/tce/optional/openssh*
/mnt/sda1/tce/optional/openssh.tcz
/mnt/sda1/tce/optional/openssh.tcz.dep
/mnt/sda1/tce/optional/openssh.tcz.md5.txt
    root@box:#mv                        /usr/local/etc/ssh/sshd_config.example
usr/local/etc/ssh/sshd_config
    root@box:#/usr/local/etc/init.d/openssh start
    root@box:#/
```

Для автоматичної активації OpenSSH-сервера при запуску ОС Linux Microcore необхідно відредагувати та зберегти відповідні конфігураційні файли системи. Внесення змін у зазначені файли виконується або за допомогою системної команди **echo**, або за допомогою текстового редактора. Оскільки Linux Microcore є специфічно побудованою системою, то для збереження змін конфігурації слід скористатися спеціальною командою **filetool.sh -b**.

Сценарій виконання дій щодо внесення змін у конфігураційні файли OpenSSH-сервера в ОС Linux Microcore наведено нижче.

```
root@box:#echo ,,openssh.tcz,, >> /mnt/hda1/tce/onboot.lst
root@box:#echo ,,/usr/local/etc/init.d/openssh start,, >> /opt/bootlocal.sh
root@box:#echo ,,/usr/local/etc/ssh,, >> /opt/.filetool.lst
root@box:#/usr/bin/filetool.sh -b
root@box:#
```

Перелік ключів для запуску SSH-клієнта ОС Linux Microcore наведено на рис. 8.

```
root@box:~# ssh
usage: ssh [-1246AaCfgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
           [-D [bind_address:]port] [-e escape_char] [-F configfile]
           [-I pkcs11] [-i identify_file]
           [-L [bind_address:]port:host:hostport]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-R [bind_address:]port:host:hostport] [-S ctl_path]
           [-W host:port] [-w local_tun[:remote_tun]
           [user@]hostname [command]
root@box:~#
```

Рис. 8. Ключі для налагодження параметрів підключення SSH-клієнта в ОС Linux Microcore

Порядок налагодження сервера та клієнта протоколу Telnet на обладнанні Cisco

Налагодження функціонування Telnet-сервера на пристроях Cisco для забезпечення організації віддаленого доступу може здійснюватися з використанням трьох підходів:

– безпарольний вхід;

– вхід із використанням паролів на мережні підключення (та командні режими);

– вхід із використанням механізму користувачів.

Для безпарольного входу порядок виконання етапів налагодження є таким:

1. Обрати мережне (мережні) підключення для подальшої активації віддаленого доступу за протоколом Telnet (обов'язково).

2. Відключити використання аутентифікації для входу в систему для обраного мережного підключення/обраних мережних підключень (обов'язково).

3. Активувати можливість Telnet-підключення для відповідного мережного підключення/відповідних мережних підключень (обов'язково).

4. Налагодити додаткові параметри (тайм-аути, системні повідомлення тощо) для відповідного мережного підключення/відповідних мережних підключень (необов'язково).

Для входу з використанням паролів на мережні підключення порядок виконання етапів налагодження є таким:

1. Обрати мережне (мережні) підключення для подальшої активації віддаленого доступу за протоколом Telnet (обов'язково).

2. Створити пароль входу для відповідного мережного підключення/відповідних мережних підключень та паролі на командні режими (обов'язково).

3. Активувати використання парольної аутентифікації для відповідного мережного підключення/відповідних мережних підключень (обов'язково).

4. Активувати можливість Telnet-підключення для відповідного мережного підключення/відповідних мережних підключень (обов'язково).

5. Налагодити додаткові параметри (тайм-аути, системні повідомлення тощо) для відповідного мережного підключення/відповідних мережних підключень (необов'язково).

Для входу з використанням механізму користувачів порядок виконання етапів налагодження є таким:

1. Створити локального користувача із зазначенням відповідного рівня привілеїв та пароля (обов'язково).

2. Обрати мережне (мережні) підключення для подальшої активації віддаленого доступу за протоколом Telnet (обов'язково).

3. Активувати використання парольної аутентифікації з використанням локальної бази користувачів для відповідного мережного підключення/відповідних мережних підключень (обов'язково).

4. Активувати можливість Telnet-підключення для відповідного мережного підключення/відповідних мережних підключень (обов'язково).

5. Налагодити додаткові параметри (тайм-аути, системні повідомлення тощо) для відповідного мережного підключення/відповідних мережних підключень (необов'язково).

Для організації звичайного підключення для Telnet-клієнта не потрібно проводити налагодження параметрів. За потреби організації специфічного складного підключення існує можливість налагодження певних специфічних параметрів, наприклад, інтерфейсу виходу підключення на маршрутизаторі.

За звичайного використання для Telnet-клієнта немає необхідності виконувати налагодження параметрів підключення. За потреби можливе використання великої кількості специфічних параметрів підключення (наприклад, тип терміналу, перевірка достовірності, інтерфейс виходу для маршрутизатора). Перелік параметрів можна визначити з довідки системи. Налагодження параметрів здійснюється безпосередньо у командному рядку під час організації сеансу. Слід зазначити, що за допомогою Telnet-клієнта можна підключатися не лише до Telnet-сервера, а й до серверів та складових інших мережних протоколів стеку TCP/IP (зокрема, поштових протоколів SMTP, POP3, протоколу маршрутизації BGP і т.д.).

Порядок налагодження сервера та клієнта протоколу SSH на обладнанні Cisco

Налагодження функціонування SSH-сервера на пристроях Cisco для забезпечення віддаленого доступу може здійснюватися з використанням двох підходів:

– з використанням імені пристрою та імені домену;

– з використанням ключових пар RSA (без використання імені пристрою та імені домену).

Слід зазначити, що одним із обов'язкових попередніх етапів налагодження SSH-сервера є створення локального користувача з зазначенням відповідного рівня привілеїв та пароля.

Для підходу з використанням імені пристрою та імені домену порядок виконання етапів налагодження є таким:

1. Виконати іменування пристрою (обов'язково).

2. Виконати іменування домену (обов'язково).

3. Згенерувати SSH-ключ (ключову пару RSA), який буде використовуватися у процесі роботи (обов'язково).

4. Налагодити додаткові параметри SSH-сервера: версію протоколу, час тайм-ауту, кількість спроб аутентифікації та ін. (необов'язково).

5. Обрати мережне (мережні) підключення для подальшої активації віддаленого доступу за протоколом SSH (обов'язково).

6. Активувати використання локальної бази даних користувачів для обраного мережного підключення/обраних мережних підключень (обов'язково).

7. Активувати можливість SSH-підключення для відповідного мережного підключення / відповідних мережних підключень (обов'язково).

8. Налагодити додаткові параметри (тайм-аути, системні повідомлення тощо) для відповідного мережного підключення/відповідних мережних підключень (необов'язково).

Для підходу з використанням ключових пар RSA (без використання імені пристрою та імені домену) порядок виконання етапів налагодження є таким:

1. Створити ключову пару RSA, яка буде використовуватися у процесі роботи (обов'язково).

2. Згенерувати ключову пару RSA із зазначенням довжини ключа (обов'язково).

3. Налагодити додаткові параметри SSH-сервера: версію протоколу, час тайм-ауту, кількість спроб аутентифікації та ін. (необов'язково).

4. Обрати мережне (мережні) підключення для подальшої активації віддаленого доступу за протоколом SSH (обов'язково).

5. Активувати використання локальної бази даних користувачів для обраного мережного підключення/обраних мережних підключень (обов'язково).

6. Активувати можливість SSH-підключення для відповідного мережного підключення/відповідних мережних підключень (обов'язково).

7. Налагодити додаткові параметри (тайм-аути, системні повідомлення тощо) для відповідного мережного підключення/відповідних мережних підключень (необов'язково).

За звичайного використання для SSH-клієнта не потрібно виконувати налагодження параметрів підключення. Специфічні параметри підключення встановлюються за рахунок використання ключів у командному рядку клієнта.

Загальні команди налагодження функціонування протоколів віддаленого доступу на пристроях Cisco

Для налагодження функціонування протоколів віддаленого доступу (зокрема, Telnet та SSH) на пристроях Cisco використовуються як деякі загальні для всіх протоколів команди, так і характерні лише для певного протоколу команди. До загальних команд належать такі команди: **password**, **username**, **login**, **transport**, **rotary**, **autocommand, login**, **security authentication** та похідні від них команди.

Команди **login, password**, **username** призначені для налагодження параметрів аутентифікації для певного мережного підключення, команди групи **transport** призначені для дозволу/заборони віддалених підключень до/з пристрою з використанням різних мережних протоколів. Команда **rotary** відповідає за налагодження нестандартних портів для підключень. Команда **autocommand** дає можливість налагодити виконання певної команди режиму користувача після підключення. Для управління сеансами мережних протоколів можуть використовуватися як певні комбінації клавіш (для призупинення сесії **Ctrl+Shift+6, x**), так і певні команди (повернення до сеансу – команда **resume**, завершення сеансу – команда **disconnect**).

Важливими командами, що дають змогу здійснювати контроль та журналювання процесу віддалених підключень є команди, похідні від команд **login** та **security**: **login block-for**, **login delay login on-failure log**, **login on-success log**, **login quiet-mode** та **security authentication failure rate** відповідно. Команда **login block-for** застосовується для блокування можливості підключення до пристрою на певний період часу, якщо перевищено кількість спроб підключення на вставлений інтервал часу. Команда **login delay** зазначає затримку між спробами підключення. Команди **login on-failure log** та **login on-success log** застосовуються для активації журналювання подій при підключенні та аутентифікації користувача у системі. Вказані команди активують журналювання подій про неуспішні та успішні спроби відповідно. Команда **login quiet-mode access-class** застосовується для активації списків доступу для віддалених підключень. Команда **security authentication failure** встановлює кількість дозволених невдалих спроб входу в систему (за хвилину), перевищення якої викличе генерацію повідомлення для журналювання подій. Призначення та синтаксис усіх вищезгаданих команд наведено нижче.

Синтаксис команди **transport input** (режим конфігурування лінії):

transport input {*value* | *values*},

де ***value*** – параметр, який може набувати значень **all**, **lapb-ta**, **lat**, **mop**, **none**, **pad**, **rlogin**, **ssh**, **telnet**, **udptn**, **v120**; залежно від версії IOS можливі й інші значення;

values **–** рядок параметрів, що формується із значень **lapb-ta**, **lat**, **mop**, **pad**, **rlogin**, **ssh**, **telnet**, **udptn**, **v120**;

all – всі протоколи;

lapb-ta – термінальний адаптер протоколу LAPB;

lat – протокол DEC LAT;

mop – протокол DEC MOP Remote Console Protocol;

none – жоден із протоколів;

pad – протокол X.3 PAD;

rlogin – протокол Rlogin;

ssh – протокол SSH;

telnet – протокол Telnet;

udptn – асинхронний UDPTN через UDP протокол;

v120 – Асинхронне підключення через ISDN.

Синтаксис команди **transport output** (режим конфігурування лінії):

transport output {*value* | *values*}.

Параметри команди аналогічні параметрам попередньої команди.

Синтаксис команди **transport preffered** (режим конфігурування лінії):

transport preffered *value*.

Параметр команди аналогічний параметру ***value*** попередньої команди, за винятком значення **all**.

Синтаксис команди **rotary** (режим конфігурування лінії):

rotary *value* [queued [by-role [round-robin] | round-robin]] | round-robin [queued [by-role]],

де ***value*** – значення номера групи, що задається для номера порту; число з діапазону 0 … 127.

queued – параметр, який вказує на необхідність використання черги, коли група заповнена;

round-robin – параметр, який вказує на необхідність кругового вибору;

by-role – параметр, який вказує на необхідність вибору за ролями.

Синтаксис команди **autocommand** (режим конфігурування лінії):

autocommand { LINE | no-suppress-linenumber LINE },

де **LINE** – текстовий рядок, який містить команду (режиму EXEC), що буде автоматично виконуватися;

no-suppress-linenumber – параметр, який призначений для активації виведення повідомлення.

Синтаксис команди **login block-for** (режим глобального конфігурування):

login block-for ***block_value*** **attempts** ***attempts_value*** **within** ***interval_value***,

де ***block_value*** – значення інтервалу часу (с), на який буде заблоковано можливість виконання підключення; може змінюватися у межах від 1 до 65535 с;

attempts – службова конструкція, за допомогою якої зазначається максимально можлива кількість спроб підключення на заданий інтервал часу;

attempts_value – максимальне значення кількості спроб підключення на встановлений інтервал часу; може змінюватися у межах від 1 до 65535;

within – службова конструкція, за допомогою якої зазначається встановлений для можливої кількості спроб підключення інтервал часу;

interval_value – значення інтервалу часу (с), на якому задається максимальне значення кількості спроб підключення; може змінюватися у межах від 1 до 65535 с.

Синтаксис команди **login delay** (режим глобального конфігурування):

login delay ***delay_value***,

де ***delay_value*** – значення інтервалу затримки (с) між спробами підключення; може змінюватися у межах від 1 до 10 с; за замовчуванням становить 1 с.

Синтаксис команди **login on-failure log** (режим глобального конфігурування):

login on-failure log [every ***login_value*****]**,

де **every** – службова конструкція, за допомогою якої зазначається необхідність виконання журналювання неуспішних спроб входу в систему;

login_value – числове значення кількості спроб підключення, може змінюватися у межах від 1 до 65535.

Синтаксис команди **login on-success log** (режим глобального конфігурування):

login on-success log [every ***login_number*****]**,

де **every** – службова конструкція, за допомогою якої зазначається необхідність виконання журналювання успішних спроб входу в систему;

login_value – числове значення кількості спроб підключення, може змінюватися у межах від 1 до 65535.

Синтаксис команди **login quiet-mode access-class** (режим глобального конфігурування):

login quiet-mode access-class { *acl_name* | *acl_number* },

де ***acl_name*** – текстова назва списку доступу;

acl_number – номер списку доступу.

Синтаксис команди **security authentication failure rate** (режим глобального конфігурування):

security authentication failure rate *rate_value* log,

де ***rate_value*** – кількість дозволених невдалих спроб входу в систему (аутентифікації) за хвилину, перевищення якої викличе генерацію повідомлення для журналювання подій;

log – службова конструкція, за допомогою якої активується можливість виконання журналювання подій, пов'язаних із невдалими спробами входу в систему.

Команди налагодження функціонування протоколу Telnet на пристроях Cisco

Для налагодження параметрів функціонування протоколу Telnet на пристроях Cisco використовуються спеціалізовані команди **ip telnet**: **ip telnet comport**, **ip telnet hidden**, **ip telnet quiet**, **ip telnet source-interface**, **ip telnet timeout retransmit**, **ip telnet tos**. Команди групи **ip telnet comport** призначені для налагодження параметрів функціонування засобів протоколу Telnet згідно із RFC-2217. Команда **ip telnet hidden** призначена для відключення виведення IP-адрес або назв вузлів протоколу Telnet. Команда **ip telnet quiet** відповідає за відключення виведення непомилкових повідомлень. Команда **ip telnet source-interface** призначена для встановлення інтерфейсу виходу сеансів протоколу Telnet. Згадана команда застосовується, як правило, на маршрутизаторах та комутаторах третього рівня. Команда **ip telnet timeout retransmit** відповідає за встановлення значення тайм-ауту повторної передачі. Команда **ip telnet tos** застосовується для встановлення значення типу сервісу (TOS, Type Of

Service). Призначення та синтаксис усіх вищезгаданих команд наведено нижче.

Синтаксис команди **ip telnet comport** (режим глобального конфігурування):

ip telnet comport { disconnect delay ***disconnect_value*** **| enable | flow level** ***flow_value*** **| receive window** ***window_value*** **}**,

де ***disconnect_value*** – значення інтервалу затримки перед закриттям TCP-з'єднання (с), число з діапазону 0 … 360;

flow_value – кількість символів для буферизації на пристрої перед відправленням повідомлення RFC-2217 SUSPEND; число з діапазону 0 … 1023;

window_value – максимальне значення вікна отримання TCP; число з діапазону 1 … 4128.

Синтаксис команди ip telnet hidden (режим глобального конфігурування):

ip telnet hidden {addresses | hostnames},

де **addresses** – службова конструкція, за допомогою якої відключається виведення адрес;

hostnames – службова конструкція, за допомогою якої відключається виведення назв вузлів.

Синтаксис команди **ip telnet quiet** (режим глобального конфігурування):

ip telnet quiet.

Команда не має параметрів.

Синтаксис команди **ip telnet source-interface** (режим глобального конфігурування):

ip telnet source-interface ***interface-type interface-id***,

де ***interface-type*** – тип інтерфейсу, може набувати значень **Ethernet**, **FastEthernet**, **Gigabit Ethernet**, **Serial**, **Loopback**, **Tunnel**, **Vlan** та ін.;

interface-id – ідентифікатор інтерфейсу, може мати одночислове позначення ***number*** (номер інтерфейсу), двочислове позначення ***module/number*** (номер модуля (адаптера)/номер інтерфейсу), тричислове позначення ***slot/module/number*** (номер слоту/номер модуля (адаптера)/номер інтерфейсу);

Синтаксис команди **ip telnet timeout retransmit** (режим глобального конфігурування):

ip telnet timeout retransmit ***retransmit-value***,

де ***retransmit-value*** – значення інтервалу повторної передачі (с), число з діапазону 1 … 2147483.

Синтаксис команди **ip telnet tos** (режим глобального конфігурування):

ip telnet tos ***tos-value***,

де ***tos-value*** – значення параметра TOS, число з діапазону 0h …FFh

Команди налагодження функціонування протоколу SSH на пристроях Cisco

Для налагодження параметрів функціонування протоколу SSH на пристроях Cisco використовуються команди **ip ssh authentication-retries**, **ip ssh break-string**, **ip ssh dh min size**, **ip ssh dscp, ip ssh logging events**, **ip ssh maxstartups**, **ip ssh port**, **ip ssh precedence**, **ip ssh rsa keypair-name**, **ip ssh source-interface**, **ip ssh time-out**, **ip ssh version**, **crypto key generate**, **crypto key generate rsa general-keys modulus**, **crypto key generate rsa usage-keys label** та деякі інші. Призначення та синтаксис усіх вищезгаданих команд наведено нижче.

Команда **ip ssh authentication-retries** призначена для встановлення кількості спроб аутентифікації, після якої SSH-клієнтові забороняється доступ. Команда **ip ssh break-string** відповідає за активацію обробки та встановлення зазначення текстового рядка, що передається SSH-клієнтом SSH-серверу, який надалі передає сигнал зупинки для асинхроного підключення. Команда **ip ssh logging events** призначена для активації журналювання подій протоколу SSH. Команда **ip ssh maxstartups** використовується для обмеження кількості сесій протоколу.

Команда **ip ssh port** відповідає за активацію безпечного доступу до пристрою через асинхронні підключення та встановлення початкового номера TCP-порту, що буде використовуватися для цих підключень. Команди **ip ssh dscp** та **ip ssh precedence** застосовуються для встановлення значень полів DSCP та поля Precedence IP-пакета, що переносить повідомлення протоколу SSH.

Команда **ip ssh source-interface** використовується для зазначення певного вихідного інтерфейсу для всіх SSH-сесій. Згадана команда застосовується, як правило, на маршрутизаторах та комута-

торах третього рівня. Команда **ip ssh time-out** використовується для обмеження часу відповіді SSH-клієнта **(**SSH-сервер перериває з'єднання, якщо дані не передаються протягом часу очікування). Команда **ip ssh version** призначена для вказування версії протоколу SSH, що буде використовуватися у процесі роботи. За замовчуванням на пристроях Cisco активовано використання протоколу SSH версії 1. Відміна дії більшості команд **ip ssh** виконується формою **no**.

Команда **ip ssh rsa keypair-name** застосовується для зазначення назви ключа RSA, що буде використовуватися у процесі роботи протоколу SSH. Ключ може формуватися двома способами: або з використанням назви пристрою та назви домену або без їх використання. Також для робіт із ключами застосовується команда **ip ssh dh min size**, за допомогою якої задається номер групи Діффі-Хеллмана для обміну ключами.

Для роботи з ключами використовуються команди групи **crypto key**. Для генерації ключів застосовуються команди **crypto key generate**, **crypto key generate rsa general-keys modulus**, **crypto key generate rsa usage-keys label**. Для видалення ключів призначені команди **crypto key zeroize**, **crypto key zeroize rsa**.

Слід звернути увагу, що однакового результату у процесі налагодження функціонування протоколу SSH на пристроях Cisco можна досягнути у разі використання різних команд. Детальний опис дії команд можна знайти в документації виробника.

Синтаксис команди **ip ssh authentication-retries** (режим глобального конфігурування):

ip ssh authentication-retries *retries-value*,

де ***retries-value*** – значення максимальної кількості спроб аутентифікації підряд, число з діапазону 0…5; за замовчуванням встановлюється 3 спроби.

Синтаксис команди **ip ssh break-string** (режим глобального конфігурування):

ip ssh break-string *text-string*,

де ***text-string*** – текстовий рядок сигналу зупинки, за замовчуванням не встановлено.

Синтаксис команди **ip ssh dh min size** (режим глобального конфігурування):

ip ssh dh min size ***dh_value***,

де ***dh_value*** – значення номер групи Діффі-Хеллмана, може набувати значень 1024 (група 1), 2048 (група 14), 4096 (група 16); за замовчуванням дорівнює 1024.

Синтаксис команди **ip ssh dscp** (режим глобального конфігурування):

ip ssh dscp ***dscp_value***,

де ***dscp_value*** – значення поля DSCP IP-пакета, може набувати значень від 0 до 63; за замовчуванням дорівнює 0.

Синтаксис команди **ip ssh logging events** (режим глобального конфігурування):

ip ssh logging events. Команда не має параметрів.

Синтаксис команди **ip ssh maxstartups** (режим глобального конфігурування):

ssh ip ssh maxstartups [*max-value*],

де ***max-value*** – значення кількості сесій протоколу, число з діапазону 0…128; за замовчуванням встановлюється 128 сесій.

Синтаксис команди **ip ssh port** (режим глобального конфігурування):

ip ssh port ***port-number*** **rotary** ***group***,

де ***port-number –*** значення номера порту; число з діапазону 2000 … 10000;

rotary – службова конструкція, призначена для активації доступу з використанням значення ***group***;

group – значення номера групи; число з діапазону 1 ... 127.

Синтаксис команди **ip ssh precedence** (режим глобального конфігурування):

ip ssh precedence ***precedence_value***,

де ***precedence_value*** **–** значення поля Precedence, може набувати значень від 0 до 7; за замовчуванням дорівнює 0.

Синтаксис команди **ip ssh rsa keypair-name** (режим глобального конфігурування):

ip ssh rsa keypair-name ***keypair-name-string***,

де ***keypair-name-string*** – текстовий рядок, який містить назву ключа RSA.

Синтаксис команди **ip ssh source-interface** (режим глобального конфігурування):

ip ssh source-interface ***interface-type interface-id***,

де ***interface-type*** – тип інтерфейсу, може набувати значень **Serial**, **Ethernet**, **FastEthernet**, **Gigabit Ethernet**, **Serial**, **Port-channel**, **Tunnel** та ін.;

interface-id **–** ідентифікатор інтерфейсу, може мати одночислове позначення ***number*** (номер інтерфейсу), двочислове позначення ***module/number*** (номер модуля (адаптера)/номер інтерфейсу), тричислове позначення ***slot/module/number*** (номер слоту/номер модуля (адаптера)/номер інтерфейсу).

Синтаксис команди **ip ssh time-out** (режим глобального конфігурування):

ip ssh time-out ***seconds***,

де ***seconds*** – значення інтервалу часу очікування відповіді клієнта (с), число з діапазону 1 ... 120; за замовчуванням встановлюється 120 с.

Синтаксис команди **ip ssh version** (режим глобального конфігурування):

ip ssh version ***version-number***,

де ***version-number*** – номер версії протоколу, може набувати значень 1 або 2; якщо значення не встановлене, то функціонування протоколу здійснюється у змішаному режимі.

Синтаксис команди **crypto key generate** (режим глобального конфігурування):

crypto key generate. Команда не має параметрів.

Синтаксис команди **crypto key generate rsa general-keys modulus** (режим глобального конфігурування):

crypto key generate rsa general-keys modulus ***modulus-value***,

де ***modulus-value*** – значення довжини ключа (бітів), число з діапазону 360 ... 2048; за замовчуванням генеруються ключі довжиною 512 бітів.

Синтаксис команди **crypto key generate rsa usage-keys label** (режим глобального конфігурування):

crypto key generate rsa usage-keys label ***keypair-name-string*** **modulus** ***modulus-value***,

де ***keypair-name-string*** – текстовий рядок, який містить назву ключової пари RSA;

modulus-value – значення довжини ключа (бітів), число з діапазону 360 ... 2048; за замовчуванням генеруються ключі довжиною 512 бітів.

Синтаксис команди **crypto key zeroize** (режим глобального конфігурування):

crypto key zeroize Команда не має параметрів.

Синтаксис команди **crypto key zeroize rsa** (режим глобального конфігурування):

crypto key zeroize rsa *keypair-name-string*,

де ***keypair-name-string*** – текстовий рядок, який містить назву ключової пари RSA.

Основні команди моніторингу та діагностики функціонування протоколів Telnet та SSH на пристроях Cisco

Для перегляду параметрів налагоджень мережних підключень, параметрів роботи протоколів віддаленого доступу та інших параметрів використовуються різні варіанти команд **show**. Перелік основних команд та їх призначення наведені у табл. 2. Для відстеження подій та повідомлень, які генеруються протоколом SSH використовуються команди **debug ip ssh** та **debug ip ssh client**.

Таблиця 2

Перелік команд show, необхідних для діагностики параметрів мережних підключень та параметрів протоколів віддаленого доступу на пристроях Cisco

Команда	Призначення
show line	Виведення інформації про наявні підключення та їх параметри
show sessions	Виведення інформації про параметри вихідних сеансів
show users	Виведення інформації про параметри вхідних підключень (зокрема, мережних) та підключених користувачів
show ssh	Виведення інформації про параметри сеансів протоколу SSH
show ip ssh	Виведення інформації про налагоджені параметри протоколу SSH (версія, час тайм-ауту, кількість спроб аутентифікації тощо)
show login	Виведення узагальненої інформації про налагодження входу в систему
show crypto key mypubkey rsa	Виведення публічного ключа RSA
show crypto key pubkey-chain rsa	Виведення публічного ключа RSA з'єднання, що збережений на комп'ютері.
show crypto key storage	Виведення інформації про місце розміщення ключової пари

show control-plane host open-ports	Виведення інформації про відкриті TCP- та UDP-порти пристрою
show tcp	Виведення детальної інформації про встановлені з'єднання транспортного протоколу TCP (використовується для визначення IP-адрес з'єднань та номерів портів протоколів віддаленого доступу)

Модельний приклад налагодження віддаленого доступу до пристроїв Cisco з використанням протоколу Telnet

Розглянемо специфіку налагодження роботи протоколу віддаленого доступу Telnet для комунікаційних пристроїв мережі, схема якої наведена на рис. 9. У даному випадку підключення здійснюється з робочої станції WS-Control до маршрутизатора R-1 та комутатора SW-1.

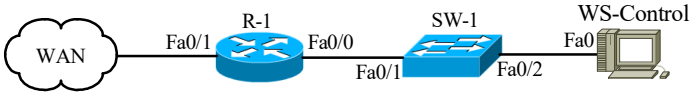


Рис. 9. Приклад мережі

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

Таблиця 3

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R-1	Fa0/0	Комутатор SW-1	Fa0/1
	Fa0/1	WAN	WAN Interface
Комутатор SW-1	Fa0/1	Маршрутизатор R-1	Fa0/0
	Fa0/2	Сервер Serv_A_1	Fa0
WS-Control	Fa0	Комутатор SW-1	Fa0/2

Таблиця 4

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	–	195.10.1.0	255.255.255.0	/24
WAN	–	196.10.1.0	255.255.255.252	/30
Маршрутизатор R-1	Інтерфейс Fa0/0	195.10.1.254	255.255.255.0	/24
	Інтерфейс Fa0/1	196.10.1.2	255.255.255.252	/30
Комутатор SW-1	Інтерфейс Vlan 1	195.10.1.250	255.255.255.0	/24

	Шлюз за замовчуванням	195.10.1.254	–	–
Робоча станція WS-Control	Мережний адаптер	195.10.1.1	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–

Для налагодження параметрів комунікаційних пристроїв із метою забезпечення підключення по протоколами Telnet/SSH використано дані табл. 5.

Таблиця 5

Параметри налагодження комунікаційних пристроїв

Параметр	Значення
Системний час	Поточний
Часовий пояс	Східноєвропейський
Перехід на літній час	Україна
Банер	Connection to router R-1
Кількість підключень VTY	5 (0 … 4)
Інтервал перед виведенням попередження про вихід із системи, с	30
Загальна тривалість сеансу, хв	10
Синхронне виведення журнальних повідомлень на екран	Активоване

Сценарій налагодження часових параметрів, повідомлення попередження та параметрів адресації інтерфейсів для маршрутизатора мережі R-1 наведений нижче. Сценарій налагодження параметрів комутатора мережі SW-1 подібний до сценарію для маршрутизатора R-1.

```
…
R-1>enable
R-1#clock set 10:04:00 11 dec 2022
R-1#configure terminal
R-1(config)#clock timezone EET 2
R-1(config)#clock summertime EET reccuring last monday october 3:00 last monday march 3:00
R-1(config)#banner motd # Connection to router R-1
                          For legal users only #
R-1(config)#interface FastEthernet 0/0
R-1(config-if)#description LINK-TO-LAN-A
R-1(config-if)#ip address 195.10.1.254 255.255.255.0
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#interface FastEthernet 0/1
```

R-1(config-if)#description LINK_TO_WAN
R-1(config-if)#ip address 196.10.1.2 255.255.255.252
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#exit
R-1#
…

Сценарій налагодження віддаленого підключення за протоколом Telnet із входом без пароля (без аутентифікації) для маршрутизатора мережі R-1 наведений нижче. Слід зазначити, що у даному сценарії передбачено прямий перехід у привілейований режим за рахунок встановлення найвищого рівня привілеїв. Сценарій налагодження параметрів комутатора мережі SW-1 подібний до сценарію для маршрутизатора R-1. У практиці експлуатації мереж такий сценарій має обмежене застосування, його рекомендовано застосовувати лише у випадку, коли мережна інфраструктура є надійно захищеною. Якщо існує ймовірність перехоплення інформації під час підключення, то розглянутий сценарій застосовувати не рекомендується.

...
R-1>enable
R-1#configure terminal
R-1(config)#line vty 0 4
R-1(config-line)#no login
R-1(config-line)#transport input telnet
R-1(config-line)#privilege level 15
R-1(config-line)#logout-warning 30
R-1(config-line)#absolute-timeout 10
R-1(config-line)#logging synchronous
R-1(config-line)#exit
R-1(config)#exit
R-1#
...

Сценарій підключення/відключення до маршрутизатора R-1 з робочої станції ОС Windows за допомогою вбудованого термінального додатка Telnet наведено нижче.

```
...
C:>telnet
Добро пожаловать в программу-клиент Microsoft Telnet
Символ переключения режима: 'CTRL+]'
Microsoft Telnet>open 195.10.1.254
```

```
Подключение к 195.10.1.254...
Connection to router R-1
For legal users only
R-1#...
...
R-1#exit
Подключение к узлу утеряно
Нажмите любую клавишу ...
Microsoft Telnet>quit
C:>
...
```

Сценарій налагодження віддаленого підключення за протоколом Telnet до маршрутизатора Cisco з використанням засобів локальної аутентифікації на базі механізму паролів на вхід до відповідних командних режимів пристрою наведений нижче. У даному сценарії застосовані паролі типу 7.

```
...
R-1>enable
R-1#configure terminal
R-1(config)#service password-encryption
R-1(config)#enable secret adminpass2
R-1(config)#line vty 0 4
R-1(config-line)#password adminpass1
R-1(config-line)#login
R-1(config-line)#transport input telnet
R-1(config-line)#logout-warning 30
R-1(config-line)#absolute-timeout 10
R-1(config-line)#logging synchronous
R-1(config-line)#exit
R-1(config)#exit
R-1#
...
```

Сценарій підключення/відключення до маршрутизатора R-1 із робочої станції ОС Windows за допомогою вбудованого термінального додатка Telnet наведено нижче. Слід зазначити, що пароль під час введення не відображається.

```
...
C:>telnet 195.10.1.254
User Access Verificaton
Password:
Connection to router R-1
For legal users only
R-1>enable
Password:
R-1#...
```

```
...
R-1#exit
Подключение к узлу утеряно.
C:>
...
```

Сценарій налагодження віддаленого підключення за протоколом Telnet до маршрутизатора Cisco з використанням засобів локальної аутентифікації на базі механізму користувачів наведений нижче. У даному сценарії застосовані паролі типу 5.

```
…
R-1>enable
R-1#configure terminal
R-1(config)#username adminer privilege 15 secret adminerpass
R-1(config)#username technic privilege 1 secret technicpass
R-1(config)#enable secret adminerpass2
R-1(config)#line vty 0 4
R-1(config-line)#login local
R-1(config-line)#transport input telnet
R-1(config-line)#logout-warning 30
R-1(config-line)#absolute-timeout 10
R-1(config-line)#logging synchronous
R-1(config-line)#exit
R-1(config)#
…
```

Сценарій підключення/відключення до маршрутизатора R-1 з робочої станції Windows за допомогою вбудованого термінального додатка Telnet наведено нижче. Слід зазначити, що пароль при введенні не відображається.

```
...
C:>telnet 195.10.1.254
User Access Verificaton
Username:adminer
Password:
Connection to router R-1
For legal users only
R-1#...
...
R-1#exit
Подключение к узлу утеряно.
```

```
C:>
...
```

Результати виконання команд моніторингу та діагностики роботи протоколу віддаленого доступу Telnet для розглянутого прикладу

З метою перегляду інформації про роботу мережних підключень, параметрів роботи протоколів віддаленого доступу та інших параметрів використовуються як загальні, так і специфічні для певного протоколу команди. Для розглянутого прикладу використано загальні команди **show line**, **show users**, **show tcp**. Результати роботи цих команд для маршрутизатора R-1 наведено відповідно на рис. 10–12. Для перевірки підключення з боку робочої станції Windows використано команду **netstat -n**. Результати роботи цієї команди наведено на рис. 13.

```
    R-1#show line
 Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
    *     0 CTY              -    -      -    -    -      0       0     0/0       -
          1 AUX   9600/9600  -    -      -    -    -      0       0     0/0       -
    *     2 VTY              -    -      -    -    -      2       0     0/0       -
          3 VTY              -    -      -    -    -      0       0     0/0       -
          4 VTY              -    -      -    -    -      0       0     0/0       -
          5 VTY              -    -      -    -    -      0       0     0/0       -
          6 VTY              -    -      -    -    -      0       0     0/0       -
    R-1#
```

Рис. 10. Результат роботи команди **show line** для маршрутизатора R-1

```
    R-1#show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00
   2 vty 0     adminer    idle                 00:00:03 195.10.1.1
  Interface    User               Mode         Idle     Peer Address
```

Рис. 11. Результат роботи команди **show users** для маршрутизатора R-1

```
    R-1#show tcp
    tty2, virtual tty from host 195.10.1.1
    Connection state is ESTAB, I/O status: 1, unread input bytes: 0
    Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
    Local host: 195.10.1.254, Local port: 23
    Foreign host: 195.10.1.1, Foreign port: 1030
```

Рис. 12. Результат роботи команди **show tcp** для маршрутизатора R-1

```
    C:>netstat –n
    Активные подключения
    Имя      Локальный адрес     Внешний адрес       Состояние
    TCP      195.10.1.1:1030     195.10.1.254:23     ESTABLISHED
    C:>
```

Рис. 13. Результат роботи команди **netstat -n** для робочої станції WS-Control

Модельний приклад налагодження віддаленого доступу до пристроїв Cisco з використанням протоколу SSH

Розглянемо специфіку налагодження роботи протоколу віддаленого доступу SSH для комунікаційних пристроїв мережі, схема якої наведена на рис. 9. У даному випадку підключення здійснюється з робочої станції WS-Control до маршрутизатора R-1 та комутатора SW-1. Під час побудови даної мережі для з'єднання пристроїв використано дані табл. 3. Для налагодження параметрів адресації пристроїв використано дані табл. 4. Для налагодження параметрів комунікаційних пристроїв з метою забезпечення підключення за протоколом SSH використано дані табл. 5.

Сценарій налагодження часових параметрів, повідомлення попередження та параметрів адресації інтерфейсів для маршрутизатора мережі R-1 аналогічний сценарію попереднього модельного прикладу. Сценарій налагодження параметрів комутатора мережі SW-1 подібний до сценарію для маршрутизатора R-1.

Сценарій налагодження віддаленого підключення за протоколом SSH до маршрутизатора Cisco з використанням імені пристрою та імені домену та з використанням засобів локальної аутентифікації на базі механізму користувачів наведений нижче. У цьому сценарії застосовані паролі типу 5.

...

R-1>enable
R-1#configure terminal
R-1(config)#username adminer privilege 15 secret adminerpass
R-1(config)#username technic privilege 1 secret technicpass
R-1(config)#enable secret adminerpass2
R-1(config)#ip domain-name mynet.net
R-1(config)#crypto key generate rsa general-keys modulus 1024
R-1(config)#ip ssh version 2
R-1(config)#line vty 0 4

R-1(config-line)#login local
R-1(config-line)#transport input ssh
R-1(config-line)#transport output ssh
R-1(config-line)#logout-warning 30
R-1(config-line)#absolute-timeout 10
R-1(config-line)#logging synchronous
R-1(config-line)#exit
R-1(config)#exit
...

Сценарій налагодження елементів захисту від атак на пристрій та налагодження підсистеми журналювання подій, пов'язаних із вдалими та невдалими спробами SSH-підключень.

...
R-1>enable
R-1#configure terminal
R-1(config)#login block-for 300 attempts 3 within 3
R-1(config)#login delay 5
R-1(config)#login on-failure log
R-1(config)#login on-success log
R-1(config)#ip ssh time-out 60
R-1(config)#ip ssh authentication-retries 5
R-1(config)#ip ssh maxstartups 5
R-1(config)#ip ssh logging events
R-1(config)#exit
R-1#exit
R-1>
...

Для підключення до маршрутизатора R-1 з робочої станції ОС Windows використано термінальний додаток Putty (SuperPutty). Сценарій підключення/відключення за допомогою цього додатка наведений нижче.

```
login as: adminer
Using keyboard-interactive authentification.
Password:
Connection to router R-1
For legal users only
R-1#...
...
R-1#exit
...
```

Сценарій налагодження віддаленого підключення за протоколом SSH до маршрутизатора Cisco з використанням ключових пар RSA

та з використанням засобів локальної аутентифікації на базі механізму користувачів наведений нижче.

```
…
R-1>enable
R-1#configure terminal
R-1(config)#username adminer privilege 15 secret adminerpass
R-1(config)#username technic privilege 1 secret technicpass
R-1(config)#enable secret adminerpass2
R-1(config)#ip ssh rsa keypair-name MySSHkeys
R-1(config)#crypto key generate rsa usage-keys label MySSHkeys modulus 1024
R-1(config)#ip ssh version 2
R-1(config)#line vty 0 4
R-1(config-line)#login local
R-1(config-line)#transport input ssh
R-1(config-line)#transport output ssh
R-1(config-line)#exit
R-1(config)#exit
R-1#
…
```

У Cisco IOS існує можливість виконання підключення з одного пристрою до іншого. Для цього застосовуються вбудовані Cisco IOS Telnet та SSH-клієнти. Приклад сценарію такого підключення з комутатора SW-1 до маршрутизатора R-1 наведений нижче.

```
…
SW-1#ssh -v 2 -l adminer 195.10.1.1
Password:
Connection to router R-1
For legal users only
R-1#
…
```

Слід зазначити, що для виконання подібного сценарію на пристрої повинна бути активована можливість виконання віддалених підключень до інших пристроїв. Ця можливість активується командою **transport output**, у якій зазначається відповідний мережний протокол.

Результати виконання команд моніторингу та діагностики роботи протоколу віддаленого доступу SSH для розглянутого прикладу

З метою перегляду інформації про роботу мережних підключень, параметрів роботи протоколів віддаленого доступу та інших параметрів використовуються як загальні, так і специфічні для певного протоколу команди. Для розглянутого прикладу використано загальні команди **show line**, **show users**, **show tcp** та специфічні команди протоколу SSH **show ssh**, **show ip ssh**, **show crypto key mypubkey rsa**. Результати роботи цих команд для маршрутизатора R-1 (за умови використання імені пристрою та імені домену для підключення) наведено відповідно на рис. 14–19. Для перевірки підключення з боку робочої станції Windows використано команду **netstat -n**. Результати роботи цієї команди наведено на рис. 20.

```
    R-1#show line
Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
    *     0 CTY              -    -      -    -    -      0        0     0/0       -
          1 AUX   9600/9600  -    -      -    -    -      0        0     0/0       -
    *     2 VTY              -    -      -    -    -      2        0     0/0       -
          3 VTY              -    -      -    -    -      0        0     0/0       -
          4 VTY              -    -      -    -    -      0        0     0/0       -
          5 VTY              -    -      -    -    -      0        0     0/0       -
          6 VTY              -    -      -    -    -      0        0     0/0       -
    R-1#
```

Рис. 14. Результат роботи команди **show line** для маршрутизатора R-1

```
    R-1#show users
        Line       User       Host(s)              Idle       Location
    *  0 con 0                 idle                 00:00:00
       2 vty 0     adminer    idle                 00:02:57 195.10.1.1
      Interface    User               Mode         Idle     Peer Address
    R-1#
```

Рис. 15. Результат роботи команди **show users** для маршрутизатора R-1

```
    R-1#show tcp
    tty2, virtual tty from host 195.10.1.1
    Connection state is ESTAB, I/O status: 1, unread input bytes: 0
    Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
```

```
Local host: 195.10.1.254, Local port: 22
Foreign host: 195.10.1.1, Foreign port: 1030
...

R-1#
```

Рис. 16. Результат роботи команди **show tcp** для маршрутизатора R_2

```
R-1#show ssh
Connection Version Mode Encryption  Hmac         State                Username
0          2.0     IN   aes256-cbc  hmac-sha1    Session started      adminer
0          2.0     OUT  aes256-cbc  hmac-sha1    Session started      adminer
%No SSHv1 server connections running.
R-1#
```

Рис. 17. Результат роботи команди **show ssh** для маршрутизатора R-1

```
R-1#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 5
Minimum expected Diffie Hellman key size : 1024 bits
R-1#
```

Рис. 18. Результат роботи команди **show ip ssh** для маршрутизатора R-1

```
R-1#show crypto key mypubkey rsa
% Key pair was generated at: 22:49:37 UTC Jan 18 2017
Key name: R-1.mynet.net
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B1BDCC
  97462A4E F581491B A8F0A289 8E2EBA0C 247844A8 B53BCF0A 94700F5D 496E9E71
  541451BD C2BFFD6F 10FEFC02 5A18712C 7755EF54 1816AD97 F11F4694 8EE277A0
  FFA1F692 3D140EC6 813433A7 22C9A27C 72F3911F 6904313B 5919AA43 F086EA34
  1F4625A6 C50CC5AF CA072709 E94E2DFF 884564C2 00D43780 6D43475C 45020301 0001
% Key pair was generated at: 22:49:38 UTC Jan 18 2017
Key name: R-1.mynet.net.server
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 0091A903 3A23444A
  0A4DAB64 6C1C3250 2661F503 328A9A3B 54B618E2 8FF0CF0B 6461FF1E CEDD0DB6
  4BC54A5B BD97A159 B6C82E7E E5A560C9 CCCFDB40 B7F8F898 EE3CC2E5 F1B2B716
  741B9063 DE7EB172 E2C59F81 F851A229 99450322 D2224140 91020301 0001
R-1#
```

Рис. 19. Результат роботи команди **show crypto key mypubkey rsa** для маршрутизатора R-1

```
C:>netstat –n
Активные подключения
Имя      Локальный адрес     Внешний адрес       Состояние
TCP      195.10.1.1:1030     195.10.1.254:22     ESTABLISHED
C:>
```

Рис. 20. Результат роботи команди **netstat -n** для робочої станції WS-Control

Завдання на лабораторну роботу

1. У середовищі програмного симулятора/емулятора створити проект мережі (рис. 21). Під час побудови звернути увагу на вибір моделей комутаторів та маршрутизаторів, мережних модулів та адаптерів, а також мережних з'єднань. Для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 3.

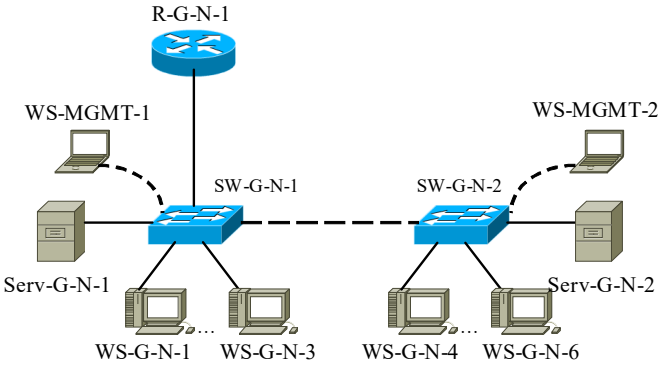


Рис. 21. Проект мережі

2. Розробити схему адресації пристроїв мережі. Для цього використовувати дані табл. 6. Результати навести у вигляді таблиці, яка аналогічна табл. 4.

3. Провести базове налагодження пристроїв, інтерфейсів та каналів зв'язку. Провести налагодження параметрів IP-адресації пристроїв мережі відповідно до даних, які отримані у п. 2.

4. Перевірити наявність зв'язку між всіма пристроями мережі

5. Провести налагодження віддаленого доступу до пристроїв мережі згідно з даними табл. 7 (за потреби створити користувачів на пристроях, рівень їх привілеїв встановити довільним чином)..

6. Дослідити процеси віддаленого доступу до налагоджених у п. 5 комунікаційних пристроїв. У разі відсутності доступу визначити проблеми та усунути їх.

7. Для маршрутизатора мережі, на якому налагоджено підключення з використанням засобів локальної аутентифікації на базі механізму користувачів, налагодити можливість підключення як за допомогою протоколу Telnet, так і за допомогою протоколу SSH.

Дослідити можливості підключення до налагодженого пристрою за допомогою додатка Putty або подібного.

8. Дослідити та проаналізувати відмітності віддаленого доступу за протоколом Telnet і за протоколом SSH у розрізі передачі даних аутентифікації та передачі даних сеансу зв'язку. Для перехоплення повідомлень використати штатні засоби програмного симулятора/емулятора або програмного аналізатор трафіка WireShark (за можливості).

Таблиця 6

Параметри IP-адресації мережі

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

30	220.G.N.0	/28	Остання IP-адреса діапазону
31	221.G.N.0	/24	Перша IP-адреса діапазону
32	222.G.N.0	/25	Остання IP-адреса діапазону
33	223.G.N.0	/26	Перша IP-адреса діапазону

Таблиця 7

Дані для вибору протоколів віддаленого доступу

№ варіанта	Протоколи віддаленого доступу		
	R-G-N-1	SW-G-N-1	SW-G-N-2
1	Telnet&Pwd	Telnet&User	SSHv1
2	Telnet&User	SSHv1	Telnet&Pwd
3	SSHv1	Telnet&Pwd	Telnet&User
4	Telnet&Pwd	Telnet&User	SSHv2
5	Telnet&User	SSHv2	Telnet&Pwd
6	SSHv2	Telnet&Pwd	Telnet&User
7	Telnet&Pwd	Telnet&User	SSHv1
8	Telnet&User	SSHv1	Telnet&Pwd
9	SSHv1	Telnet&Pwd	Telnet&User
10	Telnet&Pwd	Telnet&User	SSHv2
11	Telnet&User	SSHv2	Telnet&Pwd
12	SSHv2	Telnet&Pwd	Telnet&User
13	Telnet&Pwd	Telnet&User	SSHv1
14	Telnet&User	SSHv1	Telnet&Pwd
15	SSHv1	Telnet&Pwd	Telnet&User
16	Telnet&Pwd	Telnet&User	SSHv2
17	Telnet&User	SSHv2	Telnet&Pwd
18	SSHv2	Telnet&Pwd	Telnet&User
19	Telnet&Pwd	Telnet&User	SSHv1
20	Telnet&User	SSHv1	Telnet&Pwd
21	SSHv1	Telnet&Pwd	Telnet&User
22	Telnet&Pwd	Telnet&User	SSHv2
23	Telnet&User	SSHv2	Telnet&Pwd
24	SSHv2	Telnet&Pwd	Telnet&User
25	Telnet&Pwd	Telnet&User	SSHv1
26	Telnet&User	SSHv1	Telnet&Pwd
27	SSHv1	Telnet&Pwd	Telnet&User
28	Telnet&Pwd	Telnet&User	SSHv2
29	Telnet&User	SSHv2	Telnet&Pwd
30	SSHv2	Telnet&Pwd	Telnet&User
31	Telnet&Pwd	Telnet&User	SSHv1
32	Telnet&User	SSHv1	Telnet&Pwd
33	SSHv1	Telnet&Pwd	Telnet&User

Примітка: Telnet&Pwd – підключення за протоколом Telnet із використанням засобів локальної аутентифікації на базі механізму паролів на вхід до відповідних командних режимів; Telnet&User – підключення за протоколом Telnet із використанням засобів локальної аутентифікації на базі механізму користувачів; SSHv1, SSHv2 – підключення за протоколом SSH відповідних версій із використанням засобів локальної аутентифікації на базі механізму користувачів.

Контрольні питання

1. Поняття та призначення протоколу віддаленого доступу.
2. Основні протоколи віддаленого доступу.
3. Загальна характеристика протоколів Telnet та SSH.
4. Сфера застосування протоколів Telnet та SSH.
5. Стандартизація протоколів Telnet та SSH.
6. Характеристики протоколів Telnet та SSH стосовно моделі OSI та стеку TCP/IP.
7. Рівні протоколу SSH.
8. Характеристика рівня безпеки протоколу Telnet.
9. Характеристика рівня безпеки протоколу SSH.
10. Реалізація протоколів Telnet та SSH у сучасних ОС.
11. Реалізація протоколів Telnet та SSH провідними виробниками мережного обладнання.
12. Перелік та призначення основних команд для налагодження протоколу Telnet на пристроях Cisco.
13. Перелік та призначення основних команд моніторингу роботи протоколу Telnet на пристроях Cisco.
14. Перелік та призначення основних команд для налагодження протоколу SSH на пристроях Cisco.
15. Перелік та призначення основних команд моніторингу роботи протоколу SSH на пристроях Cisco.

СПИСОК ЛІТЕРАТУРИ

1. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 334 с.

2. Буров Є.В. Комп'ютерні мережі. Підручник. Том 2. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 204 с.

3. Микитишин А.Г. Комп'ютерні мережі. Книга 1. Навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник – Львів, «Магнолія 2006», 2013. – 256 с.

4. Микитишин А.Г. Комп'ютерні мережі. Книга 2. Навчальний посібник. / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів, «Магнолія 2006», 2013. – 328 с.

5. Odom Wendell. CCNA 200-301 Official Cert Guide. Volume 1. / Wendell Odom. Cisco Press, 2020. – 1095 p.

6. Odom Wendell. CCNA 200-301 Official Cert Guide. Volume 2. / Wendell Odom. Cisco Press, 2020. – 1444 p.

7. Навчальний курс CCNAv7: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

8. Навчальний курс CCNAv7: Switching, Routing, and Wireless Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.

9. Навчальний курс CCNAv7: Enterprise Networking, Security, and Automation [Електронний ресурс] – Режим доступу: www.netacad.com.

10. Навчальний курс CCNA Routing and Switching: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

11. Навчальний курс CCNA Routing and Switching: Routing and Switching Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.

12. Навчальний курс CCNA Routing and Switching: Scaling Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

13. Навчальний курс CCNA Routing and Switching: Connecting Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

Н а в ч а л ь н о - м е т о д и ч н е в и д а н н я

КОМП'ЮТЕРНІ МЕРЕЖІ

Частина 1

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
ДЛЯ ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

Підготували
Воротніков Володимир Володимирович
Єфіменко Андрій Анатолійович
Дячук Ольга Юріївна
Колощук Марія Сергіївна

Редактор
Комп'ютерне верстання – **А. А. Єфіменко**

Свідоцтво про реєстрацію № __ від _____ 20__ року
Підписано до друку __.__.16. Формат 60×84/16.
Ум. друк. арк. ____. Зам. __ офс.

Безкоштовно

Друкарня Державного університету «Житомирська політехніка»