Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С.,
Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А.

КОМП'ЮТЕРНІ МЕРЕЖІ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

І К Т

КОМП'ЮТЕРНІ МЕРЕЖІ

Київ
2017

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем і мереж

Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С.,
Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А.

КОМП'ЮТЕРНІ МЕРЕЖІ

навчальний посібник
з дисципліни «Комп'ютерні мережі»

КОМПРІНТ
КИЇВ - 2017

УДК 004.7(072)
ББК 32.97
К 63

Рекомендовано до друку Вченою радою Національного університету біоресурсів і природокористування України (протокол № 4 від 22.11.2017 р.)

Рецензенти:

Лахно В.А. - доктор технічних наук, професор, професор кафедри інформаційних систем та математичних дисциплін ПВНЗ «Європейський університет»;

Ляшенко С.А. - доктор технічних наук, професор кафедри безпеки життєдіяльності, директор центру дистанційного навчання Харківського національного технічного університету сільського господарства ім. П. Василенка;

Болбот І.М. - кандидат технічних наук, доцент кафедри автоматики та робототехнічних систем ім. акад. І.І. Мартиненка Національного університету біоресурсів і природокористування України.

Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А.

К 63 **Комп'ютерні мережі** [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька // - К.: Компрінт, 2017.- 821с.

Навчальний посібник призначений для студентів вищих навчальних закладів ОС «Бакалавр» за спеціальностями «Комп'ютерна інженерія», «Інженерія програмного забезпечення», які вивчають дисципліну «Комп'ютерні мережі». Матеріали посібника підготовлені на основі методологічних досліджень авторів та відповідного курсу лекцій, Посібник містить теоретичний матеріал, який надає можливість сформувати уявлення стосовно взаємозв'язку комп'ютерних мереж та інформаційних технологій, програмних засобів та схем зєднань. Представлений теоретичний матеріал доповнено практичними роботами з використанням сучасних програмних методів.

ЗМІСТ

1. Розділ Загальні принципи побудови інформаційно-комунікаційних мереж

1.1. Введення в комп’ютерні мережі та основні протоколи мережі.

Серед основних потреб людини необхідність взаємодії з іншими людьми - одна з найважливіших. Спілкування майже так само важливо для нас, як повітря, вода, їжа і дах.

У сучасному світі за рахунок використання мереж ми пов'язані один з одним, як ніколи раніше. Люди з творчими ідеями можуть миттєво зв'язуватися з іншими людьми і втілювати свої ідеї в реальність. Новини та відкриття стають відомими у всьому світі в лічені секунди. Ми можемо виходити в мережу і грати в ігри з іншими людьми, що знаходяться на інших континентах.

Уявіть собі світ без Інтернету. Більше немає Google, YouTube, обміну миттєвими повідомленнями, Facebook, Вікіпедії, онлайн-ігор, Netflix, iTunes і легкого доступу до поточної інформації. Немає сайтів порівняння цін, не можна купувати товари через Інтернет і не стояти за ними в черзі, неможливо швидко знайти телефонні номери і подивитися маршрут одним клацанням миші. Як би ми жили без усього цього? Але ж так було всього лише 15-20 років тому. Але за ці роки мережі передачі даних поступово розширювалися і міняли своє призначення, покращуючи якість життя людей усього світу.

Досягнення в мережевих технологіях, мабуть, є одними з найбільш значних змін в світі. Мережі створюють світ, в якому кордони країн, відстані і фізичні кордони перестають мати значення і становлять все менше перешкод.

Інтернет змінив характер соціального, комерційного, політичного і особистого взаємодії. Можливість миттєвих комунікацій через Інтернет сприяє створенню глобальних спільнот. Глобальні спільноти забезпечують соціальну взаємодію незалежно від місця розташування або часового поясу. Інтернет-спільноти для обміну ідеями та інформацією можуть підвищити ефективність взаємодії по всьому світу.

Мережі змінили наш спосіб навчання. Отримати послуги висококваліфікованих викладачів тепер можуть не тільки студенти, які проживають в безпосередній близькості від освітнього закладу. Натисніть кнопку «Відтворення» на відео, щоб подивитися відеоролик про зміни, що відбулися в навчальних класах.

Дистанційне навчання не знає географічних перешкод і дозволяє надати учням більше можливостей. Надійні і стійко працюють мережі роблять процес навчання ефективніше. З їх допомогою можна надавати навчальні матеріали в самих різних форматах, включаючи інтерактивні заняття, контрольні роботи та зворотний зв'язок.

Глобалізація Інтернету привела до виникнення нових форм спілкування, які дають людям можливість створювати інформацію, доступну глобальної аудиторії.

Миттєвий обмін повідомленнями забезпечує безпосередній зв'язок в режимі реального часу між двома або більше учасниками.

Соціальні мережі - інтерактивні веб-сайти, де люди і спільноти створюють свій контент і діляться ним з друзями, близькими, колегами і всім світом.

Інструменти спільної роботи - у відсутності обмежень, пов'язаних з місцем розташування або часовим поясом, інструменти спільної роботи дозволяють співробітникам спілкуватися один з одним (часто через інтерактивне відео в режимі реального часу). Широке поширення мереж передачі даних означає, що користувачі в віддалених регіонах можуть брати участь в громадській, науковій, соціального життя також, як і користувачі в великих населених пунктах.

Блоги (скорочення від «веб-логи») - веб-сторінки, які можна легко оновлювати і редагувати. На відміну від комерційних веб-сайтів блоги дають можливість донести свої думки до глобальної аудиторії будь-якій людині без особливих технічних знань в області створення сайтів.

Вікі-ресурси, вики - це веб-сторінки, які групи людей можуть змінювати і переглядати разом. При цьому блог - це, скоріше, персональний щоденник, тоді як вікі-сторінку створюють разом. Таким чином з'являються більше можливостей для перевірки і редагування. Багато компаній використовують вики в якості інструменту організації внутрішньої спільної роботи.

Подкасти - записи, якими люди діляться з широкою аудиторією. Аудіофайл розміщують на веб-сайті (або в блозі або в розділі вики), звідки інші користувачі можуть його завантажити і відтворювати на комп'ютері, ноутбуці і інших мобільних пристроях.

Обмін файлами через однорангові мережі (Peer-to-peer, P2P) дозволяє обмінюватися файлами один з одним, не зберігаючи їх на центральному сервері. Користувачі підключаються до мережі P2P шляхом установки програмного забезпечення P2P. Спільний доступ до файлів P2P був прийнятий не всіма. Багато хто стурбований тим, що таким чином порушуються закони про захист авторських прав.

У діловому світі мережі передачі даних спочатку використовувалися для управління фінансовою інформацією, інформацією про замовника і системою нарахування заробітної плати. Ці комерційні мережі розвивалися і робили можливим надання різних типів інформаційних послуг, таких як електронна пошта, відео, обмін повідомленнями і телефонія.

Все більше поширюється використання мереж для ефективного і економічно вигідного навчання співробітників. Можливості онлайн-навчання дозволяють скоротити тривалі і дорогі відрядження, при цьому забезпечується гарантія того, що всі співробітники будуть безпечно і ефективно підготовлені до виконання своєї роботи.

Інтернет використовується для традиційних форм розваг. Ми слухаємо записи виконавців, дивимося кінофільми, читаємо книги і завантажуємо матеріали, щоб в подальшому скористатися ними в оффлайн режимі. Спортивні заходи та концерти можна дивитися в реальному часі, а також записувати і переглядати за запитом.

Мережі допомагають створювати нові форми розваг, наприклад онлайн-ігри. Користувачі змагаються у всіх іграх, які тільки можуть вигадати

розробники. Онлайн-ігри настільки реальні, що нам здається, ніби ми знаходимося з іншими гравцями в одному приміщенні.

Завдяки спільній роботі в мережі зростає і наша активність в реальному житті. Значно зросла кількість глобальних спільнот за інтересами. Ми ділимося враженнями і захопленнями з людьми, які знаходяться далеко від нас. Спортивні вболівальники обмінюються думками та новинами, пов'язаними з їх улюбленими командами. Колекціонери розміщують цінні колекції в Інтернеті і отримують про них відгуки від фахівців.

Який би спосіб для відпочинку та розваг ми не вибрали, мережі допоможуть нам отримати ще більше задоволення!

Існують мережі будь-якого розміру, починаючи від простих мереж з двох комп'ютерів і до систем, що з'єднують мільйони пристроїв. Натисніть на зображення на малюнку, щоб прочитати про мережах різних розмірів.

У невеликих домашніх мережах можливо організувати загальний доступ до ресурсів, таким як принтери, документи, зображення, музика.

Мережі малих і домашніх офісів часто налаштовують люди, які працюють з дому або віддаленого офісу і яким необхідне підключення до корпоративної мережі або іншим централізованим ресурсів. Крім того, індивідуальні підприємці використовують мережі малого та домашнього офісу в рекламних цілях і для продажу продукції, замовлення витратних матеріалів та взаємодії з клієнтами.

На підприємствах і в великих організаціях мережі можуть використовуватися в ще більш широкому масштабі, щоб співробітники могли збирати, зберігати і отримувати інформацію на мережевих серверах. Крім того, мережі дозволяють налагодити швидкий зв'язок між співробітниками через електронну пошту, обмін миттєвими повідомленнями, а також за допомогою інструментів спільної роботи. Крім забезпечення переваг усередині організації більшість компаній також використовує мережі для надання продуктів і послуг замовникам через Інтернет.

На сьогоднішній день Інтернет є найбільшою мережею світу. Насправді поняття «Інтернет» означає «мережу всіх мереж». Інтернет буквально являє собою об'єднання підключених один до одного приватних і загальнодоступних мереж (деякі з них були описані вище).

Всі комп'ютери, підключені до мережі і безпосередньо беруть участь в обміні даними, вважаються вузлами. Вузли також називають кінцевими пристроями.

Сервери - це комп'ютери з встановленим програмним забезпеченням, що дозволяє надавати дані (наприклад, доступ до електронної пошти або веб-сторінок) іншим кінцевим пристроям в мережі. Для роботи кожної служби необхідно окреме серверне програмне забезпечення. Наприклад, для роботи веб-служб в мережі на вузлі повинно бути встановлено ПО веб-сервера. Комп'ютер з серверним програмним забезпеченням може одночасно обслуговувати один або кілька клієнтів. Крім того, на одному комп'ютері можна паралельно встановити декілька типів серверного ПО. У домашніх або невеликих корпоративних мережах одному комп'ютеру доводиться виступати в якості файлового сервера, веб-сервера і сервера електронної пошти.

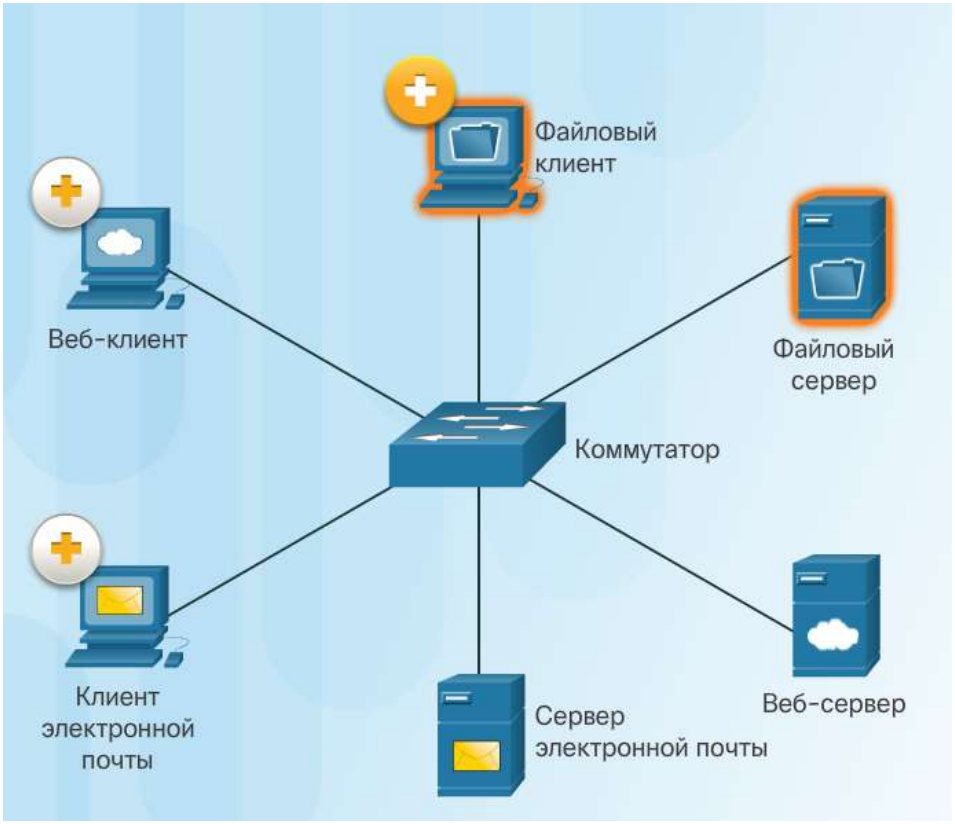


Рис. 1.1.1 – Зразок мережевого з'єднання

Клієнти - це комп'ютери з встановленим програмним забезпеченням, яке дозволяє їм запитувати і відображати інформацію, отриману з сервера. Прикладом клієнтського програмного забезпечення є веб-браузер, наприклад Chrome або FireFox. Крім того, на одному комп'ютері можна запускати кілька типів клієнтського програмного забезпечення. Наприклад, у користувача є можливість перевіряти електронну пошту, переглядати веб-сторінки, обмінюватися миттєвими повідомленнями і слухати інтернет-радіо.

Зазвичай клієнтське і серверне програмне забезпечення запускається на різних комп'ютерах, але ці ролі може грати і один комп'ютер. У невеликих корпоративних і домашніх мережах багато комп'ютерів працюють і як сервери, і як клієнти. Такі мережі називаються одноранговых.

Рис. 1.1.2 Одноранговa мережа

Переваги і недоліки одноранговых мереж показані на малюнку

Маршрут, за яким повідомлення йде від джерела до місця призначення, може бути простим (наприклад, один кабель, що з'єднує один комп'ютер з іншим), або складним (наприклад, мережі, буквально охоплюють весь світ).

Така мережева інфраструктура забезпечує стабільний і надійний канал для передачі даних.

Мережева інфраструктура включає в себе три категорії компонентів мережі:

- пристрої
- средств підключення
- сервіси

Натисніть кожну з кнопок на малюнку, щоб виділити відповідні компоненти мережі.

Пристрої й засоби підключення - це фізичні елементи або апаратне забезпечення мережі. Апаратне забезпечення часто є видимою частиною мережевий платформи: ноутбук, ПК, комутатор, маршрутизатор, бездротова точка доступу або кабелі, які використовуються для з'єднання пристроїв.

Сервіси включають в себе безліч мережевих додатків, які люди використовують щодня, наприклад сервіси електронної пошти та веб-хостингу. Процеси забезпечують функціональність, за допомогою якої повідомлення будуть відправлені і переміщаються в межах мережі. Процеси менш очевидні для нас, але критично важливі для роботи мереж.

Мережеві пристрої, з якими користувачі знайомі найкраще, називаються кінцевими пристроями. Приклади кінцевих пристроїв представлені на рис. 1.2

Кінцевий пристрій є або відправником (джерелом), або одержувачем (адресатом) повідомлення, переданого по мережі. Кожному кінцевого пристрою в мережі призначається адреса, щоб пристрої можна було відрізнити. Якщо термінал ініціює обмін даними, то в якості одержувача повідомлення воно використовує адресу кінцевого пристрою призначення.

Проміжні пристрої з'єднують окремі кінцеві пристрої з мережею і можуть поєднувати кілька окремих мереж для створення об'єднаної мережі. Такі пристрої забезпечують підключення та проходження потоків даних по мережі.

Рис. 1.1.3 Проміжні пристрої мережі.

Для визначення шляху передачі повідомлення проміжні пристрої використовують адресу кінцевого пристрою призначення в поєднанні з інформацією про зв'язки в мережі. Приклади поширених проміжних пристроїв і перелік їх функцій показані на малюнку.

Зв'язок в мережі здійснюється через середовища передачі даних Засіб підключення надає собою канал, по якому повідомлення передається від джерела до адресата.

У сучасних мережах в основному використовуються три типи засобів підключення, що зв'язують пристрої і забезпечують маршрут передачі даних. Як показано на рис. 1, це такі кошти підключення.

Металеві дроти в кабелях - дані кодуються в електричні імпульси.

Скляні або пластикові волокна (оптоволоконний кабель) - дані кодуються в світлові імпульси.

Бездротова передача - дані кодуються за допомогою електромагнітних хвиль радіочастотного діапазону.

Типи засобів підключення розрізняються можливостями і перевагами. Засоби мережевого підключення даних мають різні характеристики і виконують різні завдання.

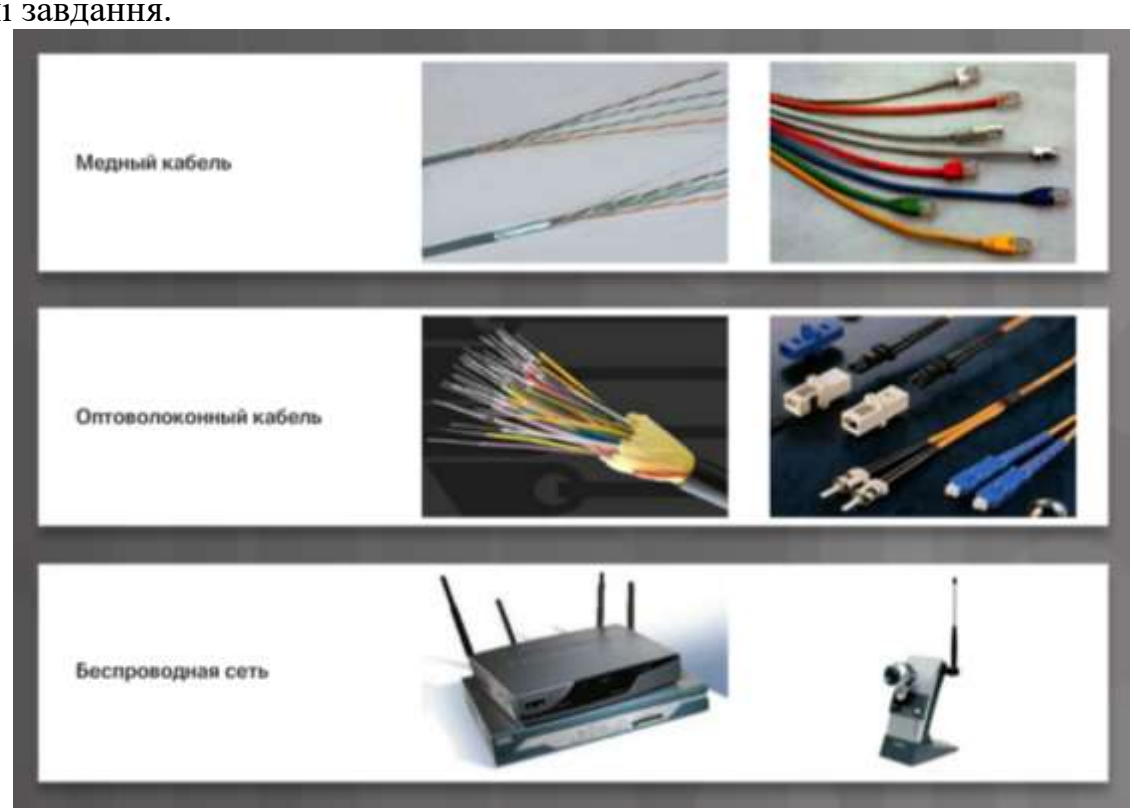


Рис. 1.1.4 Фізичне підключення мережі

Для представлення різних пристроїв і каналів, з яких складається мережа, на схемах мереж часто використовуються символи, такі як на рис. 1. Схема забезпечує наочний спосіб розуміння, яким чином пристрої у великій мережі пов'язані між собою. Цей тип зображення мережі називається схемою топології. Здатність розуміти логічні уявлення фізичних мережевих компонентів має критичне значення в візуалізації організації і функціонування мережі.

Крім цього під час обговорення способів підключення пристроїв і засобів підключення один до одного використовується спеціалізована термінологія.

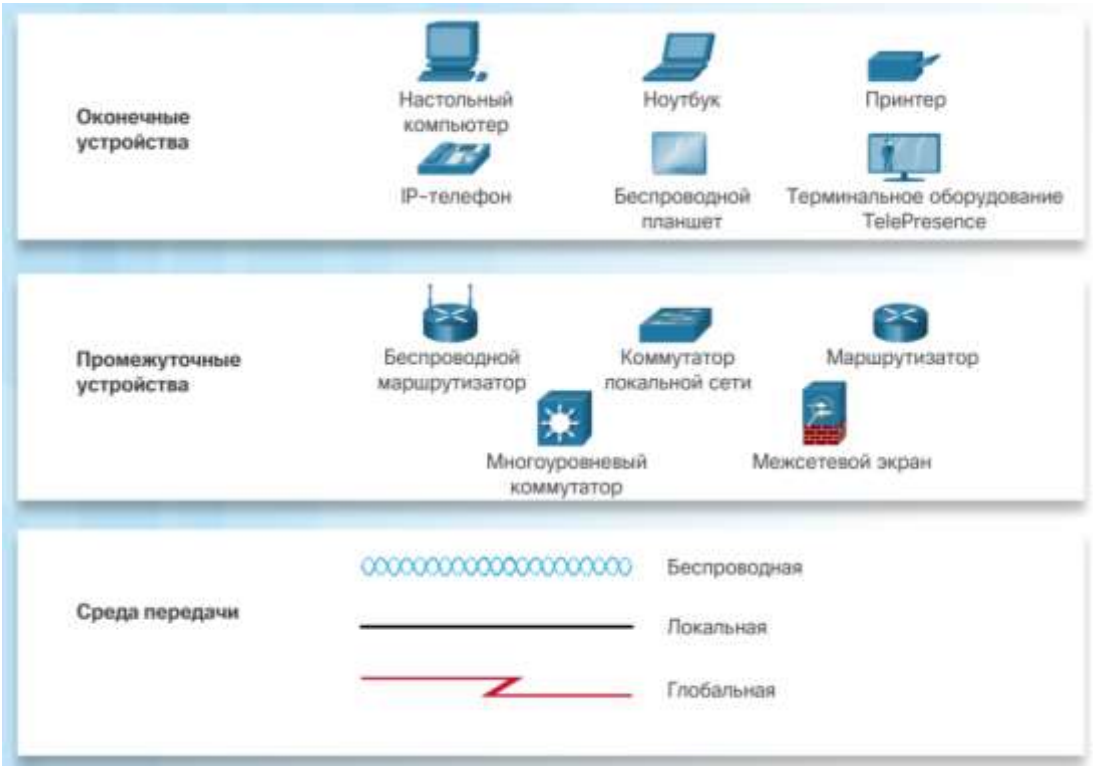


Рис. 1.1.5 Пристрої мережі

Мережева інтерфейсна плата (Network Interface Card, NIC) - інтерфейсна плата або адаптер мережі LAN, який забезпечує фізичне підключення до мережі на настільному комп'ютері або іншому пристрої. Засіб підключення, що з'єднує комп'ютер з мережевим пристроєм, підключається безпосередньо до мережевої плати.

Фізичний порт - роз'єм на мережевому пристрої, через який кабелі підключені до комп'ютера або іншого мережевого пристрою.

Інтерфейс - спеціалізовані порти в мережевому пристрої, які підключаються до окремих мереж. Оскільки маршрутизатори використовуються для зв'язування мереж, порти маршрутизатора називаються мережевими інтерфейсами.

Топологічні схеми необхідні кожному, хто працює з мережею. Вони представляють візуальну карту з'єднань в мережі.

Рис. 1.1.6 Фізична топологія мережі

Рис. 1.1.7 Логічна топологія мережі

Схеми фізичної топології - фізичне розташування проміжних пристроїв і кабельних ліній. (Рис. 1)

Схеми логічної топології - визначення пристроїв, портів і схеми адресації.

Мережеві інфраструктури можуть значно відрізнятися за наступними критеріями.

- Розмір площі покриття
- Кількість підключених користувачів
- Кількість і типи доступних служб
- область відповідальності

Локальна мережа (LAN) - мережева інфраструктура, що надає доступ користувачам і кінцевим пристроям на невеликій території; зазвичай є домашньою мережею, мережею малого або великого підприємства, управляється однією особою або IT-відділом і належить їм.

Глобальна мережа (WAN) - мережева інфраструктура, що надає доступ до інших мереж на великій території; зазвичай належить провайдерам телекомунікаційних послуг і знаходиться під їх управлінням.

Міська мережа (Metropolitan Area Network, MAN) - мережева інфраструктура, яка охоплює територію більше, ніж локальна мережа, але менше глобальної мережі (наприклад, місто). Як правило, управляє міськими мережами одна організація, наприклад великий мережевий оператор.

Бездротові локальні мережі (WLAN) - аналогічні локальних мереж, але з'єднують користувачів і кінцеві пристрої на невеликій території за допомогою бездротового зв'язку.

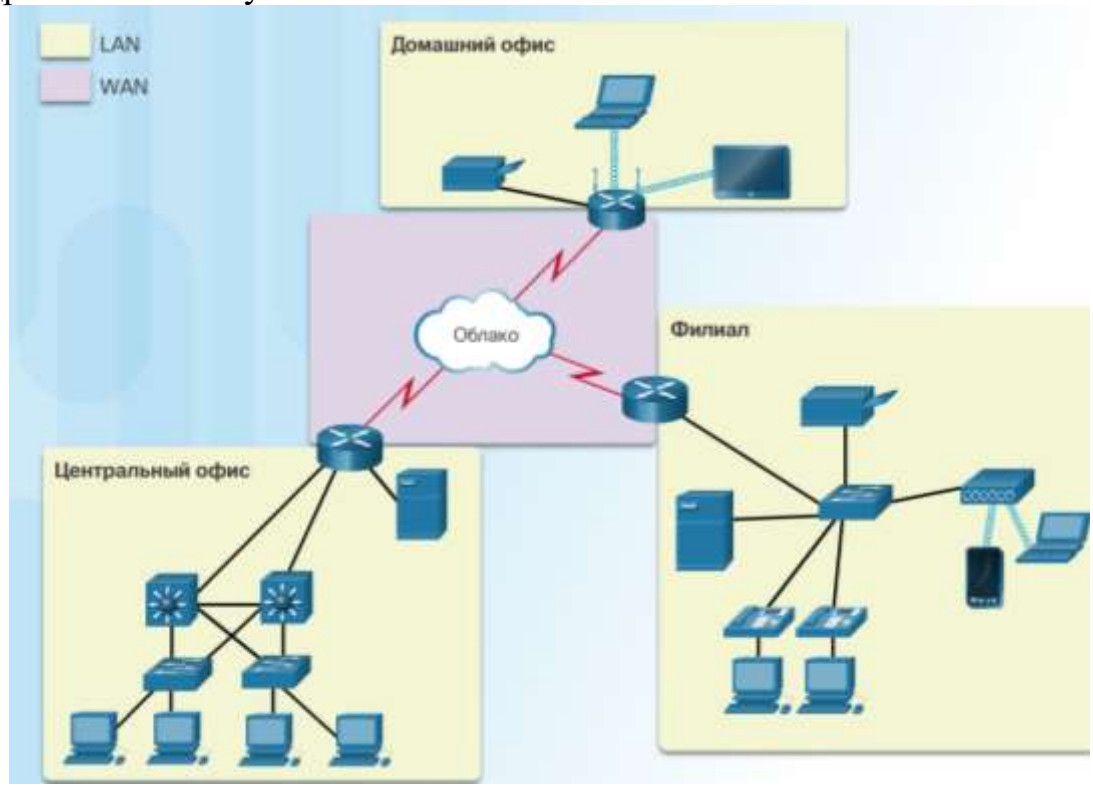


Рис. 1.1.8 Схема об'єднання локальних мереж у глобальні мережі

Мережа зберігання даних (SAN) - мережева інфраструктура, розроблена для підтримки файлових серверів, зберігання даних, їх отримання з сховища і реплікації.

Мережі LAN - мережева інфраструктура, яка охоплює невелику територію. Особливості мереж LAN.

Мережі LAN пов'язують кінцеві пристрої в обмеженій області, наприклад в будинку, школі, офісній будівлі або комплексі будівель.

Мережі LAN зазвичай адмініструє одна організація або приватна особа. Адміністратор управляє політикою безпеки і контролем доступу на мережевому рівні.

Мережі LAN надають високошвидкісний доступ до внутрішніх кінцевим і проміжним пристроїв.

Глобальні мережі - мережева інфраструктура, яка охоплює велику територію. Глобальними мережами зазвичай керують оператори зв'язку (SP) або Інтернет-провайдери (ISP).

Особливості глобальних мереж.

Мережі WAN пов'язують локальні мережі в великих географічних областях, таких як міста, штати, регіони, країни або континенти.

Керують глобальними мережами зазвичай різні оператори зв'язку.

Мережі WAN зазвичай забезпечують менш швидкісні з'єднання між локальними мережами.

Інтернет - це об'єднання взаємопов'язаних мереж в світовому масштабі. На даному малюнку Інтернет показаний як об'єднання підключених один до одного мереж LAN і WAN. Деякі мережі LAN в прикладі безпосередньо з'єднуються між собою через мережу WAN. Потім глобальні мережі з'єднуються між собою. Червоні лінії з'єднання глобальних мереж відображають все розмаїття способів підключення мереж. Глобальні мережі можуть з'єднуватися один з одним за допомогою мідних проводів, оптоволоконного кабелю і бездротової передачі даних.

Інтернет не належить будь-якій особі або групі людей. Забезпечення ефективного спілкування за допомогою такої різноманітної інфраструктури вимагає застосування послідовних і загальновизнаних технологій і стандартів, а також спільної роботи багатьох установ, що адмініструють мережі. Питаннями регулювання структури і стандартизації протоколів і процесів Інтернету займаються спеціальні організації. Ці організації включають в себе Інженерну групу з розвитку Інтернету (Internet Engineering Task Force, IETF), Асоціацію з присвоєння імен і номерів портів (International Corporation for Assigned Names and Numbers, ICANN) і Рада з архітектури мережі Інтернет (Internet Architecture Board, IAB) , а також багато інших.

Примітка. Термін internet (з малої літери і) використовується в англійській мові для опису декількох підключених один до одного мереж. Глобальну систему взаємопов'язаних комп'ютерних мереж і доступу позначають терміном Internet (з великої літери).

Мережі Інтранет і Екстранет

Два інших терміни, схожих з терміном «Інтернет»

- інтранет
- екстранет

Термін «Інтранет» часто використовується для позначення приватних мереж LAN і WAN, які належать організації і доступні тільки її членам, співробітникам і іншим авторизованим особам.

Організація може використовувати Екстранет для захищеного і безпечного доступу співробітників, які працюють в інших організаціях, але яким необхідний доступ до даних компанії. Приклади мереж Екстранет.

- Компанія, що надає доступ зовнішнім постачальникам або підрядникам.
- Лікарня, де використовується система запису до лікарів, які мають можливість призначати дату прийому пацієнтів.
- Місцеве управління освіти, яке надає школам свого району дані про розмір бюджету і кадрах.

Існує безліч способів підключення користувачів і організацій до Інтернету.

Домашні користувачі, віддалені співробітники компаній і малі офіси, як правило, для доступу в Інтернет потребують підключення до постачальників

послуг Інтернету. Варіанти підключення істотно змінюються в залежності від інтернет-провайдера і географічного розташування. Однак популярні варіанти включають в себе широкосмугову кабельну мережу, широкосмуговий цифрову абонентську лінію (DSL), бездротові глобальні мережі і мобільні сервіси.

Організаціям зазвичай потрібен доступ до інших корпоративних вузлів і Інтернету. Для бізнес-сервісів, в тому числі веб-конференцій, IP-телефонів, центрів обробки та зберігання даних потрібні швидкі з'єднання.

Канали для бізнесу зазвичай надаються операторами зв'язку. Популярні послуги бізнес-класу включають DSL, орендовані лінії і мережу Metro Ethernet.

Інтернет-підключення для дому та невеликого офісу

Кабельне підключення - зазвичай пропонують постачальники послуг кабельного телебачення. Дані передаються по тому ж кабелю, який використовується для передачі сигналів кабельного телебачення. Цей спосіб забезпечує підключення до Інтернету з високою пропускною здатністю і постійним доступом до мережі.

DSL - цифрова абонентська лінія забезпечує підключення до Інтернету з високою пропускною здатністю і постійним доступом до мережі. DSL використовує телефонні лінії зв'язку. Зазвичай невеликі і домашні офіси використовують асиметричні лінії DSL (ADSL), в яких дані користувачеві передаються з більшою швидкістю, ніж від користувача.

Стільниковий зв'язок - для доступу в Інтернет використовується мобільна телефонна мережа. У будь-якій точці, де доступний цей сигнал, можна отримати доступ в Інтернет. Продуктивність буде обмежена можливостями телефону і базової станції, до якої він підключений.

Супутниковий зв'язок - супутникові інтернет-канали можна використовувати в районах, де немає інших способів підключення. Для використання супутникових антен необхідно, щоб супутник перебував в зоні прямої видимості.

Телефонний комутований доступ - це економічний варіант підключення з використанням будь-якої телефонної лінії і модему. Низька пропускна здатність комутованій лінії зазвичай недостатня для передачі великого обсягу даних. Однак така лінія може бути корисна для мобільного доступу в дорозі.

Для підключення будинків і невеликих офісів все частіше використовуються оптоволоконні кабелі. Це дозволяє інтернет-провайдерам забезпечувати більш високі швидкості передачі даних, а також надавати більше послуг, наприклад Інтернет, телефон і телебачення.

Спосіб підключення залежить від географічного місця розташування користувачів і наявності в регіоні оператора зв'язку.

Корпоративні варіанти підключення відрізняються від варіантів для домашнього користувача. Компанії може вимагатися більш висока пропускна здатність, виділена лінія і керовані послуги. Доступні варіанти передачі даних залежить від технологій, які використовують оператори зв'язку, що знаходяться поруч.

Виділена орендована лінія - орендовані лінії являють собою зарезервовані канали в мережі оператора зв'язку, що забезпечують зв'язок між географічно віддаленими офісами для передачі голосу і даних в приватній мережі. Плата за

оренду таких каналів зв'язку зазвичай стягується щомісячно або щорічно. Вони можуть бути дорогими.

Глобальна мережа Ethernet - глобальні мережі Ethernet дозволяють розширити мережі LAN до WAN. Про технологію локальних мереж Ethernet ви дізнаєтеся з наступних глав. Переваги технології Ethernet тепер доступні і в глобальних мережах.

DSL - корпоративне DSL-підключення є в різних форматах. Популярністю користуються симетричні цифрові абонентські лінії (Symmetric Digital Subscriber Lines, SDSL), аналогічні абонентської версії DSL, але за одного значення швидкість при отриманні і відправці даних.

Супутниковий зв'язок - як і у випадку невеликих і домашніх офісів, супутникові послуги забезпечують підключення там, де дротовий зв'язок недоступна.

Спосіб підключення залежить від географічного місця розташування користувачів і наявності в регіоні оператора зв'язку.

Як приклад розглянемо навчальний будівля, побудована 30 років тому. У деяких аудиторіях були прокладені кабелі передачі даних, телефонної мережі і телебачення. Ці мережі були розрізнені, а значить, не могли взаємодіяти один з одним, як показано на малюнку. Всі мережі використовували різні технології для передачі сигналу. У кожній мережі для забезпечення успішної зв'язку використовувався свій власний набір правил і стандартів.

конвергентна мережу

Рис. 1.1.9 Мультисервісні мережі

Сьогодні розрізнені мережі даних, телефонні і відео мережі об'єднуються. На відміну від виділених мереж конвергентні мережі дозволяють передавати дані, голос і відео між різними типами пристроїв при використанні однієї і тієї ж мережевої інфраструктури, як показано на малюнку. Мережева інфраструктура використовує одні й ті ж правила, угоди і стандарти реалізації.

Мережі повинні підтримувати широкий набір додатків і сервісів, а також безліч типів кабелів і пристроїв, з яких складається фізична інфраструктура. Термін «мережева архітектура» в цьому контексті відноситься до технологій, які підтримують інфраструктуру, а також до запрограмованим послуг і правилам або протоколам, які служать для передачі даних в мережі.

Рис. 1.1.10 Основні вимоги до мережі

У міру розвитку мереж стає очевидним, що для задоволення потреб користувачів архітектура повинна відповідати чотирьом основним вимогам.

- відмовостійкість
- масштабованість
- Якість обслуговування (QoS)
- Безпека

Інтернет повинен бути завжди доступний мільйонам користувачів, які розраховують на його безперебійну роботу. Для цього потрібно відмовостійка мережева архітектура. Відмовостійка мережу - це мережа, що забезпечує найменший вплив збоїв на найменшу кількість пристроїв. Вона також побудована так, щоб швидко відновлюватися при виникненні відмови. Ці мережі використовують кілька шляхів передачі даних від джерела до місця призначення. Якщо один шлях недоступний, повідомлення можна негайно відправити по іншій лінії зв'язку. Наявність декількох шляхів до місця призначення називається резервуванням.

Один із способів резервування в надійних мережах - впровадження мереж з пакетною комутацією. При комутації пакетів трафік ділиться на пакети, які направляються по мережі загального доступу. Таке єдине повідомлення, як електронний лист або відеопотік, ділиться на безліч блоків даних, званих пакетами. Кожен пакет містить інформацію про адресу джерела і місце призначення повідомлення. Маршрутизатор в мережі коммутируют пакети в залежності від поточного стану мережі. Це означає, що пакети даних одного повідомлення можуть йти до місця призначення різними шляхами. Як показано на малюнку, динамічна зміна маршруту в разі недоступності каналу зв'язку не впливає на користувача, користувач цього не помічає.

Рис. 1.1.11 Схема відмовостійкості мережі

Інакше влаштовані мережі з комутацією каналів, які традиційно використовуються для голосового зв'язку. У мережі з комутацією каналів, перш ніж користувачі зможуть обмінюватися даними, встановлюється виділене з'єднання між джерелом і місцем призначення. У разі обриву з'єднання користувачеві доводиться встановлювати з'єднання заново.

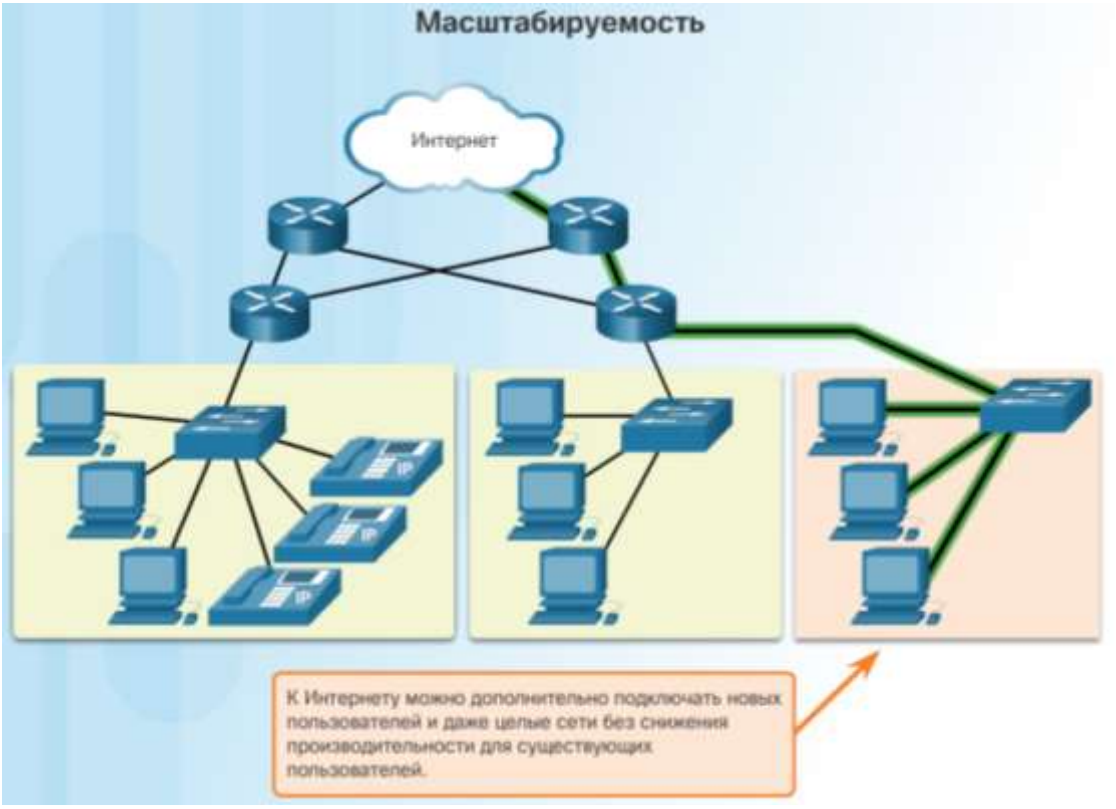


Рис. 1.1.12 Принципова схема масштабованості мережі

Масштабовану мережу можна швидко розширити, забезпечивши підтримку нових користувачів і додатків без зниження ефективності обслуговування існуючих. На малюнку показано, як можна легко додати нову мережу до існуючої. Крім цього, масштабованість мереж можлива завдяки тому, що проектувальники дотримуються прийнятих стандартів і протоколів. Це дозволяє виробникам програмного і апаратного забезпечення докласти всіх зусиль до поліпшення продуктів і послуг і не думати про розробку нового набору правил для роботи в мережі.

Якість обслуговування (QoS) сьогодні є одним з постійно зростаючих вимог до мережі. Нові веб-додатки, наприклад передача голосу і відео в режимі реального часу, задають більш високі вимоги до якості послуг, що надаються. Чи доводилося вам коли-небудь дивитися відео з постійними розривами і паузами? За рахунок об'єднання функцій передачі даних, голосу і відео в одній мережі QoS стає основним механізмом запобігання перевантажень мережі і надійної доставки контенту всім користувачам.

Перевантаження мережі виникає, коли попит на канали зв'язку перевищує можливості мережі. Пропускна здатність мережі вимірюється в кількості біт, що передаються за одну секунду, тобто в бітах в секунду (біт / с). При паралельних спробах передачі інформації попит на канали зв'язку може перевищувати можливості мережі. Це створює перевантаження мережі.

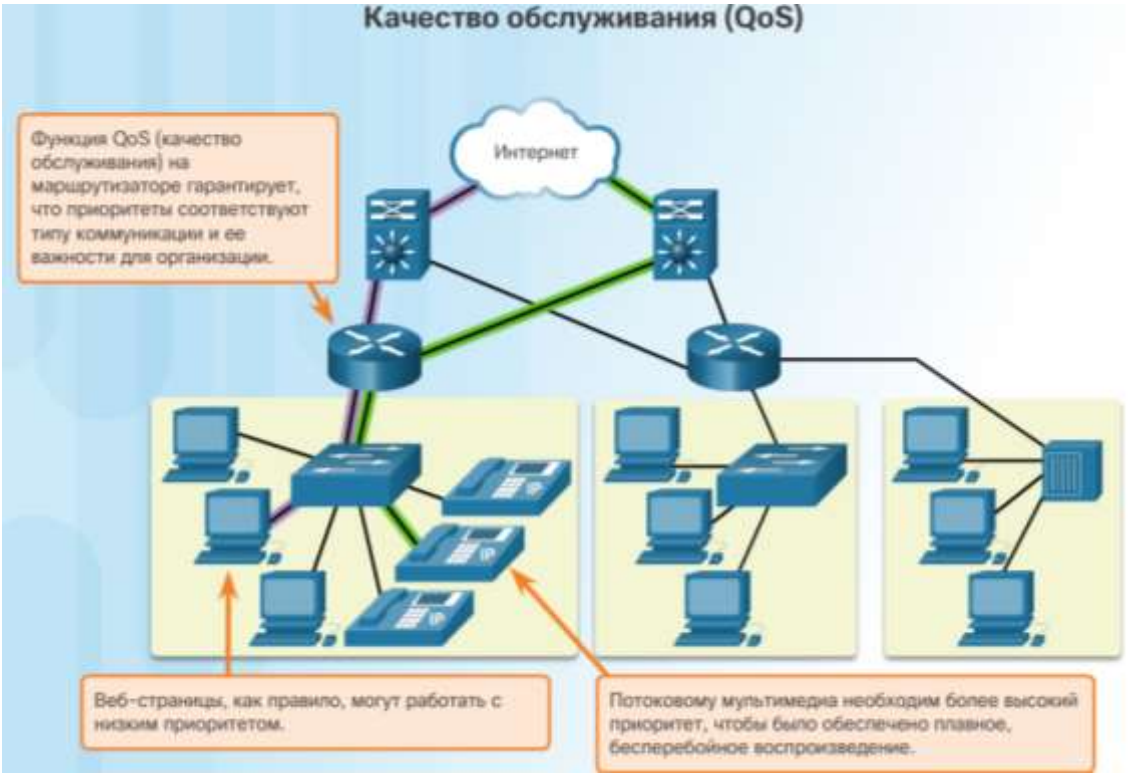


Рис. 1.1.13 Принципова схема забезпечення якості зв'язку у мережі

Коли обсяг трафіку перевищує можливості доставки по мережі, пристрої поміщають пакети в чергу в пам'яті і утримують їх до тих пір, поки не будуть доступні ресурси передачі. На малюнку один користувач запитує веб-сторінку, а інший робить телефонний дзвінок. Завдяки політиці QoS маршрутизатор обробляє потік даних і голосовий трафік, віддаючи пріоритет голосового зв'язку в разі перевантаження мережі.

Мережева інфраструктура, сервіси та дані, які містяться в пристроях, підключених до мереж, є важливі особисті і корпоративні активи. Існує два типи проблем безпеки мережі, які необхідно врахувати: безпека мережевої інфраструктури і безпеку інформації.

Забезпечення безпеки інфраструктури мережі включає в себе фізичний захист всіх пристроїв, які необхідні для підключення до мережі, і запобігання несанкціонованого доступу до встановленого на них ПЗ управління.

Безпека інформації означає захист пакетів даних, переданих по мережі, а також інформації, що зберігається на підключених до мережі пристроях. Існує три основних вимоги для досягнення безпеки мережі.

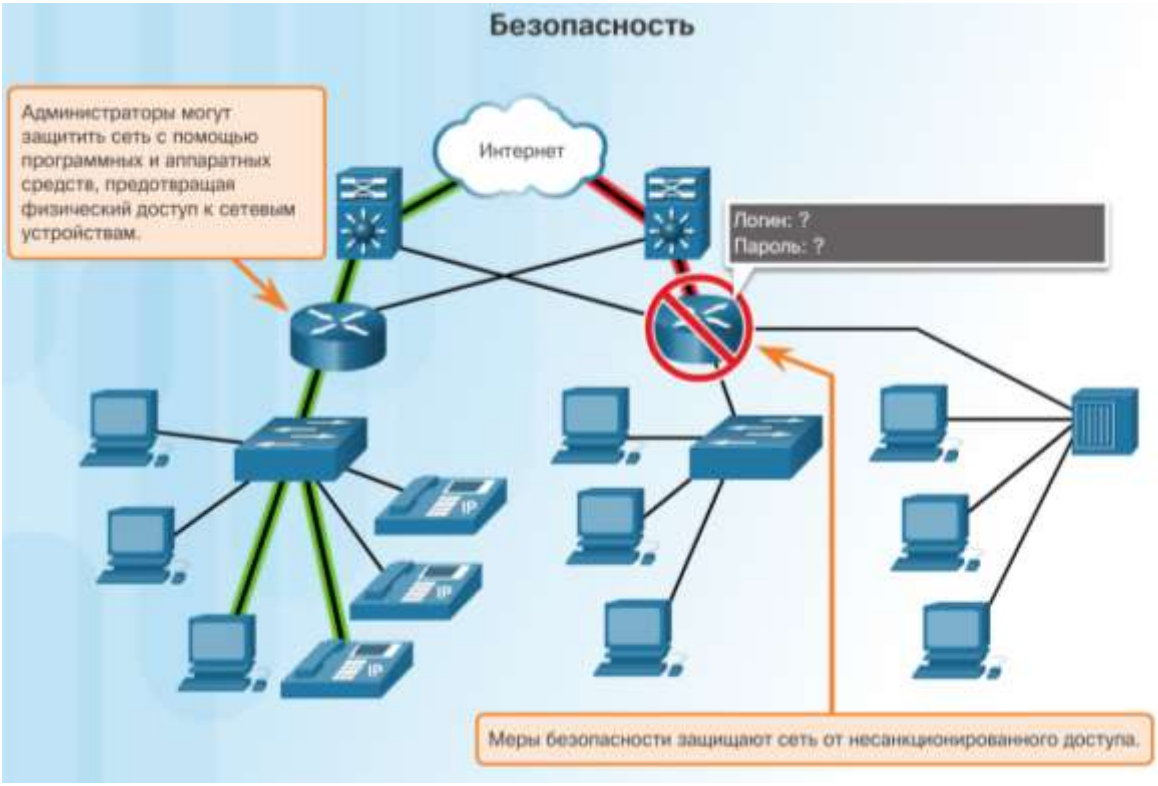


Рис. 1.1.14 Основи безпеки мережі

Конфіденційність - тільки зазначені й авторизовані одержувачі можуть мати доступ до даних.

Цілісність - гарантія того, що інформація не була змінена в процесі передачі від вихідного пункту до місця призначення.

Доступність - своєчасний і надійний доступ до даних для авторизованих користувачів.

У міру розвитку нових технологій і появи на ринку нових кінцевих пристроїв підприємства і споживачі повинні постійно пристосовуватися до сучасних умов, що змінюються. Роль мережі змінюється, щоб забезпечити зв'язок між користувачами, пристроями та інформацією. Існує кілька нових тенденцій в розвитку мережевих технологій, які вплинуть на організації та споживачів. Серед деяких основних тенденцій можна виділити наступні.

«Принеси на роботу свій пристрій» (Bring Your Own Device, BYOD)

- Спільна робота через Інтернет
- Спільний перегляд
- хмарні обчислення
- Концепція «Принеси на роботу свій пристрій»

Концепція доступу з будь-якого пристрою до будь-якого контенту будь-яким способом - основна глобальна тенденція, яка вимагає перегляду способів використання пристроїв. Ця популярна тенденція називається «принеси на роботу свій пристрій» (Bring Your Own Device, BYOD).

Згідно з концепцією BYOD кінцеві користувачі можуть застосовувати особисті пристрої для доступу до інформації в корпоративній мережі або мережі комплексу будівель. У міру збільшення популярності споживчих пристроїв і відповідного падіння цін очікується, що кожен із співробітників і учнів може мати в особистому користуванні найдосконаліші обчислювальні і мережеві інструменти. Ці персональні засоби включають в себе ноутбуки,

нетбуки, планшети, смартфони і електронні книги. Це можуть бути пристрої, куплені компанією, навчальним закладом або самим користувачем.

BYOD означає можливість використання будь-якого пристрою в будь-якому місці будь-яким користувачем. Наприклад, в минулому для доступу до кампусової мережі або Інтернету учні повинні були використовувати один з комп'ютерів навчального закладу. Ці пристрої розглядалися, як правило, тільки як засобу для роботи в класі або бібліотеці. Мобільний або віддалений доступ до кампусової мережі відкриває учням нові можливості, забезпечуючи широкий вибір варіантів навчання.

Спільна робота через Інтернет

Користувачі підключаються до мережі не тільки для доступу до додатків для роботи з даними, а й для спільної роботи один з одним. Спільна робота - це «робота з іншими виконавцями на спільному проекті». Такі інструменти спільної роботи, як Cisco WebEx, дають працівникам, студентам, вчителям, замовникам і партнерам можливість миттєвого підключення, взаємодії та досягнення цілей.

Для компаній спільна робота стає критично важливим аспектом конкурентоспроможності. Спільна робота є пріоритетом також в сфері освіти. Спільна робота допомагає в навчанні, розвиває навички взаємодії в команді, які необхідні для групових проектів.

Спільний перегляд

Інша тенденція в сфері мережевих технологій, яка важлива для спілкування та спільної роботи, - використання відео. Відео використовується для обміну інформацією, спільної роботи, а також для розваги. Відеодзвінки можна здійснювати з будь-якого місця, де є підключення до Інтернету.

Відеоконференції - це ефективний засіб спілкування як на локальному, так і на глобальному рівні. Використання відео стає ключовою вимогою для ефективної спільної роботи у міру того, як компанії розширюють географічні і культурні кордони. Натисніть кнопку «Відтворення» на відео і подивіться, як система TelePresence допомагає в роботі і повсякденному житті.

Хмарні обчислення - інша глобальна тенденція, яка змінює спосіб доступу і зберігання даних. Хмарні обчислення дозволяють зберігати особисті файли або резервну копію цілого жорсткого диска на серверах в Інтернеті. Наприклад, додатками для роботи з текстом і для редагування фотографій можна користуватися з хмари.

Для підприємств хмара розширює можливості, не вимагаючи при цьому великих капіталовкладень у створення нової інфраструктури, навчання нового персоналу або ліцензування нового програмного забезпечення. Ці економічні сервіси доступні за запитом на будь-якому пристрої в будь-якій точці світу і забезпечують належний рівень безпеки і функціональності.

Як показано на малюнку, існує чотири основні типи хмар: загальнодоступні, приватні, гібридні і призначені для користувача. Клацніть на кожне хмара, щоб дізнатися докладні відомості.

Хмарні обчислення можливі завдяки центрам обробки даних. Центр обробки даних (ЦОД) - це приміщення, в якому розташовуються комп'ютерні системи і відповідні компоненти. ЦОД може займати одне приміщення в будівлі, один або кілька поверхів або всю будівлю. ЦОД зазвичай дорого

створювати і обслуговувати. З цієї причини тільки великі організації використовують власні ЦОД, щоб розміщувати корпоративні дані і надавати послуги користувачам. Невеликі організації, які не мають власного ЦОД, можуть знизити загальну вартість володіння, орендуючи сервери та системи зберігання в хмарному ЦОД постачальника послуг.

Тенденції в розвитку мережевих технологій не тільки впливають на спосіб спілкування на роботі і в школі, вони також змінюють наш спосіб життя вдома.

До новітніх тенденцій домашніх мереж належать «технології інтелектуального будинку». Технологія інтелектуального будинку інтегрована в побутові пристрої і дозволяє їм підключатися до інших пристроїв і, таким чином, бути більш інтелектуальними або більш автоматизованими. Наприклад, припустимо, що ви приготували блюдо, і перед тим, як піти з дому на весь день, поставили його в духовку. Уявіть, що духовка «знає» про те, що їй треба приготувати, і підключена до вашого «календарем подій», тому вона знає, коли ви прийдете додому і почне готувати їжу точно до вашого приходу. Вона навіть може змінити тривалість і температуру приготування, в разі, якщо ваші плани зміняться. Крім того, за допомогою смартфонів або планшетів користувачі можуть безпосередньо підключитися до духовки і внести необхідні зміни. Коли страва готова, духовка відправляє на вказане для користувача пристрій повідомлення про те, що страва готова і підігрівається.

Це вже майже реальність. В даний час на стадії розробки знаходяться технології інтелектуального будинку для всіх приміщень будинку. Технологія інтелектуального будинку стане більш реальною, коли домашні мережі і технологія високошвидкісного Інтернету отримають більш широке поширення. Нові технології домашніх мереж постійно розробляються, щоб задовольнити зростаючі технологічні потреби.

Організація мережі по лініях електроживлення - тенденція домашньої мережі, що використовує існуючі електричні кабелі для з'єднання пристроїв, як показано на малюнку. Концепція «відсутності нових проводів» означає можливість підключення пристрою до мережі з будь-якого місця, де є електричні розетки. Це дозволяє економити витрати на прокладку кабелів для передачі даних, в той час як в рахунках за електрику сума не змінюється. З використанням тієї ж проводки, по якій надходить електрика, мережі передачі даних по лініях електроживлення відправляють інформацію на певних частотах.

За допомогою стандартного адаптера мережі електроживлення пристрою можуть підключатися до мережі LAN всюди, де є електричні розетки. Організація мережі по лініях електроживлення особливо корисна там, де неможливо використовувати точки бездротового доступу або вони не забезпечують доступ для всіх пристроїв в будинку. Організація мережі по лініях електроживлення не може виступати в заміною для виділених кабельних мереж передачі даних. Однак цей варіант можна використовувати в якості альтернативного в тому випадку, коли кабельні та бездротові мережі передачі даних незастосовні.

Бездротовий широкосмуговий доступ

Для технологій інтелектуального будинку підключення до Інтернету абсолютно необхідно. Для підключення до мережі Інтернет будинків і

невеликих компаній зазвичай використовується кабельне або DSL-підключення. Однак у багатьох випадках можна використовувати і бездротову мережу.

Постачальник бездротових інтернет-послуг (Wireless Internet Service Provider, WISP)

Постачальник бездротових інтернет-послуг (WISP) підключає абонентів до певних бездротових точок доступу за допомогою бездротових технологій, аналогічних домашнім безпроводової локальної мережі (WLAN). Найчастіше WISP зустрічаються в сільській місцевості, де лінії DSL або кабельні мережі недоступні.

Іноді антену встановлюють на окрему вишку, але частіше її розміщують на існуючих конструкціях, таких як водонапірна вежа або радіовежа. Невелика антена на даху у абонента знаходиться в зоні прийому передавача WISP. Блок доступу підключається до дротової мережі в будинку. З точки зору домашнього користувача, настройка практично не відрізняється від настройки DSL або кабельних ліній зв'язку. Головна відмінність полягає в тому, що підключення від будинку до оператора зв'язку - це бездротове підключення, а не через фізичний кабель.

Інша бездротове рішення для дому та малих підприємств - бездротовий широкосмуговий доступ. Для нього застосовується та ж стільниковий технологія, що і для доступу в Інтернет за допомогою планшета або смартфона. Антена встановлюється зовні будинку, забезпечуючи бездротове або дротове підключення пристроїв в будь-якій точці будинку. У більшості випадків домашній бездротовий широкосмуговий доступ безпосередньо конкурує з рішеннями DSL і кабельними послугами.

Забезпечення мережевої безпеки є невід'ємною частиною обчислювальних мереж, незалежно від їх масштабів: від домашньої мережі, в якій до Інтернету підключений тільки один комп'ютер, до корпоративної мережі, що нараховує тисячі користувачів. Забезпечуючи мережеву безпеку, ви повинні враховувати існуючі середовища, а також інструменти і вимоги мережі. Необхідно захищати дані, підтримуючи якість обслуговування на заявленому рівні.

Сфера мережевої безпеки охоплює протоколи, технології, пристрої, інструменти, методи захисту даних і відображення загроз. Загрози безпеці можуть бути як зовнішніми, так і внутрішніми. Багато зовнішні загрози сьогодні поширюються через Інтернет.

До найбільш поширених зовнішніх загроз відносяться:

- Віруси, черв'яки і «троянські коні» - шкідливе програмне забезпечення і довільний код, виконувані на призначених для користувача пристроях
- Шпигунське і рекламне ПО - програмне забезпечення, яке встановлюється на призначене для користувача пристрій і таємно збирає відомості про користувача
- Атаки нульового дня, також звані атаками нульового години, здійснюються в перший день, коли про уразливість стає відомо
- Хакерські атаки - атаки компетентного зловмисника на призначені для користувача пристрої або мережеві ресурси

- Атаки типу «відмова в обслуговуванні» - атаки, розроблені для зниження продуктивності або аварійного завершення процесів на мережевому пристрої
- Перехоплення і розкрадання даних - атака з метою збору приватної інформації з корпоративної мережі
- Крадіжка особистої інформації - атака для розкрадання облікових даних користувача, щоб отримати доступ до даних приватного характеру

Не менш важливо враховувати внутрішні загрози. Багато досліджень показують, що найбільш поширені порушення інформаційної безпеки пов'язані з внутрішніми користувачами мережі. Це можуть бути випадки втрати або крадіжки пристроїв, помилки співробітників і навіть їх зловмисні дії. При використанні концепції «Принеси на роботу своє власне пристрій» корпоративні дані ще набагато більш уразливі. Таким чином, при створенні політики забезпечення безпеки важливо враховувати і зовнішні, і внутрішні загрози національній безпеці.

Жодне окреме рішення не може повністю убезпечити мережу від численних сучасних загроз. Саме тому заходи щодо забезпечення мережевої безпеки необхідно впроваджувати відразу на декількох рівнях, задіявши одночасно кілька рішень. Якщо який-небудь один компонент системи безпеки не може визначити загрози і захистити мережу, то йому на допомогу прийдуть інші компоненти.

Реалізувати політики безпеки в домашній мережі, як правило, досить просто. Такі політики зазвичай впроваджуються на підключаються кінцевих пристроях, а також в точці підключення до Інтернету, і навіть можуть бути реалізовані як сервіси, що надаються за договором Інтернет-провайдером.

Реалізація політик мережевої безпеки для корпоративної мережі, навпаки, зазвичай включає в себе безліч компонентів, вбудованих в мережі для контролю і фільтрації трафіку. В ідеалі передбачається, що всі компоненти працюють разом, що знижує обсяг обслуговування і підвищує безпеку.

Для забезпечення безпеки домашніх або невеликих офісних мереж повинні використовуватися як мінімум наступні компоненти.

Антивірусну програму й анти-шпигунське ПЗ дозволяє запобігти зараженню кінцевих пристроїв шкідливими програмами.

Фільтрація на межсетевом екрані - блокування спроб несанкціонованого доступу до мережі. Сюди може входити система реалізованих на вузлі міжмережевих екранів, яка використовується для запобігання несанкціонованому доступу до кінцевого пристрою, або базовий сервіс фільтрації на домашньому маршрутизаторі для запобігання несанкціонованому доступу в мережу ззовні.

Крім перерахованого вище, в більших мережах і корпоративних мережах часто є інші вимоги безпеки.

Виділені міжмережеві екрани - ширші можливості брандмауера, який може фільтрувати великий обсяг трафіку з підвищеною деталізацією.

Списки контролю доступу (Access Control List, ACL) - подальша фільтрація доступу, а також пересилання трафіку.

Системи запобігання вторгнень (Intrusion prevention system, IPS) - визначення швидко поширюються загроз, таких як атаки нульового дня або нульового години.

Віртуальні приватні мережі (Virtual Private Network, VPN) - забезпечення безпечного доступу для віддалених співробітників.

Вимоги безпеки повинні враховувати мережеву середу, а також різні додатки і вимоги до обчислювальних пристроїв. І в домашніх, і в корпоративних мережах необхідно забезпечувати безпеку даних, пропонуючи то якість обслуговування, яке очікують користувачі будь-якої технології. Крім того, впроваджені рішення для забезпечення безпеки повинні легко адаптуватися до зростання мереж і мінливих вимог.

Вивчення загроз мережевої безпеки і методів їх відображення починається з чіткого розуміння інфраструктури комутації і маршрутизації, використовуваної для організації мережевих сервісів.

Мережеві протоколи і комунікації

Мережі грають все більшу і більшу роль у взаємодії між людьми. Люди спілкуються в мережі з абсолютно різних місць. Дискусії в аудиторіях переносяться в чати, а обговорення в мережі тривають в аудиторіях. Щодня розробляються нові сервіси для використання переваг мережі.

Замість розробки унікальних, окремих систем для кожного нового сервісу, в мережевий галузі в цілому почали застосовувати підхід, який дозволяє розробникам зрозуміти принцип роботи поточних мережевих платформ і підтримувати ці платформи. Такий підхід використовується для спрощення розробки нових технологій з метою підтримки майбутніх потреб зв'язку та вдосконалення технологій.

В основі такого підходу до розробки лежить використання загальноприйнятих моделей, що описують мережеві правила і функції.

У цьому розділі ви дізнаєтеся про ці моделі, а також про стандарти роботи мереж і принципах обміну даними по мережі.

Мережа може бути складною (пристрої, підключені через Інтернет) або простий (два комп'ютери, підключені безпосередньо за допомогою одного кабелю). Можливо і щось середнє. Мережі можуть відрізнятися за розміром, формою і функціями. Проте для зв'язку недостатньо мати тільки фізичне з'єднання між кінцевими пристроями. Для успішного обміну даними ці пристрої повинні «знати», як обмінюватися інформацією.

Люди обмінюються ідеями різними способами. При цьому всі способи комунікацій мають три загальних елемента. Перший - це джерело повідомлення, або відправник. Відправником може бути людина або електронний пристрій, з яким потрібно відправити повідомлення іншій людині або пристрою. Другий елемент - це адресат, або одержувач повідомлення. Адресат отримує і інтерпретує повідомлення. Третій елемент, званий каналом, являє собою засіб підключення, за яким повідомлення передається від джерела до одержувача.

Комунікації починаються з повідомлення (інформації), яке потрібно передати від джерела до одержувача. Відправлення цього повідомлення за допомогою індивідуального спілкування або по мережі регулюється правилами, які називаються протоколами. Ці протоколи відповідають способу комунікації. При щоденному особистому спілкуванні правила обміну даними через один засіб зв'язку, наприклад телефон, не обов'язково збігаються з протоколом використання іншого засобу зв'язку, наприклад пошти.

Розглянемо, наприклад, індивідуальне спілкування двох людей. До початку спілкування вони повинні домовитися про спосіб спілкування. Якщо спілкування буде відбуватися за допомогою голосу, спочатку вони повинні домовитися про те, якою мовою вони будуть спілкуватися. Потім, коли у них є повідомлення друг для друга, вони повинні зуміти висловити його таким чином, щоб воно стало зрозумілим. Наприклад, якщо хтось говорить англійською, але неправильно структурує пропозицію, повідомлення може бути витлумачено невірно. Кожна з цих завдань описує протоколи, які потрібно застосувати для успішної комунікації. Це відноситься також до комп'ютерної комунікації.

Подумайте над тим, скільки різних правил або протоколів регулюють способи комунікації, що існують в сучасному світі.

Для початку спілкування один з одним люди повинні використовувати встановлені правила або угоди, що регулюють розмова. Протоколи необхідні для ефективної комунікації. Щоб повідомлення було успішно доставлено і зрозуміле, ці правила, або протоколи, необхідно дотримуватися. Протоколи відповідають наступним вимогам:

- Відомі відправник і одержувач
- Загальноприйняті мову і граматика
- Швидкість і час доставки
- Вимоги до утвердження або підтвердження

Протоколах, застосовуваним для зв'язку в мережі, властиві багато з цих фундаментальних особливостей. Крім адреси джерела і місця призначення для відповідності згаданим вище вимогам комп'ютерні і мережеві протоколи визначають спосіб передачі повідомлення через мережу. Поширені комп'ютерні протоколи відповідають вимогам. Кожен з цих пунктів ми розглянемо більш докладно.

Один з перших етапів відправки повідомлення - кодування. Кодування - це процес перетворення інформації в форму, прийнятну для подальшої передачі. Декодування - зворотний процес, в результаті якого інформація перетворюється в початковий вигляд.

Уявіть собі людину, яка, плануючи спільний відпустку з одним, дзвонить йому, щоб обговорити пункт призначення майбутньої поїздки. Щоб передати повідомлення, дівчина висловлює свої думки на обраною мовою. Вона вимовляє слова, використовуючи звуки і інтонацію, щоб донести повідомлення. Друг слухає її і декодує звуки, щоб зрозуміти отримане повідомлення.

Кодування використовується також при обміні даними за допомогою комп'ютера. Кодування даних при обміні між вузлами повинна бути в форматі, відповідному засобу підключення. Перш за все, вузол-відправник перетворює передане по мережі повідомлення в біти. Кожен біт кодується набором звуків, світлових хвиль або електричних імпульсів, в залежності від типу засобу мережевого підключення. Вузол призначення приймає і декодує сигнали і інтерпретує повідомлення.

При відправці повідомлення від джерела до адресата необхідно використовувати певний формат або структуру. Формат залежить від типу повідомлення і каналу доставки.

Одна з найбільш поширених форм письмових комунікацій між людьми - лист. Загальноприйнятий формат особистих листів не змінюється століттями. У культурах більшості країн особистий лист складається з наступних елементів.

- ідентифікатор одержувача
- Звернення або вітання
- вміст повідомлення
- заключна фраза
- ідентифікатор відправника

Крім того, більшість особистих листів потрібно не тільки скласти в правильному форматі, але і запечатати в конверт для доставки, . На конверті в

спеціально відведеному місці вказується адреса відправника та одержувача. Якщо адресат або формат невірний, лист не дійде. Процес розміщення одного формату повідомлення (лист) всередині іншого (конверт) називається інкапсулюція. Деінкапсуляція відбувається в той момент, коли одержувач дістає лист з конверта.

Для доставки і обробки листи в комп'ютерній мережі необхідно дотримуватися певних правил форматування. Комп'ютерні повідомлення інкапсулюються подібно до того, як лист вкладається в конверт. Для інкапсуляції кожного повідомлення комп'ютера перед відправкою по мережі використовується особливий формат, який називається кадром. Кадр діє як конверт: в ньому вказані адреса вузла-джерела і адреса призначення. Зверніть увагу, що адреса джерела та адресу призначення вказані як в адресній частині кадру, так і в Інкапсульована повідомленні. Різниця між цими двома типами адрес буде розглянута далі в цій главі.

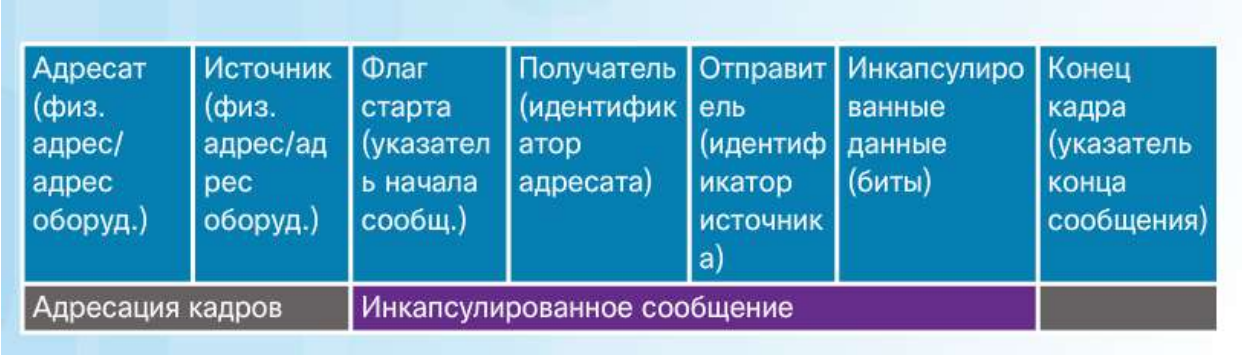


Рис. 1.1.15 Заголовок Кадра даних

Формат і вміст кадру залежать від типу повідомлення і каналу передачі. Невірно відформатовані повідомлення не можуть бути доставлені на вузол призначення і оброблені на ньому.

Ще одне правило комунікації - це розмір. В процесі розмови люди ділять свої висловлювання на більш дрібні частини, або пропозиції. Розмір цих пропозицій обмежений тим, скільки приймає особа може сприйняти за один раз. У деяких випадках розмову можна поділити на багато дрібніших пропозицій так, щоб співрозмовник сприйняв і зрозумів кожну частину висловлювання. Уявіть собі, як можна було б читати цей курс, якби він виглядав як одне довге речення. В такому випадку прочитати і зрозуміти його було б досить складно.

Аналогічним чином при передачі довгого повідомлення від одного вузла до іншого по мережі необхідно поділити його на частини. Розміри цих частин, або кадрів, дуже строго регулюються. Крім усього іншого, вони залежать від використовуваного каналу. Занадто довгі або короткі кадри не доставляються.

Обмеження за розміром кадрів змушують вузол-джерело ділити довгі повідомлення на частини, що відповідають вимогам до мінімального і максимального розміру. Довге повідомлення розбивається на окремі кадри, кожен з яких містить частину вихідного повідомлення. Кожен кадр містить інформацію про адреси. Вузол-адресат відновлює вихідне повідомлення по частинам.

Спосіб доступу визначає, коли конкретна людина зможе відправити повідомлення. Якщо дві людини починають говорити одночасно, відбувається

інформаційна колізія і обом доводиться починати спочатку, . Комп'ютерам теж необхідно вибирати спосіб доступу. Щоб дізнатися, коли почати відправку повідомлень і як реагувати на конфлікти, вузлів в мережі потрібно визначити спосіб доступу.

Синхронізація впливає і на кількість відправляється інформації, і на швидкість її доставки. Якщо одна людина говорить занадто швидко, інакше складно розчути і зрозуміти повідомлення, . У разі мережевих комунікацій вузли-джерела і вузли призначення застосовують методи управління потоком, щоб узгодити час для успішного обміну даними.

Якщо людина ставить запитання і не отримує відповіді за прийнятний час, він передбачає, що відповіді не буде, і реагує відповідним чином. Він може повторити питання або продовжити розмову. У мережевих вузлів також є правила, що визначають час очікування відповіді і дії, що виконуються після закінчення цього часу.

Способи доставки повідомлень можуть різнитися. Іноді інформацію потрібно передати тільки одній людині. В інших випадках її потрібно одночасно передати групі людей або навіть всім жителям певного району.

Крім того, буває, що відправнику потрібно переконатися, що повідомлення успішно доставлено. Для цього одержувач повинен відправити підтвердження доставки. Якщо підтвердження не потрібно, метод доставки повідомлення називається непідтвердженими.

Вузлів у мережі використовують аналогічні варіанти доставки повідомлень.

Метод розсилки «один до одного» називається одно-адресна. Це означає, що у повідомлення є тільки один адресат.

Якщо вузол розсилає повідомлення методом «один до багатьох», це багато-адресна розсилка. Багатоадресна розсилка передбачає одночасну відправку одного і того ж повідомлення групі вузлів.

Якщо всім мережевим вузлам необхідно отримати повідомлення в один і той же час, використовується широкомовлення. Широкомовлення це спосіб доставки повідомлень «один до всіх». Деякі протоколи передбачають багатоадресну відправку спеціального повідомлення всіх пристроїв аналогічно широкомовної розсилки. Крім того, підтвердження отримання від вузлів може вимагатися для одних повідомлень і не турбуватися для інших.

Група взаємопов'язаних протоколів, необхідних для виконання комунікацій, називається набором протоколів. Набір протоколів реалізується мережевими пристроями і вузлами в програмному або апаратному забезпеченні або в тому і в іншому.

Один з кращих способів уявити, як протоколи взаємодіють в одному наборі, розглянути взаємодію у вигляді стека. Стек протоколів показує, як окремі протоколи реалізовані в одному наборі. Протоколи розглядаються з точки зору рівнів. Причому кожен вищий рівень обслуговування залежить від функцій, визначених протоколами нижчих рівнів. Нижні рівні стека відповідають за переміщення даних по мережі і надання сервісів верхніх рівнів, які відповідають за утримання пересилаються.

Як показано на малюнку, ми можемо використовувати рівні для опису процесів, що відбуваються в нашому прикладі особистого спілкування. На

нижньому, фізичному рівні є дві людини, кожен з яких може вимовити слова вголос. На середньому рівні (рівні правил) є домовленість спілкуватися однією мовою. На верхньому рівні (рівні змісту) знаходяться фактично вимовлені слова. У цьому полягає суть комунікацій.

На рівні спілкування між людьми одні правила комунікації формалізовані, інші просто зрозумілі, виходячи з звичаїв і практики. Для успішного обміну даними між пристроями набір мережевих протоколів повинен описувати точні вимоги до процедури. Мережеві протоколи визначають загальний формат і набір правил для обміну повідомленнями між пристроями. Найбільш популярними мережевими протоколами є протокол передачі гіпертексту (Hypertext Transfer Protocol, HTTP), протокол управління передачею (Transmission Control Protocol, TCP) і протокол Інтернету (Internet Protocol, IP).

Примітка. Під IP в цьому курсі розуміються обидва протоколи IPv4 і IPv6. Протокол IPv6 - остання версія протоколу IP, що прийшла на заміну більш поширеною версією IPv4.

Зв'язок між веб-сервером і веб-клієнтом - приклад взаємодії декількох протоколів. На малюнку показані наступні протоколи.

Протокол HTTP - протокол прикладного рівня, який управляє взаємодією веб-сервера і веб-клієнта. HTTP визначає зміст і формат запитів і відповідей, якими обмінюються клієнт і сервер. Програмне забезпечення та веб-клієнта, і веб-сервера реалізує HTTP як частина програми. Для управління процесом передачі повідомлень між клієнтом і сервером HTTP звертається до інших протоколах.

Протокол TCP - це транспортний протокол, керуючий окремими сеансами зв'язку. TCP поділяє повідомлення HTTP на більш дрібні частини, звані сегментами. Ці сегменти передаються між веб-сервером і клієнтськими процесами, запущеними на вузлі призначення. TCP також відповідає за управління розміром і швидкістю, з якою відбувається обмін повідомленнями між сервером і клієнтом.

Рис. 1.1.16 Схема інкапсуляції даних

Протокол IP відповідає за прийом форматованих сегментів TCP, інкапсуляцію їх в пакети, присвоєння їм відповідних адрес і їх доставку до вузла призначення.

Протокол Ethernet - протокол мережевого доступу, який описує дві основні функції: зв'язок по каналу передачі даних і фізичне переміщення даних по засобу підключення. Протоколи мережевого доступу відповідають за прийом пакетів від протоколу IP і їх форматування для відправки через засіб підключення.

Набір протоколів є безліч протоколів, які використовуються разом для надання комплексних мережевих сервісів. Набір протоколів може бути визначений організацією зі стандартизації або розроблений постачальником. Набори протоколів, як і ті чотири, що показані на малюнку, можуть включати велику кількість протоколів. Однак в рамках даного курсу розглядається тільки набір протоколів TCP / IP.

Набір протоколів TCP / IP є відкритим стандартом, тобто ці протоколи знаходяться у вільному доступі, і будь-який розробник може використовувати ці протоколи в апаратному або програмному забезпеченні.

Кожен стандартний протокол прийнятий галузевими компаніями і затверджений організацією зі стандартизації. Використання стандартів в розробці і реалізації протоколів гарантує, що продукти від різних виробників буде успішно взаємодіяти між собою. Якщо який-небудь виробник не дотримується строго стандарти протоколу, то його обладнання або ПЗ не зможе успішно взаємодіяти з продуктами інших виробників.

Деякі протоколи є приватними. Це означає, що опис протоколу і принципи його роботи визначаються однією конкретною компанією або постачальником.

Прикладами приватних протоколів є застарілі набори протоколів AppleTalk і Novell Netware. Нерідко постачальник (або група постачальників) розробляє приватний протокол для задоволення потреб своїх замовників, а потім сприяє прийняттю цього приватного протоколу в якості відкритого стандарту.

Рис. 1.1.17 Набір протоколів і стандартів запропоновані різними організаціями

Наприклад, так було з протоколом Ethernet. Натисніть посилання, щоб подивитися відео-презентацію, в якій Боб Меткалф (Bob Metcalfe) описує історію його розробки.

Першою мережею з комутацією пакетів і попередником сучасного Інтернету була мережа Advanced Research Projects Agency Network (ARPANET), яка з'явилася в 1969 році, зв'язавши центральні ЕОМ в чотирьох місцях розташування. Мережа ARPANET фінансувалася Міністерством оборони США і використовувалася в університетах і науково-дослідних лабораторіях.

На сьогоднішній день набір протоколів TCP / IP об'єднує велику кількість протоколів, як показано на малюнку. Клацніть кожен протокол, щоб подивитися розшифровку його назви і опис. Окремі протоколи реалізовані на різних рівнях відповідно до моделі протоколу TCP / IP: на прикладному, транспортному, мережевому рівнях і рівні доступу до мережі. Протоколи TCP / IP працюють на прикладному, транспортному, мережевому рівнях. Протоколи рівня мережевого доступу забезпечують доставку IP-пакетів з фізичного засобу підключення. Ці протоколи нижчих мережевих рівнів розроблені організаціями зі стандартизації.

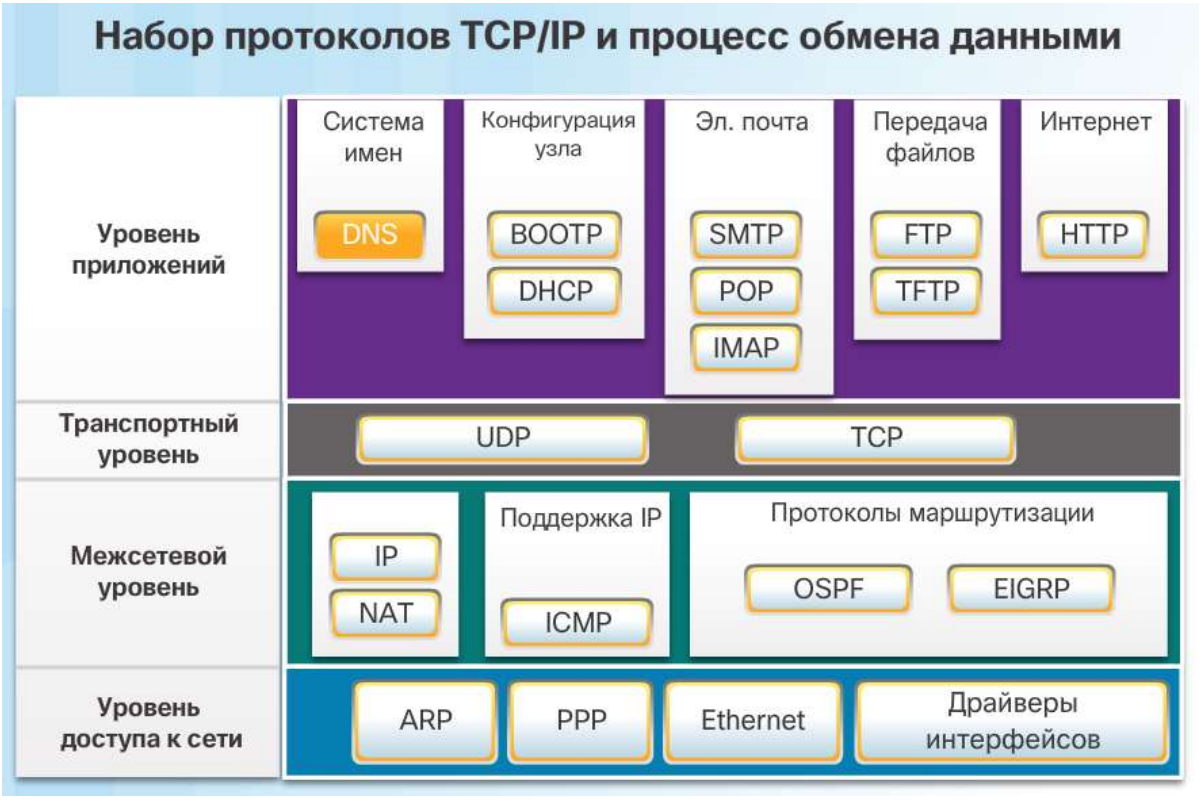


Рис. 1.1.18 Набір протоколів які найбільше застосовуються у мережі

Набір протоколів TCP / IP реалізований у вигляді стека TCP / IP як на відправляє, так і на приймаючому вузлах для забезпечення наскрізної доставки даних по мережі. Протоколи Ethernet використовуються для передачі IP-пакетів по засобу підключення, використовуваному мережею LAN.

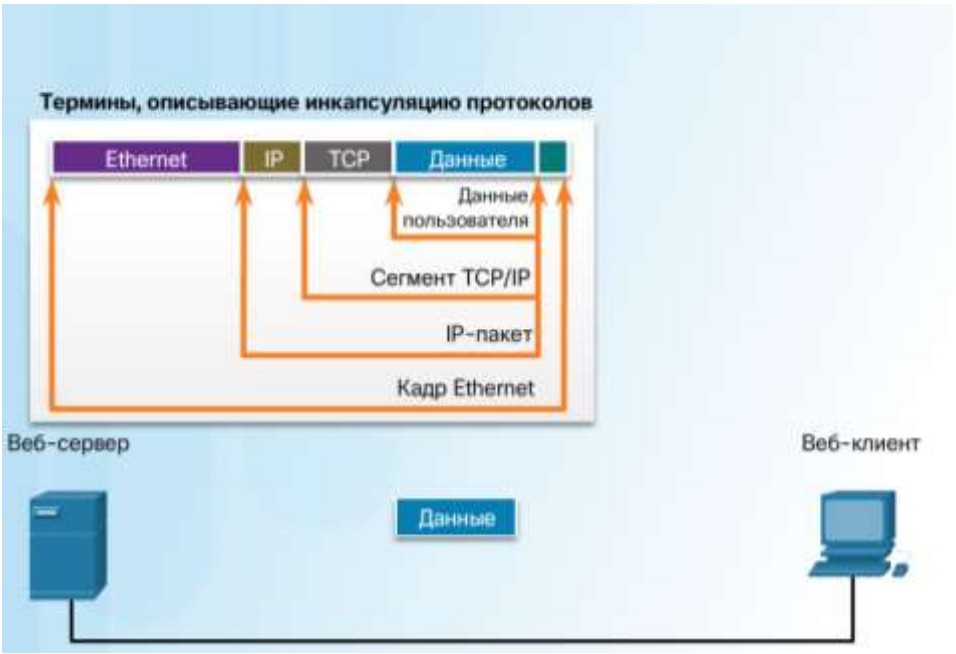


Рис. 1.1.19 Набір протоколів і процес обміну даними

1. Анімація на рис. 1 показує, як веб-сервер перетворює сторінку на гіпертекстовому мовою опису документів (HTML) в дані для відправки.

2. Тема протоколу HTTP прикладного рівня додається в початок даних в форматі HTML. Тема містить різні дані, включаючи версію HTTP, яку

використовує сервер, а також код стану, який вказує, що у нього є інформація для веб-клієнта.

3. Протокол прикладного рівня HTTP передає дані веб-сторінки в форматі HTML на транспортний рівень. Протокол транспортного рівня TCP використовується для управління окремим сеансом зв'язку між веб-сервером і веб-клієнтом.

4. Потім інформація IP додається перед інформацією TCP. IP призначає відповідні IP-адреси джерела і місця призначення. Така інформація називається IP-пакетом.

5. Протокол Ethernet додає в початок і в кінець IP-пакета інформацію, яка називається кадром каналу даних. Цей кадр доставляється на найближчий маршрутизатор на шляху до клієнта. Маршрутизатор видаляє інформацію Ethernet, аналізує IP-пакет, визначає найкращий шлях для пакета, вкладає його в новий кадр і пересилає на наступний маршрутизатор по дорозі до місця призначення. Кожен маршрутизатор видаляє і додає нову інформацію кадру канального рівня перед пересиланням пакета.

6. Потім ці дані передаються по об'єднаній мережі, що складається з коштів підключення і проміжних пристроїв.

7. Клієнт отримує кадри канального рівня, що містять дані, що передаються. При обробці кадру заголовки протоколів видаляються в зворотному порядку. Спочатку обробляється і видаляється інформація Ethernet, слідом за нею - інформація IP-протоколу, потім TCP і, нарешті, HTTP.

8. Потім дані веб-сторінки передаються програмного забезпечення браузера клієнта.

Відкриті стандарти сприяють сумісності, конкуренції та інновацій. Крім того, вони гарантують, що продукт окремої компанії не зможе монополізувати ринок або отримати несправедливу перевагу в порівнянні з конкурентами.

Хороший приклад - покупка бездротового маршрутизатора для будинку. Існує безліч варіантів маршрутизаторів різних виробників, кожен з яких включає стандартні протоколи, такі як IPv4, DHCP, 802.3 (Ethernet) і 802.11 (бездротова мережа LAN). Відкриті стандарти також дозволяють клієнту з операційною системою OS X від компанії Apple завантажити веб-сторінку з веб-сервера під керуванням операційної системи Linux. Це пов'язано з тим, що обидві операційні системи використовують протоколи відкритих стандартів, наприклад з набору протоколів TCP / IP.

Організації по стандартизації відіграють важливу роль у підтримці відкритого Інтернету зі вільно доступною специфікацією і протоколами, які можуть бути реалізовані будь-яким постачальником. Організація з стандартизації може розробити набір правил самостійно або в інших випадках може вибрати приватний протокол в якості основи для стандарту. Якщо використовується приватний протокол, розробка стандарту, як правило, відбувається за участю постачальника, який його створив.

Організації по стандартизації зазвичай є незалежними від постачальників некомерційними організаціями, створеними для розробки і просування концепції відкритих стандартів.

Організації по стандартизації зазвичай є незалежними від постачальників некомерційними організаціями, створеними для розробки і просування

концепції відкритих стандартів. Кожна організація відіграє свою роль в розробці та просуванні стандартів протоколу TCP / IP.

За розвиток Інтернету відповідають наступні організації.

Суспільство Інтернет (Internet Society, ISOC) відповідає за сприяння відкритій розробці та розширенню використання Інтернету у всьому світі.

Рада по архітектурі мережі Інтернет (Internet Architecture Board, IAB) відповідає за загальне керівництво і розробку інтернет-стандартів.

Інженерна група з розвитку Інтернету (Internet Engineering Task Force, IETF) розробляє, оновлює і підтримує технології Інтернету і TCP / IP. Вона також випускає документи для розробки нових і оновлення існуючих протоколів, відомі як «Робочі пропозиції» (Request for Comments, RFC).

Дослідницька група інтернет-технологій (Internet Research Task Force, IRTF), яка проводить довгострокові дослідження Інтернету і протоколів TCP / IP, включає в себе Групу дослідження захисту від спаму (Anti-Spam Research Group, ASRG), Групу дослідження криптографічного захисту (Crypto Forum Research Group, CFRG) і Групу дослідження тимчасових мереж (Peer-to-Peer Research Group, P2PRG).

На рис. 2 показані наступні організації по стандартизації.

Корпорація з управління доменними іменами і IP-адресами (Internet Corporation for Assigned Names and Numbers, ICANN) - некомерційна організація в США, яка координує дії по виділенню IP-адрес, управління доменними іменами, а також іншими даними, що використовуються в протоколах TCP / IP.

Адміністрація адресного простору Інтернет (Internet Assigned Numbers Authority, IANA) відповідає за контроль і управління розподілом IP-адрес, управління доменними іменами і ідентифікаторами протоколів для ICANN.

Організації по стандартизації в галузі електроніки та зв'язку

Інші організації зі стандартизації займаються розробкою і просуванням стандартів в галузі електроніки та зв'язку, що застосовуються при доставці IP-пакетів у вигляді сигналів за допомогою проводового або бездротового засіб підключення.

Інститут інженерів з електротехніки та електроніки (Institute of Electrical and Electronics Engineers, IEEE; вимовляється по-англійськи «ай тріпл і») - організація, що займається впровадженням технологічних інновацій і створенням стандартів в різних галузях, включаючи енергетику, охорону здоров'я, телекомунікації та мережеві технології. На рис. 1 наведені деякі мережеві стандарти.

Альянс галузей електронної промисловості (Electronic Industries Alliance, EIA) найбільш відомий своїми стандартами, пов'язаними з електричною проводкою, роз'ємами і 19-дюймовими стійками, які використовуються для монтажу мережевого обладнання.

Асоціація телекомунікаційної промисловості (Telecommunications Industry Association, TIA) відповідає за розвиток стандартів зв'язку в різних областях, включаючи радіоустаткування, базові станції стільникового зв'язку, пристрої передачі голосу по IP (VoIP), супутниковий зв'язок та багато іншого.

Міжнародний союз електрозв'язку, сектор стандартизації телекомунікацій (International Telecommunications Union-Telecommunication Standardization

Sector, ITU-T) - одна з найбільших і найстаріших організацій за стандартами зв'язку. ITU-T визначає стандарти для стиснення відео, телебачення по протоколу IP (IPTV) і широкосмугового зв'язку, наприклад ліній DSL.

Багаторівнева модель для опису мережевих протоколів і операцій забезпечує наступні переваги.

Спрощення розробки протоколів, оскільки протоколи, що працюють на певному рівні, визначають формат оброблюваних даних і інтерфейс верхніх і нижніх рівнів.

Стимулювання конкуренції, так як продукти різних постачальників можуть взаємодіяти один з одним.

Запобігання впливу змін технологій або функцій одного рівня на інші рівні (верхні і нижні).

Спільну мову для опису функцій мережевої взаємодії.

Як показано на малюнку, модель TCP / IP і модель взаємодії відкритих систем (Open Systems Interconnection, OSI) - основні використовувані моделі функціонування мережі. Кожна з них являє собою базовий тип багаторівневої моделі мережевої взаємодії.

Протокольна модель відповідає структурі певного набору протоколів. TCP / IP є протокольною моделлю, оскільки в ній описуються функції, які виконуються на кожному рівні протоколів, що входять в набір протоколів TCP / IP. TCP / IP також використовується в якості еталонної моделі.

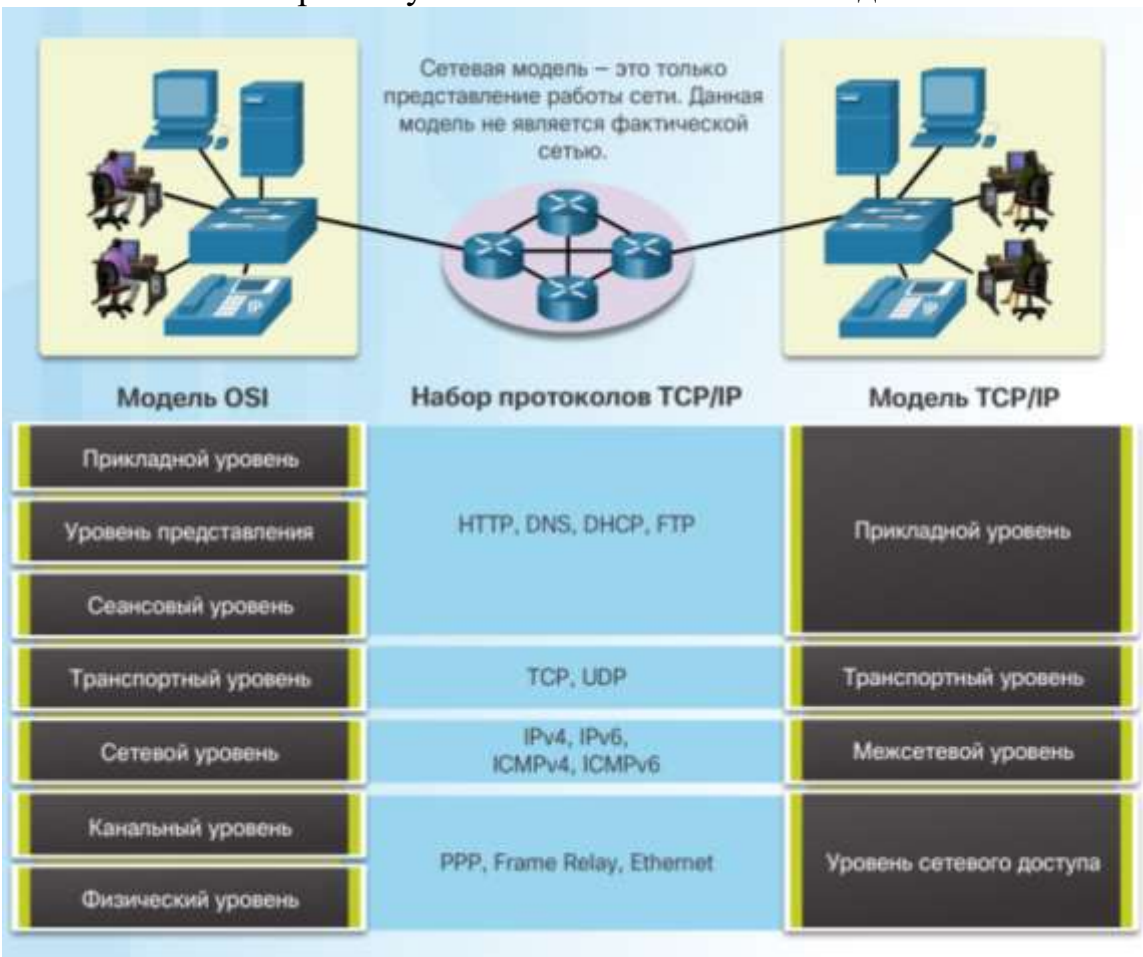


Рис. 1.1.20 Приклад протоколів які використовуються у моделі OSI та TCP/IP

Еталонна модель забезпечує однакове застосування всіх мережевих протоколів і сервісів, описуючи те, що необхідно зробити на певному рівні, але

не наказуючи конкретні способи виконання. Модель OSI є популярною еталонною моделлю об'єднаної мережі, одночасно будучи протокольної моделлю для набору протоколів OSI.

Модель OSI визначає широкий список функцій і сервісів, що реалізуються на кожному рівні. Крім того, вона описує взаємодію кожного рівня з вищим і нижчим рівнями. Розглянуті в рамках цього курсу протоколи TCP / IP співвідносяться як з моделлю OSI, так і з моделлю TCP / IP. Клацніть назву кожного рівня моделі OSI, щоб переглянути докладні відомості про нього.

Функціональні можливості кожного рівня і зв'язок між рівнями стануть більш зрозумілі в міру докладного розгляду протоколів у цьому курсі.

Примітка. Якщо рівні моделі TCP / IP позначаються тільки за назвою, то 7 рівнів моделі OSI часто позначаються за номером. Наприклад, фізичний рівень називається першим рівнем моделі OSI.

Протокольна модель мережевої взаємодії TCP / IP була створена на початку 70-х років і іноді називається моделлю мережі Інтернет. Як показано на малюнку, така модель визначає чотири категорії функцій, необхідних для успішної взаємодії. Архітектура набору протоколів TCP / IP побудована на основі цієї моделі. Ось чому модель Інтернету зазвичай називають моделлю TCP / IP.

Більшість протокольних моделей описує стек протоколів певного постачальника. Як приклад стека протоколів від певного постачальника можна назвати такі застарілі набори протоколів, як Novell Netware і AppleTalk. Проте оскільки модель TCP / IP представляє собою відкритий стандарт, жодна компанія не має права контролювати її визначення. Стандарт протоколів TCP / IP розглядається на загальнодоступному форумі і визначається в загальнодоступних документах RFC.

Порівняння моделей OSI і TCP / IP

Рис. 1.1.21 Порівняння моделі OSI та TCP/IP

Набір протоколів TCP / IP може бути описаний з точки зору еталонної моделі OSI. У моделі OSI рівень доступу до мережі і прикладний рівень моделі TCP / IP додатково підрозділяються для опису окремих функцій, які реалізуються на цих рівнях.

На рівні доступу до мережі набір протоколів TCP / IP не визначає список протоколів, використовуваних для передачі по фізичному засобу підключення; він описує тільки передачу з мережевого рівня фізичним мережевим протоколам. Рівні 1 і 2 моделі OSI описують процедури доступу до засобів підключення і фізичним засобам відправки даних по мережі.

Рівень 3 моделі OSI, або мережевий рівень, відповідає мережному рівню моделі TCP / IP. Цей рівень описує протоколи, що визначають шляхи передачі даних в мережі.

Рівень 4 моделі OSI, або транспортний рівень, відповідає транспортному рівню моделі TCP / IP. Цей рівень описує загальні сервіси та функції, які забезпечують впорядковану і надійну доставку даних від джерела до місця призначення.

Прикладний рівень TCP / IP включає в себе ряд протоколів, які підтримують певні функції для роботи різноманітних додатків кінцевих користувачів. Рівні 5, 6 і 7 моделі OSI використовуються в якості зразків розробниками і постачальниками прикладного програмного забезпечення для виробництва продуктів, призначених для роботи в мережі.

Обидві моделі (TCP / IP і OSI) широко застосовуються в відношенні протоколів різних рівнів. Так як модель OSI поділяє канальний і фізичний рівні, саме вона використовується для цих рівнів.

Теоретично одне повідомлення, наприклад відеокліп або повідомлення електронної пошти, може бути відправлено по мережі від джерела до місця призначення як один масивний і безперервний потік бітів. Якби повідомлення дійсно так передавалися, інші пристрої не змогли б відправляти і отримувати повідомлення в тій же мережі протягом всього процесу передачі даних. Такі великі потоки даних приводили б до суттєвих затримок. Крім того, якби будь-яка з ланок інфраструктури мережі відмовило під час передачі даних, ціле повідомлення було б втрачено і його необхідно було б передати повторно в повному обсязі.

В цьому випадку слід розділити дані на більш дрібні і зручні частини для передачі по мережі. Такий поділ потоку даних на більш дрібні частини називається сегментацією. Сегментація повідомлення надає дві основні переваги.

Відправка невеликих окремих частин від джерела до одержувача в мережі дозволяє підтримувати безліч різних чергуються сеансів обміну повідомленнями, це називається мультиплексування.

Сегментація дозволяє підвищити надійність мережевої взаємодії. Якщо будь-яку частину повідомлення не вдається доставити до місця призначення через відмову мережі, необхідно буде повторно передати тільки відсутні частини повідомлення.

Недолік використання сегментації і мультиплексування для передачі повідомлень через мережу - складність, яка властива всьому процесу. Уявіть собі, що необхідно відправити лист з 100 сторінок, але кожен конверт вміщує

лише одну сторінку. Процес написання адрес, наклеювання марок, отримання і відкриття всіх 100 конвертів забирає багато часу у відправника і одержувача.

В області мережевих комунікацій всі сегменти повідомлення повинні пройти подібний процес, щоб повідомлення було доставлено до потрібного місця призначення і було відтворено вміст вихідного повідомлення, .

Одиниця даних протоколу (PDU)

У міру того як дані додатків передаються по стеку протоколів до переміщення через засіб мережевого підключення, різні протоколи додають в них інформацію на кожному з рівнів. Це називається процесом інкапсуляції.

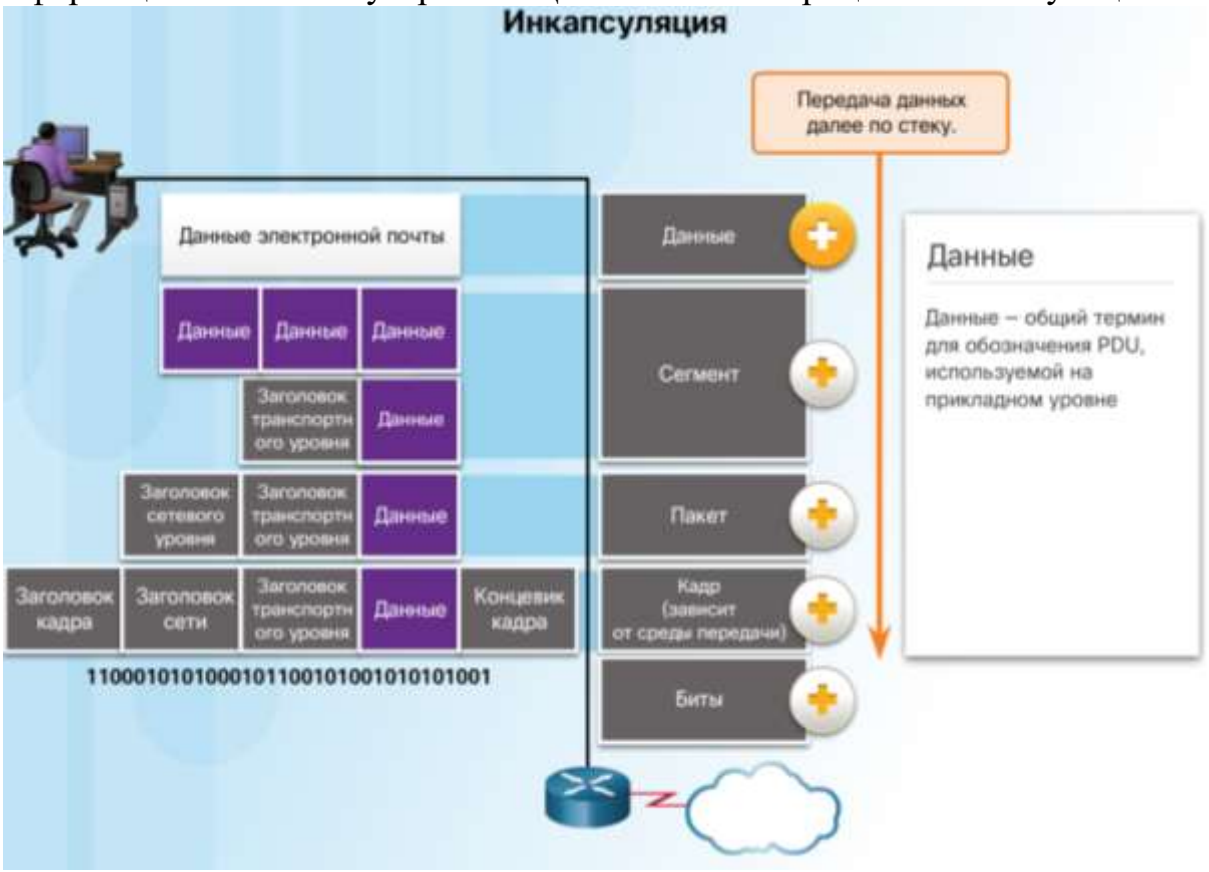


Рис. 1.1.22 Приклад інкапсуляції даних

Форма, яку приймає масив даних на кожному з рівнів, називається протокольним блоком даних (PDU). В ході інкапсуляції кожний наступний рівень інкапсулює PDU, отриману від вищого рівня відповідно до використовуваним протоколом. На кожному етапі процесу PDU отримує інше ім'я, що відбиває нові функції. Універсальної схеми іменування для PDU немає, і в цьому курсі PDU називаються відповідно до термінологією набору протоколів TCP / IP, як показано на малюнку. Щоб переглянути детальну інформацію клацніть кожну PDU на малюнку.

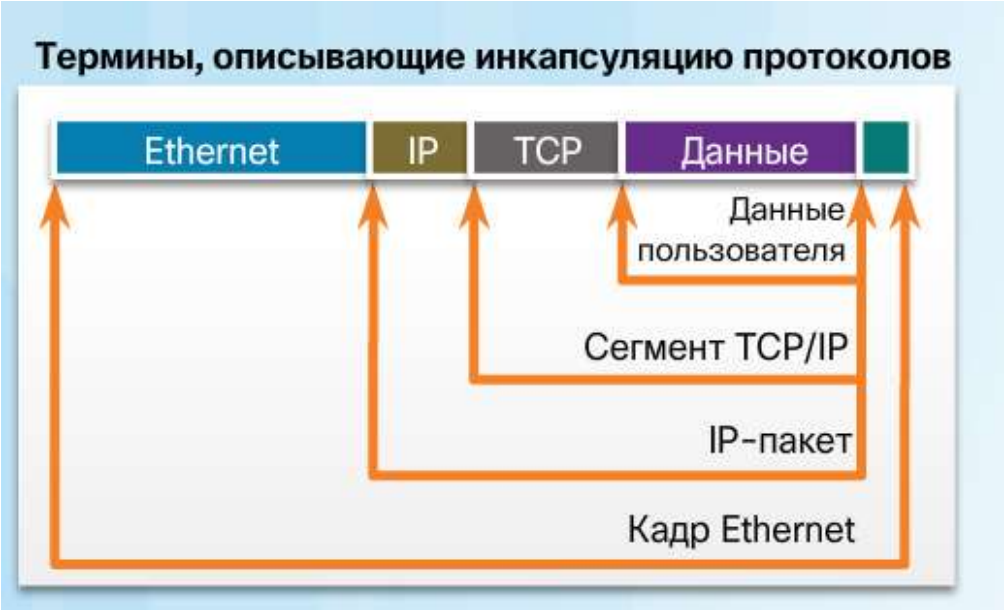


Рис. 1.1.23 Терміни які описують інкапсуляцію протоколів

При відправці повідомлення по мережі процес інкапсуляції йде від верхнього рівня до нижнього. Дані на кожному рівні виявляються вкладеними всередину інкапсульованого протоколу. Наприклад, сегмент TCP є частиною даних всередині IP-пакета.

Натисніть кнопку «Відтворення» на малюнку і подивіться, як йде процес інкапсуляції, коли веб-сервер відправляє веб-сторінку веб-клієнта.

Зворотний процес на приймаючому вузлі називається деінкапсуляцією. Деінкапсуляція - це процес видалення одного або декількох заголовків пристроєм одержувача. У міру просування даних по стеку до додатків для кінцевих користувачів вони деінкапсуліруются.

Мережевий і канальний рівні відповідають за передачу даних з пристрою-джерела на пристрій призначення. , протоколи на обох рівнях містять адреси джерела і місця призначення, але ці адреси служать різним цілям.

Адреса джерела і місця призначення мережевого рівня необхідний для доставки IP-пакета від джерела до місця призначення в тій же або у віддаленій мережі.

Адреса джерела і місця призначення канального рівня необхідний для доставки кадру каналу даних від однієї мережевої інтерфейсної плати (NIC) до іншої мережевої інтерфейсної плати в тій же мережі.

IP-адреса - це логічний адресу мережевого рівня, або рівня 3, необхідний для доставки IP-пакета від джерела до місця призначення, .

IP-пакет містить два IP-адреси.

IP-адреса джерела - IP-адреса пристрою-відправника, початкового джерела пакета.

IP-адреса місця призначення - IP-адреса пристрою-одержувача, кінцевого місця призначення пакету.

Адреси канального рівня

Фізична адреса канального рівня (рівня 2) грає іншу роль. Призначення адреси канального рівня - доставити кадр каналу даних з одного мережевого інтерфейсу на інший в одній і тій же мережі. Цей процес показаний на рис. 1-3.

Перш ніж IP-пакет можна буде відправити провідний або бездротової мережі, його необхідно інкапсулювати в кадр каналу даних для подальшого переміщення по фізичній засобу підключення.

В ході пересилання IP-пакетів від вузла до маршрутизатора, між маршрутизаторами і, нарешті, від маршрутизатора до вузла в кожній точці на шляху свого проходження IP-пакет інкапсулюється в новий кадр каналу передачі даних. Кожен кадр канального рівня містить адресу каналу-джерела (який передав цей кадр мережевої плати) та адреса каналу призначення (мережевий плати, що приймає цей кадр).

Протокол канального рівня (рівня 2) використовується тільки для доставки пакета між мережевими інтерфейсними платами в одній мережі. Маршрутизатор видаляє інформацію рівня 2 після отримання пакету мережевий інтерфейсної платою і додає нову інформацію канального рівня перед пересиланням пакета інший мережевий інтерфейсної плати по дорозі до місця призначення.

На канальному рівні IP-пакет інкапсулюється в кадр, що містить наступну інформацію канального рівня.

Адреса джерела канального рівня - фізичну адресу мережевої інтерфейсної плати пристрою, який передає пакет.

Адреса місця призначення канального рівня - фізичну адресу мережевої інтерфейсної плати пристрою, який отримує пакет. Це адреса найближчого транзитного маршрутизатора або пристрою призначення.

Щоб зрозуміти, як пов'язані пристрої в мережі, важливо зрозуміти роль як адрес мережевого рівня, так і адрес канального рівня.

Адреси мережевого рівня, або IP-адреси, являють собою мережеві адреси джерела і місця призначення. IP-адреса складається з двох частин.

Мережева частина - ліва частина адреси, яка визначає, якої мережі належить IP-адреса. Всі пристрої в одній мережі матимуть однакову мережеву частину адреси.

Вузлова частина - інша частина адреси, яка визначає конкретний пристрій в мережі. Вузлова частина унікальна для кожного пристрою в мережі.

Примітка. Маска підмережі використовується для відділення мережевий частини від вузлової частини. Маска підмережі розглядається в наступних розділах.

В даному прикладі є клієнтський комп'ютер (PC1), який взаємодіє з файловим сервером (FTP server), що знаходяться в тій же IP-мережі.

IP-адреса джерела - IP-адреса пристрою-відправника, клієнтського комп'ютера PC1: 192.168.1.110.

IP-адреса місця призначення - IP-адреса пристрою-одержувача, FTP server: 192.168.1.9.

Зверніть увагу, що на малюнку мережева частина IP-адреси джерела і IP-адреси місця призначення належать одній мережі.

Роль адрес канального рівня

Якщо відправник і одержувач IP-пакета знаходяться в одній і тій же мережі, кадр каналу даних відправляється безпосередньо приймаючому пристрою. У мережі Ethernet адреси каналу даних називаються MAC-адресою

(Media Access Control) Ethernet. MAC-адреси фізично присвоєні мережевий інтерфейсної плати Ethernet.

MAC-адресу джерела - це адреса канального рівня, або MAC-адресу Ethernet пристрою, що відправляє кадр каналу даних з інкапсульованим IP-пакетом. MAC-адресу мережевої інтерфейсної плати Ethernet PC1: AA-AA-AA-AA-AA-AA в шестнадцатиричном поданні.

MAC-адресу місця призначення - адреса канального рівня пристрою одержувача, якщо воно знаходиться в тій же мережі, що і пристрій-відправник. У цьому прикладі MAC-адресою одержувача є MAC-адресу файлового сервера (FTP server): CC-CC-CC-CC-CC-CC в шестнадцатиричном поданні.

Тепер кадр з інкапсульованим IP-пакетом може бути переданий безпосередньо з PC1 на FTP server.

Яка роль адреси мережевого рівня і адреси канального рівня при взаємодії між своїм пристроєм і пристроєм у віддаленій мережі? В даному прикладі є клієнтський комп'ютер (PC1), який взаємодіє з сервером (Web Server), що знаходиться в іншій IP-мережі.

Якщо відправник і одержувач пакета знаходяться в різних мережах, IP-адреси джерела і місця призначення представлятимуть вузли в різних мережах. На це буде вказувати мережева частина IP-адреси вузла призначення.

IP-адреса джерела - IP-адреса пристрою-відправника, клієнтського комп'ютера PC1: 192.168.1.110.

IP-адреса місця призначення - IP-адреса пристрою-одержувача, Web Server: 172.16.1.99.

Зверніть увагу, що на малюнку мережева частина IP-адреси джерела і IP-адреси місця призначення належать різним мережам.

Якщо відправник і одержувач IP-пакета знаходяться в різних мережах, кадр каналу даних Ethernet не може бути відправлений безпосередньо до вузла призначення, оскільки він недоступний в мережі відправника. Кадр Ethernet потрібно вислати на інший пристрій: маршрутизатор або шлюз. У нашому прикладі шлюз - R1. R1 має адресу каналу даних Ethernet в тій же мережі, що і PC1. Це дозволяє PC1 отримати доступ до маршрутизатора безпосередньо.

MAC-адресу джерела - MAC-адресу Ethernet відправляє пристрої, PC1. MAC-адресу інтерфейсу Ethernet на PC1 - AA-AA-AA-AA-AA-AA.

MAC-адресу місця призначення - пристрій-відправник використовує MAC-адресу Ethernet шлюзу або маршрутизатора, якщо отримує і передає пристрою знаходяться в різних мережах. У цьому прикладі MAC-адресою місця призначення є MAC-адресу інтерфейсу Ethernet R1 (11-11-11-11-11-11). Цей інтерфейс прикріплений до тієї ж мережі, що і PC1.

Кадр Ethernet з інкапсульованим IP-пакетом тепер може бути переданий на R1. R1 пересилає пакет до місця призначення (Web Server). Це може означати, що R1 пересилає пакет на інший маршрутизатор або безпосередньо на Web Server, якщо він знаходиться в одній з мереж, підключених до R1.

Для кожного вузла в локальній мережі важливо правильно налаштувати IP-адреса основного шлюзу. Всі пакети, призначені для відправки в віддалену мережу, направляються на шлюз за замовчуванням. MAC-адреси Ethernet і шлюз за замовчуванням розглядаються в наступних розділах.

Мережі даних - це системи кінцевих і проміжних пристроїв, а також кошти мережевого підключення, що з'єднують ці пристрої. Для успішного обміну даними ці пристрої повинні знати, як обмінюватися інформацією.

Ці пристрої повинні відповідати правилам і протоколам, який регламентує процес обміну даними. TCP / IP - приклад набору протоколів. Більшість протоколів створюється організаціями зі стандартизації, такими як IETF або IEEE. Інститут інженерів з електротехніки та електроніки (IEEE) - професійна організація для фахівців, що працюють в області електротехніки та електроніки. Міжнародна організація по стандартизації (ISO) є найбільшим в світі розробником міжнародних стандартів для широкого спектру продуктів і послуг.

Найбільш широко поширеними мережевими моделями є моделі OSI і TCP / IP. Зв'язування протоколів, які використовуються для визначення правил передачі даних на різних рівнях цих моделей, корисно для розуміння того, які пристрої і сервіси застосовуються в певних точках, коли дані проходять через мережі LAN і WAN.

Дані, що проходять вниз по стеку моделі OSI, сегментируются на частини і інкапсулюються з адресами і іншими атрибутами. Потім цей процес йде в зворотному напрямку - ці частини декапсуліруются і передаються вгору по стеку протоколів в місці призначення. Модель OSI описує процеси шифрування, форматування, сегментації і інкапсуляції даних для подальшої передачі по мережі.

Набір протоколів TCP / IP - це протокол відкритого стандарту, прийнятий галузевими компаніями і затверджений організацією зі стандартизації. Набір протоколів IP - це набір протоколів, необхідний для передачі і отримання інформації за допомогою мережі Інтернет.

Назви одиниць даних протоколу складаються відповідно до структури протоколів з набору TCP / IP: дані, сегмент, пакет, кадр і біти.

Застосування моделей дозволяє окремим особам, компаніям і професійним асоціаціям аналізувати поточні мережі і проектувати мережі майбутнього.

Мережевий доступ

У моделі взаємодії відкритих систем (OSI) функції мережі передачі даних розділені на кілька рівнів. При передачі даних кожен рівень взаємодіє з рівнями, ієрархічно розташованими вище і нижче по відношенню до нього. Два з рівнів моделі OSI пов'язані між собою настільки тісно, що, відповідно до моделі TCP / IP, фактично є єдиним рівнем. Це наступні 2 рівня: канальний рівень і фізичний рівень.

На Користувач пристрою саме канальний рівень забезпечує підготовку даних до їх передачі та управління доступом даних до фізичної середовищі. Однак передачею даних в фізичну середу управляє фізичний рівень, який формує сигнали шляхом кодування двійкових розрядів даних.

На приймаючій стороні фізичний рівень приймає сигнали з коштів підключення. Після декодування сигналу назад в дані фізичний рівень передає кадр на канальний рівень для контролю, прийому і обробки.

На початку цього розділу представлена інформація про основні функції фізичного рівня, а також про стандарти і протоколи, які керують передачею даних по фізичному середовищі локальної мережі. Крім того, в цьому розділі розповідається про функції канального рівня і пов'язаних з ним протоколах.

Рівень доступу до мережі на основі стека протоколів TCP / IP еквівалентний канального рівня (рівень 2) і фізичного рівня (рівень 1) OSI.

Фізичний рівень OSI забезпечує засоби транспортування бітів, що утворюють кадр даних канального рівня, по засобу мережевого підключення. Фізичні компоненти - це електронні пристрої, засоби підключення, а також інші з'єднувачі і роз'єми, що забезпечують передачу сигналів, за допомогою яких представлені біти інформації. Всі апаратні компоненти, в тому числі мережні інтерфейсні плати (NIC), інтерфейси і з'єднувачі, а також матеріали і конструкція кабелів описані в стандартах, що відносяться до фізичного рівня. Стандарти фізичного рівня регламентують три функціональні області: фізичні компоненти, методи кодування кадрів і способи передачі сигналів.

Для роботи мережі важливо забезпечити необхідний засіб підключення. Без належного фізичного підключення (проводового або бездротового) зв'язок між двома пристроями буде неможлива.

Провідна зв'язок здійснюється за допомогою мідних і оптоволоконних кабелів.

У мережах використовуються три основні типи мідних кабелів: неекранована кручена пара (UTP), екранована кручена пара (STP) і коаксіальний кабель. Кабелі UTP є найбільш поширеною середовищем передачі на основі мідного дроту.

Оптоволоконні кабелі в даний час широко використовуються для підключення пристроїв мережевої інфраструктури. Вони забезпечують більш високу дальність передачі і пропускну спроможність (швидкість передачі даних), ніж інші засоби підключення. На відміну від мідних проводів оптоволоконний кабель дозволяє передавати сигнали з більш низьким загасанням. Такий кабель також абсолютно несприйнятливий до впливу електромагнітних і радіочастотних перешкод.

Засоби бездротового підключення забезпечують передачу двійкових розрядів даних у вигляді електромагнітних сигналів радіочастотного або мікрохвильового діапазону.

Число пристроїв, що підтримують бездротовий зв'язок, продовжує збільшуватися. Саме тому кошти бездротового підключення стали найпопулярнішою середовищем для домашніх мереж і швидко набирають популярність в корпоративних мережах.

Канальний рівень відповідає за обмін кадрами між вузлами через фізичне середовище передачі даних. Він забезпечує доступ до середовища передачі даних для вищих рівнів, а також управляє способами прийому і передачі даних в цьому середовищі.

У різних варіантах реалізації протоколів канального рівня застосовуються різні способи управління доступом до середовища. Ці методи управління доступом до середовища визначають, чи використовують вузли дане середовище спільно і яким чином це відбувається. Вибір способу управління доступом до середовища залежить від топології і наявності необхідності спільного доступу до середовища. Топології локальної та глобальної мережі можуть бути фізичними або логічними. Саме логічна топологія впливає на вибір типу кадрування в мережі і управління доступом до середовища. Глобальні мережі зазвичай реалізуються за допомогою топології типу «точка-точка» (point-to-point), «зірка» (hub and spoke) або «ячеистая» (mesh). У локальних мережах зі спільним використанням середовища передачі кінцеві пристрої можуть з'єднуватися з використанням зіркоподібній (star), шинної (bus), кільцевої (ring) або розширеної зіркоподібній (extended star) фізичної топології.

Всі протоколи канального рівня інкапсулюють одиницю даних протоколу (PDU) рівня 3 в межах поля даних кадру. Однак структура кадру і полів, що містяться в заголовку і кінцівки, відрізняється в залежності від протоколу.

типи підключень

Незалежно від того, підключаєтеся ви до домашнього локального принтера або ж до веб-сайту в іншій країні, для передачі даних по мережі необхідно спочатку встановити фізичне підключення до локальної мережі. Як фізичного підключення може використовуватися дротове з'єднання за допомогою кабелю або бездротове з'єднання по радіоканалу.

Тип використовуваного фізичного підключення залежить від конфігурації мережі. Наприклад, в офісах багатьох компаній співробітники використовують настільні комп'ютери або ноутбуки, фізично підключені кабелями до загального комутатора. Мережі такого типу називають провідними. Дані в них передаються з фізичного кабелю.

Крім можливості проводового підключення багато компаній забезпечують бездротове підключення для ноутбуків, планшетних комп'ютерів і смартфонів. При використанні бездротових пристроїв дані передаються за допомогою радіохвиль. Бездротове підключення поширюється по мірі того, як приватні користувачі і компанії оцінюють його переваги. При бездротовому підключенні пристрою в бездротовій мережі повинні підключатися до бездротової точки доступу (access point, AP).

Рис. 1.1.24 Вигляд WI-FI роутера

Комутатори і бездротові точки доступу - це зазвичай два окремі види спеціалізованих пристроїв, розгорнутих в мережі. Однак також існують пристрої, що забезпечують можливість як проводового, так і бездротового підключення. Наприклад, багато індивідуальні користувачі застосовують домашні маршрутизатори з інтегрованими послугами (ISR), як показано на малюнку 1. Маршрутизатор ISR мають комутаційний компонент з декількома портами, що дозволяє підключати кілька пристроїв до локальної мережі (LAN) за допомогою кабелів, як показано на малюнку 2 . Крім того, до складу багатьох маршрутизаторів ISR також входить точка доступу (AP), що забезпечує підключення бездротових пристроїв.

Мережеві інтерфейсні плати

Мережеві інтерфейсні плати (Network Interface Card, NIC) служать для підключення пристрою до мережі. Мережеві плати Ethernet використовуються для проводового підключення, як показано на малюнку 1, а мережеві плати бездротової локальної мережі (Wireless Local Area Network, WLAN) - для бездротового підключення. Пристрій кінцевого користувача може містити один або обидва типи мережевих плат. Наприклад, якщо мережевий принтер оснащений тільки мережевою платою Ethernet, то він повинен підключатися до мережі за допомогою кабелю Ethernet. Інші пристрої, наприклад планшети і смартфони, можуть бути оснащені тільки мережевою платою WLAN і тому для них необхідно використовуватися бездротове підключення.

З точки зору продуктивності не всі фізичні з'єднання рівноцінні.

Наприклад, продуктивність бездротового пристрою може знижуватися при збільшенні відстані до бездротової точки доступу. Чим далі пристрій знаходиться від точки доступу, тим слабкіше одержуваний їм сигнал. Це може призводити до зниження пропускної здатності або повній відсутності бездротового зв'язку. Для ретрансляції бездротового сигналу в ті частини будинку, які розташовані занадто далеко від бездротової точки доступу, можна використовувати підсилювач бездротового сигналу. Продуктивність проводового підключення, на відміну від бездротового, не погіршується.

Всі бездротові пристрої змушені спільно використовувати радіоканали бездротової точки доступу. Це означає, що при одночасному підключенні великої кількості бездротових пристроїв до мережі її продуктивність може знизитися. Провідним пристроям не потрібно ділити ресурси доступу до мережі з іншими пристроями. Кожне проводове пристрій має окремий канал зв'язку за своїм кабелю Ethernet. Це важливо враховувати при роботі з деякими програмами, такими як онлайн-іграми, потоковим відео і відеоконференціями, для яких необхідна більш висока пропускна здатність в порівнянні з іншими додатками.

Далі ви докладніше ознайомитеся з підключеннями фізичного рівня і дізнаєтеся про те, як вони впливають на передачу даних.

фізичний рівень

Фізичний рівень OSI забезпечує засоби транспортування бітів, що утворюють кадр даних канального рівня, за коштами мережевого підключення. Цей рівень приймає від канального рівня цілий кадр даних і кодує його у вигляді послідовності сигналів, які потім пересилаються по засобу підключення локальної мережі. Закодовані біти, з яких складається кадр, приймаються або кінцевим, або проміжним пристроєм.

В ході передачі від вузла джерела до вузла призначення (вузлу-адресату) дані піддаються таким перетворенням.

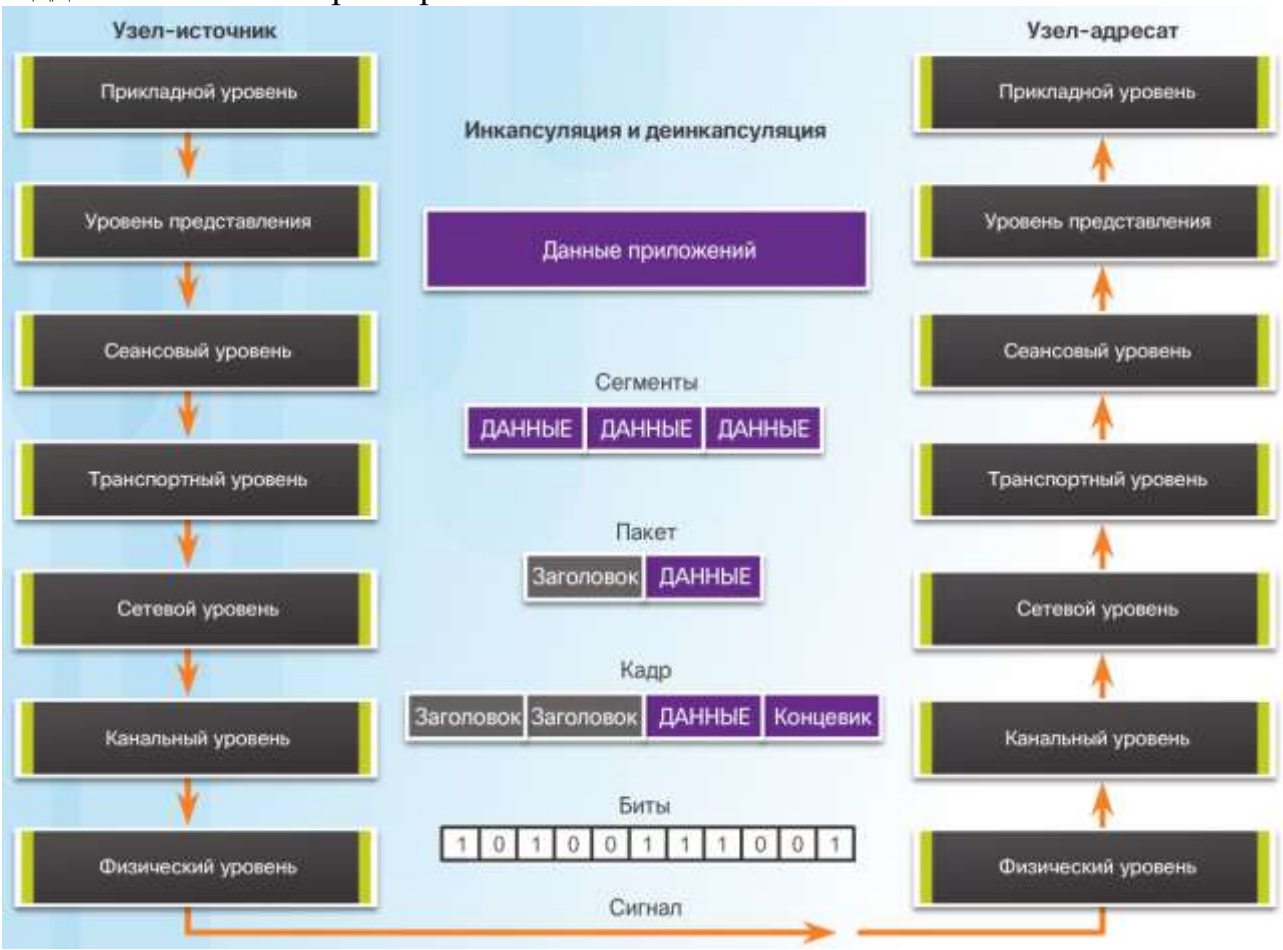


Рис. 1.1.25 Процес формування PDU файла

На транспортному рівні призначені для користувача дані сегментуються, на мережевому - розподіляються по пакетам, а потім інкапсулюються в кадри канального рівня.

Фізичний рівень кодує кадри і формує електричні, оптичні або радіосигнали, за допомогою яких представлена інформація про бітах в кожному кадрі.

Потім ці сигнали послідовно передаються по засобам підключення.

Фізичний рівень вузла призначення приймає ці окремі сигнали від засобів підключення, відновлює подаються ними біти і передає ці біти на канальний рівень у вигляді цілого кадру.

Засоби підключення фізичного рівня

Існує три основних типи засобів мережевого підключення. Фізичний рівень створює уявлення бітів і групує їх для кожного з цих типів наступним чином.

Мідний кабель: сигнали являють собою послідовність електричних імпульсів.

Оптоволоконний кабель: сигнали являють собою керовані зміни світлового випромінювання.

Бездротова мережа: сигнали являють собою радіосигнали мікрохвильового діапазону.

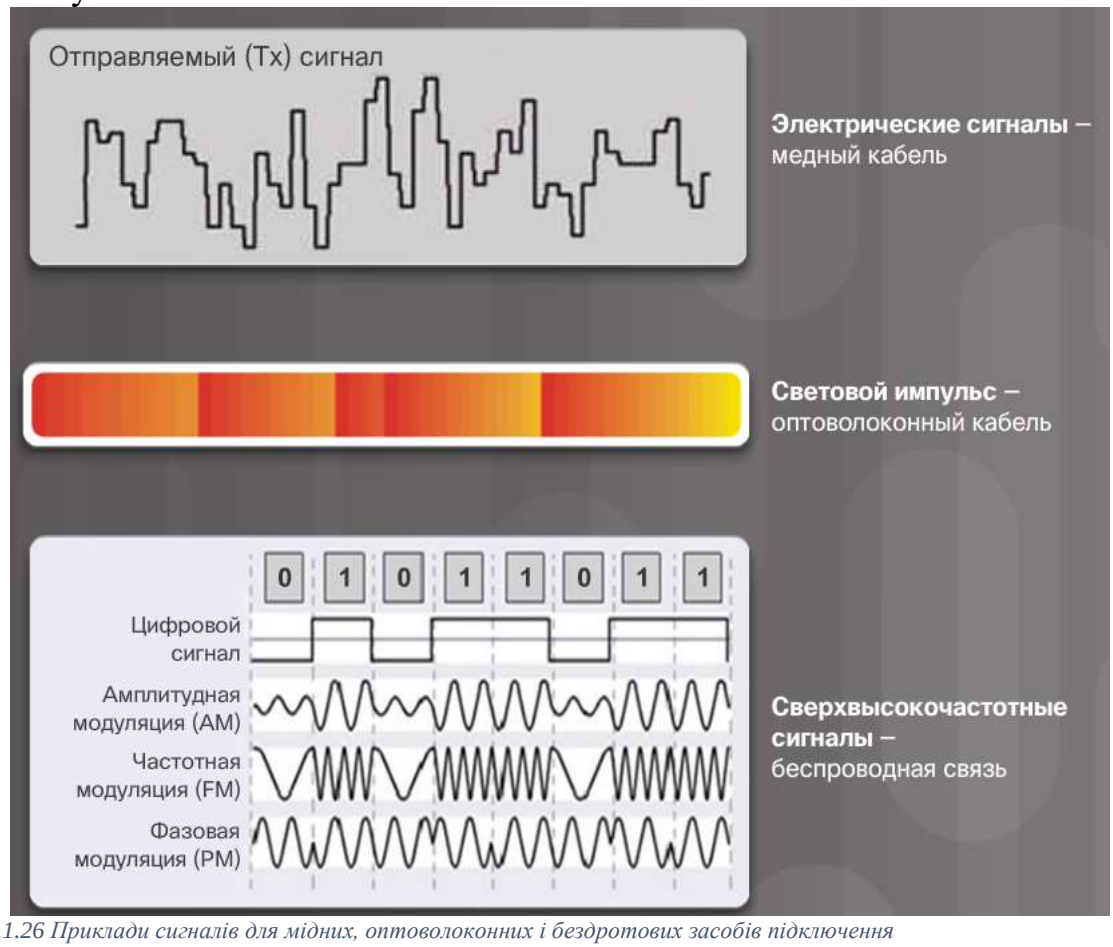


Рис. 1.1.26 Приклади сигналів для мідних, оптоволоконних і бездротових засобів підключення

Для забезпечення функціональної сумісності на фізичному рівні всі аспекти цих функцій регламентуються організаціями зі стандартизації.

Стандарти фізичного рівня

Протоколи і операції вищих рівнів моделі OSI реалізовані в програмному забезпеченні, створеному розробниками програмного забезпечення та комп'ютерними фахівцями. Служби і протоколи в стеці протоколів TCP / IP визначаються Інженерної групою з розвитку Інтернету (IETF).

Фізичний рівень складається з електронних схем, засобів підключення і роз'ємів, що розробляються інженерами. Тому закономірно, що стандарти, які регламентують це обладнання, визначаються відповідними організаціями з електротехніки та зв'язку.

Рис. 1.1.27 Стандарти Фізичного рівня моделі OSI

У створенні та реалізації стандартів фізичного рівня бере участь цілий ряд різних міжнародних і національних організацій, урядових регулюючих організацій, а також приватних компаній. Наприклад, стандарти на обладнання, засоби підключення, кодування і сигнали фізичного рівня розробляють такі організації.

- Міжнародна організація по стандартизації (ISO)
- Асоціація телекомунікаційної промисловості / Асоціація електронної промисловості (TIA / EIA)
- Міжнародний союз електрозв'язку (ITU)
- Американський національний інститут стандартизації (ANSI)
- Інститут інженерів з електротехніки та електроніки (IEEE)

Регіональні органи регулювання телекомунікацій, в тому числі Федеральна комісія із зв'язку (FCC) в США і Європейський інститут телекомунікаційних стандартів (ETSI)

Крім цього, нерідко місцеві специфікації розробляються регіональними групами по кабельних стандартам, наприклад CSA (Канадська асоціація по стандартизації), CENELEC (Європейський комітет електротехнічної стандартизації) і JSA / JIS (Японська асоціація по стандартизації).

функції

Стандарти фізичного рівня регламентують три функціональні області.

Фізичні компоненти - це електронні пристрої, засоби підключення, а також інші з'єднувачі і роз'єми, що забезпечують передачу сигналів, за допомогою яких представлені біти інформації. Всі апаратні компоненти, в тому числі мережні інтерфейсні плати (NIC), інтерфейси і з'єднувачі, а також матеріали і

конструкція кабелів описані в стандартах, що відносяться до фізичного рівня. Різні порти і інтерфейси маршрутизатора Cisco 1941 також є прикладами фізичних компонентів, роз'єми і схеми підключення контактів для яких визначаються стандартами.

кодування

Кодування (фізичне кодування) - це спосіб перетворення потоку бітів в певний «код». Коди - це групи бітів, що використовуються для формування передбачуваних комбінацій, які можуть розпізнаватися як відправником, так і одержувачем. У мережі під кодуванням розуміються зміни напруги або струму згідно із заданими правилами з метою представлення значень бітів: нулів і одиниць.

Наприклад, при манчестерському кодуванні нулі будуть представлені переходом від високої напруги до низького; а одиниці - переходом від низької напруги до високого. Приклад манчестерського кодування показаний на малюнку 1. Перехід станів сигналу відбувається в середині кожного бітового інтервалу. Цей тип кодування застосовується в ранніх модифікаціях Ethernet зі швидкістю 10 Мбіт / с. Для більш високих швидкостей передачі потрібно більш складне кодування.

Способи передачі сигналів

Для представлення значень бітів «1» і «0» в середовищі передачі фізичний рівень повинен генерувати електричні, оптичні або радіосигнали. Метод уявлення бітів за допомогою сигналів називається способом передачі сигналів. Стандарти фізичного рівня повинні визначати, який тип сигналу відповідає одиниці («1»), а який нулю («0»). Для передачі сигналу можна використовувати просте зміна тривалості електричного або оптичного імпульсу. Наприклад, довгий імпульс може позначати 1, а короткий - 0.

Цей спосіб аналогічний кодування за допомогою азбуки Морзе. Азбука Морзе - це один із способів передачі текстових повідомлень по телефонних дротах або між судами в море за допомогою звукових або світлових імпульсів або натискань телеграфного ключа різної тривалості.

Рис. 1.1.28 Манчестерське кодування

Існує безліч способів передачі сигналів. Найбільш поширений спосіб передачі даних - із застосуванням модуляції. Модуляція - це процес зміни параметрів однієї хвилі (т. Н. Несучої) згідно характеристикам інший хвилі (сигналу).

Природа фактичних сигналів, що представляють біти в засобах підключення, буде залежати від використовуваного способу передачі.

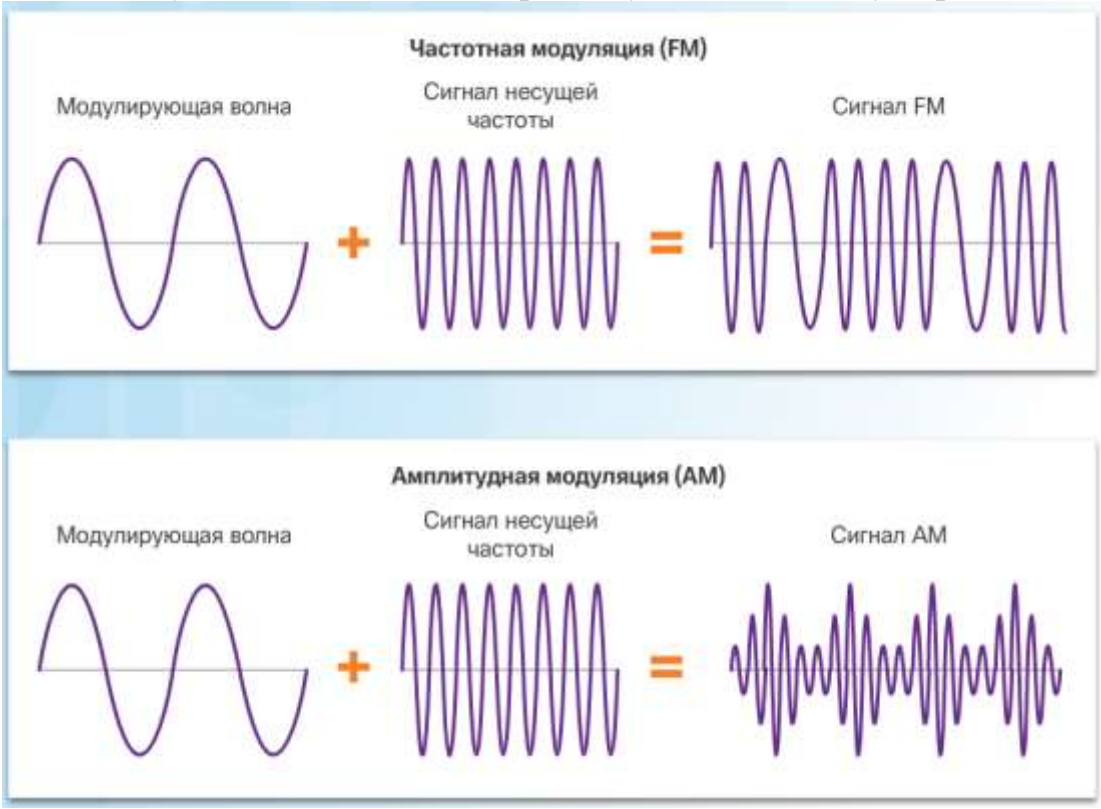


Рис. 1.1.29 Частотна модуляція сигналу

Пропускна здатність

Різні фізичні засоби підключення підтримують різні швидкості передачі бітів. Основними характеристиками передачі даних є пропускна здатність (bandwidth) і продуктивність (throughput).

Пропускна здатність (bandwidth) - це кількісна характеристика, що відображає можливості передачі даних по конкретному засобу підключення. У цифрових мережах під пропускною спроможністю розуміється обсяг даних, який можна передати з однієї точки в іншу за певний час. Зазвичай пропускна здатність вимірюється в кілобітах в секунду (Кбіт/с), мегабитах в секунду (Мбіт/с) або гігабіта в секунду (Гбіт/с). Іноді під пропускною спроможністю розуміють швидкість доставки бітів, хоча це не зовсім точно. Наприклад, і в мережі Ethernet 10 Мбіт/с, і в мережі Ethernet 100 Мбіт/с біти передаються зі швидкістю поширення електричного сигналу. Різниця полягає в кількості бітів, переданих в секунду.

Фактична пропускна здатність мережі визначається поєднанням наступних факторів.

Властивості фізичних засобів підключення

Технології передачі і виявлення сигналів в мережі

На реальну пропускну здатність впливають властивості фізичних засобів підключення, використовувані технології і закони фізики.

продуктивність

Продуктивність (throughput) - це кількість бітів, що передаються за коштами підключення за певний період часу.

Через безліч чинників продуктивність (throughput) зазвичай не відповідає заявленій пропускної здатності (bandwidth) в реалізаціях на фізичному рівні. На продуктивність впливає ряд факторів, в тому числі такі.

- обсяг трафіку
- Тип трафіку

Сумарна затримка, що залежить від кількості мережевих пристроїв між джерелом і пунктом призначення

Затримки в мережі впливають на підсумкове час, необхідний для доставки даних з однієї точки в іншу.

Продуктивність мережі, що складається з декількох мереж або декількох сегментів, не може перевищувати швидкість самого повільного з'єднання між джерелом і одержувачем. Навіть якщо все або більшість сегментів мають високу пропускну здатність, один-єдиний сегмент з низькою продуктивністю створить вузьке місце і продуктивність всієї мережі буде знижена.

Існує безліч веб-сервісів перевірки швидкості, що дозволяють дізнатися реальну продуктивність інтернет-з'єднання. На малюнку показаний приклад результату тестування швидкості.

Існує також третій параметр, що характеризує передачу корисних даних, який називається корисною пропускною здатністю (goodput). Корисна пропускна здатність - це обсяг корисних даних, що передаються за певний період часу. Корисна пропускна здатність (goodput) дорівнює продуктивності (throughput) за вирахуванням службового трафіку, необхідного для створення сеансів, підтверджень і інкапсуляції.

Типи фізичних засобів підключення

Фізичний рівень забезпечує подання потоку бітів у вигляді змін рівнів напруги, модульованих радіочастотних сигналів або світлових імпульсів. Організаціями зі стандартизації були спільно вироблені вимоги до фізичних, електричних та механічних властивостей засобів підключення для різних видів комунікацій. Ці специфікації гарантують належну роботу кабелів і роз'ємів з різними реалізаціями канального рівня.

Наприклад, для засобів підключення на основі мідного кабелю визначено такі стандарти.

- Тип використовуваного мідного кабелю
- Пропускна здатність
- Тип використовуваних роз'ємів
- Призначення і кольорове маркування контактів роз'ємів кошти підключення
- Максимально допустима довжина кабелю

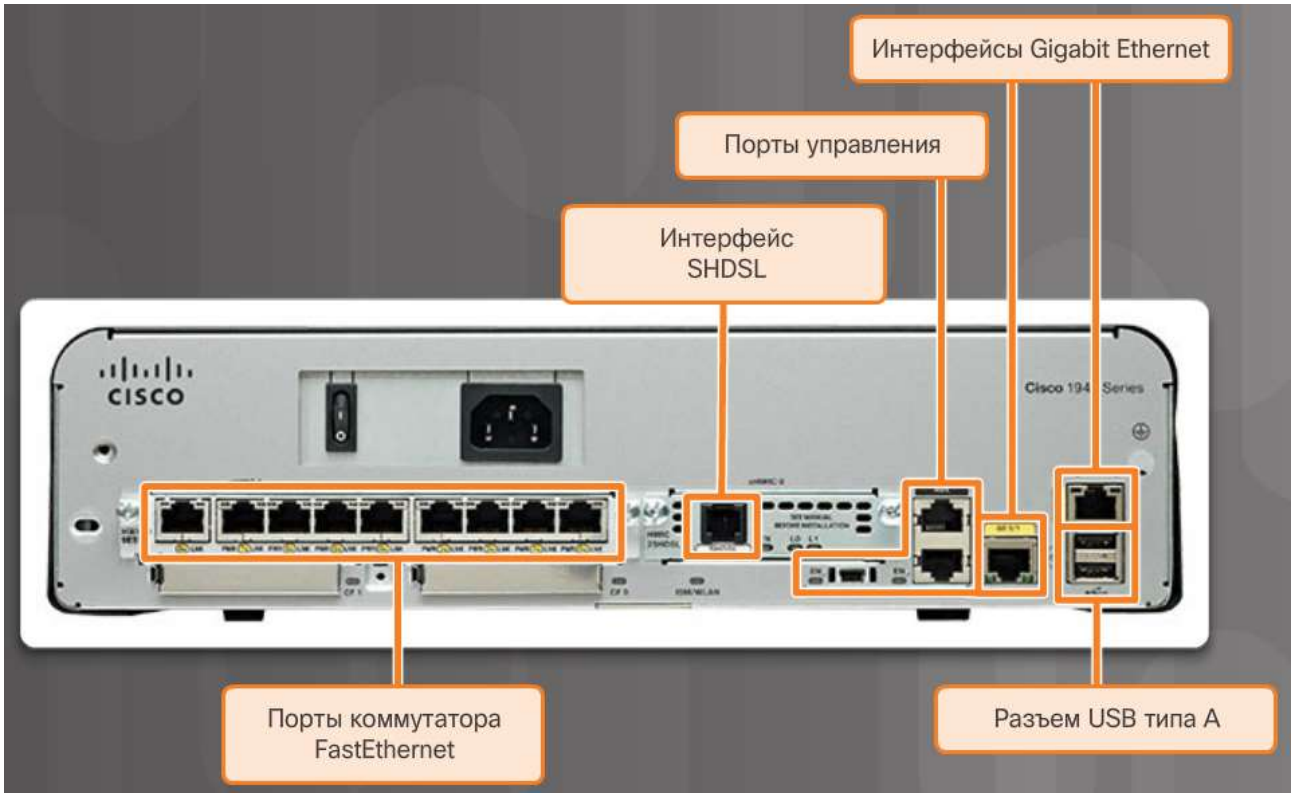


Рис. 1.1.30 Типи інтерфейсів і портів, наявні в маршрутизаторі 1941.

Характеристики мідних кабелів

Мідні кабелі використовуються в мережах через їх невисоку вартість, простоти монтажу і низького електричного опору. Однак при передачі сигналів по мідних кабелях можуть бути встановлені обмеження по дальності передачі і завадостійкості.

Дані по мідних кабелях передаються у вигляді електричних імпульсів. Приймач в мережевому інтерфейсі цільового пристрою повинен отримати такий сигнал, який можна легко декодувати для відновлення відправленого сигналу. Однак чим більше дальність передачі сигналу, тим сильніше він спотворюється. Це називається загасанням сигналів. Тому для всіх засобів підключення на основі мідних кабелів в стандартах встановлені суворі обмеження на дальність передачі.

Тимчасові характеристики і значення напруги електричних імпульсів також схильні до впливу таких джерел перешкод.

Електромагнітні перешкоди (ЕМП) або радіочастотні перешкоди (РЧП). Сигнали ЕМП і РЧП можуть спотворювати і порушувати сигнали даних, що передаються по мідному кабелю. Потенційними джерелами ЕМП та РЧП є джерела радіочастотного випромінювання та електромагнітні пристрої, наприклад флуоресцентні лампи або електродвигуни (див. Малюнок).

Перехідні перешкоди. Це перешкоди, викликані впливом електричних або магнітних полів сигналу одного кабелю на сигнал сусіднього кабелю. У телефонних каналах перехідні перешкоди можуть призвести до часткової чутності стороннього розмови по сусідньому каналу. Причина цього в тому, що при проходженні електричного струму по дроту навколо нього створюється слабке круговий магнітне поле, яке може впливати на сусідній провід.

Натисніть кнопку «Відтворення» на малюнку і подивіться, як перешкоди можуть впливати на передачу даних.

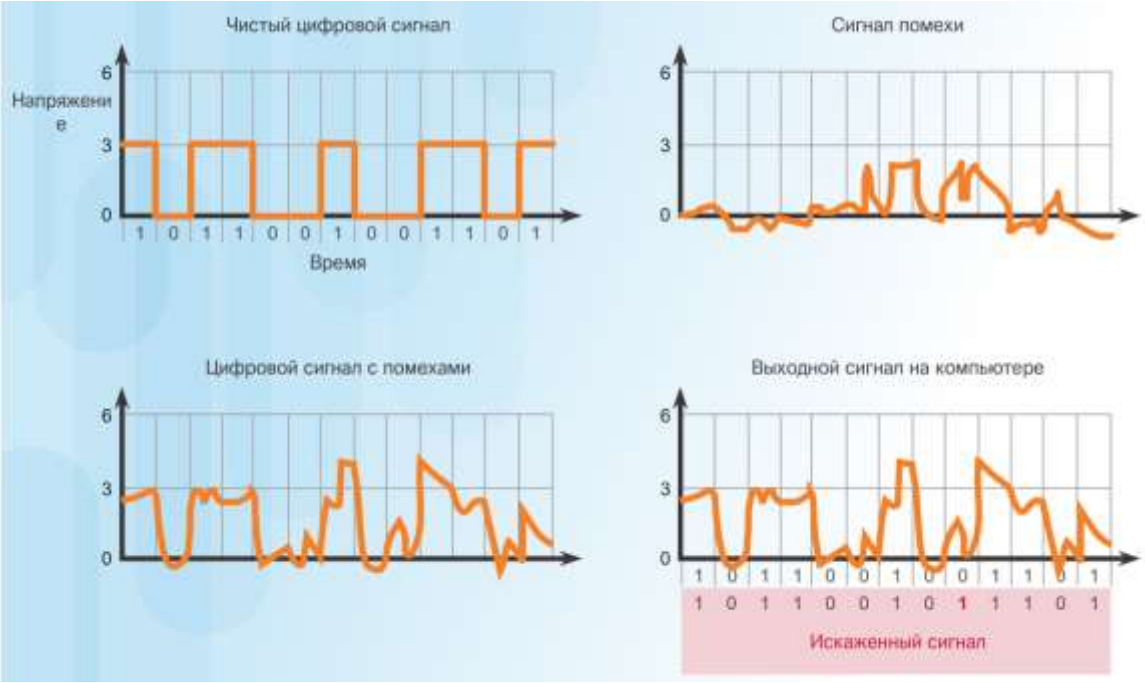


Рис. 1.1.31 Як виникають перешкоди у сигналі

Для захисту від шкідливого впливу ЕМП і РЧП деякі типи мідних кабелів обгорнуті металевої екранує оболонкою. Такі кабелі вимагають належного заземлення.

У деяких типах мідних кабелів дроти кожної пари скручені між собою, що забезпечує ефективне придушення перехідних перешкод.

Захищеність мідного кабелю від електронних перешкод можна також підвищити за рахунок наступних заходів.

Вибір типу і категорії кабелю, найбільш придатних для даного мережевого оточення

Проектування кабельної інфраструктури будівлі з обходом відомих і можливих джерел електромагнітних полів

Дотримання правил прокладки і підключення кабелів при монтажі

Типи мідних кабелів

Для побудови мереж використовується три основних типи мідних кабелів.

- Неекранована кручена пара (UTP)
- Екранована кручена пара (STP)
- коаксіальні кабелі

Ці кабелі використовуються для з'єднання вузлів локальної мережі і підключення пристроїв мережевої інфраструктури, таких як комутатори, маршрутизатори і бездротові точки доступу. У стандартах фізичного рівня описані вимоги до кабелів для кожного з типів з'єднання і відповідних їм пристроїв.

Різні стандарти фізичного рівня вимагають використання різних роз'ємів. Ці стандарти визначають фізичні розміри і допустимі електричні характеристики кожного типу роз'ємів. У засобах мережевого підключення для забезпечення простого підключення і відключення використовуються модульні гнізда і штекери. При цьому фізичні роз'єми одного типу можуть використовуватися для декількох типів підключень. Наприклад, роз'єм RJ-45

широко використовується в локальних мережах (LAN) з одним типом засобів підключення, а в деяких глобальних мережах (WAN) - з іншим типом.

Кабель на основі неекранованої кручений пари

Кабелі на основі неекранованої кручений пари (UTP) є найпоширенішим засобом підключення. Кабелі UTP з роз'ємами RJ-45 використовуються для з'єднання вузлів з проміжними мережевими пристроями, такими як комутатори і маршрутизатори.

Кабель UTP для локальних мереж складається з чотирьох скручених пар провідників з кольоровим маркуванням, які укладені в загальну гнучку пластикову оболонку, що захищає кабель від незначних пошкоджень. Скручування провідників знижує вплив перешкод від інших провідників.

На малюнку показано, як кольорове маркування дозволяє ідентифікувати пари і провідники, а також полегшує оконцовке кабелів.

Кабель на основі екранованої кручений пари

Кабелі на основі екранованої кручений пари (STP) краще захищені від перешкод, ніж кабелі UTP. Але при цьому вони значно дорожче, і їх складніше монтувати. Як і для кабелів типу UTP, для кабелів STP використовується роз'єм RJ-45.

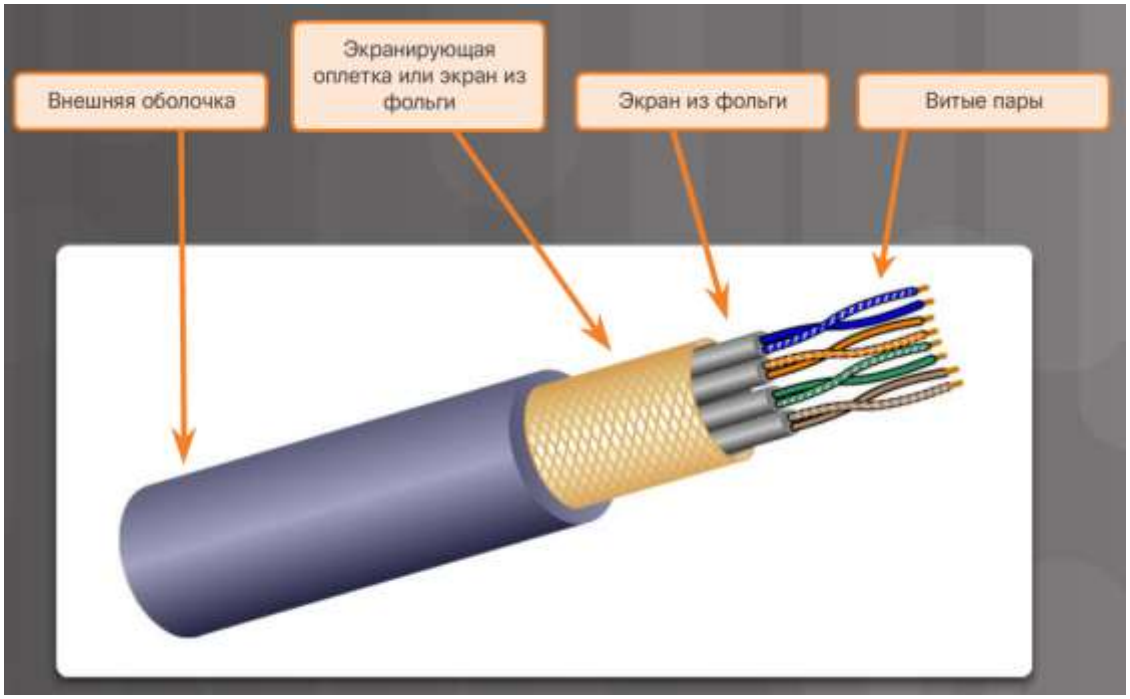


Рис. 1.1.32 Будова витої пари

У кабелях STP застосовується як екранування для захисту від ЕМП і РЧП, так і скручування провідників для захисту від перехідних перешкод. Для отримання найбільш повного ефекту від екранування кабелі STP оснащуються спеціальними екранованими роз'ємами для ліній передачі даних STP. Якщо такий кабель не заземлити належним чином, то екран може діяти як антена і приймати небажані сигнали.

На малюнку показаний кабель STP, що складається з чотирьох пар провідників, обгорнутих в окремі екрани з фольги, які зверху ще разом обгорнуті загальної екранує опліткою або фольгою.

Коаксіальний кабель

Коаксіальний кабель називається так тому, що він містить два співвісних провідника. Як показано на малюнку, коаксіальний кабель складається з наступних елементів.

Мідний провідник, який використовується для передачі електричних сигналів.

Шар гнучкої пластикової ізоляції навколо мідного провідника.

Мідна оплетка або металеву фольгу, навколишнє шар ізолюючого матеріалу і виступає в якості другого проводу в ланцюзі, а також екрану для внутрішнього провідника. Цей другий шар, званий екраном, також знижує рівень зовнішніх електромагнітних завад.

Зовні кабель покритий кабельної оболонкою для захисту від незначних фізичних ушкоджень.

З коаксіальним кабелем використовуються різні типи роз'ємів.

Хоча в сучасних мережах Ethernet коаксіальні кабелі фактично поступилися місцем кабелям UTP, кабелі коаксіальної структури використовуються в наступних областях.

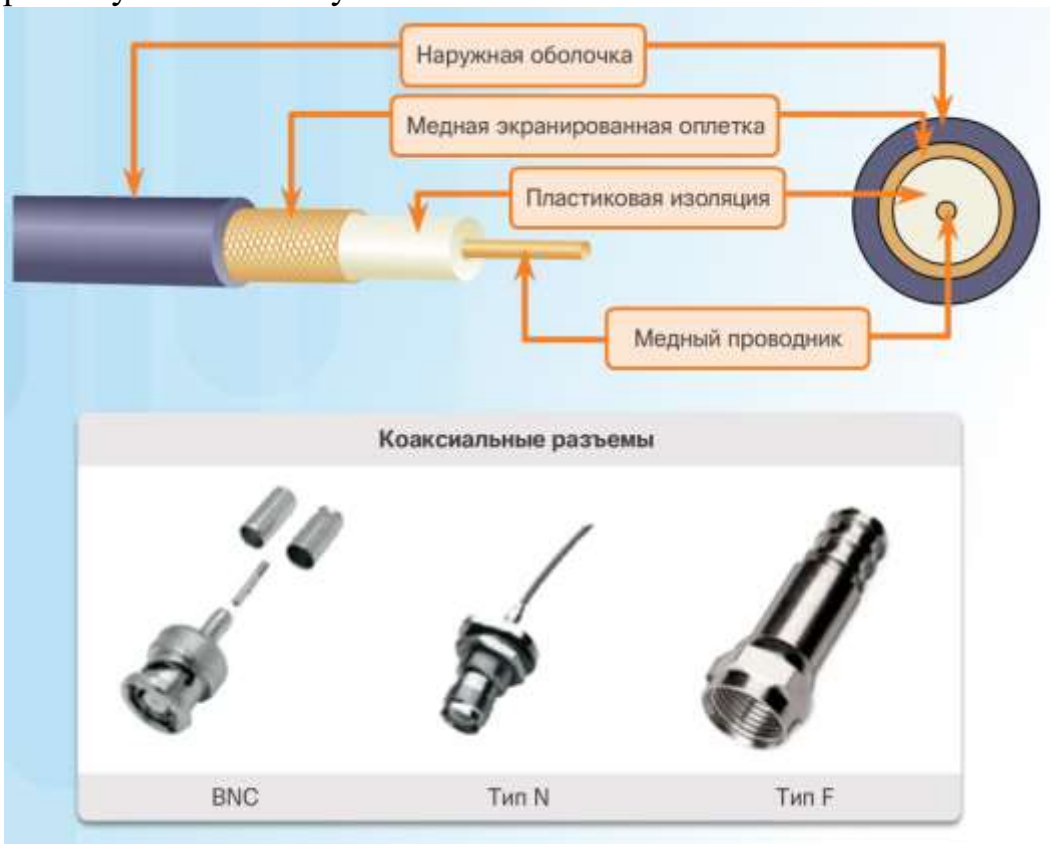


Рис. 1.1.33 Будова коаксіального кабеля

Устаткування бездротових мереж. Коаксіальні кабелі використовуються для підключення антен до пристроїв бездротового зв'язку. Коаксіальний кабель забезпечує передачу енергії радіочастотних сигналів між антенами і радіоустаткуванням.

Мережі кабельного телебачення з доступом в Інтернет. Оператори кабельних мереж пропонують своїм клієнтам доступ в Інтернет, частково замінюючи коаксіальні кабелі і відповідні підсилювальні елементи на оптоволоконні кабелі. Однак з'єднання в приміщеннях клієнтів як і раніше виконуються коаксіальними кабелями.

Безпека мідних кабелів

При роботі з мідними кабелями всіх трьох типів необхідно враховувати їх потенційну пожежонебезпека і Електронебезпека.

Їх пожежонебезпека обумовлена можливою горючестью ізоляції та оболонок або токсичністю виділяється при їх нагріванні або горінні диму. Служби або організації технічного нагляду за будівництвом можуть встановлювати відповідні стандарти безпеки для прокладки кабелів і підключення обладнання.

Електронебезпека мідних кабелів зумовлена їх здатністю проводити електричні струми в непередбачених випадках. При цьому персонал і обладнання піддаються різним небезпекам. Наприклад, струм від несправного мережевого пристрою може надходити на корпуса інших мережевих пристроїв. Крім того, при з'єднанні пристроїв, джерела живлення яких мають різні електричні потенціали, на мережевих кабелях можуть створюватися небажані рівні напруги. Такі ситуації можливі при використанні мідних кабелів для з'єднання мереж в різних будівлях або на різних поверхах будівлі, що мають незалежні джерела електропостачання. Нарешті, мідні кабелі можуть проводити напруги, викликані потраплянням блискавок в мережеві пристрої.

Ці небажані напруги і струми можуть пошкоджувати мережеві пристрої і підключені до них комп'ютери, а також травмувати персонал. Тому, щоб уникнути нещасних випадків і пошкодження обладнання при монтажі мідних кабелів, необхідно строго дотримуватися будівельні норми і правила.

На малюнку показані основні принципи монтажу кабельних з'єднань, що знижують небезпеку займання або ураження електричним струмом.

Властивості кабелів UTP

Кабель на основі неекранованої кручений пари (UTP), який використовується в якості засобу мережевого підключення, складається з чотирьох скручених пар мідних провідників з кольоровим маркуванням, укладених в загальну гнучку пластикову оболонку. Завдяки невеликому діаметру кабелю його зручно монтувати.

У кабелях UTP не передбачено екранування для захисту від ЕМП і РЧП. Замість цього для обмеження негативного впливу перехідних перешкод застосовуються такі рішення, свого часу знайдені проектувальниками кабелів.

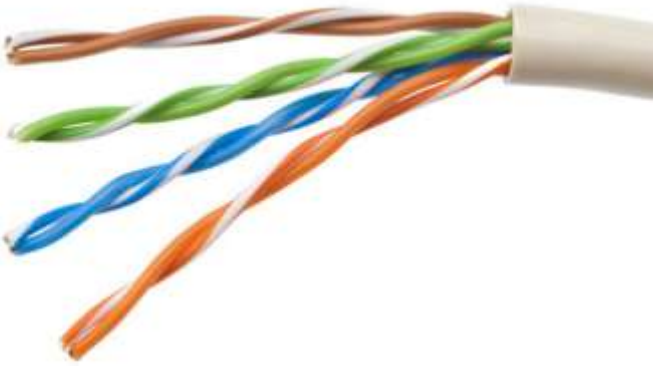


Рис. 1.1.34 Вита пара стандарту UTP 3

Тепер проектувальники об'єднують дроти одного електричного кола в пару. При розміщенні двох проводів одного електричного кола в безпосередній близькості один до одного магнітні поля навколо них протилежні одна одній.

Тому два магнітних поля взаємно компенсуються, а також забезпечується компенсація впливу зовнішніх ЕМП і РЧП.

Різний крок витків в парах. Для підвищення ефекту придушення перешкод проектувальники використовують різний крок витків в сусідніх парах одного кабелю. Кабелі UTP повинні точно відповідати специфікаціям, який регламентує допустиму кількість витків на 1 метр кабелю. Зверніть увагу, що на малюнку помаранчевий і біло-помаранчевий дроту скручені рідше, ніж синій і біло-синій. Пари різних кольорів скручені з різним кроком скрутки.

У кабелях UTP захист від спотворень сигналу і ефективне самоекранірованіе пар проводів здійснюються виключно за рахунок ефекту придушення перешкод, що досягається скручуванням дротів в парі.

Стандарти прокладки кабелів UTP

Кабелі UTP відповідають вимогам стандартів, спільно вироблених організаціями TIA і EIA. Зокрема, в стандарті TIA / EIA-568A описуються технічні вимоги до прокладання кабелю в локальних мережах. Це найбільш часто вживаний в цій сфері стандарт. У ньому, зокрема, визначено такі елементи.

- типи кабелів
- довжина кабелів
- роз'єми
- оконцовке кабелів
- Методи тестування кабелів

Електричні характеристики мідних кабелів визначаються Інститутом інженерів з електротехніки та електроніки (IEEE). IEEE класифікує кабелі UTP згідно їх характеристикам. Кабелі поділяються на категорії відповідно до можливої швидкістю передачі даних по ним. Наприклад, кабель категорії 5 (Cat5) зазвичай використовується в мережах Fast Ethernet 100BASE-TX. До іншим категоріям кабелів відносяться: розширена категорія 5 (Cat 5e), категорія 6 (Cat6) і категорія 6a.

Кабелі більш високих категорій призначені для передачі даних на більш високій швидкості. В результаті розробки і впровадження нових технологій Ethernet для гігабітних швидкостей передачі даних в даний час мінімально допустимим типом кабелів є Cat5e, а для прокладки нових мереж рекомендується Cat6.

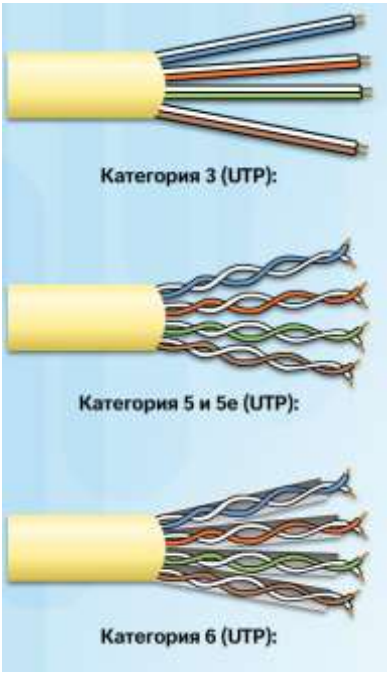


Рис. 1.1.35 Типи витої пари

Рис 1.

Щоб переглянути детальну інформацію про різних категоріях кабелів натисніть на кожну з них на малюнку.

Деякі виробники випускають кабелі з характеристиками вище, ніж у кабелів категорії 6a TIA / EIA, і позиціонують їх як кабелі категорії 7.

Роз'єми для кабелів UTP

Кабелі UTP і STP зазвичай оснащуються роз'ємами RJ-45. Цей роз'єм використовується в фізичних мережах цілого ряду різних стандартів, в тому числі Ethernet. У стандарті TIA / EIA 568 описано відповідність кольорового маркування проводів і схем підключення контактів для кабелів Ethernet.

Як показано на малюнку 1, роз'єм RJ-45 є штекерним роз'ємом, що встановлюються на кінці кабелю обтискним способом. Гніздова частина цього роз'єму може встановлюватися в мережевому пристрої, на стіні, офісної перегородці або комутаційної панелі.

Рис. 1.1.36 Штекерна і гніздова частина роз'єму

При оконцовке мідних кабелів виникає ймовірність втрат сигналу і появи шумів в каналі зв'язку. При неправильної оконцовке кожен кабель стає потенційною причиною зниження продуктивності на фізичному рівні. Висока якість оконцовкі мідних кабелів гарантує оптимальну продуктивність при використанні як сучасних, так і майбутніх мережевих технологій.

На малюнку 2 показані приклади неправильної і правильної оконцовкі кабелю UTP.

Типи кабелів UTP

У різних ситуаціях можуть застосовуватися різні схеми підключення проводів кабелів UTP до роз'ємів. Іншими словами, окремі дроти кабелю можуть підключатися до різних груп контактів роз'єму RJ-45 в різному порядку.

Нижче описані основні типи кабелів, які можна отримати, застосовуючи різний порядок підключення проводів.

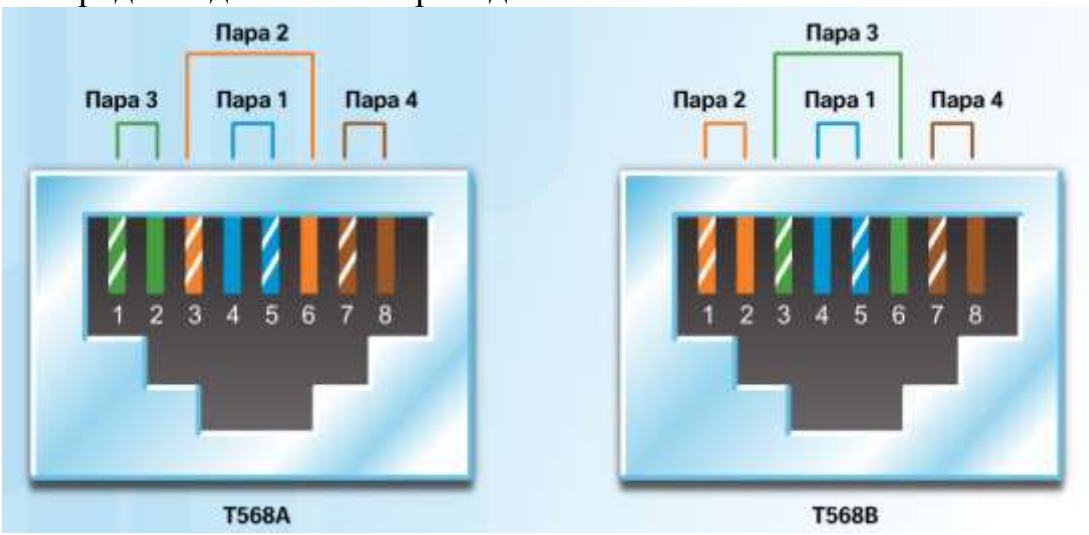


Рис. 1.1.37 Схема обжиму витої пари.

Прямий кабель Ethernet: найбільш поширений тип мережевого кабелю; як правило, використовується для підключення вузла до комутатора і комутатора до маршрутизатора.

Перехресний кабель Ethernet: використовується для з'єднання однотипних пристроїв, наприклад для підключення комутатора до комутатора, комп'ютера до комп'ютера або маршрутизатора до маршрутизатора.

Консольний кабель (Rollover): фірмовий кабель Cisco; використовується для підключення робочої станції до консольного порту маршрутизатора або комутатора.

На малюнку приведена інформація про типи кабелів UTP, відповідних стандартах і типових варіантах застосування. Також на малюнку показано розташування різних пар провідників для стандартів TIA 568A і TIA 568B.

Неправильне використання перехресного або прямого кабелю між пристроями не зашкодить їм, але зв'язок і взаємодія між ними будуть неможливі. Подібна помилка часто відбувається в ході практичних занять. Тому при відсутності зв'язку між пристроями в першу чергу потрібно перевірити правильність підключення.

Тестування кабелів UTP

Після завершення монтажу необхідно використовувати кабельний тестер UTP (наприклад, показаний на малюнку) для перевірки наступних параметрів.

- схема проводки
- Довжина кабеля
- Втрати сигналу через загасання
- Рівень перехідних перешкод

Рекомендується перевірити, що всі вимоги до монтажу кабелів UTP ретельно виконані.

Властивості оптоволоконних кабелів

Оптоволоконні кабелі дозволяють передавати дані на великі відстані і з більш високою пропускною здатністю, ніж інші засоби мережевого підключення. На відміну від мідних проводів оптоволоконний кабель дозволяє передавати сигнали з більш низьким загасанням. Такий кабель також абсолютно несприйнятливий до впливу електромагнітних і радіочастотних перешкод. Оптичні кабелі зазвичай використовуються для з'єднання мережевих пристроїв один з одним.

Оптичне волокно - це гнучка, дуже тонка і прозора нитка з хімічно чистого скла товщиною трохи більше за людську волосину. Для передачі по оптоволоконному кабелю біти кодуються за допомогою світлових імпульсів. Оптоволоконний кабель діє як світловод, або «оптичний хвилевід», що забезпечує передачу світлового сигналу між двома кінцями кабелю з мінімальними втратами.

В якості аналогії уявіть собі порожній сердечник від рулону паперових рушників, внутрішні стінки якого вкриті дзеркально відображає матеріалом. Його довжина становить тисячу метрів. За допомогою невеликої лазерної указки через нього зі швидкістю світла передаються сигнали азбуки Морзе. По суті, саме так функціонує оптоволоконний кабель, тільки він має набагато менший діаметр і створений із застосуванням найсучасніших оптичних технологій.

В даний час оптоволоконні кабелі використовуються в наступних чотирьох областях.

Корпоративні мережі. Оптоволоконні кабелі використовуються в якості магістральних кабелів та для з'єднань між пристроями мережної інфраструктури.

Технологія «оптоволокно до квартири» (FTTH). Оптоволоконні кабелі використовуються для постійного широкосмугового доступу індивідуальних користувачів і невеликих підприємств до мережі.

Мережі телекомунікації. Оптоволоконні кабелі використовуються провайдерами послуг для міжнародного та міжміського зв'язку.

Підводні кабельні мережі. Оптоволоконні кабелі використовуються для будівництва надійних високошвидкісних ліній зв'язку, здатних працювати в важких умовах великих глибин і забезпечувати зв'язок на великих відстанях, аж до трансокеанських. Клацніть посилання для перегляду телегеографіческой карти, на якій показані маршрути підводних кабелів.

Конструкція оптоволоконного кабелю

Оптоволокно складається з двох видів скляних компонентів (сердечника і внутрішньої оболонки) і захисної зовнішньої оболонки. Натисніть на кожен компонент для отримання додаткової інформації.

Рис. 1.1.38 Будо оптоволоконного кабеля

Хоча оптоволокно дуже тонке і може легко гнутися, але завдяки властивостям сердечника і оболонки воно дуже міцне. Завдяки своїй міцності оптичне волокно може використовуватися в найважчих умовах експлуатації.

Типи оптоволоконних кабелів

Світлові імпульси, за допомогою яких біти даних кодуються для передачі, можуть генеруватися наступними джерелами.

- лазери
- Світловипромінюючі діоди (LED).

На стороні прийому напівпровідникові пристрої, які називаються фотодіодами, приймають світлові імпульси і перетворять їх в напруги. Передане по оптоволоконному кабелю лазерне випромінювання небезпечно для очей. Тому при роботі з активним оптоволоконним кабелем слід дотримуватися запобіжних заходів.

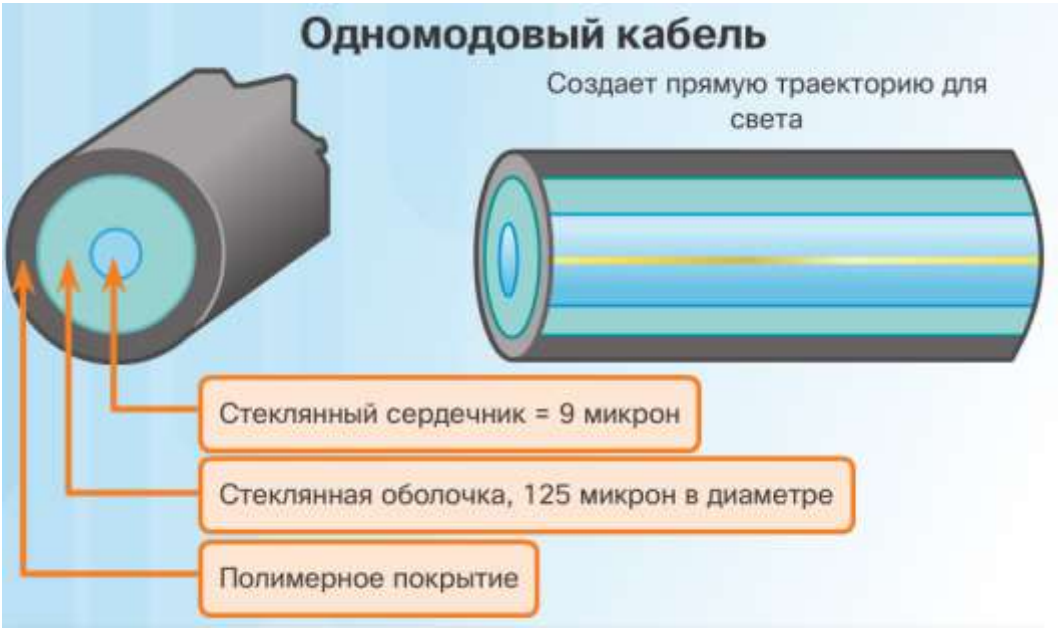


Рис. 1.1.39 Будово одномодового оптоволоконного кабеля

Оптоволоконні кабелі поділяються на два основних типи.

Одномодовий оптоволоконний кабель (ООК). Має сердечник дуже малого діаметру. Для передачі променя світла потрібна дорога лазерна технологія (див. Малюнок 1). Широко використовується для організації ліній зв'язку довжиною кілька сотень кілометрів, наприклад для далекої телефонії і кабельного телебачення.

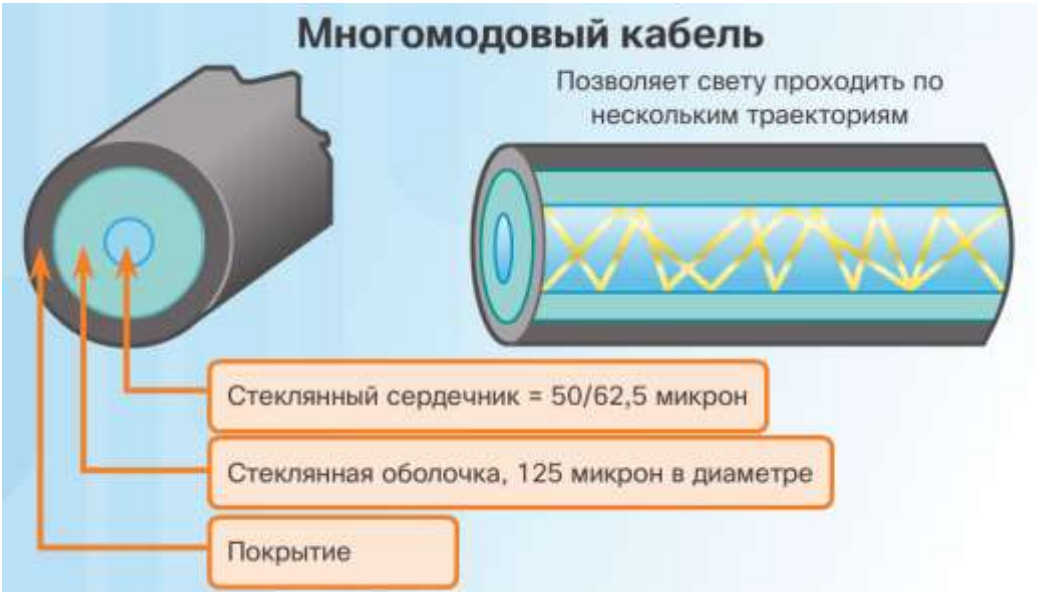


Рис. 1.1.40 Будова багатомодового оптоволоконного кабеля

Багатомодовий оптоволоконний кабель (МОК). Має сердечник більшого діаметра. Для передачі світлових імпульсів використовуються світлодіодні випромінювачі. Як показано на малюнку 2, світло, що випромінюється світлодіодом, входить в багатомодове волокно під різними кутами. Такі кабелі популярні в локальних мережах, оскільки дозволяють використовувати для роботи недорогі світлодіоди. Багатомодовий кабель забезпечує пропускну здатність до 10 Гбіт / с на відстані до 550 метрів.

Одне з основних відмінностей між МОК і ООК - рівень дисперсії. Під дисперсією в даному контексті мається на увазі розширення світлового

імпульсу у міру його руху через оптичне волокно. Чим вище дисперсія, тим більше втрати сигналу.

оптоволоконні роз'єми

Оптоволоконний роз'єм монтується на кінці оптичного волокна. Існують різні типи оптоволоконних роз'ємів. Основні відмінності між цими типами полягають в розмірах і методах механічних з'єднань. Тип застосовуваних в мережі роз'ємів визначається видом устаткування, що підключається.

Для отримання додаткової інформації про кожного з трьох типів найбільш популярних оптоволоконних роз'ємів (ST, SC і LC) натисніть на кожен з них на малюнку 1.

Оскільки світло по оптоволокну передається тільки в одному напрямку, для роботи в повнодуплексному режимі потрібні два оптоволокна. Тому в оптичних з'єднувальних кабелях є два волокна, на кінцях кожного з яких змонтовані стандартні Одноволоконні роз'єми. Деякі оптоволоконні роз'єми допускають підключення до них як передають, так і приймаючих волокон. Такі роз'єми називаються дуплексними.

Рис. 1.1.41 Типи з'єднання оптоволоконних кабелів

Для підключення пристроїв мережевої інфраструктури потрібні сполучні оптоволоконні кабелі. Деякі з поширених типів сполучних кабелів показані на малюнку 2. Щоб розрізняти одномодові і багатомодові сполучні кабелі, використовується кольорове маркування. Жовта маркування використовується для одномодових оптоволоконних кабелів, а помаранчева (або блакитна) - для багатомодових.

Роз'єми невикористовуваних оптоволоконних кабелів повинні бути захищені невеликий пластиковою кришкою.

Тестування оптоволоконних кабелів

Оконцовке і зрощування оптоволоконних кабелів вимагають спеціальної підготовки і обладнання. Неправильна оконцовке оптоволоконного кабелю призводить до зниження дальності поширення сигналу або повного порушення передачі.

До найбільш поширених проблем при оконцовке і зрощуванні оптоволоконних кабелів відносяться наступні.

Зміщення: з'єднуються оптичні волокна не вирівняні відносно один одного.

Зазор між торцями волокон: волокна не повністю стикаються в місці зрощення або підключення.

Якість обробки торців волокна: торці волокон недостатньо відполіровані або погано очищені від бруду.

Для швидкої і простої перевірки кабелю на об'єкті експлуатації досить посвітити яскравим електричним ліхтарем в один кінець волокна, одночасно спостерігаючи за другим кінцем. Якщо світло видно, то волокно придатне для роботи. Хоча така перевірка і не дозволяє проконтролювати характеристики волокна, вона являє собою швидкий і недорогий спосіб виявлення пошкоджених волокон.

Показаний на малюнку оптичний тимчасової рефлектометр (OTDR) можна використовувати для перевірки кожного сегмента оптоволоконного кабелю. Це пристрій вводить тестовий імпульс світла в кабель і вимірює зворотне розсіювання і відображення світла як функцію часу. Оптичний рефлектометр розраховує приблизне відстань до місць виявлення несправностей оптоволокна по всій довжині кабелю.

Оптоволоконні кабелі і мідні кабелі: порівняння

Оптоволоконні кабелі мають безліч переваг перед мідними. На малюнку приведені деякі з основних відмінностей між ними.

Оскільки волокна, використовувані в оптоволоконних кабелях, не є провідниками, цей тип засобів підключення не схильний до електромагнітних перешкод і не проводить небажані електричні струми в разі проблем із заземленням. Так як оптичні волокна мають малу товщину і відрізняються порівняно малими втратами сигналу, вони дозволяють передавати інформацію на набагато більші відстані в порівнянні з мідними кабелями. Деякі специфікації фізичного рівня для оптоволоконних засобів підключення допускають використання оптичних кабелів довжиною до кількох кілометрів.

В даний час в більшості корпоративних мереж оптоволоконні кабелі в основному використовуються в якості магістральних для організації високошвидкісних з'єднань «точка-точка» між пристроями розподілу даних, а також для зв'язку між будівлями в комплексах будинків. Оскільки оптоволокно не проводить електрику і відрізняється малими втратами сигналу, воно оптимально підходить для цих цілей.

Властивості засобів бездротового підключення

Засоби бездротового підключення забезпечують передачу двійкових розрядів даних у вигляді електромагнітних сигналів радіочастотного або мікрохвильового діапазону.

Засоби бездротового підключення забезпечують найбільший рівень мобільності в порівнянні з будь-якими іншими засобами, тому число пристроїв, що підтримують бездротове підключення, зростає з кожним днем. У міру

збільшення пропускної здатності бездротове підключення завойовує все більшу популярність у корпоративних мережах.

На малюнку показані різні символи, пов'язані з бездротовим з'єднанням.

Бездротова середовище має такі особливості, які необхідно враховувати.

Зона покриття. Бездротові технології передачі даних добре працюють на відкритих просторах. Однак деякі будівельні матеріали, що використовуються при зведенні будівель і споруд, а також умови місцевості можуть обмежувати зону покриття.

Перешкоди. Якість бездротових з'єднань вразливе до перешкод і може погіршуватися при роботі таких звичайних пристроїв, як бездротові телефони, деякі типи флуоресцентних ламп, мікрохвильові печі, а також під впливом інших бездротових комунікацій.

Безпека. Для доступу до середовища бездротового підключення не потрібно підключатися до фізичних кабелям. Тому доступ до цього середовища можуть отримувати несанкціоновані користувачі та пристрої. Отже, головним аспектом адміністрування бездротової мережі є безпека.

Спільний доступ до засобу підключення. Мережі WLAN працюють в напівдуплексному режимі, що означає, що в кожен момент часу передачу або прийом може здійснювати тільки один пристрій. Засоби бездротового підключення спільно використовують всі бездротові користувачі. Чим більше користувачів одночасно підключаються до WLAN, тим менша пропускна здатність доводиться на кожного з них. Напівдуплексний режим буде розглянуто пізніше в цій главі.

Хоча популярність бездротового підключення настільних комп'ютерів до мережі зростає, найбільш популярним засобом мережевого підключення на фізичному рівні залишаються мідні й оптоволоконні кабелі.

Типи засобів бездротового підключення

Стандарти IEEE і телекомунікаційні галузеві стандарти бездротової передачі даних охоплюють як канальний, так і фізичний рівні. Для отримання додаткової інформації клацніть кожен стандарт, наведений на малюнку.

Примітка. Для створення мереж передачі даних можуть використовуватися і інші бездротові технології, наприклад стільниковий або супутниковий зв'язок. Однак в цьому розділі ці бездротові технології не розглядаються.

У кожному зі згаданих стандартів специфікації фізичного рівня застосовуються до наступних галузей.

- Кодування даних за допомогою радіосигналів
- Частота і потужність передачі
- Вимоги до прийому і декодування сигналів
- Проектування і будівництво антен

Wi-Fi є товарним знаком Wi-Fi Alliance. Wi-Fi використовується з сертифікованими продуктами, які відносяться до пристроїв бездротової локальної мережі (WLAN) і підтримують стандарти IEEE 802.11. Додаткову інформацію про стандарти бездротової мережі 802.11 см.

Бездротова локальна мережа

Найчастіше бездротова передача даних використовується для бездротового зв'язку пристроїв через локальну мережу (LAN). Як правило, для створення бездротової LAN потрібні такі мережеві пристрої.

Бездротова точка доступу (AP): концентрує бездротові сигнали від користувачів. Підключається до мережевої інфраструктури на основі мідних кабелів, наприклад Ethernet. Бездротові маршрутизатори для дому та невеликих підприємств (див. Малюнок) в одному пристрої поєднують функції маршрутизатора, комутатора і точки доступу.

Бездротові мережеві плати: забезпечують можливість бездротового підключення для кожного вузла в мережі.

У міру розвитку технології був створений цілий ряд стандартів бездротової локальної мережі (WLAN) на основі Ethernet. Тому, купуючи бездротові пристрої, слід звертати особливу увагу на їх сумісність.

Переваги бездротових технологій передачі даних очевидні, особливо в плані економії витрат на прокладку дорогих кабелів в приміщеннях і зручностей за рахунок мобільності мережевих пристроїв. Мережеві адміністратори повинні розробляти і застосовувати суворі правила і протоколи безпеки для захисту бездротових локальних мереж від несанкціонованого доступу і потенційного збитку.

канальний рівень

Як показано на малюнку 1, канальний рівень моделі OSI (рівень 2) виконує наступні функції.

- Забезпечення доступу вищих рівнів до засобу підключення
- Прийом пакетів рівня 3 і упаковка їх в кадри
- Підготовка мережевих даних для передачі по фізичній мережі
- Управління передачею і прийомом даних в засобі підключення

Обмін кадрами між вузлами по фізичним засобам мережевого підключення, наприклад по кабелях UTP або оптоволоконним кабелях

- Прийом пакетів і їх перенаправлення протоколам вищого рівня
- виявлення помилок

На другому рівні мережеве пристрій, підключений до загального засобу підключення, називається вузлом. Вузли формують і пересилають кадри. Як показано на малюнку 2, канальний рівень відповідає за обмін кадрами Ethernet між вузлами джерела і призначення по фізичним засобам підключення.

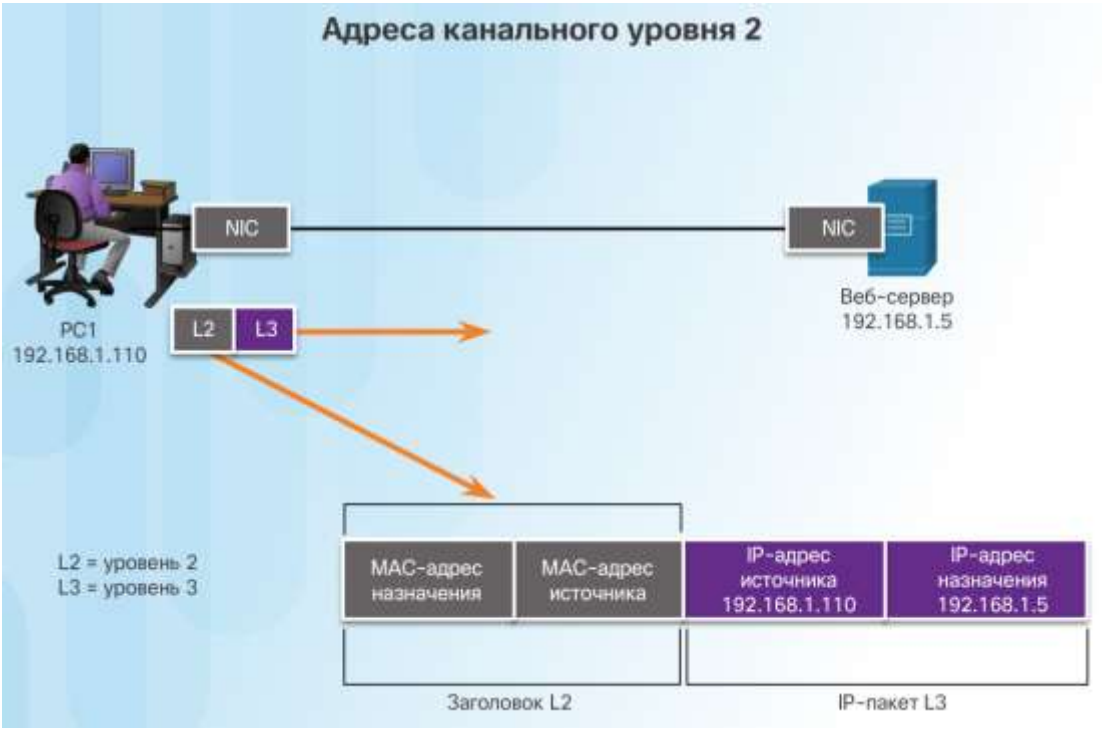


Рис. 1.1.42 Схема адресації канального рівня

Канальний рівень ефективно розділяє переходи між засобами підключення, що виникають в ході пересилання пакетів, від комунікаційних процесів на більш високих рівнях мережевої моделі OSI. Канальний рівень відправляє пакети протоколу вищого рівня і приймає їх від нього (в даному випадку це протокол IPv4 або IPv6). Протоколу вищого рівня не потрібно знати, який засіб підключення буде використовуватися при передачі даних.

Підрівні канального рівня

Канальний рівень поділяється на наступних два підрівні.

Управління логічним з'єднанням (Logical Link Control, LLC). Цей верхній підрівень взаємодіє з мережевим рівнем. Він поміщає в кадр інформацію, яка вказує, який протокол мережевого рівня використовується для даного кадру. Дана інформація дозволяє різним протоколам 3-го рівня, таким як IPv4 і IPv6, використовувати один і той же мережевий інтерфейс і одне і те ж засіб підключення.

Управління доступом до середовища (Media Access Control, MAC). Це нижній підрівень, який визначає процеси доступу до середовища, що виконуються обладнанням. Він забезпечує адресацію канального рівня і доступ до різних мережевих технологій.

Рис. 1.1.43 Заголовок Ethernet-кадра

На малюнку показано поділ канального рівня на підрівні LLC і MAC. Підрівень LLC взаємодіє з мережевим рівнем, а підрівень MAC забезпечує роботу різних технологій мережевого доступу. Зокрема, підрівень MAC взаємодіє з технологією локальної мережі Ethernet для передачі і прийому кадрів по мідному або оптоволоконному кабелю. Також підрівень MAC взаємодіє з такими бездротовими технологіями, як Wi-Fi і Bluetooth для бездротової передачі і прийому кадрів.

Управління доступом до середовища

Протоколи рівня 2 визначають інкапсуляцію пакету в кадр, а також методи введення інкапсульованих пакетів в різні засоби підключення і зворотного вилучення цих пакетів. Технологія, використовувана для введення кадру в засіб підключення і його зворотного вилучення, називається методом управління доступом до середовища.

Під час проходження пакетів від вузла джерела до вузла адресата вони зазвичай передаються по різним фізичним мереж. Ці фізичні мережі можуть складатися з фізичних засобів підключення різного типу, наприклад мідних і оптоволоконних кабелів, засобів бездротового підключення на основі електромагнітних сигналів, а також радіочастотних, мікрохвильових і супутникових каналів.

Якби канального рівня не існувало, мережевий рівень, наприклад IP, повинні були б забезпечувати з'єднання для всіх типів засобів підключення, які могли зустрітися на шляху проходження пакету. Більш того, протоколу IP довелося б щоразу адаптуватися до нової мережевої технології або середовищі. Такий процес ускладнив би оновлення і розвиток протоколів і засобів мережевого підключення. В цьому і полягає основна причина використання багаторівневого підходу до побудови мереж.

Надання доступу до середовища

В рамках одного сеансу зв'язку можуть знадобитися різні методи управління доступом до середовища. Всі мережеві середовища, за якими проходять пакети в ході передачі від локального вузла до віддаленого, можуть мати різні характеристики. Наприклад, локальна мережа Ethernet складається з безлічі вузлів, що конкурують за доступ до засобу підключення. Послідовні канали призначені виключно для прямого з'єднання двох пристроїв.

Інтерфейси маршрутизатора інкапсулюють пакет в відповідний кадр. Для доступу до кожного каналу використовується відповідний метод управління доступом до середовища. При будь-якому обміні пакетами мережного рівня можливі багаторазові переходи між канальним рівнем і середовищем.

На кожному транзитній ділянці шляху маршрутизатор виконує такі операції.

- Приймає кадр з середовища
- Деінкапсулірует кадр
- Повторно инкапсулирует пакет в новий кадр
- Передає новий кадр, який відповідає середовищі даного сегмента фізичної мережі

Стандарти канального рівня

На відміну від протоколів верхніх рівнів стека TCP / IP протоколи канального рівня, як правило, не визначаються документами RFC (Request for Comments, RFC). Незважаючи на те, що Інженерна група з розвитку Інтернету (IETF) підтримує функціональні протоколи і служби для стека протоколів TCP / IP на верхніх рівнях, IETF не визначає функції і принципи роботи рівня доступу до мережі для цієї моделі.

Ухвалою відкритих стандартів і протоколів, які можна застосувати до канального рівня доступу, займаються такі організації.

- Інститут інженерів з електротехніки та електроніки (IEEE)
- Міжнародний союз електрозв'язку (ITU)
- Міжнародна організація по стандартизації (ISO)
- Американський національний інститут стандартизації (ANSI)

Управління доступом до середовища

Приміщенням кадрів даних в середу управляє підрівень управління доступом до середовища.

Управління доступом до середовища працює аналогічно правилам дорожнього руху, що регулює виїзд автомобілів на дорогу. Відсутність будь-яких заходів управління доступом до середовища можна порівняти з ситуацією, коли водії виїжджають на дорогу, ігноруючи рух інших транспортних засобів. Однак не всі дороги та в'їзди однакові. Транспортні засоби можуть виїжджати на дорогу, або вливаючись в потік, або чекаючи своєї черги у знака «Стоп», або підкоряючись сигналам світлофора. На в'їзних дорогах різного типу водії підпорядковуються різним правилам.

Точно так само існують різні методи контролю приміщення кадрів в засіб підключення. Правила доступу до різних засобів підключення визначаються протоколами канального рівня. Ці методи управління доступом до засобу підключення визначають, чи використовують вузли даний засіб спільно і яким чином це відбувається.

Вибір методу управління доступом до засобу підключення залежить від наступних факторів.

Топологія: як з'єднання між вузлами виглядає на канальному рівні.

Спільне використання засобу підключення: як здійснюється загальний доступ вузлів до засобу підключення Спільне використання засобу підключення може здійснюватися за принципом «точка-точка», як в глобальній мережі, або за принципом розділяється доступу до середовища, як в локальних мережах.

Фізична і логічна топологія

Топологія мережі описує розташування або взаємозв'язок мережевих пристроїв, а також з'єднання між ними. Топології LAN і WAN можна розглядати з двох точок зору.

Фізична топологія. Цей термін відноситься до фізичних з'єднань і визначає, яким чином з'єднуються один з одним кінцеві пристрої та пристрої мережевої інфраструктури, такі як маршрутизатори, комутатори і бездротові точки доступу. Фізична топологія найчастіше організована за схемою «точка-точка» або «зірка». (Див. Рисунок 1.)

Логічна топологія: термін, використовуваний для опису шляхів передачі кадрів між вузлами. Структура логічної топології складається з віртуальних з'єднань між вузлами мережі. Ці логічні шляхи сигналів визначені протоколами канального рівня. Логічна топологія каналів «точка-точка» порівняно проста, хоча спільно використовуваного середовища підключення дозволяє застосовувати різні методи управління доступом. Див. Малюнок 2.

При управлінні доступом даних до середовища канальний рівень «бачить» логічну топологію мережі. Саме логічна топологія впливає на вибір типу кадрування в мережі і управління доступом до середовища.

Поширені фізичні топології глобальних мереж

З'єднання в глобальних мережах зазвичай організовуються за допомогою наступних фізичних топологій.

«Точка-точка» (Point-to-Point): це найпростіша топологія, що представляє собою постійне з'єднання між двома кінцевими точками. Саме з цієї причини дана топологія глобальної мережі є найбільш поширеною.

«Зіркоподібна» (Hub and spoke): версія зіркоподібній топології для глобальної мережі, в якій центральний вузол з'єднаний з периферійними за допомогою з'єднань «точка-точка».

Ніздрювата (Mesh): ця топологія забезпечує високу доступність, але вимагає, щоб кожна крайова система була пов'язана з усіма іншими системами. Тому адміністративні та фізичні витрати можуть бути досить значними. Кожен канал в такій мережі фактично є каналом, пов'язаним з іншим вузлом сполученням «точка-точка».

На малюнку показані три найбільш поширені фізичні топології глобальної мережі.

Гібрид - це варіант або поєднання будь-яких з вищевказаних топологій. Наприклад, частково-чарункова мережа - це гібридна топологія, в якій поєднані деякі, але не всі, кінцеві пристрої.

Фізична топологія «точка-точка»

Фізичні двоточкові топології безпосередньо пов'язують два вузла, як показано на малюнку.

У такій мережі двом вузлам не потрібно використовувати середу спільно з іншими вузлами. Крім того, вузлу не потрібно визначати, адресований чи входить кадр саме йому або ж іншого вузла. Отже, протоколи управління логічними з'єднаннями канального рівня можуть бути дуже простими, оскільки всі кадри в середовищі можуть передаватися тільки між двома вузлами. Вузол на одному кінці поміщає кадри в середу, а вузол на іншому кінці двухточечного з'єднання отримує ці кадри з середовища.

Логічна топологія «точка-точка»

Прикінцеві вузли, які взаємодіють з двухточечной мережі, можуть бути фізично з'єднані за допомогою декількох проміжних пристроїв. Однак те, як ці фізичні пристрої використовуються в мережі, не впливає на логічну топологію.

Як показано на малюнку 1, що знаходяться на деякій відстані один від одного вузол джерела і вузол призначення можуть з'єднуватися один з одним не безпосередньо. У деяких випадках логічне з'єднання між вузлами формує так званий віртуальний канал. Віртуальний канал - це логічне з'єднання, створене в мережі між двома мережевими пристроями. Два вузла на обох кінцях віртуального каналу обмінюються кадрами між собою. Це відбувається і в тому випадку, якщо кадри передаються через проміжні пристрої, як показано на малюнку 2. Віртуальні канали - це важливі компоненти логічних з'єднань, що використовуються в деяких технологіях рівня 2.

Метод доступу до середовища, що використовується протоколом канального рівня, визначається логічною двухточечной топологією, а не фізичної топологією. Це означає, що логічне двухточечное з'єднання між двома вузлами не обов'язково пов'язує два фізичних вузла, розташовані на різних кінцях одного фізичного каналу зв'язку.

Фізичні топології локальних мереж

Фізична топологія визначає, як саме фізично з'єднані кінцеві системи. У локальних мережах з спільно використовуваної середовищем кінцеві пристрої можуть бути з'єднані за допомогою наступних фізичних топологій.

Зірка (Star): в топологиях типу «зірка» кінцеві пристрої підключаються до центрального проміжного пристрою. У ранніх топологиях типу «зірка» кінцеві пристрої з'єднувалися за допомогою концентраторів Ethernet. Однак тепер у топологиях типу «зірка» використовуються комутатори Ethernet. Топологію типу «зірка» відрізняють простий монтаж, висока масштабованість (просте додавання і видалення кінцевих пристроїв) і просте усунення неполадок.

Розширена зірка (Extended Star): в розширеній зіркоподібній топології додаткові комутатори Ethernet забезпечують з'єднання з іншими зіркоподібними топологиями. Розширена зірка - це приклад гібридної топології.

Шина (Bus): все кінцеві системи пов'язані один з одним загальним кабелем, що має на кінцях спеціальні заглушки («термінатори»). Для з'єднання кінцевих пристроїв комутатори не потрібні. Шинні топології на основі коаксіальних кабелів використовувалися раніше в мережах Ethernet завдяки своїй дешевизні і простому монтажу.

Кільце (Ring): кожна крайова система з'єднується з сусідньою системою, утворюючи мережу в формі кільця. На відміну від шинної топології кільцева

топологія не вимагає застосування термінаторів. Кільцеві топології використовувалися в застарілих мережах FDDI (Fiber Distributed Data Interface) і Token Ring.

На малюнку показана організація з'єднань між кінцевими пристроями в локальних мережах. Як правило, при графічному зображенні структури мереж прямими лініями позначаються локальні мережі Ethernet, включаючи топології типу «зірка» та «розширена зірка».

Напівдуплексна і полнодуплексная передача даних

Дуплексний зв'язок - це зв'язок з можливістю передачі інформації між двома пристроями в обох напрямках. При полудуплексной зв'язку передача даних в кожен момент часу можлива тільки в одному напрямку (т. Е. Їх можна або передавати, або приймати), тоді як при полнодуплексной зв'язку дані можна передавати і приймати одночасно.

Напівдуплексна зв'язок: обидва пристрої можуть передавати і отримувати інформацію через середу, але не одночасно. Напівдуплексний режим використовується в застарілих шинних топологиях і при використанні концентраторів Ethernet. Мережі WLAN також працюють в напівдуплексному режимі. Напівдуплексний режим дозволяє здійснювати передачу або прийом по загальному середовищу одночасно тільки одного пристрою і використовується в разі застосування методів конкурентного доступу. На малюнку 1 показаний напівдуплексний режим зв'язку.

Повнодуплексна зв'язок: обидва пристрої одночасно можуть передавати і приймати дані по засобам підключення. Канальний рівень передбачає одночасну доступність середовища обом вузлів для передачі. Комутатори Ethernet за замовчуванням працюють в повнодуплексному режимі, але можуть працювати і в напівдуплекса при підключенні до таких пристроїв, як комутатори Ethernet. На малюнку 2 показаний повнодуплексний режим зв'язку.

Важливо, щоб два пов'язаних інтерфейсу, наприклад мережевий інтерфейс вузла і інтерфейс комутатора Ethernet, використовували один і той же двобічний режим. В іншому випадку буде виникати невідповідність дуплексних режимів, що приводить до зниження ефективності і затримок в каналі зв'язку.

Методи управління доступом до середовища передачі

У деяких мережевих топологиях безліч вузлів використовує загальне засіб підключення. Такі мережі називаються мережами з множинним доступом. Прикладами таких мереж є локальні мережі Ethernet і бездротові локальні мережі (WLAN). У будь-який момент може виникнути ситуація, коли кілька пристроїв намагається відправити або отримати дані, використовуючи один і той же засіб підключення.

У деяких мережах з множинним доступом необхідні правила регулювання доступу пристроїв до загальної фізичної середовищі. Існує два основні методи управління доступом до загального середовища.

Конкурентний доступ: всі вузли, що працюють в напівдуплексному режимі, змагаються за використання середовища, але здійснювати передачу в кожен момент часу може лише один пристрій. Однак існує спеціальний протокол, що визначає, що повинно відбуватися в разі одночасної передачі обома пристроями. Прикладами такого типу управління доступом є локальні

мережі Ethernet з концентраторами і бездротові локальні мережі (WLAN). На малюнку 1 показаний конкурентний доступ.

Керований доступ: кожному вузлу відводиться власний час для використання середовища. Такі детерминистические типи мереж є неефективними через те, що пристрій має чекати своєї черги для доступу до середовища. Прикладами такого типу управління доступом є застарілі мережі Token Ring.

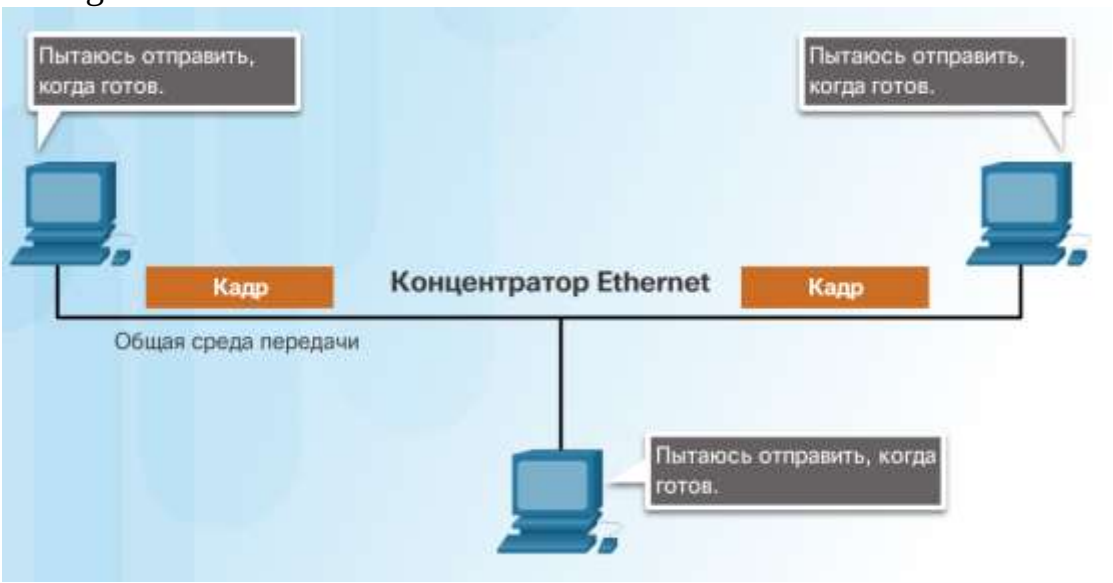


Рис. 1.1.44 Схема адресації в мережі Token Ring

За замовчуванням комутатори Ethernet працюють в повнодуплексному режимі. Це дозволяє комутатора і підключеному до нього в повнодуплексному режимі пристрою здійснювати передачу і прийом одночасно.

Конкурентний доступ - CSMA / CD

Прикладами мереж з конкурентним доступом є бездротові локальні мережі (WLAN), локальні мережі Ethernet з концентраторами і застарілі мережі Ethernet з шинної топологією. Всі ці мережі працюють в напівдуплексному режимі. При цьому необхідний спеціальний протокол, що визначає, коли пристрій може здійснювати передачу, і що відбувається в разі одночасної передачі декількома пристроями.

У напівдуплексних мережах Ethernet використовується протокол множинного доступу з прослуховуванням несучої і виявленням зіткнень (Carrier Sense Multiple Access / Collision Detection; CSMA / CD). На малюнку 1 показана мережа Ethernet з концентратором. Протокол CSMA працює за наступним алгоритмом:

1. У PC1 є кадр Ethernet, який потрібно передати в PC3.

2. Мережева плата PC1 повинна визначити, чи здійснює хто-небудь передачу по середовищі. Якщо вона не виявляє сигнал несучої, іншими словами, не приймає дані від іншого пристрою, то робить висновок про те, що мережа вільна для передачі.

3. Мережева плата PC1 передає кадр Ethernet.

4. Концентратор Ethernet приймає кадр. Концентратор Ethernet також називають багатопортовим ретранслятором. Він здійснює регенерацію всіх бітів, прийнятих на вхідному порте, і їх розсилку через всі інші порти.

5. Якщо інший пристрій, наприклад PC2, хоче здійснити передачу, але в даний момент приймає кадр, воно повинно дочекатися звільнення каналу.

6. Кадр буде доставлений всім пристроям, підключеним до концентратора. Але оскільки в кадрі адреса був призначений додатковий цільового каналу даних, що відноситься до PC3, то тільки цей пристрій буде приймати і зберігати весь кадр. Мережеві плати всіх інших пристроїв ігнорують кадр.

Якщо два пристрої виконують передачу одночасно, виникає конфлікт. Обидва пристрої виявлять конфлікт в мережі. Це називається виявленням конфліктів (CD). Мережева плата розпізнає цей конфлікт, порівнюючи відправлені дані з прийнятими або визначаючи перевищення нормальної амплітуди сигналу в середовищі передачі даних. Дані, що передаються обома пристроями, будуть пошкоджені, через що потрібно їх повторна відправка.

Конкурентний доступ - CSMA / CA

Іншим видом доступу CSMA, використовуваним в бездротових локальних мережах IEEE 802.11, є множинний доступ з прослуховуванням несучої і уникненням зіткнень (Carrier Sense Multiple Access / Collision Avoidance; CSMA / CA). При доступі CMSA / CA для контролю звільнення середовища використовується метод, аналогічний CSMA / CD. У CMSA / CA також використовуються додаткові процедури. CMSA / CA не може виявити конфлікти, а намагається уникнути їх, чекаючи своєї черги для передачі. Кожне передавальний пристрій включає в передану інформацію відомості про час, необхідний йому для передачі. Всі інші бездротові пристрої приймають цю інформацію і знають, як довго середовище передачі даних буде зайнята (див. Малюнок). Після передачі бездротовим пристроєм кадру 802.11 приймач повертає підтвердження, інформуючи відправника про отримання кадру.

Незалежно від виду мережі (будь то локальна мережа Ethernet з концентраторами або бездротова локальна мережа), системи з конкурентним доступом погано масштабуються при інтенсивному використанні засоби підключення. Слід зазначити, що в локальних мережах Ethernet з комутаторами конкурентний доступ не використовується, оскільки комутатор і мережева плата вузла працюють в повнодуплексному режимі.

кадр

Канальний рівень готує пакет для переміщення по середовищі передачі даних локальної мережі, додаючи до нього заголовок і кінцевик з метою створити кадр. Опис кадру є ключовим елементом кожного протоколу канального рівня. Хоча кадри канального рівня описуються безліччю різних протоколів канального рівня, кадри будь-якого типу складаються з трьох основних компонентів.

- Заголовок
- дані
- кінцевик

Всі протоколи канального рівня інкапсулюють одиницю даних протоколу (PDU) рівня 3 в межах поля даних кадру. Однак структура кадру і полів, що містяться в заголовку і кінцівки, відрізняється в залежності від протоколу.

Не існує такої структури кадру, яка відповідала б вимогам всіх видів передачі даних у всіх типах засобів підключення. Кількість інформації, що

управляє, яка має бути присутня в кадрі, залежить від оточення і змінюється відповідно до вимог управління доступом для конкретної середовища і логічної топології.

поля кадру

Кадрування ділить потік на дешіфруемие групи. Керуюча інформація міститься в заголовок і кінцевик у вигляді значень в різних полях. Цей формат надає фізичним сигналам структуру, яку вузли здатні приймати і декодувати в пакети в точці призначення.

Рис. 1.1.45 Типи полів кадру.

Прапори початку і кінця кадру: використовуються для визначення меж початку і кінця кадру.

Адресація: вказує вузли джерела і призначення в середовищі передачі даних.

Тип: вказує протокол рівня 3 в поле даних.

Управління: вказує особливі служби управління потоком, наприклад якість обслуговування (QoS). Служба QoS використовується для пріоритетної пересилання певних типів повідомлень. Кадри каналів передачі даних, в яких пересилаються пакети протоколу VoIP, зазвичай користуються пріоритетом, оскільки вони чутливі до затримок.

Дані: містить корисну навантаження кадру (т. Е. Заголовок пакета, заголовок сегмента і дані).

Виявлення помилок: ці поля кадру використовуються для виявлення помилок і поміщаються після даних для формування концевика.

Не кожен протокол включає в себе всі ці поля. Фактичний формат кадру визначається стандартами для конкретного канального протоколу.

Протоколи канального рівня додають кінцевик в кінець кожного кадру. Кінцевик використовується, щоб перевірити наявність помилок в прийнятому кадрі. Цей процес називається виявленням помилок. Для цього в кінцевик кадру розміщується спеціальна інформація, отримана шляхом математичної або логічної обробки вмісту кадру. Біти виявлення помилок додаються на канальному рівні, т. К. Сигнали в середовищі передачі даних можуть бути схильні до перешкод, перекручувань або втрат, в результаті чого значення представлених цими сигналами бітів можуть змінюватися.

Передавальний вузол шляхом логічної обробки вмісту кадру створює так званий циклічний надлишковий код (cyclic redundancy check, CRC). Значення цього коду поміщається в поле контрольної послідовності кадру (Frame Check Sequence, FCS) і надає інформацію про вміст кадру. Поле FCS в кінцевик кадру Ethernet дозволяє приймаючому вузлу перевіряти кадр на наявність помилок передачі. Додаткову інформацію про кінцевик кадру см. В розділі «Додаток».

Адреса рівня 2

Канальний рівень забезпечує адресацію, яка використовується під час пересилання кадру по спільно використовуваної середовища передачі даних в локальній мережі. Адреси пристроїв на цьому рівні називаються фізичними адресами. Адресація канального рівня міститься в заголовку кадру і вказує вузол призначення кадру в локальній мережі. Заголовок кадру може також містити адресу джерела кадру.

На відміну від логічних адрес рівня 3, які є ієрархічними, фізичні адреси не вказують, в якій мережі знаходиться пристрій. Фізична адреса - це адреса конкретного фізичного пристрою. Якщо пристрій переміщається в іншу мережу або підмережа, воно продовжить функціонувати з тим же фізичним адресою рівня 2.

На малюнках 1-3 представлені функції адрес рівнів 2 і 3. В ході пересилання IP-пакетів від вузла до маршрутизатора, між маршрутизаторами і, нарешті, від маршрутизатора до вузла в кожній точці на шляху свого проходження IP-пакет инкапсулируется в новий кадр каналу передачі даних. Кожен кадр канального рівня містить адресу каналу-джерела (який передав цей кадр мережевої плати) та адреса каналу призначення (мережевий плати, що приймає цей кадр).

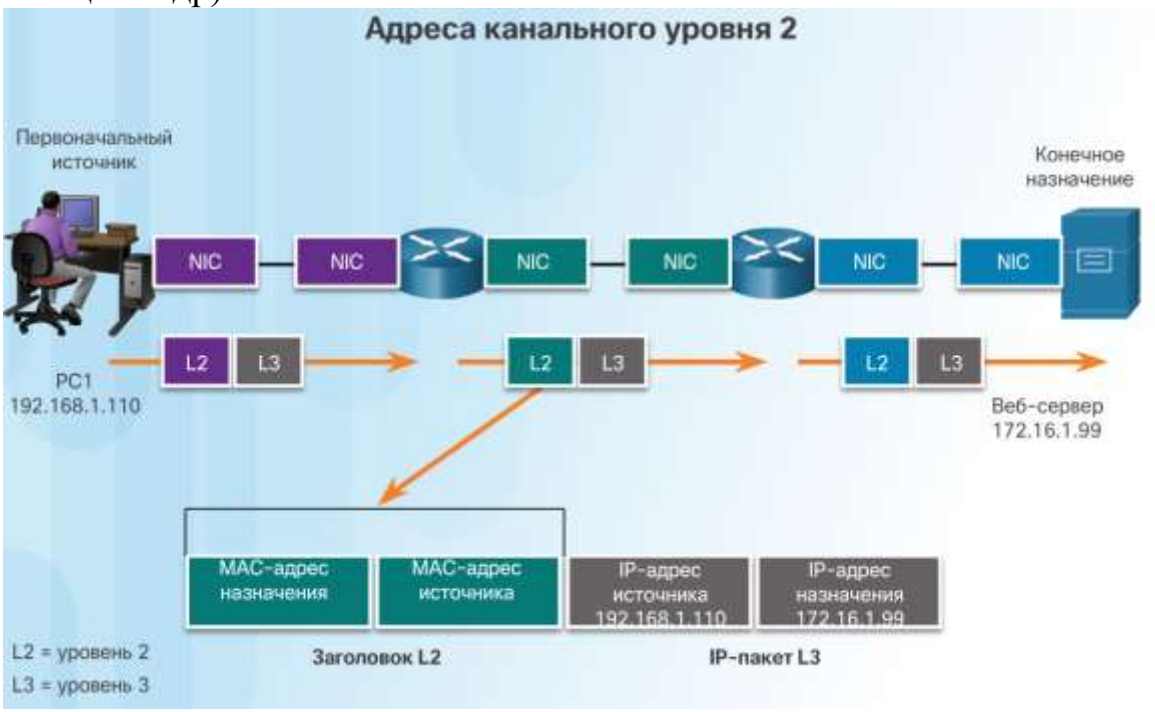


Рис. 1.1.46 Схема адресації на канальному рівні

Адреса, відповідний конкретному пристрою і не є ієрархічним, не можна використовувати для пошуку пристроїв у великих мережах або в Інтернеті. Це було б так само складно, як шукати єдиний конкретний будинок по всій земній кулі, знаючи лише номер будинку і назва вулиці. Однак фізичну адресу можна

використовувати для виявлення пристрою в обмеженій зоні. Тому адреса канального рівня використовується тільки для локальної доставки пакетів. Адреси цього рівня не мають сенсу за межами локальної мережі. Порівняйте їх з рівнем 3, де адреси в заголовку пакета передаються від вузла джерела на вузол призначення, незалежно від кількості транзитних ділянок мережі на протязі маршруту.

Якщо дані повинні перейти в інший сегмент мережі, необхідно проміжне пристрій, наприклад маршрутизатор. Маршрутизатор повинен прийняти кадр згідно фізичній адресою і деінкапсуліровать його для аналізу ієрархічного адреси або IP-адреси. За допомогою IP-адреси маршрутизатор може визначити місце розташування пристрою призначення в мережі, а також найкращий шлях до нього. Дізнавшись, куди необхідно переслати пакет, маршрутизатор створює для нього новий кадр, який відправляється в наступний мережевий сегмент до місця призначення.

Кадри LAN і WAN

У мережі на основі стека протоколів TCP / IP всі протоколи рівня 2 моделі OSI працюють з протоколом IP на рівні 3 моделі OSI. Однак фактично використовуваний протокол рівня 2 залежить від логічної топології мережі і фізичного середовища передачі даних.

Кожен протокол управляє доступом до середовища для зазначених логічних топологій рівня 2. Це означає, що при реалізації цих протоколів в якості вузлів, що діють на канальному рівні, може використовуватися цілий ряд різних мережевих пристроїв. До таких пристроїв відносяться мережеві плати на комп'ютерах, а також інтерфейси на маршрутизаторах і комутаторах рівня 2.

Протокол рівня 2, який використовується для конкретної топології мережі, визначається технологією, яка використовується для реалізації цієї топології. Ця технологія, в свою чергу, визначається розміром мережі (з точки зору кількості вузлів і території) і сервісами, що надаються в цій мережі.

У локальних мережах зазвичай використовуються технології, які забезпечують високу пропускну здатність і підтримують велику кількість вузлів. Порівняно невелика протяжність локальних мереж (в межах одного будинку або комплексу будинків) і висока щільність користувачів забезпечують рентабельність цієї технології.

Однак використання технології з високою пропускною здатністю зазвичай нерентабельно для глобальних мереж, що охоплюють великі території (наприклад, міста або цілі області). Зважаючи на високу вартість фізичних каналів великої протяжності і технологій, що використовуються для передачі сигналів на великі відстані, пропускна здатність таких мереж, як правило, визначається рівнем рентабельності.

Різниця в пропускної здатності вимагає використання різних протоколів для локальних і глобальних мереж.

До протоколів канального рівня відносяться:

- Ethernet
- Бездротова мережа 802.11
- Протокол точка-точка (протокол PPP)
- HDLC

- Протокол ретрансляції кадрів (протокол Frame Relay)

1.2. Доступ до мережі та огляд моделі OSI.

На сьогоднішній день Ethernet є найбільш часто використовуваної технологією для локальних мереж (LAN). Це сімейство мережевих технологій, які регламентуються стандартами IEEE 802.2 і 802.3. Стандарти Ethernet регламентують як протоколи рівня 2, так і технології рівня 1. Для протоколів рівня 2, як і у випадку з усіма стандартами групи IEEE 802, технологія Ethernet спирається на роботу цих двох окремих підрівнів канального рівня, а також на підрівні управління логічним зв'язком (LLC) і MAC.

На канальному рівні структура кадру практично ідентична для всіх швидкостей Ethernet. У структурі кадру Ethernet на початку і кінці PDU рівня 3 додаються заголовки і кінцевики для інкапсуляції відправляється.

Існує два стилю формування кадрів Ethernet: стандарт Ethernet IEEE 802.3 і стандарт Ethernet DIX, який тепер називається Ethernet II. Найбільш істотною відмінністю між цими двома стандартами є додавання в стандарті 802.3 початку обмежувача кадру (SFD) і зміна поля «Тип» на поле «Довжина». Ethernet II - це формат кадру Ethernet, що використовується в мережах TCP / IP. Кадр Ethernet, що представляє собою результат реалізації набору стандартів IEEE 802.2 / 3, надає функції MAC-адресації і перевірки помилок.

Адресація Ethernet рівня 2 підтримує одно-адресний, багатоадресний і широкомовний режими передачі даних. Ethernet використовує протокол дозволу адрес (ARP) для визначення MAC-адрес призначення і їх зіставлення з відомими IPv4-адрес.

У кожного вузла в IPv4-мережі є MAC і IPv4-адреси. IP-адреси використовуються для визначення джерела і призначення пакета. MAC-адреси Ethernet використовуються для відправки пакета від однієї мережевої плати Ethernet на іншу мережеву плату Ethernet в одній і тій же IP-мережі. Протокол дозволу адрес (ARP) використовується для зіставлення відомого IPv4-адреси з MAC-адресою, що дає можливість инкапсулировать пакет в кадрі Ethernet з відповідним адресою рівня 2.

У своїй роботі протокол дозволу адрес (ARP) використовує конкретні типи широкомовних і одно-адресних повідомлень Ethernet, які також називаються ARP-запитами і відповідями. Протокол дозволу адрес (ARP) дозволяє зіставляти IPv4-адреси з MAC-адресами і вести таблицю зіставлень.

У більшості мереж Ethernet кінцеві пристрої, як правило, підключаються до повнодуплексного комутатора рівня 2 за принципом «точка-точка». Комутатор локальної мережі (LAN) рівня 2 здійснює комутацію і фільтрацію тільки на основі MAC-адреси канального рівня моделі OSI. Комутатор рівня 2 створює таблицю MAC-адрес, яку в подальшому використовує для пересилання пакетів. Для передачі даних між незалежними IP-підмережами комутаторів рівня 2 необхідні маршрутизатори.

Фізичний рівень OSI забезпечує засоби транспортування бітів, що утворюють кадр даних канального рівня, за допомогою засобу мережевого зв'язку.

В даний час Ethernet є основною технологією для локальних мереж (LAN) у всьому світі. Ethernet функціонує на канальному та фізичному рівнях. Стандарти протоколів Ethernet визначають багато аспектів мережевого обміну

даними, включаючи формат і розмір кадру, інтервал відправлення та кодування. При передачі повідомлень між вузлами в мережі Ethernet, вузли форматують їх відповідно до стандартів макета кадрів.

Потому що технологія Ethernet складається з стандартів на цих більш низьких рівнях, принцип її роботи можна краще зрозуміти на прикладі моделі OSI. Модель OSI відокремлює функціональні можливості адресації канального рівня, формування кадрів і доступу до середовища передачі даних від стандартів фізичного рівня такого середовища. Стандарти Ethernet регулюють як протоколи рівня 2, так і технології рівня 1. Незважаючи на те, що технічні вимоги Ethernet підтримують різні середовища передачі даних, пропускна смуга та інші варіанти рівнів 1 і 2, основна формат кадрів і схема адреси будуть однаковими для всіх різновидів Ethernet .

В цьому розділі детально розглянуті характеристики та робота технології Ethernet за її розвитком, починаючи з спільно використовуваної середовища передачі даних та вільного обміну даними і закінчуючи сучасною високошвидкісною і повнодуплексною технологією.

Інкапсуляція Ethernet

На сьогоднішній день Ethernet є самої часто використовуваною технологією для локальних мереж (LAN).

Ethernet функціонує на канальному та фізичному рівнях. Це семейство мережевих технологій, які регулюються стандартами IEEE 802.2 та 802.3. Технологія Ethernet підтримує передачу даних на наступних швидкості.

- 10 Мбіт / с
- 100 Мбіт / с
- 1 000 Мбіт / с (1 Гбіт / с)
- 10 000 Мбіт / с (10 Гбіт / с)
- 40 000 Мбіт / с (40 Гбіт / с)
- 100 000 Мбіт / с (100 Гбіт / с)

Как показано на рис. 1, стандарти Ethernet регулюються як протоколи рівня 2, так і технології рівня 1. Для протоколів рівня 2, як і у випадку з усіма стандартами групи IEEE 802, технологія Ethernet опирається на роботу цих двох окремих подурівень канального рівня, а також на подуровні управління логічної зв'язок (LLC) і MAC.

Підрівень ТОВ технології Ethernet забезпечує зв'язок між верхніми та нижніми рівнями. Як правило, це відбувається між мережевим програмним забезпеченням та обладнаним забезпеченням пристрою. LLC Підрівень використовує дані мережевих протоколів, які звичайно представлені у вигляді IPv4-пакета, і додає керуючу інформацію для доставки пакета до призначення вузла. ТОВ використовується для зв'язку з верховими рівнями додатків і передачі пакету на нижні рівні.

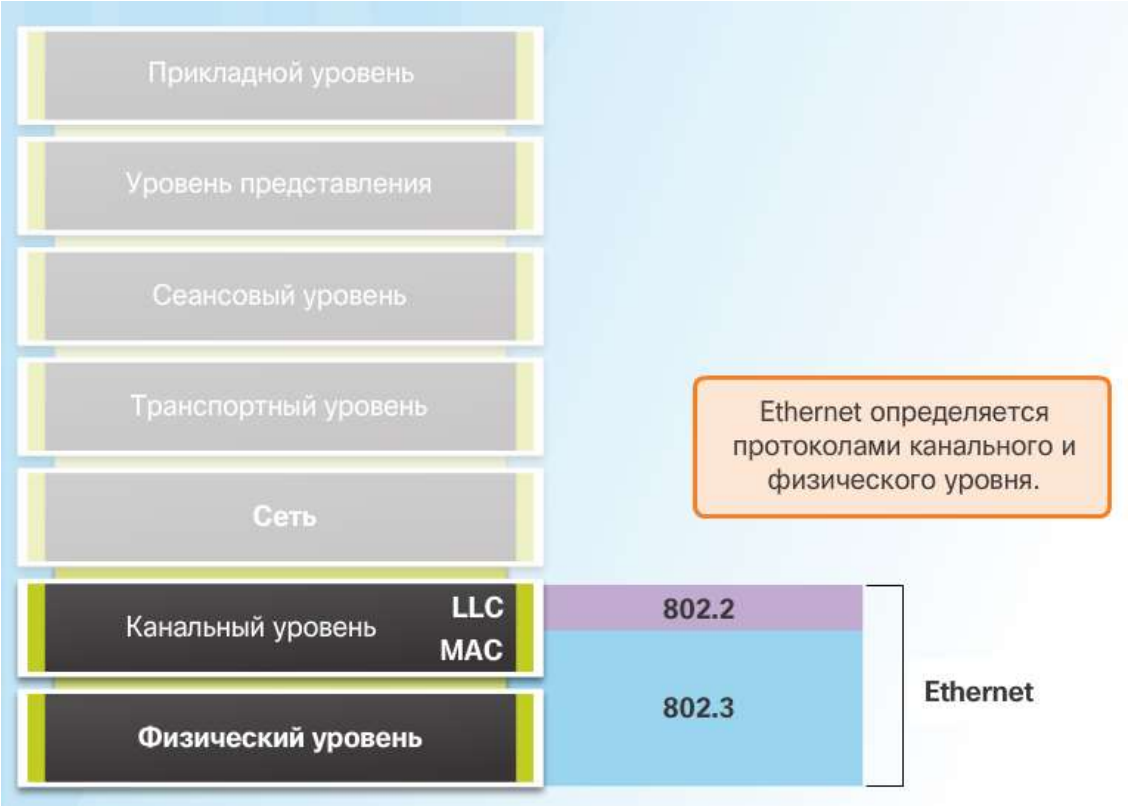


Рис. 1.1 Стандарти канального рівня

ТОВ реалізується в програмному забезпеченні, і його застосування не залежить від обладнання. ТОВ для комп'ютера можна розглядати як програмне забезпечення драйвера мережевої плати (NIC). Драйвер мережевої карти - це програма, яка безпосередньо взаємодіє з комп'ютерними засобами комп'ютера на мережевій платі для передачі даних між підрівнем MAC і фізичною середовищем.

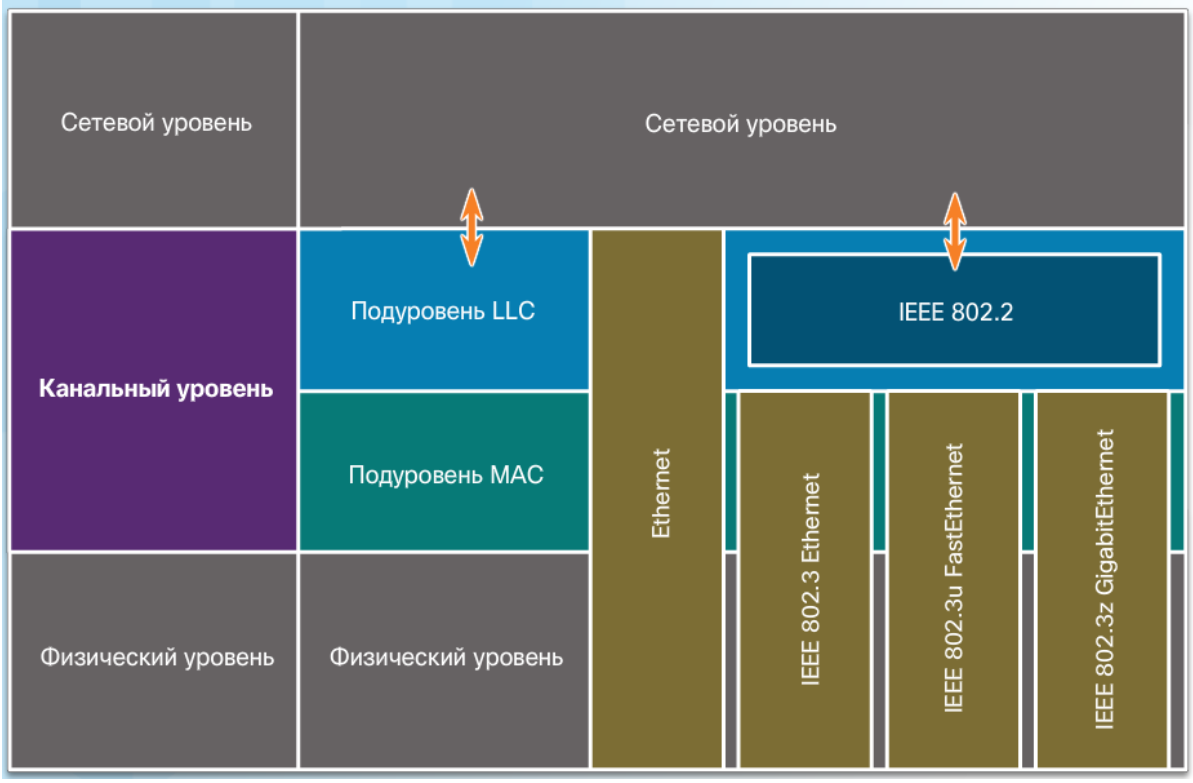


Рис. 1.2 Заголовок Ethernet-кадра

MAC представляє собою більш низький підрівень канального рівня. MAC реалізується апаратно - зазвичай в мережевій платі комп'ютера.

Підрівень MAC

Як показано на малюнку, Підрівень технології MAC Ethernet виконує два основні завдання.

- Інкапсуляція даних
- Управління доступом до середовища.
- Інкапсуляція даних

Процес інкапсуляції даних включає в себе збірку кадрів перед його відправкою та розбіркою кадрів після його отримання. При формуванні кадра на рівні MAC до одиниці протоколу (PDU) мережевого рівня додаються заголовок і затримка.

Інкапсуляція даних забезпечує три основні функції.

Розділ кадра: процес формування кадрів надає важливі роздільники, які використовуються для визначення групи біт, що складають кадр. Ці розмежувальні біти забезпечують синхронізацію між передаючими та отриманими вузлами.

Адресація: процес інкапсуляції містить протокол одиниці даних (PDU) рівня 3 і також забезпечує адресацію канального рівня.

Обнаруження помилок: кожен кадр містить обмеження, що дозволяє виявляти помилки передачі.

Використання кадрів полегшує передачу даних в передачу даних, а також дозволяє групувати біти на приймаючому вузлі.

Втора функція підрівень MAC - управління доступом до середовища передачі даних. Управління доступом до середовища передачі даних відповідає за розміщення кадрів у цьому середовищі та видалення з неї кадрів. Як зрозуміло з назви цієї функції, вона дозволяє керувати доступом до середовища передачі даних. Це Підрівень напряму взаємодіє з фізичним рівнем.

Основна логічна топологія Ethernet - це шина з множинним доступом; Відповідно, середовище передачі даних використовується всіма вузлами (пристроями) в одному сегменті мережі. Ethernet - це організація мережі на основі конкурентного доступу. Конкурентоспроможний доступ означає, що будь-який пристрій може постійно намагатися передавати дані в загальному середовищі при наявності таких даних для відправки. У півдуплексних локальних мережах Ethernet для виявлення та усунення колізій використовується метод множинного доступу з контролем носія та виявлення колізій (Carrier Sense Multiple Access / Collision Detection; CSMA / CD). У сучасних локальних мережах Ethernet використовуються повнодуплексні комутатори, які дозволяють одночасно декількома пристроями відправляти і отримувати дані без колізій.

Розвиток Ethernet

З моменту створення Ethernet в 1973 р. Стандарти вдосконалені, слідуючи за появою більш швидких і гнучких версій технологій. Можливість постійного вдосконалення технології Ethernet з течією часу - одна з основних причин її популярності. Швидкість ранніх версій Ethernet була порівняно низькою, всього 10 Мбіт / сек. Новіші версії мережі Ethernet працюють зі швидкістю 10 гігабіт в

секунду та більше. Перемістіть повзунок на тимчасовій шкалі рис. 1, щоб побачити, як змінювалися стандарти Ethernet з потоком часу.

Рис. 1.3 Структура Ethernet-кадра

На канальному рівні структура кадра практично ідентична для всіх швидкостей Ethernet. У структурі кадру Ethernet на початку і кінці одного рівня даних протоколу (PDU) рівня 3 додаються заголовки і обмеження для інкапсуляції відправленого повідомлення, як показано на рис. 2

Ethernet II - це формат кадра Ethernet, що використовується в мережах TCP/IP.

Поля кадра Ethernet

Мінімальний розмір кадра Ethernet - 64 байта, максимальний - 1518 байт. До цього числа відносяться всі байти, починаючи з поля «MAC-адреса призначення» і закінчуючи полем «Контрольна послідовність кадру (FCS)». Полі «Преамбула» при описі розміру кадра не включено.

Любой кадр із довжиною менше 64 байт вважається «фрагментом колізій» або «карликовим кадром» і автоматично відхиляється приймаючими станціями. Кадри з довжиною більше 1500 байт називаються Jumbo-кадрами (значно вищі за допустимий розмір) або Baby Giant (ледве вищі за допустимий розмір).

Якщо розмір переданого кадра менше меншого значення або більше максимального значення, одержувач пристрою скидає такий кадр. Відкинуті кадри, швидше за все, є результатом колізій або інших небажаних сигналів і, отже, вважаються недійсними.

MAC-адреса і шістнадцятирічна система з числом

MAC-адреса Ethernet - це 48-бітове двоїчне значення, виражене у вигляді 12 шістнадцятирічних чисел (4 бали за кожну шістнадцятку цифру).

Якщо 8 біт (1 байт) - це загальноприйнята бінарна група, то двійовий код 00000000-11111111 може бути представлений в шістнадцятирічній системі числення як діапазон 00-FF, як показано на рис. 2. Щоб заповнити 8-бітне представлення, завжди відображаються ведучі нулі. Наприклад, двоїчне значення 0000 1010 показано в шістнадцятирічній системі як 0A.

Шестнадцатерична система з розрахунку використовується для представлення MAC-адрес Ethernet та IP-адрес версії 6.

Структура MAC-адресів

Значення MAC-адреси - це безпосередній результат застосування правил, які розроблені інститутом IEEE для постачальників, щоб забезпечити унікальні

на глобальному масштабі адреси для кожного пристрою Ethernet. Відповідно до цих правил кожен постачальник, який займається реалізацією пристроїв Ethernet, повинен бути зареєстрований в IEEE. IEEE присвоює постачальнику 3-байтовий (24-бітний) код, який називається унікальним ідентифікатором організації (OUI).

Інститут IEEE вимагає від постачальників дотримання двох простих правил, як показано на малюнку:

Усі MAC-адреси, призначені мережевою платою або іншим пристроєм Ethernet, повинні обов'язково порядок використання цього ідентифікатора OUI постачальника в перших 3 байтах.

Для всіх MAC-адрес з єдиним ідентифікатором OUI необхідно встановити унікальні значення в останніх 3 байтах.

Примітка. Можуть існувати дублюючі MAC-адреси, що пов'язано з помилками при виробництві або впровадженні віртуальних машин. В будь-якому випадку MAC-адреса обов'язково буде змінюватися в новій мережевій платі або програмному забезпеченні.

Обробка кадрів

MAC-адресу часто називається «вбудованим» або «зашитим» адресою (burned-in address, BIA), оскільки історично склалося так, що він записується в ПЗУ (постійний запам'ятовуючий пристрій) на мережевий платі. Це означає, що адреса вноситься в чіп ПЗУ на апаратному рівні без можливості подальшої зміни.

Примітка. Операційні системи і мережеві плати сучасних комп'ютерів підтримують можливість зміни MAC-адреси за допомогою програм. Це зручно при спробі отримання доступу до мережі, в якій використовується фільтрація на основі BIA. Отже, фільтрація або відстеження трафіку на основі MAC-адреси більше не є надійним способом.

При запуску комп'ютера мережева плата спочатку копіює MAC-адресу з ПЗУ в ОЗУ. Коли пристрій пересилає повідомлення в мережу Ethernet, воно додає до кадру інформацію заголовка. Інформація заголовка містить MAC-адреси джерела і призначення.

Натисніть кнопку «Відтворення», щоб переглянути відеоролик про процес пересилання кадру. При надходженні кадру Ethernet на мережеву плату вона перевіряє MAC-адресу призначення, щоб визначити, чи збігається він з фізичним MAC-адресою пристрою, збереженим в ОЗУ. Якщо не вдається виявити збіги, пристрій відхиляє кадр. При наявності збігу мережева плата передає кадр вгору за рівнями моделі OSI, де відбувається процес деінкапсуляції.

Примітка. Мережеві плати пристроїв Ethernet приймають кадри також в тому випадку, якщо MAC-адресу призначення є широкомовної розсилкою або групою під LGPL, в яку включений вузол.

Всіх пристроїв, які можуть бути вузлами джерела або призначення кадру Ethernet, необхідно присвоїти MAC-адресу. До них відносяться робочі станції, сервери, принтери, мобільні пристрої і маршрутизатори.

Уявлення MAC-адрес

На вузлі Windows MAC-адресу адаптера Ethernet можна визначити за допомогою команди ipconfig / all. На рис. 1 на екрані відображається фізичну

адресу (MAC-адресу) комп'ютера в форматі 00-18-DE-DD-A7-B2. Якщо у вас є відповідні права доступу, ви можете виконати цю операцію на своєму комп'ютері. На вузлах MAC або Linux використовується команда ifconfig.

Залежно від пристрою і операційної системи ви побачите різні уявлення MAC-адрес, як показано на рис. 2. Для маршрутизаторів і комутаторів Cisco використовується формат XXXX.XXXX.XXXX, де X - це шістнадцятковий символ.

Індивідуальний MAC-адресу

У мережі Ethernet для одноадресної, многоадресной і широкомовної розсилки рівня 2 використовуються різні MAC-адреси.

Індивідуальний MAC-адресу - це унікальна адреса, яка використовується при відправленні кадру від одного передавального пристрою до одного пристрою призначення.

У прикладі, показаному в анімації, вузол з IPv4-адресою 192.168.1.5 (джерело) запитує веб-сторінку з сервера з IPv4-адресою одноадресної розсилки 192.168.1.200. Для відправки та прийому одноадресна пакета в заголовку IP-пакета повинен вказуватися IP-адреса призначення. Крім того, в заголовку кадру Ethernet повинен бути MAC-адресу призначення. IP-адреса і MAC-адресу - це дані для доставки пакета одному вузлу.

Для визначення MAC-адреси призначення на вузлі джерела використовується протокол дозволу адрес (ARP). Протокол дозволу адрес (ARP) розглядається далі в цій главі.

MAC-адресу призначення може бути адресою одноадресної, широкомовної або під LGPL, але MAC-адресу джерела завжди повинен бути індивідуальним.

MAC-адресу широкомовної розсилки

У пакеті широкомовної розсилки міститься IPv4-адрес призначення, в вузловий частини якого присутні тільки одиниці (1). Ця нумерація в адресі означає, що всі вузли в локальній мережі (домені широкомовної розсилки) отримають і оброблять пакет. Широкомовні розсилання передбачені в багатьох мережевих протоколах, наприклад DHCP і ARP.

Як показано в анімації, вузол джерела відправляє IPv4-пакет широкомовної розсилки на всі пристрої в мережі. IPv4-адрес призначення (192.168.1.255) - це адреса широкомовної розсилки. Якщо IPv4-пакет широкомовної розсилки інкапсульований в кадрі Ethernet, MAC-адресу призначення є MAC-адресою широкомовної розсилки в шістнадцятковому форматі FF-FF-FF-FF-FF-FF (48 одиниць в двійковому форматі).

MAC-адресу під LGPL

Групові адреси дозволяють вихідного пристрою розсилати пакет групі пристроїв. Пристрої, які відносяться до групи під LGPL, отримують її IP-адреса. Діапазон IPv4-адрес під LGPL - від 224.0.0.0 до 239.255.255.255. Діапазон IPv6-адрес під LGPL починається з FF00 :: / 8. Оскільки адреси під LGPL представляють собою групу адрес (яка іноді називається також групою вузлів), вони використовуються тільки як адреси призначення пакета. Джерело завжди має адресу одноадресної розсилки.

Адреси під LGPL використовуються, наприклад, в іграх з віддаленим підключенням, в яких бере участь кілька людей з різних місць. Крім того, такі

адреси використовуються при дистанційному навчанні в режимі відеоконференції, коли кілька учнів підключено до одного і того ж курсу.

Як і у випадку з адресами для одноадресної і широкомовної розсилки, IP-адресою для під LGPL потрібен відповідний MAC-адресу, щоб фактично передавати кадри по локальній мережі. MAC-адресу під LGPL, пов'язаний з IPv4-адресою під LGPL, - це особливе значення, яке починається з 01-00-5E в шестнадцатиричном форматі. Інша частина MAC-адреси під LGPL створюється шляхом перетворення нижніх 23 біт IP-адреси групи під LGPL в 6 шістнадцятирічних символів. Для IPv6-адреси MAC-адресу під LGPL починається з 33-33.

В анімації в якості прикладу використовується шістнадцятковий адресу під LGPL 01-00-5E-00-00-C8. Останній байт (або 8 біт) IPv4-адреси 224.0.0.200 - це десяткове значення 200. Найпростіший спосіб визначити шістнадцятковий еквівалент полягає в тому, щоб спочатку перетворити це значення в двійковий формат, вставивши пробіл між групами з 4 біт: 200 (десяткове значення) = 1100 1000 (двійкове значення). Потім можна використовувати таблицю перетворення двійкового формату в шістнадцятковий: 1100 1000 (двійкове значення) = 0xC8.

Основна інформація про комутатори

Комутатор Ethernet рівня 2 використовує MAC-адреси для прийняття рішення про пересилання. Пристрій не має інформації про протокол, який передається в частині кадру, виділеної для даних, наприклад, в IPv4-пакеті. Комутатор пересилає пакети тільки на основі MAC-адрес Ethernet рівня 2.

На відміну від застарілих концентраторів Ethernet, які повторюють біти на всіх портах, крім вхідного, комутатор Ethernet звертається до таблиці MAC-адрес для пересилання кожного конкретного кадру. На малюнку показаний тільки що включений 4-портовий комутатор. У ньому ще немає інформації про MAC-адресах чотирьох підключених комп'ютерів.

Примітка. Таблицю MAC-адрес іноді називають таблицею асоціативної пам'яті (CAM). Хоча поняття «таблиця асоціативної пам'яті» використовується щодо часто, в цьому курсі ми будемо називати її таблицею MAC-адрес.

Отримання інформації про MAC-адресах

Комутатор створює таблицю MAC-адрес динамічно, перевіряючи MAC-адресу джерела в кадрах, прийнятих портом. Він пересилає кадри на основі збігу між MAC-адресою призначення в кадрі і записом в таблиці MAC-адрес.

При кожному надходженні кадру Ethernet в комутатор виконується наступний процес.

Отримання інформації: перевірка MAC-адреси джерела

При кожному надходженні кадру в комутатор виконується перевірка на наявність нової інформації. Перевіряються MAC-адресу джерела, зазначений в кадрі, і номер порту, по якому кадр надходить в комутатор.

Якщо MAC-адресу джерела відсутній, він додається в таблицю разом з номером вхідного порту. У прикладі на рис. 1 комп'ютер PC-A відправляє кадр Ethernet комп'ютера PC-D. Комутатор додає MAC-адресу комп'ютера PC-A в таблицю.

Якщо MAC-адресу джерела вже існує, комутатор оновлює таймер поновлення для цього запису. За замовчуванням в більшості комутаторів Ethernet дані в таблиці зберігаються протягом 5 хвилин.

Примітка. Якщо MAC-адресу джерела вказано в таблиці, але з іншим портом, комутатор вважає цей запис нової. Запис замінюється на той же MAC-адресу, але з більш актуальним номером порту.

Пересилання: перевірка MAC-адреси призначення

Якщо MAC-адресу призначення є адресою одноадресної розсилки, комутатор шукає збіг між MAC-адресою призначення в кадрі і записом в таблиці MAC-адрес.

Якщо MAC-адресу призначення є в таблиці, комутатор пересилає кадр через вказаний порт.

Якщо MAC-адреси призначення немає в таблиці, комутатор пересилає кадр через всі порти, крім вхідного порту. Цей процес називається одноадресної розсилкою без адреси. Як показано на рис. 2, в таблиці комутатора немає MAC-адреси призначення для комп'ютера PC-D, тому він пересилає кадр через всі порти, крім порту 1.

Примітка. Якщо MAC-адресу призначення є адресою широкомовної або під LGPL, комутатор також пересилає кадр через всі порти, крім вхідного порту.

фільтрація кадрів

Оскільки комутатор отримує кадри від різних пристроїв, його таблиця MAC-адрес заповнюється через перевірку MAC-адреси джерела кожного кадру. Якщо в таблиці MAC-адрес комутатора є MAC-адресу призначення, він може виконувати фільтрацію кадрів і пересилати його через один порт.

На рис. 1 і 2 показаний комп'ютер PC-D, що пересилає кадр назад комп'ютера PC-A. Спочатку в комутаторі з'явиться інформація про MAC-адресу комп'ютера PC-D. Оскільки в таблиці комутатора вже є MAC-адресу комп'ютера PC-A, він пересилає кадр тільки через порт 1.

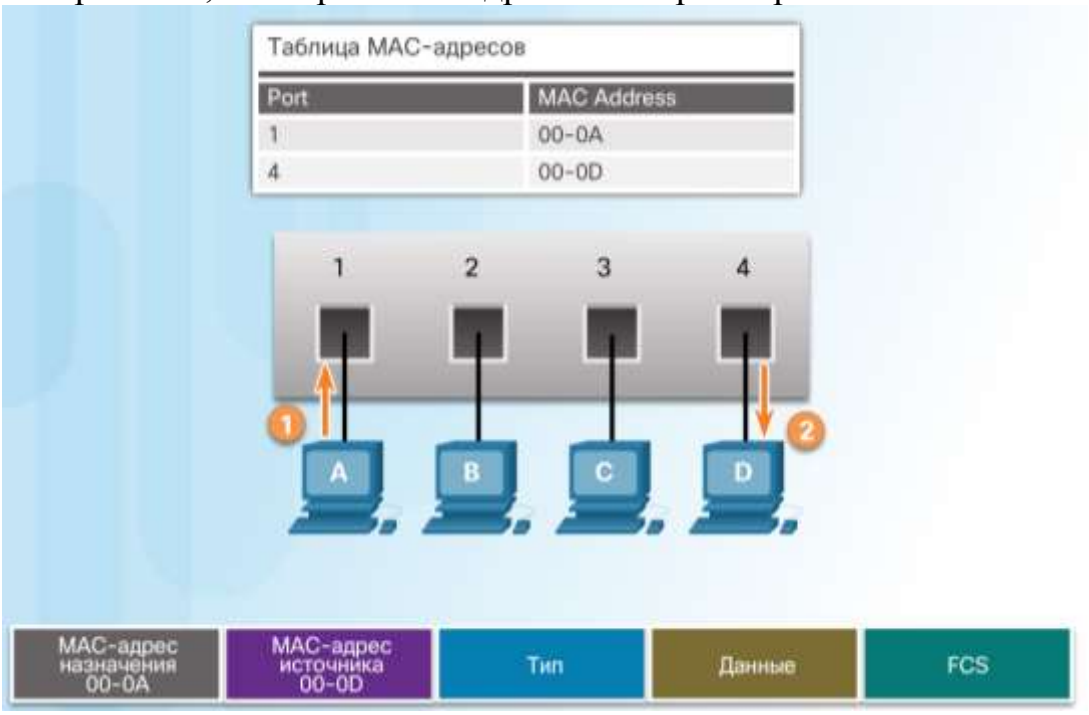


Рис. 1.4 Формування ARP-таблиці на комутаторі

На рис. 3 показаний комп'ютер PC-A, що пересилає інший кадр комп'ютера PC-D. У таблиці MAC-адрес вже є MAC-адресу комп'ютера PC-A, тому таймер 5-хвилинного поновлення цього запису скидається. Оскільки в таблиці

комутатора вже є MAC-адресу комп'ютера PC-D, він пересилає кадр тільки через порт 4.

У таблиці комутатора може бути кілька MAC-адрес, пов'язаних з одним портом. Зазвичай це відбувається тоді, коли комутатор з'єднаний з іншим комутатором. У таблиці MAC-адрес комутатора вводиться окремий запис для кожного кадру, одержуваного з іншого MAC-адреси джерела.

Якщо IP-адреса пристрою знаходиться у віддаленій мережі, відправити кадр Ethernet в пристрій призначення безпосередньо неможливо. Замість цього кадр Ethernet відправляється по MAC-адресу шлюзу, т. Е. Маршрутизатора.

Натисніть кнопку «Відтворення», щоб переглянути відеоролик про обмін даними між комп'ютером PC-A і шлюзом за замовчуванням.

Примітка. У цьому відеоролику в IP-пакеті, відправляється з комп'ютера PC-A на пристрій у віддаленій мережі, вказані IP-адреса джерела комп'ютера PC-A і IP-адреса призначення віддаленого вузла. У повернутому IP-пакеті вказані IP-адреса джерела віддаленого вузла і IP-адреса призначення, т. Е. Адреса комп'ютера PC-A.

Варіанти пересилання кадру на комутаторах Cisco

Комутатори використовують один з двох способів пересилання для комутації даних між мережевими портами:

- Комутація з проміжним зберіганням (store-and-forward)
- Наскрізна комутація (cut-through)
- На рис. 1 наведені відмінності між цими двома способами.

При комутації з проміжним зберіганням, коли комутатор отримує кадр, він зберігає дані в буфері доти, поки не буде отримано весь кадр. Під час збереження комутатор аналізує кадр, щоб отримати інформацію про його адресата. При цьому комутатор також виконує перевірку на наявність помилок, використовуючи кінцеву частину кадру Ethernet - циклічний надлишковий код (CRC).

CRC використовує математичну формулу, засновану на кількості біт (одиниць) в кадрі, що дозволяє визначити наявність помилок в отриманому кадрі. Після підтвердження цілісності кадру він перенаправляється через відповідний порт до вузла призначення. Якщо ж в кадрі виявлена помилка, комутатор відхилить його. Відхилення кадрів з помилками дозволяє зменшити ширину смуги пропускання, яка споживається пошкодженими даними. Комутація з проміжним зберіганням необхідна для аналізу якості обслуговування (QoS) в конвергировать мережах, в яких потрібно класифікація кадру для призначення пріоритетів трафіку. Наприклад, при передачі мови по IP потоки даних повинні мати більший пріоритет, ніж трафік, який використовується для перегляду веб-сторінок.

На рис. 2 можна відтворити анімацію, яка демонструє комутацію з проміжним зберіганням.

Натисніть тут, щоб дізнатися додаткову інформацію про комутації з проміжним зберіганням і наскрізний комутації.

Наскрізна комутація (Cut-Through)

При використанні наскрізний комутації комутатор обробляє дані в міру їх надходження навіть в тому випадку, якщо передача ще не завершена.

Комутатор додає в буфер тільки ту частину кадру, яка потрібна для читання MAC-адреси призначення, щоб він зміг визначити, на який порт пересилати дані. MAC-адресу призначення вказана в перших 6 байтах кадру після преамбули. Комутатор шукає MAC-адресу призначення в своїй таблиці комутації, визначає порт вихідного інтерфейсу і направляє кадр на вузол призначення через певний порт комутатора. Комутатор не перевіряє кадр на наявність будь-яких помилок.

Розпочніть відтворення анімацію, що демонструє принцип наскрізної комутації.

Існують два варіанти наскрізний комутації.

Комутація з швидкою пересиланням. Комутація з швидкою пересиланням забезпечує найменший рівень затримки. При такій комутації пакет пересилається відразу ж після читання адреси призначення. Оскільки при комутації з швидкою пересиланням переадресація починається до отримання на інших ділянках зображення цілком, можуть виникнути випадки, коли пакети передаються з помилками. Це відбувається рідко, а мережевий адаптер призначення відхиляє пакет з помилками після його отримання. У режимі швидкої пересилання затримка вимірюється з моменту отримання першого біта до передачі першого біта. Комутація з швидкою пересиланням є типовим способом наскрізний комутації.

Комутація з виключенням фрагментів. При комутації з виключенням фрагментів комутатор зберігає перші 64 байта кадру перед його відправкою. Комутацію з виключенням фрагментів можна розглядати як компромісний варіант між комутацією з проміжним зберіганням і комутацією зі швидкою пересиланням. Причина, по якій при комутації з виключенням фрагментів зберігаються тільки перші 64 байта кадру, полягає в тому, що більшість мережевих помилок і колізій відбувається саме в перших 64 бітах. Комутація з виключенням фрагментів дозволяє підвищити ефективність комутації з швидкою пересиланням завдяки виконанню невеликий перевірки помилок у перших 64 бітах кадру, щоб перед пересиланням кадру переконатися у відсутності колізії. Комутація з виключенням фрагментів є компромісом між великою затримкою з високою цілісністю (комутація з проміжним зберіганням) і малою затримкою з меншою цілісністю (комутація з швидкою пересиланням).

Деякі комутатори налаштовані на використання наскрізної комутації для кожного порту до тих пір, поки не буде досягнуто вказане користувачем гранична кількість помилок, після чого автоматично встановлюється комутація з проміжним зберіганням. Після того, як частота повторення помилок знизиться до встановленого граничного значення, порт автоматично переключиться на використання наскрізної комутації.

Буферизація пам'яті на комутаторах

Комутатор Ethernet може використовувати метод буферизації для зберігання кадрів до їх пересилання. Крім того, буферизацию можна використовувати в тому випадку, якщо порт призначення зайнятий через його перевантаження, і комутатор зберігає кадр до тих пір, поки не з'явиться можливість його передачі.

Як показано на малюнку, існують два методи буферизації пам'яті: буферизація на базі портів і буферизація спільно використовуваної пам'яті.

Буферизація пам'яті на базі портів

В процесі буферизації пам'яті на базі портів кадри зберігаються в чергах, пов'язаних з певними вхідними та вихідними портами. Кадр пересилається на вихідний порт тільки в тому випадку, якщо всі кадри, що знаходяться в черзі перед ним, були успішно відправлені. Один кадр може стати причиною затримки передачі всіх кадрів в пам'яті через зайнятість порту призначення. Така затримка виникає і в тому випадку, якщо інші кадри можна передати на відкриті порти призначення.

Буферизація спільно використовуваної пам'яті

При буферизації спільно використовуваної пам'яті всі кадри поміщаються в буфер, який є загальним для всіх портів комутатора. Обсяг буферної пам'яті, який потрібно кожному порту, виділяється динамічно. Кадри в буфері динамічно зв'язуються з портом призначення. Це дозволяє отримувати пакет на один порт і потім пересилати його на інший порт без переміщення в іншу чергу.

Комутатор зберігає зіставлення кадру зі зв'язаними портами, на які необхідно переслати пакет. Збережене зіставлення видаляється після успішної передачі кадру. Кількість кадрів, збережених в буфері, обмежена розміром всього буфера пам'яті і не обмежується буфером одного порту. Це дозволяє передавати кадри більшого обсягу, при цьому число скинутих кадрів буде менше. Це особливо важливо для асиметричної комутації. Асиметрична комутація дозволяє використовувати різні швидкості передачі даних на різних портах. Це забезпечує виділення більшої смуги пропускання деяких портів, наприклад, порту, підключеному до сервера.

Щоб отримати додаткову інформацію про комутатори локальної мережі (LAN), зокрема про фіксовані і модульних комутаторах, про комутації рівня 3 і технології Cisco Express Forwarding (CEF), див. Додаток до глави.

Налаштування дуплексного режиму і швидкості

До двох базових параметрах комутатора відносяться пропускна здатність і двобічний режим, які задаються для кожного окремого порту комутатора. Важливо, щоб настройки дуплексного режиму і пропускної спроможності порту комутатора і підключених пристроїв, таких як комп'ютер або інший комутатор, збігалися.

Для обміну даними в мережах Ethernet використовуються два види установок дуплексного режиму: напівдуплексний і повнодуплексний.

Повнодуплексний режим: одночасна відправка і отримання даних в обидві сторони.

Напівдуплексний режим: відправка даних тільки однією стороною.

Автовизначення - це додаткова функція, які потребують більшість комутаторів і мережевих плат Ethernet. Автовизначення дозволяє двом пристроям автоматично обмінюватися інформацією про швидкість і можливості дуплексного режиму. Комутатор і підключений пристрій вибирають режим з максимальною продуктивністю. Якщо обидва пристрої підтримують повнодуплексний режим, для роботи вибирається цей режим разом з максимальною пропускною здатністю, загальною для двох пристроїв.

Наприклад, мережева плата Ethernet комп'ютера PC-A, показана на рис. 1, може працювати в повнодуплексному або напівдуплексному режимі на швидкості 10 або 100 Мбіт / с. Комп'ютер PC-A з'єднаний через порт 1 з

комутатором S1, який може працювати в повнодуплексному або напівдуплексному режимі на швидкості 10, 100 або 1 000 Мбіт / с (1 Гбіт / с). Якщо в обох пристроях є автовизначення, то буде обрано повнодуплексний режим і швидкість 100 Мбіт / с.

Примітка. У більшості комутаторів і мережевих плат Ethernet компанії Cisco використовується автовизначення швидкості і налаштувань дуплексного режиму. Порти Gigabit Ethernet працюють тільки в повнодуплексному режимі.

Розбіжність дуплексних режимів

Одна з найпоширеніших проблем з продуктивністю каналів Ethernet на швидкості 10/100 Мбіт / с виникає тоді, коли один порт працює в напівдуплексному режимі, а інший порт - в повнодуплексному, як показано на рис. 2. Це відбувається при скиданні одного або обох портів каналу, в результаті чого автоопределение не призводить до однакової конфігурації обох пристроїв зв'язку. Це також може статися тоді, коли користувачі змінюють конфігурацію на одній стороні каналу і забувають про іншу. Автоопределение має бути включено або відключено на обох сторонах каналу.

Функція Auto-MDIX

рім правильного налаштування дуплексного режиму необхідно визначити відповідний тип кабелю для кожного порту. Раніше для з'єднань між певними пристроями (типу «комутатор-комутатор», «комутатор-маршрутизатор», «комутатор-вузол» і «маршрутизатор-головне пристрій») було потрібно використання кабелів особливого типу (перехресних або прямих). Більшість сучасних комутуючих пристроїв підтримують команду конфігурації інтерфейсу mdix auto, яка доступна через CLI і дозволяє використовувати автоматичну функцію Auto-MDIX (інтерфейс, що залежить від середовища передачі з перехресним з'єднанням).

Якщо функція Auto-MDIX включена, комутатор визначає необхідний тип кабелю, підключеного до порту, і налаштовує інтерфейс відповідним чином. Таким чином, для підключення до мідних портів 10/100/1000 Мбіт / с на комутаторі можна використовувати або перехресний, або прямий кабель незалежно від типу пристрою на іншому кінці з'єднання.

Пристрій призначення в тій же мережі

Пристрою в локальній мережі Ethernet присвоюються два основних адреси.

Фізична адреса (MAC-адресу): використовується для обміну даними між мережевими платами Ethernet пристроїв, що знаходяться в одній мережі.

Логічна адреса (IP-адреса): використовується для відправки пакетів від джерела до призначення.

IP-адреси використовуються для визначення адрес джерела і призначення. IP-адреса призначення може перебувати в тій же IP-мережі, що і джерело, або у віддаленій мережі.

Примітка. У більшості додатків використовується система доменних імен (DNS), що дозволяє визначити IP-адресу при вказівці імені домена, наприклад, www.cisco.com. DNS розглядається в главі далі.

Адреси рівня 2 або фізичні адреси, як і MAC-адреси в мережі Ethernet, мають інше призначення. Вони використовуються для доставки кадру, що передається по каналу в інкапсульованих IP-пакеті, від однієї мережевої плати

до іншої в тій же мережі. Якщо IP-адреса призначення знаходиться в тій же мережі, то MAC-адресою призначення є адреса пристрою призначення.

На малюнку показані MAC-адреси Ethernet і IP-адреса комп'ютера PC-A, який відправляє IP-пакет на файловий сервер в тій же мережі.

Кадр Ethernet рівня 2 містить наступне:

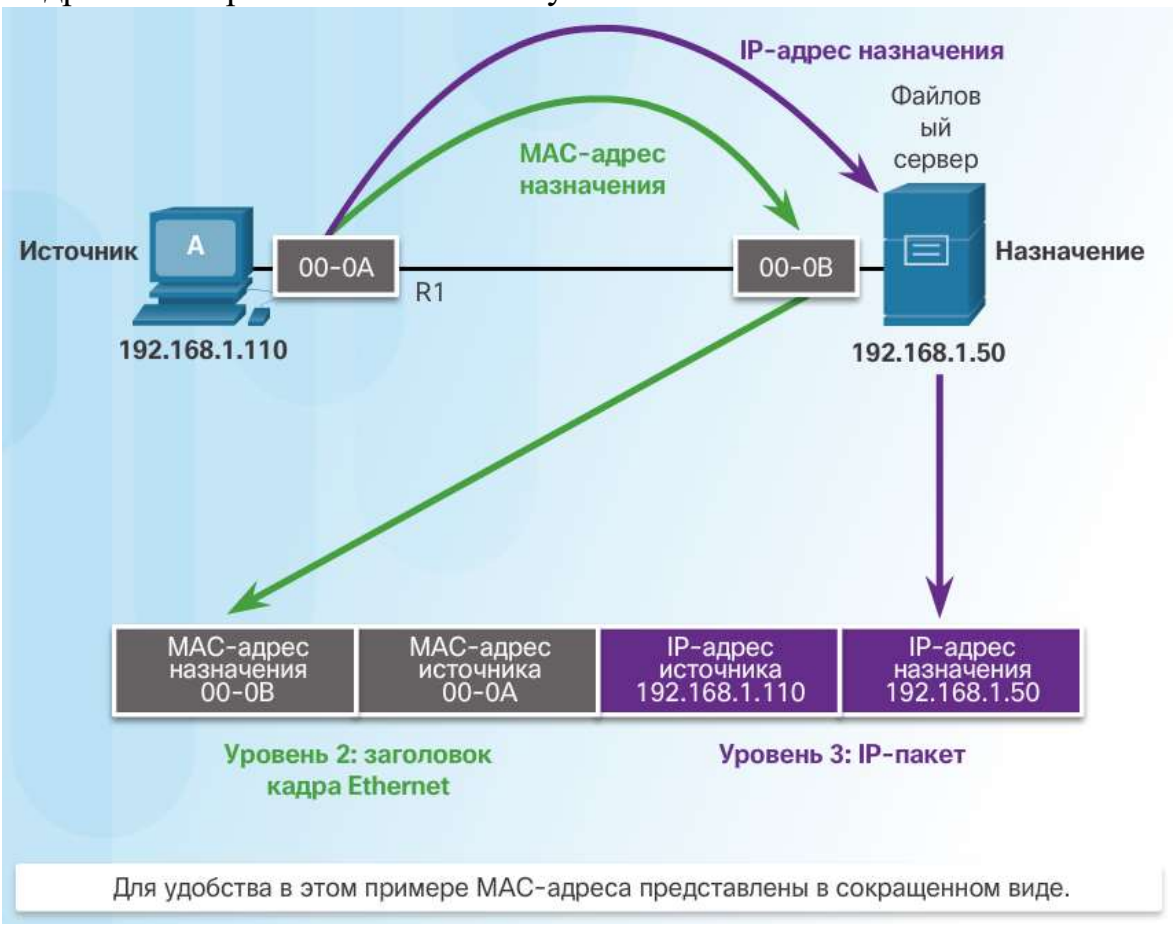


Рис. 1.5 Обмін даними в локальній мережі

MAC-адресу призначення: це MAC-адресу мережевої плати Ethernet файлового сервера.

MAC-адресу джерела: це MAC-адресу мережевої плати Ethernet комп'ютера PC-A.

IP-пакет рівня 3 містить наступне:

- IP-адреса джерела: це IP-адреса пристрою джерела, т. Е. Комп'ютера PC-A.
- IP-адреса призначення: це IP-адреса пристрою призначення, т. Е. Файлового сервера.

Якщо IP-адреса призначення знаходиться у віддаленій мережі, то MAC-адресою призначення є адреса шлюзу вузла за замовчуванням, наприклад, мережевий плати маршрутизатора, як показано на малюнку. Якщо використовувати аналогію з роботою пошти, то це схоже на ситуацію, коли хто-небудь передає лист в місцеве поштове відділення. Все, що необхідно зробіти - це принести лист на пошту, а далі відповідальність за відправку листа адресату несе вже поштове відділення.

На малюнку показані MAC-адреси Ethernet і IPv4-адрес комп'ютера PC-A, який відправляє IP-пакет на веб-сервер у віддаленій мережі. Маршрутизатор

перевіряють IPv4-адрес призначення для визначення найкращого способу пересилання IPv4-пакета. Це аналогічно відправці пошти на адресу отримувача.

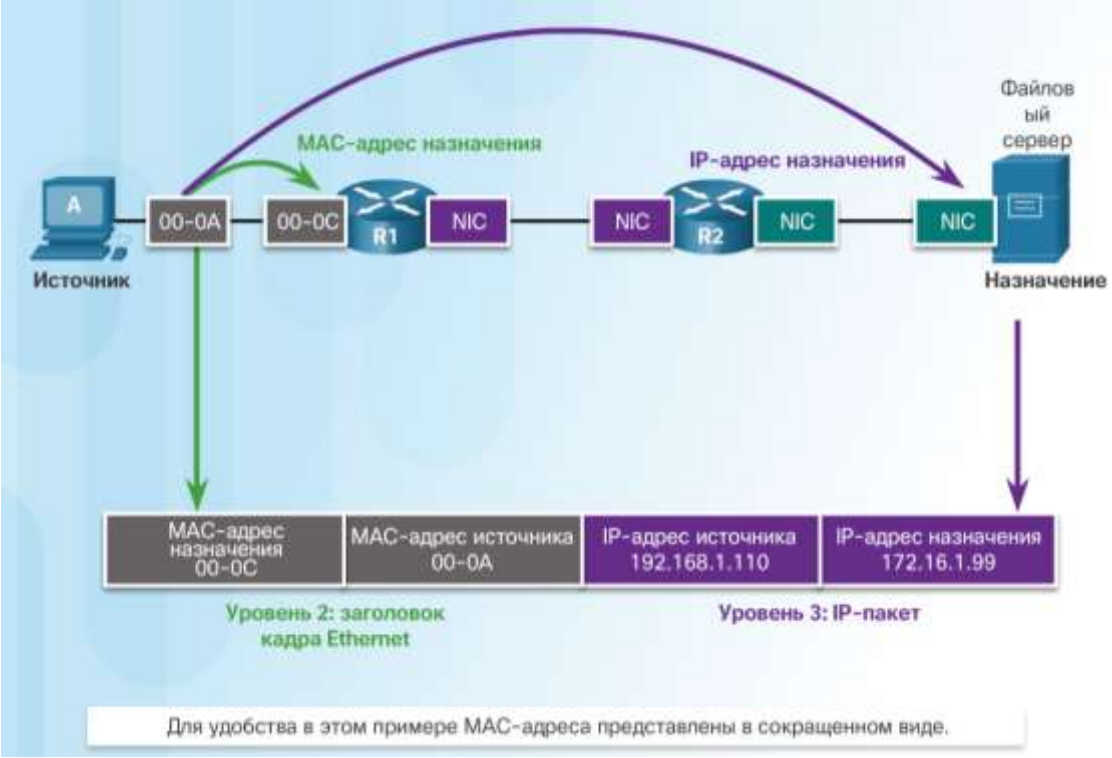


Рис. 1.6 Обмін даними з віддаленою мережею

При отриманні маршрутизатором кадру Ethernet відбувається деінкапсуляція інформації рівня 2. На основі IP-адреси призначення маршрутизатор визначає наступне транзитне пристрій і інкапсулює IP-пакет в новий кадр для передачі в вихідний інтерфейс. У кожному каналі на своєму шляху IP-пакет инкапсулируется в кадрі в залежності від використовуваної технології каналу передачі даних, яка пов'язана з цим каналом, наприклад, технології Ethernet. Якщо таке транзитне пристрій є призначенням, то MAC-адресою призначення буде адресу мережевої плати Ethernet цього пристрою.

Яким чином IPv4-адреси IPv4-пакетів в потоці даних асоціюються з MAC-адресами в кожному каналі на шляху до вузла призначення? Для цього використовується протокол дозволу адрес (ARP).

Протокол дозволу адрес (ARP): введення

Слід пам'ятати, що у кожного пристрою з IP-адресою в мережі Ethernet є також MAC-адреса. Коли пристрій відправляє кадр Ethernet, він містить обидва цих адреси:

MAC-адресу призначення: це MAC-адресу мережевої плати Ethernet, який є MAC-адресою пристрою призначення або маршрутизатора.

MAC-адресу джерела: це MAC-адресу мережевої плати Ethernet відправника.

Для визначення MAC-адреси призначення пристрій використовує протокол дозволу адрес (ARP). Протокол ARP виконує дві основні функції.

- Зіставлення IPv4-адрес і MAC-адрес
- Збереження таблиці зіставлень

функції ARP

Зіставлення IPv4-адрес і MAC-адрес

Коли пакет відправляється на канальний рівень для інкапсуляції в кадрі Ethernet, пристрій звертається до таблиці у своїй пам'яті, щоб знайти MAC-адресу, який зіставлений з IPv4-адресою. Ця таблиця називається таблицею ARP або кешем ARP. Таблиця ARP зберігається в оперативній пам'яті пристрою.

Передавальний пристрій шукає в своїй таблиці ARP IPv4-адрес призначення і відповідний MAC-адресу.

Якщо IPv4-адрес призначення пакета знаходиться в тій же мережі, що і IPv4-адрес джерела, пристрій шукає в таблиці ARP IPv4-адрес призначення.

Якщо IPv4-адрес призначення пакета знаходиться не в тій же мережі, що IPv4-адрес джерела, пристрій шукає в таблиці ARP IPv4-адрес шлюзу.

В обох випадках необхідно знайти IPv4-адрес і відповідний MAC-адресу пристрою.

Кожен запис або рядок в таблиці ARP пов'язує IPv4-адрес з MAC-адресою. Відношення між двома значеннями називається зіставленням. Це означає, що IPv4-адрес можна знайти в таблиці і з його допомогою визначити відповідний MAC-адресу. Таблиця ARP тимчасово зберігає (кеширует) зіставлення пристроїв в локальній мережі (LAN).

Якщо пристрій знайде IPv4-адрес, то в якості MAC-адреси в кадрі використовується відповідний MAC-адресу. Якщо запис не знайдено, пристрій відправляє ARP-запит.

ARP-запит відправляється в тому випадку, коли пристрій може потребувати MAC-адресу, пов'язану з IPv4-адресою, але в його таблиці ARP немає даних про IPv4-адресу.

Повідомлення ARP-запиту инкапсулируются безпосередньо в кадрі Ethernet. Тема IPv4 відсутня. У повідомленні ARP-запиту міститься наступне:

IPv4-адрес призначення: це IPv4-адрес, для якого потрібно визначити відповідний MAC-адресу.

MAC-адресу призначення: це невідомий MAC-адресу, який в повідомленні запиту ARP відсутня.

ARP-запит инкапсулируется в кадрі Ethernet з наступною інформацією в заголовку:

MAC-адресу призначення: широкомовна адреса, що вимагає прийняття і обробки ARP-запиту усіма мережевими платами Ethernet в локальній мережі (LAN).

MAC-адресу джерела: це відправник MAC-адреси в ARP-запиті.

Тип: в повідомленні ARP-запиту є поле «Тип» зі значенням 0x806. Воно інформує приймаючу мережеву плату про те, що для частини кадру, виділеної для даних, необхідно використовувати процес ARP.

Оскільки ARP-запити є широкомовної розсилкою, вони розсилаються через всі порти комутатора, крім приймаючої порту. Всі мережеві плати Ethernet в локальній мережі (LAN) обробляють широкомовні розсилання. Кожен пристрій обробляє ARP-запит на предмет збігу цільового IPv4-адреси з власною адресою. Маршрутизатор не пересилає широкомовні розсилання іншим інтерфейсів.

Тільки у одного пристрою в локальній мережі (LAN) буде IPv4-адрес, що співпадає в цільовим IPv4-адресою в ARP-запиті. Відповідь від інших пристроїв не надходить.

Натисніть кнопку «Відтворення», щоб переглянути відеоролик про ARP-запиті IPv4-адреси призначення, який знаходиться в локальній мережі.

Тільки пристрій з IPv4-адресою, пов'язаних з цільовим IPv4-адресою в ARP-запиті, повертає ARP-відповідь. У повідомленні ARP-відповіді міститься наступне:

IPv4-адрес відправника: це IPv4-адрес відправника, т. Е. Пристрої, чий MAC-адресу був запитаний.

MAC-адресу відправника: це MAC-адресу відправника, т. Е. MAC-адресу, який був запитаний відправником в ARP-запиті.

ARP-відповідь інкапсулюються в кадрі Ethernet з наступною інформацією в заголовку:

MAC-адресу призначення: це MAC-адресу відправника ARP-запиту.

MAC-адресу джерела: це відправник MAC-адреси в ARP-відповіді.

Тип: в повідомленні ARP-запиту є поле «Тип» зі значенням 0x806. Воно інформує приймаючу мережеву плату про те, що для частини кадру, виділеної для даних, необхідно використовувати процес ARP.

Одно-адресний ARP-відповідь отримає тільки той пристрій, що відправило ARP-запит. Після отримання ARP-відповіді виріб додасть IPv4-адрес і відповідний MAC-адресу в свою таблицю ARP. Тепер пакети для цього IPv4-адреси можна інкапсулювати в кадрах, використовуючи відповідний йому MAC-адресу.

Натисніть кнопку «Відтворення», щоб переглянути відеоролик про ARP-відповіді.

Натисніть тут, щоб завантажити слайди з відеоролика.

Якщо на ARP-запит не відповідає ні один пристрій, пакет відкидається, оскільки сформувати кадр неможливо.

Записи в таблиці ARP отримують мітку часу. Якщо до моменту закінчення мітки часу пристрій не отримає кадр від будь-якого пристрою, запис для цього пристрою буде видалена з таблиці ARP.

Крім того, в таблицю ARP можна додавати статичні записи зіставлення, але це робиться не часто. Термін дії статичних записів в таблиці ARP чи не закінчується з часом, тому їх необхідно видаляти вручну.

Примітка. Для IPv6 використовується протокол, аналогічний протоколу дозволу адрес (ARP) для IPv4, який називається «протокол виявлення сусідів» ICMPv6. Для IPv6 використовуються повідомлення опитування і оголошення сусідів, які схожі за своїм призначенням з ARP-запитами і відповідями в IPv4.

Якщо IPv4-адрес призначення знаходиться не в тій же мережі, що IPv4-адрес джерела, влаштуванню джерела необхідно відправити кадр в свій шлюз за замовчуванням. Це інтерфейс локального маршрутизатора Якщо пристрій джерела є пакет в IPv4-адресою в іншій мережі, воно инкапсулирует цей пакет в кадрі, використовуючи MAC-адресу призначення маршрутизатора.

IPv4-адрес шлюзу зберігається в конфігурації IPv4 вузлів. Коли вузол створює пакет для адресата, він порівнює IPv4-адрес призначення і свій власний IPv4-адрес, щоб визначити, чи знаходяться ці два IPv4-адреси в одній і

тій же мережі рівня 3. Якщо вузол призначення знаходиться в іншій мережі, джерело шукає в своєю таблиці ARP запис з IPv4-адресою шлюзу. Якщо запис відсутній, то для визначення MAC-адреси шлюзу за замовчуванням використовується процес ARP.

Видалення записів з таблиці ARP

У кожному пристрої є таймер кешу ARP, який видаляє записи з таблиці ARP, які не використовуються протягом зазначеного періоду часу. Цей період може бути різним у залежності від операційної системи пристрою. Наприклад, деякі операційні системи Windows зберігають записи кеша ARP протягом 2 хвилин, як показано на малюнку.

Крім того, можна використовувати деякі команди, щоб вручну видалити всі або деякі записи з таблиці ARP. Після видалення запису процес відправки ARP-запиту і отримання ARP-відповіді необхідно задіяти повторно, щоб зареєструвати зіставлення в таблиці ARP.

таблиці ARP

На маршрутизаторі Cisco для відображення таблиці ARP використовується команда show ip arp, як показано на рис. 1.

На комп'ютерах під управлінням Windows 7 для відображення таблиці ARP використовується команда arp -a, як показано на рис. 2.

Широкомовні розсилання ARP

Оскільки ARP-запит є кадром широкомовної розсилки, його отримують і обробляють всі пристрої в локальній мережі. У стандартній корпоративної мережі такі широкомовні розсилання, швидше за все, не зроблять істотного впливу на продуктивність мережі. Але якщо в мережі багато пристроїв і всі вони одночасно спробують отримати доступ до мережевих служб, це може на короткий період часу негативно вплинути на роботу мережі, як показано на малюнку. Після того як пристрої розішлють початкові запити широкомовної розсилки ARP і отримають необхідні MAC-адреси, будь-який вплив на мережу буде зведено до мінімуму.

Спуфінга за допомогою протоколу дозволу адрес (ARP)

У деяких випадках використання протоколу дозволу адрес (ARP) може представляти певний ризик для безпеки. Такі атаки отримали назву ARP-спуфинг або «отруєння» ARP-кешу. В ході таких атак зловмисник відправляє відповідь на ARP-запит IPv4-адреси з адресою іншого пристрою, наприклад, шлюзу, як показано на малюнку. Зловмисник відправляє ARP-відповідь зі своїм MAC-адресою. Одержувач ARP-відповіді додасть фальсифікований MAC-адресу в свою таблицю ARP, що дозволить зловмисникові отримувати відправляються пакети.

Комутатори корпоративного рівня оснащені функцією захисту від такого роду атак, яка називається Dynamic ARP Inspection (DAI). Функція DAI не розглядається в цьому курсі.

1.1. Протоколи мережевого рівня. Адресація в мережі.

Мережеві додатки і сервіси на одному крайовому пристрої можуть взаємодіяти з додатками і сервісами, запущеними на іншому крайовому пристрої. Яким чином забезпечується максимальна ефективність передачі цих даних по мережі?

Протоколи мережевого рівня моделі OSI визначають адресацію і процеси, які дозволяють упаковувати і передавати дані транспортного рівня. Інкапсуляція мережевого рівня забезпечує проходження даних по мережі до адресата (або іншої мережі) з мінімальним навантаженням.

В цьому розділі основна увага приділена ролі мережевого рівня. У ній аналізується процес поділу мереж на групи вузлів для управління потоком пакетів даних в межах однієї мережі. Крім того, в ній описуються способи спрощення обміну даними між мережами. Такий міжмережевий обмін даними називається маршрутизацією.

Мережевий рівень

Мережевий рівень, або третій рівень моделі OSI, надає послуги, що дозволяють кінцевим пристроям обмінюватися даними по мережі. Для виконання такої наскрізної передачі на мережевому рівні використовуються чотири основні процеси.

Адресація кінцевих пристроїв. Кінцевим пристроям необхідно призначити унікальну IP-адресу для можливості їх ідентифікації в мережі.

Інкапсуляція. Мережевий рівень отримує одиницю даних протоколу (PDU) від транспортного рівня. Під час виконання процесу, який називається инкапсуляцией, мережевий рівень додає інформацію заголовка IP, наприклад IP-адреса вузла джерела (відправляє) і вузла призначення (одержує).

Маршрутизація. Мережевий рівень надає сервіси, за допомогою яких пакети направляються до вузла призначення в іншій мережі Для переміщення до інших мереж пакет повинен бути оброблений маршрутизатором. Роль маршрутизатора полягає в тому, щоб вибрати шляхи для пакетів і направити їх до вузла призначення. Такий процес називається маршрутизацією. До того як досягти вузла призначення, пакет може пройти через кілька проміжних пристроїв. Кожен маршрут на шляху пакета до вузла призначення називається переходом.

Деінкапсуляція. Після прибуття пакета на мережевий рівень вузла призначення цей вузол перевіряє IP-заголовок пакета. Якщо IP-адреса призначення в заголовку збігається з його власним IP-адресою, заголовок IP видалена з пакета. Після деінкапсуляції пакета, виконуваної мережевим вузлом, отримана одиниця даних протоколу (PDU) рівня 4 пересилається відповідній службі на транспортному рівні.

На відміну від транспортного рівня (рівень 4 моделі OSI), який управляє передачею даних між процесами, запущеними на кожному вузлі, мережевий рівень вказують структуру пакета і тип обробки, які використовуються для переміщення даних від одного вузла до іншого. Функціонування без урахування даних, переданих в кожному пакеті, дозволяє мережному рівню передавати пакети для кількох типів комунікації між декількома вузлами.

Протоколи мережевого рівня

Існує кілька протоколів мережевого рівня. Однак, як показано на малюнку, зазвичай реалізуються тільки 2 протоколу мережевого рівня:

- Інтернет-протокол версії 4 (IPv4)
- протокол IPv6

Інкапсуляція протоколу IP

Протокол IP инкапсулирует сегмент транспортного рівня або інші дані шляхом додавання заголовка IP. Цей заголовок використовується для доставки пакета на вузол призначення. Тема IP залишається незмінним з моменту відправки пакета з вузла джерела до його прибуття на мережевий рівень вузла призначення.

Рис. 1.1.1 процес створення одиниці даних протоколу (PDU) транспортного рівня

Процес інкапсуляції даних від рівня до рівня забезпечує можливість розробляти і масштабувати сервіси на різних рівнях без впливу на інші рівні. Це означає, що сегменти транспортного рівня можна легко упакувати за допомогою протоколів IPv4 або IPv6 або будь-якого нового протоколу, який може бути створений в майбутньому.

Маршрутизатор можуть використовувати ці протоколи мережевого рівня, щоб працювати в мережі одночасно. Під час маршрутизації, яку ведуть такі проміжними пристроями, враховується вміст заголовка тільки того пакету, який інкапсулює сегмент. У всіх інших випадках частина даних пакета (т. Е. Інкапсульована одиниця даних протоколу (PDU) транспортного рівня) під час виконання процесів на мережевому рівні залишається незмінною

Протокол IP був розроблений як протокол з низьким навантаженням. Він забезпечує лише ті функції, які необхідні для доставки пакета від вузла джерела до вузла призначення по взаємозалежної системі мереж. Цей протокол не призначений для моніторингу та управління потоком пакетів. Ці функції, при необхідності, виконуються іншими протоколами на інших рівнях, в першу чергу - протоколом TCP на рівні 4.

Рис. 1.1.2 опис основних характеристик протоколу IP

IP є протоколом без встановлення з'єднання, а це означає, що перед відправкою даних виділене наскрізне з'єднання не встановлюється. По своїй суті обмін даними без встановлення з'єднання аналогічний відправлення листа без попереднього повідомлення одержувача.

При передачі даних без встановлення з'єднання використовується аналогічний принцип. Протокол IP не використовує з'єднання і, отже, йому не потрібно первинного обміну контрольної інформацією для встановлення наскрізного з'єднання до початку пересилання пакетів. IP також не потребує додаткових полях в заголовку для підтримки встановленого з'єднання. Цей процес значно знижує навантаження IP. Проте без попередньо встановленого наскрізного підключення відправникам невідомо, чи є пристрої-адресати і чи здатні вони функціонувати в момент відсилання пакетів, а також отримає пакет вузол призначення і чи зможуть пристрої-адресати отримати доступ до пакету і прочитати його.

Протокол IP. негарантована доставка

На малюнку показана особливість протоколу IP, яка розкриває суть його недостовірної або негарантованої доставки. Протокол IP не гарантує отримання всіх доставляються пакетів.

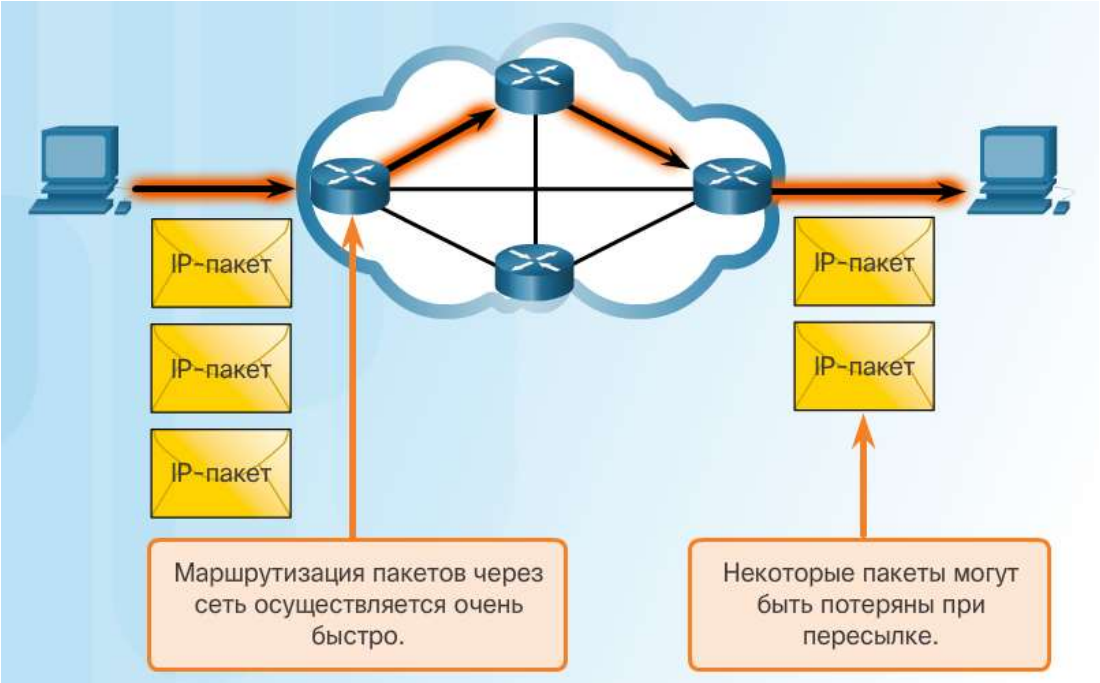


Рис. 1.1.3 Схема передачі протоколу IP

«Ненадійний» протокол - той, який не здатний контролювати недоставлені або пошкоджені пакети і відновлювати їх. Це пов'язано з тим, що, хоча відправляються пакети IP і містять відомості про місце доставки, в них відсутня інформація, яку можна обробити, щоб повідомити відправнику про успішно виконану доставці. Пакети можуть прибути на вузол призначення пошкодженими або з порушенням порядку або не прибути зовсім. У разі виникнення таких помилок інформація, яка міститься в заголовку IP, не дозволяє виконати повторну пересилку пакетів.

Якщо відсутність пакетів або недотримання черговості створює проблеми для додатків, що використовують дані, сервіси верхнього рівня, наприклад TCP, повинні усунути ці проблеми. Це забезпечує високу ефективність роботи протоколу IP. У пакеті протоколів TCP / IP забезпечення надійності - завдання транспортного рівня.

Протокол IP діє незалежно від середовища, яка служить для передачі даних на нижніх рівнях стека протоколів. Як показано на малюнку, будь-який окремий пакет IP може передаватися по кабелю (за допомогою електричних імпульсів, наприклад оптичних сигналів по оптоволоконному кабелю) або у вигляді радіосигналів в бездротових мережах.

Канальний рівень OSI повинен прийняти пакет IP і підготувати його для передачі в комунікаційному середовищі. Це означає, що пересилання пакетів IP не обмежується будь-якої конкретної комунікаційним середовищем.

Проте існує одна важлива характеристика середовища передачі, яка враховується на мережевому рівні: максимальний розмір одиниці даних протоколу (PDU), який здатна переслати щосереди. Ця характеристика називається максимальним розміром переданого блоку даних (MTU). Частина обміну контрольними даними між канальним рівнем і мережевим рівнем - це встановлення максимального розміру пакета. Канальний рівень передає значення MTU на мережевий рівень. Потім мережевий рівень визначає розмір пакетів.

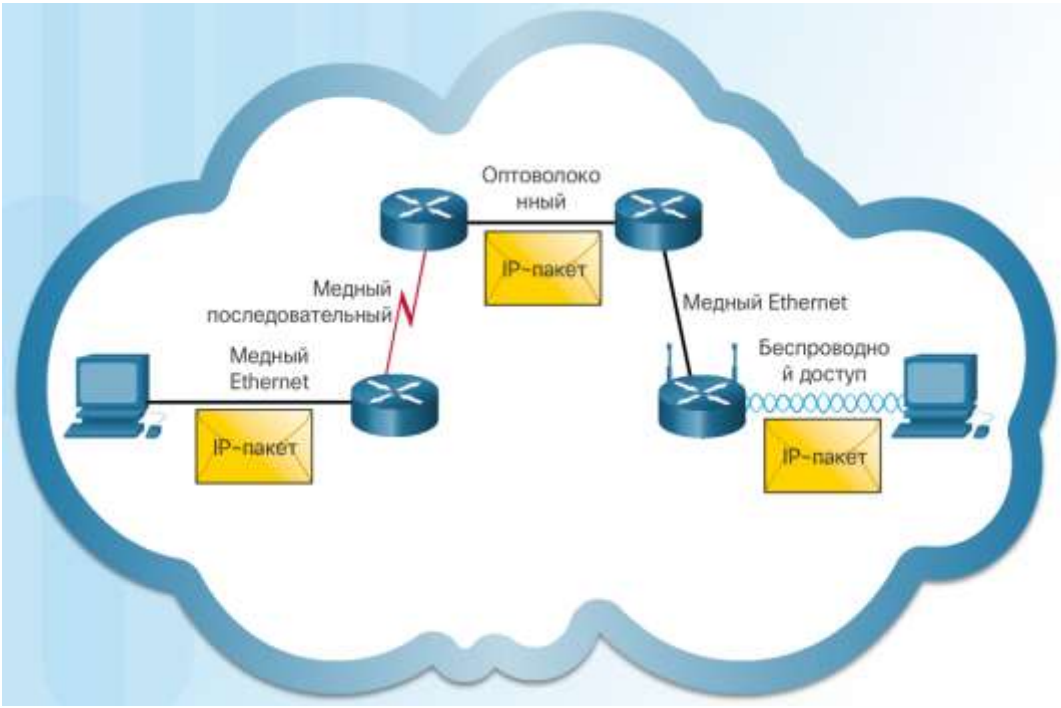


Рис. 1.1.4 IP протокол передається у любому середвищі

У деяких випадках проміжний пристрій (як правило, це маршрутизатор) буде поділений пакет під час його пересилання з одного середовища передачі даних в середу з меншим максимальним розміром переданого блоку даних (MTU). Цей процес називається поділом пакета або фрагментацією.

Заголовок пакета IPv4 складається з декількох полів, які включають важливу інформацію про пакет. Ці поля містять двійкові числа, які аналізуються процесом рівня 3. Двійкові значення кожного поля визначають різні параметри IP-пакета. Схеми заголовків протоколу, зчитувальні зліва направо і зверху вниз, надають наочну інформацію про полях протоколів. Схема заголовків IP-протоколу на малюнку визначає поля IPv4-пакета.

Серед найбільш важливих полів в заголовку IPv4 можна виділити наступні.

Версія. Включає в себе 4-бітове двійкове значення, що визначає версію IP-пакета. Для пакетів IPv4 в цьому полі завжди вказано значення 0100.

Диференційовані сервіси (DS). Поле, яке раніше називалося «Тип сервісу» (ToS); DS - це 8-бітове поле, що використовується для визначення пріоритету кожного пакета. 6 найбільш важливих бітів поля диференційованих послуг (DSCP) і останні 2 біти - це біти явного повідомлення про затори (ECN).

Час існування (Time-to-Live, TTL). Містить 8-бітове двійкове значення, яке використовується для обмеження часу існування пакету. Відправник пакета встановлює початкове значення часу існування (TTL), яке зменшується на одиницю кожного разу при обробці пакета маршрутизатором. Якщо значення в полі TTL зменшується до нуля, маршрутизатор відкидає пакет і відправляє на IP-адреса джерела повідомлення про перевищення часу протоколу ICMP (управління повідомленнями в мережі).

Поле Протокол використовується для визначення протоколу наступного рівня. Це 8-бітове двійкове значення, яке вказує тип корисного навантаження даних, які переносить пакет, що дозволяє мережному рівню пересилати дані на

відповідний протокол більш високого рівня. Зазвичай використовуються значення ICMP (1), TCP (6) і UDP (17).

IPv4-адрес джерела містить 32-бітове двійкове значення, яке представляє IPv4-адрес джерела пакету. IPv4-адрес джерела - це завжди індивідуальний адресу.

IPv4-адрес призначення містить 32-бітове двійкове значення, яке представляє IPv4-адрес призначення пакета. IPv4-адрес призначення - одноадресная розсилка, багатоадресна розсилка, або широкомовна адреса.

Два найбільш часто використовуваних поля - це IP-адреса джерела та IP-адреса призначення. Ці поля визначають, звідки надійшов пакет і куди він прямує. Зазвичай в процесі передачі від вузла джерела до вузла призначення ці адреси не змінюються.

Поля «Розмір заголовка» (Internet Header Length, IHL), «Загальний розмір» і «Контрольна сума заголовка» використовуються для визначення і перевірки пакета.

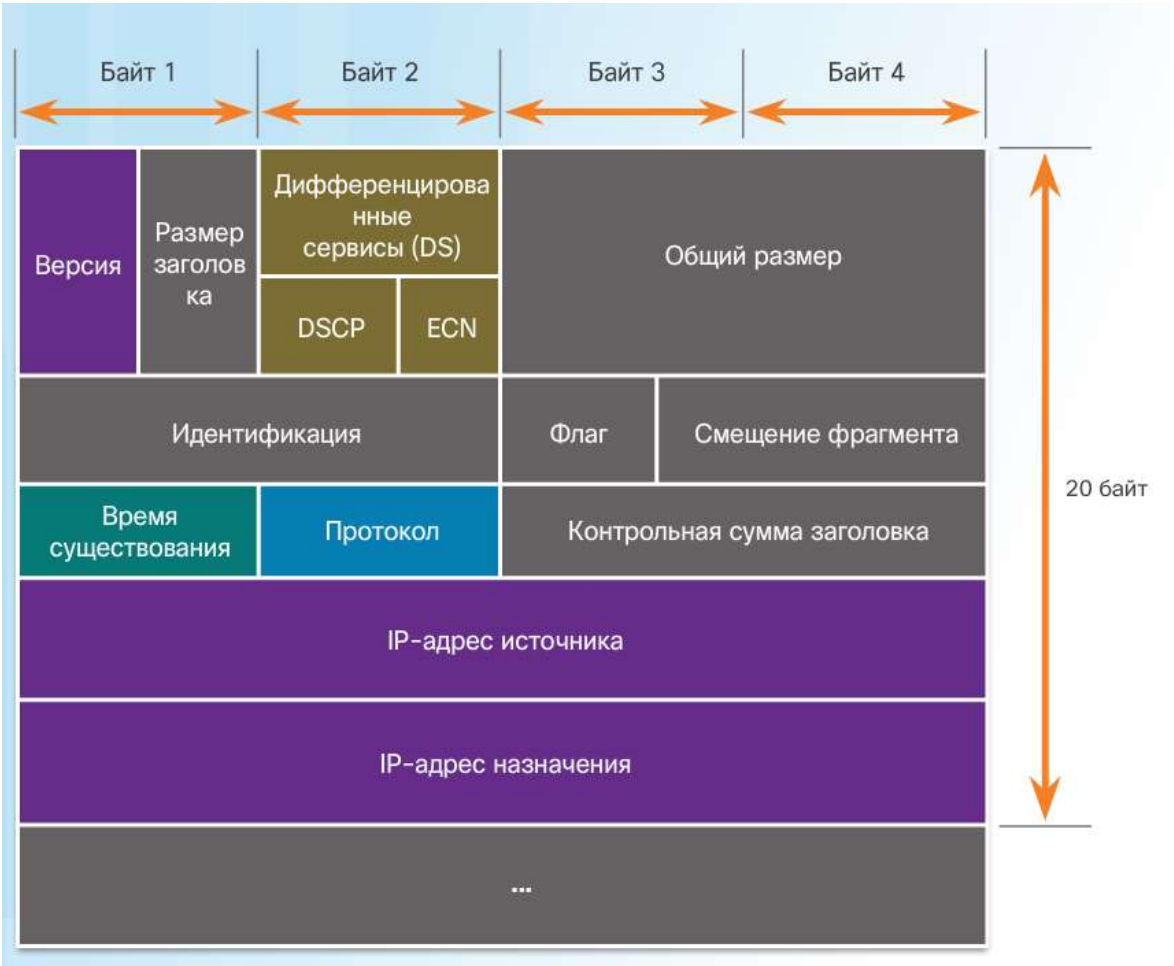


Рис. 1.1.5 Заголовок протоколу IPv4

Решта поля використовуються для переупорядочивания фрагментированного пакета. У зв'язку з цим IPv4-пакет використовує поля «Ідентифікація», «Прапори» і «Зсув фрагмента» для відстеження фрагментів. Маршрутизатора може знадобитися виконати фрагментацію пакету при його пересиланні з одного середовища передачі даних в інше середовище з меншим максимальним розміром переданого блоку даних (MTU).

Поля «Параметри» і «Заповнювач» використовуються рідко і в цьому розділі не розглядаються.

Протягом багатьох років протокол IPv4 періодично оновлювався для вирішення нових завдань. Проте навіть в результаті змін IPv4 і раніше має три основних недоліки.

Брак IP-адрес. IPv4 може запропонувати лише обмежена кількість унікальних публічних IP-адрес. Незважаючи на те що існує приблизно 4 мільярди IPv4-адрес, збільшене число нових пристроїв, в яких використовується протокол IP, а також потенційне зростання менш розвинених регіонів привели до необхідності додаткового збільшення кількості адрес.

Розширення таблиці інтернет-маршрутизації. Таблиця маршрутизації використовується маршрутизаторами для визначення оптимальних шляхів пересилання даних. У міру збільшення кількості серверів (вузлів), підключених до Інтернету, також зростає число мережевих маршрутів. Ці маршрути IPv4 споживають значну кількість пам'яті і ресурсів процесорів інтернет-маршрутизаторів.

Брак наскрізних з'єднань. Перетворення мережевих адрес (NAT) являє собою технологію, яка зазвичай застосовується в мережах IPv4. NAT дозволяє різним пристроям спільно використовувати один публічний IPv4-адрес. При цьому, оскільки публічний IPv4-адрес використовується спільно, IPv4-адрес вузла внутрішньої мережі прихований. Це може представляти проблему при використанні технологій, для яких необхідні наскрізні з'єднання.

На початку 90-х років фахівці інженерної групи з розвитку Інтернету (IETF) підняли питання про недоліки протоколу IPv4 і почали пошуки альтернативних рішень. Результатом пошуків стала розробка протоколу IP версії 6 (IPv6). IPv6 допомагає подолати обмеження протоколу IPv4 і значно розширює доступні можливості, пропонуючи функції, які оптимально відповідають поточним і прогнозованим мережевим вимогам.

До поліпшень, які пропонує протокол IPv6, відносяться наступні.

Розширене адресний простір. IPv6-адреси використовують 128-бітну ієрархічну адресацію, на відміну від протоколу IPv4, який використовує 32 біта.

Покращена обробка пакетів. Структура заголовка IPv6 була спрощена завдяки зменшенню кількості полів.

Відсутність необхідності в використанні NAT. Завдяки великій кількості публічних IPv6-адрес немає необхідності в перетворенні мережевих адрес (NAT) між приватними і публічними адресами IPv4. Це дозволяє усунути деякі проблеми, пов'язані з перетворенням мережевих адрес, які виникають при роботі додатків, що вимагають наскрізного з'єднання.

32-бітове адресний простір IPv4 передбачає приблизно 4 294 967 296 унікальних адрес. Адресний простір протоколу IPv6 підтримує 340 282 366 920 938 463 463 374 607 431 768 211 456 або 340 ундецілліонов адрес, що приблизно дорівнює кількості піщинок на Землі.

Рис. 1.1.6 Візуальне порівняння адресного простору протоколів IPv4 та IPv6

Одним з основних конструктивних поліпшень протоколу IPv6 в порівнянні з IPv4 є спрощений заголовок IPv6.

Наприклад, показаний на рис. 1 заголовок IPv4 складається з 20 октетів (до 60 байт, якщо використовується поле «Параметри») і 12 основних полів заголовка, не враховуючи поля «Параметри» і «Заповнювач». Як видно на малюнку, в IPv6 деякі поля залишилися колишніми, деякі поля заголовка IPv4 більш не використовуються, а в деяких полях змінені назви і розташування.

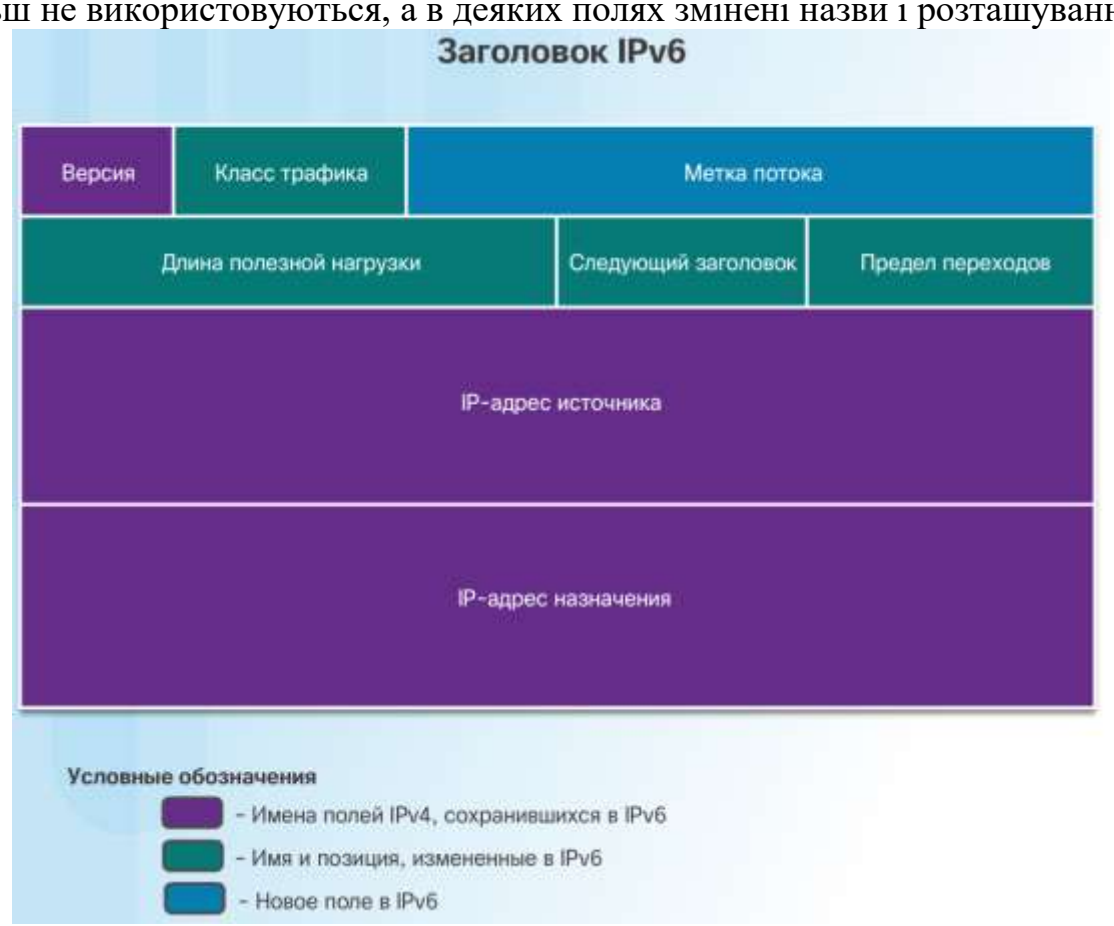


Рис. 1.1.7 Заголовок IP пакету

У той же час заголовок IPv6, складається з 40 октетів (головним чином через довжину адрес IPv6 джерела і призначення) і 8 полів заголовків (3 основних поля заголовків IPv4 і 5 додаткових полів). Як видно на малюнку, назви деяких полів залишилися такими ж, як і в IPv4, в деяких полях змінені назви і розташування, крім того, додано нове поле.

Поля в заголовку пакета IPv6:

Версія. Це поле містить 4-бітове двійкове значення, яке визначає версію IP-пакета. Для пакетів IPv6 в цьому полі завжди вказано значення 0110.

Клас трафіку. Це 8-бітове поле, відповідне полю «Диференційовані сервіси (DS)» в заголовку IPv4.

Мітка потоку. Це 20-бітове поле вказує на те, що всім пакетам з однаковими мітками потоку призначається однаковий тип обробки маршрутизаторами.

Довжина корисного навантаження. Це 16-бітове поле вказує довжину блоку даних або корисного навантаження пакета IPv6.

Наступний заголовок. Це 8-бітове поле, відповідне полю «Протокол» в заголовку IPv4. Воно вказує тип корисного навантаження даних, які переносить пакет, що дозволяє мережному рівню пересилати дані на відповідний протокол більш високого рівня.

Межа переходу. Це 8-бітове поле, що заміняє поле «Час існування» (TTL) в IPv4. Це значення зменшується на одиницю кожним маршрутизатором, пересилати пакет. Коли лічильник досягає значення 0, пакет відкидається, і на що відправляє вузол пересилається повідомлення ICMPv6, яке означає, що пакет не досяг свого призначення, так як був перевищений межа переходів.

IPv6-адреса джерела. Це 128-бітове поле, що визначає IPv6-адреса приймаючого вузла.

IPv6-адреса призначення. Це 128-бітове поле, що визначає IPv6-адреса приймаючого вузла.

Пакет IPv6 також може містити заголовки розширень (EH), які надають додаткову інформацію мережевого рівня. Заголовки розширень є додатковими і поміщаються між заголовком IPv6 і корисним навантаженням. Заголовки розширень використовуються для фрагментації, забезпечення безпеки, підтримки мобільності і багато чого іншого.

Рис. 1.1.8 Поля заголовку IPv6

На відміну від IPv4, маршрутизатори не ділять на частини спрямовані IPv6-пакети.

Іншим призначенням мережевого вузла є пересилання пакетів між вузлами. Вузол може відправити пакет на наступні адреси.

Самому собі. Вузол може відправити луна-запит на спеціальний IPv4-адрес, який представлений як 127.0.0.1 і називається інтерфейсом loopback. Відправка луна-запиту на інтерфейс loopback тестує стек протоколу TCP / IP на вузлі.

Локальний вузол. Вузол в тій же локальній мережі, в якій також знаходиться відправляє вузол. Вузли використовують один і той же мережеву адресу.

Віддалений вузол. Вузол у віддаленій мережі. Вузли не використовують один і той же мережеву адресу.

Якому вузлу адресований пакет - локальному або віддаленому - визначається комбінацією IPv4-адреси і маски підмережі пристрою джерела (або відправляє пристрої), які порівнюються з IPv4-адресою і маскою підмережі пристрою призначення.

У домашній або корпоративної мережі можуть перебувати кілька дротяних і бездротових пристроїв, з'єднаних один з одним за допомогою проміжного пристрою, такого як комутатор локальної мережі (LAN) і (або) точка бездротового доступу (WAP). Це проміжний пристрій забезпечує з'єднання між локальними вузлами в локальній мережі. Локальні вузли можуть отримувати доступ один до одного і обмінюватися інформацією без використання будь-яких додаткових пристроїв. Якщо вузол відправляє пакет пристрою, яке налаштоване в цій же IP-мережі в якості головного пристрою, пакет просто пересилається з інтерфейсу вузла через проміжне пристрій прямо на пристрій призначення.

Зрозуміло, в більшості випадків нам потрібно, щоб наші пристрої могли встановлювати з'єднання за межами сегмента локальної мережі: підключатися до інших будинків, офісів та Інтернету. Пристрої, які не входять в сегмент локальної мережі, називаються віддаленими вузлами. Якщо вихідне пристрій відправляє пакет до віддаленого пристрою призначення, то в цьому випадку потрібна допомога маршрутизаторів і виконання маршрутизації. Маршрутизація - це процес визначення найкращого шляху до вузла призначення. Маршрутизатор, підключений до сегменту локальної мережі, називається шлюзом за замовчуванням.

Шлюз за замовчуванням - це мережевий пристрій, який направляє трафік в інші мережі. Це маршрутизатор, який може направляти трафік за межі локальної мережі.

Якщо в якості аналогії мережі використовувати кімнату, шлюзом за замовчуванням буде вхідні двері. Щоб потрапити в іншу кімнату або мережу, потрібно знайти вхідні двері.

В якості альтернативи, ПК або комп'ютер, якому ніхто не знає IP-адреса шлюзу, подібний до чоловіка в кімнаті, яка не знає, де знаходиться двері. Ця людина може розмовляти з іншими людьми в кімнаті або в мережі, але якщо він не знає адресу шлюзу або якщо шлюзу взагалі не існує, то він не може вийти з кімнати.

Таблиця маршрутизації вузла, як правило, містить шлюз. Вузол отримує IPv4-адрес шлюзу або динамічно від протоколу динамічної настройки вузла (DHCP) або з вручну налаштованих параметрів. На рис. 1 комп'ютери PC1 і PC2 налаштовані на використання шлюзу з IPv4-адресою 192.168.10.1. У таблиці маршрутизації ПК при наявності налаштованого шлюзу створюється маршрут за замовчуванням. Маршрут за замовчуванням - маршрут або шлях, по якому йде комп'ютер, коли він намагається зв'язатися з віддаленої мережею.

Рис. 1.1.9 Основний шлюз виходу в глобальну мережу

Маршрут за замовчуванням визначається в залежності від конфігурації шлюзу і поміщається в таблицю маршрутизації головного комп'ютера. І комп'ютер PC1, і комп'ютер PC2 матимуть маршрут за замовчуванням для відправки всього трафіку, призначеного для віддалених мереж, до маршрутизатора R1.

На вузлі під управлінням ОС Windows для відображення таблиці маршрутизації вузла можна використовувати команду route print або netstat -r. Обидві команди видають однаковий результат. Спочатку отримані вихідні дані можуть здатися занадто великими, однак розібратися в них досить легко.

Після введення команди netstat -r або рівноцінної їй команди route print будуть відображені наступні три розділи, які стосуються поточним мережевим підключенням TCP / IP.

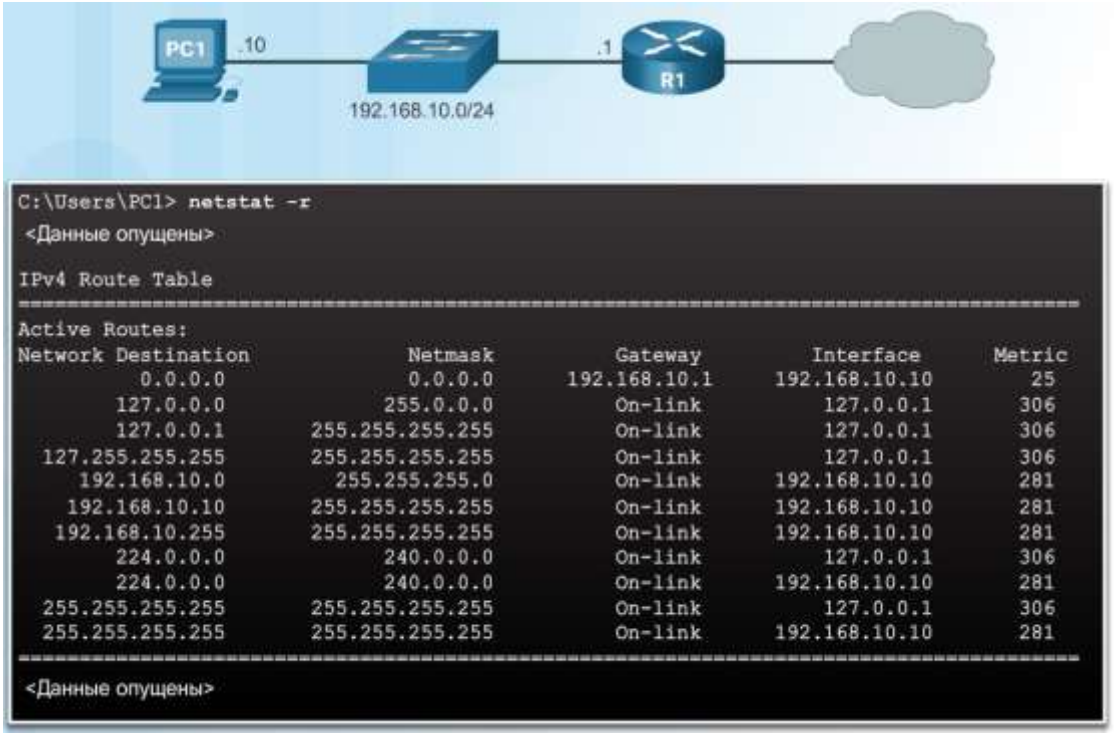


Рис. 1.1.10 Використання утиліти netstat -r

Список інтерфейсу. Містить адресу управління доступом до середовища (MAC-адресу) і присвоєний номер інтерфейсу з підтримкою мережі на вузлі, включаючи адаптери Ethernet, Wi-Fi і Bluetooth.

Таблиця маршрутизації IPv4. Містить всі відомі маршрути IPv4, включаючи прямі підключення, локальні мережі та локальні маршрути, які використовуються за замовчуванням.

Таблиця маршрутизації IPv6. Містить всі відомі маршрути IPv6, включаючи прямі підключення, локальні мережі та локальні маршрути, які використовуються за замовчуванням.

Коли вузол відправляє пакет іншому вузлу, він використовує свою таблицю маршрутизації, щоб визначити місце відправки пакета. Якщо вузол призначення знаходиться у віддаленій мережі, пакет пересилається на шлюз за замовчуванням.

Що відбувається, коли пакет прибуває на шлюз за замовчуванням (зазвичай маршрутизатор)? Маршрутизатор перевіряє свою таблицю маршрутизації, щоб визначити місце пересилання пакета.

Маршрути з прямим підключенням. Ці маршрути надаються активними інтерфейсами маршрутизаторів. Маршрутизатор додають маршрут з прямим підключенням, коли інтерфейс налаштований з IP-адресою і активований. Кожен з інтерфейсів маршрутизатора підключений до різного сегменту мережі.

Дистанційні маршрути. Ці маршрути надаються віддаленими мережами, підключеними до інших маршрутизаторів. Маршрути до цих мереж можуть бути налаштовані на локальному маршрутизаторе вручну адміністратором мережі або призначені динамічно за допомогою локального маршрутизатора, який обмінюється даними маршрутизації з іншими маршрутизаторами, використовуючи для цього протоколи динамічної маршрутизації.

Маршрут за замовчуванням. Подібно вузлу, маршрутизатори також використовують маршрут за замовчуванням, як крайня міра, якщо іншого маршруту до потрібної мережі в таблиці маршрутизації немає.

Як показано на малюнку, на маршрутизаторі з операційною системою Cisco IOS для відображення його таблиці IPv4-маршрутизації може використовуватися команда show ip route.

Таблиця маршрутизації надає інформацію про маршрутизації для мереж з прямим підключенням і віддалених мереж, а також про порядок визначення маршруту, його достовірності та рейтингу, коли маршрут був останній раз оновлений і який інтерфейс слід використовувати, щоб досягти запитуваної призначення.

Коли на інтерфейс маршрутизатора надходить пакет, маршрутизатор аналізує його заголовок, щоб визначити мережу призначення. Якщо мережа призначення збігається з маршрутом в таблиці маршрутизації, маршрутизатор пересилає пакет, використовуючи інформацію в таблиці маршрутизації. Якщо існують два і більше ймовірних маршруту до одного пункту призначення для визначення маршруту, який з'явиться в таблиці маршрутизації, використовується метрика.

При активації інтерфейсу маршрутизатора, налаштованого за допомогою IPv4-адреси і маски підмережі, автоматично створюються такі два елементи таблиці маршрутизації.

C означає мережу з прямим підключенням. Мережі з прямим підключенням створюються автоматично, коли інтерфейс налаштовується за допомогою IP-адреси і активується.

L означає, що це локальний інтерфейс. Це IPv4-адрес інтерфейсу на маршрутизаторі.

На малюнку представлені описи записів таблиці маршрутизації на маршрутизаторі R1 для мережі з прямим підключенням 192.168.10.0. Ці записи автоматично додані в таблицю маршрутизації при налаштуванні і активації інтерфейсу GigabitEthernet 0/0. Натисніть на кожен знак плюса («+»), щоб переглянути додаткову інформацію про записи таблиці маршрутизації в мережі з прямим підключенням.

Коли пакет, призначений для віддаленої мережі, надходить на маршрутизатор, він порівнює мережу призначення з маршрутом, зазначеним в таблиці маршрутизації. Якщо збіг знайдено, маршрутизатор пересилає пакет на адресу маршрутизатора наступного переходу, використовуючи для цього інтерфейс, вказаний у записі маршрутизатора.

Припустимо, що комп'ютер PC1 або PC2 відправив пакет, призначений або для мережі 10.1.1.0, або для мережі 10.1.2.0. Коли пакет прибуває на інтерфейс Gigabit маршрутизатора R1, маршрутизатор R1 порівнює IPv4-адрес призначення пакета з записами в своїй таблиці маршрутизації. Таблиця маршрутизації показана на рис. 2. Виходячи зі змісту своєї таблиці маршрутизації, маршрутизатор R1 пересилає пакет зі свого послідовного інтерфейсу Serial 0/0/0 на адресу 209.165.200.226 наступного переходу.

Зверніть увагу: мережі з прямим підключенням з джерелом маршруту C і L не мають адреси наступного переходу. Це пов'язано з тим, що маршрутизатор може пересилати пакети безпосередньо до вузлів в цих мережах за допомогою зазначеного інтерфейсу.

Важливо також розуміти, що маршрутизатор не може пересилати пакети, якщо в таблиці маршрутизації відсутня маршрут для мережі призначення. Якщо маршрут, що позначає мережу призначення, в таблиці не вказано, пакет відкидається (тобто не пересилається). Проте, оскільки вузол може використовувати шлюз для пересилання пакета невідомому адресату, маршрутизатор також може використовувати маршрут за замовчуванням, щоб створювати шлюз «останньої надії». Маршрут за замовчуванням може бути налаштований вручну або отриманий динамічно.

Маршрутизатор - це комп'ютер

Існує безліч тіпів маршрутізаторів для использование в різніх інфраструктурах. Маршрутизатор Cisco прізначені для использование в самих різніх компаніях и Мережа.

Філії: віддалені працівники, невелікі підприємства и філії СЕРЕДНЯ розміру. Використовують Маршрутизатори Cisco G2 з інтегрованімі сервісамі (2-е поколение).

Мережі WAN: Великі компании, организации та підприємства. Використовують комутатори Cisco Серії Catalyst и маршрутизаторів Cisco з агрегацією сервісів (Aggregation Services Router, ASR).

Оператори зв'язку: Великі оператори зв'язку. Використовують Cisco ASR, система маршрутізації операторського класу Cisco CRS-3 и Маршрутизатори Серії 7600.

Основна увага в Програмі сертифікації CCNA пріділено лінійці маршрутізаторів для использование в філіях. На малюнку зображено маршрутизаторів Cisco 1900 2900 и 3900 G2 з інтегрованімі сервісамі.

Незалежності від своих функцій, розміру або складності всі моделі маршрутізаторів Фактично представляються собою комп'ютери. Як и комп'ютерів, планшетів и інтелектуальнім прилаштувати, маршрутізаторів необхідні следующие компоненти:

Центральний процесор (ЦП).

Операційна система (ОС).

Пам'ять, яка Включає оперативний Пристрій (ОЗУ), Постійний запам'ятовуючий Пристрій (ПЗУ), незалежне оперативний Пристрій (NVRAM) и флеш-пам'ять.

Як і всім комп'ютерам, планшетів, ігрових консолей і інтелектуальним пристроям, пристроїв Cisco потрібно центральний процесор, що обробляє

команди операційної системи, такі як ініціалізація системи, функції маршрутизації і комутації.

Виділений на малюнку компонент - це центральний процесор маршрутизатора Cisco тисяча дев'ятсот сорок один з встановленим радіатором. Радіатор допомагає розсіювати тепло, що виділяється центральним процесором.

Центрального процесора необхідна операційна система для виконання маршрутизації і комутації. Операційна система Cisco IOS - це системне програмне забезпечення, яке використовується для більшості пристроїв Cisco незалежно від їх розміру і типу. Вона є на маршрутизаторах, комутаторах для локальних мереж (LAN), невеликих точках бездротового доступу, великих маршрутизаторах з великою кількістю інтерфейсів і на багатьох інших пристроях.

Маршрутизатор має доступ до енергозалежною або незалежній пам'яті. Енергозалежною пам'яті для збереження даних потрібне постійне харчування. При виключенні електроживлення маршрутизатора або при його перезапуску вміст цієї пам'яті втрачається. Незалежна пам'ять зберігає дані навіть при перезавантаженні пристрою.

У зв'язку з цим в маршрутизаторі Cisco використовується чотири типи пам'яті:

ОЗУ. Це незалежна пам'ять використовується в маршрутизаторах Cisco для зберігання додатків, процесів і даних, необхідних для їх обробки центральним процесором. Маршрутизатор Cisco використовують швидкий тип ОЗУ, званий синхронним динамічним ОЗУ (SDRAM). Натисніть зображення ОЗУ на малюнку, щоб подивитися додаткову інформацію.

ПЗУ. Ця незалежна пам'ять використовується для зберігання важливих інструкцій по експлуатації та обмеженої версії IOS. Таким чином, ПЗУ - це вбудована в мікросхему мікропрограма всередині маршрутизатора, яка може бути змінена тільки компанією Cisco. Натисніть зображення ПЗУ на малюнку, щоб подивитися додаткову інформацію.

NVRAM. Ця незалежна пам'ять використовується як місце постійного зберігання файлу завантажувального конфігурації (startup-config).

Флеш. Це незалежна пам'ять комп'ютера, що використовується в якості місця постійного зберігання IOS і інших системних файлів, таких як файли журналів, файли голосового конфігурації, HTML файли, конфігурації резервного копіювання та багато іншого. При перезавантаженні маршрутизатора IOS копіюється з флеш-пам'яті в ОЗУ.

Рис. 1.1.11 Схема зберігання інформації у маршрутизаторі

Всі платформи маршрутизатора мають параметри і компоненти за замовчуванням. Наприклад, маршрутизатори Cisco 1941 поставляються разом з пам'яттю SDRAM об'ємом 512 МБ, яка може бути розширена до 2,0 ГБ. Маршрутизатор Cisco 1941 також поставляються разом з флеш-пам'яттю об'ємом 256 МБ, яка може бути розширена за допомогою двох зовнішніх слотів Compact Flash. Кожен слот підтримує високошвидкісні карти пам'яті ємністю до 4 ГБ.

Незважаючи на існування кількох типів і моделей маршрутизаторів, кожен з них має ідентичні загальні апаратні компоненти.

На малюнку показано внутрішній устрій маршрутизатора Cisco 1841 першого покоління маршрутизаторів ISR. Натисніть кожен компонент, щоб побачити його короткий опис. Зверніть увагу, на малюнку також виділені інші компоненти, такі як блок живлення, охолоджуючий вентилятор, теплові екрани і модуль апаратного стиснення даних (AIM), які в цьому розділі не розглядаються.

Підключення на маршрутизаторі Cisco можна розділити на дві категорії: внутрішньосмугові інтерфейси маршрутизатора і порти управління. Натисніть на виділені області на рис. 1, щоб подивитися додаткову інформацію.

Як і у випадку з комутатором Cisco, на маршрутизаторі Cisco існує кілька способів доступу до середовища інтерфейсу командного рядка (CLI) призначеного для користувача режиму EXEC. Нижче представлені найбільш поширені з них.

Консоль - це фізичний порт управління, що забезпечує позасмуговий доступ до пристрою Cisco. Позасмуговий доступ здійснюється через виділений адміністративний канал, який використовується виключно в цілях технічного обслуговування пристрою.

Secure Shell (SSH) - метод, що дозволяє віддалено встановити захищене підключення CLI через віртуальний інтерфейс по мережі. На відміну від консольного підключення для SSH-підключень на пристрої повинні бути активні мережеві служби, включаючи активний інтерфейс з налаштованим адресою.

Telnet - це незахищений протокол, що дозволяє віддалено почати сеанс CLI через віртуальний інтерфейс по мережі. На відміну від SSH, Telnet не забезпечує захищене зашифроване з'єднання. Дані для аутентифікації

користувача, паролі і команди передаються по мережі у вигляді простого тексту.

Примітка. Деякі пристрої, такі як маршрутизатори, також можуть підтримувати застарілий допоміжний порт, який раніше використовувався, щоб віддалено почати сеанс CLI за допомогою модему. Аналогічно консольного підключення допоміжний порт забезпечує позасмугове підключення і не вимагає настройки або наявності будь-яких мережевих служб.

Telnet і SSH вимагає внутрішньогосмугового підключення до мережі, а це означає, що адміністратор повинен отримати доступ до маршрутизатора через один з інтерфейсів WAN або LAN. Натисніть на виділені області на рис. 2, щоб подивитися додаткову інформацію.

Внутрішньосмугові інтерфейси отримують і пересилають IP-пакети. Кожен налаштований і активний інтерфейс на маршрутизаторі є учасником або вузлом в різній IP-мережі. Для кожного інтерфейсу необхідно налаштувати IPv4-адрес і маску підмережі інший мережі. Операційна система Cisco IOS не допускає, щоб два активних інтерфейсу на одному маршрутизаторі належали одній і тій же мережі.

Процес завантаження складається з трьох основних етапів, це:

1. Виконання процедури POST (самотестування після включення живлення) і завантаження програми початкового запуску.

2. Пошук і завантаження програмного забезпечення Cisco IOS.

3. Пошук і завантаження файлу завантажувального конфігурації або перехід в режим настройки.

1. Виконання самотестування при включенні харчування (POST) і завантаження програми початкового запуску/

Під час самотестування маршрутизатор з ПЗУ виконує діагностичні процедури на кількох компонентах апаратного забезпечення, включаючи використання ЦП, ОЗУ і NVRAM. Після завершення процедури POST маршрутизатор запускає програму початкового запуску. Основна мета програма початкового запуску - знайти операційну систему Cisco IOS і завантажити її в ОЗУ.

Примітка. На цьому етапі при наявності підключення до маршрутизатора через консоль на екрані будуть відображатися вихідні дані.

2. Пошук і завантаження операційної системи Cisco IOS.

Як правило, система IOS зберігається у флеш-пам'яті і копіюється в ОЗУ для виконання центральним процесором. Якщо образ IOS у флеш-пам'яті не виявлено, маршрутизатор може спробувати знайти його за допомогою сервера TFTP. Якщо повний образ IOS що невиявлений, тоді в ОЗУ з ПЗУ буде скопійована її скорочена версія. Ця версія IOS призначена для діагностики проблем і може бути використана для завантаження повної версії IOS у флеш-пам'ять.

3. Пошук і завантаження файлу конфігурації/

Потім програма початкового запуску копіює файл завантажувального конфігурації з пам'яті NVRAM в ОЗУ. Ця конфігурація стає поточною. Якщо файл завантажувального конфігурації відсутній в пам'яті NVRAM, маршрутизатор може спробувати знайти сервер спрощеного протоколу передачі

файлів (TFTP). Якщо сервер TFTP не буде знайдений, маршрутизатор відобразить вікно режиму настройки.

Примітка. У програмі цього курсу для конфігурації маршрутизатора режим настройки не використовується. Якщо на екрані з'являється запит перейти в режим настройки, слід завжди вказувати значення no (немає). В разі обрання опції «yes» (так) і виконаний перехід в режим настройки, натисніть комбінацію клавіш Ctrl + C на будь-якому етапі, щоб припинити процес налаштування.

Маршрутизатор і комутатори Cisco багато в чому схожі. Вони підтримують схожі операційні системи, використовують аналогічні командні структури і безліч ідентичних команд. Крім того, при впровадженні цих пристроїв в мережу виконуються однакові настройки вихідної конфігурації.

2. Розділ Побудова комп'ютерних мереж на базі концентраторів, мостів, комутаторів.

2.1 Технології IPv4 та IPv6. Маски мережі.

Адресація є найважливішою функцією протоколів мережевого рівня. Адресація забезпечує обмін даними між вузлами - незалежно від того, чи знаходяться вони в одній мережі або в різних мережах. Протоколи IPv4 iIPv6 здійснюють ієрархічну адресацію пакетів даних.

Проектування, впровадження і управління ефективним планом IP-адресації забезпечують надійність і ефективність роботи мереж.

У цьому розділі докладно розглядаються структура адрес і їх застосування в створенні і тестуванні IP-мереж і підмереж.

Двійкова система числення складається з цифр 0 і 1, званих бітами. Десяткова система числення складається з 10 цифр: від 0 до 9.

Розуміння двійковій системи важливо для нас, оскільки вузли, сервери і мережеві пристрої використовують саме двійкову адресацію. Зокрема, для ідентифікації один одного вони використовують двійкові IPv4-адреси.

Кожен адреса являє собою рядок з 32 біт, розділену на 4 частини, звані октетами. Кожен октет містить 8 біт (або 1 байт), розділені крапкою. Наприклад, вузлу PC1 на малюнку призначений IPv4-адрес 11000000.10101000.00001010.00001010. Адресою його шлюзу буде відповідний адресу інтерфейсу Gigabit Ethernet interface маршрутизатора R1: 11000000.10101000.00001010.00000001.

Робота з двійковими числами - не така легка задача. Для простоти використання IPv4-адреси зазвичай виражаються в десятковому форматі з точкою-роздільником. Вузлу PC1 призначений IPv4-адрес 192.168.10.10; адреса шлюзу - 192.168.10.1.

На рис. 1.x зіставляється адреса в десятковому форматі з точкою-роздільником і 32-бітний двійковий адресу вузла PC1.

Рис. 2.1.1 Співставлення адресів у двійковому коді і десятковому коді

Для чіткого розуміння адресації мережі необхідно знати принципи двійковій адресації і отримати практичні навички перетворення IPv4-адрес з двійкової системи числення в десяткову з точкою роздільником.

У цьому розділі ви дізнаєтеся, як переводити числа з двійкової в десяткову систему числення.

Щоб переводити числа з двійкової в десяткову систему числення, потрібно розуміти позиційну систему числення. Принцип позиційної системи числення полягає в тому, що значення цифри визначається її «позицією» в послідовності цифр. Вам вже знайома найбільш поширена система числення - десяткова (з основою 10).

Для перетворення двійкового IPv4-адреси в десятковий еквівалент з точкою-роздільником розділіть IPv4-адрес на чотири 8-бітних октету. Потім занесіть двійкові позиційне значення в якості двійкового числа першого октету і виконайте відповідне обчислення.

Наприклад, припустимо, що IPv4-адрес вузла - 11000000.10101000.00001011.00001010. Для перетворення двійкового адреси в десятковий формат, почніть з першого октету, як показано на рис. 1. Введіть 8-бітове двійкове число в якості позиційного значення рядка 1, а потім виконайте обчислення, результатом якого буде десяткове число 192. Це число складе перший октет десяткового запису з точкою-роздільником.

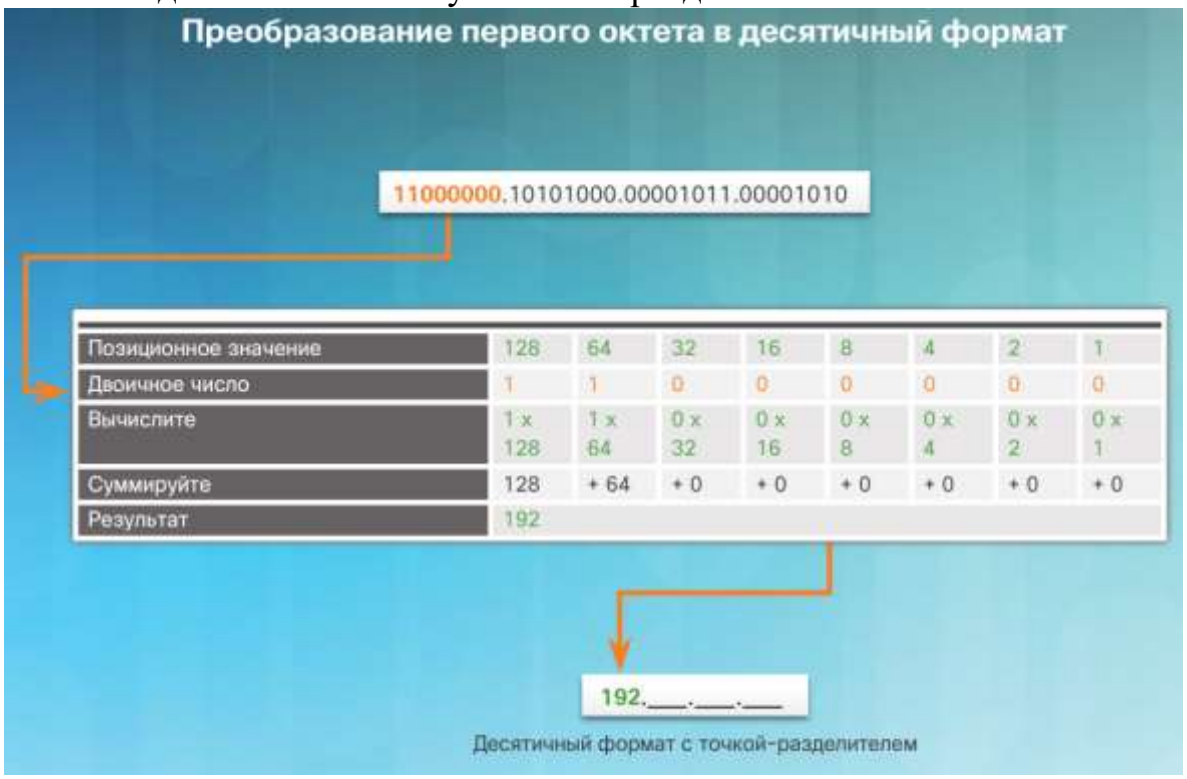


Рис. 2.1.2

Потім перетворіть другий октет, як показано на рис. 2. Підсумкове десяткове значення - 168; це буде другий октет.

Перетворіть третій октет, як показано на рис. 4, і останній четвертий октет IP-адреси. Результат: 192.168.11.10.

Необхідно також розуміти, як перетворювати IPv4-адреси в десятковому форматі з точкою-роздільником в двійковий формат. Корисним інструментом є

таблиця довічних позиційних значень. Нижче показано, як використовувати таблицю для перетворення десяткових чисел в двійковий формат:

Рис. 2.1.3

На рис. 1.x задається питання: чи більше або дорівнює десяткове число в октеті (n) найстаршому біту (128). Якщо ні, введіть двійковий 0 в якості позиційного значення числа 128. Якщо так, введіть двійкову 1 в якості позиційного значення числа 128 і відніміть 128 з десяткового числа.

Рис. 2.1.4

На рис. задається питання: чи більше або дорівнює залишок (n) наступного за старшинством біту (64). Якщо ні, введіть двійковий 0 в якості позиційного значення числа 64; в іншому випадку введіть двійкову 1 і відніміть 64 з десяткового числа.

Рис. 2.1.5

На рис. 1.x задається питання: чи більше або дорівнює залишок (n) наступного за старшинством біту (32). Якщо ні, введіть двійковий 0 в якості позиційного значення числа 32; в іншому випадку введіть двійкову 1 і відніміть 32 з десяткового числа.

Щоб краще зрозуміти цей процес, розглянемо IP-адреса 192.168.11.10. Скориставшись описаної вище процедурою, почнемо з таблиці довічних позиційних значень і першого десяткового числа 192.

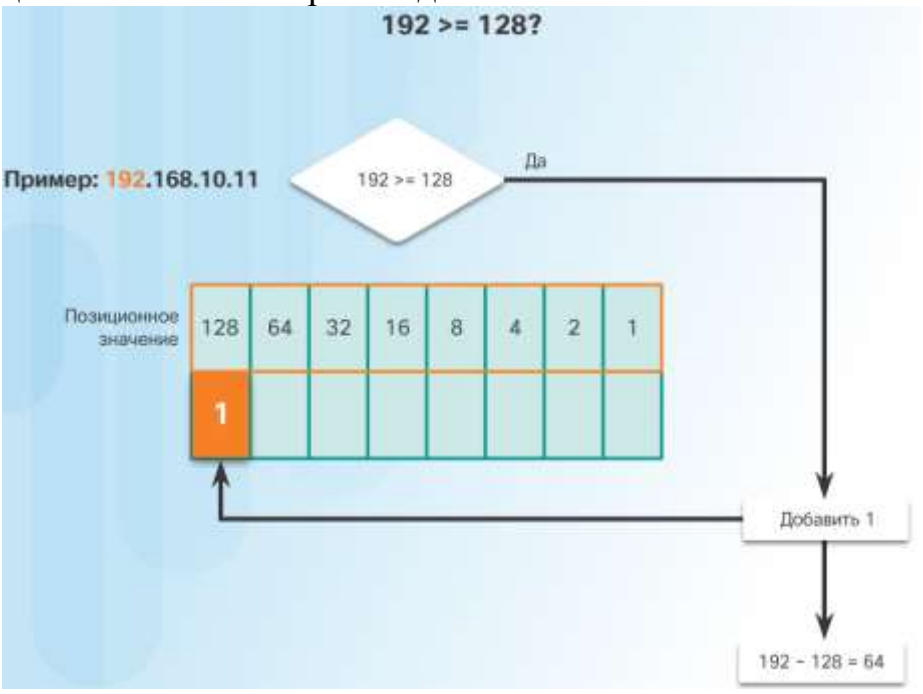


Рис. 2.1.6

На рис. показано порівняння числа 192, щоб визначити, більше воно або дорівнює старшому біту 128. Оскільки 192 більше 128, додайте 1 в якості старшого позиційного значення, що відповідає числу 128. Потім відніміть 128 з

192; отримуємо різницю (залишок) 64. На рис. 2 виконується порівняння числа 64 з наступним по старшинству бітом 64. Оскільки вони рівні, додайте 1 в якості наступного за старшинством позиційного значення. Введіть двійковий 0 в що залишилися позиції, як показано на рис. 1.x. Двійкове значення першого октету - 11000000.

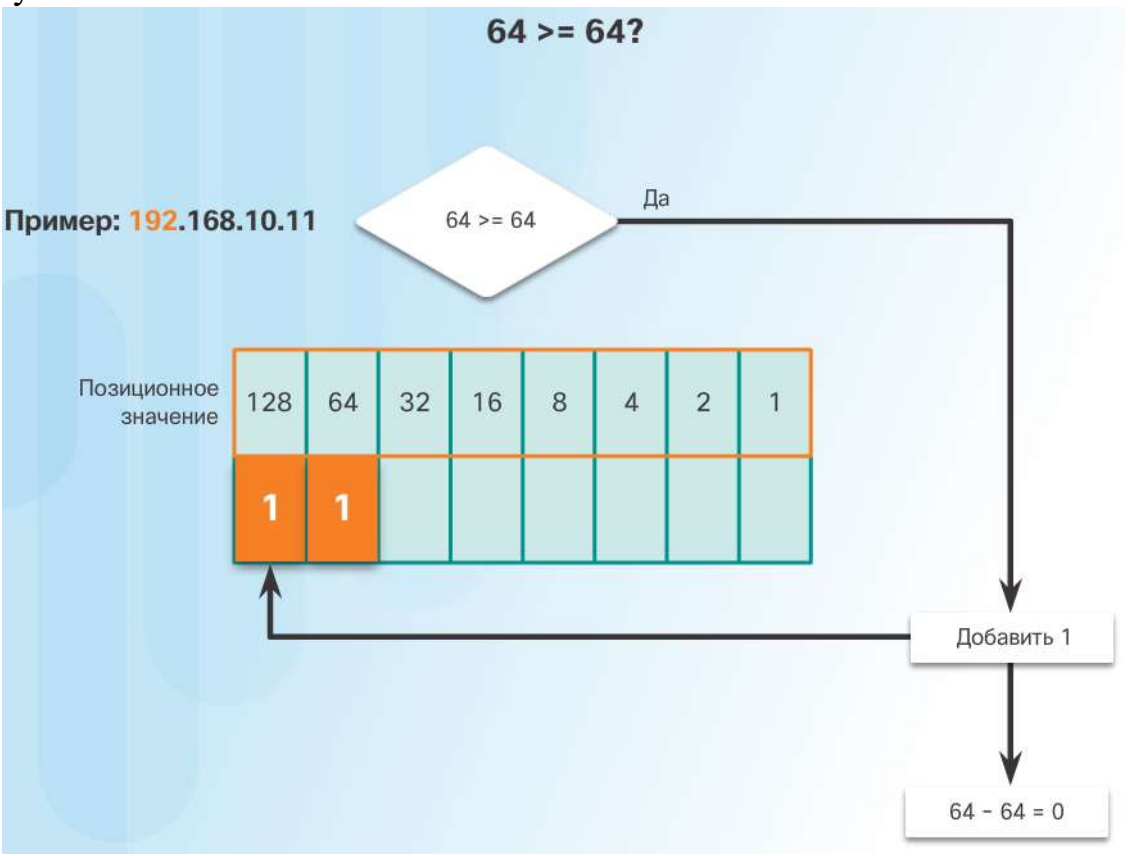


Рис. 2.1.7

Наступний октет - 168. На рис. 1.x виконується порівняння числа 168 зі старшим бітом 128. Оскільки 168 більше 128, введіть 1 у якості старшого позиційного значення. Потім відніміть 128 з 168; отримуємо різницю (залишок) 40. На рис. 5 виконується порівняння числа 40 з наступним по старшинству бітом 64. Оскільки 40 менше 64, введіть 0 в якості наступного за старшинством позиційного значення. На рис. 6 виконується порівняння з наступним по старшинству бітом 32. Оскільки 40 більше 32, введіть 1 у якості позиційного значення і відніміть 32 з 40; отримуємо залишок 8. Число 8 відповідає конкретному позиційному значенням. Тому введіть 0 в якості позиційного значення числа 16 і введіть 1 у якості позиційного значення числа 8. Введіть нулі в усі інші позиції. Як видно на рис. 8, двійкове значення третього октету - 10101000.

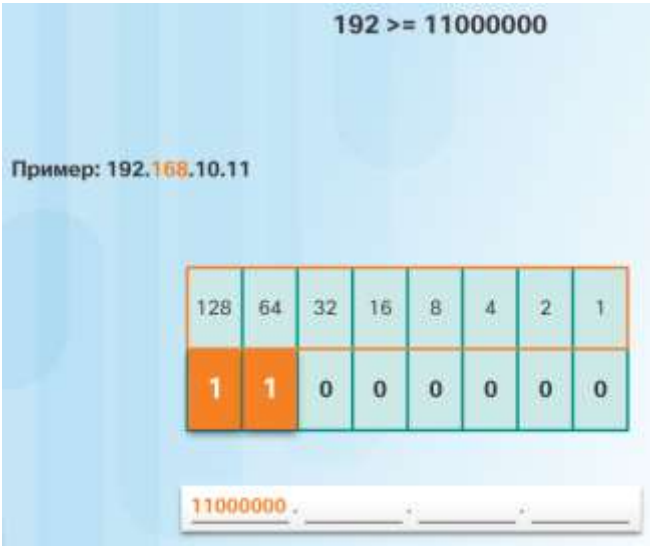


Рис. 2.1.8

Третій октет - 11. У випадку простих або невеликих десяткових чисел процедуру вирахування можна пропустити. Наприклад, на рис. 9 показано отримане двійкове число. Це число можна досить легко отримати без вирахування (8 + 2 + 1 = 11). Двійкове значення другого октету - 00001011.

Рис. 2.1.9

Четвертий октет - 10 (8 + 2). Як видно на рис. 10, двійкове значення четвертого октету - 00001010.

Перетворення між двійковій і десяткової системами числення може спочатку здатися складним, але чим більше ви будете практикуватися, тим простіше зможете це робити.

Розуміння двійковій системи числення необхідно, щоб встановити, чи знаходяться два вузла в одній і тій же мережі. Як ви пам'ятаєте, IPv4-адрес є ієрархічним адресою, який складається з двох частин: мережевий і вузловий. Визначаючи ту чи іншу частину, необхідно звертати увагу не на десяткове значення, а на 32-бітний потік. Як показано на малюнку, в 32-бітному потоці одна частина бітів визначає мережу, а інша - вузол.

Біти в мережевій частині адреси повинні бути однаковими у всіх пристроїв, що знаходяться в одній мережі. Біти в вузловий частини адреси

повинні бути унікальними для кожного вузла в мережі. Якщо два вузла мають одну бітову комбінацію в певній мережевої частини 32-бітного потоку, то ці два вузли знаходяться в одній і тій же мережі.

Але як вузли визначають, яка з частин 32-бітного потоку є мережевий, а яка - вузловий? Для цього використовується маска підмережі.

В ході налаштування IPv4-конфігурації вузла необхідно задати три IPv4-адреси в десятковому форматі з точкою-роздільником.

Маска підмережі використовується для визначення мережевої і вузловий частин IPv4-адреси.

Шлюз за замовчуванням - локальний шлюз (тобто IPv4-адрес інтерфейсу локального маршрутизатора), який використовується для звернення до віддалених мереж.

При призначенні пристрою IPv4-адреси для визначення адреси мережі, до якого належить даний пристрій, використовується маска підмережі. Мережевий адреса являє всі пристрої в одній мережі.

Для ідентифікації мережевий і вузловий частини IPv4-адреси маска підмережі по бітово порівнюється з IPv4-адресою зліва направо, як показано на рис. 3. Одиниці в масці підмережі визначають мережеву частину, а нулі - вузлову частину. Зверніть увагу, що маска підмережі насправді не містить мережевий або вузловий частини IPv4-адреси; вона лише вказує комп'ютеру, де шукати ці частини в конкретному IPv4-адресу.

Сам процес, який використовується для визначення мережевої і вузловий частин адреси, називається логічною операцією І (AND).

Логічна операція І - одна з трьох основних довічних операцій, використовуваних в дискретної логіці. Двома іншими операціями є АБО (OR) і НЕ (NOT). При тому, що всі три операції використовуються в мережах передачі даних, для визначення мережевої адреси застосовується тільки операція І. Тому в цьому розділі ми будемо говорити тільки про операції І.

Логічне І - це порівняння двох бітів, результати якого показані на рис. 1. Зверніть увагу, що 1 І 1 = 1.

Щоб визначити мережеву адресу IPv4-сайтів, на IPv4-адресою і масці підмережі побитово застосовується логічна операція І. Застосування логічної операції І до адресою і масці підмережі в результаті дає мережеву адресу.

Для демонстрації використання операції І для визначення мережевої адреси розглянемо вузол з IPv4-адресою 192.168.10.10 і маскою підмережі 255.255.255.0. На рис. 2 показаний IPv4-адрес вузла і його двійковий еквівалент. Двійковий адресу маски підмережі вузла показаний на рис. 3.

Фрагменти, виділені жовтим на рис. 4, визначають біти І, що дають двійкову одиницю в рядку результатів операції І. Решта порівняння бітів дали виконавчі нулі. Зверніть увагу, що в останньому октеті більше немає бітів з двійковій 1.

Нарешті, на рис. 5 показаний отриманий мережеву адресу: 192.168.10.0 255.255.255.0. Таким чином, вузол 192.168.10.10 знаходиться в мережі 192.168.10.0 255.255.255.0.

Подання мережевих адрес і адрес вузлів шляхом у вигляді маски підмережі в десятковому форматі з точкою-роздільником може бути дуже громіздким. На

щастя, існує альтернативний, більш простий, спосіб визначення маски підмережі, званий довжиною префікса.

Довжина префікса означає кількість біт, встановлених на одиницю (1) в масці підмережі. Вона позначається похилою рискою вправо («/»), після якої йде набір одиниць. Отже, потрібно підрахувати число бітів в масці підмережі і поставити перед цим значенням косу риску.

Наприклад, див. Таблицю на малюнку. У першому стовпчику перераховані різні маски підмережі, які можуть використовуватися з адресою вузла. У другому стовпці зазначений отриманий 32-бітний двійковий адресу. В останньому стовпці вказана отримана довжина префікса.

Маска подсети	32-битный адрес	Длина префикса
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Рис. 2.1.10

Про використання різних типів довжини префікса ви дізнаєтеся пізніше. Зараз же ми будемо говорити про маску підмережі / 24 (тобто 255.255.255.0).

Деякі пристрої в межах мережі вимагають призначення фіксованого IP-адреси. Наприклад, принтерів, серверів і мережевих пристроїв потрібен постійний IP-адреса. З цієї причини зазначеним пристроїв, як правило, призначаються статичні IP-адреси.

Вузла також можна призначити статичний IPv4-адрес, як показано на малюнку Призначення вузлів статичних адрес прийнятно в невеликих мережах. У великій же мережі призначення статичної адреси кожного вузла займе дуже багато часу. При цьому дуже важливо вести точний облік призначених статичних IP-адрес.

У більшості мереж передачі даних найбільша за чисельністю група вузлів - це комп'ютери, планшети, смартфони, принтери і IP-телефони. Крім того, нерідкі випадки, коли кількість користувачів і їх пристроїв часто змінюються. Призначення статичного IPv4-адреси кожному пристрою непрактично. Тому IPv4-адреси призначаються пристроям динамічно, за допомогою протоколу динамічної настройки вузла (Dynamic Host Configuration, DHCP).

Як показано на малюнку, вузол може отримувати IPv4-адрес автоматично. Вузол - це DHCP-клієнт, і він запитує IPv4-адрес у DHCP-сервера. DHCP-сервер надає IPv4-адрес, маску підмережі, шлюз за замовчуванням і інші параметри конфігурації.

DHCP - це найбільш поширений спосіб привласнення IPv4-адрес вузлів у великих мережах. Інша переваги DHCP полягає в тому, що адреси присвоюються вузлам тимчасово, як би «здається в оренду» на певний період.

Якщо вузол вимикається або йде з мережі, його адреса повертається в пул для повторного використання. Це особливо корисно для мобільних користувачів, які використовують мережу ще не всегда.

Вузол, успішно підключений до мережі, може обмінюватися даними з іншими пристроями одним з трьох способів.

Одноадресна розсилка - процес відправки пакета з одного вузла на інший конкретний вузол.

Широкомовлення - процес відправки пакета з одного вузла на всі вузли в мережі.

Багатоадресна розсилка - процес відправки пакета з одного вузла обраній групі вузлів, можливо, в різних мережах.

Ці три типи зв'язку використовуються в мережах передачі даних для різних цілей. У всіх трьох типах IPv4-адрес вузла джерела розміщений в заголовку пакета в якості адреси джерела.

Одноадресна розсилка використовується для звичайного обміну даними між вузлами як в мережі типу «клієнт / сервер», так і в тимчасовій мережі. Для одноадресної розсилки пакетів в якості адреси призначення використовуються адреси пристрою призначення. Пакети можуть бути спрямовані через об'єднану мережу.

У IPv4-мережі індивідуальні адреси, що застосовуються до кінцевого пристрою, називаються вузловими адресами. Для одноадресної розсилки адреси, присвоєні двом кінцевим пристроям, використовуються в якості IPv4-адрес джерела і призначення. В процесі інкапсуляції вузол джерела використовує свій IPv4-адрес як адреса джерела, а IPv4-адрес вузла призначення як адреса призначення. Незалежно від того, чи є адреса призначення, який визначив пакет, одноадресна, широкомовною або багатоадресних, адреса джерела будь-якого пакета завжди є адресою одноадресної розсилки вузла джерела.

IPv4-адреси вузла є одноадресних і входять в діапазон адрес від 0.0.0.0 до 223.255.255.255. Однак в цьому діапазоні є безліч адрес, зарезервованих для спеціальних цілей. Такі адреси будуть розглянуті пізніше.

Широкомовна передача використовується для відправки пакетів всім вузлам в мережі через широкомовний мережеву адресу. Пакет широкомовної розсилки містить IPv4-адрес призначення, в вузловий частини якого присутні тільки одиниці (1). Це означає, що пакет отримають і оброблять всі вузли в локальній мережі (домені широкомовної розсилки). Широкомовні розсилання передбачені в багатьох мережевих протоколах, наприклад DHCP. Коли вузол отримує пакет, відправлений на широкомовний мережеву адресу, вузол обробляє пакет так же, як і пакет, відправлений на адресу одноадресної розсилки.

Є два типи широкомовної розсилки: пряма і обмежена. Пряма широкомовлення відправляється всіх вузлів в конкретній мережі. Наприклад, вузол в мережі 172.16.4.0/24 відправляє пакет на адресу 172.16.4.255. Обмежена широкомовлення відправляється на адресу 255.255.255.255. За замовчуванням, маршрутизатори не відсилаються широкомовні розсилання.

Наприклад, вузол в межах мережі 172.16.4.0/24 відправляє трансляцію розсилку всіх вузлів усередині своєї мережі, використовуючи пакет з адресою призначення 255.255.255.255.

Широкомовний пакет використовує ресурси в мережі і змушує кожне приймаюче вузол в мережі обробляти цей пакет. Таким чином, трафік широкомовної розсилки повинен бути обмеженим, щоб не впливати на продуктивність мережі і інших пристроїв. Оскільки маршрутизатори поділяють домени широкомовної розсилки, поділ мереж може підвищити продуктивність мережі за рахунок усунення надмірного трафіку широкомовного розсилання.

Багатоадресна розсилка зменшує трафік, дозволяючи вузлу відправляти один пакет обраній групі вузлів, які підписані на групу під LGPL.

Для під LGPL в протоколі IPv4 зарезервовані адреси від 224.0.0.0 до 239.255.255.255. Групові IPv4-адреси від 224.0.0.0 до 224.0.0.255 зарезервовані для під LGPL в межах локальної мережі. Ці адреси використовуються для груп під LGPL в локальній мережі. Маршрутизатор, підключений до локальної мережі, розпізнає, що ці пакети адресовані локальної групи під LGPL, і не пересилає їх далі. Зазвичай зарезервовані локальні адреси застосовуються в протоколах маршрутизації за допомогою многоадресной передачі для обміну даними маршрутизації. Наприклад, адреса 224.0.0.9 зарезервований для протоколу маршрутизації (Routing Information Protocol, RIP) версії 2 для обміну даними з іншими маршрутизаторами RIPv2.

Вузли, які отримують конкретні багатоадресні дані, називаються клієнтами під LGPL. Клієнти під LGPL використовують сервіси, запитані програмою клієнта для підписки на групу під LGPL.

Кожна група під LGPL представлена одним груповим IPv4-адресою призначення. Коли IPv4-вузол підписується на групу під LGPL, він обробляє пакети, адресовані на цей груповий адресу, а також пакети, адресовані на його унікальний індивідуальний адресу.

Публічні IPv4-адреси являють собою адреси, на глобальному рівні маршрутизовані між маршрутизаторами інтернет-провайдерів (Internet Service Provider, ISP). Однак не всі доступні IPv4-адреси можна використовувати в Інтернеті. Є блоки адрес, звані приватними адресами, які в більшості компаній призначаються в якості IPv4-адрес внутрішніх вузлів.

В середині 1990-х через вичерпання адресного простору IPv4 були введені приватні IPv4-адреси. Приватні IPv4-адреси не є чимось унікальним і можуть використовуватися у внутрішній мережі.

Зокрема, блоками приватних адрес є:

10.0.0.0 / 8 або від 10.0.0.0 до 10.255.255.255

172.16.0.0 / 12 або від 172.16.0.0 до 172.31.255.255

192.168.0.0 / 16 або від 192.168.0.0 до 192.168.255.255

Важливо знати, що адреси в цих блоках адрес не припустимі для використання в Інтернеті і повинні фільтрувати (відхилятися) інтернет-маршрутизаторами. Наприклад, на цьому малюнку користувачі мережі 1, 2 або 3 відправляють пакети на віддалені вузли призначення. Маршрутизатор ISP бачитимуть, що IPv4-адреси джерела в цих пакетах є приватними, і тому будуть відхиляти пакети.

Більшість організацій використовує приватні IPv4-адреси для своїх внутрішніх вузлів. Однак ці адреси RFC 1918 НЕ маршрутизируются в Інтернеті і повинні бути перетворені в публічні IPv4-адреси. Перетворення мережевих адрес (Network Address Translation, NAT) використовується для перетворення приватного IPv4-адреси в публічний IPv4-адрес. Це зазвичай виконується на маршрутизаторі, який забезпечує з'єднання між внутрішньою мережею і мережею ISP.

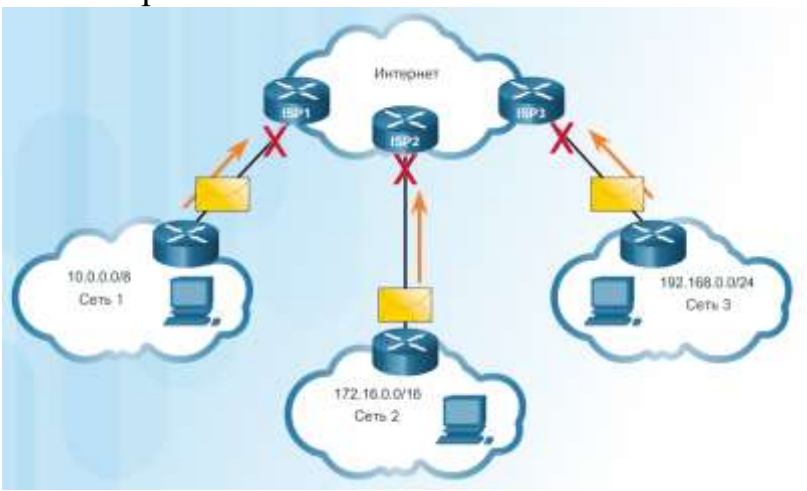


Рис. 2.1.11 локальні адреси не мають виходу в глобальну мережу

Домашні маршрутизатори виконують ту ж функцію. Наприклад, більшість домашніх маршрутизаторів призначають IPv4-адреси своїм провідним і бездротовим вузлам на основі приватного адреси 192.168.1.0 / 24. Інтерфейсу домашнього маршрутизатора, який підключається до мережі ISP, призначається публічний IPv4-адрес для його використання в Інтернеті.

Деякі адреси (наприклад, мережеві і широкомовні) не можна призначати вузлам. Також є особливі адреси, які можна призначати вузлам, але з обмеженнями способів взаємодії цих вузлів в мережі.

Адреси loopback (127.0.0.0 / 8 або від 127.0.0.1 до 127.255.255.254): частіше визначаються як тільки одну адресу 127.0.0.1 - це особливі адреси, які використовують вузли, щоб направляти трафік самим собі. Наприклад, вони можуть використовуватися вузлом, щоб перевірити працездатність конфігурації TCP / IP, як показано на малюнку. Подивіться, як адреса loopback 127.0.0.1 відповідає на exo-запит. Також зверніть увагу, як будь-яку адресу в цьому блоці адрес повертає пакет на локальний вузол (наприклад, див. Процес відправки другої команди ping на малюнку).

Локальні адреси каналу (169.254.0.0 / 16 або від 169.254.0.1 до 169.254.255.254) більш відомі як адреси, які призначаються за допомогою автоматичного призначення приватних IP-адрес (Automatic Private IP Addressing, APIPA). Вони використовуються клієнтом Windows DHCP для самостійної конфігурації в разі, якщо жоден DHCP-сервер не доступний. Підходять для невеликої тимчасової мережі.

Адреси TEST-NET (192.0.2.0/24 або від 192.0.2.0 до 192.0.2.255) використовуються виключно з метою навчання і можуть використовуватися в якості прикладу для документування при створенні мереж.

Примітка. У блоці адрес від 240.0.0.0 до 255.255.255.254 є експериментальні адреси, які відповідно до документа RFC 3330, можуть бути в майбутньому перетворені в доступні адреси.

У 1981 р IPv4-адреси в мережі Інтернет призначалися за допомогою класової адресації згідно RFC 790 (Призначені адреси). Замовникам був призначений мережеву адресу на основі одного з трьох класів, A, B або C. Відповідно до стандарту RFC, діапазони індивідуальних адрес діляться на наступні класи:

Клас A (від 0.0.0.0/8 до 127.0.0.0/8) розроблений для дуже великих мереж з більш ніж 16 млн адрес вузлів. Для позначення мережевого адреси IPv4-адреси класу A використовували фіксований префікс / 8 з першим октетом. Решта три октету використовувалися для адрес вузлів. Всі адреси класу A вимагають, щоб найстарший розряд старшого октету дорівнював нулю. Це означає, що існувало тільки 128 можливих мереж класу A. Клас A показаний на рис. 1.

Клас B (128.0.0.0 / 16 - 191.255.0.0 / 16) розроблений для підтримки потреб невеликих і великих мереж, що містять приблизно 65 000 вузлів. Адреса класу B використовував фіксований префікс / 16, два старших октету для позначення мережевого адреси. Два октету визначали адреси вузлів. Для адрес класу B два найстарших розряду старшого октету рівні 10, що забезпечує можливість створення більше 16 000 мереж. Клас B показаний на рис. 2.

Клас C (192.0.0.0 / 24 - 223.255.255.0 / 24) призначений для невеликих мереж з кількістю вузлів не більше 254. Блоки адрес класу C використовували префікс / 24 для трьох старших октетів для вказівки адреси мережі і останній октет - для вказівки адрес вузлів . Три старших біта старшого октету рівні 110, що забезпечує можливість створення більш 2 млн мереж. Клас C показаний на рис. 3.

Примітка. Також є блок одноадресної передачі класу D (від 224.0.0.0 до 239.0.0.0) і блок експериментальних адрес класу E (від 240.0.0.0 до 255.0.0.0).

Як показано на малюнку, по класовій адресації 50% доступних IPv4-адрес виділялося 128 мереж класу A, 25% адрес - мереж класу B, і решта 25% - мереж класів C, D і E. Проблема полягала в тому, що велика кількість адрес не використовувалося, і доступність IPv4-адрес була дуже обмеженою. Не всі вимоги організацій можна без проблем віднести до цих трьох класів. Наприклад, компанії, в мережі якої знаходиться 260 вузлів, буде потрібно мати адресу класу B з понад 65 000 адресами, при цьому 64 740 адрес пропадуть дарма.

В кінці 1990-х класова адресація була замінена більш нової і актуальної безкласової системою адресації. Проте, в деяких мережах донині застосовується класова адресація. Наприклад, при призначенні комп'ютера IPv4-адреси операційна система перевіряє присвоюється адреса, щоб визначити, до якого класу належить ця адреса: A, B або C. Потім операційна система бере префікс, який використовується цим класом, і призначає маску підмережі за замовчуванням.

Використовувана в даний час система називається безкласової адресацією. Офіційна назва - безкласову міждоменну маршрутизацію (Classless Inter-Domain Routing, CIDR; вимовляється як «сайдр»). У 1993 р організація IETF (Інженерна група з розвитку Інтернету) створила нові стандарти, які дозволили

операторам зв'язку призначати IPv4-адреси в будь-яких бітових межах (мається на увазі довжина префікса) замість адрес класу A, B або C. Це повинно було відстрочити вичерпання IPv4-адрес.

Рис. 2.1.12 Схема розподілу кількості мереж і хостів у різних класах

У IETF розуміли, що безкласову міждоменну маршрутизацію (CIDR) була тільки тимчасовим рішенням і для підтримки швидкого розвитку кількості користувачів Інтернету необхідний новий IP-протокол. У 1994 р в IETF почалися пошуки наступника IPv4. Ним став протокол IPv6.

Для підтримки мережних вузлів, наприклад, веб-серверів, доступних через Інтернет, компанія повинна мати блок призначених публічних адрес. Як ви пам'ятаєте, публічні адреси повинні бути унікальними, а використання цих публічних адрес регулюється і призначається окремо для кожної організації. Це вірно як для IPv4-, так і для IPv6-адрес.

Призначення IPv4- і IPv6-адрес регулюється Адміністрацією адресного простору Інтернет (IANA) (http://www.iana.org). IANA управляє блоками IP-адрес і розподіляє їх між регіональними інтернет-реєстраторами (RIR). Натисніть на символ кожного регіонального інтернет-реєстратора (RIR) на малюнку, щоб переглянути додаткову інформацію.

Регіональні інтернет-реєстратори (RIR) відповідають за розподіл IP-адрес між інтернет-провайдерами (ISP), які, в свою чергу, надають блоки IPv4-адрес організаціям і менш великим провайдерам. Організації можуть отримати свої адреси безпосередньо від регіональних інтернет-реєстраторів (RIR) (в залежності від правил конкретного регіонального інтернет-реєстратора (RIR)).

Протокол IPv6 був розроблений як наступник протоколу IPv4. IPv6 має більшу 128-бітове адресний простір, що досить для 340 ундецілліонов адрес. (Це число 340, за яким слід 36 нулів.) Однак протокол IPv6 - це не тільки більшу кількість адрес. Коли фахівці IETF почали розробку наступника IPv4, вони використовували цю можливість для усунення обмежень протоколу IPv4 і внесення додаткових поліпшень. Серед таких поліпшень - протокол керуючих

повідомлень версії 6 (ICMPv6), який включає в себе дозвіл адрес і автонастройку адрес, що було відсутнє в протоколі ICMP для IPv4 (ICMPv4). Протоколи ICMPv4 і ICMPv6 будуть розглянуті далі в цій главі.

Скорочення адресного простору протоколу IPv4 - основний стимулюючий чинник для переходу до використання IPv6. У міру того як Африка, Азія і інші регіони планети все більше потребують підключення до мережі Інтернет, залишається все менше IPv4-адрес, щоб відповідати таким темпам розвитку. Як показано на малюнку, у чотирьох з п'яти регіональних інтернет-реєстраторів (RIR) не залишилося вільних IPv4-адрес.

Теоретичне максимальну кількість IPv4-адрес - 4,3 мільярда. Приватні адреси разом з механізмом перетворення мережевих адрес (NAT) дозволяли якийсь час уповільнити процес виснаження адресного простору IPv4. Однак, механізм перетворення мережевих адрес (NAT) має певні обмеження, які погіршують комунікації в тимчасової мережі.

Сучасний Інтернет істотно відрізняється від Інтернету останніх десятиліть. Сьогодні це не просто електронна пошта, веб-сторінки і передача файлів між комп'ютерами. У міру розвитку Інтернет стає Інтернетом речей. Скоро можна буде отримати доступ до Інтернету не тільки через комп'ютери, планшети і смартфони. Завтра практично всі пристрої - від автомобілів і біомедичного обладнання до побутової техніки і природної екосистеми буду оснащені сенсорами і підключені до Інтернету.

У зв'язку з поширенням Інтернету обмеженим адресним простором IPv4, проблемами з перетворенням мережевих адрес і проникненням Інтернету в наше життя прийшло час для переходу на протокол IPv6.

Точної дати для переходу на протокол IPv6 немає. У найближчому майбутньому протоколи IPv4 і IPv6 будуть існувати спільно. Повний перехід може зайняти багато років. Фахівці IETF створили різні протоколи і інструменти, які дозволяють мережевим адміністраторам поступово переводити свої мережі на протокол IPv6. Методи переходу можна розділити на 3 категорії.

Подвійний стек: як показано на рис. 1, подвійний стек дозволяє протоколам IPv4 і IPv6 співіснувати в одному і тому ж сегменті мережі. Пристрої з подвійним стеком одночасно працюють з протокольними стеками IPv4 і IPv6.

Туннелирование: як показано на рис. 2, туннелирование - це спосіб передачі пакета IPv6 через IPv4-мережу. IPv6-пакет инкапсулируется всередині IPv4-пакета, як і інші типи даних.

Перетворення: як показано на рис. 3, перетворення мережевих адрес 64 (NAT64) дозволяє пристроям під керуванням IPv6 обмінюватися даними з пристроями під керуванням IPv4 за допомогою методу перетворення, схожого на метод перетворення NAT для IPv4. IPv6-пакет перетворюється в пакет IPv4-пакет і навпаки.

Примітка. Туннелирование і перетворення використовуються тільки при необхідності. Кінцева мета - це природний обмін даними в форматі IPv6 між джерелом і призначенням.

Довжина IPv6-адрес становить 128 біт, написаних у вигляді рядка шістнадцятирічних значень. Кожні 4 біта представлені однією шістнадцятковій цифрою, причому загальна кількість шістнадцяткових значень дорівнює 32, як

показано на рис. 1. IPv6-адреси не чутливі до регістру, їх можна записувати як малими, так і великими літерами.

Кращий формат запису IPv6-адреси: x: x: x: x: x: x: x: x, де кожен «x» складається з чотирьох шістнадцятирічних цифр. Октети - це термін, який використовується для позначення 8 біт IPv4-адреси. В IPv6-адреси сегмент з 16 біт або чотирьох шістнадцятирічних цифр неофіційно називають гекстетом. Кожен «x» - це 1 гекстет, 16 біт або 4 шістнадцяткові цифри.

Переважний формат означає, що IPv6-адреса записана за допомогою 32 шістнадцяткових цифр. Тим не менш, це не найоптимальніший спосіб представлення IPv6-адреси. Нижче ми побачимо два правила, які допоможуть скоротити кількість цифр, необхідних для подання IPv6-адреси.

Правило 1. Пропуск початкових нулів

Предпочитаемый формат	2001:0DB8:0000:1111:0000:0000:0000:0200
Без начальных нулей	2001:DB8:0:1111:0:0:0:200

Рис. 2.1.13 правило пропуску нулів

Перше правило для скорочення запису IPv6-адрес - пропуск усіх початкових 0 (нулів) в шістнадцятковій запису. наприклад:

- 01AB можна уявити як 1AB
- 09F0 можна уявити як 9F0
- 0A00 можна уявити як A00
- 00AB можна уявити як AB

Це правило застосовується тільки до початкових нулях, а НЕ до кінцевих, інакше адреса буде незрозумілий. Наприклад, гекстет «ABC» може бути представлений як «0ABC», або як «ABC0» (а це різні значення).

Правило 2. Пропуск всіх нульових сегментів

Друге правило для скорочення запису адрес IPv6 полягає в тому, що подвійна двокрапка (: :) може замінити будь-яку єдину, суміжну рядок одного або декількох 16-бітних сегментів (гекстетов), що складаються з нулів.

Подвійна двокрапка (: :) може використовуватися в адресі лише один раз, в іншому випадку в результаті може виникнути декілька адрес. Поєднання цього правила з методом пропуску нулів допомагає значно скоротити запис IPv6-адреси. Зазвичай це називається стиснутим форматом.

Предпочитаемый формат	2001:0DB8:0000:1111:0000:0000:0000:0200
Без начальных нулей	2001:DB8:0:1111:0:0:0:200
Сжатый формат	2001:DB8:0:1111::200

Рис. 2.1.14 Правило пропускання нулів та їх запис

Неправильна адреса:
2001: 0DB8 :: ABCD :: 1234

Можливі розшифровки адрес, неоднозначно записаних в стислому форматі:

- 2001: 0DB8 :: ABCD: 0000: 0000: 1234
- 2001: 0DB8 :: ABCD: 0000: 0000: 0000: 1234
- 2001: 0DB8: 0000: ABCD :: 1234
- 2001: 0DB8: 0000: 0000: ABCD :: 1234

Існує три типи IPv6-адрес.

Індивідуальний (або одноадресної розсилки, unicast): служить для однозначного визначення інтерфейсу на пристрої під управлінням протоколу IPv6. Як показано на малюнку, IPv6-адреса джерела повинен бути індивідуальним.

Груповий (або під LGPL, multicast): використовується для відправки одного IPv6-пакета на кілька адрес призначення.

Довільний (або довільної розсилки, anycast): будь-яке індивідуальне IPv6-адреса, який може бути призначений декільком пристроям. Пакет, що відправляється на адресу довільній розсилки, направляється до найближчого пристрою до цієї адреси. Довільні адреси в даному курсі не розглядаються.

На відміну від IPv4, IPv6 не використовує широкомовний адресу. Однак є груповий IPv6-адреса для всіх вузлів, що дає аналогічний результат.

Як ви пам'ятаєте, префікс, або мережева частина адреси IPv4, може бути позначений маскою підмережі в десятковому форматі з розділовими точками або довжиною префікса (запис з похилою рискою). Наприклад, IPv4-адрес 192.168.1.10 з маскою підмережі в десятковому форматі з розділовими точками 255.255.255.0 еквівалентний запису 192.168.1.10/24.

Рис. 2.1.15

Протокол IPv6 використовує довжину префікса для позначення префіксної частина адреси. IPv6 не використовує для маски підмережі десяткове подання з розділовими точками. Довжина префікса позначає мережну частину IPv6-адреси за допомогою адреси або довжини префікса IPv6.

Діапазон довжини префікса може становити від 0 до 128. Традиційна довжина IPv6-префікса для локальних (LAN) та інших типів мереж - / 64. Це означає, що довжина префікса, або мережева частина адреси, становить 64 біта, а що залишилися 64 біта залишаються для ідентифікатора інтерфейсу (вузловий частини) адреси.

Індивідуальний адреса служить для однозначного визначення інтерфейсу пристрою під керуванням протоколу IPv6. Пакет, який відправляється на таку

адресу, буде отримано інтерфейсом, призначеним для цієї адреси. Як і у випадку з протоколом IPv4, IPv6-адреса має бути індивідуальним. IPv6-адреса призначення може бути як індивідуальним, так і груповим.

Найбільш поширеними типами індивідуальних IPv6-адрес є глобальні індивідуальні адреси (global unicast addresses, GUA) і локальні адреси каналу.

Глобальний індивідуальну адресу аналогічний публічного IPv4-адресою. Ці адреси, до яких можна прокласти маршрут по Інтернету, є унікальними по всьому світу. Глобальні індивідуальні адреси можуть бути налаштовані статично або привласнені динамічно.

Локальні адреси каналу використовуються для обміну даними з іншими пристроями по одному локальному каналу. У протоколі IPv6 термін «канал» означає сіть. Локальні адреси каналів обмежені одним каналом. Вони повинні бути унікальні тільки в рамках цього каналу, оскільки поза каналу до них не можна прокласти маршрут. Іншими словами, маршрутизатори не зможуть пересилати пакети, маючи локальну адресу каналу джерела або призначення.

Іншим типом індивідуальної адреси є унікальний локальний індивідуальну адресу. Унікальні локальні IPv6-адреси мають деякі спільні особливості з приватними адресами RFC 1918 для IPv4, але при цьому між ними є й істотні відмінності. Унікальні локальні адреси використовуються для локальної адресації в межах вузла або між обмеженою кількістю вузлів. Ці адреси не слід маршрутизировать в глобальному протоколі IPv6 і перетворювати в глобальний IPv6-адреса. Унікальні локальні адреси знаходяться в діапазоні від FC00 :: / 7 до FDFF :: 7.

У випадку з IPv4 приватні адреси об'єднані з перетворенням мережевих портів і адрес (NAT / PAT) для забезпечення перетворення адрес з приватних в публічні. Це пов'язано з обмеженим адресним простором IPv4. Багато сайтів використовують приватні адреси RFC 1918 року, щоб забезпечити безпеку або захистити мережу від потенційних загроз. Однак забезпечення безпеки ніколи не було метою технологій NAT / PAT, тому організація IETF завжди рекомендувала приймати відповідні запобіжні заходи при використанні маршрутизаторів в Інтернеті. Унікальні локальні адреси можуть використовуватися для пристроїв, яким ніколи не знадобиться використання інших мереж або отримання з них даних.

Локальний IPv6-адреса каналу забезпечує обмін даними з іншими пристроями з включеним протоколом IPv6 в тому ж каналі (підмережі) і тільки в ньому. Пакети з локальною адресою каналу джерела або призначення не можуть бути спрямовані за межі каналу, в якому створюється пакет.

Глобальний індивідуальний адреса не обов'язкова. Проте, кожен IPv6-сумісний мережевий інтерфейс повинен мати локальний адресу каналу.

Якщо локальний адресу каналу не налаштований вручну на інтерфейсі, пристрій автоматично створює його самостійно, не звертаючись до DHCP-сервера. Вузли під керуванням IPv6 створюють локальний IPv6-адреса каналу навіть в тому випадку, якщо пристрої не був призначений глобальний індивідуальний IPv6-адреса. Це дає їм змогу під керуванням IPv6 обмінюватися даними з іншими пристроями під керуванням IPv6 в одній підмережі, в тому числі зі шлюзом за замовчуванням (маршрутизатором).

Локальні IPv6-адреси каналу знаходяться в діапазоні FE80 :: / 10. / 10 вказує, що перші 10 бітів - 1111 1110 10xx xxxx. Діапазон значень першого гекстета: від 1111 1110 1000 0000 (FE80) до 1111 1110 1011 1111 (FEBF).

Глобальні індивідуальні IPv6-адреси (GUA) унікальні по всьому світу і доступні для маршрутизації через Інтернет IPv6. Ці адреси еквівалентні публічним IPv4-адрес. Корпорація з управління доменними іменами і IP-адресами (Internet Committee for Assigned Names and Numbers, ICANN), оператор Адміністрації адресного простору Інтернет (IANA) виділяє блоки IPv6-адрес п'яти регіональним інтернет-реєстраторам (RIR). В даний час призначаються тільки глобальні індивідуальні адреси з першими трьома бітами 001 або 2000 :: / 3. Іншими словами, перша шістнадцяткова цифра адреси GUA починається з 2 або 3. Це лише 1/8 від всього доступного адресного простору IPv6, за винятком дуже незначної кількості інших типів адрес індивідуальних і групових адрес.

Примітка. Адреса 2001: 0DB8 :: / 32 зарезервований для документації, в тому числі в для використання в прикладах.

Глобальний індивідуальну адресу складається з трьох частин.

- Префікс глобальної маршрутизації
- ідентифікатор підмережі
- ідентифікатор інтерфейсу
- Префікс глобальної маршрутизації

Префікс глобальної маршрутизації - це префіксально або мережева частина адреси, що призначається інтернет-провайдером замовнику або вузлу. Зазвичай / 48 є префіксом глобальної маршрутизації, який інтернет-реєстратори призначають своїм замовникам: як корпоративних мереж, так і індивідуальним користувачам.

Розмір префікса глобальної маршрутизації визначає розмір ідентифікатора підмережі.

Ідентифікатор підмережі використовується організаціями для позначення підмереж на своєму сайті. Чим вище значення ідентифікатора підмережі, тим більше існує підмереж.

Рис. 2.1.16 Ідентифікатор мережі

Ідентифікатор IPv6-інтерфейсу еквівалентний вузловий частини IPv4-адреси. Термін «ідентифікатор інтерфейсу» використовується в тому випадку, коли один вузол може мати кілька інтерфейсів, кожен з яких має один або більше IPv6-адрес. Настійно рекомендується в більшості випадків

використовувати підмережі / 64. Іншими словами, 64-бітний ідентифікатор інтерфейсу, як показано на малюнку 2.

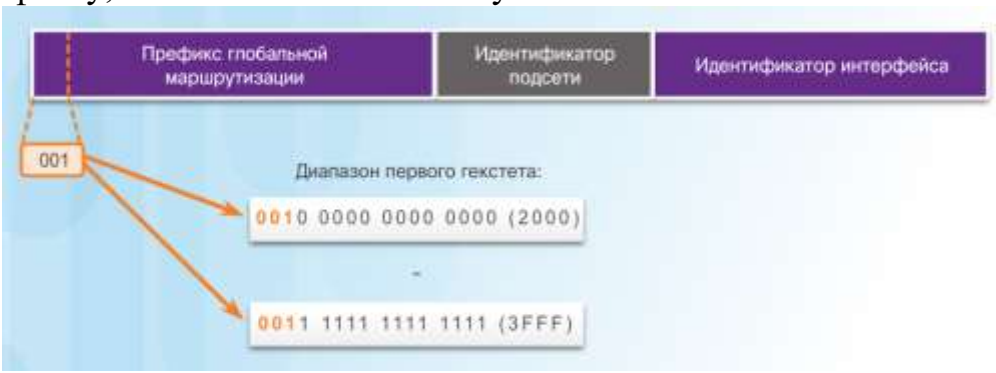


Рис. 2.1.17

Примітка. На відміну від IPv4, при використанні протоколу IPv6 пристрою можна призначити адресу вузла, що складається з одних 0 або з одних 1. Адреса з одних 1 можна використовувати з тієї причини, що в протоколі IPv6 не використовуються широкомовні адреси. Можна також використовувати адресу з одних 0, але він зарезервований як адреса довільної розсилки маршрутизатора підмережі, і його слід призначати тільки маршрутизаторів.

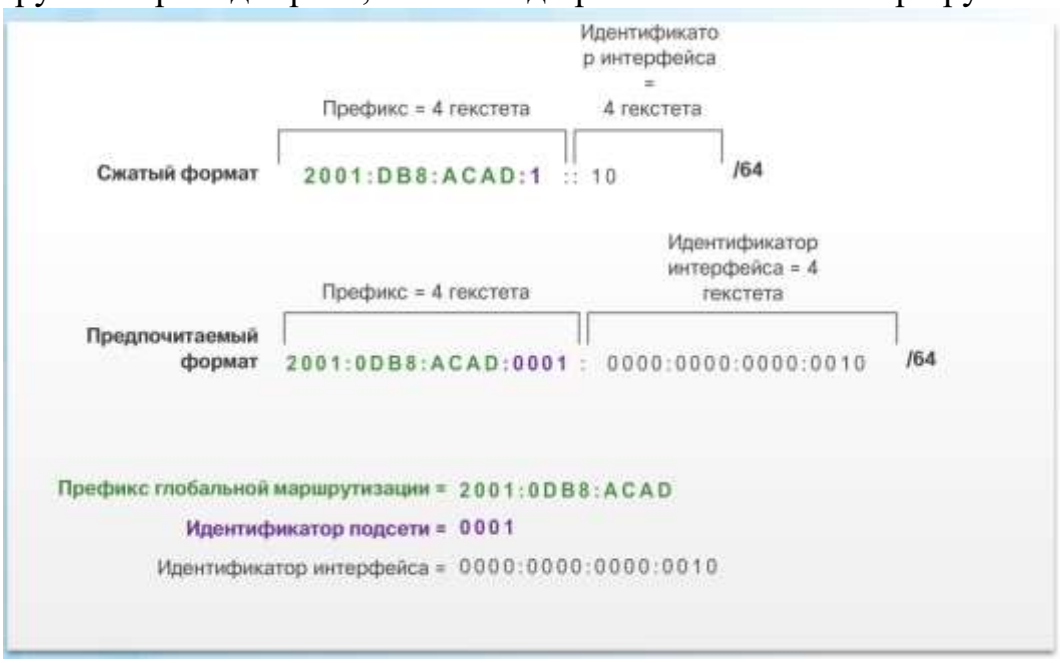


Рис. 2.1.18

Найпростіший спосіб прочитати більшість IPv6-адрес - підрахувати кількість гекстетов. Як показано на рис. 3, в глобальному індивідуальному адресу з префіксом / 64 перші чотири гекстета позначають мережеву частину адреси, а четвертий гекстет - ідентифікатор підмережі. Решта чотири гекстета використовуються для ідентифікатора інтерфейсу.

Більшість команд конфігурації і перевірки IPv6-мережі в операційній системі Cisco IOS схожі на свої аналоги для IPv4-мережі. У багатьох випадках єдина відмінність між ними - використання в командах ipv6 замість ip.

Для настройки глобального індивідуального IPv6-адреси в інтерфейсі використовується команда ipv6 address ipv6-address / prefix-length.

Зверніть увагу на відсутність пробілів всередині ipv6-address і prefix-length.

Для прикладу налаштування використовується топологія, показана на рис. 1, і такі IPv6-підмережі:

- 2001: 0DB8: ACAD: 0001: / 64 (або 2001: DB8: ACAD: 1 :: / 64)
- 2001: 0DB8: ACAD: 0002: / 64 (або 2001: DB8: ACAD: 2 :: / 64)
- 2001: 0DB8: ACAD: 0003: / 64 (або 2001: DB8: ACAD: 3 :: / 64)

Як показано на рис. 2, для настройки індивідуального глобального IPv6-адреси в інтерфейсах GigabitEthernet 0/0, GigabitEthernet 0/1 і Serial 0/0/0 маршрутизатора R1 використовуються наступні команди:

Ручна настройка IPv6-адреси на вузлі аналогічна настройці IPv4-адреси.

Адреса шлюзу, налаштований на комп'ютер PC1, - це 2001: DB8: ACAD: 1 :: 1. Це глобальний індивідуальну адресу інтерфейсу маршрутизатора R1 GigabitEthernet в одній мережі. Крім того, адреса шлюзу може збігатися з локальною адресою каналу інтерфейсу GigabitEthernet. Припустимо будь-який з цих варіантів настройки.

Скористайтеся інструментом перевірки синтаксису (рис. 3), щоб налаштувати глобальний індивідуальний IPv6-адреса.

Як і у випадку з IPv4, настройка статичних адрес для клієнтів не поширюється на великі мережі. Саме тому більшість мережевих адміністраторів IPv6-мережі будуть призначати IPv6-адреси динамічно.

Пристрій може автоматично отримувати глобальний індивідуальний IPv6-адреса двома способами.

Автоматична настройка без збереження стану адреси (Stateless Address Autoconfiguration, SLAAC).

Адресація DHCPv6 з урахуванням станів.

Примітка. Якщо використовується DHCPv6 або SLAAC, локальний адресу каналу локального маршрутизатора автоматично вказується як адреса шлюзу.

Динамічна конфігурація глобального індивідуального адреси за допомогою SLAAC

SLAAC - це спосіб, який дозволяє пристрою отримати свій префікс, довжину префікса і адреса шлюзу від IPv6-маршрутизатора без допомоги DHCPv6-сервера. При використанні SLAAC пристрої отримують всю необхідну інформацію з повідомлень Router Advertisement (RA) від ICMPv6-маршрутизатора.

IPv6-маршрутизатори кожні 200 секунд відправляють повідомлення RA ICMPv6 всіх пристроїв в мережі під управлінням IPv6. На вузол, який відправив повідомлення RS ICMPv6, також відправляється відповідь було надіслане RA.

IPv6-маршрутизація не включена за замовчуванням. Щоб маршрутизатор працював як IPv6-маршрутизатор, необхідно використовувати команду глобального конфігурування ipv6 unicast-routing.

Примітка. IPv6-адреси можуть бути налаштовані на маршрутизаторі, що не є IPv6-маршрутизатором.

Повідомлення RA ICMPv6 вказує IPv6-пристрою, як йому отримати інформацію по адресації. Остаточне рішення залежить від операційної системи пристрою. Повідомлення RA ICMPv6 включає наступну інформацію.

Префікс мережі і довжину префікса: повідомляють пристрою, до якої мережі воно відноситься.

Адреса шлюзу: локальний IPv6-адреса каналу, IPv6-адреса джерела повідомлення RA.

DNS-адресу та ім'я домену: адреси DNS-серверів і ім'я домену.

Повідомлення RA може виглядати наступним чином.

- Варіант 1: тільки SLAAC.
- Варіант 2: SLAAC і DHCPv6 без збереження станів.
- Варіант 3: Динамічний DHCPv6 зі збереженням станів (без SLAAC).
- RA, варіант 1: SLAAC

За замовчуванням повідомлення RA пропонує приймаючому пристрою використовувати дані в повідомленні RA для створення власного глобального індивідуального IPv6-адреси і отримання іншої інформації. Участь DHCPv6-сервера не потрібно.

SLAAC не припускав збереження стану, що означає відсутність центрального сервера (наприклад, DHCPv6-сервера, що запам'ятовує стану адрес), що виділяє глобальні індивідуальні адреси і зберігає список пристроїв і їх адрес. У разі застосування SLAAC клієнтський пристрій використовує інформацію в повідомленні RA для створення власного глобального індивідуальної адреси. Як показано на рис. 2, дві частини адреси створюються в такий спосіб:

Префікс: вказується в повідомленні RA

Ідентифікатор інтерфейсу: створюється або за допомогою розширеного унікального ідентифікатора EUI-64, або шляхом створення випадкового 64-бітного числа.

За замовчуванням повідомлення RA відправляють відповідно до варіанту 1 (тільки SLAAC). Інтерфейс маршрутизатора може бути налаштований на відправку оголошень маршрутизатора за допомогою SLAAC і DHCPv6-сервера без збереження стану адрес (або тільки DHCPv6-сервера зі збереженням стану адрес).

RA, варіант 2: SLAAC і DHCPv6-сервер без збереження стану адрес

У цьому варіанті повідомлення RA вказує пристрою використовувати:

SLAAC для створення власного глобального індивідуального IPv6-адреси.

Локальний адреса каналу маршрутизатора, IPv6-адреса джерела RA, як адресу шлюзу.

DHCPv6-сервер, що не зберігає стану адрес, для отримання іншої інформації, такої як адреса DNS-сервера і ім'я домену.

DHCPv6-сервер без збереження стану адрес розподіляє адреси DNS-серверів і імена доменів. Він не виділяє глобальні індивідуальні адреси.

RA, варіант 3: DHCPv6-сервер зі збереженням стану адрес

DHCPv6-сервер зі збереженням стану адрес аналогічний DHCP-сервера в системі IPv4. За допомогою служб DHCPv6-сервера зі збереженням стану адрес пристрій може автоматично отримувати дані адреси, включаючи глобальний індивідуальну адресу, довжину префікса і адреси DNS-серверів.

У цьому варіанті повідомлення RA вказує пристрою використовувати:

Локальний адреса каналу маршрутизатора, IPv6-адреса джерела RA в якості адреси шлюзу за замовчуванням.

DHCPv6-сервер зі збереженням стану адрес для отримання глобального індивідуального адреси, адреса DNS-сервера, ім'я домену та іншу необхідну інформацію.

DHCPv6-сервер зі збереженням стану адрес виділяє і веде список пристроїв і призначених їм IPv6-адрес. DHCP-сервер в IPv4-мережі зберігає стану адрес.

Примітка. Адреса шлюзу може бути отриманий тільки динамічно з повідомлення RA. DHCPv6-сервер, незалежно від того, чи зберігає він стану адрес чи ні, не надає адресу шлюзу.

Процес EUI-64 і випадково згенерований ідентифікатор інтерфейсу

Якщо повідомлення RA має тип SLAAC або SLAAC + для DHCPv6-сервера без збереження стану адрес, клієнт повинен генерувати власний ідентифікатор інтерфейсу. Клієнт отримує з повідомлення RA префіксних частина адреси, але повинен створити власний ідентифікатор інтерфейсу. Ідентифікатор інтерфейсу може бути створений за допомогою EUI-64 або являти собою випадково сгенерированное 64-бітове число, як показано на рис. 1.

Процес EUI-64

Організація IEEE розробила розширений унікальний ідентифікатор (Extended Unique Identifier, EUI) або змінений процес EUI-64. Цей процес використовує 48-бітний MAC-адресу Ethernet клієнта і в середину цієї адреси вставляє ще 16 біт для створення 64-бітного ідентифікатора інтерфейсу.

MAC-адреси Ethernet зазвичай мають шістнадцятковий формат і складаються з двох частин.

Унікальний ідентифікатор організації (Organizationally Unique Identifier, OUI) - це 24-бітний (шість шістнадцяткових цифр) код постачальника, призначений IEEE.

Ідентифікатор пристрою - це унікальне 24-бітове (шість шістнадцяткових цифр) значення із загальним унікальним ідентифікатором організації (OUI).

Ідентифікатор інтерфейсу EUI-64 має двійковий формат і складається з трьох частин.

24-бітний OUI на основі MAC-адреси клієнта, в якому сьомий біт (універсально / локальний (U / L) біт) є зворотним, тобто якщо сьомий біт має значення 0, то він стає 1, і навпаки.

В середину вставляється 16-бітове значення FFFE (в шістнадцятковому форматі).

24-бітний ідентифікатор пристрою на основі MAC-адреси клієнта.

Процес EUI-64 проілюстрований на рис. 2 за допомогою MAC-адреси маршрутизатора R1 GigabitEthernet FC99: 4775: CEE0.

Крок 1.Разделіте MAC-адресу між OUI і ідентифікатором пристрою.

Крок 2. Вставте шістнадцяткове значення FFFE в довічним форматі 1111 1111 1111 1110.

Крок 3. Перетворіть перші 2 шістнадцяткових значення OUI в двійковий формат і відобразіть біт U / L (біт 7). В даному прикладі 0 в сьомому бите змінюється на одиницю.

В результаті генерується наступний EUI-64 ідентифікатор інтерфейсу FE99: 47FF: FE75: CEE0.

Примітка. Використання зворотного біта (U / L) і причини дзеркального відображення його значення описані в документі RFC 5342.

Глобальний індивідуальний IPv6-адреса PCA, динамічно створений за допомогою SLAAC і процесу EUI-64. Найпростіший спосіб визначити, чи дійсно адреса був створений за допомогою EUI-64, - перевірити, чи є в середині ідентифікатора інтерфейсу значення FFFE, як показано на рис. 3.

Перевага EUI-64 MAC-адреси Ethernet полягає в тому, що його можна використовувати для визначення ідентифікатора інтерфейсу. Крім того, мережеві адміністратори можуть легко відстежувати IPv6-адреса до кінцевих пристроїв за допомогою унікального MAC-адреси. Однак це турбує інших користувачів у зв'язку з загрозою їх конфіденційності. Вони стурбовані тим, що їх пакети можна відстежити до фізичного комп'ютера. Щоб уникнути таких побоювань можна використовувати випадково згенерований ідентифікатор інтерфейсу.

Що випадково згенерували ідентифікатори інтерфейсу

Залежно від операційної системи пристрій може використовувати випадково згенерований ідентифікатор інтерфейсу замість MAC-адрес і EUI-64. Наприклад, починаючи з Windows Vista в операційних системах Windows використовується випадково згенерований ідентифікатор інтерфейсу замість створеного через EUI-64. В ОС Windows XP і в попередніх операційних системах Windows використовувався EUI-64.

Після створення ідентифікатора інтерфейсу або за допомогою EUI-64, або через випадкову генерацію його можна об'єднати з префіксом IPv6 з повідомлення RA для створення глобального індивідуального адреси, як показано на рис. 4.

Примітка. Щоб забезпечити унікальний індивідуальний IPv6-адреса клієнт може використовувати процес виявлення дубльованих адрес (Duplicate Address Detection, DAD). Це аналогічно ARP-запиту власного адреси. Відсутність відповідного повідомлення означає, що адреса унікальний.

Все IPv6-пристрої повинні мати локальні IPv6-адреси каналу. Локальний адреса каналу може бути створений динамічно або налаштований вручну як статичний локальну адресу каналу.

Локальний адресу каналу динамічно створюється за допомогою префікса FE80 :: / 10 і отриманого за допомогою процесу EUI-64 або випадково згенерованого 64-бітного ідентифікатора інтерфейсу. Як правило, операційні системи, застосовують один і той же метод до глобальних індивідуальним адресами, створеним за допомогою SLAAC, і динамічно призначеним адресами каналу, як показано на рис. 2.

Маршрутизатор Cisco автоматично створюють локальний IPv6-адреса каналу після призначення інтерфейсу глобального індивідуальної адреси. За замовчуванням маршрутизатори Cisco IOS використовують процес EUI-64 для створення ідентифікатора інтерфейсу для всіх локальних адрес каналу в IPv6-інтерфейси. Для послідовних інтерфейсів маршрутизатор буде використовувати MAC-адресу інтерфейсу Ethernet. Нагадуємо, що локальний адресу каналу повинен бути унікальним тільки в даному каналі або мережі. Однак недолік використання динамічно призначеного локального адреси каналу - це занадто довгий індетіфікатор інтерфейсу, що утруднює визначення і запам'ятовування

призначених адрес. На рис. 3 показаний MAC-адреса інтерфейсу GigabitEthernet 0/0 маршрутизатора R1. Ця адреса використовується для динамічного створення локальних адрес каналу на одному інтерфейсі.

Щоб було легше впізнавати і запам'ятовувати ці адреси на маршрутизаторах, зазвичай виконується статична настройка локальних IPv6-адрес каналу на маршрутизаторах.

Ручна настройка локальної адреси каналу дозволяє створювати адреса, який легше дізнатися і запам'ятати. Як правило, достатньо створити розпізнаються локальні адреси на маршрутизаторах. Це зручно тому, що локальні адреси маршрутизаторів використовуються як адреси шлюзу за замовчуванням і в оголошеннях маршрутизації.

Локальні адреси каналів можна налаштовувати вручну за допомогою аналогічної команди, яка використовувалася для створення глобальних індивідуальних IPv6-адрес, але з додатковим параметром link-local. Якщо адреса починається з гекстета в діапазоні від FE80 до FEBF, то параметри локального каналу повинні слідувати за адресою.

Локальний адреса каналу FE80 :: 1 використовується для вказівки на те, що він належить маршрутизатора R1. Такий же локальний адресу каналу IPv6 налаштований на всіх інтерфейсах маршрутизатора R1. FE80 :: 1 можна налаштувати на кожному каналі, оскільки він повинен бути унікальним тільки на даному каналі.

Як і у випадку з маршрутизатором R1, маршрутизатор R2 буде налаштований з адресою FE80 :: 2 в якості локального адреси каналу IPv6 на всіх його інтерфейсах.

Команда для перевірки конфігурації IPv6-інтерфейсу схожа на аналогічну команду для IPv4.

Команда show interface відображає MAC-адресу інтерфейсів Ethernet. Процес EUI-64 використовує цей MAC-адресу для створення ідентифікатора інтерфейсу локальної адреси каналу. Крім того, команда show ipv6 interface brief відображає скорочені вихідні дані для кожного з інтерфейсів. Вихідні дані [up / up] в тому ж рядку, що і інтерфейс, відображають стан інтерфейсу 1-го і 2-го рівнів. Аналогічні дані відображаються в стовпцях Status (Стан) та Protocol (Протокол) при вихідних даних еквівалентної команди IPv4.

Зверніть увагу, що кожен інтерфейс має два IPv6-адреси. Друга адреса для кожного інтерфейсу - це глобальний індивідуальну адресу. Перша адреса, який починається з FE80, - це локальний індивідуальну адресу каналу для інтерфейсу. Як ви пам'ятаєте, локальний адресу каналу автоматично приєднується до інтерфейсу при призначенні глобального індивідуальної адреси.

Крім того, зверніть увагу, що послідовний локальну адресу маршрутизатора R1 0/0/0 ідентичний інтерфейсу GigabitEthernet 0/0. Послідовні інтерфейси не мають MAC-адрес Ethernet, тому операційна система Cisco IOS використовує MAC-адресу першого доступного інтерфейсу Ethernet. Це можливо з тієї причини, що локальні інтерфейси каналу повинні бути унікальними тільки на даному каналі.

Як правило, локальний адресу каналу інтерфейсу маршрутизатора - це адреса шлюзу для пристроїв в даному каналі або мережі.

Команду show ipv6 route можна використовувати для перевірки занесення в таблицю маршрутизації IPv6-мереж і IPv6-адрес конкретних інтерфейсів. Команда маршрут show ipv6 route відображає тільки мережі на основі протоколу IPv6, а не IPv4.

У таблиці маршрутизації буква C навпаки маршруту означає, що це мережа з прямим підключенням. Коли інтерфейс маршрутизатора налаштовується з глобальним індивідуальним адресою і знаходиться в активному стані (up / up), IPv6-префікс і довжина префікса додаються в таблицю IPv6-маршрутизації в якості підключеного маршруту.

Примітка. L вказує на локальний маршрут, т. Е. Певний IPv6-адреса, призначений інтерфейсу. Це не локальний адресу. Локальні адреси не включені в таблицю маршрутизації маршрутизатора, оскільки ці адреси не маршрутизації.

Глобальний індивідуальну адресу IPv6, що настроюється на інтерфейсі, також заноситься в таблицю маршрутизації в якості локального маршруту. Локальний маршрут має префікс / 128. Локальні маршрути використовуються таблицею маршрутизації для ефективної обробки пакетів з адресою призначення адреси інтерфейсу маршрутизатора.

Команда ping для IPv6 аналогічна такий же команді, використовуваної з протоколом IPv4. Як показано на рис. 3, ця команда використовується для перевірки підключення 3-го рівня між маршрутизатором R1 і PC1. При відправці луна-запиту на локальну адресу каналу з маршрутизатора операційна система Cisco IOS запросить у користувача відкрити вихідний інтерфейс. Оскільки локальний адресу каналу призначення може перебувати на одному або декількох каналах або мережах, маршрутизатора необхідно уточнити, на який інтерфейс відправляти луна-запит.

Групові IPv6-адреси аналогічні груповим IPv4-адрес. Як ви пам'ятаєте, груповий адреса використовується для відправки одного пакета по одному або декількох адресах призначення (групі під LGPL). Групові IPv6-адреси мають префікс FF00 :: / 8.

Примітка. Групові адреси можуть бути тільки адресами призначення, а не адресами джерела.

Існує два типи групових IPv6-адрес:

- Присвоєний груповий адресу.
- Групова адреса запитаного вузла.

Просування групові адреси зарезервовані для заданих груп пристроїв. Присвоєний груповий адресу - це одна адреса, що використовується для здійснення зв'язку з групою пристроїв, що працюють на одному протоколі або сервісі. Просування групові адреси використовуються разом з конкретними протоколами, наприклад з протоколом DHCPv6.

Розглянемо дві поширені групи привласнених групових IPv6-адрес.

Група під LGPL для всіх вузлів FF02 :: 1. Це група під LGPL, до якої підключені всі пристрої під управлінням протоколу IPv6. Пакет, який надійшов цій групі, приймається і обробляється усіма IPv6-інтерфейсами в каналі або

мережі. Ця група адрес працює так само, як широкомовна адреса в протоколі IPv4. На малюнку наводиться приклад здійснення зв'язку з допомогою групових адрес для всіх вузлів. IPv6-маршрутизатор відправляє повідомлення RA ICMPv6 групі під LGPL для всіх вузлів. Повідомлення RA передає всіх пристроїв IPv6, що знаходяться в мережі, інформацію про адресації: префікс, довжину префікса і шлюз за замовчуванням.

Група під LGPL для всіх маршрутизаторів FF02 :: 2. Це група під LGPL, до якої підключені всі IPv6-маршрутизатори. Маршрутизатор стає частиною цієї групи, коли переходить під управління протоколом IPv6 за допомогою команди глобального конфігурування ipv6 unicast-routing. Пакет, який надійшов цій групі, приймається і обробляється усіма IPv6-маршрутизаторами в каналі або мережі.

Пристрої під керуванням протоколу IPv6 відправляють повідомлення RS ICMPv6 на груповий адресу для всіх маршрутизаторів. Повідомлення RS запитує повідомлення RA у IPv6-маршрутизатора, яке допоможе пристрою в процесі адресному конфігурації.

Групова адреса запитуваних вузлів аналогічний груповій адресі для всіх вузлів. Перевага групової адреси запитуваних вузлів полягає в тому, що він відповідає спеціальному адресою під LGPL Ethernet. Це дозволяє мережевий платі Ethernet фільтрувати кадр, аналізуючи MAC-адресу призначення без його відправки в IPv6-процес, щоб переконатися, що пристрій дійсно є вузлом призначення IPv6-пакета.

Хоча протокол IP не дає гарантію доставки, набір протоколів TCP / IP забезпечує відправку повідомлень навіть в разі виникнення будь-яких помилок. Ці повідомлення відправляються за допомогою ICMP-сервісів. Призначення таких повідомлень - надавати зворотний зв'язок про проблеми, пов'язані з обробкою IP-пакетів в певних умовах, а не підвищувати надійність протоколу IP. З міркувань безпеки повідомлення ICMP не обов'язкові і часто навіть не дозволені в мережі.

ICMP може використовуватися як з IPv4, так і з IPv6. ICMPv4 - це протокол обміну повідомленнями для IPv4. Протокол ICMPv6 надає ті ж послуги для IPv6, але при цьому включає в себе додаткові функціональні можливості. В рамках даного курсу термін ICMP буде використовуватися для позначення як ICMPv4, так і ICMPv6.

Існує безліч типів ICMP-повідомлень і причин їх відправки. Розглянемо деякі найбільш поширені повідомлення.

Використовуються наступні ICMP-повідомлення (однакові для ICMPv4 і ICMPv6).

- Підтвердження вузла.
- Вузол призначення або сервіс недоступні.
- Перевищено інтервал очікування.
- Переадресація маршруту.

Відлуння-запит по протоколу ICMP можна використовувати, щоб визначити, чи функціонує вузол. Локальний вузол відправляє вузлу луна-запит ICMP. Якщо вузол доступний, вузол призначення відправляє луна-відповідь. На

малюнку натисніть кнопку «Відтворення», щоб подивитися відеоролик про принцип роботи луна-запиту і луна-відповіді ICMP. Таке використання exo-запитів по протоколу ICMP лягло в основу утиліти ping.

Вузол призначення або сервіс недоступні

Коли вузол або шлюз отримує пакет, який не може доставити, він може використовувати ICMP-повідомлення «Вузол призначення недоступний» (Destination Unreachable), щоб повідомити джерела про те, що вузол призначення або сервіс для цього пакета недоступні. Таке повідомлення містить код, який визначає причину, по якій пакет не може бути доставлений.

Приклади деяких кодів повідомлень про недоступному вузлі призначення для ICMPv4:

0 - мережа недоступна.

1 - вузол недоступний.

2 - протокол недоступний.

3 - порт недоступний.

Прімечаніе.Протокол ICMPv6 має практично такі ж коди повідомлень про недоступному вузлі призначення.

Повідомлення ICMPv4 про перевищення інтервалу очікування (Time Exceeded) використовується маршрутизатором для вказівки на те, що пакет неможливо переслати, оскільки значення в полі «Час існування» (Time to Live, TTL) пакета було змінено на 0. Якщо маршрутизатор отримує пакет і змінює значення в поле TTL IPv4-пакета на нуль, він відкидає пакет і відправляє на вузол джерела повідомлення про перевищення інтервалу очікування.

Протокол ICMPv6 також відправляє повідомлення про перевищення інтервалу очікування, в разі якщо маршрутизатор не може переслати IPv6-пакет через закінчення його терміну дії. У протоколі IPv6 полі TTL відсутня; щоб з'ясувати, чи не минув термін дії пакета, використовується поле «межа переходів» (hop limit).

Повідомлення ICMPv6 Router Solicitation (RS) (Запит до маршрутизатора) і Router Advertisement (RA) (Відповідь від маршрутизатора)

Інформаційні повідомлення та повідомлення про помилки, що виникають в протоколі ICMPv6, дуже схожі на повідомлення про контроль і помилки, які використовуються протоколом ICMPv4. Однак протокол ICMPv6 відрізняється розширеною функціональністю і новими можливостями, яких немає в ICMPv4. Повідомлення ICMPv6 инкапсулируются в IPv6-пакети.

ICMPv6 включає чотири нових протоколу в складі протоколу виявлення сусідніх вузлів (Neighbor Discovery Protocol, ND або NDP).

Обмін повідомленнями між IPv6-маршрутизатором і IPv6-пристроєм:

- Повідомлення «Запит до маршрутизатора» (Router Solicitation, RS).
- Повідомлення «Відповідь маршрутизатора» (Router Advertisement, RA).

Обмін повідомленнями між IPv6-пристроями:

- Повідомлення із запитом пошуку сусідів (NS).
- Повідомлення про оголошення сусідніх вузлів (NA).

Примітка. ND-протокол ICMPv6 також включає повідомлення перенаправлення, яке має аналогічну з повідомленням перенаправлення, використовуваним в ICMPv4, функцію.

Повідомлення NS і NA використовуються для дозволу адрес і для виявлення дубльованих адрес (Duplicate Address Detection, DAD).

Протокол дозволу адрес використовується в тому випадку, коли пристрою в локальній мережі (LAN) відомий індивідуальний IPv6-адреса призначення, але невідомий MAC-адресу Ethernet. Щоб визначити MAC-адресу призначення, пристрій відправляє повідомлення NS на адресу запитуваної вузла. Повідомлення включає відомий (цільової) IPv6-адреса. Пристрій з цільовим IPv6-адресою відправляє у відповідь повідомлення NA, що містить його MAC-адресу Ethernet. На рис. 2 показаний обмін повідомленнями NS і NA між двома PC. Для отримання більш детальної інформації натисніть на кожне повідомлення.

Коли пристрою призначений глобальний індивідуальну адресу або локальний індивідуальну адресу каналу, для цієї адреси рекомендується виконати процедуру DAD, щоб переконатися в його унікальності. Для перевірки унікальності адреси пристрій відправляє повідомлення NS з власним IPv6-адресою в якості цільового, як показано на рис. 3. Якщо інший пристрій в мережі присвоєно цю адресу, воно відповість повідомленням NA. Це повідомлення NA повідомляє пристрій-відправника про те, що дана адреса вже використовується. Якщо відповідне повідомлення NA не повертається протягом певного періоду часу, індивідуальний адресу визнається унікальним і допустимим до використання.

Примітка. Процес виявлення дубльованих адрес не обов'язковий, проте документ RFC 4861 рекомендує виконує його для індивідуальних адрес.

Ping - це інструмент тестування, який використовує ехо-запити і луна-відповіді ICMP для перевірки з'єднання між вузлами. Команда ping працює з вузлами під керуванням протоколів IPv4 та IPv6.

Для перевірки з'єднання з іншим вузлом в мережі за допомогою команди ping на вузловий адресу відправляється луна-запит. Якщо вузол з вказаною адресою отримує луна-запит, він відправляє луна-відповідь. Після отримання кожного луна-відповіді служба луна-тестування надає дані про час, що пройшов між відправленням запиту й одержанням відповіді. Це дозволяє виміряти продуктивність мережі.

У команди ping спостерігається певний проміжок очікування відповіді. Якщо протягом цього інтервалу відповіді не отримано, команда ping видає повідомлення про відсутність відповіді. Зазвичай це свідчить про наявність проблеми, але також це може вказувати на те, що в мережі працюють функції безпеки, які блокують луна-запити.

Після відправлення всіх запитів утиліта ping видає звіт, що містить рівень успішності запитів і Середній сумарний час доставки запитів і отримання відповідей.

Відправка луна-запитів на локальну адресу loopback

Ми використовуємо команду ping в особливих випадках перевірки та тестування з'єднання. Один з таких випадків - тестування внутрішньої конфігурації IPv4 або IPv6 на локальному вузлі. Для виконання цієї перевірки

відправимо луна-запит на адресу loopback 127.0.0.1 для IPv4 (:: 1 для IPv6). Тестування loopback-адреси IPv4 показано на малюнку.

Відповідь від адреси 127.0.0.1 для IPv4 або :: 1 для IPv6 означає, що IP-мережу налаштована на вузлі правильно. Ця відповідь надходить з мережевого рівня. Однак відповідь не є ознакою того, що адреси, маски або шлюзи були налаштовані вірно. Він також нічого не говорить про стан нижчого рівня мережевого стека. Ця відповідь є просто результатом перевірки IP-мережі на мережевому рівні. Якщо ми отримуємо повідомлення про помилку, це означає, що протокол TCP / IP не працює на даному вузлі.

Виконання команди ping. Тестування підключення до локальної мережі (LAN).

Команду ping також можна використовувати для перевірки здатності вузла обмінюватися даними по локальній мережі. Зазвичай це робиться шляхом відправки луна-запиту на IP-адреса шлюзу вузла. Відправка луна-запиту на шлюз дозволяє переконатися, що вузол і інтерфейс маршрутизатора, який виступає в ролі шлюзу, нормально функціонують в локальній мережі.

Для цієї перевірки найчастіше використовується адреса шлюзу, оскільки маршрутизатор практично завжди знаходиться в робочому стані. Якщо адреса шлюзу не відповідає, луна-запит може бути відправлений на IP-адресу іншого, свідомо робочого, вузла локальної мережі.

Якщо шлюз або інший вузол відповідає на запит, значить, локальний вузол може успішно працювати в локальній мережі. Якщо шлюз не відповідає, а інший вузол відповідає, то проблема може бути з інтерфейсом маршрутизатора, що виступає в ролі шлюзу.

Перша можлива причина: на вузлі був налаштований неправильну адресу шлюзу. Друга можлива причина: інтерфейс маршрутизатора функціонує нормально, але встановлена система безпеки перешкоджає обробці або відправці відповідей на ехо-запити.

Команду ping також можна використовувати для перевірки здатності вузла обмінюватися даними з іншими мережами. З локального вузла можна відправити луна-запит на робочий IPv4-вузол віддаленої мережі, як показано на малюнку.

Якщо луна-запит був відправлений успішно, можна перевірити міжмережевого взаємодія на великій ділянці. Успішна відправка міжмережевого луна-запиту підтверджує підключення до локальної мережі, працездатність маршрутизатора, що виконує роль шлюзу, а також працездатність інших маршрутизаторів на шляху між локальною мережею і мережею віддаленого вузла.

Крім того, може бути перевірена працездатність віддаленого вузла. Якби віддалений вузол не міг передавати дані за межі своєї локальної мережі, він би не відповів на ехо-запит.

Примітка. Багато мережних адміністратори обмежують або забороняють введення ICMP-повідомлень в корпоративну мережу; в зв'язку з цим заходи щодо забезпечення безпеки можуть стати причиною відсутності луна-відповіді.

Команда ping використовується для перевірки з'єднання між двома вузлами, але не дозволяє отримати інформацію про пристрої, що знаходяться між ними. Команда traceroute (tracert) - це утиліта, що дозволяє скласти список

переходів, через які успішно проходить луна-запит на шляху до вузла призначення. Даний список може дати важливу підтверджує інформацію, а також інформацію про усунення неполадок. Якщо запит доходить до вузла призначення, утиліта trace заносить в список інтерфейс кожного маршрутизатора на шляху між вузлами. Якщо на якомусь переході на маршруті відбувається збій передачі даних, то адреса останнього маршрутизатора, який відповів на трасування, може вказати на місце знаходження проблеми або обмеження системи безпеки.

Час проходження сигналу в прямому і зворотному напрямках (Round Trip Time, RTT)

Утиліта traceroute визначає сумарний час проходження сигналу в прямому і зворотному напрямках (RTT) для кожного переходу на маршруті і повідомляє про можливу відсутність відповіді на одному з переходів. RTT - це час, який потрібен на доставку пакета на віддалений вузол і отримання відповіді це цього вузла. Символ зірочки (*) використовується для позначення втраченого пакета або відсутності відповіді на пакет.

Цю інформацію можна використовувати для виявлення проблемного маршрутизатора на маршруті. Якщо результат команди показує великий час відповіді або втрату даних на якомусь переході, це ознака того, що ресурси маршрутизатора або його сполук можуть бути під кінець.

Утиліта traceroute використовує значення в поле TTL в IPv4 і в поле межі переходів (Hop Limit) в IPv6 в заголовках 3-го рівня (разом з повідомленням ICMP про перевищення інтервалу очікування).

Розпочніть відтворення відео на малюнку, щоб переглянути, як утиліта traceroute використовує TTL.

Перша послідовність повідомлень, відправлених командою traceroute, в поле TTL матиме значення 1. Дане значення TTL викликає перевищення інтервалу очікування відповіді на IPv4-пакет на першому маршрутизаторі. Потім цей маршрутизатор відповідає ICMPv4-повідомленням. Тепер traceroute знає адресу першого переходу.

Потім traceroute поступово збільшує значення в поле TTL (2, 3, 4 ...) для кожної послідовності повідомлень. Таким чином трасуються адреси кожного переходу, у міру того як перевищення інтервалу очікування відповіді відбувається далі на маршруті. Значення в поле TTL продовжує збільшуватися до тих пір, поки не буде досягнутий вузол призначення, або до певного заздалегідь встановленого максимального рівня.

Після досягнення останнього вузла призначення цей вузол відповідає або повідомленням ICMP про недоступність порту або луна-відповіддю ICMP (замість повідомлення ICMP про перевищення інтервалу очікування).

Проектування, впровадження і управління ефективним планом IP-адресації забезпечують надійність і ефективність роботи мереж. Це особливо актуально у випадках, коли збільшується кількість вузлів мережі. Розуміння ієрархічної структури IP-адреси і того, як змінити ієрархію для підвищення ефективності маршрутизації, є важливою частиною планування схеми IP-адресації.

У вихідному IPv4-адресу існує два рівні ієрархії: мережа і вузол. Ці два рівні адресації дають можливість створювати базові угруповання в мережі, які полегшують маршрутизацію пакетів в мережу призначення. Маршрутизатор пересилає пакети на підставі мережної частини IP-адреси. Після того, як мережа знайдена, по вузлової частини адреси можна визначити пристрій призначення.

Однак у міру зростання мережі в багатьох організаціях, коли до мережі підключаються сотні і навіть тисячі вузлів, дворівнева ієрархія стає неефективною.

При поділі мережі на підмережі в ієрархію мережі додається ще один рівень, і фактично створюється ієрархія з трьох рівнів: мережа, підмережа і вузол. При додаванні нового рівня ієрархії в IP-мережі створюються додаткові підгрупи. Це дозволяє прискорити доставку пакетів і забезпечити додаткову фільтрацію, сприяючи скороченню обсягу «локального» трафіку.

широкомовні домени

Пристрої в локальній мережі Ethernet використовують трансляцію розсилку, щоб знайти:

Інші пристрої. Пристрій використовує протокол дозволу адрес (ARP) для відправки широкомовної розсилки на 2-му рівні за відомим IPv4-адресою в локальній мережі, щоб виявити призначений MAC-адресу.

Сервіси. Вузол, як правило, отримує свої настройки IPv4-адреси за допомогою протоколу динамічної настройки вузла (DHCP), який здійснює трансляцію розсилку в локальній мережі, щоб знайти DHCP-сервер.

Комутатори виконують трансляцію розсилку на всі інтерфейси, за винятком того інтерфейсу, через який була отримана розсилка. Наприклад, якби комутатор, показаний на малюнку, отримав трансляцію розсилку, він би переслав її інших комутаторів і іншим користувачам, підключеним до мережі.

Маршрутизатор не виконують трансляцію розсилку. Коли маршрутизатор отримує широкомовлення, він не пересилає її на інші інтерфейси. Наприклад, коли маршрутизатор R1 отримує широкомовлення на свій інтерфейс Gigabit Ethernet 0/0, він не пересилає її на інші інтерфейси.

Таким чином, кожен інтерфейс маршрутизатора підключений до широковещательному домену, і широкомовні розсилання виконуються тільки в рамках певного домену розсилки.

Проблеми з великими широкомовними доменами

Великий широкомовний домен являє собою мережу, що з'єднує безліч вузлів. Проблема великого широковещательного домену полягає в наступному: вузли можуть генерувати надлишкову розсилку і негативно впливати на роботу мережі. На малюнку 1 локальна мережа LAN 1 пов'язує 400 користувачів, які можуть генерувати трансляцію розсилку. В результаті:

Робота мережі сповільнюється через значного обсягу трафіку.

Пристрої також працюють повільніше, оскільки їм потрібно підтвердити і обробити кожен пакет широкомовної розсилки.

Для вирішення цієї проблеми треба скоротити розмір мережі, створивши менші широкомовні домени. Такий процес називається поділом на підмережі. Такі більш дрібні мережі називаються підмережами.

На малюнку 2, наприклад, 400 користувачів локальної мережі LAN 1 з адресою 172.16.0.0 / 16 були розділені на дві підмережі по 200 користувачів кожна - 172.16.0.0 / 24 і 172.16.1.0 / 24. Розсилка обмежує дрібнішими широкомовними доменами. Таким чином, широкомовлення з локальної мережі LAN 1 цієї статті не поширюється на мережу LAN 2.

Зверніть увагу на зміну довжини префікса с / 16 на / 24. Використання біт в вузловий частини для створення додаткових підмереж - основа поділу на підмережі.

Примітка. Терміни підмережа і мережу часто використовуються як синоніми. Більшість мереж самі є подсетями більших блоків адрес.

Причини для поділу на підмережі

Поділ на підмережі знижує загальний обсяг мережевого трафіку і підвищує продуктивність мережі. Крім того, це дає можливість адміністраторам застосовувати заходи безпеки. Наприклад, визначити підмережі, яким дозволено і яким не дозволено взаємодіяти один з одним.

Існує кілька способів використання підмереж для управління мережевими пристроями. Мережеві адміністратори можуть групувати пристрої в підмережі за такими принципами.

- Місцезнаходження, наприклад по поверхах будівлі
- Підрозділ
- Тип пристрою

Будь-який інший значущий для мережі принцип.

Зверніть увагу, що на кожному малюнку для підмереж використовується довший префікс, що позначає мережу.

У цьому розділі описується процес поділу на підмережі. Розуміння принципу поділу мережі на підмережі - головний навик, яким повинен володіти кожен мережевий адміністратор. Розроблено різні методи, які допомагають зрозуміти суть цього процесу. У цьому розділі розглянуто двійковий метод. На перший погляд поділ на мережі може здатися складним, але чим більше уваги ви будете приділяти деталям і чим більше будете практикуватися, тим цей процес стане для вас простіше і зрозуміліше.

межі октетів

Кожен інтерфейс маршрутизатора підключається до однієї мережі. IPv4-адрес і маска підмережі, налаштовані на інтерфейсі маршрутизатора, ідентифікують певний широкомовний домен. Пам'ятайте, що довжина префікса і маска підмережі - це різні способи представлення одного і того ж - мережевий частини адреси.

Длинапре фикса	Маска подсети	Маска подсети в двоичной системе (с = сеть, у = узел)	Количество узлов
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

Рис. 2.1.19

Для створення IPv4-підмереж ми задіємо один або кілька біт з вузловий частини в якості біт мережевої частини. Для цього ми розширюємо маску підмережі. Ми запозичуємо біти з вузловий частини адреси і створюємо додаткові біти для мережі. Чим більше запозичене біт з вузловий частини, тим більше підмереж можна створити.

Поділ мереж найпростіше виконати на кордонах октетів / 8, / 16 і / 24. Показана на малюнку таблиця визначає довжину цих префіксів, відповідні маски підмережі, біти мережевої і вузловий частин, а також число вузлів, які можна підключити в підмережі. Зверніть увагу, що збільшення довжини префікса скорочує число вузлів в кожній підмережі.

Поділ на підмережі на кордоні октетів

Розглянемо наступний приклад, щоб зрозуміти як використовувати кордону октетів для поділу на підмережі. Припустимо, підприємство обрало приватну адресу 10.0.0.0/8 в якості адреси внутрішньої мережі. Цей мережеву адресу може зв'язати 16 777 214 вузлів в один широкомовний домен. Однак це не кращий варіант.

Разделение на подсети 10.x.0.0/16

Адрес подсети (256 возможных подсетей)	Диапазон узлов (65 534 возможных узла в каждой подсети)	Широковещательный адрес
10.0.0.0/16	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0/16	10.1.0.1 - 10.1.255.254	10.1.255.255
10.2.0.0/16	10.2.0.1 - 10.2.255.254	10.2.255.255
10.3.0.0/16	10.3.0.1 - 10.3.255.254	10.3.255.255
10.4.0.0/16	10.4.0.1 - 10.4.255.254	10.4.255.255
10.5.0.0/16	10.5.0.1 - 10.5.255.254	10.5.255.255
10.6.0.0/16	10.6.0.1 - 10.6.255.254	10.6.255.255
10.7.0.0/16	10.7.0.1 - 10.7.255.254	10.7.255.255
...	...	...
10.255.0.0/16	10.255.0.1 - 10.255.255.254	10.255.255.255

Рис. 2.1.20

Підприємство може далі розбити адреса 10.0.0.0/8 на підмережі на кордоні октету / 16, як показано на малюнку 1. Це дасть можливість підприємству визначити 256 підмереж (тобто 10.0.0.0/16 - 10.255.0.0/16), кожна з яких зможе зв'язати 65 534 вузла. Зверніть увагу, що перші два октету ідентифікують адресу мережевої частини, тоді як останні два октету визначають IP-адреса вузла.

В якості альтернативи, підприємство може виконати поділ на підмережі на кордоні октету / 24, як показано на малюнку 2. Це дасть можливість підприємству визначити 65 536 підмереж, кожна з яких зможе зв'язати 254 вузла. Кордон октету / 24 дуже популярна при поділі на підмережі, тому що вона дозволяє розмістити раціональне число вузлів і формує зручні для використання підмережі на кордоні октету.

Поділ на підмережі з безкласової адресацією

У раніше наведених прикладах ми використовували біти вузлів із загальних префіксів мережі / 8, / 16 і / 24. Однак підмережа може запозичувати біти з будь-якої позиції біт в вузловий частини для створення інших масок.

Наприклад, адреса мережі / 24 зазвичай розбивається на підмережі за допомогою більш довгих префіксів, запозичуючи біти з четвертого октету. Завдяки цьому адміністратор може гнучко призначати мережеві адреси меншому числу кінцевих пристроїв.

Длинапрефикса	Маска подсети	Маска подсети в двоичной системе (n = сеть, h = узел)	Количество подсетей	Количество узлов
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2

Рис. 2.1.21

Як показано на рисунку:

Рядок / 25 - запозичення 1 біта з четвертого октету формує 2 підмережі з підтримкою 126 вузлів в кожній

Рядок / 26 - запозичення 2 біт формує 4 підмережі з підтримкою 62 вузлів в кожній

Рядок / 27 - запозичення 3 біт формує 8 підмереж з підтримкою 30 вузлів в кожній

Рядок / 28 - запозичення 4 біт формує 16 підмереж з підтримкою 14 вузлів в кожній

Рядок / 29 - запозичення 5 біт формує 32 підмереж з підтримкою 6 вузлів в кожній

Рядок / 30 - запозичення 6 біт формує 64 підмереж з підтримкою 2 вузлів в кожній

Для кожного біта, запозиченого в четвертому октеті, доступну кількість підмереж подвоюється зі скороченням числа адрес вузлів на сіть.

Приклад поділу на підмережі з безкласової адресацією

Розглянемо наступний приклад, щоб зрозуміти як використовувати поділ на підмережі з безкласової адресацією.

Розглянемо адресу приватної мережі 192.168.1.0/24, показаний на малюнку 1. Перші три октету показані в десятковій системі числення, тоді як останній октет - в двійковій. Це зроблено тому, що ми будемо запозичувати біти останнього октету для створення підмереж з мережі 192.168.1.0/24.

Судячи по довжині префікса / 24, маска підмережі дорівнює 255.255.255.0. Перші три октету ідентифікують частина мережі, а решта 8 біт в останньому октеті ідентифікують частина вузла. Якщо не розбивати на підмережі, така мережа підтримує один LAN-інтерфейс для 254 IPv4-адрес вузлів. Якщо потрібна додаткова локальна мережа (LAN), основну мережу потрібно розділити на підмережі.

Створення двох підмереж

Розглянемо топологію на малюнку 1, щоб побачити, як мережа розділена на підмережі за допомогою префікса / 25. Маршрутизатор R1 має два сегменти локальної мережі (LAN), підключені до інтерфейсів GigabitEthernet. Кожній локальній мережі (LAN) призначена одна з підмереж.

Мережевий адреса IPv4 дорівнює 192.168.1.0 і містить всі біти 0 в вузловий частини адреси.

Перший IPv4-адрес вузла дорівнює 192.168.1.1 і містить всі біти 0 і крайній правий біт 1 в вузловий частини адреси.

Останній IPv4-адрес вузла дорівнює 192.168.1.126 і містить всі біти 1 і крайній правий біт 0 в вузловий частини адреси.

Широкомовний IPv4-адрес дорівнює 192.168.1.127 і містить всі біти 1 в вузловий частини адреси.

Інтерфейсів маршрутизатора повинен бути призначений IP-адреса в допустимих межах вузлів для заданої підмережі. Це і є адреса, який буде використовуватися вузлами мережі в якості шлюзу. В якості адреси інтерфейсу маршрутизатора рекомендується використовувати перший або останній доступний адреса діапазону мережі. На малюнку 4 показана налаштування інтерфейсів маршрутизатора R1 з першим IPv4-адресою під відповідні підмережі за допомогою команди налаштування інтерфейсу ip адреси.

Налаштування IPv4-адреси і шлюзу повинні бути виконані на вузлах кожної підмережі. На малюнку 5 показана настройка IPv4-адреси для вузла PC2 в мережі 192.168.1.128/25. Зверніть увагу: IPv4-адресою шлюзу є адреса 192.168.1.129, налаштований на інтерфейсі G0 / 1 маршрутизатора R1, а міський підмережі є 255.255.255.128.

Формула розрахунку мереж

Кількість підмереж = 2n, де n - це кількість зайнятих біт від порції хоста.

Формула розрахунку хостів (вузлів)

Кількість хостів в підмережі = 2n-2, де n - це кількість вільних біт (нулів) в порції хоста, а «-2» - це відрахування адреси мережі (в порції хоста всі нулі) і широкомовної адреси (в порції хоста все одиниці) .

Пояснення формул розрахунку мереж

IP адреса

IP адреса складається з 32 бітів, які поділені на 4 частини по 8 біт відповідно (ці частини називаються октетами). У житті використовується запис IP адреси в десятковому вигляді.

Приклади IP адрес:

172.16.2.15 = 10101100.00010000.00000010.00001111

178.68.128.168 = 10110010.01000100.10000000.10101000

217.20.147.94 = 11011001.00010100.10010011.01011110

З цих 32 бітів частина відноситься до адреси хоста, якому належить цей IP адреса, а інша частина відноситься до адреси мережі, в якій знаходиться цей хост. Перша частина (зліва направо) IP адреси позначає адресу мережі, а друга частина (решта біти) - адреса хоста. Щоб дізнатися, скільки бітів відноситься до адреси мережі, треба скористатися маскою мережі.

маска мережі

Маска мережі теж складається з 32 бітів, але на відміну від IP адреси, в масці одиниці і нулики не можуть перемішуватися. У житті використовується запис мережевої маски в десятковому вигляді.

Приклади масок мережі:

255.255.255.0 = 11111111.11111111.11111111.00000000

255.0.0.0 = 11111111.00000000.00000000.00000000

255.255.240.0 = 11111111.11111111.11110000.00000000

255.255.255.128 = 11111111.11111111.11111111.10000000

префікс маски

Ще частіше, маска мережі записується у вигляді короткого префікса маски. Число в префікс позначає кількість біт відносяться до адреси мережі.

/ 16 = 11111111.11111111.00000000.00000000 = 255.255.0.0

/ 24 = 11111111.11111111.11111111.00000000 = 255.255.255.0

/ 26 = 11111111.11111111.11111111.11000000 = 255.255.255.192

IP адреса і маска мережі

Щоб дізнатися, яка частина IP адреси відноситься до порції мережі, необхідно виконати бінарну логічну операцію AND (I).

Бінарна логічна операція AND (I)

Сенс операції полягає в порівнянні двох бітів, причому тільки в одному випадку бінарна операція дає одиницю на виході - у разі порівняння двох одиниць. В інших випадках логічна операція AND дає на виході 0.

Результати порівняння логічною операцією AND двох бітів:

1 AND 1 = 1

1 AND 0 = 0

0 AND 1 = 0

0 AND 0 = 0

Операція AND над IP адресою і маскою

Уявімо, що у нас є IP адреса 192.168.1.31 з маскою мережі у вигляді префікса / 24, наша задача обчислити адресу мережі, порцію мережі, порцію хоста.

Спочатку треба перевести IP адреса з десяткової системи числення в двійкову систему. Потім перевести префікс в двійковий вигляд і нормальний

вигляд маски мережі (десятковий). Далі залишиться тільки скласти IP адреса з маскою за допомогою логічної операції AND.

192.168.1.31/24

192.168.1.31 = 11000000.10101000.00000001.00011111

/ 24 = 11111111.11111111.11111111.00000000 = 255.255.255.0

11000000.10101000.00000001.00011111 (IP)

AND

11111111.11111111.11111111.00000000 (Mask)

=

11000000.10101000.00000001.00000000 (Адреса мережі в двійковому вигляді)

192.168.1.0/24 (Адреса мережі в десятковому вигляді з мережевим префіксом)

Ось ми і дізналися адресу мережі. Одинички в масці вказують на довжину порції адреси мережі (11000000.10101000.00000001.), А нулики - на порцію адреси хоста (.00011111).

Приклади розрахунку мереж

Розподіл мережі здійснюється присвоєнням бітів з порції адреси хоста до порції адреси мережі. Тим самим ми збільшуємо можливу кількість підмереж, але зменшуємо кількість хостів в підмережі. Щоб дізнатися, скільки виходить підмереж із привласнених бітів треба скористатися cisco формулою розрахунку мереж: 2n, де n є кількістю присвоєних біт.

Приклад розрахунку мережі на 2 підмережі.

У нас є адреса мережі 192.168.1.0/24, нам треба розділити наявну мережу на 2 підмережі. Спробуємо забрати від порції хоста 1 біт і скористатися формулою: 21 = 2, це означає, що якщо ми заберемо один біт від частини хоста, то ми отримаємо 2 підмережі. Присвоєння одного біта з порції хоста збільшить префікс на один біт: / 25. Тепер треба виписати 2 однакових IP адреси мережі в двійковому вигляді змінивши лише присвоєний біт (у першій підмережі присвоєний біт буде дорівнює 0, а у другій підмережі = 1). Захоплений біт я виділю більш жирним шрифтом червоного кольору.

2 підмережі (захоплений біт я виділю більш жирним шрифтом червоного кольору):

1) 11000000.10101000.00000001.00000000

2) 11000000.10101000.00000001.10000000

Тепер запишемо поряд з двійковим видом десятковий, і додамо новий префікс. Червоним позначив порцію підмережі, а синім - порцію хоста.

1) 11000000.10101000.00000001.00000000 = 192.168.1.0/25

2) 11000000.10101000.00000001.10000000 = 192.168.1.128/25

Все, мережа розділена на 2 підмережі. Як ми бачимо вище, порція хоста тепер становить 7 біт.

Щоб вирахувати, скільки адрес хостів можна отримати використовуючи 7 біт, необхідно скористатися cisco формулою розрахунку хостів: 2n-2, де n = кількість біт в порції хоста.

27 - 2 = 126 хостів. На початку статті було сказано, що віднімається цифра 2 є двома адресами, які не можна привласнити хосту: адреса мережі і широкомовна адресу.

Адреса мережі, це коли в порції хоста всі нулі, а широкомовний адресу, це коли в порції хоста все одиниці. Випишемо ці адреси для кожної підмережі в двійковому і десятковому вигляді:

11000000.10101000.00000001.00000000 = 192.168.1.0/25 (адреса мережі першої підмережі)

11000000.10101000.00000001.01111111 = 192.168.1.127/25 (широкомовна адреса першої підмережі)

11000000.10101000.00000001.10000000 = 192.168.1.128/25 (адреса мережі другий подсети)

11000000.10101000.00000001.11111111 = 192.168.1.255/25 (широкомовна адреса другий подсети)

Приклад розрахунку мережі на 4 підмережі.

У нас є адреса мережі 192.168.1.0/24, треба розділити мережу на 4 підмережі. Вираховуємо за формулою, скільки нам треба зайняти біт від хоста: 22 = 4. Префікс змінюється на / 26.

4 підмережі (захоплений біт я виділю більш жирним шрифтом червоного кольору):

1) 11000000.10101000.00000001.00000000

2) 11000000.10101000.00000001.01000000

3) 11000000.10101000.00000001.10000000

4) 11000000.10101000.00000001.11000000

Червоним позначив порцію підмережі, а синім - порцію хоста:

1) 11000000.10101000.00000001.00000000 = 192.168.1.0/26

2) 11000000.10101000.00000001.01000000 = 192.168.1.64/26

3) 11000000.10101000.00000001.10000000 = 192.168.1.128/26

4) 11000000.10101000.00000001.11000000 = 192.168.1.192/26

Все, мережа розділена на 4 підмережі. Порція хоста тепер становить 6 біт.

26 - 2 = 62 хостів.

11000000.10101000.00000001.00000000 = 192.168.1.0/26 (адреса мережі першої підмережі)

11000000.10101000.00000001.00111111 = 192.168.1.63/26 (широкомовна адреса першої підмережі)

11000000.10101000.00000001.01000000 = 192.168.1.64/26 (адреса мережі другий подсети)

11000000.10101000.00000001.01111111 = 192.168.1.127/26 (широкомовна адреса другий подсети)

11000000.10101000.00000001.10000000 = 192.168.1.128/26 (адреса мережі третьої підмережі)

11000000.10101000.00000001.10111111 = 192.168.1.191/26 (широкомовна адреса третьої підмережі)

11000000.10101000.00000001.11000000 = 192.168.1.192/26 (адреса мережі четвертої підмережі)

11000000.10101000.00000001.11111111 = 192.168.1.255/26 (широкомовна адреса четвертої підмережі)

Створення підмереж з префіксом / 16

Якщо потрібна більша кількість підмереж, необхідно використовувати IPv4-мережу з великим числом біт в вузловий частини для запозичення.

Наприклад, адреса мережі 172.16.0.0 має маску за замовчуванням / 16 або 255.255.0.0. Ця електронна адреса має по 16 біт в мережевий і вузловий частини. 16 біт в вузловий частини можна використовувати для створення підмереж. У таблиці на малюнку представлені всі можливі сценарії поділу на підмережі з префіксом / 16.

Хоча вчити на пам'ять всю таблицю немає необхідності, потрібно добре розуміти принцип отримання кожного значення таблиці. Нехай вас не лякає її розмір. Великий вона вийшла з-за 8 додаткових біт, які можна запозичити, і таким чином кількість підмереж і вузлів просто збільшується.

Створення 100 підмереж з префіксом / 16

Розглянемо велике підприємство, якому необхідно хоча б 100 підмереж, і яке обрало приватну адресу 172.16.0.0/16 в якості адреси внутрішньої мережі.

При запозиченні біт з адреси / 16 почніть запозичувати біти в третьому октеті, продовжуючи зліва направо. Запозичте один біт кожен раз до тих пір, поки не буде досягнуто число біт, необхідне для створення 100 підмереж.

На малюнку 1 показано кількість підмереж, яке може бути створено при запозиченні біт з третього і четвертого октетів. Зверніть увагу, що тепер може бути запозичене до 14 біт з вузловий частини.

Щоб задовольнити потреби підприємства, потрібно запозичувати 7 біт (тобто 2 ^ 7 = 128 підмереж).

Як ви пам'ятаєте, маска підмережі повинна змінюватися для відображення запозичених біт. У цьому прикладі при запозиченні семи біт маска буде розширена на 7 біт в третьому октеті. У десятковому форматі маска буде мати вигляд 255.255.254.0 або префікс / 23, оскільки третій октет в довічним форматі має вигляд 11111110, а четвертий октет - 00000000.

Виробництво 1 000 підмереж з префіксом / 8

Деяким організаціям, наприклад, невеликим операторам зв'язку або великих підприємств, може знадобитися ще більшу кількість підмереж. Як приклад візьмемо невеликого оператора зв'язку, якому потрібно тисячі підмереж для клієнтів. Кожному клієнту потрібно великий простір в вузловий частини для створення власних підмереж.

Адреса мережі 10.0.0.0 має маску підмережі за замовчуванням / 8 або 255.0.0.0. Це означає, що при поділі на підмережі для запозичення є 8 біт в мережевій частині адреси і 24 біта в вузловий частини. Таким чином, невеликий оператор зв'язку розіб'є на підмережі всю мережу 10.0.0.0/8.

Як і завжди, для створення підмережі потрібно запозичити біти з вузловий частини адреси вихідної мережі. Починаючи з першого зліва доступного біта в вузловий частини, ми будемо запозичувати по одному біту за один раз до тих пір, поки не отримаємо кількість біт, необхідних для створення 1000 підмереж. Як видно з малюнка 1, 10 біт потрібно запозичувати для створення 1 024 підмереж. Це означає, що потрібно запозичувати 8 біт в другому октеті і 2 додаткових біта в третьому.

Поділ на підмережі на основі вимог вузлів

При плануванні підмереж потрібно врахувати два параметри.

Необхідна кількість адрес вузлів в кожній мережі.

Необхідна кількість окремих підмереж.

У таблиці на малюнку показані особливості поділу на підмережі з префіксом / 24. Зверніть увагу, на зворотну залежність між числом підмереж і числом вузлів. Чим більше біт запозичене для створення підмереж, тим менше є біт в вузловий частини. Якщо потрібно більше вузлів, значить, потрібно більше біт в вузловий частини, що призводить до зменшення кількості підмереж.

Кількість адрес вузлів, необхідних в найбільшій підмережі, визначає, скільки біт потрібно залишити в вузловий частини адреси. Як ви пам'ятаєте, два адреси використовувати не можна, тому фактично кількість доступних адрес розраховується як 2 ^ n-2.

Іноді потрібно конкретну кількість підмереж, а кількість адрес вузлів в кожній підмережі менш важливо. Наприклад, в організації може знадобитися розділити мережевий трафік згідно внутрішню структуру чи при налаштуванні мережі в підрозділі, як показано на малюнку. Наприклад, організація може прийняти рішення об'єднати в одну мережу всі пристрої, що використовуються фахівцями технічного відділу, а всі пристрої, що використовуються керівництвом, винести в окрему мережу. У цьому випадку кількість підмереж має більш високий пріоритет при визначенні кількості біт для запозичення.

Як ви пам'ятаєте, кількість підмереж, що створюються при запозиченні біт, можна розрахувати за формулою 2 ^ n (де n - кількість запозичених біт). Ключовим моментом є співвідношення кількості необхідних підмереж і кількості вузлів, необхідних для найбільшої підмережі. Чим більше біт було запозичене для створення додаткових підмереж, тим менше вузлів буде доступно в кожній з підмереж.

Приклад вимог мережі

Мережеві адміністратори повинні розробити схему мережевої адресації, щоб забезпечити максимальну кількість вузлів в кожній мережі і кількість підмереж. Схема адресації повинна передбачати розширення як кількості адрес вузлів в кожній підмережі, так і загальної кількості підмереж.

У цьому прикладі штаб-квартира оператора зв'язку виділила адресу приватної мережі 172.16.0.0/22 (10 біт в вузловий частини) для філії. Як показано на малюнку 1, в результаті ми отримуємо 1 022 адрес вузлів.

Топологія мережі філій, показана на малюнку 2, складається з 5 сегментів локальної мережі (LAN) і 4 міжмережевих з'єднань між маршрутизаторами. Таким чином, потрібні 9 підмереж. Найбільша підмережа повинна містити 40 вузлів.

Мережевий адреса 172.16.0.0/22 має 10 біт в вузловий частини, як показано на малюнку 3. Оскільки найбільшою підмережі потрібно 40 вузлів, для забезпечення їх адресації потрібно не менше 6 біт в вузловий частини. Це число визначається за такою формулою: 2 ^ 62 = 62 вузла.

За формулою визначення кількості підмереж отримуємо 16 підмереж: 2 ^ 4 = 16. Оскільки в нашому прикладі мережевої інфраструктури потрібні 9 підмереж, це відповідає нашим вимогам і забезпечує певний запас для зростання в майбутньому.

Таким чином, перші 4 біта в вузловий частини можна використовувати для створення підмереж, як показано на малюнку 4. Якщо запозичувати 4 біта, нова довжина префікса буде / 26 з маскою підмережі 255.255.255.192.

Як показано на малюнку 5, підмережі можна призначити сегментам локальної мережі (LAN) і з'єднанням між маршрутизаторами.

При традиційному поділі на підмережі адреси витрачаються даремно

У традиційному розбитті на підмережі кожної підмережі виділяється однакова кількість адрес. Якщо все підмережі мають однакові вимоги до кількості вузлів, такі блоки адрес фіксованого розміру будуть ефективними. Проте, найчастіше це не так.

Наприклад, в топології, показаної на малюнку 1, використовуються сім підмереж: по одній для кожної з чотирьох локальних мереж (LAN) і по одній для кожного з трьох каналів мережі WAN між маршрутизаторами. У традиційному розбитті на підмережі з вказаною адресою 192.168.20.0/24 з вузловий частини в останньому октеті можна запозичити три біта, щоб забезпечити створення семи підмереж. Як показано на малюнку 2, при запозиченні трьох біт можна створити 8 підмереж, а решти п'яти біт в вузловий частини вистачить для 30 адрес вузлів в кожній підмережі. Така схема дозволяє створити необхідні підмережі і відповідає вимогам до вузла в найбільших локальних мережах (LAN).

Хоча при такому стандартному розподілі на підмережі забезпечується відповідність вимогам до найбільших локальних мереж (LAN) і поділ простору адрес на відповідну кількість підмереж, це все одно призводить до значного необгрунтованого витрачання зайвих адрес.

Наприклад, в кожній підмережі для трьох каналів WAN потрібно тільки дві адреси. Оскільки кожна з підмереж містить 30 доступних для використання адрес, в кожній з підмереж виявляється 28 невикористовуваних адрес. Як показано на малюнку 3, в результаті ми отримуємо 84 невикористовуваних адреси (28x3).

Крім того, це також обмежує розширення мережі в майбутньому, зменшуючи загальне число доступних підмереж. Таке неефективне використання адрес характерно для традиційного поділу на підмережі. Застосування традиційної схеми поділу на підмережі за таким сценарієм не є ефективним і має на увазі недоцільне витрачання ресурсів.

Поділ підмережі на декілька підмереж з використанням маски підмережі довільної довжини (Variable Length Subnet Mask, VLSM) дозволяє розподіляти набагато менше «зайвих» адрес.

Маски подсети довільної довжини

Зверніть увагу, що у всіх попередніх прикладах поділу на підмережі до всіх подсетям застосовувалася одна маска підмережі. Це означає, що всі підмережі містять однакове число доступних адрес вузлів.

Як показано на малюнку 1, при традиційній схемі поділу на підмережі створюються підмережі однакового розміру. Всі підмережі в традиційній схемі використовують одну і ту ж маску підмережі. Як показано на малюнку 2, VLSM дозволяє розділити простір мережі на нерівні частини. VLSM-маска підмережі може варіюватися в залежності від кількості біт, які були запозичені для конкретної подсети. Ці біти утворюють «змінну» частина маски.

Поділ на підмережі за допомогою VLSM схоже з традиційним поділом на підмережі в тому, що для створення підмереж запозичуються біти. Як і раніше

застосовуються формули розрахунку числа вузлів в кожній підмережі і числа створюваних підмереж.

Різниця полягає в тому, що поділ на підмережі не виконується за один етап. При використанні VLSM мережу спочатку розділяється на підмережі, а потім підмережі, в свою чергу, також розбиваються на підмережі. Цей процес можна повторювати багаторазово для створення підмереж різних розмірів.

Примітка. При використанні VLSM, завжди починайте з забезпечення відповідності вимогам до вузлів в найбільших подсетях. Продовжуйте розбиття до тих пір, поки не будуть задоволені вимоги до вузлів в найменшій підмережі.

Базова модель VLSM

Щоб краще зрозуміти процес застосування VLSM, повернемося до попереднього прикладу, показаному на малюнку 1. Мережа 192.168.20.0/24 була розбита на вісім підмереж однакового розміру. Сім з восьми підмереж були виділені. Чотири підмережі використовувалися для локальних мереж (LAN), а три підмережі - для каналів мережі WAN між маршрутизаторами. Як ви пам'ятаєте, в подсетях, використовуваних для каналів мережі WAN, були невикористовувані адреси, так як в цих подсетях потрібні тільки дві адреси - по одному для кожного інтерфейсу маршрутизатора. Щоб запобігти неефективне використання адрес, за допомогою VLSM можна створити більш дрібні підмережі для каналів мережі WAN.

Щоб створити більш дрібні підмережі для каналів мережі WAN, одна з підмереж буде розділена. У цьому прикладі остання підмережа 192.168.20.224/27 буде додатково розбита на підмережі.

Як ви пам'ятаєте, якщо відомо необхідну кількість адрес вузлів, можна використовувати формулу 2 ^ n-2 (де n - кількість біт в вузловий частини). Щоб отримати два доступних адреси, в його вузловий частини повинні залишитися два біта.

Оскільки в розбитому на підмережі адресному просторі 192.168.20.224/27 є 5 біт в вузловий частини, ще три біта можна запозичити, залишивши 2 біта в вузловий частини, як показано на малюнку 2. На даному етапі розрахунки в точності збігаються з розрахунками при традиційному розбитті на підмережі. Біти запозичуються, визначаючи діапазони підмереж.

Така схема VLSM-розбиття на підмережі зменшує кількість адрес в кожній підмережі до відповідного розміру з'єднань з глобальною мережею. Розбиття підмережі 7 для мереж WAN залишає доступними підмережі 4, 5 і 6 для майбутніх мереж, а також 5 додаткових підмереж для мереж WAN.

VLSM на практиці

При використанні VLSM-підмереж для сегментів локальної (LAN) та глобальної (WAN) мережі можна виділяти адреси без непотрібних втрат.

Як показано на малюнку 1, вузлів у всіх локальних мережах (LAN) буде присвоєно допустимий адресу вузла в діапазоні цієї підмережі і з маскою / 27. У кожного з чотирьох маршрутизаторів буде LAN-інтерфейс з підмережею / 27, а також один або кілька послідовних інтерфейсів з підмережею / 30.

У стандартній схемі адресації IPv4-адрес першого вузла в кожній підмережі призначається LAN-інтерфейсу маршрутизатора. WAN-інтерфейсами маршрутизаторів призначаються IP-адреси і маска для підмереж / 30.

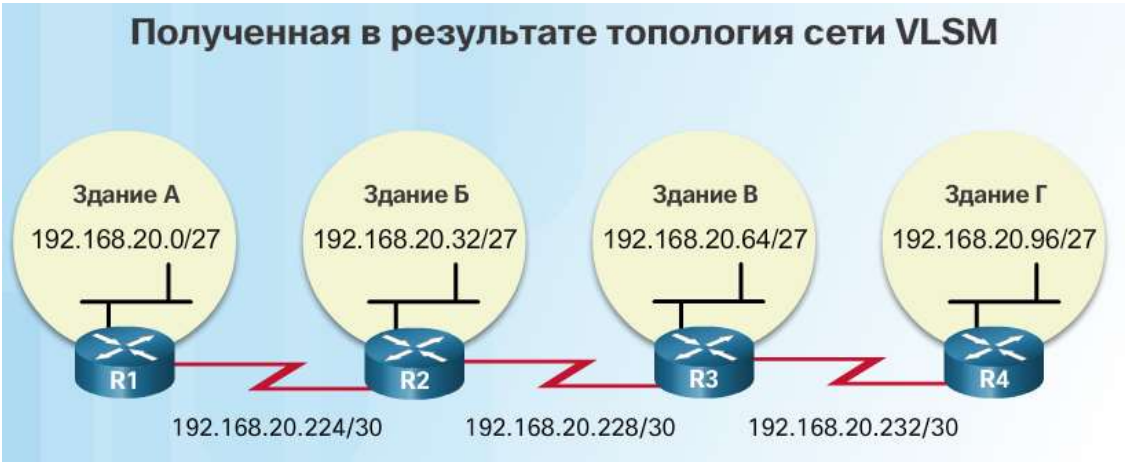


Рис. 2.1.22

Вузли в кожній підмережі матимуть IPv4-адрес з діапазону адрес цієї підмережі і відповідну маску. Вузли використовуватимуть адресу підключеного LAN-інтерфейсу маршрутизатора в якості адреси шлюзу за замовчуванням.

Шлюз за замовчуванням для вузлів Будинки А (192.168.20.0/27) буде 192.168.20.1.

Шлюз за замовчуванням для вузлів Будинки Б (192.168.20.32/27) буде 192.168.20.33.

Шлюз за замовчуванням для вузлів Будинки В (192.168.20.64/27) буде 192.168.20.65.

Шлюз за замовчуванням для вузлів Будинки Г (192.168.20.96/27) буде 192.168.20.97.

схема VLSM

Схема адресації може бути використана, щоб визначити, які блоки адрес доступні і які з них вже призначені, як показано на малюнку 1. Цей метод дозволяє запобігти призначення вже виділених адрес.

Як показано в схемі VLSM на малюнку 2, щоб більш ефективно використовувати адресний простір, для каналів мережі WAN були створені підмережі / 30. Щоб об'єднати невикористовувані блоки адрес в нерозривне адресний простір, остання підмережа / 27 була додатково розбита на підмережі для створення підмереж / 30. Перші 3 підмережі були призначені каналах мережі WAN.

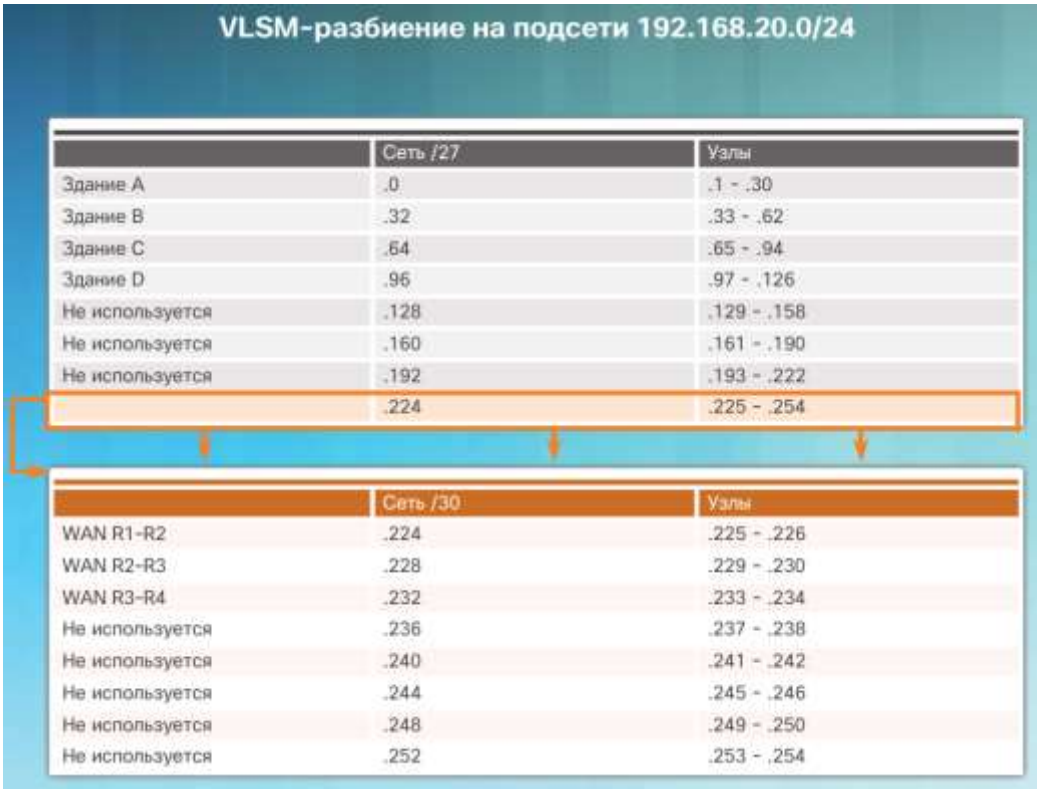


Рис. 2.1.23

При подібному проектуванні схеми адресації залишаються три невикористовувані підмережі з нерозривним адресним простором / 27 і п'ять невикористовуваних підмереж з нерозривним адресним простором / 30.

Планування адресації мережі

Як показано на малюнку, виділення в корпоративній мережі адресного простору на мережевому рівні необхідно ретельно спроектувати. Адреси не повинні призначатися випадковим чином.

При плануванні підмереж необхідно враховувати вимоги організації до використання мережі і передбачувану структуру підмереж. Для початку необхідно вивчити вимоги до мережі. Це означає, що потрібно вивчити всю мережу, визначити її основні частини і розділити їх на сегменти. План розподілу адрес містить інформацію про необхідному розмірі підмережі, кількості вузлів і принципі призначення адрес вузлам. Крім того, необхідно визначити вузли, яким потрібно виділити статичні IPv4-адреси, і вузли, які зможуть отримувати мережеві настройки по протоколу DHCP.

Визначаючи розмір підмережі, необхідно оцінити кількість вузлів, яким будуть потрібні IPv4-адреси в кожній підмережі в рамках розділеної приватної мережі. Наприклад, при проектуванні мережі кампусу потрібно оцінити кількість вузлів в локальній мережі адміністраторів, в локальній мережі викладачів і в локальній мережі учнів. У домашній мережі можна оцінити кількість вузлів в локальній мережі житлової зони і в локальній мережі домашнього офісу.

Як уже згадувалося раніше, діапазон приватних IPv4-адрес, які використовуються в локальній мережі (LAN), вибирається мережевим адміністратором, і до вибору цього діапазону слід поставитися з належною увагою. Необхідно переконатися, що кількості адрес буде достатньо для

активних в даний момент вузлів і для майбутнього розширення мережі. Запам'ятайте діапазони приватних IPv4-адрес:

10.0.0.0 - 10.255.255.255 з маскою підмережі 255.0.0.0 або / 8

172.16.0.0 - 172.31.255.255 з маскою підмережі 255.240.0.0 або / 12

192.168.0.0 - 192.168.255.255 з маскою підмережі 255.255.0.0 або / 16

На підставі вимог до IPv4-адрес можна визначити діапазон або діапазони вузлів для розгортання. Після розбиття обраного простору приватних IPv4-адрес на підмережі будуть отримані адреси вузлів, що відповідають вимогам до мережі.

Публічні адреси, використовувані для підключення до Інтернету, зазвичай виділяються оператором зв'язку. Хоча в даному випадку застосовуються ті ж принципи розбивки на підмережі, це не завжди є обов'язком адміністратора мережі організації.

Планування виділення адрес в мережі

На малюнку показано три основні моменти, які необхідно врахувати при плануванні виділення адрес.

Запобігання дублювання адрес: кожен вузол в мережевій інфраструктурі повинен мати унікальну адресу. Без належного планування та документування адреса може бути призначений декільком вузлам, що призведе до проблем доступу до мережі цих вузлів.

Надання доступу та управління ним: деякі вузли, такі як сервери, надають ресурси і внутрішнім, і зовнішнім вузлів. Призначений сервера адресу 3-го рівня можна використовувати для управління доступом до цього сервера. Якщо адреса призначена випадковим чином і ніде не задокументовано, управляти доступом буде складніше.

В рамках моніторингу безпеки та продуктивності вузлів мережевий трафік аналізується на наявність IP-адрес джерела, які генерують або отримують велике число пакетів. При належному плануванні і документуванні адресації в мережі проблемні пристрою можна легко виявити.

Присвоєння адрес пристроїв

У мережі існують пристрої різних типів, яким потрібні адреси, включаючи наступні:

Клієнтські пристрої кінцевих користувачів. Більшість мереж динамічно виділяють адреси за допомогою протоколу динамічної настройки вузла (DHCP). Це скорочує навантаження на персонал, який займається підтримкою мережі, і фактично усуває помилки введення. Також адреси видаються на певний період часу. Зміна схеми розбиття на підмережі означає необхідність повторної настройки DHCP-сервера та поновлення IP-адрес клієнтами. Клієнти IPv6 можуть отримати відомості про адресу за допомогою DHCPv6 або SLAAC.

Сервери і периферійні пристрої. Вони повинні мати передбачуваний статичний IP-адресу. Використовуйте суцільну нумерацію для таких пристроїв.

Сервери, доступні з Інтернету. У багатьох мережах сервери повинні бути доступні для віддалених користувачів. У більшості випадків цих серверів присвоюються приватні внутрішні адреси. Маршрутизатор або міжмережевий екран, розташовані по периметру мережі, повинні бути налаштовані на перетворення внутрішнього адреси сервера в публічний адресу.

Проміжні пристрої. Таким пристроїв адреси призначаються для управління мережею, її моніторингу та забезпечення безпеки. Оскільки нам необхідно знати, як зв'язатися з проміжними пристроями, у таких пристроїв повинні бути передбачувані статично задані адреси.

Шлюз. IP-адреси призначаються кожному інтерфейсу маршрутизаторів і пристроїв брандмауера, які служать шлюзом для вузлів в мережі. Як правило, для інтерфейсу маршрутизатора використовується наймолодший або найстарший адресу в мережі.

У таблиці на малюнку показаний приклад виділення адрес для невеликої мережі.

При проектуванні схеми IP-адресації зазвичай рекомендується використовувати готовий шаблон призначення адрес кожному типу пристроїв. Це допомагає адміністраторам додавати і видаляти пристрої, фільтрувати трафік на основі IP-адрес, а також спрощує документування.

Глобальний індивідуальну адресу IPv6

Поділ IPv6-мережі на підмережі має на увазі використання іншого підходу, ніж поділ на підмережі IPv4-мережі. Ті ж причини для розбиття адресного простору IPv4 на підмережі для управління мережевим трафіком існують і в разі IPv6. Однак через велику кількість IPv6-адрес економити адреси не доводиться. Головну увагу під час розподілу IPv6-адрес може бути приділено оптимальному ієрархічним підходу для управління і призначення підмереж IPv6. Щоб швидко отримати уявлення про структуру глобальних індивідуальних адрес IPv6, див. Малюнок.

Розбиття на підмережі IPv4 передбачає не тільки обмеження широкомовних доменів, але і боротьбу з нестачею адрес. Визначення маски підмережі і використання VLSM дозволяє заощадити адреси IPv4. Розбиття на підмережі IPv6 не припускав економії адресного простору. Ідентифікатор підмережі включає більш ніж достатньо підмереж. Метою розбиття IPv6-мережі на підмережі є створення ієрархії адрес на основі кількості необхідних підмереж.

Рис. 2.1.24

Як ви пам'ятаєте, існують два типи призначаються IPv6-адрес. Локальний адреса каналу IPv6 ніколи не розбивається на підмережі, оскільки він існує

тільки в локальному каналі. Однак, глобальний індивідуальну адресу IPv6 може бути розбитий на підмережі.

Глобальний індивідуальну адресу IPv6 зазвичай містить 48-розрядний глобальний префікс маршрутизації, 16-бітний ідентифікатор підмережі і 64-бітний ідентифікатор інтерфейсу.

Розбиття на підмережі з використанням ідентифікатора підмережі

Для створення внутрішніх підмереж організація може використовувати розділ 16-бітного ідентифікатора підмережі в глобальному індивідуальному адресу IPv6.

Ідентифікатор підмережі підтримує більш ніж достатньо підмереж і вузлів, які можуть знадобитися в одній підмережі. Наприклад, 16-бітний розділ дозволяє:

Створювати до 65 536/64 підмереж (без урахування можливості запозичення будь-якого числа біт з ідентифікатора інтерфейсу адреси).

Підтримувати до 18 квінтильйонів IPv6-адрес вузлів для кожної підмережі (тобто 18 000 000 000 000 000 000).

Примітка. Розбиття на підмережі за допомогою 64-бітного ідентифікатора інтерфейсу (або вузловий частини) також можливо, але потрібно рідко.

Крім того, розбиття на підмережі IPv6 простіше в реалізації, ніж IPv4, оскільки не потрібно виконувати перетворення в двійковий формат. Щоб визначити наступну доступну підмережа, досить розрахувати наступне шістнадцяткове число.

Наприклад, організації б присвоєно глобальний префікс маршрутизації 2001: 0DB8: ACAD :: / 48 з 16-бітовим ідентифікатором підмережі. Це дозволить організації створити 64 підмережі, як показано на малюнку. Зверніть увагу, що префікс глобальної маршрутизації є однаковим для всіх підмереж. Для кожної підмережі збільшується тільки гекстет ідентифікатора підмережі в шістнадцятковому форматі.

Процес сегментації мережі шляхом поділу її на кілька дрібніших мереж називається розбиттям на підмережі.

Кожен мережеву адресу містить допустимий діапазон адрес вузлів. Всі пристрої, підключені до однієї і тієї ж мережі, матимуть IPv4-адрес вузла цієї мережі, а також загальну маску підмережі або префікс мережі. Вузли можуть безпосередньо обмінюватися трафіком, якщо вони знаходяться в одній підмережі. Трафік не може передаватися між підмережами без використання маршрутизатора. Щоб визначити, чи є трафік локальним або віддаленим, маршрутизатор використовує маску підмережі. Префікс і маска підмережі - це різні способи представлення одного і того ж - мережевий частини адреси.

Для створення IPv4-підмереж ми задіємо один або кілька біт з вузловий частини в якості біт мережевої частини. Два істотних фактора, які впливають на визначення блоку IP-адрес за допомогою маски підмережі, - це кількість необхідних підмереж і максимальну кількість вузлів, яке повинно бути в підмережі. Існує зворотна залежність між числом підмереж і числом вузлів. Чим більше біт запозичене для створення підмереж, тим менше залишиться біт в вузловий частини і, отже, тим менше вузлів буде доступно в кожній підмережі.

Для розрахунку кількості адрес, які будуть доступні в кожній підмережі, використовується формула 2 ^ n (де n - кількість біт в вузловий частини). Однак мережеву адресу і широкомовний адресу недоступні для використання в рамках діапазону. Таким чином, необхідний розрахунок доступного для використання кількості адрес за формулою 2 ^ n-2.

Поділ підмережі на декілька підмереж з використанням маски підмережі довільної довжини (VLSM) дозволяє розподіляти набагато менше «зайвих» адрес.

Поділ IPv6-мережі на підмережі має на увазі використання іншого підходу, ніж поділ на підмережі IPv4-мережі. Простір IPv6-адрес поділяється не з метою економії адрес, а для забезпечення ієрархічної логічної структури мережі. Якщо IPv4-мережі поділяються на подсети в основному для боротьби з нестачею адрес, то метою поділу IPv6-мережі на підмережі є створення ієрархії адрес на основі кількості маршрутизаторів і обслуговуваних ними мереж.

Для забезпечення найкращого використання доступного адресного простору потрібне ретельне планування. У процесі планування адрес необхідно враховувати їх розмір, розташування, призначення та вимоги до доступу.

Після установки IP-мережі її необхідно протестувати для перевірки підключень і продуктивності.

2.2 Протоколи TCP/UDP. Транспортний рівень моделі OSI.

Мережі передачі даних і Інтернет об'єднують людей, забезпечуючи між ними надійний зв'язок. Один пристрій дозволяє використовувати різні додатки і сервіси, такі як електронна пошта, веб-ресурси і обмін миттєвими повідомленнями, які служать для відправки повідомлень або отримання інформації. Дані кожного з цих додатків упаковуються, передаються і доставляються відповідного додатку на пристрої призначення.

Процеси, описані в транспортному рівні OSI, забезпечують прийом даних від рівня додатків і їх підготовку для пересилання на мережевому рівні. Комп'ютер-відправник встановлює зв'язок з комп'ютером-одержувачем, щоб визначити, як розділити дані на сегменти, як запобігти їх втрати і як перевірити доставку всіх сегментів. Транспортний рівень можна порівняти з відділом відвантаження продукції, який займається підготовкою до відправки одного замовлення, що складається з декількох посилок.

Роль транспортного рівня

Рис. 2.2.1

Транспортний рівень відповідає за встановлення тимчасового сеансу зв'язку і передачу даних між двома додатками. Додаток створює дані, які пересилаються з програми на вузлі джерела з додатком на вузлі призначення незалежно від типу вузла призначення, а також середовища, в якій повинні передаватися дані, маршруту, використовуваного даними, перевантаження

каналу або розміру мережі. Як показано на малюнку, транспортний рівень - це канал між рівнем додатків і нижніми рівнями, які відповідають за передачу даних по мережі.

Функції транспортного рівня

Відстеження окремих сеансів зв'язку

На транспортному рівні кожен певний набір даних, що передаються між додатком джерела і додатком призначення, називається сеансом зв'язку (рис. 1). Вузол може мати кілька додатків, які одночасно обмінюються даними по мережі. Кожне з цих додатків взаємодіє з одним або декількома іншими додатками на одному або декількох віддалених вузлах. Транспортний рівень відповідає за підтримку та відстеження цих кількох сеансів зв'язку.

Сегментація даних і подальша збірка сегментів

Рис. 2.2.2

Дані необхідно підготувати для пересилки в середовищі, розділивши їх на відповідні для цього частини. У більшості мереж існують обмеження на обсяг даних, які можна включити в один пакет. Протоколи транспортного рівня включають сервіси, які поділяють дані додатків на окремі блоки необхідного розміру (рис. 2). Такий сервіс забезпечує інкапсуляцію, необхідну для кожної частини даних. До кожного блоку даних додається заголовок, який надалі використовується для повторного складання. Цей заголовок дозволяє відстежувати потік даних.

На вузлі призначення транспортний рівень повинен забезпечити відновлення окремих частин в один повний потік даних, придатний для обробки на рівні додатків. Протоколи на транспортному рівні описують, як використовувати інформацію в заголовку транспортного рівня для повторного

складання частин даних в потоки з метою їх подальшої передачі на рівні додатків.

визначення додатків

Щоб переслати потоки даних відповідних додатків, транспортному рівню необхідно визначити цільове додаток (рис. 3). Для цього транспортний рівень привласнює кожному з додатком окремий ідентифікатор - номер порту. Кожному програмного процесу, якому потрібен доступ до мережі, призначається номер порту, унікальний для цього вузла.

Мультиплексування сеансів зв'язку

При передачі по мережі даних деяких типів (наприклад, потокового відео) у вигляді одного повного потоку може використовуватися вся доступна смуга пропускання, що в свою чергу призведе до блокування інших процесів передачі даних, які виконуються в цей же час. Крім того, це ускладнює відновлення після збоїв і повторну передачу пошкоджених даних.

Як показано на малюнку, сегментація даних на більш дрібні блоки дозволяє чергувати (мультиплексировать) велика кількість різних процесів передачі даних від різних користувачів в одній і тій же мережі.

Транспортний рівень додає до кожного сегменту даних спеціальний заголовок, що складається з декількох полів в двійковому вигляді і дозволяє ідентифікувати сегменти. Саме значення в цих полях дозволяють різним протоколам транспортного рівня виконувати свої завдання з управління процесом передачі даних.

Надійність транспортного рівня

Транспортний рівень також відповідає за забезпечення надійності сеансу зв'язку. Різні програми висувають різні вимоги до надійності передачі даних.

Протокол IP відповідає тільки за структуру, адресацію і маршрутизацію пакетів. Він не визначає спосіб доставки або передачі пакетів. Транспортні протоколи наказують спосіб передачі повідомлень між вузлами. Як показано на малюнку, TCP / IP надає два протоколи транспортного рівня: TCP (протокол управління передачею) і UDP (протокол передачі датаграм користувача). Протокол IP використовує ці транспортні протоколи для забезпечення зв'язку і передачі даних між вузлами.

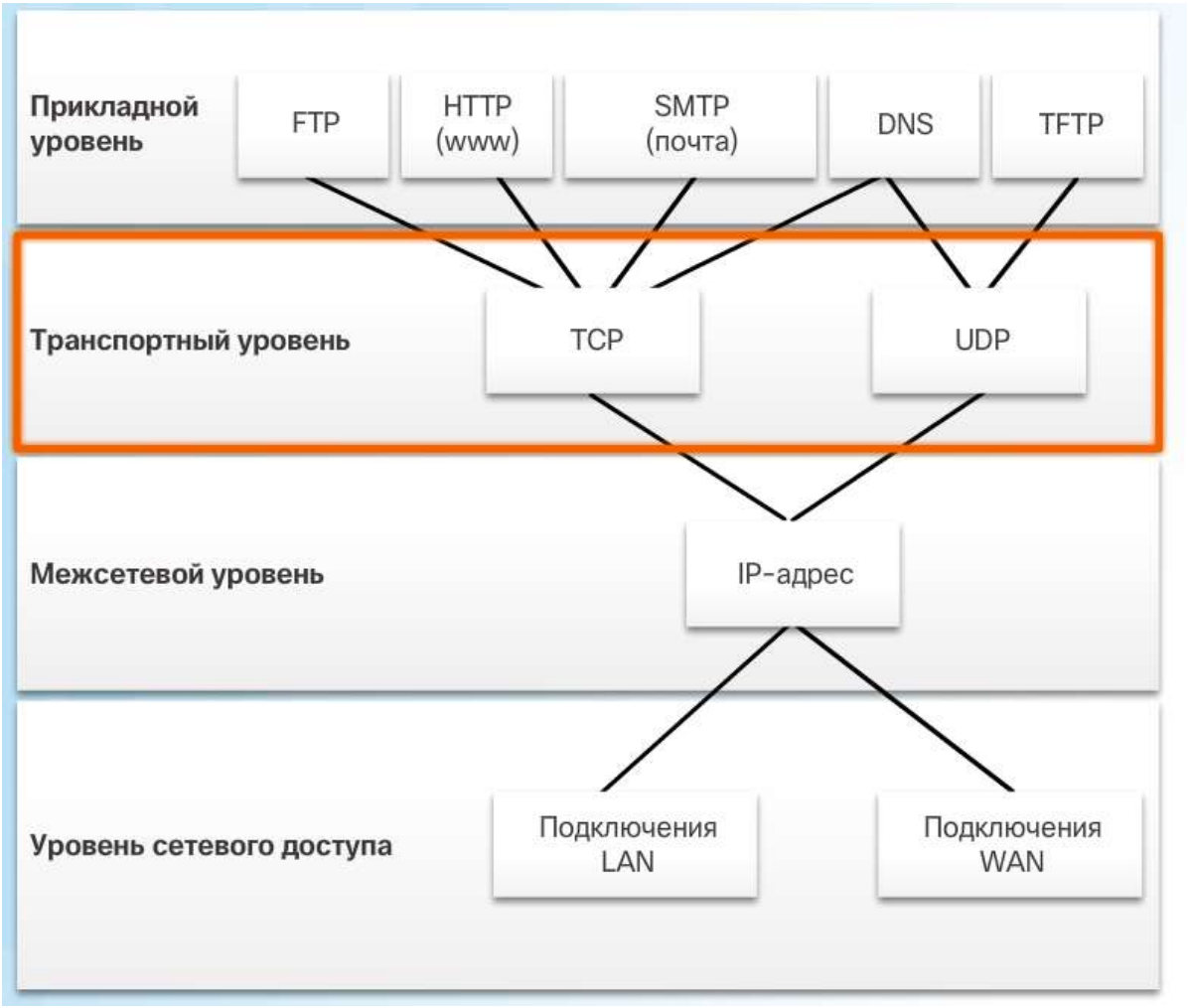


Рис. 2.2.3

TCP вважається надійним і повнофункціональним протоколом транспортного рівня, який забезпечує передачу всіх даних на вузол призначення. Однак це вимагає додаткових полів в заголовку TCP, що збільшує розмір пакетів, а також уповільнює процес передачі даних. UDP, на відміну від нього, - простіший протокол транспортного рівня, що не гарантує надійність. Він має менше полів, і тому швидше, ніж TCP.

TCP

Передача з використанням TCP аналогічна відправці пакетів з трекингом, шлях яких відстежується від відправника до одержувача. Якщо замовлення розбитий на кілька частин, замовник може зайти на веб-сайт транспортної компанії і подивитися порядок доставки.

TCP використовує такі три основні операції для забезпечення надійності.

Відстеження кількості сегментів, відправлених на той чи інший вузол тим чи іншим додатком.

Підтвердження отриманих даних.

Повторна передача сегментів з непідтвердженими даними після закінчення певного часу очікування.

UDP

Однак функції контролю доставки в протоколі TCP, що забезпечують надійне взаємодія додатків, викликають додаткові накладні витрати і можуть привести до затримок при передачі даних. Є певний компроміс між надійністю і тим навантаженням, яке вона представляє для мережевих ресурсів. Додаткові

накладні витрати, необхідні для забезпечення надійності деяких додатків, можуть знизити корисність самого додатка і навіть негативно позначитися на його продуктивності. У таких випадках перевагу слід віддати протоколу UDP.

Він забезпечує тільки основні функції для обміну сегментами даних між додатками. При цьому даний протокол відрізняється незначними накладними витратами і практично відсутністю перевірки даних. UDP відомий як протокол негарантованої доставки даних. Стосовно до комп'ютерних мереж негарантована доставка вважається ненадійною, оскільки при цьому немає підтвердження про отримання відправлених даних на вузлі призначення. UDP немає задіє процеси транспортного рівня, які повідомляють відправнику про успішну доставку даних.

Роботу протоколу UDP можна порівняти з відправкою по пошті звичайного, не замовного, листи. Відправник не знає, чи зможе адресат отримати лист, а поштове відділення не несе відповідальність за відстеження листи або інформування відправника про те, доставлено чи лист за адресою.

Відповідний протокол транспортного рівня для відповідного додатку

Деякі програми необхідно, щоб сегменти переданих даних надходили в строго визначеної послідовності, в якій вони можуть бути успішно оброблені. Іншим додаткам потрібно, щоб дані були повністю отримані перш, ніж їх можна буде використовувати. В обох випадках в якості транспортного протоколу використовується TCP. На підставі цих вимог розробники додатків повинні визначити, який транспортний протокол підходить для них найкраще.

Наприклад, таким програмам, як бази даних, веб-браузери та поштові клієнти, необхідно, щоб всі відправлені дані надійшли на вузол призначення в своєму первісному стані. Відсутність будь-якої інформації може привести до пошкодження даних, які в такому випадку будуть передані в повному обсязі або будуть нечитабельним. Тому ці програми розроблялися виключно для роботи по протоколу TCP.

В інших випадках втрата деяких даних під час передачі по мережі може бути допустима для додатка, але при цьому затримки передачі є неприпустимими. Таким додатків краще використовувати протокол UDP, оскільки він вимагає менших накладних витрат. Протокол UDP більш кращий для потокового відтворення аудіо, відео та передачі голосової інформації в режимі реального часу по протоколу IP (VoIP). Пересилання підтверджень і повторна передача можуть уповільнити доставку даних.

Наприклад, якщо один або два сегмента відеопотоку, переданого в режимі реального часу, не будуть доставлені, це викличе короткочасні перешкоди при передачі зображення. В такому випадку може призвести до шумів зображення або звуку, однак користувач цього може і не помітити. Якби пристрою призначення доводилося повторно запитувати втрачені дані, для їх повторного відправлення довелося б затримати весь потік, що призвело б до значного зниження якості звуку або зображення. В цьому випадку краще відобразити відео, наскільки якісно, наскільки це вийде зробити, використовуючи вже отримані сегменти, і пожертвувати надійністю.

Примітка. Додатки для потокової передачі збереженого аудіо і відео використовують протокол TCP. Наприклад, якщо ваша мережа несподівано не в змозі забезпечити пропускну здатність, необхідну для перегляду фільму за

запитом, додаток призупиняє відтворення відео. У цей час у вікні програвача може відображатися повідомлення про буферизації даних. В цей час протокол TCP намагається відновити потік. Після того як порядок всіх сегментів відновлений, а пропускна здатність мережі знаходиться на мінімально необхідному рівні, протокол TCP відновлює сеанс зв'язку, щоб продовжити відтворення.

Функції протоколу TCP

Щоб зрозуміти відмінності між протоколами TCP і UDP, необхідно з'ясувати, як кожен з них використовує певні засоби забезпечення надійності, а також як вони відстежують сеанси зв'язку. Крім підтримки таких базових функцій, як сегментація даних і їх зворотна зборка, протокол TCP, як показано на малюнку, також забезпечує наступні можливості.

Встановлення сеансу зв'язку

TCP є протоколом зі встановленням з'єднання. Перед пересиланням будь-якого трафіку протокол із установленням з'єднання погоджує і налаштовує постійне з'єднання (або сеанс) між пристроєм джерела і пристроєм призначення. Сеанс дозволяє пристроям узгодити обсяг трафіку, який можна переслати в заданий момент часу, а також ретельно контролювати передачу даних між цими двома пристроями.

надійність доставки

У мережевий термінології надійність (reliability) означає гарантовану доставку на вузол призначення всіх без винятку сегментів даних, відправлених вузлом-джерелом. Внаслідок багатьох причин при передачі по мережі один з сегментів може бути пошкоджений або повністю втрачено.

Доставка в однаковому порядку

Оскільки в мережах можуть використовуватися кілька маршрутів з різними швидкостями передачі інформації, в процесі доставки даних їх порядок може змінитися. Використовуючи нумерацію і упорядкування сегментів, TCP може гарантувати, що вони будуть зібрані в правильному порядку.

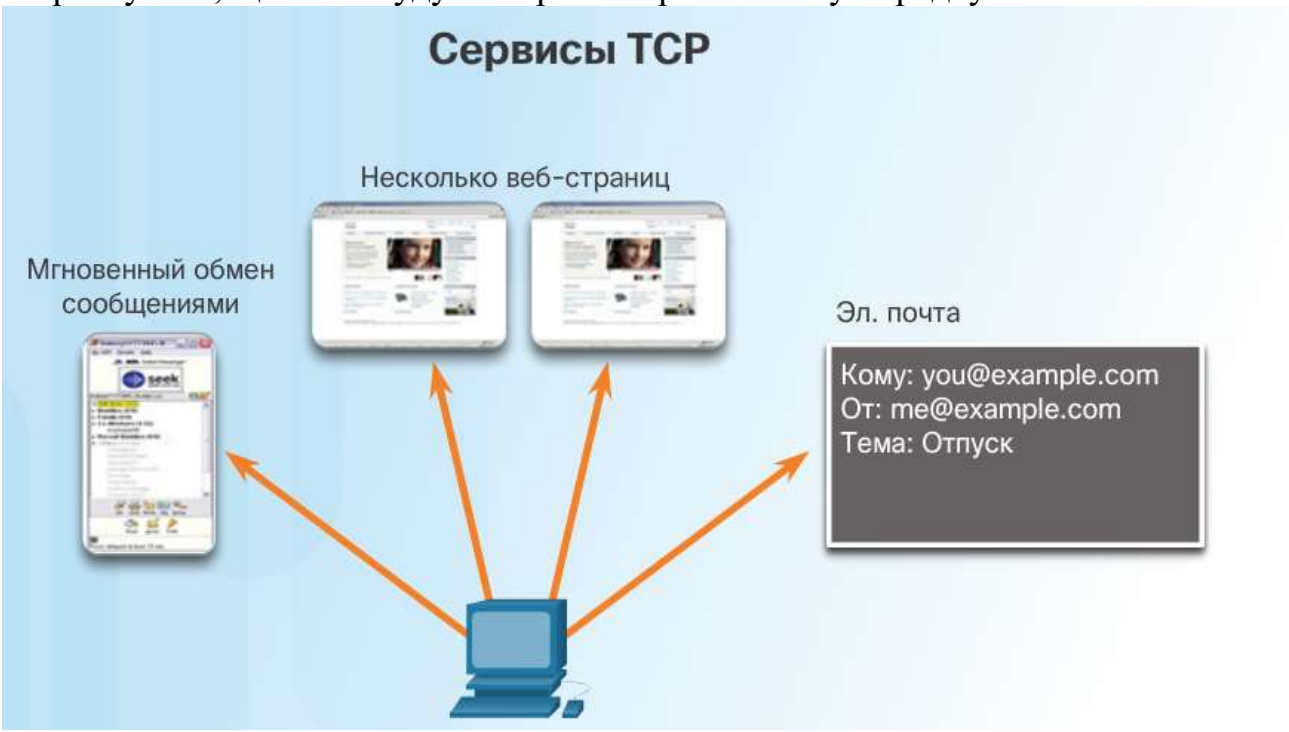


Рис. 2.2.4

Управління потоком передачі даних

Ресурси мережевих вузлів, такі як пам'ять або обчислювальні потужності, обмежені. Коли протокол TCP отримує інформацію про те, що ці ресурси використовуються надто активно, він може зажадати від відправляє додатки знизити швидкість потоку даних. Для цього TCP регулює кількість інформації, що передається джерелом. Функція управління потоком передачі даних дозволяє запобігти повторну відправку даних в разі, якщо ресурси одержує вузла перевантажені.

Заголовок протоколу TCP

Протокол TCP забезпечує контроль стану. Протокол з контролем стану відстежує стан сеансу передачі даних. Для відстеження стану сеансу зв'язку протокол TCP фіксує, яку інформацію він відправив, і яка інформація була підтверджена. Сеанс зв'язку з контролем стану починається з встановлення сеансу обміну даними і припиняється після його завершення.

Як показано на малюнку, кожен сегмент TCP містить 20 додаткових байтів в заголовку, інкапсуліруя дані рівня додатків.

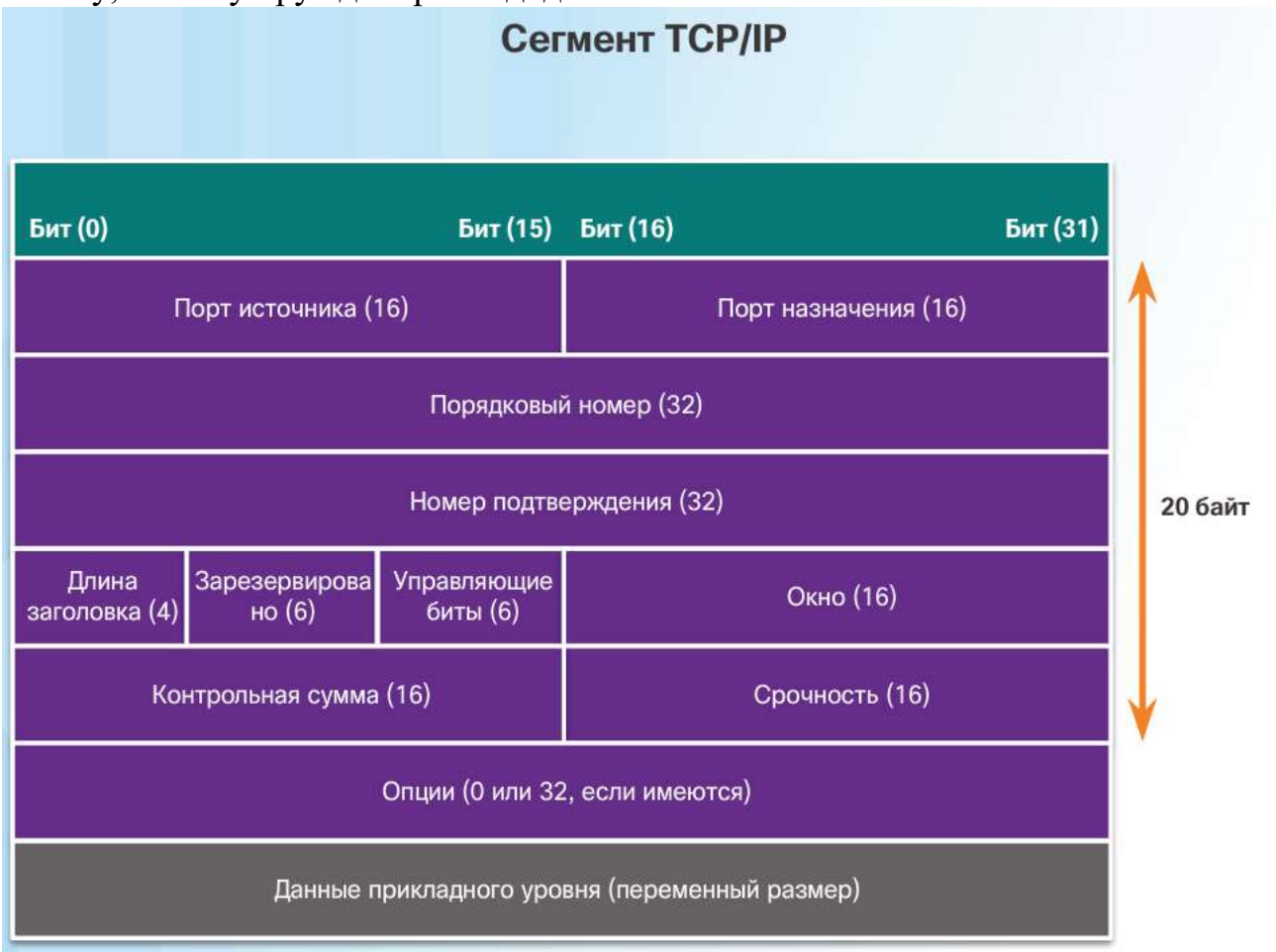


Рис. 2.2.5

Порт джерела (16 біт) і порт призначення (16 біт): використовується для визначення програми.

Порядковий номер (32 біта): використовується для повторного складання даних.

Номер підтвердження (32 біта): означає, що дані отримані.

Довжина заголовка (4 біта): параметр, який також називається зміщенням даних. Позначає довжину заголовка сегмента TCP.

Зарезервовано (6 біт): поле, зарезервоване для подальшого використання.

Біти управління (6 біт): включає двійкові коди, або прапори, які вказують призначення і функцію сегмента TCP.

Розмір вікна (16 біт): вказує кількість сегментів, які можна прийняти одночасно.

Контрольна сума (16 біт): використовується для перевірки помилок в заголовку і даних сегмента.

Терміновість (16 біт): позначає, чи є дані терміновими.

Функції протоколу UDP

Протокол передачі датаграм користувача (UDP) - це транспортний протокол негарантованої доставки. UDP - це полегшений транспортний протокол, який пропонує таку ж сегментацію і повторне складання даних, як і протокол TCP, але при цьому не забезпечує надійність і управління потоком, властиві TCP. UDP є настільки простим протоколом, що зазвичай описується з точки зору того, чого він не надає в порівнянні з протоколом TCP.

заголовок UDP

UDP - це протокол без відстеження стану (stateless), а це означає, що ні клієнт, ні сервер не зобов'язані відслідковувати стан сеансу зв'язку. Якщо при використанні UDP в якості транспортного протоколу потрібна надійність передачі даних, її має забезпечувати сам додаток.

Одним з основних вимог для передачі відео і голосу по мережі в режимі реального часу є наявність постійного високошвидкісного потоку. Додатки для передачі відео і голосу допускають втрати деякої кількості даних, які будуть ледь помітні або непомітні зовсім, і відмінно підходять для використання протоколу UDP.

Рис. 2.2.6

Частини повідомлення в UDP називаються датаграму, як показано на малюнку. Ці датаграми відправляються без гарантії доставки протоколом транспортного рівня. Протокол UDP забезпечує низькі накладні витрати (всього 8 байт).

Окремі сеанси зв'язку

Транспортний рівень повинен бути в змозі розділяти кілька каналів передачі даних з різними вимогами та керувати ними. Користувачі повинні мати можливість одночасно отримувати і відправляти пошту, обмінюватися миттєвими повідомленнями, переглядати веб-сайти і спілкуватися по телефону за допомогою VoIP. Кожне з цих додатків одночасно відправляє і отримує дані

по мережі, незважаючи на різні вимоги до надійності. Крім того, дані, що передаються під час телефонної розмови, не направляються в веб-браузер, а текст миттєвих повідомлень не відображається в листах електронної пошти.

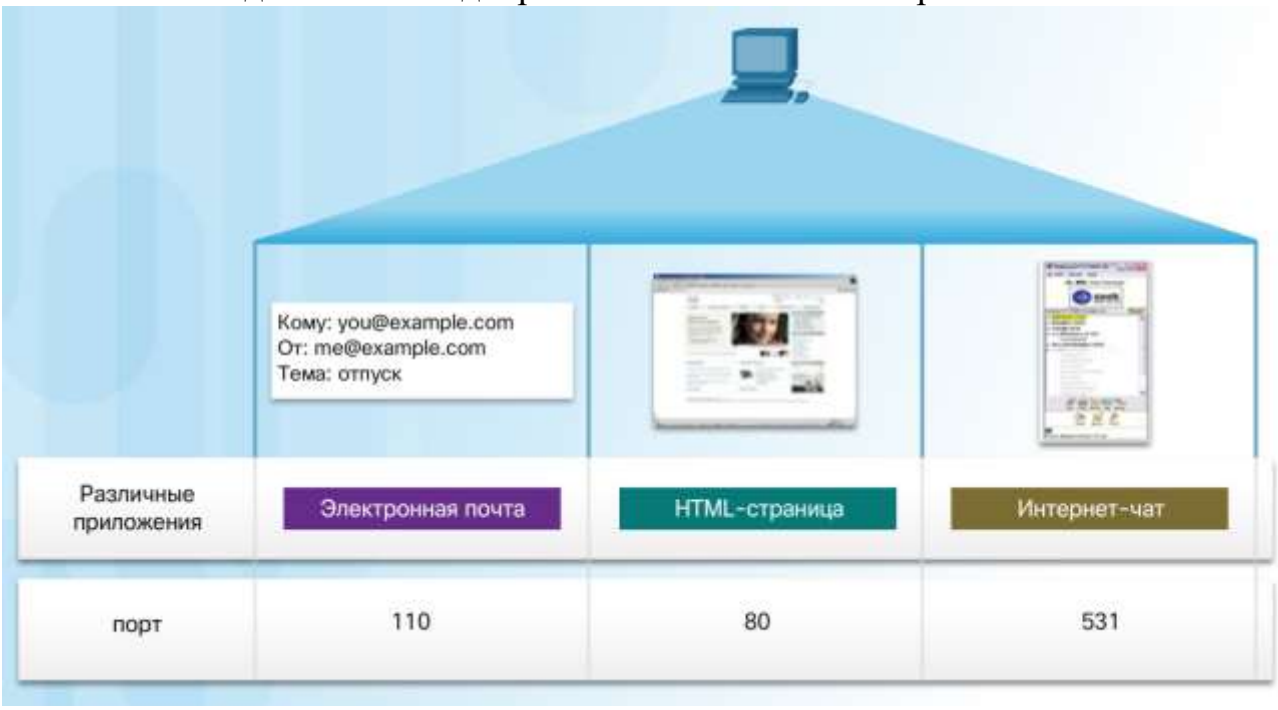


Рис. 2.2.7

Для управління такими одночасними сеансами зв'язку протоколи TCP і UDP використовують поля заголовка, які служать для унікальної ідентифікації відповідних додатків. У ролі таких унікальних ідентифікаторів виступають номера портів.

номери портів

Номер порту джерела пов'язаний з відправляють додатком на локальному вузлі. Номер порту призначення пов'язаний з додатком призначення на віддаленому вузлі.

порт джерела

Номер порту джерела генерується динамічним чином пристроєм-відправником для ідентифікації сеансу зв'язку між двома пристроями. Завдяки цьому можна встановлювати кілька сеансів зв'язку одночасно. Іншими словами, пристрій може одночасно передавати на веб-сервер відразу кілька запитів HTTP на обслуговування. Окремі сеанси зв'язку по протоколу HTTP відслідковуються за номерами портів джерела.

Порт призначення

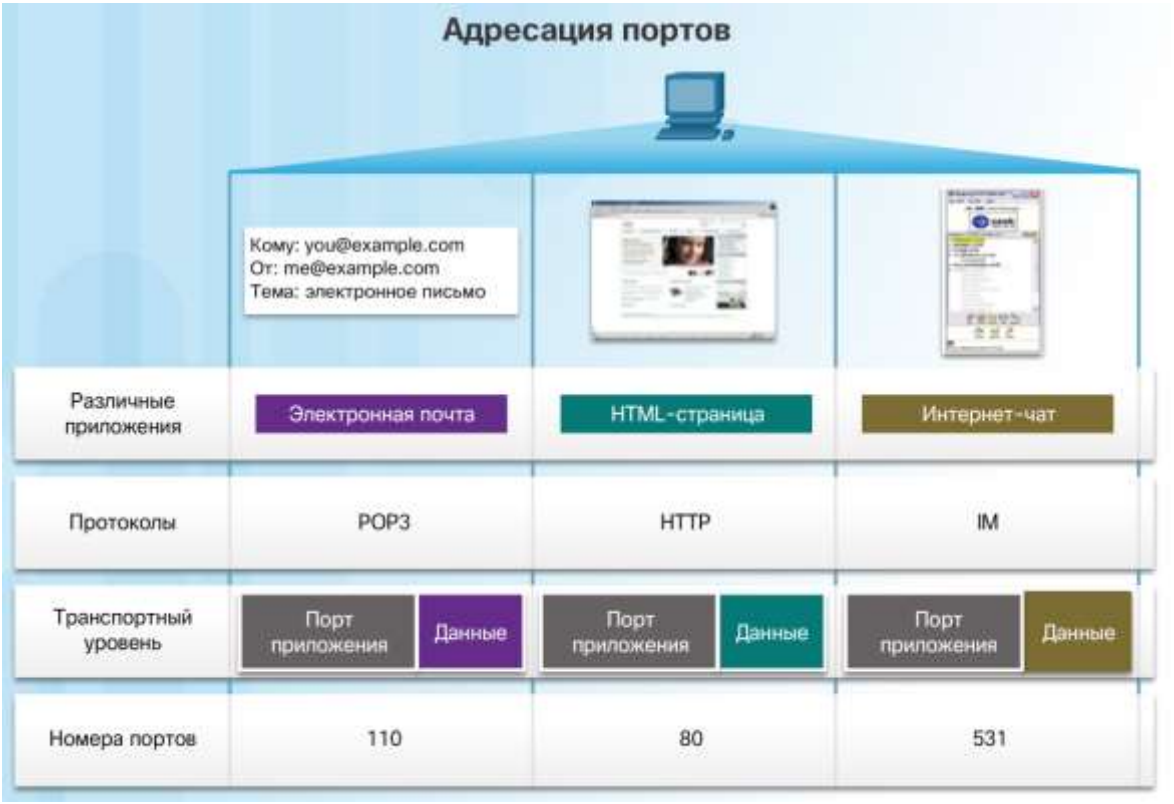


Рис. 2.2.8

Клієнт вказує номер порту призначення в сегменті, щоб повідомити сервер призначення інформацію про те, який сервіс запитується (див. Малюнок). Наприклад, якщо клієнт в описі для порту призначення вказує порт 80, то сервер, що приймає це повідомлення, вже знає, що запитуються веб-служби. Сервер може одночасно надавати веб-служби через порт 80 і організувати підключення по протоколу FTP через порт 21 для обміну файлами.

пари сокетов

Номери порту джерела і порту призначення записуються в сегмент. Потім ці сегменти инкапсулируются в пакеті IP. У пакеті IP записується IP-адреса джерела і призначення. Комбінація IP-адреси джерела і номера порту джерела або IP-адреси призначення і номера порту призначення називається сокетом. Сокет використовується для визначення сервера і служб, запропонованих клієнтом. Сокет клієнта може мати такий вигляд, де 1099 - це номер порту джерела: 192.168.1.5:1099.

Сокет веб-сервера може мати такий вигляд: 192.168.1.7:80.

Разом ці два сокета утворюють наступну пару: 192.168.1.5:1099, 192.168.1.7:80.

Сокети дозволяють розрізняти кілька процесів, що виконуються на клієнті, а також розпізнавати різні підключення до процесу сервера.

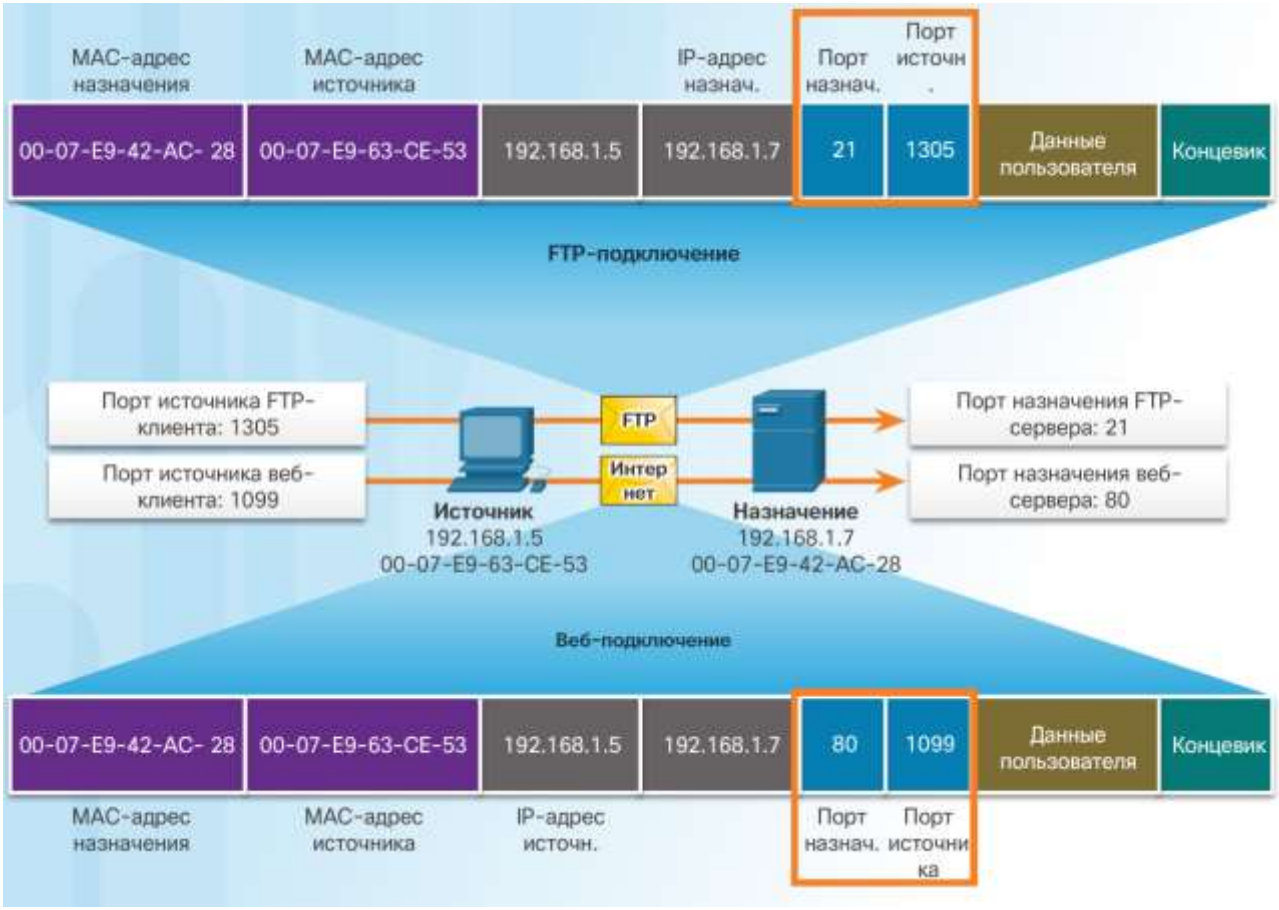


Рис. 2.2.9

Номер порту джерела грає роль зворотної адреси для запитувача додатки. Протоколи транспортного рівня відстежують порт і додаток-джерело запиту, щоб відповідному додатку можна було відправити відгук.

Групи номерів портів

Розробка різних стандартів адресації, включаючи нумерацію портів, виконується Адміністрацією адресного простору Інтернет (Internet Assigned Numbers Authority, IANA). Існує кілька типів номерів портів (див. Малюнок 1).

Загальновідомі порти (номера 0-1023). Ці номери зарезервовані для сервісів і додатків. Вони зазвичай використовуються додатками, такими як веб-браузери та поштові клієнти, а також клієнтами віддаленого доступу. За рахунок того, що добре відомі порти пов'язані з певними типами серверних додатків, клієнтські програми можна запрограмувати таким чином, щоб вони запитували підключення до цього конкретного порту і пов'язаного з ним сервісу.

Зареєстровані порти (номера 1024-49151). IANA за запитом організацій привласнює дані порти для будь-яких специфічних процесів або додатків. Ці процеси в основному являють собою окремі додатки, які користувач вирішив встановити, а не широко поширені програми, яким зазвичай присвоюють загальновідомі номери портів. Наприклад, для процесу HSRP (Hot Standby Routing Protocol) компанія Cisco зареєструвала порт 1985.

Динамічні або приватні порти (номера 49152-65535). Як правило, ці порти, які також називаються тимчасовими, динамічно присвоюються клієнтської ОС, коли ініціюється підключення до сервісу. Після чого такий порт використовується для визначення клієнтської програми під час обміну даними.

Примітка. У деяких клієнтських ОС для призначення портів джерела замість динамічних портів можуть використовуватися зареєстровані порти.

На рис. 2 показані деякі загальновідомі порти і пов'язані з ними програми. Деякі додатки можуть використовувати як протокол TCP, так і UDP. Наприклад, для відправки запитів клієнтів на DNS-сервер використовується протокол UDP. Однак взаємодія двох DNS-серверів один з одним завжди здійснюється по протоколу TCP.

команда netstat

Невідомі TCP-з'єднання можуть становити значну загрозу безпеці. Вони можуть вказувати на наявність сторонніх підключень до локального вузла. У деяких випадках потрібно визначити, які TCP-з'єднання відкриті і діють на мережевому вузлі. Перевірити стан цих з'єднань допомагає важливе програмний засіб - netstat. Команда netstat дозволяє отримати список використовуваних протоколів, локальних адрес і номерів портів, адреса і номер порту на віддаленому вузлі, а також повідомляє стан з'єднань.

За замовчуванням команда netstat намагається вирішити IP-адреси в імена доменів, а номери портів - в назви загальновідомих додатків. Щоб відобразити IP-адреси і номери портів в числовій формі, вкажіть параметр -n.

Процеси TCP-сервера

Кожен процес додатки, запущений на сервері, використовує певний номер порту (або заданий за замовчуванням, або налаштований вручну системним адміністратором). Не допускається використання двома різними службами на одному і тому ж сервері одного і того ж порту з однаковим протоколом транспортного рівня.

Наприклад, додаток веб-сервера і додаток передачі файлів, які запущені на одному вузлі, не можуть бути налаштовані на використання одного і того ж порту (наприклад, TCP-порту 80). Активне серверний додаток, якому присвоєно якийсь певний порт, вважається відкритим, що означає, що транспортний рівень може приймати і обробляти сегменти, що направляються на цей порт. Будь вхідний запит, який адресований правильному сокету, буде прийнятий, а дані будуть передані з додатком сервера. На сервері може бути одночасно відкрито відразу кілька портів, по одному для кожного активного застосування сервера.

Встановлення TCP-з'єднання

У деяких країнах при зустрічі двох людей прийнято обмінюватися рукостисканнями. Рукостискання розглядається обома сторонами як сигнал для дружнього вітання. Підключення в мережі здійснюються приблизно так само. При підключених по протоколу TCP клієнт вузла встановлює зв'язок з сервером.

в три етапи:

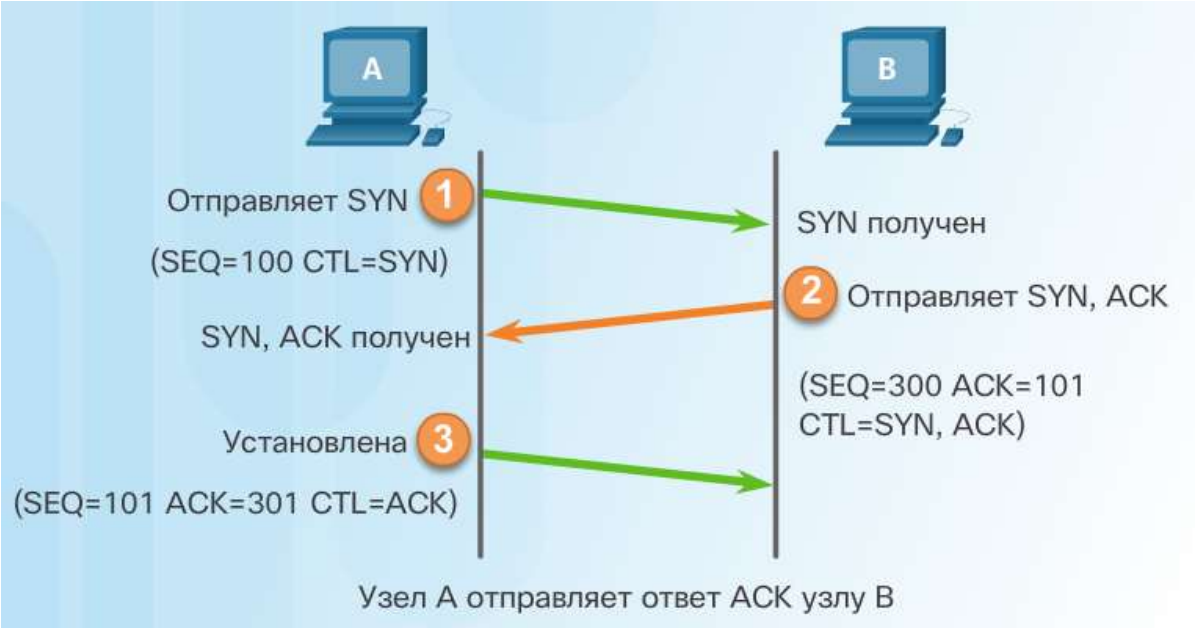


Рис. 2.2.10

Етап 1. Ініціює клієнт запитує сеанс обміну даними «клієнт-сервер» з сервером.

Етап 2. Сервер підтверджує сеанс обміну даними «клієнт-сервер» і запитує сеанс обміну даними «сервер-клієнт».

Етап 3. Ініціює клієнт підтверджує сеанс обміну даними «сервер-клієнт».

Припинення TCP-сеансу

Щоб розірвати з'єднання в заголовку сегмента повинен бути встановлений керуючий прапор Finish (FIN). Для завершення кожного одностороннього TCP-сеансу використовується двостороннє квитирование (рукостискання), яке складається з сегмента FIN і сегмента ACK (підтвердження). Отже, щоб завершити один сеанс зв'язку, підтримуваний протоколом TCP, необхідні чотири операції обміну даними, які завершать обидва сеансу.

Використовуйте кнопки 1-4 на малюнку, щоб подивитися процес закриття TCP-з'єднання.

Примітка. У даному трактуванні поняття «клієнт» і «сервер» використовуються в якості довідки для полегшення розуміння, але процес завершення зв'язку може бути ініційований будь-яким з двох вузлів з відкритим сеансом.

Етап 1. Коли у клієнта більше немає даних для відправки в потоці, він відправляє сегмент з встановленим прапором FIN.

Етап 2. Сервер відправляє підтвердження ACK, щоб підтвердити отримання FIN для завершення сеансу зв'язку «клієнт-сервер».

Етап 3. Сервер відправляє клієнту сегмент FIN, щоб завершити сеанс зв'язку «сервер-клієнт».

Етап 4. Клієнт відправляє у відповідь сегмент ACK для підтвердження отримання сегмента FIN від сервера.

Після підтвердження усіх сегментів сеанс закривається.

Аналіз тристороннього квитирования TCP

Вузли відстежують кожен сегмент даних, переданих під час сеансу, і обмінюються інформацією про отримані дані з використанням відомостей в заголовку TCP. TCP - це повнодуплексний протокол, в якому кожне з'єднання

являє два односторонніх потоку обміну даними, або сеансу. Для встановлення зв'язку вузли використовують тристоронню квитирование. Біти управління в заголовку TCP позначають етап і стан підключення.

Тристороння квитирование:

Спочатку встановлюється, чи присутній пристрій призначення в мережі.

Потім перевіряється, чи є на пристрої призначення активний сервіс і чи приймає він запити на номер порту призначення, який ініціює клієнт планує використовувати.

Далі пристрою призначення повідомляється, що клієнт джерела планує встановити сеанс зв'язку на цьому номері порту.

По завершенні обміну даними всі сеанси закриваються, а з'єднання переривається. Механізми підключення і здійснення сеансу зв'язку включають в себе функції TCP, що забезпечують надійність.

Шість бітів в поле бітів управління в заголовку сегмента TCP називаються прапорами. Кожен прапор являє собою біт, який або включений, або вимкнений. Клацніть поле бітів управління на малюнку, щоб відобразити всі ці шість бітів. Ми розглянули прапори SYN, ACK і FIN. Прапор RST використовується для скидання з'єднання при виникненні помилки або в разі перевищення часу очікування. Клацніть тут, щоб дізнатися докладніше про прапори PSH і URG.

Надійність TCP - впорядкована доставка

Сегменти, відправлені по протоколу TCP, можуть бути доставлені на вузол призначення в зміненому порядку. Щоб одержувач зміг розшифрувати початкове повідомлення, дані в цих сегментах повторно збираються в вихідному порядку. Для цього в заголовку кожного пакета вказуються порядкові номери. Порядковий номер відповідає порядковому номеру першого байта даних сегмента TCP.

Під час налаштування сеансу зв'язку задається початковий порядковий номер сеансу (ISN). Цей номер ISN є стартове значення лічильника байт, переданих віддаленого додатком. У міру передачі даних під час сеансу порядковий номер збільшується на число переданих байт. Таке відстеження байтів даних дозволяє однозначно визначати і підтверджувати кожен сегмент. Можна з'ясувати, які сегменти відсутні.

Рис. 2.2.11

Примітка. Номер ISN не обов'язково повинен починатися з «1», фактично це випадкове число. Це дозволяє запобігти певний тип шкідливих атак. Для зручності в прикладах в цьому розділі в якості номера ISN використовується число 1.

Порядкові номери сегментів вказують порядок повторного складання і впорядкування отриманих сегментів, як показано на малюнку.

Одержує TCP-процес поміщає дані з сегмента в який одержує буфер. Сегменти розташовуються відповідно до порядковими номерами і після повторного складання передаються на рівень додатків. Всі сегменти, які надходять з невідповідними порядковими номерами, зберігаються для подальшої обробки. Потім, коли надходять сегменти з відсутніми байтами, такі сегменти обробляються по порядку.

Управління потоком TCP. Розмір вікна і підтвердження

У протоколі TCP також є механізми управління потоком передачі даних, тобто об'ємом даних, який вузол призначення може надійно отримати і обробити. Управління потоком дозволяє підтримувати надійність передачі по протоколу TCP, регулюючи швидкість потоку даних між вузлами джерела і призначення протягом певного сеансу. Для цього в заголовку TCP є 16-бітове поле, яке називається «розмір вікна».

На малюнку наведено приклад розміру вікна і підтверджень. Розмір вікна - це кількість байтів, яке пристрій призначення здатне прийняти і обробити за один раз під час сеансу TCP. У цьому прикладі початковий розмір вікна вузла PC B для представленого сеансу TCP встановлений рівним 10 000 байт.

Починаючи з першого байта (з порядковим номером 1), останнім байтом, який вузол PC A може відправити без отримання підтвердження, буде 10 000-й байт. Це називається вікном відправки вузла PC A. Дані про розмір вікна включаються в кожен сегмент TCP, щоб вузол призначення міг в будь-який час змінити цей розмір в залежності від доступності ресурсів буфера.

Примітка. На малюнку джерело передає 1 460 байт даних в кожному сегменті TCP. Це називається максимальним розміром сегмента (MSS).

Початковий розмір вікна узгоджується під час встановлення сеансу TCP в процесі тристороннього квитирования. Пристрій джерела повинно обмежити кількість байт даних, відправлених пристрою призначення, відповідно до розміру вікна останнього. Тільки після того як пристрій джерела отримає підтвердження прийому байтів, воно може продовжити відправку інших даних в цьому сеансі. Зазвичай вузол призначення не чекає отримання всіх байтів для заданого розміру вікна, щоб відправити підтвердження. У міру отримання і обробки байтів вузол призначення відправляє підтвердження, щоб повідомити вузлу джерела про можливість продовжувати відправку додаткових байтів.

Зазвичай вузол PC B не чекає отримання 10 000-го байта, щоб відправити підтвердження. Це означає, що вузол PC A може відрегулювати своє вікно відправки в міру отримання підтверджень від вузла PC B. На малюнку показано, що при отриманні вузлом PC A підтвердження з номером 2 921 він збільшує вікно відправки ще на 10 000 байт (поточний розмір вікна вузла PC B) до 12 920. Після цього вузол PC A може продовжити відправку наступних 10 000 байт на вузол PC B, поки на 12 920-м байті не буде досягнуто нове вікно відправки.

Процес відправки підтверджень вузлом призначення в міру обробки отриманих байтів і постійне регулювання вікна відправки джерела називається «ковзаючі вікна».

Коли обсяг пам'яті, доступний в буфері вузла призначення знижується, він може зменшити розмір вікна і повідомити вузлу джерела про те, скільки байт тепер джерела слід відправляти без отримання підтвердження.

Рис. 2.2.12

Примітка. Пристрої зазвичай використовують протокол ковзають вікон. При використанні ковзних вікон одержувачу не потрібно чекати перед

відправкою підтвердження, поки розмір вікна досягне певної кількості байтів. Одержувач зазвичай відправляє підтвердження після отримання кожних 2 сегментів. Кількість таких сегментів, після яких відправляється підтвердження, може варіюватися. Перевага ковзають вікон полягає в тому, що цей протокол дозволяє відправнику передавати сегменти безперервно в тому випадку, якщо одержувач підтверджує отримання попередніх сегментів. Докладні відомості про ковзають вікнах не розглядаються в цій навчальній програмі.

Управління потоком TCP. запобігання перевантажень

У разі виникнення перевантаження в мережі перевантажений маршрутизатор перестає обробляти пакети. Коли пакети з сегментами TCP не доходять до свого вузла призначення, вони не підтверджуються. Визначивши швидкість передачі даних, при якій сегменти TCP відправляються, але не підтверджуються, вузол джерела може приблизно визначити рівень завантаженості мережі.

У разі перевантаження відбувається повторна передача втрачених сегментів TCP з вузла джерела. При відсутності належного контролю над повторною подібна відправка втрачених сегментів TCP може тільки погіршити ситуацію. Крім відправки в мережу нових пакетів з сегментами TCP виникає ефект зворотного зв'язку, коли передані повторно втрачені сегменти TCP ще більше перевантажують мережу. Щоб уникнути таких ситуацій і для запобігання перевантажень мережі в протоколі TCP передбачено низку відповідних механізмів, таймерів і алгоритмів.

Коли вузол джерела виявляє, що сегменти TCP не підтверджуються своєчасно або не підтверджуються зовсім, він може скоротити кількість байтів, які він відправляє, перш ніж отримає підтвердження. Слід зазначити, що вузол джерела скорочує саме кількість непідтверджених байтів, які він відправляє, а не розмір вікна, певний вузлом призначення.

Примітка. Докладні відомості про механізми, таймерах і алгоритмах, що використовуються для запобігання перевантажень, не включені в цей курс.

UDP: низькі накладні витрати або надійність?

UDP - це простий протокол, який забезпечує базові функції транспортного рівня. Він характеризується істотно меншими накладними витратами в порівнянні з протоколом TCP. Він не використовує встановлення з'єднання і не пропонує складні механізми повторної передачі даних, упорядкування та управління потоком, які забезпечують надійність.

Це зовсім не означає, що додатки, які використовують UDP, завжди ненадійні або що UDP - неповноцінний протокол. Це лише означає, що функції забезпечення надійності не реалізуються протоколом транспортного рівня і при необхідності повинні бути реалізовані на інших рівнях.

Низькі накладні витрати, властиві UDP, роблять його просто незамінним у випадках, коли потрібно протокол, який здійснює лише транзакції по відправці запитів і отримання відповідей. Наприклад, вибір на користь протоколу TCP для DHCP може обернутися непотрібним збільшенням обсягу мережевого трафіку. При виникненні проблем із запитом або відповіддю пристрій просто відправляє запит повторно, якщо відповідь на нього не отримано.

Збірка датаграмм UDP

Як і у випадку з сегментами TCP, коли на вузол призначення відправляються датаграми UDP, вони можуть використовувати різні шляхи і прибути в неправильному порядку. Протокол UDP не відслідковує порядкові номери, як це робить TCP. Як показано на малюнку, у UDP немає способу повторно скомпонувати датаграми в тому порядку, який використовувався при їх передачі.

Таким чином, протокол UDP просто повторно збирає дані в тому порядку, в якому вони були прийняті, і пересилає їх з додатком. Якщо послідовність даних важлива для роботи програми, воно повинно визначити правильну послідовність і вибрати оптимальний спосіб обробки даних.

Процеси і запити UDP-сервера

Як і додатків, що використовують протокол TCP, серверним додаткам на основі протоколу UDP присвоюються відомі або зареєстровані номера портів, як показано на малюнку. Коли ці додатки або процеси запущені на сервері, вони приймають дані, що збігаються з присвоєним номером порту. Якщо UDP отримує датаграмму, адресовану одному з цих портів, він пересилає дані додатки відповідного додатку виходячи з його номера порту.

Примітка. Сервер RADIUS (Remote Authentication Dial-in User Service), зображений на малюнку, надає служби перевірки автентичності, авторизації та обліку для управління доступом користувачів. Інформація про використання сервера RADIUS не включені в даний курс.

Програми, що використовують TCP

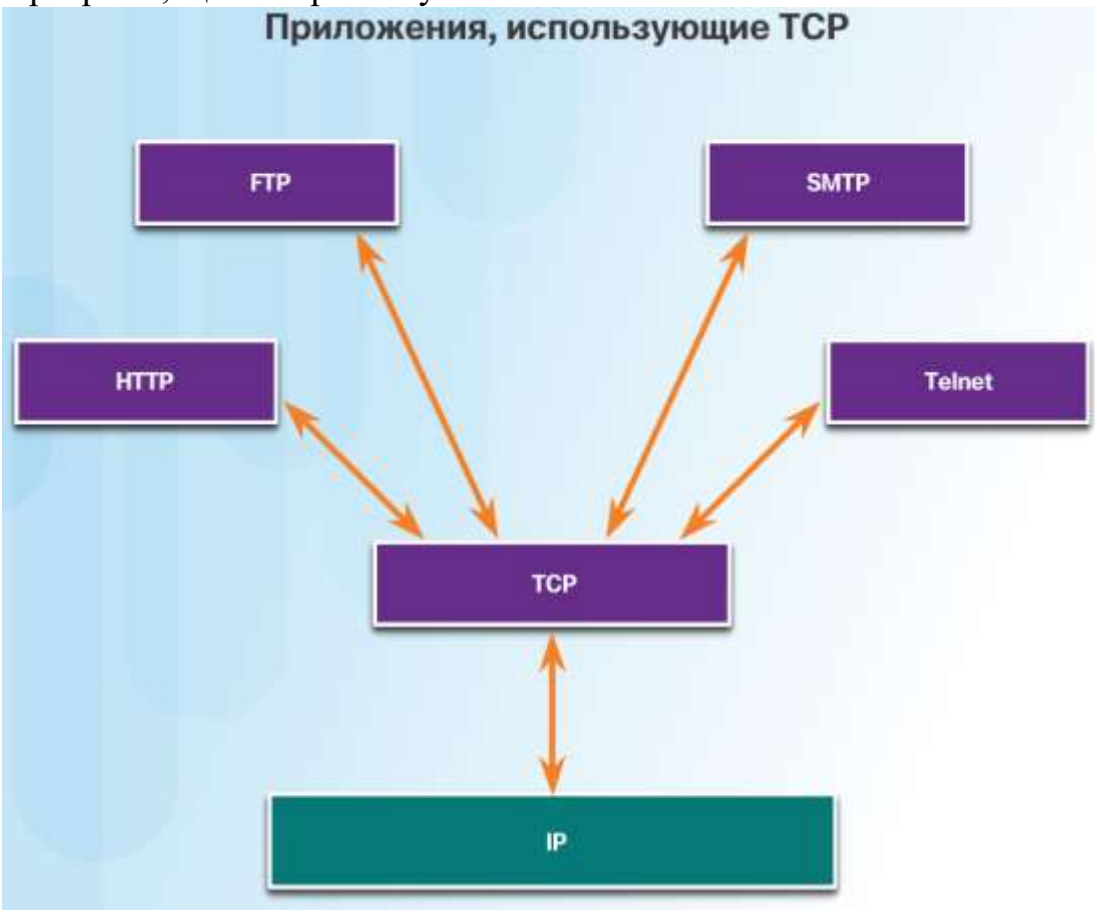


Рис. 2.2.13

Протокол TCP - це відмінний приклад того, як різні рівні набору протоколів TCP / IP можуть виконувати певні ролі. TCP сам виконує всі

завдання, пов'язані з розбивкою потоку даних на сегменти, забезпеченням надійності їх передачі, управлінням потоком і переупорядочение сегментів. TCP звільняє додаток від необхідності брати на себе управління будь-який з цих завдань. Додатки, подібні до тих, які показані на малюнку, можуть просто відправити потік даних протоколу транспортного рівня і використовувати сервіси TCP.

Програми, що використовують UDP

Існують три типи додатків, які найкраще підходять для роботи з протоколом UDP

Додатки для передачі аудіо в режимі реального часу і мультимедійні додатки - такі додатки допускають втрату деяких даних, однак для них важлива низька затримка або повна її відсутність Прикладами можуть служити VoIP і потокове відео.

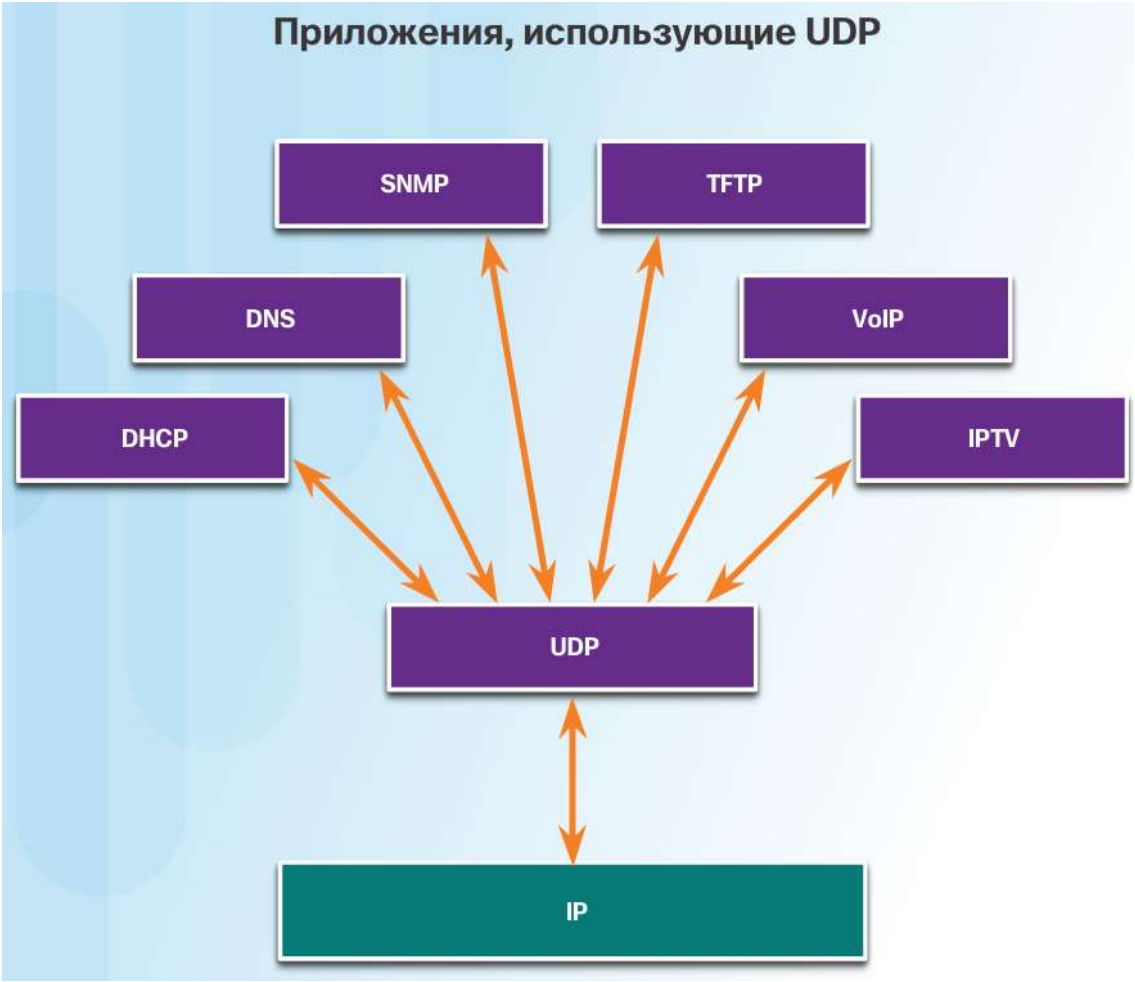


Рис. 2.2.14

Додатки, які здійснюють лише транзакції по відправці запитів і отримання відповідей, - коли вузол відправляє запит і невідомо, чи надійде відповідь чи ні Як приклад можна вказати DNS і DHCP.

Додатки, які самостійно забезпечують надійність передачі даних, - ненаправленої обмін даними, при якому управління потоком, виявлення помилок, відправка підтверджень і відновлення після збоїв не потрібні або виконуються самим додатком (наприклад, SNMP і TFTP).

І хоча DNS і SNMP за замовчуванням використовують протокол UDP, вони також можуть використовувати і TCP. DNS використовує протокол TCP в

разі, коли розмір DNS-запиту або DNS-відповіді перевищує 512 байт (наприклад, коли в DNS-відповіді міститься велика кількість дозволів імен). Аналогічним чином за певних обставин адміністратор мережі може налаштувати SNMP на використання протоколу TCP.

Транспортний рівень надає сервіси для доставки даних, використовуючи такі операції.

Поділ даних, отриманих від додатка, на сегменти

Додавання заголовка для визначення кожного сегмента і управління ним

Використання інформації в заголовку для повторного складання сегментів в дані додатки

Передача скомпонованих даних відповідного додатку

UDP і TCP - це поширені протоколи транспортного рівня.

Датаграми UDP і сегменти TCP мають заголовки, додані перед даними. Вони включають в себе номер порту джерела і номер порту призначення. Такі номери портів дозволяють направляти дані відповідному додатку, яке виконується на комп'ютері призначення.

Протокол TCP не надсилає дані в мережу до тих пір, поки не отримає від вузла призначення підтвердження готовності прийняти їх. Після цього TCP обробляє потік даних і повторно пересилає всі сегменти, які не були підтверджені як отримані вузлом призначення. Щоб забезпечити надійність, TCP використовує квитирование, таймери, повідомлення підтверджень і динамічна зміна вікна. Проте забезпечення надійності призводить до додаткових накладними витратами для мережі, оскільки при цьому потрібні великі заголовки сегментів і пересилання більшої кількості трафіку між вузлами джерела і призначення.

Якщо потрібно швидко доставити дані додатка по мережі або пропускна здатність мережі недостатня для додаткових накладних витрат, пов'язаних з пересиланням керуючих повідомлень між джерелом і адресатом, то розробникам слід вибирати UDP як протокол транспортного рівня. Протокол UDP не володіє ні однією з функцій забезпечення надійності, властивих TCP. Проте це зовсім не означає, що сам по собі обмін даними буде ненадійним. Протоколи рівня додатків можуть мати механізми і сервіси, які обробляють втрачені або відсталі датаграми, якщо це необхідно для застосування.

Розробник програми вибирає протокол транспортного рівня, який найкращим чином відповідає вимогам програми. Важливо пам'ятати, що всі інші рівні також беруть участь в процесі обміну даними по мережі і впливають на її продуктивність.

2.3 Сеансовий і прикладний рівень моделі OSI.

Такі програми, як веб-браузери, онлайн-ігри, чат та електронна пошта, дозволяють нам відносно легко відправляти і отримувати дані. Зазвичай ми користуємося цими додатками, навіть не замислюючись про те, як вони працюють. Однак мережеві фахівці зобов'язані знати, яким чином додаток може форматувати, передавати і інтерпретувати повідомлення, надісланого і отримуваного в мережі.

Використання багаторівневої структури моделі OSI спрощує візуалізацію механізмів, що дозволяють спілкуватися по мережі.

- рівень додатків
- рівень додатків

Рівень додатків найближче знаходиться до кінцевого користувача. Як показано на малюнку, на цьому рівні забезпечується взаємодія додатків, що використовуються для комунікації, і базової мережі, по якій передаються повідомлення. Протоколи рівня додатків використовуються для обміну даними між програмами, що виконуються на вузлі джерела і вузлі призначення.

Верхні три рівня моделі OSI (додатків, уявлення і сеансовий) визначають функції одного рівня додатків в моделі TCP / IP.

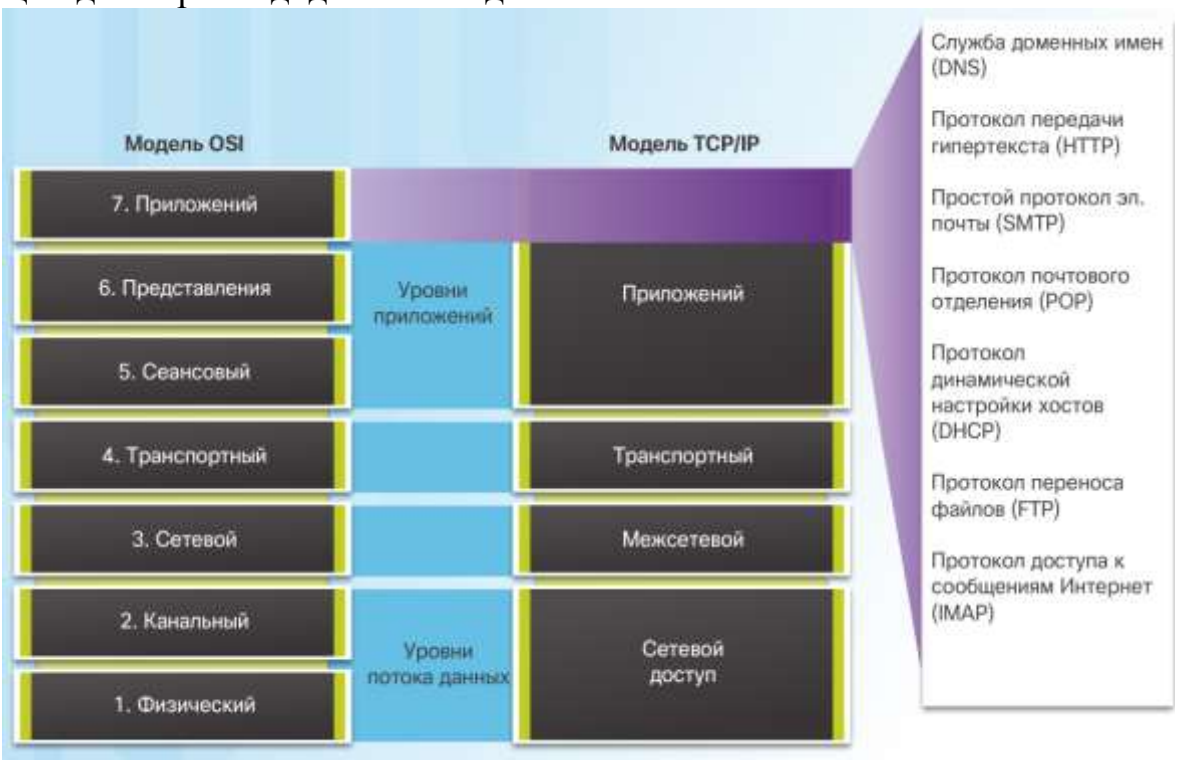


Рис. 2.3.1

Існує безліч протоколів програм, постійно розробляються нові протоколи. До деяких з найбільш відомих протоколів програм відносяться: протокол передачі гіпертексту (Hypertext Transfer Protocol, HTTP), протокол передачі файлів (File Transfer Protocol, FTP), простий протокол передачі файлів (Trivial File Transfer Protocol, TFTP), протокол доступу до повідомлень в Інтернеті (Internet Message Access Protocol, IMAP) і протокол системи доменних імен (Domain Name System, DNS).

- Рівень представлення і сеансовий рівень

- рівень представлення

Рівень представлення виконує три основні функції:

Форматування або подання даних з вихідного пристрою в формі, придатній для отримання пристроєм призначення

Стиснення даних таким чином, щоб їх можна було розпакувати на пристрої призначення

Шифрування даних для передачі і дешифрування при отриманні.

Як показано на малюнку, на рівні уявлення форматируются дані для рівня додатків і встановлюються стандарти форматів файлів. До числа широко відомих форматів відеофайлів відносяться QuickTime і Стандарт стиснення рухомих зображень (Motion Picture Experts Group, MPEG). До деяких з найбільш відомих форматів обміну графічними даними, які використовуються в мережах, відносяться Формат обміну графічними зображеннями (Graphics Interchange Format, GIF), Стандарт від об'єднаної групи експертів по фотографії (Joint Photographic Experts Group, JPEG) і Формат яку переносять мережевий графіки (Portable Network Graphics, PNG).

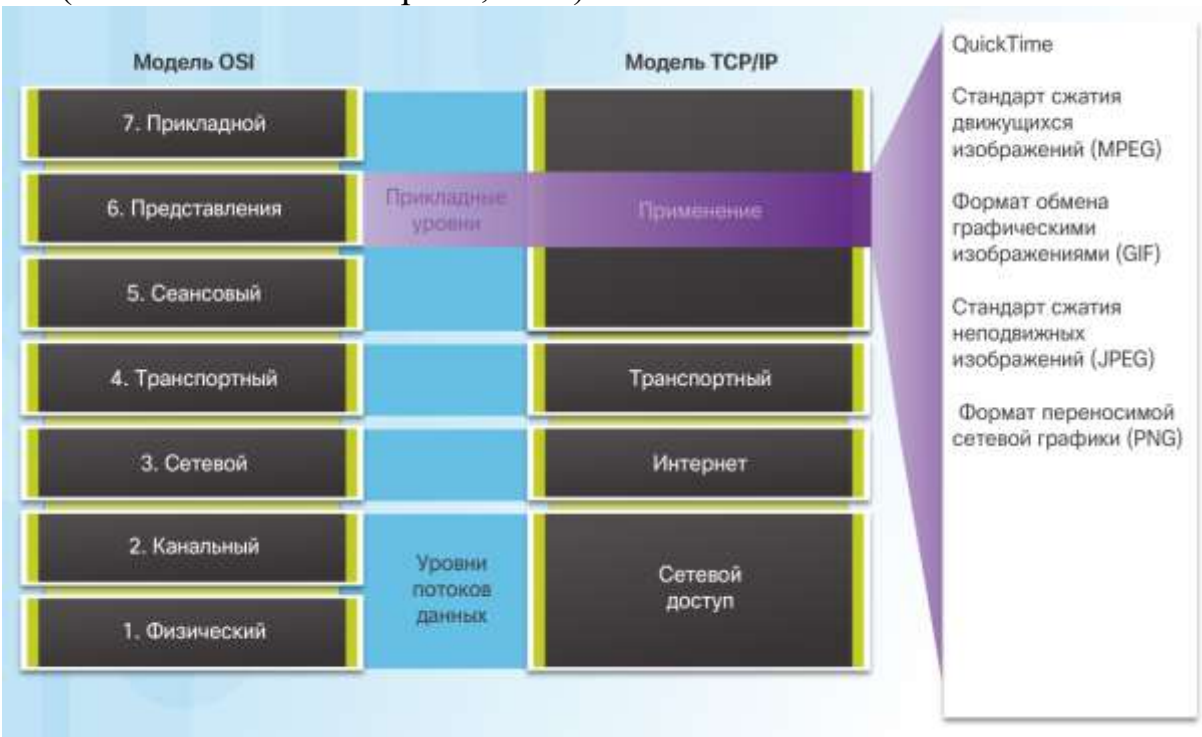


Рис. 2.3.2

сеансовий рівень

Як випливає з назви, функція сеансового рівня - встановлення і підтримання зв'язку між додатками джерела і призначення. На сеансовому рівні відбувається обмін даними для встановлення зв'язку, підтримки її в активному стані і для перезапуску сеансів, які були перервані або неактивні протягом тривалого часу.

Протоколи рівня додатків TCP / IP

Протоколи рівня додатків TCP / IP визначають формати і управляють даними, необхідними для багатьох поширених функцій обміну даними через Інтернет. Клацніть кожен протокол рівня додатків на малюнку, щоб дізнатися про нього більше.

Під час сеансу зв'язку протоколи рівня додатків використовуються і пристроями-джерелами, і пристроями призначення. Для успішного обміну даними протоколи рівня додатків на вузлах джерела і призначення повинні бути сумісними.

Модель «клієнт-сервер»

У моделі типу «клієнт-сервер» пристрій, що подає запит інформацію, називається клієнтом, а пристрій, який відповідає на цей запит, - сервером. Вважається, що процеси моделі «клієнт-сервер» відбуваються на рівні додатків. Клієнт починає обмін даними, відправляючи запит на отримання даних з сервера, який у відповідь відправляє один або кілька потоків даних клієнта. Протоколи рівня додатків описують формат запитів і відповідей між клієнтами і серверами. На додаток до фактичної передачі даних для цього обміну даними також може знадобитися аутентифікація користувачів і ідентифікація переданих файлів даних.

Одним із прикладів мережі типу «клієнт-сервер» є використання сервісу електронної пошти для відправки, отримання та зберігання повідомлень електронної пошти. Поштовий клієнт на домашньому комп'ютері відправляє запит серверу електронної пошти на отримання списку нових повідомлень. Сервер відповідає, відправляючи запитане повідомлення ел. пошти клієнта. Як показано на малюнку, передача даних в напрямку від клієнта до сервера називається відправкою (завантаженням на сервер, upload), а в напрямку від сервера до клієнта - скачуванням (завантаженням з сервера, download).

однорангові мережі

У моделі тимчасової мережі (P2P) дані запитуються з рівноправного пристрою без використання виділеного сервера.

Мережева модель P2P складається двох частин: P2P-мереж і P2P-додатків. Обидві частини мають схожі функції, але на практиці працюють по-різному.

У P2P-мережі два комп'ютери (або більше двох) підключаються між собою по мережі і можуть відкривати доступ до своїх ресурсів (наприклад, до принтерів і файлів) без використання виділеного сервера. Кожне підключений до мережі кінцеве пристрій (спеціальний робочий вузол) може виконувати функції як сервера, так і клієнта. Один комп'ютер може грати роль сервера для однієї операції, одночасно виступаючи в ролі клієнта для інших операцій. Ролі клієнта і сервера встановлюються в залежності від запиту.

Простий приклад обміну даними по мережі P2P показаний на малюнку. Крім підтримки функції файлового обміну подібна мережа дозволить користувачам запускати мережеві ігри або спільно використовувати підключення до Інтернету.

Найбільш поширені P2P-додатки

Всі комп'ютери в мережі, на яких запущено P2P-додаток, можуть виступати в ролі клієнта або сервера для інших комп'ютерів в мережі з цим же додатком. Найбільш поширені P2P-мережі:

- eDonkey
- G2
- BitTorrent
- Bitcoin

Деякі P2P-додатки розроблені на основі протоколу Gnutella, який передбачає обмін цілими файлами між користувачами. Як показано на малюнку, клієнтське програмне забезпечення, сумісне з протоколом Gnutella, дозволяє користувачам підключатися до сервісів Gnutella через Інтернет, а також знаходити і використовувати ресурси, доступ до яких був відкритий іншими одноранговими вузлами Gnutella. Існують різні клієнтські програми, які використовують протокол Gnutella, серед яких gtk-gnutella, WireShare, Shareaza і Bearshare.

Багато P2P програми дозволяють користувачам одночасно надавати один одному доступ до частин різних файлів. Для пошуку інших користувачів, які мають необхідними частинами файлів, клієнти використовують невеликі торрент-файли, які дозволяють встановлює підключення безпосередньо до цих користувачам. У цьому файлі також записана інформація про трекер, на якому зберігаються дані про те, якими файлами розташовують користувачі. Клієнти запитують частини файлів одночасно у різних користувачів, сукупність яких називають роєм. Ця технологія називається BitTorrent. Існує безліч різних клієнтів BitTorrent, наприклад BitTorrent, uTorrent, Frostwire і qBittorrent.

Примітка. До загального доступ можуть бути надані будь-які типи файлів. Багато з них захищені авторським правом. Це означає, що тільки правовласник може використовувати і поширювати такі файли. Завантаження та поширення файлів, захищених авторським правом, без згоди власника авторських прав є порушенням закону. Порушення авторського права може спричинити кримінальне обвинувачення і цивільні позови. Щоб більш детально ознайомитися з юридичною стороною питання, виконайте лабораторну роботу на наступній сторінці.

Протоколи HTTP і HTTPS

Протокол HTTP заснований на механізмі «запит-відповідь». Коли клієнт (зазвичай веб-браузер) відправляє запит веб-сервера, протокол HTTP визначає типи повідомлень, які використовуються для цієї взаємодії. Три основних типи повідомлень: GET, POST і PUT (див. Рис.):

GET - це запит даних клієнтом. Клієнт (веб-браузер) відправляє повідомлення GET веб-сервера, щоб запросити HTML-сторінки.

POST - відправляє на веб-сервер файли даних.

PUT - відправляє на веб-сервер ресурси і контент, наприклад зображення.

Незважаючи на те що протокол HTTP досить гнучкий, він не є безпечним. Повідомлення запиту передаються сервера відкритим текстом, який може бути перехоплений і прочитаний. Аналогічним чином, відповіді сервера (зазвичай це HTML-сторінки) передаються в незашифрованому вигляді.

Для захищеного двостороннього обміну даними в Інтернеті використовується захищена модифікація протоколу HTTP Secure (HTTPS). HTTPS дозволяє використовувати аутентифікацію і шифрування для захисту даних, що пересилаються між клієнтом і сервером. У HTTPS використовується той же процес «запит-відповідь», що і в HTTP, але потік даних зашифрована за допомогою SSL (Secure Socket Layer) перед передачею по мережі.

Протоколи електронної пошти

Один з основних сервісів, пропонованих інтернет-провайдерами (ISP) - розміщення (хостинг) серверів електронної пошти. Але щоб електронна пошта

заробила на комп'ютері або іншому кінцевому пристрої, необхідний ряд додатків і сервісів, як показано на малюнку. Електронна пошта - це набір засобів для доставки, зберігання та вилучення електронних повідомлень в мережі. Електронні листи зберігаються на серверах електронної пошти в базах даних.

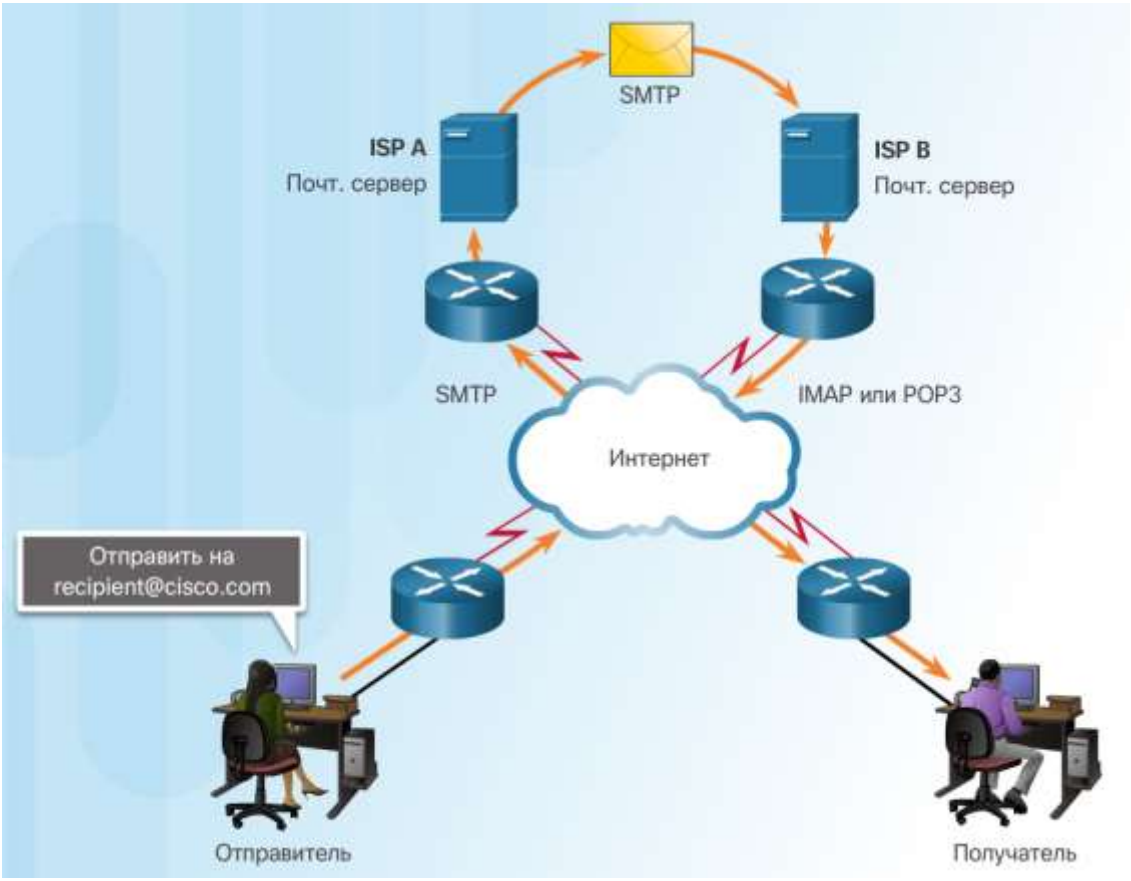


Рис. 2.3.3

Клієнти електронної пошти для відправки та отримання повідомлень звертаються до серверів електронної пошти. Сервери електронної пошти взаємодіють з іншими серверами електронної пошти для обміну повідомленнями між доменами. Поштовий покупець не з'єднується безпосередньо з іншим поштовим клієнтом для відправки повідомлення. Обидва клієнта повинні довірити транспортування повідомлень сервера електронної пошти.

Для роботи з електронною поштою використовуються три окремих протоколу: SMTP, POP і IMAP. В процесі рівня додатків, на якому виконується відправка пошти, використовується протокол SMTP. Але отримання електронної пошти клієнтом виконується по одному з двох протоколів програм: POP або IMAP.

Принцип роботи SMTP

У форматі SMTP повідомлення складається з заголовка і тіла повідомлення. Якщо тіло повідомлення може містити текст довільної довжини, то в заголовку адреси електронної пошти одержувача і відправника повинні бути вказані у відповідному форматі.

Коли клієнт відправляє повідомлення електронної пошти, процес SMTP-клієнта підключається до процесу SMTP-сервера на загальновідомому порте 25. Під час активного з'єднання, клієнт намагається відправити йому повідомлення

електронної пошти сервера. Коли сервер отримує повідомлення, він поміщає його в чергу повідомлень локального облікового запису або пересилає іншого сервера електронної пошти, як показано на малюнку.

Цільовий сервер електронної пошти (сервер призначення) в момент доставки повідомлення може виявитися недоступним або перевантажений. На цей випадок у SMTP передбачено тимчасове зберігання повідомлень з наступною повторної відправкою. Періодично сервер перевіряє чергу повідомлень і намагається відправити їх повторно. Якщо повідомлення не вдається доставити протягом встановленого часу, воно повертається відправнику з повідомленням про неможливість доставки.

Принцип роботи POP

Протокол POP для програм для отримання повідомлень від сервера електронної пошти. При використанні POP повідомлення завантажуються клієнтом з сервера і видаляються на сервері. Це принцип роботи POP за замовчуванням.

Мережевий сервіс POP на сервері пасивно очікує запитів підключення клієнтів до TCP-порту 110. Для використання цього мережевого сервісу клієнт відправляє запит на установку TCP-з'єднання з сервером. Після установки з'єднання сервер POP3 посилає вітання. Потім клієнт і сервер POP обмінюються командами і відповідями, поки підключення не буде закрито або перервано.

Так як при використанні POP повідомлення електронної пошти завантажуються клієнтом і видаляються з сервера, це означає, що вони не зберігаються централізовано. Так як протокол POP не зберігаються повідомлення, його недоцільно використовувати компаніям малого бізнесу, яким необхідне рішення для централізованого резервного копіювання.

Принцип роботи IMAP

Протокол IMAP передбачає інший метод отримання поштових повідомлень з сервера. Його відмінність від POP полягає в тому, що при підключенні користувача до сервера IMAP в клієнтську програму завантажуються тільки копії повідомлень. Вихідні повідомлення залишаються на сервері до тих пір, поки вони не будуть видалені вручну. Користувачі переглядають копії повідомлень в клієнтах електронної пошти.

Користувачі можуть організувати на сервері ієрархічну файлову структуру для впорядкування і зберігання пошти. Ця структура також дублюється клієнтом електронної пошти. Якщо користувач вирішує видалити повідомлення, воно синхронно видаляється з клієнта і з сервера.

Служба доменних імен (DNS)

У мережах передачі даних пристрою ідентифікуються по числовим IP-адресами для відправки та отримання даних. Доменні імена були створені для того, щоб перетворити числова адреса в просте і легко запам'ятовується ім'я.

Людям набагато простіше запам'ятати імена доменів у вигляді http://www.cisco.com, ніж 198.133.219.25, що є фактичною адресою даного сервера в числовому вигляді. Якщо компанія Cisco вирішить змінити числову адресу www.cisco.com, це станеться непомітно для користувачів, так як ім'я домену залишиться без змін. Нова адреса буде просто прив'язаний до існуючого імені домена без порушення зв'язку з сервером.

Протокол DNS визначає автоматизований сервіс, який зіставляє імена ресурсів з відповідними числовими адресами мереж. У цьому протоколі описується формат для запитів, відповідей і самих даних. При обміні даними по протоколу DNS використовується єдиний формат, який називається повідомленням. Такий формат повідомлення використовується для всіх типів запитів клієнта і відповідей сервера, повідомлень про помилки і передачі записів ресурсів між серверами.

Формат повідомлень DNS

На DNS-серверах зберігаються різні типи записів ресурсів, що використовуються для розпізнавання імен. Ці записи містять ім'я, адреса і тип запису. До деяких типів записи відносяться:

A - IPv4 адресу кінцевого пристрою

NS - довірений сервер імен

AAAA - IPv6 адресу кінцевого пристрою

MX - запис обміну поштовими повідомленнями.

Коли клієнт виконує запит, процес DNS-сервера спочатку шукає це ім'я в своїх записах, щоб дозволити його. Якщо ім'я не вдалося вирішити по локальних записів, сервер звертається до інших серверів для вирішення імені. Коли збіг знайдено, числова адреса повертається вихідного сервера, який певний час зберігає цей запис на випадок повторного запиту.

Клієнтський сервіс DNS на комп'ютері Windows також зберігає раніше дозволені імена в пам'яті. Команда ipconfig / displaydns виводить на екран всі збережені записи DNS.

ієрархія DNS

У протоколі DNS використовується ієрархічна структура для створення бази даних і розпізнавання імен. Ця ієрархія виглядає як перевернуте дерево з коренем нагорі і гілками, що ростуть вниз (див. Малюнок). Ієрархічна структура DNS будується по іменах доменів

і поділяється на невеликі керовані зони. У кожного DNS-сервера є окремий файл з базою даних. Сервер управляє прив'язкою імен до IP-адресами тільки в окремій невеликій частині загальної структури DNS. Отримавши запит на перетворення імені, який не належить до власної зоні DNS, DNS-сервер пересилає цей запит на обробку іншому DNS-сервера у відповідній зоні.

Примітка. DNS - це масштабований сервіс розпізнавання імен вузлів, який розподілений по безлічі серверів мережі.

Різні домени верхнього рівня представляють або певний вид організації, або країну походження.

команда nslookup

Під час налаштування мережевого пристрою вказують один або кілька адрес DNS-серверів, які клієнт DNS може використовувати для розпізнавання імен. Зазвичай адреси DNS-серверів надає інтернет-провайдер (ISP). Коли користувальницький додаток потрібне підключення до віддаленого пристрою по його імені, клієнт DNS опитує сервер імен, щоб перетворити ім'я в числову адресу.

В операційних системах комп'ютерів зазвичай є утиліта nslookup, яка дозволяє користувачеві вручну опитувати сервери для розпізнавання імен

вузлів. Цю утиліту можна також використовувати для усунення проблем з дозволом імен та для перевірки поточного стану серверів імен.

На рис. 1 показано, що після виконання команди nslookup виводиться DNS-сервер за замовчуванням, налаштований для даного вузла. У командному рядку nslookup можна ввести ім'я вузла або домену. Утиліта nslookup має багато параметрів для розширеного тестування і перевірки процесу DNS.

Протокол динамічної настройки мережевого вузла (Dynamic Host Configuration Protocol, DHCP)

Служба протоколу динамічної настройки вузла (DHCP) для IPv4 автоматизує призначення адрес IPv4, масок підмережі, шлюзів та інших мережевих параметрів IPv4. Це називається динамічної адресацією. Альтернативою динамічної адресації є статична адресація. При використанні статичної адресації адміністратор мережі вручну вводить дані IP-адрес на вузлах.

При підключенні вузла до мережі встановлюється зв'язок з DHCP-сервером і запитується адреса. DHCP-сервер вибирає адресу з заданого діапазону адрес, який називається пулом, і призначає його (здає в оренду) вузла.

У більших мережах, а також в мережах з часто змінюваними користувачами адреси бажано призначати за допомогою DHCP. Можуть з'явитися нові користувачі, яким потрібно підключитися до мережі. А іншим користувачам можуть встановити нові комп'ютери, які також вимагають підключення. Замість використання статичної адресації для кожного з'єднання набагато ефективніше автоматично призначати IPv4-адреси за допомогою DHCP.

Адреси, призначені за допомогою DHCP, видаються на певний час. Після закінчення цього часу адреса повертається в пул для повторного використання, якщо вузол був вимкнений або він відключений від джерела. Користувачі можуть вільно переходити на інше місце і знову підключитися до мережі по DHCP.

Як показано на малюнку, серверами DHCP можуть бути різні типи пристроїв. Сервер DHCP в більшості середніх і великих мереж зазвичай являє собою локальний виділений сервер на базі комп'ютера. У домашніх мережах сервер DHCP зазвичай знаходиться на локальному маршрутизаторі, який з'єднує домашню мережу з мережею інтернет-провайдера (ISP).

У більшості мереж використовується і DHCP, і статична адресація. DHCP використовується для вузлів загального призначення, таких як кінцеві призначені для користувача пристрої. Статична адресація застосовується для мережевих пристроїв: шлюзів, комутаторів, серверів і принтерів.

DHCPv6 (DHCP для IPv6) пропонує аналогічні сервіси для клієнтів IPv6. Важлива відмінність полягає в тому, що DHCPv6 не надає адресу шлюзу. Він може бути отриманий тільки динамічно за допомогою повідомлення «Відповідь маршрутизатора» (Router Advertisement, RA).

Принцип роботи DHCP

Як показано на малюнку, в той час коли пристрій IPv4 з налаштованим DHCP завантажується або підключається до мережі, клієнт виконує трансляцію розсилку повідомлення виявлення DHCP (DHCPDISCOVER), щоб знайти в

мережі всі доступні сервери DHCP. Сервер DHCP відповідає повідомленням з пропозицією DHCP (DHCPOFFER), яке дозволяє клієнту орендувати адресу. Повідомлення з пропозицією містить призначаються адресу IPv4 і маску підмережі, адресу IPv4 DNS-сервера і адреса IPv4 шлюзу. У реченні оренди також вказується її термін.

Клієнт може отримати кілька повідомлень DHCPOFFER, якщо в локальній мережі більше одного сервера DHCP. У такому випадку клієнт повинен вибрати одне з них, для чого він відправляє повідомлення із запитом DHCP (DHCPREQUEST), в якому клієнт вказує конкретний сервер і пропозиція оренди, яке він приймає. Клієнт також може запросити адреса, який раніше був привласнений йому сервером.

Якщо адреса IPv4, запитуваний клієнтом або пропонований сервером, як і раніше доступний, сервер повертає повідомлення з підтвердженням DHCP (DHCPACK), яке підтверджує, що дана адреса надано клієнту. Якщо пропозиція більше не дійсно, обраний сервер відповідає повідомленням з негативним підтвердженням DHCP (DHCPNAK). Якщо повернуто повідомлення DHCPNAK, процес вибору повинен початися повторно з відправкою нового повідомлення DHCPDISCOVER. Після того як клієнт орендував адреса, оренду необхідно буде продовжити до закінчення терміну її дії за допомогою іншого повідомлення DHCPREQUEST.

DHCP-сервер забезпечує унікальність всіх IP-адрес (один і той же IP-адреса не може бути призначений одночасно двом різним мережевих пристроїв). Більшість інтернет-провайдерів використовують DHCP для виділення адрес своїм клієнтам.

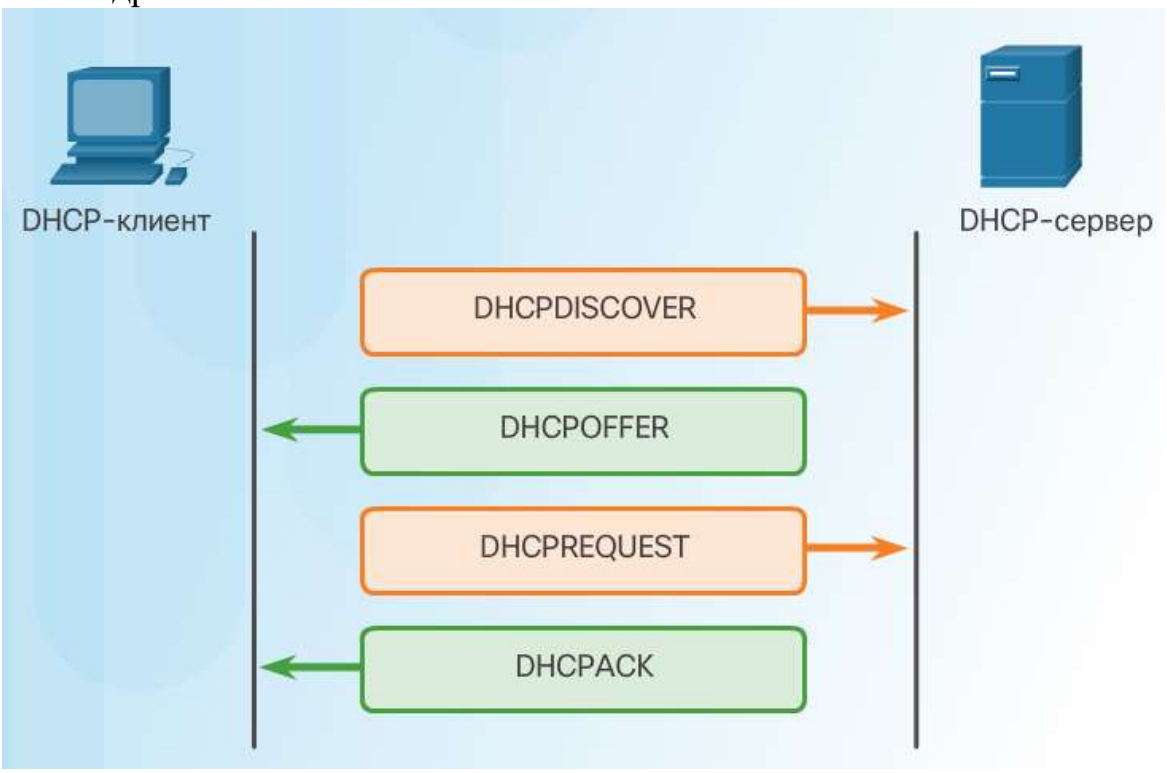


Рис. 2.3.4

DHCPv6 використовує набір повідомлень, аналогічний повідомленнями IPv4, показаним на рис. DHCPv6 використовує такі повідомлень SOLICIT, ADVERTISE, INFORMATION REQUEST і REPLY

Протокол передачі файлів

Протокол передачі файлів (FTP) - ще один поширений протокол рівня додатків. Протокол FTP був розроблений для передачі даних між клієнтом і сервером. FTP-клієнт являє собою додаток, запущене на комп'ютері, яке використовується для отримання даних з сервера, на якому функціонує служба FTP, або відправки даних на цей сервер

Як показано на малюнку, для передачі даних по FTP потрібно два з'єднання між клієнтом і сервером: одне для команд і відповідей, інше - для фактичної передачі файлів.

Клієнт встановлює перше з'єднання з сервером через порт 21 протоколу TCP для управління трафіком, який складається з команд клієнта і відповідей сервера.

Потім клієнт встановлює друге з'єднання з сервером для безпосередньої передачі даних через порт 20 протоколу TCP. Це підключення створюється для кожної передачі даних.

Дані можуть передаватися в будь-якому напрямку. Клієнт може завантажити (прийняти) дані з сервера або відправити (послати) дані на сервер.

протокол SMB

Протокол обміну блоками серверних повідомлень (Server Message Block, SMB) - це протокол обміну файлами між клієнтом і сервером, що описує структуру загальних ресурсів мережі, таких як каталоги, файли, принтери і послідовні порти. Це протокол типу «запит-відповідь». Всі повідомлення SMB мають загальний формат. У цьому форматі використовується фіксована довжина заголовка, після якого слід параметр змінного розміру і компонент даних.

За допомогою повідомлень SMB можна виконувати наступні дії:

Здійснювати запуск, аутентифікацію і завершення сеансів

Керувати доступом до файлів і принтерів

Вирішувати з додатком відправляти повідомлення на інший пристрій і приймати їх.

Загальний доступ до файлів і сервісів друку на основі SMB є відмінною рисою мереж Microsoft. Починаючи з серії систем Windows 2000 компанія Microsoft змінила базову архітектуру з використанням протоколу SMB. У попередніх версіях продуктів Microsoft в сервісах SMB для розпізнавання імен використовувався протокол, відмінний від TCP / IP. Починаючи з версії Windows 2000, у всіх наступних продуктах Microsoft використовується система доменних імен DNS, яка дозволяє протоколам TCP / IP безпосередньо підтримувати загальні ресурси SMB, як показано на рис. 1. На рис. 2 показаний процес обміну файлами по SMB між комп'ютерами з операційною системою Windows.

На відміну від обміну файлами по протоколу FTP, клієнти встановлюють довгострокове підключення до серверів. Після установки з'єднання користувач може отримати доступ до ресурсів на сервері аналогічно доступу до ресурсів на локальному вузлі.

Операційні системи LINUX і UNIX також дозволяють відкривати загальний доступ до ресурсів в мережах Microsoft, використовуючи версію SMB під назвою SAMBA. Операційні системи Apple Macintosh також підтримують роботу з загальними ресурсами по протоколу SMB.

Рівень додатків відповідає за прямий доступ до базових процесів, які керують обміном даними в мережі. Цей рівень виконує роль джерела і призначення повідомлень в мережах передачі даних. Додатки, сервіси та протоколи рівня додатків дозволяють користувачам взаємодіяти з мережею передачі даних ефективним і зрозумілим чином.

Додатки - це комп'ютерні програми, за допомогою яких користувач може почати процес передачі даних.

Сервіси - це фонові програми, які забезпечують зв'язок між рівнем додатків і більш низькими рівнями мережевої моделі.

Протоколи являють собою структуру загальноприйнятих правил і процесів, за допомогою яких сервіси, виконувані на одному пристрої, можуть обмінюватися даними з рядом різних мережевих пристроїв.

Доставка даних може здійснюватися від сервера клієнту за запитом або між однорангових пристроями. При обміні даними між однорагновими пристроями з'єднання типу «клієнт-сервер» встановлюється в залежності від того, які пристрої є вузлами джерела і призначення в поточний момент. Для установки і використання цих зв'язків сервіси рівня додатків на всіх кінцевих пристроях обмінюються повідомленнями у відповідності зі специфікаціями протоколу.

Наприклад, протоколи типу HTTP підтримують функцію доставки веб-сторінок на кінцеві пристрої. SMTP, IMAP і POP підтримують відправку та отримання електронної пошти. Протоколи SMB і FTP дозволяють користувачам відкривати доступ до своїх файлів. P2P-додатки спрощують обмін файлами в розподіленої мережі. Система доменних імен DNS служить для перетворення популярних імен, які використовуються для посилання на мережеві ресурси, в числові адреси, які може використовувати мережу. Хмарні сховища - це віддалені сервіси, де розміщуються дані і додатки, щоб користувачам не було потрібно багато локальних ресурсів. Крім того, такі сервіси спрощують доступ до вмісту з різних пристроїв з будь-якої точки світу.

Всі ці компоненти взаємодіють на рівні додатків. Рівень додатків дає користувачам можливість працювати і розважатися в мережі Інтернет.

Розділ Основи маршрутизації у локальних мережах

3.1 Статична маршрутизація

Маршрутизація виконується на рівні ядра мережі шляхом передачі даних через об'єднану мережу від джерела до одержувача. Маршрутизатор є пристрої, які відповідають за передачу пакетів з однієї мережі в іншу.

Маршрутизатор отримують дані про віддалених мережах динамічно за допомогою протоколів маршрутизації або вручну - за допомогою статичних маршрутів. У багатьох випадках маршрутизатори одночасно використовують протоколи динамічної маршрутизації і статичні маршрути. Дана глава присвячена статичної маршрутизації.

Статичні маршрути дуже поширені, при цьому вони не вимагають такої ж кількості обчислень і операцій, як протоколи динамічної маршрутизації.

У цій главі приклади топології використовуються для настройки статичних маршрутів IPv4 і IPv6, а також для демонстрації способів усунення неполадок. В рамках глави буде розглянуто ряд важливих команд IOS і відповідні вихідні дані. У цьому розділі також міститься знайомство з таблицею маршрутизації з використанням безпосередньо підключених мереж і додаються статичних маршрутів.

Маршрутизатора можна повідомити про віддалених мережах одним з двох способів:

Вручну - віддалені мережі вручну вводяться в таблицю маршрутизації за допомогою статичних маршрутів.

Динамічно - віддалені маршрути автоматично додаються за допомогою протоколу динамічної маршрутизації.

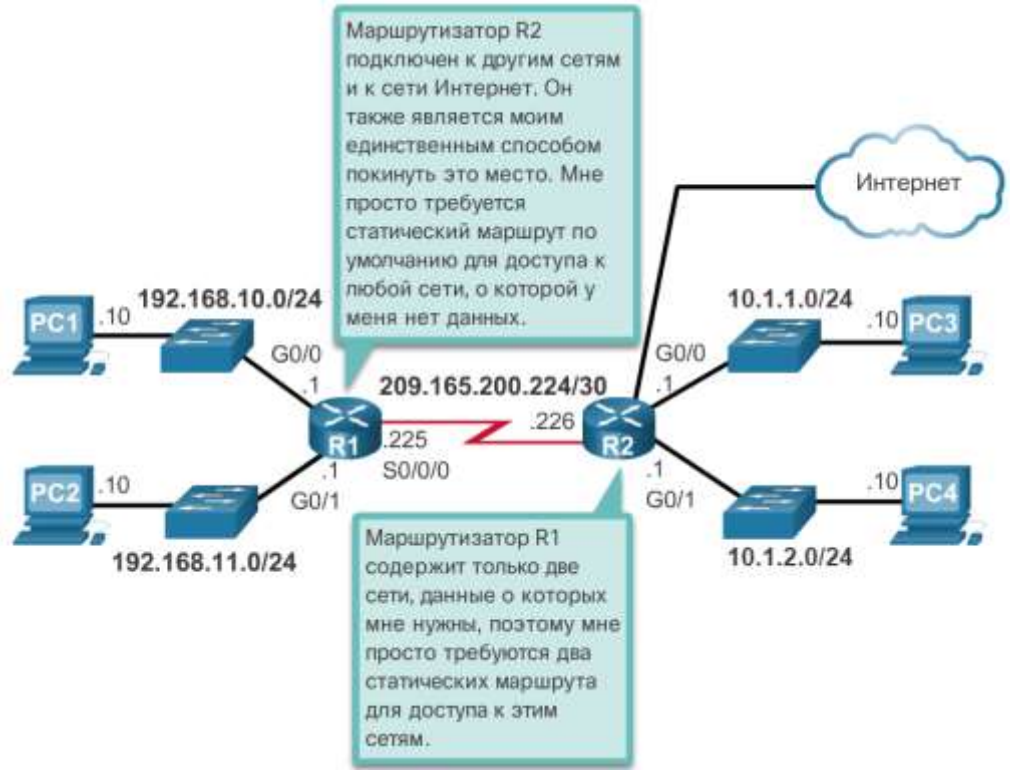


Рис. 3.1.1

На рис. представлений приклад сценарію статичної маршрутизації. Адміністратор може вручну налаштувати статичний маршрут для доступу до

конкретної мережі. На відміну від протоколу динамічної маршрутизації, статичні маршрути не оновлюються автоматично, і при змінах в мережевій топології їх необхідно повторно налаштовувати вручну.

Статична маршрутизація має свої переваги в порівнянні з динамічної маршрутизацією, а саме:

статичні маршрути не оголошуються по мережі, що робить їх більш безпечними.

Статичні маршрути використовують більш вузьку смугу пропускання, ніж протоколи динамічної маршрутизації; для розрахунку і зв'язку маршрутів цикли ЦП не використовуються.

Шлях, який використовується статичним маршрутом для відправки даних, відомий.

Використання статичної маршрутизації також має недоліки:

Початкове налаштування і її підтримка вимагають тимчасових витрат.

При налаштуванні часто припускаються помилок, особливо в великих мережах.

Для внесення змін до даних маршруту потрібне втручання адміністратора.

Недостатні можливості масштабування для зростаючих мереж, обслуговування при цьому стає досить трудомістким.

Для якісного впровадження потрібно доскональне знання всієї мережі.

На малюнку представлено порівняння функцій динамічної та статичної маршрутизації. Зверніть увагу, що переваги одного методу одночасно є недоліками іншого.

Статичні маршрути рекомендується використовувати в невеликих мережах, для яких заданий тільки один шлях до зовнішньої мережі. Вони також забезпечують безпеку в великих мережах з певним типом трафіку або в каналах до інших мереж, для яких потрібні розширені функції контролю. Важливо розуміти, що статична і динамічна маршрутизація не є взаємовиключними. У більшості мереж використовується комбінація протоколів динамічної маршрутизації і статичних маршрутів. Це може привести до того, що для маршрутизатора задається кілька шляхів до мережі призначення за допомогою статичних маршрутів і динамічно одержуваних маршрутів. Однак слід пам'ятати, що значення адміністративного відстані (AD) є критерієм вибору джерел маршруту. Джерела маршрутів з низькими значеннями AD краще джерел маршрутів з більш високими значеннями AD. Значення AD для статичного маршруту дорівнює 1. Таким чином, статичний маршрут має пріоритет над усіма динамічно отриманими маршрутами, які будуть мати більш високі значення AD.

Завдання статичної маршрутизації

Статична маршрутизація використовується в трьох ситуаціях:

- забезпечення спрощеного обслуговування таблиці маршрутизації в невеликих мережах, які не планується суттєво розширювати.
- маршрутизація до тупикових мереж і від них. Тупикова мережа являє собою мережу, доступ до якої здійснюється через один маршрут, і маршрутизатор має тільки одне сусіднє пристрій.

- використання єдиного маршруту за замовчуванням для подання шляху до будь-якої мережі, що не має більш точного збігу з іншим маршрутом в таблиці маршрутизації. Маршрути за замовчуванням використовуються для відправки трафіку в будь-який пункт призначення за межами наступного маршрутизатора в висхідному напрямку.

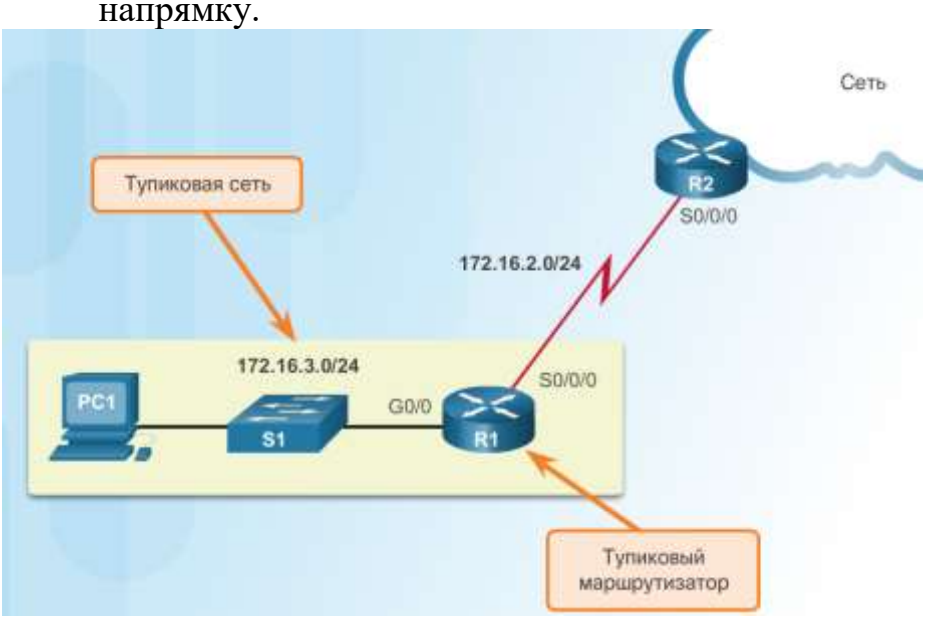


Рис. 3.1.2

На малюнку представлений приклад підключення до тупикової мережі і використання маршруту за замовчуванням. Зверніть увагу, що на малюнку у будь-якій мережі, підключеної до маршрутизатора R1, буде тільки один шлях для доступу до інших місць призначення (до мереж, підключеним до маршрутизатора R2, або до місць призначення за межами маршрутизатора R2). Це означає, що мережа 172.16.3.0 є тупиковою, а маршрутизатор R1 - тупиковим маршрутизатором.

У цьому прикладі статичний маршрут можна налаштувати на маршрутизаторі R2 для доступу до мережі LAN маршрутизатора R1. Крім того, оскільки для маршрутизатора R1 існує тільки один спосіб відправки нелокального трафіку, статичний маршрут за замовчуванням можна налаштувати на маршрутизаторі R1 для вказівки на маршрутизатор R2 як на наступний перехід для всіх інших мереж.

Як показано на малюнку, статичні маршрути найчастіше використовуються для підключення до конкретної мережі або надання «шлюзу останньої надії» для тупикової мережі. Їх також можна використовувати для таких цілей:

зменшення числа оголошених маршрутів шляхом об'єднання деяких суміжних мереж в один статичний маршрут;

створення резервного маршруту на випадок відмови основного маршруту.

Далі ми розглянемо такі типи статичних маршрутів IPv4 і IPv6:

- стандартний статичний маршрут;
- статичний маршрут за замовчуванням;
- сумарний статичний маршрут;
- плаваючий статичний маршрут.

Протоколи IPv4 і IPv6 підтримують настройку статичних маршрутів. Статичні маршрути рекомендується використовувати при підключенні до певної віддаленої мережі.

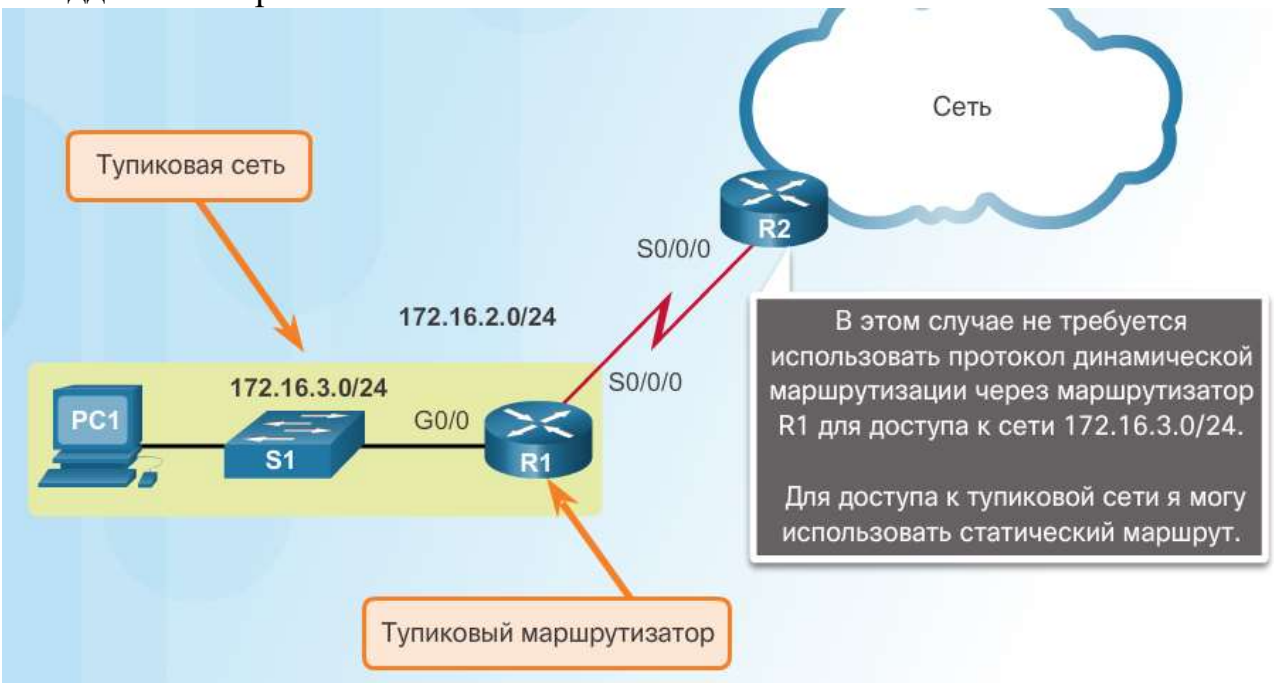


Рис. 3.1.3

На малюнку показано, що маршрутизатор R2 можна налаштувати з використанням статичного маршруту для доступу до тупикової мережі 172.16.3.0/24.

Примітка. В даному прикладі продемонстровано тупикова мережа, але насправді статичний маршрут можна використовувати для підключення до будь-якої мережі.

Маршрут за замовчуванням - це маршрут, який відповідає всім пакетам і використовується маршрутизатором, якщо пакет не відповідає жодному з інших, більш точних маршрутів з таблиці маршрутизації. Маршрут за замовчуванням можна отримати динамічно або налаштувати статично. Статичний маршрут за замовчуванням - це просто статичний маршрут з IPv4-адресою призначення, рівним 0.0.0.0/0. Під час налаштування статичного маршруту за замовчуванням створюється «шлюз останньої надії».

Статичні маршрути за замовчуванням використовуються в наступних випадках:

При відсутності інших маршрутів в таблиці маршрутизації, які збігаються з IP-адресою призначення пакета - іншими словами, за відсутності більш точного збігу. Статичні маршрути часто використовуються при підключенні прикордонного маршрутизатора компанії до мережі інтернет-провайдера.

Якщо маршрутизатор підключений тільки до одного маршрутизатора. У такій ситуації цей маршрутизатор називають тупиковим.

Для зменшення числа записів в таблиці маршрутизації можна об'єднати кілька статичних маршрутів в один статичний маршрут. Це можливо за таких умов:

Рис. 3.1.4

Мережі призначення є суміжними і можуть бути об'єднані в один мережеву адресу.

Всі статичні маршрути використовують один і той же вихідний інтерфейс або один IP-адреса наступного переходу.

Як видно з малюнка, маршрутизатора R1 потрібно чотири окремих статичних маршруту для підключення до мереж в діапазоні 172.20.0.0/16 - 172.23.0.0/16. Замість цього можна налаштувати один сумарний статичний маршрут, який буде забезпечувати підключення до цих мереж.

Примітка. Додаткові відомості про розрахунок та налаштування об'єднаних статичних маршрутів см. В додатку до глави.

Ще одним типом статичного маршруту є плаваючий статичний маршрут. Плаваючі статичні маршрути - це статичні маршрути, які використовуються для надання резервного шляху основного статичному маршруту або динамічному маршруту на випадок збою в роботі каналу. Плаваючий статичний маршрут використовується тільки тоді, коли основний маршрут недоступний.

Для цієї мети плаваючий статичний маршрут налаштовується за більш високим значенням адміністративного відстані, ніж основний маршрут. Адміністративне відстань визначає надійність маршруту. При наявності декількох шляхів до адресою призначення маршрутизатор вибирає шлях з найнижчим значенням адміністративного відстані.

Припустимо, що адміністратор повинен створити плаваючий статичний маршрут в якості резервного для маршруту, одержуваного по протоколу EIGRP. При налаштуванні плаваючого статичного маршруту необхідно використовувати більш високе значення адміністративного відстані, ніж для EIGRP. EIGRP має адміністративне відстань 90. Якщо плаваючий статичний маршрут налаштований з адміністративним відстанню 95, то динамічний маршрут, встановлений за допомогою EIGRP, має пріоритет перед плаваючим статичним маршрутом. Якщо маршрут, одержуваний по EIGRP, втрачений, то замість нього використовується плаваючий статичний маршрут.

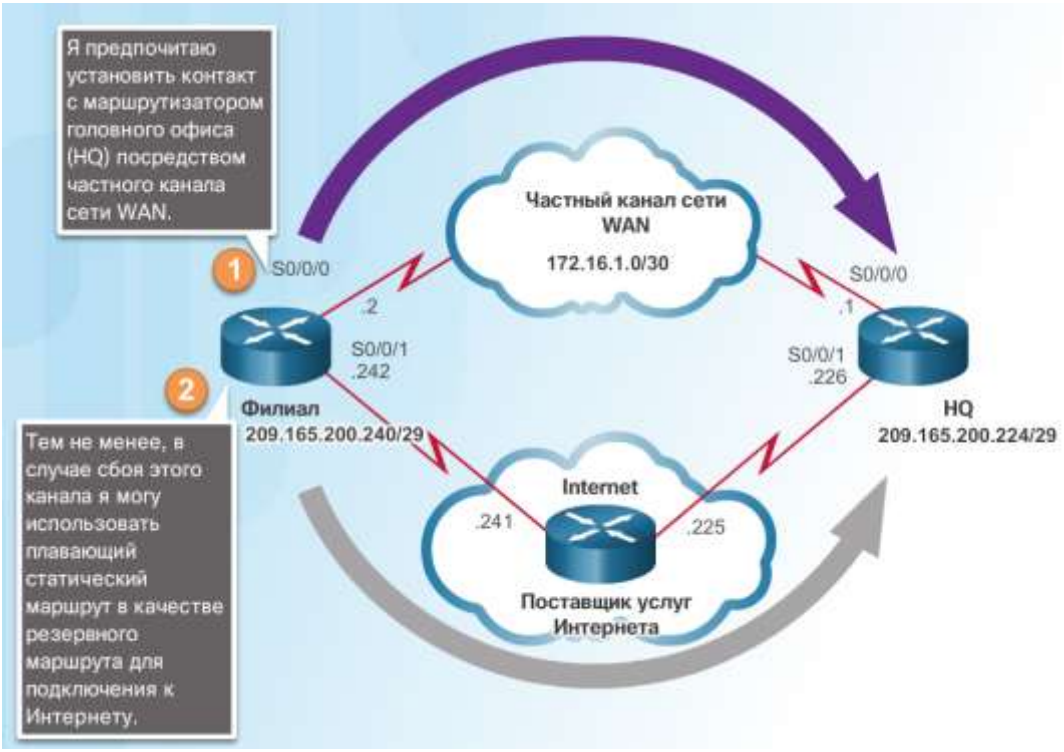


Рис. 3.1.5

На малюнку маршрутизатор філії (Branch) перенаправляє весь трафік на маршрутизатор головного офісу (HQ) по приватному каналу мережі WAN. У цьому прикладі маршрутизатори здійснюють обмін даними про маршрут за допомогою протоколу EIGRP. Плаваючий статичний маршрут з адміністративним відстанню, рівним 91 або більше, можна налаштувати для використання в якості резервного маршруту. При збої приватного каналу мережі WAN і видаленні маршруту EIGRP з таблиці маршрутизації маршрутизатор вибирає плаваючий статичний маршрут як оптимальний шлях для доступу до мережі LAN головного офісу.

Статичні маршрути настроюються за допомогою команди глобальної конфігурації ip route. Базовий синтаксис команди показаний на малюнку.

Для настройки статичної маршрутизації обов'язково зазначаються такі параметри:

мережеву адресу - адресу віддаленої мережі призначення, який необхідно додати в таблицю маршрутизації; даний параметр часто називають префіксом.

subnet-mask - маска підмережі або просто маска віддаленої мережі, яку необхідно додати в таблицю маршрутизації. Маску підмережі можна змінити для об'єднання групи мереж.

Необхідно також використовувати один або обидва наступних параметра:

```
Router(config)# ip route network-address subnet-mask
{ip-address | exit-intf}
```

Параметр	Описание
network-address	Сетевой адрес назначения удаленной сети, которую необходимо добавить в таблицу маршрутизации.
subnet-mask	• Маска подсети удаленной сети, которую необходимо добавить в таблицу маршрутизации. • Маску подсети можно изменить для объединения группы сетей.
ip-address	• Как правило, называется IP-адресом следующего перехода маршрутизатора. • Обычно используется при подключении к среде широковещательного доступа (т. е. Ethernet). • Как правило, создает рекурсивный поиск.
exit-intf	• Используйте выходной интерфейс для пересылки пакетов в сеть назначения. • Также называется непосредственно присоединенным статическим маршрутом. • Обычно используется при подключении в конфигурации «точка-точка».
distance	• (Дополнительно) Настраивает административное расстояние. • Обычно используется для настройки плавающего статического маршрута.

Рис. 3.1.6

ip-address - IP-адреса підключається маршрутизатора, який використовується для пересилки пакетів в віддалену мережу призначення. Такий IP-адреса найчастіше називають наступним переходом або наступним вузлом.

exit-intf - вихідний інтерфейс, який використовується для передачі пакета на наступний перехід.

Функція distance використовується для створення плаваючого статичного маршруту шляхом настройки значення адміністративного відстані, що перевищує значення адміністративного відстані маршруту, одержуваного динамічно.

Наступний перехід може бути ідентифікований IP-адресою, вихідним інтерфейсом або обома параметрами відразу. Залежно від того, як зазначено місце призначення, створюється один з трьох можливих типів маршруту:

Маршрут наступного переходу - вказується тільки IP-адресу наступного переходу.

Статичний маршрут з прямим підключенням - вказується тільки вихідний інтерфейс маршрутизатора.

Повністю заданий статичний маршрут - вказуються IP-адреса наступного переходу і вихідний інтерфейс.

Налаштування статичного маршруту наступного переходу

У статичному маршруті наступного переходу вказується тільки IP-адресу наступного переходу. Вихідний інтерфейс визначається виходячи з наступного транзитного ділянки. Наприклад, на рис. 1 на маршрутизаторі R1 налаштоване

три статичних маршруту наступного переходу за допомогою IP-адреси наступного переходу, маршрутизатора R2.

Рис. 3.1.7

Перед пересиланням маршрутизатором будь-якого пакету за допомогою таблиці маршрутизації визначається вихідний інтерфейс, який буде використовуватися для пересилання пакета. Така операція називається вирішуваною маршруту.

На рис. 2 детально показаний процес пересилання пакетів в таблиці маршрутизації для R1. Якщо пакет адресований мережі 192.168.2.0/24, маршрутизатор R1:

1. здійснює пошук збігів по таблиці маршрутизації і виявляє, що необхідно переслати пакети на IPv4-адрес наступного переходу 172.16.2.2, як зазначено в позначенні 1 на малюнку. Для кожного маршруту, який посилається тільки на IPv4-адрес наступного переходу і не посилається на вихідний інтерфейс, повинен бути зазначений IPv4-адрес наступного переходу, перетворений з допомогою іншого маршруту в таблиці маршрутизації для вихідного інтерфейсу.

2. Маршрутизатор R1 тепер повинен визначити спосіб доступу до мережі 172.16.2.2; таким чином, він повторно перевіряє наявність збігів для 172.16.2.2. В цьому випадку IPv4-адрес відповідає маршруту для підключеної безпосередньо мережі 172.16.2.0/24 з вихідним інтерфейсом Serial 0/0/0, що позначено міткою 2 на малюнку. Пошуковий запит повідомляє таблиці маршрутизації, що даний пакет пересилається з цього інтерфейсу.

Для пересилання пакетів в мережу 192.168.2.0/24 потрібно два процеси пошуку по таблиці маршрутизації. Процес повторного пошуку маршрутизатором в таблиці маршрутизації перед пересиланням пакета відомий

як рекурсивний пошук. Оскільки рекурсивний пошук витрачає ресурси маршрутизатора, рекомендується по можливості уникати його.

Рекурсивний статичний маршрут є допустимим (т. Е. Може бути доданий в таблицю маршрутизації), тільки якщо зазначений наступний перехід безпосередньо чи опосередковано пов'язаний з допустимим вихідним інтерфейсом. Якщо для вихідного інтерфейсу встановлений параметр down (відключений) або administratively down (відключений адміністратором), то статичний маршрут не буде доданий в таблицю маршрутизації.

Налаштування безпосередньо підключеного статичного маршруту

Під час налаштування статичного маршруту також можна використовувати вихідний інтерфейс для налаштування адреси наступного переходу.

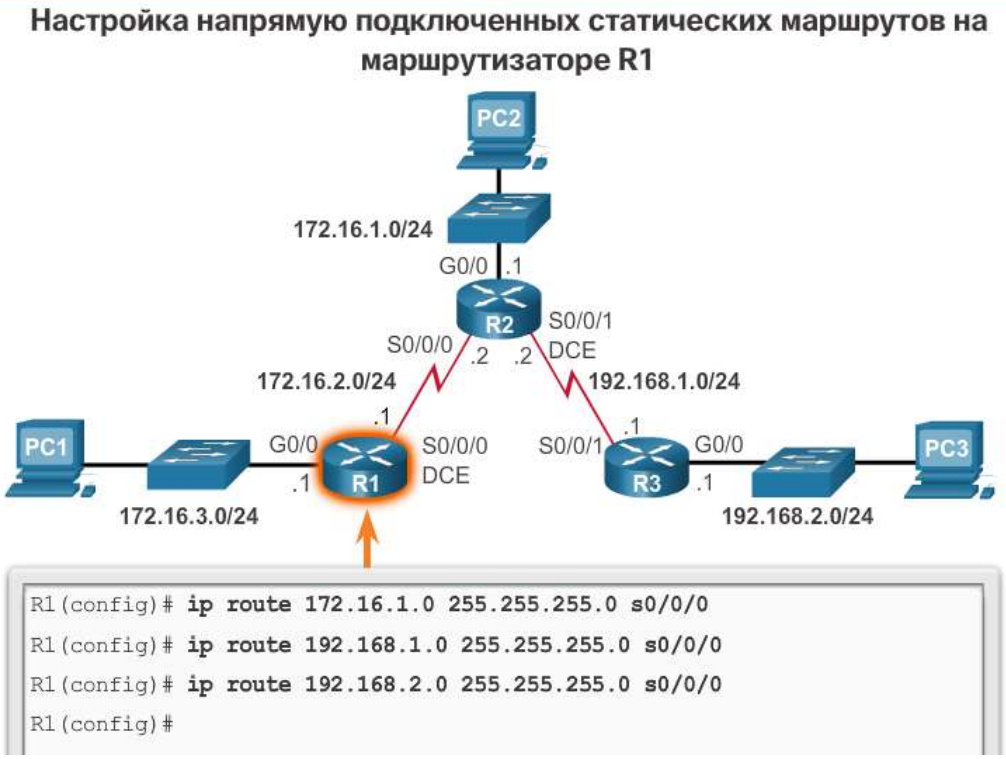


Рис. 3.1.8

На рис. 1 три безпосередньо підключених статичних маршруту налаштовані на маршрутизаторі R1 з використанням вихідного інтерфейсу. У таблиці маршрутизації R1 на рис. 2 показано, що коли пакет адресований мережі 192.168.2.0/24, маршрутизатор R1 шукає збіги в таблиці маршрутизації і виявляє, що він може переслати пакет зі свого інтерфейсу Serial 0/0/0. Інші пошукові процеси не потрібні.

Зверніть увагу, як відрізняється таблиця маршрутизації для маршруту, налаштованого з вихідним інтерфейсом, від маршруту, налаштованого з рекурсивної записом.

Налаштування безпосередньо підключеного статичного маршруту з вихідним інтерфейсом дозволяє таблиці маршрутизації перетворити вихідний інтерфейс в ході одного процесу пошуку замість двох. Хоча запис в таблиці маршрутизації вказує на «пряме підключення», адміністративне відстань статичного маршруту як і раніше дорівнює 1. Тільки безпосередньо підключений інтерфейс може мати адміністративне відстань, рівну 0.

Примітка. Для інтерфейсів типу «точка-точка» можна використовувати статичні маршрути, які вказують на вихідний інтерфейс або адреса наступного переходу. Для багатоточкових або широкомовних інтерфейсів рекомендується використовувати статичні маршрути, які вказують на адресу наступного переходу.

Використовуйте інструмент перевірки синтаксису на рис. 3 і 4 для настройки і перевірки безпосередньо підключених статичних маршрутів на маршрутизаторах R2 і R3.

Примітка. Технологія CEF (Cisco Express Forwarding) використовується за умовчанням на більшості пристроїв, що працюють під управлінням операційної системи IOS 12.0 (або пізнішої версії). CEF забезпечує можливість оптимізованого пошуку для ефективної пересилання пакетів за рахунок двох основних структур даних, що зберігаються в площині даних: бази даних про пересилання (FIB), яка є копією таблиці маршрутизації, і таблиці суміжності, яка містить відомості про адресації другого рівня. Відомості, об'єднані в цих таблицях, використовуються спільно, тому використання рекурсивного пошуку при пошуку IP-адреси наступного переходу не потрібно. Іншими словами, коли на маршрутизаторі включена функція CEF, статичний маршрут, який використовує IP-адреса наступного переходу, вимагає одиничного пошуку. Незважаючи на те що статичні маршрути, які використовують тільки вихідний інтерфейс в мережах типу «точка-точка», широко поширені, використання методу пересилання CEF за замовчуванням усуває необхідність в такому підході. Технологія CEF докладно описана далі в цьому курсі.

У повністю заданому статичному маршруті вказуються як вихідний інтерфейс, так і IP-адреса наступного переходу. Це ще один тип статичного маршруту, який використовується в більш ранніх версіях IOS, які не мають функції CEF. Такий статичний маршрут використовується у випадках, коли вихідний інтерфейс являє собою інтерфейс множинного доступу і необхідно явно визначити наступний перехід. Наступний перехід повинен бути безпосередньо підключений до зазначеного вихідного інтерфейсу.

Рис. 3.1.9

Припустимо, що канал мережі між маршрутизаторами R1 і R2 є каналом Ethernet і що інтерфейс GigabitEthernet 0/1 маршрутизатора R1 підключений до цієї мережі, як показано на рис. 1. Функція CEF не включена. Щоб виключити рекурсивний пошук, можна реалізувати статичний маршрут з прямим підключенням за допомогою наступної команди:

R1 (config) # ip route 192.168.2.0 255.255.255.0 GigabitEthernet 0/1

Однак подібні дії можуть привести до непередбачених або суперечливих результатів. Різниця між мережею Ethernet з множинним доступом і послідовної мережею типу «точка-точка» полягає в тому, що мережа «точка-точка» містить тільки один пристрій - маршрутизатор на іншому кінці каналу. Мережі Ethernet можуть містити безліч різних пристроїв, що використовують одну мережу з множинним доступом, включаючи вузли і навіть кілька маршрутизаторів. Якщо вихідний інтерфейс Ethernet просто позначений в статичному маршруті, у маршрутизатора недостатньо даних, щоб визначити, який пристрій є пристроєм наступного переходу.

Маршрутизатор R1 знає, що пакет повинен бути инкапсулирован в кадрі Ethernet і відправлений за межі інтерфейсу GigabitEthernet 0/1. Однак маршрутизатора R1 невідомий IPv4-адрес наступного переходу, тому він не може визначити MAC-адресу призначення для кадру Ethernet.

Можливість функціонування статичного маршруту визначається топологією і настройками на інших маршрутизаторах. Якщо вихідний інтерфейс є мережею Ethernet, рекомендується використовувати повністю заданий статичний маршрут, включаючи як вихідний інтерфейс, так і IP-адреса наступного переходу.

Як показано на рис. 2, при пересиланні пакетів на маршрутизатор R2 вихідний інтерфейс є інтерфейсом GigabitEthernet 0/1, а IPv4-адрес наступного переходу дорівнює 172.16.2.2.

Примітка. При використанні CEF настройка повністю заданого статичного маршруту не потрібно. В такому випадку слід використовувати статичний маршрут, який використовує адресу наступного переходу.

Поряд з командами ping і traceroute для перевірки статичних маршрутів також використовуються такі команди:

- show ip route
- show ip route static
- show ip route Мережевий

Статичний маршрут за замовчуванням

Маршрутизатор зазвичай використовують маршрути за замовчуванням, налаштовані локально або отримані від іншого маршрутизатора, за допомогою протоколу динамічної маршрутизації. Маршрут за замовчуванням не вимагає збігу ніяких самих лівих бітів між маршрутом за замовчуванням і IPv4-адресою призначення. Маршрут за замовчуванням використовується, якщо жоден з маршрутів в таблиці маршрутизації не збігається з IP-адресою місця призначення пакету. Іншими словами, при відсутності більш точних збігів в якості «шлюзу останньої надії» використовується маршрут за замовчуванням.

Статичні маршрути за замовчуванням зазвичай використовуються при підключенні:

прикордонного маршрутизатора до мережі інтернет-провайдера або.

тупикового маршрутизатора (маршрутизатора тільки з одним сусіднім маршрутизатором в висхідному напрямку).

Як показано на малюнку, синтаксис команди для статичного маршруту за замовчуванням аналогічний синтаксису команди для будь-якого іншого статичного маршруту за винятком того, що адреса мережі вказується як 0.0.0.0, а маска підмережі - 0.0.0.0.

Налаштування статичного маршруту за замовчуванням

Маршрутизатор R1 можна налаштувати, використовуючи три статичних маршруту для доступу до всіх віддаленим мереж в приведеною як приклад топології. Однак R1 є тупиковим маршрутизатором, оскільки він пов'язаний тільки з маршрутизатором R2. Таким чином, набагато більш ефективним методом є настройка статичного маршруту за замовчуванням.

Рис. 3.1.10

У прикладі, показаному на малюнку, виконується настройка статичного маршруту за замовчуванням на маршрутизаторі R1. При використанні настройки, показаної в прикладі, всі пакети, які не відповідають записам більш точного маршруту, пересилаються на адресу 172.16.2.2.

Перевірка статичної маршруту за замовчуванням

Рис. 3.1.11

На малюнку в вихідних даних команди show ip route static відображається вміст статичних маршрутів в таблиці маршрутизації. Зверніть увагу на символ зірочки (*) поруч з маршрутом, що має код S. Як показано в таблиці кодів на малюнку, символ зірочки вказує на те, що даний статичний маршрут є кандидатом в маршрути за замовчуванням, і саме тому він обраний як «шлюз останньої надії ».

Ключем для даної конфігурації виступає маска / 0. Маска підмережі в таблиці маршрутизації визначає число бітів, які повинні співпасти між IP-адресою призначення пакета і маршрутом в таблиці маршрутизації. Двійкове значення 1 говорить про те, що потрібно збіг бітів. Двійкове значення 0 вказує, що збіг бітів не потрібно. Маска / 0 в даному записі маршруту вказує на те, що не потрібно збіг жодного з бітів. Статичний маршрут за замовчуванням зіставляє все пакети, для яких не існує більш точного збігу.

Статичні маршрути для протоколу IPv6 налаштовуються за допомогою команди глобальної конфігурації ipv6 route. На рис. 1 продемонстрована спрощена версія синтаксису команди.

Більшість параметрів ідентичні IPv4-версії цієї команди. Статичний маршрут IPv6 можна реалізувати наступним чином:

- стандартний статичний маршрут IPv6;
- статичний маршрут IPv6 за замовчуванням;
- об'єднаний статичний маршрут IPv6;
- плаваючий статичний маршрут IPv6.

Як і у випадку з IPv4, ці маршрути можна налаштувати як рекурсивні, підключені безпосередньо або повністю задані маршрути.

Рис. 3.1.12

Для того щоб маршрутизатор міг здійснювати пересилку пакетів для IPv6, необхідно налаштувати команду глобальної конфігурації ipv6 unicast-routing. На рис. 2 показана процедура включення одноадресної маршрутизації IPv6.

Параметри наступного переходу

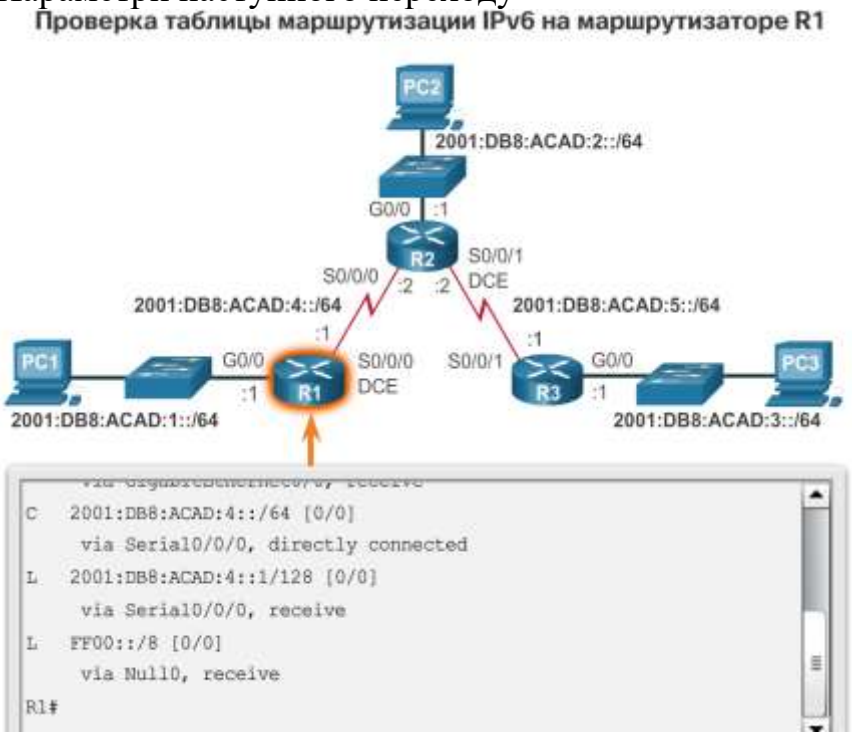


Рис. 3.1.13

В даному прикладі на малюнках 1-3 представлені таблиці маршрутизації R1, R2 і R3. Зверніть увагу, що всі маршрутизатори містять записи тільки для безпосередньо підключених мереж і пов'язаних з ними локальних адрес. Жоден

маршрутизатор не має інформації про мережі за межами підключених до нього інтерфейсів.

Наприклад, R1 не має відомостей про таких мережах:

- 2001: DB8: ACAD: 2 :: / 64 - локальна мережа, підключена до маршрутизатора R2
- 2001: DB8: ACAD: 5 :: / 64 - послідовна мережа між маршрутизаторами R2 і R3
- 2001: DB8: ACAD: 3 :: / 64 - локальна мережа, підключена до маршрутизатора R3

Наступний перехід може бути ідентифікований IPv6-адресою, вихідним інтерфейсом або обома параметрами відразу. Залежно від того, як зазначено місце призначення, створюється один з трьох можливих типів маршруту.

Статичний маршрут IPv6 наступного переходу - вказується тільки IPv6-адреса наступного переходу.

Статичний маршрут IPv6 з прямим підключенням - вказується тільки вихідний інтерфейс маршрутизатора.

Повністю заданий статичний маршрут IPv6 - вказуються IP-адреса наступного переходу і вихідний інтерфейс.

Налаштування статичного маршруту IPv6 наступного переходу

У статичному маршруті наступного переходу вказується тільки IPv6-адреса наступного переходу. Вихідний інтерфейс визначається виходячи з наступного транзитного ділянки. Наприклад, на рис. 1 на маршрутизаторі R1 налаштовані три статичних маршруту наступного переходу.

Як у випадку з IPv4, перед пересиланням маршрутизатором будь-якого пакета система обробки таблиці маршрутизації повинна визначити маршрут і вихідний інтерфейс, який буде використовуватися для пересилання пакета. Процес розв'язання маршруту буде відрізнятися в залежності від методу пересилання пакетів, що використовується маршрутизатором. Технологія CEF (Cisco Express Forwarding) використовується за умовчанням на більшості платформ, що працюють під управлінням ПО Cisco IOS версії 12.0 або більш пізньої версії.

Рис. 3.1.14

На рис продемонстрований процес визначення маршруту при пересиланні пакетів в таблиці маршрутизації маршрутизатора R1 без використання CEF. Якщо пакет адресований мережі 2001: DB8: ACAD: 3 :: / 64, маршрутизатор R1 виконує наступні дії:

1. R1 шукає збіги в таблиці маршрутизації і виявляє, що потрібно пересилання пакетів на IPv6-адреса наступного переходу 2001: DB8: ACAD: 4 :: 2. Для кожного маршруту, який посилається тільки на IPv6-адреса наступного переходу і не посилається на вихідний інтерфейс, повинен бути зазначений IPv6-адреса наступного переходу, перетворений з допомогою іншого маршруту в таблиці маршрутизації для вихідного інтерфейсу.

2. Тепер маршрутизатор R1 повинен визначити спосіб доступу до 2001: DB8: ACAD: 4 :: 2. Таким чином, він виконує повторний пошук збігів. В цьому випадку IPv6-адреса відповідає маршруту для безпосередньо підключеної мережі 2001: DB8: ACAD: 4 :: / 64 з вихідним інтерфейсом Serial 0/0/0. Пошуковий запит повідомляє таблиці маршрутизації, що даний пакет пересилається з цього інтерфейсу.

Таким чином, він фактично використовує два процеси пошуку в таблиці маршрутизації для пересилки будь-якого пакета в мережу 2001: DB8: ACAD: 3 :: / 64. Процес повторного пошуку маршрутизатором в таблиці маршрутизації перед пересиланням пакета відомий як рекурсивний пошук.

Рекурсивний статичний маршрут IPv6 є допустимим (т. Е. Є кандидатом для додавання в таблицю маршрутизації), тільки якщо зазначений наступний перехід прямо чи опосередковано пов'язаний з допустимим вихідним інтерфейсом.

Налаштування безпосередньо підключеного статичного маршруту Ipv6

Під час налаштування статичного маршруту в мережах типу «точка-точка» замість IPv6-адреси наступного переходу можна поставити вихідний інтерфейс. Цей альтернативний метод використовувався в більш ранніх версіях IOS або в тих випадках, коли відключена функція CEF, що дозволяло уникнути проблем, пов'язаних з рекурсивним пошуком.

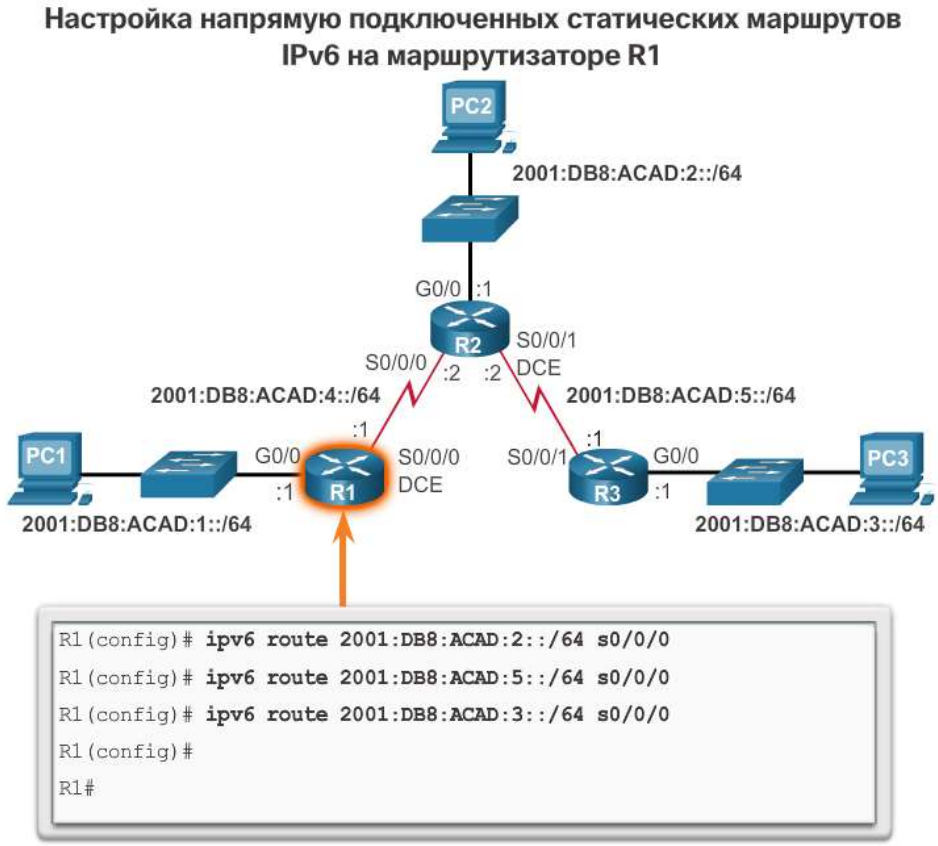


Рис. 3.1.15

Так, наприклад, на рис. на маршрутизаторі R1 налаштовані три безпосередньо підключених статичних маршруту з використанням вихідного інтерфейсу.

У таблиці маршрутизації IPv6 для маршрутизатора R1 на рис. 2 показано, що коли пакет адресований мережі 2001: DB8: ACAD: 3 :: / 64, маршрутизатор R1 шукає збіги в таблиці маршрутизації і виявляє, що він може переслати пакет зі свого інтерфейсу Serial 0/0/0. Інші пошукові процеси не потрібні.

Зверніть увагу, як відрізняється таблиця маршрутизації для маршруту, налаштованого з вихідним інтерфейсом, від маршруту, налаштованого з рекурсивним елементом.

Налаштування безпосередньо підключеного статичного маршруту з вихідним інтерфейсом дозволяє таблиці маршрутизації перетворити вихідний інтерфейс в ході одного процесу пошуку замість двох. Слід пам'ятати, що при використанні механізму пересилання CEF настройка статичних маршрутів із заданим вихідним інтерфейсом не потрібно. Одиничний пошук виконується з використанням комбінації таблиці даних про пересилання (FIB) і таблиці суміжності, що зберігаються в площині даних.

У повністю заданому статичному маршруті вказуються як вихідний інтерфейс, так і IPv6-адреса наступного переходу. Як і повністю задані статичні маршрути для IPv4, ці маршрути використовуються в тому випадку, коли на

маршрутизаторі не включена функція CEF, і вихідний інтерфейс розміщений в мережі з множинним доступом. При використанні CEF статичний маршрут, який використовує тільки IPv6-адреса наступного переходу, буде кращим методом навіть в тому випадку, коли вихідний інтерфейс є мережею з множинним доступом.

На відміну від IPv4, в IPv6 можлива ситуація, коли потрібне використання повністю заданого статичного маршруту. Якщо статичний маршрут IPv6 використовує IPv6-адреса типу link-local в якості адреси наступного переходу, то необхідно використовувати повністю заданий статичний маршрут, що включає вихідний інтерфейс. На рис.1 показаний приклад повністю заданого статичного маршруту IPv6, який використовує IPv6-адреса типу link-local в якості адреси наступного переходу.

Причина, по якій потрібно використання повністю заданого статичного маршруту, полягає в тому, що IPv6-адреса типу link-local не додано в таблицю маршрутизації IPv6. Адреси типу link-local є унікальними тільки в даному каналі або мережі. Адреси наступного переходу типу link-local можуть бути допустимими адресами в декількох мережах, підключених до маршрутизатора. З цієї причини необхідно додати вихідний інтерфейс.

Рис. 3.1.16

На рис. 1 показана настройка повністю певного статичного маршруту з використанням адреси типу link-local маршрутизатора R2 в якості адреси наступного переходу. Зверніть увагу, що в IOS потрібно визначення вихідного інтерфейсу.

Перевірка статичних маршрутів IPv6

Поряд з командами ping і traceroute для перевірки статичних маршрутів також використовуються такі команди:

- show ipv6 route
- show ipv6 route static

- show ipv6 route мережу

Статичний маршрут за замовчуванням - це маршрут, яким відповідають всі пакети. Замість зберігання маршрутизаторами маршрутів для всіх мереж в Інтернеті вони можуть зберігати один маршрут за замовчуванням, що представляє всі мережі, що не додані в таблицю маршрутизації. Маршрут за замовчуванням не вимагає збігу будь-яких самих лівих бітів між маршрутом за замовчуванням і IPv6-адресою призначення.

Маршрутизатор зазвичай використовують маршрути за замовчуванням, налаштовані локально або отримані від іншого маршрутизатора за протоколом динамічної маршрутизації. Вони використовуються в тому випадку, коли жоден маршрут не відповідає IP-адресою призначення в таблиці маршрутизації. Іншими словами, при відсутності більш точних збігів в якості «шлюзу останньої надії» використовується маршрут за замовчуванням.

Статичні маршрути за замовчуванням зазвичай використовуються при підключенні:

Прикордонного маршрутизатора до мережі інтернет-провайдера.

Маршрутизатора, для якого існує сусідній маршрутизатор тільки в висхідному напрямку. Маршрутизатор не має інших сусідніх пристроїв і, отже, вважається тупиковим маршрутизатором.

Як показано на малюнку, синтаксис команд для статичного маршруту за замовчуванням схожий на синтаксис команд для будь-якого іншого маршруту, за винятком того, що для параметра ipv6-prefix / prefix-length задано значення :: / 0, що відповідає всім маршрутам.

Синтаксис основної команди статичного маршрутизатора за замовчуванням наступний:

ipv6 route :: / 0 {ipv6-address | exit-intf}

На відміну від IPv4 в IPv6 не вказується явно, що маршрут IPv6 за замовчуванням є шлюзом «останньої надії».

Ключем для даної конфігурації є маска. :: / 0. Слід пам'ятати, що параметр IPv6 prefix-length в таблиці маршрутизації визначає число бітів, які повинні співпасти між IP-адресою призначення пакета і маршрутом в таблиці маршрутизації. Маска :: / 0 вказує на те, що не потрібно збіг жодного з бітів. Ще не з'явиться більш точний збіг, статичний маршрут IPv6 за замовчуванням відповідає всім пакетам.

Плаваючі статичні маршрути - це статичні маршрути, адміністративна дистанція яких більше, ніж адміністративна дистанція інших статичних маршрутів або динамічних маршрутів. Подібні маршрути рекомендується використовувати в якості резервного каналу для основного каналу, як показано на малюнку.

За замовчуванням статичні маршрути мають значення адміністративного відстані, що дорівнює 1, тому вони мають пріоритет перед маршрутами, отриманими від протоколів динамічної маршрутизації. Наприклад, для деяких поширених протоколів динамічної маршрутизації використовуються наступні адміністративні відстані:

EIGRP = 90

IGRP = 100
OSPF = 110
IS-IS = 115
RIP = 120

Адміністративну дистанцію статичного маршруту можна збільшити і, таким чином, зробити цей маршрут менш пріоритетним, ніж інший статичний маршрут або маршрут, отриманий через протокол динамічної маршрутизації. Таким чином, статичний маршрут «плаває» і не використовується в той час, коли маршрут з більш коротким адміністративним відстанню працює. Однак, якщо кращий маршрут втрачений, плаваючий статичний маршрут може бути використаний, і трафік буде вставлений у цій альтернативним маршрутом.

Усунення несправностей. відсутність маршруту

Деякі з факторів впливу на мережі, які можуть викликати зміну їх статусу, наведені нижче:

- збій інтерфейсу;
- призвести до втрати з'єднання з вини провайдера;
- переповнення каналів;
- невірно задана адміністратором конфігурація.

При зміні в мережі з'єднання може бути розірвано. Мережеві адміністратори відповідають за виявлення проблем та їх усунення. Для того щоб знайти і усунути можливі проблеми, мережевий адміністратор повинен бути знайомий з інструментами, що допомагають швидко ізолювати проблеми з маршрутизацією.

Загальні команди ОС IOS для пошуку і усунення неполадок:

- ping
- traceroute
- show ip route
- show ip interface brief
- show cdp neighbors detail

Дистанційні мережі являють собою мережі, доступ до яких можливий тільки шляхом пересилання пакета на інший маршрутизатор. Статичні маршрути легко налаштувати. Однак у великих мережах виконання таких операцій вручну може бути дуже трудомістким. Статичні маршрути і раніше використовуються навіть в разі впровадження протоколу динамічної маршрутизації.

Статичні маршрути можна налаштувати з використанням IP-адреси наступного переходу, який, як правило, є IP-адресою маршрутизатора наступного вузла. Якщо використовується IP-адреса наступного переходу, процес таблиці маршрутизації повинен перетворити цю адресу в вихідний інтерфейс. На послідовних каналах з конфігурацією типу «точка-точка» краще налаштовувати статичний маршрут з вихідним інтерфейсом. У мережах множинного доступу, наприклад, Ethernet, можна одночасно налаштувати IP-адреса наступного переходу і вихідний інтерфейс на статичному маршруті.

Адміністративне відстань за замовчуванням для статичних маршрутів дорівнює 1. Адміністративне відстань також застосовується для статичних

маршрутів, налаштованих як з використанням адреси наступного переходу, так і з вихідним інтерфейсом.

Статичний маршрут вноситься в таблицю маршрутизації тільки в разі, якщо IP-адреса наступного переходу можна визначити через вихідний інтерфейс. Незалежно від того, чи налаштований статичний маршрут з IP-адресою наступного переходу або вихідним інтерфейсом, в разі, якщо вихідний інтерфейс, використовуваний для переадресації пакета, не включений в таблицю маршрутизації, статичний маршрут також не включається в таблицю маршрутизації.

Маршрут за замовчуванням налаштований з мережевою адресою 0.0.0.0 та маскою підмережі 0.0.0.0 для IPv4, а також параметром prefix / prefix-length :: / 0 для IPv6. Якщо в таблиці маршрутизації немає більш точного збігу, для переадресації повідомлення таблиця використовує маршрут за замовчуванням.

Плаваючий статичний маршрут можна налаштувати як резервний шлях для головного каналу, змінивши його адміністративне значення.

3.2 Динамічна маршрутизація

Масштаб мереж даних, які ми використовуємо в повсякденному житті для навчання, роботи або в розважальних цілях, варіюється від невеликих локальних мереж до великих глобальних об'єднаних мереж. У домашніх умовах користувач може встановити маршрутизатор, а також два або більше комп'ютерів. В рамках організації мова може йти про використання декількох маршрутизаторів і комутаторів, що забезпечують обмін даними між сотнями або навіть тисячами комп'ютерів.

Маршрутизатор виконують пересилання пакетів, використовуючи дані таблиці маршрутизації. Інформацію про маршрути до віддалених мереж маршрутизатор отримує за допомогою статичних і динамічних маршрутів.

У великій мережі, що складається з декількох мереж і підмереж, налагодження та обслуговування статичних маршрутів між цими мережами вимагає частого адміністративного втручання і значних непродуктивних витрат. Непродуктивні витрати особливо зростають при необхідності внесення змін до мережі, наприклад, при збої в роботі каналу або реалізації нової підмережі. Використання протоколів динамічної маршрутизації може зменшити обсяг завдань по налаштуванню і обслуговуванню і забезпечити більшу масштабованість мережі.

У цій главі розглядаються протоколи динамічної маршрутизації. Динамічна маршрутизація порівнюється зі статичної. Далі описано застосування динамічної маршрутизації на основі протоколу маршрутної інформації RIPv1 і RIPv2. В кінці глави докладно розглядається таблиця маршрутизації.

Еволюція протоколів динамічної маршрутизації

Протоколи динамічної маршрутизації використовуються в мережах з кінця 80-х рр. XX ст. Протокол RIP став одним з перших протоколів маршрутизації. Перша версія (RIPv1) з'явилася в 1988 р, проте окремі базові алгоритми цього протоколу застосовувалися ще в мережі ARPANET, створеної Агентством Міністерства оборони США з перспективних досліджень в 1969 р

Поряд з розвитком і ускладненням мереж, виникла необхідність в нових протоколах маршрутизації - Пізніше протокол RIP був оновлений до версії RIPv2, яка краще відповідала потребам нових великих мереж того часу. Однак версія RIPv2 все ж не відповідає масштабам сучасних мережевих рішень. Відповідно до вимог мереж більшого розміру були розроблені два удосконалених протоколу маршрутизації: протокол маршрутизації «алгоритм найкоротшого шляху» (OSPF) і протокол маршрутизації IS-IS. Компанія Cisco розробила внутрішній протокол маршрутизації шлюзів (IGRP) і вдосконалений протокол IGRP (EIGRP), які також забезпечують хорошу масштабованість при реалізації мереж більшого розміру.

Крім перерахованих вимог, виникла необхідність в з'єднанні різних мереж і здійсненні маршрутизації між ними. В даний час для зв'язку між мережами інтернет-провайдерів використовується протокол BGP. Протокол BGP також забезпечує обмін даними маршрутизації між інтернет-провайдерами та їх великими приватними клієнтами.

З появою численних пристроїв, що використовують IP-адреси, адресний простір IPv4 виявилося практично вичерпаним, що призвело до появи протоколу IPv6. Для обміну даними на основі протоколу IPv6 були розроблені нові версії протоколів IP-маршрутизації

Компоненти протоколів динамічної маршрутизації

Протоколи маршрутизації спрощують обмін інформацією про маршрути між маршрутизаторами. Протокол маршрутизації являє собою набір процесів, алгоритмів і повідомлень, які використовуються для обміну даними маршрутизації і наповнення таблиці маршрутизації оптимальними шляхами. Протоколи динамічної маршрутизації використовуються для вирішення наступних завдань:

- виявлення віддалених мереж;
- оновлення даних маршрутизації;
- вибір оптимального шляху до мереж призначення;
- пошук нового оптимального шляху в разі, якщо поточний шлях недоступний.

Протоколи динамічної маршрутизації включають в себе наступні компоненти:

Структури даних. Як правило, для роботи протоколів маршрутизації використовуються таблиці або бази даних. Дана інформація зберігається в ОЗУ.

Повідомлення протоколу маршрутизації. Протоколи маршрутизації використовують різні типи повідомлень для виявлення сусідніх маршрутизаторів, обміну інформацією про маршрути і виконання інших завдань, пов'язаних з отриманням актуальної інформації про мережу.

Алгоритм - алгоритм являє собою певний список дій, які використовуються для виконання завдання. Протоколи маршрутизації використовують алгоритми, що спрощують обмін даних маршрутизації і визначення оптимального шляху.

За допомогою протоколів маршрутизації маршрутизатори динамічно обмінюються інформацією про віддалених мережах і автоматично звіряють цю інформацію з власними таблицями маршрутизації. Щоб запустити анімовану модель процесу, клацніть кнопку Play (Відтворення) на малюнку.

Протоколи маршрутизації визначають оптимальний шлях або маршрут до кожної мережі. Потім маршрут звіряється з таблицею маршрутизації. Цей маршрут буде додано до таблиці маршрутизації, якщо в таблиці немає іншого джерела маршрутизації з меншим адміністративним відстанню. Наприклад, статичний маршрут маршрутизатора R1 з адміністративним відстанню 1 буде мати пріоритет над тією ж самою мережею, якщо інформація про цю мережі отримана за допомогою протоколу динамічної маршрутизації. Основною перевагою протоколів динамічної маршрутизації є те, що вони забезпечують обмін маршрутизирующий інформацією між маршрутизаторами в випадках змін в топології. Подібний обмін даними дозволяє маршрутизаторам автоматично отримувати інформацію про нові мережах, а також знаходити альтернативні шляхи в разі збою каналу до поточної мережі.

Застосування статичної маршрутизації

Перш ніж приступити до вивчення переваг протоколів динамічної маршрутизації, слід розглянути причини, в силу яких мережеві фахівці використовують статичну маршрутизацію. Динамічна маршрутизація безперечно має ряд переваг в порівнянні зі статичною; тим не менш, статична маршрутизація до цього дня використовується в різних мережах. Насправді, в мережах дуже часто використовується поєднання статичної та динамічної маршрутизації.

Статична маршрутизація, як правило, використовується в наступних випадках:

забезпечення спрощеного обслуговування таблиці маршрутизації в невеликих мережах, які не планується суттєво розширювати;

маршрутизація до тупикової мережі і з неї (тупикової мережею є мережа з одним вихідним маршрутом за замовчуванням, яка не має даних про інших віддалених мережах);

використання єдиного маршруту за замовчуванням (для подання шляху до будь-якої мережі, що не має більш точного збігу з іншим маршрутом в таблиці маршрутизації).

Рис. 3.2.1

Переваги та недоліки статичної маршрутизації

У таблиці на малюнку показані основні переваги та недоліки статичної маршрутизації. Реалізація статичної маршрутизації в невеликої мережі не представляє складнощів. Статичні маршрути залишаються незмінними, завдяки чому усунути неполадки, пов'язані з ними, щодо просто. При статичної маршрутизації не потрібно розсилка повідомлень про оновлення, тому навантаження на обчислювальні ресурси майже повністю відсутня.

Недоліки статичної маршрутизації:

- Реалізація статичних маршрутів у великих мережах пов'язана з певними складнощами.
- Управління настройками статичних маршрутів забирає багато часу.
- У разі збою каналу статичний маршрут не може використовуватися для повторної маршрутизації трафіку.

Застосування протоколів динамічної маршрутизації

Протоколи динамічної маршрутизації дозволяють адміністратора управляти трудомісткими процесами настройки і обслуговування статичних маршрутів.

Уявіть собі виконання настройки статичної маршрутизації на семи маршрутизаторах

Тепер уявіть, що компанія виросла і тепер необхідно обслуговувати чотири регіони і 28 маршрутизаторів. Що станеться в разі збою каналу? Як забезпечити доступність резервних маршрутів?

Динамічна маршрутизація є оптимальним вибором для однієї з великих мереж, показаної на малюнку.

Переваги та недоліки динамічної маршрутизації

У таблиці на малюнку представлені основні переваги та недоліки динамічної маршрутизації. Протоколи динамічної маршрутизації ідеально підходять для мереж будь-якого типу, що містять кілька маршрутизаторів. Протоколи забезпечують високий рівень масштабованості, а також автоматично визначають оптимальні маршрути при змінах в топології. Процес настройки протоколів динамічної маршрутизації вимагає певних знань і зусиль, однак у великих мережах набагато простіше налаштувати динамічну маршрутизацію, ніж статичну.

При використанні динамічної маршрутизації є деякі недоліки: Для реалізації динамічної маршрутизації потрібне знання додаткових команд. У порівнянні зі статичної маршрутизацією динамічна маршрутизація демонструє більш низький рівень безпеки, оскільки інтерфейси, визначені протоколом маршрутизації, виконують відправку повідомлень про оновлення маршрутів. Маршрути можуть відрізнятися в залежності від пакетів. Алгоритм маршрутизації використовує додаткові ресурси ЦП, ОЗУ і смуги пропускання каналу.

Зверніть увагу, як динамічна маршрутизація дозволяє усунути недоліки статичної маршрутизації.

Режим конфігурації протоколу RIP на маршрутизаторі

Незважаючи на те що RIP рідко використовується в сучасних мережах, він може послужити основою для розуміння принципів маршрутизації мережі. У цьому розділі подано короткий огляд базової настройки протоколу RIP і перевірки протоколу RIPv2.

Рис. 3.2.2

Вивчіть топологію на рис. 1 і таблицю адресації на рис. 2. В рамках даного сценарію на всіх маршрутизаторах налаштовані основні функції управління; всі інтерфейси, заявлені в топології, налаштовані і активовані. Статичні маршрути і активні протоколи маршрутизації відсутні. Таким чином, на даний момент доступ до віддалених мереж неможливий. Як протоколу динамічної маршрутизації використовується протокол RIPv1. Для включення протоколу RIP використовуйте команду router rip (див. Рис. 3). Дана команда не запускає роботу протоколу RIP. З її допомогою здійснюється перехід в режим конфігурації маршрутизатора, де виконується настройка параметрів маршрутизації протоколу RIP. За замовчуванням при активації RIP використовується версія RIPv1.

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
R1	G0/0	192.168.1.1	255.255.255.0
	S0/0/0	192.168.2.1	255.255.255.0
R2	G0/0	192.168.3.1	255.255.255.0
	S0/0/0	192.168.2.2	255.255.255.0
	S0/0/1	192.168.4.2	255.255.255.0
R3	G0/0	192.168.5.1	255.255.255.0
	S0/0/1	192.168.4.1	255.255.255.0

Рис. 3.2.3

Для відключення і видалення протоколу RIP використовуйте команду глобальної конфігурації no router rip. Дана команда зупиняє роботу протоколу RIP і видаляє всі існуючі налаштування протоколу.

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# router rip
R1(config-router)#
```

Рис. 3.2.4

На рис. 4 показані різні команди протоколу RIP, які можна налаштувати. Виділені ключові слова розглядаються в даному розділі.

Оголошення мереж

При переході в режим конфігурації протоколу RIP маршрутизатор отримує вказівку активувати RIPv1. Однак маршрутизатора необхідно повідомити, які локальні інтерфейси він повинен використовувати для обміну даними з іншими маршрутизаторами, а також які локально підключені мережі він повинен оголосити для цих маршрутизаторів.

Включення маршрутизації по протоколу RIP для тієї чи іншої мережі проводиться за допомогою команди network мережеву адресу режиму конфігурації маршрутизатора. Вкажіть класовий мережеву адресу для кожної безпосередньо підключеної мережі. Дана команда виконує наступні дії:

Включає протокол RIP на всіх інтерфейсах, які відносяться до конкретної мережі. Пов'язані інтерфейси тепер можуть і відправляти, і отримувати пакети оновлень протоколу RIP.

Оголошує зазначену мережу в оновленнях маршрутизації RIP, що відправляються іншим маршрутизаторів кожні 30 секунд.

Примітка. Протокол RIPv1 є протоколом класової маршрутизації для IPv4. Тому IOS автоматично перетворює зазначену адресу підмережі (при його наявності) в класовий мережеву адресу. Наприклад, при введенні команди network 192.168.1.32 в поточному файлі конфігурації виконується автоматичне перетворення вхідних даних в network 192.168.1.0. IOS не створює повідомлення про помилку, однак замість цього виправляє введені дані і вказує класовий мережеву адресу.

Рис. 3.2.5

На рис. 1 команда network використовується для оголошення безпосередньо підключених мереж маршрутизатора R1.

Рис. 3.2.6

Використовуйте інструмент перевірки синтаксису на рис. 2 для настройки аналогічної конфігурації на маршрутизаторах R2 і R3.

Перевірка маршрутизації по протоколу RIP

Команда show ip protocols відображає поточні настройки протоколу маршрутизації IPv4 на маршрутизаторі. Вихідні дані, представлені на рис. 1, підтверджують настройку більшості параметрів протоколу RIP, включаючи наступні:

1. Маршрутизація RIP налаштована і запущена на маршрутизаторі R1.
2. Значення різних таймерів, наприклад наступне оновлення маршрутизації, відправляються маршрутизатором R1 через 15 секунд.
3. Поточна налаштована версія протоколу RIP - RIPv1.
4. Маршрутизатор R1 в даний час виконує об'єднання в межах класової мережі.
5. Класові мережі оголошуються маршрутизатором R1. Це мережі, які маршрутизатор R1 включає в власні поновлення RIP.

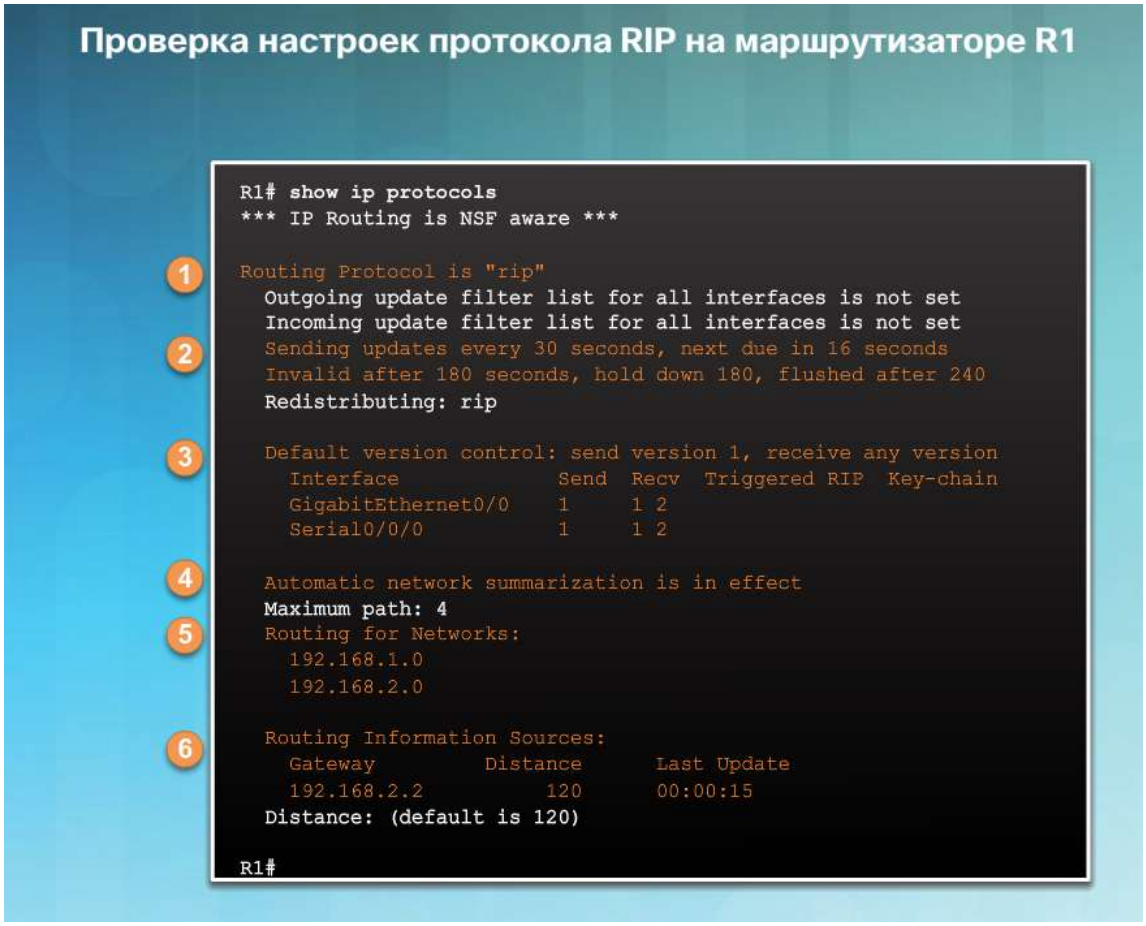


Рис. 3.2.7

6. Перераховано сусідні пристрої RIP, включаючи наступну інформацію: IP-адреса наступного переходу; пов'язане значення адміністративного відстані, яке маршрутизатор R2 використовує для оновлень, що відправляються даними сусіднім пристроєм; час отримання останнього оновлення від даного сусіднього пристрою.

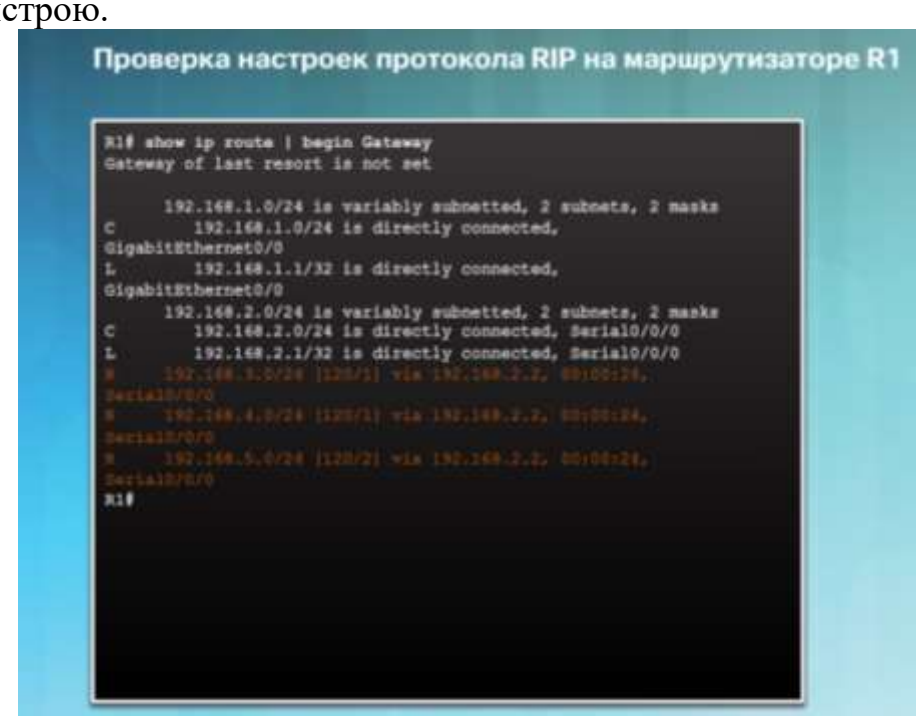


Рис. 3.2.8

Примітка. Дану команду рекомендується використовувати для перевірки роботи інших протоколів маршрутизації (наприклад, EIGRP і OSPF).

Команда show ip route відображає маршрути RIP, додані в таблицю маршрутизації. Згідно рис. 2, маршрутизатора R1 тепер відомо про зазначені мережах.

Використовуйте інструмент перевірки синтаксису на рис. 3 для перевірки налаштувань і маршрутів маршрутизаторів R2 і R3 RIP.

Включення і перевірка протоколу RIPv2

При налаштуванні процесу RIP на маршрутизаторі Cisco, за замовчуванням використовується протокол RIPv1 (див. Рис. 1). Однак навіть в тих випадках, коли маршрутизатор відправляє тільки повідомлення RIPv1, він може інтерпретувати повідомлення RIPv1 і RIPv2. Маршрутизатор RIPv1 ігнорує поля RIPv2 в запису маршруту.

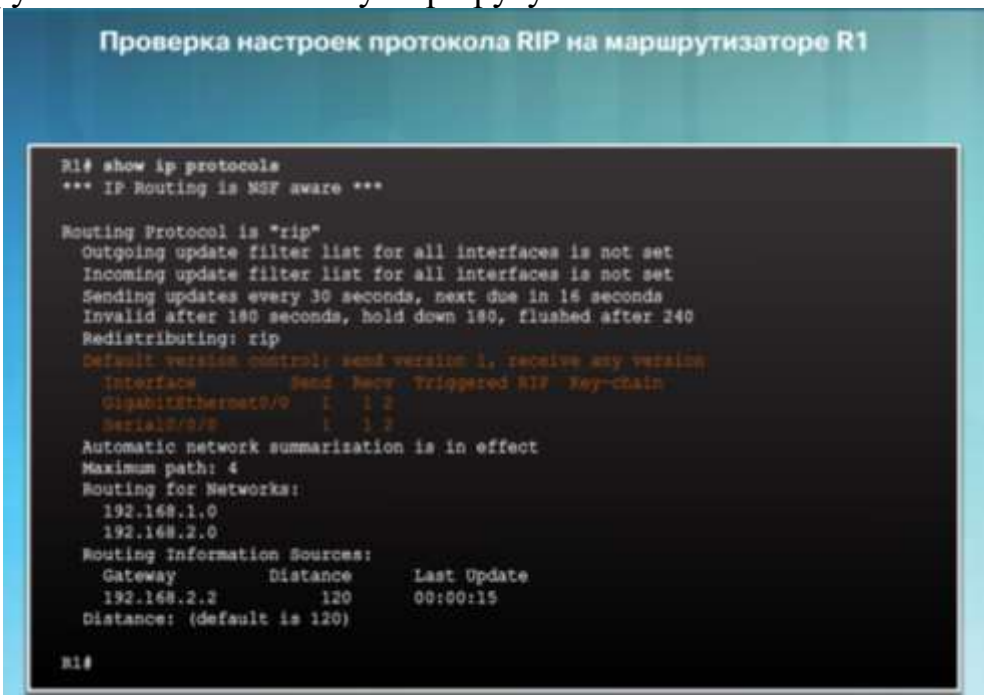


Рис. 3.2.9

Для включення RIPv2 використовуйте команду режиму конфігурації маршрутизатора version 2, як показано на рис. 2. Зверніть увагу на те, як за допомогою команди show ip protocols перевіряється, що маршрутизатор R2 налаштований для відправки і прийому тільки повідомлень версії 2. Процес RIP тепер включає маску підмережі в усі оновлення, що відносить протокол RIPv2 до безкласовим протоколам маршрутизації.

Рис. 3.2.10

Примітка. За командою version 1 включається тільки протокол RIPv1. Команда no version відновлює параметри налаштування за замовчуванням - маршрутизатор відправляє оновлення версії 1, при цьому беручи оновлення версій 1 і 2.

Рис. 3.2.11

На рис. 3 показана нова таблиця маршрутизації, де немає маршрутів RIP. Це пов'язано з тим, що маршрутизатор R1 тепер прослуховує тільки поновлення RIPv2. Маршрутизатор R2 і R3 і раніше відправляють поновлення RIPv1. Отже, команда version 2 повинна бути налаштована на всіх маршрутизаторах в домені маршрутизації.

Використовуйте інструмент перевірки синтаксису на рис. 4 для включення протоколу RIPv2 на маршрутизаторах R2 і R3.

Відключення автоматичного підсумовування

Як показано на рис. 1, протокол RIPv2 за замовчуванням автоматично підсумовує мережі в межах основної мережі аналогічно протоколу RIPv1.

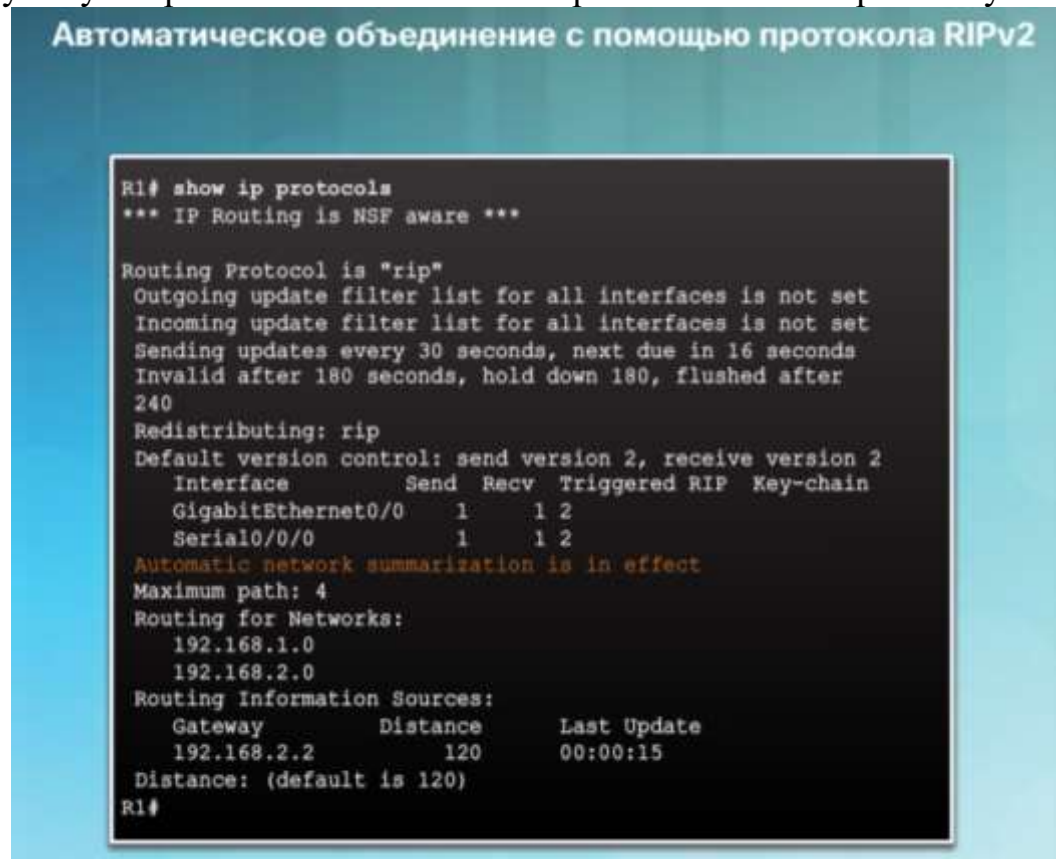


Рис. 3.2.12

Для зміни поведінки протоколу RIPv2 за замовчуванням (автоматичне об'єднання), використовуйте команду режиму конфігурації маршрутизатора no auto-summary, як показано на рис. 2. Дана команда не виконує потрібні дії, якщо використовується протокол RIPv1. Після відключення функції автоматичного підсумовування протокол RIPv2 припиняє підсумовування мереж по їх класового адресою на прикордонних маршрутизаторах. Тепер протокол RIPv2 включає всі підмережі і відповідні маски в свої відновлення маршрутизації. Тепер команда show ip protocols повідомляє, що автоматичне об'єднання мереж не застосовується (automatic network summarization is not in effect).

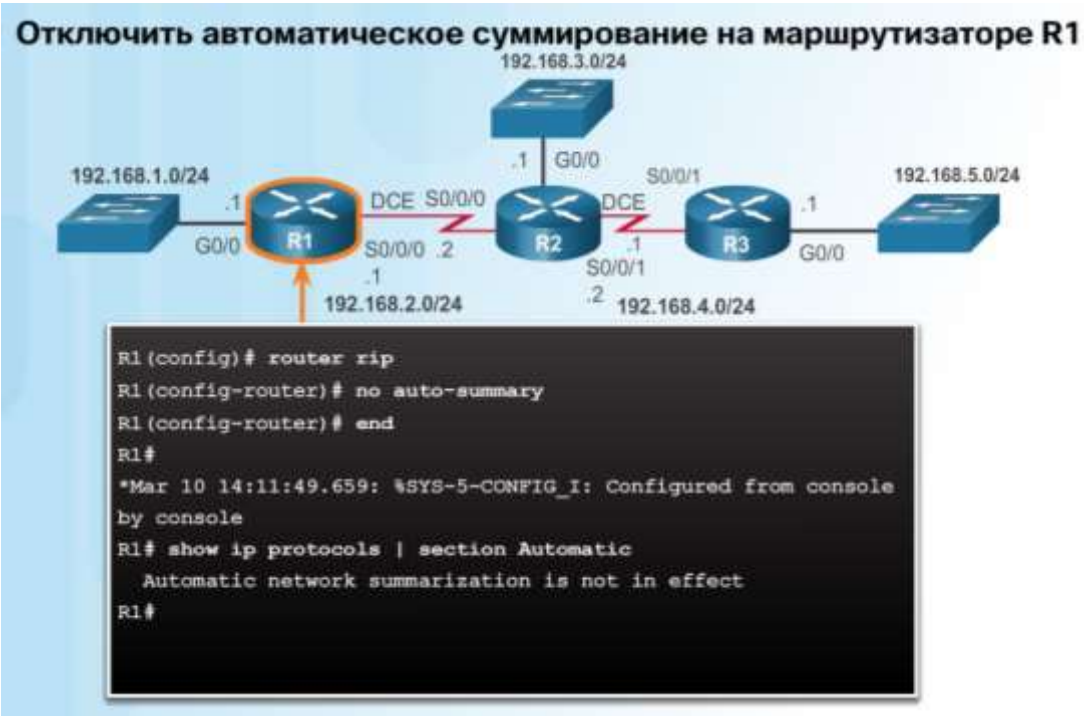


Рис. 3.2.13

Примітка. RIPv2 необхідно включити до відключення функції автоматичного об'єднання.

Використовуйте інструмент перевірки синтаксису на рис. 3, щоб відключити функцію автоматичного об'єднання на маршрутизаторах R2 і R3.

Налаштування пасивних інтерфейсів

За замовчуванням поновлення RIP пересилаються через всі інтерфейси, що підтримують протокол RIP. Якщо інтерфейс підключений до маршрутизатора, який не підтримує протокол RIP, то відправка оновлень RIP через такий інтерфейс не має сенсу.

Рис. 3.2.14

Ознайомтеся з топологією на рис.1. Протокол RIP відправляє поновлення з інтерфейсу G0 / 0 навіть в тому випадку, коли пристрій RIP відсутня в цій мережі LAN. Маршрутизатор R1 не отримує про це даних і, в результаті, відправляє оновлення кожні 30 секунд. Відправка непотрібних оновлень в LAN має наступні наслідки:

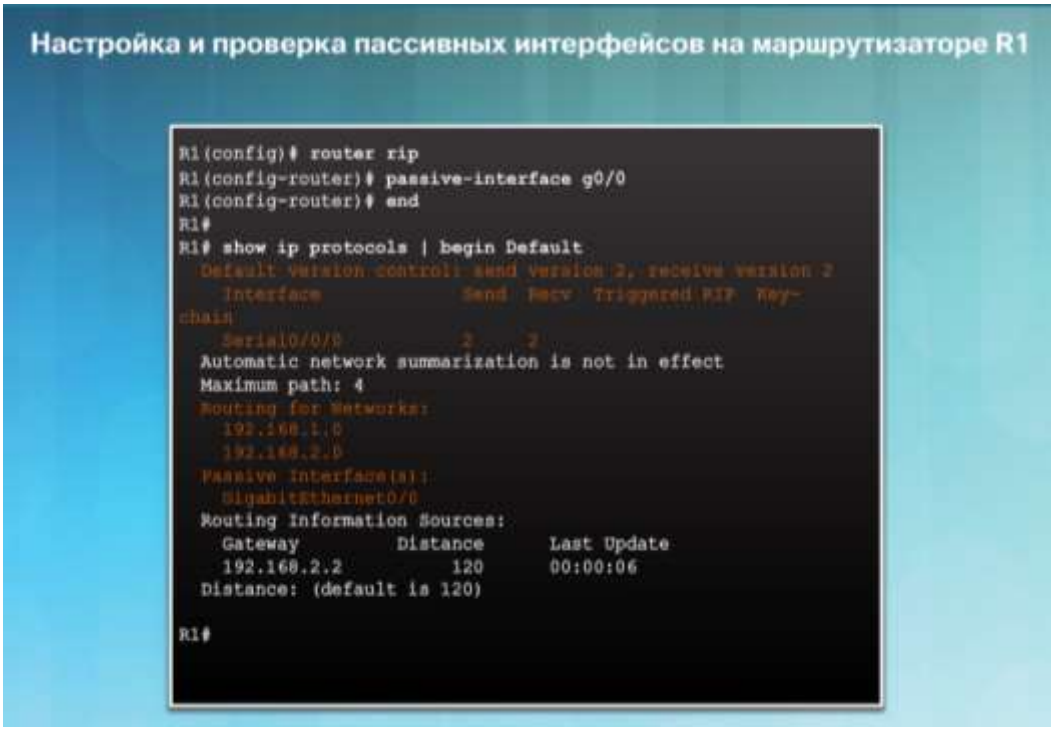


Рис. 3.2.15

Необгрунтоване витрачання смуги пропускання: смуга пропускання використовується для передачі непотрібних оновлень. Оновлення RIP відправляються за допомогою многоадресной або широкомовної розсилки, тому комутаторитакож пересилають поновлення через всі порти.

Споживання ресурсів: всі пристрої в мережі LAN повинні обробляти оновлення до транспортних рівнів, на яких поновлення видаляються.

Ризики для інформаційної безпеки: оголошення оновлень по широкомовної розсилки є загрозою інформаційної безпеки. Пакети оновлень протоколу RIP можуть бути перехоплені за допомогою ПО для аналізу мережевих протоколів (сніфери). Оновлення маршрутизації можна змінити і відправити назад на маршрутизатор, яка може пошкодити таблиці маршрутизації через неправдиві метрик, які невірно направляють трафік.

Використовуйте команду конфігурації маршрутизатора passive-interface, щоб заборонити передачу оновлень маршрутизації через інтерфейс маршрутизації, але при цьому дозволити оголошення мережі для інших маршрутизаторів. Команда припиняє відправку оновлень маршрутизації з зазначеного інтерфейсу. Проте, мережа, до якої відноситься зазначений інтерфейс, як і раніше оголошується в оновленнях маршрутизації, які відправляються з інших інтерфейсів.

Маршрутизаторів R1, R2 і R3 не потрібно пересилати поновлення RIP зі своїх інтерфейсів LAN. Конфігурація, показана на рис. 2, визначає інтерфейс G0/0 маршрутизатора R1 як пасивний. Для перевірки інтерфейсу Gigabit Ethernet як пасивного використовується команда show ip protocols. Зверніть увагу, що інтерфейс G0 / 0 більше не вказується як інтерфейс, який приймає або відправляє оновлення версії 2, замість цього він вказується в розділі пасивних інтерфейсів. Також слід звернути увагу на те, що мережа 192.168.1.0 і раніше вказується в розділі маршрутизації мереж, тобто дана мережа все ще вказана як запис маршруту в оновленнях RIP, що відправляються маршрутизатора R2.

Примітка. Всі протоколи маршрутизації підтримують команду passive-interface.

Використовуйте інструмент перевірки синтаксису на рис. 3 для настройки інтерфейсу LAN як пасивного інтерфейсу на маршрутизаторах R2 і R3.

Також за допомогою команди passive-interface default можна налаштувати всі інтерфейси як пасивні. Інтерфейси, які не повинні бути пасивними, можуть бути заново активовані за допомогою команди no passive-interface.

Поширення маршруту за замовчуванням

Зверніться до рис.1. В даному сценарії граничний маршрутизатор R1 підключений до інтернет-провайдера через один інтерфейс. Отже, все, що потрібно маршрутизатора R1 для доступу до мережі Інтернет - це статичний маршрут за замовчуванням з інтерфейсу Serial 0/0/1.

Рис. 3.2.16

Аналогічні статичні маршрути за замовчуванням можна налаштувати на маршрутизаторах R2 і R3, проте набагато більші можливості масштабування забезпечуються в тому випадку, коли маршрут одноразово прописаний на граничному маршрутизаторі R1, після чого маршрутизатор R1 передає його на всі інші маршрутизатори за допомогою протоколу RIP. Щоб забезпечити можливість підключення до мережі Інтернет для всіх інших мереж в домені маршрутизації RIP, статичний маршрут за замовчуванням необхідно оголосити для всіх інших маршрутизаторів, що використовують протокол динамічної маршрутизації.

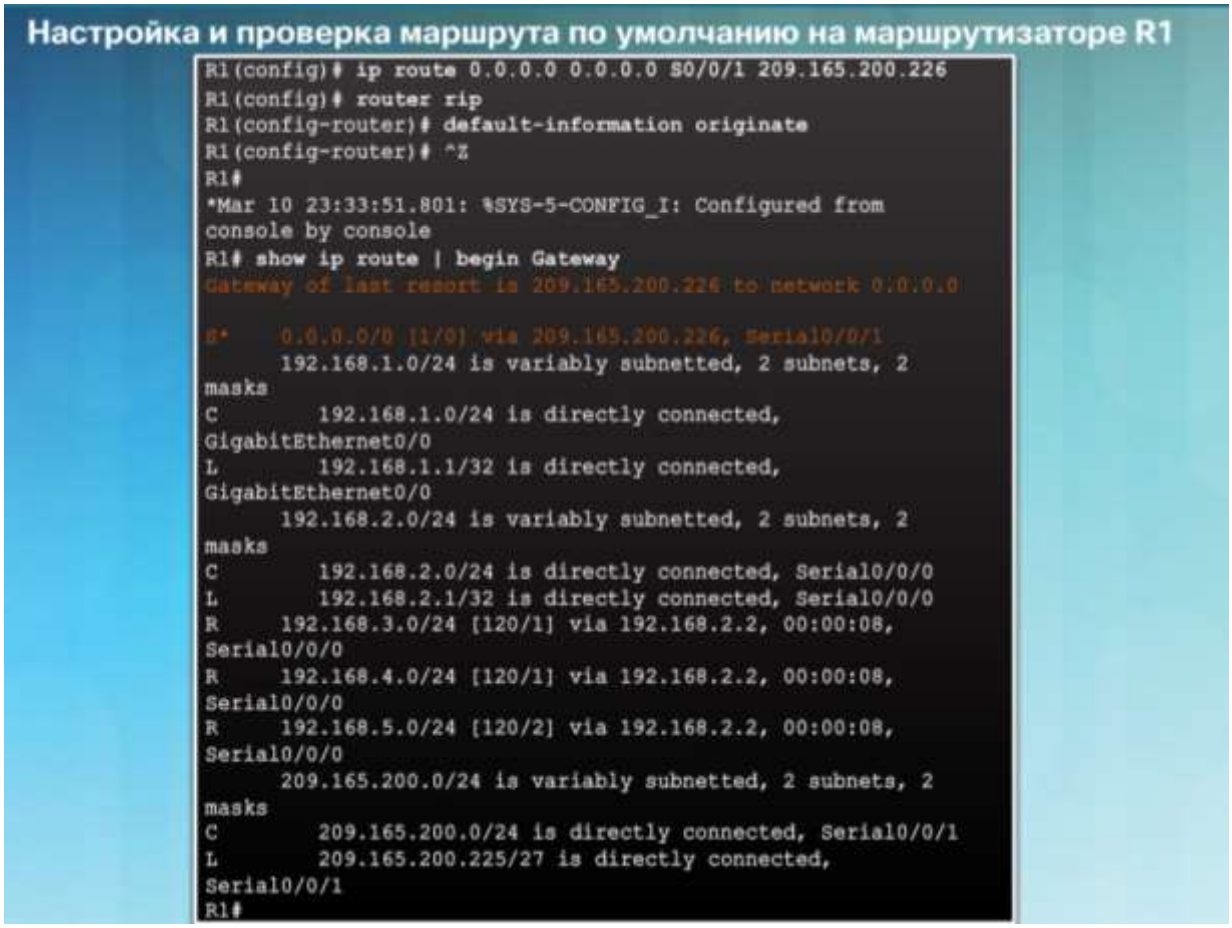


Рис. 3.2.17

Щоб організувати передачу маршруту за замовчуванням, слід налаштувати граничний маршрутизатор таким чином:

Задати статичний маршрут за замовчуванням за допомогою команди ip route 0.0.0.0 0.0.0.0.

Застосувати команду конфігурації маршрутизатора default-information originate. Маршрутизатор R1 отримує вказівку ініціювати передачу інформації, яка застосовується за умовчанням. Це досягається шляхом передачі статичного маршруту за замовчуванням в оновленнях RIP.

У прикладі на рис. 2 виконується настройка повністю заданого статичного маршруту за замовчуванням до мережі інтернет-провайдера. Далі цей маршрут поширюється по мережі за допомогою протоколу RIP. Зверніть увагу, що тепер в таблиці маршрутизації маршрутизатора R1 налаштований «шлюз останньої надії» і встановлений маршрут за замовчуванням.

Використовуйте інструмент перевірки синтаксису на рис. 3, щоб підтвердити передачу маршруту за замовчуванням на маршрутизатори R2 і R3.

Записи таблиці маршрутизації

Топологія, показана на рис. 1, використовується як довідкова топологія в рамках даного розділу. Слід зазначити, що в даній топології:

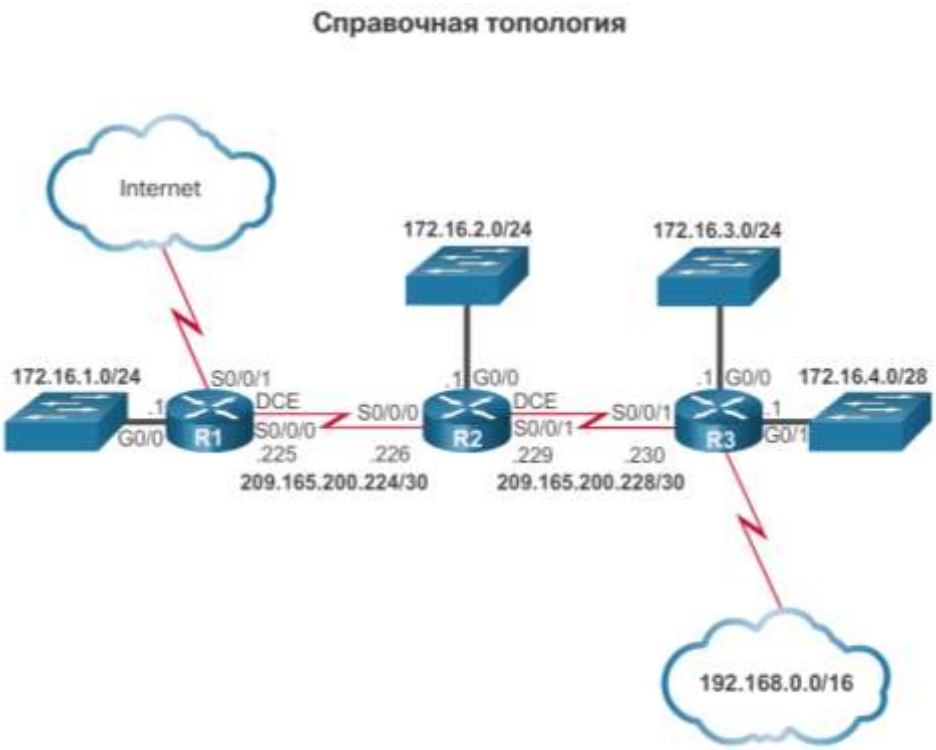


Рис. 3.2.18

R1 підключений до Інтернету і є граничним маршрутизатором. Отже, цей маршрутизатор відправляє статичний маршрут за замовчуванням на маршрутизатори R2 і R3.

Маршрутизатор R1, R2 і R3 містять «розірвані» мережі, розділені інший класової мережею.

Маршрутизатор R3 також вводить маршрут Суперсети 192.168.0.0/16.

На рис. 2 показана таблиця маршрутизації IPv4 маршрутизатора R1, що містить безпосередньо підключені, статичні і динамічні маршрути.

Таблиця маршрутизации маршрутизатора R1

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                   is directly connected, Serial0/0/1
   172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C     172.16.1.0/24 is directly connected, GigabitEthernet0/0
L     172.16.1.1/32 is directly connected, GigabitEthernet0/0
R     172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R  192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03, Serial0/0/0
   209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C     209.165.200.224/30 is directly connected, Serial0/0/0
L     209.165.200.225/32 is directly connected, Serial0/0/0
R     209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12,
                         Serial0/0/0
C     209.165.200.232/30 is directly connected, Serial0/0/1
L     209.165.200.233/30 is directly connected, Serial0/0/1
R1#
```

Рис. 3.2.19

Примітка. Ієрархія таблиці маршрутизації в Cisco IOS спочатку реалізована з використанням схеми класової маршрутизації. Хоча таблиця маршрутизації включає класову і безкласову адресацію, загальна структура і раніше будується на основі класової схеми.

Записи з прямим підключенням

Як показано на рис. 1, таблиця маршрутизації маршрутизатора R1 містить три безпосередньо підключені мережі. Зверніть увагу, що два записи таблиці маршрутизації створюються автоматично при налаштуванні інтерфейсу активного маршрутизатора з використанням IP-адреси і маски підмережі.

Напрямую подключённые интерфейсы маршрутизатора R1

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                  is directly connected, Serial0/0/1
   172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C     172.16.1.0/24 is directly connected, GigabitEthernet0/0
L     172.16.1.1/32 is directly connected, GigabitEthernet0/0
R     172.16.2.0/24 [120/1] via 209.165.200.226,00:00:12, Serial0/0/0
R     172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03, Serial0/0/0
   209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C     209.165.200.224/30 is directly connected, Serial0/0/0
L     209.165.200.225/32 is directly connected, Serial0/0/0
R     209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
C     209.165.200.232/30 is directly connected, Serial0/0/1
L     209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```

Рис. 3.2.20

На рис. 2 показана одна із записів таблиці маршрутизації на маршрутизаторі R1 для безпосередньо підключеної мережі 172.16.1.0. Ці записи автоматично додані в таблицю маршрутизації при налаштуванні і активації інтерфейсу GigabitEthernet 0/0. Записи містять наступну інформацію:

Напрямую подключённые маршруты на маршрутизаторе R1

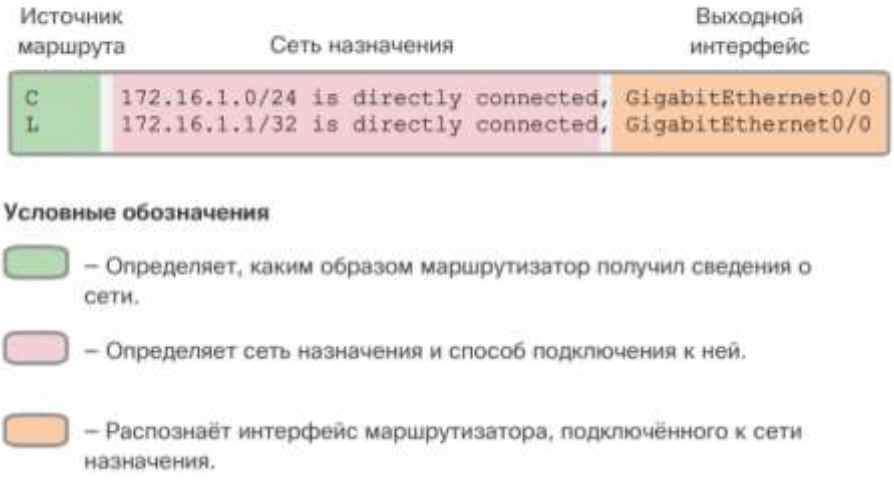


Рис. 3.2.21

Джерело маршруту - визначає, яким способом було отримано маршрут. Інтерфейси з прямим підключенням мають два коду джерела маршруту. Код C визначає безпосередньо підключену мережу. Безпосередньо підключені мережі створюються автоматично, коли інтерфейс налаштовується за IP-адресою і активується. Код L визначає локальний маршрут. Локальні мережі

створюються автоматично, коли інтерфейс налаштовується за IP-адресою і активується.

Мережа призначення - адреса віддаленої мережі і тип її підключення.

Вихідний інтерфейс - визначає вихідний інтерфейс, який буде використовуватися при пересиланні пакетів в мережу призначення.

Маршрутизатор зазвичай має кілька настроєних інтерфейсів. Таблиця маршрутизації містить дані про безпосередньо підключених і віддалених мережах. Як і для мереж з прямим підключенням, джерело маршруту визначає, яким чином був виявлений маршрут. До поширених кодами для віддалених мереж відносяться наступні коди:

S - визначає, що маршрут був створений адміністратором вручну для доступу до окремої мережі. Такий маршрут називається статичним.

D - визначає, що дані про маршрут отримані динамічно від іншого маршрутизатора за допомогою протоколу маршрутизації EIGRP.

O - визначає, що дані про маршрут отримані динамічно від іншого маршрутизатора за допомогою протоколу маршрутизації OSPF.

R - визначає, що дані про маршрут отримані динамічно від іншого маршрутизатора за допомогою протоколу маршрутизації RIP.

Записи віддаленої мережі

На малюнку показано запис в таблиці маршрутизації IPv4 на маршрутизаторі R1 для маршруту до віддаленої мережі 172.16.4.0 на маршрутизаторі R3. Запис містить наступну інформацію.

Рис. 3.2.22

Джерело маршруту - визначає, яким способом було отримано маршрут.

Мережа призначення - визначення адреси віддаленої мережі.

Адміністративне відстань визначає достовірність джерела маршруту. Статичні маршрути мають адміністративне відстань 1. Для безпосередньопідключених маршрутів адміністративне відстань дорівнює 0.

Адміністративне відстань протоколів динамічної маршрутизації більше 1. Конкретне значення залежить від типу протоколу.

Метрика - визначає значення, призначені для доступу до віддаленої мережі. Перевага маршрути мають низькі значення. Метрика для статичних і підключених маршрутів дорівнює 0.

Наступний перехід - вказує IPv4-адрес наступного маршрутизатора, на який буде відправлений пакет.

Тимчасова мітка маршруту - визначає час останнього відгуку маршрутизатора.

Вихідний інтерфейс - визначає вихідний інтерфейс для відправки пакета до кінцевого пункту призначення.

Терміни таблиці маршрутизації

Як видно з малюнка, динамічно створена таблиця маршрутизації надає достатній обсяг даних. Отже, критично важливо розуміти вихідні дані, створювані таблицею маршрутизації. Під час обговорення вмісту таблиці маршрутизації використовуються спеціальні терміни.

Таблица маршрутизации маршрутизатора R1

```
R1#show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0
R        172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R        172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R        172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
      Serial0/0/0
      209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/0/0
L        209.165.200.225/32 is directly connected, Serial0/0/0
R        209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12,
         Serial0/0/0
C        209.165.200.232/30 is directly connected, Serial0/0/1
L        209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```

Рис. 3.2.23

Таблиця IP-маршрутизації Cisco не є плоскою базою даних. Таблиця маршрутизації фактично є ієрархічною структурою, яка використовується для прискорення процедури пошуку маршрутів і пересилання пакетів. У межах цієї структури існує кілька ієрархічних рівнів.

Маршрути обговорюються з використанням наступних критеріїв:

- остаточний маршрут;
- маршрут 1-го рівня;
- батьківський маршрут 1-го рівня;
- дочірній маршрут 2-го рівня.

Остаточний маршрут являє собою запис в таблиці маршрутизації, що містить або IPv4-адрес наступного переходу, або вихідний інтерфейс. Безпосередньо підключені, динамічно одержувані і локальні маршрути є остаточними.

Окончательные маршруты маршрутизатора R1

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0
R        172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R        172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12,
          Serial0/0/0
R        172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
      Serial0/0/0
      209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/0/0
L        209.165.200.225/32 is directly connected, Serial0/0/0
R        209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12,
         Serial0/0/0
C        209.165.200.232/30 is directly connected, Serial0/0/1
L        209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```

Рис. 3.2.24

Виділені області на малюнку представляють собою приклади остаточних маршрутів. Зверніть увагу, що ці маршрути вказують або IPv4-адрес наступного переходу, або вихідний інтерфейс.

Маршрут 1-го рівня

Маршрут 1-го рівня є маршрут з маскою підмережі, значення якої дорівнює або менше значення класової маски мережевого адреси. Отже, маршрут 1-го рівня може розглядатися як:

- мережевий маршрут - мережевий маршрут, який містить маску підмережі зі значенням, рівним значенню маски класу;
- маршрут Суперсети - маршрут Суперсети є мережеву адресу з маскою, значення якої менше значення маски класу (наприклад, сумарний адреса);
- маршрут за замовчуванням - маршрут за замовчуванням є статичний маршрут з адресою 0.0.0.0/0.

Джерелом маршруту 1-го рівня може бути безпосередньо підключена мережа, статичний маршрут або протокол динамічної маршрутизації.

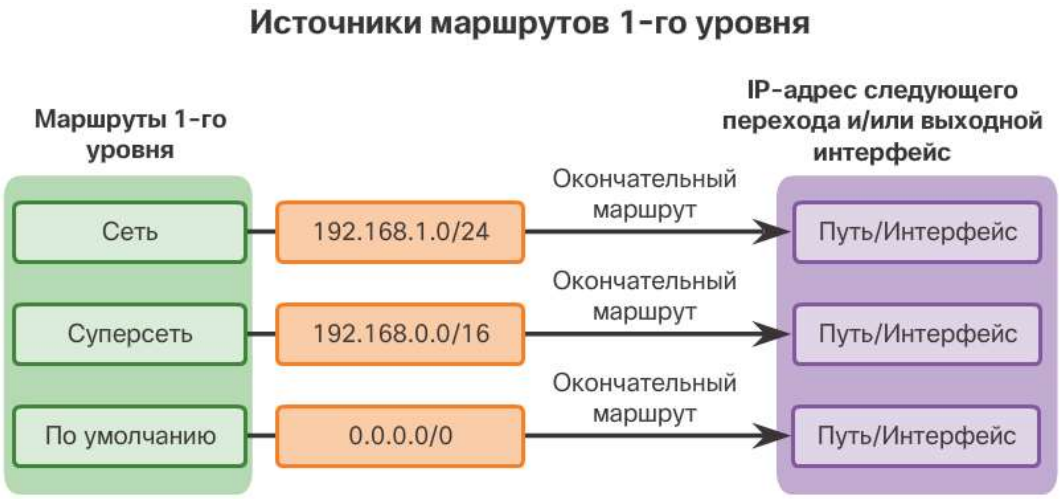


Рис. 3.2.25

На рис. показано, як маршрути 1-го рівня можуть також використовуватися в якості остаточних маршрутів.

Примеры маршрутов 1-го уровня

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network
0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
masks
C        172.16.1.0/24 is directly connected,
GigabitEthernet0/0
L        172.16.1.1/32 is directly connected,
GigabitEthernet0/0
R        172.16.2.0/24 [120/1] via 209.165.200.226,
00:00:12, Serial0/0/0
R        172.16.3.0/24 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R        172.16.4.0/28 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
Serial0/0/0
      209.165.200.0/24 is variably subnetted, 5 subnets, 2
masks
C        209.165.200.224/30 is directly connected,
```

Рис. 3.2.26

На рис. 2 представлені маршрути 1-го рівня.

Батьківський маршрут 1-го рівня

Як показано на рис. 1, маршрути 172.16.0.0 і 209.165.200.0 є батьківськими маршрутами 1-го рівня. Батьківський маршрут - це мережевий маршрут 1-го рівня з поділом на підмережі. Батьківський маршрут ніколи не може бути остаточним маршрутом.

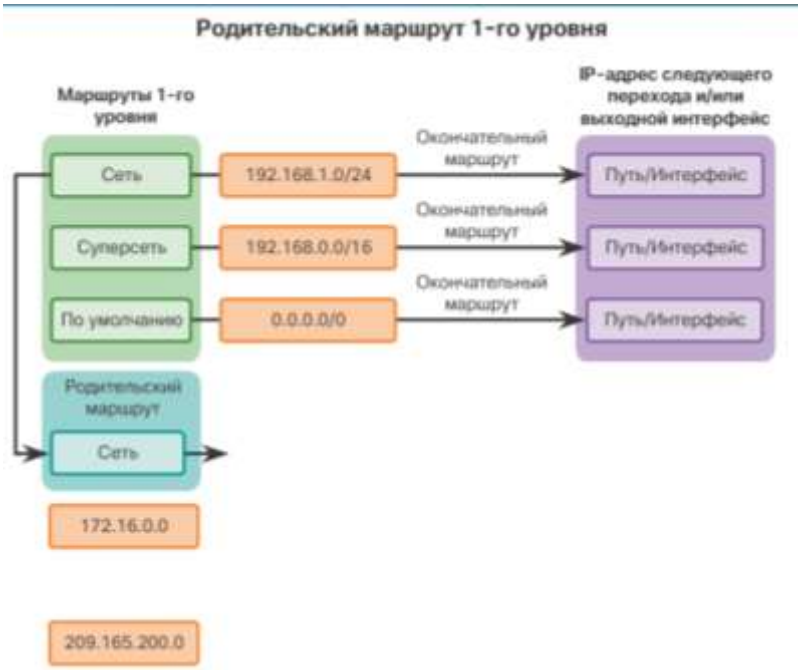


Рис. 3.2.27

На рис. 2 показані батьківські маршрути 1-го рівня в таблиці маршрутизації маршрутизатора R1. У таблиці маршрутизації такий маршрут, як правило, надає заголовок для окремих підмереж, які в ньому містяться. У кожного запису відображається класовий мережеву адресу, число підмереж і число різних масок підмережі, на які поділено класовий адресу.

Родительские маршруты 1-го уровня на маршрутизаторе R1

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network
0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
masks
C        172.16.1.0/24 is directly connected,
GigabitEthernet0/0
L        172.16.1.1/32 is directly connected,
GigabitEthernet0/0
R        172.16.2.0/24 [120/1] via 209.165.200.226,
00:00:12, Serial0/0/0
R        172.16.3.0/24 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R        172.16.4.0/28 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
Serial0/0/0
      209.165.200.0/24 is variably subnetted, 5 subnets, 2
masks
C        209.165.200.224/30 is directly connected,
Serial0/0/0
```

Рис. 3.2.28

Дочірній маршрут 2-го рівня

Дочірній маршрут 2-го рівня є маршрут, який є підмережею класового мережевого адреси. Як показано на рис. 1, батьківський маршрут 1-го рівня - це маршрут 1-го рівня мережі, розділеної на підмережі. Як показано на рис. 2, батьківські маршрути 1-го рівня містять в собі дочірні маршрути 2-го рівня.

Рис. 3.2.29

Як і у випадку з маршрутом 1-го рівня, джерелом маршруту 2-го рівня може бути безпосередньо підключена мережа, статичний маршрут або динамічно отриманий маршрут. Дочірні маршрути 2-го рівня також є остаточними маршрутами.

Рис. 3.2.30

Примітка. Ієрархія таблиці маршрутизації в Cisco IOS використовує схему класової маршрутизації. Батьківський маршрут 1-го рівня є класовий мережеву

адресу маршруту підмережі. Це стосується навіть тих випадків, коли протокол безкласової маршрутизації є джерелом маршруту підмережі.

На рис. 3 показані дочірні маршрути в таблиці маршрутизації маршрутизатора R1.

Процес пошуку маршруту

При надходженні пакета на інтерфейс маршрутизатора маршрутизатор вивчає заголовок IPv4, визначає IPv4-адрес і переходить до процедури пошуку маршруту.

Рис. 3.2.31

На рис. 1 маршрутизатор вивчає мережеві маршрути 1-го рівня на наявність оптимального відповідності адреси призначення пакета IPv4:

1. Якщо оптимальним збігом є остаточний маршрут 1-го рівня, то для пересилання пакета використовується саме він.

Рис. 3.2.32

2. Якщо оптимальним збігом є батьківський маршрут 1-го рівня, перейдіть до наступного кроку.

На рис. 2 маршрутизатор вивчає дочірні маршрути (маршрути підмережі) батьківського маршруту на наявність оптимального збігу:

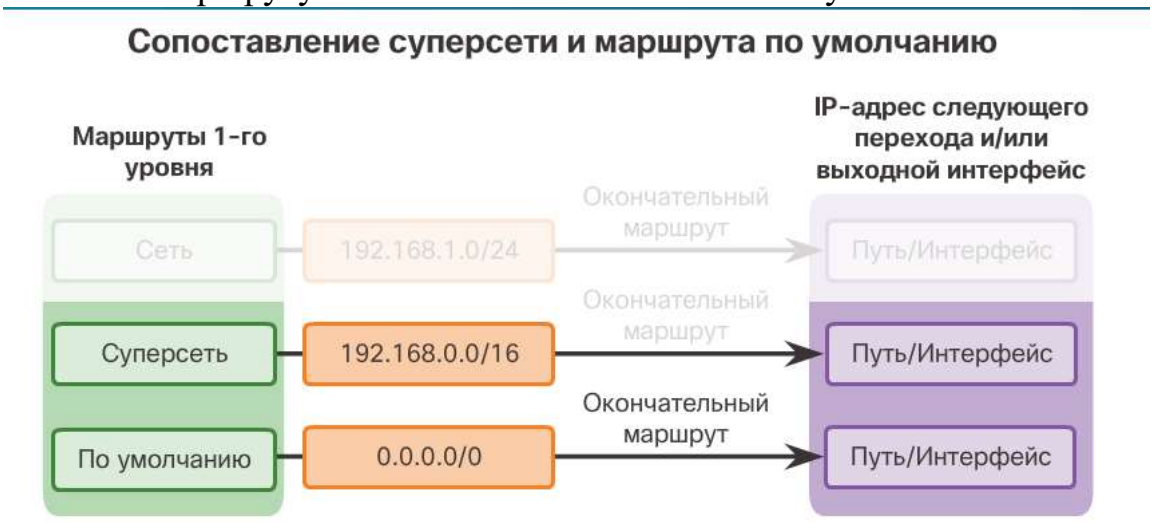


Рис. 3.2.33

3. Якщо є збіг з батьківським маршрутом 2-го рівня, підмережа використовується для пересилання пакета.

4. Якщо збігів з дочірніми маршрутами 2-го рівня немає, перейдіть до наступного кроку.

На рис. 3 маршрутизатор продовжує пошук відповідного суперсетевого маршруту 1-го рівня в таблиці маршрутизації, включаючи маршрут за замовчуванням (якщо такий є).

5. Якщо знайдено менш точний збіг з маршрутами за замовчуванням або маршрутами Суперсети 1-го рівня, маршрутизатор використовує такий маршрут для пересилання пакета.

6. При відсутності збігу з будь-яким маршрутом в таблиці маршрутизації маршрутизатор відкидає пакет.

римітка. Якщо в мережі не застосовується технологія Cisco Express Forwarding (CEF), то маршрут, який посилається лише на IP-адресу наступного переходу без вказівки вихідного інтерфейсу, повинен бути перетворений в маршрут, в якому вказано вихідний інтерфейс. Якщо технологія CEF не використовується, то на основі IP-адреси наступного переходу виконується рекурсивний пошук до тих пір, поки маршрут не буде перетворений так, щоб забезпечити перехід на вихідний інтерфейс. За замовчуванням технологія CEF включена.

Оптимальний маршрут = найдовше збіг

Що мається на увазі під твердженням «маршрутизатор повинен виконати пошук найкращого збігу в таблиці маршрутизації»? Найкраще збіг - це найдовше збіг.

Щоб IPv4-адрес призначення пакета збігся з маршрутом в таблиці маршрутизації, потрібна мінімальна кількість збігів по крайнім лівим бітам в IPv4-адресу пакета і маршруту в таблиці маршрутизації. Маска підмережі

маршруту в таблиці маршрутизації використовується для визначення обов'язкового мінімального числа співпадаючих крайніх лівих бітів. Слід пам'ятати, що пакет IPv4 містить тільки IPv4-адрес, а не маску підмережі.

Рис. 3.2.34

Найкращим збігом є маршрут в таблиці маршрутизації, в якому максимальне число крайніх лівих бітів збігається з IPv4-адресою призначення пакета. Маршрут з найбільшим числом еквівалентних крайніх лівих бітів (найдовше збіг) завжди є кращим.

На малюнку показаний пакет, призначений для відправки в мережу 172.16.0.10. Маршрутизатора є три можливих маршрути, які збігаються з цим пакетом - 172.16.0.0/12, 172.16.0.0/18 і 172.16.0.0/26. Маршрут 172.16.0.0/26 має найдовше збіг, тому для пересилання пакета вибирається саме цей маршрут. Пам'ятайте, що для того, щоб ці маршрути розглядалися як збігаються, необхідна мінімальна кількість співпадаючих бітів, вказане маскою підмережі маршруту.

Записи в таблиці маршрутизації IPv6

Компоненти таблиці маршрутизації IPv6 дуже схожі з компонентами таблиці маршрутизації IPv4. Наприклад, таблиця маршрутизації заповнюється з використанням безпосередньо підключених інтерфейсів, статичних маршрутів і динамічно одержуваних маршрутів.

Оскільки IPv6 є безкласовим протоколом, всі маршрути, по суті, є остаточними маршрутами 1-го рівня. Батьківських маршрутів 1-го рівня для дочірніх маршрутів 2-го рівня не існує.

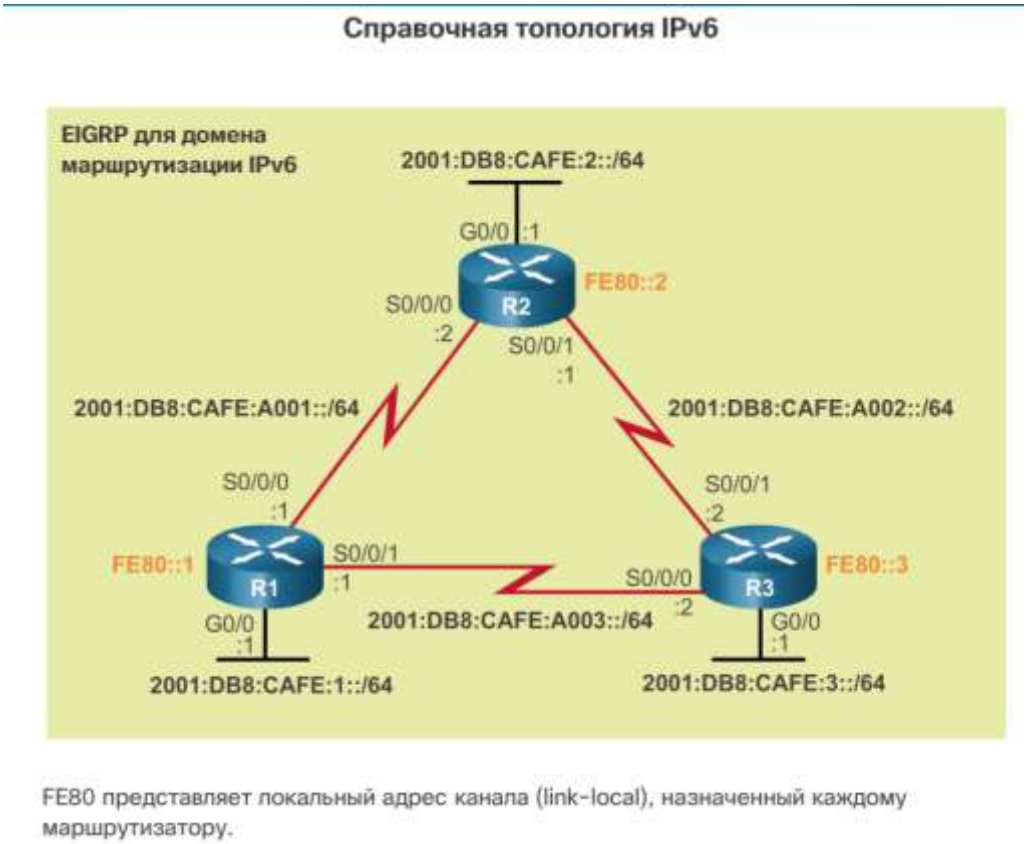


Рис. 3.2.35

Топологія, представлена на малюнку, використовується як довідкова топологія в рамках даного розділу. Слід зазначити, що в даній топології:

- маршрутизатори R1, R2 і R3 налаштовані в повно-комірчастої топології; всі маршрутизатори містять резервні шляху до різних мереж;
- маршрутизатор R2 є граничним маршрутизатором з підключенням до мережі інтернет-провайдера, при цьому статичний маршрут за замовчуванням не оголошується;
- протокол EIGRP для IPv6 налаштований на всіх трьох маршрутизаторах.

Примітка. Таблиці маршрутизації заповнюються за допомогою протоколу EIGRP для IPv6, проте принципи використання і настройки протоколу EIGRP не розглядаються в рамках даного курсу.

Записи з прямим підключенням

На рис. 1 таблиця маршрутизації маршрутизатора R1 відображається за допомогою команди show ipv6 route. Хоча вихідні дані команди відображаються трохи інакше, ніж у версії IPv4, в них все одно вказується аналогічна інформація про маршрут.

Таблица маршрутизации IPv6 маршрутизатора R1

```
R1# show ipv6 route
<Данные опущены>

C 2001:DB8:CAFE:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L 2001:DB8:CAFE:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
D 2001:DB8:CAFE:2::/64 [90/2170112]
     via FE80::2, Serial0/0/0, receive
D 2001:DB8:CAFE:3::/64 [90/2170112]
     via FE80::3, Serial0/0/1, receive
C 2001:DB8:CAFE:A001::/64 [0/0]
     via Serial0/0/0, directly connected
L 2001:DB8:CAFE:A001::1/128 [0/0]
     via Serial0/0/0, receive
D 2001:DB8:CAFE:A002::/64 [90/2681856]
     via FE80::2, Serial0/0/0, receive
     via FE80::3, Serial0/0/1, receive
C 2001:DB8:CAFE:A003::/64 [0/0]
     via Serial0/0/1, directly connected
L 2001:DB8:CAFE:A003::1/128 [0/0]
     via Serial0/0/1, receive
L FF00::/8 [0/0]
     via Null0, receive
R1#
```

Рис. 3.2.36

На рис. представлена підключена мережа і записи локальної таблиці маршрутизації для безпосередньо підключених інтерфейсів. Три записи додано при налаштуванні і активації інтерфейсів.

Напрямую подключенные маршруты на маршрутизаторе R1

```
R1# show ipv6 route
<Данные опущены>

C 2001:DB8:CAFE:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L 2001:DB8:CAFE:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
D 2001:DB8:CAFE:2::/64 [90/2170112]
     via FE80::2, Serial0/0/0, receive
D 2001:DB8:CAFE:3::/64 [90/2170112]
     via FE80::3, Serial0/0/1, receive
C 2001:DB8:CAFE:A001::/64 [0/0]
     via Serial0/0/0, directly connected
L 2001:DB8:CAFE:A001::1/128 [0/0]
     via Serial0/0/0, receive
D 2001:DB8:CAFE:A002::/64 [90/2681856]
     via FE80::2, Serial0/0/0, receive
     via FE80::3, Serial0/0/1, receive
C 2001:DB8:CAFE:A003::/64 [0/0]
     via Serial0/0/1, directly connected
L 2001:DB8:CAFE:A003::1/128 [0/0]
     via Serial0/0/1, receive
L FF00::/8 [0/0]
     via Null0, receive
R1#
```

Рис. 3.2.37

Як показано на рис., в записах безпосередньо підключеного маршруту відображаються наступні дані:

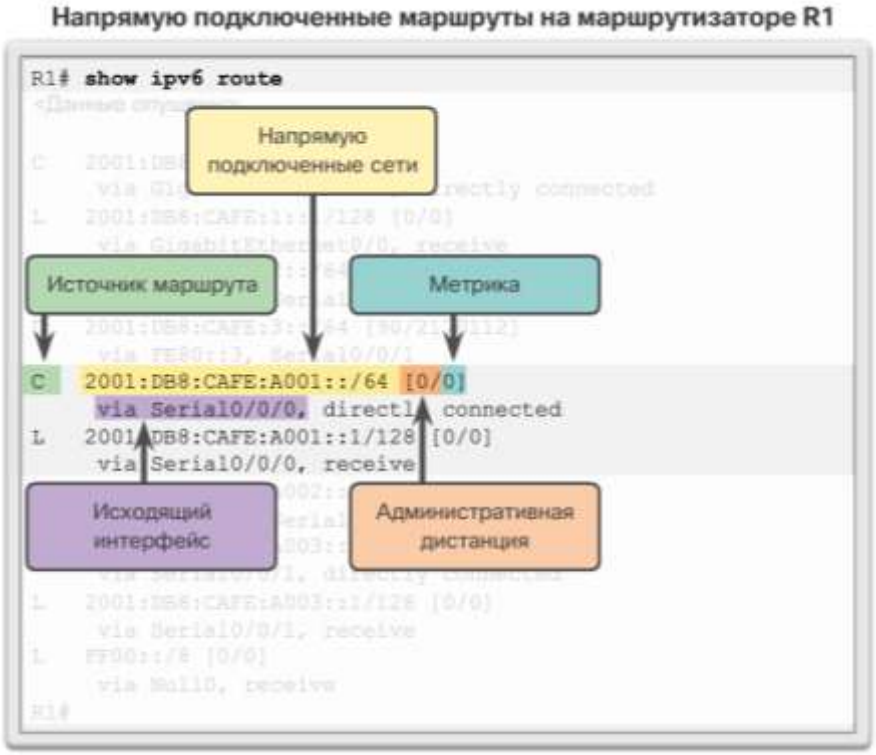


Рис. 3.2.38

Джерело маршруту - визначає, яким способом було отримано маршрут. Безпосередньо підключені інтерфейси містять два коду джерела маршруту (кодом «C» позначаються безпосередньо підключені мережі, а кодом «L» - локальні маршрути).

Безпосередньо підключена мережа - IPv6-адреса безпосередньо підключеної мережі.

Адміністративна дистанція - визначення надійності джерела маршруту. IPv6 використовує ті ж значення адміністративної дистанції, що і IPv4. Значення 0 вказує на оптимальний, найбільш надійне джерело.

Метрика - визначає значення, призначені для доступу до віддаленої мережі. Перевага маршрути мають низькі значення.

Вихідний інтерфейс - визначає вихідний інтерфейс, який буде використовуватися при пересиланні пакетів в мережу призначення.

Примітка. Послідовні канали мають задану пропускну здатність, значення якої дозволяють спостерігати за вибором оптимального маршруту метриками протоколу EIGRP. Задана пропускна здатність не є реальною характеристикою сучасних мереж. Це значення використовується виключно в цілях візуальної ілюстрації швидкості з'єднання.

Записи віддаленої мережі IPv6

На рис. 1 наведені записи таблиці маршрутизації для трьох віддалених мереж (т. Е. Мереж LAN R2, LAN R3 і каналу між R2 і R3). Три записи додані протоколом EIGRP.

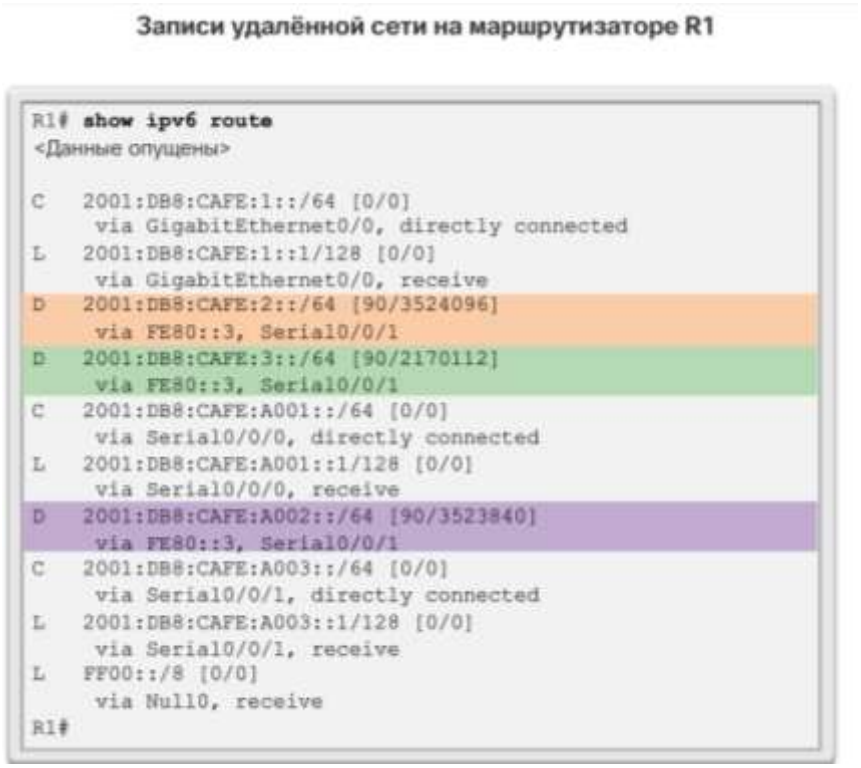


Рис. 3.2.39

На рис. 2 представлена запис з таблиці маршрутизації маршрутизатора R1, відповідна маршруту до віддаленої мережі 2001: DB8: CAFE: 3 :: / 64 на маршрутизаторі R3. Запис містить наступну інформацію.

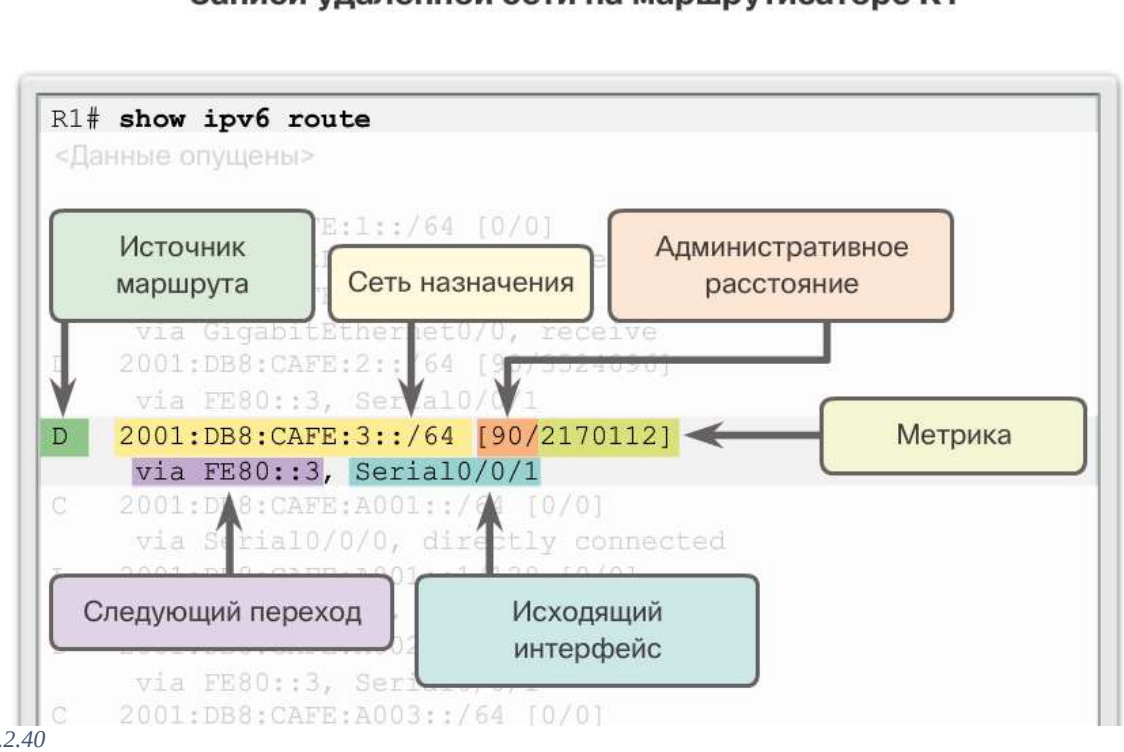


Рис. 3.2.40

Джерело маршруту - визначає, яким способом було отримано маршрут. До поширених кодами відносяться: «O» (OSPF), «D» (EIGRP), «R» (RIP) і «S» (статичний маршрут).

Мережа призначення - визначає адреси віддаленої мережі IPv6.

Адміністративна дистанція - визначає надійність джерела маршруту. IPv6 використовує ті ж значення адміністративної дистанції, що і IPv4.

Метрика - визначає значення, призначені для доступу до віддаленої мережі. Перевага маршрути мають низькі значення.

Наступний перехід - вказує IPv6-адреса наступного маршрутизатора, на який буде відправлений пакет.

Вихідний інтерфейс - визначає вихідний інтерфейс для відправки пакета до кінцевого пункту призначення.

Коли пакет IPv6 надходить на інтерфейс маршрутизатора, маршрутизатор вивчає заголовок IPv6 і визначає IPv6-адреса призначення. Після цього маршрутизатор виконує описану нижче процедуру пошуку маршруту.

Маршрутизатор вивчає мережеві маршрути 1-го рівня на наявність максимальної відповідності умовам адресою призначення пакета IPv6. Як і в IPv4, найкращим вважається найдовше збіг. Наприклад, при наявності декількох збігів в таблиці маршрутизації, маршрутизатор вибирає маршрут з найдовшим збігом. Збіг визначається збігом крайніх лівих бітів IPv6-адреси призначення з префіксом IPv6 і довжиною префікса в таблиці маршрутизації IPv6.

Протоколи динамічної маршрутизації спрощують обмін інформацією про маршрути між маршрутизаторами. Протоколи динамічної маршрутизації виконують такі завдання: виявлення віддалених мереж, підтримка актуальності даних для маршрутизації, вибір оптимального шляху до мереж призначення, пошук нового оптимального шляху в разі, якщо поточний шлях недоступний. Незважаючи на те що протоколи динамічної маршрутизації вимагають меншого втручання з боку адміністратора, ніж статична маршрутизація, для їх роботи все ж потрібно спеціально виділена частина ресурсів маршрутизатора, включаючи ресурси ЦП та смугу пропускання каналу.

У багатьох випадках мережі використовують комбінацію статичної та динамічної маршрутизації. Динамічна маршрутизація є оптимальним вибором для великих мереж, в той час як статична маршрутизація ідеально підходить для кінцевих тупикових мереж.

Протоколи маршрутизації відповідають за виявлення віддалених мереж, а також за надання точних даних про мережу. При зміні топології протоколи маршрутизації передають дані про зміни в рамках домена маршрутизації. Процес приведення всіх таблиць маршрутизації в узгоджене стан, при якому всі маршрутизатори в одному домені або області мають повні і точні дані про мережі, називається конвергенцією. Деякі протоколи маршрутизації сходяться швидше, ніж інші.

В окремих випадках маршрутизатори отримують дані декількох маршрутів до однієї мережі від протоколів статичної та динамічної маршрутизації. Коли маршрутизатор отримує дані про мережі призначення з одного або декількох джерел маршрутизації, маршрутизатори Cisco використовують значення адміністративної дистанції для вибору джерела. Всі протоколи динамічної маршрутизації мають унікальне значення адміністративної дистанції поряд зі статичними маршрутами і безпосередньо підключеними мережами. Чим нижче значення адміністративної дистанції, тим більш привабливим є джерело маршруту. Безпосередньо підключена мережа завжди є кращим джерелом. Ще

одне джерело після неї є статичні маршрути, і після них - різні протоколи динамічної маршрутизації.

Записи в таблиці маршрутизації містять наступну інформацію: джерело маршруту, мережа призначення, вихідний інтерфейс. Можливі джерела маршруту: пряме підключення; локальний маршрут; статичний маршрут; маршрут, отриманий за допомогою протоколу динамічної маршрутизації.

Таблиці маршрутизації IPv4 можуть містити чотири типи маршрутів: остаточні маршрути; маршрути 1-го рівня; батьківські маршрути 1-го рівня; дочірні маршрути 2-го рівня. Оскільки IPv6 є безкласовим протоколом, всі маршрути, по суті, є остаточними маршрутами 1-го рівня. Батьківських маршрутів 1-го рівня для дочірніх маршрутів 2-го рівня не існує.

3.3 Комутовані мережі та їх налаштування

Сучасний світ динамічний і мінливий: компанії вибирають все більш ефективні методи ведення щоденного бізнесу і, одночасно з цим, постійно удосконалюються мережеві технології. В наші дні користувачі розраховують на отримання прямого доступу до ресурсів компанії - в будь-який час і з будь-якої точки світу. Під цими ресурсами маються на увазі не тільки традиційні види даних, але також відео і голосова інформація. Також зростає потреба в технологіях спільної роботи. Ці технології забезпечують загальний доступ до ресурсів в режимі реального часу для віддалених користувачів, ніби вони фізично перебувають в одному місці.

Різні пристрої повинні органічно взаємодіяти один з одним для забезпечення швидкого, безпечного і надійного з'єднання між вузлами. Комутатори локальних мереж забезпечують підключення кінцевих користувачів до корпоративної мережі і головним чином відповідають за управління інформацією всередині середовища LAN. Маршрутизатори забезпечують передачу інформації між локальними мережами і, як правило, не взаємодіють з окремими вузлами. Всі вдосконалені сервіси залежать від доступності надійної маршрутизації і комутованої мережевої інфраструктури, на якій вони можуть бути побудовані. Дана інфраструктура повинна бути ретельно розроблена, правильно розгорнута і організована для забезпечення стійкості платформи.

З цього розділу починається вивчення поняття потоку трафіку в сучасній мережі. У розділі також розглядаються деякі сучасні моделі проектування мереж і способи побудови комутаторами локальної мережі таблиць маршрутизації та використання інформації про MAC-адреси для ефективної передачі даних між вузлами.

Індивідуально або в групі (за рішенням інструктора) обговоріть різні способи, за допомогою яких вузли відправляють і отримують дані, голосову інформацію і потокове відео.

Створіть матрицю (таблицю) зі списком типів мережевих даних, які можуть бути відправлені і прийняті. Наведіть п'ять прикладів.

Примітка. Приклад матриці представлений в документі, підготовленому для цього завдання з моделювання.

Збережіть результати вашої роботи в паперовому або електронному вигляді. Будьте готові обговорити вашу матрицю і інструкції в аудиторії.

Наш цифровий світ безперервно розвивається. Можливість доступу в Інтернет і корпоративні мережі більше не обмежуються територією офісу, географічним місцем розташування або часового поясу. У сучасних компаніях співробітники можуть отримати доступ до необхідних ресурсів та інформації практично з будь-якої точки світу, в будь-який час і з будь-якого пристрою (див. Рис. 1.1). Подібні вимоги призводять до необхідності вибудовувати мережі нового покоління - мережі, що забезпечують більшу безпеку, надійність і доступність.

Мережі нового покоління повинні не тільки відповідати існуючим очікуванням і підтримувати сучасне обладнання, але також взаємодіяти з застарілими платформами часто доводиться враховувати в рамках мережевого проектування.

Рис. 3.3.1

На рис. продемонстровані новітні платформи (об'єднані мережі), які сприяють забезпеченню доступу в мережу коли завгодно, звідки завгодно і з будь-якого пристрою.

Рис. 3.3.2 Новітнє мережеве обладнання

З метою організації колективної роботи в корпоративних мережах застосовують об'єднані рішення з використанням голосових систем, IP-телефонів, голосових шлюзів, відеопідтримки і відео-конференц-зв'язку (рис. 1.5). Конвергентна мережа з підтримкою спільної роботи, крім сервісів обробки даних, може включати в себе такі функції:

1. Управління викликами: обробка телефонних дзвінків, ідентифікація абонента, переведення виклику, утримання лінії і конференції.
2. Голосові повідомлення: голосова пошта.

3. Мобільний зв'язок: прийом важливих дзвінків незалежно від місцезнаходження.
4. Автовідповідач: більш швидке обслуговування клієнтів завдяки можливості напряму дзвінків безпосередньо до відповідного відділу або співробітнику.

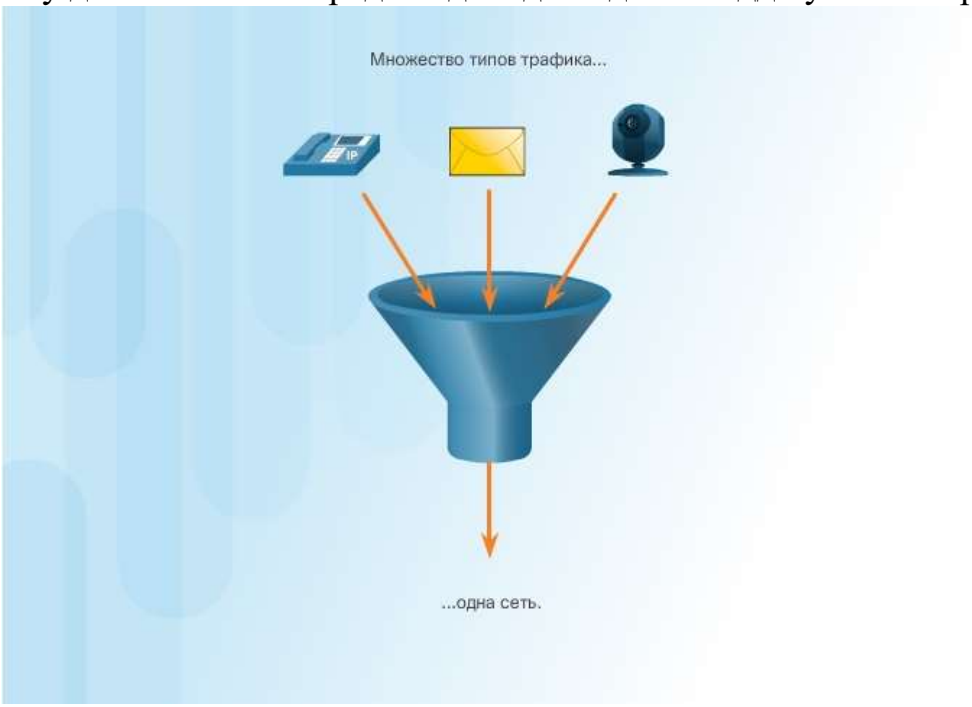


Рис. 3.3.3

Одне з основних переваг переходу на об’єднану мережу полягає в тому, що встановлювати і контролювати потрібно лише одну фізичну мережу. Це дозволяє значно заощадити на установці і управлінні окремими мережами для передачі голосу, відео та інших даних. Подібне мережеве рішення включає в себе управління IT-інфраструктурою, і таким чином, будь-які дії, додавання і зміни здійснюються через інтуїтивний інтерфейс управління. Крім того, об'єднана мережа підтримує програмні телефони на базі ПК і двоточкове відео, завдяки чому користувачі можуть спілкуватися по відеозв'язку так само легко, як при звичайному телефонному дзвінку.

Об'єднання сервісів в одну мережу призвело до еволюції мережевих технологій від традиційної ролі передачі даних в інформаційну магістраль для обміну даними, передачі голосу і відеозв'язку. Для забезпечення надійної передачі різних типів інформації подібна фізична мережа повинна бути ретельно розроблена і реалізована. Для управління таким складним середовищем потрібно структуроване проектування.

З огляду на зростання вимог до об'єднаних мереж розвиток останніх вимагає нового архітектурного підходу, що враховує впровадження інтелекту, спрощення операцій і масштабованість мережі в залежності від потреб майбутніх користувачів. Одна з останніх розробок в області проектування мереж - концепція мережі без кордонів Cisco.

Мережа без кордонів Cisco - це мережева архітектура, яка об'єднує інноваційну ідею і проектування. Рунтуючись на цій архітектурі, організації можуть забезпечити підтримку мережі без кордонів, яка безпечно, надійно і зручно пов'язує користувачів будь-яких пристроїв, в будь-який час і в будь-якому місці. Ця мережева архітектура розроблена спеціально для вирішення

інформаційних і ділових питань, наприклад підтримки об'єднаної мережі і безупинно мінливих схем організації робіт.

Мережа без кордонів Cisco надає платформу для об'єднання дротового і бездротового доступу, включаючи застосування політик, розмежування доступу і управління продуктивністю пристроїв різних типів. Мережа без кордонів, яка використовує таку архітектуру, будується на основі масштабованої і відмовостійкої ієрархічної інфраструктури апаратного забезпечення (див. Рис. 1.6). Об'єднуючи цю апаратну інфраструктуру з програмними рішеннями на основі політик, мережа без кордонів Cisco надає два головних набору сервісів: мережеві сервіси та сервіси для користувачів і кінцевих пристроїв. Для управління всіма цими сервісами використовується інтегроване рішення. В результаті різні мережеві елементи можуть спільно працювати, користувачі отримують повсюдний доступ до ресурсів в будь-який час, забезпечуються оптимізація, масштабованість і безпека.

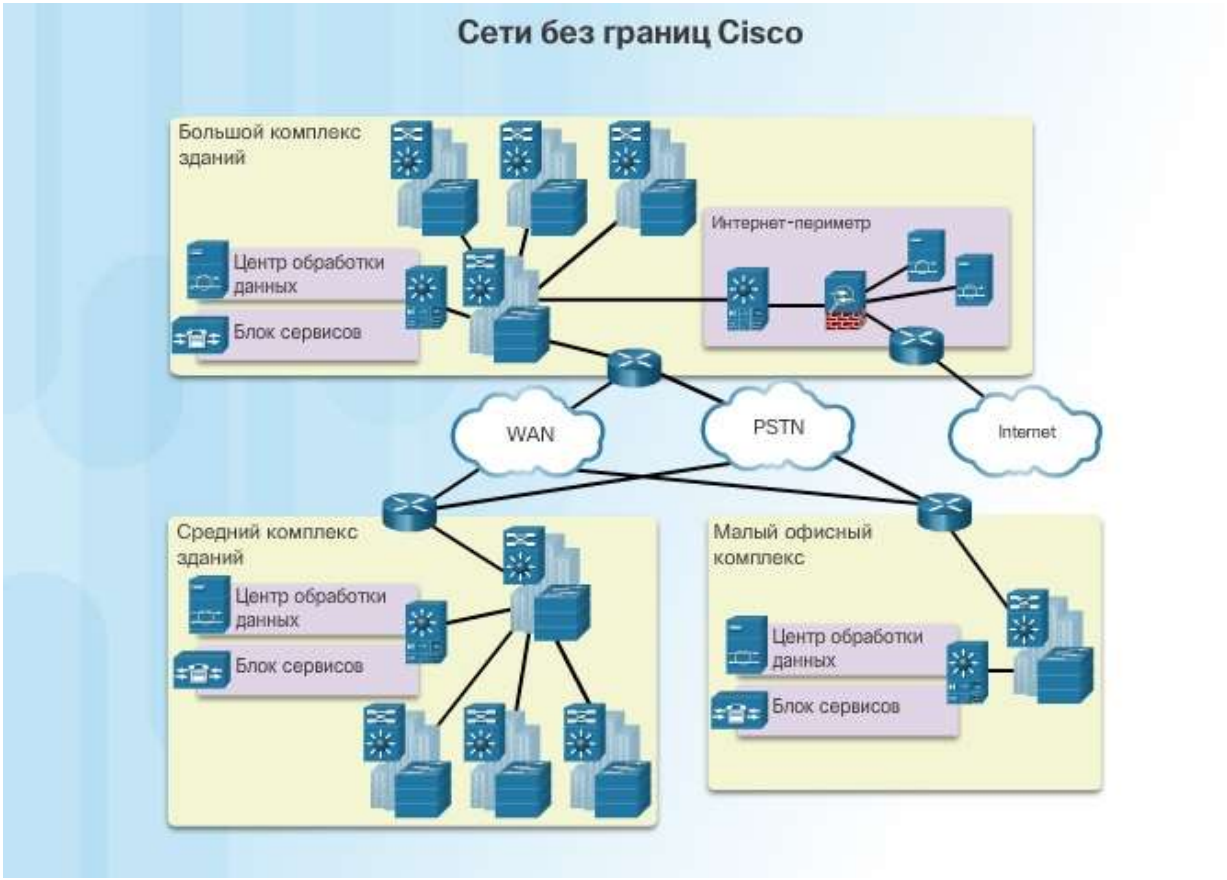


Рис. 3.3.4

Для забезпечення максимальної доступності, гнучкості, безпеки і зручності експлуатації комутованої мережі без кордонів в процесі її створення необхідно слідувати чітким принципам проектування. Комутована мережа без кордонів повинна відповідати поточним і можливим майбутнім вимогам до роботи сервісів і технологій. Керівництво з проектування комутованої мережі без кордонів побудовано на наступних принципах:

Ієрархічність - спрощує розуміння ролі кожного пристрою на кожному рівні, забезпечує підтримку в процесі розгортання, експлуатації та управління, а також знижує кількість несправностей на кожному рівні.

Модульність - сприяє бездоганному розширенню мережі та впровадження інтегрованих сервісів у міру необхідності.

Відмовостійкість - забезпечує безперебійну роботу мережі відповідно до очікувань користувачів.

Гнучкість - забезпечує раціональний розподіл навантаження трафіку за рахунок використання всіх мережевих ресурсів.

Перераховані принципи залежать один від одного. Саме тому вкрай важливо розуміти природу і способи їх взаємодії в рамках комутованої мережі. Ієрархічне проектування комутованої мережі без кордонів створює основу, яка дозволяє мережевим розробникам об'єднувати функції безпеки, мобільності та уніфікованої комунікації. Як показано на рис. 1.6 і 1.7, основою ієрархічного проектування мереж кампусного типу є двічі перевірені і схвалені до застосування трирівневі і дворівневі моделі.

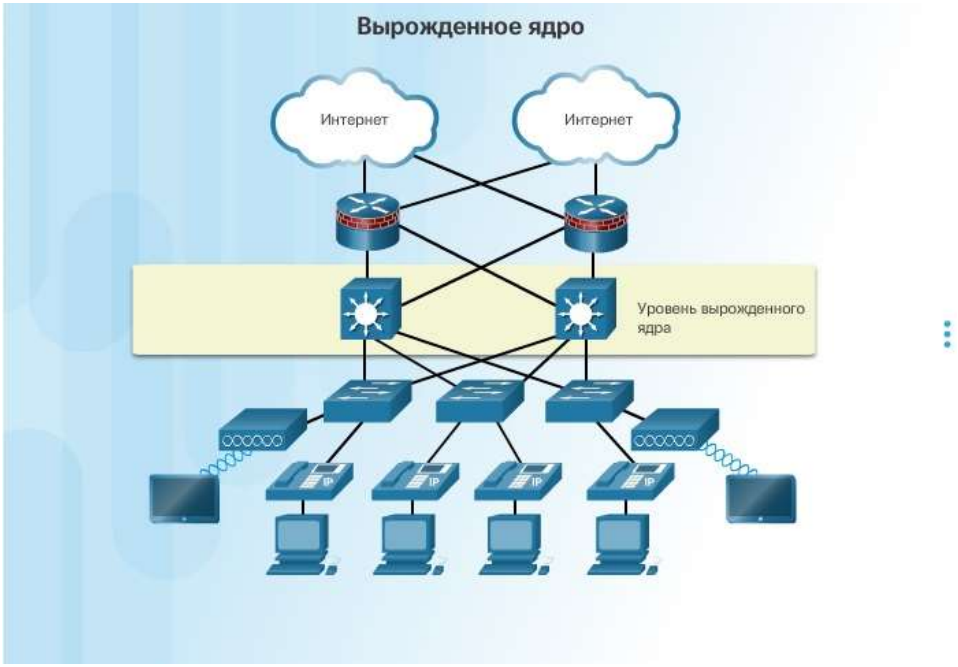


Рис. 3.3.5

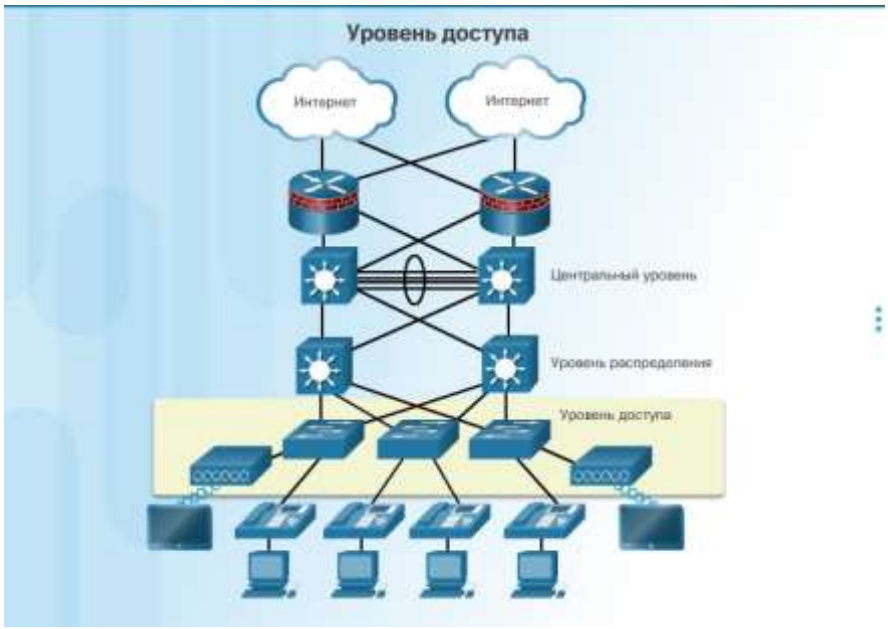


Рис. 3.3.6

Три основні рівні в рамках розглянутих багаторівневих проектів є рівні доступу, розподілу і ядра. Кожен рівень можна розглядати як чіткий, структурований модуль кампусової мережі, наділений певними ролями і функціями. Введення принципу модульності в ієрархічну архітектуру мережі дає додаткову гарантію - кампусні мережі модульних конструкцій демонструють більшу надійність і гнучкість по відношенню до забезпечення найважливіших мережевих сервісів. Модульність також сприяє розширенню мережі та внесення змін, що відбуваються з плином часу.

Рівень доступу являє периметр мережі, де трафік входить або залишає мережу кампусного типу. Традиційно основна функція комутатора рівня доступу полягає в забезпеченні користувачеві мережевого доступу. Комутатори рівня доступу підключаються до комутаторів рівня розподілу, які реалізують технології мережевої інфраструктури, такі як маршрутизація, якість обслуговування і безпеку.

Для відповідності вимогам мережевих додатків і кінцевих користувачів комутаційні платформи нового покоління надають більш однорідні, інтегровані і інтелектуальні сервіси для різних типів кінцевих пристроїв по периметру мережі. Впровадження інтелектуальних функцій в комутатори рівня доступу забезпечує більш ефективну і безпечну роботу додатків мережі.

Рівень розподілу взаємодіє між рівнем доступу і рівнем ядра для забезпечення багатьох важливих функцій:

- можливість агрегації великих дротових мереж в комунікаційному шафі;
- агрегація широкомовних доменів рівня 2 і кордонів маршрутизації рівня 3;
- надання доступу інтелектуальної комутації, маршрутизації і функцій політики доступу до іншої частини мережі;
- забезпечення високого рівня доступності ядра для кінцевих користувачів і наявність маршрутів дорівнює вартості за допомогою резервних комутаторів рівня розподілу;
- надання диференційованих послуг додатків з різними класами обслуговування по периметру мережі.

Рівень ядра - це мережева магістраль. Даний рівень об'єднує кілька рівнів мережі кампусного типу. Рівень ядра служить агрегатором для всіх інших будівельних блоків кампусової мережі і пов'язує кампус з іншими сегментами мережі. Основне завдання рівня ядра полягає в забезпеченні ізоляції збоїв і високошвидкісного магістрального підключення.

На рис. 1.8 представлена трирівнева архітектура мережі кампусні типу для організацій, в яких рівні доступу, розподілу і ядра є окремими рівнями. Для створення спрощеного, що масштабується, рентабельного і ефективного проекту фізичної структури кабельної мережі рекомендується вибудовувати фізичну топологію мережі по типу розширеної зірки від центральної будівлі до всіх інших будівель в рамках одного комплексу.

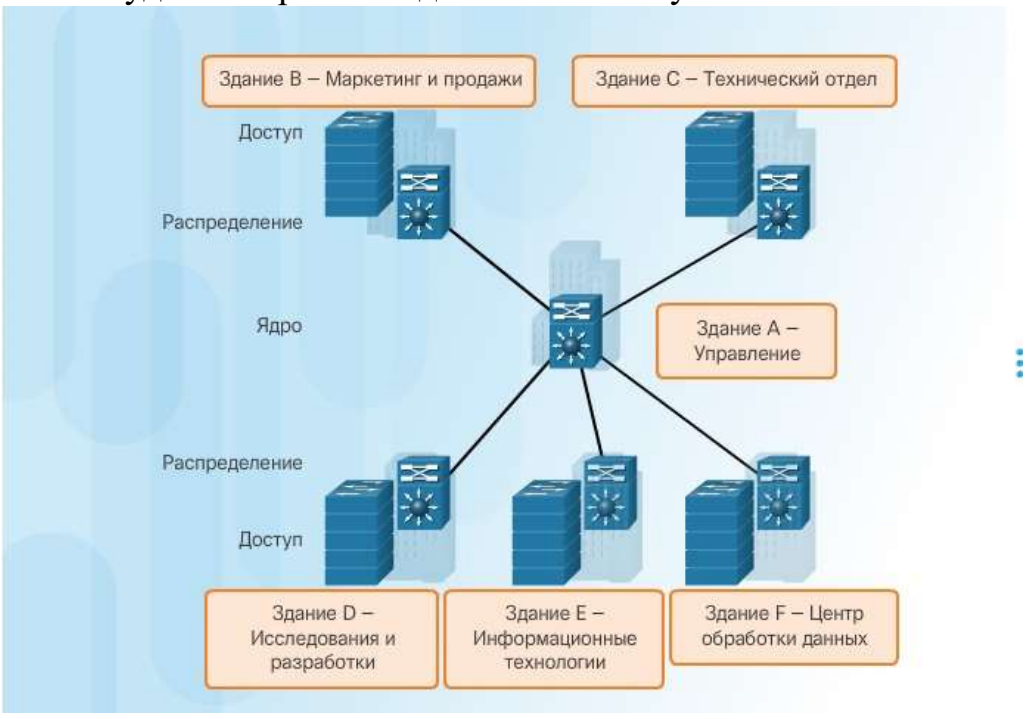


Рис. 3.3.7

У деяких випадках, коли відсутня висока масштабованість фізичної інфраструктури або мережі, розмежування рівнів розподілу і ядра не потрібно. Поділ між рівнем ядра і рівнем розподілу може не знадобитися в невеликій кампусової мережі, в якій кількість підключених до мережі користувачів невелика, або коли підрозділ кампусу складається з однієї будівлі. При такому варіанті рекомендується використовувати альтернативну дворівневу схему мережі комплексу будівель, яку ще називають схемою мережі зі згорнутим ядром.

За останні два десятиліття роль комутованих мереж істотно зросла. Зовсім недавно повсюдно використовувалися плоскі комутовані мережі 2-го рівня. Для передачі трафіку локальної мережі в організації плоскі комутовані мережі 2-го рівня використовували Ethernet-підключення та поширені вузлові ретранслятори. Як показано на рис. 1, в ієрархічній топології відбулася радикальна заміна мереж на комутовані LAN. Комутована локальна мережа забезпечує більшу гнучкість, оптимізоване управління трафіком і наступні додаткові функції:

- Якість обслуговування
- Додаткова безпека
- Підтримка підключених бездротових мереж
- Підтримка таких нових технологій, як IP-телефонія і мобільні сервіси

На рис. 1.9 показано ієрархічне проектування, що використовується в комутованій мережі без кордонів.

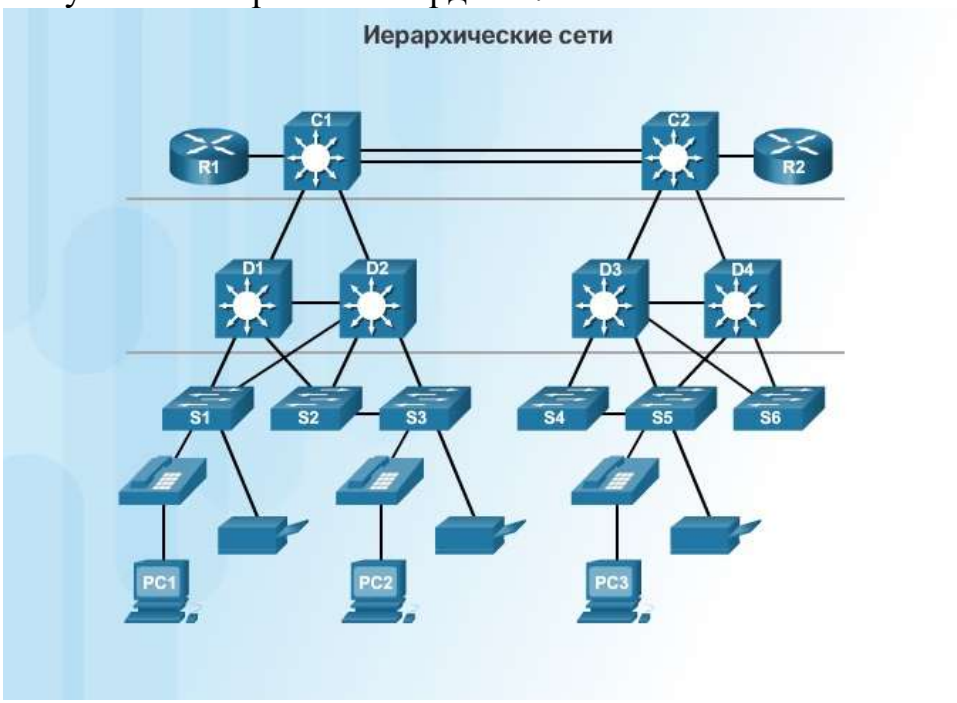


Рис. 3.3.8

У корпоративних мережах використовуються різні типи комутаторів. Правильний вибір типів комутаторів, які відповідають вимогам мережі, грає велику роль. На рис. 1.10 представлений ряд поширених чинників, що мають важливе значення при виборі комутаторів для корпоративної мережі.

При виборі типу комутатора проектувальник мережі повинен вибрати стековий або нестековий комутатор з фіксованою або модульною конфігурацією. Ще один фактор, який необхідно враховувати при виборі

пристрою - це висота комутатора, яка вимірюється кількістю монтажних одиниць. Останній критерій стосується комутаторів, які монтуються в стійку (нарощувані). Наприклад, на рис. 1.11 зображені комутатори з фіксованою конфігурацією висотою в одну стандартну одиницю (1U). Розглянуті вище параметри іноді називають форм-факторами комутатора.

Рис. 3.3.9

Комутатори з фіксованою конфігурацією

Комутатори з фіксованою конфігурацією підтримують тільки встановлені функції та параметри (рис. 2). Для кожної моделі передбачений ряд певних функцій і параметрів. Наприклад, гігабітний комутатор з двадцятьма чотирма портами не підтримує додаткові порти. Кількість і типи підтримуваних портів в комутаторах з фіксованою конфігурацією залежать від конфігурації того чи іншого комутатора.

Модульні комутатори

Комутатори з модульної конфігурацією підтримують більше функцій. Зазвичай модульні комутатори поставляються з шасі різного розміру, що дозволяє встановлювати різну кількість модульних лінійних плат (рис. 1.12). На лінійних платах знаходяться порти. Лінійну плату вставляють в шасі комутатора подібно до того, як плати розширення вставляють в ПК. Чим більше шасі, тим більше модулів воно підтримує. Існують шасі різного розміру. У модульний комутатор з однієї лінійної картою на 24 порту може бути встановлена додаткова лінійна карта на 24 порти, в результаті чого загальна кількість портів збільшиться до 48.

Рис. 3.3.10

Стекові комутатори з фіксованою конфігурацією

Стекові комутатори можуть бути з'єднані за допомогою спеціального кабелю, що забезпечує високу пропускну здатність між комутаторами (рис. 1.13). Технологія Cisco StackWise дозволяє з'єднувати до дев'яти комутаторів. Комутатори можна розмістити один над іншим і з'єднати їх кабелями по шлейфовому типу. Розміщені в стек комутатори працюють з ефективністю одного комутатора великих розмірів. Стекові комутатори рекомендується використовувати при виконанні завдань, коли важливі відмовостійкість і доступність пропускної здатності, а застосування модульного комутатора виявляється занадто дорогим. Перехресне з'єднання цих стекових комутаторів забезпечує швидке відновлення мережі в разі відмови одного комутатора. Для з'єднань в стекових комутаторах передбачений спеціальний порт. Багато стекових комутаторів Cisco також підтримують технологію StackPower, що дозволяє елементам стека обмінюватися живленням.

Рис. 3.3.11

Комутація як загальна концепція мережевих і телекомунікаційних технологій.

Концепція комутації та пересилання кадрів універсальна для мережевих і телекомунікаційних технологій. У локальної, глобальної та телефонної мережах використовуються різні типи комутаторів. Основна концепція комутації полягає в прийнятті пристроєм рішення на основі двох критеріїв:

- вхідний порт
- адреса призначення

Рішення про те, як комутатор пересилає трафік, приймається в залежності від потоку трафіку. Термін «вхідний» використовується для опису порту, через який кадр входить в пристрій. Термін «вихідний» використовується для опису кадрів, які залишають пристрій з певного порту.

Комутатор LAN веде таблицю, за допомогою якої визначає, як пересилати трафік через комутатор. Натисніть кнопку «Відтворення» на малюнку, щоб переглянути анімацію, яка ілюструє процес комутації. У наведеному прикладі розглядаються наступні ситуації.

Інтелектуальні здібності комутатора LAN полягають в його здатності використовувати свою таблицю для пересилання трафіку на основі цільового входу і адреси призначення повідомлення. У випадку з комутатором LAN є тільки одна таблиця комутації, яка описує суворий зв'язок між адресами і портами; тому повідомлення з даними адресами призначення завжди залишає комутатор з одного і того ж вихідного порту, незалежно від порту, через який воно входить.

Комутатори Ethernet 2-го рівня пересилають кадри Ethernet, грунтуючись на MAC-адресі призначення кадру.

Динамічне заповнення таблиці MAC-адрес комутатора

Комутатори використовують MAC-адреси для направлення мережевого трафіку через комутатор на відповідний порт до місця призначення. Комутатор складається з набору мікросхем і відповідного програмного забезпечення, за допомогою якого дані проходять через комутатор. Щоб комутатор знав, який порт використовувати для передачі кадру, він повинен спочатку дізнатися, які пристрої існують на кожному порту. У міру того, як комутатор дізнається ставлення портів до пристроїв, він створює таблицю MAC-адрес або таблицю асоціативної пам'яті (CAM). CAM (асоціативна пам'ять, англ. Content Addressable Memory) - це особливий тип пам'яті, який використовується в прикладних програмах швидкого пошуку.

Комутатори LAN визначають спосіб обробки вхідних кадрів шляхом ведення таблиці MAC-адрес. Комутатор створює свою таблицю MAC-адрес, записуючи MAC-адресу кожного пристрою, підключеного до кожного зі своїх портів. Комутатор використовує дані з таблиці MAC-адрес для відправлення кадрів, призначених для конкретного пристрою з порту, який був призначений на цей пристрій.

При надходженні кожного кадру Ethernet на комутатор виконується наступний двоетапний процес:

Крок 1. Отримання інформації: перевірка MAC-адреси джерела.

При кожному надходженні кадру в комутатор виконується перевірка на наявність нової інформації. Перевіряються MAC-адресу джерела, зазначена в кадрі, і номер порту, з якого кадр надходить в комутатор: якщо MAC-адресу джерела відсутня, він додається в таблицю разом з номером вхідного порту. Якщо MAC-адреса джерела вже існує, комутатор оновлює таймер поновлення для цього запису. За замовчуванням на більшості комутаторів Ethernet дані в таблиці зберігаються протягом 5 хвилин. *Примітка*: якщо MAC-адреса джерела вказана в таблиці, але з іншим портом, комутатор вважає цей запис новим. Запис замінюється на той же MAC-адрес, але з більш актуальним номером порту.

Крок 2. Пересилання: перевірка MAC-адреси призначення

Якщо MAC-адресу призначення є адресою одноадресної розсилки, комутатор шукає збіг між MAC-адресою призначення кадру і записом в таблиці MAC-адрес: якщо MAC-адресу призначення є в таблиці, комутатор пересилає кадр через вказаний порт. Якщо MAC-адреси призначення немає в таблиці, комутатор пересилає кадр через всі порти, крім вхідного порту. Це називається одноадресною розсилкою невідомого одержувача. Примітка: якщо MAC-адреса призначення є адресою широкомовної розсилки, комутатор також пересилає кадр через всі порти, крім вхідного порту.

У той час як мережі підприємства розширюються, їх продуктивність помітно знижується. У зв'язку з цим в мережі були додані мости Ethernet (попередня версія комутатора) для обмеження розмірів колізійних доменів. У 90-х рр. розвиток технологій дозволило замінити мости Ethernet на комутатори для локальних мереж Ethernet. Ці комутатори могли передати прийняття рішення про пересилання рівня 2 від програмного забезпечення в спеціалізовані інтегральні мікросхеми (ASIC). ASIC скорочують час обробки пакетів в пристрої і дозволяють пристроям обробляти більше даних без зниження

продуктивності. Цей метод пересилання кадрів даних на рівні 2 назвали комутацією з проміжним зберіганням (режим «store-and-forward»). Даний термін протиставлений терміну «наскрізна комутація».

При використанні методу комутації з проміжним зберіганням рішення про переадресації кадру приймається після отримання повного кадру і його перевірки на предмет помилок за допомогою математичного механізму - циклічного надлишкового коду (CRC).

У сегментах Ethernet на основі концентраторів мережеві пристрої «борються» за контроль над середовищем передачі, оскільки пристрої повинні передавати дані по черзі. Сегменти мережі, в яких пристрою можуть використовують смугу пропускання, називаються колізійними доменами. Якщо два або більше пристроїв в одному колізійному домені одночасно намагаються передавати дані, виникає колізія.

Якщо комутаційний порт Ethernet працює в напівдуплексному режимі, кожен сегмент знаходиться в своєму власному колізійному домені. Якщо ж порти комутатора Ethernet працюють в повнодуплексному режимі, колізії виключені і, отже, колізійний домен відсутній. За замовчуванням порти комутатора Ethernet автоматично узгоджують повнодуплексний режим, якщо суміжне пристрій може також працювати в повнодуплексному режимі. Якщо комутаційний порт підключений до пристрою, що працює в напівдуплексному режимі, такому як традиційний концентратор, то даний порт буде працювати в напівдуплексному режимі. У разі напідуплексного режиму комутаційний порт буде частиною колізійного домену.

Як показано на рисунку 1.14 , повнодуплексний режим встановлюється в тому випадку, якщо обидва пристрої підтримують його при максимальній загальній пропускній здатності.

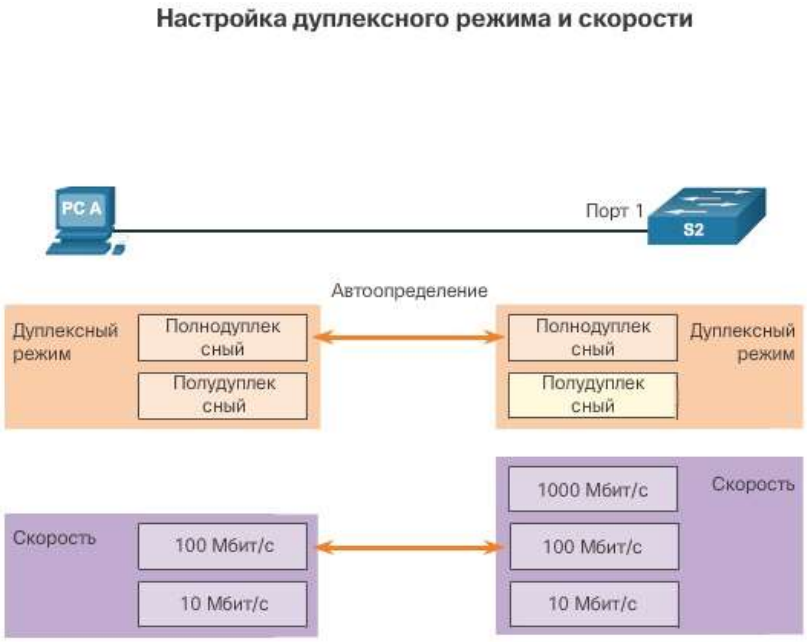


Рис. 3.3.12

Сукупність з'єднаних комутаторів формує єдиний широкомовний домен. Тільки пристрій мережевого рівня, наприклад маршрутизатор, може розділити широкомовний домен рівня 2. Маршрутизатори використовуються для

сегментації доменів широкомовної розсилки, але вони також сегментують домен колізій. Коли пристрій відправляє широкомовне розсилання рівня 2, MAC-адрес призначення в кадрі представлений одиницями в двійковому форматі.

Широкомовний домен рівня 2 називають широкомовною доменом MAC-адрес. У широкомовний домен MAC-адрес входять всі пристрої локальної мережі, які отримують кадри широкомовної розсилки від вузла.

Коли комутатор отримує широкомовний кадр, він пересилає кадр з усіх своїх портів, за винятком вхідного порту, на якому широкомовний кадр був отриманий. Кожен пристрій, підключений до комутатора, отримує копію широкомовного кадру і обробляє її. У деяких випадках широкомовні розсилання необхідні для початкового місцезнаходження інших пристроїв і мережевих сервісів, але, крім цього, вони знижують ефективність мережі. Смуга пропускання мережі використовується для поширення широкомовного трафіку. Надмірна кількість широкомовних розсилок і висока інтенсивність трафіку в мережі можуть привести до перевантаженості і в результаті до зниження продуктивності мережі.

Коли два комутатора з'єднані, широкомовний домен збільшується. В цьому випадку широкомовний кадр пересилається по всім підключеним портам.

Комутатори LAN мають певні характеристики, що дозволяють їм знижувати перевантаження мережі. За замовчуванням порти комутаторів, з'єднаних між собою, намагаються встановити зв'язок в повнодуплексному режимі, тим самим виключаючи колізійні домени. Кожен повнодуплексний комутаційний порт забезпечує повну пропускну здатність для одного або декількох пристроїв, підключених до цього порту. Повнодуплексне з'єднання дозволяє одночасно передавати і отримувати сигнал. Повнодуплексні з'єднання значно покращують продуктивність локальної мережі, крім того, вони необхідні для передачі даних зі швидкістю 1 Гбіт/с і вище.

Комутатори з'єднують сегменти локальних мереж, використовують таблицю MAC-адрес для визначення сегмента, якому потрібно відправити кадр, і можуть скоротити або повністю усунути колізії. Нижче наведені деякі важливі характеристики комутаторів, які сприяють зниженню перевантаженості мережі.

Висока щільність портів. Комутатори мають високу щільністю портів: часто висота комутаторів з 24 і 48 портами дорівнює одному стоєчному модулю, а швидкість їх може досягати 100 Мбіт/с, 1 Гбіт/с і 10 Гбіт/с. Комутатори великих підприємств можуть підтримувати декілька сотень портів.

Великі буфери кадрів. Можливість зберігати більше отриманих кадрів перед їх відкиданням вельми корисна, особливо при наявності перевантажених портів, до яких підключені сервери або інші частини мережі.

Швидкість порту. Залежно від вартості комутатора можлива підтримка сукупності швидкостей. Найбільш поширені порти зі швидкостями 100 Мбіт/с, 1 або 10 Гбіт/с (швидкість 100 Гбі/ с також не є неможливою).

Швидка внутрішня комутація. Можливість швидкого внутрішнього пересилання забезпечує високу продуктивність. В якості методу можна використовувати швидку внутрішню шину або загальну пам'ять, яка впливає на загальну продуктивність комутатора.

Низька вартість кожного порту. Комутатори забезпечують високу щільність портів при мінімумі витрат.

Для цієї вправи використовуйте програму Packet Tracer. Підключення до Інтернету не потрібно. Працюючи в парі з однокурсником, створіть два проекти мережі для реалізації наступних сценаріїв.

Сценарій 1. Проект навчальної аудиторії (LAN)

15 кінцевих пристроїв учнів представлені одним або двома комп'ютерами. Одне кінцеве пристрій інструктора бажано представити сервером. Потокові відео презентації через підключення LAN.

Сценарій 2. Адміністративний проект (WAN)

Всі вимоги, описані в сценарії 1. Доступ до і від віддаленого адміністративного сервера для відео-презентацій і переданих оновлень для ПО мережного додатки. Обидва типи - локальна мережа і WAN - повинні поміститися на одному файловому екрані Packet Tracer. Всі проміжні пристрої повинні мати маркування із зазначенням моделі (або імені) комутатора і моделі (або імені) маршрутизатора.

Збережіть результат своєї роботи і будьте готові обґрунтувати ваш вибір пристроїв і їх розміщення інструктору і іншим учням.

Короткі висновки:

1. Спостерігається тенденція мереж до об'єднання з використанням єдиного комплекту проводів і пристроїв для передачі голосу, відео та інших даних. Крім того, відбулися різкі зміни в організації діяльності підприємств. Співробітники більше не обмежені територією офісу або географічним місцем розташування. Тепер ресурси повинні бути доступні в будь-який час і в будь-якій точці світу. Архітектура мереж без кордонів Cisco робить доступними різні елементи (від ключів доступу до точок бездротового доступу) для колективної роботи і дозволяє користувачам здійснювати доступ до ресурсів з будь-якого місця і в будь-який час.
2. Традиційна трирівнева ієрархічна модель архітектури розділяє мережу на рівні ядра, розподілу і доступу, забезпечуючи оптимізацію кожної частини мережі для виконання певної функції. Така архітектура забезпечує модульність, відмовостійкість і гнучкість - фактори, що становлять основу платформи, в рамках якої проектувальники мереж можуть поєднувати безпеку, мобільність і переваги уніфікованих комунікацій. У деяких мережах не потрібні роздільні рівні ядра і розподілу. У таких мережах функції рівнів ядра і розподілу часто об'єднані.
3. Комутатори Cisco для локальних мереж використовують ASIC для пересилання кадрів на основі MAC-адреси призначення. Перед цим комутатор повинен спочатку використовувати MAC-адресу джерела вхідних кадрів, щоб створити таблицю MAC-адрес в асоціативній пам'яті (CAM). Якщо MAC-адресу призначення міститься в цій таблиці, кадр пересилається тільки на певний порт призначення. Якщо MAC-адресу призначення не міститься в таблиці MAC-адрес, кадри розсилаються з усіх портів, крім того, на якому цей кадр був отриманий.
4. У комутаторах використовується або комутація з проміжним зберіганням, або наскрізна комутація. Комутація з проміжним зберіганням переводить весь кадр в буфер і перевіряє CRC перед пересиланням кадру. Наскрізна комутація зчитує

тільки першу частину кадру і починає пересилати його відразу після прочитання адреси призначення. Перед пересиланням не виконується виявлення помилок, хоча це і не займає багато часу.

5. Комутатори намагаються автоматично узгодити повнодуплексний зв'язок за замовчуванням. Порти комутатора не блокують широкомовні розсилання, а об'єднання комутаторів може збільшити розмір домену широкомовної розсилки, що, в свою чергу, часто призводить до зниження продуктивності мережі.

Комутатори - це пристрої, що використовуються для з'єднання декількох пристроїв в одній мережі. У правильно спроектованій мережі комутатори локальної мережі відповідають за напрямок потоку даних і управління ним на рівні доступу до мережевих ресурсів.

Комутатори Cisco налаштовуються автоматично, тому немає необхідності виконувати додаткову настройку. Однак комутатори Cisco працюють під управлінням Cisco IOS, і для відповідності певним вимогам мережі їх можна налаштувати вручну. Таким чином, можна виконати для порту настройки швидкості, пропускної спроможності і параметрів безпеки.

Комутаторами Cisco можна управляти як локально, так і віддалено. Для віддаленого управління на комутаторі потрібно налаштувати IP-адресу і шлюз за замовчуванням. І це лише дві конфігурації зі списку розглянутих в цьому розділі конфігурацій.

Комутатори працюють на рівні доступу, де мережеві пристрої клієнтів підключені до мережі безпосередньо, а співробітники IT-відділів прагнуть забезпечити для своїх користувачів безперешкодний доступ до мережі. Рівень доступу є одним з найбільш уразливих ділянок мережі, оскільки він повністю відкритий для користувачів. Комутатори повинні бути захищені від усіх типів атак, оскільки вони захищають дані користувачів і забезпечують високошвидкісні підключення. Безпека портів - одна з функцій безпеки комутаторів Cisco.

У цій главі розглядається ряд основних параметрів конфігурації комутатора, необхідних для підтримки безпечної, доступної комутованої мережеві середовища.

Послідовність завантаження комутатора

Після включення комутатор Cisco проходить наступні стадії завантаження:

1. По-перше, комутатор завантажує програму самотестування при включенні живлення (POST), що зберігається в ПЗУ. POST перевіряє ЦП підсистеми. Програма тестує ЦП, оперативну динамічну пам'ять (DRAM) і частини флеш-пристроїв, які складають файлову систему пристрою.
2. Після цього на комутаторі запускається програмне забезпечення початкового завантажувача. Початковий завантажувач - це невелика програма, яка зберігається в ПЗУ і запускається відразу після успішного завершення перевірки POST.
3. Початковий завантажувач виконує низкоуровневую ініціалізацію ЦП. Він ініціалізує регістри ЦП, які контролюють фізичну пам'ять, кількість пам'яті і швидкість.
4. Потім програма запускає файлову систему флеш-пам'яті на материнській платі.

5. Нарешті, початковий завантажувач знаходить і завантажує образ операційної системи IOS за замовчуванням і передає їй управління комутатором.

Початковий завантажувач знаходить образ Cisco IOS на комутаторі наступним чином: комутатор намагається завантажитися автоматично за допомогою інформації з змінної середовища BOOT. Якщо змінна не налаштована, комутатор намагається завантажити і виконати перший виконуваний файл, виконавши рекурсивний пошук у глибину по всій файлової системи флеш-пам'яті. При пошуку в глибину по каталогу перед пошуком в вихідному каталозі виконується пошук в кожному підкаталозі. На комутаторах серії Catalyst 2960 файл образу зазвичай міститься в каталозі, який названий так само, як і файл образу (крім файлів з розширенням .bin). Потім операційна система IOS ініціалізує інтерфейси, використовуючи команди Cisco IOS з файлу завантажувального конфігурації, який зберігається в енергонезалежному ОЗУ (NVRAM).

На рисунку 2.1 змінна середовища BOOT налаштована за допомогою команди режиму глобальної конфігурації boot system. Зверніть увагу, що IOS знаходиться в окремій папці, і шлях до папки вказано. Використовуйте команду show boot, щоб дізнатися, як налаштований файл поточного завантаження IOS.

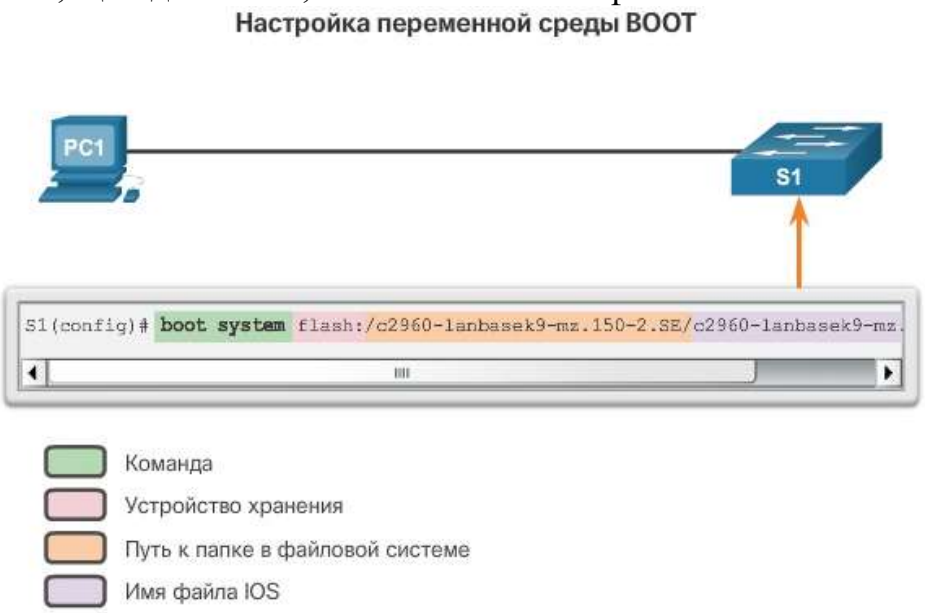


Рис. 3.3.13

Відновлення після системного збою

Початковий завантажувач забезпечує доступ до комутатора, якщо ОС не можна використати через відсутність або пошкодження системних файлів. У початковому завантажувачі є інтерфейс командного рядка, що забезпечує доступ до файлів, які зберігаються у флеш-пам'яті.

Доступ в початковий завантажувач можна отримати через консольне підключення, виконавши такі дії:

Крок 1. Підключіть ПК за допомогою консольного кабелю до консольного порту комутатора. Налаштуйте програму емуляції терміналу для підключення до комутатора.

Крок 2. Відключіть кабель живлення комутатора.

Крок 3. Заново підключіть шнур живлення до комутатора і після закінчення 15 секунд натисніть і утримуйте кнопку Mode, поки системний індикатор блимає зеленим світлом.

Крок 4. Утримуйте кнопку Mode, поки системний індикатор блимне жовтим, а потім загориться зеленим. Після цього відпустіть кнопку Mode.

Крок 5. У програмі емуляції терміналу з'явиться командний рядок початкового завантажувача switch.

Командний рядок початкового завантажувача підтримує команди для форматування файлової флеш-системи, переустановлення операційної системи і відновлення втраченого або забутого пароля. Наприклад, команду dir можна використовувати для перегляду списку файлів в зазначеному каталозі, як показано на рисунку 2.2.

Примітка. Зверніть увагу, що в цьому прикладі IOS знаходиться в корені папки флеш-пам'яті.

Список каталогов в начальном загрузчике

```
Switch# dir flash:
Directory of flash:/

    2  -rwx    11607161   Mar 1 2013 03:10:47 +00:00  c2960-
lanbasek9-mz.150-2.SE.bin
    3  -rwx        1809   Mar 1 2013 00:02:48 +00:00  config.text
    5  -rwx        1919   Mar 1 2013 00:02:48 +00:00  private-
config.text
    6  -rwx       59416   Mar 1 2013 00:02:49 +00:00  multiple-fs

32514048 bytes total (20841472 bytes free)
Switch#
```

Рис. 3.3.14

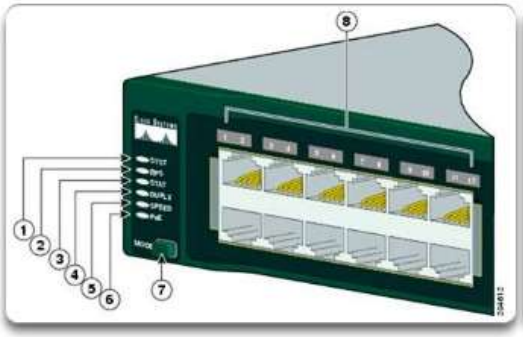
Світлодіодні індикатори комутатора

Комутатори Cisco Catalyst оснащені декількома індикаторами стану. Індикатори комутатора дозволяють швидко оцінити активність і продуктивність комутатора. Комутатори різних моделей і з різними функціями оснащені різними індикаторами, їх розташування на передній панелі також може відрізнятися.

На рисунку 2.3 показані індикатори та кнопка Mode комутатора Cisco Catalyst 2960. Кнопка Mode використовується для перемикання стану порту, дуплексного режиму порту, швидкості порту і стану PoE (якщо ця функція підтримується) на індикаторах портів. Нижче описується призначення

світлодіодних індикаторів і значення їх кольорів.

Индикаторы коммутатора



Индикаторы коммутатора Catalyst 2960

1	Системный индикатор	5	Индикатор скорости порта
2	Индикатор RPS (если на коммутаторе поддерживается RPS)	6	Индикатор состояния питания через Ethernet (если на коммутаторе поддерживается питание через Ethernet)
3	Индикатор состояния порта (это режим по умолчанию)	7	Кнопка режима
4	Индикатор дуплексных режимов	8	Индикаторы порта

Рис. 3.3.15

Системний індикатор вказує, чи отримує система живлення і чи працює вона нормально. Якщо індикатор не горить, то система вимкнена. Якщо індикатор горить зеленим світлом, то система працює нормально. Якщо індикатор горить жовтим, система отримує живлення, але працює з перебоями.

Індикатор системи резервного живлення (RPS) відображає стан RPS. Якщо цей індикатор не горить, то система RPS вимкнена або підключена неправильно. Якщо індикатор горить зеленим, то резервне джерело живлення підключене і готове до забезпечення резервного живлення. Якщо індикатор блимає зеленим, то RPS підключена, але недоступна, оскільки забезпечує живлення інших пристроїв. Якщо індикатор горить жовтим, то резервне джерело живлення знаходиться в режимі очікування або несправне. Якщо індикатор блимає жовтим, то внутрішнє джерело живлення комутатора не працює і задіяне джерело резервного живлення.

Індикатор стану порту вказує на обраний режим стану порту. Даний режим є режимом за замовчуванням. При виборі відповідної функції світлодіодні індикатори порту будуть відображати кольори з різними значеннями. Якщо індикатор вимкнений, то зв'язок відсутній або порт був відключений адміністратором. Якщо індикатор горить зеленим, то зв'язок є. Якщо індикатор блимає зеленим, це свідчить про активність порту, і він відправляє або отримує дані. Якщо колір індикатора чергується між зеленим і жовтим, то зв'язок порушений. Якщо індикатор горить жовтим, то порт заблокований, щоб гарантувати відсутність петлі в домені пересилання (зазвичай порти знаходяться в цьому стані протягом перших 30 секунд після активації). Якщо індикатор блимає жовтим, порт заблокований в цілях запобігання можливої петлі в домені пересилання.

Індикатор дуплексного режиму порту вказує на обраний двобічний режим порту. Індикатор дуплексного режиму порту вимкнений, якщо порт працює в

напівдуплексному режимі. Якщо індикатор порту горить зеленим, то порт знаходиться в повнодуплексному режимі.

Індикатор швидкості портів вказує на обраний режим швидкості портів. При виборі відповідної функції світлодіодні індикатори порту будуть відображати кольори з різними значеннями. Якщо індикатор вимкнений, то порт працює на швидкості 10 Мбіт/с. Якщо індикатор горить зеленим, то порт працює на швидкості 100 Мбіт/с. Якщо індикатор блимає зеленим, то порт працює на швидкості 1000 Мбіт/с.

Індикатор режиму живлення через Ethernet (PoE) - цей індикатор присутній, якщо підтримується PoE. Якщо індикатор вимкнений, значить, режим PoE знято, живлення або функціональність портів не порушені. Якщо індикатор блимає жовтим, то режим PoE знято, але принаймні живлення одного з портів порушено або виник збій в роботі PoE. Якщо індикатор горить зеленим, то обраний режим PoE, і індикатори порту будуть відображати кольори з різними значеннями. Якщо цей індикатор не горить, то PoE теж вимкнений. Якщо індикатор горить зеленим, то PoE функціонує. Якщо колір індикатора чергується між зеленим і жовтим, то PoE був вимкнений, оскільки подача живлення пристрою з справним живленням може перевищити допустиму потужність комутатора. Якщо індикатор блимає жовтим, то PoE вимкнений через неполадки. Якщо індикатор горить жовтим, то PoE дл я порту був відключений.

Підготовка до базового управління комутатором

Щоб налаштувати на комутаторі можливість для віддаленого управління, на комутаторі потрібно налаштувати IP-адресу і маску підмережі. Пам'ятайте, що для управління комутатором з віддаленої мережі для нього необхідно налаштувати шлюз. Подібна настройка мало чим відрізняється від настройки інформації про IP-адреси на фізичних вузлах. На рисунку 2.4 IP-адресу слід призначити інтерфейсу SVI комутатора S1. SVI - це віртуальний інтерфейс, а не фізичний порт комутатора.

Рис. 3.3.16

Поняття SVI відноситься до мереж VLAN. Мережі VLAN - це пронумеровані логічні групи, яким можна привласнити фізичні порти. Конфігурації і настройки, які застосовані до VLAN, також застосовуються до всіх портів, призначених для цієї VLAN.

За замовчуванням комутатор налаштований для управління через VLAN 1. За замовчуванням всі порти асоціюються з VLAN 1. З метою безпеки не рекомендується використовувати мережу VLAN 1 як мережу управління VLAN.

Зверніть увагу, що ці параметри IP застосовуються тільки для доступу до віддаленого управління комутатором; параметри IP не дозволяють комутатору маршрутизовувати пакети на 3-му рівні.

Налаштування доступу для базового управління комутатором з IPv4

Крок 1. Налаштування інтерфейсу управління

IPv4-адрес і маска підмережі налаштовані на SVI управління комутатора з режиму інтерфейсної настройки VLAN. Як показано на рис. 2.5, для входу в режим конфігурації інтерфейсу використовується команда *interface vlan 99*. Для настройки IPv4-адреси використовується команда *ip address*. Команда *no shutdown* активує інтерфейс. В даному прикладі мережа VLAN 99 налаштована з IPv4-адресою 172.17.99.11.

Настройка интерфейса управления коммутатора

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	S1# **configure terminal**
Войдите в режим конфигурации интерфейса для SVI.	S1(config)# **interface vlan 99**
Настройте IP-адрес интерфейса управления.	S1(config-if)# **ip address 172.17.99.11 255.255.255.0**
Включите интерфейс управления.	S1(config-if)# **no shutdown**
Вернитесь в привилегированный режим.	S1(config-if)# **end**
Сохраните текущую конфигурацию в качестве загрузочной конфигурации.	S1# **copy running-config startup-config**

Рис. 3.3.17

Інтерфейс SVI для мережі VLAN 99 не буде відображатися як up / up, поки не буде створена VLAN 99 і не з'явиться пристрій, підключений до порту комутатора, пов'язаного з VLAN 99. Для того щоб створити мережу VLAN з ідентифікатором 99 і прив'язати її до інтерфейсу, використовуйте наступні команди:

S1 (config) # vlan vlan_id
S1 (config-vlan) # Ім'я vlan_name
S1 (config-vlan) # exit
S1 (config) # інтерфейс interface_id
S1 (config-if) # switchport access vlan vlan_id

Крок 2. Налаштування шлюзу

Якщо потрібне віддалене управління комутатором з мереж без прямого підключення, на комутаторі слід налаштувати шлюз. Шлюз за замовчуванням -

це маршрутизатор, до якого підключений комутатор. Комутатор пересилає IP-пакети з IP-адресами призначення за межі локальної мережі на шлюз за замовчуванням. Як показано на рис. 2.6, маршрутизатор R1 є шлюзом за замовчуванням для комутатора S1. Інтерфейс маршрутизатора R1, підключений до комутатора, має IPv4-адрес 172.17.99.1. Зазначена адреса є адресою шлюзу для комутатора S1.

Настройка интерфейса управления коммутатора

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	`S1# configure terminal`
Войдите в режим конфигурации интерфейса для SVI.	`S1(config)# interface vlan 99`
Настройте IP-адрес интерфейса управления.	`S1(config-if)# ip address 172.17.99.11 255.255.255.0`
Включите интерфейс управления.	`S1(config-if)# no shutdown`
Вернитесь в привилегированный режим.	`S1(config-if)# end`
Сохраните текущую конфигурацию в качестве загрузочной конфигурации.	`S1# copy running-config startup-config`

Рис. 3.3.18

Для того щоб налаштувати шлюз для комутатора, використовуйте команду ***ip default-gateway***. Введіть IPv4-адрес шлюзу. Шлюз за замовчуванням - це IPv4-адрес інтерфейсу маршрутизатора, до якого підключений комутатор. Використовуйте команду ***copy running-config startup-config*** для створення резервної копії цієї конфігурації (рис. 2.7).

Настройка шлюза по умолчанию коммутатора

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	`S1# configure terminal`
Настройте шлюз по умолчанию для коммутатора.	`S1(config)# ip default-gateway 172.17.99.1`
Вернитесь в привилегированный режим.	`S1(config)# end`
Сохраните текущую конфигурацию в качестве загрузочной конфигурации.	`S1# copy running-config startup-config`

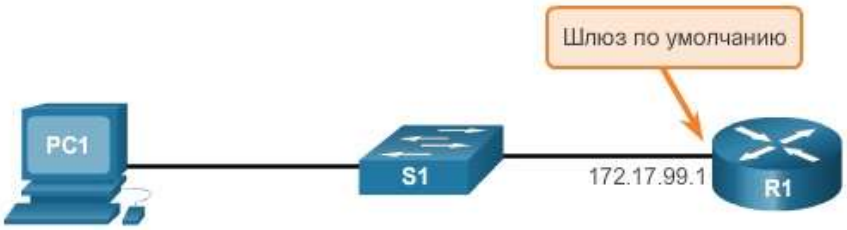


Рис. 3.3.19

Крок 3. Перевірка конфігурації

Як показано на рис. 2.8, команду ***show ip interface brief*** слід використовувати при визначенні стану як фізичних, так і віртуальних інтерфейсів. Наведені вихідні дані підтверджують, що інтерфейс VLAN 99 налаштований з IPv4-адресою і маскою підмережі.

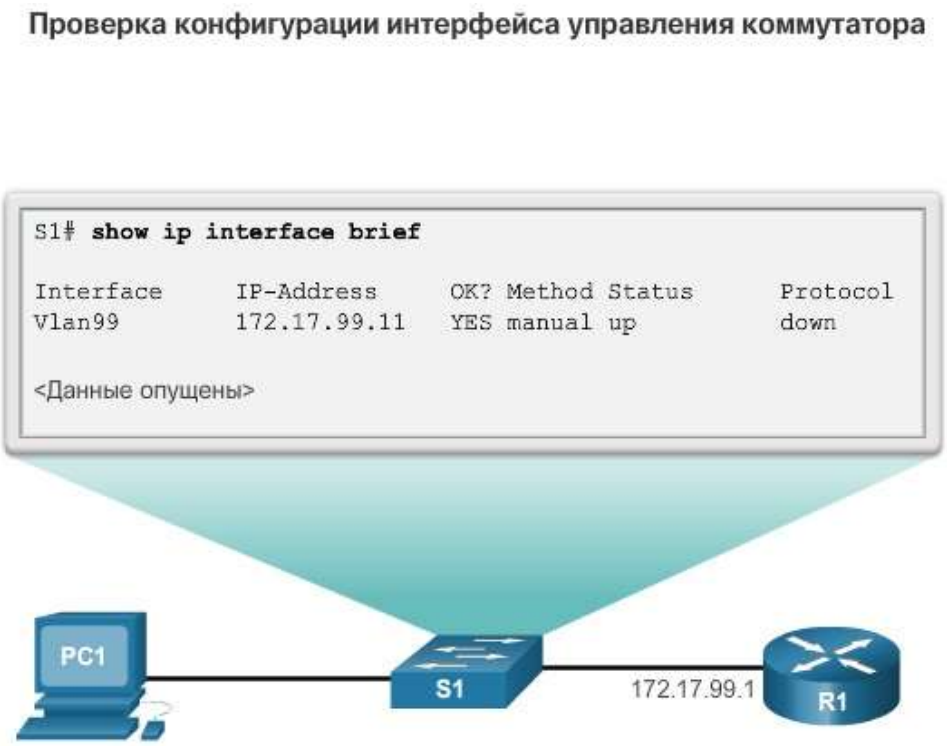


Рис. 3.3.20

Рис. 2.8 Перевірка стану конфігурації комутатора

На рисунку 2.9 зображено повно- і напівдуплексний зв'язок

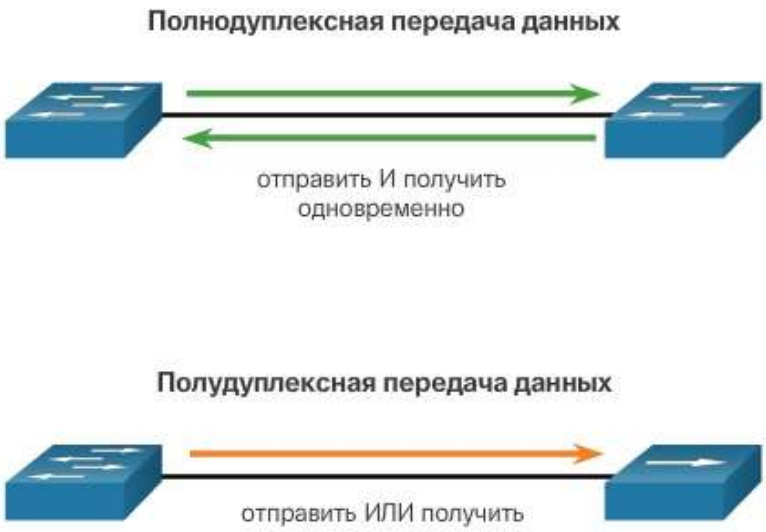


Рис. 3.3.21

Повнодуплексний зв'язок підвищує продуктивність комутованої LAN. Повнодуплексний зв'язок підвищує ефективність смуги пропускання, дозволяючи передавати і отримувати дані одночасно в обох напрямках. Даний вид зв'язку також називають двобічним зв'язком. Використання цього методу оптимізації продуктивності мережі вимагає мікросегментації. Мікросегментування локальні мережі створюється, коли до комутаційного

порту підключено тільки один пристрій, а порт працює в повнодуплексному режимі. Коли комутаційний порт працює в повнодуплексному режимі, то колізійні домени, пов'язані з портом, відсутні.

На відміну від повнодуплексного зв'язку, напівдуплексний зв'язок є односпрямованим, тобто відправка і прийом даних не відбуваються одночасно. Напівдуплексний зв'язок погано позначається на продуктивності, тому що одноразово дані можуть передаватися тільки в одному напрямку, часто викликаючи колізії. Напівдуплексні з'єднання частіше зустрічаються в застарілому обладнанні, наприклад в концентраторах. На даний момент повнодуплексний зв'язок замінив напівдуплексний зв'язок в більшості пристроїв.

Для роботи мережевих адаптерів Gigabit Ethernet і 10Gb потрібно повнодуплексне з'єднання. У повнодуплексному режимі на мережевому адаптері відключено виявлення колізій. Кадри, відправлені двома сполученими пристроями, не можуть зіткнутися, тому що пристрої використовують два окремих канали в мережевому кабелі. Для функціонування повнодуплексних з'єднань потрібен комутатор, що підтримує повнодуплексну конфігурацію, або пряме підключення за допомогою кабелю Ethernet між двома пристроями.

Ефективність конфігурації стандартної загальної мережі Ethernet зазвичай становить 50-60% від зазначеної смуги пропускання. Повнодуплексний зв'язок забезпечує 100% ефективність в обох напрямках (передача і отримання), що підвищує потенційне використання смуги пропускання до 200%.

Двобічний режим і швидкість

Порти комутаторів можна налаштувати вручну з певними параметрами швидкості і дуплексного режиму. Використовуйте команду режиму конфігурації інтерфейсу ***duplex***, щоб вручну встановити двобічний режим для порту комутатора. Використовуйте команду режиму конфігурації інтерфейсу ***speed***, щоб вручну задати швидкість для порту комутатора. На рис. 2.10 порт F0/1 на комутаторах S1 і S2 налаштовується вручну за допомогою ключового слова ***full*** для команди ***duplex*** і ключового слова 100 для команди ***speed***.

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	S1# configure terminal
Войдите в режим конфигурации интерфейса.	S1(config)# interface FastEthernet 0/1
Настройте дуплексный режим интерфейса.	S1(config-if)# duplex full
Настройте скорость интерфейса.	S1(config-if)# speed 100
Вернитесь в привилегированный режим.	S1(config-if)# end
Сохраните текущую конфигурацию в качестве загрузочной конфигурации.	S1# copy running-config startup-config

Рис. 3.3.22

За замовчуванням на комутаторах Cisco Catalyst 2960 і 3560 налаштування дуплексного режиму і швидкості виставлені в режим Auto. Порти 10/100/1000

функціонують в напівдуплексному або в повнодуплексному режимі, якщо встановлена швидкість 10 або 100 Мбіт/с, і тільки в повнодуплексному, якщо задана швидкість 1000 Мбіт/с. Автоузгодження корисно, коли настройки швидкості і дуплексу для пристрою, підключеного до порту, невідомі або можуть змінюватися. При підключенні до відомих пристроїв, таким як сервери, виділені робочі станції або мережеві пристрої, рекомендується вручну задавати параметри швидкості і дуплексу.

При пошуку і усунення проблем з портом комутатора необхідно перевірити настройки двостороння і швидкості.

Примітка. Розбіжності в налаштуваннях дуплексного режиму і швидкості портів комутаторів можуть викликати проблеми з підключенням. Помилка при автоузгодження призводить до неспівпадання в налаштуваннях.

Всі порти оптоволоконних кабелів, наприклад порти 1000BASE-SX, працюють тільки на попередньо встановленою швидкості і завжди в повнодуплексному режимі.

Використовуйте інструмент перевірки синтаксису на рис. 2.11 , щоб налаштувати порт F0 / 1 комутатора S1.

Функція Auto-MDIX

До недавнього часу при з'єднанні пристроїв були потрібні певні типи кабелів (прямі або кросові). Для з'єднання двох комутаторів або комутатора і маршрутизатора були потрібні різні кабелі стандарту Ethernet. Використання функції автоматичного визначення кабелю (auto-MDIX) вирішило цю проблему. Навіть коли auto-MDIX інтерфейс розпізнає необхідний тип кабельного з'єднання (пряме або кроссовое) і налаштовує підключення відповідним чином. При підключенні до комутаторів без функції auto-MDIX необхідно використовувати прямі кабелі для з'єднання з пристроями, такими як сервери, робочі станції або маршрутизатори. Перехресні кабелі повинні використовуватися для підключення до інших комутаторів або ретрансляторів.

Включена функція auto-MDIX дозволяє використовувати будь-який тип кабелю для підключення до інших пристроїв, а інтерфейс автоматично налаштовується для успішної взаємодії. На нових комутаторах Cisco цю функцію включає команда режиму інтерфейсної настройки ***mdix auto***. При використанні функції auto-MDIX на інтерфейсі швидкість інтерфейсу і двобічний режим повинні бути налаштовані в режим auto, щоб функція працювала належним чином.

Команди для включення функції auto-MDIX показані на рис. 2.12.

Настройка функции авто-MDIX

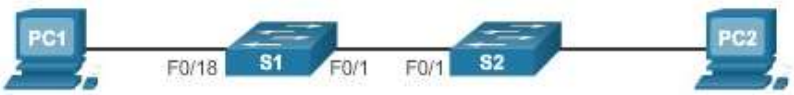
Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	S1# configure terminal
Войдите в режим конфигурации интерфейса.	S1(config)# interface fastethernet 0/1
Настройте интерфейс на автосогласование дуплексного режима с подключенным устройством.	S1(config-if)# duplex auto
Настройте интерфейс для согласования скорости с подключенным устройством.	S1(config-if)# speed auto
Включите функцию авто-MDIX на интерфейсе.	S1(config-if)# mdix auto
Вернитесь в привилегированный режим.	S1(config-if)# end
Сохраните текущую конфигурацию в качестве загрузочной конфигурации.	S1# copy running-config startup-config

Рис. 3.3.23

Примітка. Функція auto-MDIX за замовчуванням включена на комутаторах Catalyst 2960 і Catalyst 3560, але недоступна на комутаторах колишніх версій Catalyst 2950 і Catalyst 3550.

Щоб переглянути настройки функції auto-MDIX для конкретного інтерфейсу, слід використовувати команду ***show controllers ethernet-controller*** з ключовим словом ***phy***. Для відображення вихідних даних, що мають відношення до функції auto-MDIX, використовуйте фільтр ***include Auto-MDIX***. Як показано на рис. 2.13, вихідні дані вказують стан функції: вмикання/вимикання (On або Off).

Проверка функции авто-MDIX




```
S1# show controllers ethernet-controller fa 0/1 phy | include
Auto-MDIX
 Auto-MDIX      :  On    [AdminState=1    Flags=0x00056248]
S1#
```

Рис. 3.3.24

Використовуйте інструмент для перевірки синтаксису на рис. 2.14, щоб налаштувати інтерфейс FastEthernet 0/1 на комутаторі S2 для коректного функціонування auto-MDIX.

Перевірка налаштувань порту комутатора

На рис. 2.15 представлені деякі з параметрів команди ***show***, які будуть корисні при перевірці основних параметрів функцій комутатора.

Команды проверки

Команды коммутатора Cisco под управлением ОС IOS	
Отобразите состояние и конфигурацию интерфейса.	S1# **show interfaces** *[interface-id]*
Отобразите текущую загрузочную конфигурацию.	S1# **show startup-config**
Отобразите текущую функционирующую конфигурацию.	S1# **show running-config**
Отобразите данные о файловой системе флеш-памяти.	S1# **show flash**
Отобразите состояние системного оборудования и программного обеспечения.	S1# **show version**
Отобразите историю введенных команд.	S1# **show history**
Отобразите данные IP для интерфейса.	S1# **show ip** *[interface-id]*
Отобразите таблицу MAC-адресов.	S1# **show mac-address-table** OR S1# **show mac address-table**

Рис. 3.3.25

На рис. показаний приклад скорочених вихідних даних команди **show running-config**.

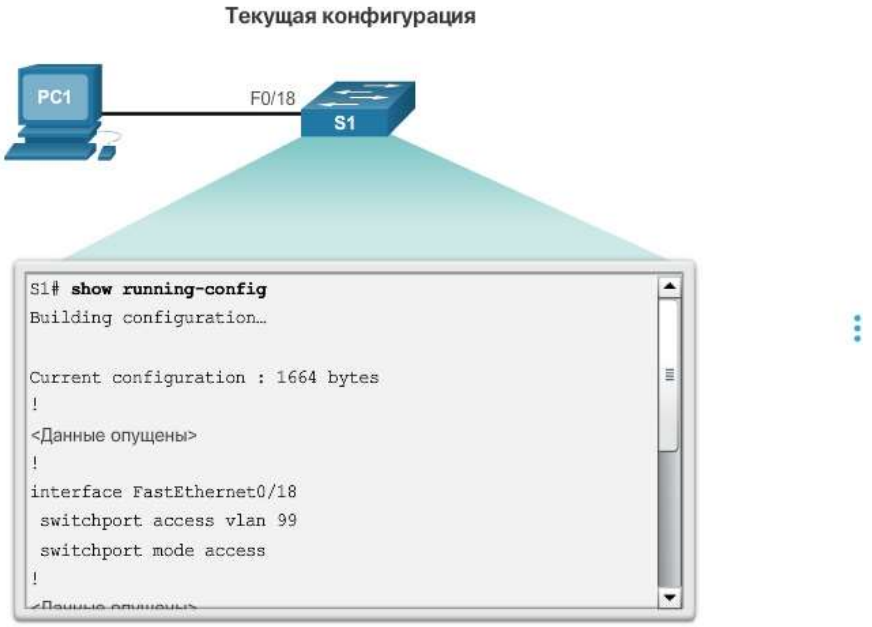


Рис. 3.3.26

Використовуйте цю команду, щоб перевірити, чи правильно налаштований комутатор. В даних виведення для комутатора S1 висвітлено певну важливу інформацію:

- Інтерфейс Fast Ethernet 0/18 налаштований з мережею управління VLAN 99.
- VLAN 99 призначений IPv4-адрес 172.17.99.11 з маскою підмережі 255.255.255.0.
- Шлюз за замовчуванням - 172.17.99.1.

Команда ***show interfaces*** є ще однією поширеною командою, яка виводить дані про стан і статистику мережевих інтерфейсів комутатора. Команда ***show interfaces*** часто використовується при налаштуванні і моніторингу мережевих пристроїв.

На рис. 2.17 показані вихідні дані команди ***show interfaces fastEthernet 0/18***. Перший рядок на малюнку вказує, що інтерфейс FastEthernet 0/18 знаходиться в стані up/up, тобто робочому стані. Наступні дані виведення показують, що включений повнодуплексний режим і встановлена швидкість 100 Мбіт/с.

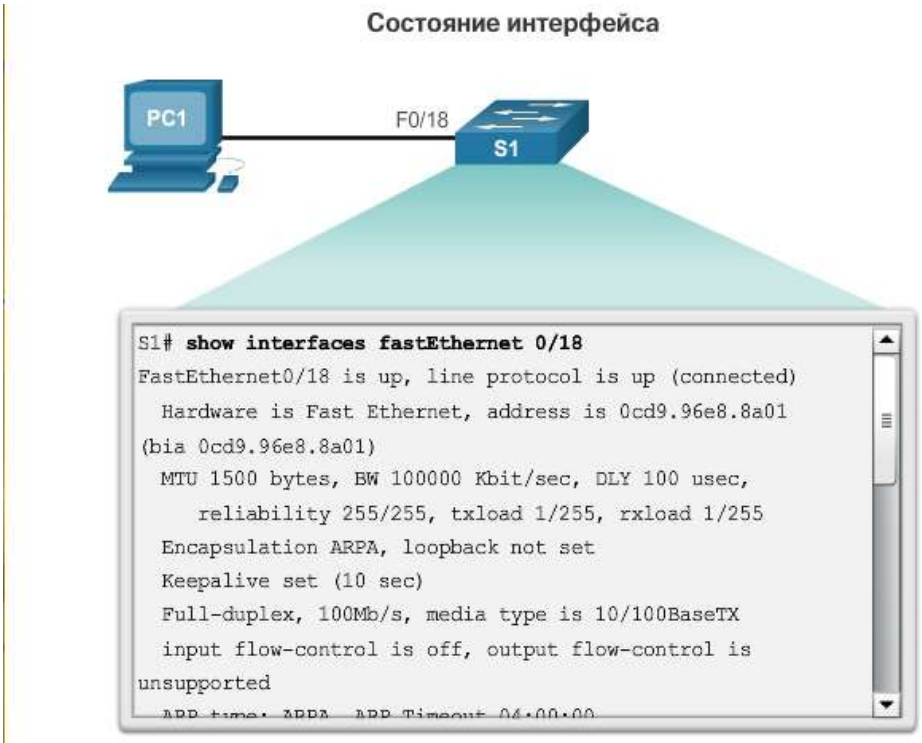


Рис. 3.3.27

Результат команди ***show interface*** можна використовувати для виявлення типових проблем середовища передачі даних. Найважливіші складові цих вихідних даних відображають стан протоколу рівня лінії і протоколу канального рівня. На рис. 2.18 показано підсумковий рядок для перевірки стану інтерфейсу.

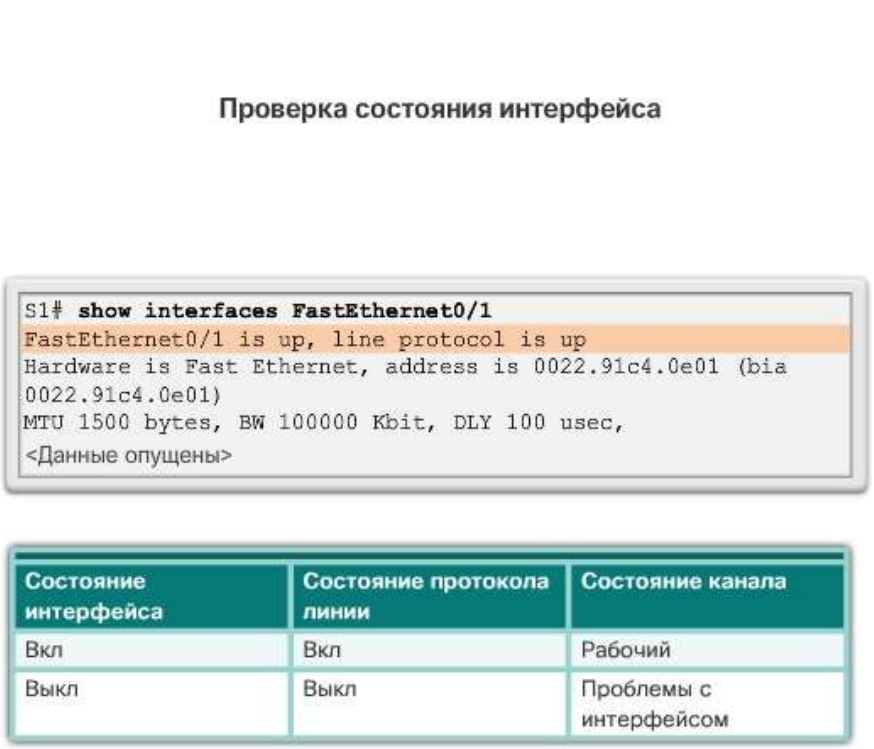


Рис. 3.3.28

Перший параметр (FastEthernet0 / 1 is up) відноситься до апаратного рівня. Він вказує, чи отримує інтерфейс сигнал виявлення несучої. Другий параметр (line protocol is up) відноситься до рівня лінії. Він вказує, чи приймаються повідомлення *keepalive* протоколу рівня лінії.

Використовуючи результат команди show interfaces, можна усунути можливі проблеми наступним чином:

- Якщо інтерфейс включений, а протокол лінії не функціонує, виникає проблема. Можливо невідповідність в типі інкапсуляції, інтерфейс на іншому кінці міг бути вимкнений в результаті збою або могли виникнути проблеми з апаратним забезпеченням.
- У разі якщо протокол рівня лінії (Line protocol) і інтерфейс відключені, можливо, не підключений кабель або існують інші проблеми з інтерфейсом. Наприклад, у зустрічно-паралельному включенні міг бути адміністративно відключений інший кінець підключення.
- Якщо інтерфейс відключений адміністратором, він був відключений вручну (за допомогою команди ***shutdown***) в активній конфігурації.

На рис. 2.19 показаний приклад результатів команди ***show interfaces***. У прикладі показані лічильники і статистика інтерфейсу FastEthernet 0/1.

Отображение состояния и статистики интерфейса

```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is upHardware is Fast
Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)MTU
1500 bytes, BW 100000 Kbit, DLY 100 usec,
<Данные опущены>
  2295197 packets input, 305539992 bytes, 0 no buffer
  Received 1925500 broadcasts, 0 runts, 0 giants, 0
  throttles
  3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 68 multicast, 0 pause input
  0 input packets with dribble condition detected
  3594664 packets output, 436549843 bytes, 0 underruns
  8 output errors, 1790 collisions, 10 interface resets
  0 unknown protocol drops
  0 babbles, 235 late collision, 0 deferred
<Данные опущены>
```

Рис. 3.3.29

У деяких випадках помилки середовища передачі даних не виявляються в достатній мірі, щоб привести до виходу з ладу з'єднання, але погіршують продуктивність мережі. На рис. 2.20 пояснюються деякі з цих поширених помилок, які можна виявити за допомогою команди ***show interfaces***.

«Помилки введення» - це сума всіх помилок в датаграмах, які були отримані при аналізі інтерфейсу. Вони включають в себе карликові (runts) і гігантські (giants) кадри, помилки CRC, відсутність буфера, кадр, переповнення і проігноровані пакети. До помилок введення, які можна виявити за допомогою команди show interfaces, відносяться наступні:

•Карликові кадри (runt frames) - кадри Ethernet, розмір яких не перевищує мінімально дозволені 64 байта. Зазвичай причиною великого числа карликових кадрів є несправні мережеві інтерфейсні плати, але вони також можуть бути викликані колізіями.

•Гігантські кадри (giants) - кадри Ethernet, розмір яких перевищує максимально допустимий.

•Помилки CRC - в Ethernet і послідовних інтерфейсах. Помилки CRC зазвичай свідчать про неполадки в середовищі передачі або кабелі. Частими причинами помилок є електричні перешкоди, погано закріплені або пошкоджені роз'єми, а також невірно вибраний тип кабелю. Велика кількість помилок CRC призводить до шуму на каналі, тому слід перевірити кабель. Також слід знайти і усунути джерела електромагнітного шуму.

•«Помилки виведення» - це сума всіх помилок, які перешкоджали остаточної передачі датаграм з перевіряється інтерфейсу. До помилок виведення, які можна виявити за допомогою команди show interfaces, відносяться наступні:

•Колізії є звичайним явищем при роботі в напівдуплексному режимі. Однак вони ніколи не повинні виникати на інтерфейсі, налаштованому для повнодуплексного режиму зв'язку.

•Пізні колізії - це колізії, які відбуваються після передачі 512 біт кадру. Найбільш поширена причина пізніх колізій - перевищення допустимої довжини кабелю. Неправильне налаштування двостороннього зв’язку також може викликати пізні колізії, наприклад, в разі, коли один кінець з'єднання налаштований на повнодуплексний режим, а інший кінець - на напівдуплексний режим. Ви виявите пізні колізії на інтерфейсі, налаштованому на напівдуплексний режим. Для вирішення даної проблеми необхідно налаштувати один і той же двобічний режим на обох кінцях з'єднання. У правильно спроектованій і налаштованої мережі пізні колізії виникати не повинні.

Більшість проблем комутованої мережі виникає при першому впровадженні. Теоретично після установки мережа повинна працювати без проблем. Однак з часом пошкоджуються кабелі, змінюється конфігурація, до комутатора підключають нові пристрої, які вимагають зміни його конфігурації. Саме тому потрібне постійне технічне обслуговування мережевої інфраструктури, що включає в себе регулярний пошук і усунення виникаючих неполадок.

Для пошуку та усунення неполадок при відсутності або поганій якості з'єднання комутатора з іншим пристроєм дотримуйтесь даного алгоритму дій:

1. Використовуйте для перевірки стану інтерфейсу команду show interfaces.
2. У разі якщо інтерфейс не працює:

•переконайтеся, що використовуються відповідні кабелі; перевірте кабелі та роз'єми на предмет пошкоджень; якщо використовується неправильний або пошкоджений кабель, замініть його.

•якщо інтерфейс все ще не працює, то проблема може полягати в розбіжності налаштувань швидкості. Швидкість інтерфейсів зазвичай узгоджується автоматично. Розбіжність в швидкості, що виникає через неправильну настройки або проблем з апаратним або програмним забезпеченням, може створити проблеми в роботі інтерфейсу. Якщо ви вважаєте, що причина саме в цьому, то вручну налаштуйте однакову швидкість на обох кінцях з'єднання.

3. У разі якщо інтерфейс працює, але залишилися проблеми зі з'єднанням:

•за допомогою команди **show interfaces** перевірте ознаки наявності надмірного шуму. Ознаками є збільшення лічильників карликових і гігантських кадрів, помилок CRC. При наявності надмірного шуму насамперед знайдіть і усуньте джерело цього шуму. Також переконайтеся, що довжина кабелю не перевищує максимально дозволену довжину, і перевірте тип використовуваного кабелю.

•якщо проблем з шумом немає, перевірте мережу на наявність колізій. При виявленні колізій або пізніх колізій перевірте налаштування дуплексного режиму на обох кінцях з'єднання. Як і настройки швидкості, дуплексні настройки зазвичай узгоджуються автоматично. Якщо ви припускаєте невідповідність дуплексних режимів, вручну налаштуйте повнодуплексний режим на обох кінцях з'єднання.

Протокол Secure shell (SSH) - це протокол, який забезпечує безпечне (зашифроване) з'єднання для управління віддаленим пристроєм. Для безпечного управління під час віддалених з'єднань Cisco рекомендує замінити протокол Telnet протоколом SSH. Telnet є більш раннім протоколом, що використовує небезпечну незашифровану передачу як даних, так і ідентифікаційної інформації (ім'я користувача і пароль) між пристроями. SSH забезпечує захист віддалених з'єднань, надаючи надійне шифрування даних аутентифікації пристрої (ім'я користувача і пароль), а також даних, що передаються між пристроями. SSH використовує TCP-порт 22. Telnet використовує TCP-порт 23.

На рис. 2.22 зловмисник має можливість переглядати пакети за допомогою програми Wireshark. На потоці Telnet можуть бути захоплені ім'я користувача і пароль.

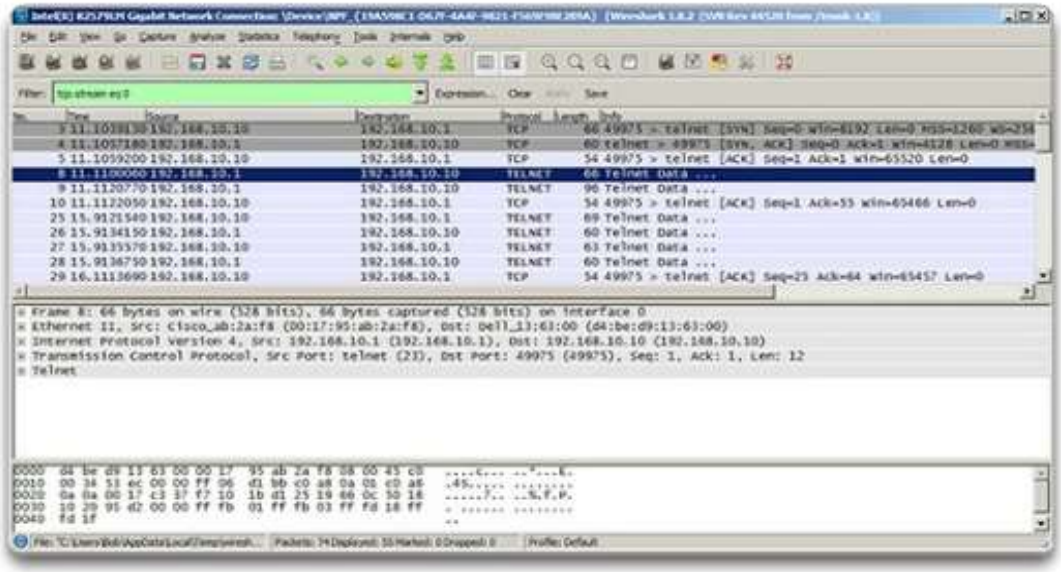


Рис. 3.3.30

На рис. зловмисник може захопити ім'я і пароль адміністратора з незашифрованого сеансу Telnet.

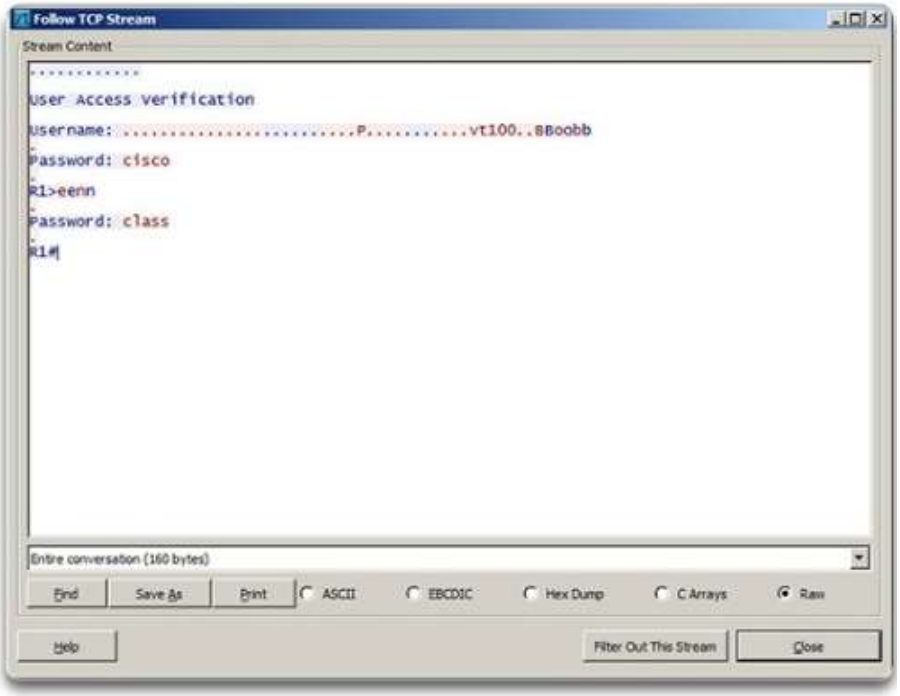


Рис. 3.3.31

На рис. показаний перегляд сеансу SSH програмою Wireshark. Зловмисник може відстежувати сеанс за допомогою IP-адреси пристрою адміністратора.

Захват SSH в программе Wireshark

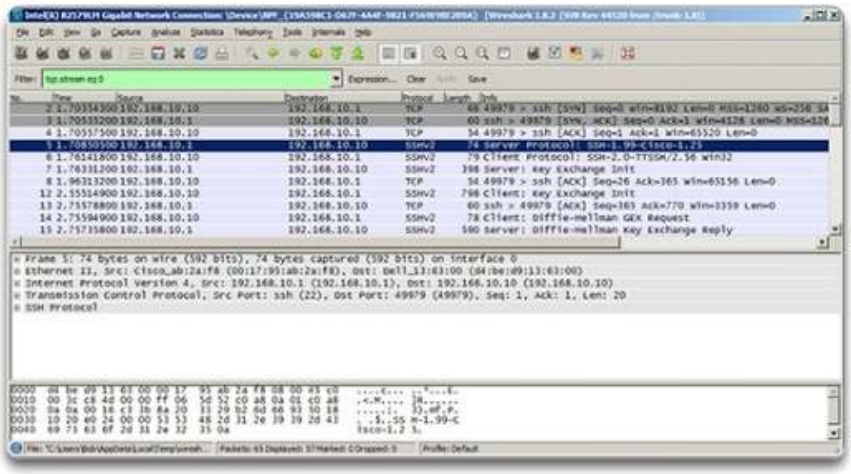


Рис. 3.3.32

Однак, як видно на рис. 2.25, ім'я користувача і пароль зашифровані.

Зашифрованные имя пользователя и пароль

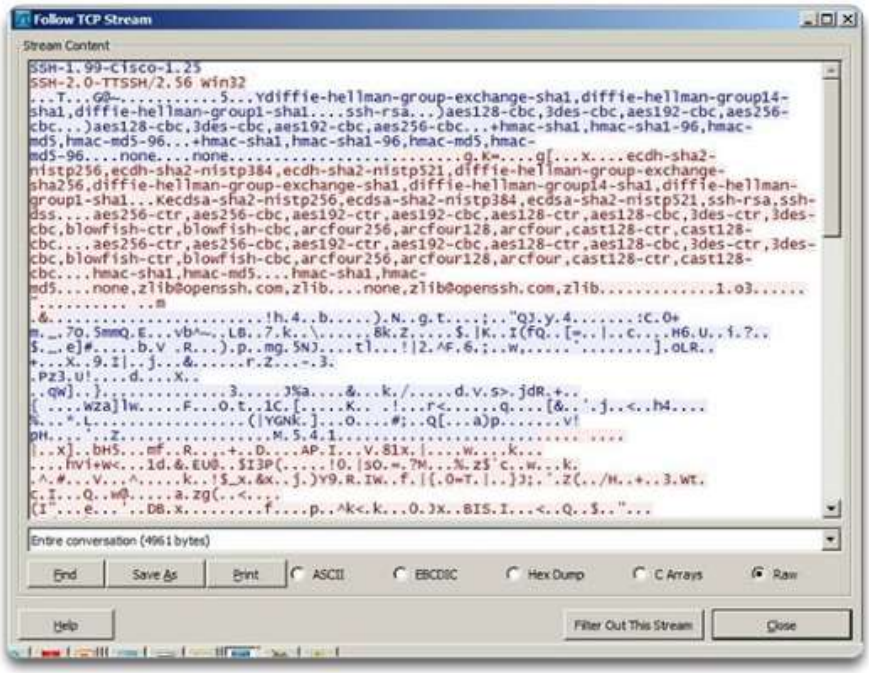


Рис. 3.3.33

Для функціонування протоколу SSH на комутаторі Catalyst 2960 комутатор повинен використовувати версію ПО IOS з криптографічними функціями і можливостями (шифруванням). Використовуйте команду ***show version*** на комутаторі, щоб дізнатися, на якій версії IOS працює в даний момент комутатор (див. Рис. 2.26). Якщо ім'я файлу IOS включає в себе поєднання k9, то дана версія IOS підтримує криптографічні функції і можливості (шифрування).

```
S1> show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M),
Version 15.0(2)SE, RELEASE SOFTWARE (fc1)

<Данные опущены>
```

Рис. 3.3.34

Перед налаштуванням протоколу SSH на комутаторі потрібно налаштувати унікальне ім'я вузла і відповідні параметри мережевого підключення.

Крок 1. Перевірка підтримки протоколу SSH.

Щоб перевірити, чи підтримується протокол SSH, використовуйте команду show ip ssh. Якщо на комутаторі працює IOS, що не підтримує криптографічні функції, дану команду не буде розпізнано.

Крок 2. Налаштування домену IP.

Налаштуйте ім'я домену IP для мережі за допомогою команди режиму глобальної настройки **ip domain-name domain-name**. На рис. 2.27 значення доменного імені - cisco.com.

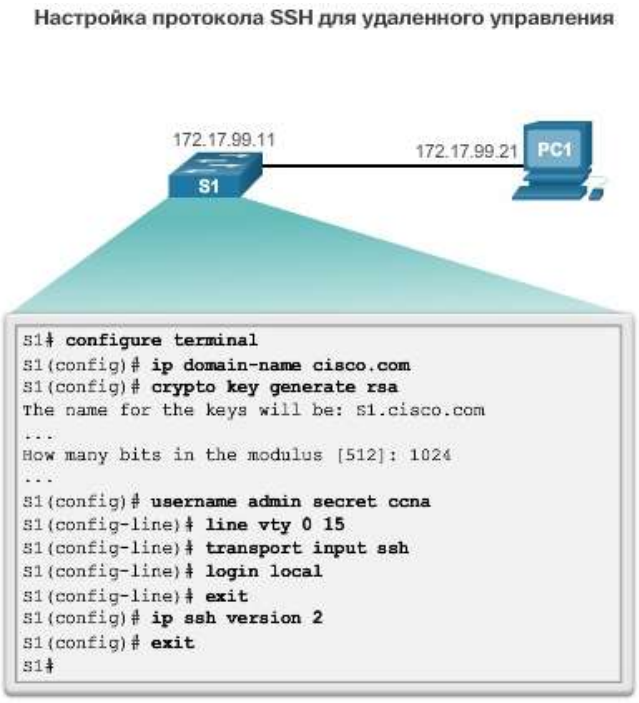


Рис. 3.3.35

Крок 3. Створення пар ключів RSA.

Не у всіх версіях IOS за замовчуванням використовується версія 2 протоколу SSH, а версія 1 SSH містить ряд відомих вразливостей. Для настройки SSH версії 2 виконайте команду режиму глобальної конфігурації ***ip ssh version 2***. Створення пари ключів RSA автоматично включає протокол SSH. Використовуйте команду режиму глобальної конфігурації ***crypto key generate rsa***, щоб включити сервер SSH на комутаторі і згенерувати пару ключів RSA. При створенні ключів RSA адміністратору потрібно ввести довжину модуля. У прикладі конфігурації на рис. 2.28 використовується розмір модуля 1024 біта. Довший модуль безпечніше, але його створення і використання вимагає більше часу.

Примітка. Для видалення пари ключів RSA використовуйте команду режиму глобальної конфігурації ***crypto key zeroize rsa***. Після видалення пари ключів RSA SSH-сервер автоматично відключається.

Крок 4. Налаштування аутентифікації користувача.

SSH-сервер може аутентифікувати користувачів локально або за допомогою сервера аутентифікації. Для використання методу локальної аутентифікації створіть ім'я користувача і пароль за допомогою команди режиму глобальної настройки **username** ім'я користувача **secret** пароль. У цьому прикладі для користувача admin призначений пароль ccna.

Крок 5. Налаштування ліній **vty**.

Увімкніть протокол SSH на лініях **vty** за допомогою команди режиму конфігурації лінії **transport input ssh**. Діапазон ліній vty комутатора Catalyst 2960 становить від 0 до 15. Дана конфігурація запобігає підключення по протоколам крім SSH (наприклад Telnet) і дозволяє комутатору приймати підключення тільки по протоколу SSH. Використовуйте команду режиму глобальної конфігурації ***line vty***, а потім команду режиму конфігурації лінії ***login local***, щоб при підключеннях SSH була потрібна локальна аутентифікація з локальної бази даних імен.

Крок 6. Увімкніть SSH версії 2.

За замовчуванням SSH підтримує обидві версії (1 і 2). Якщо підтримуються обидві версії, результат команди ***show ip ssh*** повідомляє про підтримку версії 1.99. У версії 1 є ряд відомих вразливостей. З цієї причини рекомендується включати тільки версію 2. Увімкніть цю версію SSH, використовуючи команду режиму глобальної конфігурації ***ip ssh version 2.***

Для настройки протоколу SSH на комутаторі S1 використовуйте інструмент перевірки синтаксису.

Перевірка SSH

Щоб з'єднатися з сервером SSH на ПК використовується SSH-клієнт, наприклад PuTTY. Для прикладів на рисунках 2.29, 2.30 і 2.31 були налаштовані наступні параметри:

- Протокол SSH включений на комутаторі S1.
- На комутаторі S1 інтерфейсу VLAN 99 (SVI) присвоєно IPv4-адрес 172.17.99.11.
- Комп'ютера PC1 присвоєно IPv4-адрес 172.17.99.21.

На рис. 2.29 ПК ініціює SSH-підключення по IPv4-адресою VLAN SVI комутатору S1.

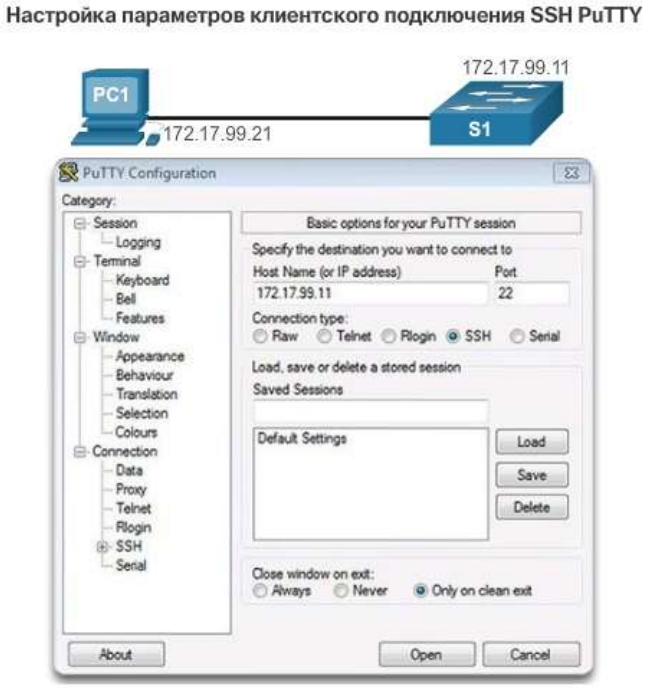


Рис. 3.3.36

На рис. 2.30 користувач отримав запит на введення імені користувача і пароля. При використанні конфігурації з попереднього прикладу введені ім'я користувача admin та пароль ccna. Після введення правильної комбінації користувач підключається до інтерфейсу командного рядка комутатора Catalyst 2960 через протокол SSH.

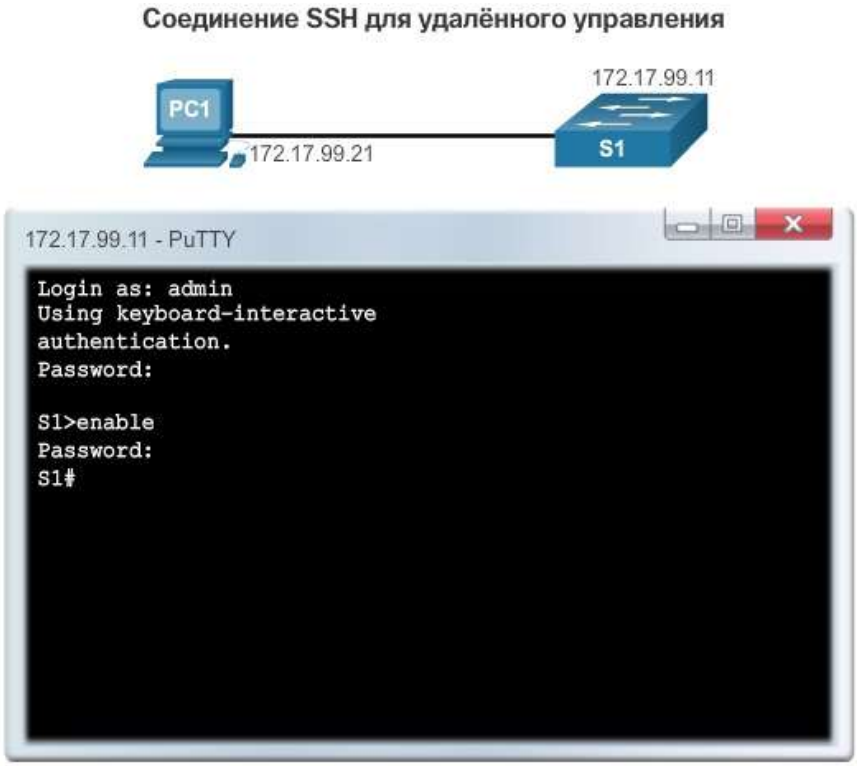


Рис. 3.3.37

Для відображення використовуваної версії і конфігурації для протоколу SSH на пристрої, який ви налаштували в якості сервера SSH, використовуйте команду ***show ip ssh***. У цьому прикладі використовується протокол SSH версії 2. Для перевірки SSH-підключень до пристрою використовуйте команду ***show ssh*** (див. рис.2.31).

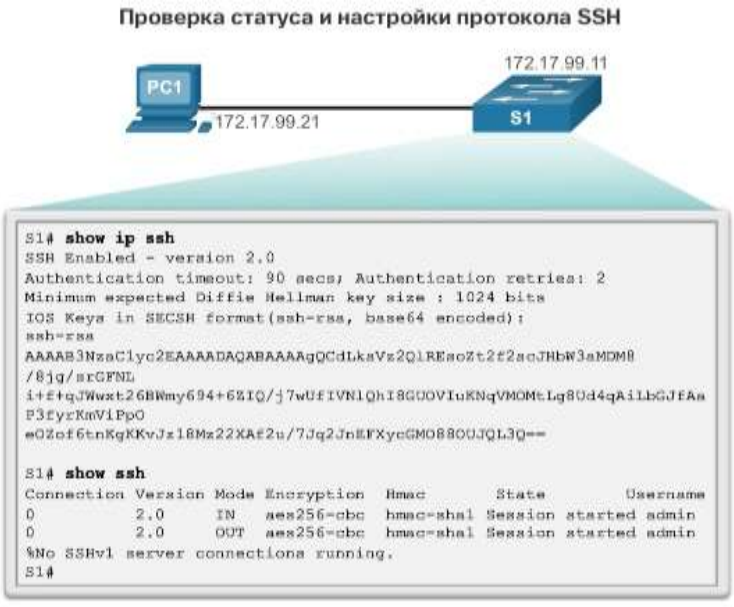


Рис. 3.3.38

Відключення невикористовуваних портів - це простий спосіб захисту мережі від несанкціонованого доступу, який використовується багатьма адміністраторами. Наприклад, якщо комутатор Catalyst 2960 має 24 порти і при цьому використовуються три підключення Fast Ethernet, рекомендується відключити 21 невикористаний порт. Перейдіть до кожного невикористовуваних порту і введіть команду Cisco IOS ***shutdown***. Якщо пізніше

порт потрібно активувати повторно, це можна зробити за допомогою команди ***no shutdown***. На рис. 2.32 відображені часткові вихідні дані для цієї конфігурації.

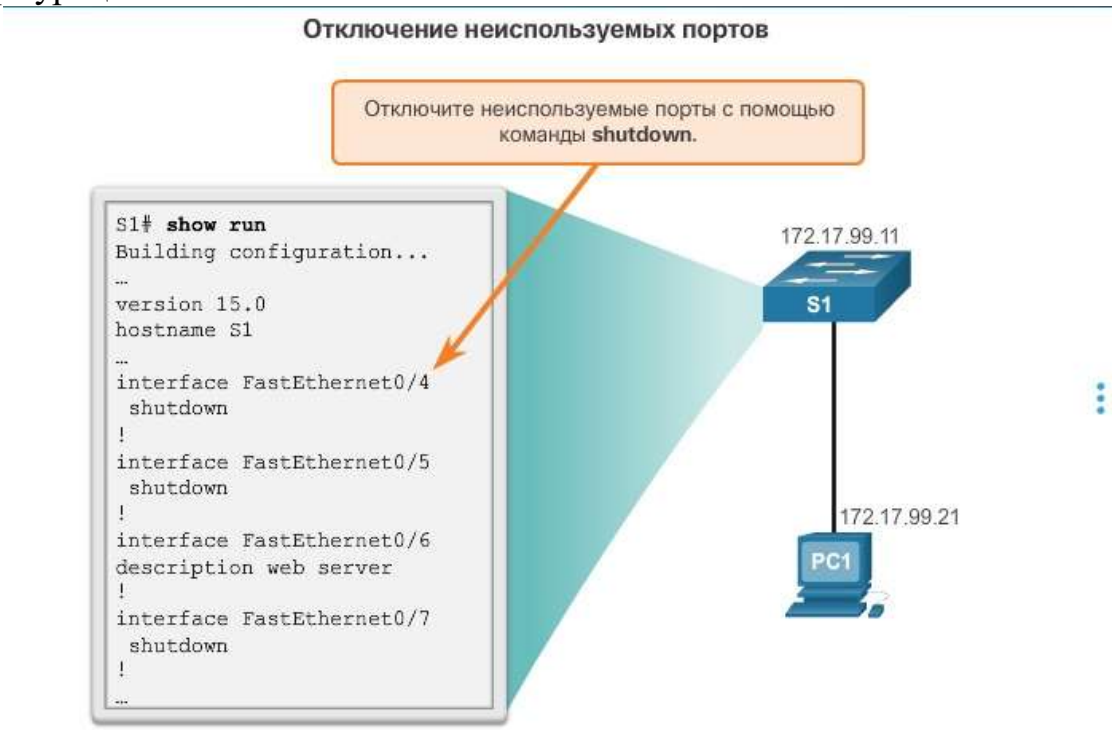


Рис. 3.3.39

Зміна конфігурації на декількох портах комутатора одночасно не представляє складності. Для того щоб налаштувати діапазон портів, використовуйте команду ***interface range.*** Switch (config) # interface range введіть модуль / перший номер - останній номер. Процес включення і виключення портів може зайняти багато часу, але він підвищує безпеку мережі і коштує витрачених зусиль.

Захист портів

Перед введенням комутатора в експлуатацію необхідно забезпечити безпеку всіх портів (інтерфейсів) комутатора. Один із способів захисту портів - використання функції безпеки портів (функція Port Security). Ця функція обмежує кількість допустимих MAC-адрес на один порт, а також надати їм доступ для MAC-адрес санкціонованих пристроїв і забороняє доступ для інших MAC-адрес.

Для того щоб дозволити доступ одному або кільком MAC-адресами, необхідно налаштувати функцію безпеки портів. У разі якщо кількість дозволених MAC-адрес на порте обмежена до одного, до цього порту може підключитися тільки пристрій з цим конкретним MAC-адресою.

Якщо порт налаштований як захищений і досягнуто максимальну кількість MAC-адрес, будь-які додаткові спроби підключення з невідомих адрес призведуть до порушення безпеки. На рис. 2.33 підведені підсумки вищевикладених відомостей.

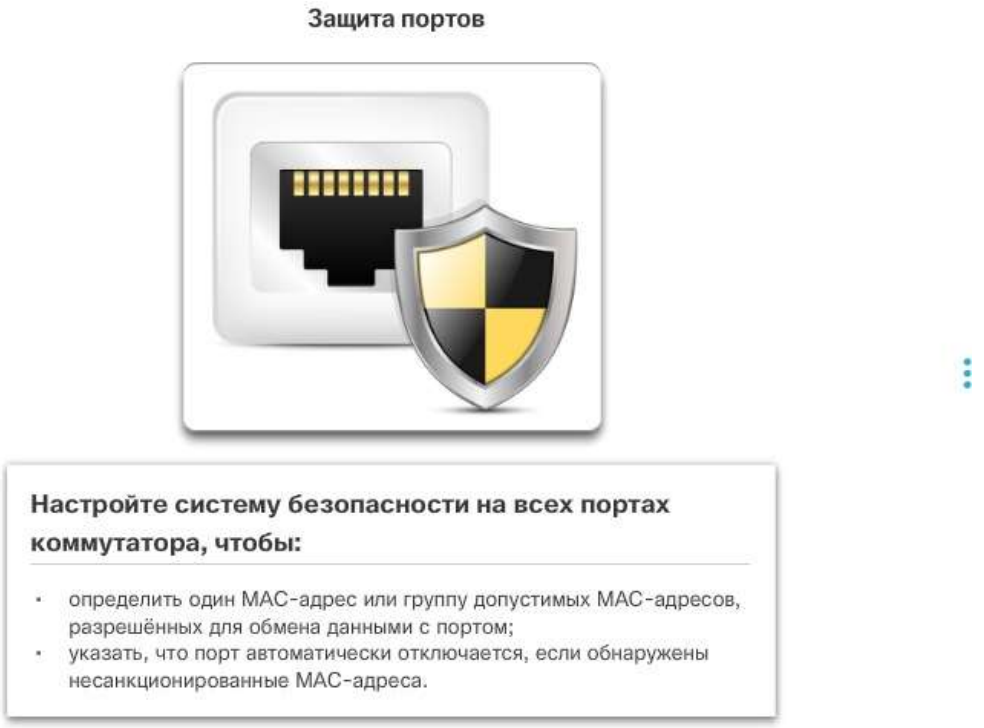


Рис. 3.3.40

Види захисту MAC-адрес

Існує безліч способів налаштувати функцію безпеки порту. Залежно від конфігурації розрізняють наступні типи захищених адрес:

- **Статичний захист MAC-адреси** - MAC-адреси, які налаштовані на порті вручну за допомогою команди режиму інтерфейсної настройки ***switchport port-security mac-address mac-address***. MAC-адреси, налаштовані таким чином, зберігаються в таблиці адрес і додаються в поточну конфігурацію комутатора.
- **Динамічний захист MAC-адреси** - MAC-адреси, які отримані динамічно і зберігаються в таблиці адрес. MAC-адреси, налаштовані таким чином, видаляються при перезавантаженні комутатора.
- **Захист MAC-адреси на основі прив'язки** - MAC-адреси, які можуть бути отримані динамічно або налаштовані вручну. Вони зберігаються в таблиці адрес і додаються в поточну конфігурацію.

Захист MAC-адреси на основі прив'язки

Для того щоб налаштувати інтерфейс для перетворення динамічно отриманих MAC-адрес в прикріплені захищені MAC-адреси і додати їх у поточну конфігурацію, необхідно включити функцію **sticky learning** (розпізнавання прикріплених адрес). Функція **sticky learning** включається на інтерфейсі за допомогою команди режиму конфігурації інтерфейсу **switchport port-security mac-address sticky**.

Після введення цієї команди комутатор перетворює всі динамічно отримані MAC-адреси, в тому числі отримані до включення цієї функції, в прикріплені безпечні MAC-адреси. Всі прикріплені захищені MAC-адреси додаються в таблицю адрес в поточну конфігурацію.

Також прикріплені захищені MAC-адреси можна задати вручну. Коли прикріплені безпечні MAC-адреси налаштовуються за допомогою команди режиму інтерфейсної настройки **switchport port-security mac-address sticky**

MAC-адресу, всі зазначені адреси додаються в таблицю адрес і в поточну конфігурацію.

Якщо прикріплені захищені MAC-адреси зберігаються в файлі завантажувального конфігурації, то після перезавантаження комутатора або відключення інтерфейсу не потрібно повторне отримання адрес. Якщо ж прикріплені захищені адреси не зберігаються, вони будуть втрачені.

При відключенні режиму **sticky learning** за допомогою команди режиму конфігурації інтерфейсу **no switchport port-security mac-address sticky** прикріплені захищені MAC-адреси залишаються в таблиці адрес, але видаляються з поточної конфігурації.

Примітка. Функція безпеки портів не працює до тих пір, поки вона не буде включена для інтерфейсу командою switchport port-security.

Інтерфейс можна налаштувати на один з трьох режимів реагування на порушення безпеки, який визначає дії, що вживаються у разі порушення. На рисунку 2.34 представлено, які типи трафіку пересилаються, коли на порту налаштований один з наступних режимів реагування на порушення безпеки.

Захист. Коли кількість захищених MAC-адрес досягає межі дозволених адрес для порту, пакети з невідомими адресами джерела відкидаються, поки не буде видалено достатню кількість захищених MAC-адрес або не буде збільшено максимальну кількість дозволених адрес. Для цього режиму не передбачено повідомлення про порушення безпеки.

Рис. 3.3.41

Обмеження. Коли кількість захищених MAC-адрес досягає межі дозволених адрес для порту, пакети з невідомими адресами джерела відкидаються, поки не буде видалено достатню кількість захищених MAC-адрес або не буде збільшено максимальну кількість дозволених адрес. Для цього режиму передбачено повідомлення про порушення безпеки.

Вимкнення. У цьому режимі (встановленому за замовчуванням) порушення безпеки порту викликає негайне відключення інтерфейсу через помилки і відключає індикатор порту. Для цього режиму передбачено збільшення значення лічильника порушень. Коли захищений порт відключений через помилки, його можна вивести з цього стану за допомогою команди режиму інтерфейсної настройки ***shutdown***, вказавши після неї команду ***no shutdown***.

Щоб змінити реакцію на порушення безпеки на комутаційному порту, використовуйте команду режиму інтерфейсної настройки ***switchport port-security violation*** {protect | restrict | shutdown}.

На рис. 2.35 підсумовано настройки за замовчуванням для функції безпеки порту на комутаторі Cisco Catalyst.

Функция безопасности порта по умолчанию

Функция	Настройка по умолчанию
Функция безопасности портов	Отключена на порте
Максимальное количество защищённых MAC-адресов	1
Режим нарушения безопасности	Shutdown. Порт отключается, когда максимальное количество защищённых MAC-адресов отключено.
Получение прикреплённого адреса	Disabled (Отключено)

Рис. 3.3.42

На рис. 2.36 показані команди інтерфейсу командного рядка Cisco IOS, необхідні для налаштування функції безпеки порту на порту Fast Ethernet F0/18 комутатора S1. Зверніть увагу, що в наведеному прикладі не вказується режим реагування на порушення безпеки. У цьому прикладі режим реагування на порушення безпеки налаштований на вимикання (режим за замовчуванням).

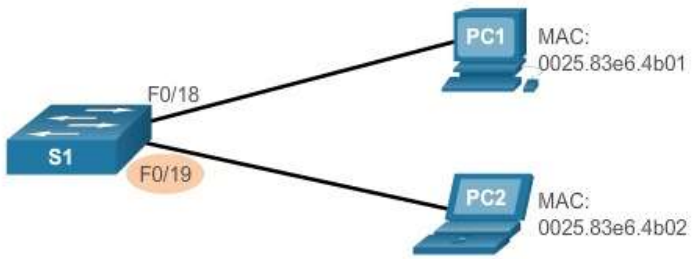
Настройка безопасности динамических портов

Команды интерфейса командной строки CISCO IOS	
Укажите интерфейс, для которого необходимо настроить безопасность порта.	`S1(config)# interface fastethernet 0/18`
Настройте режим интерфейса в режим доступа (access).	`S1(config-if)# switchport mode access`
Включите средства безопасности портов на интерфейсе.	`S1(config-if)# switchport port-security`

Рис. 3.3.43

На рис. показано, як включити закріплені захищені MAC-адреси для функції безпеки порту на порту 0/19 Fast Ethernet комутатора S1. Як зазначено вище, максимальну кількість захищених MAC-адрес можна налаштувати вручну. У цьому прикладі синтаксис команди Cisco IOS використовується для настройки максимальної кількості MAC-адрес для порту 0/19 на значення 10. Режим реагування на порушення безпеки за замовчуванням налаштований на вимикання.

Настройка безопасности портов с привязкой к MAC-адресам



Команды интерфейса командной строки CISCO IOS	
Укажите интерфейс, для которого необходимо настроить безопасность порта.	`S1(config)# interface fastethernet 0/19`
Настройте режим интерфейса в режим доступа (access).	`S1(config-if)# switchport mode access`
Включите средства безопасности портов на интерфейсе.	`S1(config-if)# switchport port-security`
Задайте максимальное количество безопасных адресов, допустимых для доступа к порту.	`S1(config-if)# switchport port-security maximum 10`
Включите получение	`S1(config-if)# switchport port-security mac-address sticky`

Рис. 3.3.44

Перевірка функції безпеки портів

Після настройки функції безпеки портів на комутаторі перевірте кожен інтерфейс, щоб переконатися в правильності настройки цієї функції і статичних MAC-адрес.

Перевірка параметрів безпеки портів

Для відображення параметрів безпеки портів для комутатора або заданого інтерфейсу скористайтеся командою ***show port-security interface*** [ідентіфікатор_інтерфейса]. Вихідні дані для динамічної настройки безпеки портів показані на рис. 2.38. За замовчуванням на цьому порту дозволений тільки один MAC-адрес.

```
S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b01:1
Security Violation Count   : 0
```

Рис. 3.3.45

Вихідні дані, представлені на рис. 2.39, показують значення для параметрів функції безпеки прикріплених портів. Відповідно до конфігурацією максимальну кількість адрес встановлено на значення 10.

Примітка. MAC-адреса визначена в якості прикріпленого MAC-адреса.

```
S1# show port-security interface fastethernet 0/19
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 10
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0025.83e6.4b02:1
Security Violation Count   : 0
```

Рис. 3.3.46

Прикріплені MAC-адреси додаються в таблицю MAC-адрес і в поточну конфігурацію. Як показано на рис. 2.40, прикріплений MAC-адресу для комп'ютера PC2 був доданий в поточну конфігурацію для комутатора S1.

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 10
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

Рис. 3.3.47

Перевірка захищених MAC-адрес

Для відображення всіх безпечних MAC-адрес, налаштованих на всіх інтерфейсах комутатора або на зазначеному інтерфейсі з інформацією старіння для кожного інтерфейсу, використовуйте команду ***show port-security address***. Безпечні MAC-адреси будуть перераховані разом з типами MAC-адрес.

Коли налаштована функція безпеки порту, порушення безпеки може призвести до відключення порту в результаті помилки. У разі якщо порт вимкнений в результаті помилки, він не функціонує і не може відправляти або отримувати трафік. На консолі відображаються серії повідомлень, пов'язаних з функцією безпеки порту (рис. 2.41).

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```

Рис. 3.3.48

Примітка. Протокол порту і стан каналу змінюються на **down**.

Індикатор порту буде вимкнений. Команда ***show interface*** показує стан порту як **«вимкнений в результаті помилки» (err-disabled)** (рис. 2.42). Тепер вихідні дані команди ***show port-security interface*** відображають стан порту як **secure-shutdown**. Оскільки режим реагування на порушення безпеки порту налаштований на вимикання, в разі порушення безпеки порт переходить в вимкнений стан в результаті помилки.

```
S1# show interface fa0/18 status
Port Name  Status        Vlan  Duplex  Speed   Type
Fa0/18     err-disabled  1     auto    auto    10/100BaseTX

S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.292b.4c75:1
Security Violation Count   : 1
```

Рис. 3.3.49

Перед повторним включенням порту адміністратор повинен виявити джерело порушення безпеки. Якщо до захищеного порту підключено несанкціоноване пристрій, порт не можна включати, поки не усунена загроза безпеці. Для повторного включення порту використовуйте команду режиму конфігурації інтерфейсу ***shutdown*** (рис. 2.43). Потім, щоб порт почав функціонувати, використовуйте команду конфігурації інтерфейсу ***no shutdown.***

```
S1(config)# interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to up
```

Рис. 3.3.50

3.4 VLAN мережі та їх налаштування

Продуктивність мережі є важливим фактором ефективності роботи організації. Однією з технологій підвищення продуктивності мережі є поділ великих широкомовних доменів на більш дрібні. Маршрутизатор влаштовані таким чином, що блокують широкомовний трафік на інтерфейсі. При цьому маршрутизатори зазвичай мають обмежену кількість інтерфейсів LAN. Основна роль маршрутизатора полягає не в наданні кінцевим пристроям доступ до мережі, а в передачі інформації між мережами.

Надання доступу в локальну мережу зазвичай забезпечується комутатором рівня доступу. Для зменшення розміру широкомовних доменів на комутаторі 2-го рівня, як і на пристрої 3-го рівня, можна створити мережу VLAN. Мережі VLAN зазвичай включаються в проекти мережі, для того щоб мережа полегшувала процес досягнення цілей організації. Незважаючи на те, що мережі VLAN в основному використовуються в комутованих локальних мережах, сучасні реалізації VLAN здатні функціонувати також в муніципальних (MAN) і глобальних (WAN) мережах.

Процес маршрутизації на 3-му рівні можна здійснювати за допомогою маршрутизатора або комутатора 3-го рівня. Використання пристрою 3-го рівня забезпечує можливість управління передачею трафіку між сегментами мережі, в тому числі сегментами, які були створені за допомогою VLAN (рис. 3.1).

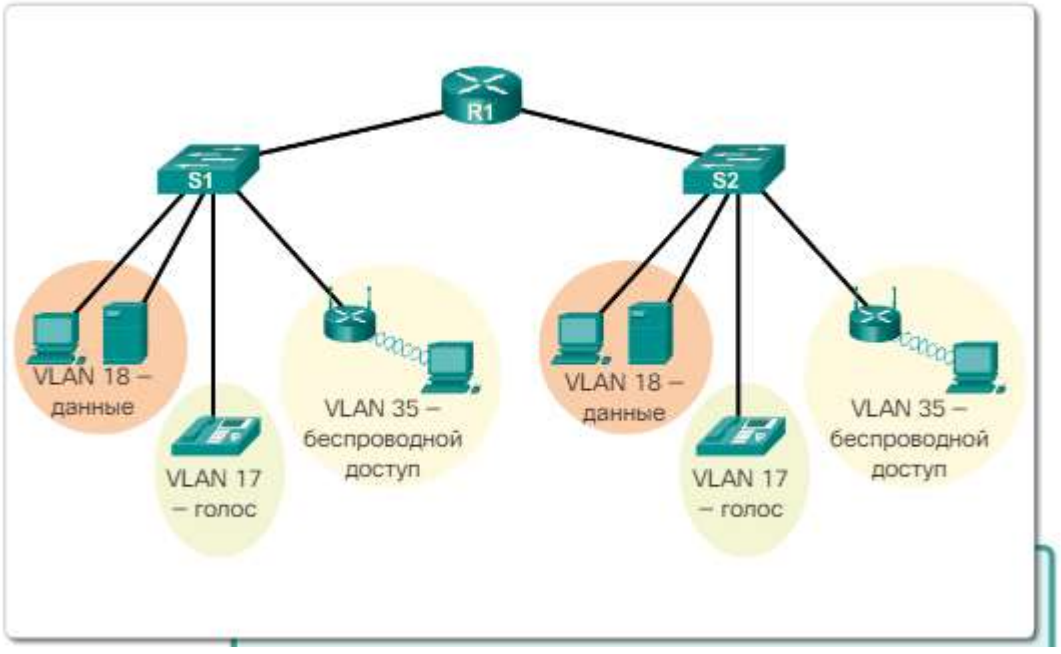


Рис. 3.4.1

У першій частині цієї глави розглядаються процедури налаштування, адміністрування, пошуку та усунення несправностей мереж VLAN і магістральних каналів VLAN. Друга частина даної глави присвячена маршрутизації між мережами VLAN за допомогою маршрутизатора.

У комутованих об'єднаних мережах мережі VLAN забезпечують гнучкість сегментації і організації. Мережі VLAN дозволяють згрупувати пристрої всередині локальної мережі. Група пристроїв в межах VLAN взаємодіє так, ніби пристрої підключені за допомогою одного кабелю. Мережі VLAN ґрунтуються не на фізичних, а на логічних підключених.

Мережі VLAN дозволяють адміністратору виробляти сегментацію за функціями, проектним групами або областями застосування, незалежно від фізичного розміщення користувача або пристрою. Пристрої в межах VLAN працюють таким чином, ніби знаходяться у власній незалежній мережі, навіть якщо ділять одну загальну інфраструктуру з іншими VLAN. Будь-який порт комутатора може належати мережі VLAN. Одноадресні, широкомовні і багатоадресні пакети пересилаються і розсилаються тільки до кінцевих станцій в межах тієї VLAN, яка є джерелом цих пакетів. Кожна VLAN вважається окремою логічною мережею. Пакети, адресовані станціям, які не належать до VLAN, повинні пересилатися через пристрій, що підтримує маршрутизацію.

У комутованої мережі може бути кілька підмереж IP без використання декількох мереж VLAN. Однак пристрої будуть знаходитися в одному і тому ж домені широкомовної розсилки рівня 2. Це означає, що всі широкомовні розсилання рівня 2, наприклад ARP-запити, будуть прийматися всіма пристроями в комутованій мережі, навіть тими, які не призначені для прийому даної розсилки.

VLAN створює логічний широкомовний домен, який може охоплювати кілька фізичних сегментів LAN. Поділяючи великі широкомовні домени на більш дрібні мережі, VLAN підвищують продуктивність мережі. Якщо пристрій в одній VLAN передає широкомовний кадр Ethernet, то цей кадр отримують всі пристрої в рамках однієї VLAN, пристрої ж в інших мережах VLAN цей кадр не отримують.

Мережі VLAN дозволяють реалізовувати політику забезпечення доступу і безпеки, враховуючи інтереси різних груп користувачів (рис. 3.2). Кожен порт комутатора може бути призначений тільки для однієї мережі VLAN (за винятком порту, підключеного до IP-телефону або до іншого комутатора).

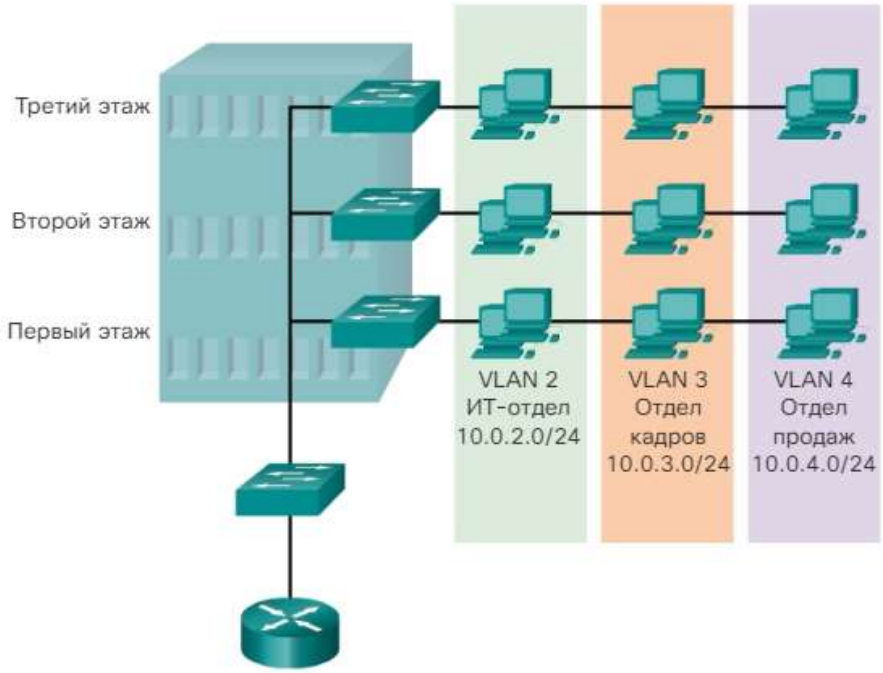


Рис. 3.4.2

Продуктивність користувачів і адаптивність мережі відіграють важливу роль у процвітанні та успіху компанії. Мережі VLAN полегшують процес

проектування мережі, що забезпечує допомогу у виконанні цілей організації. До основних переваг використання VLAN відносяться:

Безпека: групи, що володіють уразливими даними, відокремлені від решти мережі, завдяки чому знижується ймовірність витоку конфіденційної інформації. Як показано на малюнку, комп'ютери викладачів знаходяться в мережі VLAN 10 і повністю відокремлені від трафіку даних учнів і гостей (рис. 3.3).

Зниження витрат: завдяки економії на дорогих оновленнях мережевої інфраструктури і більш ефективному використанню наявної смуги пропускання і висхідних каналів відбувається зниження витрат.

Підвищення продуктивності: поділ однорідних мереж 2-го рівня на кілька логічних робочих груп (широкомовних доменів) зменшує кількість зайвого мережевого трафіку і підвищує продуктивність.

Зменшення розміру доменів широкомовної розсилки: поділ мережі на мережі VLAN зменшує кількість пристроїв в домені широкомовної розсилки. Мережа, показана на малюнку, складається з шести комп'ютерів і трьох широкомовних доменів: для викладачів, для учнів і гостьового домена.

Рис. 3.4.3

Підвищення продуктивності IT-відділу: мережі VLAN спрощують управління мережею, оскільки користувачі з аналогічними вимогами до мережі використовують одну і ту ж мережу VLAN. При введенні в експлуатацію нового комутатора на призначених портах реалізуються всі правила і процедури, вже застосовані в цій конкретній VLAN. Також IT-фахівцям легше визначати функцію мережі VLAN, призначаючи їй відповідне ім'я. На даному малюнку для простої ідентифікації мережу VLAN 10 була названа «Для викладачів», VLAN 20 - «Для учнів» і VLAN 30 - «Гостьова».

Спрощене управління проектами та програмами: мережі VLAN об'єднують користувачів і мережеві пристрої для відповідності діловим або географічним вимогам мережі. Управління проектом і робота на прикладному рівні спрощені завдяки використанню поділу функцій. Приклад такої прикладної задачі - платформа розробки додатків для електронного навчання викладачів.

Кожній VLAN в комутованій мережі відповідає IP-мережа. Таким чином, в проекті VLAN необхідно враховувати використання ієрархічної схеми мережевої адресації. Ієрархічна адресація передбачає впорядковане призначення номерів IP-мережі сегментам або мереж VLAN з урахуванням роботи мережі в цілому. Як показано на рис. 3.3, блоки суміжних мережевих адрес резервуються і налаштовуються на пристроях в певній галузі мережі.

У сучасних мережах використовується безліч різних типів мереж VLAN. Деякі типи VLAN визначаються класами трафіку. Інші типи VLAN обумовлені функціями, які вони виконують.

VLAN для даних. Віртуальна локальна мережа для даних - це мережа VLAN, яка налаштована спеціально для передачі трафіку, що генерується користувачем. Мережа VLAN, передає голосовий трафік або трафік управління, не є мережею VLAN для передачі даних. Рекомендується відокремлювати голосової і керуючий трафік від трафіку даних. VLAN для передачі даних іноді називають користувальницької мережею VLAN. Мережі VLAN для даних використовуються для поділу мережі на групи користувачів або пристроїв.

Мережа VLAN за замовчуванням. Всі порти комутатора стають частиною VLAN за замовчуванням після первинного завантаження комутатора. Порти комутатора, що знаходяться в мережі VLAN за замовчуванням, є частиною одного широкомовного домену. Завдяки цьому будь-який пристрій, підключений до будь-якого порту комутатора, може обмінюватися даними з іншими пристроями на інших портах комутатора. Мережею VLAN за замовчуванням для комутаторів Cisco встановлена VLAN 1. На рис. 3.4 команда ***show vlan brief*** була виконана на комутаторі, налаштованому за замовчуванням. Зверніть увагу, що на всі порти за замовчуванням призначені мережі VLAN 1.

VLAN 1

```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -----------------------
1    default             active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                   Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                   Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1,  Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

- По умолчанию все порты назначены сети VLAN 1.
- Сетью native VLAN по умолчанию является сеть VLAN 1.
- Сетью управления VLAN по умолчанию является сеть VLAN 1.
- VLAN 1 нельзя переименовывать или удалять

Рис. 3.4.4

VLAN 1 підтримує всі функції будь-якої мережі VLAN, проте її не можна перейменувати або видалити. За замовчуванням весь керуючий трафік 2-го рівня пов'язаний з мережею VLAN 1.

Native VLAN. Мережа native VLAN призначена для транкових портів 802.1Q. Транкові порти - це канали між комутаторами, які підтримують передачу трафіку, пов'язаного з більш ніж однією мережею VLAN. Транковий порт 802.1Q підтримує трафік, що надходить від декількох VLAN (тегований трафік), а також трафік, який надходить не від VLAN (нетегований трафік). Тегованим називається трафік, для якого в вихідний заголовок кадру Ethernet вставлений 4-байтовий тег, який визначає мережу VLAN, до якої відноситься цей кадр. Транковий порт 802.1Q розміщує нетегований трафік в мережі native VLAN, якій за умовчанням є VLAN 1.

Мережі native VLAN визначені в специфікації IEEE 802.1Q для забезпечення зворотної сумісності з нетегованим трафіком, характерним для застарілих сценаріїв локальних мереж. Мережа native VLAN служить загальним ідентифікатором на протилежних кінцях транкового каналу.

Радимо встановити native VLAN як невикористану VLAN, що відрізняється від мережі VLAN 1 і інших VLAN. Фактично прийнято виділяти фіксовану VLAN для виконання ролі мережі native VLAN для всіх транкових портів в комутованому домені.

Керуюча VLAN (Management VLAN). Керуюча VLAN - це будь-яка мережа VLAN, налаштована для доступу до функцій управління комутатора. Мережа VLAN 1 за замовчуванням є керуючою VLAN. Для створення керуючої VLAN віртуальному інтерфейсу комутатора (SVI) даної VLAN призначаються IP-адреса і маска підмережі, завдяки чому комутатором можна управляти за протоколами HTTP, Telnet, SSH або SNMP. Оскільки в вихідних налаштуваннях комутатора Cisco VLAN 1 є мережею VLAN за замовчуванням, VLAN 1 не слід використовувати в якості керуючої VLAN.

У минулому керуюча VLAN для комутатора 2960 була єдиним активним інтерфейсом SVI. У версіях ОС Cisco IOS 15.x для комутаторів Catalyst серії 2960 можлива підтримка більше одного активного інтерфейсу SVI. У версіях ОС Cisco IOS 15.x необхідно документувати певний активний інтерфейс SVI, призначений для віддаленого управління. Незважаючи на те, що теоретично комутатор може володіти більш ніж однієї керуючої VLAN, використання декількох мереж даного типу збільшує схильність мережевим атакам.

На рис. всі порти призначені мережі VLAN 1 за замовчуванням. Жодна мережа не призначена в якості VLAN з нетегірованим трафіком, і жодна інша мережа VLAN не є активною. Таким чином, мережею VLAN з нетегірованим трафіком буде керуюча мережа VLAN. Подібна настройка вважається загрозою безпеки.

Для підтримки передачі голосу по IP (VoIP) потрібна окрема мережа VLAN. Для VoIP-трафіку потрібно:

• гарантована смуга пропускання для забезпечення високої якості голосової передачі;

• пріоритет передачі перед іншими типами мережевого трафіку;

• можливість маршрутизації в обхід перевантажених ділянок;

• затримка менше 150 мс по всій мережі.

Для того щоб відповідати цим вимогам, вся мережа повинна бути спеціально спроектована для підтримки VoIP. В рамках даного посібника не розглядаються особливості настройки мережі для підтримки VoIP, проте

коротка інформація про те, як голосова VLAN працює між комутатором, IP-телефоном Cisco і комп'ютером, буде корисна.

На рис. VLAN 150 призначена для передачі голосового трафіку. Комп'ютер учня PC5 підключений до IP-телефону Cisco, а телефон підключений до комутатора S3. PC5 знаходиться в мережі VLAN 20, яка використовується для передачі даних учнів.

Рис. 3.4.5

Транк - це канал типу «точка-точка» між двома мережевими пристроями, який підтримує більше однієї мережі VLAN. Транк віртуальних мереж розширює мережі VLAN по всій мережі. Cisco підтримує стандарт IEEE 802.1Q для координації транків в інтерфейсах Fast Ethernet, Gigabit Ethernet і 10-Gigabit Ethernet.

Використання мереж VLAN без транкових каналів істотно знижує корисні можливості VLAN. Транки віртуальних мереж забезпечують поширення всього трафіку VLAN між комутаторами так, щоб пристрої, що знаходяться в одній мережі VLAN, але підключені до різних комутаторів, могли обмінюватися даними без втручання маршрутизатора.

Транк віртуальних мереж не належить до будь-якої певної мережі VLAN, а, скоріше, є «кабельним каналом» передачі багатьох VLAN між комутаторами і маршрутизаторами. Транк може також використовуватися між мережним пристроєм і сервером або іншим пристроєм, оснащеним відповідним мережним адаптером з підтримкою 802.1Q. За замовчуванням транкові порти комутатора Cisco Catalyst підтримуються всі мережі VLAN.

На рис. 3.6 канали між комутаторами S1 і S2, а також між S1 і S3 налаштовані для передачі трафіку, що відправляється по всій мережі від VLAN

10, 20, 30 і 99. Дана мережа не зможе працювати без транкових каналів VLAN.

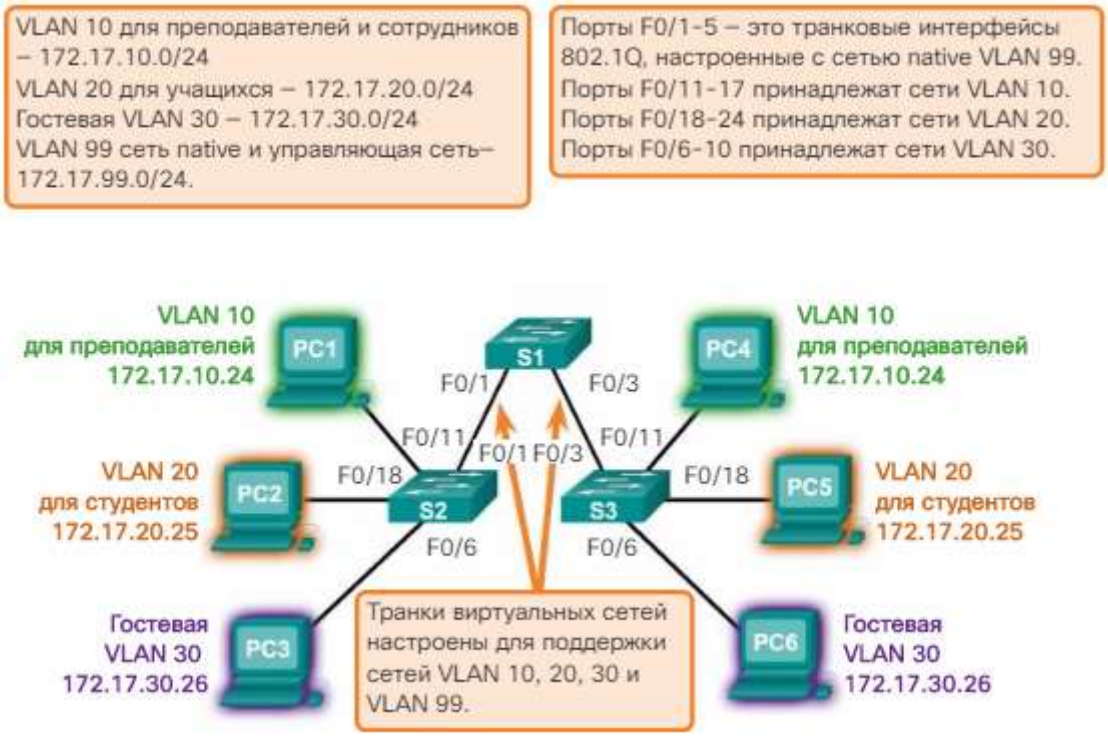


Рис. 3.4.6

Мережі без VLAN. При нормальній експлуатації, коли комутатор отримує широкомовний кадр на одному зі своїх портів, він пересилає кадр на усі порти, крім того, на якому він був отриманий. В анімації на рис. 3.7 вся мережа налаштована в одній підмережі (172.17.40.0/24), мережі VLAN не налаштовані. В результаті, коли комп'ютер викладача (PC1) відправляє широкомовний кадр, комутатор S2 відправляє цей широкомовний кадр на усі свої порти. В кінцевому підсумку вся мережа отримує широкомовлення, оскільки мережа є широкомовною доменом.

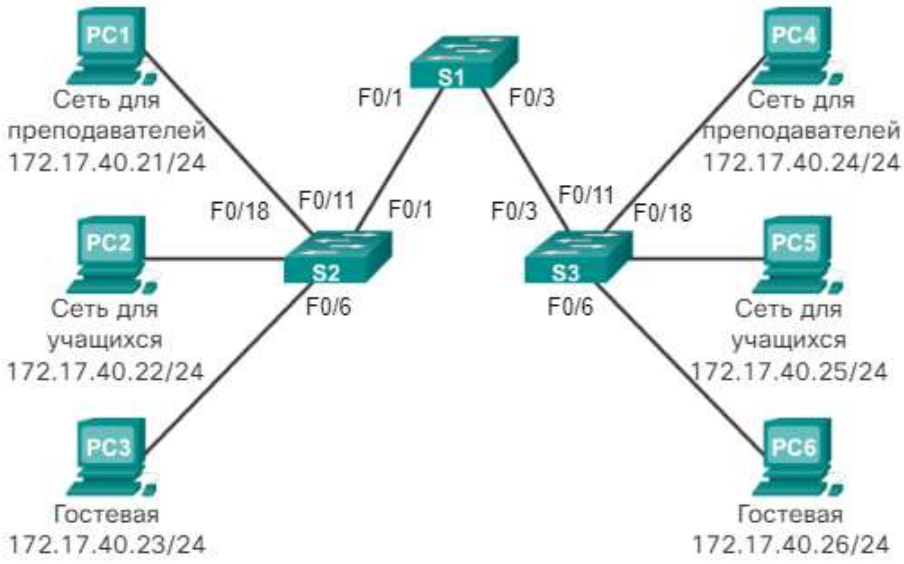


Рис. 3.4.7

В даному прикладі всі пристрої знаходяться в одній і тій же підмережі IPv4. Якби в інших підмережах IPv4 перебували пристрою, то і вони отримали б той же фрейм широкомовної розсилки. Широкомовні розсилання, такі як ARP-запит, призначені тільки для пристроїв, що знаходяться в одній підмережі.

Мережа з VLAN. Як показано в анімації на рис. 3.6, мережа була розділена на сегменти за допомогою двох VLAN. Пристрої для викладачів були призначені мережі VLAN 10, а пристрої учнів - мережі VLAN 20. Коли з комп'ютера викладача (PC1) відправляється широкомовний кадр на комутатор S2, комутатор пересилає кадр тільки на ті порти комутатора, які налаштовані для підтримки VLAN 10.

Порти, що забезпечують з'єднання між комутаторами S1 і S2 (порт F0/1) і між комутаторами S1 і S3 (порт F0/3), є транкових каналами і налаштовані для підтримки всіх VLAN в мережі.

Коли комутатор S1 отримує широкомовний кадр через порт F0/1, він пересилає широкомовний кадр з єдиного іншого порту, налаштованого для підтримки мережі VLAN 10, тобто порту F0/3. Отримавши фрейм широкомовної розсилки на порту F0/3, комутатор S3 пересилає цей кадр з іншого порту, налаштованого для підтримки мережі VLAN 10, тобто порту F0/11. Широкомовний кадр прибуває на єдиний інший комп'ютер в мережі, налаштований для VLAN 10, тобто на комп'ютер для викладачів PC4.

У разі, коли мережі VLAN реалізовані на комутаторі, передача одноадресна, багатоадресного і широкомовного трафіку від вузла в певній VLAN ведеться пристроями в межах цієї мережі VLAN.

Тегування кадрів Ethernet для ідентифікації мережі VLAN

Комутатори серії Catalyst 2960 є пристроями 2-го рівня. Для пересилання пакетів вони використовують дані заголовка кадру Ethernet. Вони не містять таблиць маршрутизації. Стандартний заголовок кадру Ethernet не містить інформацію про VLAN, до якої відноситься кадр. Тому, коли кадри Ethernet розміщуються в транкові каналі, необхідно додати інформацію про мережі VLAN, яким вони належать. Цей процес називається тегуванням і виконується за допомогою заголовка IEEE 802.1Q, зазначеного в стандарті IEEE 802.1Q. Тема 802.1Q містить тег розміром 4 байта, який додається в оригінальний заголовок кадру Ethernet і ідентифікує VLAN, до якої відноситься кадр.

Коли комутатор отримує кадр на порту, налаштованому в режимі доступу до призначеної мережею VLAN, він додає в заголовок кадру тег VLAN, заново обчислює **перевірочну** послідовність кадру (FCS) і відправляє цей тегований кадр з магістрального порту.

Детальніше про поле тегу VLAN

Поле тегу VLAN складається з поля типу, поля пріоритету, поля ідентифікатора канонічного формату і поля ідентифікатора VLAN.

Тип - це 2-байтовое значення, яке називається значенням ідентифікатора протоколу тегування (TPID). Значення для Ethernet має вигляд шістнадцятирічного числа 0x8100.

Пріоритет користувача - це 3-бітове значення, яке підтримує реалізацію рівня або сервісу.

Ідентифікатор канонічного формату (CFI) - це 1-бітовий ідентифікатор, який забезпечує передачу кадрів Token Ring по каналах Ethernet.

VLAN-ідентифікатор (VID) - це 12-бітний ідентифікаційний номер VLAN, який підтримує до 4096 ідентифікаторів VLAN.

Після того як комутатор додасть поля типу і керуючої інформації тегу, він перераховує значення FCS і додає в кадр нового значення FCS (рис. 3.8).

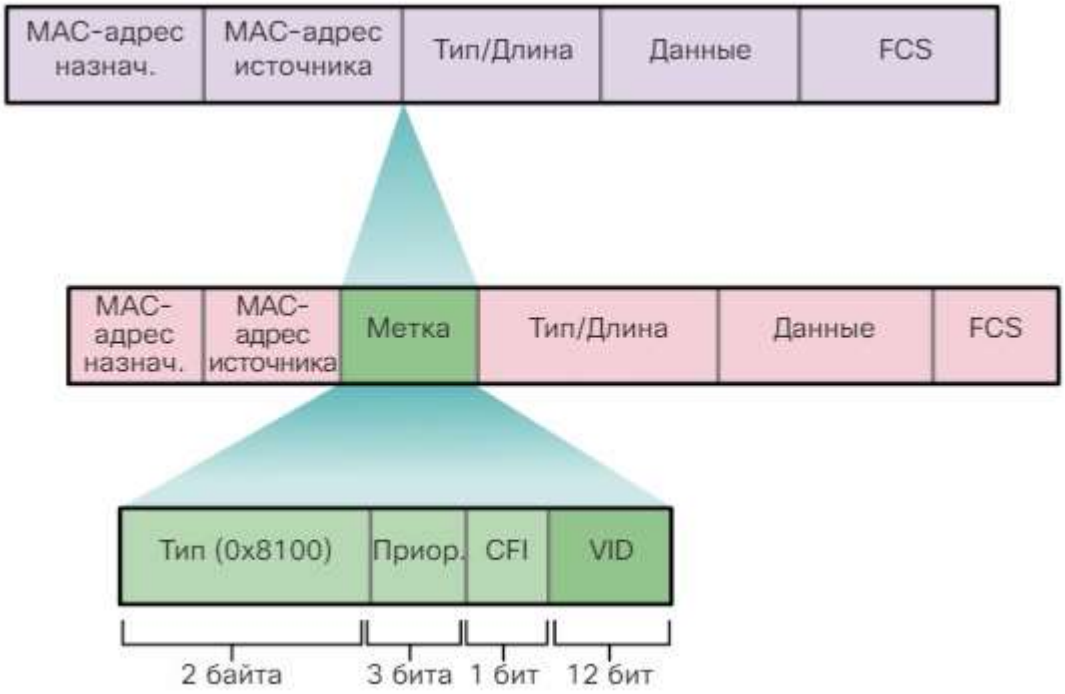


Рис. 3.4.8

Тегування кадрі в мережі native VLAN

Деякі пристрої, що підтримують транкінг, додають тег VLAN в пакети VLAN з нетегірованним трафіком. Керуючий трафік, що відправляється в мережі native VLAN, тегований не зовсім правильно. Якщо магістральний порт 802.1Q отримує тегований кадр з таким же ідентифікатором VLAN, як у мережі VLAN з нетегованим трафіком, то він відкидає цей кадр. Отже, під час налаштування порту комутатора в комутаторі Cisco налаштовуйте пристрій таким чином, щоб вони не відправляли теговані кадри по мережі native VLAN. До пристроїв від інших виробників, які підтримують тегування кадрів в мережі native VLAN, відносяться IP-телефони, сервери, маршрутизатори і комутатори немає від Cisco.

Нетеговані кадри в мережі native VLAN

Коли транковий порт комутатора Cisco отримує нетеговані кадри (які рідко зустрічаються в добре спроектованої мережі), він пересилає ці кадри в мережу native VLAN. Якщо з мережею native VLAN без супутніх пристрої (що буває досить часто), а також немає інших транкових портів (що також часто трапляється), то кадр відкидається. Мережею native VLAN за замовчуванням є мережа VLAN 1. При налаштуванні транкового порту 802.1Q порту ідентифікатора VLAN за замовчуванням (PVID) привласнюють значення ідентифікатора мережі native VLAN. Весь нетегований трафік, що надходить в порт 802.1Q або з нього, пересилається відповідно до значення PVID. Наприклад, якщо мережа VLAN 99 налаштована як native VLAN, то значення PVID одно 99, а весь нетегований трафік пересилається в мережу VLAN 99. Якщо мережа native VLAN була перенастроєна, то значення PVID присвоюється рівним 1.

На рис. 3.9 комп'ютер PC1 підключений до транкового каналу 802.1Q за допомогою концентратора. PC1 відправляє нетегований трафік, який комутатори пов'язують з мережею VLAN з нетегованим трафіком,

налаштованої на магістральних портах, і пересилають його відповідним чином. Тегований трафік в транкові каналі, отриманий комп'ютером PC1, відкидається. У цьому сценарії мережа є погано спроектованою з кількох причин: в ній використовується концентратор, є вузол, підключений до транкового каналу, і це означає, що існують порти доступу комутаторів, призначені мережі native VLAN. У цьому сценарії також показано, що для підтримки застарілих сценаріїв необхідна специфікація IEEE 802.1Q для VLAN з нетегованим трафіком.

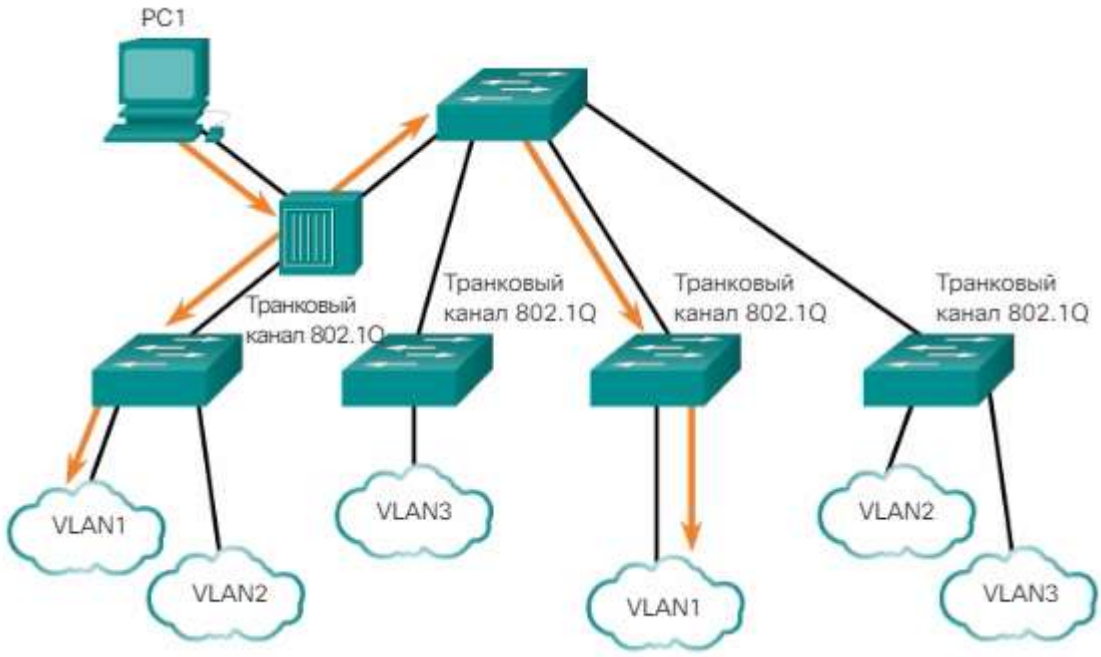


Рис. 3.4.9

Не забувайте, що для підтримки VoIP потрібна окрема голосова VLAN.

Порт доступу, який використовується для підключення IP-телефону Cisco, може бути налаштований для використання двох окремих мереж VLAN: одна мережа VLAN для голосового трафіку, а інша мережа VLAN для трафіку даних від пристрою, підключеного до телефону. Канал між комутатором і IP-телефоном служить транковим каналом для передачі і голосового трафіку, і трафіку даних.

IP-телефон Cisco містить вбудований комутатор 10/100 на 3 порти. Порти забезпечують виділені підключення наступним пристроїв:

- порт 1 підключається до комутатора або іншого пристрою VoIP;
- порт 2 - це внутрішній інтерфейс 10/100, через який передається трафік IP-телефону;
- порт 3 (порт доступу) підключається до ПК або іншого пристрою.

На комутаторі доступ налаштований для відправки пакетів протоколу CDP, що вказують підключеному IP-телефону відправляти голосовий трафік на комутатор одним з трьох способів, залежно від типу трафіку:

1. в голосової VLAN, тегованих значенням пріоритету класу обслуговування (CoS) рівня 2;

2. в мережі VLAN доступу, тегованих значенням пріоритету CoS рівня 2;

3. в нетегованій VLAN доступу (без значення пріоритету CoS рівня 2).

На рис. 310 комп'ютер учня PC5 підключений до IP-телефону Cisco, а телефон підключений до комутатора S3. VLAN 150 призначена для передачі голосового трафіку, а PC5 знаходиться в VLAN 20, використовуваної для даних учнів.

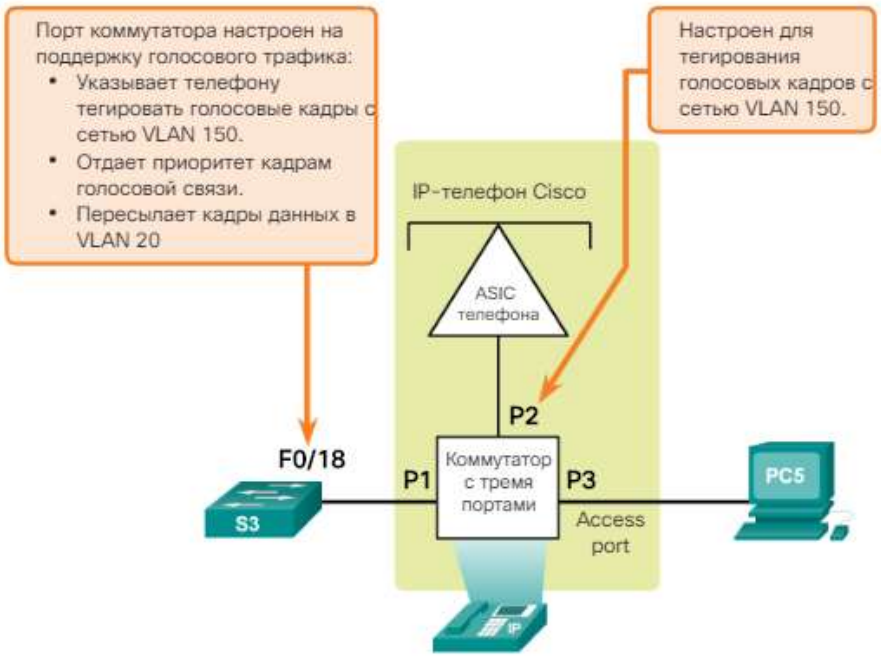


Рис. 3.4.10

На рис. 3.10 наведено приклад вихідних даних. В рамках даної книги не розглядаються команди Cisco IOS для голосового зв'язку, але в виділення в прикладі даних, що виводяться показаний інтерфейс F0/18, налаштований з VLAN для даних (VLAN 20) і VLAN для голосового зв'язку (VLAN 150).

Діапазони VLAN на комутаторах Catalyst

Різні комутатори Cisco Catalyst підтримують різну кількість мереж VLAN. Кількість підтримуваних мереж VLAN досить велике для задоволення потреб більшості організацій. Наприклад, комутатори Catalyst 2960 і 3560 здатні підтримувати більш 4 тисяч мереж VLAN. Віртуальні локальні мережі стандартного діапазону на цих комутаторах мають ідентифікатор від 1 до 1 005, а мережі VLAN розширеного діапазону - від 1 006 до 4 094. На рис. 3.11 показані доступні VLAN на комутаторі Catalyst 2960 під керуванням Cisco IOS версії 15.x.

Віртуальні локальні мережі стандартного діапазону:

- Використовуються в малих і середніх мережах підприємств і організацій.
- Визначаються ідентифікатором VLAN від 1 до 1005.
- Ідентифікатори від 1 002 до 1005 резервуються для мереж VLAN типу Token Ring і FDDI.
- Ідентифікатори 1 і ідентифікатори від 1002 до 1005 створюються автоматично і не можуть бути видалені.

- Конфігурації зберігаються в файлі бази даних VLAN під ім'ям vlan.dat. Файл vlan.dat розташований у флеш-пам'яті комутатора.
- Протокол VTP (транковий протокол VLAN), що допомагає управляти конфігураціями VLAN між комутаторами, може розпізнавати і зберігати тільки мережі VLAN стандартного діапазону.

Мережі VLAN розширеного діапазону

- Дозволяють операторам зв'язку розширювати свою інфраструктуру для великого числа клієнтів. Деяким великим міжнародним корпораціям потрібні ідентифікатори VLAN розширеного діапазону.
- Визначаються ідентифікатором VLAN від 1006 до 4094.
- Конфігурації мереж не записуються в файл vlan.dat.
- Підтримують менше функцій VLAN, ніж мережі VLAN стандартного діапазону.
- За умовчанням вони зберігаються в файлі поточної конфігурації.
- Протокол VTP не розпізнає мережі VLAN розширеного діапазону.

Примітка. 4096 - це максимальна кількість VLAN, доступних на комутаторах Catalyst, оскільки в поле ідентифікатора VLAN заголовка IEEE 802.1Q налічується 12 біт.

```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ----------------------------- --------- ----------------------
1    default             active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                   Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                   Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1, Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

Рис. 3.4.11

Під час налаштування мереж VLAN стандартного діапазону відомості про конфігурацію зберігаються у флеш-пам'яті комутатора, у файлі *vlan.dat*. Флеш-пам'ять є постійною, тому не вимагає виконання команди ***copy running-config startup-config***. Однак, оскільки під час створення мереж VLAN на комутаторі Cisco часто необхідно налаштовувати і інші параметри, рекомендується зберігати зміни поточної конфігурації в початкову завантажувальний конфігурацію.

На рис. 3.12 показаний синтаксис команди Cisco IOS, який використовується для додавання мережі VLAN до комутатора і присвоєння їй імені. Під час налаштування комутатора рекомендується привласнювати ім'я кожної мережі VLAN.

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	`S1# configure terminal`
Создайте сеть VLAN с допустимым номером идентификатора.	`S1(config)# vlan vlan-id`
Укажите уникальное имя для идентификации сети VLAN.	`S1(config-vlan)# name vlan-name`
Вернитесь в привилегированный режим.	`S1(config-vlan)# end`

Рис. 3.4.12

На рис. 3.13 показано, яким чином на комутаторі S1 налаштовується мережа VLAN для учнів (VLAN 20). У прикладі топології комп'ютер учня (комп'ютер PC2) не прив'язаний до мережі VLAN, але має IP-адресу 172.17.20.22.

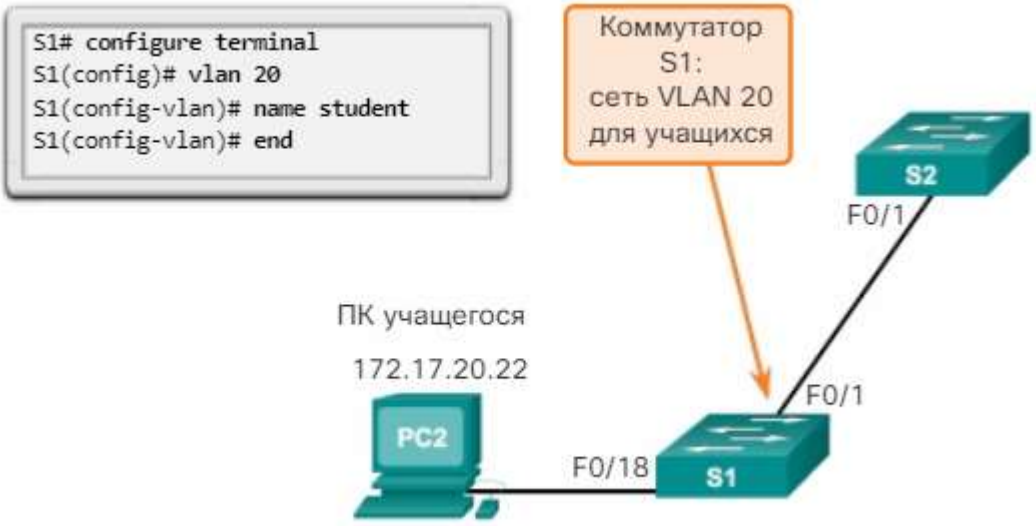


Рис. 3.4.13

Використовуйте інструмент перевірки синтаксису для створення мережі VLAN і введіть ***команду show vlan brief***, щоб відобразити вміст файлу *vlan.dat*.

Крім одного ідентифікатора VLAN, можна ввести групу ідентифікаторів VLAN, розділених комами, або діапазон ідентифікаторів VLAN, розділених дефісами, за допомогою команди ***vlan vlan_id***. Наприклад, для створення мереж VLAN 100, 102, 105, 106 і 107 використовуйте наступну команду:

S1 (config) # vlan 100,102,105-107

Призначення портів мереж VLAN

Наступний крок після створення мережі VLAN - призначення портів мереж VLAN. Порт доступу може належати тільки одній VLAN. Винятком з цього правила є випадок, коли порт підключений до IP-телефону і, як наслідок, з портом пов'язано дві мережі VLAN: одна - для передачі голосу, друга - для передачі даних.

На рис. 3.14 показаний синтаксис для визначення порту в якості порту доступу і призначення його мережі VLAN. Виконувати команду switchport mode accessнеобязательно, але настійно рекомендується з метою забезпечення безпеки. За допомогою цієї команди інтерфейс переходить в режим постійного доступу.

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной конфигурации.	`S1# configure terminal`
Войдите в режим конфигурации интерфейса.	`S1(config)# interface interface_id`
Переведите порт в режим доступа.	`S1(config-if)# switchport mode access`
Назначьте порт сети VLAN.	`S1(config-if)# switchport access vlan vlan_id`
Вернитесь в	`S1(config-if)# end`

Рис. 3.4.14

Примітка. Використовуйте команду ***interface range***, щоб одночасно налаштувати декілька інтерфейсів.

У прикладі на рис. 3.14 VLAN 20 призначена порту F0/18 на комутаторі S1; таким чином, комп'ютер учня (комп'ютер PC2) розташований в мережі VLAN 20. Мережі VLAN налаштовуються на комутаційному порте, а не на пристрої. Для комп'ютера PC2 IPv4-адрес і маска підмережі пов'язані з мережею VLAN, налаштованої на комутаційному порте (VLAN 20 в даному прикладі). Під час налаштування VLAN 20 на інших комутаторах мережевий адміністратор знає, що потрібно налаштувати інші комп'ютери учнів до тієї ж підмережі, в якій знаходиться комп'ютер PC2 (172.17.20.0/24).

Використовуйте інструмент перевірки синтаксису для призначення мережі VLAN і введіть команду ***show vlan brief***, щоб відобразити вміст файлу vlan.dat.

Команда ***switchport access vlan*** примусово створює VLAN на комутаторі (рис. 3.15). Наприклад, мережа VLAN 30 відсутня в даних, що виводяться командою ***show vlan brief*** на комутаторі. *Я*кщо на будь-якому інтерфейсі без попередньої конфігурації ввести команду ***switchport access vlan 30***, то комутатор відобразить наступне:

% Access VLAN does not exist. Creating vlan 30

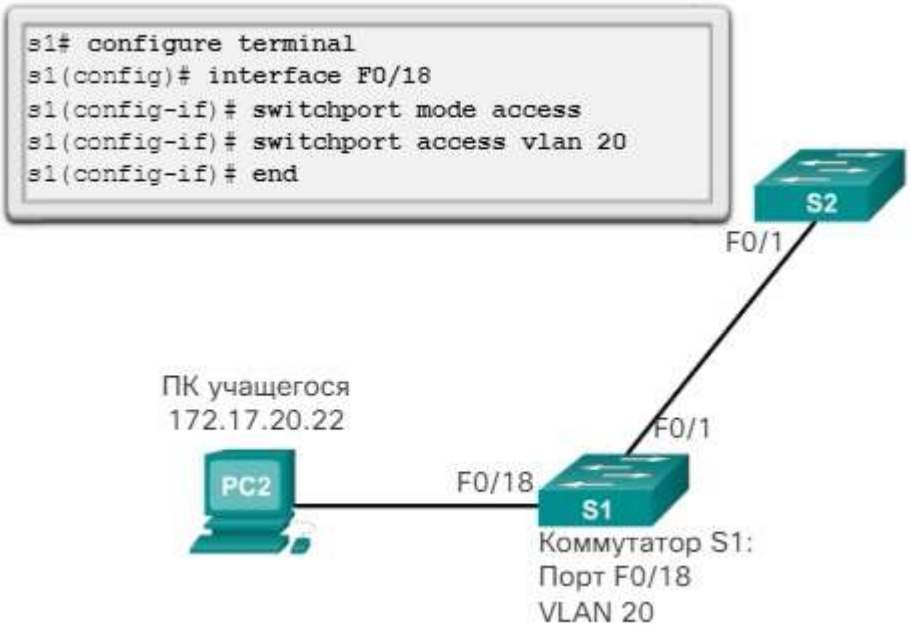


Рис. 3.4.15

Існує безліч способів змінити приналежність портів VLAN. На рис. 3.16 показаний синтаксис для зміни приналежності порту комутатора мережі VLAN 1 за допомогою команди режиму конфігурації інтерфейсу ***no switchport access vlan***.

Раніше інтерфейс F0/18 був призначений мережі VLAN 20. Для інтерфейсу F0/18 потрібно ввести команду ***no switchport access vlan***. Вивчіть дані, які будуть виведені командою **show vlan brief**. Команда ***show vlan brief*** показує призначення VLAN і тип приналежності для всіх портів комутатора. Команда ***show vlan brief*** виводить по одному рядку для кожної VLAN. У вихідних даних для кожної VLAN вказані ім'я, стан і порти комутатора VLAN.

Мережа VLAN 20 все ще активна, хоча їй не призначені порти. На рис. 3.16 вихідні команди show interfaces f0/18 switchport підтверджують, що мережа доступу VLAN для інтерфейсу F0/18 було скинуто до VLAN 1.

```
S1# config t
S1(config)# interface F0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show vlan brief

VLAN Name                Status     Ports
---- ------------------- --------- -----------------------------------
1    default             active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                    Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                    Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                    Gi0/2
20   student             active     Fa0/11
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
S1#
```

Рис. 3.4.16

Належність порту VLAN може бути легко змінена. Для того щоб змінити приналежність порту VLAN, немає необхідності спочатку видаляти порт з мережі VLAN. При зміні VLAN, до якої належить порт доступу, на іншу існуючу VLAN, попередня приналежність просто замінюється на нову. На рис. 4 порт F0 / 11 призначений мережі VLAN 20.

Команды коммутатора Cisco под управлением ОС IOS	
Перейдите в режим глобальной конфигурации.	`S1# configure terminal`
Удалите назначение сети VLAN из порта.	`S1(config-if)# no switchport access vlan`
Вернитесь в привилегированный исполнительский режим.	`S1(config-if)# end`

Рис. 3.4.17

Видалення віртуальних локальних мереж

На рисунку 3.19 показана команда режиму глобальної настройки ***no vlan vlan_id*** для видалення VLAN 20 з комутатора. При мінімальній настройці комутатора S1 всі порти належать VLAN 1. Команда ***show vlan brief*** дозволяє переконатися, що після використання команди ***no vlan 20*** мережу VLAN 20 видалена з файлу *vlan.dat*.

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief

VLAN Name                 Status    Ports
---- ----------------     --------- -------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                    Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                    Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                    Gi0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Рис. 3.4.18

Увага! Перед видаленням мережі VLAN необхідно спочатку перепризначити всі її порти іншій мережі VLAN. Після видалення VLAN всі порти, що не були переміщені в активну мережу VLAN, не зможуть обмінюватися даними з іншими вузлами, поки вони не будуть призначені активній VLAN.

Інший варіант - видалити весь файл *vlan.dat* за допомогою команди привілейованого режиму ***delete flash: vlan.dat.*** Скорочену версію команди (delete vlan.dat) можна використовувати в тому випадку, якщо файл *vlan.dat* не переміщений зі свого розташування за замовчуванням. Після виконання цієї команди і перезавантаження комутатора раніше налаштовані VLAN будуть

видалені. Фактично, це дозволяє відновити на комутаторі його заводські настройки VLAN.

Примітка. Щоб відновити заводські настройки в разі з комутатором Catalyst, перед його перезавантаженням потрібно ввести команду ***erase startup-config*** разом з командою ***delete vlan.dat.***

Перевірка інформації про мережу VLAN

Встановивши комп'ютерну мережу VLAN, її конфігурації можна перевірити за допомогою команд Cisco IOS категорії «**show**».

На рис. 3.20 показані параметри команд ***show vlan*** і ***show interfaces***.

Команда `show vlan`

Синтаксис команд в интерфейсе командной строки Cisco IOS	
`show vlan [brief | id vlan-id | name vlan-name | summary]`	
Отобразите одну строку для каждой сети VLAN, содержащую имя, состояние и порты сети VLAN.	`brief`
Отобразите сведения об одной сети VLAN, идентифицируемой с помощью номера идентификатора VLAN. Для идентификатора VLAN диапазон составляет от 1 до 4094.	`id vlan-id`
Отобразите сведения об одной сети VLAN, идентифицируемой с помощью ее имени. Имя сети	`name vlan-name`

Команда `show interfaces`

Синтаксис команд в интерфейсе командной строки Cisco IOS	
`show interfaces [interface-id | vlan vlan-id] | switchport`	
В число допустимых интерфейсов входят физические порты (в том числе тип, модуль и номер порта) и каналы порта. Диапазон каналов порта от 1 до 6.	`interface-id`
Идентификация сети VLAN. Диапазон от 1 до 4094.	`vlan vlan-id`
Отобразите административное и рабочее состояние порта коммутации, в том числе параметры блокировки и защиты порта.	`switchport`

Рис. 3.4.19

У прикладі на рис. 3.21 команда ***show vlan name student*** генерує вихідні дані, які важко інтерпретувати. Команда ***show vlan summary*** відображає список всіх налаштованих мереж VLAN. У вихідних даних на рис. 3.21 показані сім мереж VLAN.

Использование команды `show vlan`

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, Fa0/18

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----------------- ------ ------ -------- ---- -------- ------
20  enet 100020 1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------

S1# show vlan summary
Number of existing VLANs              : 7
Number of existing VTP VLANs          : 7
Number of existing extended VLANS     : 0

S1#
```

Рис. 3.4.20

Команда show interfaces vlan vlan_id відображає відомості, які не розглядаються в цьому розділі. У другому рядку на рис. 3.22 відображена важлива інформація, яка вказує, що мережа VLAN 20 знаходиться в робочому стані.

Использование команды `show interfaces vlan`

```
S1# show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia
  001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 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 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 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Рис. 3.4.21

Використовуйте інструмент перевірки, щоб відобразити інформацію про VLAN і комутаційному порте і перевірити призначення і режим VLAN.

Транк віртуальної мережі - це канал OSI 2-го рівня між двома комутаторами, який передає трафік в усі мережі VLAN (якщо список допустимих мереж VLAN не обмежений вручну або динамічно). Для того щоб активувати транкові канали, налаштуйте порти на будь-якому кінці фізичного каналу за допомогою паралельних наборів команд.

Щоб налаштувати комутаційний порт на одному кінці магістрального каналу, використовуйте команду ***switchport mode trunk***. За допомогою цієї команди інтерфейс переходить в постійний транковий режим. На порту починається узгодження протоколу DTP для перетворення каналу в транковий, навіть якщо інтерфейс, підключений до нього, не погоджується на таку зміну. В даному посібнику команда ***switchport mode trunk*** є єдиним способом налаштування магістрального каналу.

Примітка. Налаштування DTP не розглядається в рамках даного посібника.

На рис. 3.23 показаний синтаксис команд Cisco IOS для визначення мережі native VLAN (крім VLAN 1). У цьому прикладі мережу VLAN 99 налаштовано як VLAN з нетегірованним трафіком за допомогою команди ***switchport trunk native vlan 99***.

Команды коммутатора Cisco под управлением ОС IOS	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Force the link to be a trunk link.	`S1(config-if)# switchport mode trunk`
Specify a native VLAN for untagged frames.	`S1(config-if)# switchport trunk native vlan vlan_id`
Specify the list of VLANs to be allowed on the trunk link.	`S1(config-if)# switchport trunk allowed vlan vlan-list`
Return to the privileged EXEC mode.	`S1(config-if)# end`

Рис. 3.4.22

Використовуйте команду Cisco IOS **switchport trunk allowed vlan** для вказівки списку мереж VLAN, яким дозволений доступ в магістральний канал.

Примітка. Ця конфігурація передбачає застосування комутаторів Cisco Catalyst 2960, які автоматично використовують інкапсуляцію 802.1Q для магістральних каналів. Інші комутатори можуть зажадати ручної настройки інкапсуляції. Завжди налаштовуйте обидва кінці транкового каналу з однієї і тієї ж мережею native VLAN. Якщо конфігурація транка 802.1Q на обох кінцях різниться, то ПО Cisco IOS повідомить про помилку

Скидання транкового каналу до стану за замовчуванням

На рис. 3.24 показані команди для видалення дозволених мереж VLAN і скидання мережі native VLAN транка. Після скидання до стану за замовчуванням транк дозволяє все VLAN і використовує VLAN 1 як native VLAN.

Команды коммутатора Cisco под управлением ОС IOS	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Set trunk to allow all VLANs.	`S1(config-if)# no switchport trunk allowed vlan`
Reset native VLAN to default.	`S1(config-if)# no switchport trunk native vlan`
Return to the privileged EXEC mode.	`S1(config-if)# end`

Рис. 3.4.23

На рис. показані команди, використовувані для скидання всіх параметрів транкового інтерфейсу до стандартних параметрів. Команда ***show interfaces f0/1 switchport*** показує, що для магістрального каналу було відновлено стан за замовчуванням.

На рис. 3.24 приклад вихідних даних показує команди, використовувані для видалення транковой функції з порту F0/1 з комутатора S1. Команда ***show interfaces f0/1 switchport*** показує, що тепер інтерфейс f0/1 знаходиться в режимі статичного доступу.

Перевірка конфігурації транкового каналу

На рис. 3.25 показана конфігурація порту F0/1 на комутаторі S1. Для перевірки конфігурації використовується команда ***show interfaces*** ідентіфікатор_інтерфейса switchport.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

Рис. 3.4.24

У верхній виділеної області показано, що адміністративний режим порту F0/1 налаштований на **trunk**. Порт знаходиться в режимі транка. У наступній виділеній області видно, що мережа native VLAN - це VLAN 99. Далі в нижній виділеної області вихідних даних показано, що всі VLAN в транковому каналі активні.

Кожній VLAN повинна відповідати IP-мережа. Якщо два пристрої в одній мережі VLAN мають різні адреси підмереж, вони не можуть обмінюватися даними. Дане невідповідність є поширеною проблемою, і для її вирішення потрібно виявити помилку в конфігурації і змінити адресу підмережі на правильну.

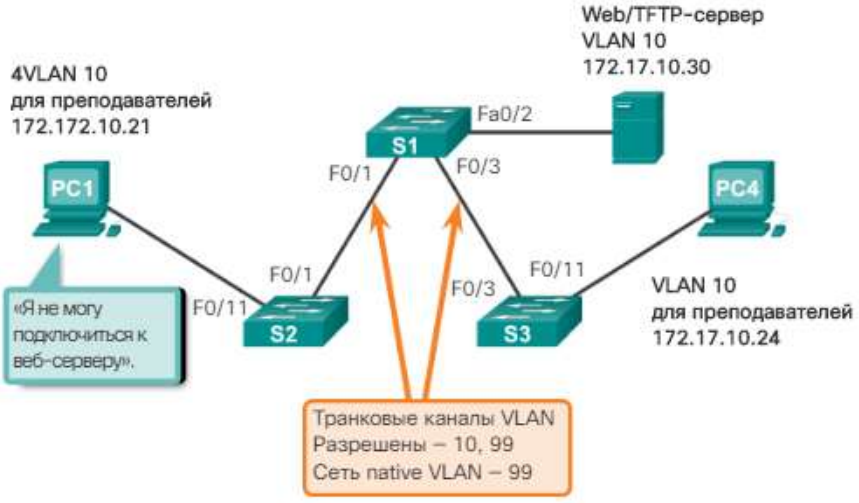


Рис. 3.4.25

На рис. 3.26 комп'ютер PC1 не може підключитися до вказаного серверу Web/TFTP. Перевірка параметрів конфігурації IPv4 на комп'ютері PC1, показана на рис. 3.26, виявляє найбільш поширену проблему при налаштуванні мереж VLAN - неправильно налаштований адресу IPv4. Комп'ютер PC1 налаштований з адресою IPv4 172.172.10.21, тоді як правильну адресу IPv4 - 172.17.10.21.

Відсутні мережі VLAN

Якщо між пристроями в VLAN немає з'єднання, а проблеми з IP-адресацією були усунені, зверніться до робочої діаграмі на рис. 3.27, щоб усунути проблему:

Крок 1. Застосуйте команду **show vlan,** щоб переконатися, що порт належить даній VLAN. Якщо порт призначений неправильній VLAN, використовуйте команду **switchport access vlan** для коригування приналежності VLAN. Використовуйте команду **show mac address-table** для перевірки адрес, отриманих на певному комутаційному порту, і VLAN, які зареєстровані на цей порт (див. рис. 3.27).

Крок 2. Якщо VLAN, якій призначений порт, видалена, порт стає неактивним. Порти віддаленої VLAN не буде зазначено в даних, що виводяться командою show vlan. Використовуйте команду **show interfaces switchport**, щоб перевірити, чи призначена порту неактивна мережа VLAN (див. рис. 3.27).

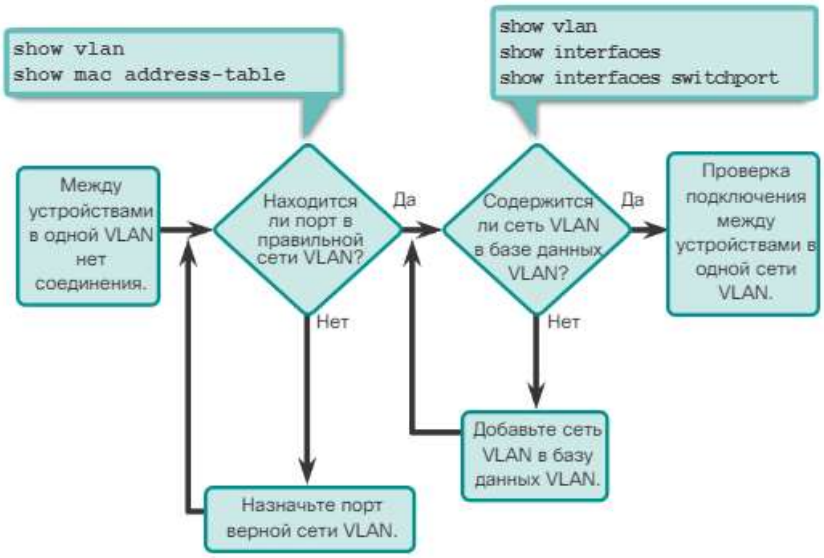


Рис. 3.4.26

На рис. 3.28 показаний приклад MAC-адрес, отриманих на інтерфейсі F0/1. Тут видно, що MAC-адресу 000c.296a.a21c був отриманий на інтерфейсі F0/1 в мережі VLAN 10. Якщо цей номер не відповідає номеру очікуваної VLAN, змініть приналежність портів мережі VLAN за допомогою команди **switchport access vlan**.

```
S1# show mac address-table interface FastEthernet 0/1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
10     000c.296a.a21c    DYNAMIC     Fa0/1
10     000f.34f9.9181    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 2
```

```
S1# show interfaces FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Рис. 3.4.27

Кожен комутатор належить VLAN. Якщо VLAN, якій належить порт, видалена, порт стає неактивним. Всі порти, що належать віддаленій мережі VLAN, не зможуть взаємодіяти з іншими сегментами мережі. Для того щоб перевірити, чи активний порт, використовуйте команду **show interface f0/1 switchport**. Якщо порт неактивний, він не буде працювати, поки не буде створена відсутня VLAN за допомогою команди режиму глобальної настройки

vlan vlan_id або поки VLAN не буде стерта з порту за допомогою команди **no switchport access vlan vlan_id.**

Типовою завданням мережевого адміністратора є усунення неполадок під час створення магістрального каналу або в портах, які некоректно працюють в якості магістральних. Іноді порт комутатора може працювати як транковий порт, навіть якщо він не налаштований для цього. Наприклад, порт доступу може приймати кадри від мереж VLAN, до яких цей порт не призначено. Це називається витоком VLAN.

На рис. 3.29 показана робоча діаграма рекомендацій щодо усунення неполадок в каналах.

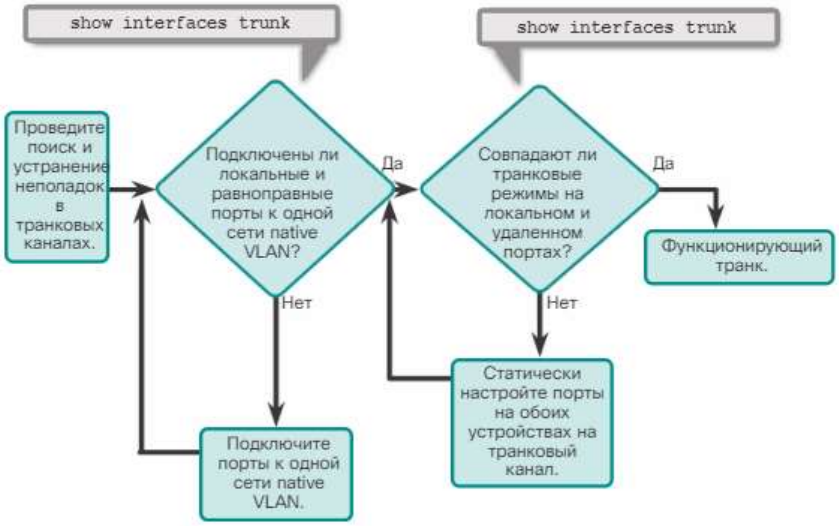


Рис. 3.4.28

Для усунення неполадок при невдалому створенні транкового каналу або витоку VLAN виконайте наступні дії:

Крок 1. Використовуйте команду **show interfaces trunk**, щоб перевірити, чи збігаються локальна VLAN і однорангова VLAN з нетегірованим трафіком. Якщо native VLAN не збігається на обох сторонах, відбувається витік VLAN.

Крок 2. Використовуйте команду **show interfaces trunk** для перевірки встановлення транкового каналу між комутаторами. По можливості налаштовуйте транкові канали статично. Порти комутатора Cisco Catalyst за замовчуванням використовують протокол DTP і намагаються узгодити транковий канал.

Для того щоб відобразити стан транка, мережі native VLAN, використовуваної на цьому транкові каналі, і перевірити установку транка, використовуйте команду **show interfaces trunk**. Приклад на рис. 3.30 показує, що мережа native VLAN на одному боці транкового каналу була змінена на VLAN 2. Якщо на одному кінці транкового підключення налаштована мережа native VLAN 99, а на іншому - native VLAN 2, то кадр, відправлений з мережі VLAN 99 на одному кінці, буде отримано в мережі VLAN 2 на іншому кінці. Трафік VLAN 99 потрапляє в сегмент VLAN 2.

```
SW1# show interfaces f0/1 trunk

Port        Mode     Encapsulation  Status     Native vlan
Fa0/1       auto     802.1q         trunking   2

<Данные опущены>
```

Рис. 3.4.29

CDP відображає повідомлення про розбіжності native VLAN в транкові каналі таким повідомленням:

При виникненні розбіжностей native VLAN відбуваються проблеми з підключенням в мережі. Трафік даних мереж VLAN, крім двох налаштованих мереж native VLAN, успішно проходить по транкові каналу, але дані, пов'язані з будь-якої з цих двох native VLAN, не проходять по транкові каналу.

Як показано на рис. 3.29, проблеми розбіжності мережі VLAN з нетегірованим трафіком не заважають створенню магістрального каналу. Щоб вирішити проблему невідповідності мережі native VLAN, налаштуйте мережу native VLAN так, щоб це була одна і та ж VLAN на обох сторонах каналу.

Причиною неполадок в транкових каналах зазвичай є неправильна конфігурація. Під час налаштування мереж VLAN і транкових каналів в комутованій інфраструктурі часто трапляються такі типи помилок конфігурації.

Розбіжності native VLAN: транкові порти налаштовані з різними мережами native VLAN. Ця помилка конфігурації виводить на консоль відповідні повідомлення і, крім інших проблем, може порушити маршрутизацію між VLAN. Це тягне за собою загрозу безпеці.

Розбіжності транкового режиму: для одного транкового порту налаштований режим, який не відповідає транкові режиму відповідного порту з іншого боку. При цій помилці конфігурації транк перестає працювати. За допомогою команди **switchport mode trunk** переконайтеся, що налаштовані обидві сторони магістрального каналу.

Дозволені мережі VLAN в транкових каналах: список мереж VLAN, дозволених в транки, що не був оновлений у відповідності з поточними вимогами VLAN. В цьому випадку по магістральному каналу передається непередбачений трафік або ж передача трафіку припиняється.

Якщо виявлена проблема з транкових каналом, а причина невідома, почніть усунення неполадок з перевірки розбіжності транкових каналів для native VLAN. Якщо причина не в цьому, перевірте розбіжності транкового режиму, потім перевірте список дозволених VLAN.

Невірний режим порту

Транкові канали зазвичай настроюються статично за допомогою команди **switchport mode trunk**. Для узгодження стану каналу транкові порти комутатора Cisco Catalyst використовують протокол DTP. Коли порт в транкові каналі налаштований в режимі транка, який несумісний з режимом транкового порту на іншій стороні, створення транкового каналу між двома комутаторами неможливо.

У сценарії, проілюстрованому на рис. 3.31, комп'ютер PC4 не може зв'язатися з внутрішнім веб-сервера. У топології вказана правильна конфігурація. У чому полягає проблема?

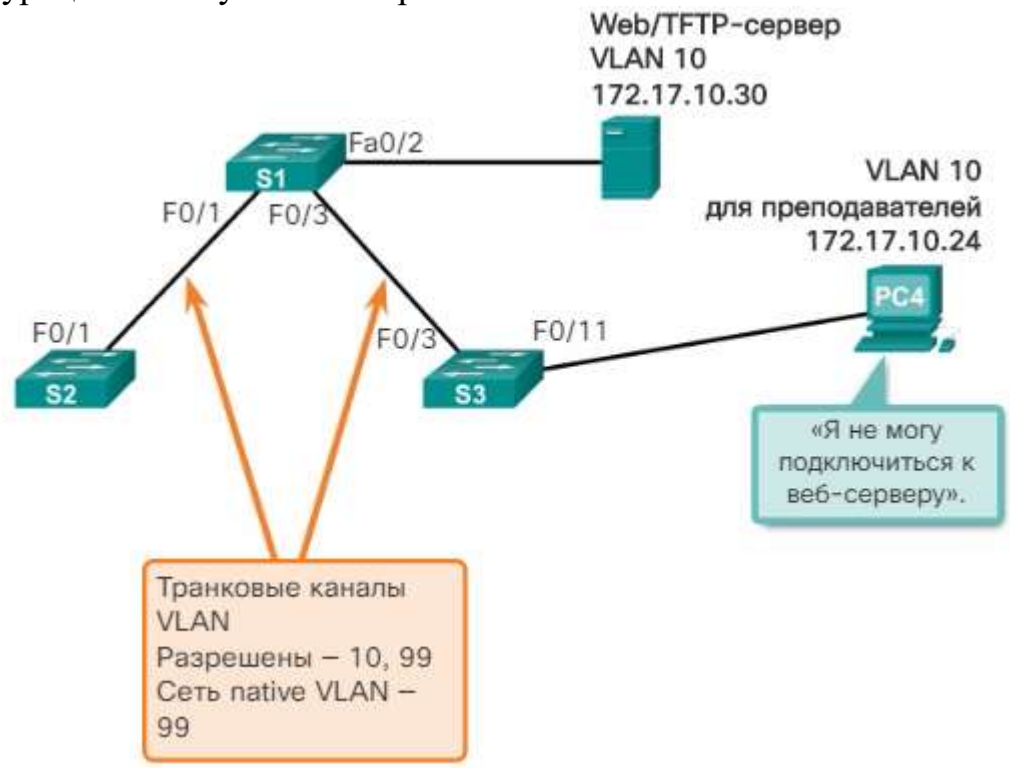


Рис. 3.4.30

Перевірте стан транкових портів на комутаторі S1 за допомогою команди **show interfaces trunk**.

Выходные данные на коммутаторе S1

```
S1# show interfaces trunk
Port  Mode  Encapsulation  Status   Native vlan
Fa0/1 on    802.1q         trunking 99
Port  Vlans allowed on trunk
Fa0/1 10,99
Port  Vlans allowed and active in management domain
Fa0/1 10,99
Port  Vlans in spanning tree forwarding state and not pruned
Fa0/1 10,99
S1# show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
```

Выходные данные на коммутаторе S3

```
S3# show interfaces trunk

S3#
S3# show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: static access
…
```

Рис. 3.4.31

Вихідні дані на рис. 3.32 показують, що інтерфейс Fa0/3 комутатора S1 в даний час знаходиться поза транковим каналом. При перевірці інтерфейсу F0/3 з'ясовується, що комутаційний порт статично налаштований в магістральному режимі. Перевірка транків на комутаторі S3 виявляє, що активні транкові порти відсутні. Подальша перевірка показує, що інтерфейс Fa0/3 знаходиться в режимі статичного доступу. Це пов'язано з тим, що порт був налаштований за допомогою команди **switchport mode access**. Це пояснює, чому транковий канал не працює.

Щоб вирішити дану проблему, змініть конфігурацію магістральний режим порту F0/3 на комутаторі S3, як показано на рис. 3.33. Після зміни конфігурації дані, що виводяться командою **show interfaces**, вказують, що тепер комутаційний порт S3 знаходиться в магістральному режимі. Дані виведення на комп'ютері PC4 показують, що його підключення до веб/TFTP-сервера по IPv4-адресою 172.17.10.30 було відновлено.

Выходные данные на коммутаторе S1

```
S1# config terminal
S1(config)# interface f0/3
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
```

Выходные данные на коммутаторе S3

```
S3# config terminal
S3(config)# interface f0/3
S3(config-if)# switchport mode trunk
S3(config-if)# end
S3# show interfaces f0/3 switchport
```

Выходные данные на компьютере PC4

```
PC4> ping 172.17.10.30
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: bytes=32 time=147ms TTL=128
…
```

Рис. 3.4.32

Невірний список віртуальної локальної мережі

Для успішної передачі трафіку з мережі VLAN по транкам VLAN повинна бути дозволена на транковому каналі. Для цього використовуйте команду **switchport trunk allowed vlan vlan-id**.

На рис. 3.34 мережу VLAN 20 (для учнів) та комп'ютер PC5 були додані в мережу. Документація була оновлена, щоб показати, що на транки дозволені мережі VLAN 10, 20 і 99. У цьому сценарії комп'ютер PC5 не може підключитися до сервера електронної пошти для учнів.

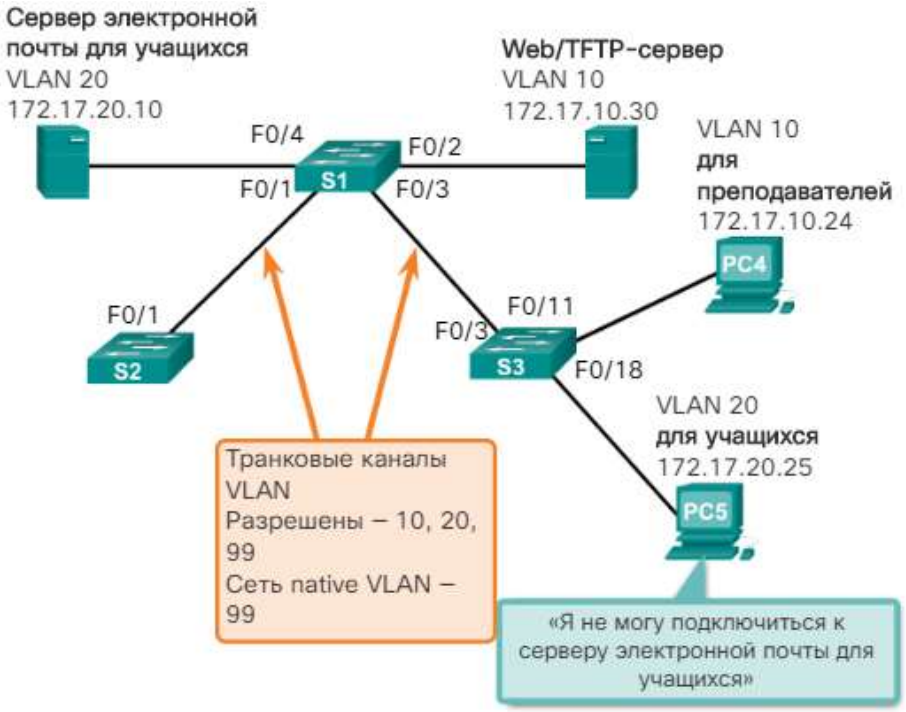


Рис. 3.4.33

Перевірте транкові порти на комутаторі S1 за допомогою команди **show interfaces trunk**, як показано на рис. 3.35. Команда **show interfaces trunk** - це чудовий інструмент для виявлення поширених проблем в транкових каналах. Ця команда вказує, що інтерфейс F0/3 на комутаторі S3 був правильно налаштований для дозволу мереж VLAN 10, 20 і 99. Перевірка інтерфейсу F0/3 на комутаторі S1 виявляє, що інтерфейси F0/1 і F0/3 дозволяють тільки мережі VLAN 10 і 99. Хтось оновив документацію, але забув переналаштувати порти на комутаторі S1.

```
S3# show interfaces trunk
Port  Mode  Encapsulation  Status    Native vlan
Fa0/3 on    802.1q         trunking  99
Port  Vlans allowed on trunk
Fa0/3 10,20,99
Port  Vlans allowed and active in management domain
Fa0/3 10,20,99
Port  Vlans in spanning tree forwarding state and not
pruned
Fa0/3 10,20,99
```

Выходные данные на коммутаторе S1

```
S1# show interfaces trunk
Port        Mode    Encapsulation  Status    Native vlan
Fa0/1       on        802.1q       trunking      99
Fa0/3       on        802.1q       trunking      99
Port     Vlans allowed on trunk
Fa0/1    10,99
Fa0/3    10,99
…
S1#
```

Рис. 3.4.34

Переналаштуйте порти F0/1 і F0/3 на комутаторі S1 за допомогою команди **switchport trunk allowed vlan** 10,20,99, як показано на рис. 3.36. Вихідні дані показують, що мережі VLAN 10, 20 і 99 тепер додані до портів F0/1 і F0/3 комутатора S1. Підключення комп'ютера PC5 до сервера електронної пошти student по IPv4-адресою 172.17.20.10 було відновлено.

```
S1# config terminal
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1(config-if)# interface f0/3
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1# show interfaces trunk
Port        Mode   Encapsulation  Status    Native vlan
Fa0/1       on        802.1q      trunking      99
Fa0/3       on        802.1q      trunking      99
Port     Vlans allowed on trunk
Fa0/1    10,20,99
Fa0/3    10,20,99
…
```

Выходные данные на компьютере PC5

```
PC5> ping 172.17.20.10
Pinging 172.17.20.10 with 32 bytes of data:
Reply from 172.17.20.10: bytes=32 time=147ms TTL=128
…
```

Рис. 3.4.35

Мережі VLAN використовуються для сегментації комутованих мереж. Комутатори 2-го рівня, наприклад Catalyst 2960, можна налаштувати для роботи з більш ніж 4 тисячами мереж VLAN. Мережа VLAN - це домен широкомовного розсилання, тому комп'ютери в різних мережах VLAN не можуть обмінюватися даними без допомоги пристроїв маршрутизації. Можливості протоколів IPv4 та IPv6 на комутаторах 2-го рівня вельми обмежені. Ці пристрої не можуть виконувати функцію динамічної маршрутизації. Хоча комутатори 2-го рівня володіють розширеними функціями IP, наприклад можливістю виконувати статичну маршрутизацію, цього недостатньо для обслуговування такого великого числа мереж VLAN.

Будь-який пристрій, що підтримує маршрутизацію 3-го рівня, наприклад маршрутизатор або багаторівневий комутатор, можна використовувати для виконання основних функцій маршрутизації. Незалежно від використовуваного пристрою, процес пересилання мережевого трафіку з однієї VLAN в іншу з використанням маршрутизації називають маршрутизацією між VLAN.

Існують три варіанти маршрутизації між VLAN:

- Застарілий метод маршрутизації між VLAN.
- Конфігурація ROS (Router-on-a-stick)
- Комутація 3-го рівня з використанням SVI.

Примітка. У цьому розділі описано перші два варіанти. Комутація 3-го рівня з використанням SVI не розглядається в рамках даного посібника.

Застарілі методи маршрутизації між VLAN. Історично першим рішенням для маршрутизації між VLAN стало використання маршрутизаторів з

декількома фізичними інтерфейсами. Кожен інтерфейс повинен був бути підключений до окремої мережі і налаштований з певною сіткою.

При такому застарілому підході маршрутизація між VLAN виконується шляхом підключення різних фізичних інтерфейсів маршрутизатора до різних фізичних портів комутатора. Порти комутатора, підключені до маршрутизатора, переводяться в режим доступу, а кожен фізичний інтерфейс призначається окремої VLAN. Кожен інтерфейс маршрутизатора може приймати трафік з VLAN, пов'язаної з інтерфейсом комутатора, до якого вона підключена, і трафік можна направляти в інші VLAN, підключені до інших інтерфейсів.

Примітка. Цей метод маршрутизації між VLAN не є ефективним і тепер рідше реалізується в комутованих мережах.

Маршрутизація між мережами VLAN з використанням методу router-on-a-stick. На відміну від традиційного методу маршрутизації між VLAN, який задіює кілька фізичних інтерфейсів маршрутизатора і комутатора, більш поширений і сучасний метод маршрутизації між VLAN цього не вимагає. Замість цього на деяких маршрутизаторах ПЗ дозволяє налаштовувати інтерфейс маршрутизатора в якості транка. Це означає, що для маршрутизації пакетів між декількома VLAN на маршрутизаторі і комутаторі потрібно тільки один фізичний інтерфейс.

Метод Router-on-a-Stick - це такий тип конфігурації маршрутизатора, при якому один фізичний інтерфейс маршрутизує трафік між кількома VLAN. Як видно на рис. 3.37, маршрутизатор підключений до комутатора S1 за допомогою одного фізичного мережевого підключення (транка).

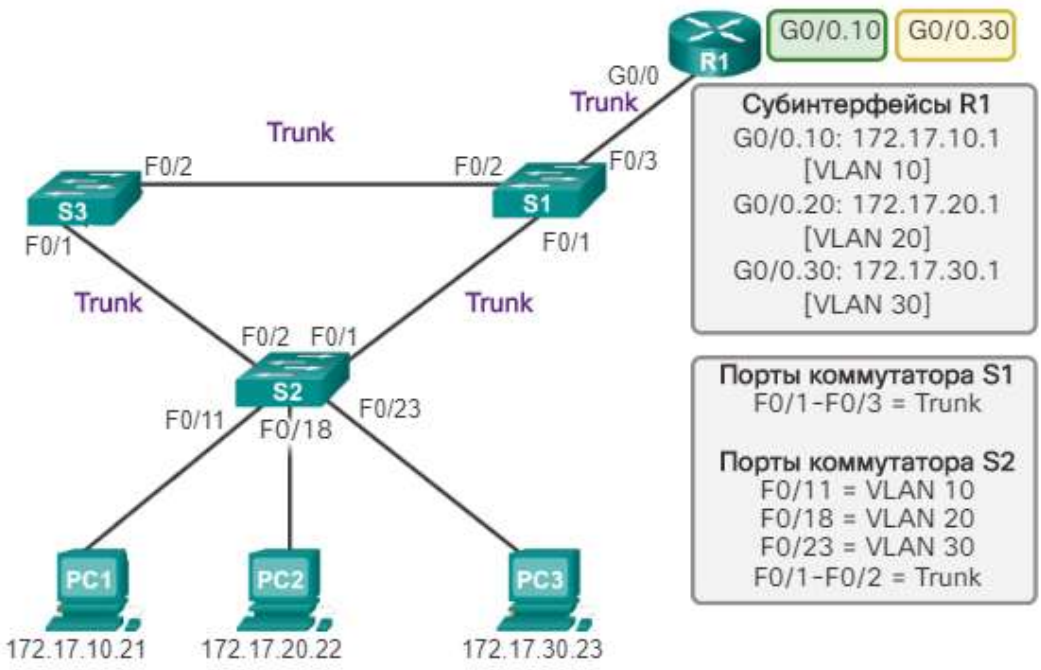


Рис. 3.4.36

Інтерфейс маршрутизатора налаштовується для роботи в якості транкового каналу і підключається до порту комутатора, який налаштований в режимі транка. Маршрутизатор виконує маршрутизацію між VLAN, приймаючи на магістральному інтерфейсі трафік з тегом VLAN, що надходить від суміжного комутатора, і потім за допомогою підлеглих інтерфейсів перенаправляючи його

між VLAN. Потім вже змаршрутизований трафік надсилається з цього ж фізичного інтерфейсу з міткою VLAN, відповідної VLAN призначення.

Підінтерфейси - це програмні віртуальні інтерфейси, пов'язані з одним фізичним інтерфейсом. Підінтерфейси налаштовуються в програмному забезпеченні маршрутизатора, і кожному підінтерфейсу призначаються IP-адреса і VLAN. Для полегшення логічної маршрутизації підінтерфейсів налаштовуються для різних підмереж, відповідних призначеним ним VLAN. Після прийняття рішення про маршрутизації на основі мережі призначення VLAN кадрів даних присвоюються мітки VLAN, після чого вони відправляються назад на фізичний інтерфейс.

Примітка. Маршрутизація між VLAN з використанням методу router-on-a-stick не масштабується при роботі більше 50 мереж VLAN.

Налаштування маршрутизації між VLAN з використанням застарілого методу: для реалізації застарілого методу маршрутизації між VLAN маршрутизатори повинні мати кілька фізичних інтерфейсів. Для маршрутизації кожен фізичний інтерфейс маршрутизатора повинен бути підключений до окремої VLAN. Крім того, на кожному інтерфейсі налаштовується IPv4-адрес з тієї підмережі, яка відповідає підключеної до нього VLAN. Завдяки налаштування IPv4-адрес на фізичних інтерфейсах мережеві пристрої, підключені до кожної з VLAN, можуть обмінюватися даними з маршрутизатором за допомогою фізичного інтерфейсу, підключеного до тієї ж VLAN. У цій конфігурації мережеві пристрої можуть використовувати маршрутизатор в якості шлюзу для доступу до пристроїв, підключеним до інших VLAN.

У процесі відправки повідомлення пристрій-джерело має визначити, чи знаходиться адресат в локальній або ж у віддаленій мережі. Для цього пристрій порівнює IPv4-адреси джерела і призначення, застосовуючи до них маску підмережі. Встановивши, що IPv4-адрес призначення знаходиться у віддаленій мережі, пристрій-джерело має визначити, куди воно повинно переслати пакет, щоб він досяг пристрою призначення. Пристрій-джерело перевіряє локальну таблицю маршрутизації, щоб визначити, куди слід відправити дані. Пристрої використовують свій шлюз за замовчуванням в якості адреси призначення на другому рівні для всього трафіку, який повинен покинути локальну мережу. Шлюз за замовчуванням - це маршрут, який пристрій використовує, коли у нього немає явно визначеного маршруту до мережі призначення. IPv4-адрес інтерфейсу маршрутизатора в локальній підмережі працює в якості шлюзу для пристрою-відправника.

Після того як пристрій-джерело визначило, що пакет повинен пройти через локальний інтерфейс маршрутизатора у підключеній мережі VLAN, воно відправляє ARP-запит, щоб визначити MAC-адреса інтерфейсу локального маршрутизатора. Після відправки маршрутизатором ARP-відповіді пристрою-джерела воно може використовувати MAC-адреса маршрутизатора для формування кадру перед його відправкою в мережу.

Оскільки в Ethernet-кадрі в якості MAC-адресу призначення вказана адреса інтерфейсу маршрутизатора, комутатор точно знає, на який порт потрібно відправити трафік, щоб він досяг інтерфейсу маршрутизатора в даній VLAN. Коли маршрутизатор отримує кадр, він видаляє MAC-адрес джерела і пристрої

призначення, щоб перевірити IPv4-адрес призначення пакета. Маршрутизатор порівнює адресу призначення з записами в своїй таблиці маршрутизації, щоб визначити, куди йому слід переслати дані, щоб вони досягли свого пункту призначення. Якщо маршрутизатор визначає, що мережа призначення є локально підключеною мережею, як у випадку з маршрутизацією між VLAN, то маршрутизатор відправляє ARP-запит з того інтерфейсу, який фізично підключений до VLAN призначення. У відповідь пристрій призначення відправляє маршрутизатора свій MAC-адреса, який маршрутизатор згодом використовує для формування кадру. Потім маршрутизатор відправляє одноадресний трафік на комутатор, який пересилає його на той порт, до якого підключено пристрій призначення.

Незважаючи на те що маршрутизація між VLAN відбувається за кілька кроків, насправді обмін даними між двома пристроями з різних VLAN через маршрутизатор займає частку секунди.

Налаштування комутатора при використанні застарілого методу маршрутизації між VLAN

Налаштування при використанні застарілого методу маршрутизації між VLAN слід починати з настройки комутатора.

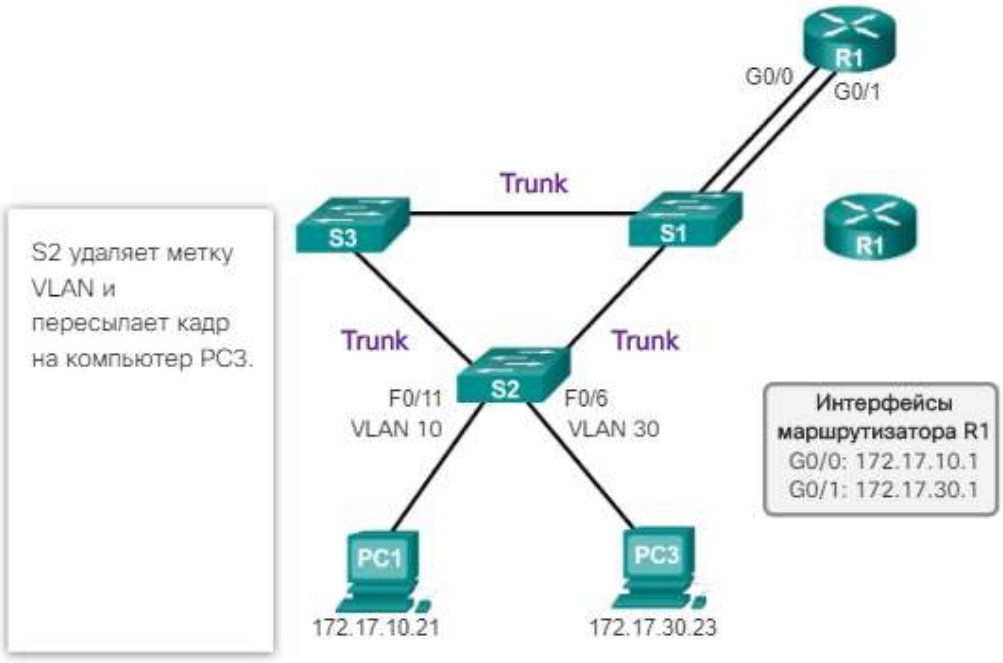


Рис. 3.4.37

Як показано на малюнку, маршрутизатор R1 підключений до портів комутатора F0 4 і F0/5, які налаштовані для VLAN 10 і 30 відповідно.

Для створення мереж VLAN використовуйте команду режиму глобальної настройки **vlan vlan_id**. У цьому прикладі мережі VLAN 10 і 30 були створені на комутаторі S1. Після створення мереж VLAN порти комутатора призначаються відповідним VLAN. Команда **switchport access vlan vlan_id** виконується для кожного інтерфейсу, до якого підключається маршрутизатор, з режиму інтерфейсної настройки на комутаторі.

У нашому прикладі інтерфейси F0/4 і F0/11 були призначені мережі VLAN 10 за допомогою команди **switchport access vlan 10**. Таким же чином

інтерфейси F0/5 і F0/6 на комутаторі S1 були призначені мережі VLAN 30 (рис. 3.39).

Нарешті, щоб конфігурація не була втрачена після перезавантаження комутатора, виконується команда **copy running-config startup-config**. Після цього поточна конфігурація зберігається в завантажувальну конфігурацію.

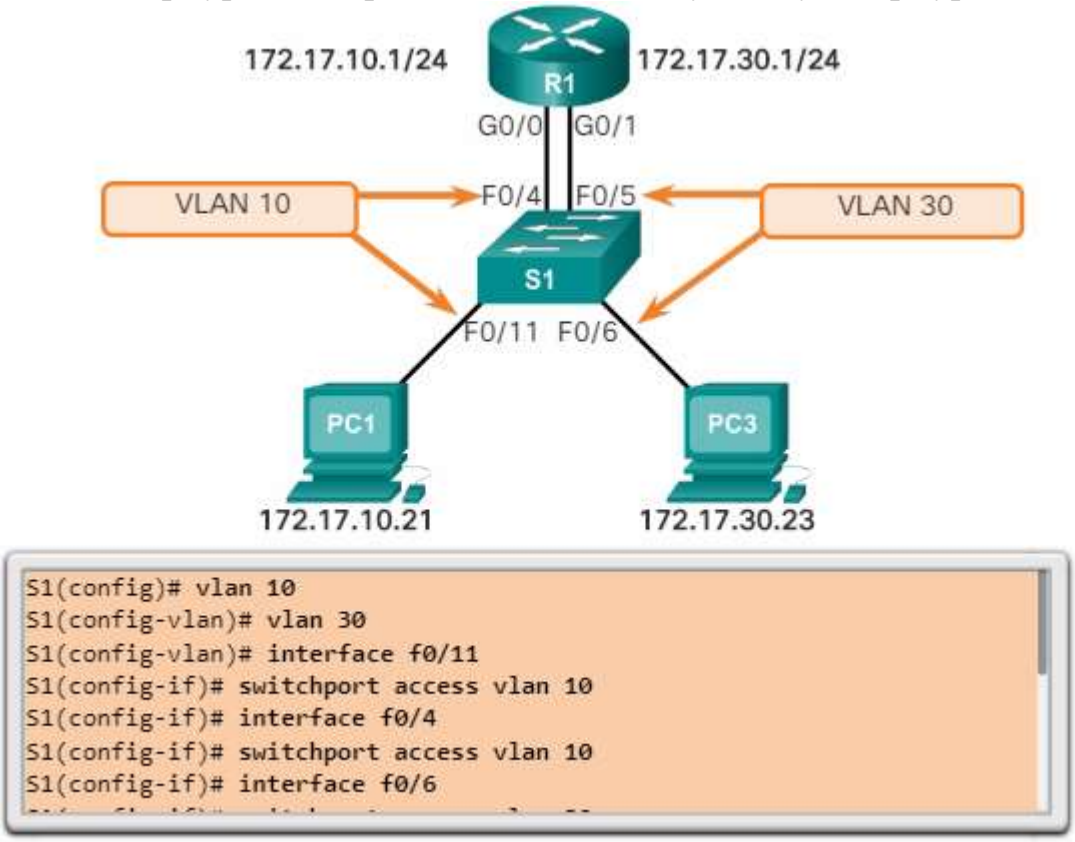


Рис. 3.4.38

Тепер маршрутизатор можна налаштувати для виконання маршрутизації між VLAN.

Інтерфейси маршрутизатора налаштовуються аналогічно тому, як інтерфейси VLAN налаштовуються на комутаторах. Щоб налаштувати конкретний інтерфейс, з режиму глобальної конфігурації перейдіть в режим конфігурації інтерфейсу.

Як показано на рис. 3.40, для кожного інтерфейсу налаштований IPv4-адрес за допомогою команди ip address IP-адреса маска_подсеті в режимі інтерфейсної настройки.

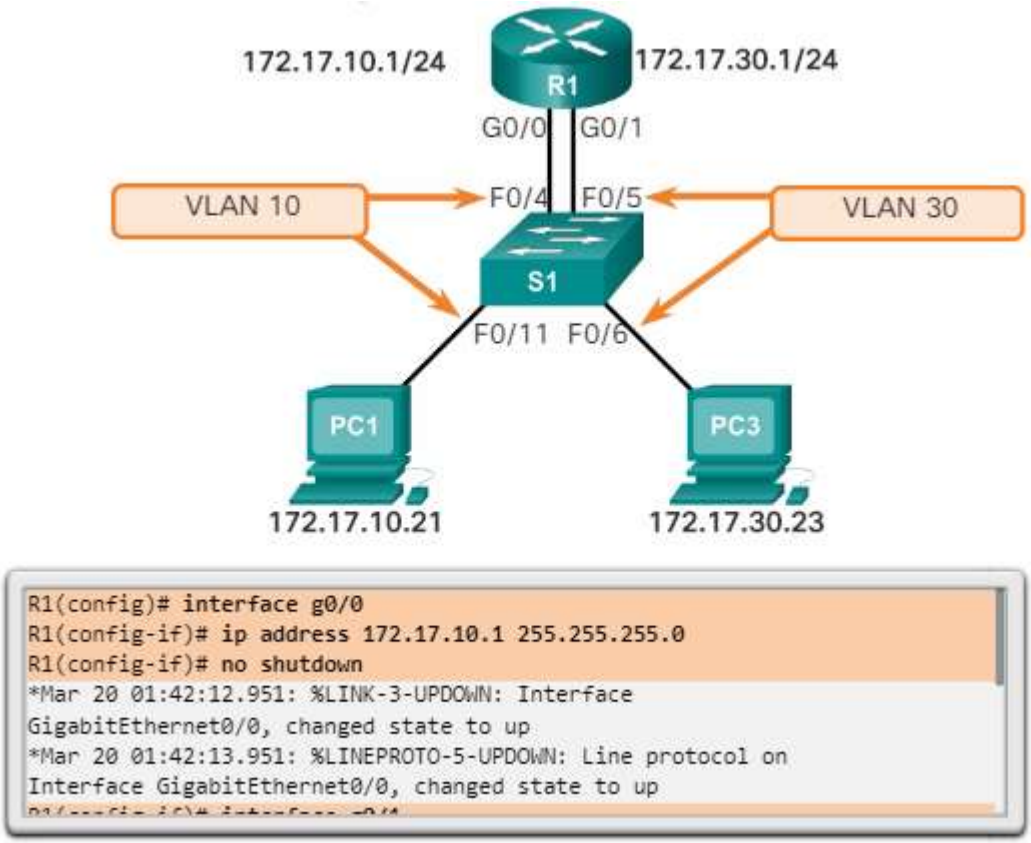


Рис. 3.4.39

В даному прикладі інтерфейс G0/0 налаштований з IPv4-адресою 172.17.10.1 і маскою підмережі 255.255.255.0 за допомогою **команди ip address 172.17.10.1 255.255.255.0.**

Інтерфейси маршрутизатора відключені за замовчуванням і перед використанням повинні бути включені за допомогою команди **no shutdown**. Після виконання команди **no shutdown** з'явиться повідомлення про те, що стан інтерфейсу змінився на **up**. Це вказує на те, що інтерфейс включений (рис. 3.41).

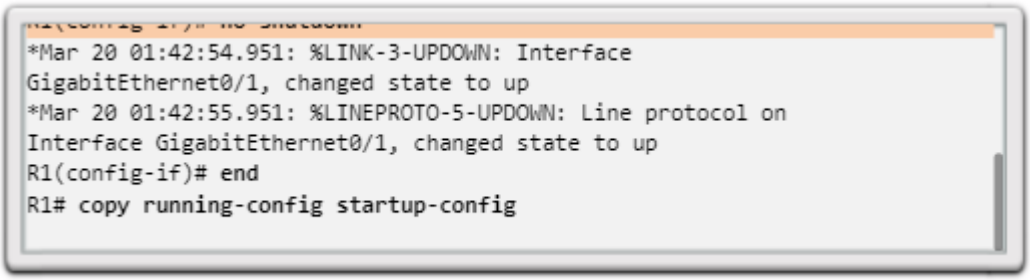


Рис. 3.41 Стан інтерфейсу включено **up**

Процедуру включення слід повторити для всіх інтерфейсів маршрутизатора. Для здійснення маршрутизації кожен інтерфейс маршрутизатора повинен бути в своїй підмережі. У цьому прикладі інший інтерфейс маршрутизатора, G0/1, був налаштований для використання IPv4-адреси 172.17.30.1, який знаходиться в іншій підмережі, ніж інтерфейс G0/0.

Після призначення IPv4-адрес фізичним інтерфейсів і активації інтерфейсів маршрутизатор готовий для виконання маршрутизації між VLAN.

Перевірте таблицю маршрутизації, користуючись командою **show ip route**.

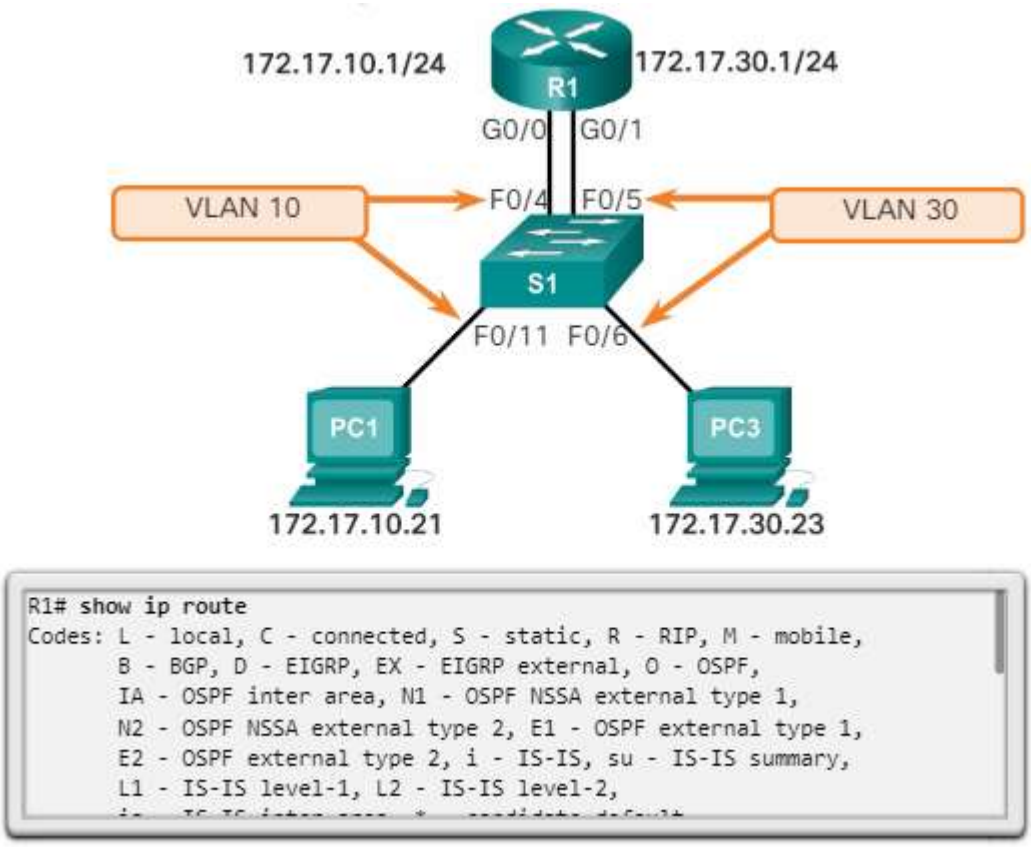


Рис. 3.4.40

На рис. 3.42 в таблиці маршрутизації відображені два маршрути. Один маршрут веде до підмережі 172.17.10.0, яка підключена до локального інтерфейсу G0/0. Інший маршрут веде до підмережі 172.17.30.0, яка підключена до локального інтерфейсу G0/1. Маршрутизатор використовує цю таблицю маршрутизації, щоб визначити, куди відправляти одержуваний трафік. Наприклад, якщо маршрутизатор отримує на інтерфейсі G0/0 пакет, який призначений для вузла з підмережі 172.17.30.0, маршрутизатор визначить, що для досягнення вузлів в підмережі 172.17.30.0 йому потрібно відправити пакет з інтерфейсу G0/1.

Зверніть увагу на букву C зліва від кожної із записів маршрутів для мереж VLAN. Дана буква вказує, що даний маршрут є локальним маршрутом для підключеного інтерфейсу, що також зазначено в запису маршруту.

Застарілий метод маршрутизації між VLAN, що використовує фізичні інтерфейси, має великі обмеження. Маршрутизатори оснащені обмеженою кількістю фізичних інтерфейсів для підключення до різних VLAN. У міру зростання кількості VLAN в мережі, що вимагають по одному фізичному інтерфейсу на кожну VLAN, кількість вільних інтерфейсів маршрутизатора швидко зменшується. Саме тому в великих мережах часто використовуються транкові канали та підінтерфейси. Створення транка дозволяє одному фізичному інтерфейсу маршрутизовувати трафік між кількома VLAN. Подібний метод маршрутизації називається **router-on-a-stick**. Його суть полягає у використанні віртуальних підінтерфейсів для подолання обмежень в кількості інтерфейсів маршрутизатора.

Підінтерфейси - це програмні віртуальні інтерфейси, які призначаються фізичним інтерфейсам. Кожному підлеглому інтерфейсу окремо призначаються

IP-адреса і довжина префіксу. Це дозволяє одному фізичному інтерфейсу працювати одночасно в декількох логічних мережах.

Примітка. Термін «довжина префікса» може використовуватися для позначення маски підмережі IPv4 в зв'язці з IPv4-адресою і довжини префіксу IPv6 в зв'язці з IPv6-адресою.

Під час налаштування маршрутизації між VLAN з використанням методу router-on-a-stick фізичний інтерфейс маршрутизатора повинен бути підключений до транкового каналу суміжного комутатора. На маршрутизаторі підінтерфейси створюються для кожної окремої мережі VLAN. Кожному підінтерфейсу призначається IP-адреса відповідно до його підмережі або мережі VLAN. Крім того, у підінтерфейс вноситься, мітку якої мережі VLAN вів буде присвоювати кадрам. Таким чином, маршрутизатор може відокремлювати трафік з кожного підлеглого інтерфейсу в міру його проходження по магістральному каналу назад на комутатор.

З функціональної точки зору, метод router-on-a-stick мало чим відрізняється від роботи маршрутизації між VLAN за застарілим методом. Відмінність полягає в тому, що при використанні методу router-on-a-stick замість фізичних інтерфейсів використовуються підінтерфейси одного фізичного інтерфейсу.

На рисунку 3.43 комп'ютер PC1 планує обмін даними з комп'ютером PC3. PC1 знаходиться в мережі VLAN 10, а PC3 - в мережі VLAN 30. Для обміну даними між PC1 і PC3 дані комп'ютера PC1 повинні бути спрямовані через маршрутизатор R1 за допомогою підінтерфейсів.

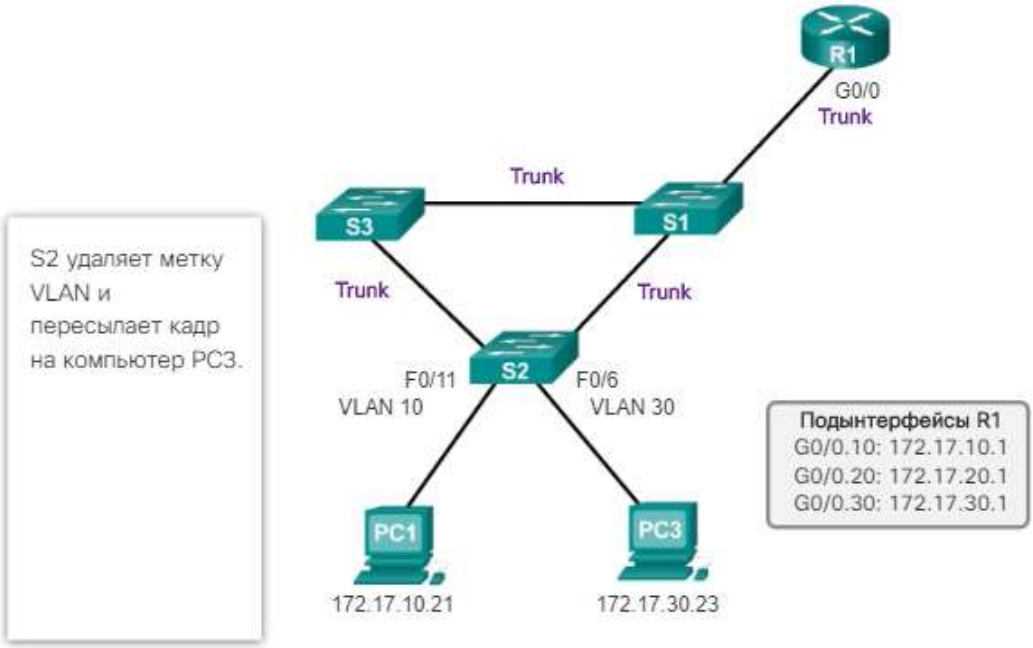


Рис. 3.4.41

Використання транкових каналів і підінтерфейсів знижує кількість використовуваних портів маршрутизаторів і комутаторів. Це дозволяє не тільки заощадити фінансові кошти, але і спростити процес налаштування. В результаті можливості підінтерфейсів маршрутизатора дозволяють використовувати набагато більшу кількість мереж VLAN, ніж при конфігурації з одним фізичним інтерфейсом на кожну VLAN.

Для того щоб включити маршрутизацію між VLAN з використанням методу router-on-a-stick, необхідно активувати транковий зв'язок на порту комутатора, підключеному до маршрутизатора.

На рис. 3.44 маршрутизатор R1 підключений до комутатора S1 через транковий порт F0/5. На комутаторі S1 додаються VLAN 10 і 30.

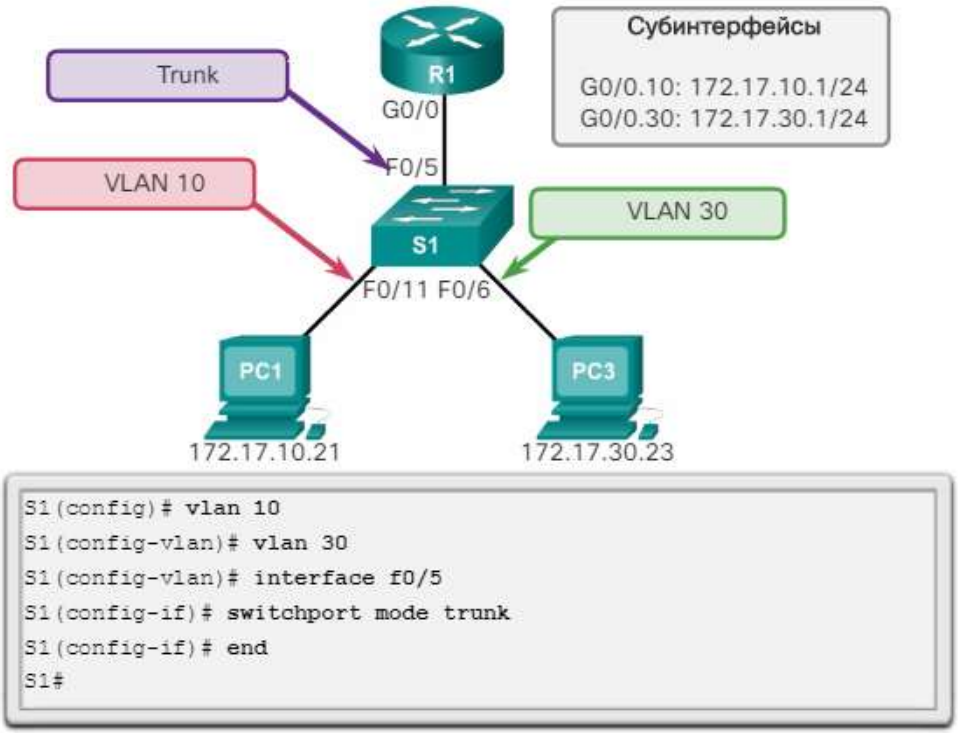


Рис. 3.4.42

Оскільки порт комутатора F0/5 налаштований як транковий порт, він не вимагає призначення будь-якої мережі VLAN. Щоб налаштувати комутаційний порт F0/5 в якості магістрального, виконайте **команду switchport mode trunk** в режимі інтерфейсної настройки для порту F0/5.

Тепер маршрутизатор можна налаштувати для виконання маршрутизації між VLAN.

Метод router-on-a-stick: настройка підінтерфейса маршрутизатора

Процедури настроювання маршрутизатора при використанні методу Router-on-a-Stick і застарілого методу маршрутизації між VLAN розрізняються. На рис. 3.45 показано, що налаштовується кілька підінтерфейсів.

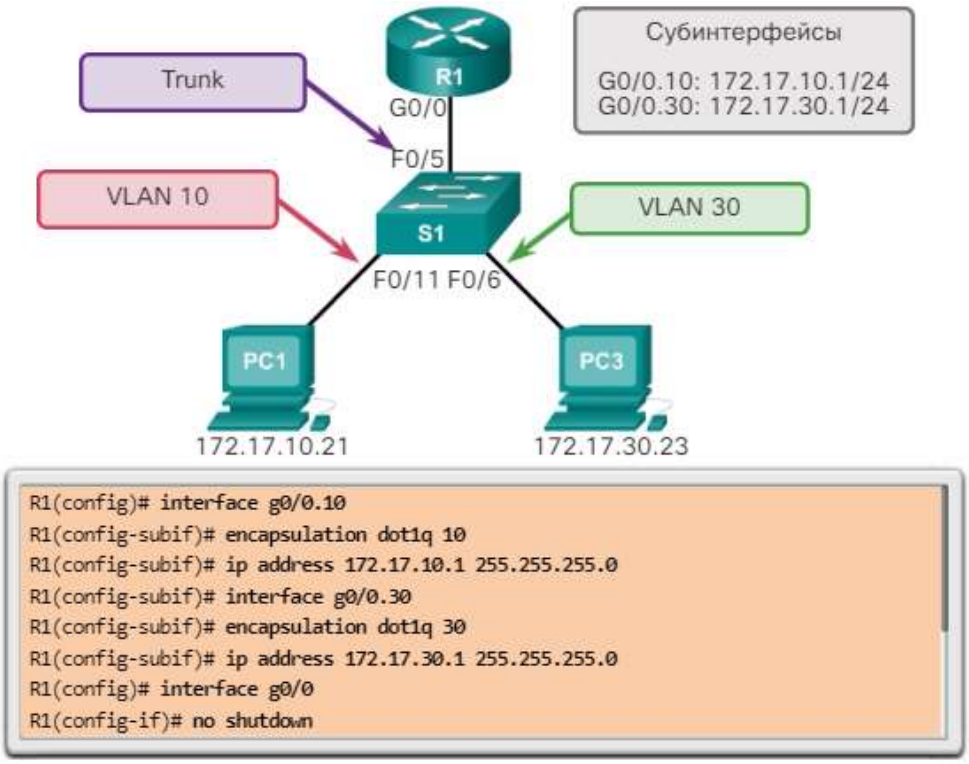


Рис. 3.4.43

Кожен підлеглий інтерфейс створюється за допомогою команди режиму глобальної настройки **interface** ідентіфікатору_інтерфейсу. Синтаксис для підлеглих інтерфейсів наступний: спочатку вказується фізичний інтерфейс, в даному випадку g0/ 0, потім точка і номер підлеглого інтерфейсу. Як показано на рис. 3.46, підлеглий інтерфейс GigabitEthernet0/0.10 створюється за допомогою команди режиму глобальної настройки **interface g0/0.10**. Номер підлеглого інтерфейсу зазвичай задається відповідно до номером VLAN.

```
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 Interface GigabitEthernet0/0, changed state to up
```

Рис. 3.4.44

Перед призначенням підлеглому інтерфейсу IP-адреси цей інтерфейс необхідно налаштувати для роботи в конкретній мережі VLAN за допомогою команди **encapsulation dot1q vlan_id.** В даному прикладі підінтерфейс G0/0.10 призначений мережі VLAN 10.

Примітка. До цієї команди можна додати ключове слово native для настройки мережі VLAN з нетегірованим трафіком стандарту IEEE 802.1Q. В даному прикладі ключове слово nativene використовувалося, щоб в якості VLAN з нетегірованим трафіком за замовчуванням збереглася VLAN 1.

Далі призначається IPv4-адрес для підлеглого інтерфейсу за допомогою команди режиму настройки інтерфейсу **ip address** IP-адреса маска_підмережі. В

даному прикладі підлеглому інтерфейсу G0/0.10 призначається IPv4-адрес 172.17.10.1 за допомогою команди **ip address 172.17.10.1 255.255.255.0**

Процедуру слід повторити для всіх підінтерфейсів маршрутизатора, необхідних для маршрутизації між мережами VLAN, налаштованими в мережі. Для здійснення маршрутизації кожному підінтерфейсу маршрутизатора необхідно призначити IP-адрес в своїй підмережі. Наприклад, інший підлеглий інтерфейс маршрутизатора, G0/0.30, налаштований для використання IPv4-адреси 172.17.30.1, який знаходиться в іншій підмережі, ніж підлеглий інтерфейс G0/0.10.

Після включення фізичного інтерфейсу налаштовані підінтерфейси будуть автоматично включені. Підінтерфейси не обов'язково включати за допомогою команди **no shutdown** на рівні режиму конфігурації підлеглого інтерфейсу ПО Cisco IOS.

Якщо відключити фізичний інтерфейс, то всі підлеглі інтерфейси також відключаються. В даному прикладі команда **no shutdown** вводиться в режимі інтерфейсної настройки для інтерфейсу G0/0, в результаті чого включаються всі налаштовані підлеглі інтерфейси.

Адміністратор може відключити окремі підлеглі інтерфейси за допомогою команди **shutdown**. Крім того, підлеглі інтерфейси можна включити окремо за допомогою команди **no shutdown** в режимі конфігурації підінтерфейсу.

Метод router-on-a-stick: перевірка підінтерфейсів

За замовчуванням маршрутизатори Cisco налаштовані для маршрутизації трафіку між локальними підінтерфейсами. У зв'язку з цим функцію маршрутизації не потрібно активувати індивідуально.

На рис. 3.47 команда **show vlan** служить для виведення інформації про підлегли інтерфейси VLAN в Cisco IOS. У вихідних даних нижче відображається інформація про двох підінтерфейсах з VLAN: GigabitEthernet0/0.10 і GigabitEthernet0/0.30.

```
R1# show vlan
<Данные опущены>
Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.10

  Protocols Configured:  Address:     Received:   Transmitted:
          IP             172.17.10.1         11             18
<Данные опущены>
Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.30

  Protocols Configured:  Address:     Received:   Transmitted:
          IP             172.17.30.1         11              8
<Данные опущены>
```

Рис. 3.4.45

Перевірте таблицю маршрутизації, користуючись командою **show ip route**

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP,M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
       L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default,
       U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP,
       l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

   172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
C     172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L     172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C     172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L     172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

Рис. 3.4.46

Зазначені в таблиці маршрути пов'язані з певними підінтерфейсами, а не окремими фізичними інтерфейсами. Таблиця маршрутизації містить два маршрути. Один маршрут веде до підмережі 172.17.10.0, яка підключена до локального підінтерфейсу G0/0.10. Інший маршрут веде до підмережі 172.17.30.0, яка підключена до локального підінтерфейсу G0/0.30. Маршрутизатор використовує цю таблицю маршрутизації, щоб визначити, куди відправляти одержуваний трафік. Наприклад, якщо на підінтерфейсу G0/0.10 маршрутизатор отримав пакет, призначений для підмережі 172.17.30.0, маршрутизатор визначить, що для досягнення вузлів в мережі 172.17.30.0 йому потрібно відправити пакет з підінтерфейсу G0/0.30.

Наступний крок після настройки маршрутизатора і комутатора для маршрутизації між VLAN - перевірка з'єднання між вузлами. Можливість доступу до пристроїв у віддалених VLAN можна перевірити за допомогою команди **ping** (рис. 3.49).

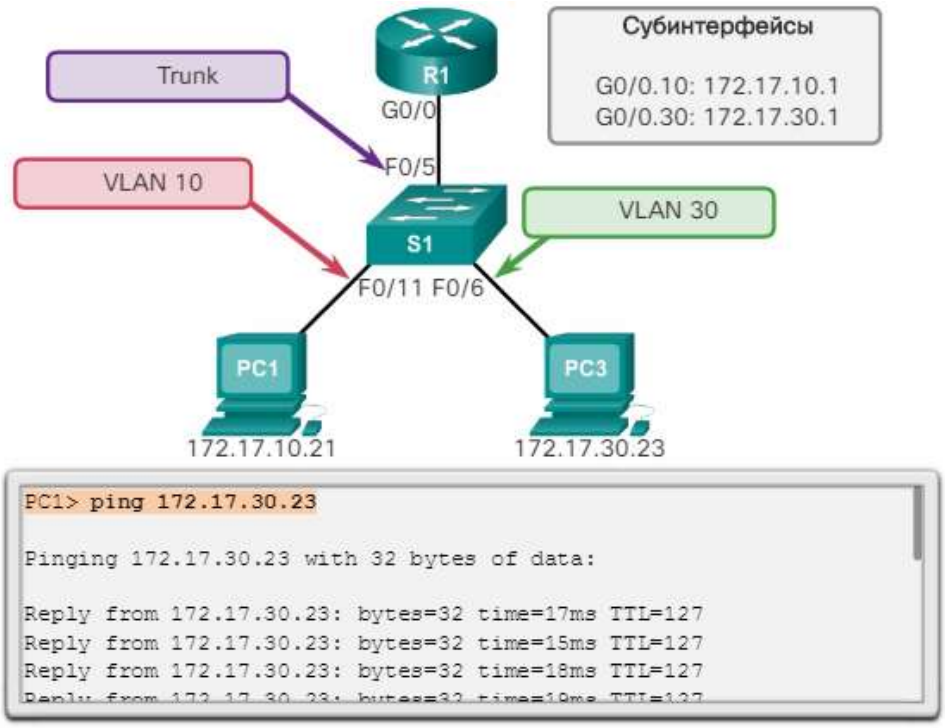


Рис. 3.4.47

У прикладі на даному малюнку команди ping і tracert ініціюються з комп'ютера PC1 за адресою призначення PC3.

Перевірка ехо-запитів.

Команда **ping** відправляє ехо-запит ICMP за адресою призначення. Коли вузол отримує ехо-запит ICMP, він відправляє ехо-відповідь ICMP, щоб підтвердити отримання ехо-запиту ICMP. Команда **ping** обчислює час, який минув між відправкою ехо-запиту і отриманням ехо-відповіді. Отримане значення використовується для визначення затримки з'єднання. Успішне отримання відповіді підтверджує наявність шляху між пристроєм-відправником і пристроєм одержувача.

Перевірка маршруту командою tracert

Команда **tracert** - це корисний інструмент для підтвердження існування шляху між двома пристроями. У системах UNIX подібний інструмент називається **traceroute**. **Tracert** також використовує протокол ICMP для визначення використовуваного шляху, але при цьому використовуються ехо-запити ICMP зі значеннями запропонованого часу життя, які визначаються в кадрі.

Значення часу життя визначає точну кількість переходів до маршрутизатора, яке може виконати ехо-запит ICMP. Перший ехо-запит ICMP відправляється з таким значенням часу життя (TTL), щоб воно закінчилося на першому маршрутизаторе по шляху до пристрою призначення.

Коли час життя ICMP ехо-запиту закінчується, від маршрутизатора на пристрій-джерело відправляється ICMP-повідомлення. Пристрій записує відповідь від маршрутизатора і відправляє інший ехо-запит ICMP, однак зі збільшеним значенням часу життя. Це дозволяє ехо-запитом ICMP пройти перший маршрутизатор і досягти другого пристрою на шляху до пристрою призначення. Далі ця процедура повторюється рекурсивно, поки ехо-запит ICMP не пройде весь шлях до пристрою призначення. Після виконання команди

tracert відображається список інтерфейсів маршрутизатора, по яких ехо-запит ICMP досяг по шляху до місця призначення.

В вищенаведеному прикладі команда **ping** змогла відправити луна-запит ICMP на IP-адреса комп'ютера PC3. Крім того, команда **tracert** підтверджує, що шлях до комп'ютера PC3 проходить через IP-адресу підлеглого інтерфейсу 172.17.10.1 маршрутизатора R1 (рис. 3.50).

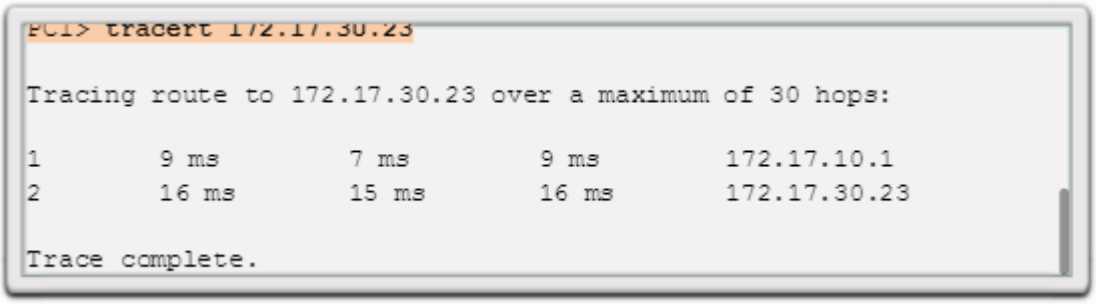


Рис. 3.4.48

У цьому розділі ми вивчили основи мереж VLAN. Мережі VLAN ґрунтуються не на фізичних, а на логічних підключених. Мережі VLAN - це механізм, що дозволяє мережевим адміністраторам створювати логічні широкомовні домени, які здатні охоплювати один або кілька комутаторів незалежно від фізичного відстані. Ця функція корисна для зменшення розміру доменів широкомовної розсилки або для логічного об'єднання груп або користувачів, які не обов'язково повинні фізично знаходитися в одному місці.

Голосова VLAN

Команда switchport access vlan використовується для створення мережі VLAN на комутаторі. Наступний крок після створення мережі VLAN - призначення портів мереж VLAN. Команда show vlan brief показує призначення VLAN і тип приналежності для всіх комутаційних портів. Кожній VLAN повинна відповідати IP-сіть.

Використовуйте команду show vlan, щоб перевірити, чи належить порт очікуваної VLAN. Якщо порт призначений невірної VLAN, використовуйте команду switchport access vlan для коригування приналежності VLAN. Використовуйте команду show mac address-table для перевірки адрес, отриманих на певному комутаційному порте, і VLAN, призначеної цього порту.

Порт комутатора може працювати портом доступу або транкових портом. Порти доступу служать для передачі трафіку від певної VLAN, призначеної конкретному порту. Транковий порт за замовчуванням належить всім VLAN. Таким чином, він передає трафік в усі мережі VLAN.

Транкові канали VLAN спрощують взаємодію між комутаторами, передаючи трафік, пов'язаний з декількома VLAN. Тегування кадрів IEEE 802.1Q дозволяє розрізняти кадри Ethernet, пов'язані з певними VLAN в міру їх проходження по загальним транкових каналах. Щоб включити магістральні канали, використовуйте команду switchport mode trunk. Використовуйте команду show interfaces trunk для перевірки встановлення магістрального каналу між комутаторами.

Узгодження транкового каналу виконується протоколом динамічного створення транкового каналу (DTP), який діє тільки за принципом наскрізного підключення між пристроями мережі. Протокол DTP - це запатентований

протокол Cisco, який автоматично включений на комутаторах Catalyst 2960 і Catalyst 3560.

Щоб повернути комутатор до його заводських налаштувань з однією мережею VLAN за замовчуванням, використовуйте команди delete flash: vlan.dat і erase startup-config.

У цьому розділі також розглядаються настройка, перевірка і усунення неполадок мереж VLAN і магістральних каналів за допомогою Cisco IOS CLI.

Маршрутизація між VLAN - це процес маршрутизації трафіку між мережами VLAN з використанням виділеного маршрутизатора або багаторівневого комутатора. Маршрутизація між VLAN спрощує обмін даними між пристроями, ізольованими межами VLAN.

Застарілий метод маршрутизації між VLAN обумовлений доступністю фізичного порту комутатора для кожної налаштованої VLAN. Даний метод був замінений на топологію router-on-a-stick, яка покладається на зовнішній маршрутизатор з подинтерфейсах, підключеними через транкові канали до комутатора 2-го рівня. При використанні методу router-on-a-stick на кожному логічному подинтерфейсах необхідно налаштувати відповідні IP-адреси і параметри VLAN. Необхідно налаштувати транк і інкапсуляцію на маршрутизаторі і на відповідному порту комутатора.

4. Розділ Базові налаштування протоколів на прикладному рівні моделі OSI

4.1 Основи безпеки у мережах. Налаштування списків контролю доступу

Один з найважливіших навичок мережевого адміністратора - управління списками контролю доступу (ACL-списками). Списки контролю доступу (ACL) забезпечують безпеку мережі.

Фахівці з проектування мереж використовують міжмережеві екрани для забезпечення захисту мережі від несанкціонованого доступу. Міжмережеві екрани або брандмауери є апаратні або програмні рішення, спрямовані на підвищення ступеня захищеності мережі. Розглянемо як приклад заблоковану двері приміщення всередині будівлі. Завдяки блокуванню в приміщення можуть увійти тільки авторизовані особи, які мають ключ або карту доступу. Аналогічним чином міжмережевий екран фільтрує неавторизовані або потенційно небезпечні пакети, запобігаючи їх проникнення в мережу.

На маршрутизаторі Cisco можна налаштувати простий міжмережевий екран, який дозволяє фільтрувати трафік на базовому рівні за допомогою ACL-списків. Використання ACL-списків дозволяє адміністраторам зупиняти трафік або допускати в мережу тільки певний трафік.

Ця глава присвячена налаштуванню стандартних списків контролю доступу (ACL) IPv4, включаючи пошук і усунення відповідних неполадок на маршрутизаторі Cisco в складі комплексної системи безпеки. Матеріал розділу включає поради, рішення, загальні рекомендації та інструкції по застосуванню ACL-списків. Підрозділ містить уроки, інтерактивні завдання та практичні вправи, які допоможуть досконало оволодіти методами роботи зі списками контролю доступу (ACL).

ACL-список - це ряд команд IOS, що визначають, пересилає маршрутизатор пакети або скидає їх, виходячи з інформації в заголовку пакета. ACL-списки є однією з найбільш використовуваних функцій операційної системи Cisco IOS.

Залежно від конфігурації ACL-списки виконують такі завдання:

Обмеження мережевого трафіку для підвищення продуктивності мережі. Наприклад, якщо корпоративна політика забороняє відеотрафік в мережі, необхідно налаштувати і застосувати ACL-списки, що блокують даний тип трафіку. Подібні заходи значно знижують навантаження на мережу і підвищують її продуктивність.

Друге завдання ACL-списків - управління потоком трафіку. За допомогою списків контролю доступу (ACL) можна обмежити доставку маршрутних оновлень, щоб гарантувати достовірність джерел таких оновлень.

Списки контролю доступу забезпечують базовий рівень безпеки щодо доступу до мережі. ACL-списки можуть відкрити доступ до частини мережі одного вузла і закрити його для інших вузлів. Наприклад, доступ до мережі

відділу кадрів може бути обмежений і дозволений лише авторизованим користувачам.

ACL-списки здійснюють фільтрацію трафіку на основі типу трафіку. Наприклад, ACL-список може дозволяти трафік електронної пошти, але при цьому блокувати весь трафік протоколу Telnet.

Списки контролю доступу здійснюють сортування вузлів з метою визначити, чи потрібно доступу до мережних служб. За допомогою ACL-списків можна дозволяти або забороняти доступ до певних типів файлів, наприклад FTP або HTTP.

За замовчуванням ACL-списки не налаштовані на маршрутизаторі, тому маршрутизатор не фільтрує трафік. Трафік, що надходить на маршрутизатор, ґрунтується виключно на даних таблиці маршрутизації. Однак якщо ACL-список використовується на інтерфейсі, маршрутизатор виконує додаткову задачу, оцінюючи всі мережеві пакети, що проходять через інтерфейс, з метою визначення дозволу пересилання пакета.

Крім дозволу або заборони трафіку, ACL-списки можна використовувати для аналізу, пересилання чи обробки окремих видів трафіку. Наприклад, за допомогою ACL-списків можна класифікувати трафік для включення обробки даних відповідно за пріоритетом. Дана можливість ACL-списків аналогічна наявності VIP-перепустки на концерт або спортивний захід. VIP-пропуск дає обраним гостям привілеї, недоступні власникам звичайних квитків, такі як пріоритет входу або доступ в закриту зону.

На рис. 3.1.1 наводиться приклад топології з використовуваними ACL-списками.

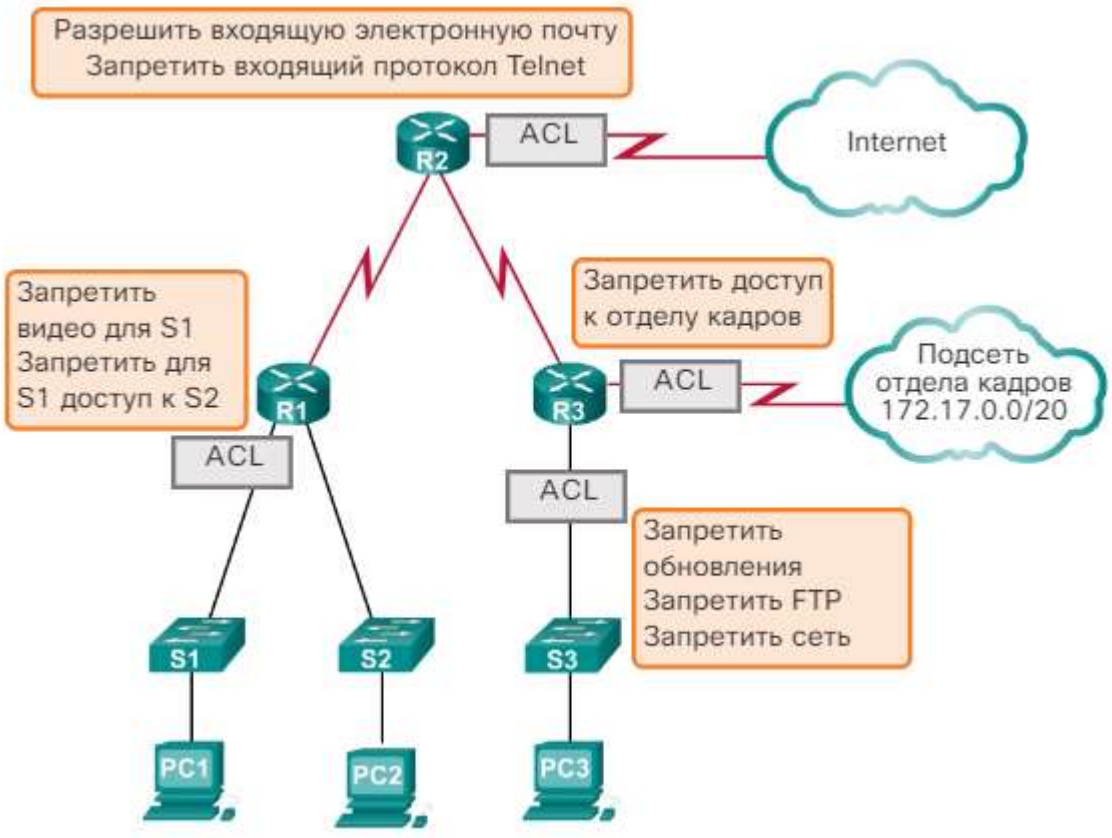


Рис. 4.1.1

Список контролю доступу ACL - це послідовний списки, які дозволяють або забороняють оператори, які ще мають назву записи контролю доступу (ACE). Записи контролю доступу також часто називають правилами ACL-списку. При проходженні мережевого трафіку через інтерфейс, де діє список контролю доступу (ACL), маршрутизатор послідовно зіставляє інформацію з пакета з кожним записом в списку контролю доступу на предмет відповідності. Цей процес називається фільтрацією пакетів.

Фільтрація пакетів забезпечує контроль доступу до мережі на основі аналізу вхідних і вихідних пакетів з подальшою переадресацією або відкиданням цих пакетів згідно із заданим критерієм. Як показано на рис. 3.1.2, фільтрація пакетів може відбуватися на рівнях 3 і 4. Стандартні списки контролю доступу (ACL) забезпечують фільтрацію тільки на рівні 3. Розширені списки контролю доступу (ACL) забезпечують фільтрацію на рівнях 3 і 4.

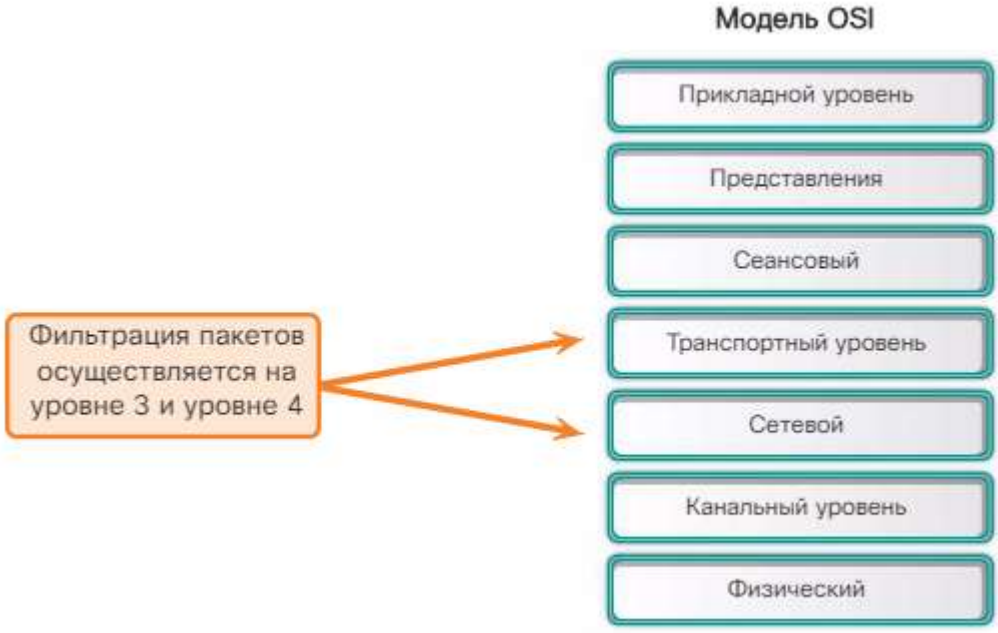


Рис. 4.1.2

У кожного запису стандартного списку контролю доступу (ACL) IPv4 міститься критерій фільтрації, в ролі якого виступає IPv4-адрес джерела. Якщо на маршрутизаторі налаштований стандартний список контролю доступу (ACL) IPv4, то, отримавши пакет, такий маршрутизатор витягує з заголовка пакета IPv4-адрес джерела. Далі маршрутизатор послідовно порівнює адресу з адресою в кожній із записів в списку контролю доступу (ACL), починаючи з першого запису. Виявивши відповідність, маршрутизатор виконує відповідну інструкцію - дозволяє або забороняє проходження пакета. При цьому інші записи в списку контролю доступу (ACL) не аналізуються. Якщо IPv4-адрес джерела не відповідає жодного запису в списку контролю доступу (ACL), такий пакет відкидається.

Останній запис в ACL-списку завжди містить непряму заборону трафіку. Ця інструкція автоматично вставляється в кінець кожного ACL-списку, хоча і не присутня в ньому фізично. Неявна заборона блокує весь трафік. Через непряму заборону ACL-список, який не містить хоча б одного дозволеного правила, заблокує весь трафік.

Списки контролю доступу визначають набір правил, що забезпечують додатковий контроль над пакетами, які приймаються інтерфейсами, транзитними пакетами, які передаються через маршрутизатор, а також пакетами, які відправляються з інтерфейсів маршрутизатора. Списки контролю доступу не застосовуються до пакетів, які створені маршрутизатором.

Як показано на рис. 3.1.3, можна налаштувати списки контролю доступу (ACL) для вхідного і вихідного трафіку.

Рис. 4.1.3

Вхідні ACL-списки - вхідні пакети обробляються перед відправкою на вихідний інтерфейс. Вхідний ACL-список ефективний, оскільки він економить ресурси на пошук маршруту, якщо пакет скидається. Якщо згідно зі списком контролю доступу (ACL) проходження пакета слід дозволити, то цей пакет маршрутизується. Вхідні списки контролю доступу (ACL) найкраще підходять для випадків, коли єдиним джерелом перевірки пакетів є мережа, підключена до вхідного інтерфейсу.

Вихідні ACL-списки - вхідні пакети маршрутизуються на вихідний інтерфейс, а потім обробляються вихідним списком контролю доступу. Вихідні ACL-списки найкраще використовувати, коли однакові фільтри застосовуються до пакетів, що надходять з безлічі вхідних інтерфейсів, перед виходом на той же вихідний інтерфейс.

Накладення шаблонної маски

ACL-списки IPv4 використовують шаблонні маски. Шаблонна маска - це рядок з 32 двозначних цифр, що використовується маршрутизатором для визначення бітів адреси, які будуть розглядатися на предмет збігу.

Як і у випадку з маскою підмережі, значення «1» і «0» в стандартній масці визначають те, яким чином будуть оброблені відповідні біти IPv4-адреси. Однак в стандартній масці ці біти використовуються для інших цілей і слідують іншим правилам.

В масці підмережі виконавчі одиниці і нулі використовуються для поділу IPv4-адреси на частини - адреса мережі, адреса підмережі та адресу хоста. У шаблонній масці виконавчі одиниці і нулі використовуються для фільтрації окремих IPv4-адрес або груп IPv4-адрес. Фільтрація дозволяє дозволити або заборонити доступ до ресурсів.

Шаблонні маски і маски підмереж розрізняються за випадковим збігом двійкових одиниць і нулів. Для збігу двійкових одиниць і нулів шаблонні маски використовують такі правила:

- Біт 0 шаблонної маски збігається з відповідним значенням біта в адресі.
- Біт 1 шаблонної маски ігнорує відповідне значення біта в адресі.

Рисунок 3.1.4 ілюструє фільтрацію IPv4-адрес за допомогою різних шаблонних масок. Розглядаючи наведений приклад, пам'ятайте, що двійковий нуль означає біт, який повинен збігатися, а двійкова одиниця - біт, який можна ігнорувати.

Рис. 4.1.4

Шаблонну маску часто називають зворотною маскою. Це пояснюється тим, що, на відміну від маски підмережі, де біт дорівнює збігом, а двійковий нуль не є збігом, в шаблонної масці все навпаки.

Використання групової маски

Таблиця на рис. 3.1.5 демонструє результати застосування шаблонної маски 0.0.255.255 до 32-бітного IPv4-адресою. Пам'ятайте, що двійковий нуль вказує на значення, яке збігається.

	Десятичный адрес	Двоичный адрес
IP-адрес для обработки	192.168.10.0	11000000.10101000.00001010.00000000
Групповая маска	0.0.255.255	00000000.00000000.11111111.11111111
Итоговый IP-адрес	192.168.0.0	11000000.10101000.00000000.00000000

Рис. 4.1.5

Примітка. На відміну від ACL-списків для IPv4, ACL-списки для IPv6 не використовують шаблонні маски. У протоколі IPv6 для вказівки того, яка частина IPv6-адреси джерела або призначення повинна збігатися, використовується довжина префіксу. Списки контролю доступу (ACL) IPv6 не розглядаються в цій книзі.

Приклади шаблонної маски: розрахунок шаблонних масок для відповідності подсетям IPv4. Розрахунок шаблонної маски може зажадати певного досвіду. На рис. 3.1.6 представлені три приклади шаблонних масок.

Пример 1

	Десятичные	Двоичные
IP-адрес	192.168.1.1	11000000.10101000.00000001.00000001
Групповая маска	0.0.0.0	00000000.00000000.00000000.00000000
Результат	192.168.1.1	11000000.10101000.00000001.00000001

Пример 2

	Десятичные	Двоичные
IP-адрес	192.168.1.1	11000000.10101000.00000001.00000001
Групповая маска	255.255.255.255	11111111.11111111.11111111.11111111
Результат	0.0.0.0	00000000.00000000.00000000.00000000

Пример 3

	Десятичные	Двоичные
IP-адрес	192.168.1.1	11000000.10101000.00000001.00000001
Групповая маска	0.0.0.255	00000000.00000000.00000000.11111111
Результат	192.168.1.0	11000000.10101000.00000001.00000000

Рис. 4.1.6

У першому прикладі шаблонної маскою передбачається, що кожен біт в IPv4-адресу 192.168.1.1 повинен точно збігатися. Умовою шаблонної маски в другому прикладі є відсутність збігів. У третьому прикладі шаблонної маски обмовляється, що будь-який вузол в мережі 192.168.1.0/24 буде збігатися.

Розрахунок шаблонних масок для відповідності діапазонами

На рис. 3.1.7 наводяться більш складний приклад. У прикладі 1 перші два октети і перші чотири біти третього октету повинні точно збігатися. Останні

чотири біти в третьому октеті і останній октет можуть бути будь-яким допустимим числом. Результатом є маска, яка визначає діапазон мереж від 192.168.16.0 до 192.168.31.0.

Пример 1

	Десятичные	Двоичные
IP-адрес	192.168.16.0	11000000.10101000.00010000.00000000
Групповая маска	0.0.15.255	00000000.00000000.00001111.11111111
Итоговый диапазон	От 192.168.16.0 до 192.168.31.255	От 11000000.10101000.00010000.00000000 до 11000000.10101000.00011111.11111111

Пример 2

	Десятичные	Двоичные
IP-адрес	192.168.1.0	11000000.10101000.00000001.00000000
Групповая маска	0.0.254.255	00000000.00000000.11111110.11111111
Результат	192.168.1.0	11000000.10101000.00000001.00000000
	Все нечётные подсети в основной сети 192.168.0.0	

Рис. 4.1.7

У прикладі 2 показана шаблонна маска, з збігами в перших двох октетах і останньому біті третього октету. Останній октет і перші сім біт в третьому октеті можуть бути будь-яким допустимим числом. Результатом є маска, що дозволяє або забороняє всі вузли з непарних підмереж основної мережі 192.168.0.0.

Розрахунок шаблонних масок може бути пов'язаний з певними труднощами. Простим способом є віднімання маски підмережі з 255.255.255.255.

Розрахунок шаблонної маски. приклад 1 (рис. 3.1.8)

Припустимо, що в першому прикладі на малюнку ви хочете дозволити доступ усім користувачам в мережі 192.168.3.0. Оскільки маска підмережі - 255.255.255.0, ви можете взяти 255.255.255.255 і відняти маску підмережі 255.255.255.0. В результаті виходить шаблонна маска 0.0.0.255.

Розрахунок шаблонної маски. приклад 2 (рис. 3.1.8)

Припустимо, що в другому прикладі на малюнку ви хочете дозволити мережевий доступ для 14 користувачів в підмережі 192.168.3.32/28. IPv4-підмережа має маску підмережі 255.255.255.240. Отже, з 255.255.255.255 необхідно відняти маску підмережі 255.255.255.240. В результаті виходить шаблонна маска 0.0.0.15.

Розрахунок шаблонної маски. приклад 3 (рис. 3.1.8)

Припустимо, що в третьому прикладі на малюнку ви хочете обчислити шаблонну маску для відповідності мереж 192.168.10.0 і 192.168.11.0. І знову

беремо 255.255.255.255 і віднімаємо маску підмережі, яка в даному випадку буде 255.255.254.0. У підсумку виходить 0.0.1.255.

Подібний результат можна отримати за допомогою команд, представлених нижче:

R1 (config) # access-list 10 permit 192.168.10.0

R1 (config) # access-list 10 permit 192.168.11.0

Більш ефективним способом є конфігурація шаблонної маски наступним чином:

R1 (config) # access-list 10 permit 192.168.10.0 0.0.1.255

Припустимо, необхідно відфільтрувати мережі в діапазоні від 192.168.16.0/24 до 192.168.31.0/24. При підсумовуванні цих мереж отримуємо 192.168.16.0/20. В цьому випадку правильної шаблонної маскою буде 0.0.15.255. За допомогою такої маски можна скласти єдине і найбільш ефективний запис для списку контролю доступу (ACL), як показано нижче.

R1 (config) # access-list 10 permit 192.168.16.0 0.0.15.255

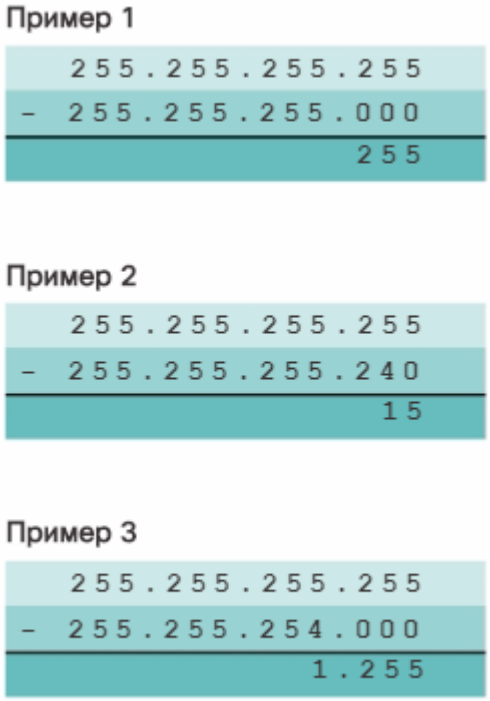


Рис. 4.1.8

Робота з десятковими данними двійкової шаблонної маски може бути трудомістким. Ключові слова **host** і **any** спрощують задачу, допомагаючи визначити найбільш часто використовувану шаблонну маску. Ці ключові слова виключають необхідність введення шаблонних масок при визначенні конкретного вузла або цілої мережі. Ці ключові слова полегшують читання ACL-списку, надаючи візуальні підказки щодо критеріїв джерела або призначення.

Ключове **слово host** застосовується для маски 0.0.0.0. Ця маска має на увазі відповідність всіх бітів IPv4-адреси. Таким чином, фільтрується єдина адреса хоста.

Ключове слово **any** можна використовувати замість IPv4-адреси і маски 255.255.255.255. Ця маска вказує ігнорувати весь IPv4-адрес або прийняти будь-яку адресу.

Приклад 1. Шаблонна маска, відповідна єдиному IPv4-адресу.

У прикладі 1, представленому на рисунку 3.1.9, замість введення 192.168.10.10 0.0.0.0 можна ввести рядок **host 192.168.10.10**.

Приклад 2. Шаблонна маска, відповідає будь-якій IPv4-адресі.

У прикладі 2, представленому на рисунку 3.1.9, замість інструкції 0.0.0.0 255.255.255.255 можна ввести окремо ключове слово.

Рис. 4.1.9

Приклади використання ключових слів в шаблонної масці

Приклад 1, наведений на рисунку 3.1.10, ілюструє застосування ключового слова **any** замість IPv4-адреси 0.0.0.0 з шаблонної маскою 255.255.255.255.

Ключевые слова any и host

Пример 1:

```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
!OR
R1(config)# access-list 1 permit any
```

Пример 2:

```
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
!OR
R1(config)# access-list 1 permit host 192.168.10.10
```

Рис. 4.1.10

Приклад 2 показує, як використовувати ключове слово для заміни шаблонної маски при визначенні одного вузла.

Складання ACL-списків може бути складним завданням. Для кожного інтерфейсу може існувати кілька правил, необхідних для управління типами трафіку, яким дозволено входити або виходити через цей інтерфейс. Маршрутизатор на рисунку 3.1.11 має два інтерфейси, сконфігуровані для IPv4 і IPv6. Якщо для обох протоколів необхідні ACL-списки на обох інтерфейсах і в обох напрямках, то потрібно буде створити 8 окремих ACL-списків. Кожен інтерфейс буде мати чотири ACL-списку: два списки для протоколу IPv4 і два - для протоколу IPv6. Для кожного протоколу потрібен один ACL-список для вхідного трафіку і один - для вихідного трафіку.

Фильтрация трафика на маршрутизаторе с помощью ACL-списков

Имея два интерфейса и два работающих протокола, этот маршрутизатор в целом мог бы иметь восемь отдельных ACL-списков.

Правила применения списков ACL

У вас может быть только один ACL-список на один протокол, интерфейс и направление:

- Один ACL-список для одного протокола (например IPv4 или IPv6)
- Один ACL-список для одного направления (например IN или OUT)
- Один ACL-список для одного интерфейса (например, GigabitEthernet0/0)

Рис. 4.1.11

Примітка. Списки контролю доступу не потрібно конфігурувати на обидва напрямки. Номери ACL-списків та їх спрямування, що застосовуються на інтерфейсі, залежать від заявлених вимог.

Наведемо кілька рекомендацій по використанню ACL-списків.

- Використовуйте ACL-списки в міжмережевих екранах маршрутизаторів, розміщених між внутрішньою і зовнішньою мережами, наприклад, Інтернетом.
- Для управління вхідними або вихідними трафіком в певній частині внутрішньої мережі використовуйте ACL-списки на маршрутизаторі, розташованому між двома сегментами мережі.
- Налаштуйте ACL-списки на прикордонних маршрутизаторах, тобто маршрутизаторах, розташованих на кордонах мереж. Це забезпечить базовий буфер від зовнішньої мережі або між менш контрольованою і більш чутливою областями мережі.
- Налаштуйте ACL-списки для кожного протоколу мережі, налаштованого на інтерфейсі прикордонного маршрутизатора.

Можна настроїти один список контролю доступу для протоколу, напрямки, інтерфейсу:

- Один ACL-список для одного протоколу - для управління потоком трафіку на інтерфейсі ACL-список повинен бути визначений для кожного протоколу, що діє на інтерфейсі.
- Один ACL-список для одного напрямку - ACL-списки одночасно контролюють трафік на одному напрямку одного інтерфейсу. Для управління вихідним і вхідним трафіком повинні бути створені два окремих ACL-списку.
- Один ACL-список для одного інтерфейсу - ACL-списки керують трафіком на одному інтерфейсі, наприклад, GigabitEthernet 0/0.

Створення ACL-списків вимагає уваги до деталей і підвищеної обережності. Помилки можуть призвести до серйозних наслідків і додаткових витрат, пов'язаних з простоями, пошуком і усуненням неполадок, а також некоректною роботою мережевих служб. Перед налаштуванням ACL-списку необхідно створити базовий план. На рисунку 3.1.12 представлений список рекомендацій, що становлять базову методику складання ACL-списку.

Рекомендации	Преимущество
Создавайте ACL-списки, исходя из корпоративной политики обеспечения информационной безопасности.	Соблюдение рекомендации обеспечивает соответствие требованиям информационной безопасности компании.
Подготовьте описание обязательных действий ваших ACL-списков.	Соблюдение рекомендации поможет избежать непреднамеренного создания потенциальных проблем доступа.
Используйте текстовый редактор для создания, редактирования и сохранения ACL-списков.	Соблюдение рекомендации поможет создать библиотеку повторно используемых ACL-списков.
Проверьте работу ACL-списков в пробной сети перед внедрением в реальную действующую сеть.	Соблюдение рекомендации поможет избежать дорогостоящих ошибок.

Рис. 4.1.12

Де слід розміщувати ACL-списки

Правильне розміщення ACL-списку може підвищити ефективність мережі. ACL-список можна розмістити для мінімізації надлишкового трафіку. Наприклад, трафік, який буде відхилений віддаленим місцем призначення, не повинен пересилатися за допомогою мережевих ресурсів по маршруту до цього місця призначення.

Кожен ACL-список повинен бути розміщений там, де він може демонструвати максимальну ефективність. Наведемо список базових правил розміщення ACL-списків (див. рис. 3.1.13):

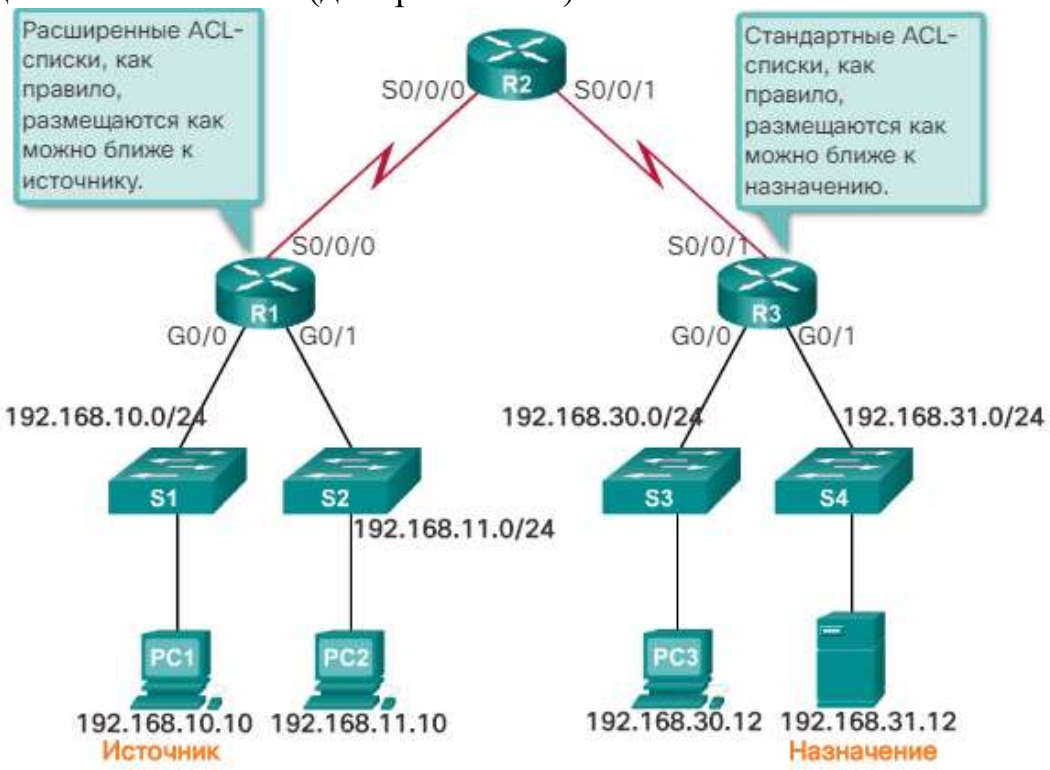


Рис. 4.1.13

Розширені ACL-списки - розширені ACL-списки слід розміщувати максимально близько до джерела трафіку, що фільтрується. Таким чином, небажаний трафік відхиляється близько до мережі-джерела, не перетинаючи інфраструктуру мережі.

Стандартні ACL-списки - оскільки стандартні списки контролю доступу не визначають адреси призначення, їх розміщують максимально близько до місця призначення. Розміщення стандартного ACL-списку біля джерела трафіку дозволяє запобігти досягнення цим трафіком інших мереж через інтерфейс, на якому застосований ACL-список.

Розміщення списку контролю доступу (ACL) і, як наслідок, тип списку може також залежати від наступних факторів.

Сфера контролю мережевого адміністратора - розміщення ACL-списку може залежати від того, чи управляє адміністратор мережею-джерелом і мережею призначення.

Пропускна здатність задіяних мереж - фільтрація небажаного трафіку біля джерела запобігає передачі трафіку до того, як він знижує пропускну здатність мережі на шляху до пункту призначення. Це особливо важливо в мережах з низькою пропускною здатністю.

Простота конфігурації - для заборони мережевим адміністратором трафіку, що надходить від декількох мереж, одним із способів може стати використання одного стандартного ACL-списку на найближчому до місця призначення маршрутизаторі. Недолік цього способу в тому, що трафік з цих мереж буде використовувати пропускну здатність. Розширений ACL-список можна застосувати на кожному маршрутизаторі, з якого йде трафік. Це дозволить зберегти пропускну здатність за допомогою фільтрації трафіку на джерелі, але для цього потрібне створення розширених ACL-списків на декількох маршрутизаторах.

Показана на рисунку 3.1.14 топологія ілюструє принципи розміщення стандартного списку контролю доступу (ACL). Адміністратор хоче заборонити проходження трафіку з мережі 192.168.10.0/24 в мережу 192.168.30.0/24.

На рисунку 3.1.14 показані два інтерфейси маршрутизатора R3, на яких можна налаштувати використання стандартного ACL-списку, відповідно до основних рекомендацій по розміщенню стандартного ACL-списку якомога ближче до місця призначення:

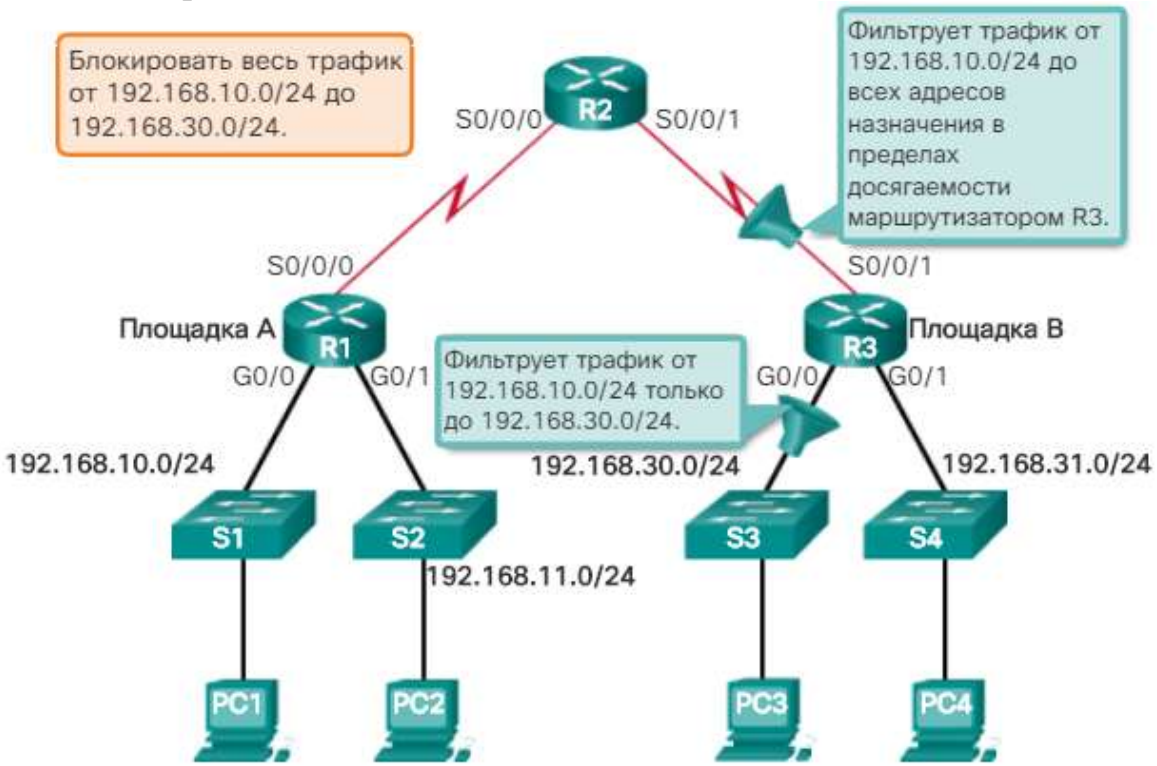


Рис. 4.1.14

Інтерфейс S0/0/1 маршрутизатора R3 - використання стандартного ACL-списку для запобігання трафіку з мережі 192.168.10.0/24 в інтерфейс S0/0/1 також не допустить цей трафік в мережу 192.168.30.0/24 і в інші мережі, до яких має доступ маршрутизатор R3, включаючи мережу 192.168.31.0/24. Оскільки метою ACL-списку є фільтрація трафіку, призначеного тільки для 192.168.30.0/24, стандартний ACL-список не повинен застосовуватися на цьому інтерфейсі.

Інтерфейс G0/0R3 - застосування стандартного списку контролю доступу до трафіку вихідного інтерфейсу G0/0 призведе до фільтрації пакетів з мереж в діапазоні від 192.168.10.0/24 до 192.168.30.0/24. Застосування даного списку не

вплине на інші мережі, досяжні R3. Пакети з мережі 192.168.10.0/24 як і раніше повинні потрапляти в мережу 192.168.31.0/24.

Синтаксис стандартного нумерованого списку контролю доступу (ACL) IPv4

Для використання стандартних нумерованих ACL-списків на маршрутизаторі Cisco необхідно спочатку створити стандартний ACL-список і потім активувати його на інтерфейсі.

Команда глобальної конфігурації **access-list** визначає стандартний ACL-список з номером в діапазоні від 1 до 99. У ОС Cisco IOS версії 12.0.1 даний діапазон розширений; для стандартних ACL-списків можуть використовуватися номери від 1300 до 1999. Це дозволяє створити до 798 можливих стандартних ACL-списків. Списки з цими додатковими номерами називаються додатковими списками контролю доступу (ACL) IPv4.

Повний синтаксис команди стандартного ACL-списку:

Router (config) # access-list номер списку доступу {deny | permit | remark} source [source-wildcard] [log]

Рисунок містить докладний опис синтаксису для стандартного ACL-списку.

Параметр	Описание
access-list-number	Номер списка ACL. Это десятичное число от 1 до 99 или от 1300 до 1999 (для стандартных списков ACL).
deny	Запрещает доступ, если условия выполняются.
permit	Разрешает доступ, если условия выполняются.
remark	Добавьте примечания к записям в списке контроля доступа, чтобы сделать этот список более простым для понимания и поиска.
source	Номер сети или хоста, с которого был отправлен пакет. Существуют два способа указать параметр *source*: • (источник). Используйте 32-разрядное значение в виде четырех десятичных чисел, разделенных точками. • Используйте ключевое слово any (любой) в качестве сокращения для адреса источника *source* source и групповой маски источника *source-wildcard* 0.0.0.0 255.255.255.255.

Рис. 4.1.15

Записи в списку контролю доступу дозволяють або забороняють трафік щодо конкретної адреси хосту або діапазону таких адрес. Щоб створити в нумерованому списку контролю доступу (ACL) 10 запис на основі ключового слова **host**, що дозволяє трафік для хосту з IP-адресою 192.168.10.10, необхідно ввести наступну команду:

R1 (config) # access-list 10 permit host 192.168.10.10

Як показано на рис. 3.1.16, для створення запису, яка дозволить діапазон IPv4-адрес в нумерованому ACL-списку 10, дозвільному все IPv4-адреси в мережі 192.168.10.0/24, необхідно ввести наступну команду:

R1 (config) # access-list 10 permit 192.168.10.0 0.0.0.255

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
R1# show access-lists
Standard IP access list 10
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config)# no access-list 10
R1(config)# exit
R1# show access-lists
R1#
```

Рис. 4.1.16

Для видалення ACL-списку використовується команда глобальної конфігурації **no access-list**. Введення команди **show access-list** підтверджує видалення ACL-списку 10 (рис. 3.1.17).

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
R1# show access-lists
Standard IP access list 10
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config)# no access-list 10
R1(config)# exit
R1# show access-lists
R1#
```

Рис. 4.1.17

Як правило, при створенні адміністратором списку контролю доступу, застосування кожного запису відомо і очевидно. Проте, для того, щоб адміністратор і інші користувачі могли згадати призначення того або іншого запису, необхідно додати відповідні коментарі. Для документування та спрощення прочитання ACL-списків використовується ключове слово **remark.** Довжина коментаря обмежена 100 символами. Досить простий ACL-список на рис. 3.1.18 наводиться як приклад. При перегляді конфігурації ACL-списку за допомогою команди **show running-config** також відображається відповідний коментар.

```
R1(config)# access-list 10 remark Permit hosts from the
192.168.10.0 LAN
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
R1# show running-config | include access-list 10
access-list 10 remark Permit hosts from the 192.168.10.0 LAN
access-list 10 permit 192.168.10.0 0.0.0.255
R1#
```

Рис. 4.1.18

Застосування стандартних списків контролю доступу (ACL) до інтерфейсів

Створивши стандартний список контролю доступу (ACL), його необхідно пов'язати з інтерфейсом за допомогою команди **ip access-group**, яка вводиться в режимі інтерфейсної настройки:

Router (config-if) # ip access-group {access-list-number | access-list-name} {in | out}

Для видалення всього ACL-списку з інтерфейсу спочатку слід ввести команду **no ip access-group** на інтерфейсі, а потім ввести глобальну команду **no access-list**.

На рис. 3.1.19 перераховані етапи і синтаксис для настройки і застосування нумерованого стандартного списку контролю доступу на маршрутизаторі.

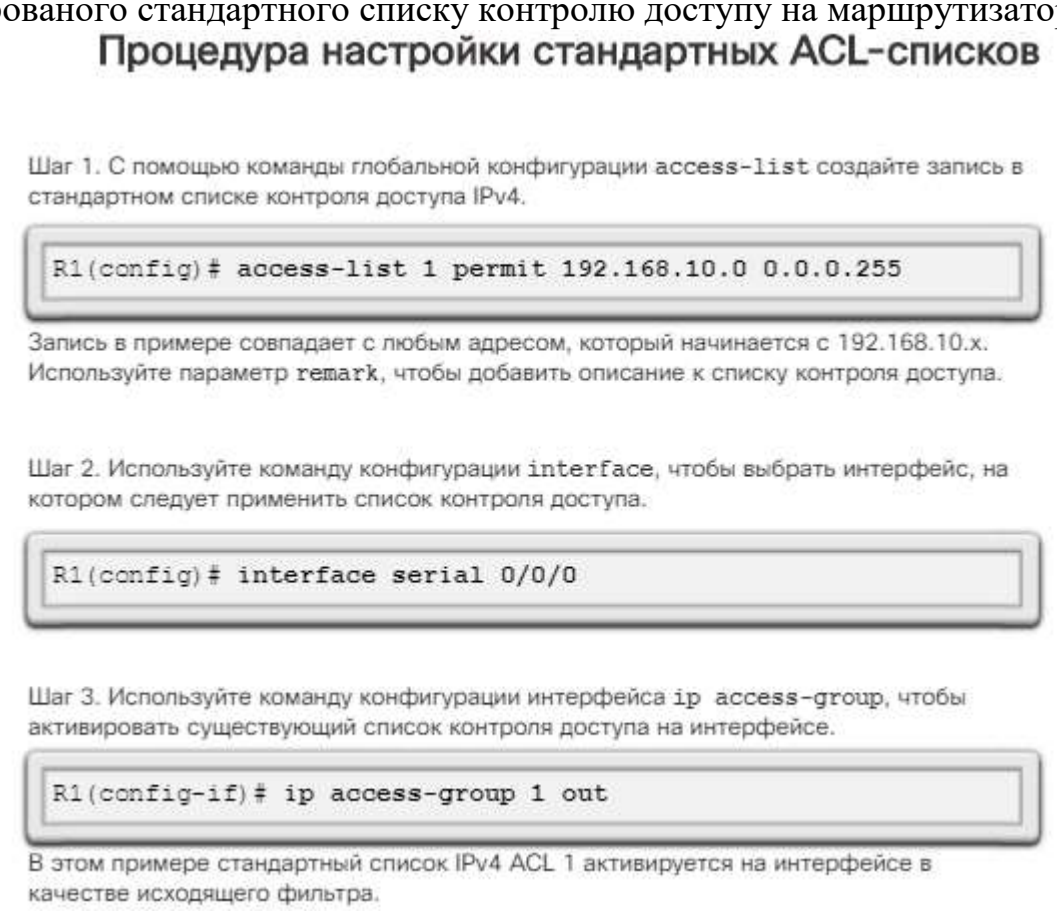


Рис. 4.1.19

На рисунку показаний список контролю доступу (ACL), що дозволяє єдину мережу.

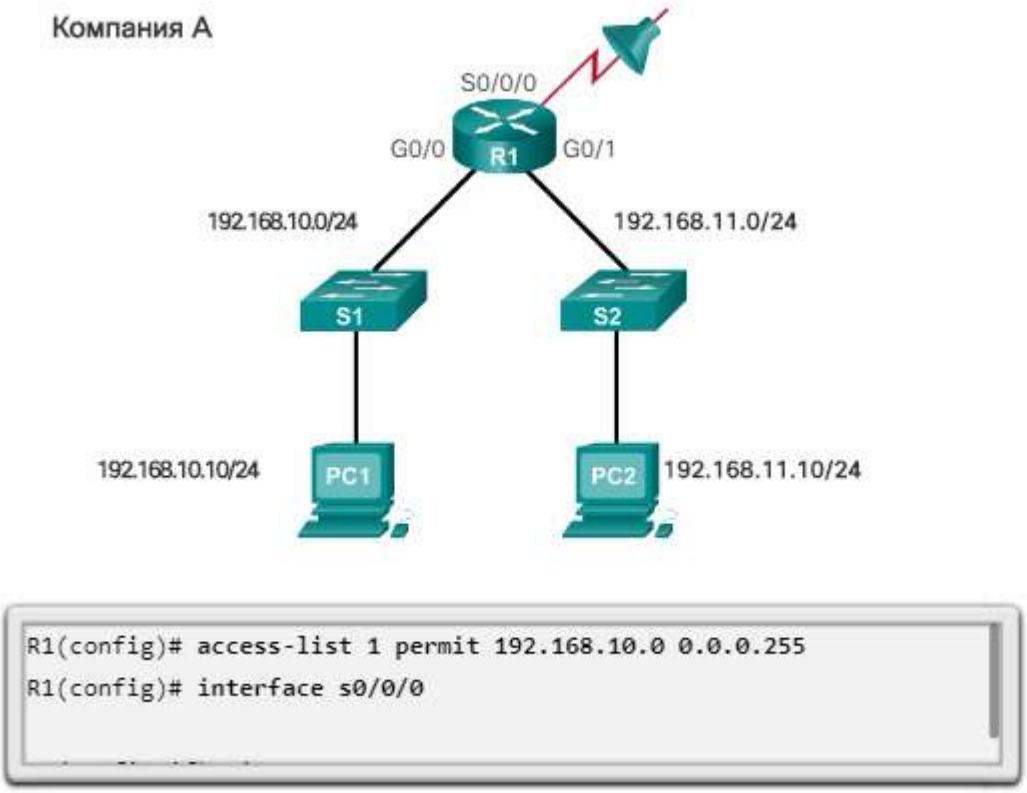


Рис. 4.1.20

Цей ACL-список дозволяє пересилати трафік тільки з мережі джерела 192.168.10.0 з інтерфейсу S0/0/0. Трафік з мереж, відмінних від 192.168.10.0, заблокований.

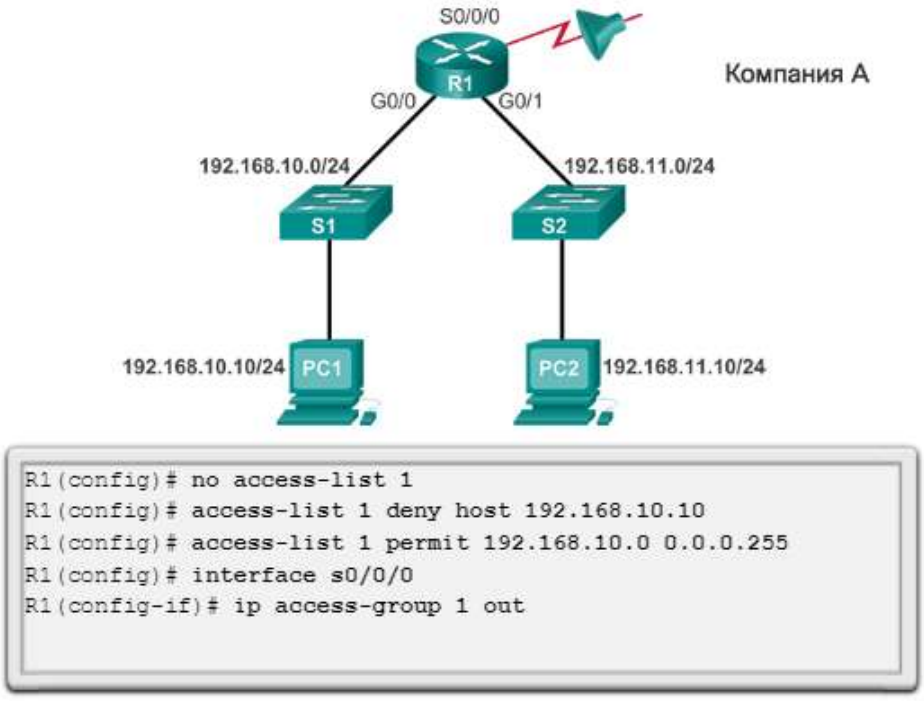
Перший рядок задає список контролю доступу як список доступу 1. Таким чином, дозволяється трафік, який відповідає заданим параметрам. В цьому випадку IPv4-адрес і шаблонна маска, яка визначає мережу джерела - 192.168.10.0 0.0.0.255. Необхідно пам'ятати про наявність неявної заборони **deny all**, який еквівалентний **рядку access-list 1 deny 0.0.0.0 255.255.255.255** або **access-list deny any** в кінці списку контролю доступу (ACL).

Команда конфігурації інтерфейсу **ip access-group 1 out** пов'язує і прив'язує ACL 1 до інтерфейсу Serial 0/0/0 як вихідного фільтра.

Тому ACL-список 1 дозволяє вихід через маршрутизатор R1 тільки вузлів з мережі 192.168.10.0/24. У той же час він забороняє будь-яку іншу мережу, включаючи 192.168.11.0.

Приклади стандартного нумерованого списку контролю доступу (ACL) IPv4

На рис. 3.1.21 наведено приклад ACL-списку, який дозволить виключити певну підмережа за винятком конкретного вузла в цій підмережі.



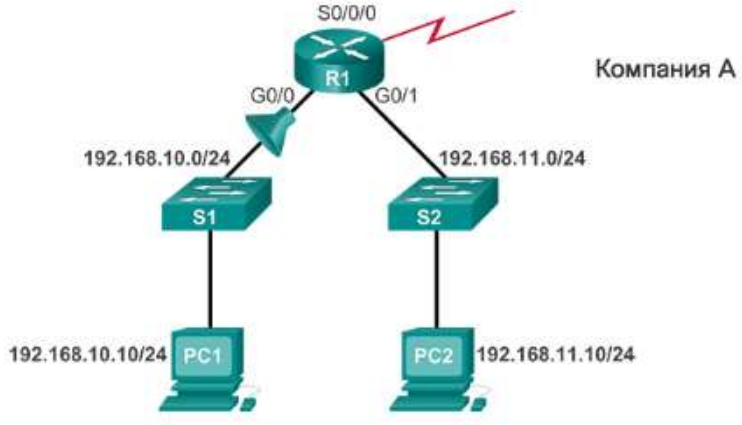

```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```

Рис. 4.1.21

Перша команда видаляє попередню версію ACL-списку 1. Наступний запис списку контролю доступу забороняє вузол PC1, розташований в мережі 192.168.10.10. Всі інші хости в мережі 192.168.10.0/24 дозволені. І знову непрямий запис відмови відповідає кожній іншій мережі.

ACL-список повторно застосований на вихідному напрямку інтерфейсу S0/0/0.

На рисунку 3.1.22 показаний список контролю доступу (ACL), що забороняє певний вузол. Цей ACL-список є заміною попередньому прикладу. У цьому прикладі, як і раніше блокується трафік від вузла PC1, але дозволений весь інший трафік.




```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit any
R1(config)# interface g0/0
R1(config-if)# ip access-group 1 in
```

Рис. 4.1.22

Перші дві команди аналогічні командам з попереднього прикладу. Перша команда видаляє попередню версію ACL 1, в той час як наступна команда списку контролю доступу забороняє вузол PC1, розташований в мережі 192.168.10.10.

Третя команда введена заново - в ній дозволяються всі інші вузли. Це означає, що дозволені всі хости в мережі 192.168.10.0/24, за винятком комп'ютера PC1, який був заборонений в попередньому рядку.

Розглянутий ACL-список застосовується на вхідному напрямку інтерфейсу G0/0. Оскільки фільтр зачіпає тільки LAN 192.168.10.0/24 на G0/0, більш ефективним буде застосувати ACL-список на вхідному інтерфейсі. Список контролю доступу (ACL) можна застосувати до s0/0/0 в вихідному напрямі, проте при цьому маршрутизатор R1 буде змушений перевіряти пакети з усіх цих служб, включаючи 192.168.11.0/24.

Присвоєння імен ACL-спискам спрощує розуміння функції того чи іншого списку. При присвоєнні ACL-списку імені замість номера режим конфігурації і синтаксис команд трохи змінюються.

На рис. 3.1.23 представлені послідовні дії, які необхідно зробити для створення стандартного іменованого ACL-списку.

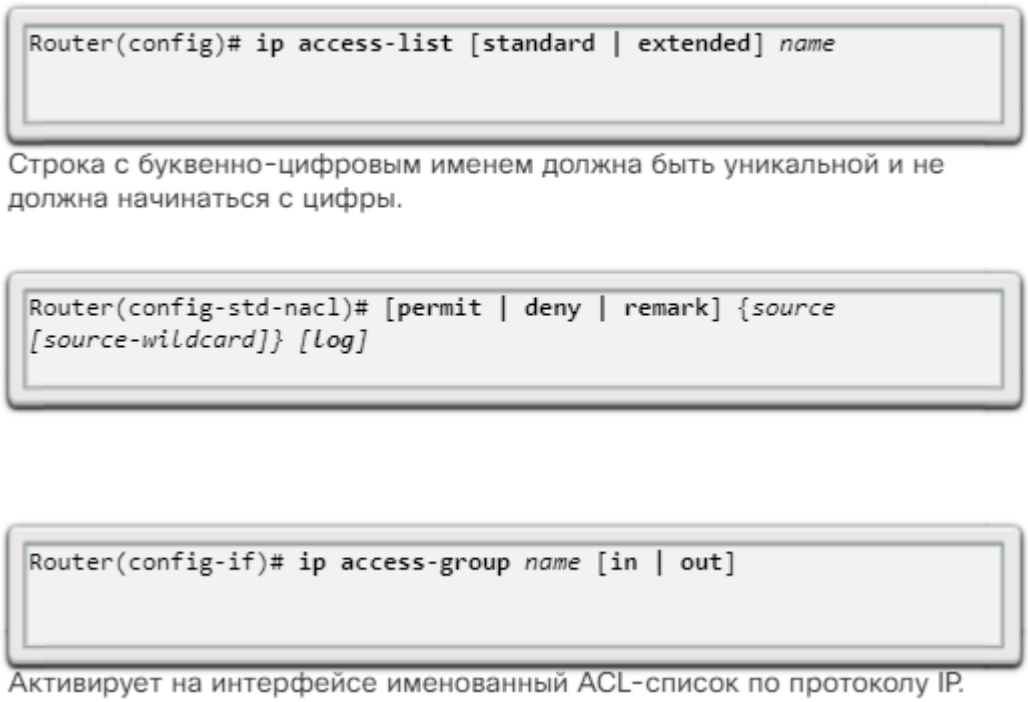
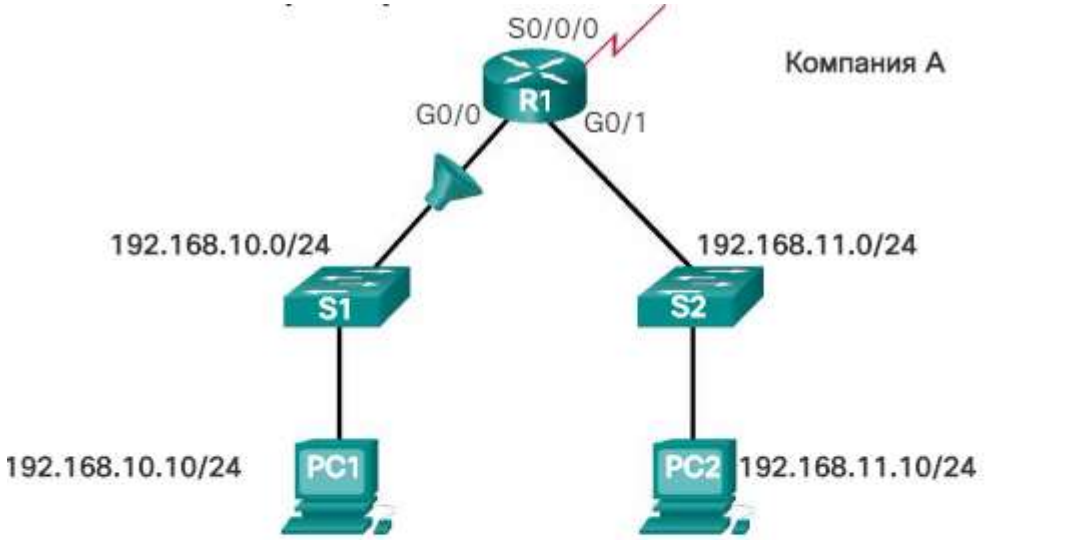


Рис. 4.1.23

Крок 1. Для створення іменованого ACL-списку почніть з виконання команди режиму глобальної конфігурації **ip access-list**. Імена ACL-списків складаються з літер та цифр, вони чутливі до регістру і повинні бути унікальними. Команда **ip access-list standard Ім'я** застосовується для створення стандартного іменованого списку контролю доступу (ACL). Після введення цієї команди маршрутизатор знаходиться в режимі конфігурації стандартного (std) іменованого (nacl) списку контролю доступу (ACL), про що свідчить друге запрошення командного рядка (рисунок 3.1.24).




```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

Рис. 4.1.24

Примітка. Для нумерованих списків контролю доступу (ACL) використовується команда глобальної конфігурації **access-list**, тоді як для іменованих списків контролю доступу (ACL) IPv4 слід використовувати команду **ip access-list.**

Крок 2. У режимі конфігурації іменованих ACL-списків застосуєте команди **permit** або **deny**, щоб задати одне або більше умов визначення відправки або відхилення пакету. До списку контролю доступу (ACL) можна додати коментар за допомогою ключового слова **remark**.

Крок 3. Застосуйте список контролю доступу (ACL) до інтерфейсу, користуючись командою **ip access-group name**. Вкажіть, коли саме слід застосовувати список контролю доступу (ACL) до пакетів - при надходженні пакетів на інтерфейс (in) або ж при відправці пакетів з інтерфейсу (out).

На рисунку 3.1.24 показані команди для налаштування стандартного іменованого списку контролю доступу (ACL) на інтерфейсі G0/0 маршрутизатора R1. Список забороняє доступ хоста 192.168.11.10 до мережі 192.168.10.0. ACL-списку присвоєно ім'я «NO_ACCESS».

Вказувати імена ACL-списків великими літерами не обов'язково, але це робить їх більш помітними при перегляді вихідних даних поточної конфігурації. Це також знижує ймовірність випадкового створення двох різних ACL-списків з однаковими іменами, але які відрізняються використанням великих і малих літер.

Після ознайомлення з процесами створення і редагування ACL-списків, більш простим способом складання ACL буде використання текстового редактора, наприклад Блокнот від Майкрософт. Таким чином можна створити або відредагувати список контролю доступу (ACL), після чого вставити його в

інтерфейс маршрутизатора. Якщо список контролю доступу (ACL) вже існує, можна відобразити цей список за допомогою команди **show running-config**, скопіювати вміст, вставити його в текстовий редактор, внести необхідні зміни, після чого скопіювати вміст з текстового редактора і вставити його назад в інтерфейс маршрутизатора.

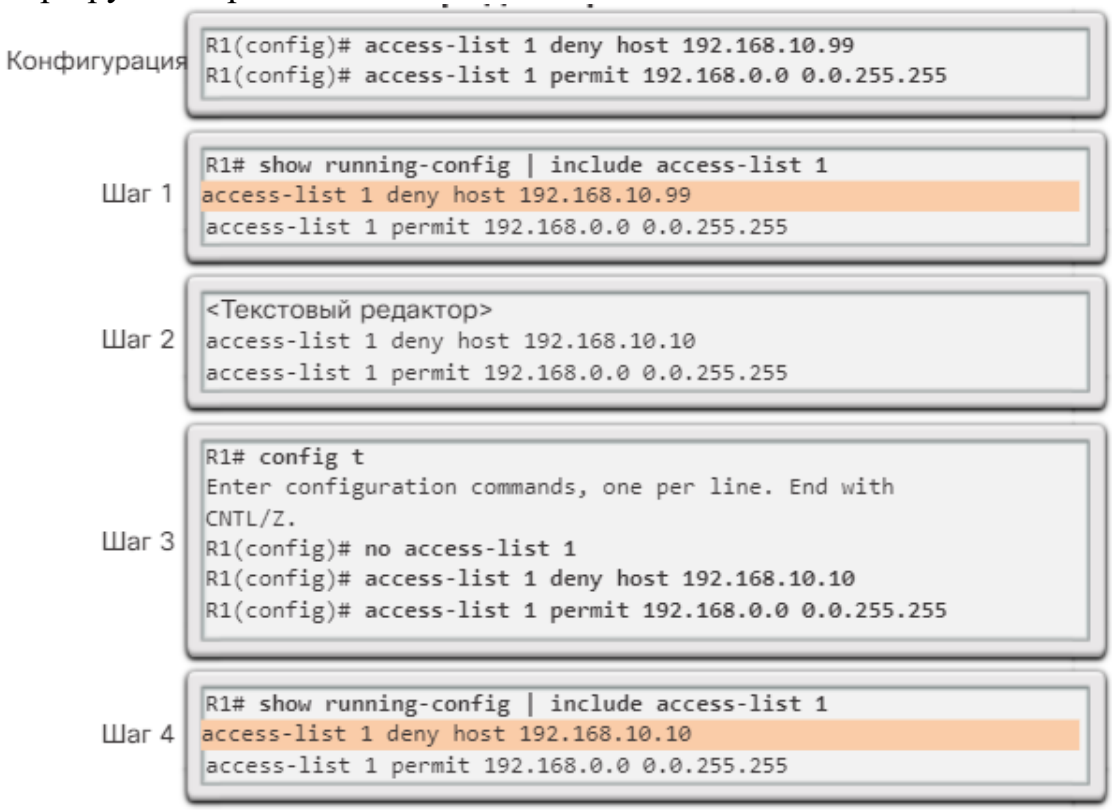


Рис. 4.1.25

Конфігурація. Припустимо, що IPv4-адрес вузла на малюнку вказано неправильно. Замість вузла 192.168.10.99 повинен бути вузол 192.168.10.10. Нижче наведено порядок дій при редагуванні ACL 1:

Крок 1. Відкрийте поточний ACL-список за допомогою команди show running-config. У прикладі на малюнку використовується ключове слово include для відображення тільки записів ACE.

Крок 2. Виділіть ACL-список, скопіюйте його і вставте в Блокнот. Внесіть необхідні зміни. Після коригування ACL-списку в Блокноті, виділіть її та скопіюйте.

Крок 3. У режимі глобальної конфігурації видаліть список доступу за допомогою команди **no access-list 1**. В іншому випадку нові оператори можна додати в існуючий список контролю доступу. Потім вставте новий список контролю доступу в конфігурацію маршрутизатора.

Крок 4. Використовуючи команду **show running-config**, перевірте внесені зміни.

Необхідно пояснити, що при застосуванні команди **no access-list,** версії ОС IOS поводяться по-різному. Якщо ACL-список, який був вилучений, все ще застосовується на інтерфейсі, деякі версії IOS діють, як ніби немає ACL-списків, які захищають мережу, в той час як інші версії блокують весь трафік. З цієї причини рекомендується видалити посилання на списки доступу з інтерфейсу перед внесенням змін до списку доступу. Якщо в новому списку

виявлена помилка, необхідно відключити його і усунути проблему. В цьому випадку в ході корекції мережа працюватиме без списку контролю доступу (ACL).

Використання порядкових номерів.

Як показано на рисунку 3.1.26, при початковій настройці списку контролю доступу (ACL) 1 був використаний наступний запис з ключовим словом host: host 192.168.10.99. Даний запис є хибним. Вузол повинен бути налаштований як 192.168.10.10. Щоб змінити список контролю доступу з використанням порядкових номерів, виконайте наступні дії:

Крок 1. Ще раз відобразите поточний ACL-список за допомогою команди **show access-lists 1**. Вихідні дані цієї команди будуть детально обговорюватися далі в цьому розділі. Порядковий номер відображається на початку кожного запису. Порядковий номер автоматично присвоюється при додаванні запису в список. Зверніть увагу, що запис з неправильною конфігурацією має порядковий номер 10.

Крок 2. Введіть команду **ip access-lists standard,** використовувану для конфігурації іменованого ACL-списку. Номер списку контролю доступу (ACL), тобто 1, використовується в якості імені. В першу чергу необхідно видалити помилковий запис за допомогою команди **no 10**, де 10 - це порядковий номер. Потім додайте новий запис з порядковим номером 10 за допомогою команди **10 deny host 192.168.10.10**.

Примітка. Записи можна перезаписати з тими ж порядковими номерами, що і у існуючих записів. Спочатку необхідно видалити поточну запис, а потім можна створювати нову.

Крок 3. Перевірте внесені зміни, використовуючи команду **show access-lists.**

Як уже згадувалося раніше, Cisco IOS реалізує внутрішню логіку для стандартних списків доступу. Порядок, в якому вводяться стандартні ACL-записи, може не збігатися з порядком, в якому вони зберігаються, відображаються або обробляються маршрутизатором. Команда **show access-lists** відображає ACL-записи з їх порядковими номерами.

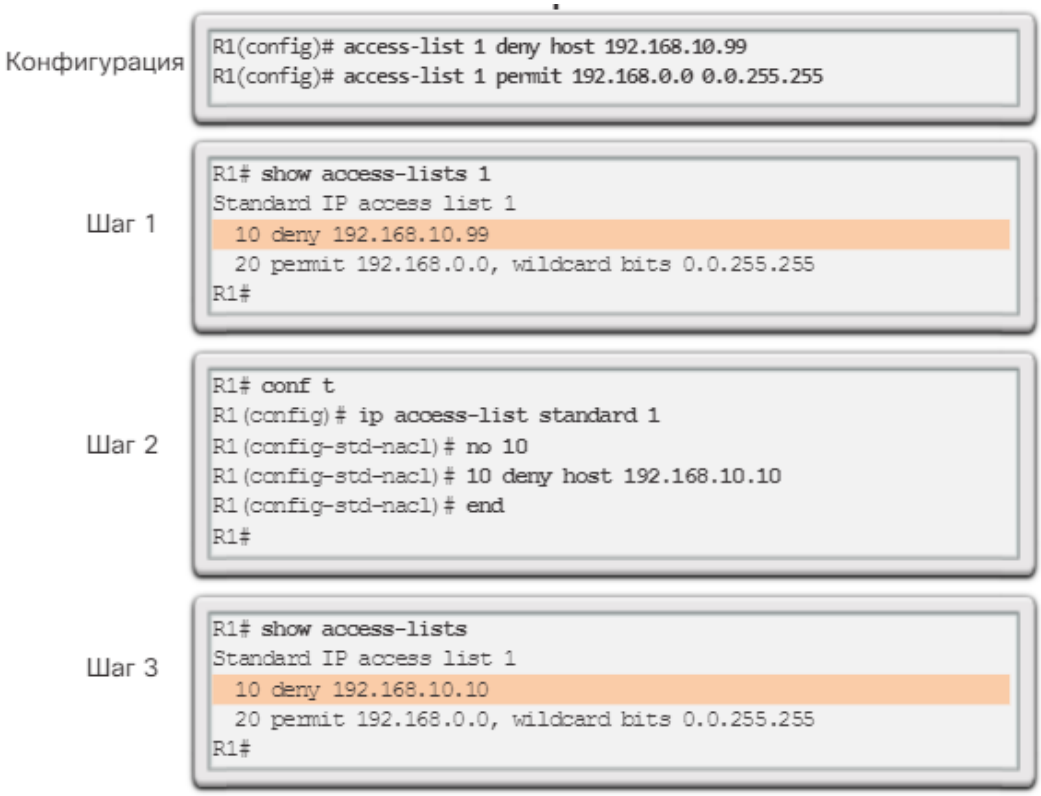


Рис. 4.1.26

У попередньому прикладі для редагування стандартного нумерованого списку контролю доступу (ACL) IPv4 використовувалися порядкові номери. Використовуючи порядкові номери записів, окремі записи можна легко вставити або видалити. Даний метод також можна використовувати при редагуванні стандартних іменованих ACL-списків.

На рисунку 3.1.27 наводиться приклад вставки рядка в іменований список контролю доступу.

У вихідних даних команди **show** можна побачити, що ACL-списку присвоєно ім'я «NO_ACCESS», він має дві нумеровані рядки, що вказують правила доступу для робочої станції з IPv4-адресою 192.168.11.10.

В режимі конфігурації іменованого списку контролю доступу (ACL) можна вставляти і видаляти записи. Для додавання запису, що містить заборону інший робочої станції, потрібно додавання нумерованого рядка. У цьому прикладі додається робоча станція з IPv4-адресою 192.168.11.11 з новим порядковим номером 15.

Прикінцеві вихідні дані команди **show** підтверджують, що тепер для нової робочої станції доступ заборонений.

Примітка. В режимі конфігурації іменованого списку контролю доступу (ACL) можна користуватися командою **no sequence-number,** яка дозволяє швидко видалити окремі записи.

```
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# 15 deny host 192.168.11.11
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    15 deny   192.168.11.11
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Примечание. Команда именованного ACL-списка `no` *`sequence-number`* применяется для удаления отдельных записей.

Рис. 4.1.27

Як показано на рис. 1, команда show ip interface використовується для перевірки ACL-списку на інтерфейсі. Вихідні дані цієї команди включають номер або назву списку доступу і напрямок, до якого був прив'язаний ACL-список. Виведені дані показують, що на маршрутизаторі R1 є список контролю доступу (ACL) 1, який застосований до вихідного інтерфейсу S0 / 0/0, а також список NO_ACCESS, який застосований до інтерфейсу g0 / 0 також в вихідному напрямі.

Приклад на рис. 3.1.28 демонструє результати виконання команди **show access-lists** на маршрутизаторі R1. Щоб переглянути окремий список доступу, застосуйте команду **show access-lists** (рис. 3.1.29), а потім введіть номер або назву списку доступу. Записи NO_ACCESS можуть виглядати дивним чином. Зверніть увагу, що порядковий номер 15 відображається перед порядковим номером 10. Це пояснюється особливостями внутрішньої будови маршрутизатора, які розглянуті далі в цьому розділі.

```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
<Данные опущены>
  Outgoing access list is 1
  Inbound access list is not set
<Данные опущены>

R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<Данные опущены>
  Outgoing access list is NO_ACCESS
  Inbound access list is not set
<Данные опущены>
```

Рис. 4.1.28

```
R1# show access-lists
Standard IP access list 1
  10 deny 192.168.10.10
  20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
  15 deny 192.168.11.11
  10 deny 192.168.11.10
  20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Рис. 4.1.29

Після застосування списку контролю доступу (ACL) до інтерфейсу і виконання перевірки команда **show access-lists** виводить статистику зі збігами для кожного запису. Зауважте, що деякі записи в вихідних даних на рисунку 3.1.30 збігаються. Коли створюється трафік, який повинен відповідати будь-якому записі ACL-списку, кількість збігів, які відображаються в вихідних даних команди **show access-lists,** має збільшитися. Наприклад, якщо з комп'ютера PC1 відправляється ping-запит на комп'ютер PC3 або PC4, то кількість збігів для запису deny в списку контролю доступу (ACL) 1 збільшиться, що буде відображено в результатах роботи згаданої вище команди.

Записи дозволу і заборони відстежують статистику збігів, проте необхідно пам'ятати, що кожен список контролю доступу має непряму відмову в останньому рядку. Цей запис не виводиться при виконанні команди **show access-lists,** тому статистика для цього запису відображатися не буде. Для перегляду статистики по непрямій записи «deny any» її можна конфігурувати вручну, після чого вона з'явиться в вихідних даних.

В процесі тестування ACL-списку лічильники можна обнулити, виконавши команду **clear access-list counters**. Цю команду можна застосовувати окремо або із зазначенням номера або імені конкретного ACL-списку. Як показано на рисунку 3.1.31, ця команда обнуляє лічильники статистики для списку контролю доступу (ACL).

```
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10 (4 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny 192.168.11.11
    10 deny 192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Выходные данные после отправки ping-запроса с PC1 на PC3

```
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10 (8 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny 192.168.11.11
    10 deny 192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Количество совпадений увеличилось.

Рис. 4.1.30

```
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10 (4 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny 192.168.11.11
    10 deny 192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# clear access-list counters 1
R1#
R1# show access-lists
Standard IP access list 1
    10 deny 192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny 192.168.11.11
    10 deny 192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
```

Совпадения обнулены.

Рис. 4.1.31

Щоб посилити безпеку адміністративних ліній, можна обмежити VTY-доступ. Вказавши явно перелік IP-адрес, з яких дозволений віддалений доступ до процесу EXEC на маршрутизаторі, ви тим самим обмежуєте VTY-доступ. Перелік IP-адрес, з яких дозволяється віддалений доступ до маршрутизатора, можна задати за допомогою списку контролю доступу (ACL) і записи **access-class** на VTY-лініях. Цей метод можна використовувати з протоколом SSH для додаткового захисту адміністративного доступу.

Команда **access-class**, встановлена в режимі конфігурації лінії, обмежує вхідні та вихідні з'єднання між зазначеним VTY (в пристрої Cisco) і адресами в списку доступу.

Синтаксис команди **access-class** виглядає наступним чином:

Router (config-line) # access-class номер списку доступу {in [vrf-also] | out}

Параметр in обмежує вхідні з'єднання між адресами в списку доступу та пристроєм Cisco, в той час як параметр out обмежує вихідні з'єднання між окремим пристроєм Cisco і адресами в списку доступу.

На рис. 3.1.32 показаний приклад, в якому у діапазоні адрес є доступ до ліній VTY 0-4. ACL-список налаштований на дозвіл доступу для мережі 192.168.10.0 до ліній VTY 0-4 і на заборону доступу для всіх інших мереж.

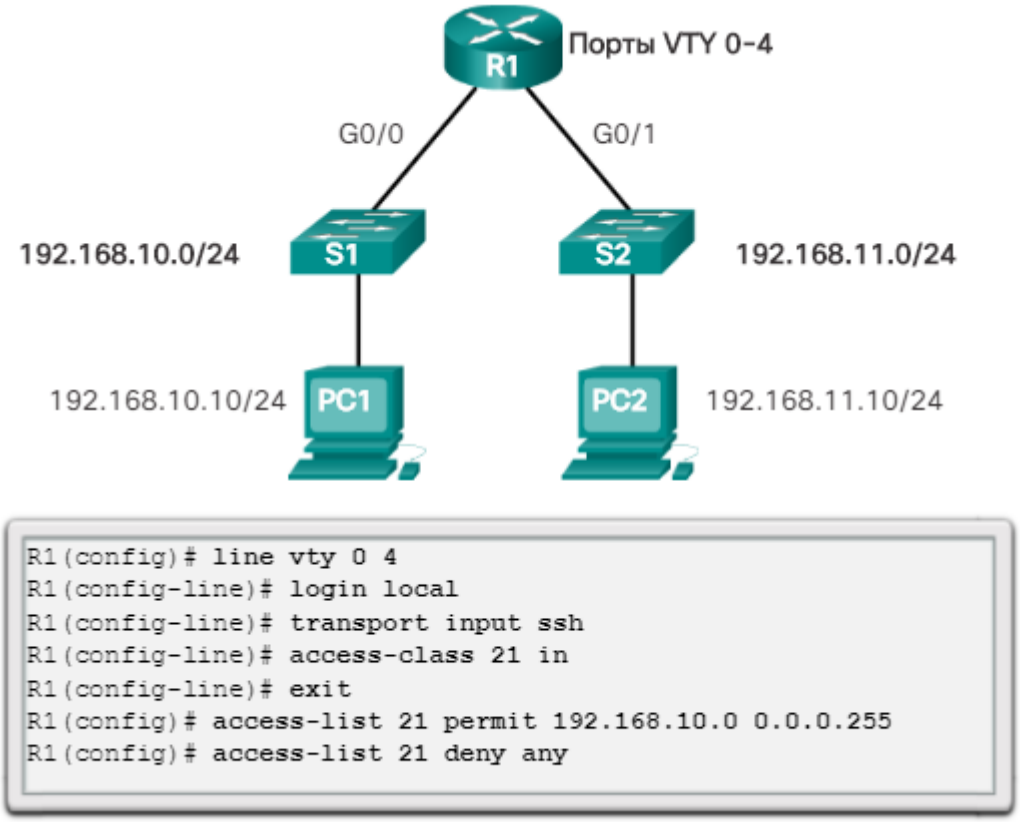


Рис. 4.1.32

Наступні положення повинні враховуватися при налаштуванні списку доступу до каналів VTY:

- До VTY-лініях можна застосовувати як іменовані, так і нумеровані списки контролю доступу (ACL).
- Однакові обмеження повинні бути встановлені на всі канали VTY, оскільки користувач може спробувати підключитися до будь-якого з них.

Примітка. Списки контролю доступу (ACL) застосовуються до пакетів, які проходять через маршрутизатор. Вони не призначені для блокування пакетів, що створюються всередині маршрутизатора. За замовчуванням вихідний список контролю доступу (ACL) не блокує з'єднання віддаленого доступу, ініційовані з маршрутизатора.

Після настройки ACL-списку для обмеження доступу до ліній VTY важливо переконатися в його належне функціонування. На рисунку 3.1.33

зображені два пристрої, які намагаються підключитися до R1 за допомогою протоколу SSH. Список доступу 21 налаштований на лінії VTY маршрутизатора R1. PC1 успішно встановив SSH-з'єднання, в той час як PC2 не вдалося це зробити. Це прогнозована поведінка, оскільки налаштований список доступу забезпечує доступ до VTY з мережі 192.168.10.0/24, забороняючи доступ всім іншим пристроям.

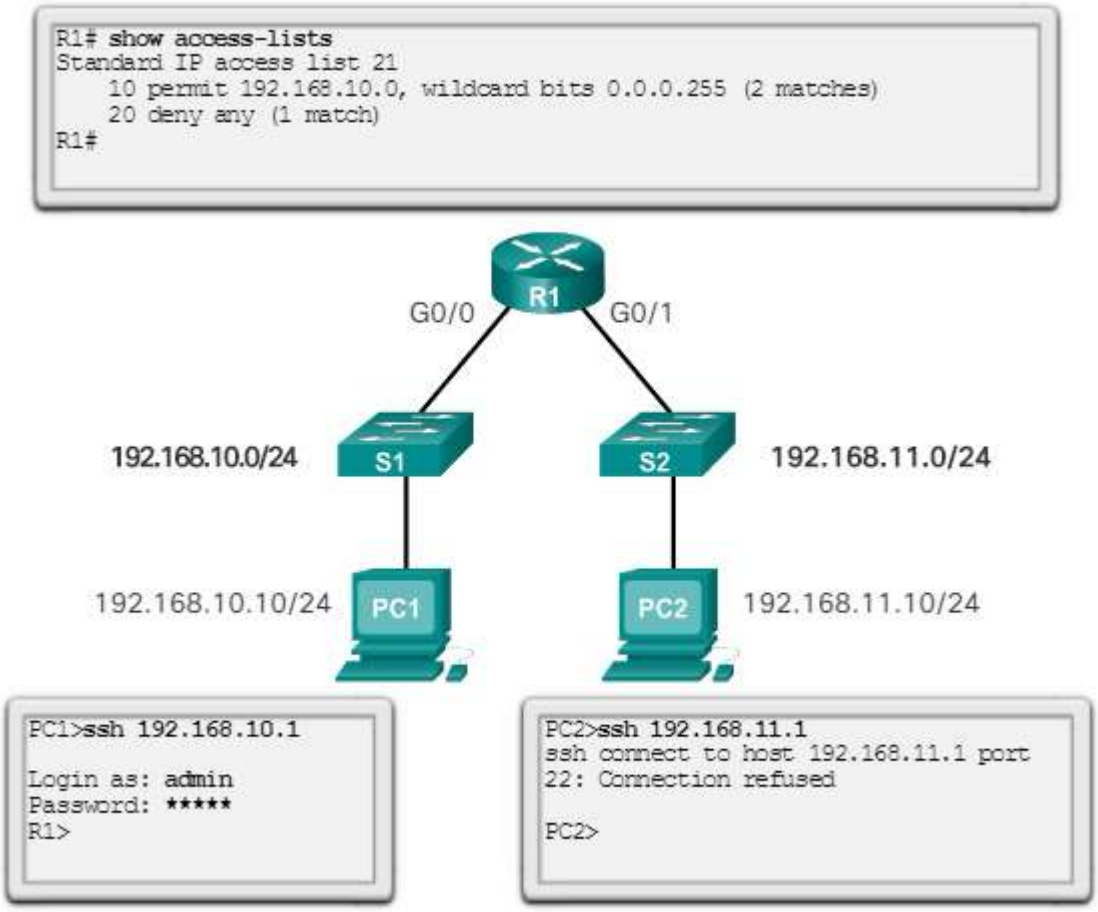
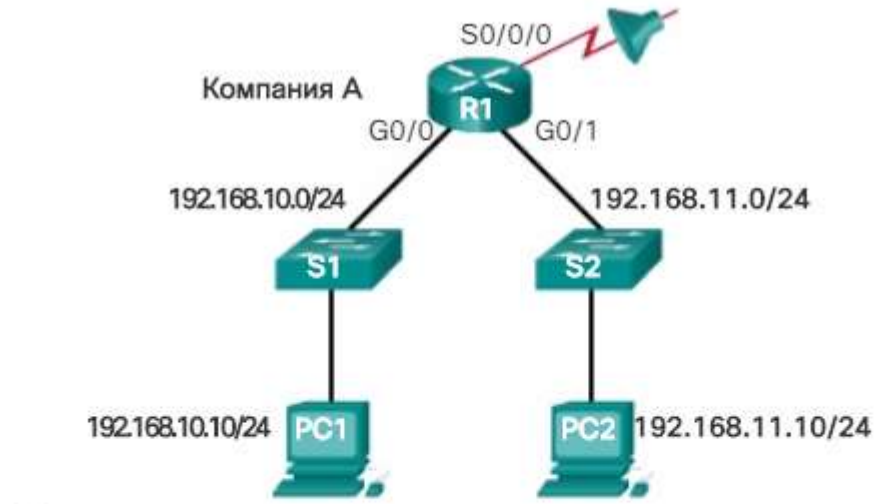


Рис. 4.1.33

Вихідні дані для R1 показують результат виконання команди **show access-lists** після спроб PC1 і PC2 встановити SSH-з'єднання. Збіг у рядку дозволу вихідних даних є результатом успішного SSH-з'єднання PC1. Збіг у рядку заборони є наслідком невдалої спроби встановити SSH-підключення PC2, пристроєм в мережі 192.168.11.0/24.

Якщо ACL-список складається з однієї команди заборони, весь трафік буде відхилятися. Таким чином, в списку повинна бути, принаймні, одна команда дозволу, тому що в іншому випадку весь трафік буде заблокований.

Для мережі на рисунку 3.1.34 застосування ACL-списку 1 або ACL-списку 2 на інтерфейсі S0/0/0 маршрутизатора R1 на вихідному напрямі дає однакові результати. Для мережі 192.168.10.0 буде дозволений доступ до цих мереж через інтерфейс S0/0/0. Для мережі 192.168.11.0 доступ до цих мереж буде заборонений. При використанні списку контролю доступу (ACL) 1 будь-який пакет, який не відповідає умові записи **permi**t, відкидається.



ACL-список 1

```
R1(config)# access-list 1 permit ip 192.168.10.0 0.0.0.255
```

ACL-список 2

```
R1(config)# access-list 2 permit ip 192.168.10.0 0.0.0.255
R1(config)# access-list 2 deny any
```

Рис. 4.1.34

Cisco IOS застосовує внутрішній алгоритм в процесі прийому і обробки стандартних записів ACE. Як вже говорилося раніше, записи в списку контролю доступу (ACL) обробляються послідовно. Тому порядок розташування цих записів має велике значення.

Наприклад, на рисунку 3.1.35 список контролю доступу (ACL) 3 містить два записи. Перша ACE використовує шаблонну маску для заборони діапазону адрес, який включає всі вузли в мережі 192.168.10.0/24. Другий запис - команда host, в якій перевіряється конкретний хост з адресою 192.168.10.10, що належить мережі 192.168.10.0/24. Внутрішній алгоритм IOS для стандартних списків доступу відхиляє другий запис і видає повідомлення про помилку, оскільки другий запис суперечить першому.

```
R1(config)# access-list 3 deny 192.168.10.0 0.0.0.255
R1(config)# access-list 3 permit host 192.168.10.10
% Access rule can't be configured at higher sequence num as
it is part of the existing rule at sequence num 10
R1(config)#
```

ACL-список 3. Запись узла конфликтует с предыдущей записью диапазона.

Рис. 4.1.35

Конфігурація ACL 4 на рис. 3.1.36 має два аналогічні записи, що використовуються в зворотному порядку. Це вірна послідовність записів, оскільки перший запис посилається на певний вузол, а не на діапазон вузлів.

```
R1(config)# access-list 4 permit host 192.168.10.10
R1(config)# access-list 4 deny 192.168.10.0 0.0.0.255
R1(config)#
```

Рис. 4.1.36

На рис. ACL 5 показує, що запис вузла можна додати після запису, що визначає діапазон вузлів, проте вузол не повинен знаходитися в межах діапазону, забороненого в попередньому записі. Адреса вузла 192.168.11.10 не є учасником мережі 192.168.10.0/24, тому запис є допустимим.

```
R1(config)# access-list 5 deny 192.168.10.0 0.0.0.255
R1(config)# access-list 5 permit host 192.168.11.10
R1(config)#
```

ACL-список 5. Запись узла можно сконфигурировать после записи диапазона при отсутствии конфликта.

Рис. 4.1.37

Система Cisco IOS змінює порядок записів в стандартних списках контролю доступу (ACL). Порядок, в якому маршрутизатор зберігає, відображає або обробляє стандартні записи списку контролю доступу (ACL), може не збігатися з порядком, в якому ці записи вводяться.

На рис. 3.1.37 показана конфігурація стандартних списків доступу. Оператори діапазону, що забороняють три мережі, налаштовуються в першу чергу, далі налаштовуються оператори інших п'яти вузлів. Всі записи host є коректними, оскільки IPv4-адреси, зазначені в записах host, що не входять у введені раніше діапазони забороняють адрес.

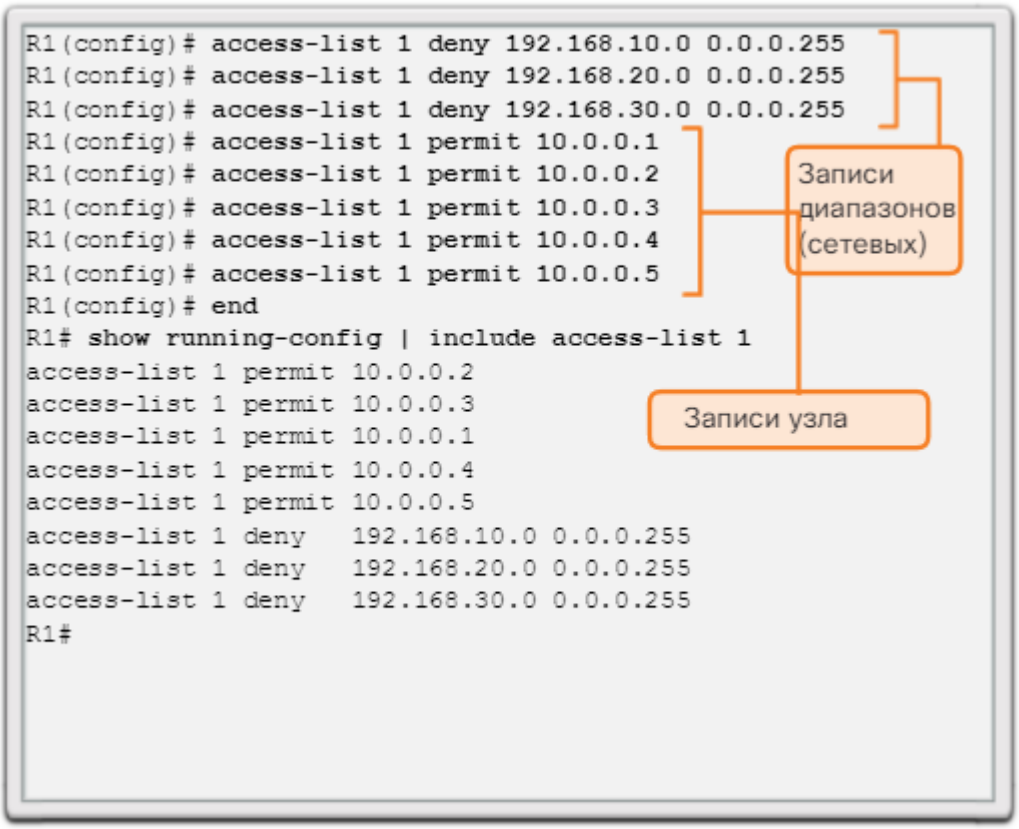


Рис. 4.1.38

Команда **show running-config** застосовується для перевірки конфігурації ACL-списку. Зверніть увагу, що оператори перераховані в іншому порядку, ніж вони були введені. Ми будемо використовувати команду **show access-lists**, щоб зрозуміти цю логіку.

Як показано на рис. 3.1.37 команда **show access-lists** відображає записи ACE відповідно до їх порядковими номерами. Можна очікувати, що у вихідних даних записи будуть відображені в такому самому порядку, в якому вони були введені. Однак вихідні дані команди **show access-lists** показують, що це не так.

Порядок, в якому перераховані стандартні ACE-записи - це послідовність, яка використовується IOS при обробці списку. Зверніть увагу, що записи згруповані в два розділи - оператори вузла йдуть після операторів діапазону. Порядковий номер вказує порядок, в якому записи були введені, а не порядок, в якому вони будуть оброблятися.

Оператори вузла перераховані першими, однак це не означає, що вони були додані в цьому порядку. IOS має оператори вузлів за допомогою спеціальної функції розстановки (hash function). В результаті такий порядок дозволяє оптимізувати пошук оператора вузла в ACL-списку. Оператори діапазону відображаються після операторів вузла. Ці оператори розташовуються в тому порядку, в якому вони були введені.

Примітка. Функція розстановки застосовується тільки до операторів вузла в стандартному списку контролю доступу IPv4. Докладні відомості про функції розстановки не розглядається в цій навчальній програмі.

Слід пам'ятати про те, що всі стандартні і нумеровані списки контролю доступу (ACL) можна редагувати за допомогою порядкових номерів. При додаванні нового запису в ACL-список порядковий номер буде впливати тільки

на розташування в списку оператора діапазону. Оператори вузла завжди будуть розташовуватися в певному порядку завдяки функції розстановки.

Повернемося до прикладу. Після збереження поточної конфігурації маршрутизатор перезавантажується. Як показано на малюнку 2, команда **show access-lists** відображає ACL-список в тому ж порядку, проте оператори перенумеровані. Порядкові номери тепер розташовані в цифровий послідовності.

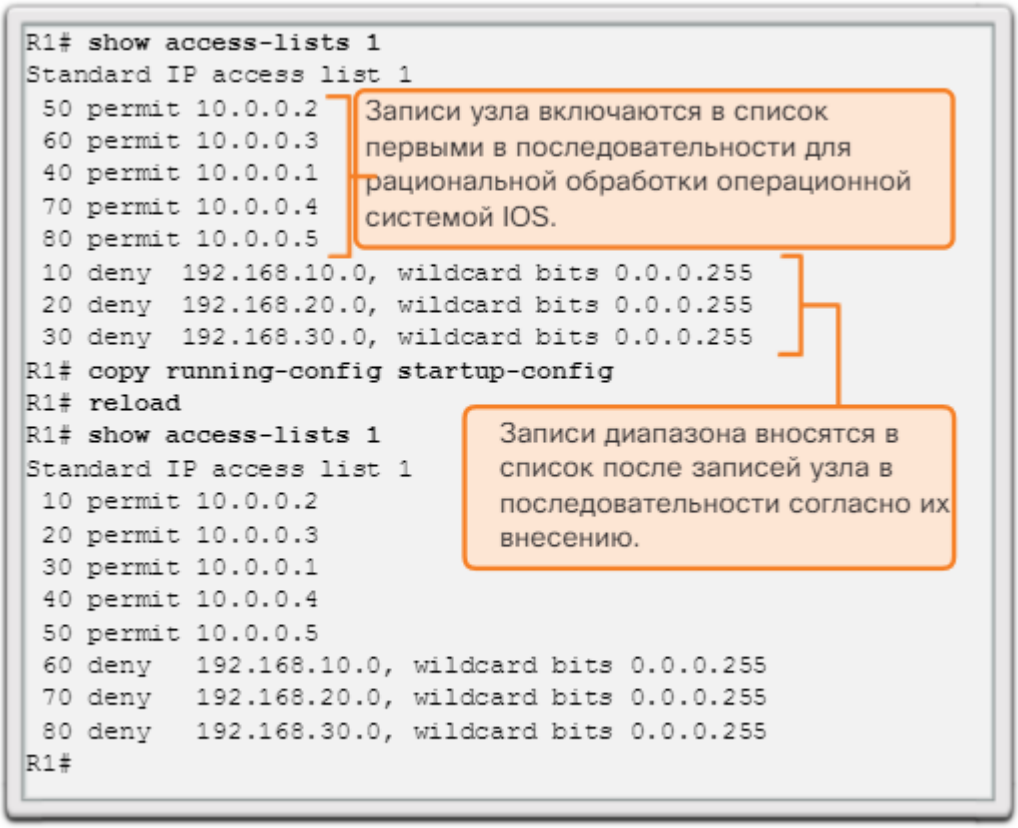


Рис. 4.1.39

Процеси маршрутизації і списки контролю доступу (ACL)

На рисунку 3.1.38 проілюстрована логіка роботи маршрутизації і процесів ACL-списку. При отриманні пакету на інтерфейс маршрутизатора процес маршрутизації залишається незмінним, незалежно від того, застосовуються ACL-списки чи ні. Оскільки кадр прибуває на інтерфейс, маршрутизатор перевіряє його на відповідність адреси призначення рівня 2 адресою інтерфейсу маршрутизатора рівня 2, і чи є кадр кадром широкомовної розсилки.

Якщо адреса кадру прийнятий, інформація кадру віддаляється, і маршрутизатор перевіряє наявність ACL-списку на вхідному інтерфейсі. При наявності ACL-списку пакет знову зіставляється із записами в списку.

Якщо пакет відповідає одному із записів, він приймається або відхиляється в залежності від умови, з яким він збігся. Якщо пакет приймається, він перевіряється на наявність відповідного запису в таблиці маршрутизації з метою визначення інтерфейсу призначення. Якщо для даного місця призначення існує запис в таблиці маршрутизації, пакет перенаправляється на вихідний інтерфейс, якщо записи немає - пакет відкидається.

Далі маршрутизатор перевіряє, чи є на вихідному інтерфейсі ACL-список. При наявності ACL-списку пакет знову зіставляється із записами в списку.

Якщо пакет відповідає одному із записів, він приймається або відхиляється в залежності від умови, з яким він збігся.

Якщо ACL-список відсутній, або пакету дозволено проходження, пакет інкапсулируется в новому протоколі рівня 2 і перенаправляється на інтерфейс наступного пристрою.

Приклад 1

Використання команд show, описаних в попередньому матеріалі, дозволяє виявити більшість поширених помилок ACL-списку. Найчастіше причиною проблем є введення записів списку в невірному порядку і використання некоректних правил при складанні списку контролю доступу (ACL). Нерідко допускаються помилки у виборі напрямку, інтерфейсу, а також адреси джерела, щодо яких застосовується список контролю доступу (ACL).

Політика безпеки. Комп'ютер PC2 не повинен мати доступ до файлового сервера. Як видно з 3.1.39, комп'ютер PC2 не має доступу до файлового серверу, проте для комп'ютера PC1 доступ також закритий. Висновок команди **show access-list** свідчить про те, що явний заборону доступу існує тільки для комп'ютера PC2. Однак в списку відсутня команда **permit**, яка розділяє доступ з інших адрес.

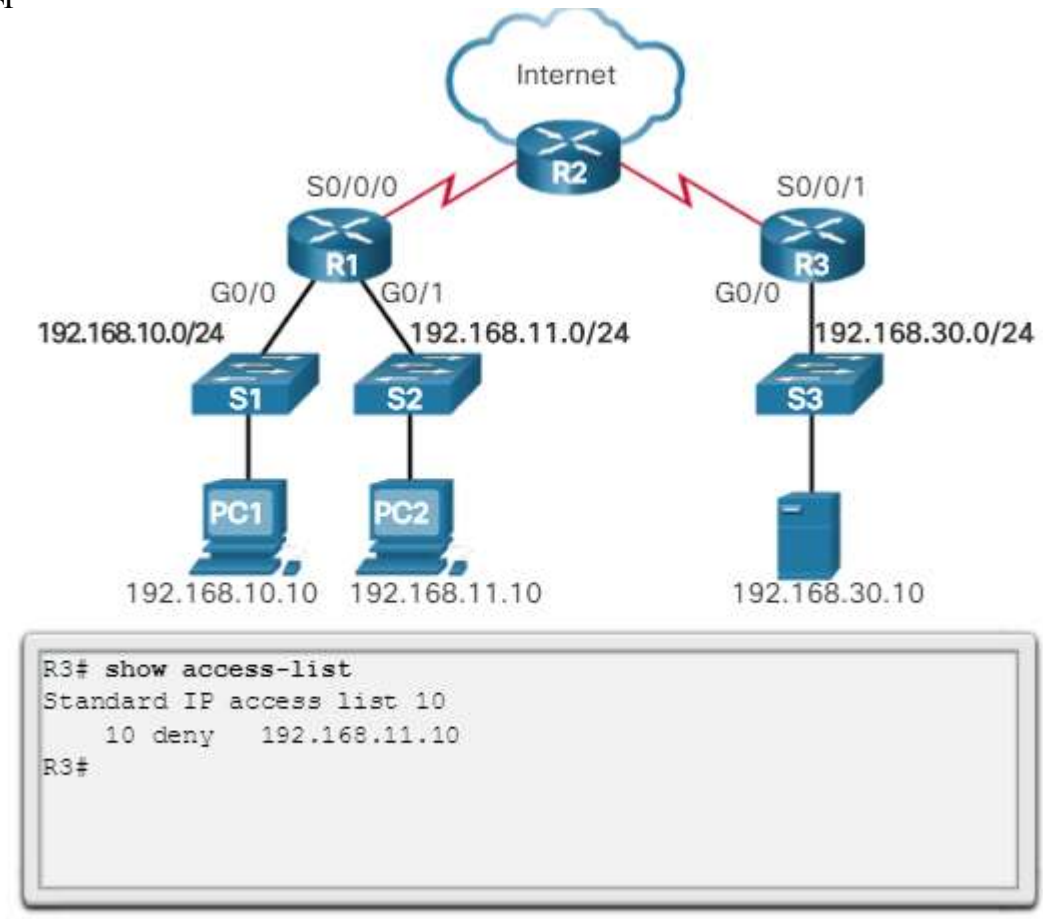


Рис. 4.1.40

Рішення. В даний час будь-який доступ з інтерфейсу G0/0 до локальної мережі 192.168.30.0/24 неявно заборонений. Необхідно додати в список контролю доступу (ACL) 10 відповідний запис, який дозволить інший трафік, як показано на рисунку 3.1.40. Тепер комп'ютер PC1 матиме доступ до файлового сервера. Висновок команди **show access-list** свідчить про те, що ping-

запит з комп'ютера PC1 на файловий сервер відповідає умові записи **permit any**.

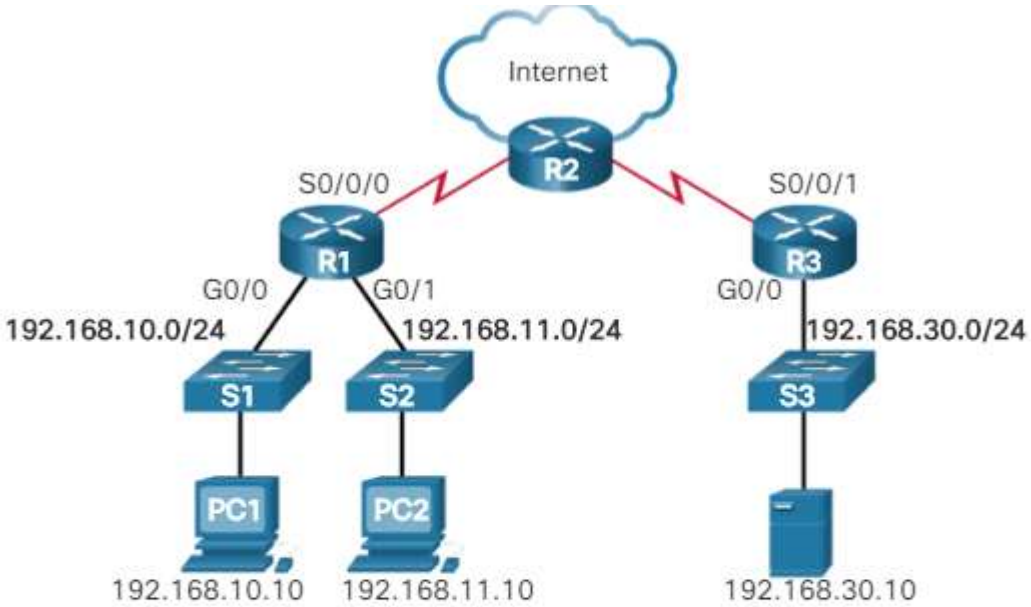
```
R3(config)# access-list 10 permit any
R3(config)# end
R3# show access-list
Standard IP access list 10
    10 deny   192.168.11.10
    20 permit any (4 match(es))
R3#
```

Рис. 4.1.41

Пошук і усунення неполадок - стандартні списки контролю доступу IPv4.

Приклад 2

Політика безпеки. Мережа 192.168.11.0/24 не повинна мати доступ до мережі 192.168.10.0/24.




```
R1# show access-list
Standard IP access list 20
    10 deny   192.168.11.10, wildcard bits 0.0.0.255 (8 match(es))
    20 permit any
```

Рис. 4.1.42

Згідно рисунку, комп'ютер PC2 не має доступу до комп'ютера PC1. Крім того, комп'ютер PC2 не має доступу в Інтернет через маршрутизатор R2. Висновок команди **show access-list** свідчить про те, що комп'ютер PC2 відповідає умові записи deny. Список контролю доступу (ACL) 20, мабуть, складений правильно. Ви припускаєте, що список неправильно застосований, і переглядаєте конфігурацію інтерфейсів маршрутизатора R1.

```
R1# show run | section interface
interface GigabitEthernet0/0
ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
interface GigabitEthernet0/1
ip address 192.168.11.1 255.255.255.0
```

Рис. 4.1.43

На рисунку 3.1.42 представлені дані, що виводяться командою **show run**, які відфільтровані таким чином, щоб відобразити лише дані про конфігурацію інтерфейсів. Результат роботи команди свідчить про те, що список контролю доступу (ACL) 20 помилково застосований до іншого інтерфейсу і в іншому напрямку. На інтерфейсі G0/1 заборонений будь-який трафік з мережі 192.168.11.0/24 у вхідному напрямку.

Рішення. Щоб усунути цю помилку, слід видалити список контролю доступу (ACL) 20 на інтерфейсі G0/1 і застосувати цей список до інтерфейсу G0/0 в вихідному напрямку, як показано на рисунку 3.1.43. Комп'ютер PC2 не має доступу до комп'ютера PC1, маючи при цьому доступ в Інтернет.

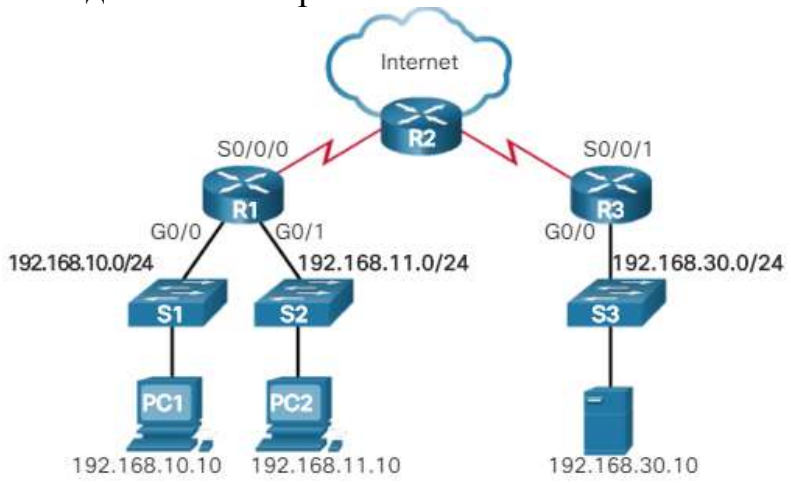
```
interface GigabitEthernet0/1
ip address 192.168.11.1 255.255.255.0
ip access-group 20 in
duplex auto
speed auto

<Данные опущены>
```

Рис. 4.1.44

Пошук і усунення неполадок - стандартні списки контролю доступу IPv4.

Приклад 3

Політика безпеки. Віддалений доступ до маршрутизатора R1 по протоколу SSH дозволений тільки для комп'ютера PC1.




```
R1# show run | section line vty
line vty 0 4
 access-class PC1-SSH in
 login
 transport input ssh
R1# show access-list
Standard IP access list PC1-SSH
```

Рис. 4.1.45

Згідно рисунку, комп'ютер PC1 не має віддаленого доступу до маршрутизатора R1 по протоколу SSH. Дані про VTY-лініях в поточній конфігурації свідчать про те, що список контролю доступу (ACL) з ім'ям PC1-SSH коректно застосований щодо вхідних з'єднань. VTY-лінії налаштовані правильно - дозволено встановлювати лише по протоколу SSH. Аналізуючи висновок команди **show access-list**, можна помітити, що IPv4-адрес відповідності не IPv4-адресою комп'ютера PC1, а інтерфейсу G0/0 маршрутизатора R1. Також зверніть увагу на те, що адміністратор застосував в списку контролю доступу (ACL) явну заборону deny any. Це цілком виправдано, оскільки в такому випадку ви будете бачити збіги, відповідні невдалим спробам з'єднання для віддаленого доступу до R1.

Рішення. Рисунок 3.1.45 ілюструє процедуру виправлення цієї помилки. Оскільки запис, що виправляється є першим, ми видаляємо його, використовуючи порядковий номер 10: **no 10**. Далі вказуємо коректний IPv4-адрес комп'ютера PC1. Команда **clear access-list** counters скидає виведену інформацію, щоб відобразити тільки нові збіги. З'єднання для віддаленого доступу до маршрутизатора R1 з комп'ютера PC2 встановлюється успішно, що підтверджується висновком команди show access-list (рис. 3.1.46)

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip access-list standard PC1-SSH
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 permit host 192.168.10.10
R1(config-std-nacl)# end
R1# clear access-list counters
```

Рис. 4.1.46

```
R1(config-std-nacl)# end
R1# clear access-list counters
R1# show access-list
Standard IP access list PC1-SSH
    10 permit 192.168.10.10 (2 match(es))
    20 deny   any
R1#
```

Рис. 4.1.47

За замовчуванням маршрутизатор не фільтрує трафік. Трафік, що надходить на маршрутизатор, ґрунтується виключно на даних таблиці маршрутизації.

За допомогою фільтрації пакетів здійснюється управління доступом до мережі шляхом аналізу вхідних і вихідних пакетів і пропускання або відкидання пакетів на основі таких критеріїв, як IP-адреса джерела, IP-адреса призначення і протокол всередині пакету. Маршрутизатор, фільтруючий пакети, використовує певні правила при пропуску або відхилення трафіку. Маршрутизатор також може фільтрувати пакети на рівні 4 - транспортному рівні.

ACL-список є послідовним списком, який дозволяє або забороняє оператори. Останнім записом ACL-списку завжди є непрямий відмова, яка

блокує весь трафік. Для того щоб виключити неявну заборону deny any, які присутні в кінці кожного списку контролю доступу (ACL) і блокують весь трафік, можна додати дозвіл **permit any**.

При проходженні мережевого трафіку через інтерфейс, де діє список контролю доступу (ACL), маршрутизатор послідовно зіставляє інформацію з пакета з кожним записом в списку контролю доступу на предмет відповідності. Якщо пошук був успішним, пакет обробляється відповідно до умовою ACL-списку, з яким він збігся.

ACL-списки налаштовуються для застосування до вхідного або вихідного трафіку.

Стандартні ACL-списки можна використовувати для вирішення або відхилення проходження трафіку тільки на основі IPv4-адрес джерела. Місце призначення пакета і порти, які беруть участь в передачі даних, не оцінюються. Основним правилом розміщення стандартного ACL-списку є його розміщення максимально близько до місця призначення.

Розширені списки ACL фільтрують пакети на основі декількох атрибутів: тип протоколу, IPv4-адрес джерела або призначення і порти джерела або призначення. Основним правилом розміщення розширеного ACL-списку є його розміщення в максимальному наближенні до джерела.

Команда глобальної конфігурації **access-list** визначає стандартний список контролю доступу (ACL) з номером в діапазоні від 1 до 99. Команда **ip access-list standard** Ім'я застосовується для створення стандартного іменованого списку контролю доступу (ACL).

Після настройки ACL-списку він підключається до інтерфейсу за допомогою команди **ip access-group** в режимі настройки інтерфейсу. Необхідно пам'ятати наступні правила щодо списків контролю доступу (ACL):

- один список на один протокол,
- один список на один напрямок,
- дин список на один інтерфейс.

Для видалення всього ACL-списку з інтерфейсу спочатку слід ввести команду **no ip access-group** на інтерфейсі, а потім ввести глобальну команду **no access-list**.

Для перевірки налаштування ACL-списку використовуються команди **show running-config і show access-lists**. Команда **show ip interface** використовується для перевірки ACL-списку на інтерфейсі і напрямки, до якого був прив'язаний список.

Команда **access-class**, введена в режимі конфігурації лінії, обмежує вхідні та вихідні з'єднання між окремими VTY і адресами в списку доступу.

4.2 Огляд протоколу DHCP та його базові характеристики

Для кожного пристрою, підключеного до мережі, потрібно унікальний IP-адресу. Мережеві адміністратори привласнюють статичні IP-адреси маршрутизаторів, серверів, принтерів та інших мережевих пристроїв, чий фізичний і логічне розташування, швидше за все, не зміниться. У більшості випадків мова йде про пристрої, що надають служби користувачам або пристроям в мережі; таким чином, що привласнюються їм адреси повинні бути постійними. Крім того, статичні адреси дозволяють адміністраторам керувати цими пристроями віддалено. Мережевим адміністраторам простіше отримати доступ до пристрою, якщо його IP-адресу легко визначити.

Однак в організації часто змінюється фізичний і логічне місце розташування користувачів і комп'ютерів. Присвоєння нових IP-адрес при кожному переміщенні співробітника може являти собою складний і трудомісткий процес. При настройці параметрів мережі для співробітників, що працюють з віддалених місць, адміністратор також може зіткнутися з низкою труднощів. Крім того, присвоєння IP-адрес вручну і настройка іншої інформації про адресації для настільних ПК також вимагає зусиль і тимчасових витрат системного адміністратора, особливо в разі розширення мережі.

Впровадження сервера з протоколом динамічної конфігурації вузла (DHCP) в локальну мережу спрощує процес присвоєння IP-адрес як стаціонарним, так і мобільних пристроїв. Використання централізованого сервера DHCP дозволяє організації управляти присвоєнням всіх динамічних IP-адрес з одного сервера. Подібна практика робить управління IP-адресацією більш ефективної і забезпечує послідовність процесів і узгодженість даних по всій організації, включаючи філії.

Протокол DHCP доступний як для IPv4 (DHCPv4), так і IPv6 (DHCPv6). У цій главі описуються функції, настройка, а також пошук і усунення неполадок протоколів DHCPv4 і DHCPv6.

DHCPv4 привласнює IPv4-адреси та інші мережеві параметри динамічно. Оскільки стаціонарні ПК зазвичай складають основну частину мережевих вузлів, протокол DHCPv4 є вкрай корисним інструментом, що дозволяє мережевим адміністраторам значно економити час.

Виділений DHCPv4-сервер масштабується і відносно легкий в управлінні. Однак в невеликому філії або домашньому офісі (SOHO) маршрутизатор Cisco можна налаштувати для забезпечення DHCPv4-служб без необхідності у виділеному сервері. ПО Cisco IOS підтримує додатковий повнофункціональний сервер DHCPv4.

Сервер DHCPv4 динамічно призначає або видає в оренду IPv4-адрес з пулу адрес на обмежений період часу на вибір сервера або до тих пір, поки у клієнта є необхідність в адресі.

Клієнти орендують дані у сервера на період, визначений адміністратором. Адміністратори налаштовують сервери DHCPv4 таким чином, щоб термін оренди закінчувався в різний час. Термін оренди зазвичай становить від 24 годин до тижня або більше. Після закінчення терміну оренди клієнт повинен запросити іншу адресу, хоча в більшості випадків клієнтові повторно призначається той же адресу.

Протокол динамической конфигурации узла сети (DHCP)

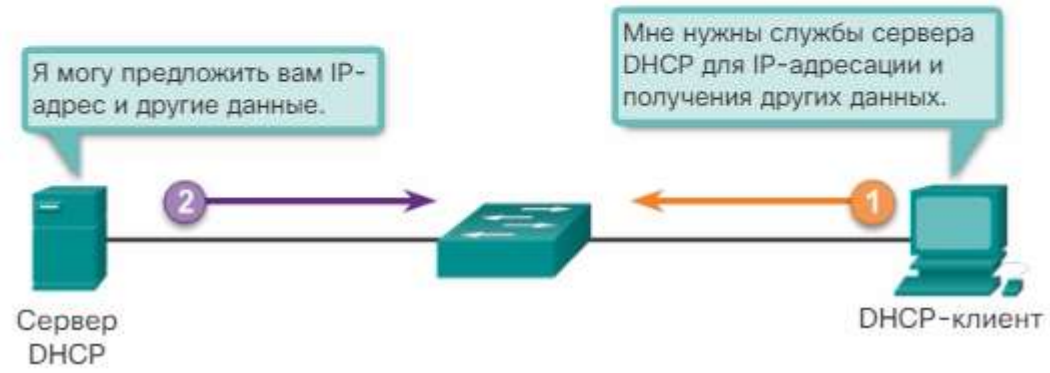


Рис. 4.2.1

Як показано на рис., DHCPv4 працює по моделі «клієнт-сервер». Коли клієнт підключається до сервера DHCPv4, сервер привласнює або здає йому в оренду IPv4-адрес. Клієнт з орендованим IP-адресою підключається до мережі до закінчення терміну оренди. Періодично клієнт повинен зв'язуватися з DHCP-сервером для продовження терміну оренди. Завдяки подібному механізму «переїхали» або відключити клієнти не займають адреси, в яких вони більше не мають потреби. Після закінчення терміну оренди сервер DHCP повертає адресу в пул, з якого адреса може бути повторно отриманий при необхідності.

Первісна оренда

При початковому завантаженні клієнта (або інший спосіб підключення до мережі) починається 4-кроковий процес отримання адреси в оренду. Як показано на рис. 2, клієнт починає процес з повідомлення DHCPDISCOVER широкомовної розсилки зі свого MAC-адреси з метою виявлення доступних DHCPv4-серверів.

Виявлення DHCP (DHCPDISCOVER)

Повідомлення DHCPDISCOVER знаходить в мережі DHCPv4-сервери. Оскільки під час завантаження у клієнта немає вірної IPv4-інформації, для зв'язку з сервером використовуються широкомовні адреси рівня 2 і рівня 3.

Пропозиція DHCP (DHCPOFFER)

Коли сервер DHCPv4 отримує повідомлення DHCPDISCOVER, він резервує доступні IPv4-адреси для видачі в оренду клієнту. Сервер також створює запис ARP, що складається з MAC-адреси запитувача клієнта і виданого клієнту IPv4-адреси. Як показано на рис. 3, DHCPv4-сервер посилає повідомлення прив'язки DHCPOFFER запитувачу клієнту. Адресою джерела одноадресної розсилки повідомлення DHCPOFFER є MAC-адресу рівня 2 сервера, адресою призначення - MAC-адресу рівня 2 клієнта.

Запит DHCP (DHCPREQUEST)

Коли клієнт отримує від сервера повідомлення DHCPOFFER, він відправляє у відповідь повідомлення DHCPREQUEST, як показано на рис. 4. Це повідомлення використовується як для первісної оренди адреси, так і для її продовження. Коли повідомлення використовується при первісної оренді,

DHCPREQUEST служить повідомленням про прийняття пропозиції прив'язки до запропонованих сервером параметрам і непрямим відхиленням для всіх інших серверів, які могли надати клієнту пропозицію прив'язки.

У корпоративних мережах часто використовується кілька DHCPv4-серверів. Повідомлення DHCPREQUEST відправляється в формі широкомовної розсилки з метою інформування даного DHCPv4-сервера та інших DHCPv4-серверів про те, що пропозиція була прийнята.

Підтвердження DHCP (DHCPACK)

При отриманні повідомлення DHCPREQUEST, сервер перевіряє, чи не використовується видається в оренду IP-адреса за допомогою відправки луна-запиту по протоколу ICMP на цю адресу. Після цього сервер створює новий запис ARP для клієнтської оренди і відповідає повідомленням одноадресної розсилки DHCPACK, як показано на рис. 5. Повідомлення DHCPACK є копією повідомлення DHCPOFFER, за винятком зміни в поле типу повідомлення. При отриманні повідомлення DHCPACK клієнт завантажує інформацію про конфігурацію і виконує ARP-перевірку присвоєного адреси. Якщо ARP-відповіді немає, значить, IPv4-адрес доступний, і клієнт починає використовувати його в якості власного адреси.

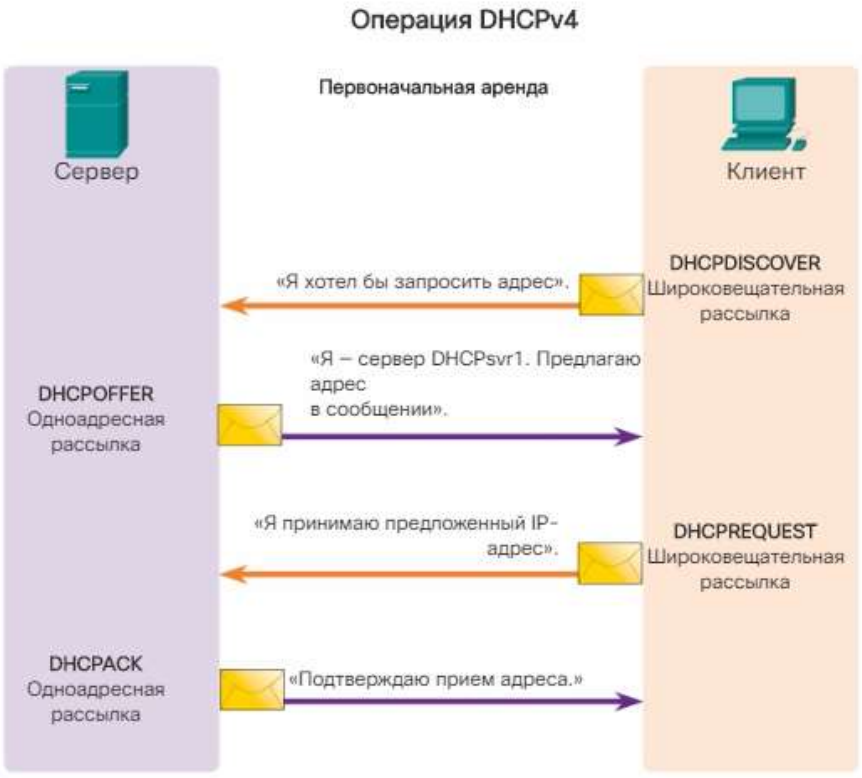


Рис. 4.2.2

Як показано на рис. 6, перед закінченням оренди клієнт відправляє повідомлення DHCPREQUEST безпосередньо DHCPv4-сервера, який спочатку запропонував IPv4-адрес. Якщо повідомлення DHCPACK ніхто не почув за певний період часу, клієнт відправляє інше повідомлення DHCPREQUEST широкомовної розсилкою, щоб інший DHCPv4-сервер міг продовжити термін оренди.

Рис. 4.2.3

При отриманні повідомлення DHCPREQUEST сервер підтверджує інформацію про оренду відповідним повідомленням DHCPACK, як показано на рис. 7.

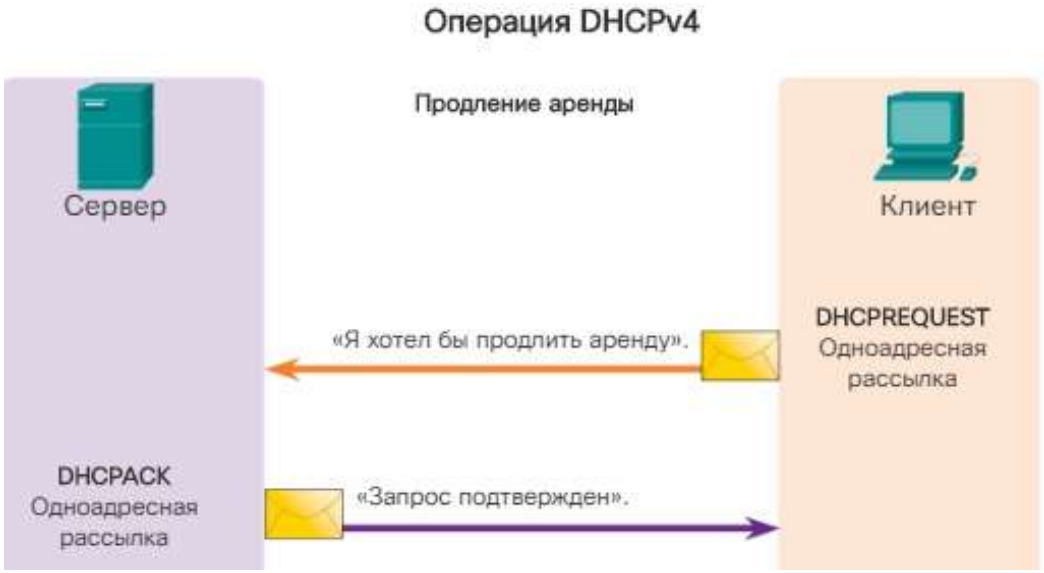


Рис. 4.2.4

Формат повідомлень DHCPv4

Для всіх транзакцій DHCPv4 використовується однаковий формат повідомлень DHCPv4. Повідомлення DHCPv4 інкапсулюється в рамках транспортного протоколу UDP. Повідомлення DHCPv4 відправляються від клієнта через протокол UDP з порту джерела 68 в порт призначення 67. Повідомлення DHCPv4 відправляються з сервера через протокол UDP з порту джерела 67 в порт призначення 68.

На малюнку показаний формат повідомлення DHCPv4. Повідомлення містить наступні поля:

Код операції (OP) -зазначає загальний тип повідомлення. Значення 1 означає повідомлення-запит; значення 2 - повідомлення-відповідь.

Тип обладнання - визначає тип апаратного обладнання, що використовується в мережі. Наприклад, 1 - Ethernet, 15 - Frame Relay, 20 - послідовна лінія. Ці ж коди використовуються в повідомленнях ARP.

Довжина фізичної адреси - задає довжину адреси.

Переходи - управління процесом передачі повідомлення. Встановлюється клієнтом на 0 перед відправкою повідомлення-запиту.

Ідентифікатор транзакції - використовується клієнтом для узгодження запиту з відповідями від DHCPv4-серверів.

Секунди - позначають кількість секунд, пройдених з моменту, коли клієнт почав намагатися отримати або продовжити оренду. Використовується DHCPv4-серверами для розстановки пріоритетності відповідей, в разі кількох клієнтських запитів.

Прапори - застосовуються клієнтом, який не знає свого IPv4-адреси при відправленні запиту. Використовується тільки один з 16 біт, який є прапором широкомовної розсилки. Значення 1 в цьому полі повідомляє DHCPv4-сервера або агенту-ретранслятору, що приймає запит, що відповідь буде надіслана в формі широкомовної розсилки.

IP-адреса клієнта - використовується клієнтом при продовженні оренди, коли клієнт має власний дійсний і використовуваний IP-адреса, але не в процесі первісного його отримання. Клієнт підставляє власний IPv4-адрес в це поле тільки в разі, якщо у нього є діючий IPv4-адрес, що співпадає з раніше призначеним; в іншому випадку значення поля встановлюється на 0.

Ваш IP-адреса - використовується сервером для присвоєння нового IPv4-адреси клієнта.

IP-адреса сервера - застосовується сервером для розпізнавання адреси сервера, який клієнт повинен використовувати для наступного кроку в процесі самонастроювання. Цей сервер може бути (або не бути) сервером, що посилає відповідь. Сервер, який посилає відповідь, завжди включає власний IPv4-адрес в окреме поле - опцію Код сервера DHCPv4.

IP-адреса шлюзу - направляє DHCPv4-повідомлення при використанні агентів-ретрансляторів DHCPv4. Використання заданого адреси шлюзу спрощує передачу DHCPv4- запитів і відповідей між клієнтом і сервером, які знаходяться в різних підмережах або мережах.

Фізична адреса клієнта - вказує фізичний рівень клієнта.

Ім'я сервера - використовується сервером, які відправляють повідомлення DHCPOFFER або DHCPACK. Дане поле є необов'язковим для заповнення. Іменем сервера може бути простий текстовий псевдонім або доменне ім'я DNS-сервера, як наприклад dhcpserver.netacad.net.

Файл завантаження – опціональне поле, яке використовується клієнтом для запиту файлу завантаження певного типу за допомогою повідомлення DHCPDISCOVER. Застосовується сервером в повідомленні DHCPOFFER для точного завдання директорії файлу завантаження і імені файлу.

Опції DHCP - поле включає в себе опції DHCP, а також деякі параметри, необхідні для основних операцій протоколу DHCP. Довжина цього поля змінюється. Поле може використовуватися як клієнтом, так і сервером.

Формат сообщений DHCPv4

Рис. 4.2.5

Повідомлення виявлення і пропозиції DHCPv4

У разі якщо до мережі хоче підключитися клієнт з настройками на динамічне отримання налаштувань IPv4, він запитує значення адресації від DHCPv4-сервера. Передача клієнтом повідомлення DHCPDISCOVER в локальну мережу відбувається під час завантаження клієнта або у разі виявлення ним активного мережного підключення. Оскільки клієнт не може знати, до якої підмережі він відноситься, повідомлення DHCPDISCOVER є широкомовлення IPv4 (IPv4-адрес призначення 255.255.255.255). Оскільки у клієнта ще немає налаштованого IPv4-адреси, використовується IPv4-адрес джерела - 0.0.0.0.

Як показано на рис. 1, IPv4-адрес клієнта (CIADDR), адреса основного шлюзу (GIADDR) і маска підмережі в повідомленні DHCPDISCOVER відповідають вибраному адресою 0.0.0.0.

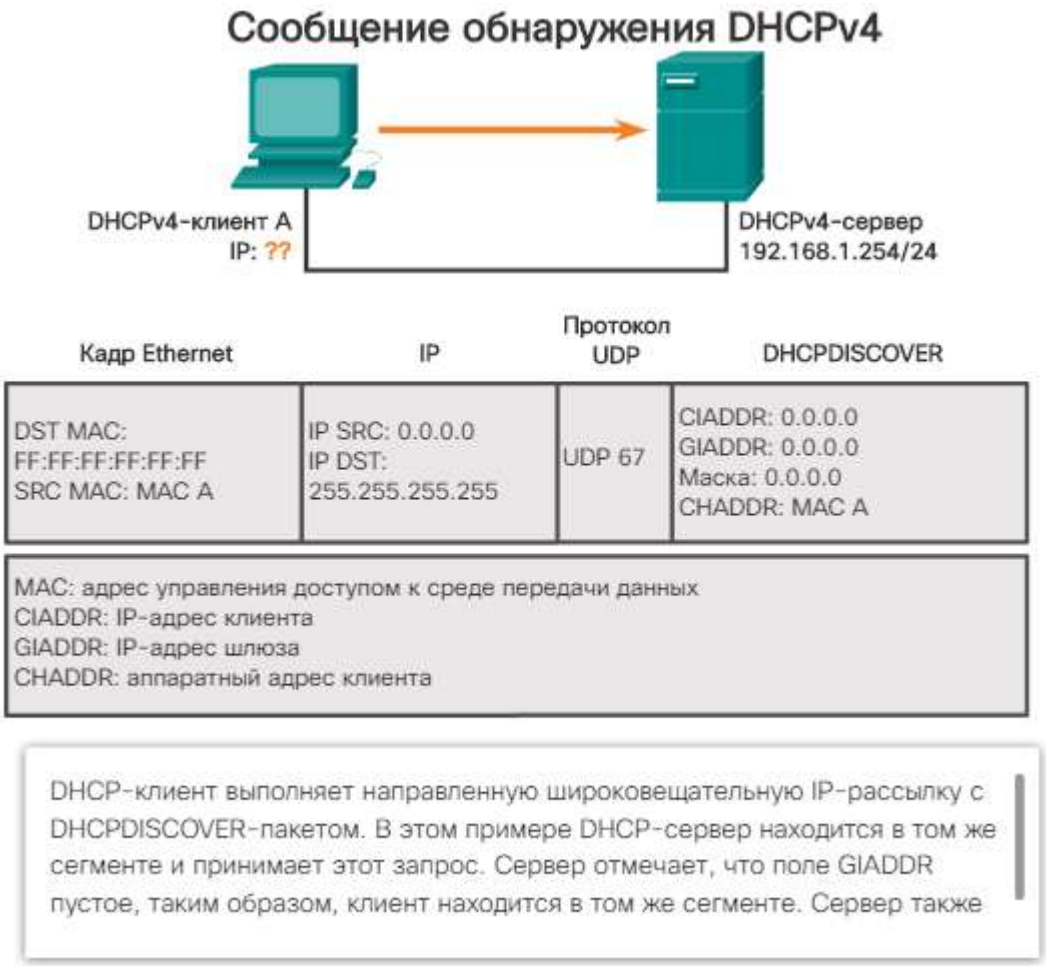


Рис. 4.2.6

Примітка . Невідомі дані відправляються як 0.0.0.0.

DHCPv4-сервер відповідає на повідомлення DHCPDISCOVER повідомленням DHCPOFFER. Це повідомлення містить попередні налаштування для клієнта, включаючи IPv4-адрес, запропонований сервером, маску підмережі, термін оренди і IPv4-адрес DHCPv4-сервера, від якого виходить пропозицію.

Повідомлення DHCPOFFER може бути також налагоджено для утримання додаткових даних, таких як час поновлення оренди і адреса DNS-сервера.

Як показано на рис. 2, сервер DHCP відповідає на повідомлення DHCPDISCOVER, висилаючи значення IP-адреси (CIADDR) і маски підмережі. Використовуючи фізичну адресу пристрою-клієнта (CHADDR), сервер створює і відправляє кадр запитувачу клієнту.

Рис. 4.2.7

Для завершення процесу клієнт і сервер відправляють повідомлення підтвердження.

Зазвичай маршрутизатори бездротового зв'язку, що використовуються в домашньому або малому офісі, підключені до інтернет-провайдера через DSL або кабельний модем. У більшості випадків маршрутизатори бездротового зв'язку налаштовані на автоматичне отримання IPv4-адрес від інтернет-провайдера.

Як приклад на малюнку показана сторінка налаштування глобальної мережі за замовчуванням для бездротового маршрутизатора в Packet Tracer. Зверніть увагу, що в якості типу веб-з'єднання вибрано **Automatic Configuration - DHCP** (Автоматична настройка - DHCP). Цей параметр використовується, коли маршрутизатор підключений до кабельного або DSL-модему і виступає в якості DHCPv4-клієнта, запитуючи IPv4-адрес у інтернет-провайдера.

Рис. 4.2.8

Завдання пошуку та усунення неполадок

Існує безліч причин виникнення проблем у роботі протоколу DHCPv4: несправності програмного забезпечення операційних систем, драйверів мережевого адаптера або агентів DHCP-ретрансляції. Проте найбільш поширеною причиною неполадок є неправильна конфігурація. Через велику кількість потенційних проблемних областей при пошуку і усунення неполадок потрібний системний підхід, як показано на рис. 1.

Поиск и устранение неполадок в работе DHCPv4

Поиск и устранение неполадок. Задача 1.	Разрешение конфликтов адресов.
Поиск и устранение неполадок. Задача 2.	Проверка физического соединения..
Поиск и устранение неполадок. Задача 3.	Проверка с использованием статическим IPv4-адресом.
Поиск и устранение неполадок. Задача 4.	Проверка конфигурации порта коммутатора.
Поиск и устранение неполадок. Задача 5.	Проверка работы протокола в той же подсети или VLAN.

Рис. 4.2.9

Пошук і усунення неполадок. Завдання 1. Вирішення конфліктів IPv4-адрес

У клієнта, підключеного до мережі, може закінчитися термін оренди IPv4-адреси. Якщо клієнт не відновить оренду, DHCPv4-сервер може перепризначити цей IPv4-адрес іншому клієнту. Після перезавантаження клієнт запросить IPv4-адрес. Якщо DHCPv4-сервер не дасть відповідь досить швидко, клієнт буде використовувати IPv4-адрес, що використовувався в останній раз. Виникає ситуація, коли два клієнта використовують один IPv4-адрес, створюючи конфлікт.

Команда **show ip dhcp conflict** відображає всі конфлікти адрес, зареєстровані DHCPv4-сервером (див. Рис. 2). Для виявлення клієнта сервером використовується команда **ping** . Для виявлення конфлікту клієнт використовує протокол дозволу адрес (ARP). При виявленні конфлікту адреса видаляється з пулу і не присвоюється до усунення конфлікту адміністратором.

Просмотр конфликтов DHCPv4

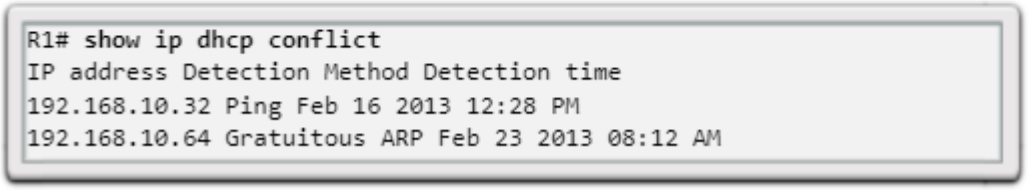


Рис. 4.2.10

Вихідні дані відображають IP-адреси, що конфліктують з сервером DHCP. В даних вказано метод виявлення (detection method) і час виявлення (detection time) конфліктуючих IP-адрес, запропонованих сервером DHCP.

Пошук і усунення неполадок. Завдання 2. Перевірка фізичного з'єднання

Спочатку використовуйте команду **show interfaces** *інтерфейс,* щоб переконатися, що інтерфейс маршрутизатора, який діє у ролі основного шлюзу для клієнта, функціонує. Якщо статус інтерфейсу відрізняється від статусу up, трафік (включаючи запити DHCP-клієнта) не проходить через порт.

Пошук і усунення неполадок. Завдання 3. Перевірка зв'язності з використанням статичного IP-адреси

При проведенні робіт по виявленню і усуненню несправностей будь-якої несправності DHCPv4 необхідно перевірити зв'язність шляхом настройки статичної IPv4-адресації на клієнтської робочої станції. Якщо робочої станції не вдається отримати доступ до мережевих ресурсів, незважаючи на наявність статично налаштованого IPv4-адреси, DHCPv4 не є джерелом проблеми. У цьому випадку необхідно провести перевірку мережевого підключення.

Пошук і усунення неполадок. Завдання 4. Перевірка настройки порту комутатора

У разі якщо DHCPv4-клієнт не може отримати IPv4-адрес від DHCPv4-сервера при завантаженні, варто спробувати отримати IPv4-адрес від DHCPv4-сервера, вручну відправивши DHCPv4-запит з пристрою-клієнта.

Примітка . Якщо між клієнтом і DHCPv4-сервером є комутатор, і клієнт не може отримати настройки DHCP, причиною можуть служити неполадки в налаштуванні порту комутатора. Причиною можуть бути проблеми, пов'язані зі створенням транкових і логічних каналів, а також з протоколами STP і RSTP. Рішенням найбільш часто виникаючих проблем клієнта DHCPv4, що відбуваються при першій установці комутатора Cisco, може стати настройка розширення PortFast і прикордонного порту.

Пошук і усунення неполадок. Завдання 5. Діагностика роботи протоколу DHCPv4 в тій же підмережі або VLAN

Важливо розрізняти, чи правильно функціонує DHCPv4 як DHCPv4-сервера, коли клієнт знаходиться в тій же підмережі або VLAN. У разі якщо протокол DHCPv4 працює коректно за умови, що клієнт знаходиться в тій же

підмережі або VLAN, проблема може полягати в агента DHCP-ретрансляції. Якщо неполадки зберігаються навіть при перевірці роботи DHCPv4 в тій же підмережі або VLAN в якості DHCPv4-сервера, проблема зазвичай полягає в DHCPv4-сервері.

На малюнку показана таблиця, яка містить п'ять завдань по виявленню і усуненню несправностей, пов'язаних з DHCPv4.

Перевірка налаштувань DHCPv4 на маршрутизаторі

Коли DHCPv4-сервер розташований в окремій від клієнта LAN, інтерфейс маршрутизатора, відповідний клієнту, повинен бути налаштований на ретрансляцію DHCPv4-запитів за допомогою настройки допоміжного IPv4-адреси. Якщо допоміжний IPv4-адрес налаштований невірно, клієнтські DHCPv4-запитом не будуть пересилатися на DHCPv4-сервер.

Для перевірки налаштувань маршрутизатора виконайте наступні дії:

Крок 1. Переконайтеся, що команда **ip helper-address** виконана на правильному інтерфейсі. Команда повинна бути виконана на вхідному інтерфейсі LAN, що містить робочі станції DHCPv4-клієнта, і спрямована на вірний DHCPv4-сервер. Вихідні дані команди **show running-config** , показані на малюнку, підтверджують, що DHCPv4-ретрансляція IPv4-адреси звертається до DHCPv4-сервера з адресою 192.168.11.6.

Команда **show ip interface** також може використовуватися для перевірки роботи DHCPv4-ретрансляції на інтерфейсі.

Крок 2. Переконайтеся, що не було виконане команда глобальної конфігурації **no service dhcp** . Дана команда відключає всі функціональні можливості DHCP-сервера та ретрансляції на маршрутизаторі. Команда **service dhcp** не відображається при виведенні поточної конфігурації, оскільки є налаштованої за замовчуванням.

На малюнку команда **show running-config | include no service dhcp** підтверджує, що служба DHCPv4 запущена, так як немає збігів для команди **show running-config | include no service dhcp** . Якщо служба була відключена, команда **no service dhcp** буде відображена в вихідних даних.

На малюнку показаний результат виконання команди show running-config pipe section interface gigabit Ethernet 0/0. Вихідні дані будуть містити параметри конфігурації для зазначеного інтерфейсу, в тому числі всі параметри DHCP. На малюнку вихідні дані містять IP-адреса і адреса допоміжної служби IP. Далі на малюнку показаний результат виконання команди show running-config pipe include no service dhcp. У наведеному прикладі вихідні дані відсутні.

Проверка работы DHCPv4-ретрансляции и службы DHCPv4

```
R1# show running-config | section interface GigabitEthernet0/0
interface GigabitEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 192.168.11.6
 duplex auto
 speed auto
R1#

R1# show running-config | include no service dhcp
R1#
```

Рис. 4.2.11

налагодження DHCPv4

Якщо маршрутизатор, конфігурований як DHCPv4-сервера, не отримує запити від клієнта, процес DHCPv4 не може бути виконаний. Необхідно виконати одну з задач по виявленню і усуненню несправностей для підтвердження того, що маршрутизатор отримує DHCPv4-запит від клієнта. Цей крок пошуку та усунення неполадок включає настройку списку контролю доступу (ACL) для налагоджувальних вихідних даних.

Примітка. Хоча можна скопіювати розширений список ACL, представлений на малюнку, і використовувати його для фільтрації повідомлень DHCP, в рамках даного курсу настройка розширених списків ACL не розглядається.

На малюнку представлений розширений ACL-список, що допускає пакети тільки з портом призначення UDP 67 або 68. Дані порти стандартно використовуються DHCPv4-клієнтами і серверами при відправці повідомлень DHCPv4. Для відображення тільки повідомлень протоколу DHCPv4 розширений ACL-список застосовується з командою **debug ip packet** .

Вихідні дані, відображені на малюнку, вказують, що маршрутизатор отримує DHCP-запити від клієнта. IP-адреса джерела - 0.0.0.0, оскільки клієнт ще не отримав IP-адреса. Адреса призначення - 255.255.255.255, так як повідомлення виявлення DHCP від клієнта відправлено широкомовної розсилкою. Вихідні дані відображають лише частину даних пакета, а не саме повідомлення DHCPv4. Проте, маршрутизатор отримав пакет широкомовної розсилки з IP-адресами джерела і призначення і портом UDP, вірним для DHCPv4. Повні налагоджувальні вихідні дані відображають всі пакети DHCPv4-обміну між DHCPv4-сервером і DHCPv4-клієнтом.

На малюнку представлений розширений список ACL, що допускає пакети тільки з портом призначення UDP 67 або 68. Перша команда: access-list 100 permit udp any eq 67. Друга команда: access-list 100 permit udp any eq 68. Потім, як показано на малюнку , запускається команда: debug ip packet 100. Вона використовується для перегляду активності, відповідної списку ACL 100, який є списком ACL, який налаштований для вирішення DHCP. На малюнку показаний маршрутизатор, який одержує два пакети широкомовної розсилки з

вихідного IP-адреси 255.255.255.255, які є запитами DHCP. Остання команда на малюнку: debug ip dhcp server events. Ця команда буде повідомляти про події сервера, а на малюнку показана активність DHCP на сервері. Цей процес включає в себе IP-адреса, повернутий в пул, а також призначений IP-адреса.

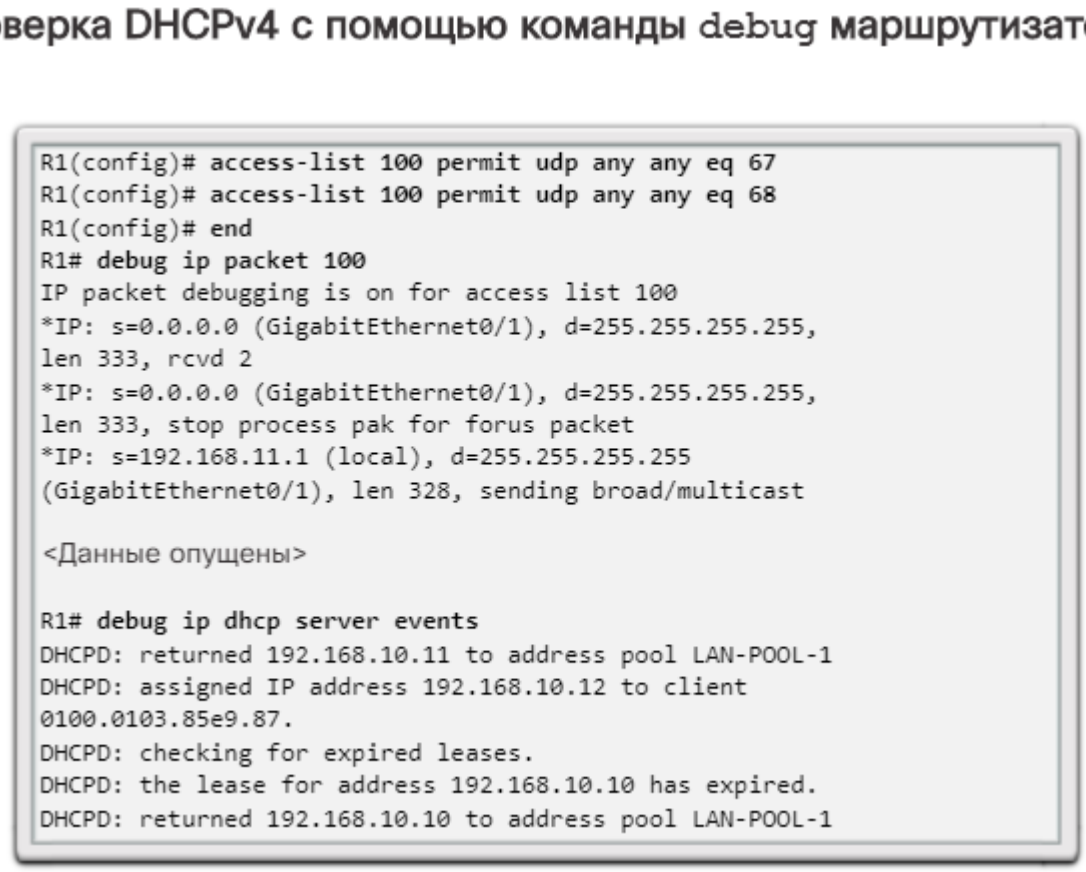


Рис. 4.2.12

Автоматична настройка без збереження стану адреси (Stateless Address Autoconfiguration, SLAAC)

Як і у випадку з IPv4-адресами, глобальні індивідуальні IPv6-адреси можна налаштувати вручну або динамічно. При цьому існує два методи, за допомогою яких глобальні індивідуальні IPv6-адреси можуть бути присвоєні динамічно:

Автоматична настройка адреси без відстеження стану (SLAAC), показана на малюнку

Протокол динамічної конфігурації мережного вузла (DHCP) для протоколу IPv6 (зі збереженням стану DHCPv6)

Загальні відомості про SLAAC

Автоматична настройка адреси без відстеження стану (SLAAC) - це спосіб отримання пристроєм глобального IPv6-адреси одноадресної розсилки без використання DHCPv6-сервера. В основі SLAAC лежить протокол ICMPv6. Протокол ICMPv6 аналогічний ICMPv4, але при цьому він має додаткові функціональні можливості і демонструє більшу стійкість до помилок. SLAAC використовує ICMPv6-повідомлення запиту маршрутизатора і оголошення маршрутизатора, щоб надати інформацію про адресації і іншу інформацію про конфігурацію, зазвичай надається DHCP-сервером.

Повідомлення запиту маршрутизатора (RS) - якщо клієнт налаштований на отримання інформації про адресації автоматично з використанням SLAAC, він посилає на маршрутизатор повідомлення RS. Повідомлення RS

відправляється на IPv6-адреса під LGPL FF02 :: 2, який підтримують всі маршрутизатори.

Повідомлення оголошення маршрутизатора (RA) - для надання інформації про адресації маршрутизатор відправляє повідомлення RA клієнтам, налаштованим на отримання IPv6-адрес автоматично. Повідомлення RA містить префікс і довжину префікса локального сегмента. Ця інформація використовується клієнтом для створення власного глобального індивідуального IPv6-адреси. Маршрутизатор передає повідомлення RA періодично або у відповідь на повідомлення RS. За замовчуванням маршрутизатори Cisco відправляють подібні повідомлення кожні 200 секунд. Повідомлення RA завжди відправляються на загальний для всіх вузлів IPv6-адреса під LGPL FF02 :: 1.

Як видно з терміну, SLAAC не відслідковує стан адреси. Служба без відстеження стану говорить про те, що жоден із серверів не підтримує інформацію про мережевому адресу. На відміну від сервера DHCP, сервер SLAAC не знає, які IPv6-адреси використовуються, а які доступні.

На малюнку показаний комутатор, до якого підключені маршрутизатор і комп'ютер. Комп'ютер посилає повідомлення IPv6 із запитом на доступність маршрутизаторів - це багатоадресне повідомлення для всіх маршрутизаторів. Маршрутизатор отримує це повідомлення і відповідає оголошенням - це багатоадресне повідомлення IPv6 для всіх вузлів.

Рис. 4.2.13

Принцип роботи SLAAC

Перш ніж роутер зможе відправляти повідомлення RA, на ньому повинна бути включена маршрутизація IPv6, як показано нижче.

Router (config) # **ipv6 unicast-routing**

1. У прикладі топології, показаної на рис. 1, комп'ютер PC1 налаштований на автоматичне отримання IPv6-адреси. З моменту завантаження PC1 не отримав повідомлень RA, тому він відправляє повідомлення RS на адресу під

LGPL, який підтримують всі маршрутизатори, щоб проінформувати локальний IPv6-маршрутизатор про необхідність отримання повідомлення RA.

Рис. 4.2.14

2. Як показано на рис. 2, R1 отримує повідомлення RS і відправляє у відповідь повідомлення RA. У повідомлення RA включені префікс і довжина префікса мережі. Повідомлення RA відправлено на загальний для всіх вузлів IPv6-адреса під LGPL FF02 :: 1 з адресою каналу маршрутизатора типу link-local як IPv6-адреси джерела.

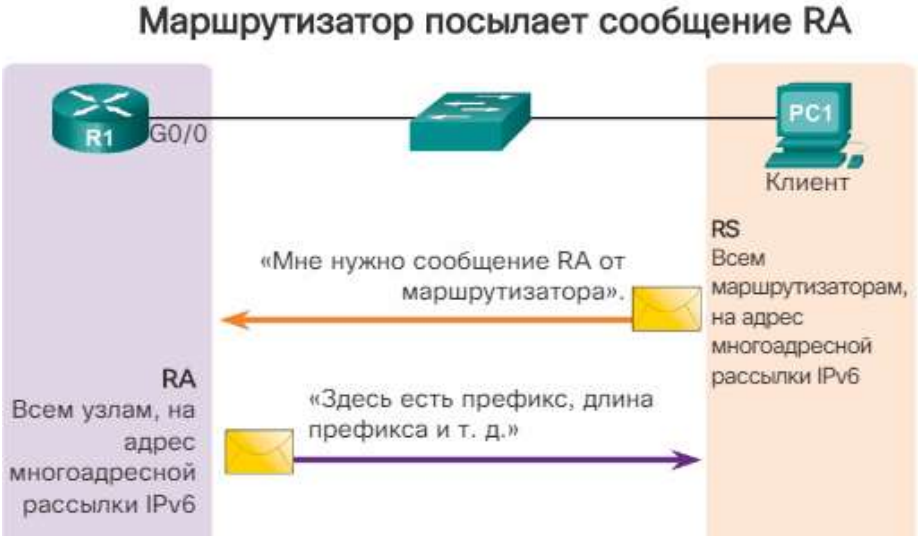


Рис. 4.2.15

3. PC1 отримує повідомлення RA, що містить префікс і довжину префікса для локальної мережі. PC1 буде використовувати цю інформацію для створення власного глобального індивідуального IPv6-адреси. PC1 має тепер 64-розрядний префікс мережі, але вимагає 64-бітний ідентифікатор інтерфейсу (IID) для створення глобального індивідуальної адреси.

Існує для способу створення PC1 власного унікального IID:

EUI-64 - за допомогою процесу EUI-64 PC1 створює IID, використовуючи свій 48-бітний MAC-адресу.

Генерація випадковим чином - 64-бітний IID може бути випадковим числом, що згенерував операційною системою клієнта.

Як показано на рис. 3, PC1 може створити 128-бітний глобальний індивідуальний IPv6-адреса з комбінації 64-бітного префікса і 64-бітного IID. PC1 буде використовувати локальний адресу каналу маршрутизатора в якості IPv6-адреси основного шлюзу.

Рис. 4.2.16

4. Оскільки SLAAC - це процес без відстеження стану, комп'ютер PC1 повинен перевірити, що новий створений IPv6-адреса є унікальним, перш ніж його використовувати. Як показано на рис. 4, комп'ютер PC1 відправляє ICMPv6-повідомлення із запитом пошуку сусідів зі спеціально сформованим груповою адресою, який називається груповою адресою запитуваної вузла. Ця електронна адреса дублює останні 24 біта IPv6-адреси комп'ютера PC1. Якщо інші пристрої не відповідають повідомленням з оголошенням сусідів, значить, практично гарантовано, що адреса є унікальним і може бути використаний PC1. Якщо повідомлення запиту пошуку сусідів отримано PC1, значить, адреса не унікальний і операційна система повинна встановити новий ідентифікатор інтерфейсу для використання.

Цей процес є частиною процесу виявлення сусідніх пристроїв ICMPv6 і відомий як виявлення адрес-дублікатів (DAD).

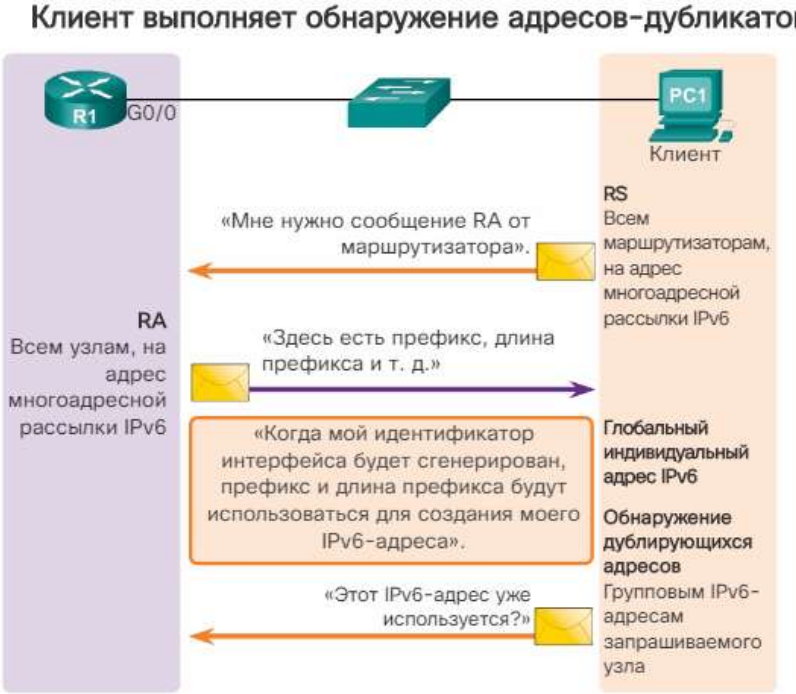


Рис. 4.2.17

SLAAC і DHCPv6

Чи налаштовано клієнт на автоматичне отримання інформації про IPv6-адресації з використанням SLAAC, DHCPv6 або поєднанням обох варіантів, залежить від налаштувань, що містяться в повідомленні RA.

Цими прапорами є прапор керованої конфігурації адрес (M) і прапор іншої конфігурації (O).

Як показано на малюнку, використовуючи різні поєднання прапорів M і O, повідомлення RA вибирають один з трьох варіантів адресації пристрої IPv6:

SLAAC (тільки оголошення маршрутизатора);

протокол DHCPv6 без відстеження стану (оголошення маршрутизатора і DHCPv6);

протокол DHCPv6 з відстеженням стану (тільки DHCPv6).

Незалежно від обраного варіанту, в запиті для коментарів RFC 4861 рекомендується, щоб всі пристрої протоколу IPv6 виконували процес виявлення адрес-дублікатів (DAD) будь-якої адреси одноадресної розсилки, включаючи адреси, сконфігуровані з використанням SLAAC або DHCPv6. Процес DAD виконується через протокол ICMPv6, який визначений в RFC 4443.

Примітка . Повідомлення RA визначає процес, який повинен бути використаний клієнтом при отриманні IPv6-адреси динамічно, однак операційна система клієнта може ігнорувати повідомлення RA і використовувати тільки DHCPv6-сервер.

На малюнку показано три варіанти повідомлення з оголошенням від маршрутизатора. Перший варіант - SLAAC, при якому маршрутизатор вказує комп'ютера, щоб він використовував тільки інформацію з повідомлення RA. Цей параметр настройки діє за замовчуванням. Другий варіант - DHCPv6 без відстеження стану з використанням SLAAC і DHCP. У цьому варіанті маршрутизатор надає інформацію в повідомленні з оголошенням, але також вказує комп'ютеру отримувати деякі дані з сервера DHCPv6. Третій варіант - з відстеженням стану DHCP. У цьому варіанті маршрутизатор вказує комп'ютеру отримувати всі дані з сервера DHCPv6.

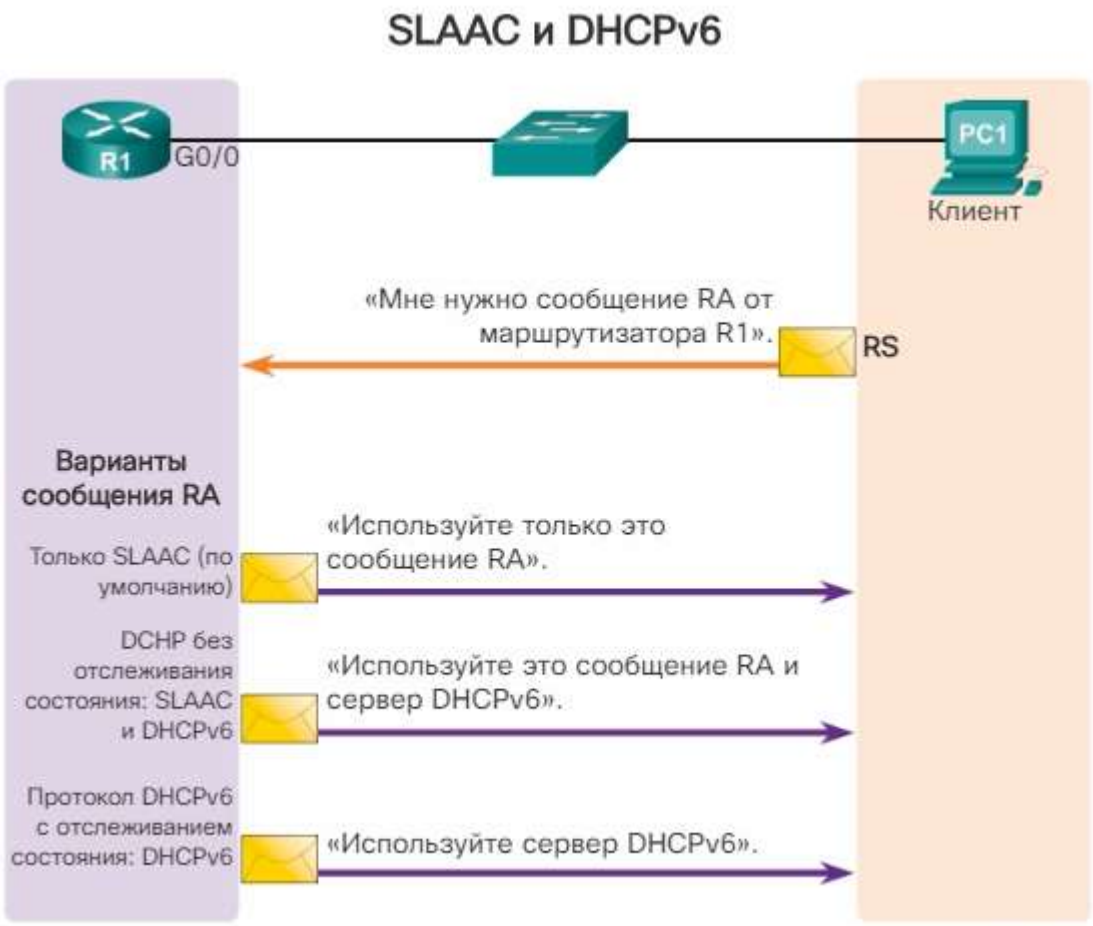


Рис. 4.2.18

функція SLAAC

Функція SLAAC (тільки оголошення маршрутизатора)

Функція SLAAC є функцією за замовчуванням на маршрутизаторах Cisco. На малюнку показано, що значення обох прапорів (M і O) в повідомленні RA встановлено на 0.

Цей варіант вказує клієнту використовувати тільки інформацію з повідомлення RA. Сюди входить інформація про префікс, довжині префікса, DNS-сервері, MTU і інформація про шлюзі за замовчуванням. Далі клієнт не отримує ніякої інформації від сервера DHCPv6. Глобальний індивідуальний IPv6-адреса створюється шляхом об'єднання префікса, отриманого в повідомленні RA, і ідентифікатора інтерфейсу, отриманого за допомогою EUI-64 або згенерованого випадковим чином.

Повідомлення RA налаштовані на вказаному інтерфейсі маршрутизатора. Для повторної активації режиму SLAAC на інтерфейсі, на якому міг бути встановлений інший варіант роботи, прапори M і O необхідно скинути на їх початкові значення, рівні 0. Для цього застосовуються такі команди режиму конфігурації інтерфейсу:

Router (config-if) # **no ipv6 nd managed-config-flag**

Router (config-if) # **no ipv6 nd other-config-flag**

На малюнку показаний процес SLAAC для комп'ютера. Маршрутизатор відправляє повідомлення з оголошенням, що містить всі дані про адресації, необхідні комп'ютера. Це відповідь на повідомлення запиту на доступність маршрутизаторів, відправлене комп'ютером.

Рис. 4.2.19

DHCPv6 без відстеження стану

Незважаючи на те що протокол DHCPv6 аналогічний DHCPv4 в своїх функціональних можливостях, два протоколи незалежні один від одного. Протокол DHCPv6 визначається в RFC 3315. Над специфікацією протоколу працювали протягом багатьох років, на що вказує найвищий номер редакції документа RFC про протокол DHCPv6 серед інтернет-документів.

Функція протоколу DHCPv6 без відстеження стану (оголошення маршрутизатора і DHCPv6)

DHCPv6 без відстеження стану повідомляє клієнту про використання інформації в повідомленні RA для адресації, при цьому додаткові параметри конфігурації доступні з сервера DHCPv6.

Глобальний індивідуальний IPv6-адреса створюється клієнтом за допомогою префікса і довжини префікса в повідомленні RA і додавання ідентифікатора IID, створеного процесом EUI-64 або згенерованого випадковим чином.

Після цього клієнт зможе зв'язатися з DHCPv6-сервером без відстеження стану для отримання додаткової інформації, що не наданої в повідомленні RA. Такою інформацією може бути, наприклад, список IPv6-адрес DNS-серверів. Цей процес відомий як протокол DHCPv6 без відстеження стану, оскільки сервер не підтримує жодну інформацію про стан клієнта, тобто список доступних і розподілених IPv6-адрес. DHCPv6-сервери без відстеження стану надають тільки параметри конфігурації для клієнта, але не виділяють IPv6-адреси.

Для DHCPv6 без відстеження стану значення прапора O встановлено рівним 1, а значення прапора M залишається зі значенням за замовчуванням, рівним 0. Значення прапора O, рівне 1, використовується для інформування клієнта про те, що на DHCPv6-сервері без відстеження стану про наявність додаткової інформації про конфігурацію.

Для того щоб змінити повідомлення RA, що відправляється на інтерфейс маршрутизатора для вказівки використання DHCPv6 без відстеження стану, використовуйте наступну команду:

Router (config-if) # **ipv6 nd other-config-flag**

На малюнку показаний процес DHCPv6 без відстеження стану для комп'ютера. Маршрутизатор відправляє повідомлення з оголошенням, що містить деякі дані про адресації, необхідні комп'ютера, а також вказівку комп'ютера, що йому необхідно знайти сервер DHCPv6 для отримання залишилася інформації. Це відповідь на повідомлення запиту на доступність маршрутизаторів, відправлене комп'ютером.

Рис. 4.2.20

DHCPv6 з відстеженням стану

Протокол DHCPv6 з відстеженням стану (тільки DHCPv6)

Даний варіант найбільш схожий з використанням з протоколу DHCPv4. В цьому випадку в повідомленні RA клієнту вказують не використовувати інформацію про адресації з повідомлення RA. Вся інформація про адресації і конфігурації повинна бути отримана від сервера DHCPv6 з відстеженням стану. DHCPv6 з відстеженням стану отримав таку назву тому, що сервер DHCPv6 підтримує інформацію про стан протоколу IPv6. Робота сервера аналогічна роботі сервера DHCPv4, розподіляє IPv4-адреси.

Прапор M вказує, чи використовується DHCPv6 з відстеженням стану. Прапор O не використовується. Для того щоб змінити значення прапора M з 0 на 1 для оголошення DHCPv6 з відстеженням стану, застосовується наступна команда:

Router (config-if) # **ipv6 nd managed-config-flag**

На малюнку показаний процес DHCPv6 з відстеженням стану для комп'ютера. Маршрутизатор відправляє повідомлення з оголошенням, яке не містить ніяких даних про адресації, і вказівка комп'ютера знайти сервер

DHCPv6 для отримання всієї необхідної інформації. Це відповідь на повідомлення запиту на доступність маршрутизаторів, відправлене комп'ютером.

Рис. 4.2.21

процеси DHCPv6

Як показано на рис. 1, робота DHCPv6 з відстеженням або без відстеження стану починається з повідомлення RA, відправленого від маршрутизатора за протоколом ICMPv6. Повідомлення RA може відправлятися періодично або у відповідь на запит пристрою, що відправив повідомлення RS.

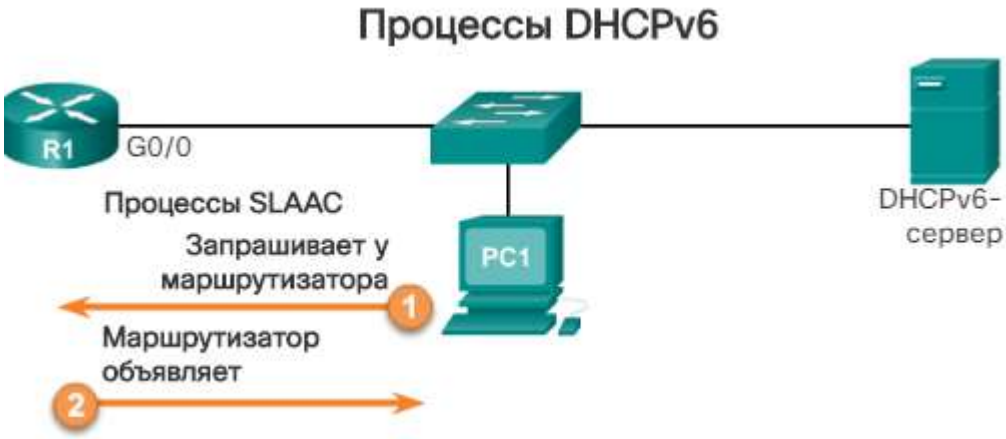


Рис. 4.2.22

Якщо варіант роботи DHCPv6 вказано в повідомленні RA, пристрій починає передачу інформації за схемою клієнт-сервер з використанням DHCPv6.

Обмін повідомленнями по протоколу DHCPv6

У разі якщо в повідомленні RA вказано варіант роботи DHCPv6 (з відстеженням стану або без), ініціюється робота DHCPv6. Повідомлення протоколу DHCPv6 надсилаються через протокол UDP. Повідомлення DHCPv6 від сервера до клієнта використовують UDP порт призначення 546. Клієнт відправляє повідомлення на сервер DHCPv6 через UDP порт призначення 547.

Клієнту - тепер DHCPv6-клієнту - необхідно визначити місце розташування сервера DHCPv6. На рис. 2 клієнт передає повідомлення DHCPv6 SOLICIT на зарезервований IPv6-адреса під LGPL FF02 :: 1: 2, який використовується усіма DHCPv6 серверами. Ця електронна адреса була під LGPL діє в рамках каналу link-local. Це означає, що маршрутизатори не направляють повідомлення в інші мережі.

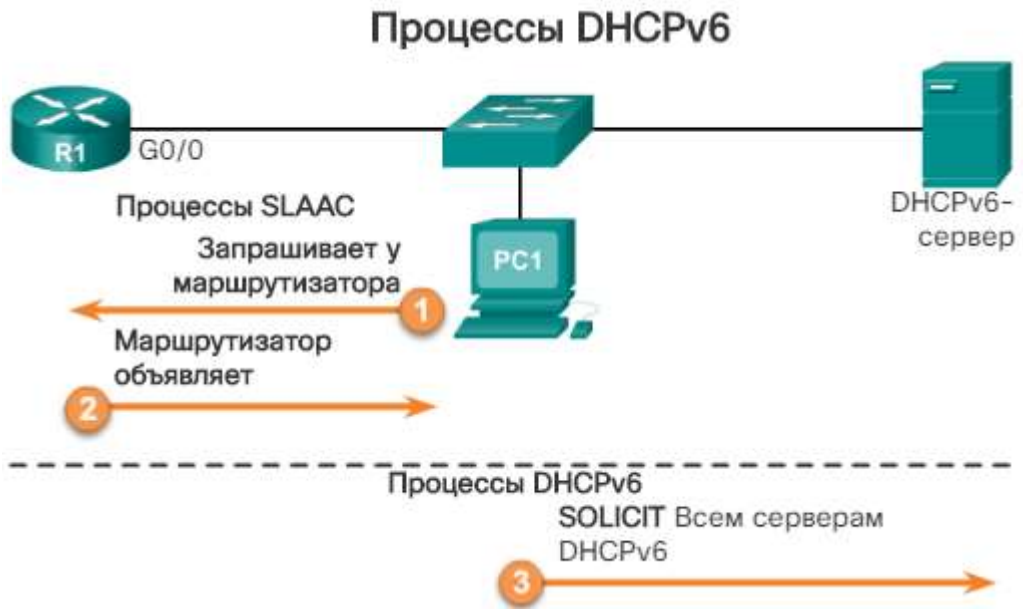


Рис. 4.2.23

Один або кілька серверів DHCPv6 відповідають одноадресна DHCPv6-повідомленням ADVERTISE, як показано на рис. 3. Повідомлення ADVERTISE повідомляє DHCPv6-клієнту, що сервер доступний для надання служби DHCPv6.

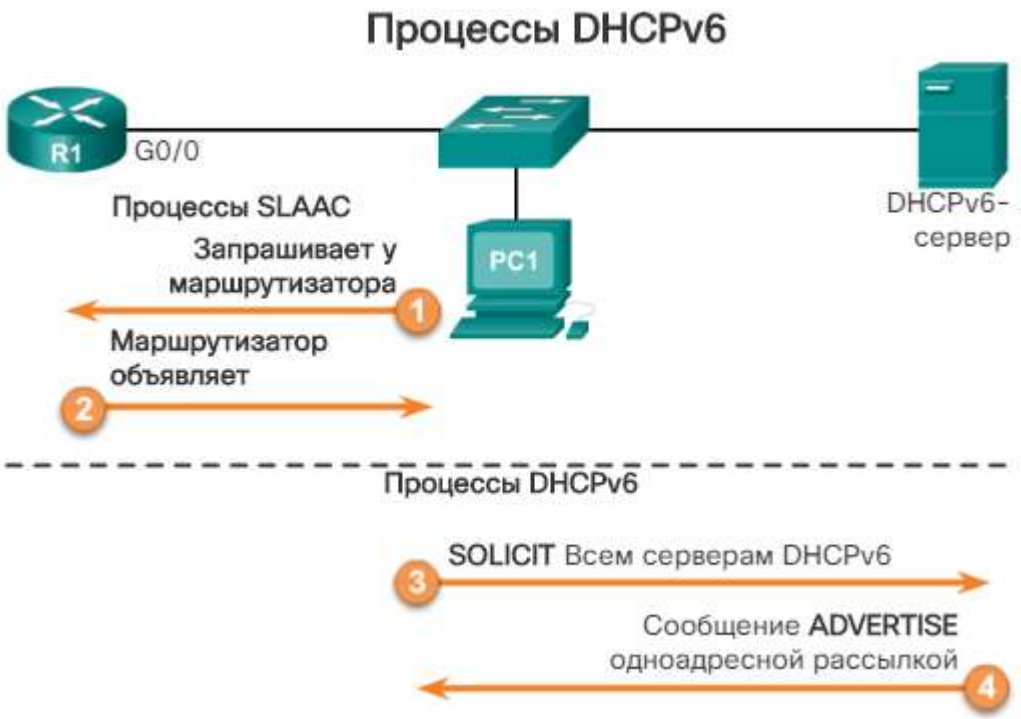


Рис. 4.2.24

На рис. клієнт відповідає сервера DHCPv6 одноадресна повідомленням REQUEST або INFORMATION-REQUEST в залежності від того, чи є DHCPv6-сервер сервером з відстеженням стану або без нього.

Рис. 4.2.25

DHCPv6-клієнт без відстеження стану - клієнт відправляє DHCPv6 повідомлення INFORMATION-REQUEST сервера DHCPv6, запитуючи тільки параметри конфігурації, наприклад, адреса DNS-сервера. Клієнт створює

власний IPv6-адреса за допомогою префікса з повідомлення RA і ідентифікатора інтерфейсу, що самогенерується.

DHCPv6-клієнт з відстеженням стану - клієнт відправляє DHCPv6 повідомлення REQUEST сервера для отримання IPv6-адреси і всіх інших конфігурацію з сервера.

На рис. 5 показано, як сервер відправляє клієнту одноадресна повідомлення DHCPv6 REPLY, що містить інформацію, запитану в повідомленні REQUEST або INFORMATION-REQUEST.

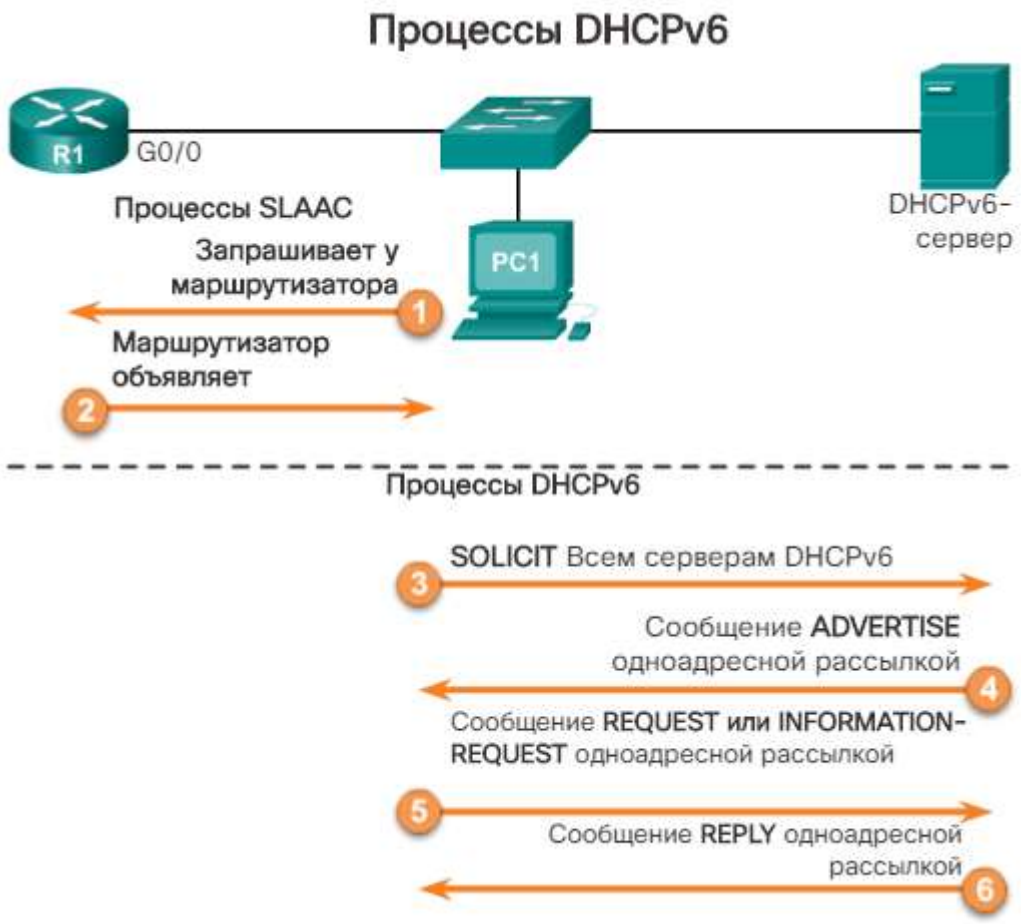


Рис. 4.2.26

Налаштування маршрутизатора в якості DHCPv6-сервера без відстеження стану

На рис. представлені чотири кроки налаштування маршрутизатора для роботи в якості DHCPv6-сервера:

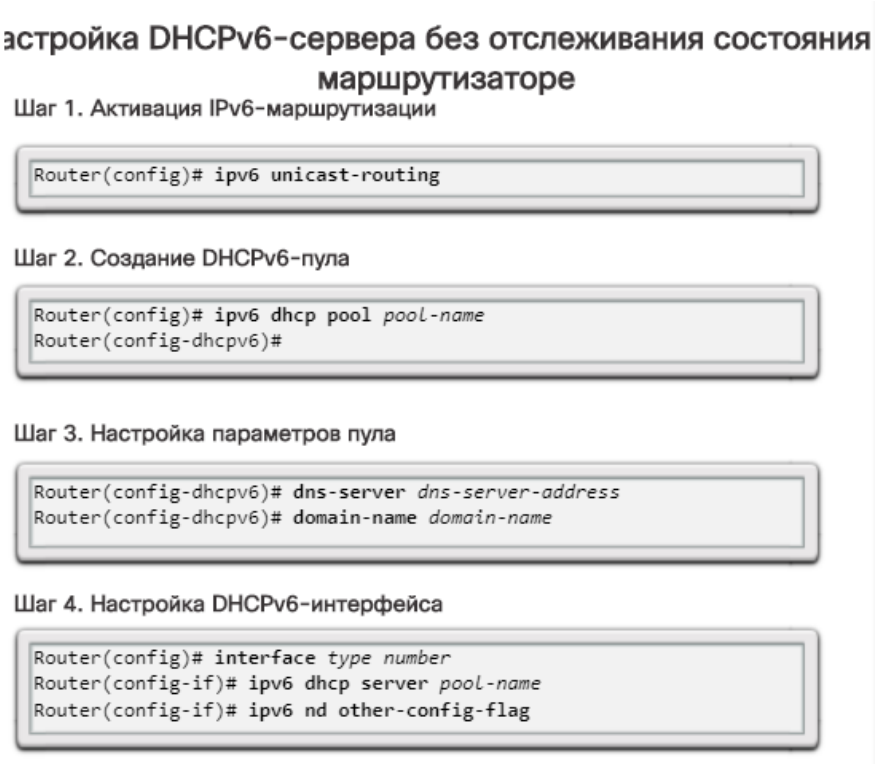


Рис. 4.2.27

Крок 1. Активація IPv6-маршрутизації

Для активації IPv6-маршрутизації необхідно виконати команду **ipv6 unicast-routing** . Виконання цієї команди не є необхідним для настройки маршрутизатора в якості DHCPv6-сервера без відстеження стану, але потрібно для маршрутизатора, щоб відправляти повідомлення RA по протоколу ICMPv6.

Крок 2. Створення DHCPv6-пулу

Команда **ipv6 dhcp pool** *pool-name* створює пул і переводить маршрутизатор в режим конфігурації DHCPv6, який визначається рядком запиту Router (config-dhcpv6) #.

Крок 3. Налаштування параметрів пулу

За допомогою функції SLAAC клієнт отримує інформацію, необхідну для створення глобального індивідуального IPv6-адреси. Клієнт також отримує інформацію про шлюзі за замовчуванням, використовуючи IPv6-адреса джерела повідомлення RA, який є адресою типу link-local маршрутизатора. При цьому сервер DHCPv6 без відстеження стану можна налаштувати для надання інформації, яка могла не бути включена в повідомлення RA, наприклад, адреси DNS-сервера і доменного імені.

Крок 4. Налаштування DHCPv6-інтерфейсу

Команда **ipv6 dhcp server** *pool-name* в режимі конфігурації інтерфейсу прив'язує створений пул DHCPv6 до інтерфейсу. Маршрутизатор відповідає на DHCPv6-запити на цьому інтерфейсі інформацією, що міститься в пулі. Значення прапора O необхідно змінити з 0 на 1, використовуючи команду інтерфейсу **ipv6 nd other-config-flag** . Повідомлення RA, відправлені на цей інтерфейс, вказують, що додаткова інформація доступна на DHCPv6-сервері без відстеження стану.

Приклад сервера DHCPv6 без відстеження стану

На рис. 2 наведено приклад конфігурації маршрутизатора, який повинен бути налаштований як DHCPv6-сервера без відстеження стану. Зверніть увагу, що маршрутизатор R3 зображений як DHCPv6-клієнт. R3 налаштований в якості клієнта для перевірки роботи DHCPv6 без відстеження стану.


```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
```

Рис. 4.2.28

Налаштування маршрутизатора в якості DHCPv6-клієнта без відстеження стану

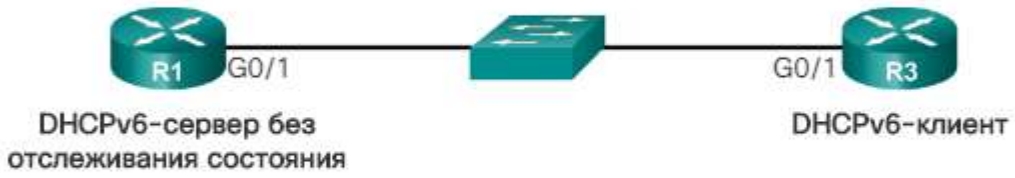
У прикладі на малюнку маршрутизатор Cisco використовується в якості клієнта DHCPv6. Наведений сценарій не є типовим і наводиться лише для демонстрації. У більшості випадків DHCPv6-клієнтом без відстеження стану виступає такий пристрій, як комп'ютер, планшет, мобільний пристрій або веб-камера.

Маршрутизатора, що працює в якості клієнта, необхідно мати IPv6-адреса типу link-local на інтерфейсі для відправки та отримання повідомлень IPv6, таких як повідомлення RS і DHCPv6. Адреса типу link-local (локальний адресу каналу) маршрутизатора створюється автоматично при включенні протоколу IPv6 на інтерфейсі. Включення IPv6 відбувається при налаштуванні глобального індивідуального адреси на інтерфейсі або за допомогою команди **ipv6 enable** . Після того як маршрутизатор отримує локальний адресу каналу, він може брати участь у виявленні сусідніх пристроїв IPv6.

У наведеному прикладі команда **ipv6 enable** використовується з огляду на те, що маршрутизатор ще не має глобального індивідуальної адреси.

Команда **ipv6 address autoconfig** включає автоматичне налаштування IPv6-адресації з використанням SLAAC. Припустимо, сервер-маршрутизатор налаштований в режимі DHCPv6 без відстеження стану. Таким чином, він відправляє повідомлення RA, щоб повідомити клієнту-маршрутизатора про те, що можна використовувати DHCPv6 без відстеження стану для отримання відомостей DNS.

астройка маршрутизатора в качестве DHCPv6-клиента без отслеживания состояния




```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address autoconfig
R3(config-if)#
```

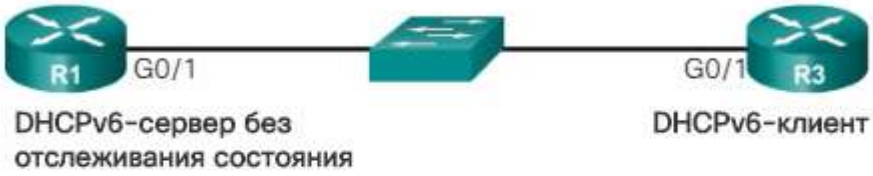
Рис. 4.2.29

Перевірка DHCPv6 без відстеження стану

Перевірка DHCPv6-сервера без відстеження стану

На рис. 1 показано, як за допомогою команди **show ipv6 dhcp pool** можна перевірити ім'я DHCPv6-пулу і його параметри. Кількість активних клієнтів дорівнює 0, оскільки сервер працює в режимі без відстеження стану.

Проверка DHCPv6-сервера без отслеживания состояния




```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATELESS
  DNS server: 2001:DB8:CAFE:AAAA::5
  Domain name: example.com
  Active clients: 0
R1#
```

Рис. 4.2.30

Команду **show running-config** також можна використовувати для перевірки всіх попередніх налаштованих команд.

Перевірка DHCPv6-клієнта без відстеження стану

У наведеному прикладі в якості DHCPv6-клієнта без відстеження стану використовується маршрутизатор. На рис. 2 вихідні дані команди **show ipv6 interface** показують, що маршрутизатор використовує режим SLACC і має

глобальний індивідуальний IPv6-адреса. Глобальний індивідуальний IPv6-адреса був створений за допомогою SLAAC, що включає в себе префікс, що міститься в повідомленні RA. IID був створений за допомогою EUI-64. Для призначення IPv6-адреси протокол DHCPv6 не використовувався.

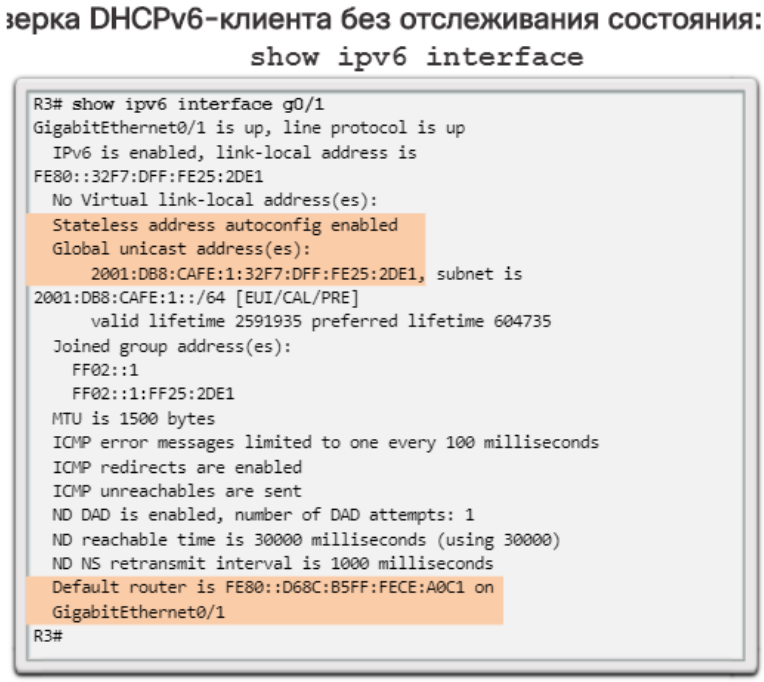


Рис. 4.2.31

Інформація про маршрутизатор за замовчуванням також отримана з повідомлення RA. Адресою маршрутизатора за замовчуванням є IPv6-адреса джерела пакету, що містить повідомлення RA і локальну адресу каналу маршрутизатора.

Представлені на рис. 3 вихідні дані команди **debug ipv6 dhcp detail** показують обмін DHCPv6-повідомленнями між клієнтом і сервером. У наведеному прикладі команда була введена на клієнта. Повідомлення INFORMATION-REQUEST показано в зв'язку з тим, що воно відправлено з DHCPv6-клієнта без відстеження стану. Зверніть увагу, що клієнт, маршрутизатор R3, посилає DHCPv6 повідомлення зі свого локального адреси каналу на адресу All_DHCPv6_Relay_Agents_and_Servers FF02 :: 1: 2.

зерка DHCPv6-клиента без отслеживания состояния: команда debug ipv6 dhcp detail

```
R3# debug ipv6 dhcp detail
   IPv6 DHCP debugging is on (detailed)
R3#
*Feb  3 02:39:10.454: IPv6 DHCP: Sending INFORMATION-REQUEST
to FF02::1:2 on GigabitEthernet0/1
*Feb  3 02:39:10.454: IPv6 DHCP: detailed packet contents
*Feb  3 02:39:10.454:   src FE80::32F7:DFF:FE25:2DE1
*Feb  3 02:39:10.454:   dst FF02::1:2 (GigabitEthernet0/1)
*Feb  3 02:39:10.454:   type INFORMATION-REQUEST(11), xid
12541745
<Данные опущены>
*Feb  3 02:39:10.454: IPv6 DHCP: Adding server
                      FE80::D68C:B5FF:FECE:A0C1
*Feb  3 02:39:10.454: IPv6 DHCP: Processing options
*Feb  3 02:39:10.454: IPv6 DHCP: Configuring DNS server
                      2001:DB8:CAFE:AAAA::5
*Feb  3 02:39:10.454: IPv6 DHCP: Configuring domain name
                      example.com
*Feb  3 02:39:10.454: IPv6 DHCP: DHCPv6 changes state from
INFORMATION-REQUEST to IDLE (REPLY_RECEIVED) on
GigabitEthernet0/1
R3#
```

Рис. 4.2.32

Вихідні дані команди debug відображають все DHCPv6 повідомлення, передані між клієнтом і сервером, включаючи параметри DNS-сервера і доменні імена, налаштовані на сервері.

Налаштування маршрутизатора в якості сервера DHCPv6 з відстеженням стану

Налаштування DHCPv6-сервера з відстеженням стану аналогічна настройці сервера без відстеження стану. Найбільш значною відмінністю є те, що сервер з відстеженням стану також є джерелом інформації про IPv6-адресації, як і сервер DHCPv4.

Крок 1. Активація IPv6-маршрутизації

Для включення IPv6-маршрутизації необхідно виконати команду **ipv6 unicast-routing** , як показано на рис. 1. Виконання цієї команди не є необхідним для настройки маршрутизатора в якості DHCPv6-сервера з відстеженням стану, але потрібно маршрутизатора, щоб відправляти повідомлення RA по протоколу ICMPv6.

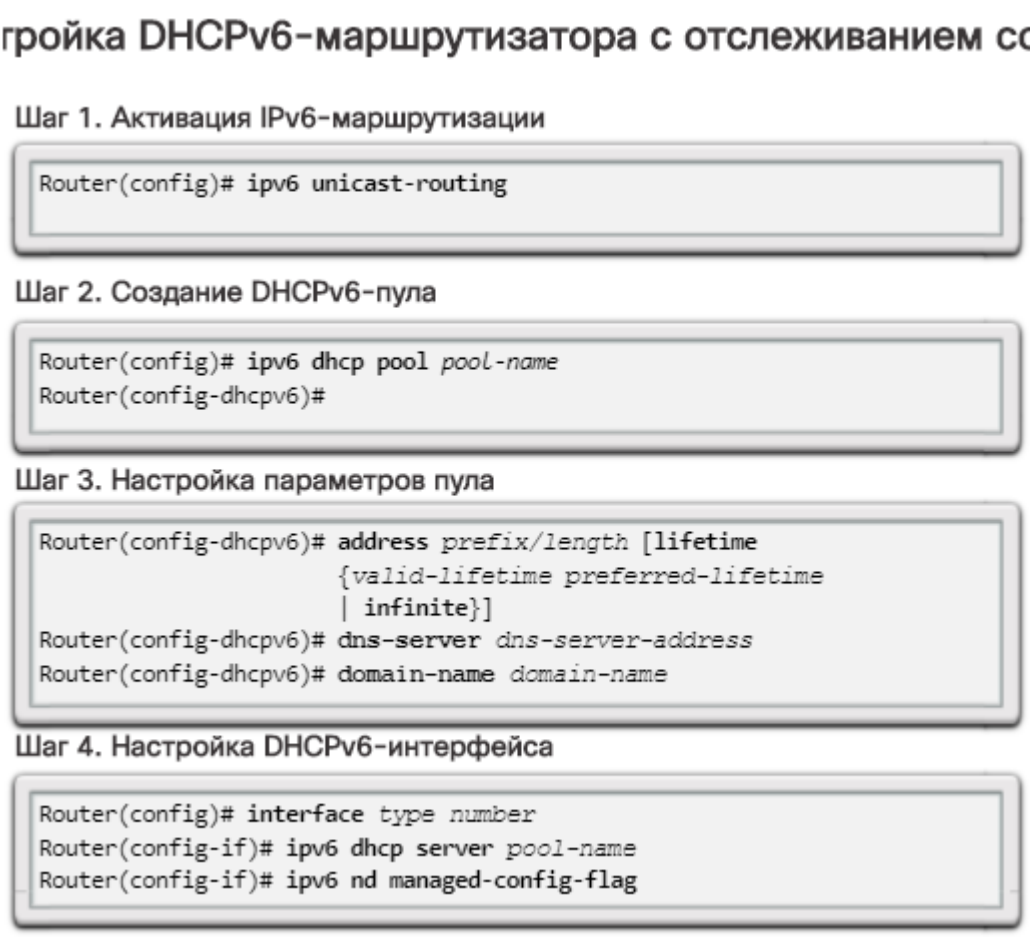


Рис. 4.2.33

Крок 2. Створення DHCPv6-пулу

Команда **ipv6 dhcp pool** *pool-name* створює пул і переводить маршрутизатор в режим конфігурації DHCPv6, який визначається рядком запиту Router (config-dhcpv6) #.

Крок 3. Налаштування параметрів пулу

При використанні DHCPv6 з відстеженням стану всі параметри адресації і інші параметри конфігурації повинні призначатися сервером DHCPv6. Команда **address prefix** використовується для позначення адресного пулу, з якого сервер буде виділяти адреси. Параметр **lifetime** вказує дійсне і детально визначений час оренди в секундах. Як і при використанні DHCPv6 без відстеження стану, клієнт використовує IPv6-адреса джерела з пакету, що міститься в повідомленні RA.

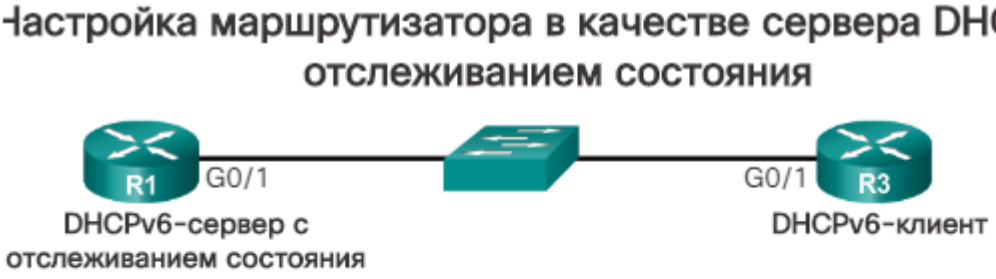
Інша інформація, надана DHCPv6-сервером з відстеженням стану, зазвичай включає адресу DNS-сервера і доменне ім'я.

Крок 4. Команди інтерфейсу

Команда **ipv6 dhcp server** *pool-name* прив'язує пул DHCPv6 до інтерфейсу. Маршрутизатор відповідає на DHCPv6-запити на цьому інтерфейсі інформацією, що міститься в пулі. Значення прапора M необхідно змінити з 0 на 1 за допомогою команди інтерфейсу **ipv6 nd managed-config-flag** . Задана каже пристрою не використовувати SLAAC, а отримати настройки IPv6-адресації і всі параметри конфігурації від DHCPv6-сервера з відстеженням стану.

Приклад сервера DHCPv6 з відстеженням стану

На рис. 2 наводиться приклад команд сервера DHCPv6 з відстеженням стану, налаштованого на маршрутизаторі R1. Зверніть увагу, що шлюз не визначений, оскільки маршрутизатор автоматично посилає власну адресу link-local в якості шлюзу за замовчуванням. Маршрутизатор R3 налаштований в якості клієнта для перевірки роботи сервера DHCPv6 з відстеженням стану.



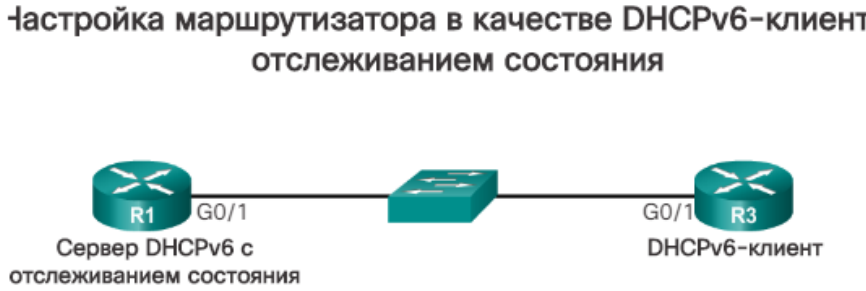

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:DB8:CAFE:1::/64
                    lifetime infinite
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# ipv6 nd managed-config-flag
```

Рис. 4.2.34

Налаштування маршрутизатора в якості DHCPv6-клієнта з відстеженням стану

Як показано на малюнку, використання команди режиму настройки інтерфейсу **ipv6 enable** дозволяє маршрутизатора отримати адресу link-local, щоб відправляти повідомлення RS і брати участь в роботі протоколу DHCPv6.

Команда режиму конфігурації інтерфейсу **ipv6 address dhcp** дозволяє маршрутизатора виконувати функцію DHCPv6-клієнта на даному інтерфейсі.



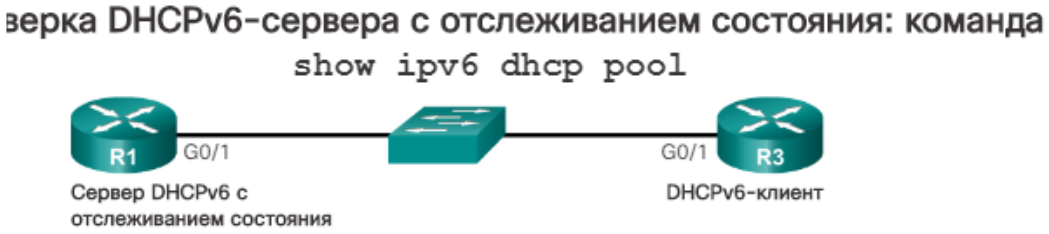

```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address dhcp
R3(config-if)#
```

Рис. 4.2.35

Перевірка DHCPv6 з відстеженням стану

Перевірка DHCPv6-сервера з відстеженням стану

На рис. 1 показано, як за допомогою команди **show ipv6 dhcp pool** можна перевірити ім'я DHCPv6-пулу і його параметри. Кількість активних клієнтів дорівнює 1. Дане значення відображає наявність клієнта R3, що одержує свій глобальний індивідуальний IPv6-адресу від цього сервера.




```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATEFUL
  Address allocation prefix: 2001:DB8:CAFE:1::/64 valid
4294967295 preferred 4294967295 (1 in use, 0 conflicts)
  DNS server: 2001:DB8:CAFE:AAAA::5
  Domain name: example.com
  Active clients: 1
R1#
```

Рис. 4.2.36

Команда **show ipv6 dhcp binding** , як показано на рис. 2, відображає автоматичне зв'язування між локальною адресою каналу і адресою, призначеним сервером. FE80 :: 32F7: DFF: FE25: 2DE1 є адресою link-local клієнта. У наведеному прикладі це інтерфейс G0 / 1 маршрутизатора R3. Ця електронна адреса прив'язаний до глобального індивідуальним IPv6-адресу 2001: DB8: CAFE: 1: 5844: 47B2: 2603: C171, призначеного маршрутизатором R1, що виступає в якості DHCPv6-сервера. Дана інформація забезпечується DHCPv6-сервером з відстеженням стану і не підтримується DHCPv6-сервером без відстеження стану.


```
R1# show ipv6 dhcp binding
Client: FE80::32F7:DFF:FE25:2DE1
  DUID: 0003000130F70D252DE0
  Username : unassigned
  IA NA: IA ID 0x00040001, T1 43200, T2 69120
    Address: 2001:DB8:CAFE:1:5844:47B2:2603:C171
            preferred lifetime INFINITY, , valid lifetime
 INFINITY,
R1#
```

Рис. 4.2.37

Перевірка DHCPv6-клієнта з відстеженням стану

Вихідні дані команди **show ipv6 interface** , наведені на рис. 3, підтверджують глобальний індивідуальний IPv6-адреса DHCPv6-клієнта (маршрутизатор R3), призначений сервером DCHP. Інформація про маршрутизатор за замовчуванням отримана не від сервера DHCPv6, а визначена за допомогою IPv6-адреси джерела повідомлення RA. Незважаючи на те що клієнт не використовує ці дані в повідомленні RA, він може використовувати IPv6-адреса джерела для отримання інформації про своє шлюзі за замовчуванням.

верка DHCPv6-клиента с отслеживанием состояния: команда show ipv6 interface

```
R3# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::32F7:DFF:FE25:2DE1
  No Virtual link-local address(es):
  Global unicast address(es):
     2001:DB8:CAFE:1:5844:47B2:2603:C171,  subnet is
2001:DB8:CAFE:1:5844:47B2:2603:C171/128
  Joined group address(es):
    FF02::1
    FF02::1:FF03:C171
    FF02::1:FF25:2DE1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds
  Default router is FE80::D68C:B5FF:FECE:A0C1 on
  GigabitEthernet0/1
R3#
```

Рис. 4.2.38

Налаштування маршрутизатора в якості агента ретрансляції DHCPv6

У разі якщо DHCPv6-сервер розташований з клієнтом в різних мережах, в якості агента DHCPv6-ретрансляції можна налаштувати маршрутизатор IPv6. Налаштування агента DHCPv6-ретрансляції аналогічна настройці IPv4-маршрутизатора в якості агента DHCPv4-ретрансляції.

Примітка . Незважаючи на те що конфігурація агента DHCPv6-ретрансляції схожа на конфігурацію DHCPv4-маршрутизатора, IPv6-маршрутизатор або агенти ретрансляції направляють DHCPv6 повідомлення дещо інакше, ніж DHCPv4-ретранслятори. Відповідні повідомлення і процес не розглядаються в рамках даного навчального курсу.

На рис. 1 наведено приклад топології, в якій сервер DHCPv6 розташований в мережі 2001: DB8: CAFE: 1 :: / 64. Адміністратор хоче використовувати цей DHCPv6-сервер в якості центрального DHCPv6-сервера з відстеженням стану для призначення IPv6-адрес всім клієнтам. Тому клієнти, розташовані в інших

мережах, як, наприклад, PC1, розташований в мережі 2001: DB8: CAFE: A :: / 64, повинні зв'язатися з сервером DHCPv6.

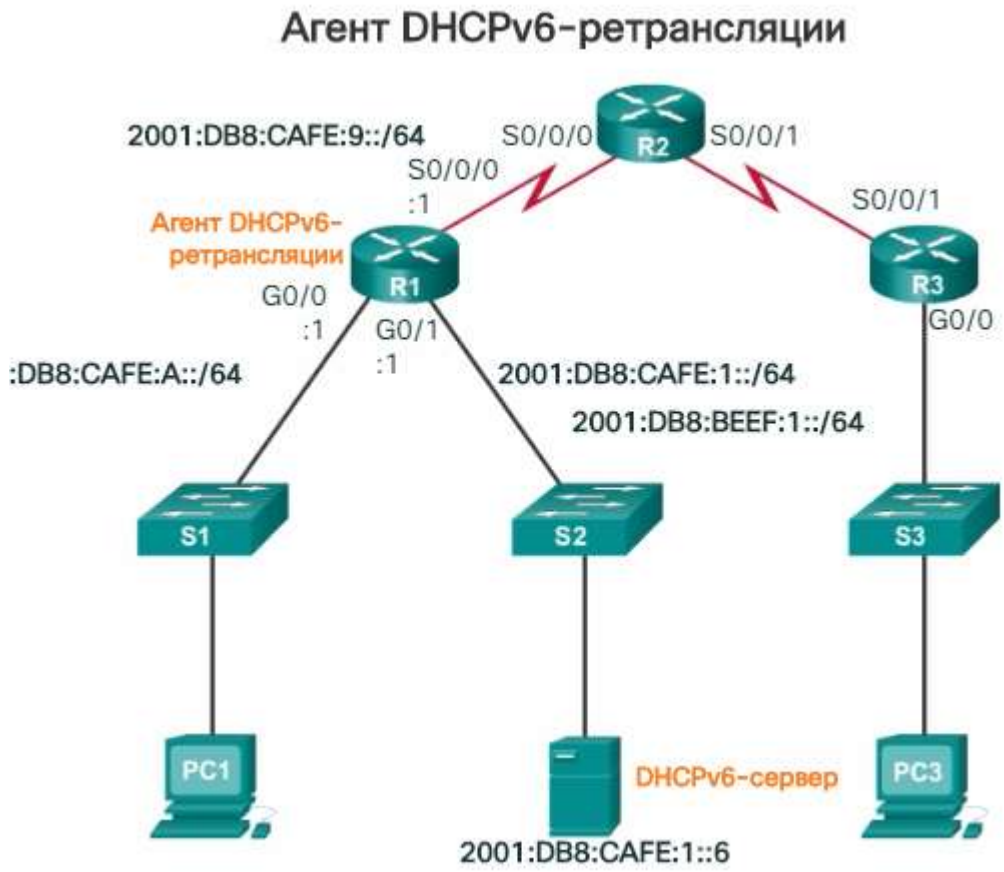


Рис. 4.2.39

DHCPv6 повідомлення від клієнта відправлені на IPv6-адреса під LGPL FF02 :: 1: 2. All_DHCPv6_Relay_Agents_and_Servers address. Ця електронна адреса має область дії локального каналу, т. Е. Маршрутизатори не відсилаються ці повідомлення. Для того щоб DHCPv6-клієнт і сервер могли обмінюватися інформацією, маршрутизатор повинен бути налаштований в якості агента DHCPv6-ретрансляції.

Налаштування агента DHCPv6-ретрансляції

Як показано на рис. 2, агент DHCPv6-ретрансляції налаштований за допомогою команди **ipv6 dhcp relay destination** . Команда виконана на інтерфейсі, відповідному DHCPv6-клієнту, з використанням адреси DHCPv6-сервера в якості адреси призначення.

Команды агента DHCPv6-ретрансляции

```
R1(config)# interface g0/0
R1(config-if)# ipv6 dhcp relay destination 2001:db8:cafe:1::6
R1(config-if)# end
R1# show ipv6 dhcp interface g0/0
GigabitEthernet0/0 is in relay mode
  Relay destinations:
    2001:DB8:CAFE:1::6
R1#
```

Рис. 4.2.40

Команда **show ipv6 dhcp interface** підтверджує, що інтерфейс G0 / 0 знаходиться в режимі ретрансляції з адресою 2001: DB8: CAFE: 1 :: 6, встановленим як адреса DHCPv6-сервера.

За допомогою інструменту перевірки синтаксису на рис. 3 виконайте команди DHCPv6-ретрансляції на відповідному маршрутизаторі, щоб PC3 міг отримувати інформацію про IPv6-адресації від DHCPv6-сервера. Зверніться до рис. 1 для перегляду топології мережі.

Завдання пошуку та усунення неполадок

Пошук і усунення неполадок в роботі маршрутизатора DHCPv6 аналогічні виявленню і усуненню несправностей в роботі маршрутизатора DHCPv4.

Пошук і усунення неполадок. Завдання 1. Вирішення конфліктів

Термін оренди IPv6-адреси (як і IPv4-адреси) може закінчитися в той момент, коли клієнту ще потрібне підключення до мережі. Команда **show ipv6 dhcp conflict** відображає всі конфлікти адрес, зареєстровані сервером DHCPv6 з відстеженням стану. При виявленні конфлікту IPv6-адрес клієнт зазвичай видаляє адресу та створює нову адресу за допомогою SLAAC або сервера DHCPv6 з відстеженням стану.

Пошук і усунення неполадок. Завдання 2. Перевірка методу розподілу

Інтерфейсну команду **show ipv6 interface** *інтерфейс* можна використовувати для перевірки методу розподілу адрес, зазначеного в повідомленні RA шляхом установки прапорів M і O. Ці відомості відображаються в останніх рядках вихідних даних. Якщо клієнт не отримує інформацію про IPv6-адресу від сервера DHCPv6 з відстеженням стану, причиною можуть бути невірні прапори M і O в повідомленні RA.

Пошук і усунення неполадок. Завдання 3. Перевірка статичної IP-адреси

При пошуку і усунення будь-якої неполадки в роботі DHCP, як у версії DHCPv4, так і в DHCPv6, підключення до мережі можна перевірити налаштуванням статичного IP-адреси на клієнтської робочої станції. При використанні протоколу IPv6, в разі, якщо робочої станції не вдається отримати доступ до мережевих ресурсів, використовуючи статично налаштований IPv6-адреса, це означає, що DHCPv6 або SLAAC не є джерелами проблеми. У цьому випадку необхідно провести перевірку мережевого підключення.

Пошук і усунення неполадок. Завдання 4. Перевірка настройки порту комутатора

Якщо DHCPv6-клієнтові не вдається отримати дані від DHCPv6-сервера, переконайтеся, що порт комутатора включений і правильно налаштований.

Примітка . Якщо при наявності комутатора між клієнтом і DHCPv6-сервером клієнт не може отримати настройки протоколу DHCP, причиною можуть бути неполадки в налаштуванні порту комутатора. Причиною можуть бути проблеми, пов'язані зі створенням транкових і логічних каналів або протоколом сполучного дерева. Рішенням найбільш часто виникаючих проблем DHCPv6-клієнта, що відбуваються при першій установці комутатора Cisco, може стати настройка розширення PortFast і прикордонного порту.

Пошук і усунення неполадок. Завдання 5. Діагностика роботи протоколу DHCPv6 в тій же підмережі або VLAN

Якщо сервер DHCPv6 з відстеженням або без відстеження стану працює нормально, але знаходиться з клієнтом в різних IPv6-мережах або мережах VLAN, проблема може полягати в агента DHCPv6-ретрансляції. Відповідний клієнту інтерфейс маршрутизатора повинен бути налаштований за допомогою команди **ipv6 dhcp relay destination** .

Поиск и устранение неполадок в работе DHCPv6

Поиск и устранение неполадок. Задача 1.	Разрешение конфликтов адресов.
Поиск и устранение неполадок. Задача 2.	Проверка метода распределения.
Поиск и устранение неполадок. Задача 3.	Проверка с использованием статического IPv6-адреса.
Поиск и устранение неполадок. Задача 4.	Проверка конфигурации порта коммутатора.
Поиск и устранение неполадок. Задача 5.	Проверка работы протокола в той же подсети или VLAN.

Рис. 4.2.41

Перевірка налаштувань DHCPv6 на маршрутизаторі

Конфігурації маршрутизатора для служб DHCPv6 з відстеженням і без відстеження стану дуже схожі, однак є важливі відмінності. На рис. 1 показані команди конфігурації для обох типів служб DHCPv6.

Службы DHCPv6 с отслеживанием состояния

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:DB8:CAFE:1::/64 lifetime
infinite
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# ipv6 nd managed-config-flag
```

Службы DHCPv6 без отслеживания состояния

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
```

Рис. 4.2.42

Адресація DHCPv6 з урахуванням станів.

На маршрутизаторі, налаштованому для надання служби DHCPv6 з відстеженням стану, для надання інформації про адресації використовується команда **address prefix** .

Для служб DHCPv6 з відстеженням стану використовується команда режиму конфігурації інтерфейсу **ipv6 nd managed-config-flag** . У наведеному прикладі клієнт ігнорує інформацію про адресації в повідомленні RA і взаємодіє з DHCPv6-сервером для отримання як інформації про адресації, так і додаткової інформації.

Адресація DHCPv6 без урахування станів.

Для служб DHCPv6 без відстеження стану використовується команда режиму конфігурації інтерфейсу **ipv6 nd other-config-flag** . Команда каже пристрою використовувати SLAAC для отримання інформації про адресації і DHCPv6-сервер без відстеження стану - для отримання інших параметрів конфігурації.

Для перегляду поточної конфігурації з метою визначення методу розподілу адрес можна використовувати команду **show ipv6 interface** . Як видно з рис. 2, останній рядок вихідних даних показує, яким чином клієнти отримують адреси та інші параметри.

SLAAC

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
  FE80::D68C:B5FF:FECE:A0C1
<Данные опущены>
Hosts use stateless autoconfig for addresses.
```

Адресация DHCPv6 без учёта состояний.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
  FE80::D68C:B5FF:FECE:A0C1
<Данные опущены>
Hosts use DHCP to obtain other configuration.
```

Адресация DHCPv6 с учётом состояний.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
  FE80::D68C:B5FF:FECE:A0C1
<Данные опущены>
Hosts use DHCP to obtain routable addresses.
```

Рис. 4.2.43

налагодження DHCPv6

Коли маршрутизатор налаштовується як сервер DHCPv6 з відстеженням або без відстеження стану, для перевірки прийому і передачі DHCPv6 повідомлень слід використовувати команду **debug ipv6 dhcp detail** . Як показано на малюнку, DHCPv6-маршрутизатор з відстеженням стану отримав від клієнта повідомлення SOLICIT. Маршрутизатор використовує інформацію про адресації в своєму IPV6-STATEFUL-пулі для прив'язки даних.

Отладка DHCPv6

```
R1# debug ipv6 dhcp detail
   IPv6 DHCP debugging is on (detailed)
R1#
*Feb  3 21:27:41.123: IPv6 DHCP: Received SOLICIT from
FE80::32F7:DFF:FE25:2DE1 on GigabitEthernet0/1
*Feb  3 21:27:41.123: IPv6 DHCP: detailed packet contents
*Feb  3 21:27:41.123:   src FE80::32F7:DFF:FE25:2DE1
(GigabitEthernet0/1)
*Feb  3 21:27:41.127:   dst FF02::1:2
*Feb  3 21:27:41.127:   type SOLICIT(1), xid 13190645
*Feb  3 21:27:41.127:   option ELAPSED-TIME(8), len 2
*Feb  3 21:27:41.127:     elapsed-time 0
*Feb  3 21:27:41.127:   option CLIENTID(1), len 10
*Feb  3 21:27:41.127:     000
*Feb  3 21:27:41.127: IPv6 DHCP: Using interface pool IPV6-
STATEFUL
*Feb  3 21:27:41.127: IPv6 DHCP: Creating binding for
FE80::32F7:DFF:FE25:2DE1 in pool IPV6-STATEFUL
<Данные опущены>
```

Рис. 4.2.44

Висновок

Глава 8. DHCP

Для взаємодії з іншими пристроями всіх мережевих вузлів потрібно унікальний IP-адресу. Статична призначення даних IP-адресації у великій мережі призводить до адміністративної навантаженні, якої можна уникнути, використовуючи протоколи DHCPv4 і DHCPv6, що застосовуються для динамічного присвоєння IPv4- і IPv6-адрес відповідно.

Протокол DHCPv4 динамічно привласнює або видає в оренду IPv4-адрес з пулу адрес на обмежений період часу - за вибором сервера або до тих пір, поки у клієнта є необхідність в адресі.

Механізм DHCPv4 дозволяє здійснювати обмін декількома різними пакетами між DHCPv4-сервером і DHCPv4-клієнтом, що дозволяє орендувати діючу інформацію про адресації на визначений період часу.

Повідомлення, які виходять від клієнта (DHCPDISCOVER, DHCPREQUEST), є повідомленнями широкомовної розсилки, що дозволяє всім DHCPv4-серверів в мережі дізнатися про запит клієнта і прийомі клієнтом інформації про адресації. Повідомлення, які виходять від сервера DHCPv4 (DHCPOFFER, DHCPACK), відправляються у вигляді одноадресної розсилки безпосередньо клієнтові.

Існує два способи динамічної конфігурації глобальних індивідуальних IPv6-адрес:

Автоматична настройка без збереження стану адреси (Stateless Address Autoconfiguration, SLAAC)

Протокол динамічної конфігурації мережного вузла (DHCP) для протоколу IPv6 (зі збереженням стану DHCPv6)

При автоматичній настройці без відстеження стану клієнт використовує дані, надані IPv6 повідомленням RA, для автоматичного вибору і конфігурації унікального IPv6-адреси. DHCPv6 без відстеження стану повідомляє клієнту про використання інформації в повідомленні RA для адресації, при цьому додаткові параметри конфігурації доступні з сервера DHCPv6.

Сервер DHCPv6 з відстеженням стану схожий з сервером DHCPv4. В цьому випадку в повідомленні RA клієнту вказують не використовувати інформацію про адресації з повідомлення RA. Вся інформація про адресації і конфігурації надається сервером DHCPv6 з відстеженням стану. Сервер DHCPv6 управляє інформацією про стан протоколу IPv6 аналогічно тому, як сервер DHCPv4 розподіляє адреси для IPv4.

Якщо DHCP-сервер розташований в різних мережах з DCHP-клієнтом, необхідно налаштувати агент ретрансляції. Агент ретрансляції пересилає певні повідомлення багатоадресної або широкомовної розсилки, в тому числі повідомлення DHCP, які виходять від хоста, розташованого в сегменті локальної мережі, і адресовані конкретному серверу, який розташований в іншому сегменті локальної мережі.

Пошук і усунення неполадок в роботі DHCPv4 і DHCPv6 включає в себе однакові завдання:

Усунення проблеми конфліктуючих адрес

Перевірка фізичного підключення

Перевірка зв'язності з використанням статичного IP-адреси

Перевірка конфігурації порту комутатора
Перевірка роботи протоколу в тій же підмережі або VLAN

4.3 NAT для IPv4

Всі публічні IPv4-адреси, що підключаються до Інтернету, повинні бути зареєстровані у регіонального реєстратора Інтернету (RIR). Організації можуть орендувати загальнодоступні адреси у постачальника послуг. Зареєстрований власник загальнодоступного IP-адреси може призначити цю адресу мережного пристрою.

Теоретично максимально допустиму кількість IPv4-адрес становить 4,3 мільярда, що жорстко обмежує адресний простір IPv4. Коли в 1981 році Боб Кан (Bob Kahn) і Гвинт Серф (Vint Cerf) розробили пакет протоколів TCP / IP, включаючи IPv4, вони не мали уявлення про те, на що перетвориться Інтернет. У той час персональний комп'ютер був дивиною для зацікавлених, а до появи інтернет-простору, «Всесвітньої павутини» (World Wide Web), залишалося ще більше десятка років.

З поширенням персональних комп'ютерів і настанням ери інтернет-простору стало очевидно, що 4,3 мільярда IPv4-адрес буде недостатньо. Довгостроковим рішенням стала поява протоколу IPv6, однак поряд з цим потрібні були швидші способи усунення проблеми вичерпання адресного простору. Організація IETF розробила ряд короткострокових рішень, в тому числі перетворення (NAT) і приватні IPv4-адреси відповідно до RFC 1918. У цьому розділі описується, як механізм перетворення NAT в поєднанні з використанням діапазону приватних адрес застосовується для збереження і більш ефективного призначення IPv4- адрес з метою забезпечення доступу до Інтернету мереж будь-яких масштабів. Матеріал цього розділу охоплює наступні аспекти:

- характеристики, термінологія і загальні принципи роботи NAT;
- різні типи перетворення, включаючи статичний NAT, динамічний NAT і NAT з перевантаженням;
- переваги і недоліки NAT;
- настройка, перевірка і аналіз статичного NAT, динамічного NAT і NAT з перевантаженням;
- використання перенаправлення портів для доступу до внутрішніх пристроїв з мережі Інтернет;
- налагодження NAT за допомогою команд **show** і **debug** ;
- застосування NAT для протоколу IPv6 з метою перетворення між IPv6- і IPv4-адресами.

Простір приватних IPv4-адрес

Кількості публічних IPv4-адрес недостатньо, щоб призначити унікальні адреси всіх пристроїв, підключеним до Інтернету. У більшості випадків мережі реалізуються з використанням приватних IPv4-адрес відповідно до RFC 1918. На рис. 1 показаний діапазон адрес, включених в RFC 1918. Найімовірніше, комп'ютера, на якому ви зараз переглядаєте матеріал навчального курсу, призначений приватну адресу.

Частные интернет-адреса определены в документе RFC 1918:

Класс	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Рис. 4.3.1

Ці приватні адреси використовуються в рамках організації або об'єкта з метою забезпечення взаємодії пристроїв на локальному рівні. Але оскільки ці адреси не визначають конкретну компанію або організацію, приватні IPv4-адреси можна використовувати для маршрутизації через Інтернет. Для того щоб надати пристрою з приватним IPv4-адресою отримувати доступ до пристроїв і ресурсів поза локальної мережі, приватний адресу спочатку необхідно перетворити в публічний адресу.

Як показано на рис. 2, NAT забезпечує перетворення приватних адрес в публічні адреси. Це дозволяє пристрою з приватним IPv4-адресою отримувати доступ до ресурсів поза своєю приватною мережі, включно з розміщеними в Інтернеті. У поєднанні з приватними IPv4-адресами NAT продемонстрував свою доцільність щодо економії публічних IPv4-адрес. Один публічний IPv4-адрес може спільно використовуватися сотнями, навіть тисячами пристроїв, для кожного з яких налаштований унікальний приватний IPv4-адрес.

Рис. 4.3.2

Без використання NAT адресний простір IPv4 було б вичерпано задовго до настання 2000 року. Незважаючи на свої переваги, NAT має ряд обмежень, про які йтиме мова розглядатися далі в цій главі. Рішенням проблеми вичерпання простору IPv4-адрес і обмежень NAT є остаточний перехід на IPv6.

Що таке NAT?

Перетворення NAT використовується в різних цілях, проте основним завданням даного механізму є економія публічних IPv4-адрес. Це досягається за рахунок того, що для внутрішньої взаємодії в мережах використовуються приватні IPv4-адреси, а перетворення в публічні адреси відбувається тільки в разі потреби. Додаткова перевага NAT - підвищення ступеня конфіденційності і безпеки мережі - пояснюється тим, що даний механізм приховує внутрішні IPv4-адреси від зовнішніх мереж.

Для маршрутизатора з підтримкою NAT можна налаштувати один або декілька діючих публічних IPv4-адрес. Ці публічні адреси відомі як пул адрес NAT. Якщо внутрішній устрій відправляє трафік за межі мережі,

маршрутизатор з підтримкою NAT перетворює внутрішній IPv4-адрес пристрою в публічний адресу з пулу NAT. Зовнішніх пристроїв здається, що весь трафік, що входить в мережу і виходить з неї, використовує публічні IPv4-адреси з наданого пулу адрес.

Маршрутизатор NAT зазвичай працює на кордоні тупикової мережі. Тупикова мережа - це мережа, у якій є тільки одне підключення до сусідньої мережі, і, як наслідок, єдиний шлях назовні і єдиний шлях до цієї мережі. У прикладі, показаному на малюнку, R2 є граничним маршрутизатором. З точки зору інтернет-провайдера, маршрутизатор R2 створює тупикову мережу.

Коли пристрою в тупиковій мережі потрібне підключення до пристрою поза ним мережі, пакет пересилається граничному маршрутизатора. Граничний маршрутизатор виконує процес NAT, перетворюючи внутрішній приватний адресу пристрою в публічний, зовнішній, маршрутизації адресу.

Примітка . Підключення до мережі інтернет-провайдера може використовувати приватну адресу або публічний адресу, яким користуються клієнтами провайдера. В рамках даної теми як приклад наведено публічний адресу.

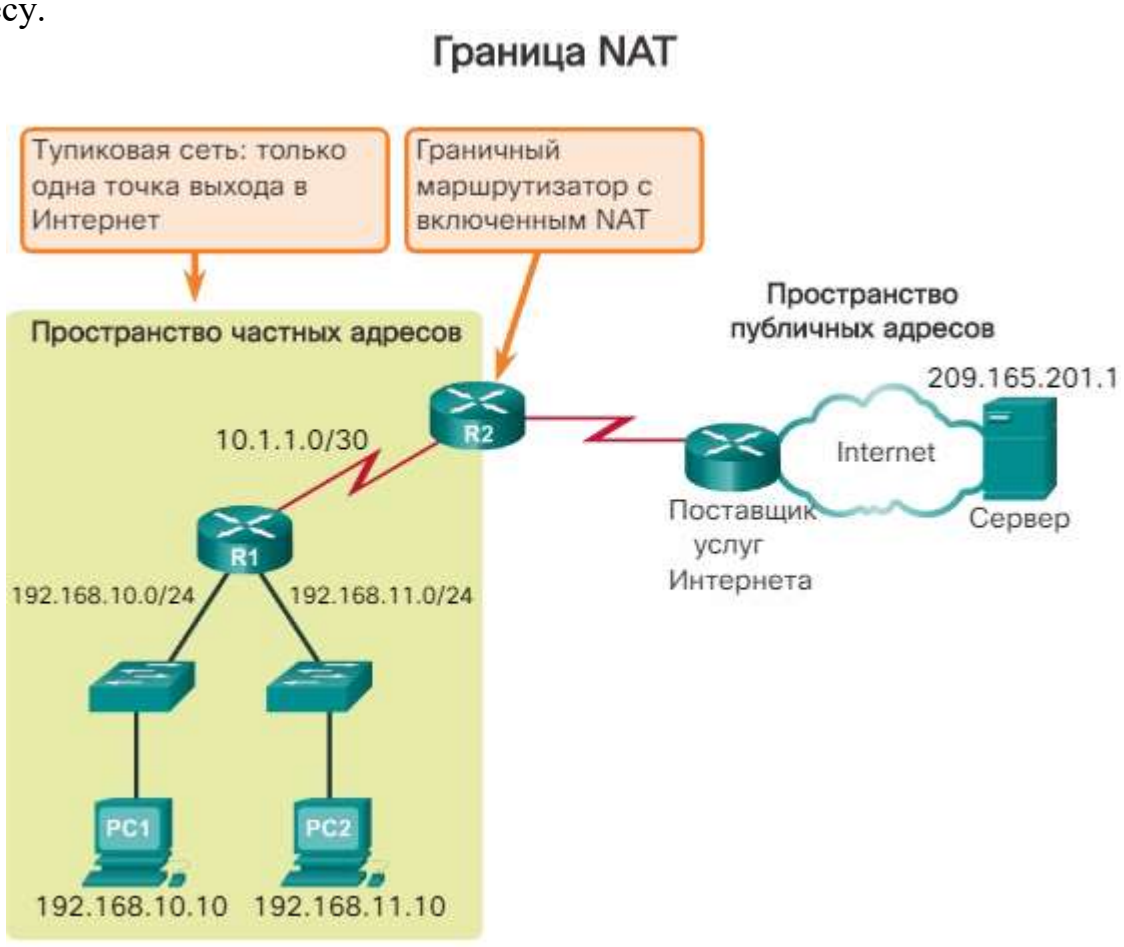


Рис. 4.3.3

Термінологія NAT

У термінології NAT під «внутрішньою мережею» мається на увазі набір мереж, чиї адреси будуть транслюватися. Термін «зовнішня мережа» відноситься до всіх інших мереж.

При використанні NAT IPv4-адреси представляють різні точки призначення в залежності від того, де вони знаходяться: в приватній або в

публічній мережі (Інтернет), а також від того, чи є трафік вхідними або вихідними.

У NAT передбачено 4 типи адрес:

- Внутрішній локальну адресу
- Внутрішній глобальна адреса
- Зовнішній локальний адресу
- Зовнішній глобальна адреса

При визначенні використовуваного типу адреси важливо пам'ятати, що термінологія NAT завжди застосовується з точки зору пристрої, адреса якого буде транслюватися:

Внутрішній адреса - це адреса пристрою, що перетворюється механізмом NAT.

Зовнішній адреса - це адреса пристрою призначення.

В рамках NAT по відношенню до адрес також використовується поняття локальності або глобальності:

Локальний адреса - це будь-яку адресу, що з'являється у внутрішній частині мережі.

Глобальний адреса - це будь-яку адресу, що з'являється у зовнішній частині мережі.

На малюнку внутрішнім локальним адресою ПК 1 є 192.168.10.10. З точки зору ПК 1 веб-сервер використовує зовнішній адресу 209.165.201.1. Якщо пакети відправляються від ПК 1 на глобальний адреса веб-сервера, внутрішній локальний адресу ПК 1 перетворюється в 209.165.200.226 (внутрішній глобальний адреса). Адреса зовнішнього пристрою зазвичай не перетвориться, так як ця адреса зазвичай вже є публічним IPv4-адресою.

Зверніть увагу, що для ПК 1 використовуються різні локальний і глобальний адреси, а для веб-сервера в обох випадках використовується один публічний IPv4-адрес. З точки зору веб-сервера трафік, що виходить від ПК 1, представляється надходять з внутрішнього глобального адреси 209.165.200.226.

Маршрутизатор NAT (R2 на малюнку) являє собою точку розмежування між внутрішньою і зовнішньою мережами, а також між локальними і глобальними адресами.

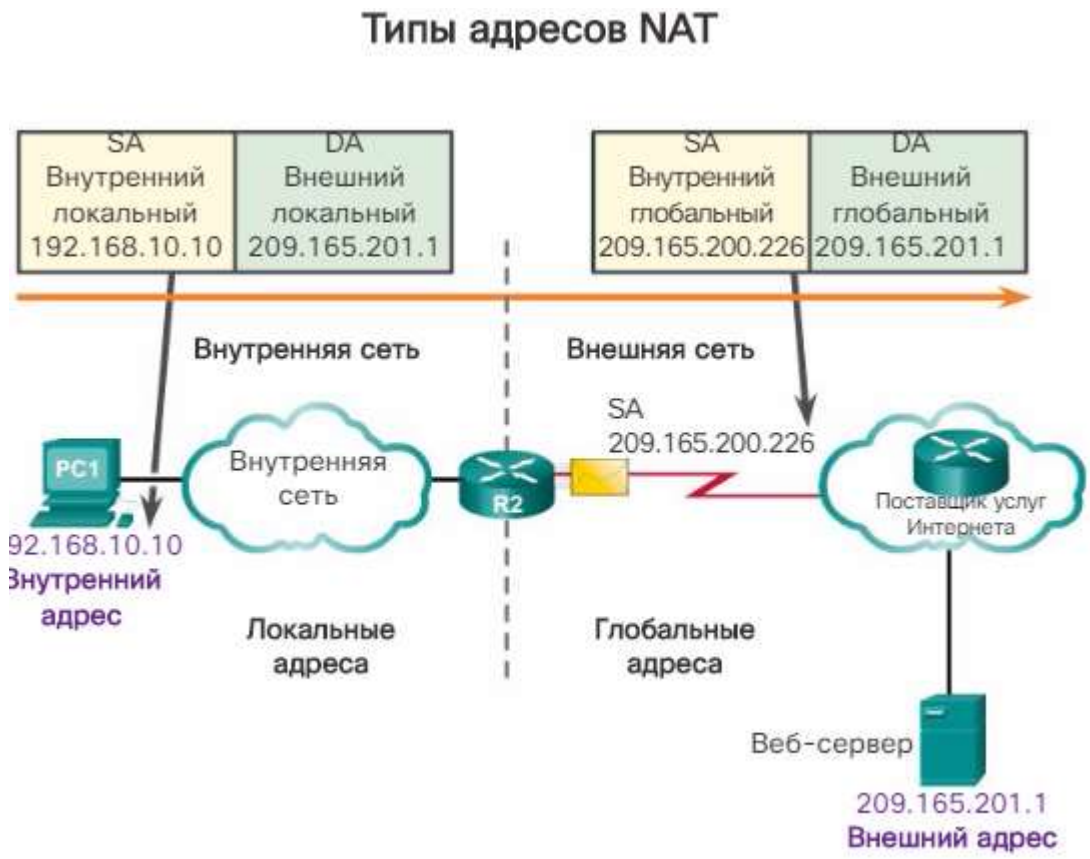


Рис. 4.3.4

Терміни «внутрішній» і «зовнішній» використовуються в поєднанні з термінами «локальний» і «глобальний», коли мова йде про конкретні адреси. На малюнку маршрутизатор R2 налаштований на використання механізму NAT. Він використовує пул публічних адрес, що призначаються внутрішніх вузлів.

Внутрішній локальну адресу - це адреса джерела, видимий з внутрішньої мережі. На малюнку ПК 1 призначений IPv4-адрес 192.168.10.10. Це внутрішній локальний адресу ПК 1.

Внутрішній глобальна адреса - це адреса джерела, видимий із зовнішньої мережі. На малюнку, якщо ПК 1 відправляє трафік веб-сервера з адресою 209.165.201.1, R2 перетворює внутрішній локальний адресу у внутрішній глобальний адресу. В цьому випадку R2 змінює IPv4-адрес джерела з 192.168.10.10 на 209.165.200.226. У термінології NAT внутрішній локальний адресу 192.168.10.10 перетвориться у внутрішній глобальний адреса 209.165.200.226.

Зовнішній глобальна адреса - це адреса призначення, видимий із зовнішньої мережі. Це глобальна маршрутизація IPv4-адрес, призначений вузлу в Інтернеті. Наприклад, веб-сервер доступний по IPv4-адресою 209.165.201.1. У більшості випадків зовнішній локальний і зовнішній глобальний адреси збігаються.

Зовнішній локальний адресу - це адреса призначення, видимий з внутрішньої мережі. У цьому прикладі ПК 1 відправляє трафік веб-сервера з IPv4-адресою 209.165.201.1. У рідкісних випадках ця адреса може відрізнятися від глобальної маршрутизації адреси призначення.

На малюнку показано, як адресується трафік, відправлений внутрішнім комп'ютером зовнішньому веб-сервера через маршрутизатор з підтримкою NAT. Також показано, як спочатку адресується і перетворюється зворотний трафік.

Примітка . Використання зовнішнього локального адреси не розглядається в матеріалі справжнього навчального курсу.

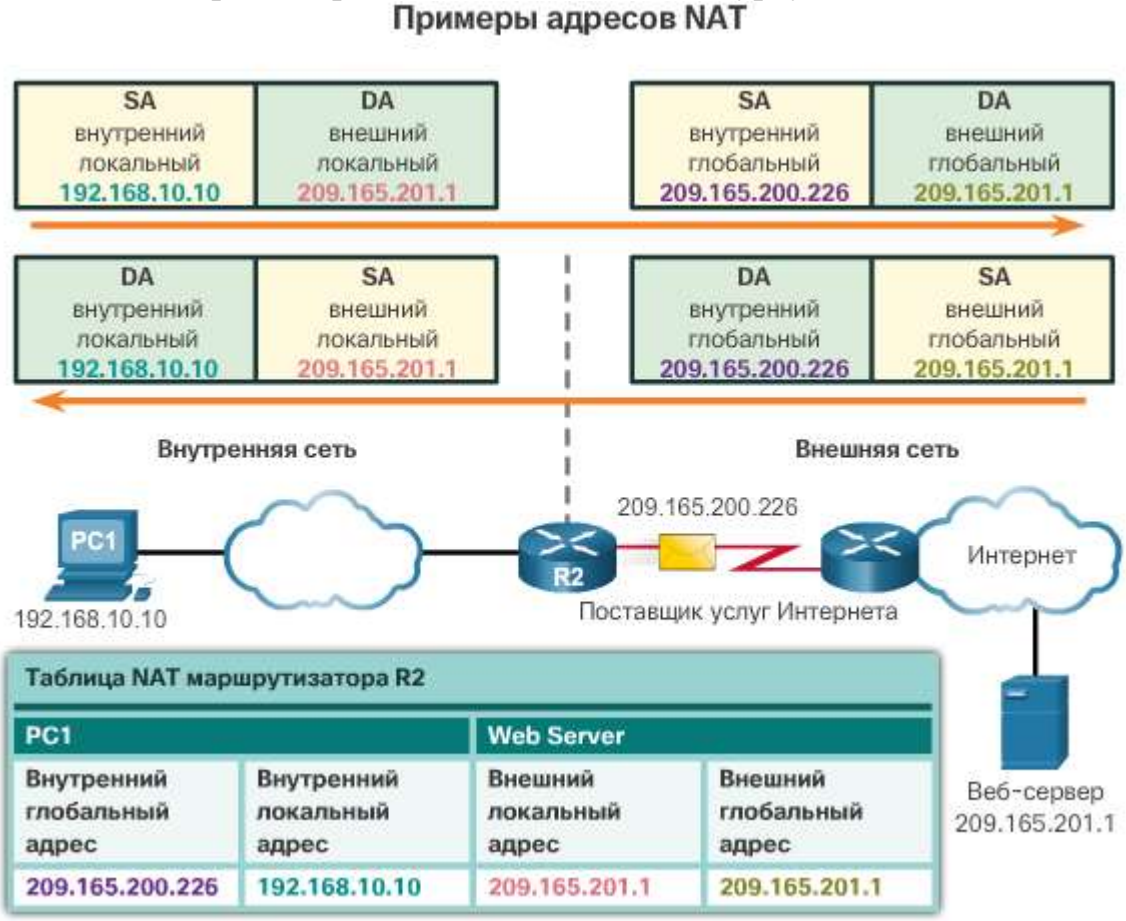


Рис. 4.3.5

Принцип роботи NAT

У цьому прикладі комп'ютера ПК 1 з приватним адресою 192.168.10.10 потрібно зв'язатися із зовнішнім веб-сервером з публічним адресою 209.165.201.1.

Для перегляду анімації натисніть кнопку «Відтворення».

ПК 1 відправляє пакет, адресований веб-сервера. Пакет пересилається маршрутизатором R1 маршрутизатора R2.

Отримавши пакет, маршрутизатор R2, що підтримує виконання NAT для даної мережі, зчитує IPv4-адрес джерела пакету, щоб визначити, чи відповідає пакет критеріям, визначеним для перетворення.

В даному випадку IPv4-адрес джерела відповідає критеріям і перетворюється з 192.168.10.10 (внутрішній локальний адресу) в 209.165.200.226 (внутрішній глобальний адреса). Маршрутизатор R2 додає це зіставлення локального і глобального адрес в таблицю NAT.

R2 відправляє за призначенням пакет з перетвореним адресою джерела.

Веб-сервер відповідає пакетом, адресованим внутрішньому глобальному адресою ПК 1 (209.165.200.226).

R2 отримує пакет з адресою призначення 209.165.200.226. R2 перевіряє таблицю NAT і знаходить запис для цього зіставлення. R2 використовує цю інформацію і перетворює внутрішній глобальний адресу (209.165.200.226) у внутрішній локальний адресу (192.168.10.10), після чого пакет пересилається PC1.

Статичне перетворення NAT

Існують три механізми перетворення:

Статична перетворення (статичний NAT) - це взаємно-однозначна відповідність між локальним і глобальним адресами.

Динамічне перетворення (динамічний NAT) - це зіставлення адрес за схемою «багато до багатьох» між локальними і глобальними адресами. Перетворення виконуються за наявністю. Наприклад, якщо є 100 внутрішніх локальних адрес і 10 внутрішніх глобальних адрес, в будь-який момент часу можуть бути перетворені тільки 10 з 100 внутрішніх локальних адрес. Через такого обмеження динамічне перетворення NAT підходить для виробничих мереж набагато менше, ніж перетворення адрес портів.

Перетворення адреси і номера порту (PAT) - це зіставлення адрес за схемою «багато до одного» між локальними та глобальними адресами. Даний метод також називається перевантаженням (NAT з перевантаженням). Наприклад, якщо є 100 внутрішніх локальних адрес і 10 внутрішніх глобальних адрес, PAT використовує порти в якості додаткового параметра для створення ефекту множення складності. Це дозволяє повторно використовувати будь-який з 10 внутрішніх глобальних адрес до 65 536 раз (в залежності від процесу: UDP, TCP або ICMP).

Статична перетворення NAT

Статичний NAT використовує зіставлення локальних і глобальних адрес за схемою «один в один». Ці відповідності задаються адміністратором мережі і залишаються незмінними.

На малюнку для маршрутизатора R2 налаштовані статичні відповідності для внутрішніх локальних адрес Сервера 1, ПК 2 і ПК 3. Коли ці пристрої відправляють трафік в Інтернет, їх внутрішні локальні адреси перетворюються в задані внутрішні глобальні адреси. Для зовнішніх мереж ці пристрої використовують публічні IPv4-адреси.

Метод статичного перетворення особливо корисний для веб-серверів або пристроїв, які повинні мати постійний адреса, доступний з Інтернету - наприклад, для веб-сервера компанії. Статичний NAT також підходить для пристроїв, які повинні бути доступні авторизованому персоналу, що працює поза офісом, але при цьому залишатися закритими для загального доступу через Інтернет. Наприклад, адміністратор може з ПК 4 підключитися за допомогою SSH до внутрішнього глобальному адресою Svr1 (209.165.200.226). Маршрутизатор R2 перетворює цей внутрішній глобальний адресу у внутрішній локальний адресу і підключає сеанс адміністратора до Svr1.

Для статичного NAT потрібна достатня кількість публічних адрес, доступних для загальної кількості одночасних сеансів користувачів.

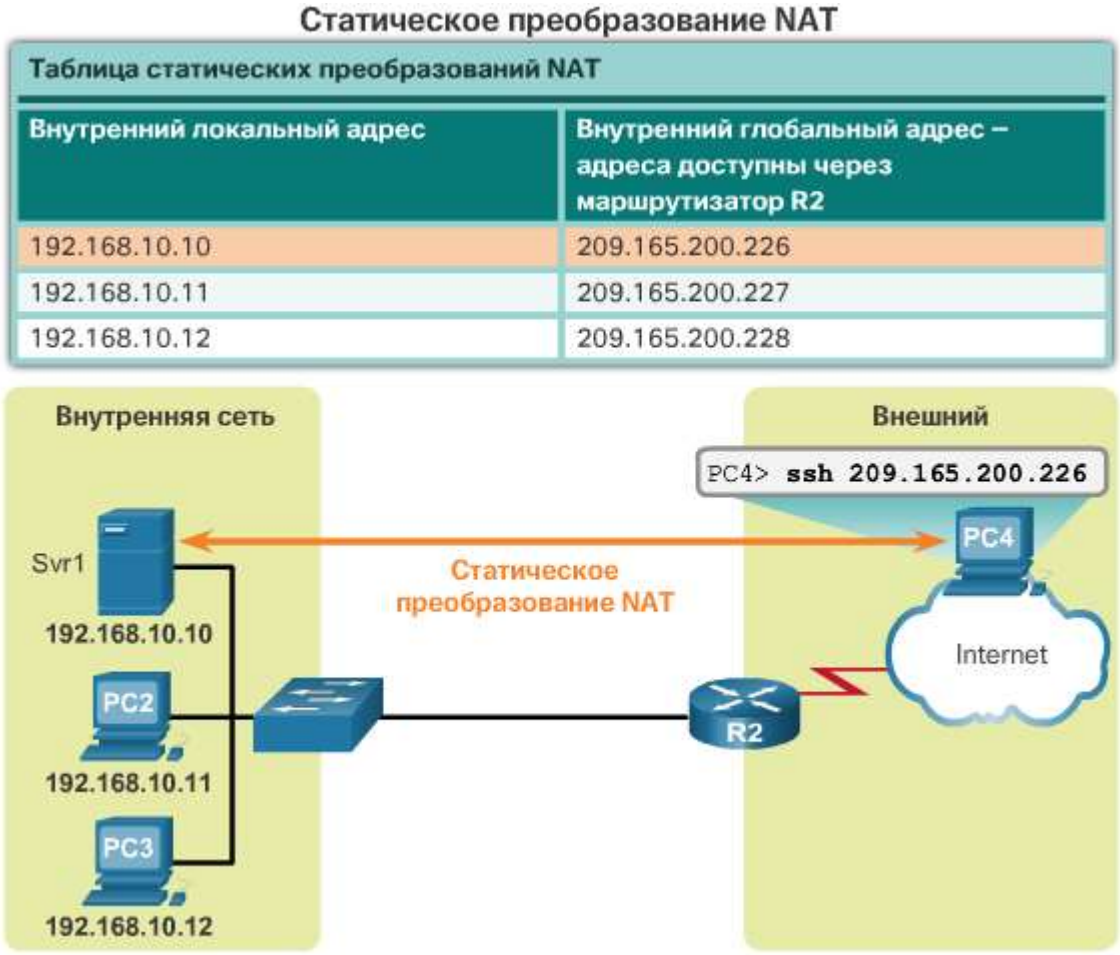


Рис. 4.3.6

Динамічне перетворення NAT

При динамічному перетворенні NAT використовується пул публічних адрес, які призначаються в порядку черги («першим прийшов - першим обслужили»). Коли внутрішній устрій запитує доступ до зовнішньої мережі, динамічне перетворення NAT призначає доступний публічний IPv4-адрес з пулу.

На малюнку ПК 3 отримує доступ до Інтернету, використовуючи перший доступний адреса в пулі динамічного NAT. Інші адреси як і раніше доступні для використання. Як і для статичного NAT, для динамічного NAT потрібна достатня кількість публічних адрес, здатне забезпечити загальна кількість одночасних сеансів користувачів.

Динамическое преобразование NAT

Внутренний локальный адрес	Внутренний пул глобальных адресов – адреса доступны через маршрутизатор R2
192.168.10.12	209.165.200.226
Присутствует	209.165.200.227
Присутствует	209.165.200.228
Присутствует	209.165.200.229
Присутствует	209.165.200.230

Рис. 4.3.7

Перетворення адрес портів (PAT)

Перетворення адреси і номера порту (PAT), також зване NAT з перевантаженням, зіставляє безліч приватних IPv4-адрес одному або декільком публічним IPv4-адрес. Так працює більшість домашніх маршрутизаторів. Інтернет-провайдер призначає одну адресу маршрутизатора, при цьому ще кілька домашніх пристроїв можуть одночасно отримувати доступ до Інтернету. NAT з перевантаженням - це найбільш поширений метод перетворення.

За допомогою даного методу безліч адрес можуть бути співставлені одному або декількох адресах, оскільки кожен приватний адресу також відстежується за номером порту. Коли пристрій запускає сеанс TCP / IP, створюється значення вихідного порту TCP або UDP або спеціально призначений ідентифікатор запиту для ICMP для визначення цього сеансу унікальним чином. Якщо маршрутизатор NAT отримує пакет від клієнта, він використовує свій номер порту джерела, щоб унікальним чином визначити конкретне перетворення NAT.

PAT гарантує, що пристрої будуть використовувати різні номери портів TCP для кожного сеансу взаємодії з сервером в Інтернеті. При поверненні відповіді від сервера номер порту джерела, який стає номером порту призначення при зворотному передачі, визначає, якого пристрою маршрутизатор перешле відповідні пакети. Процес PAT також перевіряє, чи були запитані вхідні пакети, таким чином підвищуючи ступінь безпеки сеансу.

Для управління анімацією використовуйте кнопки «Відтворення» і «Пауза» на малюнку.

Анімація ілюструє процес перетворення адрес портів (PAT). Щоб розрізняти перетворення, механізм PAT додає унікальні номери портів джерела до внутрішнього глобальному адресою.

Оскільки маршрутизатор R2 обробляє кожен пакет, він використовує номер порту (в розглянутому прикладі одна тисячі триста тридцять одна і 1555) для ідентифікації пристрою, з якого надійшов пакет. Адреса джерела (SA) - це внутрішній локальний адресу з доданим призначеним номером порту TCP / IP. Адреса призначення (DA) - це зовнішній локальний адресу з доданим номером порту потрібної служби. В даному прикладі порт служби дорівнює 80, т. Е. Порту для протоколу HTTP.

Для адреси джерела маршрутизатор R2 перетворює внутрішній локальний адресу у внутрішній глобальний адресу з доданим номером порту. Адреса призначення не змінюється, але тепер він вважається зовнішнім глобальним IPv4-адресою. Коли веб-сервер відповідає, шлях повторюється, тільки в зворотному порядку.

Наступний доступний порт

У попередньому прикладі номера портів клієнта, тисячі триста тридцять один і 1555, не змінювалися на маршрутизаторі з підтримкою NAT. Дана ситуація не дуже ймовірна, оскільки велика ймовірність того, що ці номери портів вже використовуються для інших активних сеансів.

Перетворення PAT намагається зберегти оригінальний порт джерела. У тому випадку, якщо початковий порт джерела вже використовується, PAT призначає перший доступний номер порту, починаючи з найменшого у відповідній групі портів - 0-511, 512-1023 або 1024-65535. Якщо доступних портів більше немає, а в пулі адрес є кілька зовнішніх адрес, PAT переходить до наступного адресою, намагаючись виділити початковий порт джерела. Даний процес триває до тих пір, поки не вичерпаються як доступні порти, так і зовнішні IPv4-адреси.

Для ознайомлення з принципом роботи PAT натисніть кнопку «Відтворення» на малюнку. У розглянутому прикладі в процесі перетворення PAT другого адресою вузла призначається наступний доступний порт (1445).

В анімації вузли вибирають один і той же номер порту - 1444. Це допустимо для внутрішнього адреси, оскільки хостам призначаються унікальні приватні IPv4-адреси. Але на маршрутизаторі з підтримкою NAT номера портів необхідно змінити. В іншому випадку пакети від двох різних вузлів виходили б з R2 з однаковою адресою джерела. В даному прикладі припустимо, що перші 420 портів в діапазоні 1024-65 535 вже використовуються. Тобто наступний доступний номер порту - 1445.

Рис. 4.3.8

Порівняння NAT і PAT

Сформульовані нижче відмінності між NAT і PAT допоможуть зрозуміти особливості кожного з цих методів перетворення.

Як показано на малюнку, NAT перетворює IPv4-адреси, виходячи зі схеми 1: 1 для приватних IPv4-адрес і публічних IPv4-адрес. У той же час PAT змінює і адреса, і номер порту.

NAT пересилає вхідні пакети одержувачу, використовуючи вхідний IPv4-адрес джерела, наданий вузлом в публічній мережі. При використанні PAT зазвичай задіюється тільки один або невелику кількість публічно представлених IPv4-адрес. Вхідні пакети з публічної мережі направляються адресатам в приватній мережі за допомогою таблиці на маршрутизаторі з NAT. Дана таблиця відстежує пари публічних і приватних портів. Це називається відстеженням з'єднань.

Пакети без сегмента 4 рівня

Що ж відбувається з пакетами IPv4, передають дані, які не є сегментом TCP або UDP? Дані пакети не містять номера порту рівня 4. PAT перетворює більшість основних протоколів, переданих за допомогою IPv4 і не використовують TCP або UDP як протокол транспортного рівня. Найпоширенішим серед таких протоколів є протокол ICMPv4. Процес перетворення PAT обробляє кожен з цих протоколів по-різному. Наприклад, повідомлення запитів ICMPv4, луна-запити і луна-відповіді містять ідентифікатор запиту (Query ID). ICMPv4 використовує ідентифікатор запиту (Query ID), щоб зіставити луна-запит з відповідним луна-відповіддю. Ідентифікатор запиту збільшується з кожним відправленим луна-запитом. PAT використовує ідентифікатор запиту замість номера порту рівня 4.

Примітка . Інші повідомлення ICMPv4 не використовують ідентифікатор запиту (Query ID). Ці повідомлення та інші протоколи, які не використовують

номери портів TCP і UDP, можуть відрізнятися один від одного і не розглядаються в рамках матеріалу справжнього навчального курсу.

Рис. 4.3.9

Переваги NAT

NAT забезпечує безліч переваг, у тому числі такі:

NAT зберігає офіційно зареєстровану схему адресації, дозволяючи приватне використання внутрішніх мереж. NAT економить адреси завдяки мультиплексуванню додатків на рівні портів. При використанні NAT з перевантаженням внутрішні вузли можуть використовувати для всіх зовнішніх взаємодій один публічний IPv4-адрес. При цьому типі настройки для підтримки безлічі внутрішніх вузлів потрібно дуже невелика кількість зовнішніх адрес.

NAT підвищує гнучкість підключень до публічної мережі. Для забезпечення надійних підключень до публічної мережі можна створити множинні пули, резервні пули і пули розподілу навантаження.

NAT забезпечує сталість схем внутрішньої мережевої адресації. Якщо в мережі не використовуються приватні IPv4-адреси і NAT, зміна схеми публічних IPv4-адрес потребують зміни адрес всіх вузлів існуючої мережі. Витрати на зміну адресації вузлів можуть виявитися істотними. NAT дозволяє зберегти існуючу схему приватних IPv4-адрес, одночасно підтримуючи простий перехід на нову схему публічної адресації. Це означає, що організація може змінити інтернет-провайдера, не змінюючи налаштувань своїх внутрішніх клієнтів.

NAT приховує IPv4-адреси кінцевого користувача. Завдяки використанню IPv4-адрес відповідно до RFC 1918 року, побічним ефектом перетворення NAT є приховування IPv4-адрес користувачів і інших пристроїв. Деякі вважають це функцією безпеки, однак більшість експертів стверджують, що перетворення

NAT не забезпечує безпеку. Міжмережевий екран з контролем стану підключень - ось що забезпечує безпеку на кордоні мережі.

Недоліки NAT

Перетворення мережевих адрес (NAT) має ряд недоліків. Той факт, що для з'єднання з Інтернетом взаємодіють безпосередньо з пристроєм, що підтримує NAT, а не з фактичним вузлом приватної мережі, створює ряд проблем.

Один з недоліків використання NAT пов'язаний з продуктивністю мережі, особливо це стосується протоколів реального часу, таких як VoIP. NAT збільшує затримки пересилання, оскільки перетворення кожного IPv4-адреси в заголовках пакетів вимагає часу. Комутація першого пакету діалогу завжди є програмним процесом; цей пакет завжди проходить більш повільним шляхом. Маршрутизатор повинен аналізувати кожен пакет, щоб вирішити, чи потрібно його перетворення. Маршрутизатор повинен змінити заголовок IPv4 і, можливо, змінити заголовок TCP або UDP. При кожному перетворенні повинна бути перерахована контрольна сума заголовка IPv4, а також контрольна сума TCP або UDP. Якщо в кеші є відповідний запис, інші пакети проходять по шляху для швидкої комутації. В іншому випадку вони теж затримуються.

Іншим недоліком використання NAT є втрата наскрізний адресації. Багато інтернет-протоколи і додатки залежать від наскрізної адресації від джерела до вузла призначення. Деякі застосунки можуть бути несумісними з NAT. Наприклад, деякі програми безпеки, такі як цифрові підписи, не працюють з NAT, оскільки IPv4-адрес джерела змінюється по шляху до вузла призначення. Програми, що використовують фізичні адреси замість доменних імен, не можуть досягти вузлів призначення при проходженні через маршрутизатор з NAT. У деяких випадках цієї проблеми можна уникнути за допомогою статичних зіставлень NAT.

Крім того, втрачається можливість наскрізної трасування IPv4. Дуже сильно ускладнюється трасування пакетів, що піддаються численним змінам адреси пакета при проходженні декількох ділянок NAT, що, в свою чергу, ускладнює усунення неполадок.

Використання NAT також ускладнює роботу з тунельними протоколами, такими як IPsec, оскільки перетворення NAT змінює значення в заголовках, що призводить до збою перевірки цілісності.

Робота служб, що вимагають ініціалізації підключень TCP з зовнішньої мережі або використовують протоколи без урахування стану, наприклад, на основі UDP, може бути порушена. Якщо на маршрутизаторі NAT відсутня установка таких протоколів, що входять пакети не зможуть досягти свого призначення. Деякі протоколи можуть підтримувати один екземпляр NAT між вузлами-учасниками (наприклад, FTP в пасивному режимі), але не працюють, якщо обидві системи відокремлені від Інтернету за допомогою NAT.

Налаштування статичного NAT

Статична перетворення NAT - це взаємно-однозначне зіставлення внутрішнього і зовнішнього адрес. Статичний NAT дозволяє зовнішніх пристроїв ініціювати підключення до внутрішніх пристроїв за допомогою статично призначеного публічної адреси. Наприклад, внутрішньому веб-

сервера може бути зіставлений внутрішній глобальний адресу, визначену таким чином, щоб він був доступний з зовнішніх мереж.

На рис. 1 показана внутрішня мережа, що має веб-сервер з приватним IPv4-адресою. На маршрутизаторі R2 налаштований статичний NAT, щоб надати доступ до веб-сервера пристроїв з зовнішньої мережі (Інтернет). Клієнт із зовнішньої мережі звертається до веб-сервера, використовуючи публічний IPv4-адрес. Статичний NAT перетворює публічний IPv4-адрес в приватний IPv4-адрес.

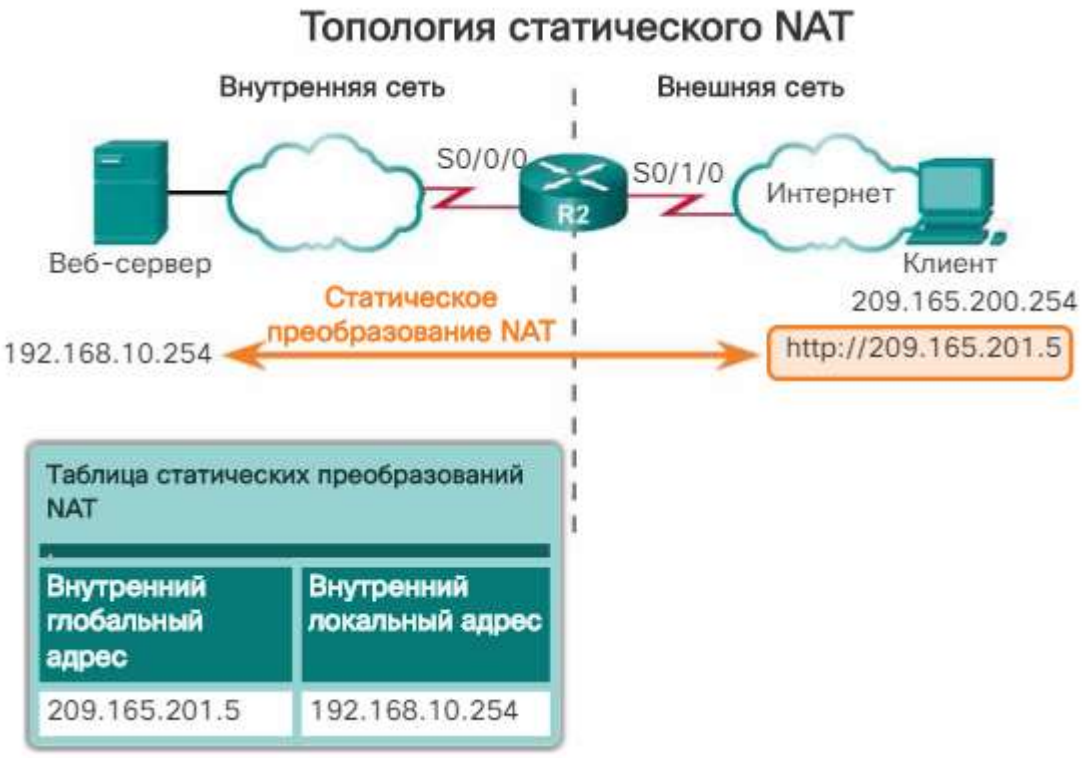


Рис. 4.3.10

Налаштування статичного NAT пов'язана з двома основними завданнями.

Крок 1. Першим завданням є створення відповідності між внутрішнім локальним і внутрішнім глобальним адресами. Наприклад, на рис. 1 в якості статичного перетворення NAT налаштовані внутрішній локальний адресу 192.168.10.254 і внутрішній глобальний адреса 209.165.201.5.

Крок 2. Після настройки відповідності інтерфейси, які беруть участь в перетворенні, налаштовуються як внутрішні або зовнішні щодо NAT. У цьому прикладі інтерфейс Serial 0/0/0 маршрутизатора R2 є внутрішнім, а Serial 0/1/0 - зовнішнім інтерфейсом.

Пакети, що надходять на внутрішній інтерфейс маршрутизатора R2 (Serial 0/0/0) від налаштованого внутрішнього локального IPv4-адреси (192.168.10.254), перетворюються, а потім передаються в зовнішню мережу. Пакети, що надходять на зовнішній інтерфейс маршрутизатора R2 (Serial 0/1/0), адресовані налаштованому внутрішньому глобальному IPv4-адресою (209.165.201.5), перетворюються для передачі внутрішнього локальної адреси (192.168.10.254) і потім передаються у внутрішню мережу.

На рис. 2 приведені команди, необхідні для налаштування статичного NAT.

Настройка статического NAT

Шаг	Действие	Примечания
1	Настройте статическое преобразование между внутренним локальным адресом и внутренним глобальным адресом. `Router(config)# ip nat inside source static local-ip global-ip`	Введите команду глобального режима настройки `no ip nat inside source static` , чтобы удалить динамическое преобразование источника.
2	Укажите внутренний интерфейс. `Router(config)# interface type number`	Введите команду `interface`. Вид запроса командной строки изменится с `(config)#` на `(config-if)#`.
3	Отметьте интерфейс как подключенный к внутренней сети. `Router(config-if)# ip nat inside`	
4	Выйдите из режима настройки интерфейса. `Router(config-if)# exit`	
5	Укажите внешний интерфейс. `Router(config)# interface type number`	

Рис. 4.3.11

6	Пометьте интерфейс как подключенный к внешней сети. `Router(config-if)# ip nat outside`	

Рис. 4.3.12

На рис. показані команди, необхідні для створення на маршрутизаторі R2 статичного зіставлення NAT для веб-сервера в прикладі топології. В рамках показаної настройки R2 перетворює в пакетах, відправлених веб-сервером, адреса 192.168.10.254 в публічний IPv4-адрес 209.165.201.5. Клієнт з Інтернету направляє веб-запити на публічну IPv4-адрес 209.165.201.5. Маршрутизатор R2 пересилає цей трафік веб-сервера за адресою 192.168.10.254.

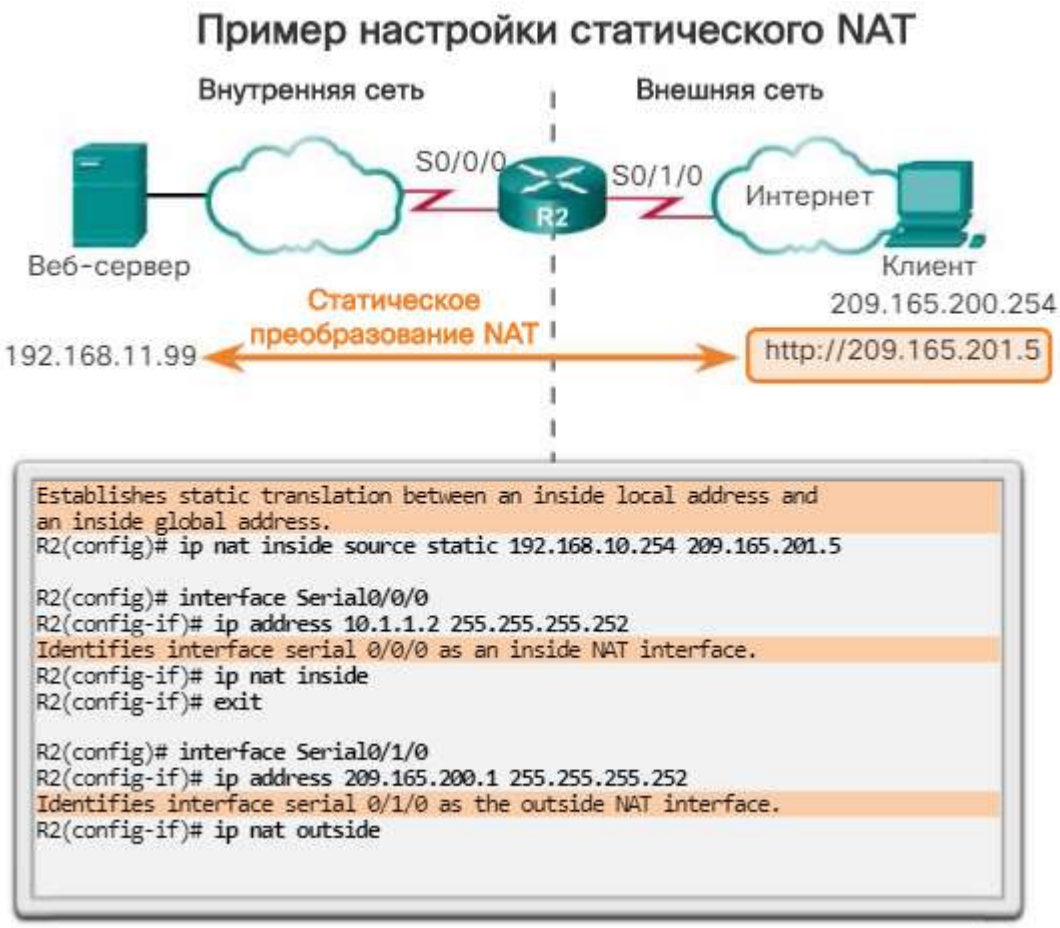


Рис. 4.3.13

Аналіз статичного перетворення NAT

На цьому малюнку показаний процес статичного перетворення NAT між клієнтом і веб-сервером з використанням попередньої настройки. Статичні перетворення зазвичай використовуються, коли клієнтам з зовнішньої мережі (Інтернет) потрібно звернутися до серверів внутрішньої мережі.

1. Клієнтові потрібно підключитися до веб-сервера. Клієнт відправляє пакет на веб-сервер, використовуючи публічний IPv4-адрес призначення 209.165.201.5. Це внутрішній глобальний адреса веб-сервера.

2. Перший пакет, отриманий маршрутизатором R2 від клієнта на зовнішньому інтерфейсі NAT, змушує R2 перевірити свою таблицю NAT. IPv4-адрес призначення знаходиться в таблиці NAT, і маршрутизатор виконує відповідні перетворення.

3. R2 замінює внутрішній глобальний адреса 209.165.201.5 внутрішнім локальним адресою 192.168.10.254. Потім R2 пересилає пакет веб-сервера.

4. Веб-сервер отримує пакет і відповідає клієнтові, використовуючи внутрішній локальний адресу 192.168.10.254.

5a. R2 отримує пакет від веб-сервера на свій внутрішній інтерфейс NAT з адресою джерела, відповідним внутрішньому локальній адресі веб-сервера, 192.168.10.254.

5b. R2 перевіряє таблицю NAT на предмет наявності перетворення для внутрішнього локального адреси. Ця електронна адреса була присутня в таблиці NAT. R2 може конвертувати адреси джерела у внутрішній глобальний адреса 209.165.201.5 і пересилає пакет клієнту.

6. Клієнт отримує пакет і продовжує діалог. Маршрутизатор NAT виконує кроки 2-5b для кожного пакета (крок 6 на малюнку не показаний).

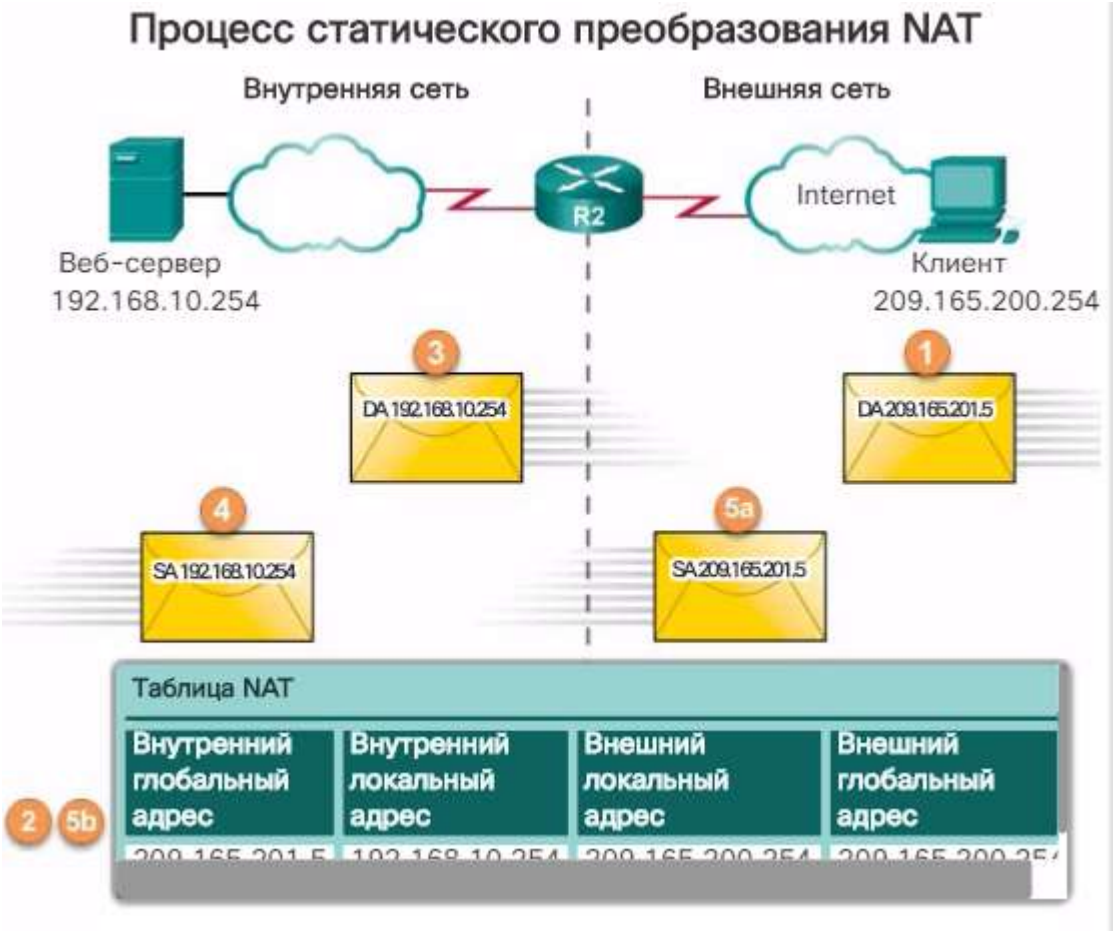


Рис. 4.3.14

Перевірка статичного NAT

Для перевірки роботи NAT використовується команда **show ip nat translations** . Ця команда відображає активні перетворення NAT. На відміну від динамічних перетворень, статичні перетворення завжди присутні в таблиці NAT. На рис. 1 показаний результат цієї команди для попереднього прикладу настройки. Оскільки в прикладі наводиться статична настройка, перетворення завжди присутній в таблиці NAT незалежно від активних взаємодій. Якщо команда вводиться в ході розмови виникла, вихідні дані будуть також містити адресу зовнішнього пристрою, як показано на рис. 1.

Проверка преобразований статического NAT

Статическое преобразование всегда представлено в таблице NAT.

```
R2# show ip nat translations
Pro Inside global  Inside local   Outside local  Outside global
--- 209.165.201.5  192.168.10.254  ---            ---
R2#
```

Статическое преобразование во время активного сеанса.

```
R2# show ip nat translations
Pro Inside global Inside local   Outside local    Outside global
--- 209.165.201.5 192.168.10.254 209.165.200.254  209.165.200.254
R2#
```

Рис. 4.3.15

Іншою корисною командою є **show ip nat statistics** . Як показано на рис. 2, команда **show ip nat statistics**інформує вас про сумарну кількість активних перетворень, параметрах настройки NAT, зокрема адрес в пулі і числі виділених адрес.

Проверка статистики статического NAT

```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 0  Misses: 0
<Данные опущены>
Client PC establishes a session with the web server

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:14 ago
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0
Hits: 5  Misses: 0


<Данные опущены>
```

Рис. 4.3.16

Щоб переконатися в правильності роботи перетворення NAT, перед тестуванням рекомендується очистити статистику всіх попередніх перетворень за допомогою команди **clear ip nat statistics** .

До початку взаємодії з веб-сервером команда **show ip nat statistics** не повинна показувати будь-яких збігів. Після установки клієнтом сеансу зв'язку з веб-сервером в вихідних даних команди **show ip nat statistics** кількість збігів у внутрішньому інтерфейсі збільшується до 5 (Serial0 / 0/0). Цим підтверджується виконання статичного перетворення NAT на R2.

Принцип роботи динамічного NAT

У той час як статичну перетворення NAT забезпечує постійну відповідність між внутрішнім локальним адресою і внутрішнім глобальним адресою, динамічне перетворення NAT підтримує автоматичне співставлення внутрішніх локальних адрес внутрішнім глобальним адресами. Ці внутрішні глобальні адреси зазвичай є публічними IPv4-адресами. У динамічному NAT для перетворення використовується група або пул публічних IPv4-адрес.

Для динамічного NAT, як і для статичного NAT, потрібно налаштування внутрішнього і зовнішнього інтерфейсів, що беруть участь в перетворенні NAT. Однак якщо статична перетворення NAT створює постійне зіставлення з однією адресою, для динамічного NAT використовується пул адрес.

Примітка . Перетворення між публічними і приватними IPv4-адресами є найпоширенішим застосуванням NAT. Проте, перетворення NAT можуть виникати між будь-якими парами адрес.

У прикладі топології, показаному на малюнку, внутрішня мережа використовує адреси з простору приватних адрес, визначеного в RFC 1918. До маршрутизатора R1 підключені дві локальних мережі - 192.168.10.0/24 і 192.168.11.0/24. Граничний маршрутизатор R2 налаштований на динамічне перетворення NAT з використанням пулу публічних IPv4-адрес від 209.165.200.226 до 209.165.200.240.

Пул публічних IPv4-адрес (внутрішній пул глобальних адрес) доступний будь-якого пристрою у внутрішній мережі за принципом черги («першим прийшов - першим обслужили»). При динамічному перетворенні NAT один внутрішній адреса перетворюється в один зовнішній адресу. Для цього типу перетворення в пулі має бути досить адрес, щоб охопити всі внутрішні пристрої, яким одночасно потрібно доступ до зовнішньої мережі. Якщо використані всі адреси пулу, пристрій повинен дочекатися доступного адреси, щоб отримати доступ до зовнішньої мережі.

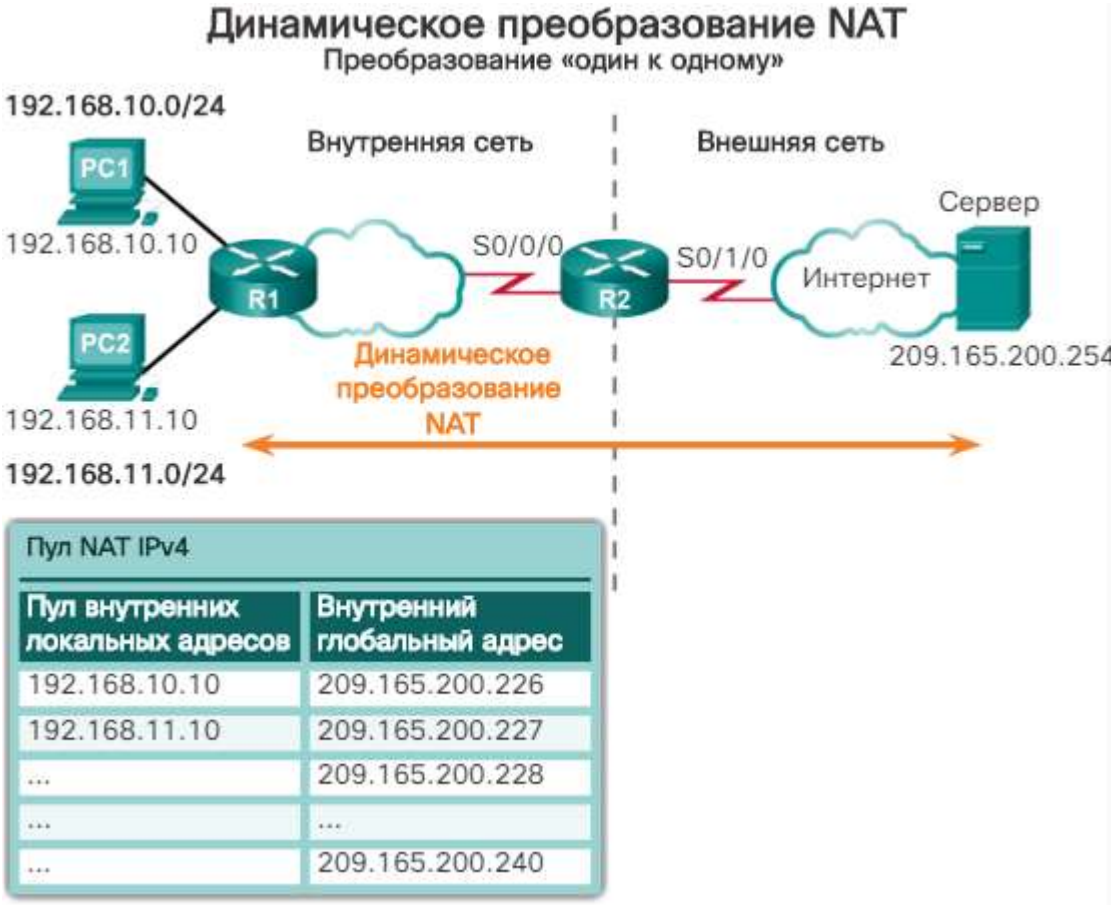


Рис. 4.3.17

Налаштування динамічного NAT

На рис. показані кроки і команди, які використовуються для настройки динамічного NAT.

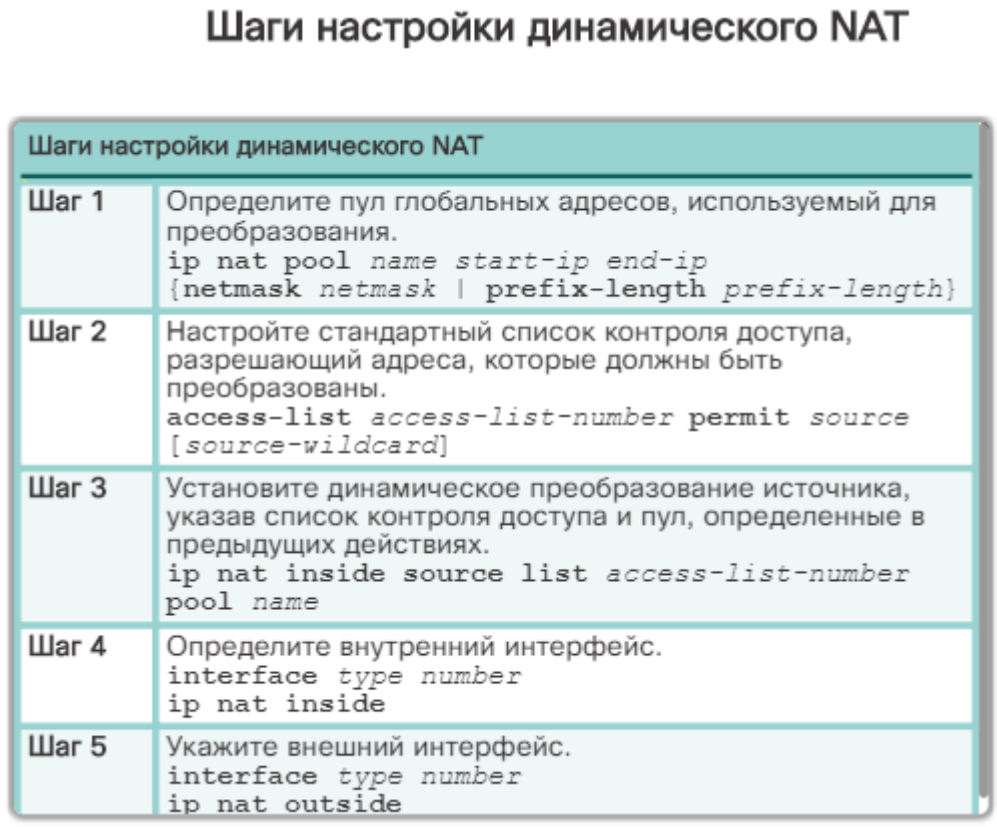


Рис. 4.3.18

Крок 1. За допомогою команди **ip nat pool** визначте пул адрес, які будуть використовуватися для перетворення. Даний пул адрес зазвичай є групою публічних адрес. Ці адреси визначаються за допомогою вказівки початкового і кінцевого IPv4-адрес пулу. Ключове слово **netmask** або **prefix-length** вказує, які біти адреси належать до мережі, а які - до діапазону адрес вузлів.

Крок 2. Налаштуйте стандартний ACL, щоб визначити (дозволити) тільки ті адреси, які повинні бути перетворені. Список контролю доступу з дуже великою кількістю дозволяють інструкцій може призвести до непередбачуваних результатів. Пам'ятайте, що в кінці кожного ACL мається на увазі рядок **deny all** .

Крок 3. Виконайте прив'язку ACL до пулу. Команда **ip nat inside source list** *номер списку доступу* **pool** *ім'я пулу* використовується для прив'язки списку контролю доступу до пулу. Ця установка використовується маршрутизатором, щоб визначити, які пристрої (**list**) отримують якісь адреси (**pool**).

Крок 4. Визначте інтерфейси, які є внутрішніми по відношенню до NAT, т. Е. Все інтерфейси, підключені до внутрішньої мережі.

Крок 5. Визначте інтерфейси, які є зовнішніми щодо NAT; це все інтерфейси, підключені до зовнішньої мережі.

На рис. 2 наведено приклад топології і відповідна настройка. Ця установка дозволяє перетворення для всіх вузлів мережі 192.168.0.0/16, що містить локальні мережі 192.168.10.0 і 192.168.11.0, коли вузли створюють трафік, що входить в S0 / 0/0 і виходить з S0 / 1/0. Адреси цих вузлів перетворюються в доступний адресу з пулу в діапазоні від 209.165.200.226 до 209.165.200.240.

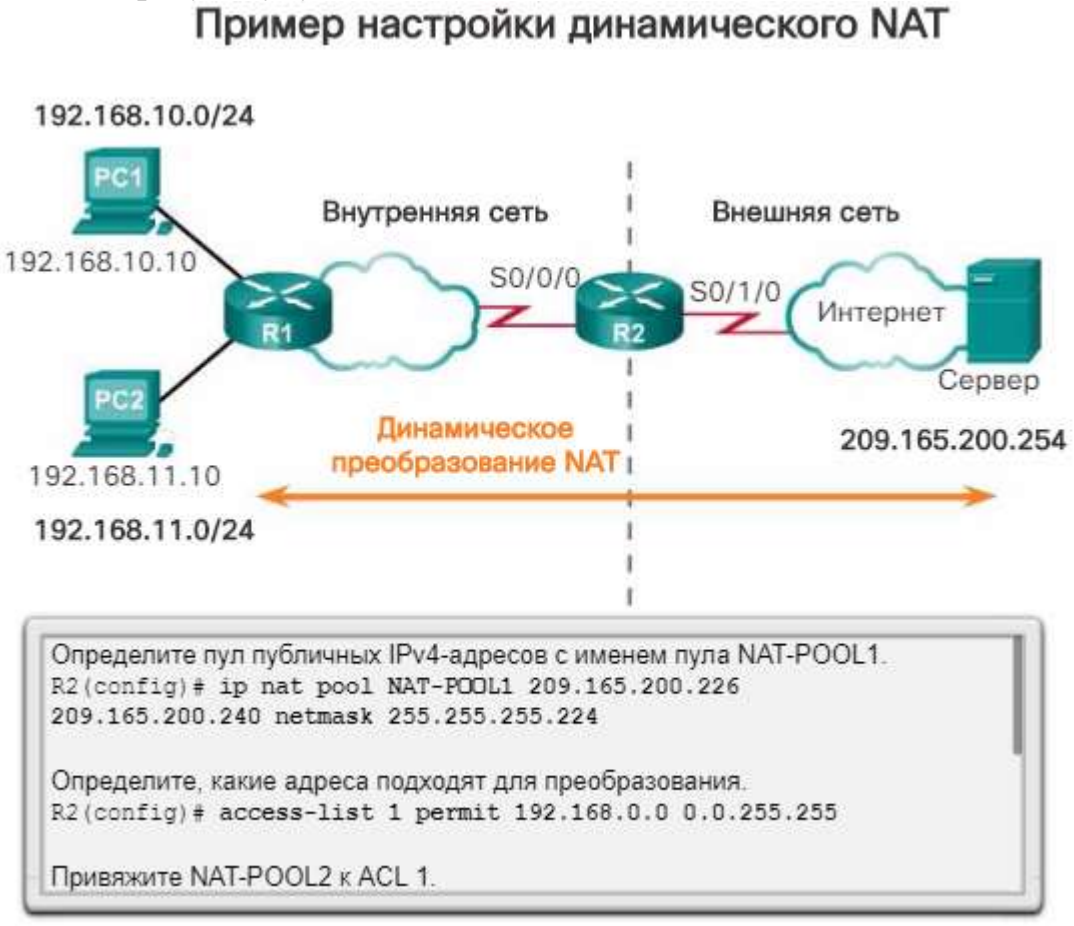


Рис. 4.3.19

На рис. показана топологія, яка використовується для налаштування в інструменті перевірки синтаксису.

Рис. 4.3.20

Аналіз динамічного NAT

На наведених малюнках показано процес динамічного перетворення NAT між двома клієнтами і веб-сервером з використанням попередньої настройки.

На рис. 1 показаний потік трафіку зсередини назовні.

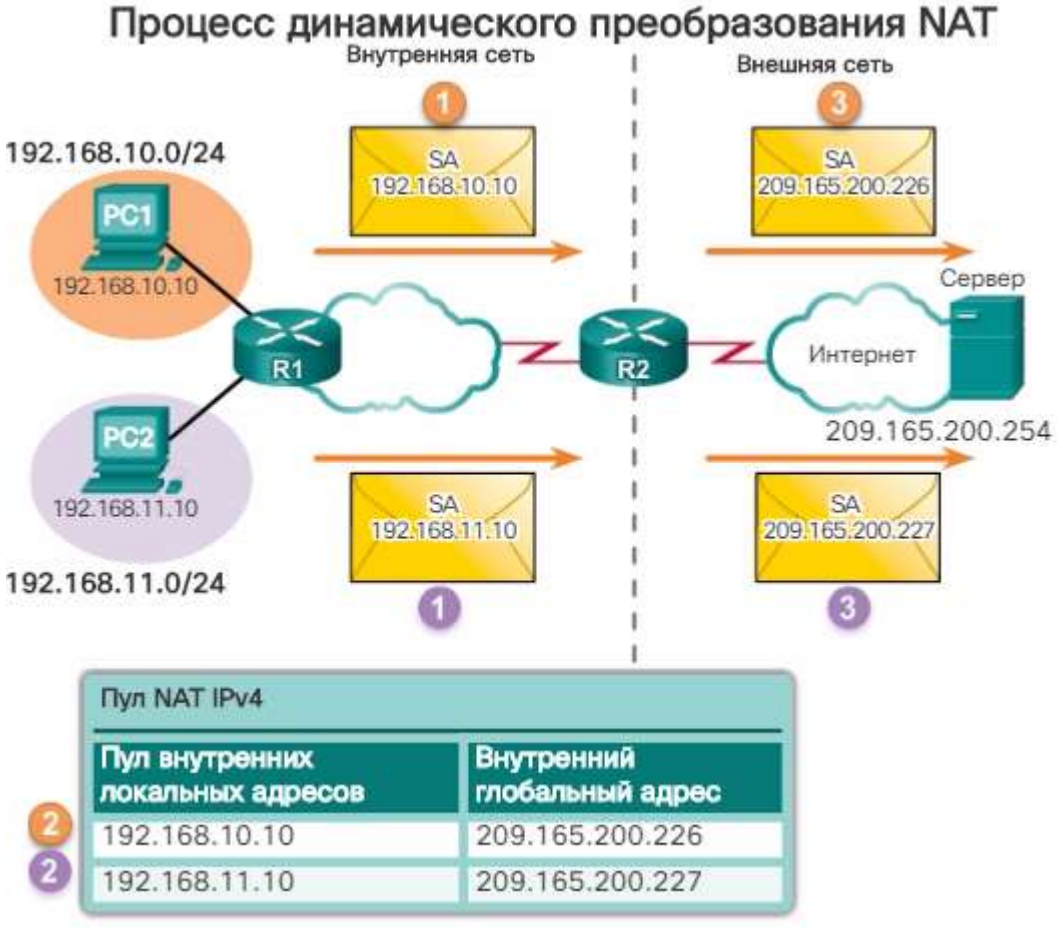


Рис. 4.3.21

1. Вузли з IPv4-адресами джерела (192.168.10.10 (PC1) і 192.168.11.10 (PC2)) відправляють пакети, що запитують підключення до сервера на публічний IPv4-адрес (209.165.200.254).

2. Маршрутизатор R2 отримує перший пакет від вузла 192.168.10.10. Оскільки цей пакет був отриманий на інтерфейс, налаштований як внутрішній інтерфейс NAT, R2 перевіряє конфігурацію NAT, щоб визначити, чи слід виконувати перетворення для даного пакета. ACL дозволяє цей пакет, тому R2 виконує його перетворення. Маршрутизатор R2 перевіряє свою таблицю NAT. Оскільки для даного IPv4-адреси немає записів перетворення, R2 вирішує, що для адреси джерела 192.168.10.10 потрібно динамічне перетворення. Маршрутизатор R2 вибирає доступний глобальний адресу з динамічного пулу адрес і створює запис перетворення - 209.165.200.226. Початковий IPv4-адрес джерела (192.168.10.10) - це внутрішній локальний адресу, а використовуваний для перетворення адреса - це внутрішній глобальний адресу (209.165.200.226) в таблиці NAT.

R2 повторює процедуру для другого вузла, 192.168.11.10, вибираючи наступний доступний глобальний адресу з динамічного пулу адрес і створюючи другий запис перетворення, 209.165.200.227.

3. R2 замінює внутрішній локальний адресу джерела ПК 1 (192.168.10.10) використовуваним для перетворення внутрішнім глобальним адресою (209.165.200.226) і пересилає пакет. Ті ж дії виконуються для пакета, відправленого ПК 2, з використанням для перетворення адреси, відповідного ПК 2 (209.165.200.227).

На рис. 2 показаний потік трафіку ззовні всередину.

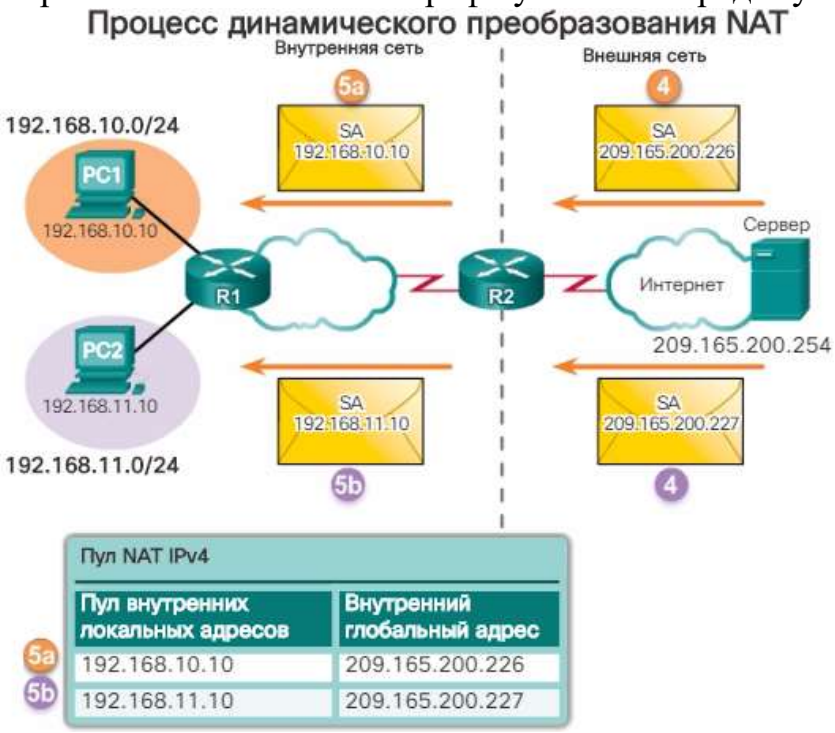


Рис. 4.3.22

4. Сервер отримує пакет від ПК 1 і відповідає, використовуючи IPv4-адрес призначення 209.165.200.226. Отримавши другий пакет, сервер відповідає ПК 2, використовуючи IPv4-адрес призначення 209.165.200.227.

5a. Отримавши пакет з IPv4-адресою призначення 209.165.200.226, маршрутизатор R2 виконує пошук в таблиці NAT. За допомогою зіставлення з таблиці маршрутизатор R2 виконує перетворення адреси назад у внутрішній локальний адресу (192.168.10.10) і пересилає пакет ПК 1.

5b. Отримавши пакет з IPv4-адресою призначення 209.165.200.227, маршрутизатор R2 виконує пошук в таблиці NAT. За допомогою зіставлення з таблиці маршрутизатор R2 виконує перетворення адреси назад у внутрішній локальний адресу (192.168.11.10) і пересилає пакет ПК 2.

6. ПК 1 з адресою 192.168.10.10 і ПК 2 з адресою 192.168.11.10 отримують пакети і продовжують діалог. Маршрутизатор NAT виконує кроки 2-5 для кожного пакета (крок 6 не наводиться на малюнках).

Перевірка динамічного NAT

У вихідних даних команди **show ip nat translations** , представлених на рис. 1, показані відомості про двох попередніх призначеннях NAT. Команда відображає всі налаштовані статичні перетворення адрес і все динамічні перетворення, створені в результаті обробки трафіку.

Проверка динамического NAT с помощью команды `show ip nat translations`

```
R2# show ip nat translations
Pro  Inside global         Inside local   Outside local  Outside global
---  209.165.200.226       192.168.10.10  ---            ---
---  209.165.200.227       192.168.11.10  ---            ---
R2#
R2# show ip nat translations verbose
Pro  Inside global         Inside local   Outside local  Outside global
---  209.165.200.226       192.168.10.10  ---            ---
     create 00:17:25,      use 00:01:54 timeout:86400000, left
23:58:05, Map-Id(In): 1,
     flags:
none, use_count: 0, entry-id: 32, lc_entries: 0
---  209.165.200.227       192.168.11.10      ---        ---
     create 00:17:22,      use 00:01:51 timeout:86400000, left
23:58:08, Map-Id(In): 1,
     flags:
none, use_count: 0, entry-id: 34, lc_entries: 0
R2#
```

Рис. 4.3.23

Додавання ключового слова **verbose** виводить додаткову інформацію про кожного перетворенні, включаючи час, що минув після створення і використання запису.

За замовчуванням термін дії записів перетворення закінчується через 24 години, якщо настройка таймерів не була змінена за допомогою команди **ip nat translation timeout** *timeout-seconds* в режимі глобальної конфігурації.

Для видалення динамічних записів до закінчення їх часу дії використовуйте команду привілейованого режиму EXEC **clear ip nat translation** (рис. 2). При проведенні перевірки настройки NAT рекомендується

видаляти динамічні записи. Як показано в таблиці, цю команду можна використовувати з ключовими словами і змінними, щоб визначити видаляються записи. Видалення конкретних записів потрібно для того, щоб не порушити роботу активних сеансів. Для видалення всіх перетворень з таблиці використовуйте команду привілейованого режиму EXEC **clear ip nat translation** *.

Удаление преобразований NAT

```
R2# clear ip nat translation *
R2# show ip nat translations

R2#
```

Команда	Описание
`clear ip nat translation *`	Удаляет все записи динамического преобразования из таблицы преобразования NAT.
`clear ip nat translation inside global-ip local-ip [outside local-ip global-ip]`	Удаляет запись простого динамического преобразования, которая содержит преобразование внутренних адресов или преобразования и внешних, и внутренних адресов.
`clear ip nat translation protocol inside global-ip`	Удаляет расширенную запись динамического преобразования.

Рис. 4.3.24

Примітка . З таблиці видаляються тільки динамічні перетворення. Статичні адреси можна прибрати з таблиці перетворень.

Як показано на рис. 3, команда **show ip nat statistics** інформує вас про сумарну кількість активних перетворень, параметрах настройки NAT, зокрема адрес в пулі і числі виділених адрес.

Проверка динамического NAT с помощью команды `show ip nat statistics`

```
R2# clear ip nat statistics

PC1 and PC2 establish sessions with the server

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 0 extended)
Peak translations: 6, occurred 00:27:07 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 2
 pool NAT-POOL1: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 2 (13%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```

Рис. 4.3.25

В якості альтернативи можна скористатися командою **show running-config** і знайти команди NAT, ACL, інтерфейсу або пулу з потрібними значеннями. Уважно вивчіть результати і виправте всі виявлені помилки.

Перетворення адреси і номера порту PAT (також зване NAT з перевантаженням) економить адреси у внутрішньому пулі глобальних адрес, дозволяючи маршрутизатора використовувати один внутрішній глобальний адреса для кількох внутрішніх локальних адрес. Іншими словами, один публічний IPv4-адрес може використовуватися для сотень або навіть тисяч внутрішніх приватних IPv4-адрес. Якщо налаштований даний тип перетворення, маршрутизатор зберігає достатній обсяг інформації протоколів більш високих рівнів, наприклад, номери портів TCP або UDP, для зворотного перетворення внутрішнього глобального адреси в потрібний внутрішній локальний адресу. При прив'язці декількох внутрішніх локальних адрес одному внутрішньому глобальному адресою для розрізнення локальних адрес використовуються номери портів TCP або UDP.

Примітка. Сумарна кількість внутрішніх адрес, які можуть бути перетворені в один зовнішній адресу, теоретично може досягати 65 536 на один IPv4-адрес. Але число внутрішніх адрес, яким можна призначити один IPv4-адрес, приблизно становить 4000.

Залежно від способу виділення публічних IPv4-адрес інтернет-провайдером існують два способи налаштування PAT. У першому випадку інтернет-провайдер виділяє організації кілька публічних IPv4-адрес, а в другому випадку виділяється єдиний публічний IPv4-адрес, необхідний організації для підключення до мережі інтернет-провайдера.

Налаштування PAT для пулу загальнодоступних IPv4-адрес

Якщо об'єкту було виділено кілька публічних IPv4-адрес, то ці адреси можуть бути частиною пулу, використовуваного PAT. Це аналогічно динамічному NAT, за винятком того, що публічних адрес недостатньо для створення взаємно-однозначних відповідностей внутрішніх і зовнішніх

адрес. Невеликий пул адрес спільно використовується великим числом пристроїв.

На рис. 1 показані дії по налаштуванню PAT для використання пулу адрес. Основна відмінність між даною налаштуванням і налаштуванням для динамічного взаємно-однозначного NAT полягає в використанні ключового слова **overload** . Ключове слово **overload** включає PAT.

Шаг 1	Определите пул глобальных адресов, который будет использоваться для преобразования с перегрузкой. `ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}`
Шаг 2	Определите стандартный список контроля доступа, разрешающий адреса, которые должны быть преобразованы. `access-list access-list-number permit source [source-wildcard]`
Шаг 3	Установите преобразование с перегрузкой, указав список контроля доступа и пул, определенные на предыдущих шагах. `ip nat inside source list access-list-number pool name overload`

Шаг 4	Определите внутренний интерфейс.
	
	`interface type number`
	`ip nat inside`

Шаг 5	Определите внешний интерфейс.
	
	`interface type number`
	`ip nat outside`

Рис. 4.3.26

У прикладі настройки, показаному на рис. 2, створюється перетворення з перевантаженням для пулу NAT з ім'ям NAT-POOL2. NAT-POOL2 містить адреси з 209.165.200.226 по 209.165.200.240. Об'єктами перетворення є вузли мережі 192.168.0.0/16. В якості внутрішнього інтерфейсу визначено інтерфейс S0 / 0/0, а в якості зовнішнього інтерфейсу - інтерфейс S0 / 1/0.

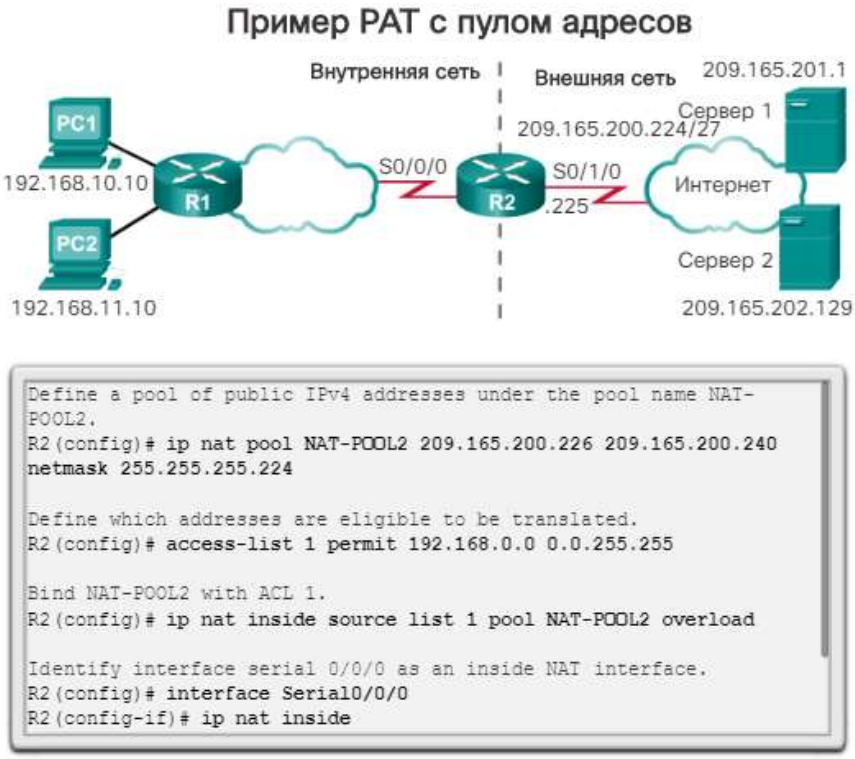


Рис. 4.3.27

Налаштування PAT. Єдина адреса

Налаштування PAT для одного публічного IPv4-адреси

На рис. 1 показана топологія реалізації PAT для перетворення одного публічного IPv4-адреси. У цьому прикладі для всіх вузлів мережі 192.168.0.0/16 (відповідної ACL-списку 1), які відправляють трафік в Інтернет через маршрутизатор R2, буде виконуватися перетворення в IPv4-адрес 209.165.200.225 (IPv4-адрес інтерфейсу S0 / 1/0). Потоки трафіку будуть визначатися номерами портів в таблиці NAT, оскільки було використано ключове слово **overload** .

Таблица NAT

Внутренний глобальный адрес	Внутренний локальный адрес	Внешний локальный адрес	Внешний глобальный адрес
209.165.200.225:1444	192.168.10.10:1444	209.165.201.1:80	209.165.201.1:80
209.165.200.225:1445	192.168.10.11:1444	209.165.202.129:80	209.165.202.129:80

Рис. 4.3.28

На рис. показані кроки, необхідні для налаштування PAT з одним IPv4-адресою. Якщо доступний тільки один публічний IPv4-адрес, для настройки з

перевантаженням зазвичай призначається публічний адресу зовнішнього інтерфейсу, що підключається до інтернет-провайдера. Всі внутрішні адреси в пакетах, які виходять із зовнішнього інтерфейсу, перетворюються в один IPv4-адрес.

Шаги настройки PAT

Шаг 1	Определите стандартный список контроля доступа, разрешающий адреса, которые должны быть преобразованы. `access-list access-list-number permit source [source-wildcard]`
Шаг 2	Настройте динамическое преобразование адреса источника, указав список ACL, выходной интерфейс и параметр overload для включения перегрузки. `ip nat inside source list access-list-number interface type number overload`

Шаг 3	Определите внутренний интерфейс.
	
	`interface type number`
	`ip nat inside`

Шаг 4	Определите внешний интерфейс. `interface type number`

Рис. 4.3.29

Крок 1. Визначте ACL, що дозволяє перетворення трафіку.

Крок 2. Налаштуйте перетворення адреси джерела, використовуючи ключові слова **interface** і **overload** . Ключове слово **interface** визначає IPv4-адрес інтерфейсу, який буде використовуватися при перетворенні внутрішніх адрес. Ключове слово **overload** вказує маршрутизатора відстежувати номери портів для кожного запису NAT.

Крок 3. Вкажіть інтерфейси, які є внутрішніми по відношенню до NAT. Це будь-який інтерфейс, підключений до внутрішньої мережі.

Крок 4. Вкажіть інтерфейс, який є зовнішнім по відношенню до NAT. Це повинен бути той же інтерфейс, що зазначений в запису перетворення джерела на кроці 2.

Ця установка аналогічна динамічному NAT, за винятком використання ключового слова **interface** замість пулу адрес для визначення зовнішнього IPv4-адреси. Таким чином, пул NAT не визначається.

Використовуйте засіб перевірки синтаксису на рис. 3, щоб налаштувати PAT на маршрутизаторі R2 з використанням одного адреси.

Рис. 4.3.30

Аналіз PAT

Процес перетворення NAT з перевантаженням є однаковим як при використанні пулу адрес, так і при використанні однієї адреси. Продовжимо попередній приклад PAT з використанням одного публічного IPv4-адреси. Комп'ютера ПК1 потрібне підключення до веб-сервера Сервер 1. Одночасно іншому клієнту, ПК 2, потрібно встановити аналогічний сеанс з веб-сервером Сервер 2. І для ПК 1, і для ПК 2 налаштовані приватні IPv4-адреси, а на маршрутизаторі R2 включено перетворення PAT.

Процес передачі пакетів від комп'ютерів до серверів

1. На рис. 1 показані комп'ютери ПК 1 і ПК 2, відправляють пакети серверів Сервер 1 і Сервер 2 відповідно. ПК 1 використовує IPv4-адрес 192.168.10.10 і порт TCP джерела 1444. ПК 2 використовує IPv4-адрес 192.168.10.11 джерела і, за випадковим збігом, той же порт TCP джерела - 1 444.

Рис. 4.3.31

2. Пакет комп'ютера ПК 1 першим досягає маршрутизатора R2. Використовуючи PAT, R2 змінює IPv4-адрес джерела на 209.165.200.225 (внутрішній глобальний адреса). У таблиці NAT відсутні інші пристрої, що використовують порт тисячі чотириста сорок-чотири, тому PAT зберігає цей же номер порту. Потім пакет пересилається сервера Сервер 1 за адресою 209.165.201.1.

3. Далі на маршрутизатор R2 приходить пакет з ПК 2. Налаштування PAT забезпечує використання для всіх перетворень одного внутрішнього глобального IPv4-адреси - 209.165.200.225. Аналогічно процесу перетворення для ПК 1, PAT змінює IPv4-адрес джерела ПК 2 на внутрішній глобальний адреса 209.165.200.225. Однак в цьому пакеті ПК 2 використовується номер порту джерела, вже міститься в поточному записі PAT, що забезпечує перетворення для ПК 1. PAT збільшує номер порту джерела, поки його значення не виявиться унікальним для даної таблиці. В даному випадку записи порту джерела в таблиці NAT і пакету від ПК 2 призначається номер тисяча чотириста сорок п'ять.

Хоча ПК 1 і ПК 2 використовують однаковий перетворений адреса - внутрішній глобальний адреса 209.165.200.225, і однаковий номер порту джерела - 1444, змінений номер порту для ПК 2 (1445) робить унікальною кожну запис в таблиці NAT. Це стає очевидним при відправці серверами відповідних пакетів клієнтам.

Процес передачі пакетів від серверів до комп'ютерів

4. Як показано на рис. 2, при типовому обміні «клієнт-сервер» сервери Сервер 1 і Сервер 2 відповідають на запити, отримані від комп'ютерів ПК 1 і ПК 2 відповідно. Сервери використовують для зворотного трафіку порт джерела з отриманого пакета в якості порту призначення та адресу джерела - як адресу призначення. Сервери поводяться так, як якщо б вони взаємодіяли з одним вузлом 209.165.200.225, проте це не так.

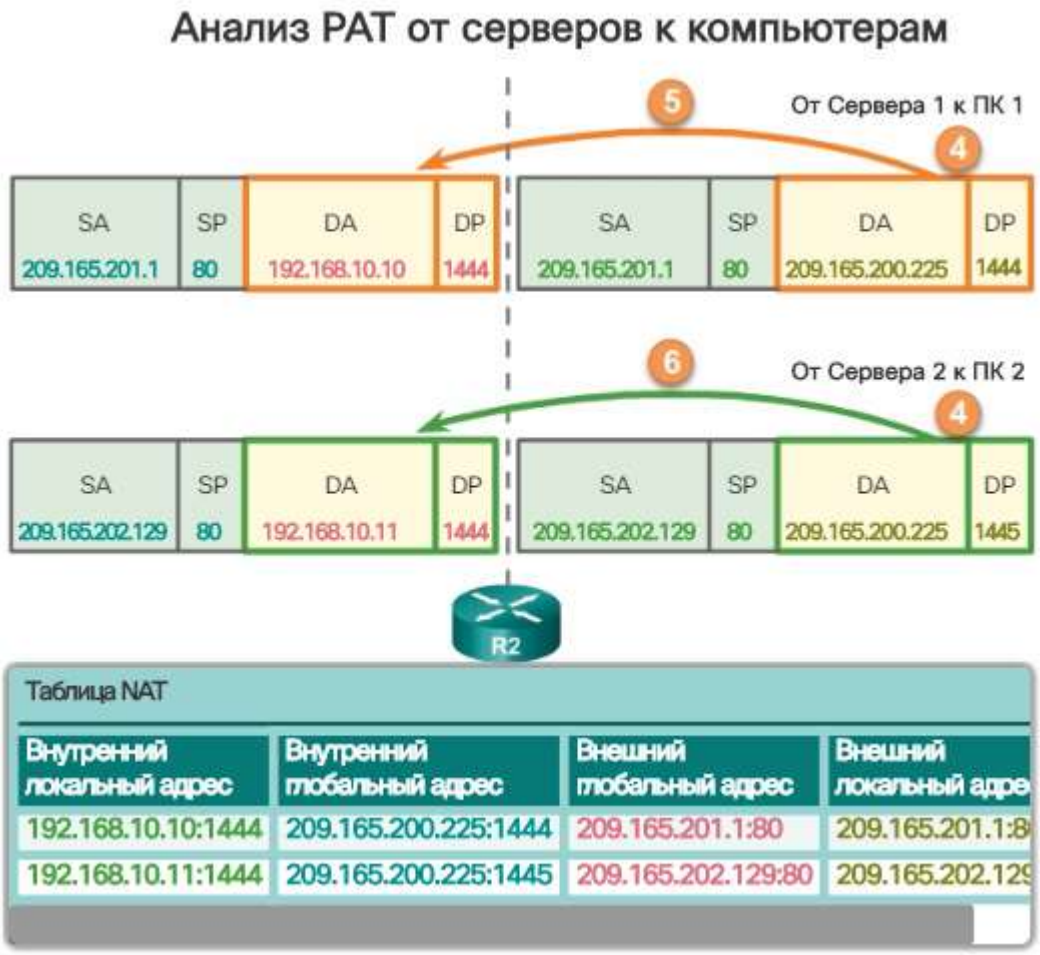


Рис. 4.3.32

5. Отримавши пакети, маршрутизатор R2 знаходить унікальну запис в таблиці NAT, використовуючи адресу призначення і порт призначення кожного пакету. У разі отримання пакета від сервера Сервер 1 адресою призначення IPv4 209.165.200.225 відповідає кілька записів, але тільки одна з них містить порт призначення 1444. Використовуючи цей запис таблиці, маршрутизатор R2 змінює IPv4-адрес призначення пакета на 192.168.10.10. Зміна порту призначення в даному випадку не потрібно. Потім пакет пересилається комп'ютера ПК 1.

6. Отримавши пакет від сервера Сервер 2, маршрутизатор R2 виконує аналогічне перетворення. Маршрутизатор знову знаходить адресу призначення IPv4 209.165.200.225 з декількома записами. Однак, використовуючи порт призначення тисяча чотириста сорок п'ять, R2 може унікально ідентифікувати запис перетворення. IPv4-адрес призначення змінюється на 192.168.10.11. В цьому випадку порт призначення також необхідно змінити назад на початкове значення 1444, збережене в таблиці NAT. Потім пакет пересилається комп'ютера ПК 2.

Перевірка PAT

Маршрутизатор R2 налаштований на надання PAT клієнтам з мережі 192.168.0.0/16. Коли внутрішні вузли виходять через маршрутизатор R2 в Інтернет, виконується перетворення їх адрес в IPv4-адрес з пулу PAT з унікальним номером порту джерела.

Для перевірки PAT використовуються ті ж команди, що й для перевірки статичного і динамічного NAT, як показано на рис. 1. Команда **show ip nat**

translations виводить перетворення для трафіку від двох різних вузлів до різних веб-серверів. Зверніть увагу, що двом різним внутрішніх вузлів виділяється один і той же IPv4-адрес 209.165.200.226 (внутрішній глобальний адреса). Для розрізнення цих двох транзакцій в таблиці NAT використовуються номери портів джерел.

Проверка преобразования PAT

```
R2# show ip nat translations
Pro Inside global          Inside local         Outside local       Outside
tcp 209.165.200.226:51839  192.168.10.10:51839  209.165.201.1:80    209.165.
tcp 209.165.200.226:42558  192.168.11.10:42558  209.165.202.129:80  209.165.
R2#
```

Рис. 4.3.33

Як показано на рис. 2, команда **show ip nat statistics** дозволяє перевірити, що в пулі NAT-POOL2 виділений один адреса для обох перетворень. У вихідних даних команди містяться відомості про кількість і тип активних перетворень, параметрах настройки NAT, кількість адрес в пулі і кількості виділених адрес.

Проверка статистики PAT

```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:00:05 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 4  Misses: 0
CEF Translated packets: 4, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool NAT-POOL2 refcount 2
 pool NAT-POOL2: netmask 255.255.255.224
     start 209.165.200.226 end 209.165.200.240
     type generic, total addresses 15, allocated 1 (6%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```

Рис. 4.3.34

Перенаправлення портів

Перенаправлення портів - це перенаправлення трафіку, адресованого певному порту, від одного вузла мережі на інший вузол. Даний метод дозволяє

зовнішнім користувачам зовні досягати порту для приватного IPv4-адреси (в локальній мережі), використовуючи маршрутизатор з підтримкою NAT.

Як правило, для роботи пірінгових програм обміну файлами і виконання таких операцій, як робота веб-сервера або вихідний FTP, потрібно, щоб порти маршрутизатора були перенаправлені або відкриті, як показано на рис. 1.

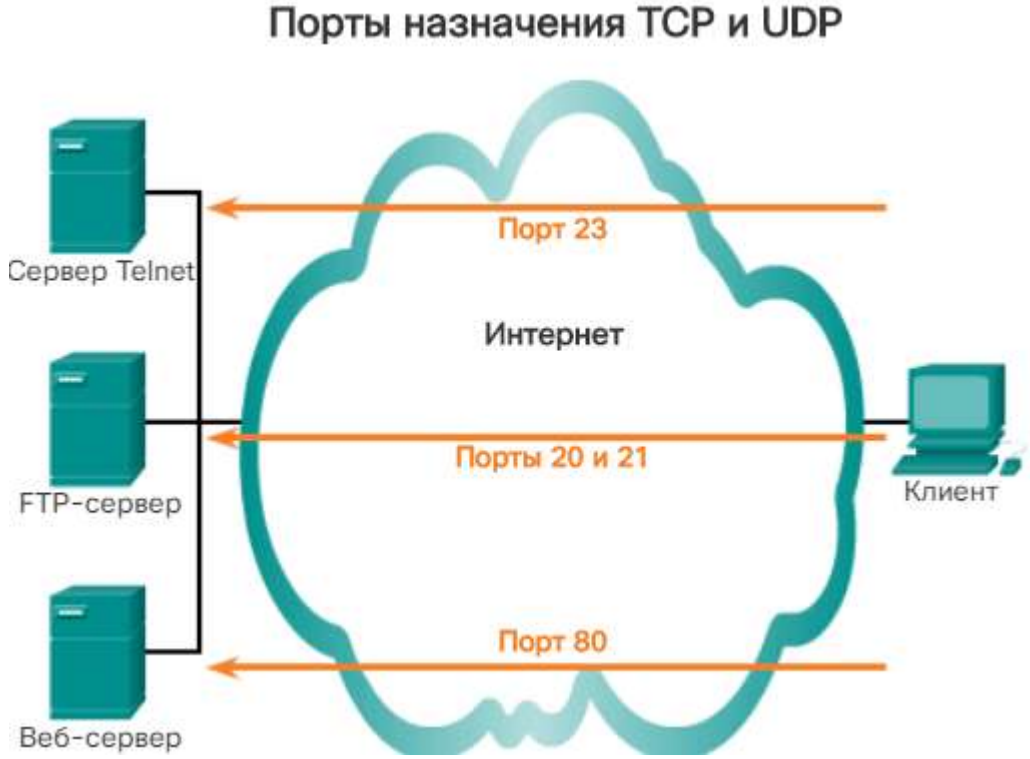


Рис. 4.3.35

Оскільки NAT приховує внутрішні адреси, пірингові програми працюють тільки зсередини - в цьому випадку NAT може зіставити вихідні запити і входять відповіді.

Проблема полягає в тому, що NAT не дозволяє ініціювати запити зовні. Цю ситуацію можна вирішити за допомогою змін, внесених вручну. Можна налаштувати перенаправлення портів, щоб визначити конкретні порти, які можуть бути переадресовані на внутрішні вузли.

Пам'ятайте, що програмні додатки для Інтернету працюють з одними портами, які повинні бути відкриті або доступні цих програм. Різні програми використовують різні порти. Це дозволяє додаткам і маршрутизаторів визначати мережеві сервіси. Наприклад, HTTP працює через загальновідомий порт 80. Коли хтось вводить адресу **http://cisco.com** , в веб-браузері відображається веб-сайт Cisco Systems, Inc. Зверніть увагу, що користувачеві не потрібно вказувати номер порту HTTP для запиту сторінки, оскільки додаток передбачає, що буде використовуватися порт 80.

Якщо необхідна інша номер порту, його можна додати до URL-адресою, відокремивши двокрапкою (:). Наприклад, якщо веб-сервер прослуховує порт 8080, користувач повинен ввести **http://www.example.com:8080** .

Перенаправлення портів дозволяє користувачам досягати внутрішніх серверів з Інтернету, використовуючи адресу WAN-маршрутизатора і відповідний номер зовнішнього порту. Внутрішні сервери зазвичай налаштовуються з використанням приватних IPv4-адрес, відповідних RFC 1918. Коли запит відправляється по IPv4-адресою порту WAN через Інтернет,

маршрутизатор переадресує запит відповідного серверу в локальній мережі. З міркувань безпеки широкосмугові маршрутизатори за замовчуванням не дозволяють перенаправлення зовнішніх веб-запитів вузлів внутрішньої мережі.

Рис. 4.3.36

На рис. 2 зображений власник невеликого підприємства, що використовує сервер PoS (пункт продажу) для відстеження продажів і запасів на складі. Сервер доступний всередині складу, але оскільки йому призначений приватну адресу IPv4, публічний доступ до цього сервера з Інтернету неможливий. Включення на локальному маршрутизаторе перенаправлення портів надає власнику доступ до сервера пункту продажів з Інтернету. Перенаправлення портів на маршрутизаторі налаштовується за допомогою номера порту призначення і приватного IPv4-адреси сервера пункту продажів. Для доступу до сервера клієнтське ПЗ повинно використовувати публічний IPv4-адрес маршрутизатора і порту призначення сервера.

Приклад маршрутизатора бездротового зв'язку

На малюнку показано вікно настройки перенаправлення на один порт для маршрутизатора бездротового зв'язку Packet Tracer. За замовчуванням перенаправлення портів на маршрутизаторі не включене.

Перенаправлення портів для додатків можна включити, вказавши внутрішній локальний адресу, на який повинні перенаправлятися запити. На малюнку запити до служби HTTP, що надходять на маршрутизатор бездротового зв'язку, перенаправляються на веб-сервер з внутрішнім локальним адресою 192.168.1.254. Якщо зовнішній WAN IPv4-адрес маршрутизатора бездротового зв'язку - 209.165.200.225, то зовнішній користувач може ввести **http://www.example.com** , і цей маршрутизатор перенаправить запит HTTP внутрішньому веб-сервера по IPv4-адресою 192.168.1.254, використовуючи номер порту за замовчуванням - 80.

Можна також вказати номер порту, що відрізняється від номера порту за замовчуванням, відповідного 80. Однак зовнішній користувач повинен знати конкретний використовуваний номер порту. Щоб визначити інший порт,

необхідно змінити значення зовнішнього порту (External Port) у вікні перенаправлення на один порт (Single Port Forwarding).

Підхід при налаштуванні перенаправлення портів залежить від виробника і моделі широкосмугового маршрутизатора в мережі. Однак деякі дії є спільними для всіх моделей. Якщо в інструкціях, наданих інтернет-провайдером, або в інструкціях, які додаються до маршрутизатора, немає чітких вказівок, перейдіть на веб-сайт http://www.portforward.com, де можна знайти керівництва для деяких широкосмугових маршрутизаторів. Дотримуйтесь інструкцій, щоб при необхідності додати або видалити порти відповідно до потреб будь-яких додатків, які потрібно вирішити або відхилити.

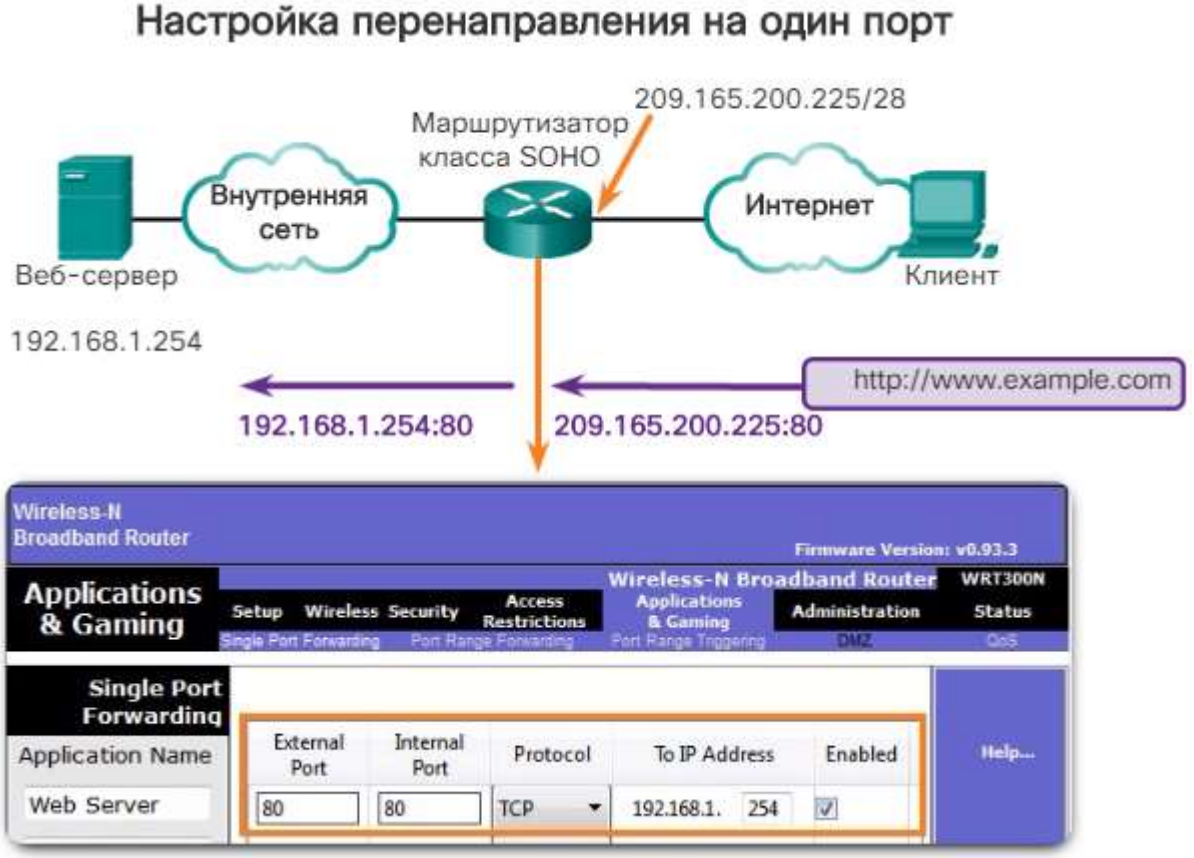


Рис. 4.3.37

Налаштування перенаправлення портів за допомогою IOS

Реалізація перенаправлення портів за допомогою команд IOS аналогічна застосування команд настройки статичного NAT. Перенаправлення портів фактично є статичним перетворенням NAT із зазначеним номером порту TCP або UDP.

На рис. показана команда статичного NAT, використовувана для настройки перенаправлення портів за допомогою IOS.

Перенаправление порта с помощью IOS

```
ip nat inside source {static {tcp | udp local-ip local-port
global-ip global-port} [extendable]
```

Параметр	Описание
`tcp` или `udp`	Указывает номер порта TCP или UDP.
`local-ip`	Это IPv4-адрес, назначенный узлу внутренней сети, обычно из пространства частных адресов в соответствии с RFC 1918.
`local-port`	Установка локального порта TCP/UDP в диапазоне от 1 до 65535. Это номер порта, к которому сервер ожидает подключения.
`global-ip`	Это глобальный уникальный IPv4-адрес внутреннего узла. Это IP-адрес, который будут использовать внешние клиенты для подключения ко внутреннему серверу.
`global-port`	Установка глобального порта TCP/UDP в диапазоне от 1 до 65535. Это номер порта, который будут использовать внешние клиенты для подключения ко внутреннему серверу.
`extendable`	Функция `extendable` применяется автоматически. С помощью ключевого слова `extendable` пользователь может настроить

Рис. 4.3.38

На рис. 2 наведено приклад налаштування перенаправлення портів за допомогою команд IOS на маршрутизаторі R2. 192.168.10.254 - це внутрішній локальний IPv4-адрес веб-сервера, що прослуховує порт 80. Користувачі отримають доступ до цього внутрішнього веб-сервера за допомогою глобального IPv4-адреси 209.165.200.225, який є глобальним унікальним загальнодоступним IPv4-адресою. В даному випадку це адреса інтерфейсу Serial 0/1/0 маршрутизатора R2. В якості глобального порту налаштований порт 8080. Він буде портом призначення, що використовуються разом з глобальним IPv4-адресою 209.165.200.225 для доступу до внутрішнього веб-сервера. У налаштуванні NAT зверніть увагу на наступні параметри команди:

local-ip = 192.168.10.254
local-port = 80
global-ip = 209.165.200.225
global-port = 8080

Рис. 4.3.39

Якщо не використовується стандартний номер порту, клієнт повинен вказати номер порту в додатку.

Як і для інших типів NAT, для перенаправлення портів необхідно налаштувати як внутрішній, так і зовнішній інтерфейси NAT.

Аналогічно статичному NAT, для перевірки перенаправлення портів можна використовувати команду **show ip nat translations** , як показано на рис. 3.

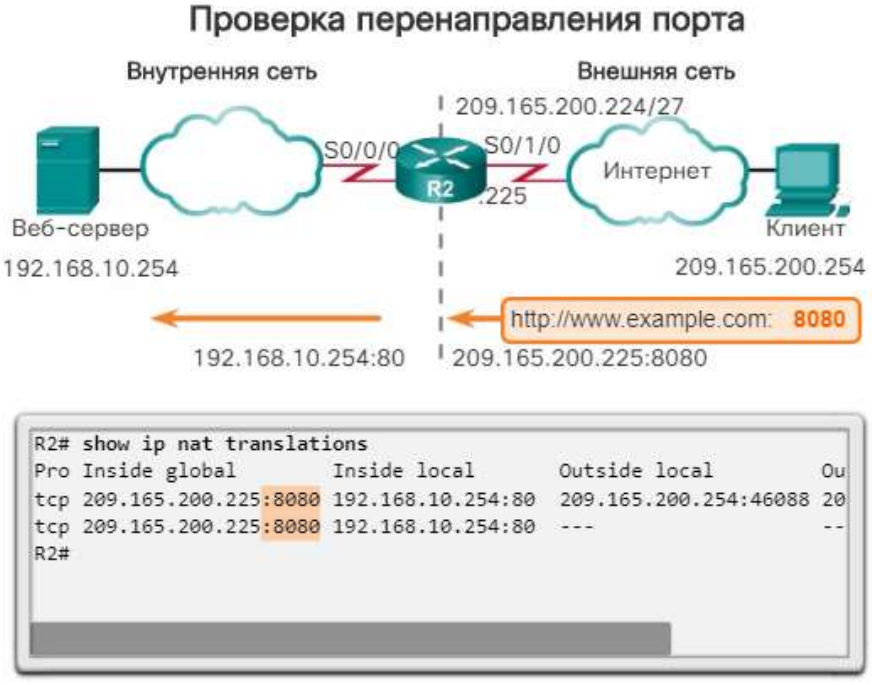


Рис. 4.3.40

У розглянутому прикладі, коли маршрутизатор отримує пакет з внутрішнім глобальним IPv4-адресою 209.165.200.225 і TCP-портом призначення 8080, він виконує пошук в таблиці NAT, використовуючи в якості ключа IPv4-адрес призначення і порт призначення. Потім маршрутизатор перетворює адресу у внутрішній локальний адресу вузла 192.168.10.254 і порт призначення 80. Потім R2 пересилає пакет веб-сервера. Для зворотних пакетів, що йдуть від веб-сервера до клієнта, цей процес інвертується.

NAT для IPv6?

З початку 90-х рр. минулого століття пріоритетним завданням для IETF стало рішення проблеми вичерпання адресного простору IPv4. Поєднання приватних IPv4-адрес RFC 1918 і NAT стало засобом уповільнення процесу вичерпання. NAT володіє помітними недоліками, і в січні 2011 р Адміністрація адресного простору Інтернет (IANA) виділила для регіональних реєстраторів Інтернету свої останні IPv4-адреси.

Одним з «ненавмисних» переваг NAT для IPv4 стало те, що ця технологія приховує приватні мережі від публічного Інтернету. Перевагою NAT є забезпечення уявній безпеки шляхом заборони комп'ютерів з публічного Інтернету доступу до внутрішніх вузлів. Але цю технологію можна вважати заміною повноцінної мережевої безпеки, наприклад, забезпечується фаєрволом.

Комісія з архітектури Інтернету (IAB) включила в RFC 5902 таке положення, що стосується перетворення IPv6:

«Зазвичай вважається, що пристрій NAT забезпечує один рівень захисту, оскільки зовнішні вузли не можуть безпосередньо почати взаємодію з вузлами, що перебувають за пристроєм NAT. Але не слід плутати пристрої NAT з міжмережевими екранами. Як зазначено в розділі 2.2 RFC4864, саме по собі перетворення не забезпечує безпеку. Функція фільтрації з відстеженням стану (stateful filtering) забезпечує той же рівень захисту, не вимагаючи функції перетворення ».

Протокол IPv6 з 128-бітовим адресою надає 340 ундецілліонов адрес. Таким чином, адресний простір не є проблемою. Протокол IPv6 був розроблений, щоб усунути необхідність в NAT для IPv4 з його перетворенням між публічними і приватними IPv4-адресами. Проте, IPv6 дійсно реалізує певну форму NAT. IPv6 включає і власний простір приватних IPv6-адрес, і перетворення NAT, реалізовані інакше, ніж для IPv4.

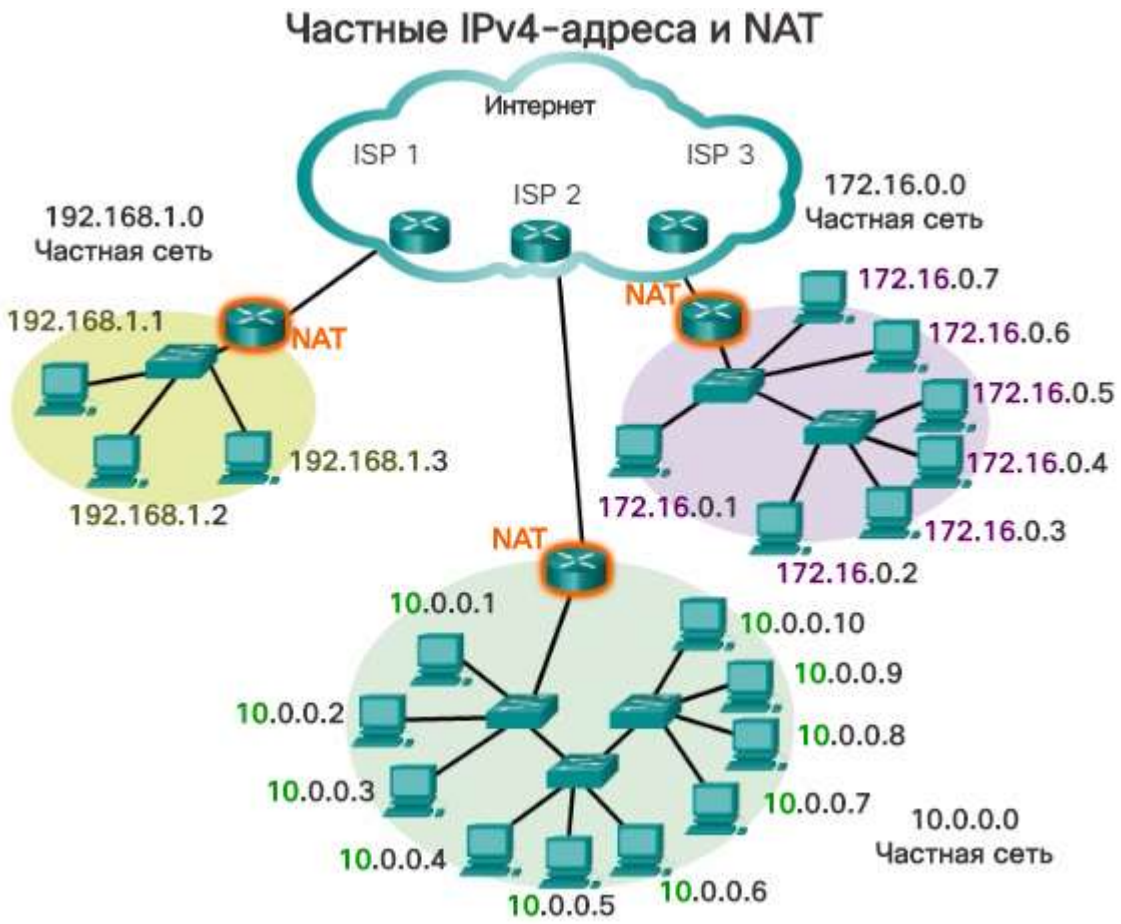


Рис. 4.3.41

Унікальні локальні IPv6-адреси

Унікальні локальні IPv6-адреси (unique local addresses, ULA) схожі на приватні адреси RFC 1918 IPv4, але при цьому істотно відрізняються від них. Мета унікальних локальних адрес - забезпечити простір IPv6-адрес для взаємодії в межах локального об'єкта. Це не означає ні надання додаткового простору IPv6-адрес, ні забезпечення рівня безпеки.

Як показано на малюнку, унікальних локальних адреса використовує префікс FC00 :: / 7, і тому перша 16-бітова група знаходиться в діапазоні від FC00 до FDFF. Якщо префікс призначається локально, наступний один біт встановлений рівним 1. Можливість використання значення 0 може бути визначена пізніше. Наступні 40 бітів - це глобальний ідентифікатор, за яким слід 16-бітовий ідентифікатор підмережі. Ці перші 64 біта об'єднуються для створення префікса унікального локального адреси. Це залишає 64 біта для ідентифікатора інтерфейсу або, згідно з термінологією IPv4 - вузловий частини адреси.

Унікальні локальні адреси визначені в RFC 4193. Унікальні локальні адреси також називаються локальними IPv6-адресами (не слід плутати з IPv6-адресами типу link-local) і мають ряд характеристик, в тому числі перерахованими нижче:

Можливість об'єднувати або приватно з'єднувати вузли без будь-яких конфліктів адрес або необхідності в перенумерації інтерфейсів, які використовують ці префікси.

Незалежність від інтернет-провайдера і можливість застосування з метою взаємодії всередині майданчика без підключення до Інтернету.

Неможливість маршрутизації через Інтернет, і навіть при випадковій «витоку» такого адреси через маршрутизації або DNS конфлікт з іншими адресами відсутня.

Унікальні локальні адреси не настільки прості, як адреси RFC 1918. На відміну від приватних IPv4-адрес, IETF не прагнула використати різновид NAT для перетворення між унікальними локальними адресами і глобальними індивідуальними адресами IPv6.

Реалізація та потенційні сфери застосування унікальних локальних IPv6-адрес все ще вивчається інтернет-спільнотою. Наприклад, організація IETF розглядає можливість використання 40-розрядної глобального ідентифікатора, який призначається централізовано при використанні префікса унікального локального адреси FC00 :: / 8. 40-розрядний глобальний ідентифікатор генерується випадковим чином або можна задати вручну при використанні префікса унікального локального адреси FD00 :: / 8. Інші адреси залишаються незмінні. Ми все ще використовуємо 16 бітів для ідентифікатора підмережі і 64 біта для ідентифікатора інтерфейсу.

Примітка . У вихідній специфікації IPv6 було виділено адресний простір для site-local адрес (з областю видимості в рамках одного майданчика), визначених у RFC 3513. IETF визнала в RFC 3879 site-local адреси застарілими, оскільки термін «майданчик» (site) був визнаний неоднозначним . Для адрес типу site-local використовувався діапазон префіксів FEC0 :: / 10, їх як і раніше можна знайти в ряді застарілих документів IPv6.

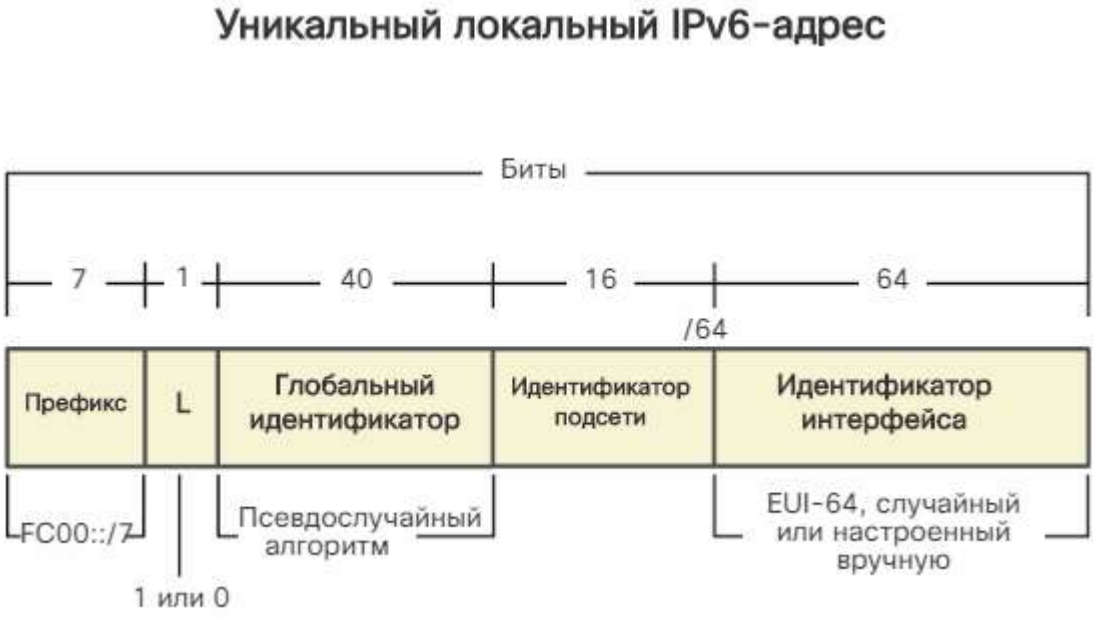


Рис. 4.3.42

Протокол NAT для IPv6

NAT для IPv6 використовується в зовсім іншому контексті, ніж NAT для IPv4. Різноманітні варіанти NAT для IPv6 використовуються з метою надання прозорого доступу між мережами, в яких використовується тільки протокол IPv6, і мережами, в яких використовується тільки протокол IPv4. NAT для IPv6 не застосовується для перетворення приватних IPv6-адрес в глобальні IPv6-адреси.

В ідеалі, IPv6 повинен по можливості використовуватися в чистому вигляді. Тобто коли пристрої IPv6 взаємодіють один з одним по мережах IPv6. Організація IETF розробила кілька методів переходу для різних сценаріїв переходу від IPv4 до IPv6, включаючи використання подвійного стека, тунелювання і трансляцію адрес.

Подвійний стек застосовується, коли пристрої запускають набір протоколів і для IPv4, і для IPv6. Тунелювання для IPv6 - це процес інкапсуляції пакетів IPv6 в пакети IPv4. Даний метод дозволяє передавати пакет IPv6 по мережі, в якій використовується тільки протокол IPv4.

NAT для IPv6 слід використовувати не як довгострокову стратегію, а лише як тимчасовий механізм, що допомагає перейти з IPv4 на IPv6. Згодом з'явилося кілька типів NAT для IPv6, включаючи NAT-PT (Network Address Translation-Protocol Translation, перетворення мережевих адрес - перетворення протоколів). Організація IETF визнала технологію NAT-PT застарілої і порекомендувала використовувати її заміну - NAT64. NAT64 не розглядається в рамках цієї навчального курсу.

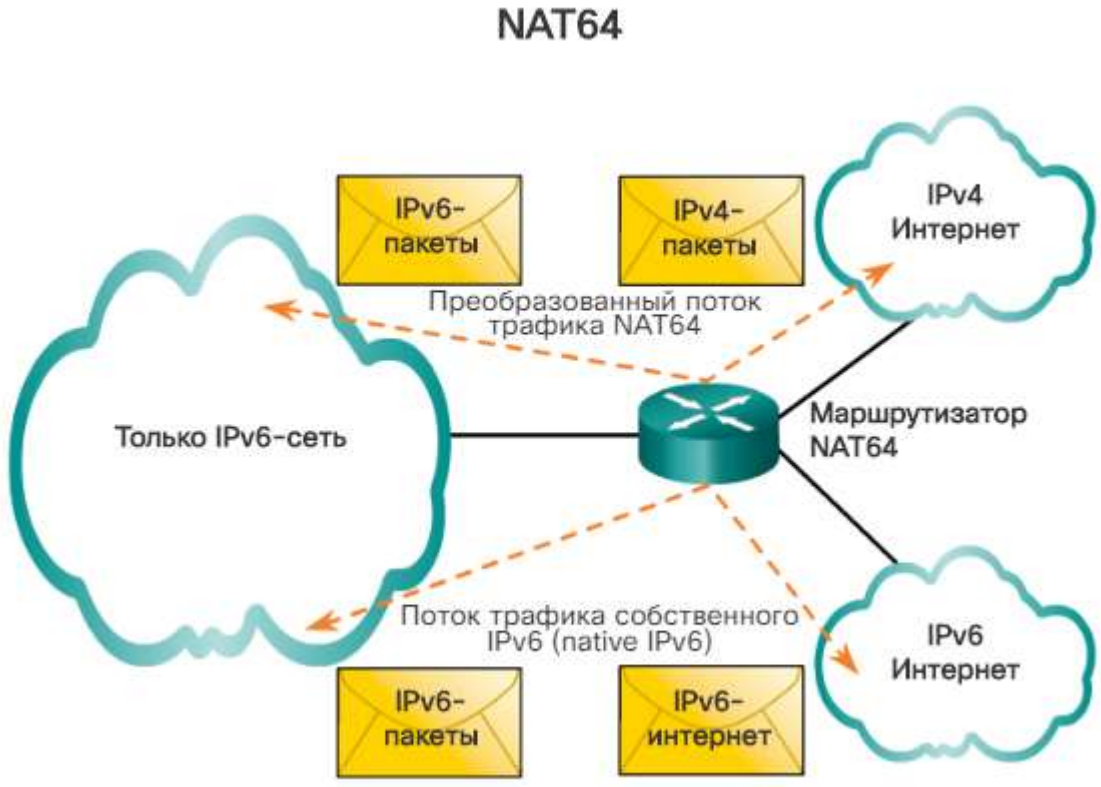


Рис. 4.3.43

Команди "show ip nat"

На рис. 1 показаний маршрутизатор R2 ввімкнені PAT, який використовує діапазон адрес від 209.165.200.226 до 209.165.200.240.

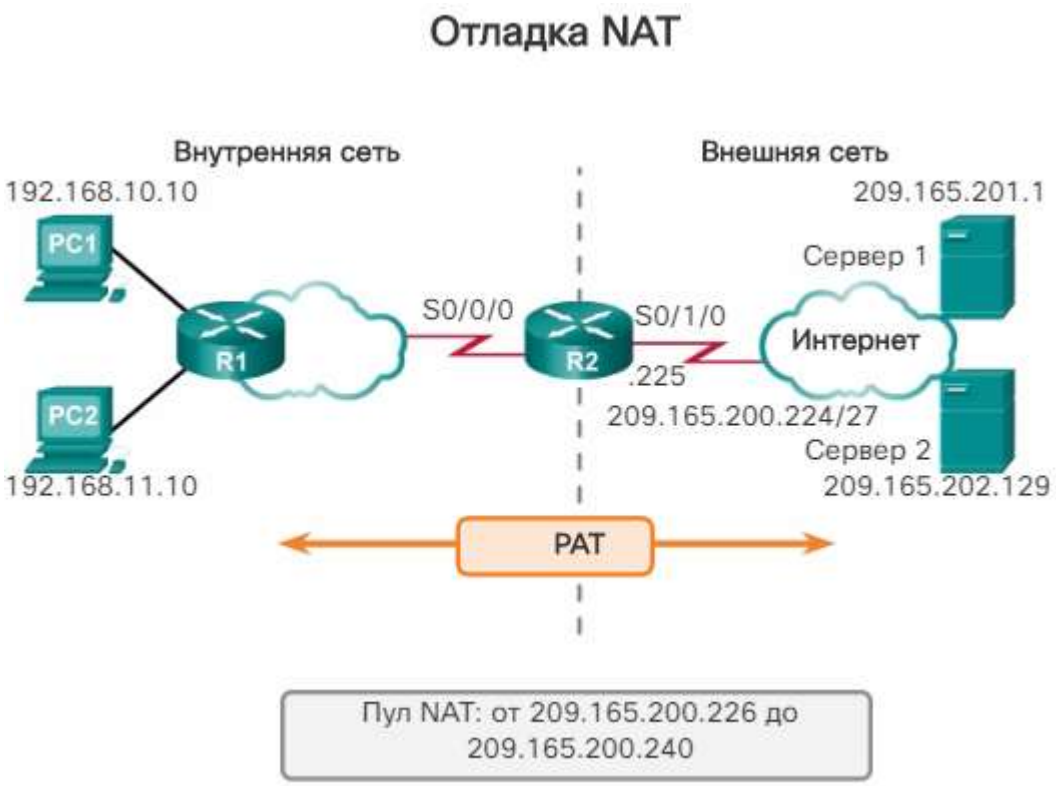


Рис. 4.3.44

Якщо в середовищі NAT виникають проблеми підключення IPv4, пошук причин неполадок часто виявляється складним завданням. Перша дія при усуненні проблеми - виключити NAT як причину. Виконайте наступні дії, щоб переконатися, що NAT працює належним чином.

Крок 1. Залежно від конфігурації чітко визначте цілі і завдання NAT. На даному етапі можна виявити проблему з налаштуванням.

Крок 2. За допомогою команди **show ip nat translations** переконайтеся, що таблиця перетворень містить правильні перетворення.

Крок 3. Використовуйте команди **clear** і **debug**, щоб переконатися, що NAT працює належним чином. Перевірте, чи створюються динамічні записи знову після їх видалення.

Крок 4. Детально вивчіть, що відбувається з перетвореним пакетом, і переконайтеся, що маршрутизатори використовують правильні дані маршрутизації для передачі пакета.

На рис. 2 показані результати виконання команд **show ip nat statistics** і **show ip nat translations** . Перед використанням команд **show** статистика і записи NAT в таблиці NAT видаляються за допомогою команд **clear ip nat statistics** і **clear ip nat translation *** . Після того, як вузол 192.168.10.10 звернеться до сервера в 209.165.201.1 по протоколу telnet, будуть відображені статистика NAT і таблиця NAT, які також допомагають переконатися в коректній роботі NAT.

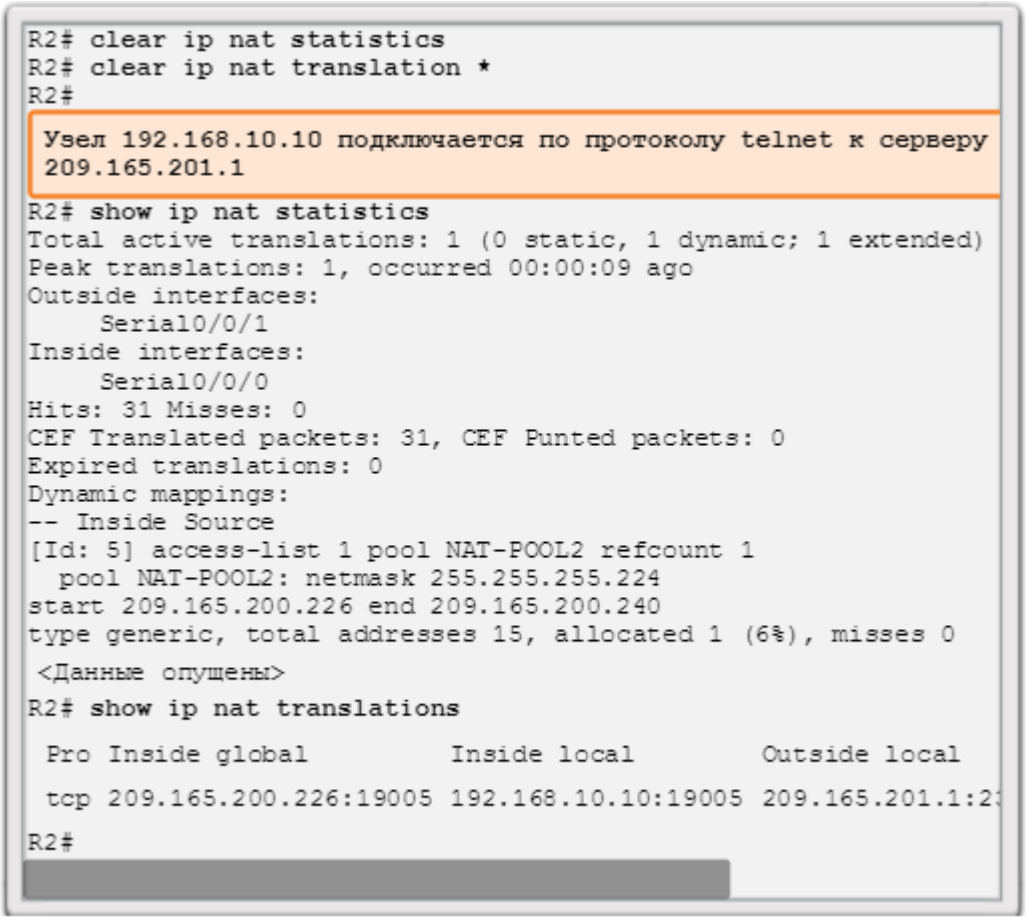


Рис. 4.3.45

У простій мережі може бути доцільно відслідковувати статистику NAT за допомогою команди **show ip nat statistics** . За допомогою команди **show ip nat statistics** відображаються відомості про загальну кількість активних перетворень, параметрах настройки NAT, кількість адрес в пулі і кількості виділених адрес. Однак в більш складному середовищі NAT, в разі кількох перетворень, ця команда не дозволяє чітко визначити проблему. У подібних випадках може знадобитися виконати команду **debug** на маршрутизаторі.

Команда "debug ip nat"

Використовуйте команду **debug ip nat** для перевірки роботи NAT шляхом виведення відомостей про кожному пакеті, перетвореному маршрутизатором. Команда **debug ip nat detailed** виводить опис кожного пакета, що розглядається в якості кандидата на перетворення. Крім того, ця команда виводить відомості про конкретні помилки і винятки, таких як неможливість виділити глобальний адресу. Команда **debug ip nat detailed** видає більше службових даних, ніж команда **debug ip nat** , але вона може надати докладні відомості, які можуть бути необхідні для налагодження NAT. Усунувши неполадки, завжди відключайте режим налагодження.

На рис. 1 показаний результат виконання **debug ip nat** . Результат показує, що внутрішній вузол (192.168.10.10) створив трафік до зовнішнього вузла (209.165.201.1), і адреса джерела був перетворений на адресу 209.165.200.226.

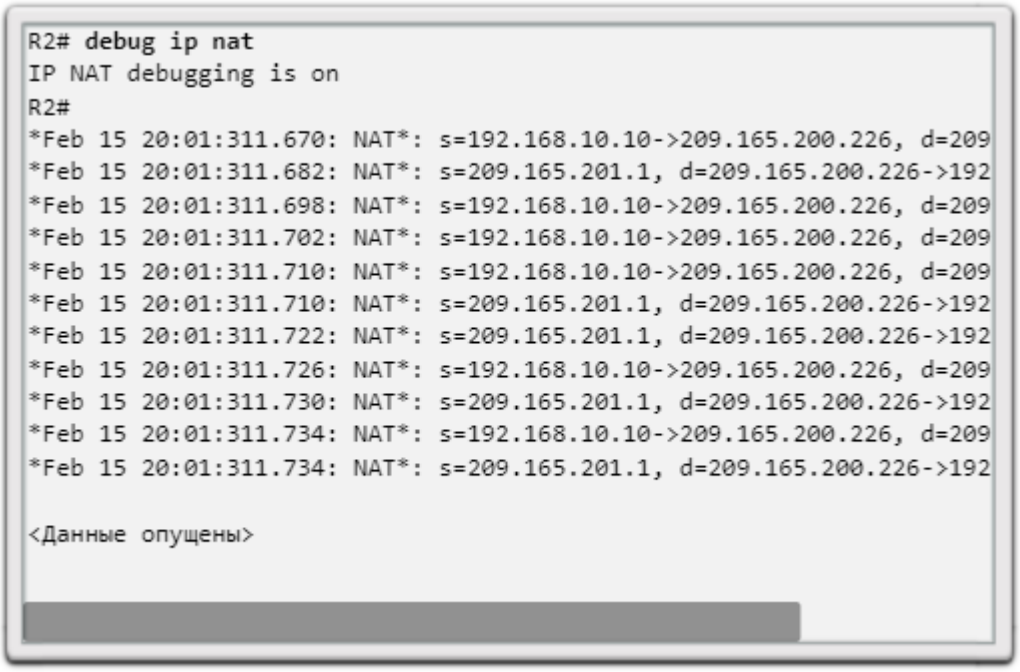


Рис. 4.3.46

При розшифруванні результатів налагодження враховуйте значення перерахованих нижче символів:

*** (Зірочка)** - символ зірочки поруч з NAT показує, що перетворення виконується шляхом зі швидкою комутацією. Комутація першого пакету діалогу завжди є програмним процесом і тому виконується повільніше. Решта пакети проходять по шляху з швидкою комутацією якщо існує запис кеша.

s = - цей символ позначає IPv4-адрес джерела.

abcd ---> **wxyz** - це значення показує, що адреса джерела abcd перетворюється в wxyz

d = - цей символ позначає IPv4-адрес призначення.

[xxxx] - значення в дужках є ідентифікаційним номером IPv4. Наведена вище інформація може бути корисна для налагодження, так як вона дозволяє здійснити кореляцію з іншими даними трасування від аналізаторів протоколів.

Примітка. Переконайтеся, що список контролю доступу (ACL), зазначений в команді для настройки NAT, дозволяє всі необхідні мережі. На рис. 2 перетворення дозволяється тільки для адрес 192.168.0.0/16. Маршрутизатор R2 не виконує перетворення для пакетів з внутрішньої мережі, адресованих в Інтернет, якщо адреси їх джерел прямо не дозволені ACL-списком 1.

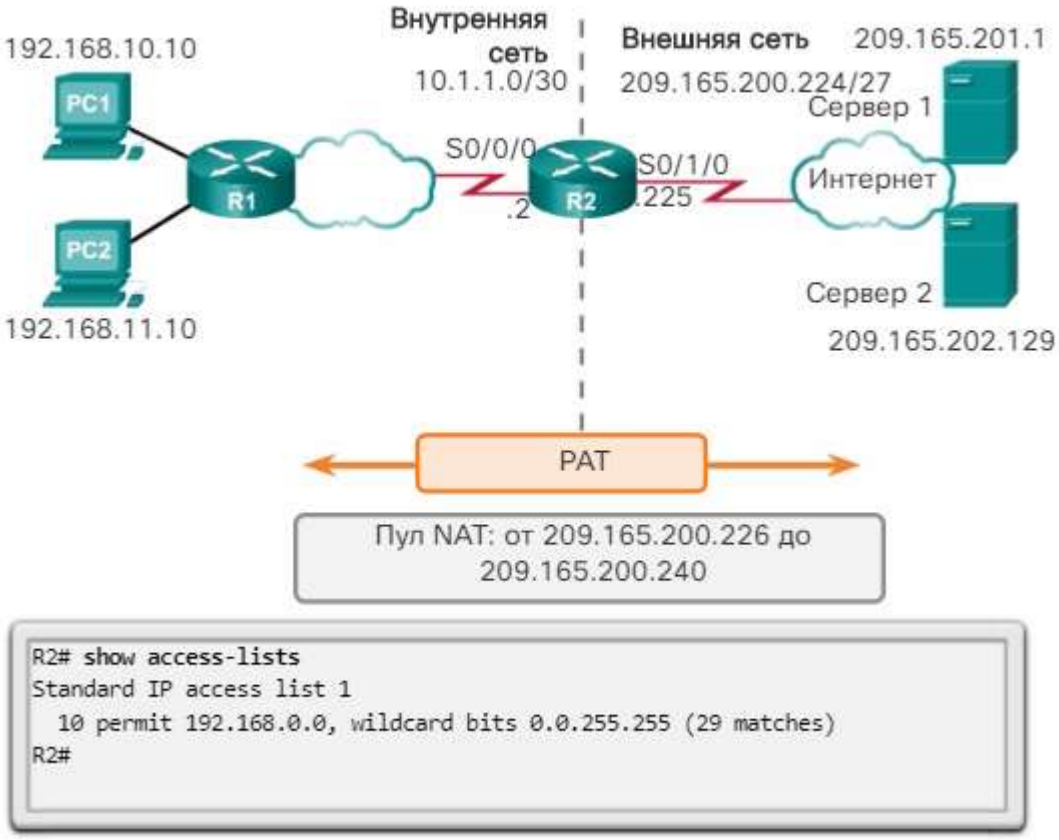


Рис. 4.3.47

Сценарій пошуку та усунення неполадок, пов'язаних з NAT

приклад впровадження

На рис. 1 показано, що вузли локальної мережі 192.168.0.0/16, ПК 1 і ПК 2 не можуть відправляти луна-запити ping до серверів в зовнішніх мережах, Сервер 1 і Сервер 2.

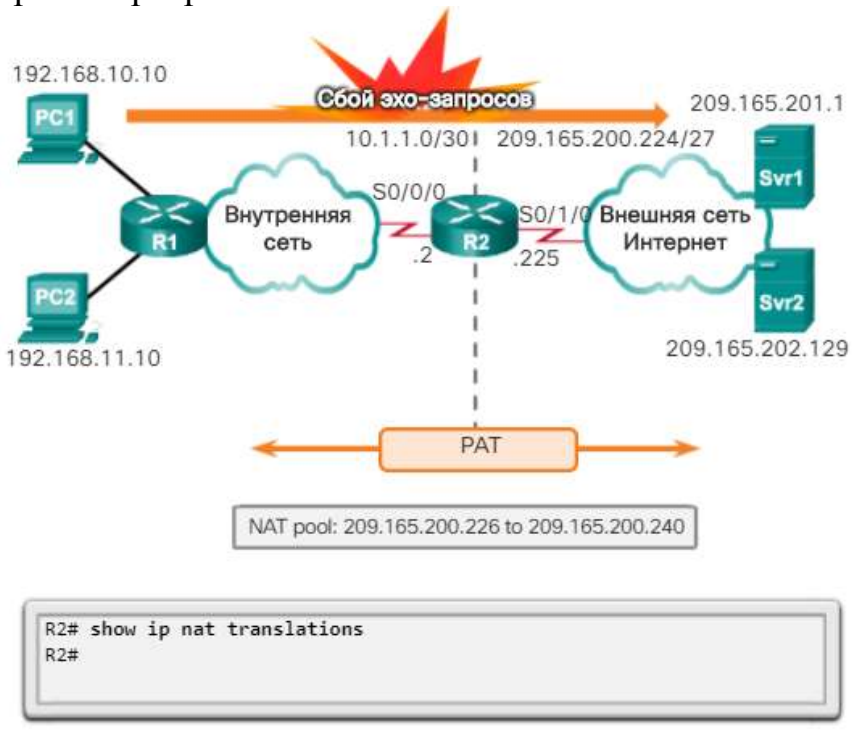


Рис. 4.3.48

Щоб приступити до усунення цієї проблеми, використовуйте команду **show ip nat translations** , що дозволяє визначити, чи містяться в

таблиці NAT записи перетворення. Результат на рис. 1 показує, що перетворення в таблиці відсутні.

Щоб визначити, чи виконувались якісь перетворення, використовується команда **show ip nat statistics** . Дана команда також визначає інтерфейси, між якими має виконуватися перетворення. У вихідних даних, наведених на рис. 2, лічильники NAT рівні 0, що говорить про те, що перетворення не виконувалося. Порівнюючи вихідні дані з топологією на рис. 1, зверніть увагу, що інтерфейси маршрутизатора NAT неправильно визначені як внутрішні і зовнішні щодо NAT. Неправильність налаштування також можна перевірити за допомогою команди **show running-config** .

```
R2# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/0
Inside interfaces:
  Serial0/1/0
Hits: 0  Misses: 0

<Данные опущены>

R2(config)# interface serial 0/0/0
R2(config-if)# no ip nat outside
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config-if)# no ip nat inside
R2(config-if)# ip nat outside
```

Рис. 4.3.49

Перед застосуванням правильного налаштування необхідно видалити поточну настройку інтерфейсів NAT.

Після правильного визначення внутрішніх і зовнішніх інтерфейсів NAT відправка ще одного луна-запиту ping від ПК 1 на Сервер 1 закінчується невдачею. За допомогою команд **show ip nat translations** і **show ip nat statistics** ще раз переконайтеся, що перетворення все ще не виконується.

На рис. 3 використовується команда **show access-lists** , що дозволяє визначити, чи дозволяє ACL-список, що вказується в командах NAT, всі необхідні мережі. Вивчення вихідних даних команди показує, що в ACL, який визначає адреси для перетворення, використана неправильна шаблонна маска. Шаблонна маска дозволяє використання тільки підмережі 192.168.0.0/24. Список контролю доступу потрібно спочатку видалити, а потім налаштувати заново, використовуючи правильну шаблонну маску.

```
R2# show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
R2#

R2(config)# no access-list 1
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Рис. 4.3.50

Після виправлення помилки з ПК 1 на Сервер 1 відправляється ще один луна-запит, і в цей раз запит виконується успішно. Як показано на рис. 4, щоб переконатися у виконанні перетворення NAT, використовуються команди **show ip nat translations** і **show ip nat statistics** .

```
R2# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:37:58 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
 Hits: 20  Misses: 0
CEF Translated packets: 20, CEF Punted packets: 0
Expired translations: 1
Dynamic mappings:
-- Inside Source
[Id: 5] access-list 1 pool NAT-POOL2 refcount 1
 pool NAT-POOL2: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 1 (6%), misses 0

  <Данные опущены>

R2# show ip nat translations
Pro Inside global      Inside local      Outside local     Outside gl
icmp 209.165.200.226:38 192.168.10.10:38 209.165.201.1:38  209.165.20
R2#
```

Рис. 4.3.51

Висновки

Глава 9. NAT для IPv4

У матеріалі даної глави розглядається використання NAT для пом'якшення вичерпання адресного простору IPv4. NAT для IPv4 дозволяє мережевим адміністраторам використовувати простір приватних адрес RFC 1918 року, одночасно надаючи підключення до Інтернету з використанням одного публічного адреси або обмеженого числа публічних адрес.

NAT економить простір публічних адрес і значно скорочує адміністративні витрати при додаванні, переміщенні і зміні адрес. NAT і PAT можуть використовуватися для економії простору загальнодоступних адрес, не впливаючи на підключення до мережі інтернет-провайдера. Однак NAT має певні недоліки - дана технологія негативно впливає на продуктивність,

мобільність пристроїв, а також на можливість наскрізного з'єднання. Тому NAT слід використовувати в якості короткочасного вирішення проблеми вичерпання адрес до впровадження довгострокового рішення, яким є IPv6.

У розділі розглянуто використання перетворення (NAT) для протоколу IPv4, а саме:

- характеристики, термінологія і загальні принципи роботи NAT;
- різні типи NAT, включаючи статичний NAT, динамічний NAT і NAT з перевантаженням;
- переваги і недоліки NAT;
- настройка, перевірка і аналіз статичного NAT, динамічного NAT і NAT з перевантаженням;
- використання перенаправлення портів для доступу до внутрішніх пристроїв з мережі Інтернет;
- чому перетворення NAT є, але не інтегровано в мережах IPv6;
- налагодження NAT за допомогою команд **show** і **debug** .

5. Розділ Введення в масштабовані мережі

5.1 Надлишковість LAN

Надлишковість мережі - ключ до забезпечення надійності мережі. Надлишкові маршрути забезпечуються за рахунок декількох фізичних каналів між пристроями. Таким чином, мережа може продовжувати роботу навіть у разі збою одного каналу або порту. Також по надлишковим каналам можна розподілити навантаження трафіку, що дозволяє збільшити ємність.

Щоб уникнути виникнення петель 2 рівня потрібно керувати кількома маршрутами. Вибираються оптимальні маршрути, і альтернативний маршрут повинен бути негайно доступний в разі збою основного маршруту. Протоколи STP використовуються для управління Надлишковістю 2 рівня.

Надлишкові пристрої, наприклад, багаторівневі комутатори або маршрутизатори, надають клієнтам можливість використання альтернативного шлюзу в разі збою основного шлюзу. Таким чином клієнт зможе використовувати кілька шляхів до декількох можливих шлюзів за замовчуванням. Протоколи забезпечення надмірності на першому хопі (FHRP) використовуються для управління призначенням клієнту шлюзу, а також для надання можливості використання альтернативного шлюзу в разі збою основного шлюзу.

Трирівнева ієрархічна модель мережі, яка використовує рівні ядра, розподілу і доступу з Надлишковістю, покликана усунути єдину точку відмови в мережі. Використання декількох фізично підключених каналів між комутаторами забезпечує фізичну Надлишковість в комутованій мережі. Це підвищує надійність і доступність мережі. Наявність альтернативних фізичних каналів для передачі даних по мережі дозволяє користувачам отримати доступ до мережевих ресурсів навіть у разі збою одного з каналів.

Для багатьох організацій доступність мережі є найважливішим фактором забезпечення відповідності вимогам бізнесу. Таким чином, модель інфраструктури мережі є критично важливим для бізнесу компонентом. Надлишковість маршруту надає рішення, що забезпечує необхідну доступність декількох мережевих служб за рахунок усунення потенційної єдиної точки відмови.

Примітка. Надлишковість на 1 рівні моделі OSI демонструється з використанням декількох каналів і пристроїв, проте для настройки мережі потрібно щось більше, ніж просто фізичне планування. Для систематичної роботи надмірності також необхідно використовувати протоколи 2 рівня OSI (наприклад STP).

Важливою частиною ієрархічної архітектури є Надлишковість, використання якої дозволяє запобігти перебої в обслуговуванні кінцевих користувачів. Для роботи надлишкових мереж потрібні фізичні маршрути, однак і логічна Надлишковість також повинна бути частиною архітектури. Проте, надлишкові маршрути в комутованій мережі Ethernet можуть привести до виникнення фізичних і логічних петель 2 рівня.

Внаслідок роботи комутаторів, особливо в процесі отримання даних і пересилання, можуть виникати логічні петлі 2 рівня. При наявності декількох

шляхів між двома пристроями та відсутності реалізації протоколу spanning-tree виникає петля 2 рівня.

Проблеми з Надлишковістю 1 рівня. Нестабільність бази даних MAC-адрес

На відміну від IP-пакетів, кадри Ethernet не містять атрибут «час життя» (TTL). Як результат, якщо не використовується механізм блокування постійного поширення цих кадрів в комутованій мережі, кадри продовжують поширюватися між комутаторами нескінченно або до тих пір, поки не відбудеться збій каналу, в результаті чого петля буде перервана. Таке постійне поширення між комутаторами може привести до нестабільності бази даних MAC-адрес. Це може статися внаслідок пересилання широкомовних кадрів.

Широкомовні кадри пересилаються з усіх портів комутатора, за винятком вихідного вхідного порту. Це гарантує, що всі пристрої в домені широкомовної розсилки можуть отримати кадр. При наявності декількох шляхів для пересилання кадрів може виникнути нескінченна петля. У разі виникнення петлі таблиця MAC-адрес на комутаторі може постійно змінюватися за рахунок оновлень відширокомовних кадрів, що призводить до нестабільності бази даних MAC-адрес.

Для перегляду анімації натисніть кнопку «Відтворення» на малюнку. Коли анімація зупиниться, прочитайте текст, розташований зліва від схеми топології. Анімація продовжиться після короткої паузи.

1. PC1 відправляє широкомовний кадр на S2. S2 приймає широкомовний кадр на інтерфейс F0 / 11. Коли S2 приймає широкомовний кадр, він оновлює свою таблицю MAC-адрес, щоб зареєструвати доступність PC1 на порте F0 / 11.

2. Оскільки цей кадр - широкомовний, S2 пересилає кадр з усіх портів, включаючи Магістраль 1 і Магістраль 2. Коли широкомовний кадр надходить на S3 і S1, їх таблиці MAC-адрес оновлюються щодо PC1, який доступний на порту F0 / 1 на S1 і на порту F0 / 2 на S3.

3. Оскільки цей кадр є широкомовним, S3 і S1 пересилають кадр з усіх портів, за винятком вихідного вхідного порту. S3 відправляє широкомовний кадр з PC1 на S1. S1 відправляє широкомовний кадр з PC1 на S3. Всі комутатори оновлюють свою таблицю MAC-адрес з урахуванням неправильного порту PC1.

4. Всі комутатори знову пересилають широкомовний кадр з усіх портів, за винятком вхідного порту. Це призводить до того, що обидва комутатора пересилають кадр на S2.

5. Коли S2 отримує широкомовні кадри від S3 і S1, таблиця MAC-адрес знову оновлюється, в цей раз з урахуванням останнього запису, отриманої від двох інших комутаторів.

Цей процес повторюється до тих пір, поки петля не буде перервана шляхом фізичного відключення з'єднань, що викликають її, або відключення живлення одного з комутаторів в петлі. При цьому створюється високе навантаження на ЦП на всіх комутаторах, що беруть участь в петлі. Оскільки між усіма комутаторами в петлі постійно передаються одні і ті ж кадри, ЦП комутатора доводиться обробляти великий обсяг даних. При цьому знижується продуктивність комутатора при надходженні допустимого трафіку.

Вузол, який бере участь в мережевий петлі, недоступний для інших вузлів в мережі. Крім того, внаслідок постійних змін в таблиці MAC-адрес комутатор

не знає, з якого порту слід пересилати кадри одно адресної розсилки. У вищевказаному прикладі для PC1 перераховані неправильні порти. Будь-кадр одноадресної розсилки, призначений для PC1, бере участь в петлі, як і кадри широкомовної розсилки. Через зростаючого числа кадрів, циклічно розповсюджуваних в мережі, поступово створюється широкомовний шторм.

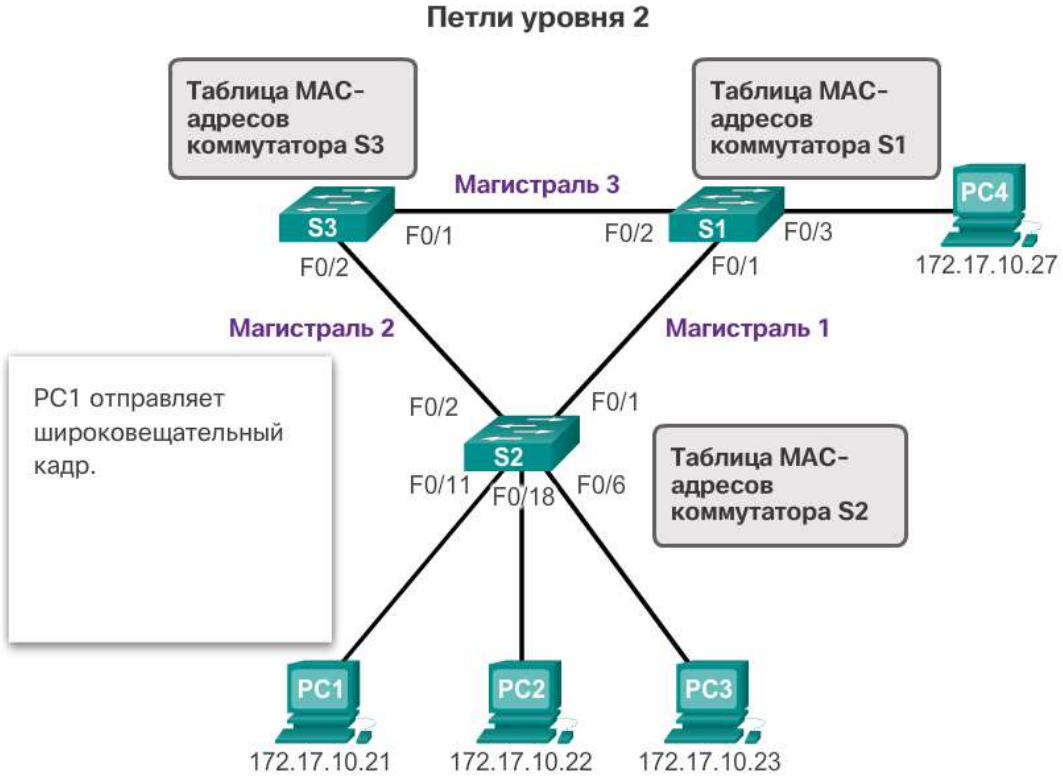


Рис. 5.1.1

Проблеми з Надлишковістю на 1 рівні. широкомовний шторм

Широкомовний шторм виникає в разі, коли в петлю на 2 рівні потрапляє стільки кадрів широкомовної розсилки, що при цьому споживається вся доступна смуга пропускання. Відповідно, для легітимного трафіку немає доступної смуги пропускання, і мережа стає недоступною для обміну даними. Описана ситуація - ефективний відмову в обслуговуванні.

Широкомовний шторм неминучий в мережі, де виникла петля. У міру того, як все більше пристроїв відправляють широкомовні розсилання по мережі, все більше трафіку потрапляє в петлю і споживає ресурси. В кінцевому рахунку це створює широкомовний шторм, що призводить до збоїв в мережі.

Широкомовні шторми також мають і ряд інших наслідків. Оскільки трафік широкомовної розсилки пересилається з усіх портів комутатора, всі підключені пристрої повинні обробляти трафік широкомовної розсилки, лавинна розсилка якого виконується нескінченно по мережі, в якій виникла петля. Через це можуть виникати збої в роботі кінцевого пристрою через високі вимог до обробки з метою підтримки високого навантаження трафіку на мережевому адаптері.

1. PC1 передає кадр широкомовної розсилки в мережу, де виникла петля.

2. Кадр широкомовної розсилки циклічно передається між усіма з'єднаними між собою комутаторами в мережі.

3. PC4 теж відправляє кадр широкомовної розсилки в мережу, де виникла петля.

4. Кадр широкомовної розсилки PC4 також потрапляє в петлю між усіма з'єднаними між собою комутаторами, як і кадр широкомовної розсилки PC1.

5. У міру того, як все більше пристроїв відправляють широкомовні розсилання по мережі, все більше трафіку потрапляє в петлю і споживає ресурси. В кінцевому рахунку це створює широкомовний шторм, що призводить до збоїв в мережі.

6. Коли мережу повністю насичена трафіком широкомовної розсилки, який циклічно передається між комутаторами, новий трафік відкидається комутатором, оскільки він не в змозі його обробити.

Оскільки пристрої, підключені до мережі, регулярно відправляють кадри широкомовної розсилки, наприклад, ARP-запити, широкомовний шторм може виникати за лічені секунди. В результаті при виникненні петлі коммутуючу мережу швидко виходить з ладу.

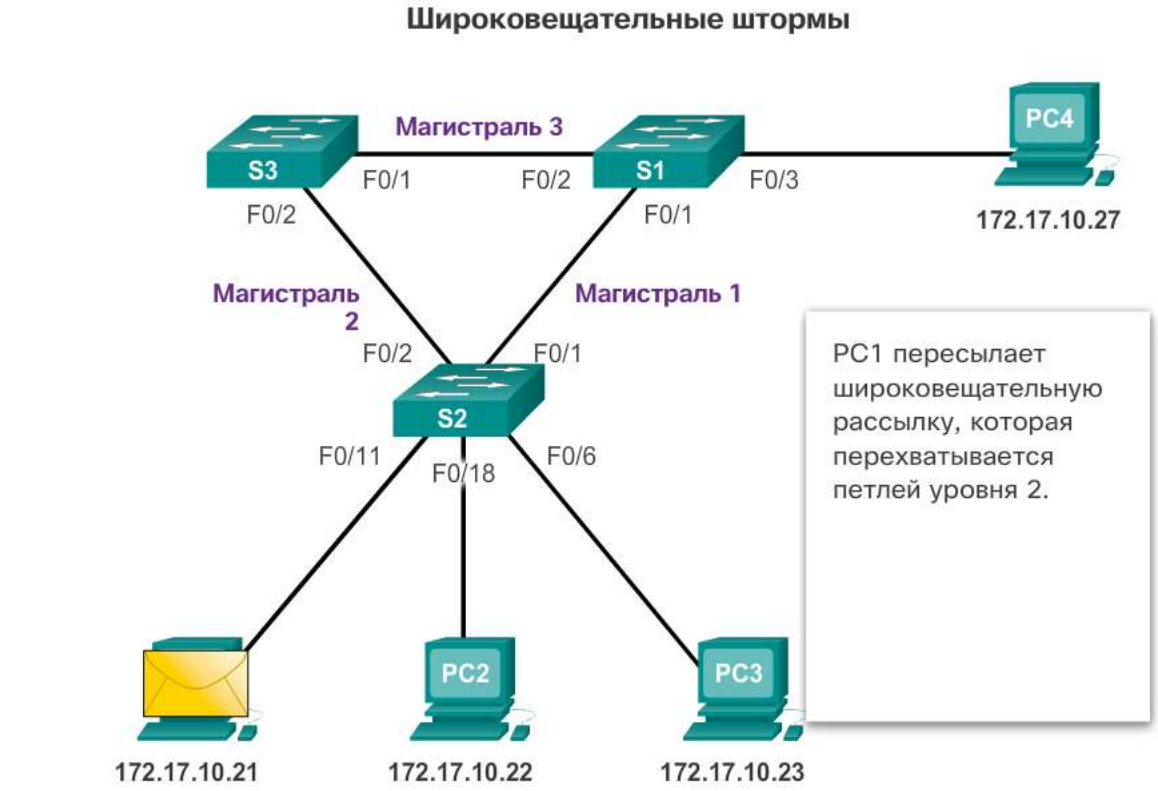


Рис. 5.1.2

Проблеми з Надлишковістю на 1 рівні. Дубльовані одноадресні кадри

Множинна передача кадрів

Кадри широкомовної розсилки є не єдиним типом кадрів, на які впливає виникнення петель. Кадри одноадресної розсилки, відправлені в мережу, де виникла петля, можуть стати причиною дублювання кадрів, що надходять на пристрій призначення.

Натисніть на кнопку «Відтворення» на малюнку, щоб переглянути анімацію з цієї проблеми. Коли анімація зупиниться, прочитайте текст, розташований праворуч від схеми топології. Анімація продовжиться після короткої паузи.

1. PC1 відправляє кадр одно адресної розсилки, призначений для PC4.

2. S2 не містить у своїй таблиці MAC-адрес записи для PC4, тому виконує лавинну розсилку цього кадру з усіх портів комутатора, намагаючись знайти PC4.

3. Кадр надходить на комутатори S1 і S3.

4. S1 містить в таблиці MAC-адрес записи для PC4, тому він відправляє кадр на PC4.

5. S3 також містить в таблиці MAC-адрес запис для PC4, тому відправляє кадр одно адресної розсилки з порту Магістраль 3 на S1.

6. S1 приймає дубльований кадр і відправляє його на PC4

7. Таким чином, PC4 приймає два однакових кадру.

Більшість протоколів верхнього рівня не призначені для розпізнавання або усунення проблеми дубльованої передачі. Як правило, протоколи, що використовують механізм нумерації послідовності, припускають, що стався збій передачі, і номер послідовності переходить в інший сеанс обміну даними. Решта протоколи намагаються передати дубльовані дані відповідного протоколу верхнього рівня для обробки і, можливо, відкидання.

Протоколи LAN 2 рівня, наприклад Ethernet, не підтримують механізми розпізнавання і запобігання нескінченних циклічних кадрів. Деякі протоколи 3 рівня використовують механізми часу життя (TTL), які обмежують кількість спроб повторної передачі пакетів мережевими пристроями 3 рівня. За відсутності такого механізму пристрою 2 рівня будуть виробляти трафік в нескінченному циклі. Механізм запобігання петлі 2 рівня (STP) розроблений як раз для вирішення даних проблем.

Щоб уникнути подібних проблем в мережі з Надлишковістю, на комутаторах повинні бути включені певні типи протоколу spanning-tree. Протокол spanning-tree за замовчуванням включено на комутаторах Cisco, запобігаючи, таким чином, виникнення петель 2 рівня.

Дублирование одноадресных кадров

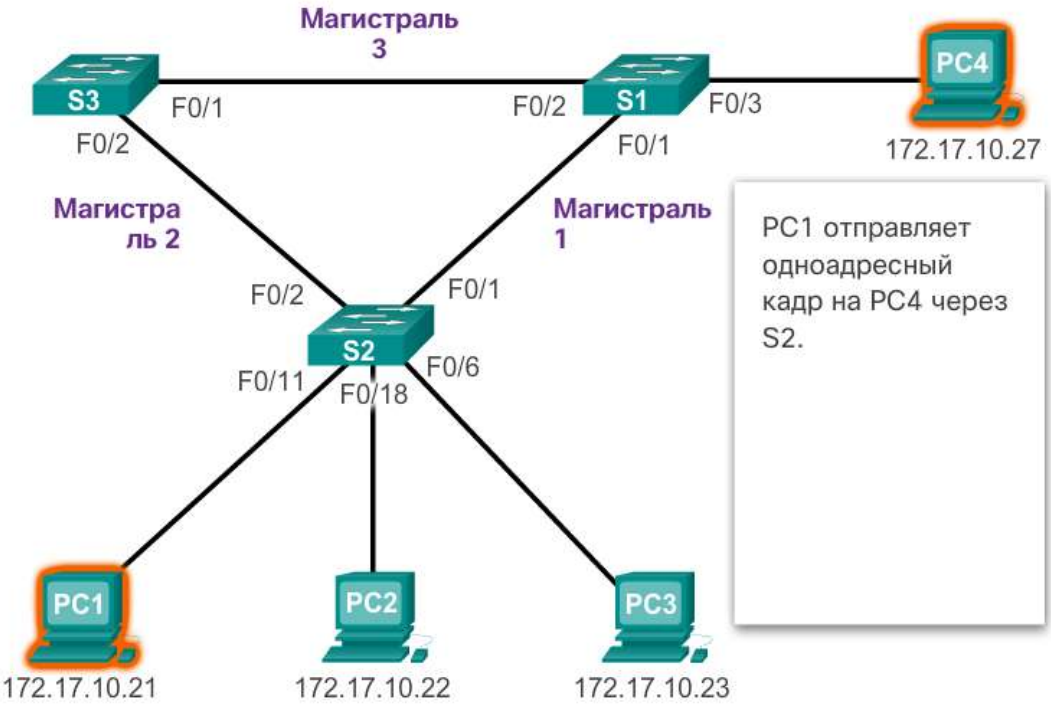


Рис. 5.1.3

Принцип роботи STP

Алгоритм протоколу spanning-tree. Вступ

Надлишковість підвищує доступність топології мережі за допомогою захисту мережі від єдиної точки відмови - наприклад, несправного мережевого кабелю або комутатора. При реалізації в проектуванні фізичної надмірності виникають петлі і дублювання кадрів. Петлі і дубльовані кадри є причиною серйозних неполадок в комутованій мережі. Протокол STP розроблений для вирішення подібних проблем.

Протокол STP забезпечує наявність тільки одного логічного шляху між усіма вузлами призначення в мережі шляхом навмисного блокування резервних шляхів, які могли б викликати петлю. Порт вважається заблокованим, коли заблокована відправка і прийом даних на цей порт. До таких даних не належать кадри BPDU, які використовуються протоколом STP для запобігання петель. Для запобігання петель в мережі надзвичайно важливо блокувати надлишкові шляху. Фізичні шляху як і раніше використовуються для забезпечення надмірності, однак ці шляхи відключені з метою запобігання петель. Якщо все буде готово для компенсації несправності мережевого кабелю або комутатора, протокол STP повторно розраховує шляху і знімає блокування з необхідних портів, щоб дозволити активацію надлишкового шляху.

У розглянутому прикладі протокол STP включений на всіх комутаторах:

1. PC1 відправляє широкомовне розсилання в мережу.

2. S2 налаштований з використанням протоколу STP, і для порту Магістраль 2 задано стан блокування. Стан блокування забороняє використання портів для пересилання даних користувачів, запобігаючи, таким чином, виникнення петлі. S2 пересилає кадр широкомовної розсилки з усіх портів комутатора, за винятком порту джерела PC1 і порту для Магістраль 2.

3. S1 приймає кадр широкомовної розсилки і пересилає його з усіх портів комутатора, звідки він надходить на PC4 і S3. S3 пересилає кадр з порту для Магістраль 2, і S2 пропускає цей кадр. Виникнення петлі 2 рівня попереджається.

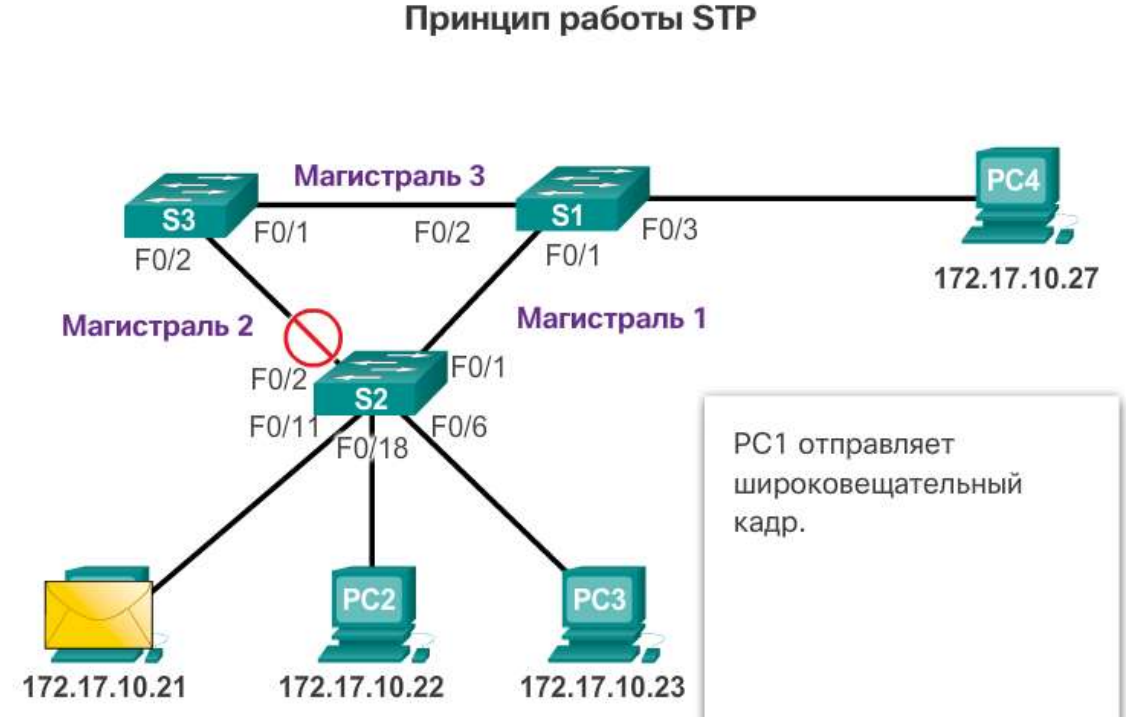


Рис. 5.1.4

У наведеному прикладі:

1. PC1 відправляє широкомовне розсилання в мережу.

2. Після цього широкомовлення пересилається по мережі.

3. Виникає збій в транкові каналі між S2 і S1, що призводить до переривання попереднього шляху.

4. S2 знімає блокування з попередньо заблокованого порту для Магістраль 2 і дозволяє передачу трафіку широкомовної мережі по альтернативному шляху, забезпечуючи подальший обмін даними. Якщо цей канал знову працює, виконується повторне сходження протоколу STP, а порт на S2 знову блокується.

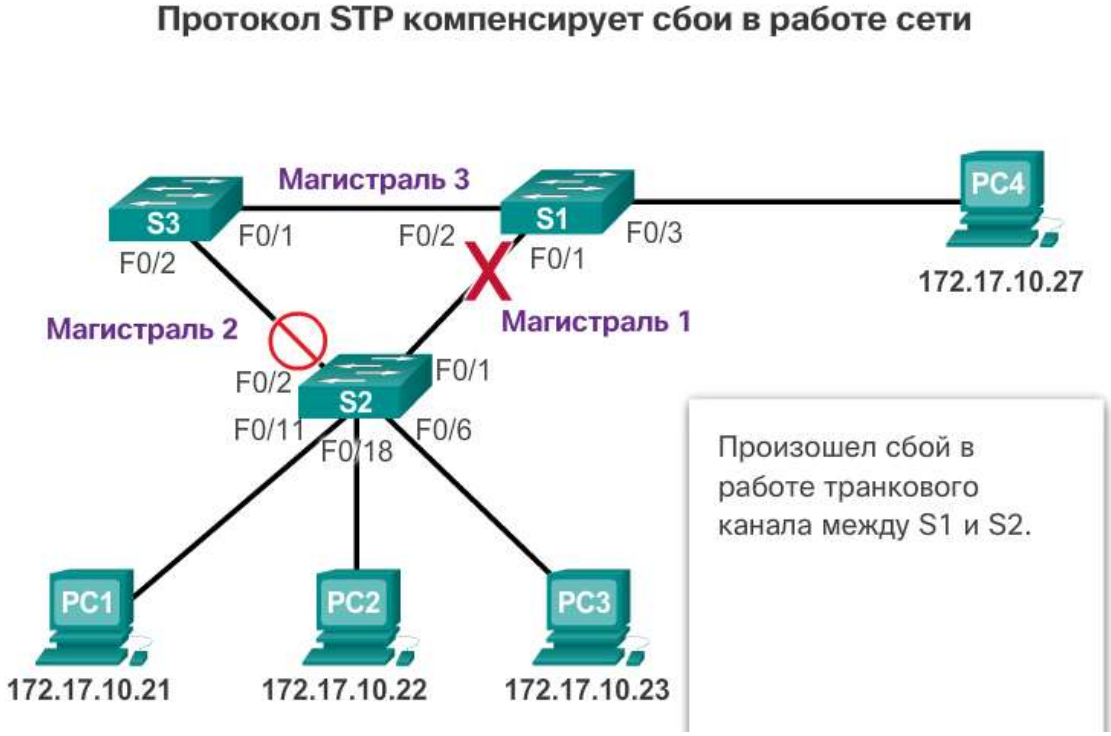


Рис. 5.1.5

Протокол STP запобігає виникненню петель за рахунок налаштування беспетлевого шляху в мережі з використанням портів, стратегічно налаштованих на їхній заблокований статус. Комутатори, що використовують протокол STP, можуть компенсувати збої за рахунок динамічної розблокування раніше блокованих портів і дозволу передачі трафіку по альтернативних шляхах.

До сих пір використовувався термін Spanning Tree Protocol (протокол spanning-tree) і абревіатура STP. Однак використання цього терміна і цієї абревіатури може бути двозначним. Багато фахівців використовують цей термін і абревіатуру для позначення різних реалізацій протоколу spanning-tree, наприклад протоколу Rapid Spanning Tree Protocol (RSTP) і протоколу Multiple Spanning Tree Protocol (MSTP). Щоб правильно пояснювати принципи протоколу spanning-tree, важливо розуміти, про яку конкретно реалізації або стандарті йдеться в даному контексті. У новій версії документації IEEE по протоколу spanning-tree (IEEE-802-1D-2004) говориться: «Протокол STP в даний час замінений протоколом Rapid Spanning Tree Protocol (RSTP)»; можна помітити, що в IEEE термін «STP» використовується для позначення вихідної реалізації протоколу spanning-tree, а «RSTP» - для опису версії протоколу

spanning-tree, зазначеної в IEEE-802.1D-2004. В рамках даної програми, якщо в контексті обговорення йдеться про вихідний протоколі STP, то щоб уникнути розбіжностей використовується фраза: «вихідний протокол spanning-tree 802.1D».

Примітка. Протокол STP заснований на алгоритмі, винайденому компанією Radia Perlman в ході роботи над проектом Digital Equipment Corporation. Алгоритм опублікований в 1985 році в документі «Алгоритм розподіленого обчислення протоколу spanning-tree в розширеній мережі LAN».

Алгоритм протоколу spanning-tree. Ролі портів

IEEE 802.1D STP використовує алгоритм протоколу spanning-tree (STA), щоб визначити, які порти комутаторів в мережі повинні бути переведені в стан блокування з метою уникнення можливих петель. STA призначає один з комутаторів як кореневого моста і використовує його як точку прив'язки для розрахунку всіх шляхів. На малюнку кореневої міст (комутатор S1) обраний за допомогою спеціального процесу вибору. Всі комутатори, які беруть участь в STP, обмінюються кадрами BPDU, щоб визначити, який комутатор має найнижче значення ідентифікатора моста (BID) в мережі. Комутатор з найменшим значенням BID автоматично стає кореневим мостом для розрахунків STA.

Примітка. Щоб спростити завдання, припустимо (поки не вказано інше), що всі порти на всіх комутаторах призначені мережі VLAN 1. У кожного комутатора є унікальний MAC-адресу, пов'язану з мережею VLAN 1.

BPDU є кадр обміну повідомленнями, яким обмінюються комутатори для STP. Кожен BPDU містить ідентифікатор BID, який визначає комутатор, який відправив BPDU. Ідентифікатор BID містить значення пріоритету, MAC-адресу відправляє комутатора і додатковий розширений ідентифікатор системи. Найнижче значення BID визначається комбінацією значень в цих трьох полях.

Після визначення кореневого моста STA розраховує найкоротший шлях до нього. Всі комутатори використовують STA для визначення портів, що підлягають блокуванню. Поки STA визначає оптимальні шляхи до кореневого моста для всіх портів комутатора в домені широкомовної розсилки, пересилання трафіку по мережі заблокована. При визначенні портів, що підлягають блокуванню, STA враховує вартість як шляху, так і порту. Вартість портів розраховується за допомогою значень вартості порту, залежить від швидкості кожного порту комутатора на даному маршруті. Сума значень вартості порту визначає загальну вартість шляху до кореневого моста. Якщо для вибору є кілька шляхів, STA вибирає шлях з найменшою вартістю.

Визначивши найкращі шляхи для кожного комутатора, алгоритм STA призначає ролі беруть участь портам комутаторів. Ролі портів описують їх зв'язок з кореневим мостом в мережі, а також вказують, чи дозволено для них пересилання трафіку:

Кореневі порти - порти комутатора, що знаходяться максимально близько до кореневого мосту. На малюнку кореневої порт на S2 - порт F0 / 1, налаштований для транкового каналу між S2 і S1. Кореневої порт на S3 - порт F0 / 1, налаштований для транкового каналу між S3 і S1. Кореневі порти вибираються для кожного комутатора окремо.

Призначені порти - все некореневі порти, яким, проте, дозволено пересилати трафік по мережі. На малюнку порти комутатора S1 (F0 / 1 і F0 / 2) є призначеними портами. На комутаторі S2 порт F0 / 2 також налаштований як призначеного порту. Призначені порти вибираються для кожного транкового каналу окремо. Якщо на одному кінці транка знаходиться кореневої порт, то на іншому - призначений. Всі порти на кореневому мосту є призначеними портами.

Альтернативні і резервні порти - альтернативні і резервні порти налаштовуються в стан блокування з метою уникнення можливих петель. На малюнку STA налаштував порт F0 / 2 на комутаторі S3 в ролі альтернативного порту. Порт F0 / 2 на комутаторі S3 знаходиться в стані блокування. Альтернативні порти вибираються тільки на транкових каналах, де жоден з кінців не є кореневим портом. Зверніть увагу, що на малюнку заблокований тільки один з кінців транка. Це забезпечує більш швидкий перехід в стан пересилки в разі потреби. (Заблоковані порти використовуються тільки в тому випадку, коли два порти на одному комутаторі з'єднані один з одним за допомогою комутатора або одного кабелю).

Відключені порти - відключеним називається порт комутатора, харчування якого відключено.

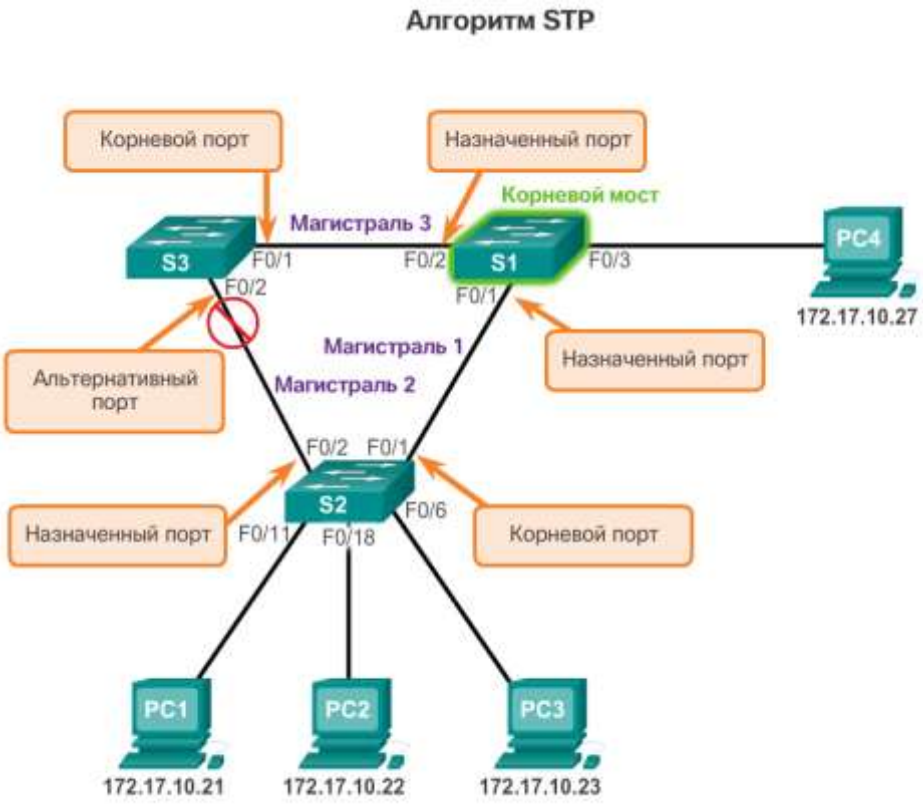


Рис. 5.1.6

Алгоритм протоколу spanning-tree. Корневий міст

Як показано на рис. всі примірники протоколу spanning-tree містять комутатор, призначений в якості кореневого моста. Кореневої міст служить точкою прив'язки для всіх розрахунків протоколу spanning-tree, дозволяючи визначити надлишкові шляху, які слід заблокувати.

Процес вибору визначає, який з комутаторів стане кореневим мостом.

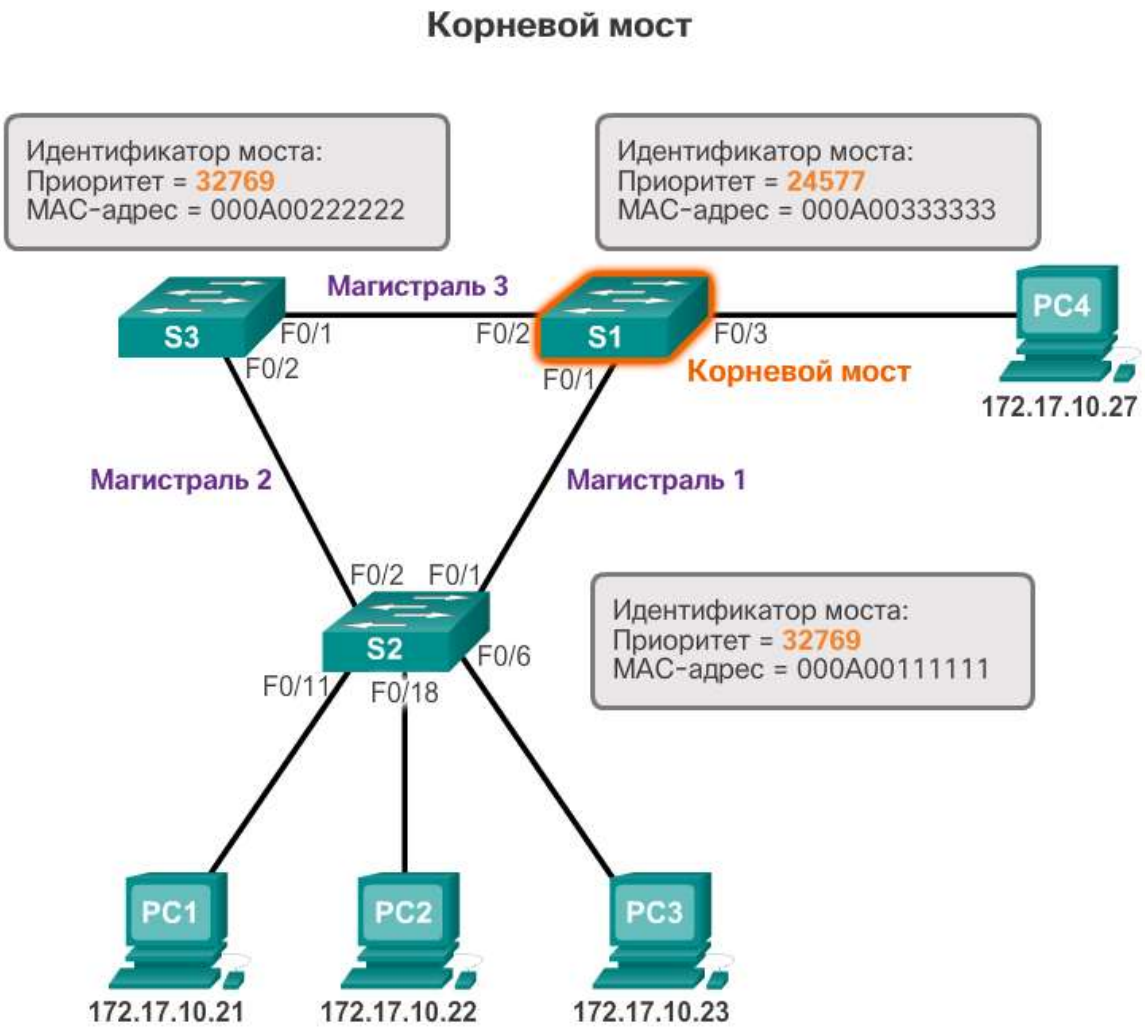


Рис. 5.1.7

На рис. 2 показані поля BID. Ідентифікатор BID складається з значення пріоритету, розширеного ідентифікатора системи і MAC-адреси комутатора.

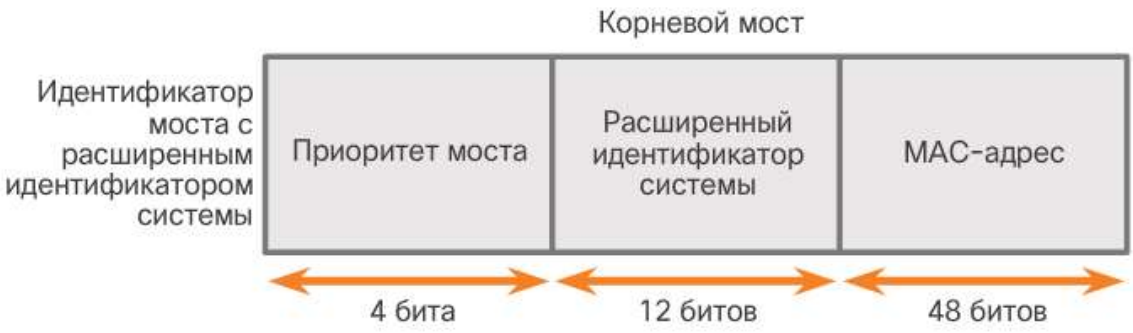


Рис. 5.1.8

Всі комутатори в домені широкомовної розсилки беруть участь в процесі вибору. Після завантаження комутатора вони починають розсилати кадри BPDU з інтервалом у дві секунди. Ці BPDU містять ідентифікатор BID комутатора і ідентифікатор кореневого моста.

Коли комутатори пересилають свої кадри BPDU, суміжні комутатори в домені широкомовної розсилки зчитують з них дані про ідентифікатор кореневого моста. Якщо ідентифікатор кореневого моста отриманого кадру BPDU має менше значення, ніж ідентифікатор кореневого моста на приймаючому комутаторі, то в цьому випадку приймає комутатор оновлює свій ідентифікатор кореневого моста, вказуючи суміжний комутатор в якості кореневого моста. Фактично це може бути не суміжний комутатор, а будь-який інший комутатор в домені широкомовної розсилки. Потім комутатор пересилає нові кадри BPDU з меншим значенням ідентифікатора кореневого моста на інші суміжні комутатори. Поступово комутатор з найменшим значенням ідентифікатора BID визначається як кореневого моста для примірника протоколу spanning-tree.

Кореневої міст вибирається для кожного екземпляра протоколу spanning-tree. Можлива наявність декількох окремих кореневих мостів. Якщо всі порти на всіх комутаторах є учасниками мережі VLAN 1, значить, існує тільки один екземпляр протоколу spanning-tree. Розширений ідентифікатор системи використовується для визначення примірника протоколу spanning-tree.

Алгоритм протоколу spanning-tree. Вартість шляху

Якщо кореневої міст обраний для примірника протоколу spanning-tree, STA починає процес визначення оптимальних шляхів до кореневого мосту від всіх некореневих комутаторів в домені широкомовної розсилки. Відомості про шляхи визначаються за допомогою підсумовування значень вартості окремих портів на шляху від некореневого комутатора до кореневого мосту. Кожен «адреса призначення», по суті, є портом комутатора.

Вартість портів за замовчуванням визначається швидкістю роботи порту. Як показано на рис. 1, значення вартості портів Ethernet 10 Гбіт / с дорівнює 2, портів Ethernet 1 Гбіт / с - 4, портів Fast Ethernet 100 - 19, а портів Ethernet 10 Мбіт / с - 100.

Примітка. У міру виходу на ринок нових, більш швидкісних технологій Ethernet значення вартості шляху можуть змінюватися з урахуванням зміни швидкостей. Нелінійні номера в таблиці дозволяють реалізувати ряд удосконалень попереднього стандарту Ethernet. Значення вже змінені відповідно до стандарту Ethernet 10 Гбіт / с. Щоб продемонструвати постійні зміни, пов'язані з високошвидкісними мережевими технологіями, комутатори Catalyst 4500 і 6500 підтримують метод вартості довшого шляху. Наприклад, 10 Гбіт / с має значення вартості шляху 2000, 100 Гбіт / с - 200, а 1 Тбіт / с - 20.

Хоча з портами комутатора пов'язано значення вартості шляху за замовчуванням, значення вартості порту можна налаштувати. Можливість настройки окремих портів надає адміністратору необхідну гнучкість при контролі шляхів протоколу spanning-tree до кореневого мосту.

Оптимальные пути к корневому мосту

Скорость канала	Стоимость (по изменённой спецификации IEEE)	Стоимость (по предыдущей спецификации IEEE)
10 Гбит/с	2	1
1 Гбит/с	4	1
100 Мбит/с	19	10
10 Мбит/с	100	100

Рис. 5.1.9

Щоб налаштувати вартість порту інтерфейсу (рис. 2), введіть команду spanning-tree cost value в режимі конфігурації інтерфейсу. Це значення може перебувати в діапазоні між 1 і 200 000 000.

Оптимальные пути к корневому мосту

Настроить стоимость порта

```
S2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)# interface f0/1
S2(config-if)# spanning-tree cost 25
S2(config-if# end
S2#
```

Сбросить стоимость порта

```
S2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)# interface f0/1
S2(config-if)# no spanning-tree cost
S2(config-if)# end
S2#
```

Рис. 5.1.10

В даному прикладі порт комутатора F0 / 1 налаштований зі значенням вартості порту 25 за допомогою команди режиму конфігурації інтерфейсу spanning-tree cost 25 на інтерфейсі F0 / 1.

Щоб відновити значення вартості порту за замовчуванням 19, введіть команду режиму конфігурації інтерфейсу no spanning-tree cost.

Вартість шляху дорівнює сумі всіх значень вартості порту по шляху до кореневого мосту (рис. 3). Шляхи з найменшою вартістю стають кращими, а всі інші надлишкові шляху блокуються. В даному прикладі значення вартості шляху від S2 до кореневого мосту S1 дорівнює 19 по шляху 1 (з урахуванням окремих значень вартості порту, зазначених в стандарті IEEE) і 38 по шляху 2. Оскільки загальна вартість шляху 1 до кореневого мосту нижче, саме цей шлях є переважним. Після цього протокол STP здійснює блокування надлишкового шляху для запобігання виникнення петлі.

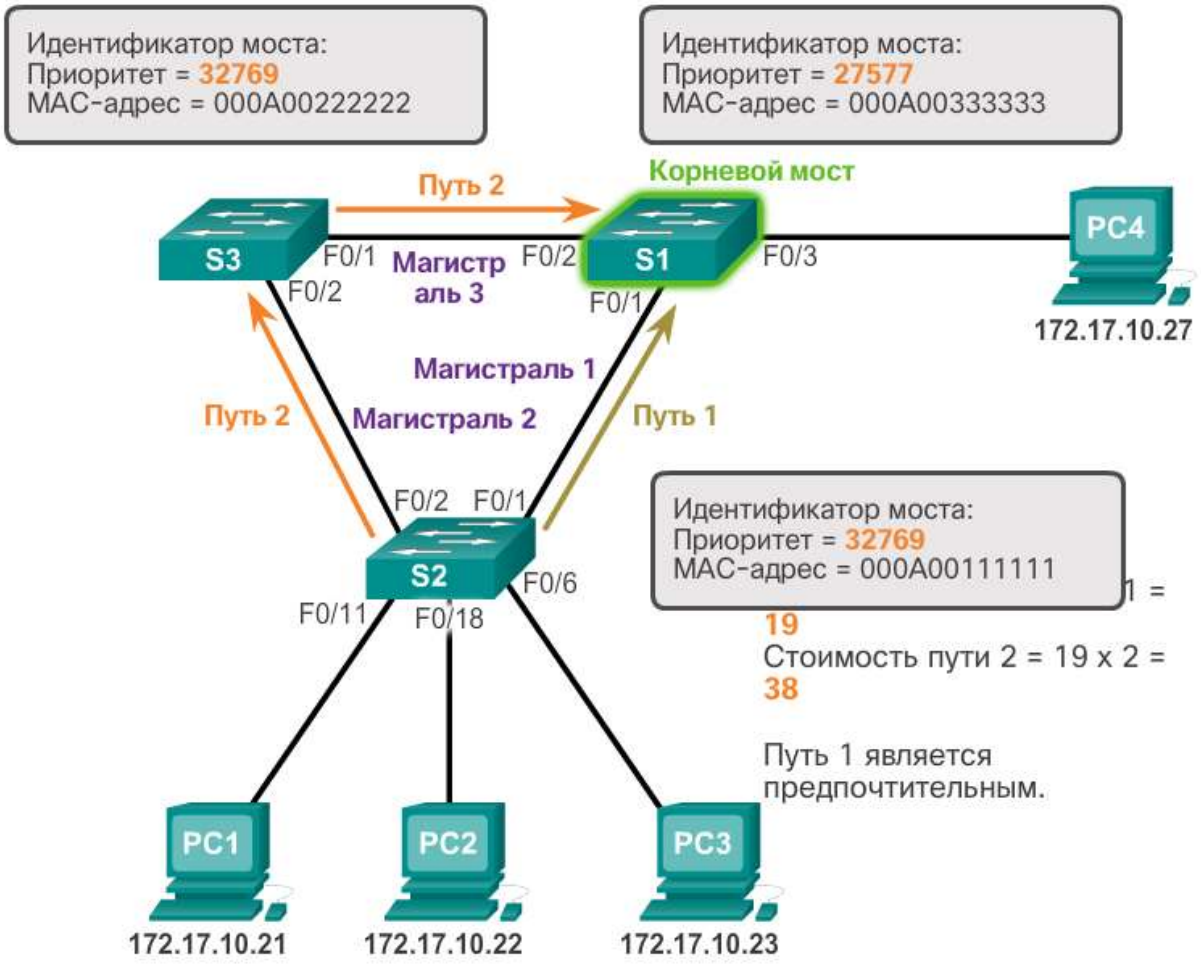


Рис. 5.1.11

Щоб перевірити вартість порту і вартість шляху до кореневого мосту, введіть команду show spanning-tree (рис. 4). Поле Cost у верхній частині вихідних даних містить підсумкове значення вартості шляху до кореневого мосту. Це значення змінюється в залежності від кількості портів комутатора, які повинні бути пройдені на шляху до кореневого мосту. У вихідних даних все інтерфейси також визначені зі значенням вартості окремого порту 19.

Оптимальные пути к корневому мосту

```
S2# show spanning-tree

VLAN001
   Spanning tree enabled protocol ieee
   Root ID     Priority  24577
               Address       000A.0033.3333
               Cost          19
               Port          1
               Hello Time    2 sec Max Age 20 sec Forward Delay 15 sec

   Bridge ID   Priority      32769  (priority 32768 sys-id-ext  1)
               Address 000A.0011.1111
               Hello time 2 sec Max Age 20 sec Forward Delay 15 sec
               Aging Time 300

Interface    Role   Sts  Cost    Prio.Nbr  Type
-----------  -----  ---- -----   --------- -----------------
F0/1         Root   FWD   19      128.1     Edge P2p
F0/2         Desg   FWD   19      128.2     Edge P2p
```

Рис. 5.1.12

Формат кадру BPDU 802.1D

Алгоритм протоколу spanning-tree залежить від обміну кадрами BPDU, яке виконується для визначення кореневого моста. Кадр BPDU містить 12 окремих полів, які містять відомості про шляхи і пріоритеті, використовувані для визначення кореневого моста і шляхів до нього.

Для перегляду додаткових відомостей натисніть на поля BPDU на рис. 1.

Поля BPDU

Номер поля	Байты	Поле
1-4	2	Protocol ID
	1	Version
	1	Message Type
	1	Flags
5-8	8	Root ID
	4	Cost of Path
	8	Bridge ID
	2	Port ID
9-12	2	Message age
	2	Max age
	2	Hello time
	2	Forward delay

Protocol ID

В поле Protocol ID «Идентификатор протокола» указан тип используемого протокола. Данное поле содержит нулевое значение.

Рис. 5.1.13

У перших чотирьох полях вказані протокол, версія, тип повідомлення і прапори стану.

Наступні чотири поля використовуються для визначення кореневого моста і вартості шляху до нього.

Останні чотири поля є полями таймера, які визначають інтервал відправки повідомлень BPDU і тривалість зберігання даних, отриманих за допомогою процесу BPDU (див. Наступний розділ).

На рис. 2 показаний кадр BPDU, отриманий за допомогою програми Wireshark. У цьому прикладі кадр BPDU містить більшу кількість полів, ніж описано вище. Повідомлення BPDU при передачі по мережі інкапсулюється в кадр Ethernet. Тема 802.3 вказує адреси джерела і призначення кадру BPDU. Кадр містить MAC-адресу призначення 01: 80: C2: 00: 00: 00, який є адресою групової розсилки для групи протоколу spanning-tree. При адресації кадру з використанням цього MAC-адреси все комутатори, налаштовані для протоколу spanning-tree, приймають і зчитують дані з кадру. Усі інші пристрої в мережі ігнорують кадр.

Пример BPDU

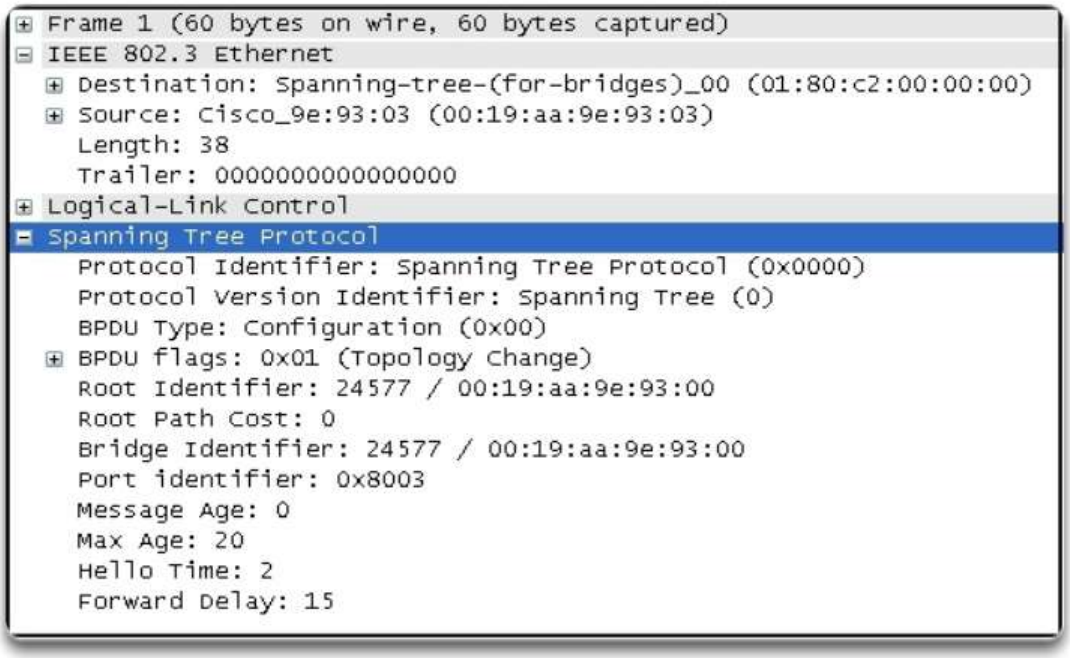


Рис. 5.1.14

У цьому прикладі ідентифікатор кореневого моста в отриманому кадрі BPDU збігається з ідентифікатором BID. Це вказує на те, що кадр отриманий з кореневого моста. Всі таймери налаштовані зі значеннями за замовчуванням.

Поширення і процес BPDU

Спочатку кожен комутатор в домені широкомовної розсилки вважає себе кореневим мостом для примірника протоколу spanning-tree, тому відправлені кадри BPDU містять ідентифікатор BID локального комутатора в якості ідентифікатора кореневого моста. За замовчуванням після завантаження комутатора кадри BPDU відправляються з інтервалом у дві секунди; тобто значення таймера вітання за замовчуванням, вказане в кадрі BPDU - дві секунди. Всі комутатори надають відомості про власний ідентифікатор BID, ідентифікатор кореневого моста і вартості шляху до кореневого мосту.

Коли суміжні комутатори приймають кадр BPDU, вони зіставляють міститься в ньому ідентифікатор кореневого моста з локальним ідентифікатором кореневого моста. Якщо ідентифікатор кореневого моста в кадрі BPDU має менше значення, ніж локальний ідентифікатор кореневого моста, комутатор оновлює локальний ідентифікатор і той ідентифікатор, який міститься в повідомленнях BPDU. Ці повідомлення вказують новий кореневий міст в мережі. Відстань до кореневого моста також позначається за допомогою оновлення вартості шляху. Наприклад, якщо кадр BPDU отриманий на порте комутатора Fast Ethernet, вартість шляху збільшується на 19. Якщо локальний ідентифікатор кореневого моста має менше значення, ніж ідентифікатор кореневого моста, отриманий в кадрі BPDU, кадр BPDU відкидається.

Після поновлення ідентифікатора кореневого моста в цілях визначення нового кореневого моста, всі наступні кадри BPDU, відправлені з цього комутатора, будуть містити новий ідентифікатор кореневого моста і оновлене

значення вартості шляху. Таким чином, всі інші суміжні комутатори можуть постійно бачити найнижче значення ідентифікатора кореневого моста. У міру проходження кадрів BPDU між іншими суміжними комутаторами вартість шляху постійно оновлюється, щоб вказати загальну вартість шляху до кореневого мосту. Всі комутатори в протоколі spanning tree використовують свій шлях для визначення оптимального шляху до кореневого мосту.

Далі подано короткий опис процесу BPDU:

Примітка. Пріоритет є первинним вирішальним фактором при виборі кореневого моста. Якщо пріоритети всіх комутаторів однакові, то пристрій з найменшим значенням MAC-адреси стає кореневим мостом.

1. Спочатку всі комутатори визначають себе як кореневий міста. Комутатор S2 пересилає кадри BPDU з усіх своїх портів. (Рис. 1)

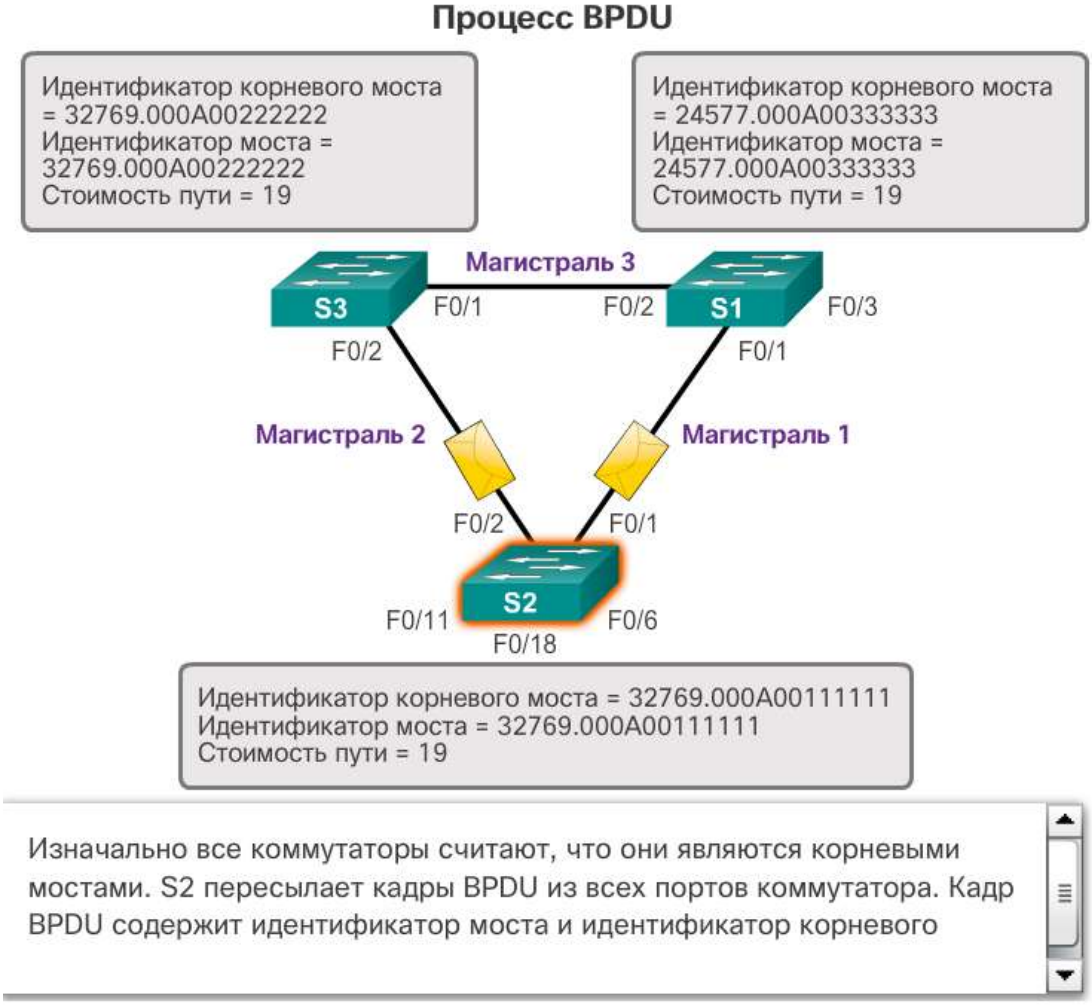


Рис. 5.1.15

2. Коли S3 отримує BPDU від S2, S3 порівнює свій ідентифікатор кореневого моста з отриманим кадром BPDU. Пріоритети однакові, тому комутатор змушений перевірити частина MAC-адреси, щоб визначити, який з MAC-адрес має більш низьке значення. Оскільки S2 містить менше значення MAC-адреси, то S3 оновлює свій ідентифікатор кореневого моста з урахуванням ідентифікатора кореневого моста S2. На цьому етапі S3 вважає S2 кореневих мостом. (Рис. 2)

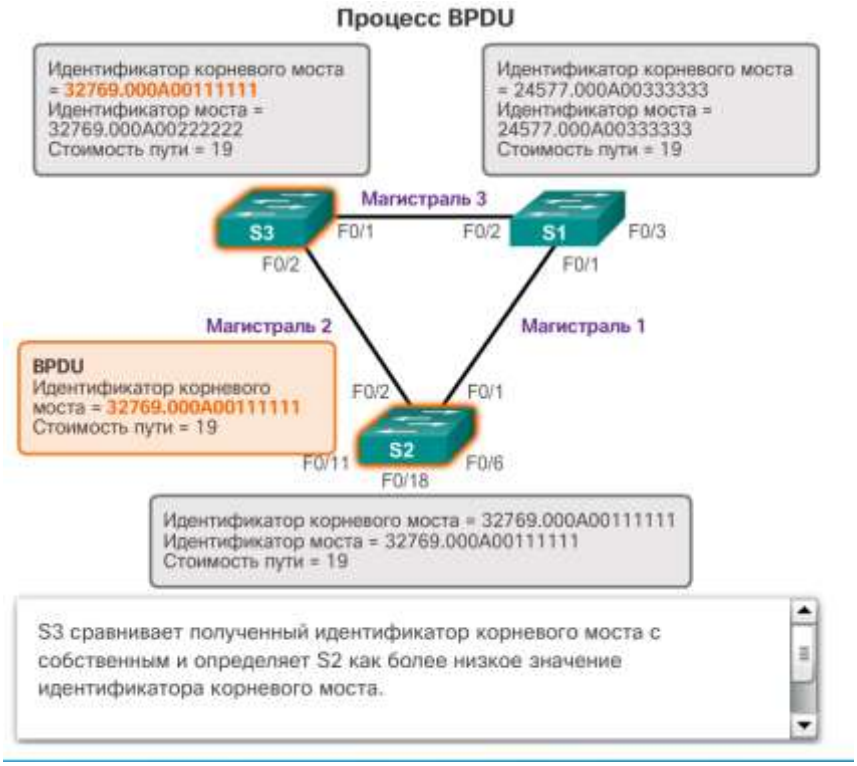


Рис. 5.1.16

3. Коли S1 порівнює свій ідентифікатор кореневого моста з ідентифікатором, що містяться в отриманому кадрі BPDU, він визначає свій локальний ідентифікатор кореневого моста як менше значення і відкидає кадр BPDU, отриманий від S2. (Рис. 3)

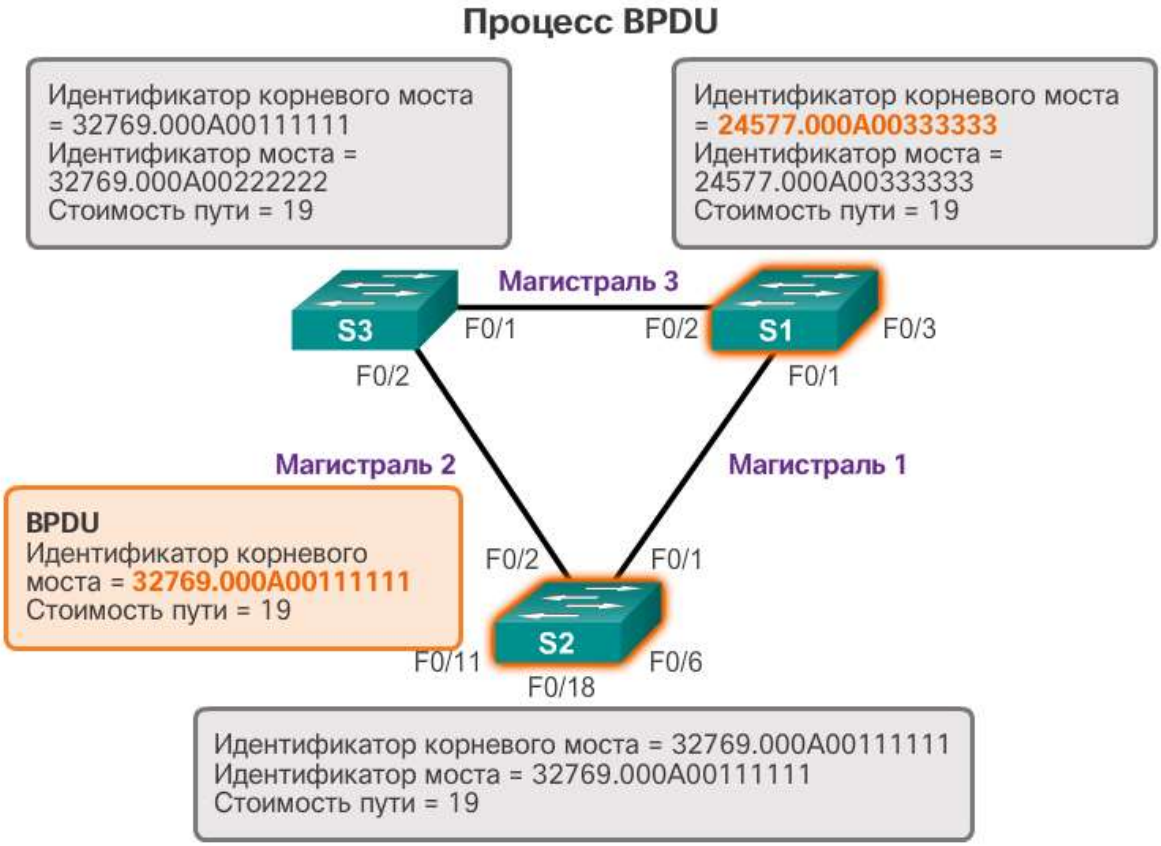


Рис. 5.1.17

4. Коли S3 відправляє свої кадри BPDU, ідентифікатором кореневого моста, в кадрі BPDU міститься ідентифікатор кореневого моста S2. (Рис. 4)

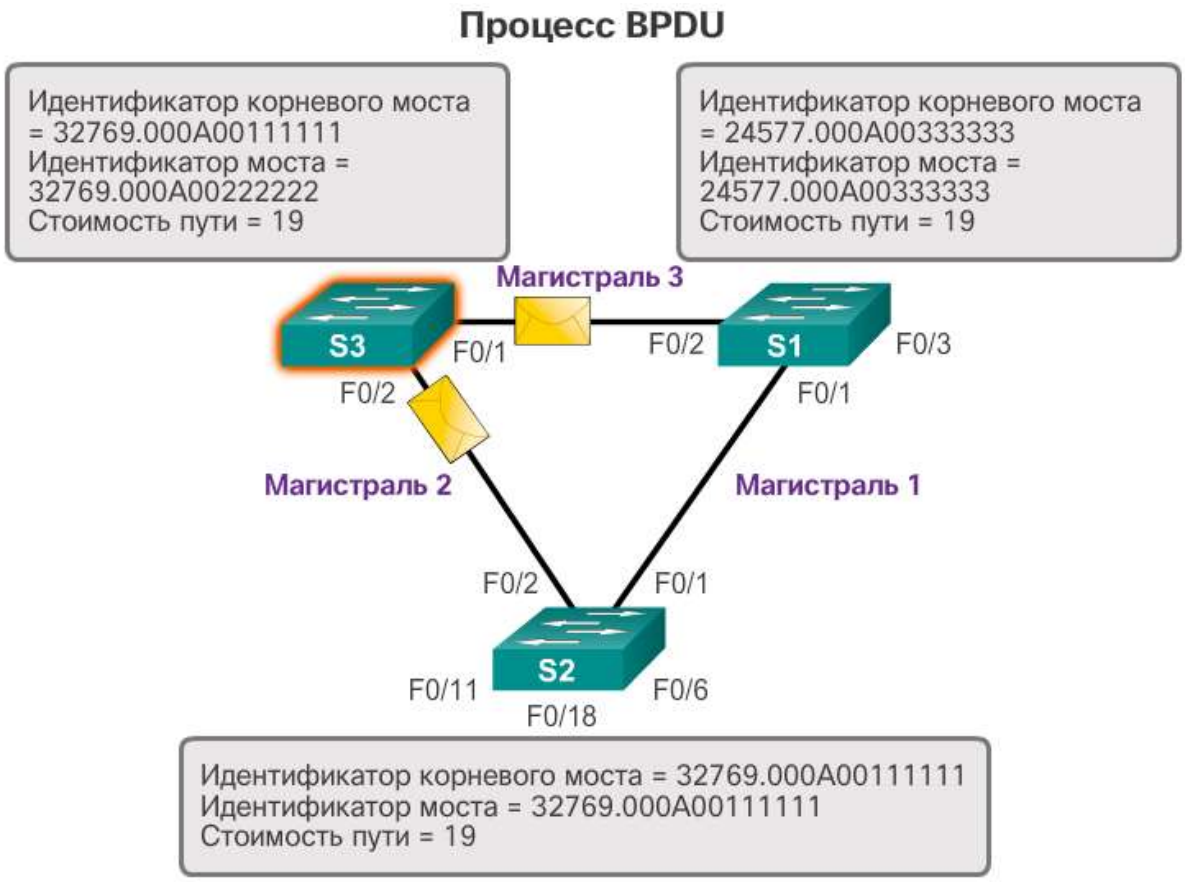


Рис. 5.1.18

5. Коли S2 отримує кадр BPDU, він відкидає його після того, як підтвердить, що ідентифікатор кореневого моста в BPDU збігається з локальним ідентифікатором кореневого моста. (Рис. 5)

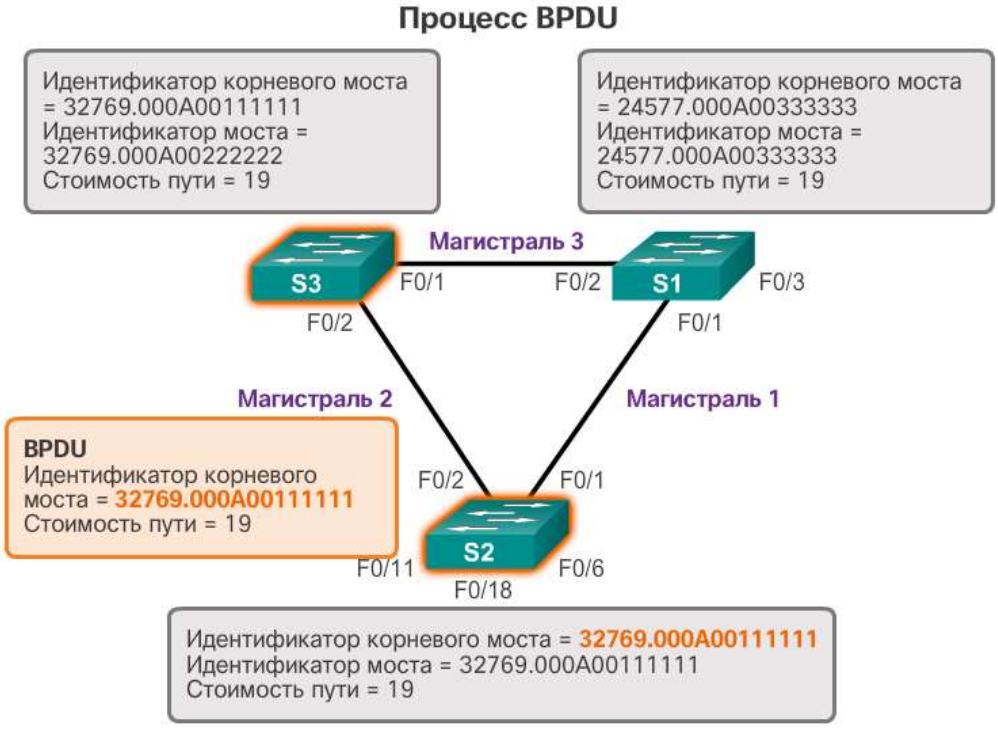


Рис. 5.1.19

6. Оскільки S1 містить більш низьке значення пріоритету в своєму ідентифікатор кореневого моста, він відкидає кадр BPDU, отриманий від S3. (Рис. 6)

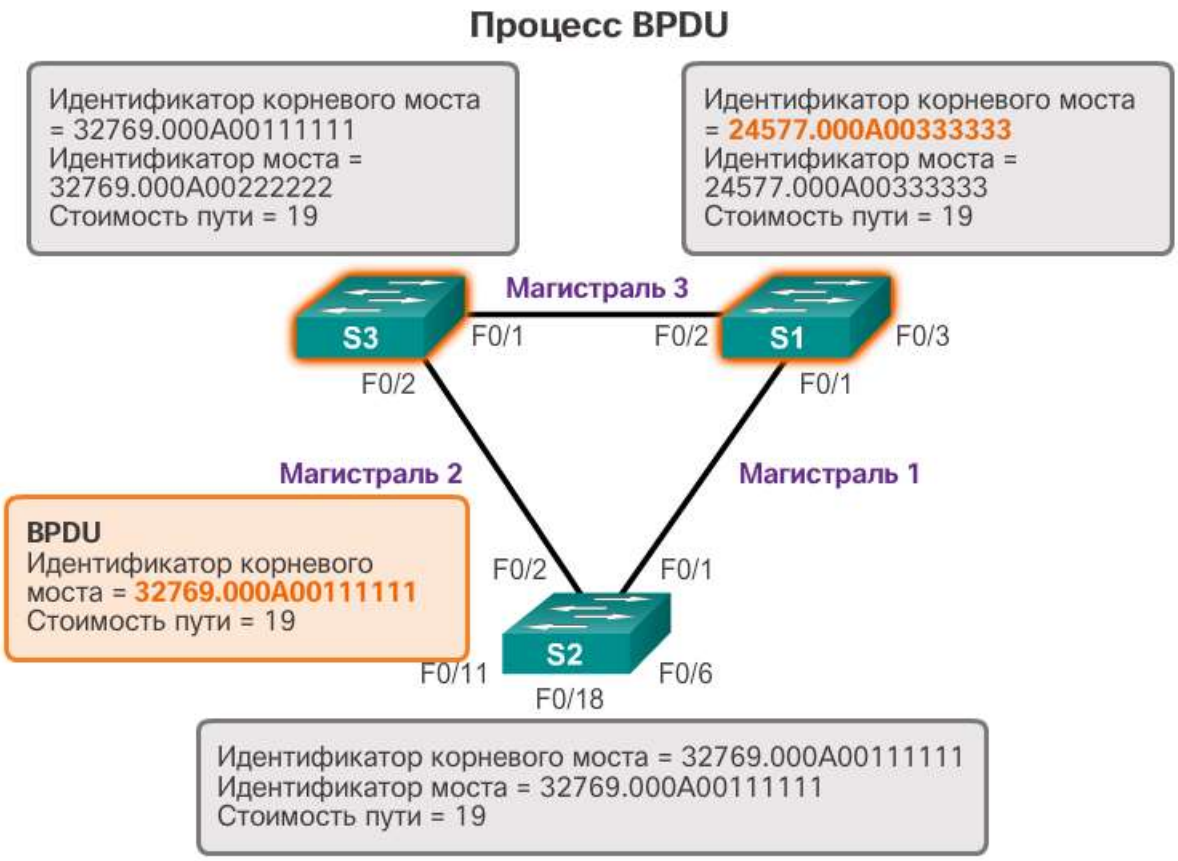


Рис. 5.1.20

7. S1 відправляє свої кадри BPDU. (Рис. 7)

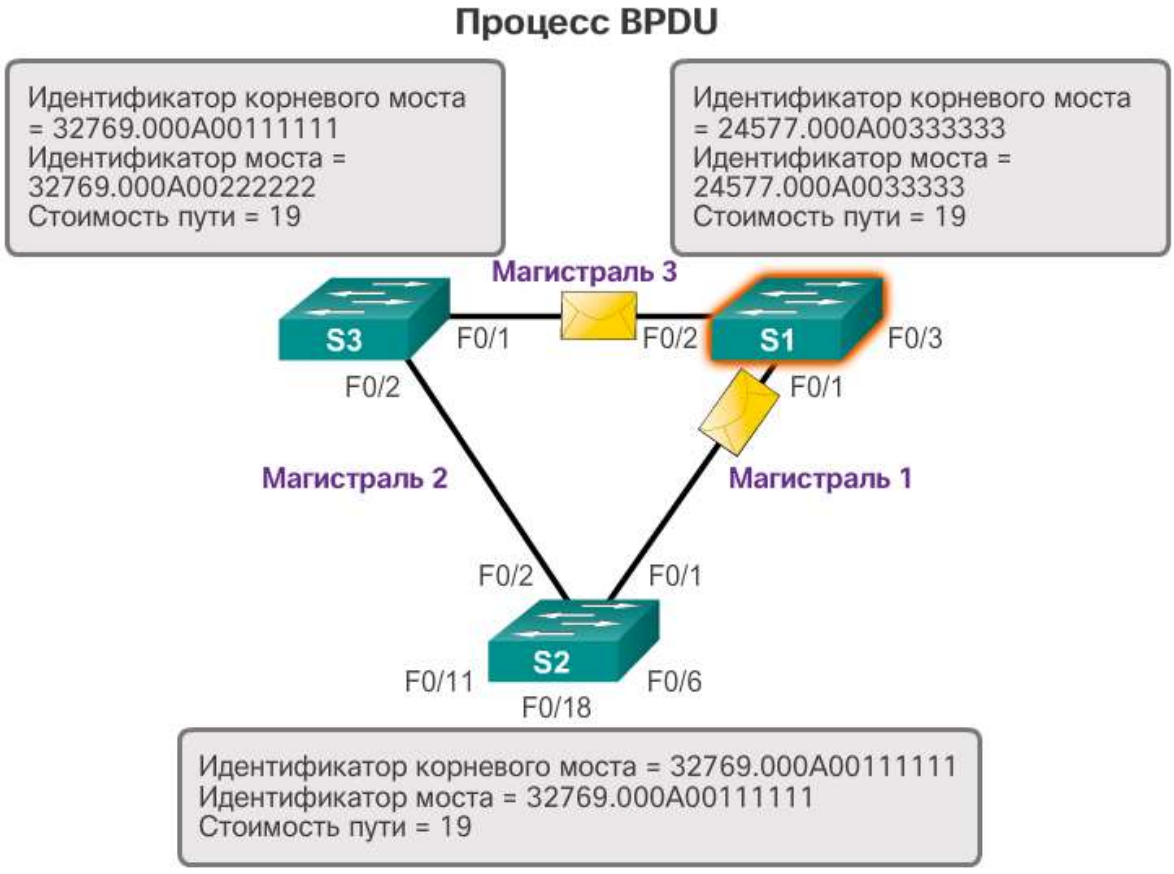


Рис. 5.1.21

8. S3 визначає, що ідентифікатор кореневого моста в кадрі BPDU містить менше значення і, отже, оновлює свої значення ідентифікатора кореневого моста, вказуючи, що S1 тепер є кореневим мостом. (Рис. 8)

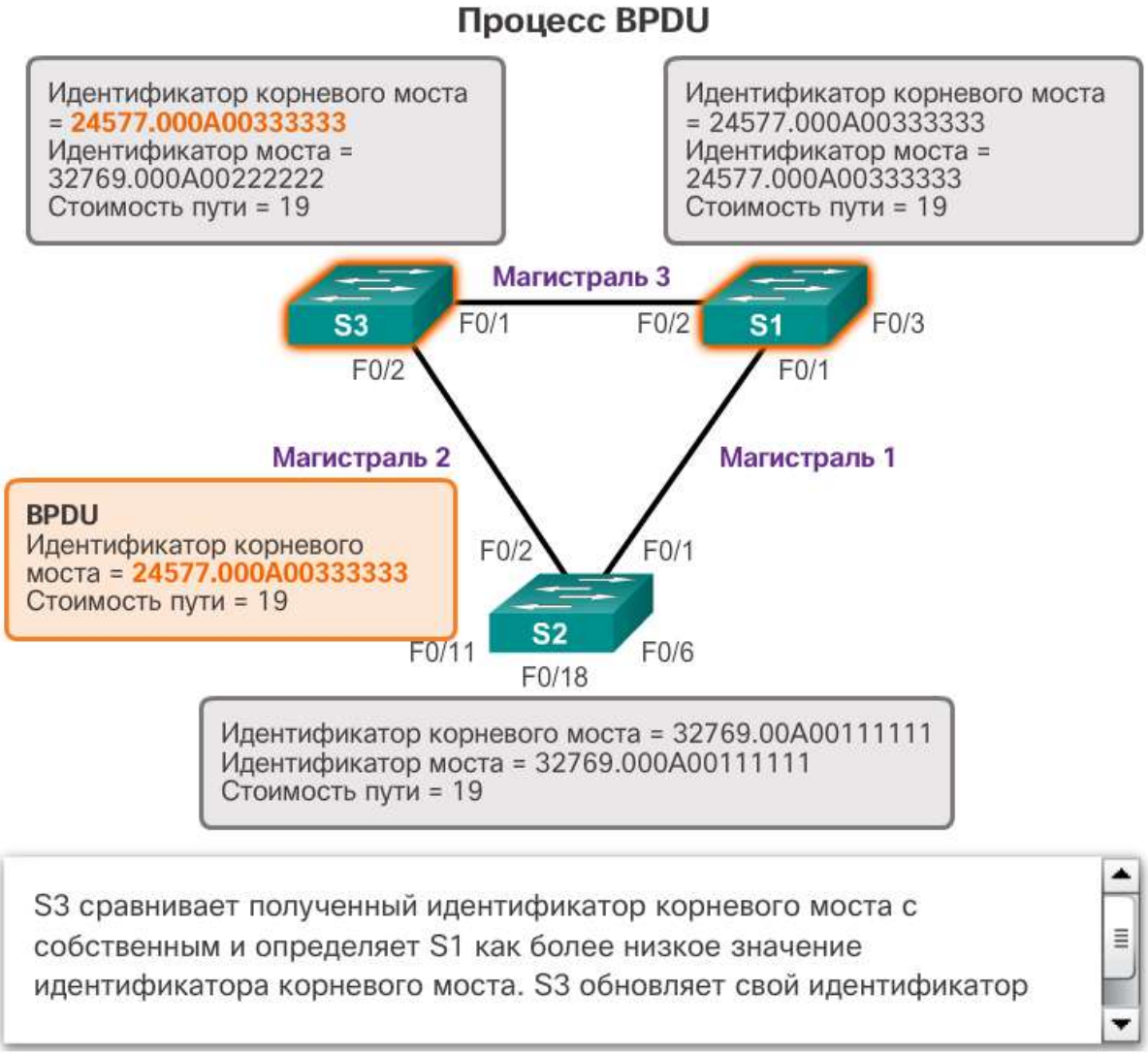


Рис. 5.1.22

9. S2 визначає, що ідентифікатор кореневого моста в кадрі BPDU містить менше значення і, отже, оновлює свої значення ідентифікатора кореневого моста, вказуючи, що S1 тепер є кореневим мостом. (Рис. 9)

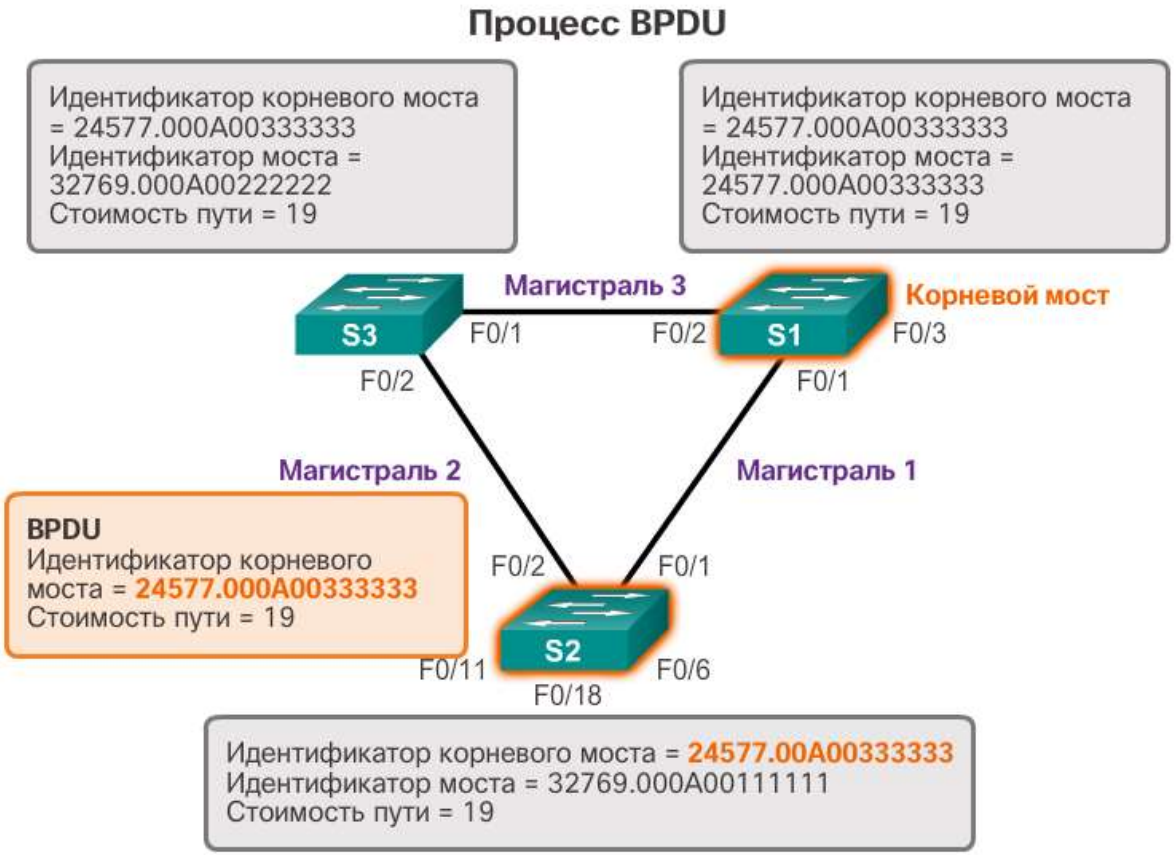


Рис. 5.1.23

Розширений ідентифікатор системи

Ідентифікатор моста (BID) використовується для визначення кореневого моста в мережі. Поле BID кадру BPDU містить три окремих поля:

- Пріоритет моста
- Розширений ідентифікатор системи
- MAC-адресу
- При виборі кореневого моста використовуються всі поля.
- Пріоритет моста

Пріоритет моста являє собою настроюється значення, яке можна використовувати для визначення комутатора, який стане кореневим мостом. Комутатор з найнижчим пріоритетом, який має на увазі найменше значення BID, стає кореневим мостом, оскільки перевага має більш низьке значення пріоритету. Наприклад, якщо ви хочете призначити в якості кореневого моста конкретний комутатор, то для нього слід задати більш низьке значення пріоритету, ніж для інших комутаторів в мережі. За замовчуванням для всіх комутаторів Cisco використовується значення пріоритету 32768. Значення варіюються в діапазоні від 0 до 61440 з кроком в 4096. Допустимі значення пріоритету: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 і 61440. Всі інші значення відхиляються. Пріоритет моста 0 має перевагу в порівнянні з усіма іншими значеннями пріоритету моста.

Розширений ідентифікатор системи

Для мереж, в яких не використовувалися мережі VLAN, розроблені більш ранні реалізації IEEE 802.1D. На всіх комутаторах використовувалося один загальний протокол spanning-tree. З цієї причини в попередніх моделях

комутаторів Cisco кадри BPDU могли обійтися без розширеного ідентифікатора системи. Завдяки повсюдному використанню мереж VLAN для сегментації мережевої інфраструктури, 802.1D було розширено з урахуванням підтримки мереж VLAN. Саме тому ідентифікатор мережі VLAN був доданий в кадр BPDU. Відомості про мережу VLAN включені в кадр BPDU за допомогою розширеного ідентифікатора системи. Всі нові моделі комутаторів за замовчуванням використовують розширені ідентифікатори системи.

Як показано на рис. 1, поле пріоритету моста має 2 байта або 16 біт в довжину; 4 біта вказують пріоритет моста, а 12 біт - розширений ідентифікатор системи, який визначає мережу VLAN, що бере участь в даному процесі STP. Завдяки тому, що довжина розширеного ідентифікатора системи складає 12 біт, довжина пріоритету моста скорочена до 4 біт. В рамках цього процесу крайні праві 12 біт резервуються для ідентифікатора мережі VLAN, а крайні ліві 4 біти - для пріоритету моста. Це пояснює, чому значення пріоритету моста можна налаштувати тільки кратним 4096 або 2 ^ 12. Якщо крайніми лівими є біти 0001 в цьому випадку значення пріоритету моста одно 4096; якщо крайніми лівими є біти 1111, то значення пріоритету моста одно 61440 (= 15 x 4096). Комутатори Catalyst серій 2960 і 3560 не підтримують налаштування пріоритету моста рівному значенням 65536 (= 16 x 4096), оскільки це передбачає використання п'ятого біта, який недоступний внаслідок використання розширеного ідентифікатора системи.

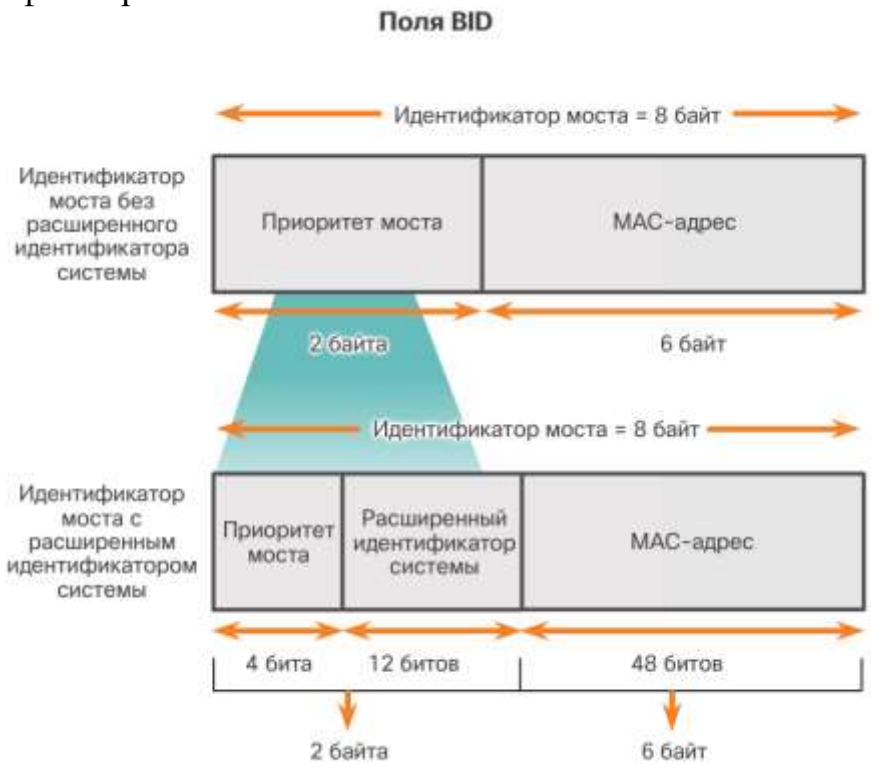


Рис. 5.1.24

Для вказівки пріоритету і мережі VLAN для кадру BPDU значення розширеного ідентифікатора системи додається до значення пріоритету моста в ідентифікатор BID.

Коли два комутатора налаштовані з однаковим пріоритетом і містять один і той же розширений ідентифікатор системи, то комутатор, MAC-адресу якого має найменшу шістнадцятирічне значення, буде мати найменший ідентифікатор

BID. Спочатку все комутатори налаштовуються з однаковим значенням пріоритету за умовчанням. Після цього MAC-адресу є вирішальним фактором, відповідно до якого комутатор стає кореневим мостом. Щоб гарантувати, що рішення щодо кореневого моста оптимально відповідає вимогам мережі, адміністраторові рекомендується настроїти вибраний комутатор кореневого моста з найменшим пріоритетом. При цьому також гарантується, що додавання в мережу нових комутаторів чи не спровокує вибір нового протоколу spanning-tree, що могло б порушити обмін даними в мережі в процесі вибору нового кореневого моста.

На рис. 2 S1 має більш низьке значення пріоритету, ніж інші комутатори, отже, цей комутатор є кращим в якості кореневого моста для цього примірника протоколу spanning-tree.

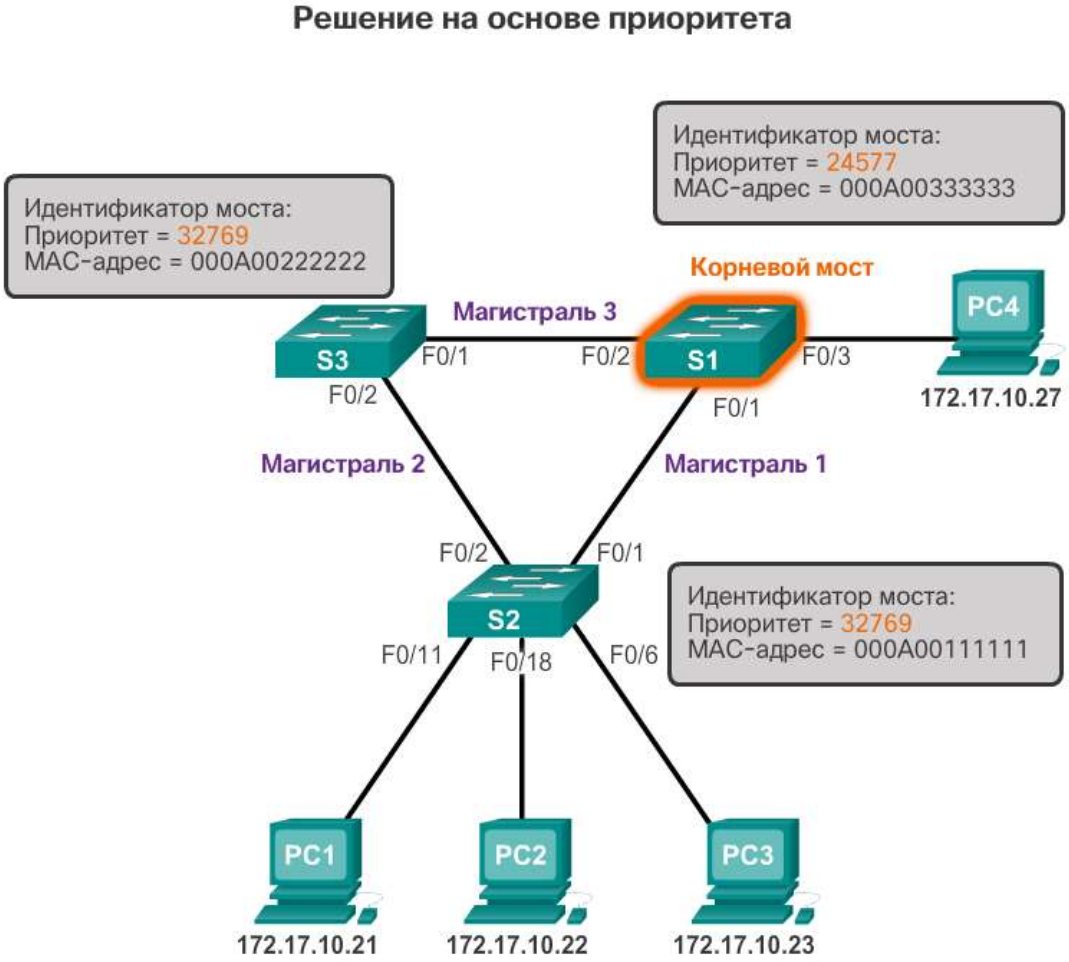


Рис. 5.1.25

Коли все комутатори налаштовані з однаковим пріоритетом, як і в тому випадку, коли всі комутатори в конфігурації за замовчуванням з пріоритетом 32768, MAC-адресу стає вирішальним фактором, з урахуванням якого комутатор стає кореневим мостом (рис. 3).

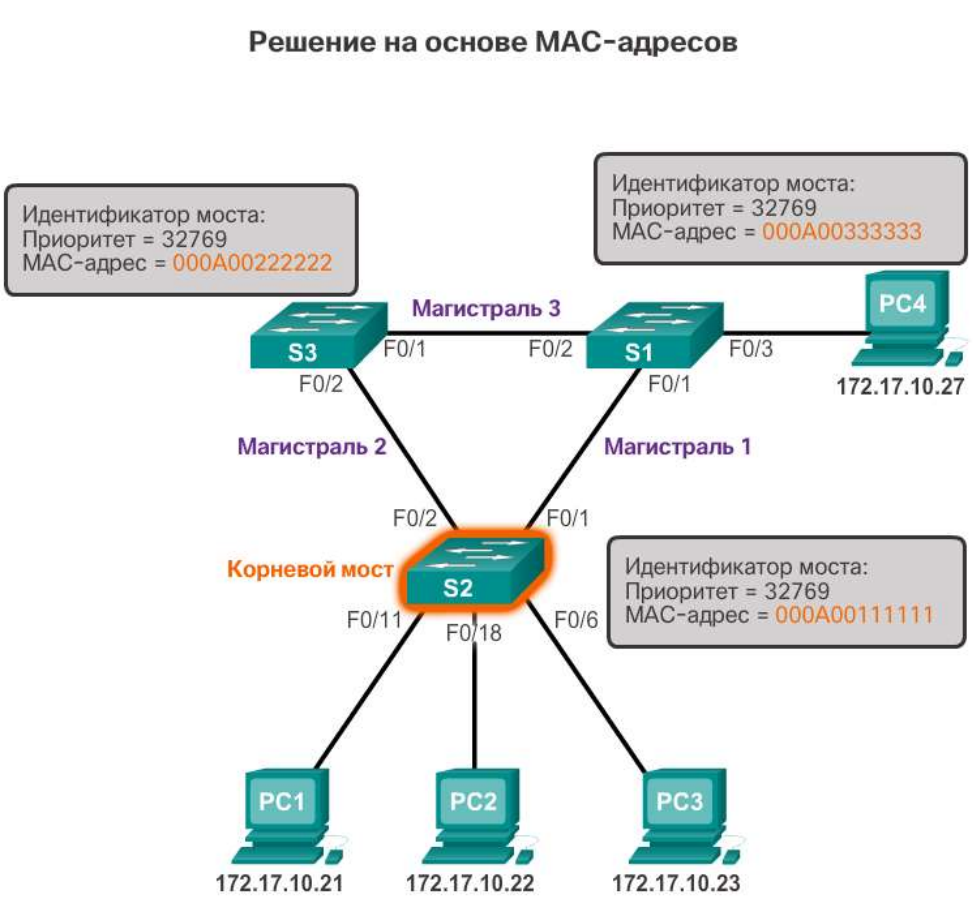


Рис. 5.1.26

Примітка. У цьому прикладі для всіх комутаторів використовується значення 32769. Це значення засноване на значенні пріоритету за умовчанням 32768 і призначення мережі VLAN 1, що знаходиться в кожному з комутаторів (32768 + 1).

MAC-адресу з найнижчим шістнадцятиричним значенням вважається кращим кореневих мостом. У цьому прикладі S2 має найменше значення MAC-адреси і, отже, призначається кореневих мостом для цього примірника протоколу spanning-tree.

З моменту створення вихідного стандарту IEEE 802.1D було розроблено кілька різновидів протоколів STP.

До різновидів протоколів STP відносяться наступні:

STP: початкова версія IEEE 802.1D (802.1D-1998 і більш ранні), в рамках якої надається топологія в мережі з надлишковими каналами. Загальний протокол spanning-tree (CST): передбачає використання тільки одного примірника протоколу spanning-tree для всієї мережі з мостовим з'єднанням незалежно від кількості мереж VLAN.

PVST + є вдосконаленим протоколом компанії Cisco, в якому для кожного окремого VLAN використовується окремий екземпляр RSTP. Розглянутий варіант протоколу spanning-tree підтримує PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard і loop guard.

802.1D-2004: оновлена версія стандарту STP, в яку входить IEEE 802.1w.

Швидкий протокол STP (RSTP) або IEEE 802.1w: доопрацьований протокол STP, який забезпечує більш швидке сходження, ніж протокол STP.

Rapid PVST +: вдосконалений корпорацією Cisco протокол RSTP, який використовує PVST +. Rapid PVST + надає окремий екземпляр 802.1w для кожної мережі VLAN. Розглянутий варіант протоколу spanning-tree підтримує PortFast, BPDU guard, BPDU filter, root guard і loop guard.

Протокол MSTP (кілька протоколів spanning-tree) (MSTP): стандарт IEEE на базі раніше існуючої власної реалізації Multiple Instance STP (MISTP) корпорації Cisco. MSTP зіставляє кілька мереж VLAN в межах одного примірника протоколу spanning-tree. Реалізація Cisco протоколу MSTP, яка забезпечує до 16 примірників протоколу RSTP і об'єднує безліч мереж VLAN з ідентичною фізичної і логічної топологією в один загальний екземпляр RSTP. Кожна реалізація підтримує функції PortFast, BPDU guard, BPDU filter, root guard і loop guard.

Мережевому фахівця, який відповідає за адміністрування комутаторів, може знадобитися прийняти рішення щодо того, який тип протоколу STP необхідно реалізувати.

Примітка. Застарілі пропрієтарні функції Cisco UplinkFast і BackboneFast в рамках даного курсу не розглядаються. Ці функції замінені реалізацією протоколу Rapid PVST +, в яку ці функції включені як частина реалізації стандарту RSTP.

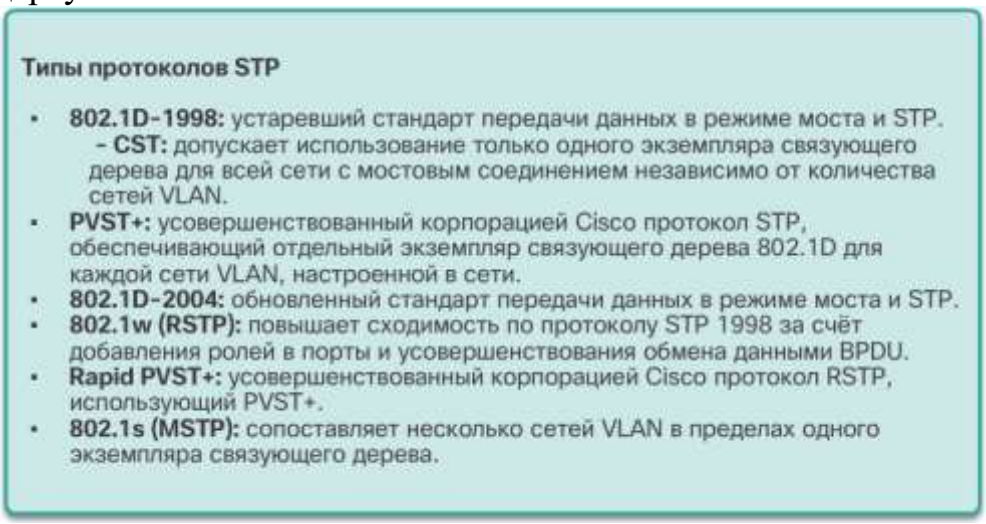


Рис. 5.1.27

Далі представлені характеристики різних протоколів STP. Виділені курсивом слова вказують, чи є конкретний протокол STP власним протоколом Cisco або стандартної реалізацією IEEE:

STP: використовує один екземпляр протоколу spanning-tree IEEE 802.1D для всієї комутованої мережі незалежно від кількості мереж VLAN. Оскільки використовується тільки один екземпляр, вимоги до ЦП і пам'яті для цієї версії нижче, ніж по відношенню до інших протоколів. Однак, оскільки використовується тільки один екземпляр, існує тільки один кореневий міст і одне дерево. Трафік для всіх мереж VLAN проходить по одному і тому ж шляху, що може привести до утворення неоптимальні потоків трафіку. З огляду на обмежень 802.1D дана версія забезпечує повільне сходження.

PVST +: вдосконалений корпорацією Cisco протокол STP, який надає окремий екземпляр реалізації 802.1D корпорації Cisco для кожної мережі VLAN, налаштованої в мережі. Розглянутий варіант протоколу spanning-tree

підтримує PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard і loop guard. При створенні екземпляра для кожної мережі VLAN збільшуються вимоги до ЦП і пам'яті, однак таким чином забезпечується можливість використання кореневих мостів окремо для кожної мережі VLAN. Така модель дозволяє оптимізувати протокол spanning-tree для трафіку кожної мережі VLAN. Збіжність цієї версії аналогічна збіжності 802.1D. Однак збіжність здійснюється окремо для кожної мережі VLAN.

RSTP (або IEEE 802.1w): швидкий протокол spanning-tree, що забезпечує більш швидке сходження, ніж вихідна реалізація 802.1D. У цій версії усунені багато проблем зі збіжністю, але, оскільки в ній все одно надається один примірник STP, проблема неоптимальні потоків трафіку як і раніше залишається невирішеною. З метою забезпечення більш швидкого сходження вимоги до ЦП і пам'яті в цій версії трохи вище, ніж для CST, але не такі високі, як для RSTP +.

Rapid PVST +: вдосконалений корпорацією Cisco протокол RSTP, який використовує PVST +. Надає окремий екземпляр 802.1w для кожної мережі VLAN. Розглянутий варіант протоколу spanning-tree підтримує PortFast, BPDU guard, BPDU filter, root guard і loop guard. У цій версії вирішена проблема збіжності і освіти неоптимальні потоків трафіку. Однак в цій версії пред'являються найвищі вимоги до ЦП і пам'яті.

MSTP: стандарт IEEE 802.1s, створений на основі попередньої власної реалізації протоколу MISTP компанії Cisco. Щоб зменшити число необхідних примірників STP, MSTP зіставляє кілька мереж VLAN, щодо яких діють однакові вимоги до потоку трафіку, в межах одного примірника протоколу spanning-tree.

MST: реалізація Cisco протоколу MSTP, яка забезпечує до 16 примірників протоколу RSTP (802.1w) і об'єднує безліч мереж VLAN з ідентичною фізичної і логічної топологіями в один загальний екземпляр RSTP. Кожна реалізація підтримує функції PortFast, BPDU guard, BPDU filter, root guard і loop guard. Вимоги до ЦП і пам'яті для цієї версії нижче, ніж аналогічні вимоги щодо протоколу Rapid PVST +, але вище, ніж для протоколу RSTP.

Для комутаторів Cisco Catalyst за замовчуванням використовується режим протоколу spanning-tree PVST +, включений на всіх портах. PVST + характеризується істотно більш повільним сходженням після зміни топології, ніж Rapid PVST +.

Примітка. Важливо відрізняти застарілий стандарт IEEE 802.1D-1998 (і більш ранні версії) від стандарту IEEE 802.1D-2004. IEEE 802.1D-2004 включає в себе функцію RSTP, а стандартом IEEE 802.1D-1998 називається вихідна реалізація алгоритму протоколу spanning-tree. Пізніші моделі комутаторів Cisco, на яких працюють нові версії IOS (наприклад комутатори Catalyst 2960 з IOS 15.0), за замовчуванням використовують PVST +, проте містять багато характеристик стандарту IEEE 802.1D-1998 у цьому режимі (наприклад, альтернативні порти замість колишніх непризначених портів) . Однак для використання швидкого протоколу spanning-tree на такому комутаторі його необхідно явно налаштувати для роботи в режимі швидкого протоколу spanning-tree.

Характеристики протокола STP

Протокол	Стандарт	Требуемые ресурсы	Сходимость	Расчёт дерева
STP	802.1D	Низкая	Медленная	Все сети VLAN
PVST+	Cisco	Высокая	Медленная	На VLAN
RSTP	802.1w	Средняя	Быстрая	Все сети VLAN
Rapid PVST+	Cisco	Очень высокая	Быстрая	На VLAN
MSTP	802.1s, Cisco	Средняя или высокая	Быстрая	На экземпляр

Рис. 5.1.28

Вихідний стандарт 802.1D визначає протокол загальних spanning-tree (CST), який має на увазі використання тільки одного примірника протоколу spanning-tree у всій коммутуючої мережі незалежно від кількості VLAN. Мережа, що використовує CST, має наступні характеристики:

Розподіл навантаження не підтримується. Один висхідний канал повинен блокувати всі мережі VLAN.

Ресурси ЦП використовуються економно. Потрібно обчислення тільки одного примірника протоколу spanning-tree.

Корпорація Cisco розробила протокол PVST + таким чином, щоб мережа могла використовувати незалежний екземпляр реалізації стандарту IEEE 802.1D для кожної мережі VLAN в межах мережі. PVST + дозволяє одному транкові порту на комутаторі блокувати окрему мережу VLAN, що не блокуючи при цьому інші мережі VLAN. PVST + можна використовувати для розподілу навантаження на 2 рівні. Оскільки всі мережі VLAN використовують окремий екземпляр STP, комутаторів в середовищі PVST + потрібен більший обсяг ресурсів ЦП і смуги пропускання BPDU, ніж в стандартній реалізації CST протоколу STP.

У середовищі PVST + параметри протоколу spanning-tree можна налаштувати таким чином, щоб половина мереж VLAN виконувала пересилку по всьому транкових каналах. На малюнку порт F0 / 3 на комутаторі S2 є портом, що забезпечує передачу даних для мережі VLAN 20, а порт F0 / 2 на комутаторі S2 - є портом, що забезпечує передачу даних для мережі VLAN 10. Для цього потрібно налаштувати комутатори таким чином, щоб один був обраний в якості кореневого моста для половини мереж VLAN в межах мережі, а другий - в якості кореневого моста для решти мереж VLAN. На малюнку комутатор S3 є кореневим мостом для мережі VLAN 20, а S1 є кореневим мостом для мережі VLAN 10. Кілька кореневих мостів STP в одній мережі VLAN дозволяють збільшити обсяг надмірності в мережі.

Мережі під керуванням PVST + мають наступні характеристики:

Підтримується оптимальний розподіл навантаження.

Підтримка одного примірника протоколу spanning-tree для кожної мережі VLAN може привести до значного необгрунтованого споживання ресурсів ЦП для всіх комутаторів в мережі (крім ресурсів смуги пропускання, що використовуються для відправки власних кадрів BPDU кожним з примірників). Це небажано тільки в тому випадку, якщо налаштоване велику кількість мереж VLAN.

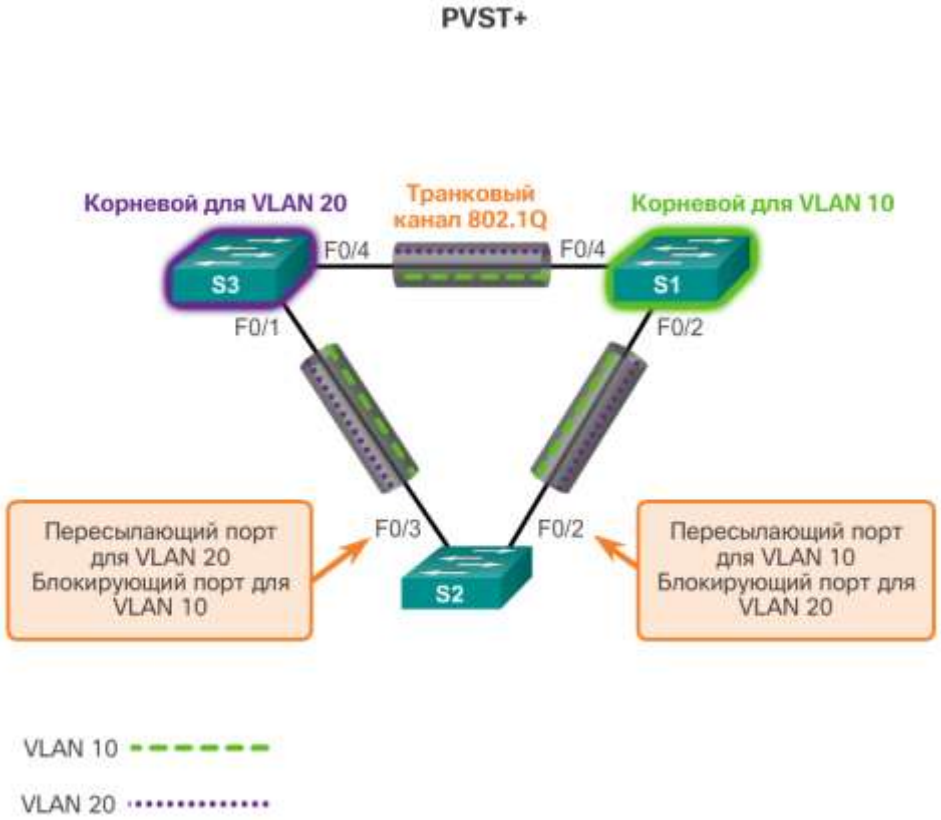


Рис. 5.1.29

Протокол STP спрощує створення логічного бездротового шляху по домену широкомовної розсилки. Протокол spanning-tree визначається за допомогою даних, отриманих в процесі обміну кадрами BPDU між з'єднаними між собою комутаторами. Щоб спростити процес отримання логічного протоколу spanning-tree, кожен порт комутатора проходить через п'ять можливих станів порту і три таймера BPDU.

Відразу після завантаження комутатора починається побудова протоколу spanning-tree. Якщо порт комутатора переходить безпосередньо зі стану блокування в стан пересилання, не використовуючи під час переходу дані про повну топології, порт може тимчасово створювати петлю даних. Саме тому протокол STP використовує п'ять станів портів. На малюнку представлені стану портів, що забезпечують відсутність петель, при формуванні логічного протоколу spanning-tree

Блокування: порт є альтернативним і не бере участі в пересилання кадрів. Порт приймає кадри BPDU, щоб визначити місце розташування і ідентифікатор кореневого моста, а також ролі порту, що виконуються кожним з портів комутатора в кінцевій активної топології STP.

Прослуховування: прослуховування шляху до кореневого мосту. Протокол STP визначив, що порт може брати участь у пересиланні кадрів відповідно до

кадрами BPDU, які комутатор прийняв до цього моменту. На цьому етапі порт комутатора не тільки приймає кадри BPDU, але також передає свої власні кадри BPDU і повідомляє суміжних комутаторів про те, що порт комутатора готується до участі в активній топології.

Вивчення: вивчення MAC-адрес. На етапі підготовки до пересилання кадрів порт починає заповнювати таблицю MAC-адрес.

Пересилання: порт вважається частиною активної топології. Він пересилає кадри даних, відправляє і приймає кадри BPDU.

Відключений: порт 2 рівня не бере участі в протоколі spanning-tree і не пересилає кадри. Відключене стан встановлюється в тому випадку, якщо порт комутатора відключений адміністратором.

Зверніть увагу, що число портів в кожному з станів (блокування, прослуховування, отримання даних або пересилання) можна відобразити за допомогою команди show spanning-tree summary.

Для забезпечення логічної бездротової топології мережі для кожної мережі VLAN в комутованій мережі протокол PVST + виконує чотири дії:

1. Вибір одного кореневого моста: тільки один комутатор може виступати в ролі кореневого моста (для даної мережі VLAN). Кореневої міст - це комутатор з найменшим значенням ідентифікатора моста. Всі порти на кореневому мосту є призначеними (зокрема, відсутні кореневі порти).

2. Вибір кореневого порту на кожному некореневим мосту: протокол STP встановлює один кореневий порт на кожному некореневим мосту. Кореневої порт є шляхом з найменшою вартістю від некореневого моста до кореневого мосту, вказуючи оптимальний шлях до кореневого мосту. Як правило, кореневі порти знаходяться в режимі пересилання.

3. Вибір призначеного порту в кожному сегменті: у кожному каналі протокол STP встановлює один виділений порт. Призначений порт вибирається на комутаторі, який надає маршрут з найменшою вартістю до кореневого мосту. Як правило, призначені порти знаходяться в режимі пересилання і виконують пересилання трафіку для сегмента.

4. Решта порти в комутованій мережі є альтернативними: альтернативні порти, як правило, залишаються в стані блокування, що дозволяє логічно розірвати дротову топологію. Коли порт знаходиться в стані блокування, він не пересилає трафік, але як і раніше може обробляти отримані повідомлення BPDU.

Состояния портов

	Состояние порта				
Операция разрешена	**Блокировка**	**Прослушивание**	**Обучение**	**Пересылка**	**Отключён**
Может получать и обрабатывать BPDU	ДА	ДА	ДА	ДА	НЕТ
Может пересылать кадры данных, полученных на интерфейс	НЕТ	НЕТ	НЕТ	ДА	НЕТ
Может пересылать кадры данных, полученные из другого интерфейса	НЕТ	НЕТ	НЕТ	ДА	НЕТ
Может получать данные MAC-адресов	НЕТ	НЕТ	ДА	ДА	НЕТ

Рис. 5.1.30

Розширений ідентифікатор системи і роботи PVST +

У середовищі PVST + розширений ідентифікатор комутатора забезпечує унікальний ідентифікатор BID для кожного комутатора в кожній з мереж VLAN.

Наприклад, мережа VLAN 2 буде використовувати ідентифікатор BID за замовчуванням 32770 (пріоритет 32768 плюс розширений ідентифікатор системи 2). Якщо пріоритет не заданий, комутатори будуть використовувати однакове значення пріоритету за умовчанням, і вибір кореневого моста для кожної мережі VLAN буде виконуватися на основі MAC-адреси. Цей метод служить для довільного вибору кореневого моста.

В окремих випадках адміністратор може вибрати окремий комутатор в якості кореневого моста. Тому може бути безліч причин, серед яких більш централізоване розташування комутатора в моделі мережі LAN, більш висока потужність обробки комутатора або просто більш зручний доступ і віддалене управління для даного комутатора. Для управління процесом вибору кореневого моста слід просто призначити більш низький пріоритет комутатора, який повинен бути обраний як кореневого моста.

Рис. 5.1.31

RSTP (IEEE 802.1w) є розвитком вихідного стандарт 802.1D; він включений в стандарт IEEE 802.1D-2004. Термінологія, що відноситься до STP 802.1w, залишається в основному тієї ж, що і для вихідного стандарту STP IEEE 802.1D. Більшість параметрів залишаються колишніми, тому користувачі, знайомі із STP, зможуть без проблем налаштувати новий протокол. Rapid PVST + - це просто реалізація RSTP корпорації Cisco для кожної окремої мережі VLAN. У Rapid PVST + для кожної мережі VLAN запускається самостійний примірник протоколу RSTP.

На малюнку показана мережа під керуванням RSTP. S1 є кореневим мостом з двома призначеними портами в стані пересилання. RSTP підтримує новий тип порту: порт F0 / 3 на комутаторі S2 є альтернативним портом в стані відкидання. Зверніть увагу, що відсутні порти, що працюють в режимі блокування. У протоколі RSTP немає стану блокування порту. Протокол RSTP визначає наступні стани портів: відкидання, вивчення чи пересилання.

Протокол RSTP прискорює повторний розрахунок протоколу spanning-tree в разі зміни топології мережі 2 рівня. В має бути діюча мережі RSTP може досягти стану збіжності набагато швидше, іноді всього за кілька сот мілісекунд. Протокол RSTP повторно визначає типи портів і їх стану. Якщо порт налаштований в якості альтернативного або резервного, він може негайно перейти в стан пересилання, не чекаючи сходження мережі. Далі подано короткий опис характеристик RSTP.

RSTP найбільш прийнятний протоколом, що дозволяє уникнути виникнення петель 2 рівня в комутованій мережі. Багато відмінності обумовлені пропрієтарними удосконаленнями Cisco вихідного стандарту 802.1D. Такі удосконалення, як кадри BPDU, які містять і відправляють дані про ролях портів тільки сусіднім комутаторів, не вимагають додаткової

настройки і, як правило, працюють краще, ніж більш ранні пропрієтарні версії Cisco. Тепер вони прозорі і інтегровані в стандартну роботу протоколу.

Пропрієтарні удосконалення Cisco для вихідного стандарту 802.1D, наприклад, функції UplinkFast і BackboneFast, не сумісні з протоколом RSTP.

Протокол RSTP (802.1w) замінює собою вихідний стандарт 802.1D, підтримуючи при цьому функції забезпечення сумісності. Зберігається велика частина термінології, що відноситься до початкового стандарту 802.1D, і більшість параметрів залишаються незмінними. Крім того, 802.1w підтримує повернення до більш ранньої версії 802.1D, що забезпечує взаємодію з попередніми моделями комутаторів на окремих портах. Наприклад, алгоритм протоколу spanning-tree RSTP вибирає кореневої міст точно так же, як і вихідна версія 802.1D.

RSTP зберігає ті ж формати BPDU, що і вихідний IEEE 802.1D, за винятком того, що в поле версії встановлено значення 2, що вказує на протокол RSTP, а поле прапорів задіє всі 8 біт.

Протокол RSTP може активно підтвердити можливість безпечного переходу порту в стан пересилання, не покладаючись на конфігурацію таймера.

Что такое RSTP?

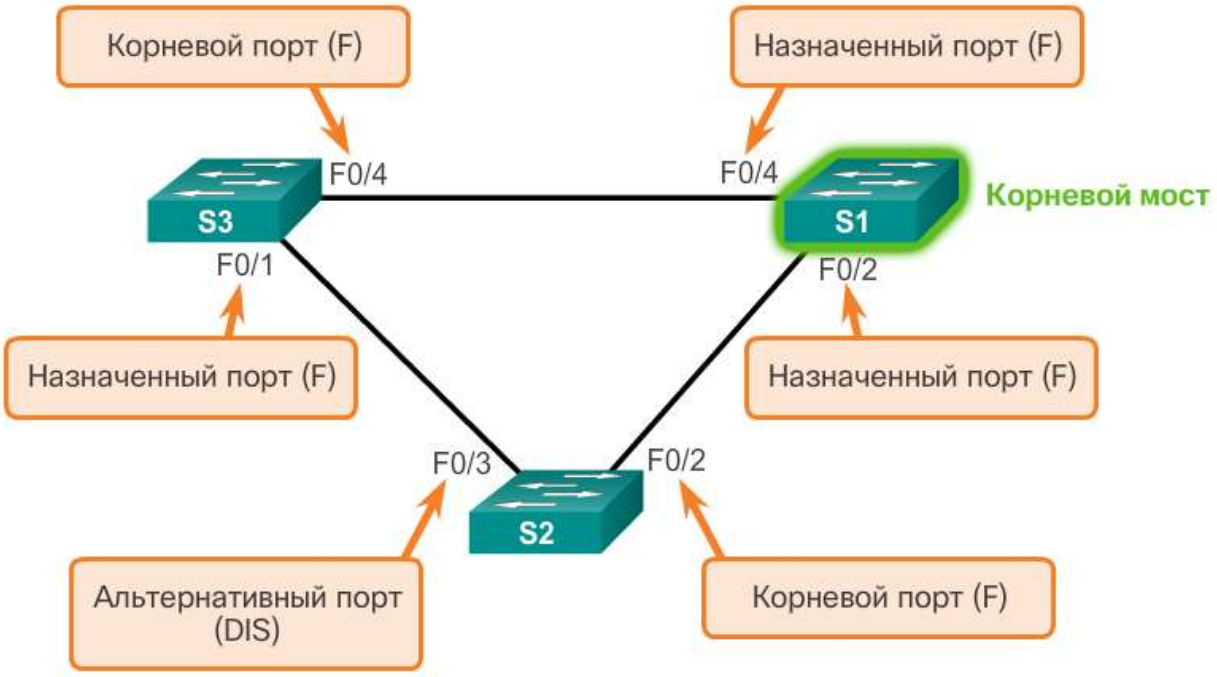


Рис. 5.1.32

Протокол RSTP використовує BPDU типу 2 версії 2. Вихідний стандарт 802.1D використовується BPDU типу 0 версії 0. Проте, комутатор під керуванням RSTP може здійснювати обмін даними безпосередньо з комутатором під керуванням вихідного протоколу STP 802.1D. Протокол RSTP відправляє кадри BPDU і заповнює байт прапора трохи інакше, ніж вихідний стандарт 802.1D:

Дані протоколу на порте можуть втратити свою актуальність відразу ж, якщо пакети вітання не прийняті три рази поспіль (за замовчуванням - протягом шести секунд) або після закінчення максимального часу існування.

Оскільки BPDU використовується в якості механізму keepalive, три поспіль пропущених BPDU вказують на втрату з'єднання між мостом і його сусіднім кореневих мостом або виділеним мостом. Швидке старіння даних дозволяє швидко виявляти збої.

Примітка. Як і комутатор під керуванням STP, комутатор RSTP відправляє BPDU, що містить поточні дані, протягом кожного періоду вітання (за замовчуванням - дві секунди), навіть в тому випадку, якщо міст RSTP не приймає ніяких BPDU від кореневого моста.

Як показано на малюнку, протокол RSTP використовує байт прапора BPDU версії 2:

Біти 0 і 7 використовуються для зміни топології і підтвердження їх надходження в вихідний 802.1D.

Біти 1 і 6 використовуються для процесу узгодження пропозиції (для швидкого сходження).

Біти з 2 по 5 виконують кодування ролі і стану порту.

Біти 4 і 5 використовуються для кодування ролі порту з використанням 2-бітного коду.

Рис. 5.1.33

Прикордонний порт під керуванням RSTP є порт комутатора, який ніколи не планується підключати до інших пристроїв комутації. Після включення він відразу ж переходить в стан пересилки.

Концепція прикордонного порту RSTP відповідає функції PVST + PortFast. Прикордонний порт безпосередньо підключений до кінцевої станції і

передбачає, що до нього не підключено ні один з пристроїв комутації. Прикордонні порти RSTP повинні негайно перейти в стан пересилання, пропускаючи, таким чином, стану прослуховування і вивчення вихідного 802.1D, які займають багато часу.

Реалізація RSTP Cisco, Rapid PVST + підтримує використання ключового слова PortFast за допомогою команди налаштування граничного порту spanning-tree portfast. Таким чином, перехід від STP до RSTP здійснюється без проблем.

Рис. 5.1.34

На рис. 1 показані приклади портів, які можна налаштувати в якості граничних. На рис. 2 показані приклади портів, відмінних від граничних.

Рис. 5.1.35

Примітка. Не рекомендується налаштовувати граничні порти, які будуть з'єднані з іншим комутатором. Це може мати негативні наслідки для RSTP, оскільки з'являється можливість виникнення тимчасової петлі, що приводить до затримки сходження RSTP.

Типи каналів

Тип каналу дозволяє розподілити за категоріями кожен порт, який бере участь в RSTP на основі дуплексного режиму порту. Залежно від того, які пристрої підключені до кожного з портів, можна виділити два різних типи каналів:

Точка-точка: порт, який працює в повнодуплексному режимі; як правило, з'єднує два комутатора і є кандидатом на швидкий перехід в стан пересилки.

Загальний: порт, який працює в напівдуплексному режимі; з'єднує комутатор з концентратором, що об'єднує кілька пристроїв.

На малюнку клацніть кожну з посилань, щоб дізнатися про різні типи каналів.

Тип каналу дозволяє визначити, чи може порт відразу перейти в стан пересилання за умови виконання певних умов. Для граничних і не прикордонні портів потрібні різні умови. Не прикордонні порти розподіляються за категоріями в двох типах каналів («точка-точка» і «загальний»). Тип каналу визначається автоматично, але його можна перевизначити за допомогою явної конфігурації порту, використовуючи команду spanning-tree link-type parameter.

Підключення до граничного порту і з'єднання «точка-точка» претендують на швидкий перехід в стан пересилки. Проте, перш ніж розглядати параметр типу каналу, RSTP повинен визначити роль порту. До характеристик ролей порту з урахуванням типів каналу відносяться наступні:

кореневі порти не використовують параметр типу каналу; кореневі порти можуть здійснювати швидкий перехід в стан пересилки після синхронізації порту;

альтернативні та резервні порти в більшості випадків не використовують параметр типу каналу;

призначені порти максимально ефективно використовують параметр типу каналу. Швидкий перехід в стан пересилки для призначеного порту виконується тільки в тому випадку, якщо для параметра типу каналу встановлено значення point-to-point.

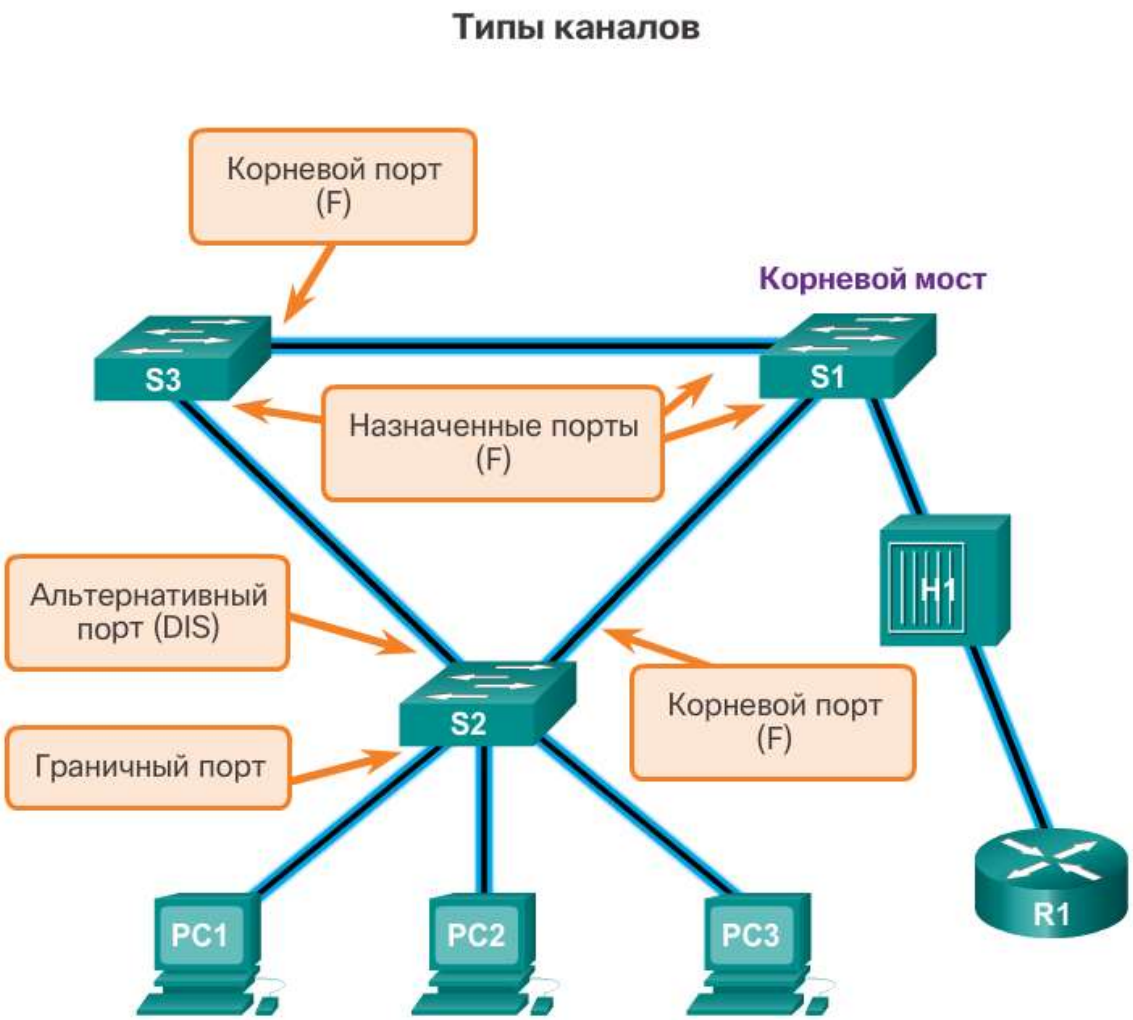


Рис. 5.1.36

У таблиці наведено конфігурація протоколу spanning-tree за замовчуванням для комутатора Cisco Catalyst 2960 Series. Зверніть увагу, що для протоколу spanning-tree за замовчуванням використовується режим PVST+.

Якщо адміністратор планує налаштувати окремий комутатор в якості кореневого моста, значення пріоритету моста необхідно скоригувати таким чином, щоб воно було нижче значень пріоритету моста для всіх інших комутаторів в мережі. Існує два різних методу налаштування значення пріоритету моста для комутаторів Cisco Catalyst.

Метод 1

Щоб налаштувати для комутатора найменше значення пріоритету моста, можна використовувати команду глобального режиму конфігурації spanning-tree vlan vlan-id root primary. Пріоритет комутатора налаштовується за використанням попередньо певного значення 24576 або найбільшого значення, кратного 4096, яке менше найнижчого значення пріоритету моста, виявленого в мережі.

Якщо потрібно альтернативний кореневої міст, слід використовувати команду глобального режиму конфігурації spanning-tree vlan vlan-id root secondary. Ця команда задає для комутатора попередньо певне значення пріоритету 28672. Таким чином, альтернативний комутатор стає кореневим мостом в разі відмови основного кореневого моста. При цьому мається на увазі,

що для інших комутаторів в мережі визначено значення пріоритету за умовчанням 32768

На рис. 1 комутатор S1 призначений в якості основного кореневого моста за допомогою команди spanning-tree vlan 1 root primary, а комутатор S2 в якості допоміжного кореневого моста за допомогою команди spanning-tree vlan 1 root secondary.

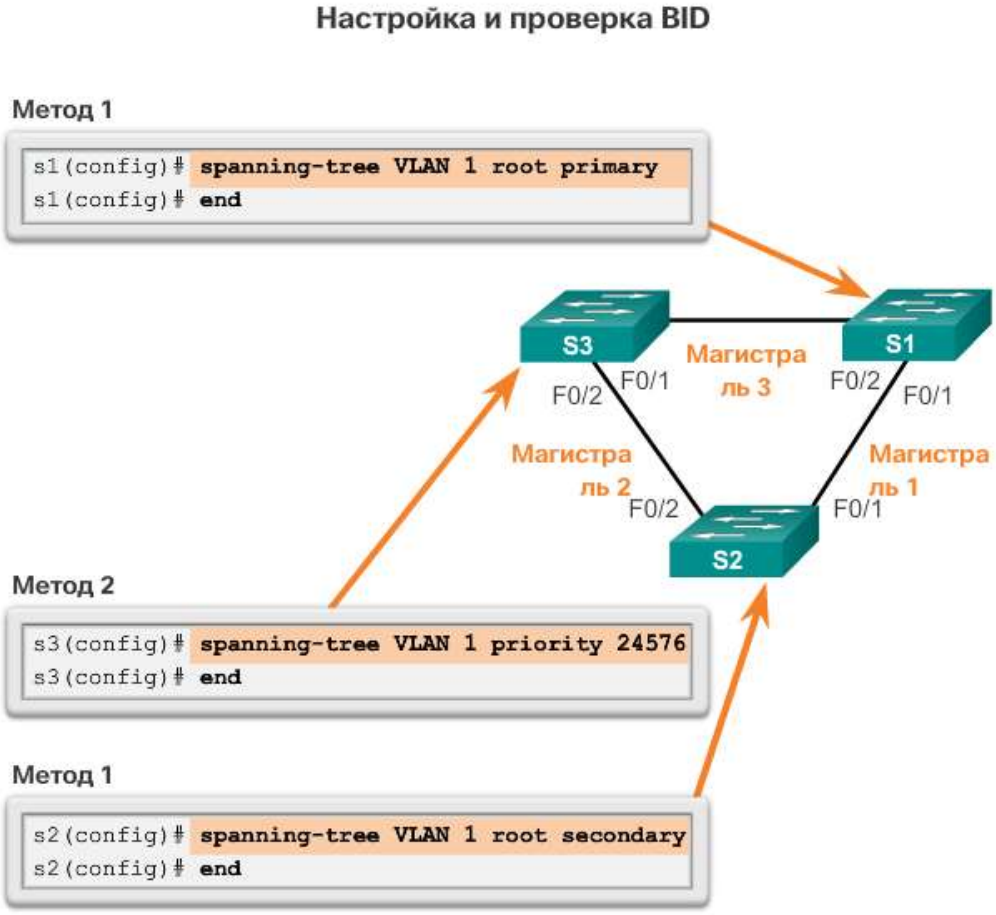


Рис. 5.1.37

Метод 2

Налаштувати значення пріоритету порту також можна за допомогою команди глобального режиму конфігурації spanning-tree vlan vlan-id priority value. Ця команда забезпечує більш ретельний контроль значення пріоритету моста. Значення пріоритету налаштовується за кроком в 4096 в діапазоні від 0 до 61440.

У цьому прикладі комутатора S3 присвоєно значення пріоритету моста 24576 за допомогою команди spanning-tree vlan 1 priority 24576

Щоб перевірити пріоритет моста для комутатора, використовуйте команду show spanning-tree. На рис. 2 для комутатора заданий пріоритет 24576. Також зверніть увагу, що комутатор призначений в якості кореневого моста для примірника протоколу spanning-tree.

Настройка и проверка BID

```
S3# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     00A.0033.3333
              This bridge is the root
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID   Priority    24577  (priority  24576  sys-id-ext  1)
              Address     000A.0033.3333
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time  300

Interface     Role    Sts    Cost     Prio.Nbr      Type
------------  -----   ----   -----    ----------    ------
Fa0/1         Desg    FWD    4        128.1         p2p
Fa0/2         Desg    FWD    4        128.2         p2p
S3#
```

Рис. 5.1.38

Виконайте вправу з перевіркою синтаксису на рис. 3, щоб налаштувати комутатори S1, S2 і S3. Використовуючи описаний вище метод 2, вручну налаштуйте комутатор S3 зі значенням пріоритету 24576 для мережі VLAN 1. Використовуючи метод 1, налаштуйте S2 в якості допоміжної кореневої мережі VLAN 1 і S1 в якості основної кореневої мережі VLAN 1. Перевірте конфігурацію за допомогою команди show spanning- tree на комутаторі S1.

PortFast є функцією Cisco для середовищ PVST +. Якщо порт комутатора налаштований за допомогою функції PortFast, то такий порт відразу переходить зі стану блокування в стан пересилання, минаючи стандартні стану переходу STP 802.1D (стану прослуховування та завантаження даних). Замість того, щоб очікувати сходження протоколу STP IEEE 802.1D в кожній мережі VLAN, PortFast можна використовувати на портах доступу для забезпечення негайного підключення цих пристроїв до мережі. Портами доступу є порти, підключені до однієї робочої станції або сервера.

У допустимої конфігурації PortFast прийом кадрів BPDU ніколи не допускається, оскільки це вказувало б на те, що до порту підключений інший міст або комутатор, а це може привести до виникнення петлі протоколу spanning-tree. Комутатори Cisco підтримують функцію BPDU guard. Коли функція BPDU guard включена, вона переводить порт в стан відключення через помилку при отриманні BPDU. Це дозволяє виключити порт. Функція BPDU guard забезпечує безпечний відгук на неприпустимі конфігурації, щоб ви могли вручну повторно підключити інтерфейс.

Технологію Cisco PortFast рекомендується використовувати для DHCP. Без PortFast комп'ютер може відправити запит DHCP до переходу порту в стан пересилання, забороняючи вузлу отримувати придатний для використання IP-адресу та інші дані. Оскільки PortFast відразу ж змінює стан на стан пересилання, комп'ютер завжди отримує придатний для використання IP-адресу.

Примітка. Оскільки PortFast призначений для мінімізації часу очікування портами доступу сходження протоколу spanning-tree, цю функцію рекомендується використовувати тільки на портах доступу. Якщо функція PortFast включена на порте, підключеному до іншого комутатора, виникне ризик виникнення петлі протоколу spanning-tree.

PortFast и BPDU Guard

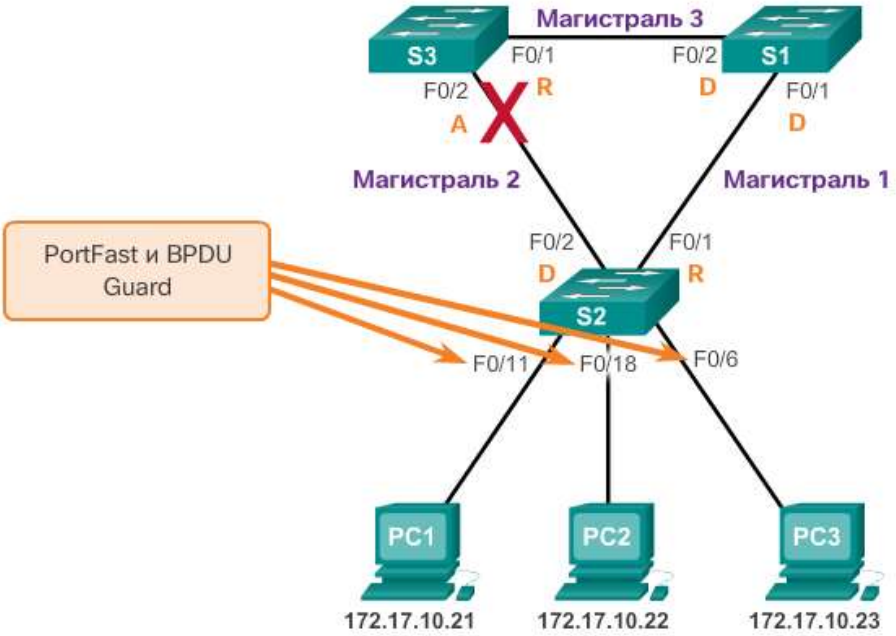


Рис. 5.1.39

Щоб налаштувати на порте комутатора PortFast, виконайте команду режиму конфігурації інтерфейсу spanning-tree portfast на кожному інтерфейсі, для якого потрібно включити PortFast, як показано на рис 2. Команда глобального режиму конфігурації spanning-tree portfast default використовується для включення PortFast на всіх нетранкових інтерфейсах.

Конфигурация PortFast и BPDU

```
S2(config)# interface FastEthernet 0/11
S2(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to
a single host. Connecting hubs, concentrators, switches,
bridges, etc... to this interface  when portfast is enabled,
can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
 have effect when the interface is in a non-trunking mode.
S2(config-if)# spanning-tree bpduguard enable
S2(config-if)# end
```

Рис. 5.1.40

Щоб налаштувати BPDU guard на порте доступу 2 рівня, використовуйте команду режиму конфігурації інтерфейсу spanning-tree bpduguard enable.

Команда глобального режиму конфігурації spanning-tree portfast bpduguard default включає BPDU guard на всіх портах з підтримкою PortFast.

Щоб перевірити, чи включений PortFast і BPDU для порту комутатора, використовуйте команду show running-config, як показано на рис. 3. PortFast і BPDU за замовчуванням відключені на всіх інтерфейсах.

PortFast и BPDU Guard

```
S2# show running-config interface f0/11
Building configuration...

Current configuration : 90 bytes
!
interface FastEthernet0/11
 spanning-tree portfast
 spanning-tree bpduguard enable
end

S2#
```

Рис. 5.1.41

Виконайте вправу з перевіркою синтаксису на рис. 4, щоб налаштувати і перевірити комутатори S1 і S2 з підтримкою PortFast і BPDU guard.

У топології на рис. 1 показані три комутатора з транки 802.1Q між ними. Існують дві мережі VLAN (VLAN 10 і VLAN 20), які налаштовуються на цих каналах як транків. Необхідно налаштувати S3 в якості кореневого моста для мережі VLAN 20, а S1 - як кореневого моста для мережі VLAN 10. Порт F0 / 3 на S2 є пересилати портом для мережі VLAN 20 і блокуючим портом для мережі VLAN 10. Порт F0 / 2 на S2 є пересилати портом для мережі VLAN 10 і блокуючим портом для мережі VLAN 20.

Крім встановлення кореневого моста, також можна встановити резервний кореневої міст. Резервний кореневої міст - це комутатор, який може стати кореневим мостом для мережі VLAN при відмові основного кореневого моста. За умови, що інші мости в мережі VLAN зберігають свій пріоритет STP за замовчуванням, цей комутатор стає кореневим мостом в разі збою основного кореневого моста.

Для настройки PVST + в цьому прикладі топології слід виконати наступні дії:

Крок 1. Виберіть комутатори, які повинні стати основними і резервними кореневими мостами для кожної з мереж VLAN. Наприклад, на рис. 1 комутатор S3 є основним мостом для мережі VLAN 20, а S1 є резервним мостом для мережі VLAN 20.

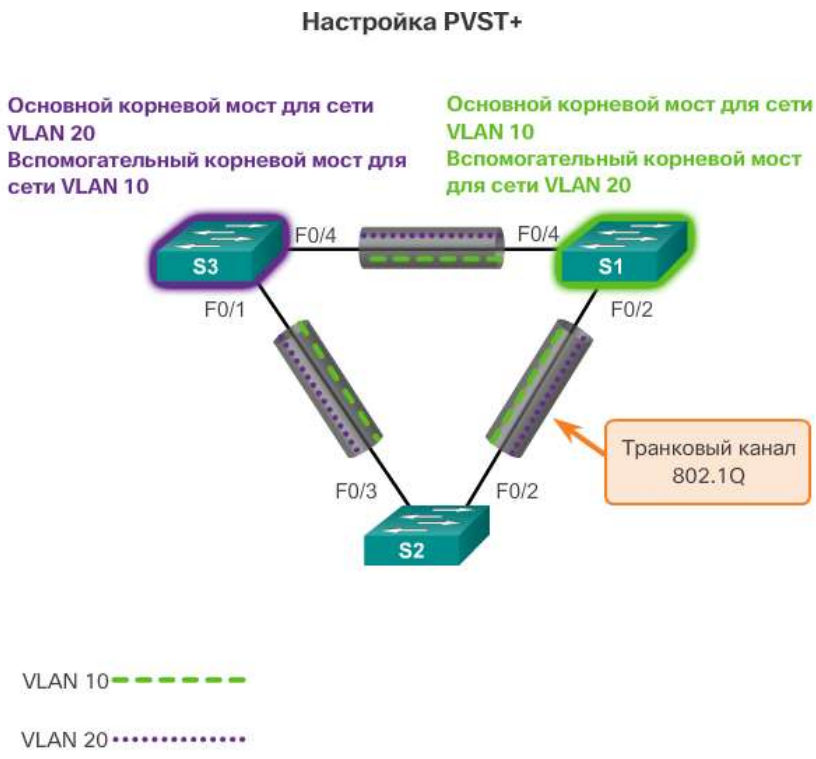


Рис. 5.1.42

Крок 2. Налаштуйте комутатор в якості основного моста для мережі VLAN, використовуючи для цього команду spanning-tree vlan number root primary, як показано на рис. 2.

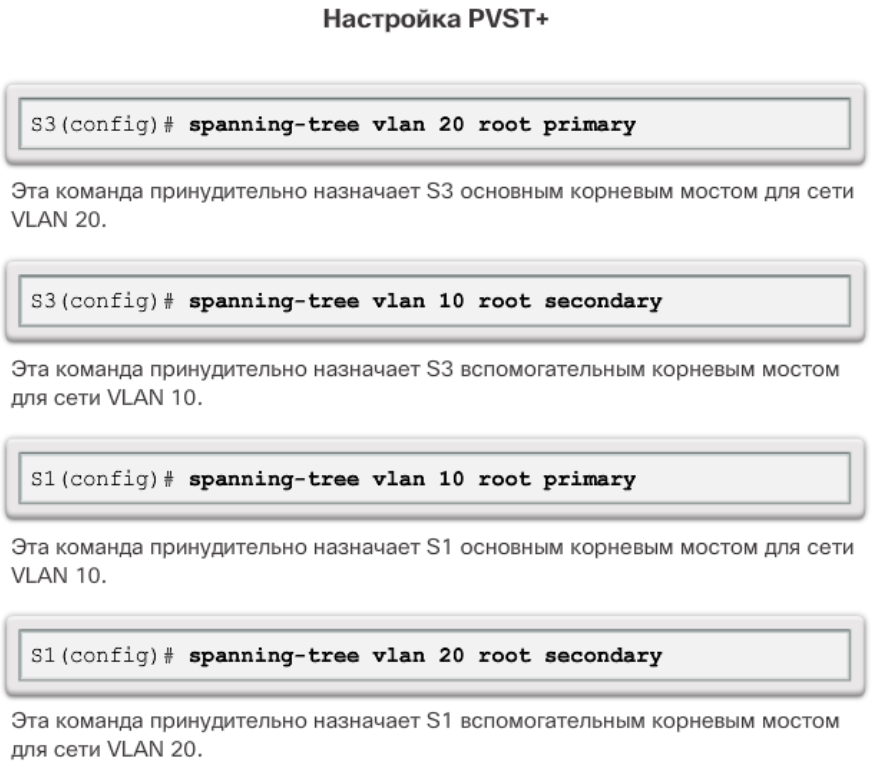


Рис. 5.1.43

Крок 3. Налаштуйте комутатор в якості резервного моста для мережі VLAN, використовуючи для цього команду spanning-tree vlan number root secondary.

Також кореневої міст можна задати, встановивши найнижче значення пріоритету протоколу spanning-tree на кожному комутаторі, щоб цей комутатор був обраний в якості основного моста для пов'язаної з ним мережі VLAN.

Зверніть увагу, що на рис. 2 комутатор S3 налаштований в якості основного кореневого моста для мережі VLAN 20, а комутатор S1 в якості основного кореневого моста для мережі VLAN 10. Комутатор S2 зберігає свій пріоритет STP за замовчуванням.

На малюнку також показано, що комутатор S3 налаштований в якості резервного кореневого моста для мережі VLAN 10, а S1 налаштований як допоміжний кореневого моста для мережі VLAN 20. Ця конфігурація забезпечує розподіл навантаження протоколу spanning-tree, при якому трафік мережі VLAN 10 проходить через комутатор S1, а трафік мережі VLAN 20 проходить через S3.

Для призначення кореневого моста, можна встановити найнижче значення пріоритету протоколу spanning-tree на кожному комутаторі, щоб цей комутатор був обраний в якості основного моста для пов'язаної з ним мережі VLAN, як показано на рис. 3. Пріоритет комутатора можна задати для будь-якого примірника протоколу spanning-tree. Ця установка визначає ймовірність вибору комутатора в якості кореневого моста. Чим нижче значення, тим вище ймовірність вибору цього комутатора. Значення встановлюються в діапазоні від 0 до 61440 з кроком 4096; всі інші значення відхиляються. Наприклад, допустимим є значення пріоритету 4096 x 2 = 8192.

Рис. 5.1.44

Як показано на рис. 4, команда show spanning-tree active дозволяє відобразити відомості про конфігурацію протоколу spanning-tree тільки для активних інтерфейсів. Вихідні дані відносяться до S1, налаштованому за допомогою PVST +. Існує ряд параметрів команди Cisco IOS, пов'язаних з командою show spanning-tree.

Настройка PVST+

```
S1# show spanning-tree active

<выходные данные опущены>
VLAN0010
   Spanning tree enabled protocol ieee
   Root ID     Priority    4106
               Address     0019.aa9e.b000
               This bridge is the root
               Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
   Bridge ID   Priority    4106  (priority  4096  sys-id-ext  10)
               Address     0019.aa9e.b000
               Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
               Aging Time  300

Interface       Role    Sts    Cost     Prio.Nbr      Type
------------    -----   ----   -----    ----------    ------
Fa0/2           Desg    FWD    19        128.2         p2p
Fa0/4           Desg    FWD    19        128.4         p2p

<выходные данные опущены>
```

Рис. 5.1.45

У вихідних даних на рис. 5 показано, що пріоритет для мережі VLAN 10 дорівнює 4096, що є найменшим з значень пріоритету для трьох відповідних мереж VLAN.

Настройка PVST+

```
S1# show running-config
Building configuration...

Current configuration : 1595 bytes
!
version 12.2
 <выходные данные опущены>
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
!
 <выходные данные опущены>
```

Рис. 5.1.46

Виконайте вправу з перевіркою синтаксису на рис. 6, щоб налаштувати і перевірити протокол spanning-tree для S1 і S3.

Протоколи spanning-tree забезпечують фізичну Надлишковість в комутованій мережі. Проте, вузол на рівні доступу ієрархічної мережі також ефективно використовує альтернативні шлюзи за замовчуванням. У разі збою маршрутизатора або інтерфейсу маршрутизатора (який виступає в якості шлюзу), вузол, для якого налаштовано використання цього шлюзу, ізолюється від зовнішніх мереж. Потрібно механізм для надання альтернативних шлюзів за замовчуванням в комутованих мережах, де два або більше маршрутизаторів підключені до одних і тих же мереж VLAN.

Примітка. В рамках обговорення забезпечення надмірності маршрутизатора, ми не робимо функціональне розходження між багаторівневим комутатором і маршрутизатором на рівні розподілу. На практиці багаторівневі комутатори часто виступають в ролі шлюзу для всіх мереж VLAN в комутованій мережі. Дане обговорення зосереджено на функціях маршрутизації, незалежно від того, яке використовується фізичний пристрій.

У комутованої мережі всі клієнти отримують тільки один шлюз за замовчуванням. Немає способів настройки допоміжного шлюзу, навіть якщо існує другий шлях для передачі пакетів з локального сегмента.

На малюнку R1 відповідає за маршрутизацію пакетів від PC1. У разі недоступності R1 протоколи маршрутизації виконують динамічне сходження. Тепер R2 маршрутизує пакети із зовнішніх мереж, які повинні були пройти через R1. Проте, трафік з внутрішньої мережі, пов'язаний з R1, включаючи трафік з робочих станцій, серверів і принтерів, для яких R1 налаштований в якості шлюзу за замовчуванням, до сих пір відправляється на R1 і скидається.

Кінцеві пристрої, як правило, налаштовуються з одним IP-адресою для шлюзу. Ця електронна адреса не змінюється при зміні топології мережі. Якщо IP-адреса шлюзу недоступний, локальний пристрій не може відправляти пакети з локального сегмента мережі, що за фактом відключає цей пристрій від решти мережі. Навіть при наявності надлишкового маршрутизатора, який може виступати в якості шлюзу для цього сегмента, динамічний метод, за допомогою якого ці пристрої можуть визначати адресу нового шлюзу, недоступний.

Рис. 5.1.47

Надлишковість маршрутизаторів

Одним із способів для усунення єдиної точки відмови на шлюзі за замовчуванням є реалізація віртуального маршрутизатора. Для реалізації цього типу надмірності маршрутизатора кілька маршрутизаторів налаштовуються для спільної роботи, що створює ілюзію одного маршрутизатора на вузлах мережі LAN, як показано на малюнку. При спільному використанні IP-адреси і MAC-адреси два або більше маршрутизаторів можуть працювати, як один віртуальний маршрутизатор.

IP-адреса віртуального маршрутизатора налаштовується в якості шлюзу за замовчуванням для робочих станцій в окремому сегменті IP. При відправці кадрів з кінцевих пристроїв на шлюз вузли використовують ARP для вирішення MAC-адреси, пов'язаного з IP-адресою шлюзу. За допомогою протоколу ARP визначається MAC-адресу віртуального маршрутизатора. Після цього кадри, які відправлені на MAC-адресу віртуального маршрутизатора, можна обробити фізично за допомогою поточного активного маршрутизатора в межах групи віртуального маршрутизатора. Протокол використовується для визначення двох або більше маршрутизаторів в якості пристроїв, що відповідають за обробку кадрів, що відправляються на MAC- або IP-адреса одного віртуального маршрутизатора. Кінцеві пристрої відправляють трафік на адреси віртуального маршрутизатора. Фізичний маршрутизатор, який пересилає цей трафік, є прозорим для кінцевих пристроїв.

Протокол резервування надає механізм для визначення маршрутизатора, який повинен виконувати активну роль в пересиланні трафіку. Він також визначає, коли роль пересилання повинна перейти до надмірного маршрутизатора. Перехід від одного ретранслює маршрутизатора до іншого є прозорим для кінцевих пристроїв.

Здатність мережі динамічно відновлюватися після збою пристрою, що виконує функцію шлюзу, називається Надлишковістю на першому хопі.

Рис. 5.1.48

Дії при перемиканні в разі відмови маршрутизатора

У разі збою активного маршрутизатора протокол резервування переводить резервний маршрутизатор на нові функції активного маршрутизатора. У разі збою активного маршрутизатора відбувається наступне.

1. Резервний маршрутизатор перестає бачити повідомлення вітання від ретранслює маршрутизатора.

2. Резервний маршрутизатор приймає роль передавального маршрутизатора.

3. Оскільки новий пересилає маршрутизатор використовує як IP-адреса, так і MAC-адресу віртуального маршрутизатора, кінцеві пристрої не помічають перебоїв в обслуговуванні.

Рис. 5.1.49

У наступному списку перераховані доступні параметри для протоколів забезпечення надмірності на першому хопі (FHRP), як показано на малюнку.

Протокол резервування (Hot Standby Router Protocol, HSRP). Є пропрієтарним протоколом Cisco, який призначений для забезпечення наскрізного перемикання IPv4-пристрої першого переходу. Протокол HSRP забезпечує високу доступність мережі завдяки наданню функцій забезпечення надмірності для маршрутизації на першому хопі для IPv4-вузлів у мережах, налаштованих з використанням IPv4-адреси шлюзу за замовчуванням. HSRP використовується групою маршрутизаторів для вибору активного і резервного пристроїв. В рамках групи інтерфейсів пристрою активним називається пристрій, що використовується для маршрутизації пакетів; резервним - пристрій, який задіюється в разі збою активного пристрою або при виконанні попередньо заданих умов. Завдання резервного маршрутизатора HSRP полягає в моніторингу робочого стану групи HSRP і швидкому переході до виконання функцій пересилання пакетів в разі збою активного маршрутизатора.

HSRP для IPv6: пропріетарний протокол FHRP Cisco, який надає ті ж функції HSRP, але для середовища IPv6. Група IPv6 HSRP містить віртуальний MAC-адресу, похідний від номера групи HSRP і віртуального локального IPv6-адреси каналу, похідного від віртуального MAC-адреси HSRP. Для

віртуального локального IPv6-адреси каналу HSRP відправляються періодичні оголошення маршрутизатора (RA), якщо група HSRP активна. Коли група стає неактивною, RA припиняються після відправки останнього з них.

Протокол резервування віртуального маршрутизатора, версія 2 (VRRPv2): відкритий протокол вибору, динамічно призначає VRRP-маршрутизаторів відповідальність за один або кілька віртуальних маршрутизаторів в IPv4-мережі LAN. Таким чином, кілька маршрутизаторів в каналі з множинним доступом можуть використовувати один віртуальний IPv4-адрес. VRRP-маршрутизатор налаштовується для запуску протоколу VRRP в комбінації з одним або декількома іншими маршрутизаторами, підключеними до мережі LAN. У конфігурації VRRP один з маршрутизаторів вибирається в якості основного віртуального маршрутизатора, а інші виступають в ролі резервних на випадок збою основного віртуального маршрутизатора.

VRRPv3 надає функції підтримки IPv4- і IPv6-адрес. VRRPv3 працює в неоднорідних середовищах і надає більш широкі можливості масштабування, ніж VRRPv2.

Протокол розподілу навантаження для шлюзів (GLBP): пропріетарний протокол FHRP Cisco, який забезпечує захист трафіку даних від несправного маршрутизатора або мережі (наприклад, HSRP і VRRP), одночасно забезпечуючи балансування навантаження (т. Н. Розподіл навантаження) по групі надлишкових маршрутизаторів.

GLBP для IPv6: пропріетарний протокол FHRP Cisco, який надає ті ж функції GLBP, але для середовища IPv6. GLBP для IPv6 забезпечує автоматичне резервування маршрутизаторів для вузлів IPv6, налаштованих з одним шлюзом за замовчуванням в мережі LAN. Кілька маршрутизаторів першого переходу в мережі LAN об'єднані в цілях надання одного віртуального IPv6-маршрутизатора першого переходу при одночасному розподілі навантаження в процесі пересилання IPv6-пакетів.

Протокол виявлення маршрутизаторів ICMP (IRDP): заявлений в RFC 1256, є попередньою версією рішення FHRP. IRDP дозволяє вузлам IPv4 визначати місце розташування маршрутизаторів, що забезпечують підключення по IPv4 до інших (нелокальним) IP-мереж.

Активний маршрутизатор HSRP має наступні характеристики:

- Відповідає на ARP-запити шлюзу, відправляючи MAC-адресу віртуального маршрутизатора.
- Виконує активну пересилання пакетів для віртуального маршрутизатора.
- Відправляє повідомлення вітання.
- Містить дані IP-адреси віртуального маршрутизатора.
- Резервний маршрутизатор HSRP має наступні характеристики:
- Прослуховує періодичні повідомлення вітання.
- Виконує активну пересилання пакетів, якщо дані не надходять з активного маршрутизатора.

Для перевірки стану HSRP використовується команда show standby. У вихідних даних на малюнку показано, що маршрутизатор знаходиться в активному стані.

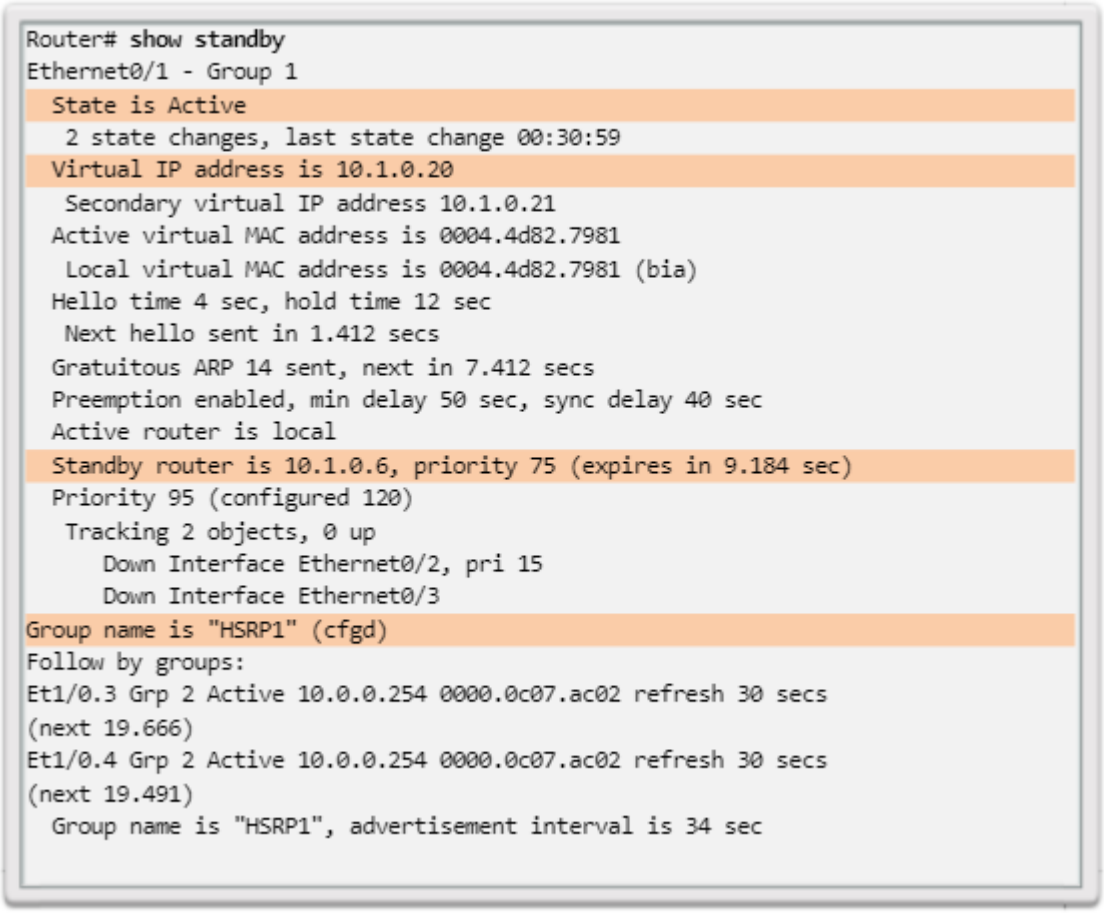


Рис. 5.1.50

Хоча HSRP і VRRP забезпечують відмовостійкість шлюзу, для резервних учасників групи надмірності смуга пропускання висхідного каналу не використовується, поки пристрій знаходиться в режимі очікування.

Тільки активний маршрутизатор в групах HSRP і VRRP пересилає трафік на віртуальний MAC-адресу. Ресурси, пов'язані з резервним маршрутизатором, використовуються не повністю. В деякій мірі є розподіл навантаження при використанні цих протоколів за рахунок створення декількох груп і призначення кількох шлюзів за замовчуванням, однак така конфігурація створює додаткове навантаження на адміністратора.

GLBP є пропрієтарним рішенням Cisco, яке забезпечує функції автоматичного вибору і одночасного використання декількох доступних шлюзів крім автоматичного перемикання між цими шлюзами в разі збою. Кілька маршрутизаторів розподіляють навантаження кадрів, які, з точки зору клієнта, відправляються на одну адресу шлюзу, як показано на рис. 1.

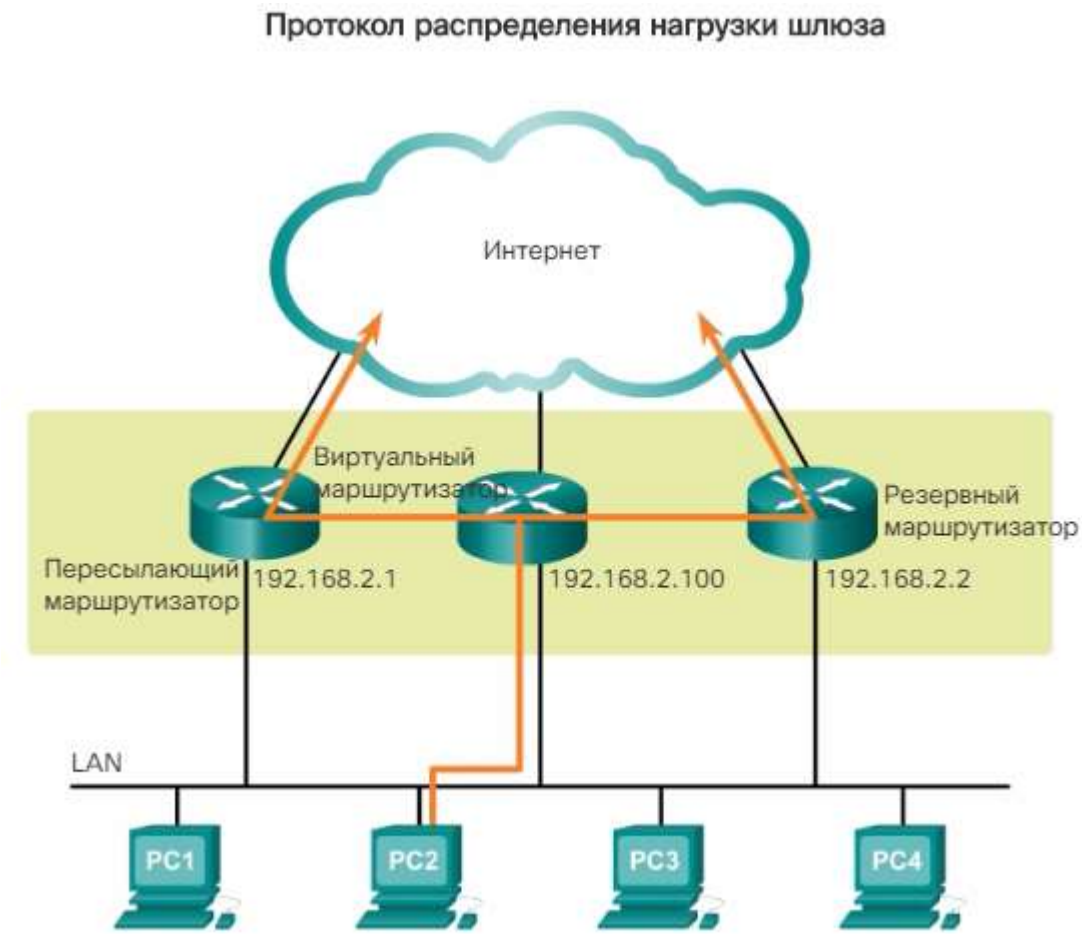


Рис. 5.1.51

Використовуючи GLBP, можна в повній мірі задіяти ресурси, не збільшуючи навантаження на адміністратора в зв'язку з налаштуванням декількох груп і управлінням декількома конфігураціями шлюзу. Протокол GLBP володіє наступними характеристиками:

Дозволяє повністю задіяти ресурси на всіх пристроях, не збільшуючи навантаження на адміністратора в зв'язку зі створенням декількох груп.

Надає один віртуальний IP-адреса і кілька віртуальних MAC-адрес.

Маршрутизує трафік на окремих шлюзах, розподілених по маршрутизаторів.

Забезпечує автоматичну повторну маршрутизацію в разі будь-якого збою.

Для перевірки статусу GLBP використовується команда show glbp. На рис. 2 показано, що група GLBP 1 знаходиться в активному стані, використовуючи IP-адреса 192.168.2.100.

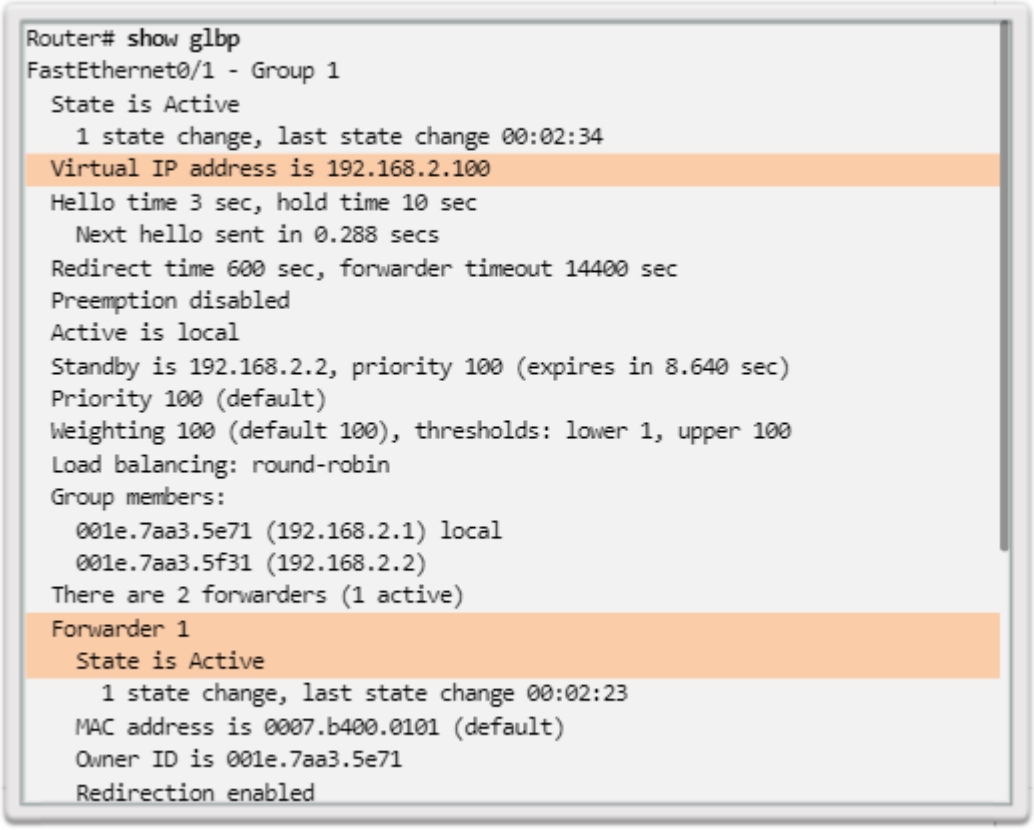


Рис. 5.1.52

Вправа з перевіркою синтаксису. HSRP і GLBP

Конфігурація HSRP і GLBP не розглядається в рамках даного курсу. Однак знання команд, використовуваних для включення HSRP і GLBP, істотно спрощує читання і розуміння вихідних даних конфігурації. Саме тому в якості додаткової практики ми пропонуємо вам виконати вправу з перевіркою синтаксису і подальшу лабораторну роботу.

До проблем, які можуть виникати в зв'язку з надмірною мережею 2 рівня, можна віднести широкомовні шторми, нестабільність бази даних MAC-адрес і дублювання кадрів одно адресної розсилки. Протокол STP є протоколом 2 рівня, який забезпечує наявність єдиного логічного шляху між усіма адресами призначення в мережі за рахунок навмисного блокування надлишкових шляхів, які можуть викликати утворення петлі.

Протокол STP відправляє кадри BPDU для обміну даними між комутаторами. Для кожного примірника протоколу spanning-tree як кореневого моста вибирається один комутатор. Адміністратор може контролювати такий вибір шляхом зміни пріоритету моста. Щоб налаштувати розподіл навантаження протоколу spanning-tree по мережі VLAN або по групі мереж VLAN в залежності від використовуваного протоколу STP, можна налаштувати кореневі мости. Потім STP призначає роль порту кожному бере участь порту, використовуючи значення вартості шляху. Вартість шляху дорівнює сумі всіх значень вартості порту по шляху до кореневого мосту. Вартість порту автоматично призначається кожному порту. Проте, це значення можна також налаштувати вручну. Шляхи з найменшою вартістю стають кращими, а всі інші надлишкові шляху блокуються.

PVST + являє собою конфігурацію IEEE 802.1D за замовчуванням на комутаторах Cisco. Цей протокол запускає один примірник STP для кожної мережі VLAN. На комутаторах Cisco для кожної окремої мережі VLAN можна реалізувати нову версію протоколу STP з більш швидкою збіжністю (RSTP) у вигляді протоколу Rapid PVST +. Протокол MST (Multiple Spanning Tree) є реалізацією протоколу MSTP корпорації Cisco, де один примірник протоколу spanning-tree використовується для певної групи мереж VLAN. Такі функції, як PortFast і BPDU guard, гарантують, що вузли в комутованій середовищі матимуть негайний доступ до мережі без порушення роботи протоколу spanning-tree.

Такі протоколи забезпечення надмірності на першому хопі, як HSRP, VRRP і GLBP, надають альтернативні шлюзи за замовчуванням для вузлів в середовищі, де використовується резервний маршрутизатор або середовище з багаторівневою комутацією. Кілька маршрутизаторів спільно використовують віртуальний IP-адреса і MAC-адресу, який виступає в ролі шлюзу на клієнті. Це гарантує, що вузли будуть підтримувати підключення в разі збою одного з пристроїв, які виступають в ролі шлюзу для мережі VLAN або групи мереж VLAN. При використанні HSRP або VRRP один маршрутизатор є активним або пересилаються маршрутизатором для конкретної групи, а інші знаходяться в режимі очікування. Крім автоматичного перемикання між шлюзами в разі збою, GLBP дозволяє також одночасно використовувати кілька шлюзів.

5.2 Агрегування каналів

Агрегування каналів називають створення між двома пристроями одного логічного каналу з використанням декількох фізичних каналів. Таким чином забезпечується розподіл навантаження між фізичними каналами замість блокування протоколом STP одного або декількох з них. EtherChannel є технологією агрегування каналів, використовувану в комутованих мережах.

У цьому розділі наведено відомості EtherChannel і представлені методи, використовувані для створення EtherChannel. EtherChannel можна налаштувати вручну або узгодити, використовуючи пропріетарний протокол агрегування портів Cisco (PAgP) або протокол LACP, певний відкритим стандартом IEEE 802.3ad. У розділі розглядаються питання настройки, перевірки та усунення неполадок в роботі EtherChannel.

Робочий день підходить до кінця. Ви намагаєтеся пояснити мережевим фахівцям вашого невеликого підприємства концепцію EtherChannel і наочно уявити роботу даної технології. Мережевим інженерам складно уявити, яким чином два комутатора теоретично можна з'єднати за допомогою декількох каналів, які всі разом виступають як один канал або підключення. Керівництво вашої компанії планує реалізувати мережу EtherChannel.

Тому в кінці зборів ви даєте групі інженерів завдання. До завтрашнього зборам вони повинні провести дослідження і продемонструвати колегам графічне представлення мережевого підключення EtherChannel. Від них вимагається пояснити іншим інженерам принципи роботи мережі EtherChannel.

При вивченні EtherChannel рекомендується знайти відповідь на питання: «Як виглядає канал EtherChannel?». Проілюструйте своє дослідження декількома слайдами, які ви представите групі мережевих інженерів. Ці слайди повинні чітко пояснити слухачам принципи фізичного створення каналів EtherChannel в межах топології мережі. Ваше завдання полягає в тому, щоб кожен, хто відвідає завтрашнє зібрання, ясно розумів, чому компанії варто розглянути можливість переходу на топологію мережі з використанням EtherChannel.

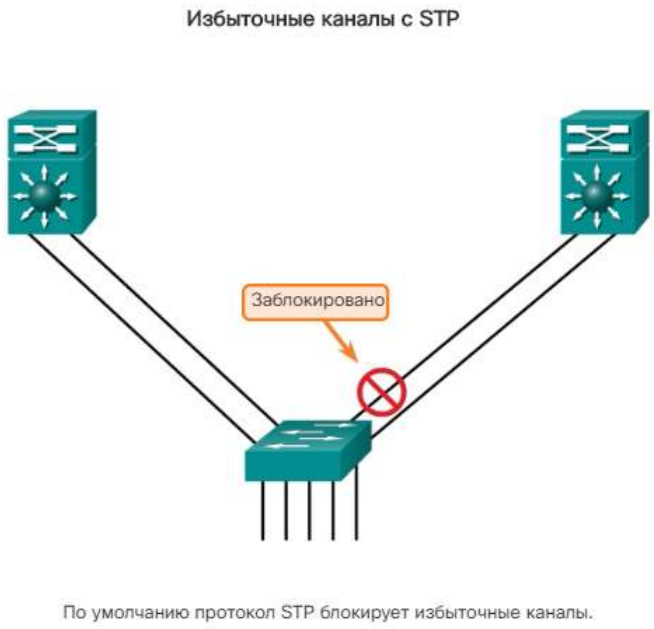


Рис. 5.2.1

Можна використовувати канали з більш високою швидкістю (наприклад 10 Гбіт / с) в агрегованому каналі між комутаторами рівня доступу і розподілу. Однак додавання каналів з більш високою швидкістю - досить дороге рішення. Крім того, у міру збільшення швидкості на каналах доступу, швидкість навіть найшвидших портів в агрегованому каналі стає недостатньою для об'єднання трафіку, що надходить з усіх каналів доступу.

Також можна збільшити число фізичних каналів між комутаторами, що дозволить збільшити загальну швидкість обміну даними між комутаторами. Однак за замовчуванням на пристроях комутації включений протокол сполучного дерева (STP). Протокол STP блокує надлишкові канали, щоб уникнути петель комутації.

З цих причин оптимальним рішенням є реалізація технології EtherChannel.

Переваги EtherChannel

Технологія EtherChannel спочатку була розроблена компанією Cisco як технологія LAN типу «комутатор-комутатор» для об'єднання декількох портів Fast Ethernet або Gigabit Ethernet в один логічний канал. При налаштуванні EtherChannel створюється віртуальний інтерфейс, який називається агрегований канал (port channel). Фізичні інтерфейси об'єднуються в інтерфейс агрегованого каналу.

Більшість завдань конфігурації виконується на інтерфейсі EtherChannel, а не на окремих портах. Це забезпечує узгоджену конфігурацію на всіх каналах.

EtherChannel використовує існуючі порти комутатора. Для забезпечення більш високої пропускної здатності не потрібно дорога заміна каналу на більш швидкий.

Між каналами, які є частиною одного і того ж EtherChannel, відбувається розподіл навантаження. Залежно від використовуваного обладнання може бути реалізований один або кілька методів розподілу навантаження. До цих методів належать, наприклад, розподіл навантаження по фізичних каналах на основі MAC-адреси джерела і MAC-адреси призначення або на основі IP-адреси джерела і IP-адреси призначення.

EtherChannel створює об'єднання, яке розглядається, як один логічний канал. Якщо між двома комутаторами існує декілька об'єднань EtherChannel, протокол STP може блокувати одне з об'єднань щоб уникнути петель комутації. Якщо протокол STP блокує один з надлишкових каналів, він блокує весь EtherChannel. При цьому блокуються всі порти, що стосуються цієї каналу EtherChannel. Якщо існує тільки один канал EtherChannel, все фізичні канали в EtherChannel активні, оскільки STP бачить тільки один (логічний) канал.

EtherChannel надає функції надмірності, оскільки загальний канал вважається одним логічним з'єднанням. Крім того, втрата одного фізичного з'єднання в межах каналу не призводить до зміни в топології. Отже, перерахунок дерева найкоротших шляхів не потрібно. За умови, що є хоча б одна фізична з'єднання, EtherChannel продовжує працювати навіть в тому випадку, якщо загальна пропускна здатність знижується через втрати з'єднання в межах EtherChannel.

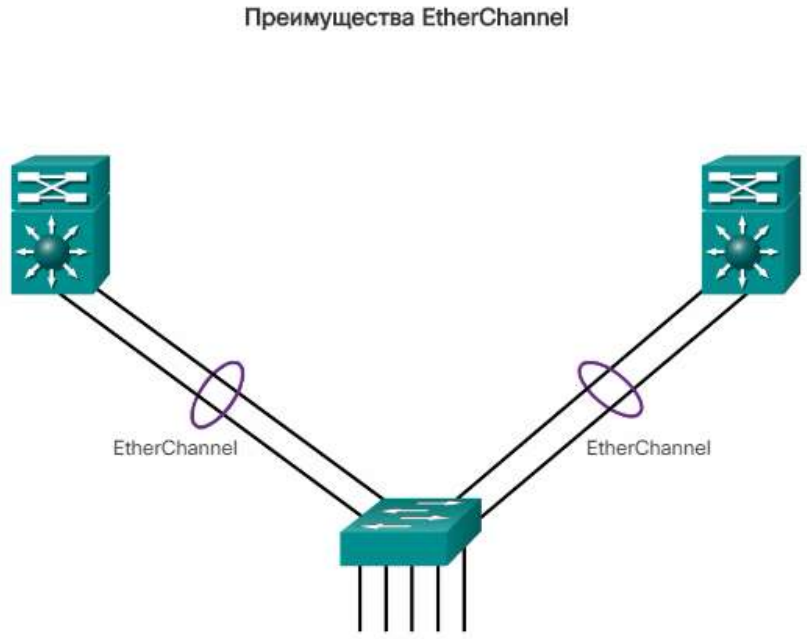


Рис. 5.2.2

EtherChannel можна реалізувати шляхом об'єднання кількох фізичних портів в один або кілька логічних каналів EtherChannel.

Примітка. Типи інтерфейсів можна змішувати. Наприклад, не можна змішувати Fast Ethernet і Gigabit Ethernet в межах одного каналу EtherChannel.

EtherChannel надає полнодуплексную смугу пропускання до 800 Мбіт / с (Fast EtherChannel) або 8 Гбіт / с (Gigabit EtherChannel) між двома комутаторами або між комутатором і вузлом. В даний час всі канали EtherChannel можуть містити до восьми сумісно налаштованих Ethernet-портів. Комутатори Cisco IOS в даний час підтримують шість каналів EtherChannel. Проте з появою нових версій IOS і зміною платформ деякі карти і платформи можуть отримати можливість підтримувати більшу кількість портів в межах одного каналу EtherChannel, а також більшу кількість каналів Gigabit EtherChannel. Концепція залишається незмінною незалежно від швидкостей або кількості танцювальних каналів. При налаштуванні EtherChannel на

комутаторах слід враховувати обмеження і характеристики апаратної платформи.

Первинним завданням EtherChannel було збільшення швидкості в агрегованих каналах між комутаторами. Однак можливості даної концепції були розширені з урахуванням зростаючої популярності EtherChannel, і тепер багато сервери також підтримують агрегування каналів за допомогою EtherChannel. EtherChannel створює зв'язок типу «один в один», тобто один канал EtherChannel з'єднує тільки два пристрої. Канал EtherChannel можна створити між двома комутаторами або між сервером з включеним EtherChannel і комутатором. Однак трафік не можна посилати на два різних комутатора по одному каналу EtherChannel.

Конфігурація порту окремого учасника групи EtherChannel повинна виконуватися узгоджено на обох пристроях. Якщо фізичні порти на одній стороні налаштовані як транкових, то фізичні порти на іншій стороні також повинні бути налаштовані як транкових з тим же самим native VLAN. Крім того, всі порти в кожному каналі EtherChannel повинні бути налаштовані як порти 2 рівня.

Примітка. На багаторівневих комутаторах Cisco Catalyst (наприклад Catalyst 3560) можна налаштувати канали EtherChannel 3 рівня, однак вони не розглядаються в рамках даного курсу. Канал EtherChannel 3 рівня має один IP-адресу, пов'язану з логічної групою портів комутатора в каналі EtherChannel.

Як показано на малюнку, кожен канал EtherChannel має логічний інтерфейс агрегованого каналу. Налаштування інтерфейсу агрегованого каналу застосовується на всі фізичні інтерфейси, пов'язані з цим каналом.

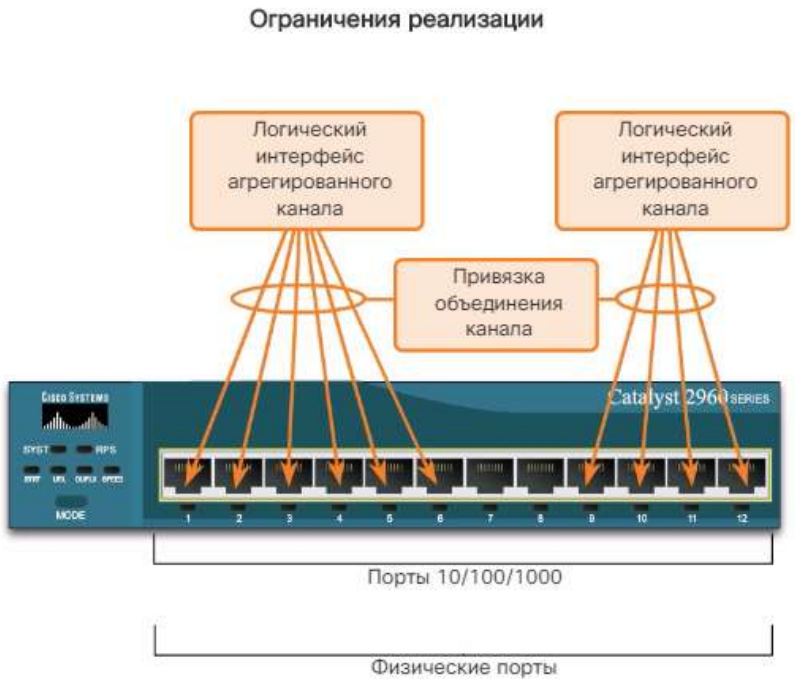


Рис. 5.2.3

Etherchannel можна утворити шляхом узгодження з використанням одного з двох протоколів, PAgP або LACP. Дані протоколи дозволяють портам з подібними характеристиками утворювати канали шляхом динамічного узгодження із суміжними комутаторами.

Примітка. Також можлива настройка статичного або безумовного каналу EtherChannel без використання PAgP або LACP.

PAgP - це пропріетарний протокол Cisco, який призначений для автоматизації створення каналів EtherChannel. Коли канал EtherChannel налаштовується за допомогою PAgP, пакети PAgP пересилаються між портами з підтримкою EtherChannel з метою узгодження створення каналу. Коли PAgP визначає збігаються з'єднання Ethernet, він групує їх в канал EtherChannel. Далі EtherChannel додається в дерево найкоротших шляхів як один порт.

Якщо включений протокол PAgP, він також бере участь в управлінні EtherChannel. Відправка пакетів PAgP виконується з інтервалом в 30 секунд. PAgP перевіряє узгодженість конфігурації і обробляє додавання і вихід з ладу каналів між двома комутаторами. Таким чином забезпечується використання узгодженої конфігурації для всіх портів при створенні EtherChannel.

Примітка. У EtherChannel всі порти обов'язково повинні мати однакову швидкість, однакові настройки дуплексу і однакові настройки VLAN. При будь-якій зміні порту після створення каналу також змінюються всі інші порти каналу.

Протокол PAgP дозволяє створити канал EtherChannel шляхом виявлення конфігурації на кожній зі сторін і забезпечення сумісності каналів, щоб канал EtherChannel міг бути включений в разі потреби. На малюнку показані режими протоколу PAgP.

On - цей режим примусово призначає інтерфейс в канал без використання PAgP. Інтерфейси, налаштовані в режимі On (Увімкнути), що не обмінюються пакетами PAgP.

PAgP desirable (рекомендований) - цей режим PAgP поміщає інтерфейс в активний стан узгодження, в якому інтерфейс ініціює узгодження з іншими інтерфейсами шляхом відправки пакетів PAgP.

PAgP auto (автоматичний) - цей режим PAgP поміщає інтерфейс в пасивний стан узгодження, в якому інтерфейс відповідає на отримані пакети PAgP, але не ініціює узгодження PAgP.

Режими повинні бути сумісними на кожній зі сторін. Якщо одна зі сторін налаштована в автоматичному режимі, вона поміщається в пасивний стан, чекаючи ініціації узгодження EtherChannel іншою стороною. Якщо для іншого боку також заданий автоматичний режим, то узгодження не почнеться і EtherChannel не утворюється. Якщо все режими відключені за допомогою команди no або жоден з режимів не налаштований, EtherChannel відключається.

Режим Увімкнути поміщає інтерфейс в канал EtherChannel без виконання узгодження. Цей режим працює тільки в тому випадку, якщо для іншого боку також заданий режим Вкл. Якщо для іншого боку параметри узгодження задані за допомогою PAgP, освіту EtherChannel не виконується, оскільки та сторона, для якої задано режим Вкл, не виконує узгодження.

S1	S2	Формирование канала
Вкл	Вкл	Да
Автоматический/Рекомендуемый	Рекомендуемый	Да
Вкл/Автоматический/ Рекомендуемый	Конфигурация не задана	Нет
Вкл	Рекомендуемый	Нет
Автоматический/Вкл	Автоматический	Нет

Рис. 5.2.4

Протокол LACP

LACP визначається стандартом IEEE (802.3ad), який забезпечує можливість об'єднання декількох фізичних портів для створення єдиного логічного каналу. LACP забезпечує можливість узгодження комутатором автоматичного об'єднання шляхом відправки сусідові пакетів LACP. Він виконує функцію, подібну до функціями PAgP для Cisco EtherChannel. Оскільки протокол LACP відноситься до стандарту IEEE, його можна використовувати для спрощення роботи з каналами EtherChannel в неоднорідних середовищах. На пристроях Cisco підтримуються обидва протоколи.

Примітка. LACP спочатку визначений як стандарт IEEE 802.3ad. Проте, тепер протокол LACP визначається більш новою версією, стандартом IEEE 802.1AX для локальних і міських мереж.

Протокол LACP надає ті ж переваги при узгодженні, що і протокол PAgP. Протокол LACP дозволяє створити канал EtherChannel шляхом виявлення конфігурації на кожній зі сторін і забезпечення сумісності каналів, щоб канал EtherChannel міг бути включений в разі потреби. На малюнку показані режими протоколу LACP.

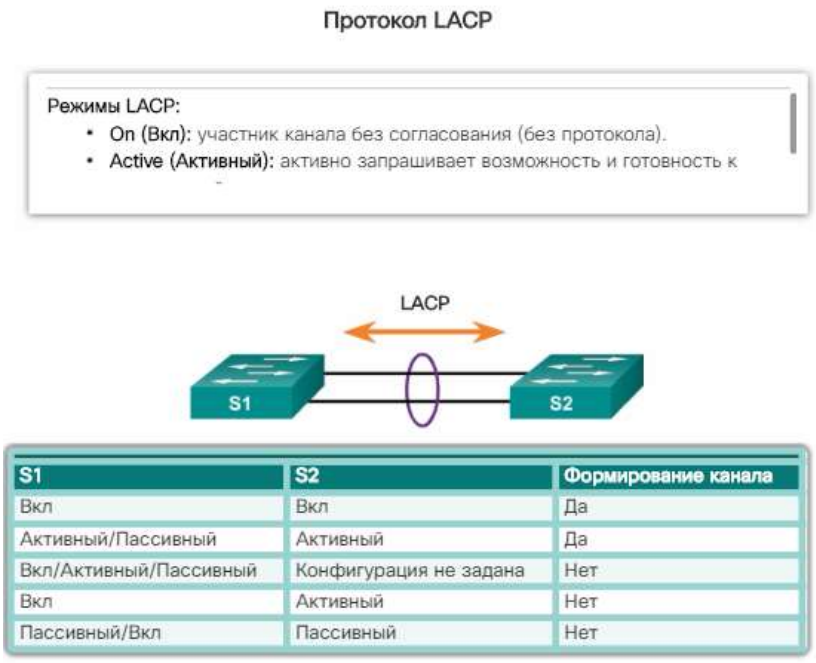
On (Увімкнути) - цей режим примусово поміщає інтерфейс в канал без використання LACP. Інтерфейси, налаштовані в режимі On, що не обмінюються пакетами LACP.

LACP active (активний) - в цьому режимі LACP порт поміщається в активний стан узгодження. У цьому стані порт ініціює узгодження з іншими портами шляхом відправки пакетів LACP.

LACP passive (пасивний) - в цьому режимі LACP порт поміщається в пасивний стан узгодження. У цьому стані порт відповідає на отримані пакети LACP, але не ініціює узгодження пакетів LACP.

Як і у випадку з PAgP, для формування каналу EtherChannel режими повинні бути сумісні на обох сторонах. Режим Увімкнути повторюється,

оскільки він створює конфігурацію EtherChannel безумовно, без динамічного узгодження PAgP або LACP.



S1	S2	Формирование канала
Вкл	Вкл	Да
Активный/Пассивный	Активный	Да
Вкл/Активный/Пассивный	Конфигурация не задана	Нет
Вкл	Активный	Нет
Пассивный/Вкл	Пассивный	Нет

Рис. 5.2.5

При налаштуванні EtherChannel рекомендується дотримуватися таких вказівок і обмеження:

Підтримка EtherChannel. Всі інтерфейси Ethernet на всіх модулях повинні підтримувати EtherChannel; при цьому не потрібно, щоб ці інтерфейси були фізично суміжними або перебували на одному модулі.

Швидкість і двобічний режим. Налаштуйте все інтерфейси в EtherChannel для роботи на одній швидкості і в одному дуплексному режимі, як показано на малюнку.

Зіставлення мереж VLAN. Всі інтерфейси в об'єднанні EtherChannel повинні бути призначені в один VLAN або налаштовані як транкового каналу (також показано на малюнку).

Діапазон мереж VLAN. EtherChannel підтримує однакові дозволені діапазони мереж VLAN на всіх інтерфейсах в транкові каналі EtherChannel. Якщо дозволений діапазон мереж VLAN не збігається, інтерфейси не зможуть створити EtherChannel навіть при виборі auto або desirable режимів.

Якщо дані параметри необхідно змінити, настройку слід виконувати в режимі конфігурації інтерфейсу агрегованого каналу. Після настройки інтерфейсу агрегованого каналу всі введені команди також застосовуються на окремі інтерфейси. Однак конфігурації, застосовані до окремих інтерфейсів, не впливають на інтерфейс агрегованого каналу. Отже, зміна конфігурації інтерфейсу, що відноситься до каналу EtherChannel, може викликати проблеми з сумісністю.

Рис. 5.2.6

Налаштування EtherChannel з використанням LACP проходить в два етапи.

Крок 1. Вкажіть інтерфейси, що складають групу EtherChannel, використовуючи команду режиму глобальної конфігурації interface range interface. Ключове слово range дозволяє вибрати кілька інтерфейсів і налаштувати їх одночасно. Рекомендується спершу відключити ці інтерфейси, щоб уникнути активності в каналі через неповну конфігурації.

Крок 2. Створіть інтерфейс агрегованого каналу за допомогою команди channel-group identifier mode active режиму конфігурації діапазону інтерфейсу. Ідентифікатор задає номер групи каналів. Ключові слова mode active визначають його як конфігурацію EtherChannel LACP.

Примітка. Функція EtherChannel відключена за замовчуванням.

На рис. 1 інтерфейси FastEthernet0 / 1 і FastEthernet0 / 2 об'єднані в агрегований канал інтерфейсу EtherChannel 1.

Настройка EtherChannel с использованием LACP

```
S1(config)# interface range FastEthernet0/1 - 2
S1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 1,2,20
```

Создает EtherChannel и настраивает транковый канал.

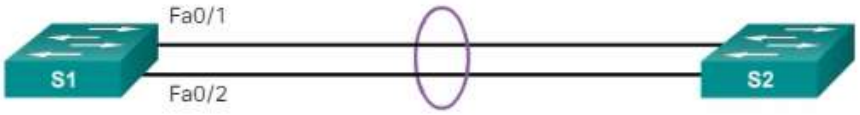


Рис. 5.2.7

Щоб змінити налаштування 2 рівня на інтерфейсі агрегованого каналу, перейдіть в режим конфігурації інтерфейсу агрегованого каналу за допомогою команди interface port-channel, після якої необхідно вказати ідентифікатор інтерфейсу. У розглянутому прикладі EtherChannel налаштовується як транкового інтерфейсу із зазначенням дозволених мереж VLAN. Як показано на рис. 1, інтерфейс агрегованого каналу 1 налаштований як транкового каналу з дозволеними мережами VLAN 1, 2 і 20.

Виконайте вправу з перевіркою синтаксису на рис. 2, щоб налаштувати EtherChannel на комутаторі S1.

Для перевірки конфігурації EtherChannel є кілька команд. Спочатку за допомогою команди show interface port-channel показує огляд статус інтерфейсу агрегованого каналу. На рис. 1 інтерфейс Port Channel 1 включений.

Проверка EtherChannel

```
S1# show interface port-channel1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0cd9.96e8.8a02 (bia
0cd9.96e8.8a02)
  MTU 1500 bytes, BW 200000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
<выходные данные опущены>
```

Выполняет проверку статуса интерфейса.

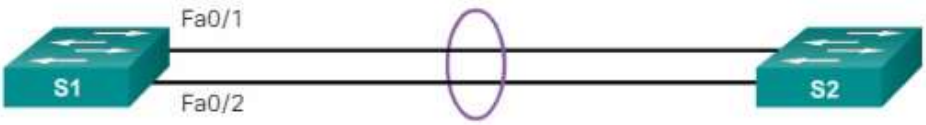


Рис. 5.2.8

Коли на одному пристрої налаштовано кілька інтерфейсів агрегованого каналу, необхідно використовувати команду show etherchannel summary, щоб відобразити по одному рядку даних на кожен канал. На рис. 2 на комутаторі налаштований один канал EtherChannel; група 1 використовує LACP.

Проверка EtherChannel

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+--------------------------
1      Po1(SU)         LACP      Fa0/1(P)    Fa0/2(P)
```

Отображает одной строкой сводную информацию по группе канала.

Рис. 5.2.9

Група інтерфейсів складається з інтерфейсів FastEthernet0 / 1 і FastEthernet0 / 2. Група є каналом EtherChannel 2 рівня, і вона задіяна, на що вказують літери SU поруч з номером агрегованого каналу.

Використовуйте команду show etherchannel port-channel, щоб відобразити відомості про конкретний інтерфейсі агрегованого каналу, як показано на рис. 3. У розглянутому прикладі інтерфейс Port Channel 1 складається з двох фізичних інтерфейсів - FastEthernet0 / 1 і FastEthernet0 / 2. Він використовує LACP в активному режимі (active). Він правильно підключений до іншого комутатора з сумісною конфігурацією, і тому агрегований канал вважається задіяним.

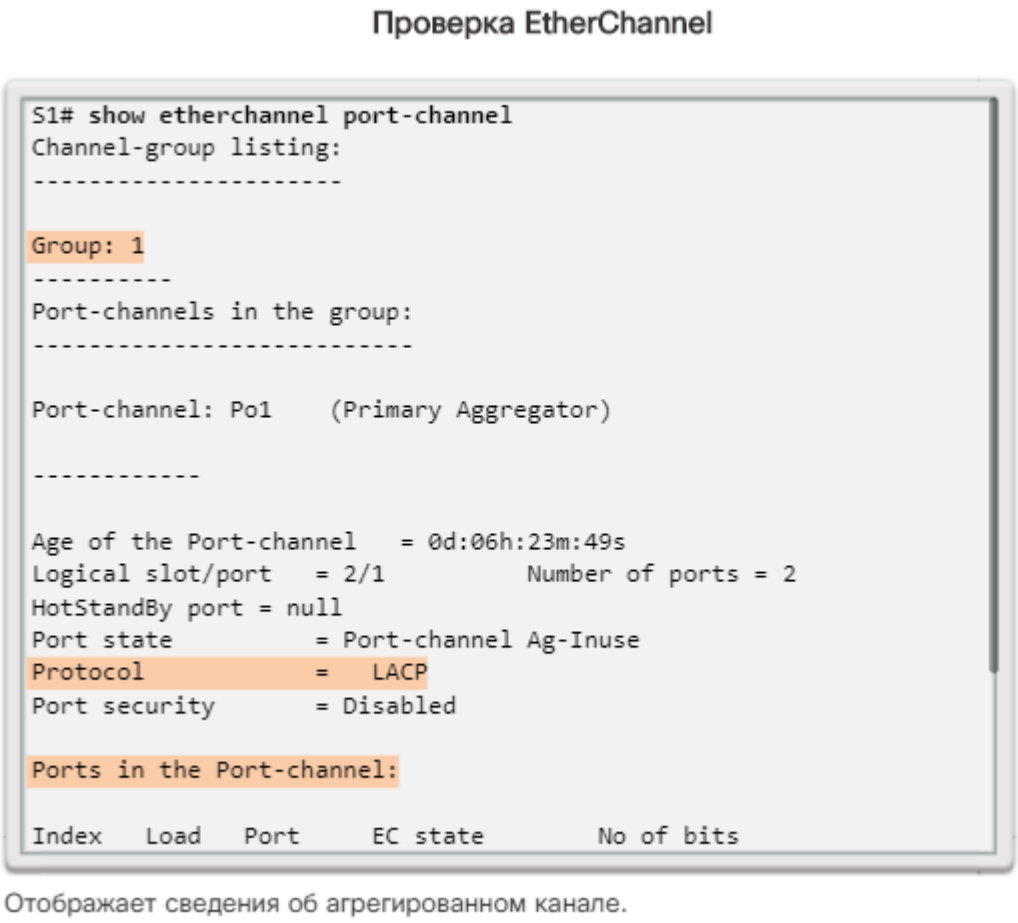


Рис. 5.2.10

Щоб переглянути дані про роль фізичного інтерфейсу в роботі EtherChannel (див. Рис. 4), слід виконати команду show interfaces etherchannel. Інтерфейс FastEthernet 0/1 відноситься до групи EtherChannel 1. Для даного каналу EtherChannel використовується протокол LACP.

Проверка EtherChannel

```
S1# show interfaces f0/1 etherchannel
Port state    = Up Mstr Assoc In-Bndl
Channel group = 1           Mode = Active          Gcchange = -
Port-channel  = Po1         GC   =   -             Pseudo port-chann
Port index    = 0           Load = 0x00            Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending f
        A - Device is in active mode.        P - Device is in passiv

Local information:
                            LACP port     Admin     Oper    Port
Port      Flags   State     Priority      Key       Key     Number
Fa0/1     SA      bndl      32768         0x1       0x1     0x102

Partner's information:

                  LACP port                         Admin  Oper   Por
Port      Flags   Priority  Dev ID          Age     key    Key    Numl
Fa0/1     SA      32768     0cd9.96d2.4000  13s     0x0    0x1    0x1

Age of the port in the current state: 0d:06h:06m:51s
```

Отображает роль конкретного интерфейса в EtherChannel.

Рис. 5.2.11

Виконайте вправу з перевіркою синтаксису на рис. 5, щоб перевірити EtherChannel на комутаторі S1.

Всі інтерфейси в EtherChannel повинні мати однакові настройки швидкості і дуплексного режиму, на транкових каналах однакові настройки native VLAN і дозволених VLAN, на портах доступу - однаковий VLAN:

призначте всі порти в EtherChannel однієї VLAN або налаштуйте їх в якості транкових каналів. Порти з різними native VLAN не можуть утворити EtherChannel.

При налаштуванні EtherChannel на транкових каналах необхідно переконатися, що у всіх транкових каналах режим транка налаштований однаково. Неузгодженість режимів транка на портах EtherChannel може привести до того, що EtherChannel не працюватиме, а порти будуть відключені (стан errdisable).

Усі вхідні в EtherChannel порти підтримують однаковий діапазон дозволених VLAN. Якщо діапазони дозволених VLAN не збігаються, порти не зможуть сформувати EtherChannel навіть при виборі auto або desirable режимів для PAgP.

Параметри динамічного узгодження для PAgP і LACP повинні бути налаштовані з урахуванням сумісності на обох кінцях EtherChannel.

Примітка. Легко сплутати протокол PAgP або LACP з DTP, оскільки обидва протоколи використовуються для автоматизації поведінки на транкових каналах. Протоколи PAgP і LACP використовуються для агрегування каналів

(EtherChannel). DTP використовується для автоматизації створення транкових каналів. Як правило, якщо налаштований транковий канал EtherChannel, то EtherChannel (PAgP або LACP) налаштовується в першу чергу, і тільки після цього налаштовується DTP.

На рис. 1 інтерфейси F0 / 1 і F0 / 2 на комутаторах S1 і S2 з'єднані за допомогою EtherChannel. У вихідних даних нижче показано, що EtherChannel вимкнений.

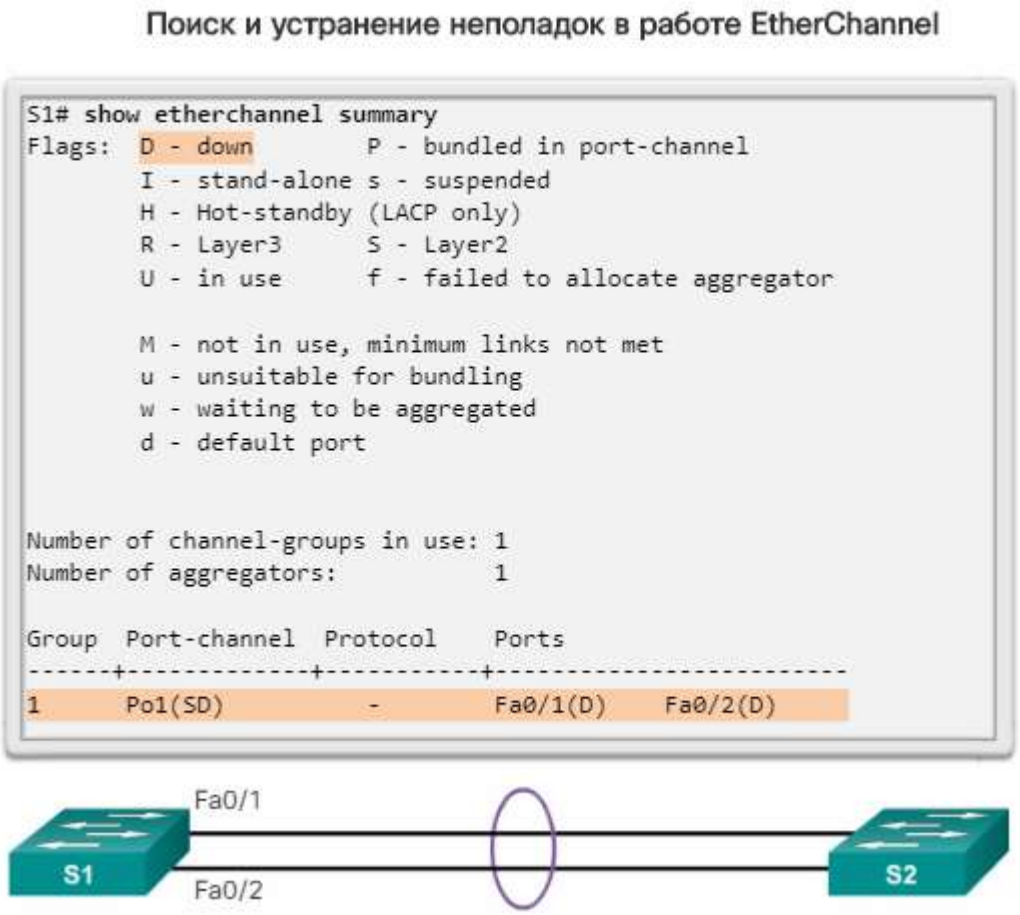


Рис. 5.2.12

На рис. 2 представлені більш докладні вихідні дані, в яких зазначено, що на комутаторах S1 і S2 налаштовані несумісні режими PAgP.

Поиск и устранение неполадок в работе EtherChannel

```
S1# show run | begin interface port-channel
interface Port-channel1
 switchport mode trunk
!
interface FastEthernet0/1
 switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet0/2
 switchport mode trunk
 channel-group 1 mode on
!
<выходные данные опущены>

S2# show run | begin interface port-channel
interface Port-channel1
 switchport mode trunk
!
interface FastEthernet0/1
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/2
 switchport mode trunk
```

Рис. 5.2.13

На рис. 3 режим PAgP в EtherChannel змінений на рекомендований режим, після чого EtherChannel переходить в активний режим.

Поиск и устранение неполадок в работе EtherChannel

```
S1(config)# no interface port-channel 1
S1(config)# interface range f0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

S1(config-if-range)# no shutdown
S1(config-if-range)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1
```

Рис. 5.2.14

Примітка. EtherChannel і STP повинні взаємодіяти. З цієї причини важливий порядок виконання пов'язаних з EtherChannel команд, і саме тому інтерфейс Port-Channel 1 (на рис. 3) знаходиться на відстані і знову доданий за допомогою команди channel-group, а не змінений безпосередньо. При спробі

змінити конфігурацію інтерфейсу безпосередньо помилки STP призводять до того, що пов’язані порти переходять в стан блокування або в стан errdisable.

Замість збереження поточних налаштувань комутаторів ви вирішили налаштувати EtherChannel хоча б для частини мережі, щоб перевірити, скоротиться чи перевантаження по трафіку між комутаторами рівнів доступу і розподілу.

Технологія EtherChannel спрямована на об'єднання декількох комутаційних каналів з метою розподілу навантаження по надлишковим шляхах між двома пристроями. Всі порти в межах одного каналу EtherChannel повинні мати однакову швидкість, однакові настройки дуплексного режиму і відомості про мережі VLAN на всіх інтерфейсах пристроїв на обох кінцях. Параметри, налаштовані в режимі конфігурації інтерфейсу агрегованого каналу, також застосовуються до окремих інтерфейсів в межах цього каналу EtherChannel. Параметри, налаштовані на окремих інтерфейсах, які не будуть застосовані до EtherChannel або до інших інтерфейсів в межах каналу EtherChannel.

PAgP - це пропріетарний протокол Cisco, який призначений для автоматизації створення каналів EtherChannel. Режими PAgP: On (Увімкнути), PAgP desirable (рекомендований) і PAgP auto (автоматичний). Протокол LACP описується стандартом IEEE, який також забезпечує об'єднання декількох фізичних портів в одному логічному каналі. Режими LACP: On (Увімкнути), LACP active (активний) і LACP passive (пасивний). Протоколи PAgP і LACP не взаємодіють один з одним. Режим On повторюється як в протоколі PAgP, так і в протоколі LACP, оскільки він створює EtherChannel безумовно, без використання PAgP або LACP. За замовчуванням канал EtherChannel не налаштований ні в одному режимі.

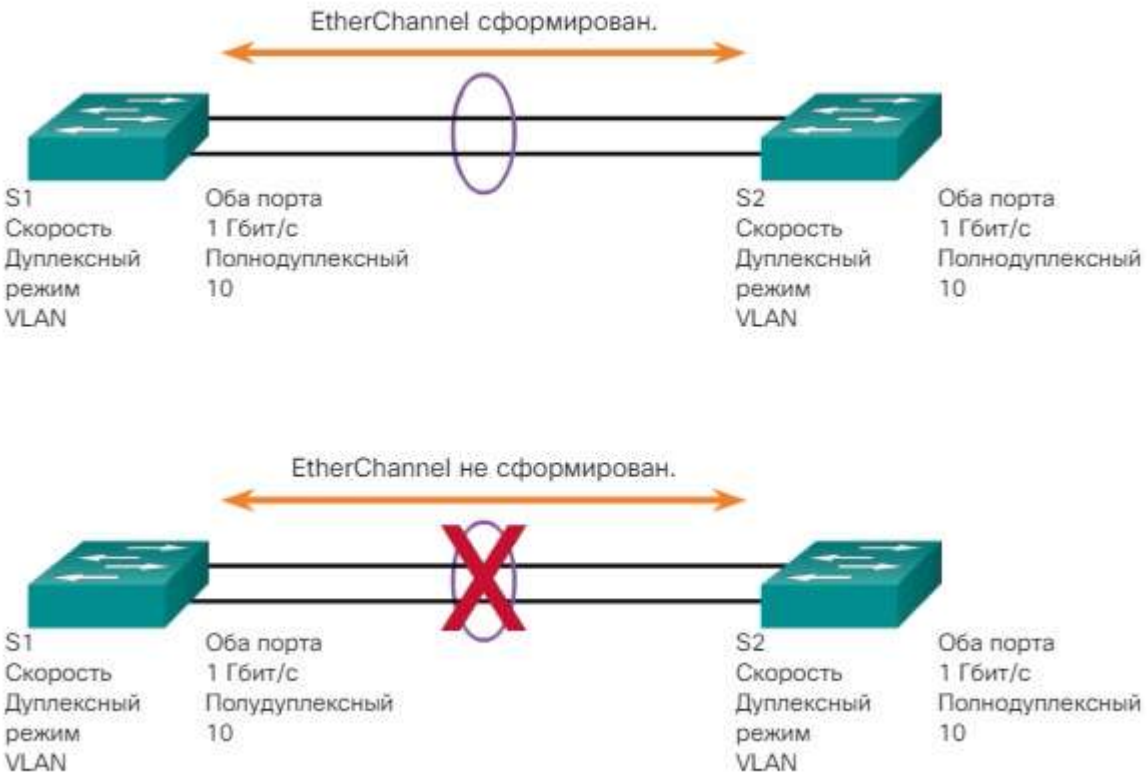


Рис. 5.2.15

5.3 Бездротові локальні мережі

Бездротові мережі забезпечують мобільність клієнта, його здатність підключатися до мережі з будь-якого місця і в будь-який час, а також можливість переміщення без втрати з'єднання. Бездротова мережа LAN (WLAN) відноситься до бездротових мереж, які зазвичай використовуються в домашніх, офісних і корпоративних середовищах. Хоча бездротова мережа використовує радіочастоти замість кабелів, вона зазвичай реалізована в комутованій мережі, а формат кадру аналогічний тому, що використовується в Ethernet.

В рамках даної глави розглядаються технологія, компоненти, система безпеки, планування, реалізація, а також процес пошуку і усунення неполадок в мережі WLAN. Також тут розглядаються типи мережевих атак, яким більшою мірою схильні до бездротові мережі.

Сьогодні корпоративні мережі розвиваються швидкими темпами, забезпечуючи підтримку користувачів, які постійно перебувають в роз'їздах. Користувачі можуть підключатися, використовуючи різні пристрої, включаючи комп'ютери, ноутбуки, планшетні комп'ютери і смартфони. В рамках даної концепції мобільності користувачі можуть підключатися до мережі, перебуваючи в русі.

Подібну мобільність забезпечують різні інфраструктури (провідні мережі LAN, мережі інтернет-провайдерів), однак найважливішою складовою корпоративної середовища є бездротова мережа LAN (WLAN).

Продуктивність праці більше не обмежується стаціонарним робочим місцем або певним періодом часу. Тепер користувачі розраховують на можливість підключення в будь-який час і з будь-якого місця: від офісу до аеропорту або будинку. У ділових поїздках співробітникам доводилося оплачувати телефонний зв'язок між рейсами для перевірки повідомлень і виконання декількох дзвінків. Тепер співробітники можуть перевіряти електронну і голосову пошту, а також стежити за станом проектів зі своїх смартфонів.

Сучасні користувачі розраховують на можливість повсюдного використання роумінгу бездротової мережі. Роумінг забезпечує доступ бездротових пристроїв до Інтернету без втрати з'єднання.

Розпочніть відтворення відео на малюнку, щоб переглянути приклад того, яким чином бездротові мережі забезпечують мобільність.

Бездротовий зв'язок тягне за собою безліч переваг як для корпоративних, так і для домашніх мереж. До таких переваг належать підвищені гнучкість і продуктивність, зниження витрат, можливість розвитку та адаптації до мінливих вимог.

У більшості компаній комутовані мережі LAN використовуються для повсякденної роботи офісу. Однак співробітники все частіше працюють віддалено і розраховують на доступ до ресурсів корпоративної мережі LAN як зі свого робочого столу, так і з інших місць. Співробітники хотіли б брати свої бездротові пристрої на наради, в кабінет колег, в конференц-зал і навіть на об'єкти клієнта, зберігаючи при цьому доступ до ресурсів підприємства. Бездротові мережі забезпечують необхідну в подібних умовах гнучкість.

Замість того, щоб витрачати час на перенесення потрібних матеріалів або пошук проводового підключення для доступу до ресурсів мережі, можна легко надати різних бездротових пристроїв доступ до ресурсів мережі LAN за допомогою бездротового зв'язку.

Доступ сприяє підвищенню продуктивності і зниження напруженості співробітників, хоча ці величини досить важко виміряти. Завдяки бездротових мереж співробітники отримують гнучкі можливості роботи - в будь-який зручний час і в будь-якому зручному місці. Вони можуть відповідати на запити клієнтів, перебуваючи в офісі або в кафе на обідній перерві. Вони можуть за лічені секунди отримати доступ до електронної пошти та інших робочих ресурсів, забезпечуючи оптимізоване управління, більш якісне і швидке досягнення результатів для клієнтів, а також збільшення прибутковості.

Використання бездротових мереж також дозволяє знизити витрати. У компаніях, де вже використовується бездротова інфраструктура, економія витрат реалізується при кожній зміні або переміщенні обладнання - наприклад, при переміщенні співробітника в межах будівлі або реорганізації обладнання або лабораторії, переміщенні в тимчасові офіси або об'єкти в рамках того чи іншого проекту.

Ще однією важливою перевагою бездротових мереж є здатність адаптуватися до зміни потреб і технологій. Додавання нового обладнання в бездротову мережу не викликає особливих труднощів. Розглянемо приклад бездротового підключення в домашніх умовах. Користувачі можуть відвідувати веб-сайти, сидячи за кухонним столом, перебуваючи у вітальні або навіть поза приміщенням. Користувачі домашньої мережі підключають нові пристрої (наприклад смартфони, планшетні комп'ютери, ноутбуки і телевізори з інтелектуальними функціями).

Як показано на рис. 2, маршрутизатор бездротової домашньої мережі дозволяє користувачам підключатися до таких пристроїв без додаткових витрат і незручних кабелів, що проводяться між окремими приміщеннями в будинку.

Бездротовий зв'язок використовується в різних професійних областях.

Хоча діапазон бездротових технологій постійно розширюється, основним предметом розгляду в даному випадку є бездротові мережі, що забезпечують мобільність користувачів. Бездротові мережі в цілому можна розділити на наступні категорії:

Бездротова персональна мережа (WPAN). Радіус дії даної мережі становить кілька метрів. У мережах WPAN використовуються пристрої з підтримкою

Бездротові мережі LAN (WLAN). Мережі даного типу працюють в діапазоні кількох сотень метрів (наприклад, в кімнаті, в будинку, в офісі і навіть в мережах комплексу будівель).

Глобальні мережі (WWAN). Ці мережі діють в радіусі декількох кілометрів (наприклад, в муніципальній мережі, мережі стільникового зв'язку або навіть в каналах міжміського зв'язку за допомогою СВЧ-реле).

Натисніть на компоненти на малюнку, щоб відобразити додаткові відомості про різні бездротових технологіях, що підтримують підключення пристроїв до описаних вище бездротових мереж:

Bluetooth. Спочатку є стандартом WPAN IEEE 802.15, який використовує процес сполучення пристроїв для обміну даними на відстанях до 100 метрів (0,1 км). Пізніші версії Bluetooth стандартизовані відповідно до Bluetooth Special Interest Group (https://www.bluetooth.org/).

Wi-Fi (wireless fidelity, бездротова достовірність). Стандарт мереж WLAN IEEE 802.11, зазвичай розгорнутих з метою надання доступу до мережі для користувачів домашньої і корпоративної мережі (включаючи передачу даних, голосу і відео) на відстанях до 300 м (0,18 милі).

WiMAX (протокол широкосмугового радіозв'язку). Стандарт мереж WWAN IEEE 802.16, який забезпечує бездротовий широкосмуговий доступ на відстанях до 50 км (30 миль). WiMAX є альтернативою кабельному і широкосмугового DSL-підключення. У 2005 році в стандарт WiMax були додані мобільні функції, завдяки чому цей стандарт можуть використовувати оператори зв'язку для надання стільникового широкосмугового доступу.

Стільниковий широкосмуговий доступ. Складається з декількох корпоративних, державних і міжнародних організацій, що використовують стільниковий доступ до мережі оператора зв'язку в цілях надання широкосмугового мобільного підключення до мережі. Вперше використаний для стільникових телефонів 2-го покоління в 1991 році (2G). У 2001 і 2006 рр. в рамках технологій мобільного зв'язку третього (3G) і четвертого (4G) поколінь стали доступний більш високі швидкості.

Супутниковий широкосмуговий доступ. Надає мережевий доступ до віддалених об'єктів за рахунок використання спрямованої супутникової антени, відрегульованим по геостаціонарних супутників (GEO). Як правило, ця технологія відрізняється більш високою вартістю і до того ж вимагає забезпечення прямої видимості.

Всі бездротові пристрої працюють в діапазоні радіохвиль електромагнітного спектра. За регулювання виділення радіочастотного (РЧ) спектра відповідає Міжнародний союз електрозв'язку, сектор стандартизації електрозв'язку (ITU-R). Для різних цілей передбачені частотні діапазони, які називають смугами. Деякі смуги в електромагнітному спектрі жорстко регулюються і використовуються в таких областях, як контроль трафіку і мережі зв'язку аварійно-рятувальних служб. Інші смуги не підлягають ліцензуванню (наприклад, промислові, наукові та медичні частотні діапазони, а також частотні діапазони національної інформаційної інфраструктури).

Бездротовий зв'язок здійснюється в діапазоні радіохвиль (т. Е. 3-300 ГГц) електромагнітного спектра. Діапазон радіохвиль розділяється на сектор радіочастот і сектор СВЧ. Зверніть увагу, що мережі WLAN, Bluetooth, стільникового зв'язку та супутникового зв'язку працюють в діапазонах УВЧ, СВЧ і КВЧ.

Пристрої бездротової мережі LAN оснащені передавачами і приймачами, налаштованими на конкретні частоти діапазону радіохвиль. Зокрема, для бездротових LAN стандарту 802.11 виділяються наступні частотні смуги:

- 2,4 ГГц (УВЧ): 802.11b / g / n / ad
- 5 ГГц (СВЧ): 802.11a / n / ac / ad

- 60 ГГц (КВЧ): 802.11ad

Рис. 5.3.1

Стандарт мережі WLAN IEEE 802.11 визначає, яким чином радіочастоти в неліцензованому частотних смугах промислового, наукового та медичного діапазонів використовуються для фізичного рівня і підрівня MAC бездротових каналів.

За минулі роки розроблений ряд реалізацій стандарту IEEE 802.11. Нижче розглянемо ці стандарти докладніше.

802.11. Розроблено в 1997 році, тепер вважається застарілим. Це вихідна специфікація мережі WLAN, яка працює в частотній смузі 2,4 ГГц і забезпечує швидкості до 2 Мбіт / с. На момент створення цього стандарту провідні мережі LAN забезпечували швидкості на рівні 10 Мбіт / с, тому нові бездротові технології не отримали визнання на початковому етапі. Бездротові пристрої оснащені однією антеною для передачі і прийому бездротових сигналів.

IEEE 802.11a. Розроблено в 1999 році. Працює в менш завантаженою частотній смузі 5 ГГц і забезпечує швидкості до 54 Мбіт / с. Оскільки цей стандарт працює на більш високих частотах, він має меншу зону покриття і менш ефективний всередині будівель. Бездротові пристрої оснащені однією антеною для передачі і прийому бездротових сигналів. Пристрої, що працюють відповідно до цього стандарту, несумісні зі стандартами 802.11b і 802.11g.

IEEE 802.11b. Розроблено в 1999 році. Працює в частотній смузі 2,4 ГГц і забезпечує швидкості до 11 Мбіт / с. Пристрої, що працюють відповідно до цих

стандартів, мають більший діапазон і демонструють вищу ефективність при використанні всередині будівель в порівнянні з пристроями стандарту 802.11a. Бездротові пристрої оснащені однією антеною для передачі і прийому бездротових сигналів.

IEEE 802.11g. Розроблено в 2003 році. Працює в частотній смузі 2,4 ГГц і забезпечує швидкості до 54 Мбіт / с. Пристрої, що працюють відповідно до цього стандарту, працюють з тією ж радіочастотою і діапазоном, що і пристрої зі стандартом 802.11b, але мають пропускну здатність стандарту 802.11a. Бездротові пристрої оснащені однією антеною для передачі і прийому бездротових сигналів. Цей стандарт сумісний зі стандартом 802.11b. Однак при роботі з клієнтами стандарту 802.11b загальна пропускна здатність знижується.

IEEE 802.11n. Розроблено в 2009 році. Працює в частотних смугах 2,4 ГГц і 5 ГГц, відомий як двосмугове пристрій. Стандартні швидкості передачі даних - 150-600 Мбіт / с; діапазон дії - до 70 м. Проте, щоб забезпечити більш високі швидкості, точок доступу і бездротових клієнтам потрібно кілька антен, що використовують технологію багатоканального входу - багатоканального виходу (MIMO). Технологія MIMO використовує декілька антен в якості передавача і приймача, що дозволяє підвищити продуктивність обміну даними. Технологія підтримує до чотирьох антен. 802.11n підтримує зворотну сумісність з пристроями 802.11a / b / g. Однак підтримка змішаної середовища обмежує швидкість передачі даних.

IEEE 802.11ac. Розроблено в 2013 році, працює в частотній смузі 5 ГГц, забезпечуючи швидкість передачі даних в діапазоні від 450 Мбіт / с до 1,3 Гбіт / с (1300 Мбіт / с). Даний стандарт використовує технологію MIMO для підвищення продуктивності обміну даними. Для даного стандарту підтримується до восьми антен. Стандарт 802.11ac підтримує зворотну сумісність з пристроями 802.11a / n, але підтримка змішаних середовищ обмежує передбачувану швидкість передачі даних.

IEEE 802.11ad. Випуск запланований на 2014 рік. Цей стандарт також називають WiGig. Він використовує рішення для трисмуговий Wi-Fi, в якому задіяні частотні смуги 2,4 ГГц, 5 ГГц і 60 ГГц. Стандарт теоретично забезпечує швидкість передачі даних до 7 Гбіт / с. Проте, смуга 60 ГГц - це технологія, для роботи якої потрібна пряма видимість, отже, проходити крізь стіни сигнал не зможе. У роумінгу пристрої користувачів коммутируются на смуги 2,4 ГГц і 5 ГГц з більш низькою частотою. Стандарт підтримує зворотну сумісність з існуючими пристроями Wi-Fi. Однак підтримка змішаної середовища обмежує швидкість передачі даних.

На малюнку представлено короткий опис кожного зі стандартів 802.11.

Сравнение стандартов 802.11

Стандарт IEEE	Максимальная скорость	Частота	Обратная совместимость
802.11	2 Мбит/с	2,4 ГГц	–
802.11a	54 Мбит/с	5 ГГц	–
802.11b	11 Мбит/с	2,4 ГГц	–
802.11g	54 Мбит/с	2,4 ГГц	802.11b
802.11n	600 Мбит/с	2,4 ГГц и 5 ГГц	802.11a/b/g
802.11ac	1,3 Гбит/с (1300 Мбит/с)	5 ГГц	802.11a/n
802.11ad	7 Гбит/с (7000 Мбит/с)	2,4 ГГц, 5 ГГц и 60 ГГц	802.11a/b/g/n/ac

Рис. 5.3.2

Дані стандарти забезпечують сумісність пристроїв, виготовлених різними виробниками. Існують три міжнародні організації, що визначають стандарти мереж WLAN:

Сектор радіозв'язку ITU-R регулює розподіл спектра радіочастот і супутникових орбіт.

IEEE визначає, яким чином радіочастоти модулюються для перенесення даних. Ця організація обслуговує стандарти локальних і міських мереж (MAN), що відносяться до групи стандартів мереж LAN / MAN IEEE 802. Стандарти 802.3 Ethernet і 802.11 WLAN є основними в групі стандартів IEEE 802. Хоча IEEE визначає стандарти для пристроїв радіочастотної модуляції, ця організація не визначає стандарти виробництва. Отже, інтерпретації стандартів 802.11 різними постачальниками можуть перешкоджати взаємодії між різними пристроями.

Wi-Fi Alliance. Wi-Fi Alliance® (http://www.wi-fi.org) є глобальною некомерційною асоціацією промислової торгівлі, завдання якої - сприяти розвитку та впровадженню мереж WLAN. У цю асоціацію ввійшли постачальники, орієнтовані на підвищення сумісності продуктів стандарту 802.11 шляхом сертифікації постачальників на відповідність галузевим нормам і стандартам.

Wi-Fi Alliance сертифікує мережі Wi-Fi і такі види сумісності:

Сумісність з IEEE 802.11a / b / g / n / ac / ad

Безпечне використання WPA2 ™ і розширюваного протоколу аутентифікації (EAP) в рамках IEEE 802.11i

За допомогою Wi-Fi Protected Setup (WPS), яка спрощує з'єднання пристроїв

- Wi-Fi Direct для спільного використання середовища пристроями
- Wi-Fi Passpoint для забезпечення більш простого і безпечного підключення до мережі точок доступу Wi-Fi

- Wi-Fi Miracast для передачі і відображення відео між пристроями без проблем

Мережі WLAN мають таке ж походження, що і локальні мережі Ethernet. IEEE прийняла портфель стандартів архітектури ієрархічних мереж 802 LAN / MAN. Двома основними робочими групами є 802: 802.3 Ethernet і 802.11 WLAN. Проте, між цими двома групами є значні відмінності.

На фізичному рівні і MAC-підрівні рівня каналу передачі даних мережі WLAN використовують радіочастоти замість кабелів. Між кабелями і радіочастотами спостерігаються такі відмінності:

Радіочастоти не мають таких обмежень, як, наприклад, кабелі, захищені оболонкою. Тому кадри даних можуть передаватися по радіочастотним каналах з метою надання доступу до них для всіх, хто може приймати радіочастотний сигнал.

Радіочастоти не захищені від зовнішніх сигналів, в той час як кабель захищений екранує оболонкою. Радіочастоти функціонують незалежно один від одного в межах однієї географічної області, проте при роботі на одній і тій же або схожій частоті можуть виникати перешкоди.

Передача радіочастот пов'язана з тими ж проблемами, які властиві будь-хвильової технології, наприклад, радіо. Наприклад, у міру віддалення радіосигналу від джерела, радіостанції можуть накладатися один на одного, що підвищує рівень статичних перешкод. В кінцевому підсумку сигнал повністю втрачається. У провідних мережах LAN використовуються кабелі відповідної довжини, що забезпечують належну потужність сигналу.

У різних країнах радіочастотні смуги настроюються по-різному. Що стосується використання мереж WLAN діють додаткові правила і набори стандартів, які не застосовні до дротових мереж LAN.

Мережі WLAN також мають наступні відмінності від провідних мереж LAN:

Мережі WLAN служать для підключення клієнтів до мережі за допомогою точки бездротового доступу (ТД) або бездротового маршрутизатора, а не за допомогою комутатора Ethernet.

Мережі WLAN використовуються для підключення мобільних пристроїв, які часто працюють від акумулятора на відміну від пристроїв локальних мереж, підключених до розетки. Використання бездротових мережевих адаптерів скорочує час роботи мобільного пристрою від акумулятора.

Мережі WLAN підтримують вузли, конкуруючі в доступі до РЧ-носіїв (частотним смугам). Стандарт 802.11 наказує використання технологій запобігання колізій (CSMA / CA) замість технологій виявлення колізій (CSMA / CD) для доступу до середовища передачі даних, що дозволяє ефективно запобігати колізії в межах тієї чи іншої середовища.

У бездротових локальних мережах і дротових локальних мережах Ethernet використовуються різні формати кадрів. Для бездротових локальних мереж в заголовок кадру 2 рівня необхідно додати додаткову інформацію.

Відносно мереж WLAN виникає більше проблем, пов'язаних з конфіденційністю, оскільки радіочастоти можуть виходити за межі об'єкта.

Для створення найпростішої бездротової мережі потрібно не менше двох пристроїв. Кожне з пристроїв повинно містити радіопередавач і радіоприймач, налаштовані на однакові частоти.

Однак для більшості бездротових розгортання потрібні:

- Кінцеві пристрої, оснащені бездротовими мережевими адаптерами
- Пристрій інфраструктури (наприклад, бездротовий маршрутизатор або точка бездротового доступу)

Для бездротового обміну даними кінцевим пристроям потрібно бездротової мережевий адаптер з вбудованим радіопередавачем / радіоприймачем, а також драйвер, необхідний для роботи адаптера. Всі сучасні ноутбуки, планшетні комп'ютери і смартфони оснащені інтегрованими безпровідними мережевими адаптерами. Однак, якщо в пристрої немає інтегрованого бездротового мережевого адаптера, можна використовувати бездротовий USB-адаптер.

На малюнку показані два бездротових USB-адаптера.

Рис. 5.3.3

Тип пристрою інфраструктури, на якому термінал виконує асоціацію та аутентифікацію, варіюється в залежності від розміру і вимог мережі WLAN.

Наприклад, користувач домашньої мережі зазвичай підключає бездротові пристрої один до одного за допомогою невеликого інтегрованого бездротового

маршрутизатора. Такі невеликі маршрутизатори з інтеграцією сервісів виконують такі функції:

Точка доступу - надає бездротовий доступ 802.11a / b / g / n / ac.

Комутатор - надає комутатор Ethernet 10/100/1000 з чотирма портами і повнодуплексним режимом для підключення провідних пристроїв.

Маршрутизатор - надає шлюз для зв'язку з іншими мережевими інфраструктурами.

Наприклад, маршрутизатор Cisco Linksys EA6500, представлений на рис. 1, зазвичай реалізується в якості пристрою бездротового доступу до корпоративної мережі малого підприємства або домашньої мережі. Бездротовий маршрутизатор підключається до DLS-модему і оголошує свої служби шляхом відправки сигналів, що містять загальний ідентифікатор набору послуг (SSID). Внутрішні пристрої виконують бездротове виявлення ідентифікатора маршрутизатора SSID і намагаються виконати асоціацію та аутентифікацію на маршрутизаторі для отримання доступу до мережі Інтернет.

Передбачувана навантаження на маршрутизатор Linksys EA6500 в цьому середовищі досить низька. Таким чином, маршрутизатор може керувати забезпеченням доступу до мережі WLAN, 802.3 Ethernet і підключенням до мережі інтернет-провайдера. Маршрутизатор також надає ряд додаткових функцій, серед яких високошвидкісний доступ, оптимізація для підтримки передачі потокового відео, підтримка IPv6, служба якості обслуговування (QoS), спрощена установка і настройка за допомогою Wi-Fi WPS, USB-порти для підключення принтерів або портативних накопичувачів.

Крім того, користувачі домашньої мережі, яким ви бажаєте покращити набір мережевих послуг як в провідний, так і в бездротової мережі, можуть скористатися бездротовими адаптерами Powerline. За допомогою цих адаптерів пристрій може безпосередньо підключитися до мережі через розетки електроживлення, що ідеально підходить для передачі потокового HD-відео і трансляції онлайн-ігор. Ці пристрої прості в установці: просто підключіться до розетки електроживлення або мережевого фільтру і підключіть пристрої простим натисканням кнопки.

Організаціям, що надають підключення до бездротової мережі для своїх користувачів, потрібно інфраструктура мережі WLAN, що забезпечує додаткові можливості підключення.

Примітка. В рамках стандарту IEEE 802.11 бездротової клієнт називається станцією (STA). У цьому розділі термін «бездротової клієнт» позначає будь-який пристрій, що підтримує підключення до бездротової мережі.

Мережа малого підприємства, показана на рис. 1, є мережею LAN стандарту 802.3 Ethernet LAN. Кожен клієнт (наприклад PC1 і PC2) підключається до комутатора через мережевий кабель. Комутатор є тією точкою, де клієнт отримує доступ до мережі. Зверніть увагу, що точка бездротового доступу також підключена до комутатора. У цьому прикладі для підключення до бездротової мережі може використовуватися точка доступу Cisco WAP4410N або WAP131.

Рис. 5.3.4

Бездротові клієнти використовують свої бездротові мережні адаптери для виявлення найближчих точок доступу, які оголосили свій ідентифікатор SSID. Після цього клієнти намагаються виконати асоціацію та аутентифікацію на точці доступу, як показано на рис. 2. Після проходження аутентифікації користувачі бездротової мережі отримують доступ до ресурсів мережі.

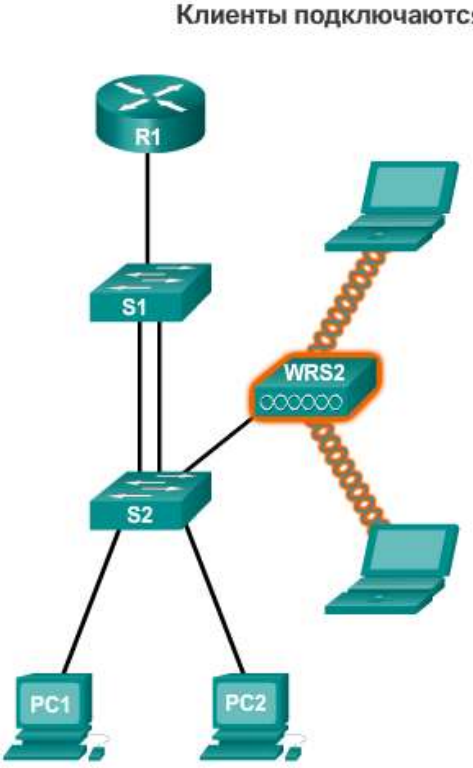


Рис. 5.3.5

Примітка. Невеликі компанії пред'являють до ресурсів бездротової інші вимоги, ніж великі компанії. Великі бездротові мережі вимагають додаткового бездротового обладнання з метою спрощення установки і управління бездротовою мережею.

Автономні точки доступу, які іноді називають «важкими», являють собою автономні пристрої, що настроюються за допомогою графічного інтерфейсу користувача або інтерфейсу командного рядка (CLI) Cisco. Автономні точки доступу рекомендується використовувати в тих випадках, коли в мережі потрібно не більше двох точок доступу. Як варіант, управління декількома точками доступу може здійснюватися за допомогою служб бездротового домену (WDS) і CiscoWorks Wireless LAN Solution Engine (WLSE).

На рис. 1 показана автономна точка доступу в невеликої мережі. Зі збільшенням попиту на ресурси бездротової мережі може виникнути потреба в більшій кількості точок доступу. Кожна точка доступу працює незалежно від інших точок доступу. Налагодження та управління ними здійснюється вручну.

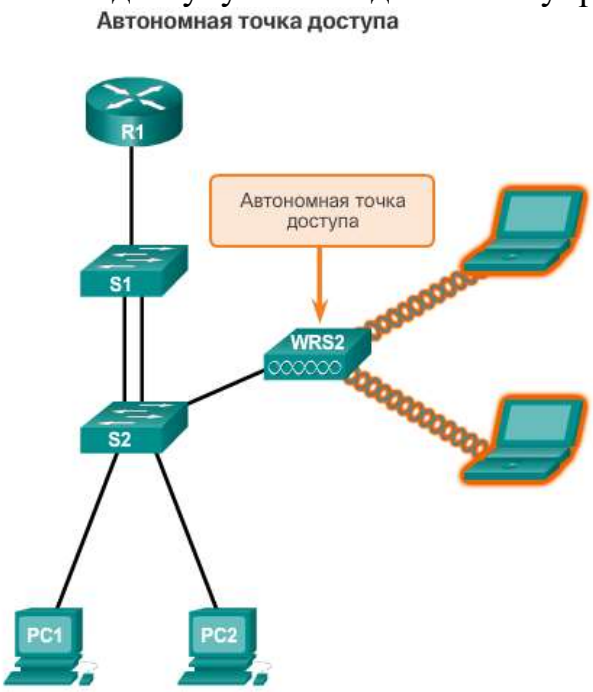


Рис. 5.3.6

Точки доступу, керовані контролером, є незалежними від сервера пристроями, для яких не потрібно початкова настройка. Cisco пропонує два бездротових рішення з використанням контролера. Точки доступу, керовані контролером, рекомендується використовувати у випадках, коли в мережі потрібно багато точок доступу. У міру додавання додаткових точок доступу настройка і управління кожною з них здійснюється контролером WLAN автоматично.

На рис. показана точка доступу, керована контролером в невеликої мережі. Зверніть увагу на те, як контролер мережі WLAN тепер необхідний для управління точками доступу. Перевага при використанні контролера полягає в тому, що його можна використовувати для управління декількома точками доступу.

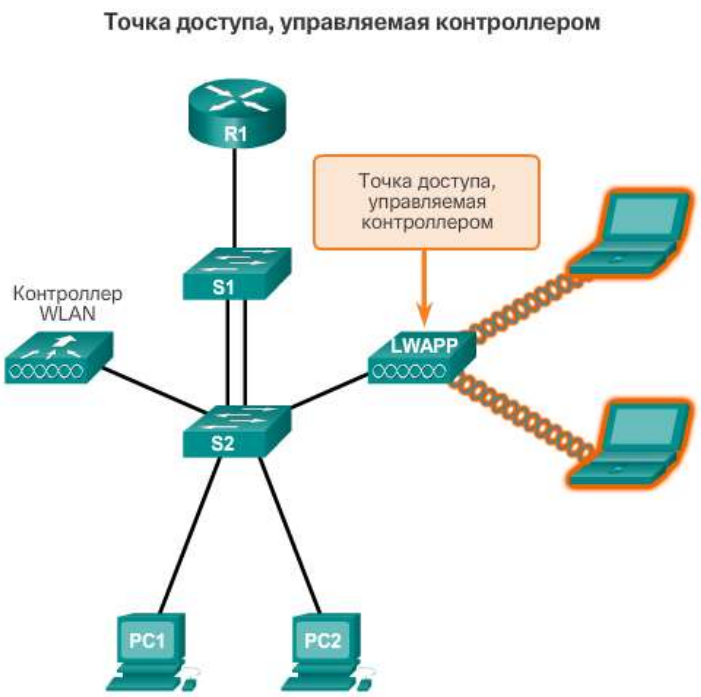


Рис. 5.3.7

Примітка. Деякі точки доступу можуть працювати як в автономному режимі, так і в режимі точки доступу, керованої контролером.

Для невеликих бездротових мереж Cisco пропонує наступні рішення у вигляді бездротових автономних точок доступу.

Точка доступу Cisco WAP4410N. Ця точка доступу ідеально підходить для невеликих компаній, яким потрібні дві точки доступу і підтримка невеликої групи користувачів.

Точки доступу Cisco WAP121 і WAP321. Ці точки доступу ідеально підходять для невеликих компаній, яким потрібно спростити бездротову мережу за рахунок використання декількох точок доступу.

Точка доступу Cisco AP541N. Ця точка доступу ідеально підходить для невеликих і середніх компаній, яким потрібен надійний і простий в управлінні кластер точок доступу.

Саме тому точки доступу WAP121, WAP321 і AP541N підтримують кластеризацію точок доступу без використання контролера. Кластер надає єдину точку адміністрування та дозволяє адміністратору переглядати розгортання точок доступу як одну бездротову мережу, а не як набір окремих бездротових пристроїв. Кластеризація дозволяє легко здійснювати установку, настройку і управління зростаючої бездротовою мережею. Кілька точок доступу можна розгорнути і налаштувати з одного конфігурацією на всіх пристроях в межах кластера. При цьому управління бездротовою мережею здійснюється як єдиною системою, і немає необхідності турбуватися про взаємні перешкоди між точками доступу або налаштовувати кожну точку доступу окремо.

Зокрема, точки доступу WAP121 і WAP321 підтримують єдину точку настройки (Single Point Setup, SPS), що забезпечує більш швидке і просте розгортання точки доступу, як показано на рис. 3. SPS дозволяє включити для мережі LAN можливість масштабування до чотирьох точок доступу WAP121 і до восьми точок доступу WAP321, що забезпечує більше покриття та підтримку

додаткових користувачів у міру зростання і зміни бізнес-вимог. Точка доступу Cisco AP541N здатна об'єднати в кластер до 10 точок доступу і підтримує кілька кластерів.

Рис. 5.3.8

Компанії, яким потрібна кластеризація декількох точок доступу, потребують більш надійному і масштабованому вирішенні. Для великих компаній, що використовують велику кількість точок доступу, Cisco надає керовані рішення на основі контролера, включаючи керовану хмарну архітектуру Cisco Meraki і архітектуру бездротової мережі Cisco Unified.

Примітка. Доступні і інші рішення на основі контролера, наприклад, контролери, які використовують режим Flex. Для отримання додаткових відомостей перейдіть на веб-сайт http://www.cisco.com.

Хмарна архітектура Cisco Meraki є рішення для управління, яке дозволяє спростити розгортання бездротової мережі. Завдяки цій архітектурі управління точками доступу здійснюється централізовано з контролера в хмарі, як показано на рис. 1. Хмарні мережі і управління забезпечують централізоване управління, видимість і контроль без використання дорогих і складних контролерів і програмного забезпечення для адміністрування оверлейного навантаження.

Цей процес дозволяє скоротити витрати і знизити рівень складності. Контролер передає настройки управління (наприклад, оновлення мікропрограмного забезпечення), настройки безпеки, настройки бездротової мережі і ідентифікатор SSID на точки доступу Meraki.

Примітка. Через хмарну інфраструктуру Meraki проходять тільки потоки керуючих даних. Призначений для користувача трафік не проходить через центри обробки даних Meraki. Таким чином, якщо Cisco Meraki не має доступу до хмари, мережа продовжує функціонувати без збоїв. Це означає, що

користувачі можуть як і раніше проходити аутентифікацію, діють правила брандмауера, а потоки трафіку передаються на повній лінійній швидкості. Лише функції управління перестають працювати (наприклад, інструменти створення звітів і настройки).

Для керованої хмарної архітектури Cisco Meraki потрібні такі компоненти:

Точки бездротового доступу під хмарним керуванням Cisco. Для різних бездротових мереж існують різні моделі.

Хмарний контролер Meraki (MCC). Контролер MCC надає для системи бездротової локальної мережі Meraki функції централізованого управління, оптимізації та моніторингу. MCC - це не пристрій, який потрібно придбати і встановити для управління точками бездротового доступу. MCC, скоріше, являє собою хмарний сервіс, який постійно виконує моніторинг, оптимізацію та створення звітів про поведінку мережі.

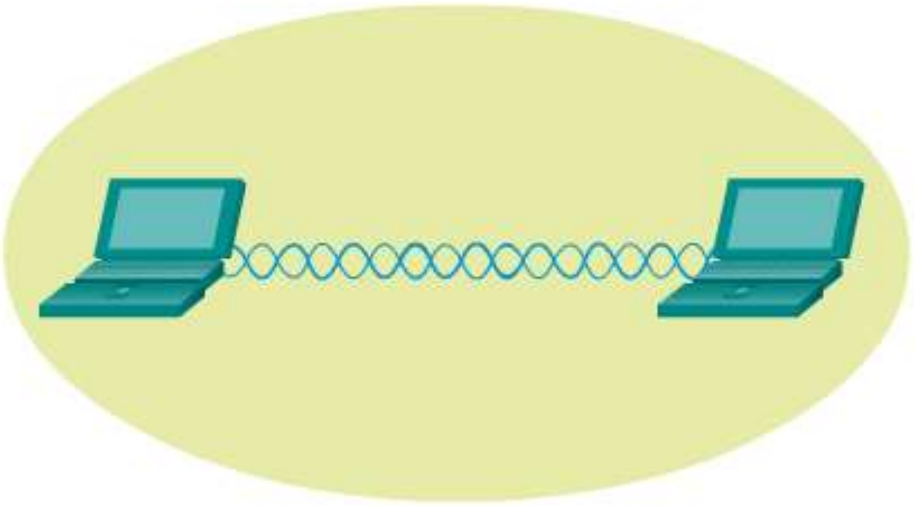
Бездротові мережі LAN можуть використовувати різні топології мережі. Стандарт 802.11 визначає два основні режими топології бездротової мережі:

Режим прямого підключення (ad hoc). В цьому режимі два пристрої з'єднані по бездротовій мережі без використання таких пристроїв інфраструктури, як бездротовий маршрутизатор або точка доступу. До прикладів цього режиму можна віднести Bluetooth і Wi-Fi Direct.

У постійному робочому режимі. В цьому режимі бездротові клієнти з'єднані один з одним за допомогою бездротового маршрутизатора або точки доступу (наприклад, як в мережах WLAN). Точки доступу підключені до мережевої інфраструктури за допомогою кабельної розподільної системи, наприклад, Ethernet.

Бездротова мережа з прямим з'єднанням увазі обмін даними між двома бездротовими пристроями в тимчасової мережі без використання точок доступу або бездротових маршрутизаторів. Наприклад, клієнтську робочу станцію з підтримкою бездротового зв'язку можна налаштувати для роботи в режимі прямого з'єднання, що забезпечує можливість підключення до неї інших пристроїв. До прикладів режиму прямого з'єднання можна віднести Bluetooth і Wi-Fi Direct.

Сводная информация по режиму прямого подключения



Сводная информация по IBSS	
Режим топологии сети WLAN	Прямое подключение
Технология беспроводной связи 802.11	Независимый базовый набор сервисов (IBSS)
Количество существующих точек доступа	0
Зона покрытия 802.11	Зона основного обслуживания (BSA)

Рис. 5.3.9

Існує версія тимчасової топології, в рамках якої смартфон або планшетний комп'ютер з з'єднанням для передачі даних через стільникову мережу використовуються для створення персональної точки бездротового доступу. Ця функція іноді називається режимом модема. Точка бездротового доступу, як правило, є тимчасовим короткостроковим рішенням, завдяки якому смартфон може забезпечувати сервіси бездротового зв'язку Wi-Fi-маршрутизатора. Інші пристрої можуть виконувати асоціацію та аутентифікацію на смартфоні або планшетному комп'ютері для доступу до мережі Інтернет. В Apple iPhone ця функція називається «Персональна точка бездротового доступу», а в пристроях Android - «Режим модема» або «Портативна точка доступу».

Архітектура IEEE 802.11 складається з декількох компонентів, які взаємодіють для надання мережі WLAN, що забезпечує підтримку клієнтів. Вона визначає два структурних елементи топології інфраструктурного режиму: базовий набір сервісів (BSS) і розширений набір сервісів (ESS).

BSS складається з однієї точки доступу, яка взаємодіє з усіма пов'язаними бездротовими клієнтами. На рис. 1 показані два набори BSS. Колами позначена зона покриття, в межах якої бездротові клієнти BSS можуть підтримувати зв'язок один з одним. Ця зона називається зоною основного обслуговування (BSA). Якщо бездротової клієнт виходить із зони основного обслуговування, він більше не може спілкуватись із іншими бездротовими пристроями в межах

зони BSA. BSS є структурним елементом топології, а BSA - фактичної зоною покриття (терміни BSA і BSS часто використовуються як взаємозамінні).

Сводная информация по базовому набору сервисов (BSS)

Сводная информация по BSS	
Режим топологии сети WLAN	Инфраструктура
Технология беспроводной связи 802.11	Базовый набор сервисов (BSS)
Количество существующих точек доступа	1

Рис. 5.3.10

MAC-адресу 2 рівня використовується для унікальної ідентифікації кожного набору BSS, який називається ідентифікатором базового набору сервісів (BSSID). Таким чином, ідентифікатор BSSID є формальним ім'ям BSS і завжди пов'язаний тільки з однією точкою доступу.

Коли один набір BSS забезпечує недостатнє радіочастотне покриття, то за допомогою загальної розподільчої системи можна зв'язати два або більше наборів BSS, що утворює розширений набір сервісів (ESS). Як показано на рис. 2, набір сервісів ESS є об'єднанням двох або більше наборів BSS, взаємопов'язаних за допомогою кабельної розподільної системи. Тепер бездротові клієнти в одній зоні BSA можуть обмінюватися даними з бездротовими клієнтами в іншій зоні BSA в межах одного набору ESS. Переміщаються мобільні бездротові клієнти в роумінгу можуть переходити з однієї зони BSA в іншу (з тим же набором ESS) і без проблем виконувати підключення.

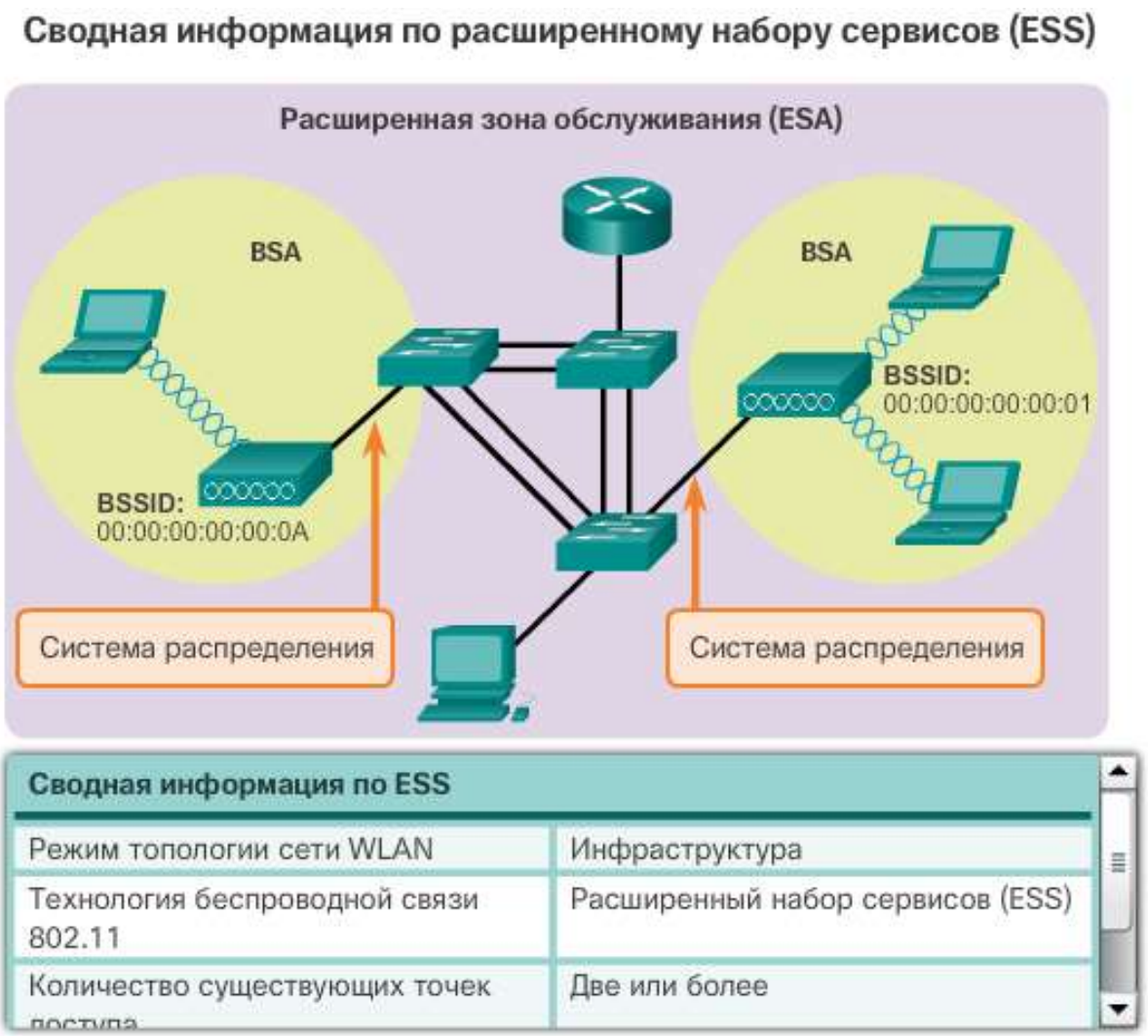


Рис. 5.3.11

Прямокутною областю позначена зона покриття, в межах якої учасники набору ESS можуть здійснювати обмін даними. Ця область називається зоною розширеного обслуговування (ESA). ESA, як правило, містить кілька наборів BSS в перекриваються і / або окремих конфігураціях.

Кожен ESS визначається ідентифікатором SSID, а в ESS кожен BSS визначається ідентифікатором BSSID. З міркувань безпеки додаткові ідентифікатори SSID можуть заповнюватися в ESS для відділення рівня доступу до мережі.

Як показано на рис. 1, всі кадри 2 рівня складаються з заголовка, корисного навантаження та розділу FCS. Формат кадру 802.11 аналогічний формату, використовуваному в Ethernet, за тим винятком, що він містить більше полів.

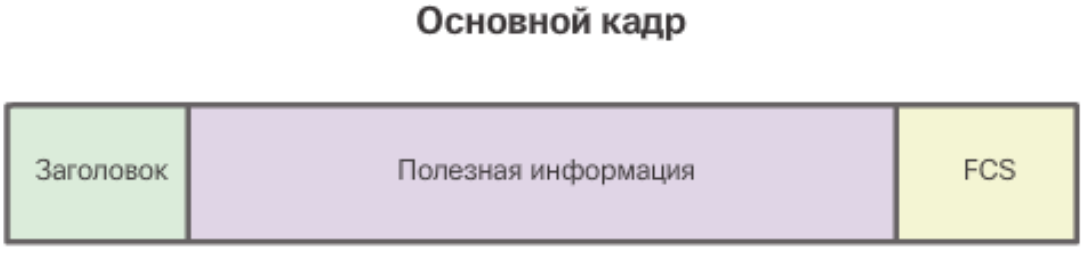


Рис. 5.3.12

Як показано на рис. всі кадри бездротової мережі 802.11 містять такі поля:

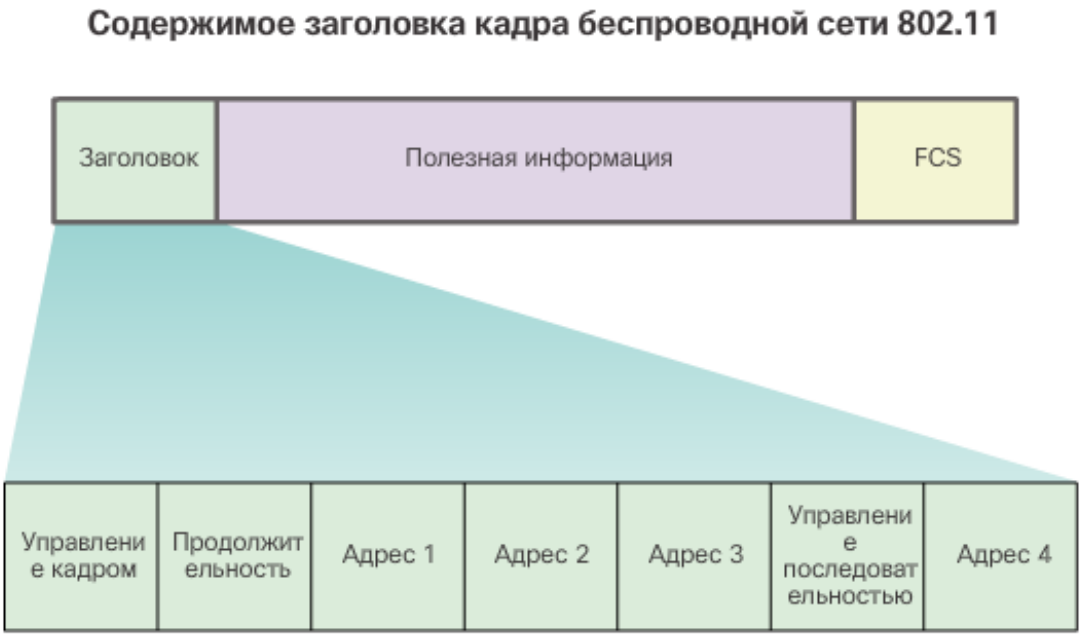


Рис. 5.3.13

Управління кадром (Frame Control). Визначає тип кадру бездротової мережі і містить підполя для версії протоколу, типу кадру, типу адреси, налаштувань управління живленням і безпеки.

Тривалість (Duration). Як правило, використовується для позначення часу, що залишився, необхідного для прийому наступного кадру, що передається.

Адреса 1 (Address1). Як правило, містить MAC-адресу приймаючої бездротового пристрою або точки доступу.

Адреса 2 (Address2). Як правило, містить MAC-адресу передавального бездротового пристрою або точки доступу.

Адреса 3 (Address3). В окремих випадках містить MAC-адресу призначення, наприклад, інтерфейс маршрутизатора (шлюзу), до якого підключений з точкою доступу.

Контроль послідовності (Sequence Control). Містить підполя для номера послідовності і номера фрагмента. Номер послідовності позначає номер послідовності кожного кадру. Номер фрагмента позначає номер кожного кадру, відправленого з фрагментированного кадру.

Адреса 4 (Address4). Зазвичай відсутній, оскільки використовується тільки в режимі прямого з'єднання.

CS. Контрольна послідовність кадру, яка використовується для контролю помилок 2 рівня.

На рис. 3 показаний захоплення кадру сигналу мережі WLAN програмою Wireshark. Зверніть увагу на те, як поле управління кадром також розширюється для відображення всіх підполів.

Захват кадра 802.11 программой Wireshark

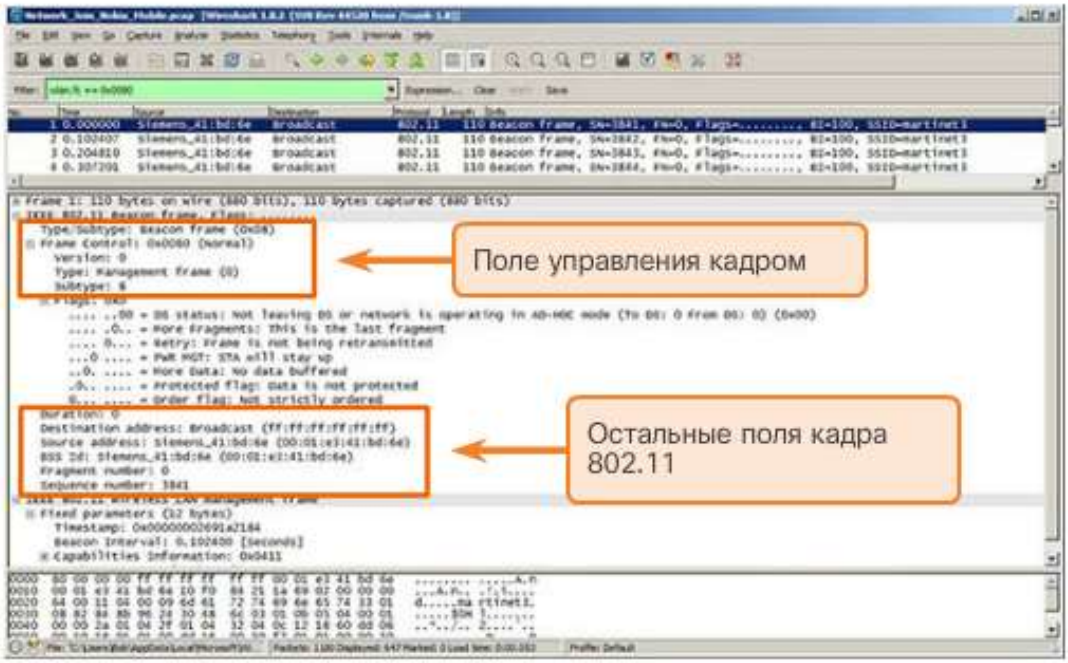


Рис. 5.3.14

Примітка. Вміст полів адреси варіюється в залежності від налаштувань поля управління кадром.

Содержимое поля управления кадром

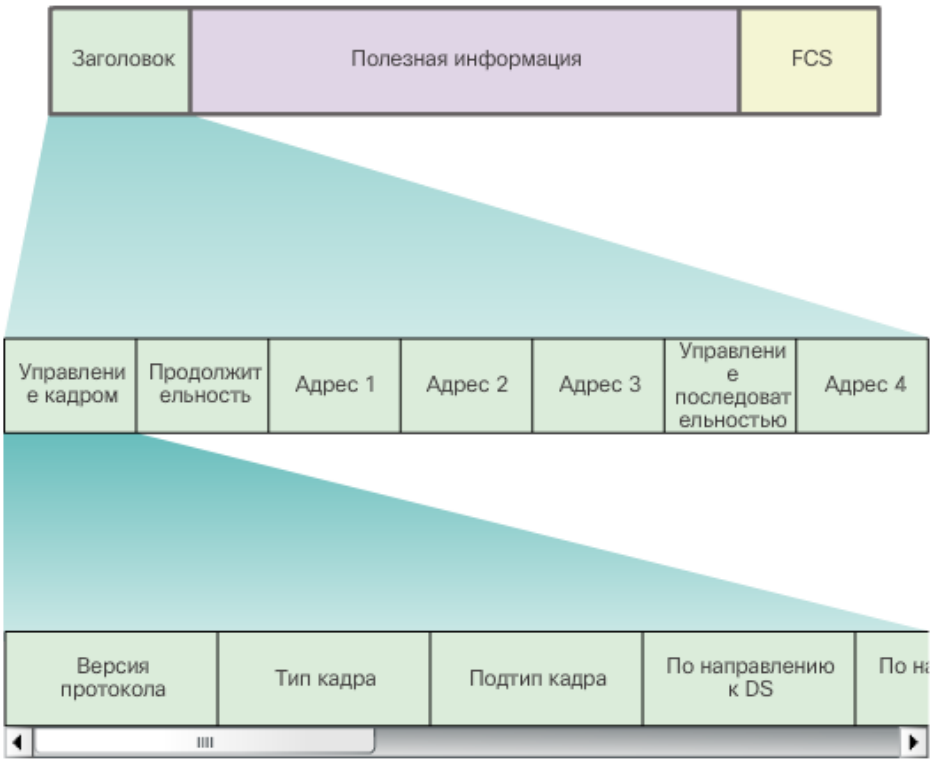


Рис. 5.3.15

Версія протоколу (Protocol Version). Вказує поточну версію використовуваного протоколу 802.11. Приймаючі пристрої використовують це значення, щоб визначити, чи підтримується версія протоколу прийнятого кадру.

Тип кадру (Frame Type) і підтип кадру (Frame Subtype). Визначає функцію кадру. Кадр бездротової мережі може бути контрольним кадром, кадром даних або кадром управління. Для кожного типу кадру є кілька полів підтипів. Кожен підтип визначає конкретну функцію, яка буде виконуватися для пов'язаного з ним типу кадру.

У напрямку до DS (ToDS) і по напрямку від DS (FromDS). Вказує, чи є кадр вхідними або вихідними по відношенню до DS. Використовується тільки в кадрах даних або бездротових клієнтів, пов'язаних з точкою доступу.

Фрагменти >>> (More Fragments). Вказує, чи планується надходження додаткових фрагментів кадру (кадру даних або управління).

Повторити (Retry). Вказує, чи виконується повторна передача кадру даних або управління.

Управління харчуванням (Power Management). Вказує, чи знаходиться передавальний пристрій в активному режимі або в режимі енергозбереження.

Додаткові дані >>> (More Data). Повідомляє пристрою в режимі енергозбереження, що точка доступу планує відправити додаткові кадри. Також використовується для точок доступу з метою вказівки на те, що планується відправка додаткових кадрів широкомовної / групового розсилання.

Безпека (Security). Вказує на те, чи використовуються в кадрі шифрування і аутентифікація. Даний підтип можна задати для всіх кадрів даних і кадрів управління, для яких заданий підтип аутентифікації.

Зарезервовано (Reserved). Може вказувати на те, що всі прийняті кадри даних повинні оброблятися по порядку.

На рис. 2 показаний захоплення кадру сигналу мережі WLAN програмою Wireshark. Зверніть увагу, що поля типу і підтипу кадру визначають, чи є кадр контрольним, кадром управління або даних. У цьому прикладі тип кадру має значення «0x0», що визначає його як кадр управління. Значення підтипу «8» визначає кадр як кадру сигналу. Цей кадр позначений як «0x08».

Захват кадра 802.11 программой Wireshark

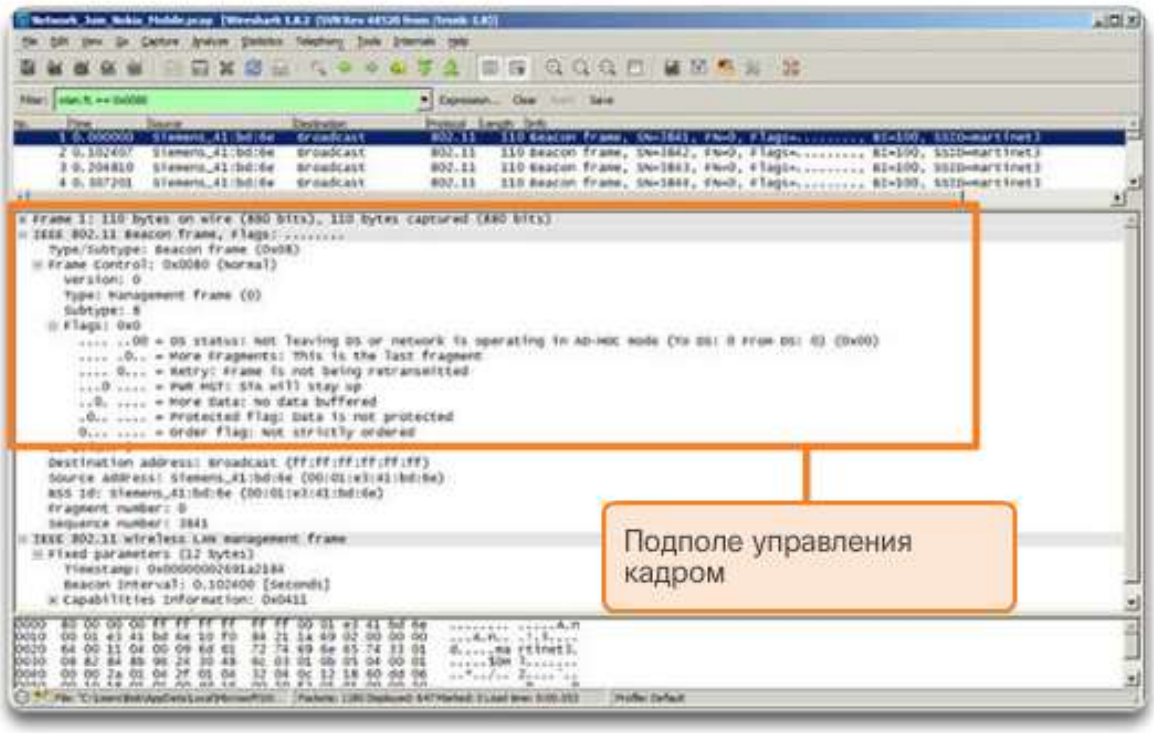


Рис. 5.3.16

Кадр управління - використовується в процесі обслуговування процесу обміну даними, наприклад, при пошуку, аутентифікації і асоціації з точкою доступу.

Контрольний кадр - використовується для спрощення обміну кадрами даних між бездротовими клієнтами.

Кадр даних - використовується для перенесення корисного навантаження (наприклад, веб-сторінок і файлів).

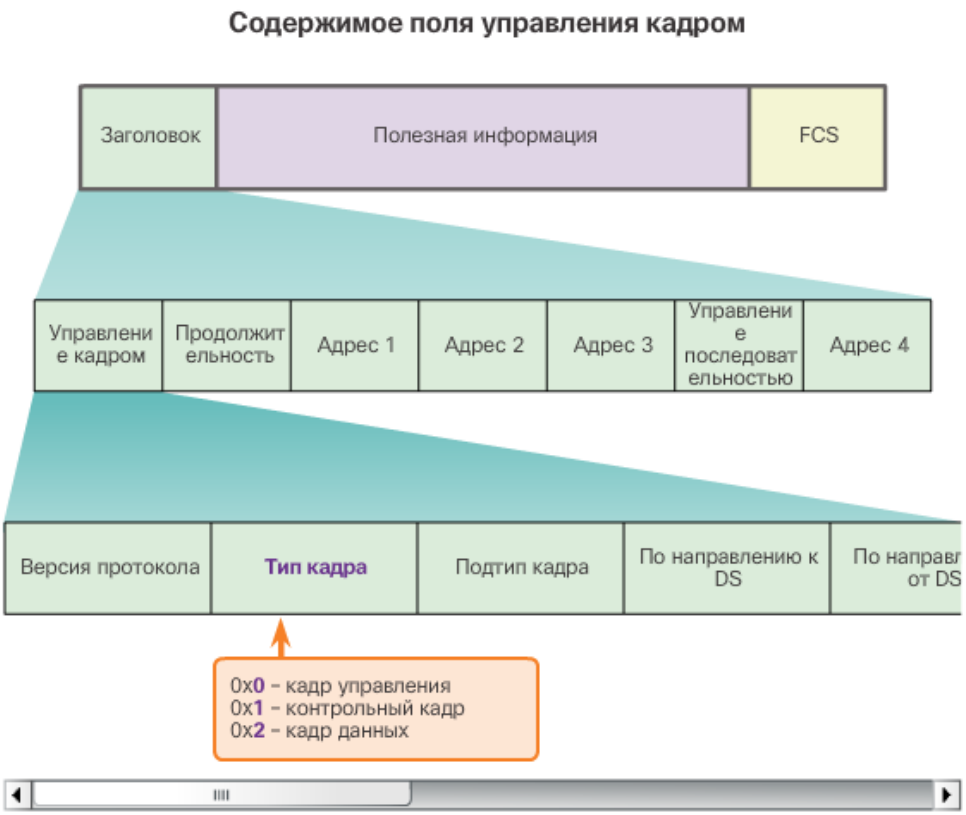


Рис. 5.3.17

Кадри управління

Кадри управління використовуються виключно для пошуку, аутентифікації і асоціації з точкою доступу.

На рис. 1 відображається значення поля стандартних кадрів управління, включаючи:

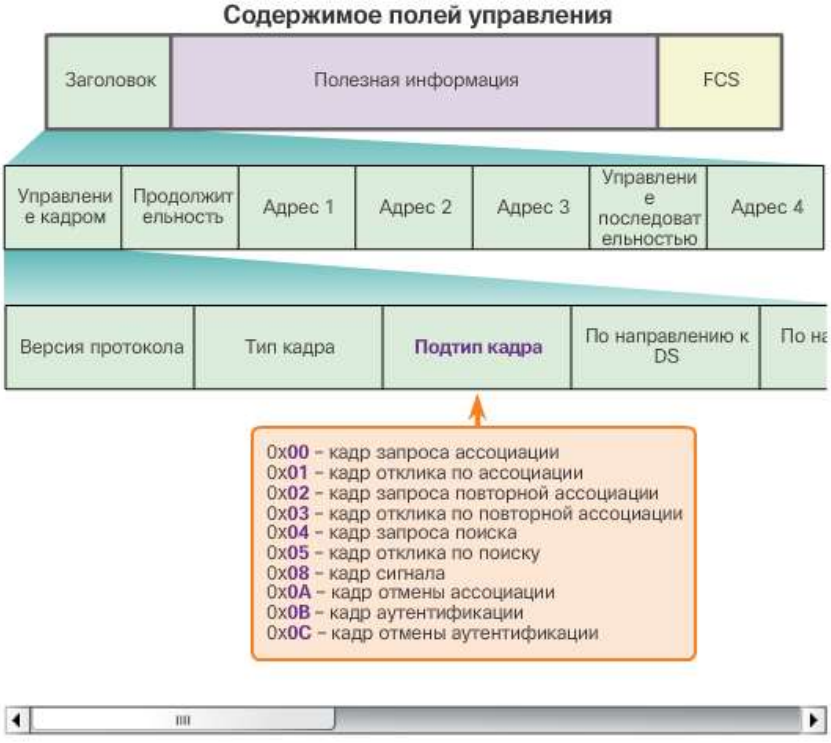


Рис. 5.3.18

Кадр запиту асоціації - (0x00). Відправляється з бездротового клієнта і дозволяє точці доступу виділити ресурси і виконати синхронізацію. Кадр

переносить дані про бездротовому підключенні, включаючи підтримувані швидкості передачі даних і ідентифікатор SSID мережі, бездротового клієнта, який хоче виконати асоціацію. Якщо запит прийнятий, точка доступу резервує пам'ять і встановлює ідентифікатор асоціації для пристрою.

Кадр відгуку на запит асоціації - (0x01). Відправляється з точки доступу бездротового клієнта і містить підтвердження або відхилення запиту асоціації. Якщо це кадр, що підтверджує асоціацію, то він містить інформацію про ідентифікатор асоціації і підтримуваних швидкостях передачі даних.

Кадр запиту повторної асоціації - (0x02). Пристрій надішле запит повторної асоціації, коли кадр скидається від діапазону точок доступу, до яких він був прив'язаний, і виконує пошук іншої точки доступу з сигналом більш високої потужності. Нова точка доступу координує пересилку будь-яких даних, які як і раніше можуть міститися в буфері попередньої точки доступу.

Кадр відгуку на запит про повторну асоціації - (0x03). Відправляється з точки доступу бездротового клієнта і містить підтвердження або відхилення запиту на повторну асоціацію. Кадр містить інформацію, необхідну для асоціації, наприклад ідентифікатор асоціації і підтримувані швидкості передачі даних.

Кадр запиту пошуку - (0x04). Відправляється з бездротового клієнта в разі, якщо йому потрібні дані від іншого бездротового клієнта.

Кадр відгуку з пошуку - (0x05). Відправляється з точки доступу після отримання кадру запиту пошуку і містить відомості про можливості, наприклад підтримувані швидкості передачі даних.

Кадр сигналу - (0x08). Регулярно відправляється з точки доступу в цілях оголошення про її присутності і надання ідентифікатора SSID та інших розумних налаштувань.

Кадр скасування асоціації - (0x0A). Відправляється з пристрою, який має намір завершити з'єднання. Дозволяє точки доступу вивільнити виділену пам'ять і видалити пристрій з таблиці асоціації.

Кадр аутентифікації - (0x0B). Передавальний пристрій відправляє кадр аутентифікації в точку доступу, яка містить його посвідчення.

Кадр скасування аутентифікації - (0x0C). Відправляється з бездротового клієнта, який очікує завершення з'єднання з іншим бездротовим клієнтом.

Сигнали - це єдині кадри управління, які можуть регулярно передаватися по широкомовної розсилки точкою доступу. Всі інші кадри пошуку, аутентифікації і асоціації використовуються тільки під час асоціації (або повторної асоціації).

На рис. 2 показаний приклад простого захоплення кадру управління програмою Wireshark. Значення полів змінюються в залежності від призначення кадру.

Кадр сигнала управления

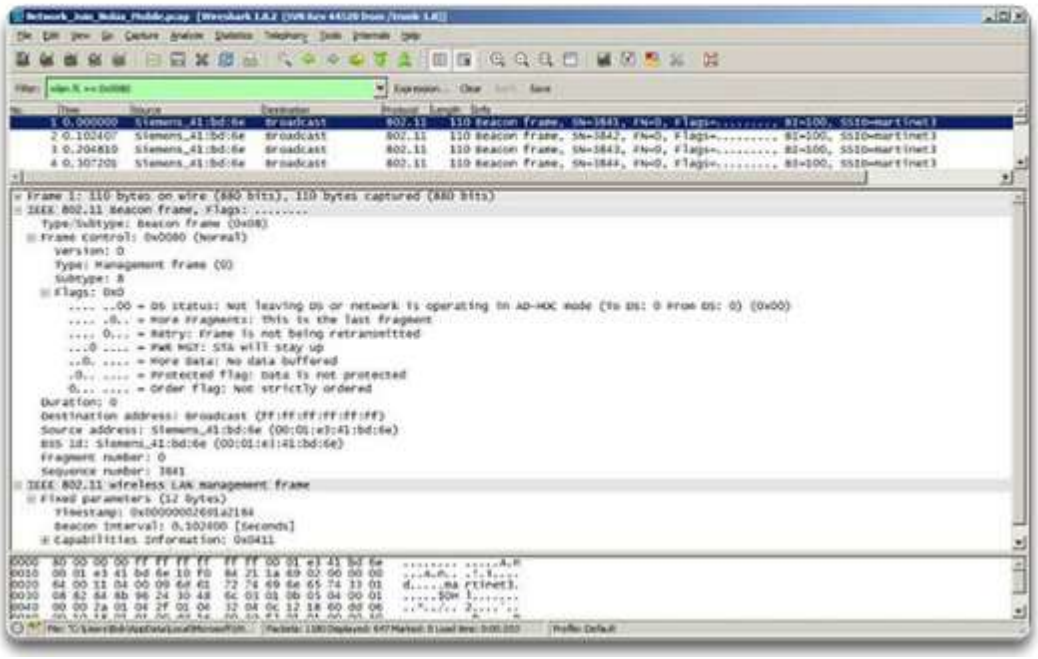


Рис. 5.3.19

Примітка. У зазначеному прикладі захоплення здійснюється за допомогою програми Wireshark. Однак програму Wireshark необхідно спеціально налаштувати для захоплення трафіку мережі WLAN. Різні операційні системи мають різний здатністю щодо захоплення трафіку, і для цього можуть вимагатися спеціальні бездротові мережні адаптери.

Контрольні кадри використовуються для управління обміном даними між бездротовим клієнтом і точкою доступу. Вони дозволяють запобігати колізії в бездротової середовищі.

На малюнку відображається значення поля стандартних кадрів управління, включаючи:

Керуючі кадри RTS (запит на передачу) - кадри RTS і CTS (дозвіл відправки) надають додаткову схему зменшення колізій для точок доступу, що містять приховані бездротові клієнти. Бездротовий клієнт відправляє кадр RTS на першому етапі двостороннього квітірованія, яке є обов'язковим етапом, виконуваних перед відправкою кадрів даних.

Керуючі кадри CTS (дозвіл відправки) - точка бездротового доступу відправляє кадр CTS як відгук на прийнятий кадр RTS. Цей кадр надає запитуючій бездротовому клієнту підтвердження відправки кадру даних. Якщо в CTS додано значення часу, то це сприяє управлінню колізіями. Ця затримка знижує шанси на передачу даних іншими клієнтами під час передачі даних робить запит клієнтом.

Кадр ACK (підтвердження) - після отримання кадру даних приймає бездротової клієнт відправляє кадр ACK відправляє клієнту, якщо не знайдені помилки. Якщо відправляє клієнт не приймає кадр ACK протягом попередньо визначеного періоду, що відправляє клієнт відправляє кадр повторно.

Контрольні кадри є невід'ємною частиною процесу бездротової передачі даних і грають важливу роль в методі вирішення конфліктів в середовищі передачі даних, відомому як множинний доступ з контролем несучої і запобіганням колізій (CSMA / CA).

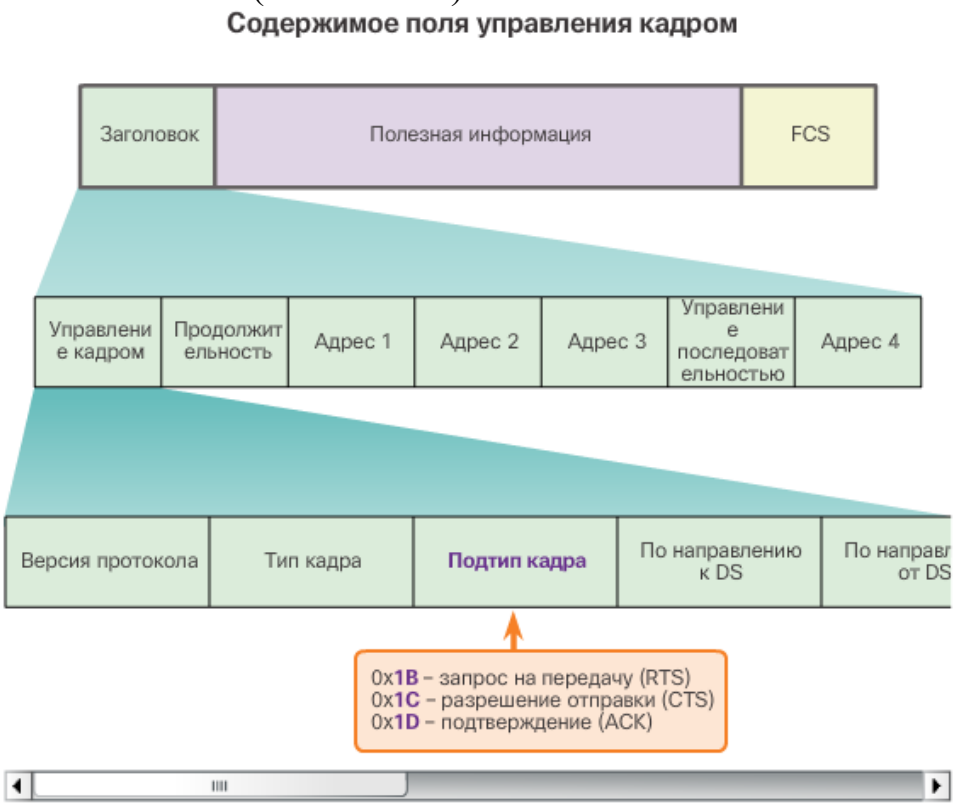


Рис. 5.3.20

Слід пам'ятати, що метод вирішення конфліктів в середовищі має на меті визначення пристроями способу і часу доступу до середовища в разі, якщо потрібно пересилання трафіку по мережі. Мережі WLAN IEEE 802.11 використовують протокол MAC CSMA / CA. Хоча його назва схоже на Ethernet CSMA / CD, його принцип дії зовсім інший.

Системи Wi-Fi працюють в напівдуплексному режимі і містять загальні зміни середовища, отже, бездротові клієнти можуть передавати і приймати дані по одному радіоканалу. Через це виникають проблеми, оскільки бездротової клієнт не отримує дані в процесі відправки. Таким чином, виявлення колізій неможливо. Для вирішення цієї проблеми Інститутом інженерів з електротехніки та електроніки (IEEE) був розроблений додатковий механізм запобігання колізій, відомий як функція розподіленої координації (DCF). За допомогою DCF бездротової клієнт передає дані тільки по вільному каналу. Всі операції передачі даних підтверджуються. Отже, якщо бездротової клієнт не приймає підтвердження, він припускає наявність колізії і повторює спробу після закінчення довільного інтервалу очікування.

Бездротові клієнти і точки доступу використовують контрольні кадри RTS і CTS для спрощення фактичної передачі даних.

Як показано на рис. 1, при відправці даних в локальній клієнт спочатку сканує середу, щоб визначити наявність активних операцій передачі даних іншими пристроями. Якщо такі операції не виявлені, бездротової клієнт відправляє кадр RTS точки доступу. Цей кадр використовується для відправки

запиту виділеного доступу для носія радіочастот на вказаний період. Точка доступу приймає кадр і по можливості надає бездротовому клієнту доступ до носія радіочастот шляхом відправки кадру CTS такої ж тривалості. Всі інші бездротові пристрої, які бачать цей кадр CTS, звільняють середу для передачі даних з передавального вузла.

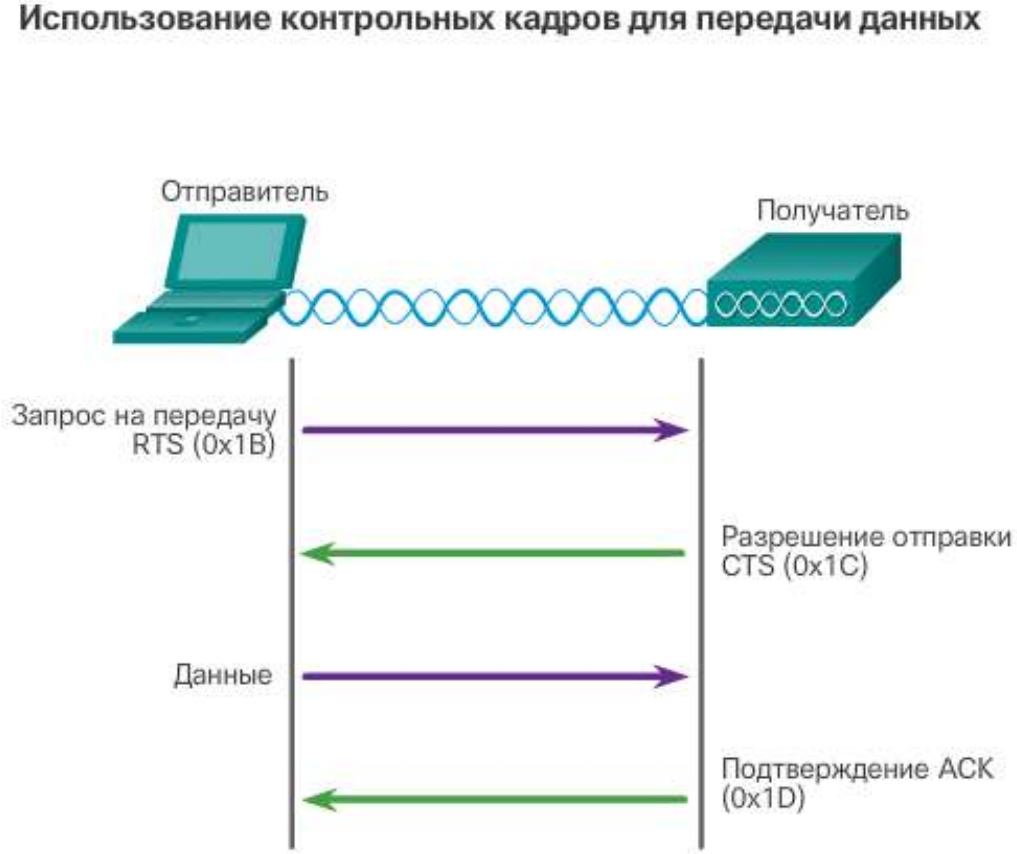


Рис. 5.3.21

Контрольний кадр CTS містить дані про тривалість, які дозволено передавати передавальному вузлу. Решта бездротові клієнти затримують передачу не менше, ніж на заданий період.

Щоб бездротові пристрої могли здійснювати обмін даними по мережі, для них потрібно спочатку виконати асоціацію з точкою доступу або бездротовим маршрутизатором. Важливим етапом процесу 802.11 є виявлення мережі WLAN і наступне підключення до неї.

Кадри управління використовуються бездротовими пристроями для виконання наступного процесу, що складається з трьох етапів.

Для виконання асоціації бездротової клієнт і точка доступу повинні узгодити особливі параметри. Щоб дозволити узгодження цих процесів, ці параметри необхідно налаштувати на точці доступу, а потім - на клієнті.

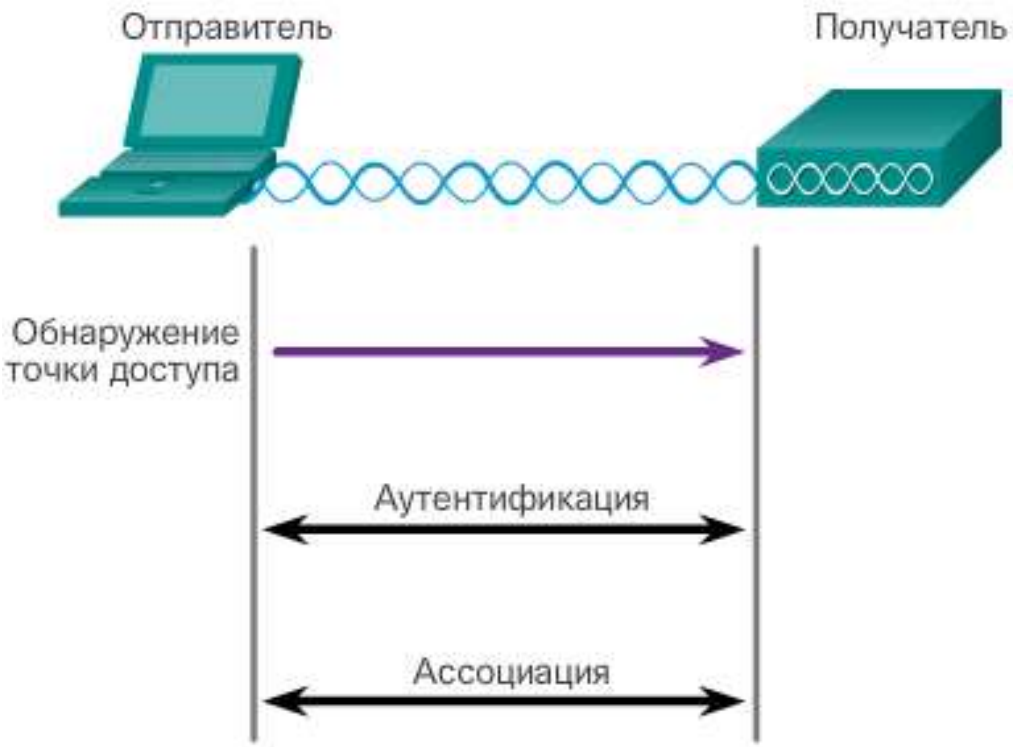


Рис. 5.3.22

На рис. 1 показані налаштування бездротової мережі на бездротовому маршрутизаторі Linksys EA6500. Загальні настроюються параметри бездротової мережі:

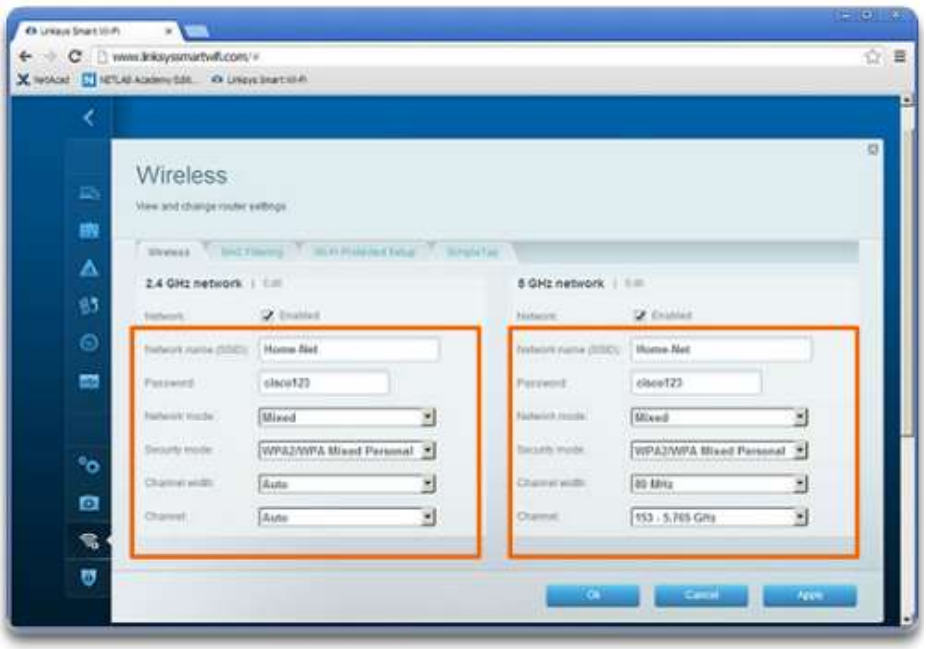


Рис. 5.3.23

Ідентифікатор SSID - ідентифікатор SSID являє собою унікальний ідентифікатор, який бездротової клієнт використовує, щоб розрізняти бездротові мережі в одній зоні. Ім'я SSID відображається в списку доступних бездротових мереж на клієнті. Залежно від конфігурації мережі ідентифікатор SSID може спільно використовуватися декількома точками доступу в мережі. Зазвичай Назва може містити від 2 до 32 символів.

Пароль - обов'язково надається бездротовим клієнтом для аутентифікації на точці доступу. Іноді пароль називають ключем безпеки. Пароль дозволяє запобігти доступ до бездротової мережі для зловмисників та інших небажаних користувачів.

Мережевий режим (Network mode) - відноситься до стандартів мережі WLAN 802.11a / b / g / n / ac / ad. Точки доступу і бездротові маршрутизатори можуть працювати в змішаному режимі, тобто. Е. Вони можуть одночасно використовувати кілька стандартів.

Режим безпеки (Security mode) - цей термін відноситься до налаштувань параметрів безпеки (WEP, WPA або WPA2). Слід завжди активувати найвищий з доступних рівнів безпеки.

Параметри каналів (Channel settings) - відноситься до частотним смугам, які використовуються для передачі бездротових даних. Бездротові маршрутизатори та точка доступу можуть вибирати налаштування каналу. Також, в разі перешкод з боку іншої точки доступу або бездротового пристрою, ці настройки також можна задати вручну.

Параметри безпеки, представлені на рис. 4, є доступні протоколи безпеки, налаштовані на бездротовому маршрутизаторі Linksys EA6500. Користувачі домашньої мережі повинні вибирати режим «WPA2 / WPA Mixed Personal», а користувачі корпоративної мережі - режим «WPA2 / WPA Mixed Enterprise». Для частотної смуги 5 ГГц доступні ті ж можливості. Щоб виконати асоціацію, кінцеве бездротове пристрій повинен також підтримувати обраний параметр безпеки.

Бездротові пристрої повинні виконувати виявлення і підключення до точки доступу або бездротового маршрутизатора. Бездротові клієнти підключаються до точки доступу, використовуючи для цього процес сканування (пошуку). Цей процес може виконуватися в наступних режимах:

Пасивний режим (Passive mode) - точка доступу відкрито оголошує свою службу шляхом регулярної відправки кадрів сигналу широкомовної розсилки, що містять ім'я SSID, відомості про підтримувані стандарти і налаштування безпеки. Основне завдання сигналу - дозволити бездротовим клієнтам отримувати дані про доступні мережах і точках доступу в даній зоні для вибору потрібної мережі і точки доступу.

Активний режим (Active mode) - бездротові клієнти повинні знати ім'я SSID. Бездротовий клієнт ініціює процес шляхом відправки по широкомовної розсилки кадру запиту пошуку на кілька каналів. Запит пошуку містить ім'я SSID і відомості про підтримувані стандарти. Активний режим може знадобитися в тому випадку, якщо для бездротового маршрутизатора або точки доступу налаштований заборона широкомовної розсилки кадрів сигналу.

На рис. 1 показано, як пасивний режим працює з точкою доступу, періодично передавальної кадр сигналу за допомогою широкомовної розсилки.

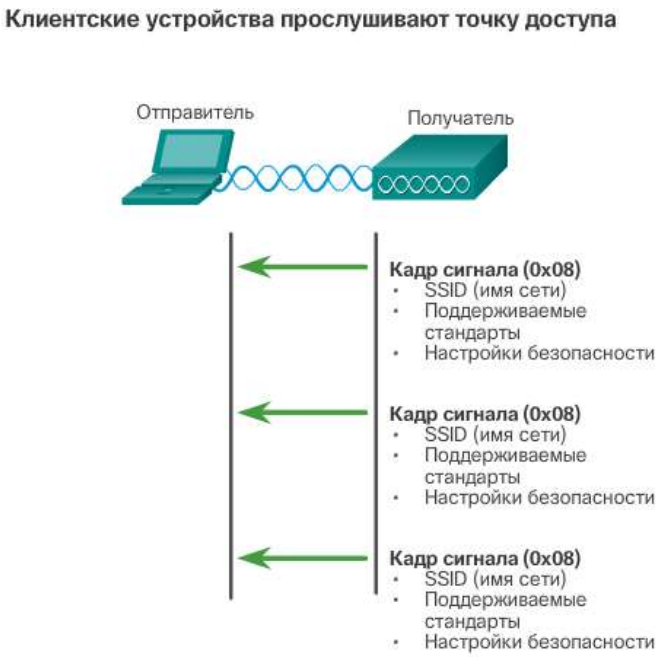


Рис. 5.3.24

На рис. 2 показано, як активний режим працює з бездротовим клієнтом, передає запит пошуку конкретного SSID за допомогою широкомовної розсилки. Точка доступу з цим SSID відправляє у відповідь кадр відгуку з пошуку.

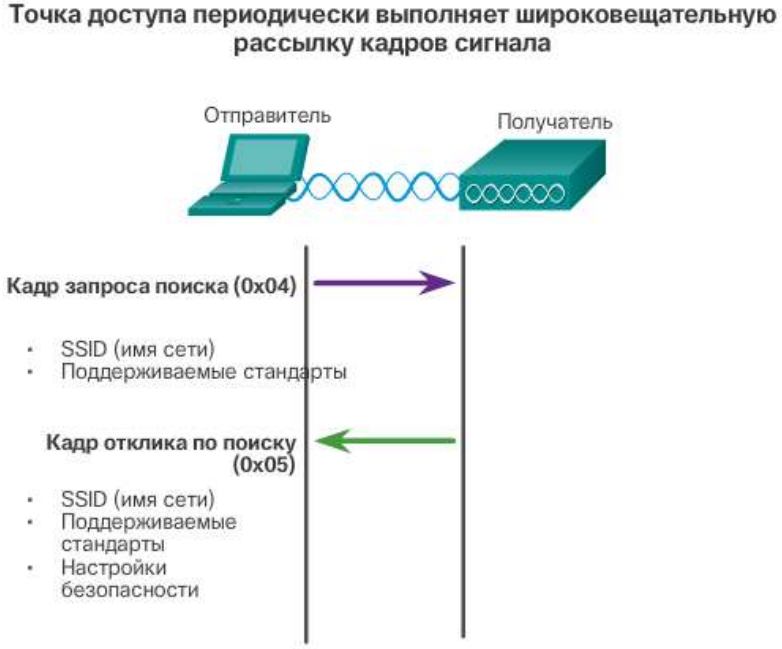


Рис. 5.3.25

Крім того, для виявлення найближчих мереж WLAN бездротового клієнт може відправити запит пошуку, який не містить ім'я SSID. Точки доступу, налаштовані для широкомовної розсилки кадрів сигналу, відправляють бездротовому клієнту відгук, що містить відгук з пошуку і вказівка імені SSID. Точки доступу, де відключений компонент передачі SSID з широкомовної розсилки, що не відправляють відгук.

Стандарт 802.11 спочатку розроблений з урахуванням двох механізмів аутентифікації:

Відкрита аутентифікація - по суті аутентифікація NULL, в рамках якої бездротової клієнт відправляє запит аутентифікації, і точка доступу відправляє у відповідь підтвердження. Відкрита аутентифікація забезпечує підключення до бездротової мережі для будь-якого бездротового пристрою. Такий метод аутентифікації слід використовувати тільки в тих випадках, коли безпека не має великого значення.

Аутентифікація узгодженого ключа - ця технологія передбачає використання ключа, попередньо погодженого клієнтом і точкою доступу.

На рис. 1 представлено короткий опис процедури аутентифікації. Однак в більшості систем, де використовується узгоджений ключ, обмін даними виконується наступним чином.

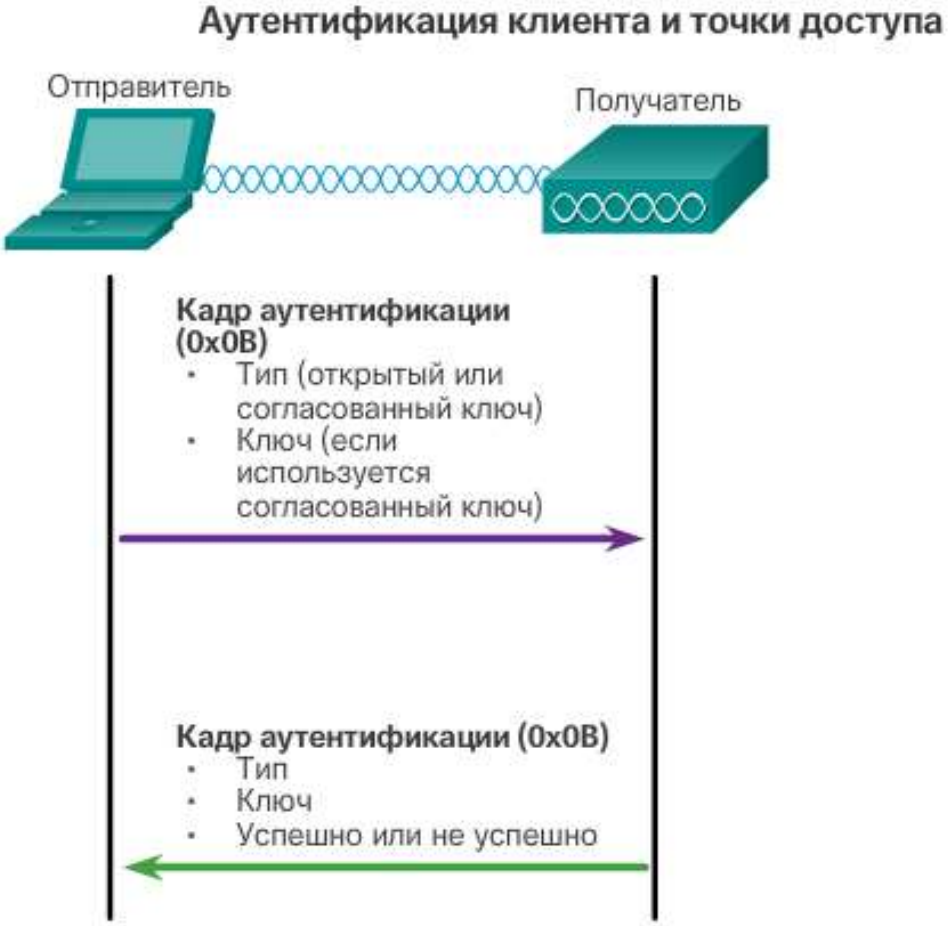


Рис. 5.3.26

1. Бездротовий клієнт відправляє кадр аутентифікації точки доступу.

2. Точка доступу відправляє у відповідь контрольний текст.

3. Клієнт виконує шифрування повідомлення, використовуючи узгоджений ключ, і відправляє зашифрований текст назад точки доступу.

4. Після цього точка доступу виконує розшифровку тексту, використовуючи свій узгоджений ключ.

5. Якщо зашифрований текст відповідає контрольному тексту, точка доступу виконує аутентифікацію клієнта. Якщо повідомлення не збігаються, бездротової клієнт не проходить аутентифікацію і не отримує бездротового доступу.

Після проходження бездротовим клієнтом аутентифікації точка доступу переходить до етапу асоціації. Як показано на рис. 2, на етапі асоціації

виконується кінцева настройка параметрів і встановлюється канал передачі даних між бездротовим клієнтом і точкою доступу.

На даному етапі:

Бездротовий клієнт пересилає кадр запиту асоціації, який містить його MAC-адресу.

Точка доступу відправляє у відповідь відгук по асоціації, що містить BSSID точки доступу, який є MAC-адресою точки доступу.

Точка доступу зіставляє логічний порт, відомий як ідентифікатор асоціації (AID) з бездротовим клієнтом. Ідентифікатор AID рівнозначний порту комутатора і дозволяє комутатора інфраструктури відстежувати кадри, що відправляються бездротовому клієнту для пересилки.

Після асоціації бездротового клієнта з точкою доступу трафік може передаватися між ними.

Як пояснювалося раніше, пристрої в бездротовій мережі LAN містять передавачі та приймачі, налаштовані на певні частоти радіохвиль для обміну даними. Зазвичай в якості діапазонів виділяються частоти. Такі діапазони потім розділяються на менші діапазони - канали.

Якщо попит на конкретний канал занадто високий, цей канал, швидше за все, стане перенасиченим. Насиченість середовища бездротової мережі знижує якість обміну даними. За останні кілька років розроблені спеціальні прийоми, які дозволяють поліпшити якість обміну даними і знизити насиченість. Перераховані нижче прийоми дозволяють знизити насиченість каналів за рахунок більш ефективного їх використання.

Розподіл сигналу в прямій послідовності (Direct-sequence spread spectrum, DSSS) - DSSS є технологією модуляції розподілу сигналу. Технологія розподілу спектра розроблена з метою поширення сигналу по більшій частотній смузі, що підвищує його стійкість до перешкод. За допомогою технології DSSS сигнал множиться на значення «штучно створеного шуму», яке також називається кодом розширення спектра. Оскільки одержувачу відомий код розширення спектра, то після його додавання він може математично видалити і повторно вибудувати вихідний сигнал. По факту це забезпечує надмірність переданого сигналу, запобігаючи, таким чином, зниження якості середовища бездротової мережі. Технологія DSSS використовується стандартом 802.11b, а також в радіотелефонах, що працюють на частоті 900 МГц, 2,4 ГГц, 5,8 ГГц, стільникових мережах CDMA і мережах GPS. (Рис. 1)

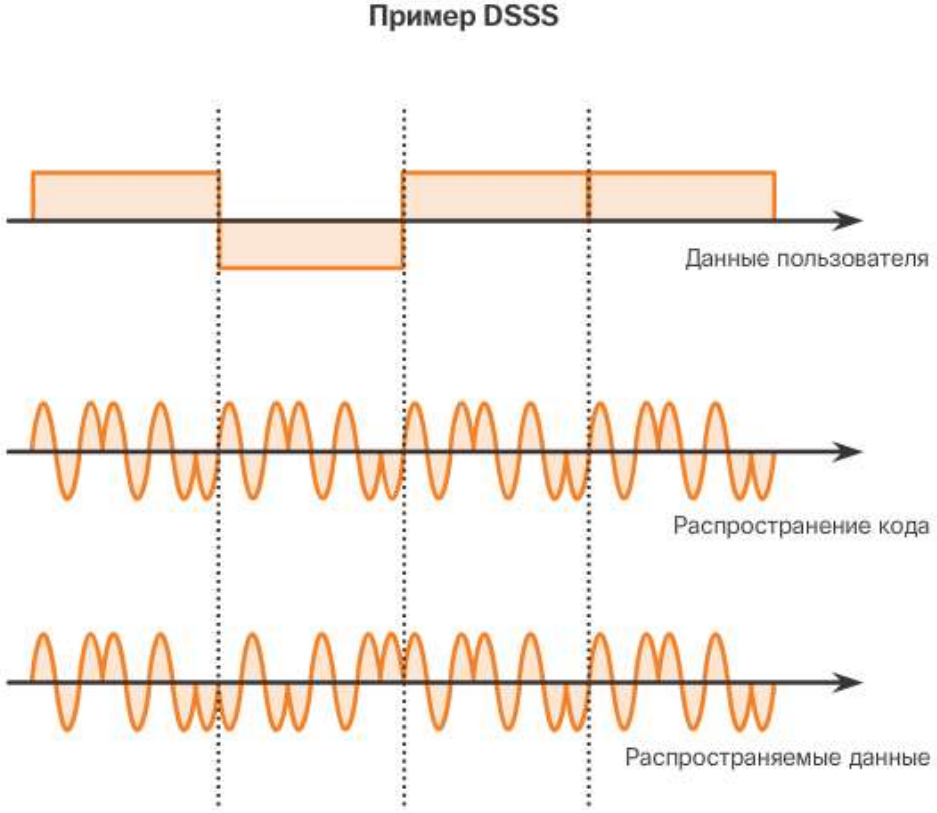


Рис. 5.3.27

Стрибкоподібна зміна робочої частоти з розширенням спектра (Frequency-hopping spread spectrum, FHSS) - для обміну даними теж використовує методи розподілу спектра. Ця технологія аналогічна DSSS, але передає радіосигнали за допомогою швидкої комутації сигналу несучої частоти по безлічі частотних каналів. При використанні FHSS відправник і одержувач повинні синхронізуватися, щоб «дізнатися», на які канали слід перейти. Цей процес переходу сигналу між каналами забезпечує більш ефективне використання каналів, що знижує їх перевантаження. Портативні рації і радіотелефони, що працюють на частоті 900 МГц, теж використовують FHSS, в той час як Bluetooth покладається на одну з варіацій цієї технології. Технологія FHSS, крім того, використовується вихідним стандартом 802.11. (Рис. 2)

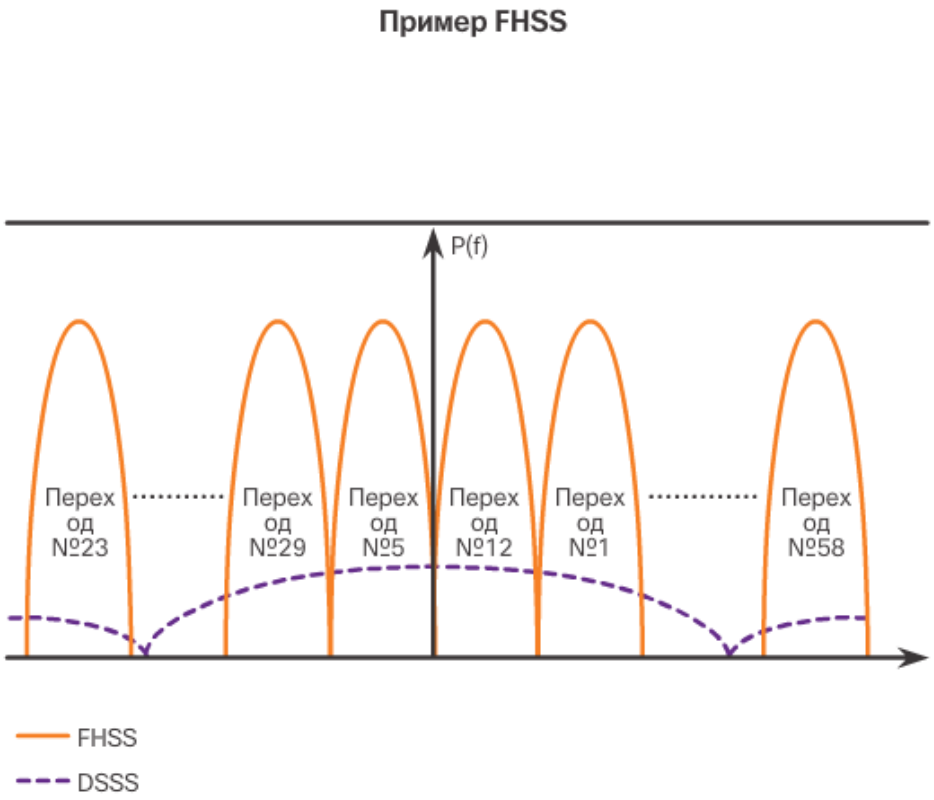


Рис. 5.3.28

Мультиплексування з ортогональним поділом частот (Orthogonal frequency-division multiplexing, OFDM) - являє собою різновид мультиплексування з поділом частот, в рамках якої один канал використовує кілька подканалов на суміжних частотах. Підканали в системі OFDM точно ортогональні відносно один одного, що дозволяє підканалах перекриватися без взаємних перешкод. В результаті система OFDM дозволяє максимально збільшити ефективність спектра без перешкод на суміжних каналах. По суті ця технологія дозволяє приймаючої станції «почути» сигнал. Оскільки OFDM використовує підканали, це робить використання каналу максимально ефективним. OFDM використовується декількома системами зв'язку, включаючи стандарт 802.11a / g / n / ac. (Рис. 3)

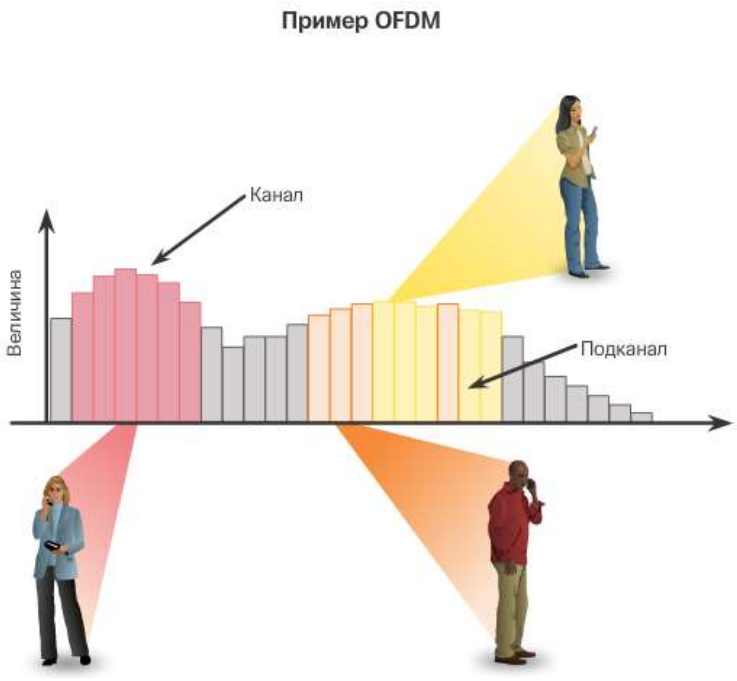


Рис. 5.3.29

Всі стандарти IEEE 802.11b / g / n працюють на СВЧ-частотах спектра радіосигналів. Стандарти IEEE 802.11b / g / n працюють в частотному діапазоні від 2,4 ГГц до 2,5 ГГц, а стандарти 802.11a / n / ac - в більш жорстко регульованої смузі 5 ГГц. На рис. 1 показано, який стандарт 802.11 працює на смугах 2,4 ГГц, 5 ГГц і 60 ГГц. Всі спектри поділені на канали з середньою частотою несучої і пропускною спроможністю, які аналогічні поділу радіочастотних смуг.

Рис. 5.3.30

Смуга 2,4 ГГц поділена на кілька каналів. В цілому загальна пропускна здатність каналу становить 22 МГц, і кожен канал відділяється смугою 5 ГГц. Стандарт 802.11b визначає 11 каналів для Північної Америки. Пропускна здатність 22 МГц укупі з поділом частот смугами 5 ГГц, має на увазі перекривання послідовних каналів, як показано на рис. 2.

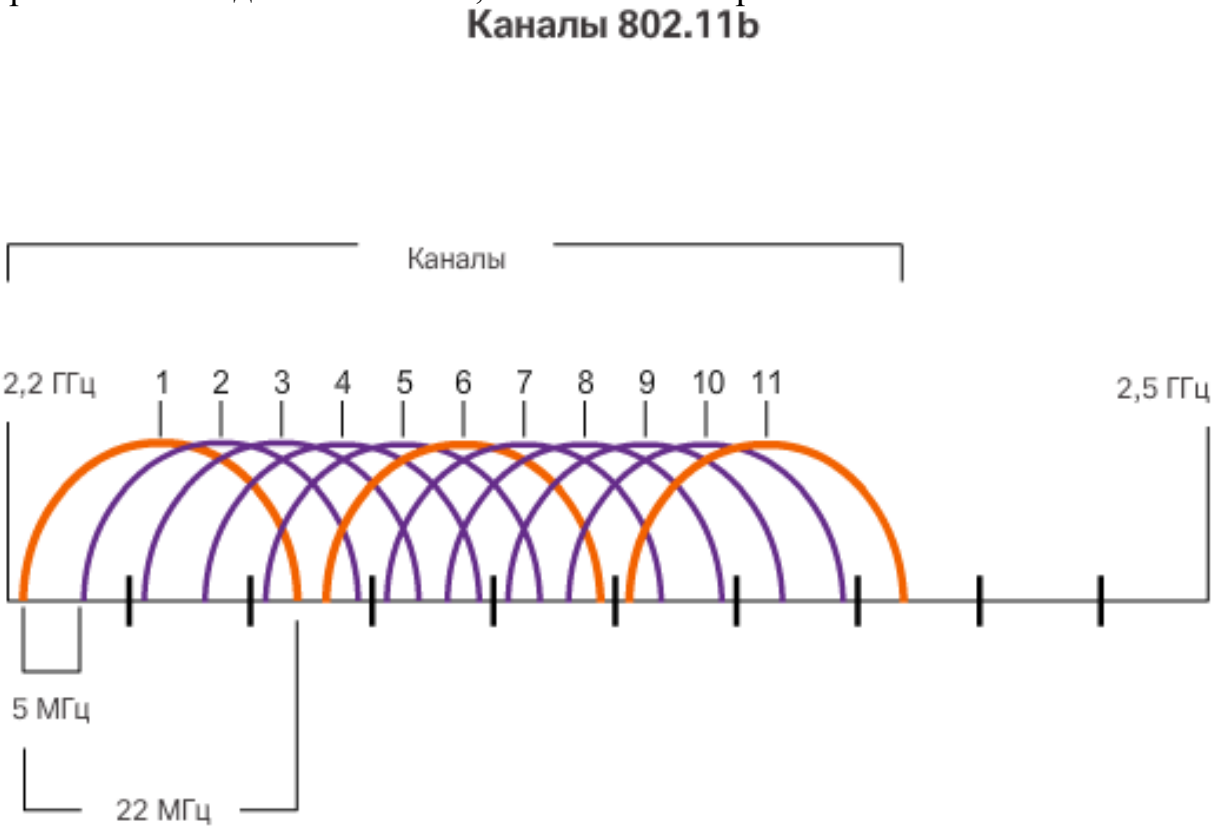


Рис. 5.3.31

Примітка. У Європі працюють 13 каналів 802.11b.

Перешкоди виникають в тому випадку, якщо небажані сигнали перекривають канал, зарезервований для бажаного сигналу, внаслідок чого можуть виникати спотворення. Щоб усунути перешкоди, можна використовувати неперекривающіеся канали. Зокрема, канали 1, 6 і 11 є неперекривающіхся каналами 802.11b, як показано на рис. 3.

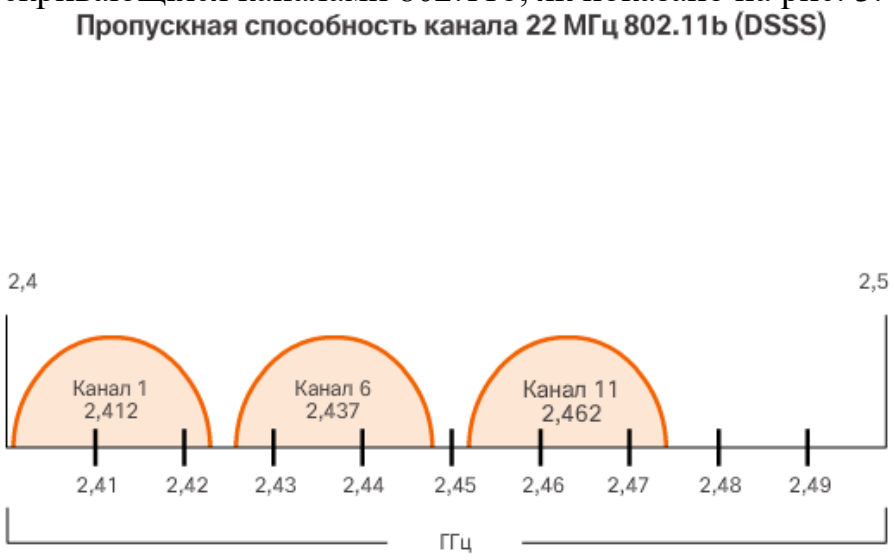


Рис. 5.3.32

Для мереж WLAN, для яких потрібно кілька точок доступу, рекомендується використовувати неперекривающіеся канали. При наявності трьох суміжних точок доступу слід використовувати канали 1, 6 і 11. Якщо таких точок доступу тільки дві, слід вибрати будь-які два канали, які відстоять один від одного на п'ять каналів (наприклад канали 5 і 10). Більшість точок доступу можуть автоматично вибирати канал з урахуванням використовуваних суміжних каналів. У деяких пристроях передбачено постійне спостереження за радіопросторі з метою динамічної коригування параметрів каналу у відповідь на зміни середовища.

У міру переходу корпоративних мереж WLAN на стандарт 802.11n вони можуть використовувати канали в більшій і менш завантаженій смузі 5 ГГц, що знижує ризик «випадкового відмови в обслуговуванні (DoS)». Наприклад, стандарт 802.11n використовує технологію OFDM і може підтримувати чотири неперекривающіхся каналу, як показано на рис. 4.

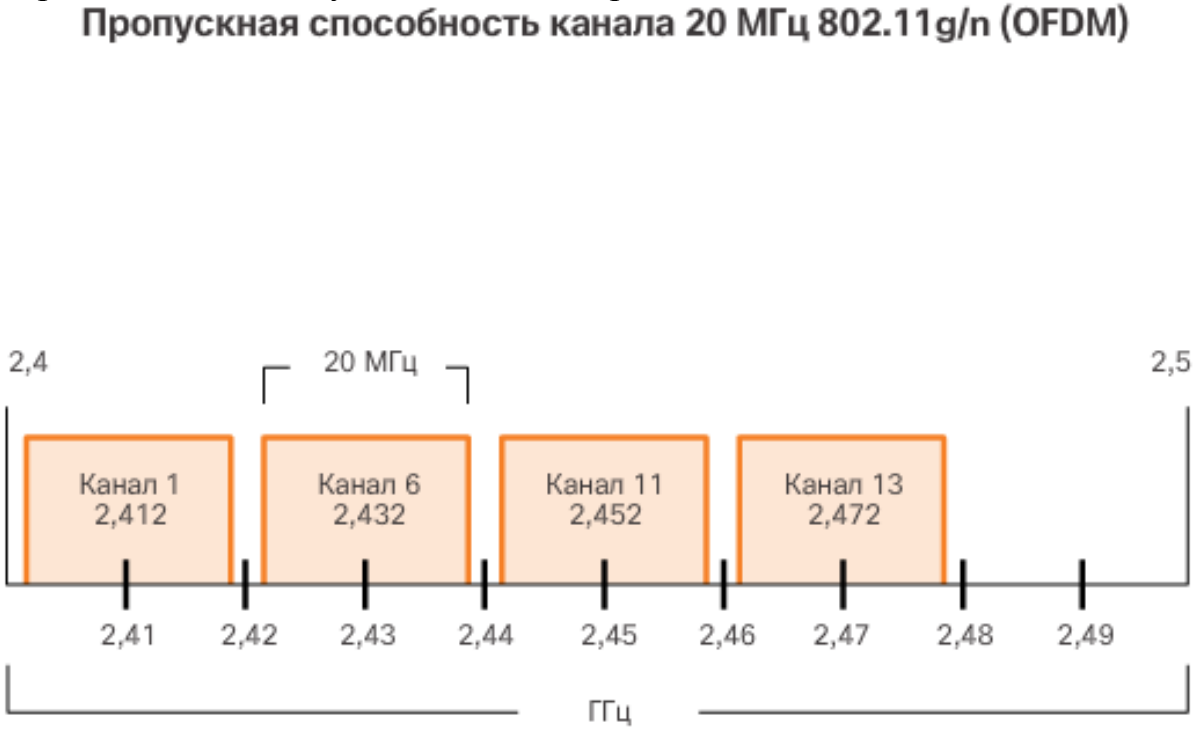


Рис. 5.3.33

Стандарт 802.11n також може використовувати з'єднання каналів, при якому два каналу 20 МГц об'єднуються в один канал 40 МГц, як показано на рис. 5. З'єднання каналів збільшує пропускну здатність за рахунок використання для доставки даних одночасно двох каналів.

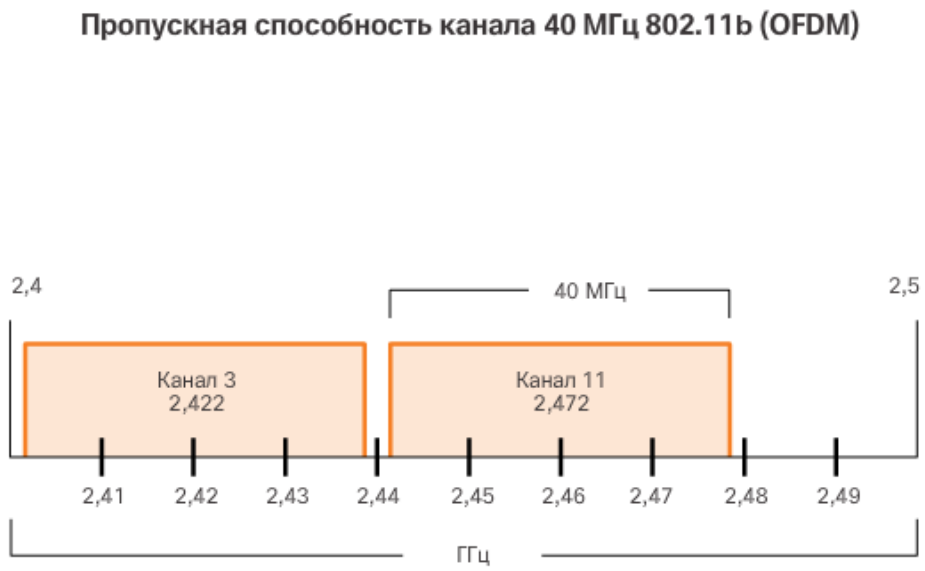


Рис. 5.3.34

Більшість сучасних точок доступу можуть автоматично регулювати канали, щоб обійти перешкоди.

Примітка. Стандарт IEEE 802.11ac використовує OFDM з шириною каналів в 80,160 і 80 + 80.

Реалізація мережі WLAN, яка максимально ефективно використовує ресурси і забезпечує обслуговування високої якості, може зажадати ретельне планування. Мережі WLAN можуть варіюватися від відносно простих до дуже складних моделей. Перш ніж приступати до реалізації бездротової мережі, необхідно розробити детальний план.

Кількість користувачів, що підтримує мережу WLAN, розраховується за досить складною схемою. Кількість користувачів залежить від доступного простору на об'єкті, кількості пристроїв, які може вмістити вказаний об'єкт, очікуваної користувачами швидкості передачі даних, використання неперекривающіхся каналів декількома точками доступу в ESS і налаштувань потужності передачі.

Див. Поверховий план на рис. 1. При плануванні розташування точок доступу адміністратору недостатньо просто позначити колами зони покриття і розмістити їх на плані. Зразкові кругові зони покриття важливі, проте є ряд додаткових рекомендацій:

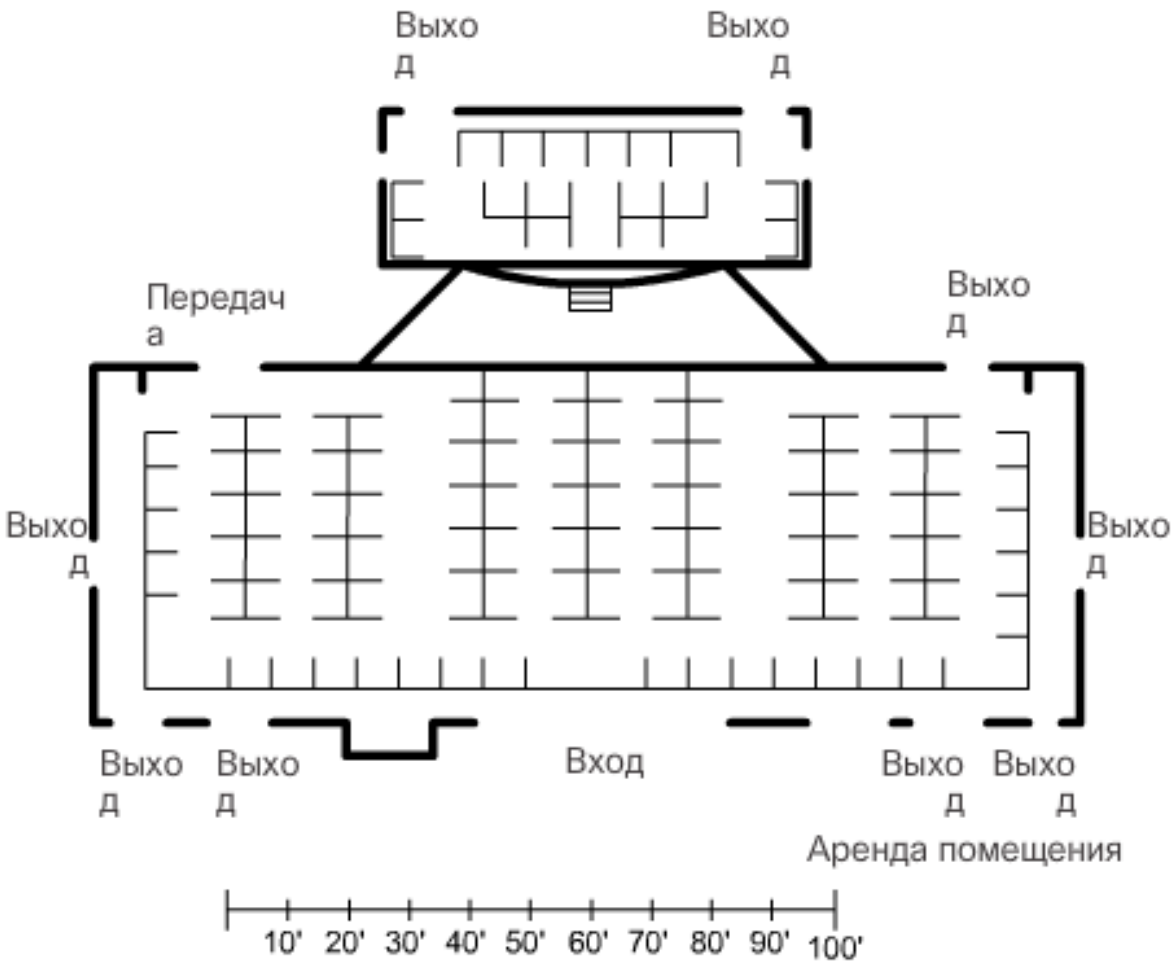


Рис. 5.3.35

- якщо точки доступу повинні використовувати існуючі кабельні системи, або присутні розташування, де можна розмістити точки доступу, слід зазначити ці місця на карті;
- точки доступу слід розміщувати вище фізичних перешкод;
- по можливості розміщувати точки доступу вертикально поруч зі стелею в центрі кожної зони;
- розміщувати AP в тих місцях, де будуть знаходитися користувачі. Наприклад, конференц-зали, як правило, більше підходять для розміщення точки доступу, ніж коридор.

Після вирішення зазначених питань слід оцінити передбачувану зону покриття точки доступу. Це значення може варіюватися в залежності від стандарту або комбінації стандартів мережі WLAN, що підлягає розгортанню, характеру об'єкта, потужності передачі, налаштованої для точки доступу, і багатьох інших факторів. При розробці плану зон покриття необхідно завжди вивчати специфікації використовуваних точок доступу.

Зони покриття BSA є зону покриття, яку забезпечує один канал. Розширений набір сервісів (ESS) повинен перекриватися на 10-15% між зонами покриття BSA в межах ESS. З перекриттям між BSA в 15%, ідентифікатором

SSID і неперекривающіхся каналами (т. Е. Один осередок на каналі 1, а інша - на каналі 6) можна створити можливість роумінгу.

На рис. 2 показаний приклад можливого перекриття зон BSA.

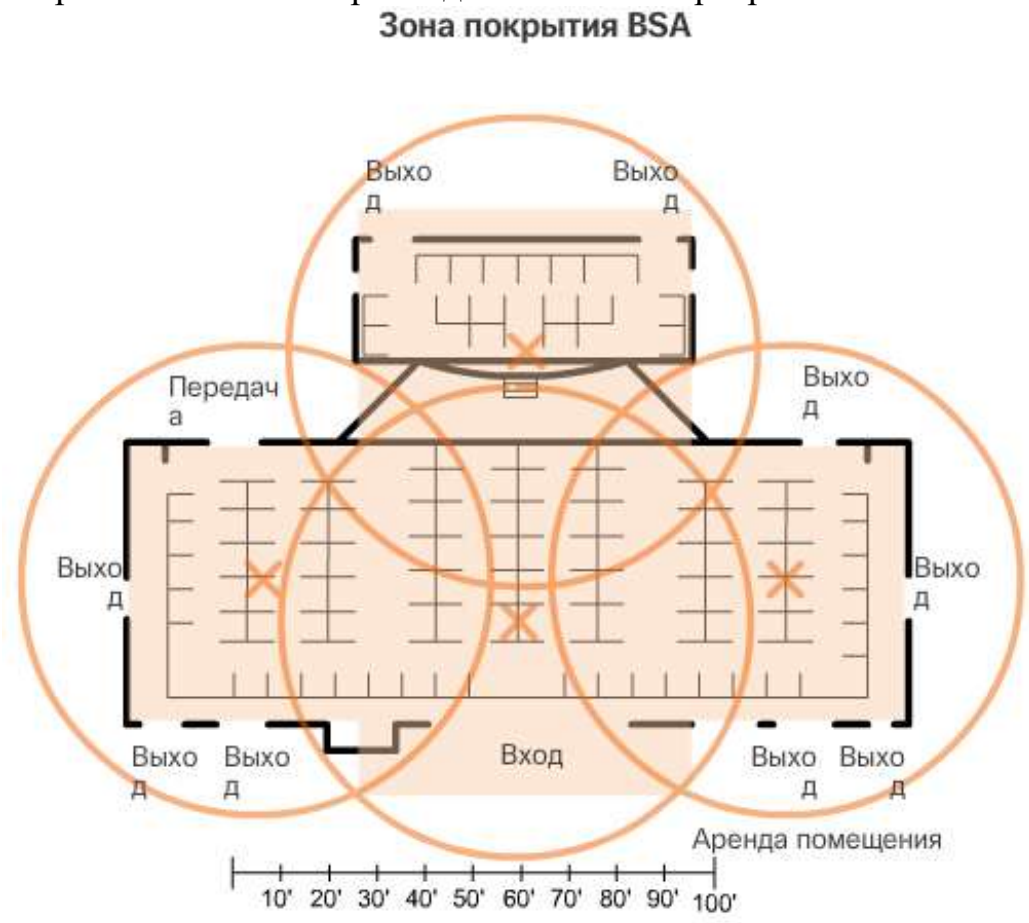


Рис. 5.3.36

Забезпечити безпеку бездротової мережі ще складніше, ніж захистити дротову мережу. Захист повинна стояти на першому місці для всіх, хто використовує або адмініструє мережі.

В діапазоні дії точки доступу мережу WLAN відкрита для всіх, хто володіє відповідними обліковими даними, за допомогою яких виконується асоціація з точкою доступу. Володіючи бездротовим мережним адаптером і знанням прийомів злому, зловмисник може не бути присутнім фізично в тому місці, де знаходиться мережа WLAN, щоб отримати до неї доступ.

Питання безпеки набувають ще більшого значення, коли мова йде про корпоративних мережах, оскільки життєдіяльність компанії, крім іншого, залежить від захищеності даних. Порушення системи безпеки можуть мати катастрофічні наслідки для компаній, особливо якщо компанія оперує фінансовою інформацією своїх клієнтів. Бездротові мережі все частіше розгортаються на підприємствах і в багатьох випадках є вже не просто більш зручним варіантом, але і критично важливою частиною мережі. Хоча мережі WLAN завжди були схильні до атак, у міру зростання їх популярності вони стають метою номер один.

Атаки можуть ініціюватися сторонніми людьми і незадоволеними співробітниками, але крім подібних недоброзичливців атака може бути ненавмисно спровокована будь-яким співробітником. Бездротові мережі особливо схильні до наступним загрозам:

- бездротові зловмисники;
- шкідливі програми;
- перехоплення даних
- атаки DoS

Атака типу «відмова в обслуговуванні»

Нижче наведені причини виникнення DoS-атаки на бездротову мережу.

Неправильне налаштування пристроїв - помилки конфігурації можуть стати причиною відключення мережі WLAN. Наприклад, адміністратор може випадково змінити конфігурацію і відключити мережу, або зловмисник з правами адміністратора може відключити мережу WLAN навмисно.

Зловмисник, навмисно перешкоджає обміну даними по бездротовій мережі - такі зловмисники прагнуть відключити бездротову мережу повністю або до тієї міри, коли санкціоновані пристрої не зможуть отримати доступ до середовища.

Випадкові перешкоди - мережі WLAN працюють на неліцензованому частотних смугах і, отже, всі бездротові мережі незалежно від функцій безпеки схильні до дії перешкод з боку інших бездротових пристроїв. Випадкові перешкоди можуть виникати в результаті роботи таких пристроїв, як мікрохвильові печі, радіотелефони, радіо-няні та ін. Смуга 2,4 ГГц більшою мірою схильна до впливу перешкод, ніж смуга 5 ГГц.

Щоб мінімізувати ризик DoS-атаки внаслідок неправильної настройки пристроїв і шкідливих атак, слід забезпечити захист всіх пристроїв, зберігати паролі в надійному місці, створювати резервні копії та змінювати конфігурацію тільки в неробочий час.

Випадкові перешкоди виникають тільки в разі роботи інших бездротових пристроїв. Оптимальним рішенням є моніторинг мережі WLAN на предмет проблем, пов'язаних з перешкодами, і рішення таких проблем у міру їх виникнення. Оскільки смуга 2,4 ГГц більшою мірою схильна до впливу перешкод, в найбільш слабких зонах можна використовувати смугу 5 ГГц. Деякі рішення для мереж WLAN забезпечують автоматичне регулювання каналів точками доступу і дозволяють використовувати смугу 5 ГГц, щоб усунути перешкоди шляхом. Наприклад, деякі рішення стандарту 802.11n / ac / ad підлаштовуються автоматично з метою протидії перешкод.

На малюнку показано, як радіотелефон або мікрохвильова піч можуть створювати перешкоди для обміну даними по мережі WLAN.

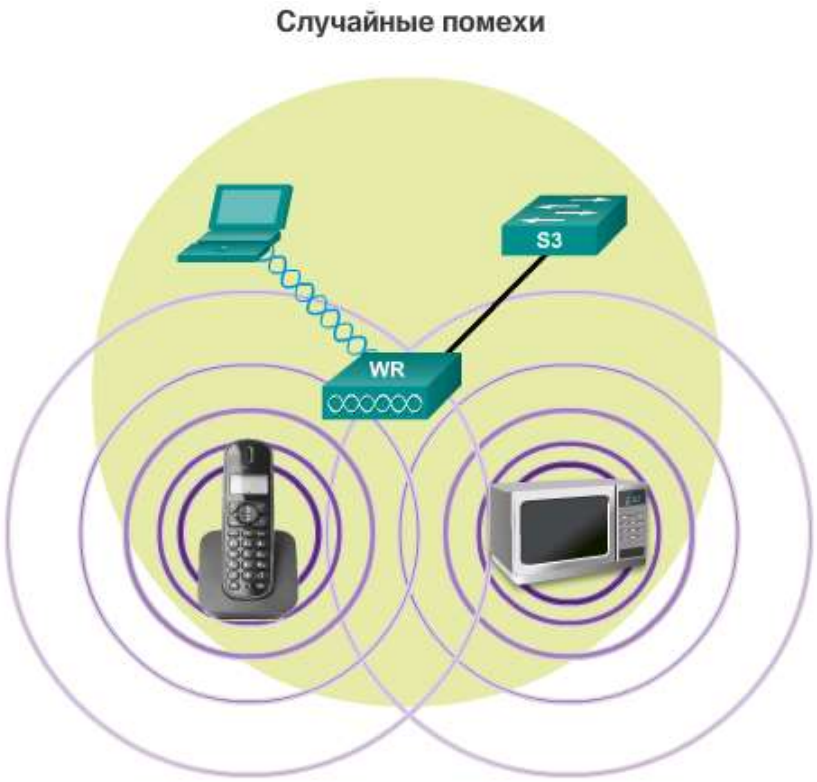


Рис. 5.3.37

Технологія Cisco CleanAir дозволяє пристроям визначати і знаходити джерела перешкод, що не належать до стандарту 802.11. Ця технологія створює мережу, яка здатна автоматично пристосовуватися до змін в середовищі.

Хоча це і малоймовірно, зловмисники можуть навмисно ініціювати DoS-атаку, використовуючи пристрої радіоелектронної протидії, які створюють випадкові перешкоди. Більш ймовірно, що зловмисники спробують оперувати кадрами управління, споживаючи, таким чином, ресурси точки доступу, і завантажать канали настільки, що вони не зможуть обслуговувати санкціонований користувача трафік.

Кадри управління можна використовувати для організації різних типів DoS-атак. Поширені два типи атак з використанням кадрів управління.

Атака шляхом помилкового відключення - для здійснення такої атаки зловмисник відправляє набір команд «скасування асоціації» на всі бездротові пристрої в межах BSS. Ці команди викликають відключення всіх клієнтів. При відключенні всі бездротові клієнти відразу ж намагаються виконати повторну асоціацію, що викликає різке збільшення обсягу трафіку. Зловмисник продовжує відправляти кадри скасування асоціації, і цикл повторюється.

Лавинна атака дозволів відправки CTS - даний тип атаки виникає, коли зловмисник використовує метод вирішення конфліктів в середовищі CSMA / CA для монополізації смуги пропускання і відхилення доступу для всіх інших бездротових клієнтів. Для цього зловмисник постійно виконує в BSS лавинную розсилку дозволів відправки CTS на помилковий STA. Всі інші бездротові клієнти, спільно використовують середу радіочастот, приймають CTS і перестають виконувати передачу даних до тих пір, поки зловмисник не припинить передачу кадрів CTS.

На рис. 1 показано, як бездротової клієнт і точка доступу використовують метод CSMA / CA для доступу до середовища.

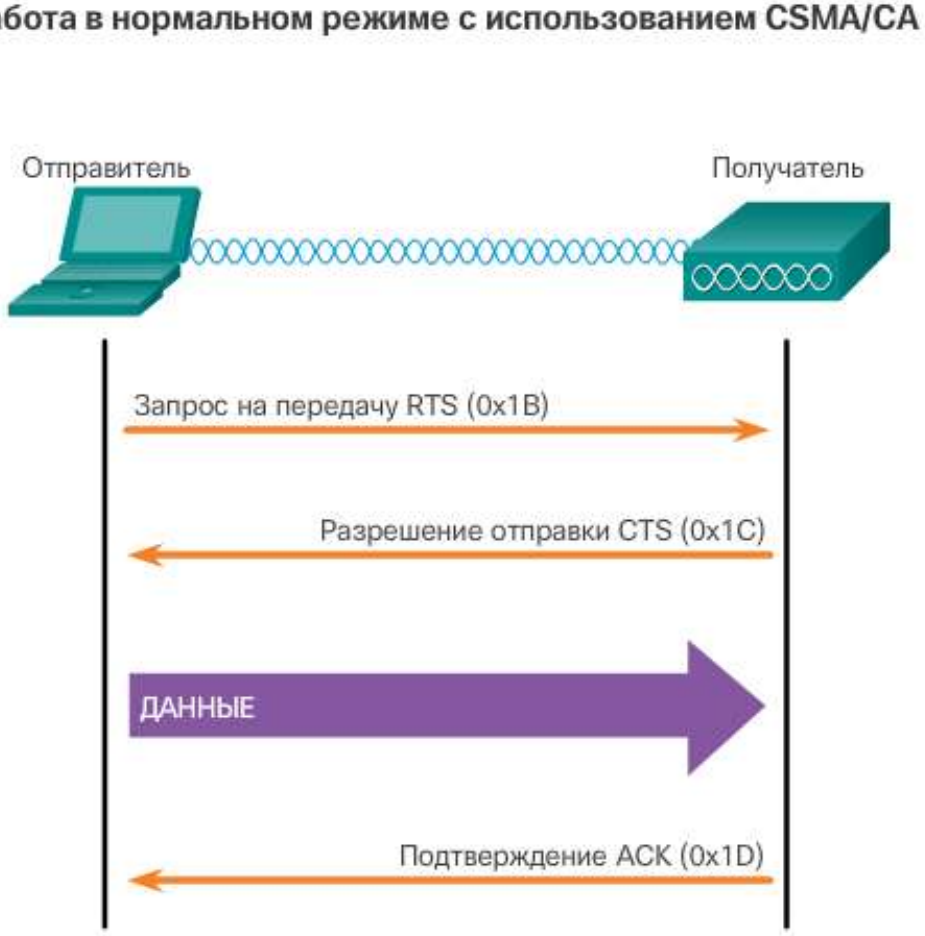


Рис. 5.3.38

На рис. 2 показано, як зловмисник створює лавинную розсилку кадрів CTS на помилковий бездротової клієнт. Тепер всі інші клієнти змушені чекати завершення періоду, заданого в кадрі CTS. Однак зловмисник продовжує відправляти кадри CTS. Отже, інші клієнти змушені постійно чекати. Таким чином, зловмисник контролює середу.

Рис. 5.3.39

Щоб знизити ризик виникнення подібних атак, корпорація Cisco розробила ряд рішень, включаючи функцію Cisco Management Frame Protection (MFP), яка також забезпечує повноцінну профілактичну захист від спуфинга кадрів і пристроїв. Система запобігання вторгнень Cisco Adaptive Wireless доповнює це рішення функціями виявлення вторгнень на ранніх термінах шляхом зіставлення сигнатур атак.

Комітет зі стандартів IEEE 802.11 також розробив два стандарти безпеки бездротової мережі. Стандарт 802.11i, який використовує Cisco MFP, визначає механізми безпеки для бездротових мереж, в той час як стандарт захисту кадрів управління 802.11w спрямований на рішення проблем, пов'язаних з маніпуляцією кадрами управління.

Шкідлива точка доступу являє собою бездротової маршрутизатор, який можна охарактеризувати наступним чином.

Такий маршрутизатор підключається до корпоративної мережі без явної авторизації і в порушення корпоративної політики. Будь-який користувач, який має доступ до об'єктів, може встановити (зі злим умислом або без) недорогий бездротовий маршрутизатор, який теоретично забезпечує доступ до ресурсів захищеної мережі.

Зловмисник може підключити або включити такий маршрутизатор з метою захоплення даних клієнта (наприклад, MAC-адреси бездротових і дротових клієнтів) або захоплення і маскування пакетів даних для отримання доступу до ресурсів мережі; або ж з метою ініціації атаки з перехопленням.

Слід також враховувати, наскільки просто створити персональну бездротову точку доступу. Наприклад, користувач, який має захищений доступ до мережі, налаштовує свій авторизований вузол Windows, як точку доступу до мережі Wi-Fi. При цьому несакціонірованние пристрої обходять заходи безпеки і отримують доступ до ресурсів мережі, як одне загальне пристрій.

Щоб запобігти установку шкідливих точок доступу, організації повинні використовувати програмне забезпечення для активного моніторингу спектра радіосигналів на предмет наявності несанкціонованих точок доступу. Наприклад, на знімку екрана програмного забезпечення для управління мережами інфраструктури Cisco Prime на малюнку показана карта радіочастот, яка визначає місце розташування зловмисника з виявленим хибним MAC-адресою.

Пример снимка экрана при обнаружении посторонней точки доступа

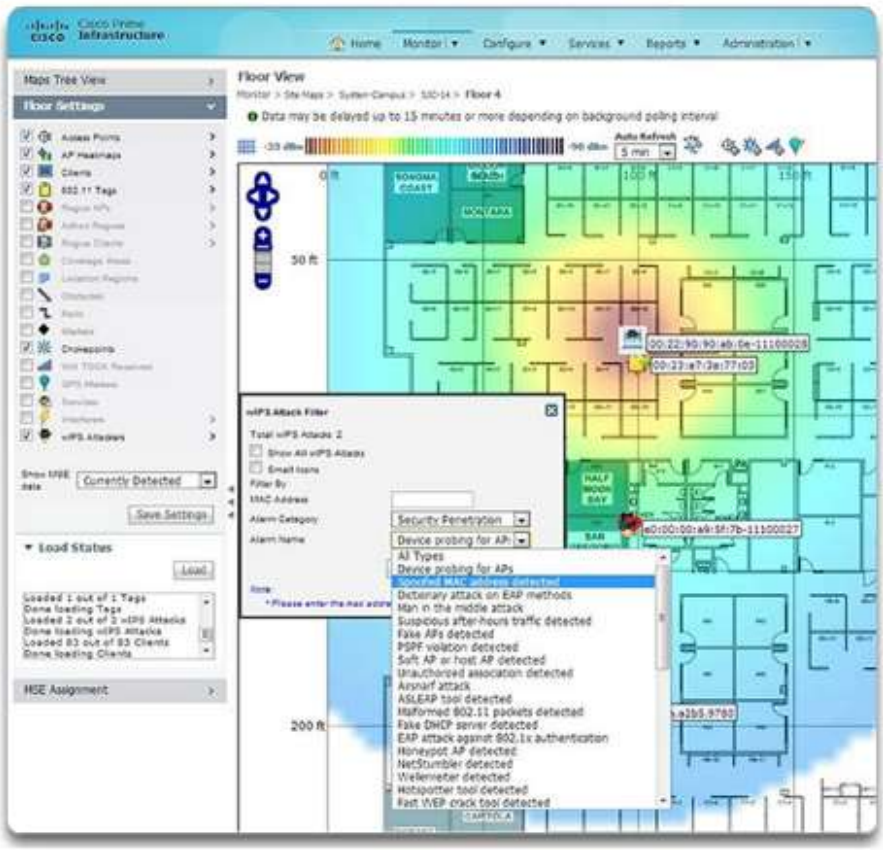


Рис. 5.3.40

Примітка. Cisco Prime є програмним забезпеченням для управління мережами, яке взаємодіє з іншими подібними програмами, забезпечуючи загальне уявлення і централізоване розміщення всіх даних про мережу. Як правило, це ПО розгортається в дуже великих організаціях.

До одного з найбільш складних типів атак, які може застосувати зловмисник, відноситься атака з перехопленням. Існує безліч способів створення атаки з перехопленням.

Один з найпоширеніших видів такої атаки називається «злий двійник», в рамках якої зловмисник впроваджує шкідливу точку доступу і налаштовує її з використанням такого ж імені SSID, що і у санкціонованої точки доступу. Місця, де пропонується безкоштовний доступ до мережі Wi-Fi, наприклад, аеропорти, кафе і ресторани - найпопулярніші мішені для атак такого типу, оскільки на цих об'єктах використовується відкрита аутентифікація.

При підключенні бездротових клієнтів можна побачити дві точки доступу, що пропонують бездротовий доступ. Ті, хто знаходяться поруч з шкідливою точкою доступу, виявляють більш потужний сигнал, і, швидше за все, виконають асоціацію з точкою доступу «злий двійник». Тепер для користувача

трафік відправляється на сторонню точку доступу, яка, в свою чергу, захоплює дані і пересилає їх на надійну точку доступу. Зворотний трафік від санкціонованої точки доступу відправляється на шкідливу точку доступу, захоплюється, а потім пересилається нічого не підозрюючи станції (STA). Зловмисник може вкрасти пароль користувача, особисту інформацію, отримати доступ до мережі і скомпрометувати систему користувача.

Наприклад, на рис. 1 зловмисник знаходиться в кафе «Латте Боба» і намагається захопити трафік від нічого не підозрюють бездротових клієнтів. Зловмисник запускає програмне забезпечення, яке робить його ноутбук точкою доступу типу «злий двійник», що має те ж ім'я SSID і канал, що і санкціонований бездротовий маршрутизатор.

Рис. 5.3.41

На рис. 2 користувач бачить два доступних бездротових підключення, але вибирає для асоціації точку доступу «злий двійник». Зловмисник захоплює призначені для користувача дані і пересилає їх на санкціоновану точку доступу, яка, в свою чергу, направляє відповідь трафік назад на точку доступу «злий двійник». Точка доступу «злий двійник» захоплює у відповідь трафік і пересилає дані нічого не підозрює користувачеві.

Рис. 5.3.42

Успішність запобігання атаки з перехопленням залежить від складності інфраструктури мережі WLAN і ретельності моніторингу мережі. Процес починається з визначення санкціонованих пристроїв в мережі WLAN. Для цього користувачі повинні пройти аутентифікацію. Після того, як визначені всі санкціоновані пристрою, можна виконати моніторинг мережі на предмет наявності підозрілих пристроїв або трафіку.

Корпоративні мережі WLAN, в яких використовуються найсучасніші пристрої WLAN, надають адміністраторам інструменти, які в комплексі працюють, як бездротова система запобігання вторгнення (IPS). До таких інструментів належать сканери, за допомогою яких виявляються шкідливі точки доступу і однорангові мережі, а також інструменти управління радіоресурсами, які здійснюють моніторинг радіочастотної смуги на предмет активності і завантаження точки доступу. Велике навантаження на точку доступу сигналізує адміністратору про можливу наявність несанкціонованого трафіку.

Безпека мережі Wi-Fi завжди викликала особливе занепокоєння, оскільки кордону мережі розширилися. Сигнали бездротового зв'язку можуть передаватися через тверді перешкоди - стелі, підлоги, стіни, за межі будинку або офісу. Без суворих заходів безпеки установка мережі WLAN - те саме повсюдного розміщення Ethernet-портів, навіть на вулиці.

Щоб запобігти загрозам з боку зловмисників, які намагаються проникнути в бездротову мережу, і захистити дані, використовувалися дві функції забезпечення безпеки.

Приховування ідентифікатора SSID. Точки доступу і деякі бездротові маршрутизатори дозволяють відключити кадр сигналу ідентифікатора SSID. Бездротові клієнти повинні вручну визначити ім'я SSID, щоб підключитися до мережі.

Фільтрація MAC-адрес. Адміністратор може вручну дозволити або заборонити клієнтам бездротовий доступ в залежності від MAC-адреси їх фізичного обладнання.

Хоча ці дві функції відсівають більшість користувачів, насправді ні приховування ідентифікатора SSID, ні фільтрація MAC-адрес не завадять вмілому зломщикові. Імена SSID легко виявити навіть в тому випадку, якщо точки доступу не виконують їх трансляцію розсилку, а MAC-адреси можна підробити. Оптимальним способом захисту бездротової мережі є використання систем аутентифікації і шифрування (див. Рис. 1).

Рис. 5.3.43

У вихідному стандарті 802.11 представлено два типи аутентифікації:

Аутентифікація відкритої системи. Всі бездротові клієнти можуть легко виконати підключення, і така система може використовуватися тільки в тих випадках, коли безпека не має особливого значення (наприклад, в місцях, де надається безкоштовний доступ до Інтернету - кафе, готелі і віддалені розташування).

Аутентифікація узгодженого ключа. Для аутентифікації і шифрування даних, що передаються між бездротовим клієнтом і точкою доступу, надає такі механізми, як WEP, WPA або WPA2. Однак для підключення пароль необхідно попередньо узгодити між сторонами.

Як показано на рис. 1, доступні три варіанти аутентифікації узгодженого ключа:

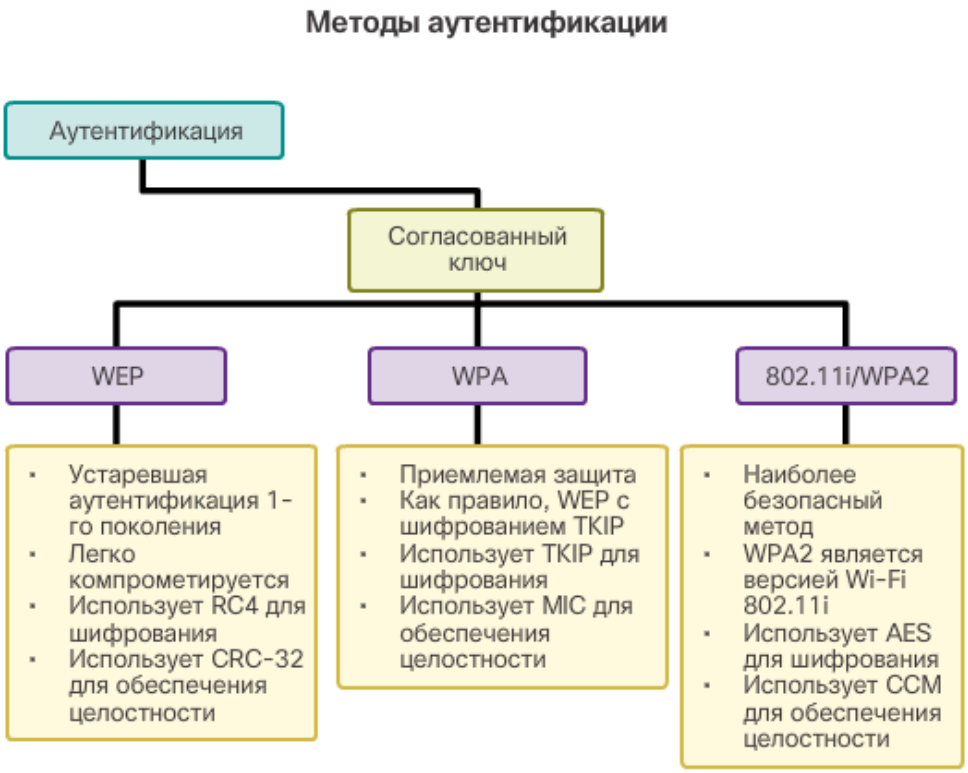


Рис. 5.3.44

Протокол шифрування бездротового зв'язку (WEP). Вихідна специфікація 802.11, яка розроблена для забезпечення конфіденційності на рівні, порівнянному з проводовим підключенням. Захист даних забезпечується за допомогою методу шифрування RC4 з використанням статичного ключа. Однак ключ ніколи не змінюється при передачі пакетів, тому його досить легко зламати.

Захищений доступ до Wi-Fi (WPA). Стандарт Wi-Fi Alliance, який використовує WEP, але забезпечує захист даних за рахунок набагато більш надійного алгоритму шифрування з використанням тимчасових ключів (TKIP). TKIP змінює ключ для кожного пакета, тому його набагато складніше зламати.

IEEE 802.11i / WPA2. Стандарт IEEE 802.11i є галузевим стандартом безпеки бездротових мереж. Версія Wi-Fi Alliance називається WPA2. 802.11i і WPA2 використовують для шифрування вдосконалений стандарт шифрування (AES). В даний час AES вважається найнадійнішим протоколом шифрування.

Використовувати WEP вже не рекомендується. Загальні ключі WEP показали свою неспроможність, і, отже, їх не слід використовувати. Щоб компенсувати слабкі сторони загальних ключів WEP, компанії спочатку намагалися приховувати ідентифікатори SSID і фільтрувати MAC-адреси. Ці методи також виявилися занадто ненадійними.

З огляду на ненадійність систем безпеки на основі WEP, протягом деякого часу використовувалися проміжні заходи безпеки. Такі постачальники, як Cisco, прагнучи задовольнити підвищені вимоги щодо безпеки, розробили власні системи, одночасно намагаючись удосконалити стандарт 802.11i. В процесі розвитку стандарту 802.11i був створений алгоритм шифрування TKIP, який був пов'язаний з методом забезпечення безпеки Wi-Fi Alliance WPA.

Сучасні бездротові мережі завжди повинні використовувати стандарт 802.11i / WPA2. WPA2 є версією Wi-Fi стандарту 802.11i, отже, терміни WPA2 і 802.11i часто є взаємозамінними.

З 2006 року всі пристрої, на які нанесено логотип Wi-Fi Certified, сертифіковані для використання WPA2.

Шифрування використовується для захисту даних. Якщо зловмисник виконав захоплення зашифрованих даних, він не зможе їх розшифрувати за короткий термін.

Стандарти IEEE 802.11i, Wi-Fi Alliance WPA і WPA2 використовують такі методи шифрування:

Шифрування з використанням тимчасових ключів (TKIP). TKIP є методом шифрування, який використовується стандартом WPA. Він забезпечує підтримку попередніх версій обладнання мереж WLAN за рахунок усунення вихідних вразливостей, характерних для методу шифрування 802.11 WEP. Він використовує WEP, однак виконує шифрування корисного навантаження 2 рівня з використанням TKIP і виконує перевірку цілісності повідомлень в зашифрованому пакеті, щоб переконатися в тому, що повідомлення не використовується несанкціоновано.

Вдосконалений стандарт шифрування (AES). AES є методом шифрування, який використовується стандартом WPA2. Цей метод є кращим, оскільки відповідає галузевому стандарту IEEE 802.11i. AES виконує ті ж функції, що і TKIP, але забезпечує значно більш надійний метод шифрування. Він використовує протокол CCMP, який дозволяє вузлам призначення розпізнавати зашифровані і незашифровані біти, що використовуються несанкціоновано.

У списку Режим безпеки мережі 2,4 ГГц відображаються доступні методи забезпечення безпеки для маршрутизатора Linksys EA6500. У ньому представлені всі методи, від самих ненадійних (т. Е. Без захисту) до найнадійніших (т. Е. Змішана корпоративна аутентифікація WPA2 / WPA (Mixed Enterprise)). Для мережі 5 ГГц доступний такий же список, що розкривається.

WPA і WPA2 підтримують два типи аутентифікації.

Персональна - призначена для домашніх мереж і невеликих корпоративних мереж. Користувачі виконують аутентифікацію, використовуючи попередньо узгоджений ключ (PSK). Бездротові клієнти виконують аутентифікацію на точці доступу, використовуючи попередньо узгоджений пароль. Спеціалізований сервер аутентифікації не потрібно.

Корпоративна - призначена для корпоративних мереж, але вимагає наявності сервера аутентифікації служби дистанційній аутентифікації користувачів (RADIUS). Хоча цей тип аутентифікації складніший для настройки, він забезпечує підвищену безпеку. Пристрій повинен виконати аутентифікацію за допомогою сервера RADIUS, після чого користувачі повинні пройти аутентифікацію, використовуючи стандарт 802.1X, який задіює для аутентифікації вдосконалений протокол аутентифікації (EAP).

У мережах, до яких пред'являються більш суворі вимоги щодо безпеки, для надання бездротовим клієнтам доступу до мережі потрібна додаткова аутентифікація або увійти в систему. Для корпоративного режиму безпеки потрібно сервер аутентифікації, авторизації та обліку (AAA) RADIUS.

IP-адреса сервера RADIUS - доступний адресу сервера RADIUS.

Номери портів UDP - офіційно призначені порти UDP 1812 для аутентифікації RADIUS і 1813 для обліку RADIUS. Також можливе використання портів UDP тисячі шістсот сорок п'ять і 1 646.

Погоджений ключ - використовується для аутентифікації на точці доступу за допомогою сервера RADIUS.

Погоджений ключ не обов'язково налаштовувати на станції (STA). Його настройка потрібно тільки на точці доступу, щоб виконати аутентифікацію за допомогою сервера RADIUS.

При вході в систему за стандартом 802.1X для обміну даними з точкою доступу і сервером RADIUS використовується протокол EAP. EAP представляє собою платформу для аутентифікації доступу до мережі. Цей протокол надає механізм безпечної аутентифікації і узгодження безпечного закритого ключа, який згодом можна використовувати для сеансу шифрування бездротового зв'язку з використанням механізмів шифрування TKIP або AES.

Сучасні бездротові маршрутизатори надають ряд функцій. Більшість з них працюють без початкового налаштування, використовуючи параметри, задані за замовчуванням. Однак рекомендується змінити вихідні конфігурації за замовчуванням.

Бездротові маршрутизатори для домашнього використання налаштовуються за допомогою графічного веб-інтерфейсу користувача.

Базовий підхід до реалізації бездротової мережі (як і до базової організації будь-якої мережі) полягає в поетапної налаштуванні і тестуванні. Наприклад, перед впровадженням будь-яких бездротових пристроїв необхідно перевірити працездатність існуючої провідної мережі і можливість доступу провідних вузлів до сервісів мережі Інтернет.

Після перевірки працездатності провідної мережі план впровадження має на увазі наступні етапи.

Крок 1. Почніть процес впровадження мережі WLAN з однієї точки доступу і одного бездротового клієнта, не включаючи систему безпеки бездротової мережі.

Крок 2. Переконайтеся в тому, що клієнт отримав IP-адресу від DHCP-сервера і може відправити луна-запит локальному дротовому маршрутизатора, а потім вийти на зовнішній мережу Інтернет.

Крок 3. Налаштуйте систему безпеки бездротової мережі, використовуючи змішану персональну аутентифікацію WPA2 / WPA (Mixed Personal). Ніколи не використовуйте WEP, якщо доступні інші варіанти.

Крок 4. Створіть резервну копію конфігурації.

Перед установкою бездротового маршрутизатора необхідно вивчити наступні настройки:

- Ім'я SSID - ім'я мережі WLAN.
- Пароль мережі (якщо потрібно) - якщо відобразився відповідний запит, слід ввести пароль, необхідний для асоціації та доступу до імені SSID.

- Пароль маршрутизатора - це пароль управління маршрутизатором, рівнозначний enable secret в привілейованому режимі EXEC.
- Ім'я SSID гостьовій мережі - з міркувань безпеки гості можуть бути ізольовані в межах іншого ідентифікатора SSID.
- Пароль гостьовій мережі - це пароль для доступу до імені SSID гостьовій мережі.
- Ім'я користувача Linksys Smart Wi-Fi - обліковий запис в мережі Інтернет, необхідна для віддаленого доступу до маршрутизатора за допомогою мережі Інтернет.
- Пароль Linksys Smart Wi-Fi - пароль для віддаленого доступу до маршрутизатора.

У таблиці на малюнку представлений приклад параметрів, використовуваних для настройки бездротового маршрутизатора Linksys EA6500.

Обзор параметров управления и настройки

Параметры управления	Параметры
Имя сети (SSID)	Home-Net
Пароль сети	cisco123
Пароль маршрутизатора	class123
Имя гостевой сети (SSID)	Home-Net-Guest
Пароль гостевой сети	cisco
Имя пользователя Linksys Smart Wi-Fi	My-Name
Пароль Linksys Smart Wi-Fi	class12345

Рис. 5.3.45

У комплекті з бездротовим маршрутизатором Linksys EA6500 поставляється компакт-диск.

Для установки і налаштування програмного забезпечення маршрутизатора Linksys EA6500 виконайте наступні дії:

Крок 1. Вставте компакт-диск в CD- або DVD-привід комп'ютера. Процес установки запуститься автоматично. Якщо компакт-диск недоступний, слід завантажити програму установки з веб-сайту http://Linksys.com/support.

На рис. 1 показано початкове вікно «Підключення Linksys EA6500», в якому представлені інструкції з підключення живлення маршрутизатора і час активного з'єднання з Інтернетом.

Начальные инструкции

Рис. 5.3.46

Примітка. У нашому прикладі бездротовий маршрутизатор НЕ буде підключатися до мережі Інтернет.

Крок 2. Натисніть Next (Далі), щоб почати установку.

Програма установки почне установку і відобразить вікно стану (рис. 2). Протягом цього періоду програма установки спробує налаштувати і включити з'єднання з Інтернетом. У цьому прикладі з'єднання з Інтернетом недоступне, і після декількох спроб підключення до мережі Інтернет вам буде запропоновано пропустити цей крок.

Состояние настройки маршрутизатора

Рис. 5.3.47

З'явиться вікно налаштувань маршрутизатора Linksys (рис. 3). У цьому вікні налаштовується ідентифікатор SSID, пароль бездротової мережі і пароль адміністратора.

Состояние настройки маршрутизатора

Рис. 5.3.48

Крок 3. Натисніть Next (Далі), щоб відобразити екран зі зведеною інформацією про налаштування маршрутизатора (рис. 4). Запишіть ці настройки, якщо вихідна таблиця раніше не була заповнена.

Сводка по настройкам маршрутизатора

Рис. 5.3.49

Крок 4. Натисніть Next (Далі), щоб відобразити параметри для настройки вікна облікового запису Linksys Smart Wi-Fi (рис. 5).

Создание учетной записи Linksys Smart Wi-Fi

Рис. 5.3.50

За допомогою цього вікна здійснюється віддалене управління маршрутизатором по мережі Інтернет. У цьому прикладі обліковий запис Linksys Smart Wi-Fi не налаштовується, оскільки не маєте доступу до Інтернету.

Крок 5. Натисніть Continue (Продовжити), щоб відобразити вікно входу в систему (рис. 6). Оскільки підключення до мережі Інтернет не налаштоване, потрібно пароль адміністратора для маршрутизатора.

Вход в систему маршрутизатора

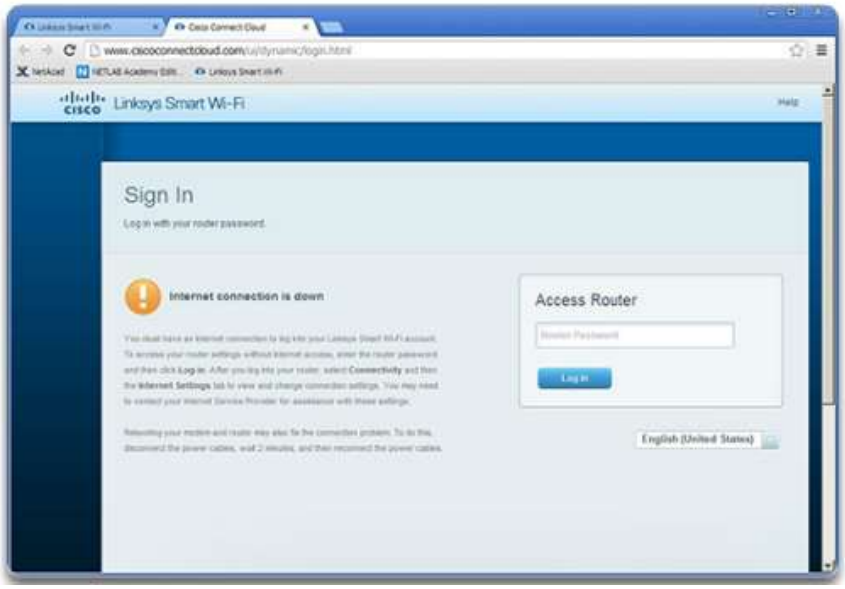


Рис. 5.3.51

Крок 6. При введенні пароля натисніть Log in (Вхід в систему) для відображення головної сторінки Linksys Smart Wi-Fi (рис. 7).

EA6500 Web Dashboard

Рис. 5.3.52

Налаштування головної сторінки Linksys Smart Wi-Fi

Налаштування маршрутизатора Smart Wi-Fi - цей розділ використовується для зміни налаштувань підключення, пошуку та усунення неполадок, бездротового зв'язку і безпеки.

Инструменты Smart Wi-Fi

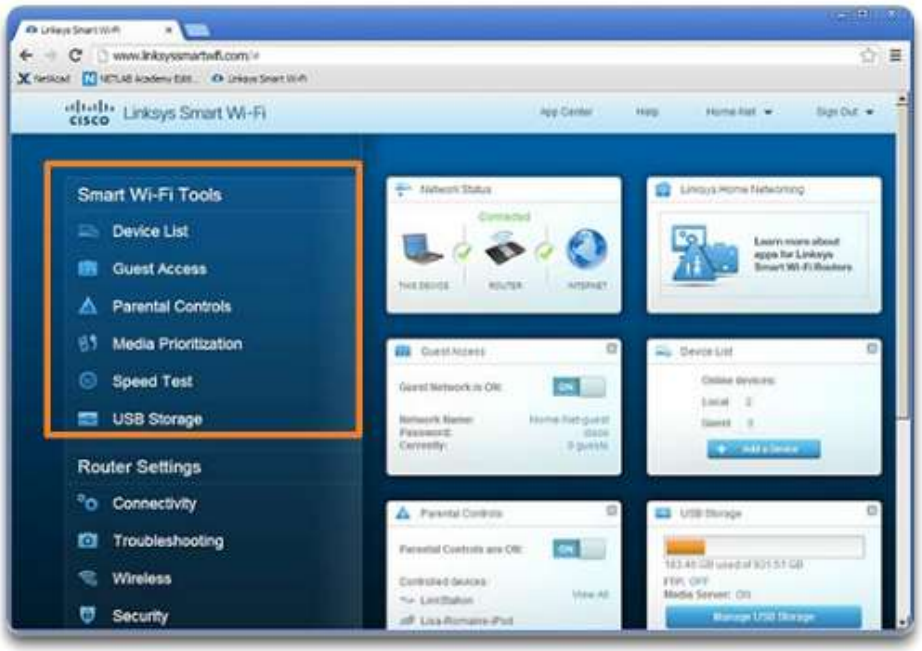


Рис. 5.3.53

Інструменти Smart Wi-Fi. Цей розділ використовується для перегляду користувачів, підключених до мережі зараз, створення окремої мережі для гостей, настройки батьківського контролю для захисту дітей, приоритизации смуги пропускання для окремих пристроїв і додатків, перевірки швидкості з'єднання з Інтернетом і контролю доступу до загальних файлів.

Настройки маршрутизатора Smart Wi-Fi

Рис. 5.3.54

Віджет Smart Wi-Fi. Надає короткий опис розділу «Інструменти Smart Wi-Fi».

Список пристроїв - відображає список пристроїв, підключених до мережі WLAN. Доступна персоналізація імен та значків пристроїв. С допомогою цієї служби також можна підключати пристрої.

Список устройств

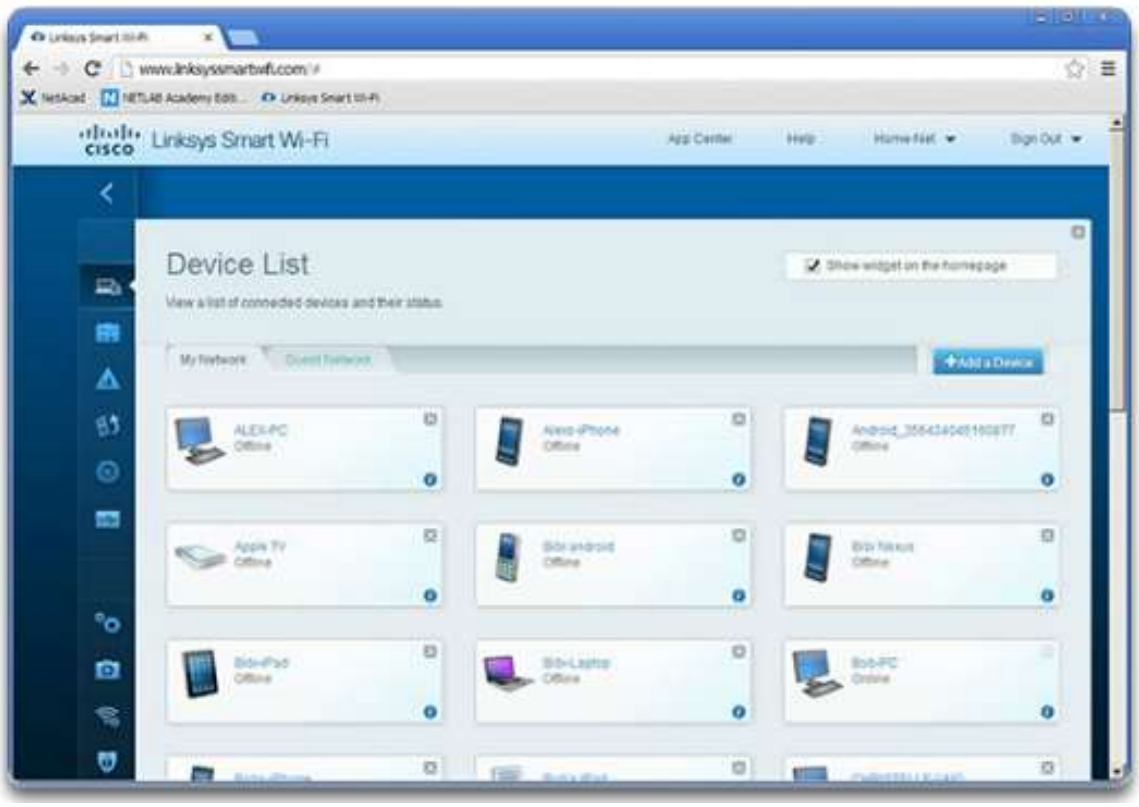


Рис. 5.3.55

Гостьовий доступ - створення окремої мережі, що підтримує до 50 гостей, забезпечуючи при цьому захист мережевих файлів за допомогою інструменту гостьового доступу.

Гостевой доступ

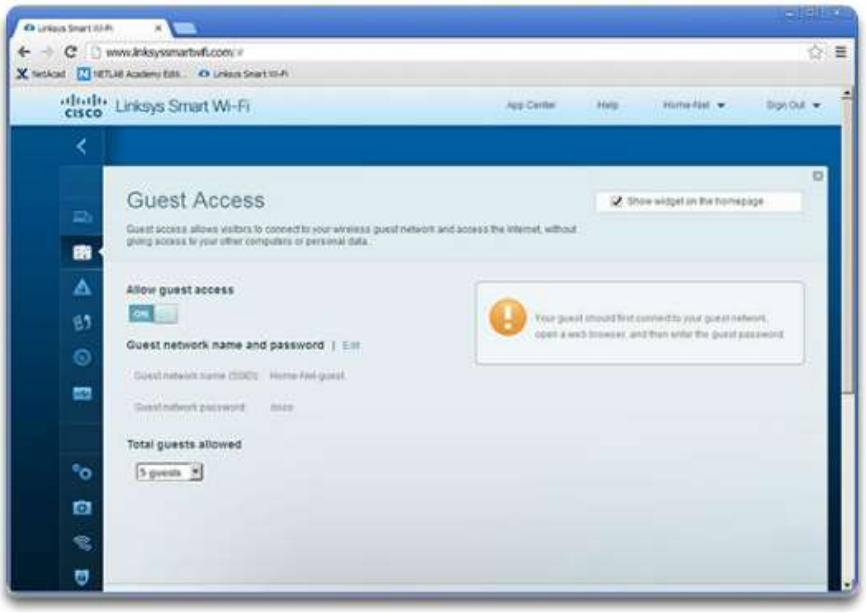


Рис. 5.3.56

Батьківський контроль - захист дітей і членів сім'ї шляхом обмеження доступу до потенційно шкідливим веб-сайтів. Цей інструмент використовується для обмеження доступу до Інтернету на окремих пристроях, контролю часу доступу окремих пристроїв до Інтернету і дат, коли такий доступ можливий; блокування окремих веб-сайтів на певних пристроях; відключення обмежень доступу до Інтернету і відключення функції батьківського контролю.

Родительский контроль

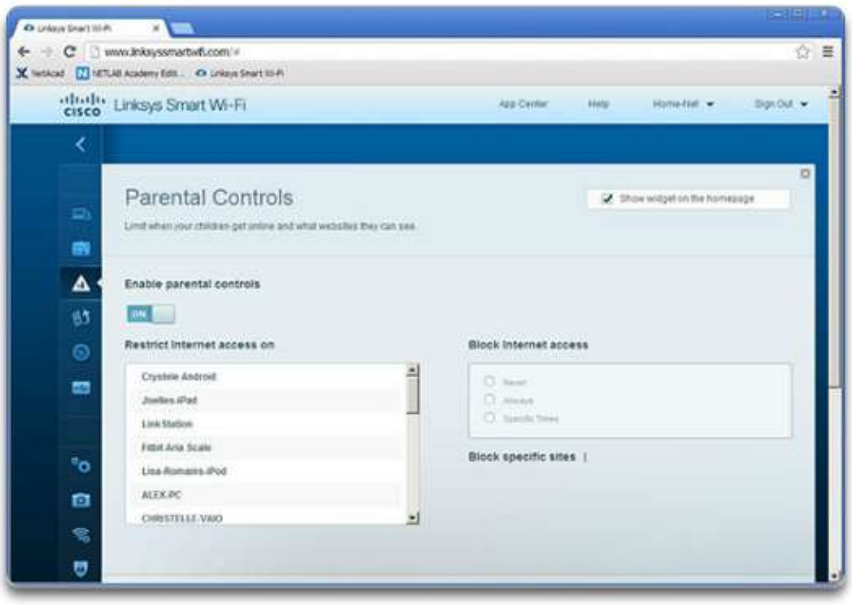


Рис. 5.3.57

Пріоритизація середовища - пріоритизація смуги пропускання для окремих пристроїв і додатків. За допомогою цього інструменту виконується

оптимізація роботи в мережі Інтернет за рахунок приоритизации смуги пропускання для додатків і пристроїв, яким вона потрібна в першу чергу. Цей інструмент можна використовувати для задіяння функції «Налаштування» інструменту приоритизации середовища, додати інші програми, яким призначається окрема смуга пропускання, а також для виділення додаткової пропускної здатності для додатків, пристроїв або онлайн-ігор шляхом настройки пріоритету смуги пропускання.

Приоритизация носителя

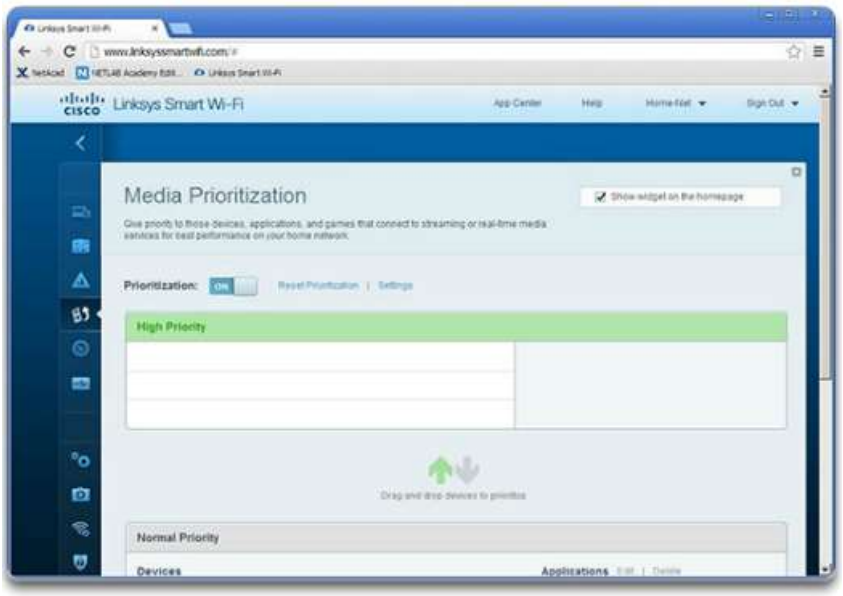


Рис. 5.3.58

Перевірка швидкості - цей інструмент використовується для перевірки швидкості завантаження і відправки на каналі Інтернет. Рекомендується використовувати для отримання базових характеристик.

Проверка скорости

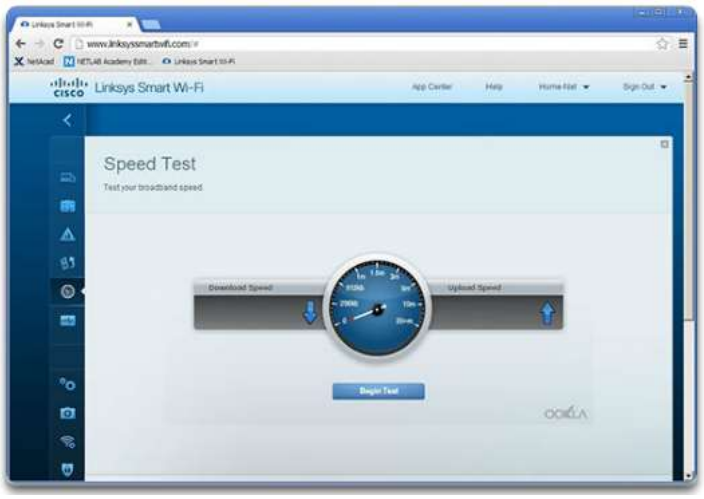


Рис. 5.3.59

Пристрій зберігання USB - Контролює доступ до загальних файлів. Визначає, яким чином користувачі можуть отримати доступ до загальних файлів. За допомогою цього інструменту користувачі можуть здійснювати доступ до пам'яті USB, створювати спільні матеріали на USB-накопичувачі,

налаштовувати параметри доступу до папки, налаштовувати параметри доступу пристроїв і комп'ютерів в мережі до FTP-сервера і налаштовувати доступ до сервера середовища.

Устройство хранения USB

Рис. 5.3.60

Як і для ОС IOS маршрутизатора Cisco, для конфігурації домашнього маршрутизатора також потрібно резервне копіювання на випадок збою. Якщо для домашнього маршрутизатора зберігається конфігурація за замовчуванням, резервне копіювання конфігурації не потрібно. Однак в разі налаштування різних інструментів Smart Wi-Fi рекомендується створити резервну копію конфігурації.

Резервне копіювання конфігурації на бездротовому маршрутизаторі Linksys EA6500 виконується досить просто:

Крок 1. Виконайте вхід в систему на головній сторінці Smart Wi-Fi. Натисніть значок Troubleshooting (Усунення неполадок) для відображення вікна статусу пошуку та усунення неполадок (рис. 1).

Откройте окно поиска и устранения неполадок

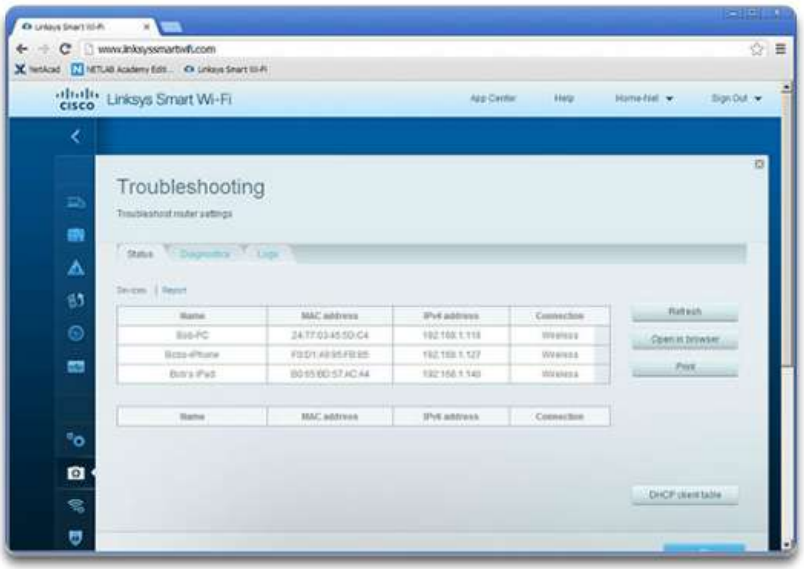


Рис. 5.3.61

Крок 2. Перейдіть на вкладку Diagnostic (Діагностика), щоб відкрити вікно діагностики та усунення неполадок (рис. 2).

Откройте окно диагностики, поиска и устранения неполадок

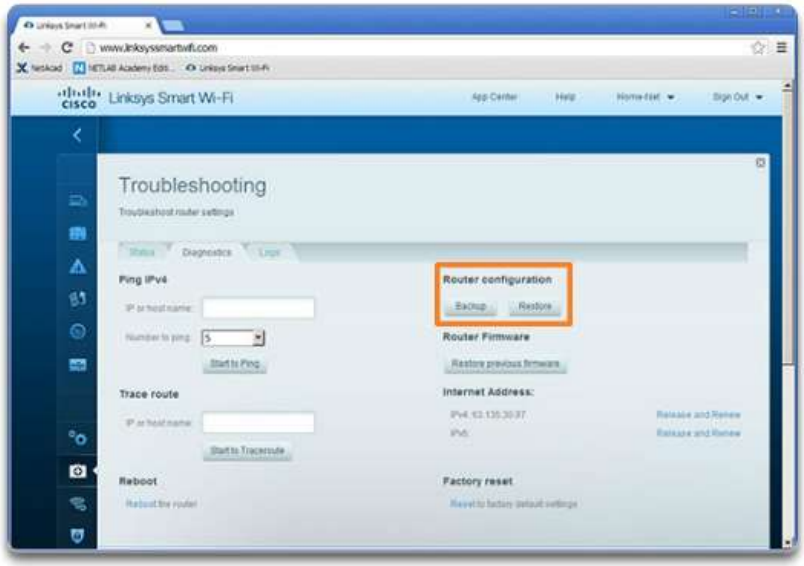


Рис. 5.3.62

Крок 3. Під заголовком «Конфігурація маршрутизатора» клацніть Backup (Резервне копіювання) і збережіть файл у відповідну папку.

Після установки точки доступу або бездротового маршрутизатора, необхідно налаштувати бездротовий мережевий адаптер на клієнті, щоб дозволити для нього підключення до мережі WLAN. Користувач також повинен переконатися в тому, що клієнт успішно підключений до обраної бездротової мережі, особливо в тому випадку, якщо є кілька мереж WLAN.

Пошук і усунення будь-яких неполадок в мережі необхідно виконувати, використовуючи систематичний підхід. Логічні мережеві моделі, наприклад OSI і TCP / IP, поділяють функції мережі на модульні рівні.

При пошуку і усунення неполадок багаторівневі моделі можна застосувати до фізичної мережі, щоб ізолювати виникли проблеми з мережею. Наприклад, якщо всі ознаки вказують на проблему з фізичним підключенням, то мережевий фахівець може зосередитися на усуненні неполадок на каналі, який працює на фізичному рівні. Якщо цей канал функціонує належним чином, технічний фахівець перевіряє на іншому рівні ті області, які можуть викликати проблему.

Існують три основні підходи до пошуку та усунення неполадок, які використовуються для вирішення проблем з мережею.

Знизу вгору: почати 1 рівні і просуватися в напрямку вгору. (Рис. 1)

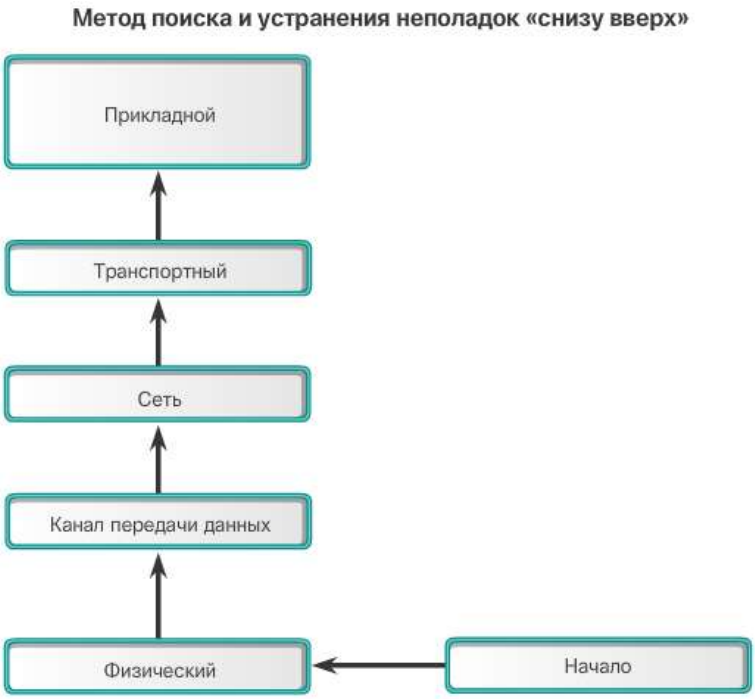


Рис. 5.3.63

Зверху вниз: почати на верхньому рівні і просуватися в напрямку вниз. (Рис. 2)

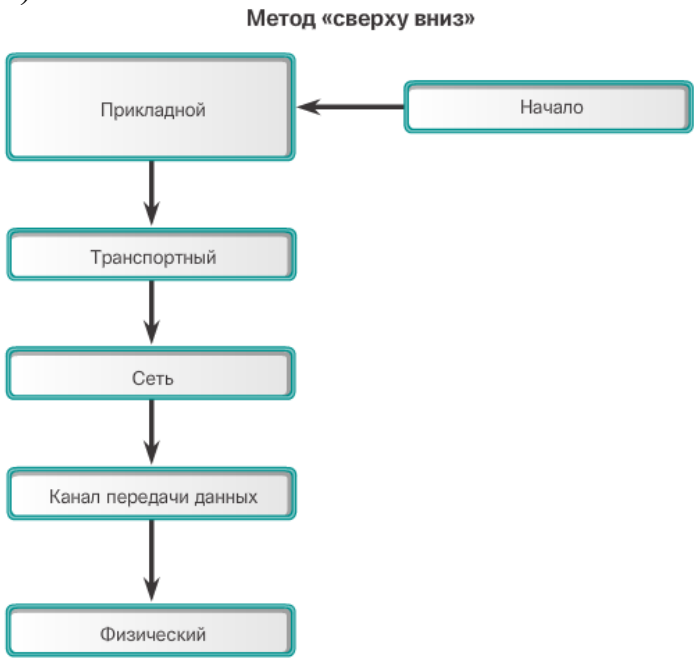


Рис. 5.3.64

«Розділяй і володарюй»: відправити луна-запит на адресу призначення. Якщо луна-запит не проходить, слід перевірити нижні рівні. Якщо луна-запит проходить, слід перевірити верхні рівні. (Рис. 3)

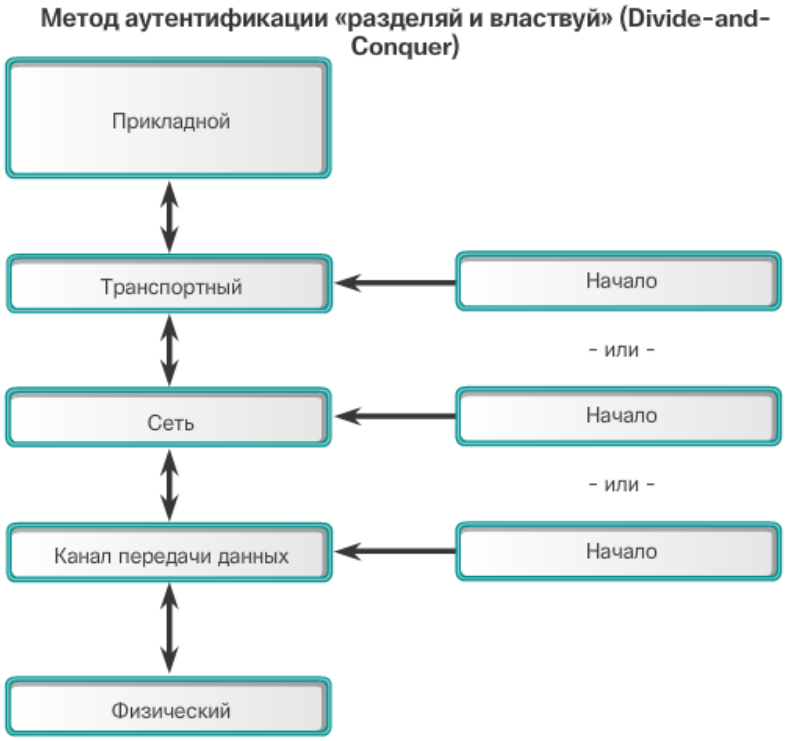


Рис. 5.3.65

При пошуку і усунення неполадок в мережі WLAN рекомендується використовувати процес виключення кандидатів.

На малюнку бездротової клієнт не може підключитися до мережі WLAN. При відсутності підключення необхідно перевірити наступне:

Перевірте конфігурацію мережі на комп'ютері за допомогою команди ipconfig. Переконайтеся, що ПК отримав IP-адреса по DHCP або був налаштований з використанням статичного IP-адреси.

Перевірте можливість підключення пристрою до провідної мережі. Підключіть пристрій до провідної мережі LAN і виконайте команду ping для відомого IP-адреси.

При необхідності слід перезавантажити драйвери, відповідні клієнту. Можливо, буде потрібно використання іншого бездротового мережевого адаптера.

Якщо бездротової мережевий адаптер справний, слід перевірити режим безпеки і настройки шифрування на клієнті. Якщо настройки безпеки не відповідають, клієнт не може отримати доступ до мережі WLAN.

Якщо комп'ютер справний, але підключення до бездротової мережі не працює належним чином, перевірте наступне:

Як далеко від точки доступу знаходиться комп'ютер? Чи знаходиться комп'ютер за межами запланованої зони покриття (BSA)?

Перевірте настройки каналу на бездротовому клієнта. Клієнтське ПЗ повинно виконати виявлення відповідного каналу, якщо ім'я SSID є вірним.

Перевірте наявність в зоні інших пристроїв, які можуть створювати перешкоди в смузі 2,4 ГГц. Прикладами даних пристроїв можуть послужити радіотелефони, радіо-няні, мікрохвильові печі, бездротові системи безпеки і потенційно шкідливі точки доступу. Дані, що надходять з цих пристроїв, можуть створювати перешкоди в роботі мережі WLAN і викликати перебої в з'єднанні між бездротовим клієнтом і точкою доступу.

Далі необхідно переконатися, що всі пристрої знаходяться на своїх місцях. Не забувайте про ймовірність виникнення проблем з фізичною безпекою. На всі пристрої підключений до джерела живлення? Чи всі пристрої включені?

Перевірте з'єднання між підключеними за допомогою кабелів пристроями на предмет несправних роз'ємів, пошкоджених або відсутніх кабелів. Якщо фізично всі необхідні компоненти на місці, перевірте дротову мережу LAN за допомогою ехо-тестування пристроїв, включаючи точку доступу. Якщо підключення на цьому етапі все ще відсутня, можливо, виникла проблема з точкою доступу або її конфігурацією.

Якщо комп'ютер не є джерелом проблеми і фізичний стан пристроїв перевірено, слід вивчити роботу точки доступу. Перевірте стан харчування точки доступу.

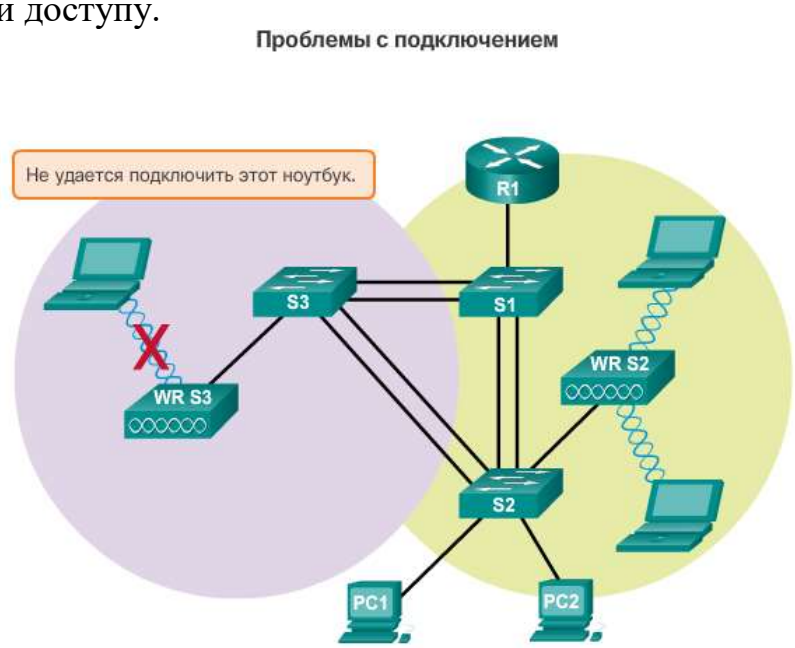


Рис. 5.3.66

Щоб оптимізувати і збільшити пропускну здатність дводіапазонних маршрутизаторів 802.11n / ac, можна зробити наступне:

Оновити бездротові клієнти. Застарілі моделі пристроїв 802.11b і навіть 802.11g можуть уповільнювати роботу всієї мережі WLAN. Щоб домогтися оптимальної продуктивності, все бездротові пристрої повинні підтримувати одні і ті ж максимально допустимі стандарти.

Розділити трафік. Найпростіший спосіб оптимізувати продуктивність бездротової мережі - розділити смугу 802.11n 2,4 ГГц і смугу 5 ГГц. Отже, з метою полегшення управління трафіком стандарт IEEE 802.11n (або вище) може використовувати дві смуги, як дві окремі бездротові мережі. Наприклад, можна використовувати мережу 2,4 ГГц для виконання основних завдань в мережі Інтернет (веб-серфінг, робота з електронною поштою і завантаження даних), а смугу 5 ГГц використовувати для потокової передачі мультимедійних файлів, як показано на рис. 1.

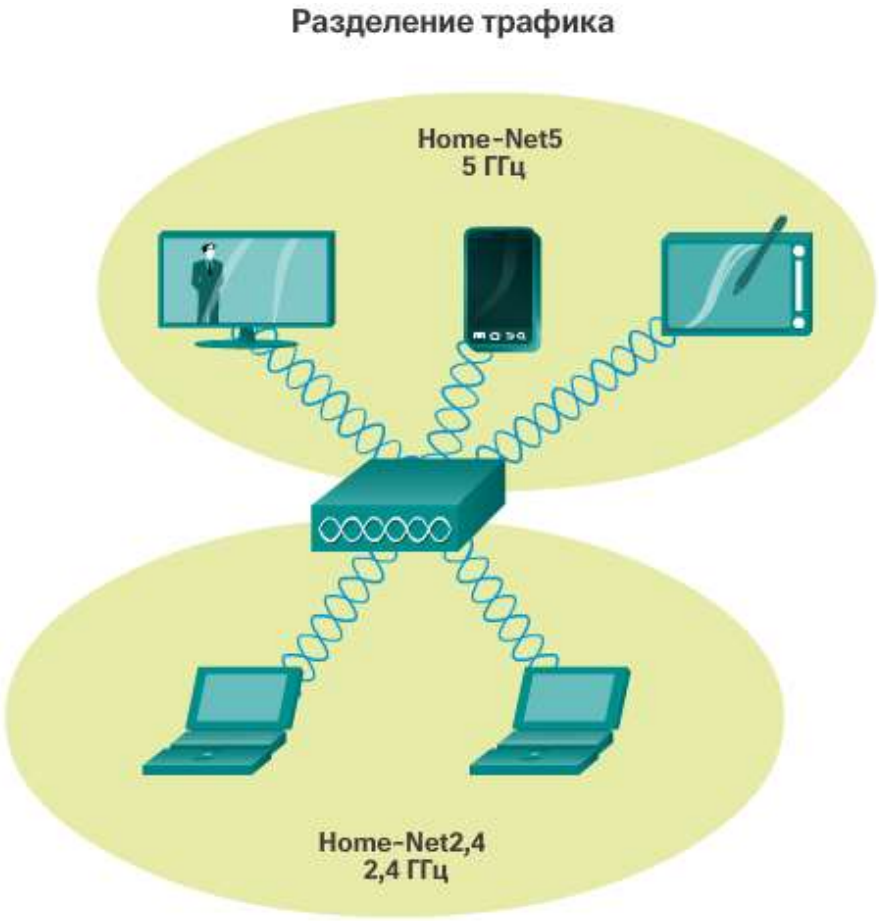


Рис. 5.3.67

Існує ряд передумов для використання поділу трафіку.

Смуга 2,4 ГГц підходить для базового інтернет-трафіку, який не чутливий до затримок.

Смугу пропускання можна використовувати спільно з іншими найближчими мережами WLAN.

Смуга 5 ГГц набагато менш завантажена, ніж смуга 2,4 ГГц, і ідеально підходить для потокової передачі мультимедійних файлів.

Смуга 5 ГГц містить більше каналів, отже, обраний канал, швидше за все, не буде схильний до дії перешкод.

За замовчуванням дводіапазонні маршрутизатори використовують однакове ім'я мережі на шпальтах 2,4 ГГц і 5 ГГц. Найпростішим способом сегментування трафіку є перейменування однієї з бездротових мереж, як показано на рис. 2. При наявності окремого описову назву набагато простіше отримати доступ до потрібної мережі.

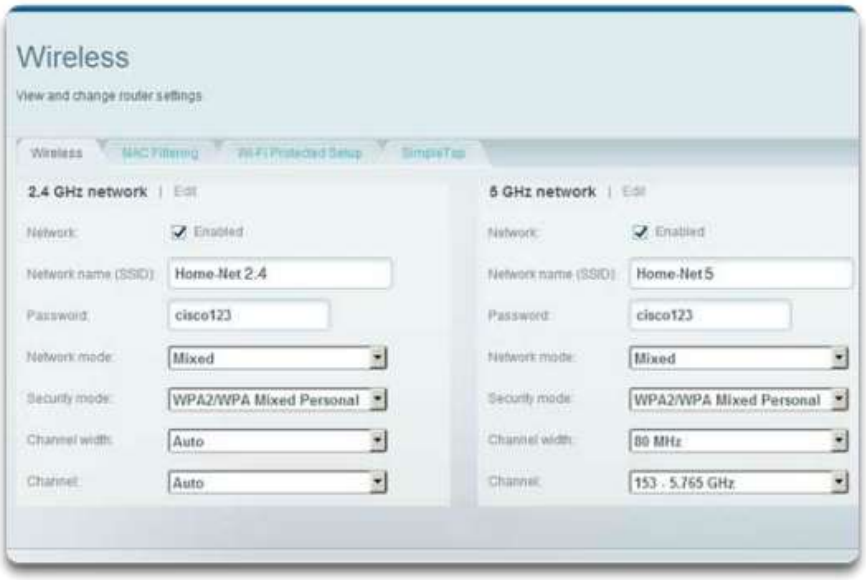


Рис. 5.3.68

Щоб розширити діапазон дії бездротової мережі, слід забезпечити відсутність будь-яких перешкод у зоні фізичного розташування бездротового маршрутизатора (меблі, арматура і високі предмети). Такі перешкоди блокують сигнал, через що діапазон дії мережі WLAN зменшується. Якщо проблема як і раніше не вирішена, можна використовувати технологію збільшення покриття Wi-Fi Range Extender або бездротову технологію Powerline.

5.4 Базові поняття протоколу OSPF, його робота та налаштування

OSPF - це популярний протокол маршрутизації з урахуванням стану каналів, який підтримує точну настройку різними способами. До найбільш поширених з цих способів відносяться управління процедурою вибору виділеного і резервного виділеного маршрутизаторів (DR і BDR, відповідно), поширення маршрутів за замовчуванням, точна настройка інтерфейсів OSPFv2 і OSPFv3, а також включення аутентифікації.

Статична маршрутизація

На малюнку представлений приклад сценарію статичної маршрутизації. Адміністратор може вручну налаштувати статичний маршрут для доступу до конкретної мережі. На відміну від протоколу динамічної маршрутизації, статичні маршрути не оновлюються автоматично, і при змінах в мережевій топології їх необхідно повторно налаштовувати вручну. Статичні маршрути не змінюються до тих пір, поки адміністратор не переналаштувати їх вручну.

Рис. 5.4.1

Статична маршрутизація використовується в трьох ситуаціях:

- забезпечення спрощеного обслуговування таблиці маршрутизації в невеликих мережах, які не планується суттєво розширювати;
- маршрутизація до тупикових мереж і від них. Тупикова мережа являє собою мережу, доступ до якої здійснюється через один маршрут, і маршрутизатор має тільки одне сусіднє пристрій.

Використання єдиного маршруту за замовчуванням для подання шляху до будь-якої мережі, що не має більш точного збігу з іншим маршрутом в таблиці маршрутизації. Маршрути за замовчуванням використовуються для відправки трафіку в будь-який пункт призначення за межами наступного маршрутизатора в висхідному напрямку.

Протоколи маршрутизації дозволяють маршрутизаторам динамічно обмінюватися відомостями про віддалених мережах, як показано на малюнку. Маршрутизатор, які отримують оновлення, автоматично додають цю інформацію в власні таблиці маршрутизації. Протоколи маршрутизації визначають оптимальний шлях або маршрут до кожної мережі. Основною перевагою протоколів динамічної маршрутизації є те, що вони забезпечують обмін маршрутизирующий інформацією між маршрутизаторами в випадках змін в топології. Подібний обмін даними дозволяє маршрутизаторам автоматично отримувати інформацію про нові мережах, а також знаходити альтернативні шляхи в разі збою каналу до поточної мережі.

У порівнянні зі статичної маршрутизацією протоколи динамічної маршрутизації вимагають меншого втручання з боку адміністратора. Проте, до витрат використання протоколів динамічної маршрутизації можна віднести той факт, що частина ресурсів маршрутизатора виділяється для роботи протоколу (включаючи час ЦП і смугу пропускання мережевого каналу). Незважаючи на переваги динамічної маршрутизації, статична маршрутизація як і раніше знаходить застосування. В окремих випадках рекомендується використовувати саме статичну маршрутизацію, так само як в інших краще вибрати динамічну маршрутизацію. Однак важливо розуміти, що статична і динамічна маршрутизації не є взаємовиключними. У більшості мереж використовується комбінація протоколів динамічної маршрутизації і статичних маршрутів.

До двох найбільш поширеним прикладів протоколів динамічної маршрутизації відносяться EIGRP і OSPF. В рамках даної глави розглядається переважно OSPF.

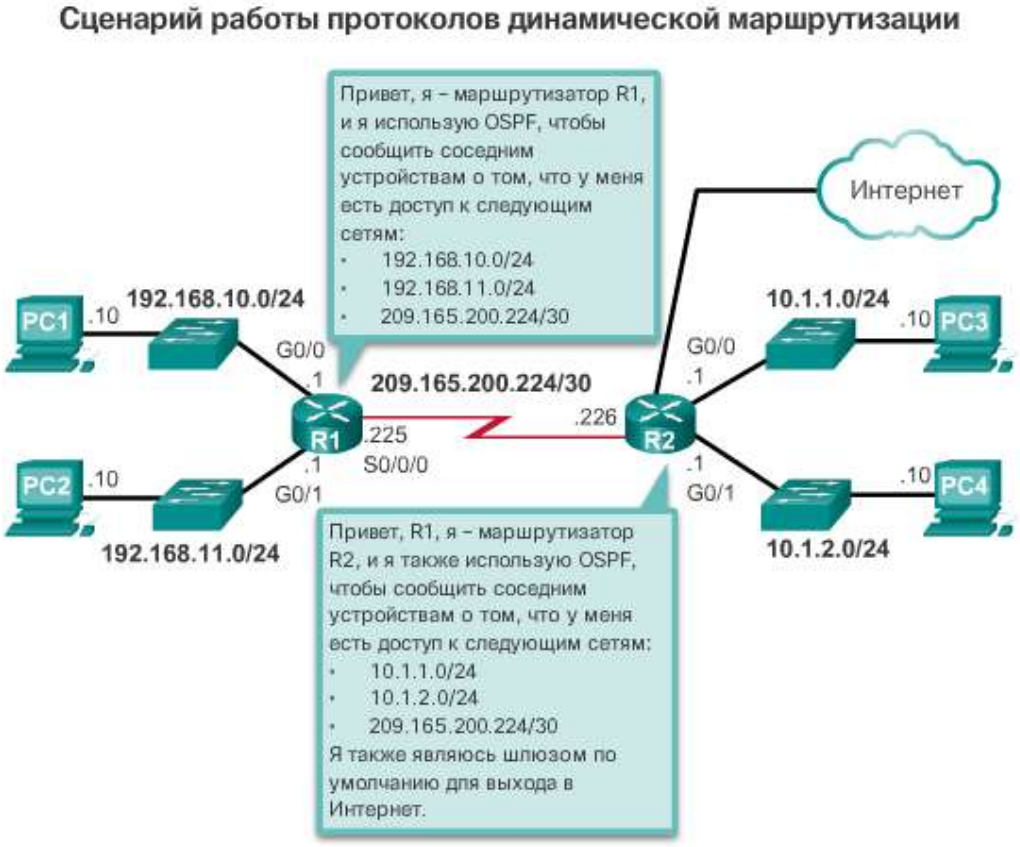


Рис. 5.4.2

OSPF - це поширений протокол маршрутизації з урахуванням стану каналів. Він був розроблений в якості заміни для протоколу на базі векторів відстані, RIP. Однак протокол OSPF має ряд значних переваг в порівнянні з протоколом RIP, забезпечуючи швидшу збіжність і можливість масштабування в мережах більшого розміру.

Як показано на малюнку, протокол OSPF має такі властивості:

- Безкласовість - протокол розроблений як безкласовий, отже, він підтримує використання VLSM і маршрутизації CIDR.
- Ефективність - зміни маршрутизації запускають відновлення маршрутизації (без періодичних оновлень). Протокол використовує алгоритм пошуку найкоротшого шляху SPF для вибору оптимального шляху.
- Швидка збіжність - швидкість поширення змін мережі.
- Масштабованість - підходить для використання як в невеликих, так і у великих мережах. Для підтримки ієрархічної структури маршрутизатори групуються в області.
- Безпека - підтримує аутентифікацію Message Digest 5 (MD5). Якщо ця функція включена, маршрутизатори OSPF приймають тільки зашифровані повідомлення маршрутизації від рівноправних вузлів з однаковим попередньо заданим паролем.

Рис. 5.4.3

Налаштування OSPF для однієї області

В рамках даної глави основна увага приділяється налаштування та усунення неполадок в роботі OSPF. Однак рекомендується повторно переглянути інформацію про базову реалізації протоколу маршрутизації OSPF.

Як приклад на рис. 1 представлена топологія, яка використовується для настройки OSPFv2.

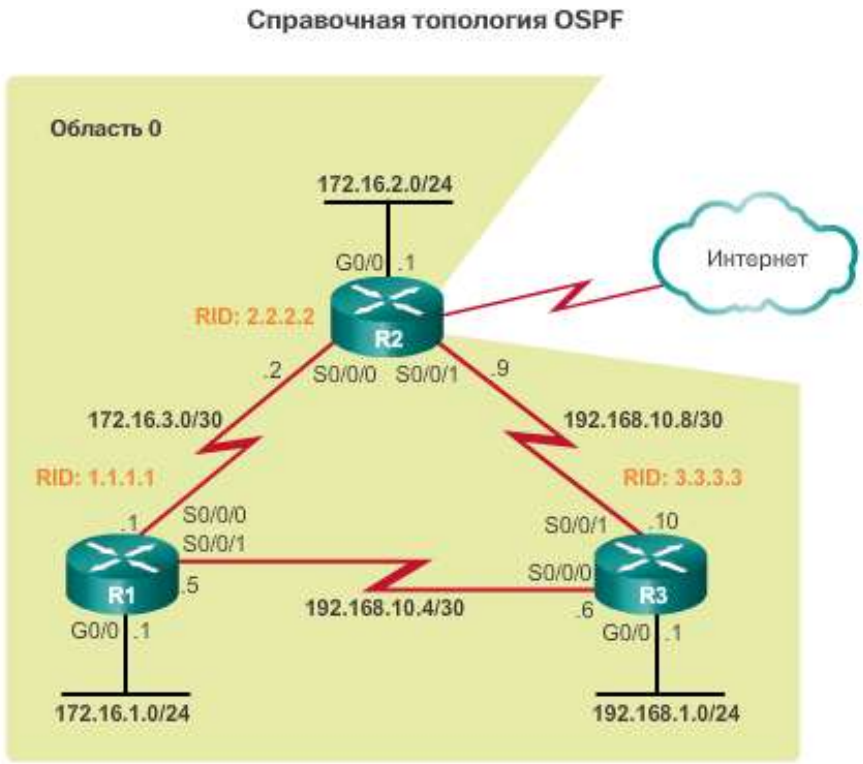


Рис. 5.4.4

Маршрутизатор в топології мають початкову конфігурацію, включаючи адреси інтерфейсів. В даний час на жодному з маршрутизаторів не настроєна статична або динамічна маршрутизація. Всі інтерфейси на маршрутизаторах R1, R2 і R3 (за винятком інтерфейсу loopback на маршрутизаторі R2) знаходяться в межах магістральної області OSPF. Маршрутизатор ISP використовується в якості шлюзу домену маршрутизації в Інтернет.

На рис. 2 інтерфейс Gigabit Ethernet 0/0 на маршрутизаторі R1 налаштовується для відображення його дійсної пропускної здатності, яка становить 1 000 000 кілобіт (т.е.1 000 000 000 біт / с). Далі, в режимі настройки маршрутизатора OSPF проводиться призначення ідентифікатора маршрутизатора, настройка еталонної пропускної здатності для швидкісних інтерфейсів і оголошення трьох мереж, підключених до маршрутизатора R1. Зверніть увагу на використання шаблонної маски для визначення конкретних мереж.

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# bandwidth 1000000
R1(config-if)# exit
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent
across all routers.
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# network 172.16.3.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
R1(config-router)#
R1(config-router)# passive-interface g0/0
R1(config-router)#
```

Рис. 5.4.5

На рис. 3 інтерфейс Gigabit Ethernet 0/0 на маршрутизаторі R2 теж налаштовується для відображення його дійсної пропускної здатності, призначається ідентифікатор маршрутизатора, налаштовується еталонна пропускна здатність для швидкісних інтерфейсів і оголошуються три мережі, підключені до маршрутизатора R2. Зверніть увагу на те, як можна уникнути використання шаблонної маски шляхом визначення фактичного інтерфейсу маршрутизатора з шаблонної маскою з чотирьох нулів. Завдяки цьому OSPF використовує маску підмережі, призначену інтерфейсу маршрутизатора, як маски оголошується мережі.

Настройка OSPF для одной области на маршрутизаторе R2

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# bandwidth 1000000
R2(config-if)# exit
R2(config)# router ospf 10
R2(config-router)# router-id 2.2.2.2
R2(config-router)# auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent
across all routers.
R2(config-router)# network 172.16.2.1 0.0.0.0 area 0
R2(config-router)# network 172.16.3.2 0.0.0.0 area 0
R2(config-router)# network 192.168.10.9 0.0.0.0 area 0
R2(config-router)#
R2(config-router)# passive-interface g0/0
R2(config-router)#
```

Рис. 5.4.6

Зверніть увагу на повідомлення про те, що маршрутизатор R3 встановив повноцінні сусідські відносини суміжності з маршрутизатором R1 з ідентифікатором 1.1.1.1 і маршрутизатором R2 з ідентифікатором 2.2.2.2. Мережа OSPF успішно зійшлася.

Перевірка OSPF для однієї області

До корисних командам для перевірки OSPF відносяться наступні:

- show ip ospf neighbor - команда використовується для того, щоб переконатися, що маршрутизатор сформував відносини суміжності з сусідніми маршрутизаторами. Якщо ідентифікатор сусіднього маршрутизатора не відображається або не вказує стан FULL, це означає, що обидва маршрутизатора не створили відносини суміжності OSPF.
- show ip protocols - ця команда забезпечує швидку перевірку критично важливих даних конфігурації OSPF. До таких даних належать ідентифікатор процесу OSPF, ідентифікатор маршрутизатора, мережі, які оголошуються маршрутизатором, сусідні пристрої, від яких маршрутизатор приймає оновлення, і значення адміністративної дистанції за замовчуванням, рівне 110 для OSPF.

- show ip ospf - ця команда використовується для відображення ідентифікатора процесу OSPF і ідентифікатора маршрутизатора, а також відомостей про OSPF SPF і про область OSPF.
- show ip ospf interface - ця команда надає докладний список інтерфейсів, де працює протокол OSPF, з її допомогою можна визначити, чи правильно були складені вирази network.
- show ip ospf interface brief - цю команду рекомендується використовувати для відображення короткої інформації та стану інтерфейсів за протоколом OSPF.

Налаштування OSPFv3 для однієї області

Далі ви зможете дізнатися основні відомості про реалізацію протоколу маршрутизації OSPFv3 для IPv6.

Як приклад на рис. 1 представлена топологія, яка використовується для настройки OSPFv3. Маршрутизатор в топології мають початкову конфігурацію, включаючи IPv6-адреси інтерфейсів. В даний час на жодному з маршрутизаторів не настроєна статична або динамічна маршрутизація. Всі інтерфейси на маршрутизаторах R1, R2 і R3 (за винятком інтерфейсу loopback на маршрутизаторі R2) знаходяться в межах магістральної області OSPF.

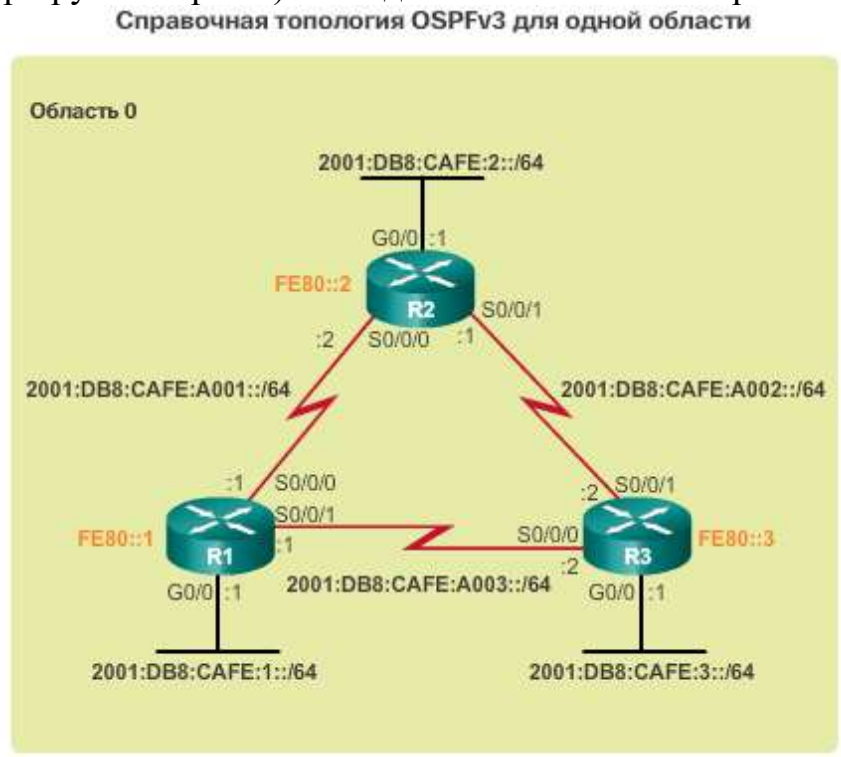


Рис. 5.4.7

На рис. 2, в режимі конфігурації маршрутизатора OSPFv3 на R1, продемонстровано ручне призначення ідентифікатора маршрутизатора і настройка еталонної пропускної здатності для швидкісних інтерфейсів. Далі описується налаштування інтерфейсів, що беруть участь в OSPFv3. Також налаштовується відображення дійсної пропускної здатності інтерфейсу Gigabit Ethernet 0/0. Зверніть увагу, що при налаштуванні OSPFv3 шаблонна маска не потрібно.

Настройка OSPFv3 для одной области на маршрутизаторе R1

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-10-IPv6:  Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all
routers.
R1(config-rtr)#
R1(config-rtr)# interface GigabitEthernet 0/0
R1(config-if)# bandwidth 1000000
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)# end
R1#
```

Рис. 5.4.8

На рис. 3, в режимі конфігурації маршрутизатора OSPFv3 на R2, продемонстровано ручне призначення ідентифікатора маршрутизатора і настройка еталонної пропускної здатності для швидкісних інтерфейсів. Далі описується налаштування інтерфейсів, що беруть участь в OSPFv3. Тут також налаштовується інтерфейс Gigabit Ethernet 0/0 для відображення його дійсної пропускної здатності.

Настройка OSPFv3 для одной области на маршрутизаторе R2

```
R2(config)# ipv6 router ospf 10
R2(config-rtr)# router-id 2.2.2.2
R2(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-10-IPv6:  Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all
routers.
R2(config-rtr)#
R2(config-rtr)# interface GigabitEthernet 0/0
R2(config-if)# bandwidth 1000000
R2(config-if)# ipv6 ospf 10 area 0
R2(config-if)#
R2(config-if)# interface Serial0/0/0
R2(config-if)# ipv6 ospf 10 area 0
R2(config-if)#
R2(config-if)# interface Serial0/0/1
R2(config-if)# ipv6 ospf 10 area 0
R2(config-if)# end
R2#
*Aug 28 19:02:47.991: %OSPFv3-5-ADJCHG: Process 10, Nbr 1.1.1.1 on
GigabitEthernet0/0 from LOADING to FULL, Loading Done
*Aug 28 19:02:48.423: %OSPFv3-5-ADJCHG: Process 10, Nbr 1.1.1.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
*Aug 28 19:02:48.959: %SYS-5-CONFIG_I: Configured from console by
console
R2#
```

Рис. 5.4.9

Перевірка OSPFv3 для однієї області

До корисних командам для перевірки OSPFv3 відносяться наступні:

- show ipv6 ospf neighbor - команда використовується для того, щоб переконатися, що маршрутизатор сформував відносини суміжності з сусідніми маршрутизаторами. Якщо ідентифікатор сусіднього маршрутизатора не відображається або не вказує стан FULL, це означає, що обидва маршрутизатора не створили відносини суміжності OSPF.
- show ipv6 protocols - дозволяє швидко перевірити критично важливі дані конфігурації OSPFv3, включаючи ідентифікатор процесу OSPF, ідентифікатор маршрутизатора і інтерфейси, включені для OSPFv3.
- show ipv6 route ospf - надає відомості про маршрутах OSPFv3, що містяться в таблиці маршрутизації.
- show ipv6 ospf interface brief - цю команду рекомендується використовувати для відображення короткої інформації та стану інтерфейсів, що беруть участь в OSPFv3.

Типи мереж OSPF

Щоб налаштувати параметри OSPF, почніть з базової реалізації протоколу маршрутизації OSPF.

Як показано на рис. 1-5, OSPF включає в себе п'ять типів мереж:

«Точка-точка» - це мережа, яка містить два маршрутизатора, підключених один до одного за одним загальним каналу. До цього каналу не підключені інші маршрутизатори. Як правило, ця конфігурація використовується в мережах WAN. (Рис. 1)

Рис. 5.4.10

Широкомовне мережу множинного доступу - містить кілька маршрутизаторів, підключених один до одного по мережі Ethernet. (Рис. 2)

Рис. 5.4.11

Не широкомовна мережа множинного доступу (NBMA) - містить кілька маршрутизаторів, підключених один до одного в мережі, яка забороняє трансляцію адресацію, наприклад, Frame Relay. (Рис. 3)

Рис. 5.4.12

«Багатоточкова мережа» - містить кілька маршрутизаторів, підключених в зіркоподібною топології через мережу NBMA. Часто використовується дляпідключення філій (кінці зірок) до центрального вузла (концентратор).

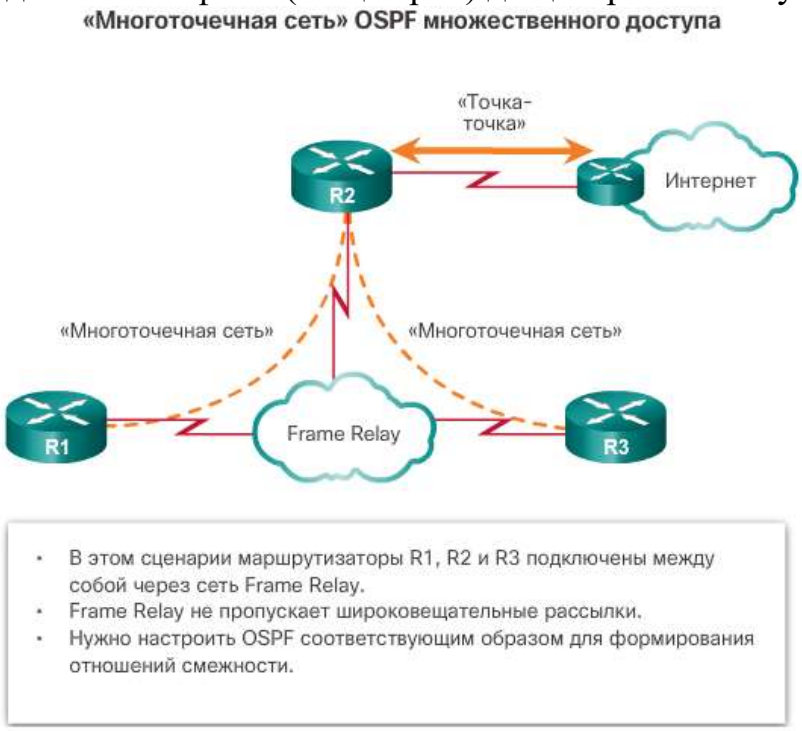


Рис. 5.4.13

(Рис. 4) Віртуальні канали - особлива мережа OSPF, використовувана для з'єднання віддалених областей OSPF з областю магістралі. (Рис. 5)

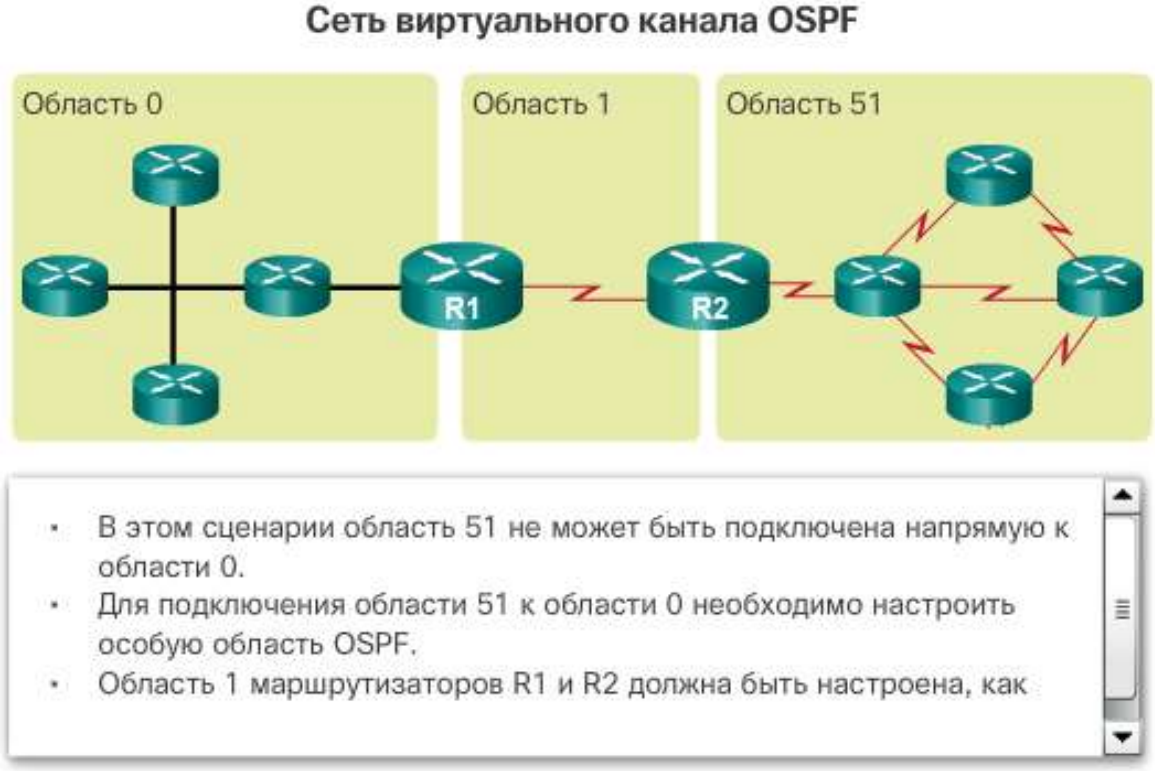


Рис. 5.4.14

Мережа множинного доступу - це мережа з декількома пристроями в одній і тій же середовищі передачі, які обмінюються даними між собою. Локальні мережі Ethernet - це найбільш поширений приклад широкомовних мереж множинного доступу. У широкомовних мережах всі пристрої в рамках мережі

бачать все широкомовні кадри і кадри груповий розсилки. Їх називають мережами з множинним доступом тому, що до них може бути включено безліч вузлів, принтерів, маршрутизаторів і інших пристроїв, які належать одній і тій же мережі. Проблеми, пов'язані з мережами множинного доступу

У мережах множинного доступу протоколу OSPF може зіткнутися з двома проблемами, пов'язаними з лавинної розсилкою пакетів LSA.

Встановлення великої кількості відносин суміжності - мережі Ethernet потенційно можуть забезпечувати взаємодію між безліччю маршрутизаторів OSPF за допомогою загального каналу. Встановлення відносин суміжності з кожним маршрутизатором не потрібно і є небажаним. Подібне призводить до виникнення надмірної кількості пакетів LSA, якими маршрутизатори обмінюються в межах однієї мережі.

Надлишкова лавинна розсилка пакетів LSA - маршрутизатори з маршрутизацією з урахуванням стану каналу виконують лавинную розсилку своїх пакетів LSA при кожній ініціалізації протоколу OSPF або в разі зміни топології. Подібна лавинна розсилка може стати надмірною.

Для розрахунку кількості необхідних відносин суміжності можна використовувати наступну формулу. Кількість відносин суміжності, необхідне для будь-якої кількості маршрутизаторів (відзначених символом n) в мережі множинного доступу розраховується наступним чином:

n (n - 1) / 2

На рис. 1 показана спрощена топологія з чотирьох маршрутизаторів, підключених до однієї мережі Ethernet множинного доступу. Без якого-небудь способу зменшити кількість цих відносин суміжності всі ці маршрутизатори сформують шість відносин суміжності, як показано на рис. 2: 4 (4 - 1) / 2 = 6. На рис. 3 показано значне збільшення кількість відносин суміжності в міру додавання маршрутизаторів до мережі.

Рис. 5.4.15

Рис. 5.4.16

Проблема управління великою кількістю відносин суміжності і лавинної розсилки пакетів LSA в мережі з множинним доступом вирішується за рахунок виділеного маршрутизатора (DR). У мережах множинного доступу протокол OSPF призначає виділений маршрутизатор (DR) як точку збору і поширення відправлених і прийнятих пакетів LSA. На випадок збою виділеного маршрутизатора (DR) також вибирається резервний призначений маршрутизатор (BDR). Маршрутизатор BDR пасивно спостерігає за цим обміном і підтримує відносини з усіма маршрутизаторами. Якщо DR перестає створювати пакети вітання (hello), то BDR самостійно приймає роль DR.

Решта маршрутизатори, які не є DR або BDR, стануть маршрутизаторами DROTHER (маршрутизатор, які не є ні DR, ні BDR).

На рис. 1 маршрутизатор R1 обраний в якості виділеного маршрутизатора для локальної мережі Ethernet, що з'єднує маршрутизатори R2, R3 і R4. Зверніть увагу, що кількість відносин суміжності скоротилося до трьох.

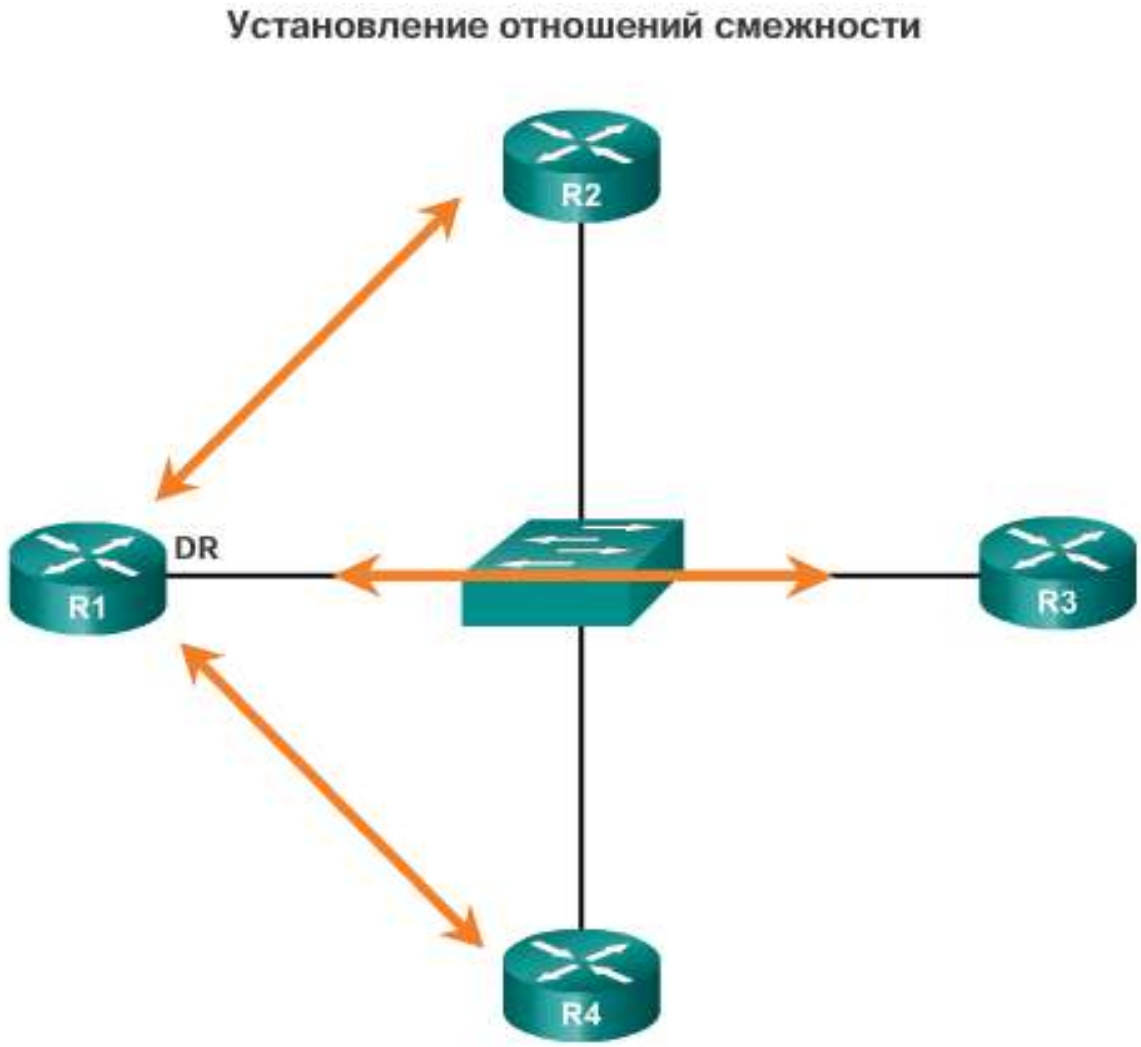


Рис. 5.4.17

Маршрутизатор в мережі множинного доступу вибирають DR і BDR. Маршрутизатор DROTHER формують повні відносини суміжності в мережі тільки з DR і BDR. Замість лавинної розсилки оголошень LSA всім маршрутизаторів в мережі, маршрутизатори DROTHER відправляють свої LSA тільки маршрутизаторів DR і BDR за допомогою адреси групової розсилки 224.0.0.6 (всі маршрутизатори DR).

Маршрутизатор R1 відправляє оголошення LSA маршрутизатора DR. BDR теж прослуховує ці оголошення. Маршрутизатор DR відповідає за пересилку оголошень LSA від R1 всім іншим маршрутизаторів. DR використовує групову розсилку 224.0.0.5 (всі маршрутизатори OSPF). В кінцевому рахунку, тільки один маршрутизатор виробляє розсилку оголошень LSA по мережі з множинним доступом.

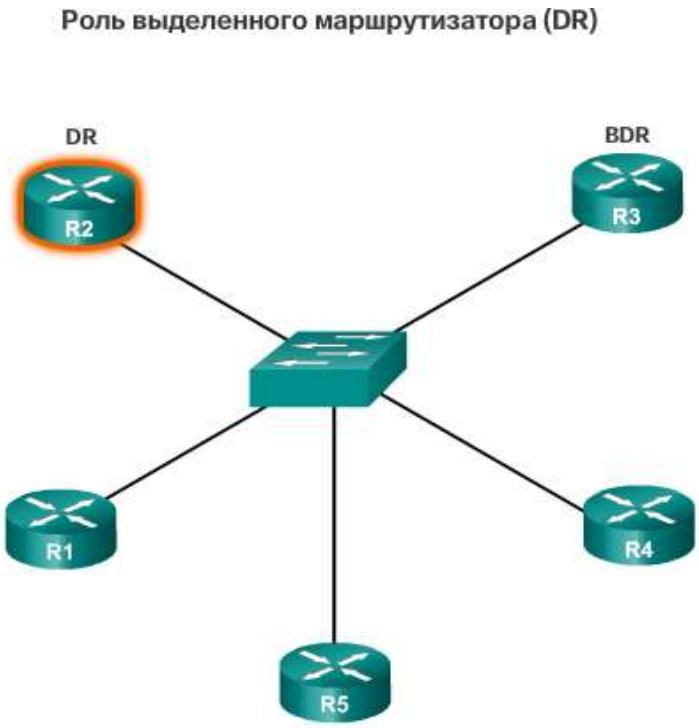


Рис. 5.4.18

Примітка. Вибір DR / BDR відбувається тільки в мережах з множинним доступом і не може статися в мережах «точка-точка».

У топології мережі з множинним доступом, зображеної на рис.1, в одній мережі Ethernet з множинним доступом (192.168.1.0/28) підключені три маршрутизатора. Кожен маршрутизатор налаштований з зазначеним IP-адресою в інтерфейсі Gigabit Ethernet 0/0.

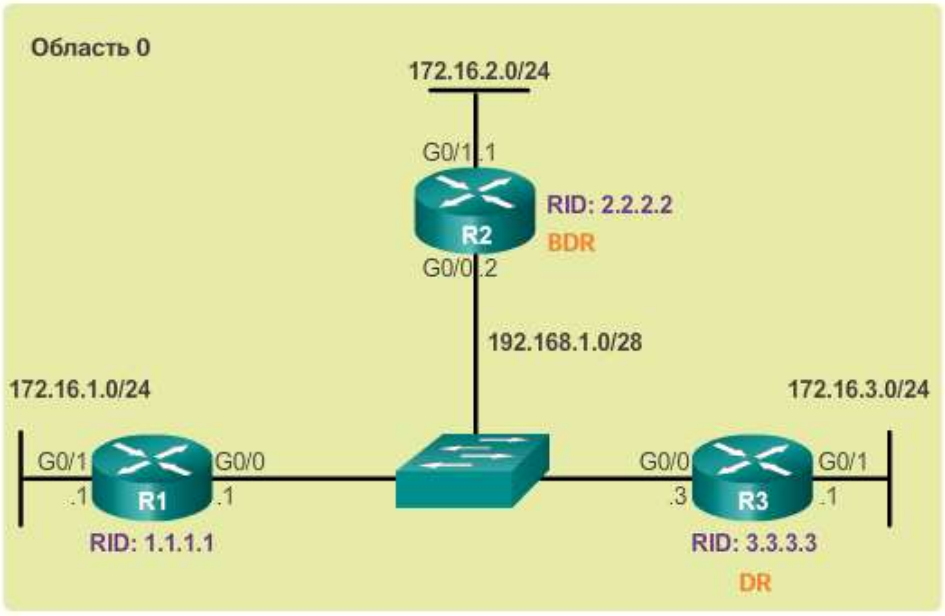


Рис. 5.4.19

Оскільки маршрутизатори з'єднані по загальній широкомовної мережі з множинним доступом, OSPF вибрав DR і BDR автоматично. В даному прикладі в якості DR був обраний маршрутизатор R3, оскільки він володіє ідентифікатором 3.3.3.3 - найвищим в цій мережі. Маршрутизатор R2 обраний в якості BDR, оскільки він володіє найвищим ідентифікатором в мережі серед решти маршрутизаторів.

Для визначення ролі маршрутизатора використовуйте команду show ip ospf interface (рис. 2). Вихідні дані, згенеровані маршрутизатором R1, підтверджують це:

Проверка роли маршрутизатора R1

```
R1# show ip ospf interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
 Internet Address 192.168.1.1/28,Area 0,Attached via Network Statement
 Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
 Topology-MTID    Cost    Disabled    Shutdown      Topology Name
       0           1         no          no            Base
 Transmit Delay is 1 sec, State DROTHER, Priority 1
 Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
 Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   oob-resync timeout 40
   Hello due in 00:00:06
 Supports Link-local Signaling (LLS)
 Cisco NSF helper support enabled
 IETF NSF helper support enabled
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 2
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 2, Adjacent neighbor count is 2
   Adjacent with neighbor 2.2.2.2  (Backup Designated Router)
   Adjacent with neighbor 3.3.3.3  (Designated Router)
 Suppress hello for 0 neighbor(s)
R1#
```

Рис. 5.4.20

R1 є ні DR, ні BDR, а є маршрутизатором DROTHER з пріоритетом за умовчанням 1. (1)

DR - це маршрутизатор R3 з ідентифікатором 3.3.3.3 по IP-адресою 192.168.1.3, а BDR - це маршрутизатор R2 з ідентифікатором 2.2.2.2 по IP-адресою 192.168.1.2. (2)

R1 має два відносини суміжності: одне з BDR, інше з DR. (3)

Вихідні дані, згенеровані маршрутизатором R2 (рис. 3), підтверджують це:

Проверка роли маршрутизатора R2

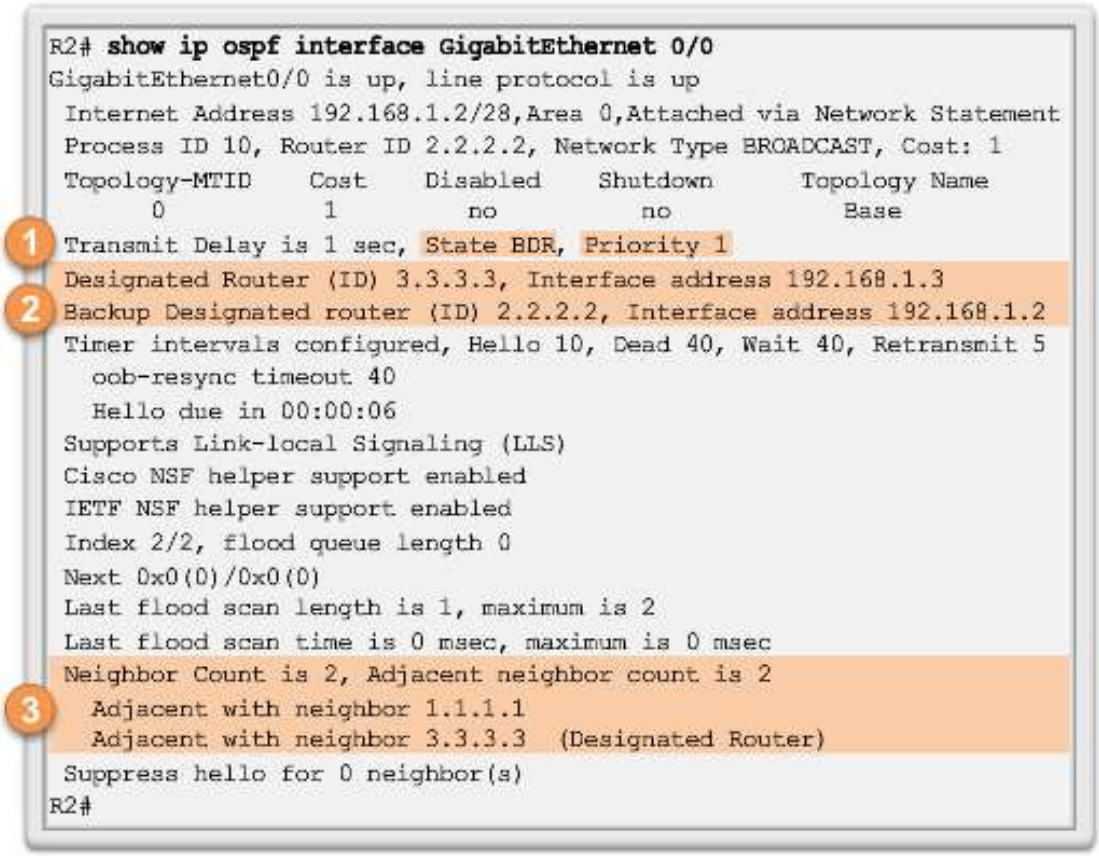


Рис. 5.4.21

R2 - це BDR з пріоритетом за умовчанням 1. (1)

DR - це маршрутизатор R3 з ідентифікатором 3.3.3.3 по IP-адресою 192.168.1.3, а BDR - це маршрутизатор R2 з ідентифікатором 2.2.2.2 по IP-адресою 192.168.1.2. (2)

R2 має два відносини суміжності: одне з сусіднім пристроєм з ідентифікатором 1.1.1.1 (R1), а інше - з DR. (3)

Вихідні дані, згенеровані маршрутизатором R3 (рис. 4), підтверджують це:

Проверка роли маршрутизатора R3

```
R3# show ip ospf interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
 Internet Address 192.168.1.3/28,Area 0,Attached via Network Statement
 Process ID 10, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
 Topology-MTID    Cost    Disabled    Shutdown      Topology Name
       0           1         no          no            Base
1 Transmit Delay is 1 sec, State DR, Priority 1
2 Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 3, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
3   Adjacent with neighbor 1.1.1.1
    Adjacent with neighbor 2.2.2.2  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
R3#
```

Рис. 5.4.22

R3 - це DR з пріоритетом за умовчанням 1. (1)

DR - це маршрутизатор R3 з ідентифікатором 3.3.3.3 по IP-адресою 192.168.1.3, а BDR - це маршрутизатор R2 з ідентифікатором 2.2.2.2 по IP-адресою 192.168.1.2. (2)

Для перевірки відносин суміжності OSPF використовуйте команду show ip ospf neighbor, як показано на рис. 1.

```
R1# show ip ospf neighbor

Neighbor ID Pri State       Dead Time  Address     Interface
1 2.2.2.2     1  FULL/BDR     00:00:36 192.168.1.2 GigabitEthernet0/0
2 3.3.3.3     1  FULL/DR      0:00:35  192.168.1.3 GigabitEthernet0/0

R1#
```

На відміну від послідовних каналів, які відображають тільки стан FULL / -, стан сусідніх пристроїв в мережах з множинним доступом може бути:

- FULL / DROTHER - це маршрутизатор DR або BDR, повністю суміжний з маршрутизатором, який не є DR або BDR. Ці два сусідніх пристрої можуть обмінюватися пакетами вітання (hello), оновленнями, запитами, відповідями і підтвердженнями.
- FULL / DR - маршрутизатор повністю смеж із зазначеним сусіднім маршрутизатором DR. Ці два сусідніх пристрої можуть обмінюватися пакетами вітання (hello), оновленнями, запитами, відповідями і підтвердженнями.

- FULL / BDR - маршрутизатор повністю смеж із зазначеним сусіднім маршрутизатором BDR. Ці два сусідніх пристрої можуть обмінюватися пакетами вітання (hello), оновленнями, запитами, відповідями і підтвердженнями.
- 2-WAY / DROTHER - маршрутизатор, який не є DR або BDR, має сусідські відносини з іншим маршрутизатором, який теж не є DR або BDR. Ці два сусідніх пристрої обмінюються пакетами вітання (hello).

Нормальний стан для маршрутизатора OSPF - FULL. Якщо маршрутизатор тривалий час знаходиться в іншому стані, це означає, що у нього виникли проблеми з формуванням відносин суміжності. Єдиним винятком з цього правила є стан 2-WAY, що нормально для широкомовної мережі з множинним доступом.

У мережах з множинним доступом маршрутизатори DROTHER формують відносини суміжності FULL тільки з маршрутизаторами DR і BDR. Однак маршрутизатори DROTHER як і раніше будуть формувати сусідські відносини суміжності 2-WAY з будь-якими маршрутизаторами DROTHER, які підключаться до мережі. Це означає, що всі маршрутизатори DROTHER в мережі з множинним доступом і раніше отримують пакети вітання (hello) від інших маршрутизаторів DROTHER. Таким чином, вони знають про всі маршрутизаторах в мережі. Коли два маршрутизатора DROTHER формують сусідські відносини суміжності, стан сусіднього пристрою можна побачити як 2-WAY / DROTHER.

Процес вибору DR / BDR за замовчуванням

Як відбувається вибір маршрутизаторів DR і BDR? Вибір ролей DR і BDR по протоколу OSPF грунтується на таких критеріях в зазначеній черговості:

1. Маршрутизатор в мережі вибирають маршрутизатор з найвищим пріоритетом інтерфейсу в якості DR. Маршрутизатор з другим за величиною пріоритетом інтерфейсу стає BDR. Пріоритет може бути представлений будь-яким числом від 0 до 255. Чим вище пріоритет, тим більша ймовірність, що маршрутизатора на екрані телевізора в якості DR. Якщо пріоритет налаштований на значення 0, то маршрутизатор не отримає роль DR. Пріоритет за замовчуванням інтерфейсів, підключених до широкомовної мережі множинного доступу, дорівнює 1. Відповідно, при відсутності інших налаштувань, все маршрутизатори мають рівне пріоритетом, і для виборів DR / BDR буде використовуватися інший метод.

2. Якщо пріоритети інтерфейсів рівні, то в якості DR буде обраний маршрутизатор з найвищим ідентифікатором. Маршрутизатор з другим за величиною ідентифікатором стає BDR.

Як ви пам'ятаєте, ідентифікатор маршрутизатора визначається одним з трьох способів:

- Ідентифікатор маршрутизатора може бути налаштований вручну.
- Якщо ідентифікатор маршрутизатора не налаштований, тоді як ідентифікатор маршрутизатора приймається найвищий IP-адреса інтерфейсу loopback.

- Якщо інтерфейси loopback не налаштовані, то ідентифікатор маршрутизатора визначається за найвищим активному IPv4-адресою.

Примітка. Якщо в мережі IPv6 на маршрутизаторі не налаштовані IPv4-адреси, то ідентифікатор маршрутизатора необхідно налаштувати вручну за допомогою команди router-id rid; в іншому випадку OSPFv3 не починається.

На малюнку всі Ethernet-інтерфейси маршрутизатора мають пріоритет за замовчуванням 1. В результаті, відповідно до вищезазначених критеріями вибору, для вибору DR і BDR використовується ідентифікатор маршрутизатора OSPF. Роль DR приймає маршрутизатор R3, оскільки він має найвищий ідентифікатор. Маршрутизатор R2, який має другий за величиною ідентифікатор, стає BDR.

Справочная топология широковещательной рассылки OSPF множественного доступа

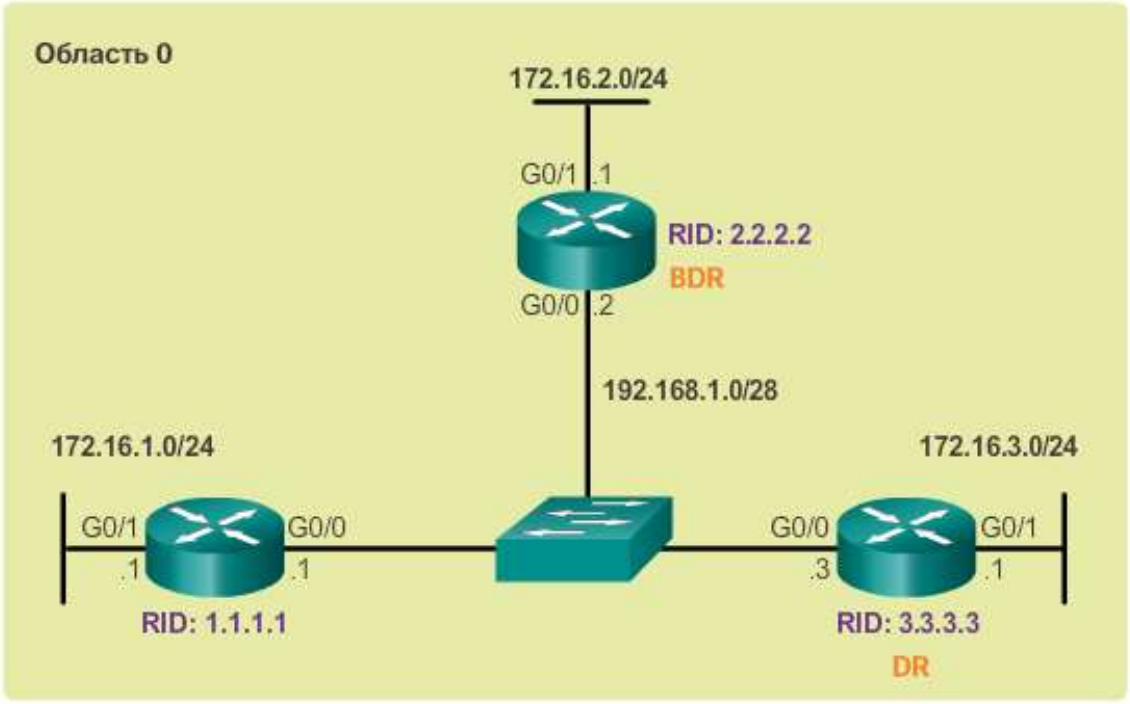


Рис. 5.4.23

Примітка. На послідовних інтерфейсах пріоритет за замовчуванням налаштований на значення 0, тому вони не вибирають DR і BDR.

Процедура вибору DR і BDR починається відразу після появи в мережі з множинним доступом першого активного маршрутизатора з інтерфейсом, де включений OSPF. Це може статися, коли маршрутизатори включені або після виконання на цьому інтерфейсі команди OSPF network. Процедура вибору займає всього кілька секунд. Якщо в мережі з множинним доступом завантажилися не всі маршрутизатори, то роль DR може отримати маршрутизатор ні з найвищим ідентифікатором. (Це може бути більш простий маршрутизатор, завантаження якого займає менше часу.)

Процес вибору DR і BDR по протоколу OSPF не є пріоритетним. Якщо після завершення вибору DR / BDR в мережі з'являється новий маршрутизатор з більш високим пріоритетом або ідентифікатором, то цей новий

маршрутизатор НЕ переймає роль DR або BDR, оскільки ці ролі вже призначені. Додавання нового маршрутизатора не приводить до нового процесу вибору.

Коли який-небудь маршрутизатор обраний як DR, то він зберігає цю роль, поки не відбудеться одна з наступних подій:

- збій DR
- Збій або зупинка OSPF-процесу на DR
- Збій або відключення інтерфейсу з множинним доступом на DR

Якщо відбувається збій DR, то його роль автоматично переймає BDR. Це відбувається навіть у тому випадку, якщо після початкового вибору DR / BDR до мережі додається інший маршрутизатор DROTHER з більш високим ідентифікатором або пріоритетом. Однак коли BDR переймає роль DR, відбувається новий вибір BDR і його роль отримує маршрутизатор DROTHER з високим ідентифікатором або пріоритетом.

DR стає центром для збору і поширення оголошень LSA, тому цей маршрутизатор повинен мати досить потужний ЦП і обсяг пам'яті для обробки робочого навантаження. На процес вибору DR / BDR можна вплинути через певні конфігурації.

Якщо на всіх маршрутизаторах пріоритети інтерфейсів рівні, то в якості DR буде обраний маршрутизатор з найвищим ідентифікатором. Ідентифікатор маршрутизатора можна налаштувати спеціально для маніпуляції вибору DR / BDR. Однак цей процес спрацює лише в тому випадку, якщо на всіх маршрутизаторах існує строгий порядок настройки ідентифікатора. У великих мережах використання даного методу може викликати труднощі.

Замість того щоб покладатися на ідентифікатор маршрутизатора, рекомендується керувати вибором за допомогою настройки пріоритетів інтерфейсів. Пріоритети - це значення для інтерфейсу, виходячи з якого інтерфейс забезпечує поліпшене керування мережею з множинним доступом. Також це дозволяє маршрутизатора виконувати роль DR в одній мережі, і DROTHER - в інший.

Щоб налаштувати пріоритет інтерфейсу, використовуйте наступні команди:

- ip ospf priority value - команда інтерфейсу OSPFv2
- ipv6 ospf priority value - команда інтерфейсу OSPFv3

Це value може бути 0 - маршрутизатор не стає DR або BDR. Від 1 до 255 - чим вище значення пріоритету, тим більша ймовірність, що маршрутизатор стане DR або BDR на даному інтерфейсі.

На малюнку всі маршрутизатори мають однаковий пріоритет OSPF, тому що для всіх інтерфейсів маршрутизатора значення пріоритету за умовчанням встановлено на 1. Тому ідентифікатор маршрутизатора використовується для визначення DR (R3) і BDR (R2). При зміні пріоритету на інтерфейсі з значення 1 на більше значення маршрутизатор стане DR або BDR під час наступного вибору.

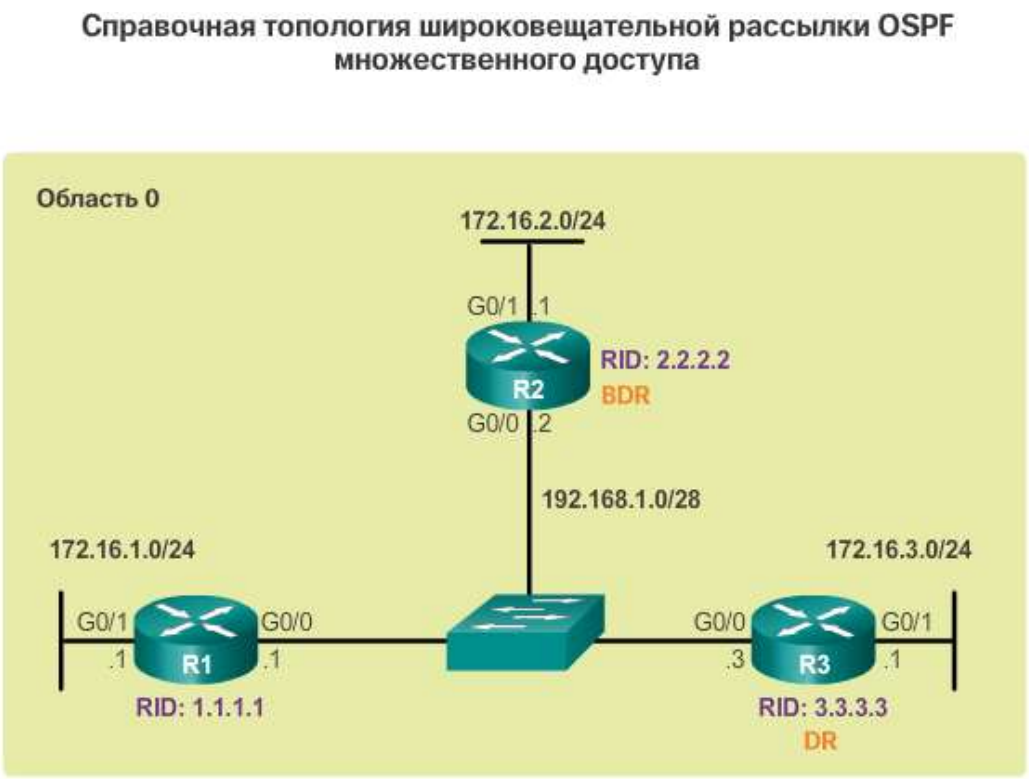


Рис. 5.4.24

Якщо пріоритет інтерфейсу налаштовується після включення OSPF, то адміністратор повинен відключити процес OSPF на всіх маршрутизаторах, а потім повторно включити його, щоб ініціювати новий процес вибору DR / BDR.

Як показано в топології на рис. 1, маршрутизатор R3 є DR, а маршрутизатор R2 - BDR. Вирішено наступне:

Рис. 5.4.25

Маршрутизатор R1 повинен виконувати роль DR і буде налаштований з пріоритетом 255.

Маршрутизатор R2 повинен виконувати роль BDR, і його пріоритет залишиться зі значенням за замовчуванням 1.

Маршрутизатор R3 не повинен виконувати роль DR або BDR і буде налаштований з пріоритетом 0.

На рис. 2 пріоритет інтерфейсу Gigabit 0/0 маршрутизатора R1 змінений з 1 на 255.

Изменение приоритета интерфейса G0/0 маршрутизатора R1

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip ospf priority 255
R1(config-if)# end
R1#
```

Рис. 5.4.26

На рис. 3 пріоритет інтерфейсу Gigabit 0/0 маршрутизатора R3 змінений з 1 на 0.

Изменение приоритета интерфейса G0/0 маршрутизатора R3

```
R3(config)# interface GigabitEthernet 0/0
R3(config-if)# ip ospf priority 0
R3(config-if)# end
R3#
```

Рис. 5.4.27

Ці зміни автоматично не набрали чинності, оскільки DR і BDR вже обрані. Тому вибір OSPF повинен бути узгоджений з допомогою одного з таких способів:

Відключити інтерфейси маршрутизатора і повторно включити їх: спочатку на DR, потім на BDR, а потім на інших маршрутизаторах.

Скинути процес OSPF за допомогою команди привілейованого режиму clear ip ospf process на всіх маршрутизаторах.

На рис. 4 продемонстрований скидання процесу OSPF на маршрутизаторі R1. Припустимо, що команда привілейованого режиму clear ip ospf process теж була виконана на маршрутизаторах R2 і R3. Зверніть увагу на що з'явилися відомості про стан OSPF.

Очистка OSPF-процесса на маршрутизаторе R1

```
R1# clear ip ospf process
Reset ALL OSPF processes? [no]: yes
R1#
*Apr  6 16:00:44.282: %OSPF-5-ADJCHG: Process 10, Nbr
2.2.2.2 on GigabitEthernet0/0 from FULL to DOWN, Neighbor
Down: Interface down or detached
*Apr  6 16:00:44.282: %OSPF-5-ADJCHG: Process 10, Nbr
3.3.3.3 on GigabitEthernet0/0 from FULL to DOWN, Neighbor
Down: Interface down or detached
R1#
```

Рис. 5.4.28

Вихідні дані, які відображаються на рис. 5, підтверджують, що тепер маршрутизатор R1 виконує роль DR з пріоритетом 255 і визначає нові сусідські відносини суміжності маршрутизатора R1.

Проверка роли и отношений смежности маршрутизатора R1

```
R1# show ip ospf interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/28, Area 0, Attached via Network Statement
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1          no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 255
  Designated Router (ID) 1.1.1.1, Interface address 192.168.1.1
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 2.2.2.2  (Backup Designated Router)
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
R1#
R1# show ip ospf neighbor

Neighbor ID  Pri   State      Dead Time Address     Interface
2.2.2.2      1   FULL/BDR     00:00:30  192.168.1.2 GigabitEthernet0/0
3.3.3.3      0   FULL/DROTHER 00:00:38  192.168.1.3 GigabitEthernet0/0
R1#
```

Рис. 5.4.29

Поширення статичного маршруту за замовчуванням

У OSPF маршрутизатор, підключений до Інтернету, використовується для поширення маршруту за замовчуванням на інші маршрутизатори в домені маршрутизації OSPF. Іноді цей маршрутизатор називають граничною, вхідним або мережевим шлюзом. Однак в термінології OSPF маршрутизатор, розташований між доменом маршрутизації OSPF і мережею без OSPF, також називають граничною маршрутизатором автономної системи (ASBR).

На рис. 1 маршрутизатор R2 підключений до одного оператора зв'язку. Тому все, що потрібно маршрутизатора R2 для отримання доступу до Інтернету - це статичний маршрут за замовчуванням до оператора зв'язку.

Распространение маршрута по умолчанию на маршрутизаторе R2

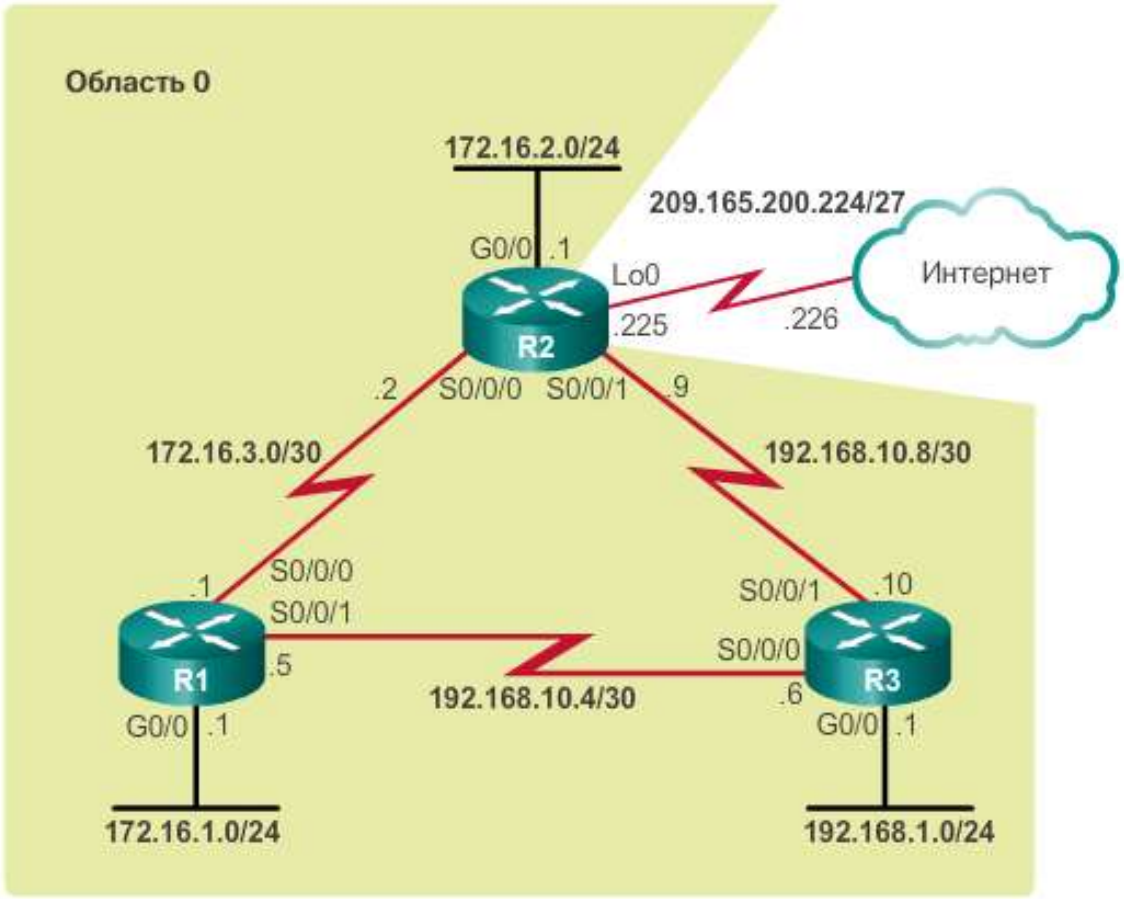


Рис. 5.4.30

Примітка. У цьому прикладі для моделювання підключення до оператора зв'язку використовується інтерфейс loopback з IP-адресою 209.165.200.225.

Для поширення маршруту за замовчуванням на граничному маршрутизаторі (R2) повинні бути налаштовані:

Статичний маршрут за замовчуванням за допомогою команди ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}.

Команда режиму конфігурації маршрутизатора default-information originate. Завдяки цьому параметру маршрутизатор R2 стає джерелом інформації про маршрут за замовчуванням і поширює статичний маршрут за замовчуванням в оновленнях OSPF.

На рис. 2 показаний процес налаштування повністю певного статичного маршруту за замовчуванням до оператора зв'язку.

Настройка маршрута по умолчанию на маршрутизаторе R2

```
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#
R2(config)# router ospf 10
R2(config-router)# default-information originate
R2(config-router)# end
R2#
```

Рис. 5.4.31

Перевірка розповсюджуваного маршруту за замовчуванням

Перевірте налаштування маршруту за замовчуванням на R2 за допомогою команди show ip route, як показано на рис. 1.

Проверка маршрута по умолчанию на маршрутизаторе R2

```
R2# show ip route | begin Gateway

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

S*  0.0.0.0/0 [1/0] via 209.165.200.226, Loopback0
    172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O   172.16.1.0/24 [110/65] via 172.16.3.1, 00:01:44,
    Serial0/0/0
C   172.16.2.0/24 is directly connected, GigabitEthernet0/0
L   172.16.2.1/32 is directly connected, GigabitEthernet0/0
C   172.16.3.0/30 is directly connected, Serial0/0/0
L   172.16.3.2/32 is directly connected, Serial0/0/0
O   192.168.1.0/24 [110/65] via 192.168.10.10, 00:01:12,
    Serial0/0/1
    192.168.10.0/24 is variably subnetted, 3 subnets, 2
     masks
O   192.168.10.4/30 [110/128] via 192.168.10.10, 00:01:12,
    Serial0/0/1
            [110/128] via 172.16.3.1, 00:01:12, Serial0/0/0
C   192.168.10.8/30 is directly connected, Serial0/0/1
L   192.168.10.9/32 is directly connected, Serial0/0/1
    209.165.200.0/24 is variably subnetted, 2 subnets, 2
     masks
C   209.165.200.224/30 is directly connected, Loopback0
L   209.165.200.225/32 is directly connected, Loopback0
R2#
```

Рис. 5.4.32

Процес поширення статичного маршруту за замовчуванням в OSPFv3 мало чим відрізняється від аналогічного процесу в OSPFv2.

На рис. 1 маршрутизатор R2 підключений до одного оператора зв'язку. Тому все, що потрібно маршрутизатора R2 для отримання доступу до Інтернету - це статичний маршрут за замовчуванням до оператора зв'язку.

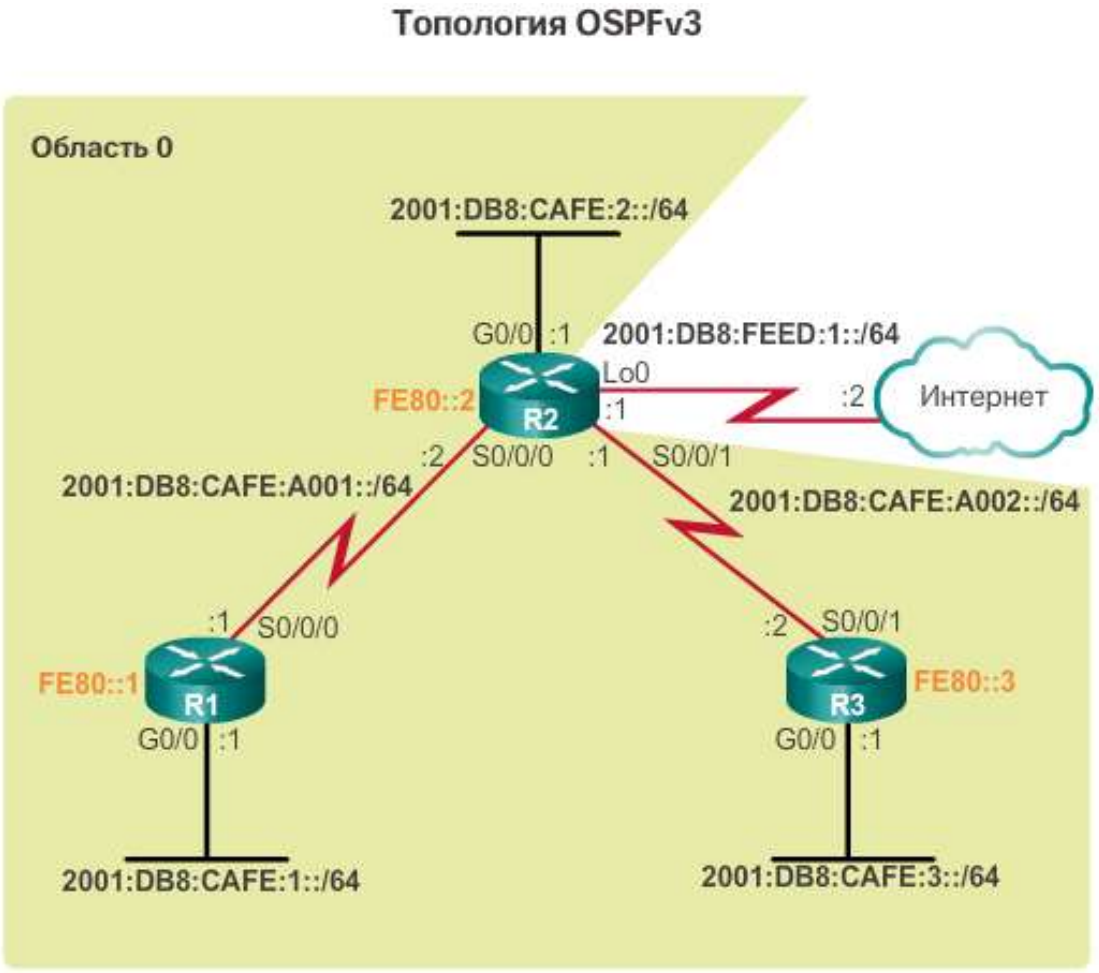


Рис. 5.4.33

Примітка. У цьому прикладі для моделювання підключення до оператора зв'язку використовується інтерфейс loopback з IP-адресою 2001: DB8: FEED: 1 :: 1/64.

На рис. 2 показана поточна таблиця маршрутизації IPv6 маршрутизатора R1. Зверніть увагу, що в ній не містяться відомості про маршрут в Інтернеті.

Проверка таблицы маршрутизации IPv6 на маршрутизаторе R1

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 8 entries
Codes:
  C - Connected, L - Local, S - Static, U - Per-user Static route
  B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
  I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
  EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
   Destination
  NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
  OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:DB8:CAFE:2::/64 [110/648]
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:3::/64 [110/648]
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:A002::/64 [110/1294]
     via FE80::2, Serial0/0/0
R1#
```

Рис. 5.4.34

Для поширення маршруту за замовчуванням на граничному маршрутизаторі (R2) повинні бути налаштовані:

Статичний маршрут за замовчуванням за допомогою команди ipv6 route :: / 0 {ipv6-address | exit-intf}.

Команда режиму конфігурації маршрутизатора default-information originate. Завдяки цьому параметру маршрутизатор R2 стає джерелом інформації про маршрут за замовчуванням і поширює статичний маршрут за замовчуванням в оновленнях OSPF.

На рис. 3 показаний процес налаштування повністю певного статичного маршруту за замовчуванням до оператора зв'язку.

Включение OSPFv3 для интерфейсов на маршрутизаторе R1

```
R2(config)# ipv6 route ::/0 2001:DB8:FEED:1::2
R2(config)#
R2(config)# ipv6 router ospf 10
R2(config-rtr)# default-information originate
R2(config-rtr)# end
R2#
*Apr 10 11:36:21.995: %SYS-5-CONFIG_I: Configured from console by
console
R2#
```

Рис. 5.4.35

Перевірка розповсюджуваного IPv6-маршруту за замовчуванням

Перевірте налаштування маршруту за замовчуванням на R2 за допомогою команди show ipv6 route, як показано на рис. 1.

Проверка маршрута по умолчанию на маршрутизаторе R2

```
R2# show ipv6 route static
IPv6 Routing Table - default - 12 entries
Codes:C -Connected, L - Local, S - Static, U - Per-user Static route
      B -BGP, R - RIP, H - NHRP, I1 - ISIS L1
      I2 -ISIS L2, IA - ISIS interarea, IS-ISIS summary,D-EIGRP
      EX -EIGRP external, ND-ND Default,NDp-ND Prefix,
      DCE-Destination, NDr -Redirect, O - OSPF Intra,OI-OSPF Inter
      OE1-OSPF ext 1, OE2 -OSPF ext 2, ON1 - OSPF NSSA ext 1
      ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via 2001:DB8:FEED:1::2, Loopback0
R2#
```

Рис. 5.4.36

Інтервали вітання (hello) і простою (dead) OSPF налаштовуються для кожного інтерфейсу. Інтервали OSPF повинні збігатися, інакше сусідські відносини суміжності не встановили.

Для перевірки тимчасових інтервалів, сконфигурированних на інтерфейсах, використовуйте команду show ip ospf interface, як показано на рис. 1. Інтервали вітання і простою Serial 0/0/0 за замовчуванням налаштовані на 10 і 40 секунд відповідно.

Проверка интервалов OSPF на маршрутизаторе R1

```
R1# show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 172.16.3.1/30, Area 0, Attached via
Network Statement
  Process ID 10, Router ID 1.1.1.1, Network Type
POINT_TO_POINT, Cost: 64
 Topology-MTID  Cost  Disabled    Shutdown      Topology Name
      0          64      no          no             Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
R1#
```

Рис. 5.4.37

На рис. 2 представлений приклад використання методу фільтрації для відображення інтервалів OSPF для інтерфейсу Serial 0/0/0 по протоколу OSPF на маршрутизаторі R1.

Проверка интервалов OSPF на фильтре маршрутизатора R1

```
R1# show ip ospf interface serial 0/0/0 | include Timer
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
R1#
```

Рис. 5.4.38

На рис. 3 використовується команда show ip ospf neighbor на маршрутизаторі R1 з метою підтвердження, що маршрутизатор R1 смеж з R2 і R3. Зверніть увагу, що у вихідних даних інтервал простою (dead) відраховується від 40 секунд. За замовчуванням це значення оновлюється кожні 10 секунд, коли R1 отримує вітання від сусіднього пристрою.

Проверка активности таймера OSPF

```
R1# show ip ospf neighbor

Neighbor ID  Pri  State    Dead Time  Address       Interface
3.3.3.3      0    FULL/-   00:00:35   192.168.10.6  Serial0/0/1
2.2.2.2      0    FULL/-   00:00:33   172.16.3.2    Serial0/0/0
R1#
```

Рис. 5.4.39

Рекомендується змінювати таймери OSPF, щоб маршрутизатори швидше могли виявити збої в мережі. Це збільшує трафік, але іноді важливіше забезпечити швидку збіжність, ніж економити на трафіку.

Примітка. Інтервали вітання (hello) і простою (dead) за замовчуванням засновані на практичних рекомендаціях і можуть бути змінені лише в крайніх випадках.

Інтервали вітання (hello) і простою (dead) OSPF можна змінити вручну за допомогою наступних команд режиму настройки інтерфейсу:

- ip ospf hello-interval seconds
- ip ospf dead-interval seconds

Щоб відновити значення інтервалів за замовчуванням, використовуйте команди no ip ospf hello-interval і no ip ospf dead-interval.

На рис. 1 представлений процес зміни інтервалу вітання на 5 секунд. Відразу після зміни інтервалу вітання (hello) Cisco IOS автоматично прирівнює інтервал простою (dead) до чотирьох інтервалах вітання. Однак щоб зміни були задокументовані в конфігурації, завжди корисно явно змінити таймер, а не покладатися на автоматичні функції IOS. Тому інтервал простою (dead) також слід налаштувати вручну на послідовному інтерфейсі 0/0/0 маршрутизатора R1 на 20 секунд.

Изменение интервалов OSPF интерфейса Serial 0/0/0 на маршрутизаторе R1

```
R1(config)# interface serial 0/0/0
R1(config-if)# ip ospf hello-interval 5
R1(config-if)# ip ospf dead-interval 20
R1(config-if)# end
R1#
R1#
*Apr  7 17:28:21.529: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2
on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1#
```

Рис. 5.4.40

Як видно в виділеному повідомленні суміжності OSPFv2 на рис. 1, маршрутизатори R1 і R2 втрачають відносини суміжності в момент закінчення таймера простою на R1. Причина в тому, що значення були змінені тільки на одній стороні послідовного каналу між R1 і R2. Як ви пам'ятаєте, інтервали вітання (hello) і простою (dead) OSPF повинні збігатися у обох сусідніх пристроїв.

Для перевірки сусідських відносин суміжності використовуйте команду show ip ospf neighbor на маршрутизаторі R1, як показано на рис. 2. Зверніть увагу, що єдиним сусіднім пристроєм вказано маршрутизатор 3.3.3.3 (R3), а маршрутизатор R1 більше не є суміжним з сусіднім пристроєм 2.2.2.2 (R2). Таймери, налаштовані на інтерфейсі Serial 0/0/0, не впливають на сусідські відносини суміжності з R3.

Проверка отношений смежности OSPF на маршрутизаторе R1

```
R1# show ip ospf neighbor

Neighbor ID  Pri   State   Dead Time  Address      Interface
3.3.3.3      0     FULL/-  00:00:37   192.168.10.6 Serial0/0/1
R1#
```

Рис. 5.4.41

Для відновлення відносини суміжності між маршрутизаторами R1 і R2 інтервал вітання (hello) на інтерфейсі Serial 0/0/0 маршрутизатора R2 встановлюється рівним 5, як показано на рис. 3. Практично миттєво в IOS Пристрій повідомить про те, що були встановлені відносини суміжності в стані FULL.

Изменение интервалов OSPF интерфейса Serial 0/0/0 на маршрутизаторе R2

```
R2(config)# interface serial 0/0/0
R2(config-if)# ip ospf hello-interval 5
R2(config-if)#
*Apr  7 17:41:49.001: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1
on Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)# end
R2#
```

Рис. 5.4.42

Для перевірки тимчасових інтервалів, сконфигурированних на інтерфейсах, використовуйте команду show ip ospf interface, як показано на рис. 4. Зверніть увагу, що час привітання (hello) становить 5 секунд, а час простою (dead) було автоматично налаштовано на 20 секунд замість 40 секунд за

замовчуванням. Пам'ятайте, що OSPF автоматично прирівнює інтервал простою (dead) до чотирьох інтервалах вітання (hello).

Проверка отношений смежности OSPF на маршрутизаторе R2

```
R2# show ip ospf interface s0/0/0 | include Timer
  Timer intervals configured, Hello 5, Dead 20, Wait 20,
Retransmit 5
R2#
R2# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:35    192.168.10.10   Serial0/0/1
1.1.1.1           0   FULL/  -        00:00:17    172.16.3.1      Serial0/0/0
R2#
```

Рис. 5.4.43

Як і у випадку з OSPFv2, інтервали OSPFv3 теж можна змінювати.

Інтервали вітання (hello) і простою (dead) OSPFv3 можна змінити вручну за допомогою наступних команд режиму настройки інтерфейсу:

- ipv6 ospf hello-interval seconds
- ipv6 ospf dead-interval seconds

Примітка. Щоб відновити значення інтервалів за замовчуванням, використовуйте команди no ipv6 ospf hello-interval і no ipv6 ospf dead-interval.

Розглянемо топологію IPv6 на рис.1. Припустимо, мережа зійшлася з використанням протоколу OSPFv3.

Топология OSPFv3

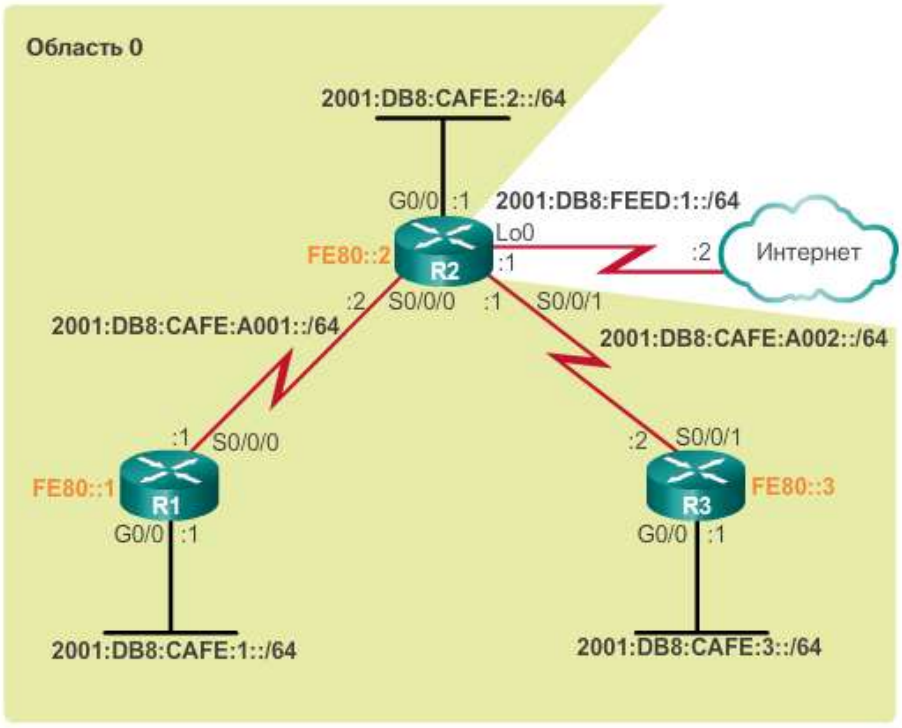


Рис. 5.4.44

У представленому прикладі на рис. 2 для OSPFv3 задається інтервал вітання, рівний 5 секундам. Відразу після зміни інтервалу вітання (hello) Cisco IOS автоматично прирівнює інтервал простою (dead) до чотирьох інтервалах вітання. Однак, як і у випадку з OSPFv2, щоб зміни були задокументовані в конфігурації, завжди корисно явно змінити таймер, а не покладатися на автоматичні функції IOS. Тому інтервал простою (dead) також слід налаштувати вручну на послідовному інтерфейсі 0/0/0 маршрутизатора R1 на 20 секунд.

Изменение интервалов OSPFv3 интерфейса Serial 0/0/0 на маршрутизаторе R1

```
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 ospf hello-interval 5
R1(config-if)# ipv6 ospf dead-interval 20
R1(config-if)# end
R1#
*Apr 10 15:03:51.175: %OSPFv3-5-ADJCHG: Process 10, Nbr
2.2.2.2 on Serial0/0/0 from FULL to DOWN, Neighbor Down:
Dead timer expired
R1#
```

Рис. 5.4.45

Після закінчення таймера простою на R1 маршрутизатори R1 і R2 втрачають відносини суміжності, як це видно в виділеному повідомленні суміжності OSPFv3 на рис. 2, оскільки значення були змінені тільки на одній стороні послідовного каналу між R1 і R2. Як ви пам'ятаєте, інтервали вітання (hello) і простою (dead) OSPFv3 повинні збігатися у сусідніх пристроїв.

Для перевірки сусідських відносин суміжності використовуйте команду show ipv6 ospf neighbor на маршрутизаторі R1, як показано на рис. 3. Зверніть увагу, що R1 більше не стулив з сусіднім маршрутизатором 2.2.2.2 (R2).

Проверка отношений смежности OSPFv3 на маршрутизаторе R1

```
R1# show ipv6 ospf neighbor
R1#
```

Рис. 5.4.46

Для відновлення відносини суміжності між маршрутизаторами R1 і R2 інтервал вітання (hello) на інтерфейсі Serial 0/0/0 маршрутизатора R2 встановлюється рівним 5, як показано на рис. 4. Практично миттєво в IOS Пристрій повідомить про те, що були встановлені відносини суміжності в стані FULL.

Изменение интервалов OSPFv3 интерфейса Serial 0/0/0 на маршрутизаторе R2

```
R2(config)# interface serial 0/0/0
R2(config-if)# ipv6 ospf hello-interval 5
R2(config-if)#
*Apr 10 15:07:28.815: %OSPFv3-5-ADJCHG: Process 10, Nbr
1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)# end
R2#
```

Рис. 5.4.47

Для перевірки тимчасових інтервалів, сконфигурированних на інтерфейсах, використовуйте команду show ipv6 ospf interface, як показано на рис. 5. Зверніть увагу, що час привітання (hello) становить 5 секунд, а час простою (dead) було автоматично налаштовано на 20 секунд замість 40 секунд за замовчуванням. Пам'ятайте, що OSPF автоматично прирівнює інтервал простою (dead) до чотирьох інтервалах вітання (hello).

Проверка отношений смежности OSPFv3 на маршрутизаторе R2

```
R2# show ipv6 ospf interface s0/0/0 | include Timer
  Timer intervals configured, Hello 5, Dead 20, Wait 20,
Retransmit 5
R2#
R2# show ipv6 ospf neighbor

            OSPFv3 Router with ID (2.2.2.2) (Process ID 10)

Neighbor ID  Pri  State   Dead Time   Interface ID  Interface
3.3.3.3        0  FULL/-  00:00:38    7             Serial0/0/1
1.1.1.1        0  FULL/-  00:00:19    6             Serial0/0/0
R2#
```

Рис. 5.4.48

Захист OSP

Маршрутизатор, що виконують певні ролі в мережі, настільки важливі, що часто вони піддаються мережевим атакам. Мережеві адміністратори повинні знати, що маршрутизатори схильні до ризику від атак так само, як і системи кінцевих користувачів.

Системи маршрутизації можуть бути атаковані за допомогою порушення суміжності маршрутизаторів або фальсифікації даних, що передаються протоколом маршрутизації. Сфальсифіковані дані про маршрути можуть бути використані для дезінформації (передача помилкових даних) один одного, організації атаки відмови в обслуговуванні (DoS) або зловмисного зміни шляху трафіку. До наслідків фальсифікації даних про маршрути відносяться:

- перенаправлення трафіку для створення петель маршрутизації;

- перенаправлення трафіку з метою його прочитання на незахищеному каналі;
- перенаправлення трафіку з метою його видалення.

Зловмиснику вдалося підключитися безпосередньо до каналу між маршрутизаторами R1 і R2. Зловмисник вводить неправдиві дані про маршрути, призначені тільки для маршрутизатора R1. У цих даних вказано, що R2 є кращим пунктом призначення для вузлового маршруту 192.168.10.10/32. Хоча в таблиці маршрутизації R1 міститься запис для мережі з прямим підключенням 192.168.10.0/24, маршрутизатор додає підроблений маршрут в свою таблицю маршрутизації через довшою маски підмережі. Маршрут з довшою збігається маскою підмережі вважається краще маршруту з коротшою маскою. Отже, коли маршрутизатор отримує пакет, він вибирає більш довгу маску підмережі, оскільки це більш точний маршрут до пункту призначення.

Краткий обзор процесса аутентификации протоколов маршрутизации

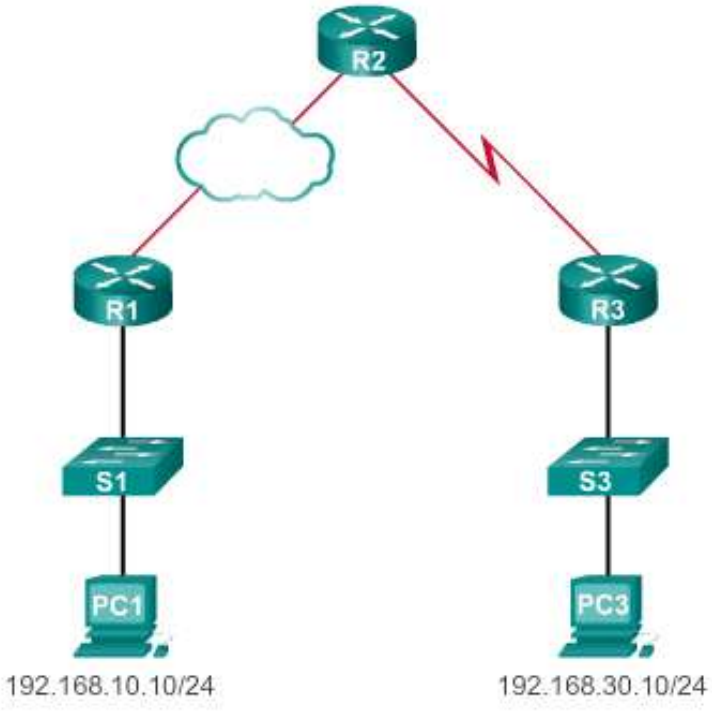


Рис. 5.4.49

Коли PC3 відправляє пакет на PC1 (192.168.10.10/24), маршрутизатор R1 не надсилає пакет на вузол PC1. Замість цього він направляє пакет на маршрутизатор R2, оскільки оптимальний шлях до 192.168.10.10/32 лежить через маршрутизатор R2. Коли маршрутизатор R2 отримує пакет, він звертається до таблиці маршрутизації і пересилає пакет назад на R1, через що виникає петля.

Щоб протистояти атакам протоколу маршрутизації, налаштуйте аутентифікацію OSPF.

Безпека оновлень маршрутів

Коли на маршрутизаторі налаштована аутентифікація сусідніх пристроїв, маршрутизатор перевіряє джерело кожного одержуваного пакету оновлень маршрутів. Ця аутентифікація реалізується шляхом обміну ключа

аутентифікації (який також називають паролем), відомого маршрутизатора-відправнику і маршрутизатора-одержувачу.

Щоб обмінюватися відомостями про відновлення маршрутизації в захищеному режимі, включите аутентифікацію OSPF. Аутентифікація OSPF може бути відсутньою (або нульовий), простий або за стандартом Message Digest 5 (MD5).

OSPF підтримує три типи аутентифікації. Нульова (Null) - це спосіб за замовчуванням, який означає, що аутентифікація для OSPF не використовується. Проста аутентифікація по паролю - також її називають аутентификацией на базі відкритого ключа, оскільки пароль в оновленні відправляється по мережі у вигляді звичайного тексту. Цей спосіб аутентифікації OSPF вважається застарілим. Аутентифікація MD5 - найбільш безпечний і рекомендований спосіб аутентифікації. Аутентифікація MD5 гарантує більш високий рівень безпеки, рівноправні вузли не обмінюються паролями. Замість цього він обчислюється за алгоритмом MD5. Відправника аутентифицируют збігаються результати.

Примітка. Різні форми аутентифікації MD5 підтримуються протоколами RIPv2, EIGRP, OSPF, IS-IS і BGP.

OSPFv3 (OSPF для IPv6) не володіє власними можливостями аутентифікації. Замість цього для захисту передачі даних між сусідніми пристроями він повністю покладається на IPsec за допомогою команди режиму конфігурації інтерфейсу ipv6 ospf authentication ipsec spi. Це сприяє спрощенню протоколу OSPFv3 і стандартизації його механізмів аутентифікації.

Налаштування аутентифікації OSPF MD5

OSPF підтримує аутентифікацію протоколу маршрутизації за допомогою MD5. Аутентифікацію MD5 можна включити глобально для всіх або для окремих інтерфейсів.

Щоб включити аутентифікацію MD5 OSPF глобально, виконайте наступні настройки:

- ip ospf message-digest-key ключ md5 пароль Команда режиму конфігурації інтерфейсу.
- area area-id authentication message-digest команда режиму конфігурації маршрутизатора.

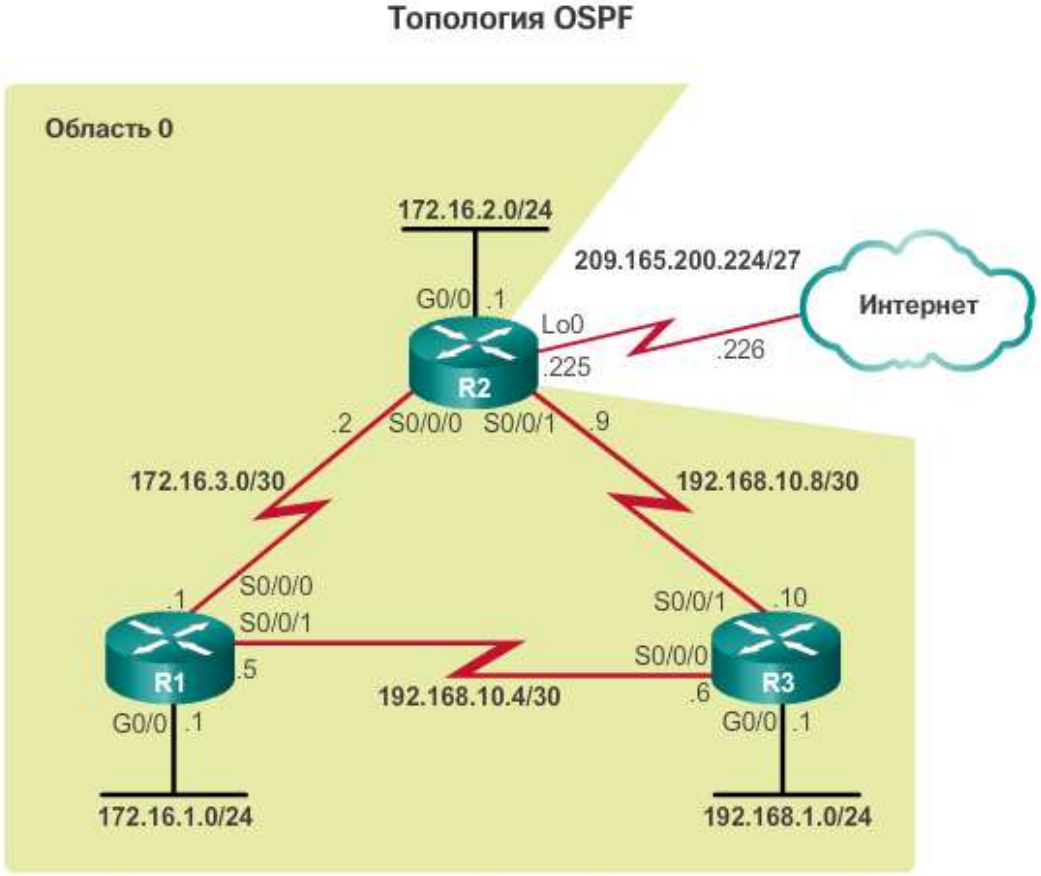
Цей метод забезпечує аутентифікацію на всіх інтерфейсах з підтримкою OSPF. Якщо на інтерфейсі не виконано команда ip ospf message-digest-key, то цей інтерфейс не зможе сформувати відносини суміжності з іншими сусідніми пристроями OSPF.

Тепер з метою підвищення гнучкості аутентифікацію можна налаштувати на інтерфейсах окремо. Щоб включити аутентифікацію MD5 на окремих інтерфейсах, налаштуйте наступне:

- ip ospf message-digest-key ключ md5 пароль команда режиму конфігурації інтерфейсу.
- ip ospf authentication message-digest команда режиму конфігурації інтерфейсу.

На одному і тому ж маршрутизаторі аутентифікація OSPF MD5 може використовуватися як глобально, так і окремо. Однак налаштування на інтерфейсі анулюють всі налаштування, виконані в глобальному режимі. Використовувані паролі аутентифікації MD5 в одній області можуть бути різними. Однак вони повинні збігатися між сусідніми пристроями.

Наприклад, припустимо, що всі маршрутизатори на малюнку зійшлися з використанням OSPF і маршрутизація проходить нормально. Аутентифікація OSPF буде реалізована на всіх маршрутизаторах.



Приклад аутентифікації OSPF MD5

На рис. 1 показаний приклад налаштування аутентифікації MD5 по протоколу OSPF на маршрутизаторі R1 на всіх інтерфейсах. Зверніть увагу, що інформаційні повідомлення, що відображають зміну статусу суміжних відносин OSPF з маршрутизаторами R2 і R3, змінилися на Down (Викл.), Оскільки R2 і R3 ще не налаштовані для підтримки аутентифікації MD5.

Глобальное включение аутентификации OSPF по алгоритму MD5 на маршрутизаторе R1

```
R1(config)# router ospf 10
R1(config-router)# area 0 authentication message-digest
R1(config-router)# exit
R1(config)#
*Apr  8 09:58:09.899: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2
on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1(config)#
*Apr  8 09:58:28.627: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3
on Serial0/0/1 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/1
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)#
```

Рис. 5.4.50

В якості альтернативи глобальної аутентифікації MD5 на рис. 2 показаний приклад налаштування маршрутизатора R1 для включення аутентифікації MD5 по протоколу OSPF для окремих інтерфейсів. І знову зверніть увагу, як стан сусідських відносин суміжності по протоколу OSPF змінилося на Down (Викл.).

Включение аутентификации OSPF по алгоритму MD5 на интерфейсах маршрутизатора R1

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/1
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# exit
R1(config)#
*Apr  8 10:20:10.647: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2
on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1(config)#
*Apr  8 10:20:50.007: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3
on Serial0/0/1 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1(config)#
```

Рис. 5.4.51

Щоб переконатися, що аутентифікація MD5 по протоколу OSPF включена, використовуйте команду привілейованого режиму show ip ospf interface. Щоб підтвердити успішне встановлення аутентифікації, слід перевірити таблиці маршрутизації.

На рис. 1 показана перевірка аутентифікації MD5 OSPF на послідовному інтерфейсі 0/0/0 на маршрутизаторі R1.

Проверка параметров аутентификации OSPF MD5 на маршрутизаторе R1

```
R1# show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 172.16.3.1/30, Area 0, Attached via
Network Statement
  Process ID 10, Router ID 1.1.1.1, Network Type
POINT_TO_POINT, Cost: 64
Topology-MTID   Cost  Disabled  Shutdown      Topology Name
      0          64      no        no             Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 5, Dead 20, Wait 20,
Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
```

Рис. 5.4.52

На рис. 2 відображається успішна перевірка аутентифікації.

Проверка таблицы маршрутизации R1

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP,
       M - mobile, B - BGP, D - EIGRP,
       EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1
       E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
       L2 - IS-IS level-2, ia - IS-IS inter area,
       * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
       H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:33:17, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O        172.16.2.0/24 [110/65] via 172.16.3.2, 00:33:17, Serial0/0/0
O     192.168.1.0/24 [110/65] via 192.168.10.6, 00:30:43, Serial0/0/1
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
O        192.168.10.8/30 [110/128] via 192.168.10.6, 00:30:43, Serial0/0/1
                         [110/128] via 172.16.3.2, 00:33:17, Serial0/0/0
R1#
```

Рис. 5.4.53

Протокол маршрутизації OSPF є одним з найбільш поширених протоколів маршрутизації, які використовуються в великих корпоративних мережах. Пошук і усунення неполадок, пов'язаних з обміном інформацією про маршрути, є одним з найважливіших навичок для мережевого фахівця, який займається реалізацією і підтримкою великих маршрутизованих корпоративних мереж, в яких протокол OSPF використовується в якості протоколу внутрішнього шлюзу.

Для пошуку та усунення неполадок в роботі OSPF важливо розуміти, як маршрутизатори OSPF переходять в різні стани OSPF під час встановлення відносин суміжності.

На малюнку представлені стану OSPF і короткий огляд функцій кожного стану.

Переход между состояниями OSPF

Рис. 5.4.54

При пошуку і усунення неполадок в роботі сусідніх пристроїв OSPF пам'ятайте, що нормальні стану - це FULL або 2WAY. Всі інші стани є тимчасовими, тобто маршрутизатор не повинен перебувати в цих станах занадто довго.

У процесі пошуку і усунення неполадок можна використовувати багато різних команд OSPF. Нижче представлені найбільш поширені з цих команд:

show ip protocols (Рис. 1) - використовується для перевірки найважливіших відомостей конфігурації OSPF, серед яких ідентифікатор процесу OSPF, ідентифікатор маршрутизатора, анонсуються маршрутизатором мережі, сусідні пристрої, від яких маршрутизатор приймає оновлення, і значення адміністративної дистанції за замовчуванням, рівне 110 для OSPF .

Проверка параметров OSPF маршрутизатора R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.1 0.0.0.0 area 0
    172.16.3.1 0.0.0.0 area 0
    192.168.10.5 0.0.0.0 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:08:35
    2.2.2.2              110      00:08:35
  Distance: (default is 110)

R1#
```

Рис. 5.4.55

show ip ospf neighbor (Рис. 2) - команда використовується для того, щоб переконатися, що маршрутизатор сформував відносини суміжності з сусідніми маршрутизаторами. Відображає ідентифікатор сусіднього маршрутизатора, пріоритет, стан OSPF, таймер простою (dead), IP-адреса інтерфейсу сусіднього пристрою, а також інтерфейсу, через який є це сусіднє пристрій. Якщо ідентифікатор сусіднього маршрутизатора не відображається або не вказує стан FULL або 2WAY, це означає, що обидва маршрутизатора не створили відносини суміжності OSPF. Якщо два маршрутизатора не встановлюють відносини суміжності, обмін інформацією про стан каналу буде неможливий. Неповні бази даних станів каналів можуть привести до помилок в деревах SPF і

таблицях маршрутизації. Маршрути до мереж призначення можуть бути відсутніми або не бути оптимальними шляхами.

Проверка отношений смежности OSPF на маршрутизаторе R1

```
R1# show ip ospf neighbor

Neighbor ID Pri State        Dead Time Address     Interface
2.2.2.2       1 FULL/BDR     00:00:30  192.168.1.2 GigabitEthernet0/0
3.3.3.3       0 FULL/DROTHER 00:00:38  192.168.1.3 GigabitEthernet0/0
R1#
```

Рис. 5.4.56

show ip ospf interface (Рис. 3) - використовується для відображення параметрів OSPF, налаштованих на інтерфейсі, наприклад ідентифікатор процесу OSPF, якому призначений інтерфейс, область, в якому знаходяться інтерфейси, вартість інтерфейсу і інтервали вітання (hello) і простою (dead). Щоб відобразити вихідні дані для певного інтерфейсу, слід додати до команди ім'я і номер інтерфейсу.

Проверка параметров OSPF интерфейса S0/0/0 на маршрутизаторе R1

```
R1# show ip ospf interface Serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 172.16.3.1/30, Area 0, Attached via Network
Statement
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT,
Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
R1#
```

Рис. 5.4.57

show ip ospf (Рис. 4) - використовується для перегляду ідентифікатора процесу OSPF і маршрутизатора. Крім того, дана команда відображає дані про область OSPF і показує час, коли останній раз виконувався алгоритм пошуку найкоротшого шляху SPF.

Отображение параметров OSPF

```
R1# show ip ospf
Routing Process "ospf 10" with ID 1.1.1.1
 Start time: 00:02:19.116, Time elapsed: 00:01:00.796
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Supports NSSA (compatible with RFC 3101)
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 1. Checksum Sum 0x00A1FF
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
```

Рис. 5.4.58

show ip route ospf (Рис. 5) - використовується тільки для відображення отриманих маршрутів OSPF в таблиці маршрутизації. Вихідні дані вказують, що маршрутизатор R1 дізнався близько чотирьох віддалених мереж через OSPF.

Проверка маршрутов OSPF в таблице маршрутизации на R1

```
R1# show ip route ospf
Codes:L - local,C - connected,S - static,R - RIP,M - mobile,B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS,su - IS-IS summary,L1 - IS-IS level-1,L2-IS-IS level-2
      ia - IS-IS inter area,*-candidate default,U-per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      + - replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:33:17, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O       172.16.2.0/24 [110/65] via 172.16.3.2, 00:33:17,Serial0/0/0
O     192.168.1.0/24 [110/65] via 192.168.10.6, 00:30:43,Serial0/0/1
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
O       192.168.10.8/30[110/128] via 192.168.10.6,00:30:43,Serial0/0/1
                        [110/128] via 172.16.3.2,00:33:17,Serial0/0/0
R1#
```

Рис. 5.4.59

clear ip ospf [process-id] process - використовується для скидання сусідських відносин суміжності OSPFv2.

Складові процедури пошуку та усунення неполадок в роботі OSPF

Як показано на малюнку, проблеми OSPF зазвичай пов'язані з:

- відносинами суміжності з сусідніми пристроями;
- відсутніми маршрутами;
- вибором шляху.

При пошуку і усунення неполадок з сусідніми пристроями переконайтеся, що маршрутизатор встановив відносини суміжності з сусідніми маршрутизаторами, використовуючи команду show ip ospf neighbors. Якщо відносини суміжності не встановлені, то маршрутизатори не зможуть обмінятися маршрутами. Переконайтеся, що інтерфейси функціонують і працюють по протоколу OSPF, використовуючи команди show ip interface brief і show ip ospf interface. Якщо інтерфейси функціонують і працюють по протоколу OSPF, переконайтеся, що інтерфейси на обох маршрутизаторах налаштовані для однієї і тієї ж області OSPF, а інтерфейси не налаштовані як пасивних.

Якщо між двома маршрутизаторами встановлені відносини суміжності, переконайтеся, що маршрути OSPF містяться в таблиці маршрутизації, використовуючи команду show ip route ospf. Якщо маршрути OSPF не містяться в таблицях, переконайтеся, що в мережі не працюють інші протоколи маршрутизації з меншими адміністративними дистанціями. Переконайтеся, що всі необхідні мережі оголошені в OSPF. Також перевірте, чи налаштований на маршрутизаторі список доступу, який фільтрує вхідні або вихідні відновлення маршрутизації.

Якщо в таблиці маршрутизації знаходяться всі необхідні маршрути, але трафік слід по неправильному шляху, перевірте вартість OSPF на інтерфейсах шляхом. Також слід дотримуватися обережності у випадках, коли швидкість інтерфейсів перевищує 100 Мбіт / с, оскільки всі інтерфейси з більш високою пропускною здатністю мають одну і ту ж вартість OSPF за замовчуванням.

Рис. 5.4.60

У цьому прикладі ретельно розглядається процес пошуку і усунення неполадок, пов'язаних з встановленням сусідства. У топології на рис. 1 все маршрутизатори налаштовані для підтримки маршрутизації OSPF.

Топология OSPF

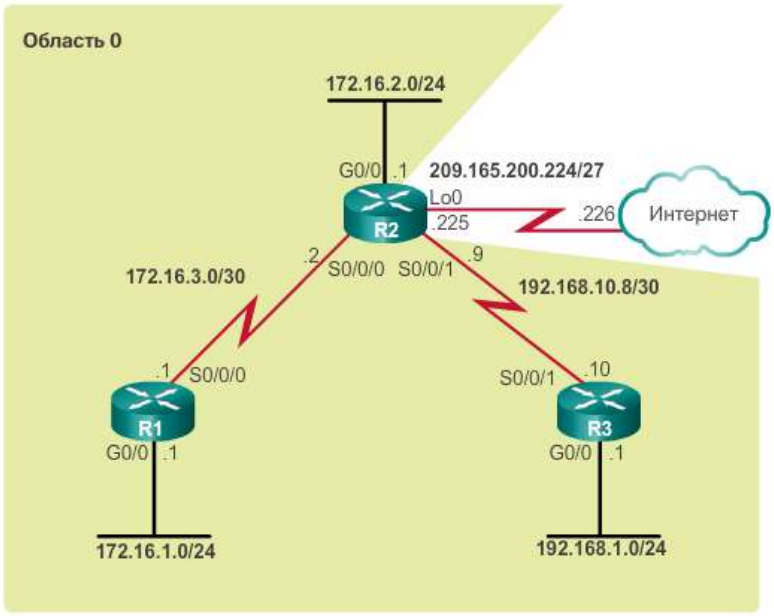


Рис. 5.4.61

Як показано на рис. 2, одного погляду на таблицю маршрутизації R1 досить, щоб зрозуміти, що цей маршрутизатор Не додає маршрути OSPF. Тому може бути кілька причин. Однак обов'язковою умовою для встановлення відносин сусідства між двома маршрутизаторами є наявність підключення 3-го рівня по моделі OSI.

Проверка маршрутов OSPF в таблице маршрутизации R1

```
R1# show ip route
Codes: L -  local, C - connected, S - static, R - RIP, M -
            mobile, B - BGP
       D -  EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
            inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
            external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i -  IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
            L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U -
            per-user static route
       o -  ODR, P - periodic downloaded static route, H -
            NHRP, l - LISP
       + -  replicated route, % - next hop override

Gateway of last resort is not set

   172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C    172.16.1.0/24 is directly connected, GigabitEthernet0/0
L    172.16.1.1/32 is directly connected, GigabitEthernet0/0
C    172.16.3.0/30 is directly connected, Serial0/0/0
L    172.16.3.1/32 is directly connected, Serial0/0/0
R1#
```

Рис. 5.4.62

Вихідні дані на рис. 3 підтверджують, що інтерфейс S0 / 0/0 включений і активний. Успішне луна-тестування також підтверджує, що послідовний інтерфейс маршрутизатора R2 активний. Успішна відправка луна-запиту не означає безумовне формування відносин суміжності, оскільки існує ймовірність виникнення пересічних підмереж. Вам як і раніше необхідно переконатися в тому, що інтерфейси на підключених пристроях використовують одну і ту ж підмережа. Якщо луна-запит був відправлений невдало, перевірте кабелі та переконайтеся, що інтерфейси на підключених пристроях встановлені правильно і справно працюють.

Проверка подключения 3-го уровня к маршрутизатору R2

```
R1# show ip interface brief
Interface                  IP-Address      OK?  Method  Status
Embedded-Service-Engine0/0 unassigned      YES  unset   administr
GigabitEthernet0/0         172.16.1.1      YES  manual  up
GigabitEthernet0/1         unassigned      YES  unset   administr
Serial0/0/0                172.16.3.1      YES  manual  up
Serial0/0/1                unassigned      YES  TFTP    up
R1#
R1# ping 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seco
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/
R1#
```

Рис. 5.4.63

Щоб на інтерфейсі працював OSPF, необхідно в режимі конфігурації процесу маршрутизації OSPF виконати відповідну команду network. Активні інтерфейси OSPF можна перевірити за допомогою команди show ip ospf interface. Вихідні дані на рис. 4 підтверджують, що інтерфейс S0 / 0/0 включений для OSPF. Відносини суміжності не будуть сформовані, якщо на відповідних інтерфейсах двох маршрутизаторів не налаштований OSPF.

Проверка, включен ли протокол OSPF на интерфейсе Serial 0/0/0 маршрутизатора R1

```
R1# show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 172.16.3.1/30, Area 0, Attached via
  Network Statement
  Process ID 10, Router ID 1.1.1.1, Network Type
  POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost  Disabled  Shutdown  Topology Name
        0           64     no          no       Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 5, Dead 20, Wait 20,
  Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Рис. 5.4.64

Перевірте настройки OSPF за допомогою команди show ip protocols. Вихідні дані на рис. 5 підтверджують, що протокол OSPF включений, а після застосування команди network містять список оголошуються мереж. Якщо IP-адреса інтерфейсу входить в мережу, налаштовану в OSPF, то інтерфейс буде включений для OSPF.

Проверка параметров OSPF маршрутизатора R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.1 0.0.0.0 area 0
    172.16.3.1 0.0.0.0 area 0
  Passive Interface(s):
    GigabitEthernet0/0
    Serial0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:50:03
    2.2.2.2              110      04:27:25
  Distance: (default is 110)

R1#
```

Рис. 5.4.65

Однак зверніть увагу, що інтерфейс Serial 0/0/0 відображається як пасивного. Як ви пам'ятаєте, команда passive-interface припиняє як вихідні, так і вхідні відновлення маршрутизації, в результаті виконання цієї команди маршрутизатор перестає відправляти і отримувати пакети вітання (hello) через інтерфейс. Тому маршрутизатори не зможуть стати сусідніми пристроями.

Щоб змінити стан інтерфейсу, використовуйте команду режиму конфігурації маршрутизатора no passive-interface, як показано на рис. 6. Після відключення пасивного інтерфейсу маршрутизатори стануть суміжними, про що ви дізнаєтеся з автоматичного повідомлення.

Отключение пассивного интерфейса на интерфейсе S0/0/0 маршрутизатора R1

```
R1(config)# router ospf 10
R1(config-router)# no passive-interface s0/0/0
R1(config-router)#
*Apr  9 13:14:15.454: %OSPF-5-ADJCHG: Process 10, Nbr
2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done
R1(config-router)# end
R1#
```

Рис. 5.4.66

Швидка перевірка таблиці маршрутизації, як показано на рис. 7, підтверджує, що тепер OSPF обмінюється відомостями про маршрутах.

Проверка маршрутов OSPF в таблице маршрутизации R1

```
R1# show ip route ospf
Codes: L -  local, C - connected, S - static, R - RIP, M -
            mobile, B - BGP
       D -  EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
            inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
            external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i -  IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
            L2 -IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U -
            per-user static route
       o -  ODR, P - periodic downloaded static route, H -
            NHRP, l - LISP
       + -  replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:00:18,
Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
masks
O      172.16.2.0/24 [110/65] via 172.16.3.2, 00:00:18,
       Serial0/0/0
```

Рис. 5.4.67

Інша проблема може виникнути, коли на підключених інтерфейсах двох сусідніх маршрутизаторів не збігаються максимальні розміри переданого блоку

даних (MTU). Максимальний розмір переданого блоку даних - це найбільший пакет мережевого рівня, що пересилається маршрутизатором з кожного інтерфейсу. Розмір MTU за замовчуванням становить 1500 байт. Однак це значення можна змінити для пакетів IPv4 за допомогою команди конфігурації інтерфейсу ip mtu sizeілі команди інтерфейсу ipv6 mtu sizedля пакетів IPv6. Якщо розміри MTU на двох підключених маршрутизаторах не збігаються, то вони все одно спробують сформувати відносини суміжності, але не зможуть обмінятися своїми LSDB (база даних станів каналів), через що відносини сусідства не утворюються.

У топології на рис. 1 все маршрутизатори налаштовані для підтримки маршрутизації OSPF.

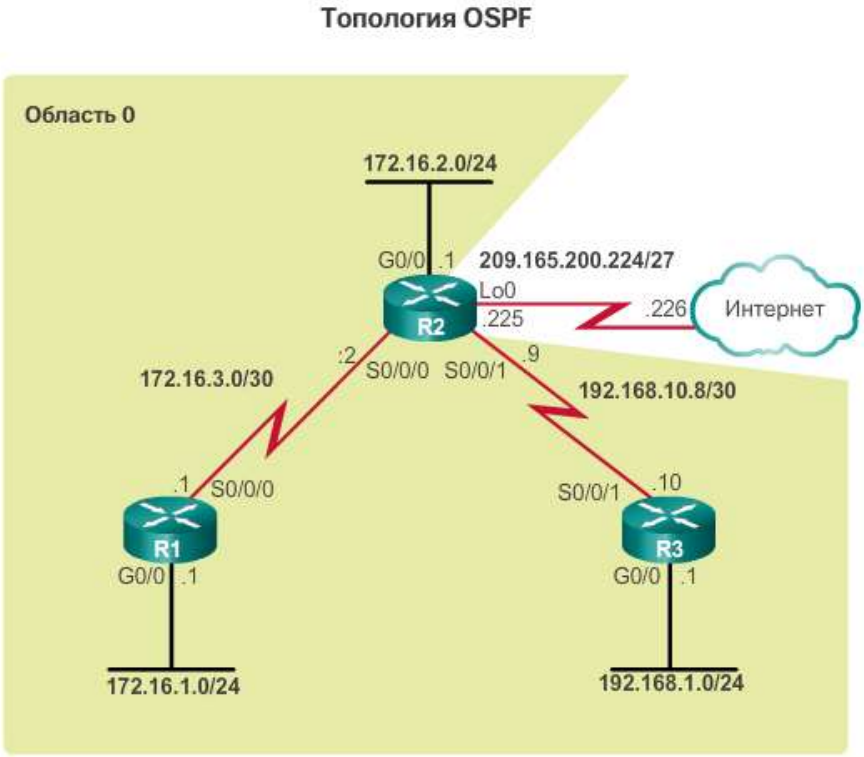


Рис. 5.4.68

Поглянувши на таблицю маршрутизації R1 (рис. 2), можна дізнатися, що він отримує відомості про маршрутизації за замовчуванням, локальну мережу маршрутизатора R2 (172.16.2.0/24) і канал між маршрутизаторами R2 і R3 (192.168.10.8/30). Однак він не отримав маршрут локальної мережі OSPF маршрутизатора R3.

Проверка маршрутов OSPF в таблице маршрутизации R1

```
R1# show ip route
Codes: L -  local, C - connected, S - static, R - RIP, M -
            mobile, B - BGP
       D -  EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
            inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
            external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i -  IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
            L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U -
            per-user static route
       o -  ODR, P - periodic downloaded static route, H -
            NHRP, l - LISP
       + -  replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:05:26,
      Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
      masks
C        172.16.1.0/24 is directly connected,
         GigabitEthernet0/0
```

Рис. 5.4.69

У вихідних даних на рис. 3 представлені налаштування параметрів OSPF на маршрутизаторі R3. Зверніть увагу, що R3 оголошує тільки канал між маршрутизаторами R2 і R3. Він не оголошує локальну мережу маршрутизатора R3 (192.168.1.0/24).

Проверка параметров OSPF маршрутизатора R3

```
R3# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0
  nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.8 0.0.0.3 area 0
  Passive Interface(s):
    Embedded-Service-Engine0/0
    GigabitEthernet0/0
    GigabitEthernet0/1
    GigabitEthernet0/3
    RG-AR-IF-INPUT1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:02:48
    2.2.2.2              110      00:02:48
  Distance: (default is 110)

R3#
```

Рис. 5.4.70

Щоб на інтерфейсі працював OSPF, необхідно в режимі конфігурації процесу маршрутизації OSPF виконати відповідну команду network. У вихідних даних на рис. 4 підтверджується, що локальна мережа маршрутизатора R3 не оголосить по OSPF.

Проверка конфигурации маршрутизатора OSPF на R3

```
R3# show running-config | section router ospf
router ospf 10
 router-id 3.3.3.3
 passive-interface default
 no passive-interface Serial0/0/1
 network 192.168.10.8 0.0.0.3 area 0
R3#
```

Рис. 5.4.71

У прикладі на рис. 5 додана команда network для локальної мережі маршрутизатора R3. Маршрутизатор R3 не повинен оголошувати свою локальну мережу сусідам OSPF.

Объявление локальной сети маршрутизатора R3 в OSPF

```
R3# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# router ospf 10
R3(config-router)# network 192.168.1.0 0.0.0.255 area 0
R3(config-router)# end
R3#
*Apr 10 11:03:11.115: %SYS-5-CONFIG_I: Configured from
console by console
R3#
```

Рис. 5.4.72

У вихідних даних на рис. 6 відображається локальна мережа маршрутизатора R3 в таблиці маршрутизації R1.

Проверка маршрутов OSPF в таблице маршрутизации R1

```
R1# show ip route ospf
Codes: L -  local, C - connected, S - static, R - RIP, M -
            mobile, B - BGP
       D -  EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
            inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
            external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i -  IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
            L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U -
            per-user static route
       o -  ODR, P - periodic downloaded static route, H -
            NHRP, l - LISP
       + -  replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:08:38,
      Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
      masks
O        172.16.2.0/24 [110/65] via 172.16.3.2, 00:08:38,
         Serial0/0/0
```

Рис. 5.4.73

Топологія OSPFv3 представлена на рис. 1.

Топология OSPFv3

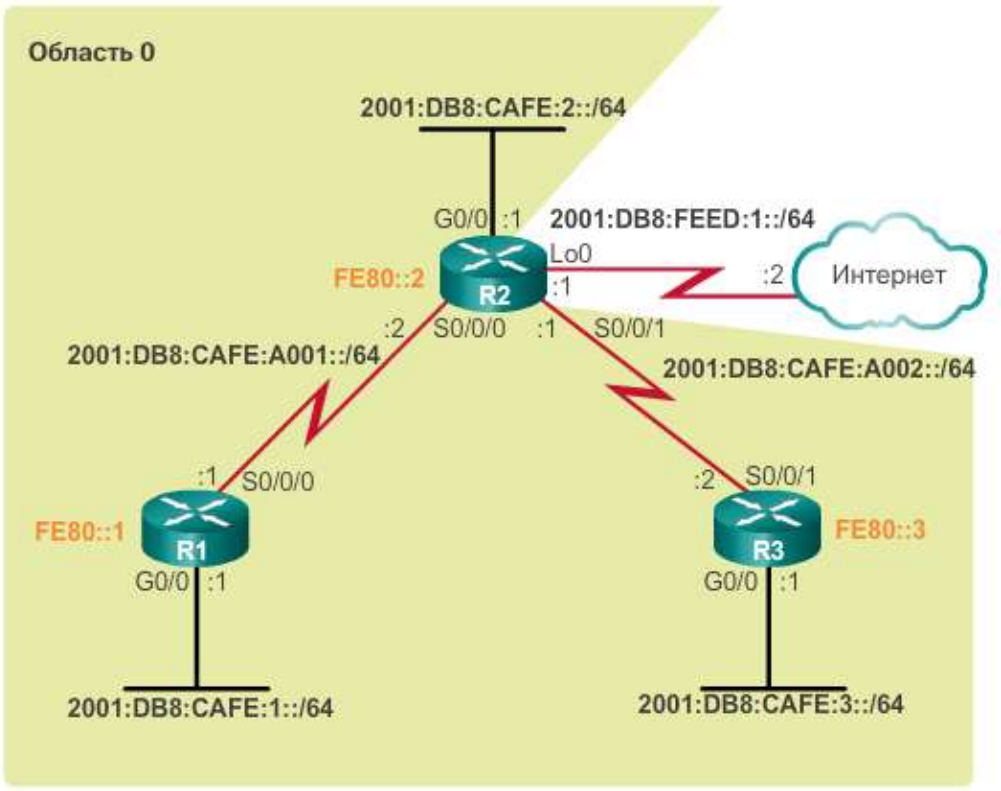


Рис. 5.4.74

Пошук і усунення неполадок в OSPFv3 мало чим відрізняється від аналогічного процесу в OSPFv2. Тому багато команд і способи усунення неполадок для OSPFv2 діють і для OSPFv3.

Наприклад, такі команди використовуються у випадку з OSPFv3:

show ipv6 protocols (Рис. 2) - ця команда використовується для перевірки найважливіших даних конфігурації OSPFv3, включаючи ідентифікатор процесу OSPFv3, ідентифікатор маршрутизатора і інтерфейси, від яких маршрутизатор отримує оновлення.

Проверка параметров OSPFv3 маршрутизатора R1

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/0
    GigabitEthernet0/0
  Redistribution:
    None
R1#
```

Рис. 5.4.75

show ipv6 ospf neighbor (Рис. 3) - команда використовується для того, щоб переконатися, що маршрутизатор сформував відносини суміжності з сусідніми маршрутизаторами. У цих вихідних даних можна побачити ідентифікатор сусіднього маршрутизатора, пріоритет сусіднього пристрою, стан OSPFv3, таймер простою (dead), ідентифікатор сусіднього інтерфейсу, а також інтерфейс, через який є це сусіднє пристрій. Якщо ідентифікатор сусіднього маршрутизатора не відображається або не вказує стан FULL або 2WAY, це означає, що обидва маршрутизатора не створили відносини суміжності OSPFv3. Якщо два маршрутизатора не встановлюють відносини суміжності, обмін інформацією про стан каналу буде неможливий. Неповні бази даних станів каналів можуть привести до помилок в деревах SPF і таблицях маршрутизації. Зазначені маршрути до мереж призначення можуть бути відсутніми або не бути оптимальними шляхами.

Проверка отношений смежности OSPFv3 на маршрутизаторе R1

```
R1# show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           0   FULL/-          00:00:33           7        Serial0/0/0
R1#
```

Рис. 5.4.76

show ipv6 ospf interface (Рис. 4) - використовується для відображення параметрів OSPFv3, налаштованих на інтерфейсі, наприклад ідентифікатор процесу OSPFv3, якому призначений інтерфейс, область, в якому знаходяться інтерфейси, вартість інтерфейсу і інтервали вітання (hello) і простою (dead). Щоб відобразити вихідні дані для певного інтерфейсу, слід додати до команди ім'я і номер інтерфейсу.

Отображение параметров OSPFv3

```
R1# show ipv6 ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::1, Interface ID 6
  Area 0, Process ID 10, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT_TO_POINT, Cost: 647
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:08
  Graceful restart helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 6
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
R1#
```

Рис. 5.4.77

show ipv6 ospf (Рис. 5) - використовується для перегляду ідентифікатора процесу OSPF і ідентифікатора маршрутизатора, а також інформації про передачах LSA.

Проверка параметров OSPFv3 интерфейса S0/0/0 на маршрутизаторе R1

```
R1# show ipv6 ospf
 Routing Process "ospfv3 10" with ID 1.1.1.1
 Event-log enabled, Maximum number of events: 1000, Mode:
cyclic
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 1. Checksum Sum 0x0017E9
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 1000 mbps
 RFC1583 compatibility enabled
    Area BACKBONE(0)
Number of interfaces in this area is 2
SPF algorithm executed 8 times
Number of LSA 13. Checksum Sum 0x063D5D
Number of DCbitless LSA 0
Number of indication LSA 0
```

Рис. 5.4.78

show ipv6 route ospf (Рис. 6) - використовується тільки для відображення отриманих маршрутів OSPFv3 в таблиці маршрутизації. Вихідні дані вказують, що маршрутизатор R1 дізнався близько чотирьох віддалених мереж через OSPFv3.

Проверка маршрутов OSPFv3 в таблице маршрутизации на R1

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static route
       B -   BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 -  ISIS L2, IA - ISIS interarea, IS - ISIS
             summary, D - EIGRP
       EX -  EIGRP external, ND - ND Default, NDp - ND
             Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1
             - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF
             NSSA ext 2
OE2 ::/0 [110/1], tag 10
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:2::/64 [110/648]
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:3::/64 [110/648]
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:A002::/64 [110/1294]
     via FE80::2, Serial0/0/0
R1#
```

Рис. 5.4.79

clear ipv6 ospf [process-id] process - використовується для скидання сусідських відносин суміжності OSPFv3.

Пошук і усунення неполадок в таблиці маршрутизації OSPF

У топології на рис. 1 все маршрутизатори налаштовані для підтримки маршрутизації OSPF.

Топология OSPFv3

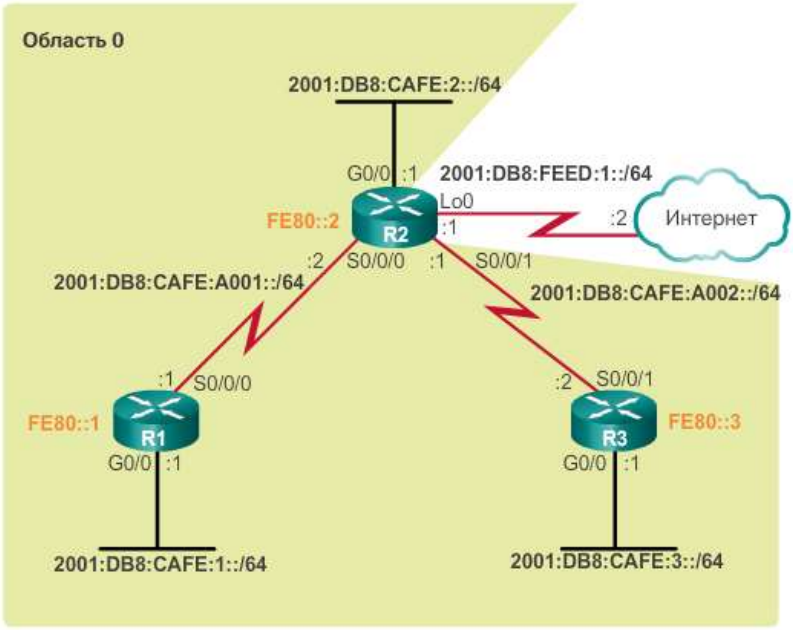


Рис. 5.4.80

Поглянувши на таблицю маршрутизації R1 (рис. 2), можна дізнатися, що він отримує відомості про маршрутизації за замовчуванням, локальну мережу маршрутизатора R2 (172.16.2.0/24) і канал між маршрутизаторами R2 і R3 (192.168.10.8/30). Однак він не отримав маршрут локальної мережі OSPF маршрутизатора R3.

Проверка маршрутов OSPFv3 в таблице маршрутизации R1

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
           Static route
       B -   BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 -  ISIS L2, IA - ISIS interarea, IS - ISIS summary,
             D - EIGRP
       EX -  EIGRP external, ND - ND Default, NDp - ND
             Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1
             - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF
             NSSA ext 2
OE2 ::/0 [110/1], tag 10
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:2::/64 [110/648]
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:A002::/64 [110/1294]
     via FE80::2, Serial0/0/0
R1#
```

Рис. 5.4.81

У вихідних даних на рис. 3 представлені налаштування параметрів OSPF на маршрутизаторі R3. Зверніть увагу, що R3 оголошує тільки канал між маршрутизаторами R2 і R3. Він не оголошує локальну мережу маршрутизатора R3 (192.168.1.0/24).

Проверка параметров OSPFv3 маршрутизатора R3

```
R3# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 3.3.3.3
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/1
  Redistribution:
    None
R3#
```

Рис. 5.4.82

Щоб на інтерфейсі працював OSPF, необхідно в режимі конфігурації процесу маршрутизації OSPF виконати відповідну команду network. У вихідних даних на рис. 4 підтверджується, що локальна мережа маршрутизатора R3 не оголосить по OSPF.

Проверка конфигурации маршрутизатора OSPFv3 на R3

```
R3# show running-config interface g0/0
Building configuration...

Current configuration : 196 bytes
!
interface GigabitEthernet0/0
 description R3 LAN
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::3 link-local
 ipv6 address 2001:DB8:CAFE:3::1/64
end

R3#
```

Рис. 5.4.83

У прикладі на рис. 5 додана команда network для локальної мережі маршрутизатора R3. Маршрутизатор R3 не повинен оголошувати свою локальну мережу сусідам OSPF.

Включение OSPFv3 в локальной сети маршрутизатора R3

```
R3# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# interface g0/0
R3(config-if)# ipv6 ospf 10 area 0
R3(config-if)# end
R3#
```

Рис. 5.4.84

У вихідних даних на рис. 6 відображається локальна мережа маршрутизатора R3 в таблиці маршрутизації R1.

Проверка маршрутов OSPFv3 в таблице маршрутизации R1

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static route
       B -  BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D
            - EIGRP
       EX -  EIGRP external, ND - ND Default, NDp - ND Prefix,
            DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 -
            OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF
            NSSA ext 2
OE2 ::/0 [110/1], tag 10
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:2::/64 [110/648]
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:3::/64 [110/1295]
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:A002::/64 [110/1294]
     via FE80::2, Serial0/0/0
R1#
```

Рис. 5.4.85

Мережі з множинним доступом можуть спричинити за собою дві складності, пов'язані з лавинної розсилкою оголошень LSA: створення множинних відносин суміжності і надлишкова розсилка LSA. Проблему управління великою кількістю відносин суміжності і лавинної розсилкою оголошень LSA в мережі з множинним доступом вирішується за рахунок виділеного і резервного виділеного маршрутизаторів (DR і BDR). Якщо DR перестає створювати пакети вітання (hello), то BDR самостійно приймає роль DR.

Маршрутизатор в мережі вибирають маршрутизатор з найвищим пріоритетом інтерфейсу в якості DR. Маршрутизатор з другим за величиною пріоритетом інтерфейсу стає BDR. Чим вище пріоритет, тим більша ймовірність, що маршрутизатора на екрані телевізора в якості DR. Якщо пріоритет налаштований на значення 0, то маршрутизатор не отримає роль DR. Пріоритет за замовчуванням інтерфейсів, підключених до широкомовної мережі множинного доступу, дорівнює 1. Відповідно, при відсутності інших налаштувань, все маршрутизатори мають рівне пріоритетом, і для виборів DR / BDR буде використовуватися інший метод. Якщо пріоритети інтерфейсів рівні, то в якості DR буде обраний маршрутизатор з найвищим ідентифікатором. Маршрутизатор з другим за величиною ідентифікатором стає BDR. Додавання нового маршрутизатора не приводить до нового процесу вибору.

Щоб поширити маршрут за замовчуванням в OSPF, на маршрутизаторі необхідно налаштувати статичний маршрут за замовчуванням і додати команду default-information originate в конфігурацію. Перевірте маршрути за допомогою команди show ip route або show ipv6 route.

Щоб протокол OSPF правильно визначив шлях, необхідно змінити еталонну пропускну здатність, задавши більш високе значення з урахуванням мереж, що містять канали, швидкість яких вище 100 Мбіт / с. Для настройки еталонної пропускної здатності використовуйте команду режиму конфігурації маршрутизатора auto-cost reference-bandwidth Mbps. Для того щоб налаштувати пропускну здатність інтерфейсу, використовуйте команду режиму конфігурації інтерфейсу bandwidth kilobits. Вартість можна налаштувати на інтерфейсі вручну за допомогою команди режиму конфігурації інтерфейсу ip ospf cost value.

Інтервали вітання (hello) і простою (dead) OSPF повинні збігатися, інакше сусідські відносини суміжності не встановили. Щоб змінити ці інтервали, використовуйте наступні команди інтерфейсу:

- ip ospf hello-interval seconds
- ip ospf dead-interval seconds
- ipv6 ospf hello-interval seconds
- ipv6 ospf dead-interval seconds

OSPF підтримує три типи аутентифікації: нульову, просту аутентифікацію за паролем і аутентифікацію за алгоритмом MD5. Аутентифікацію OSPF MD5 можна налаштувати на інтерфейсах глобально або на окремих інтерфейсах. Щоб переконатися, що реалізація MD5 по протоколу OSPF включена, використовуйте команду привілейованого режиму show ip ospf interface.

При пошуку і усунення неполадок в роботі сусідніх пристроїв OSPF пам'ятайте, що нормальні стану - це FULL або 2WAY. Для пошуку та усунення неполадок в роботі OSPF IPv4 потрібні наступні команди:

- show ip protocols
- show ip ospf neighbor
- show ip ospf interface
- show ip ospf
- show ip route ospf
- clear ip ospf [process-id] process

Пошук і усунення неполадок в роботі OSPFv3 мало чим відрізняється від аналогічної процедури для OSPFv2. Тут представлені команди, еквівалентні тим, що використовуються з OSPFv3: show ipv6 protocols, show ipv6 ospf neighbor, show ipv6 ospf interface, show ipv6 ospf, show ipv6 route ospf, а також clear ipv6 ospf [process-id] process.

5.5 Використання протоколу OSPF для декількох областей

OSPF для декількох областей використовується для поділу мережі OSPF великого розміру. При збільшенні кількості маршрутизаторів в одній області збільшується навантаження на ЦП і відбувається створення великої бази даних станів каналів. Цей розділ містить інструкції щодо того, як можна ефективно розділити одну велику область на кілька областей. Область 0, використовувана в OSPF для однієї області, називається магістральної областю.

У розділі докладно розглядаються пакети LSA передача даних між областями. Крім того, ця глава містить інтерактивні завдання для настройки OSPFv2 і OSPFv3. На завершення розділу наводяться команди show, що використовуються для перевірки конфігурацій OSPF.

Використання OSPF для однієї області є доцільним в невеликих мережах з нескладною системою каналів маршрутизаторів і легко визначаються маршрутами до окремих вузлів призначення.

Але якщо область стає занадто великою, необхідно приділити увагу таким проблемам (див. рис.):

Рис. 5.5.1

Велика таблиця маршрутизації - OSPF не виконує об'єднання маршрутів за замовчуванням. Якщо об'єднання маршрутів не здійснюється, таблиця маршрутизації може стати дуже великий залежно від розміру мережі.

Велика база даних станів каналів (LSDB) - оскільки LSDB охоплює топологію всієї мережі, кожен маршрутизатор повинен підтримувати запис для кожної мережі в області, навіть якщо не всі маршрути обрані для таблиці маршрутизації.

Часті розрахунки алгоритму SPF - у великій мережі неминучі зміни, тому маршрутизатори витрачають багато циклів ЦП на перерахунок алгоритму SPF і оновлення таблиці маршрутизації.

Щоб підвищити ефективність і масштабованість OSPF, протокол OSPF підтримує ієрархічну маршрутизацію за допомогою областей. Область OSPF - це група маршрутизаторів, спільно використовують в своїх базах даних станів каналів однакові дані про стан каналів.

OSPF для декількох областей

Поділ великий області OSPF на області меншого розміру називається OSPF для декількох областей. Використання OSPF для декількох областей є доцільним в мережах більшого розміру, оскільки це дозволяє скоротити споживання ресурсів ЦП і пам'яті.

Наприклад, кожен раз, коли маршрутизатор отримує нові дані про топології, такі як додавання, видалення або зміна каналу, маршрутизатор повинен повторно виконати алгоритм SPF, створити нове дерево SPF і оновити таблицю маршрутизації. Алгоритм SPF вимагає значних ресурсів ЦП, і час, необхідний для виконання відповідних розрахунків, залежить від розміру області. Занадто велика кількість маршрутизаторів в одній області збільшують розмір бази даних LSDB і навантаження на ЦП. Отже, поділ маршрутизаторів на області дозволяє ефективно розділити одну базу даних потенційно великого розміру на кілька баз даних меншого розміру, якими згодом легше управляти.

У разі OSPF для декількох областей потрібно ієрархічна структура мережі. Головна область називається магістральної областю (областю 0), а всі інші області повинні підключатися до магістральної області. При ієрархічної організації маршрутизація продовжує здійснюватися між областями (це називається міжобласний маршрутизацією), при цьому багато рутинних операцій маршрутизації, наприклад повторний розрахунок бази даних, виконуються всередині області.

Як показано на рис. 1, ієрархічна топологія OSPF для декількох областей забезпечує наступні переваги:

Таблиці маршрутизації меншого розміру. Число записів в таблиці маршрутизації зменшується, так як адреси мереж в області можуть бути об'єднані. Наприклад, маршрутизатор R1 може об'єднати маршрути з області 1 в область 0, а маршрутизатор R2 - маршрути з області 51 в область 0. Маршрутизатор R1 і R2 також поширюють статичний маршрут за замовчуванням в область 1 і область 51.

Зниження накладних витрат на оновлення станів каналів. Через зменшення кількості маршрутизаторів, які обмінюються пакетами LSA, знижуються вимоги до обробки даних і пам'яті.

Зниження частоти розрахунків найкоротшого шляху SPF. Вплив змін топології локалізується в межах області. Наприклад, це мінімізує вплив оновлень маршрутизації, так як лавинна розсилка пакетів LSA припиняється на кордоні області.

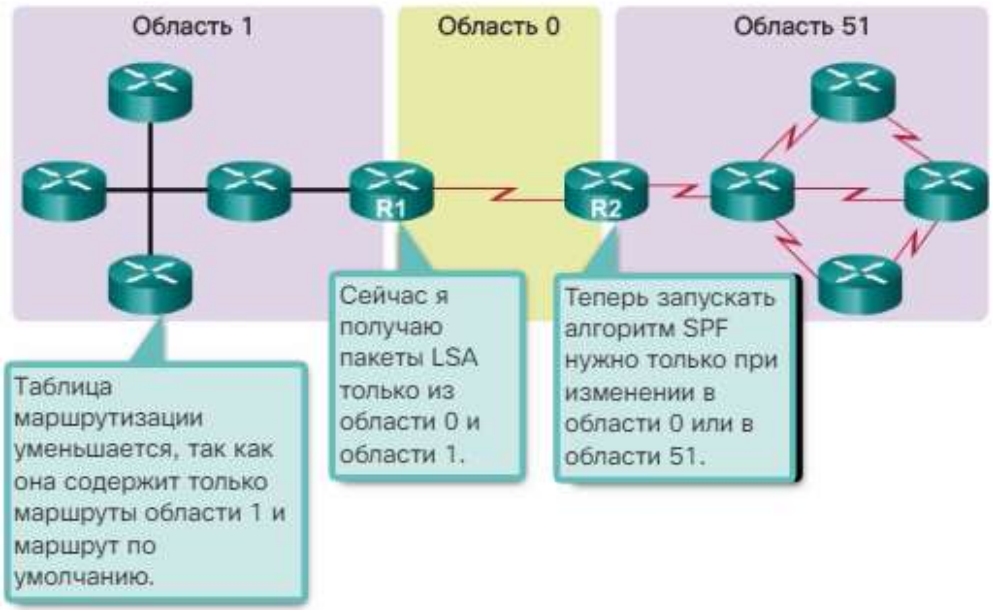


Рис. 5.5.2

Припустимо, відмовив канал між двома внутрішніми маршрутизаторами в області 51 (див. рис. 2).

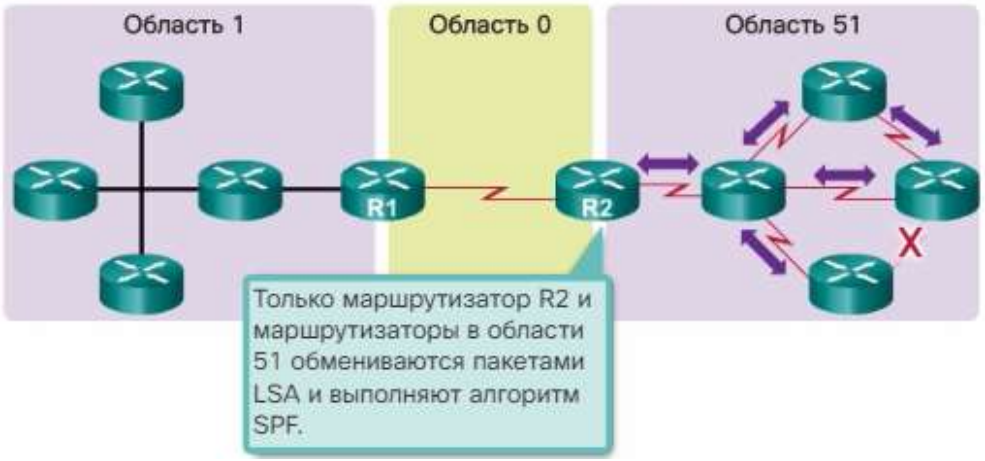


Рис. 5.5.3

У цьому випадку тільки маршрутизатори в області 51 виконають обмін пакетами LSA і заново вирахують найкоротший шлях по алгоритму SPF. Маршрутизатор R1 не отримує пакети LSA з області 51 і не виконує перерахунок за алгоритмом SPF.

Дворівнева ієрархія областей OSPF

OSPF для декількох областей реалізований у вигляді дворівневої ієрархії областей:

Магістральна (транзитна) область - область OSPF, основною функцією якої є швидке і ефективне переміщення IP-пакетів. Магістральні області з'єднують

інші типи областей OSPF. Зазвичай в магістральної області кінцеві користувачі відсутні. Магістральна область також називається нульовою областю OSPF. В ієрархічній мережі нульова область визначається як ядра, до якого безпосередньо підключені всі інші області. (Рис. 1)

Рис. 5.5.4

Звичайна (немагістральних) область - область, яка забезпечує зв'язок для користувачів і ресурсів. Звичайні області, як правило, створюються на основі функціонального або географічного групування. За замовчуванням звичайна область забороняє передачу трафіку від однієї області до іншої по свої каналах. Весь трафік з інших областей повинен проходити через транзитну область. (Рис. 2)

Рис. 5.5.5

Примітка. Можливо кілька підтипів звичайних областей, в тому числі стандартна область, тупикова область, повністю закрита область і не повністю закрита область (not-so-stubby area, NSSA). Тупикова, повністю закрита і не повністю закрита області в цьому розділі не розглядаються.

OSPF реалізує надійну дворівневу ієрархію областей. Використовувана фізична структура мережі повинна встановлювати відповідність з дворівневою структурою областей, причому всі немагістральних області повинні бути безпосередньо підключені до області 0. Весь трафік, який передається з однієї області в іншу, повинен проходити через магістральну область. Подібний трафік називається міжобласним.

Оптимальне число маршрутизаторів в області залежить від багатьох факторів, таких як стійкість мережі, однак Cisco рекомендує дотримуватися таких умов:

Область не повинна містити більше 50 маршрутизаторів.

Маршрутизатор не повинен знаходитися більш ніж в 3 областях.

Число сусідніх маршрутизаторів для будь-якого окремого маршрутизатора не повинно перевищувати 60.

Тема 6.1.2 Принцип роботи пакетів LSA в OSPF для декількох областей

Типи пакетів LSA протоколу OSPF

Пакети LSA - це структурні елементи бази даних станів каналів (LSDB) протоколу OSPF. Окремо вони використовуються як записи бази даних і містять відомості про конкретну мережі OSPF, в той час як в сукупності вони описують всю топологію мережі або області OSPF.

Документи RFC для OSPF в даний час визначають до 11 різних типів LSA (рис. 1). Однак будь-яка реалізація OSPF для декількох областей повинна підтримувати перші п'ять типів LSA: від LSA 1 до LSA 5 (рис. 2). У цьому розділі основна увага приділяється першим п'яти типам LSA.

Типы пакетов LSA протокола OSPF

Тип LSA	Описание
1	LSA маршрутизатора
2	LSA сети
3 и 4	Суммарные LSA
5	Внешний пакет LSA для автономной системы
6	LSA протокола OSPF для групповой рассылки
7	Определённый для областей NSSA
8	LSA внешних атрибутов для протокола BGP
9, 10 или 11	Непрозрачные пакеты LSA

Рис. 5.5.6

Наиболее распространённые типы пакетов LSA протокола OSPF

Тип LSA	Описание
1	LSA маршрутизатора
2	LSA сети
3 и 4	Суммарные LSA
5	Внешний пакет LSA для автономной системы
6	LSA протокола OSPF для групповой рассылки
7	Определённый для областей NSSA
8	LSA внешних атрибутов для протокола BGP
9, 10 или 11	Непрозрачные пакеты LSA

Рис. 5.5.7

Кожен канал маршрутизатора визначається як тип LSA. Пакет LSA містить поле ідентифікатора каналу, який визначає номер мережі і маску об'єкта, з яким з'єднаний канал. Залежно від типу ідентифікатор каналу приймає різні значення. Пакети LSA відрізняються за способом їх створення і поширення в домені маршрутизації.

Примітка. У OSPFv3 підтримуються додаткові типи LSA.

OSPF LSA типу 1

Як показано на малюнку, всі маршрутизатори за допомогою пакетів LSA типу 1 оголошують свої безпосередньо підключені канали підтримують роботу OSPF, пересилаючи мережеву інформацію суміжних сусідам по OSPF. Пакет LSA містить список безпосередньо підключених інтерфейсів, типи каналів і стану каналів.

Распространение сообщений LSA типа 1

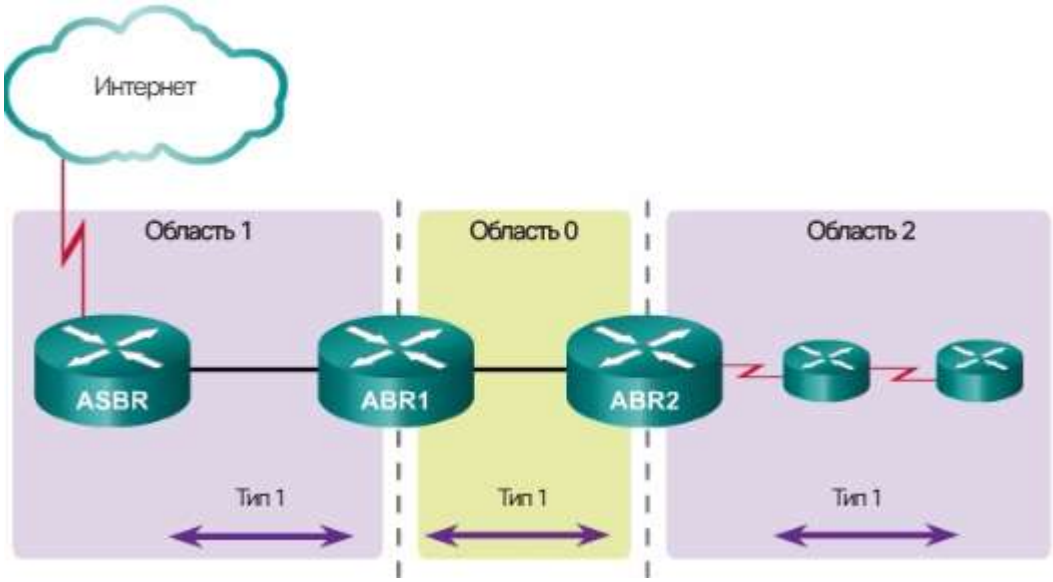


Рис. 5.5.8

Пакети LSA типу 1 також називаються записами про стан каналів маршрутизатора.

Пакети LSA типу 1 розсилаються тільки всередині області, в якій вони були створені. Потім маршрутизатори ABR оголошує мережі, дані про яких

отримані з пакетів LSA типу 1, для інших областей, використовуючи пакети LSA типу 3.

Ідентифікатор каналу пакета LSA типу 1 визначається ідентифікатором вихідного маршрутизатора.

OSPF LSA типу 2

Пакети LSA типу 2 використовуються тільки в нешироковещательнимі мережах з множинним доступом (NBMA), де здійснюється вибір маршрутизаторів DR і мінімальна кількість маршрутизаторів в сегменті множинного доступу дорівнює двом. Пакети LSA типу 2 містять ідентифікатор маршрутизатора і IP-адреса маршрутизатора DR, а також ідентифікатори всіх інших маршрутизаторів в сегменті множинного доступу. Пакет LSA типу 2 створюється для кожної мережі з множинним доступом в області.

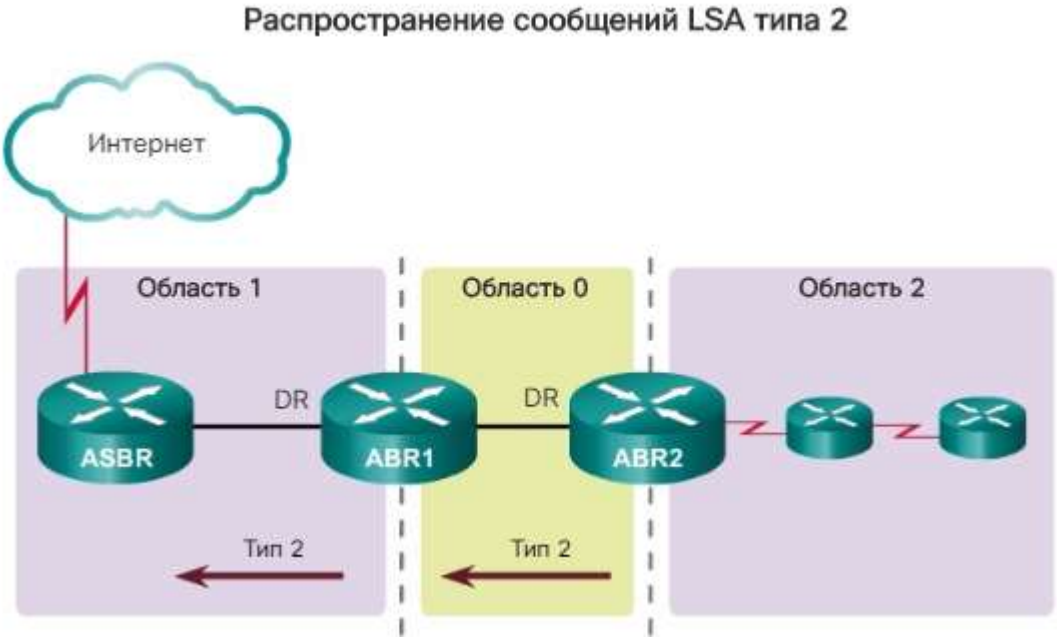


Рис. 5.5.9

Призначення пакетів LSA типу 2 - надання іншим маршрутизаторів інформації про мережах з множинним доступом у відповідній області.

DR розсилає пакети LSA типу 2 тільки всередині області, в якій вони були створені. Пакети LSA типу 2 цієї статті не пересилаються за межі області.

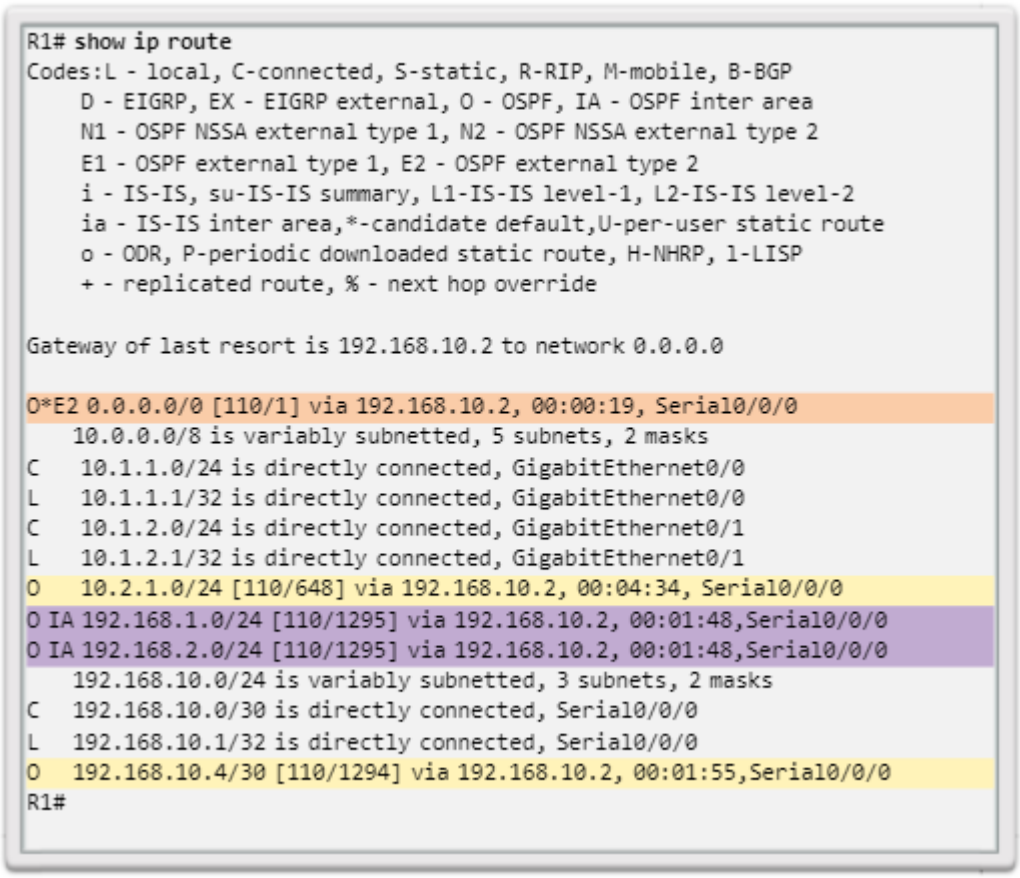
Пакети LSA типу 2 також називаються записами про стан каналів мережі.

Як показано на малюнку, маршрутизатор ABR1 є маршрутизатором DR для мережі Ethernet в області 1. Він створює пакет LSA типу 2 і пересилає його в область 1. Маршрутизатор ABR2 - це DR для мережі з множинним доступом в області 0. В області 2 немає мереж з множинним доступом, тому в цій області не передаються пакети LSA типу 2.

Ідентифікатор стану каналу для пакета LSA мережі - це IP-адреса інтерфейсу DR, через який передається цей пакет.

На рис. 1 показаний приклад таблиці маршрутизації для топології з кількома областями і каналом, підключеним до зовнішньої мережі, що не підтримує протокол OSPF. Маршрути OSPF в таблиці маршрутизації IPv4 визначаються наступними дескрипторами:

Записи таблицы маршрутизации для маршрутизатора и сети



```
R1# show ip route
Codes:L - local, C-connected, S-static, R-RIP, M-mobile, B-BGP
     D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
     N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
     E1 - OSPF external type 1, E2 - OSPF external type 2
     i - IS-IS, su-IS-IS summary, L1-IS-IS level-1, L2-IS-IS level-2
     ia - IS-IS inter area,*-candidate default,U-per-user static route
     o - ODR, P-periodic downloaded static route, H-NHRP, l-LISP
     + - replicated route, % - next hop override

Gateway of last resort is 192.168.10.2 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 192.168.10.2, 00:00:19, Serial0/0/0
    10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C    10.1.1.0/24 is directly connected, GigabitEthernet0/0
L    10.1.1.1/32 is directly connected, GigabitEthernet0/0
C    10.1.2.0/24 is directly connected, GigabitEthernet0/1
L    10.1.2.1/32 is directly connected, GigabitEthernet0/1
O    10.2.1.0/24 [110/648] via 192.168.10.2, 00:04:34, Serial0/0/0
O IA 192.168.1.0/24 [110/1295] via 192.168.10.2, 00:01:48,Serial0/0/0
O IA 192.168.2.0/24 [110/1295] via 192.168.10.2, 00:01:48,Serial0/0/0
    192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C   192.168.10.0/30 is directly connected, Serial0/0/0
L   192.168.10.1/32 is directly connected, Serial0/0/0
O   192.168.10.4/30 [110/1294] via 192.168.10.2, 00:01:55,Serial0/0/0
R1#
```

Рис. 5.5.10

O. Пакети LSA маршрутизатора (тип 1) і мережі (тип 2) містять інформацію про маршрутизації всередині області. У таблиці маршрутизації ці дані про стан каналів позначені O, що показує, що маршрут проходить всередині області.

IA. Коли маршрутизатор ABR отримує сумарні пакети LSA, він додає їх в свою базу даних LSDB, після цього даний пакет регенерується в локальну область. Коли маршрутизатор ABR отримує LSA типу 3, він додає їх в свою базу даних LSDB і розсилає їх у своїй області. Потім внутрішні маршрутизатори інтегрують цю інформацію в свої бази даних. Сумарні LSA відображаються в таблиці маршрутизації як IA (interarea routes = міжобласні маршрути).

E1 або O E2. LSA-анонси про зовнішні маршрутах відображаються в таблиці маршрутизації, відмічені як зовнішні маршрути типу 1 (E1) або типу 2 (E2).

На рис. 2 показана таблиця маршрутизації IPv6, що містить записи маршрутизатора OSPF, міжобласний маршрутизації і зовнішньої маршрутизації.

Записи таблицы маршрутизации OSPFv3

```
R1# show ipv6 route
IPv6 Routing Table - default - 9 entries
Codes:C - Connected, L - Local, S - Static, U-Per-user Static route
     B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
     I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
     EX - EIGRP external, ND-ND Default,NDp-ND Prefix,DCE-Destination
     NDr - Redirect, O-OSPF Intra, OI-OSPF Inter, OE1-OSPF ext 1
     OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OE2 ::/0 [110/1], tag 10
    via FE80::2, Serial0/0/0
C   2001:DB8:CAFE:1::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:CAFE:1::1/128 [0/0]
    via GigabitEthernet0/0, receive
O   2001:DB8:CAFE:2::/64 [110/648]
    via FE80::2, Serial0/0/0
OI  2001:DB8:CAFE:3::/64 [110/1295]
    via FE80::2, Serial0/0/0
C   2001:DB8:CAFE:A001::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:CAFE:A001::1/128 [0/0]
    via Serial0/0/0, receive
O   2001:DB8:CAFE:A002::/64 [110/1294]
    via FE80::2, Serial0/0/0
L   FF00::/8 [0/0]
    via Null0, receive
R1#
```

Рис. 5.5.11

Розрахунок маршруту OSPF

.Як показано на малюнку, використовується наступний порядок розрахунку оптимальних маршрутів:

Пошаговые действия сходимости OSPF

```
R1# show ip route | begin Gateway
Gateway of last resort is 192.168.10.2 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 192.168.10.2, 00:00:19, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.1.1.0/24 is directly connected, GigabitEthernet0/0
L       10.1.1.1/32 is directly connected, GigabitEthernet0/0
C       10.1.2.0/24 is directly connected, GigabitEthernet0/1
L       10.1.2.1/32 is directly connected, GigabitEthernet0/1
O       10.2.1.0/24 [110/648] via 192.168.10.2, 00:04:34,Serial0/0/0
O IA 192.168.1.0/24 [110/1295] via 192.168.10.2, 00:01:48,Serial0/0/0
O IA 192.168.2.0/24 [110/1295] via 192.168.10.2, 00:01:48,Serial0/0/0
     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C       192.168.10.0/30 is directly connected, Serial0/0/0
L       192.168.10.1/32 is directly connected, Serial0/0/0
O       192.168.10.4/30 [110/1294] via 192.168.10.2, 00:01:55,Serial0/0/0
R1#
```

- Расчёт маршрутов OSPF внутри области.
- Расчёт оптимальных межобластных маршрутов OSPF.
- Расчёт оптимальных маршрутов к внешним сетям, не поддерживающим протокол OSPF

Рис. 5.5.12

1. Всі маршрутизатори розраховують оптимальні шляхи до вузлів призначення в своїй області (внутрішньообласні маршрути) і додають ці записи

в таблицю маршрутизації. Це пакети LSA типу 1 і типу 2, відмічені в таблиці маршрутизації кодом O. (1)

2. Всі маршрутизатори розраховують оптимальні шляхи до інших областей в рамках об'єднаної мережі. Ці оптимальні шляхи є записами міжобласних маршрутів, або пакетами LSA типу 3 і типу 4, і позначаються кодом O IA. (2)

3. Всі маршрутизатори (за винятком що знаходяться в тупиковій області) розраховують оптимальні шляхи до мереж, які знаходяться в зовнішніх автономних системах (тип 5). Ці шляхи позначаються кодом O E1 або O E2, в залежності від конфігурації. (3)

Після збіжності маршрутизатор може взаємодіяти з будь-якою мережею всередині або поза автономної системи OSPF.

OSPF може бути реалізований як протокол для однієї області або для декількох областей. Обраний тип реалізації OSPF залежить від конкретних вимог і існуючої топології.

Як показано на малюнку, реалізація OSPF для декількох областей складається з 4 кроків.

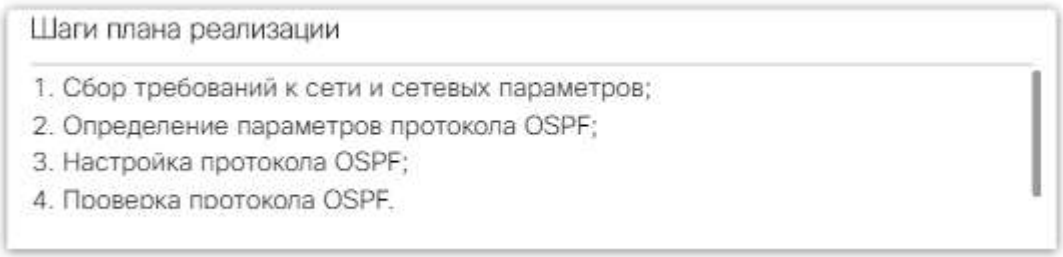


Рис. 5.5.13

Кроки 1 і 2 є частиною процесу планування.

Крок 1. Збір вимог і параметрів мережі. Цей етап передбачає визначення кількості вузлів і мережевих пристроїв, схему IP-адресації (якщо вона вже впроваджена), розмір домена маршрутизації, розмір таблиць маршрутизації, ризик змін топології і інші мережеві характеристики.

Крок 2. Визначення параметрів OSPF. На основі інформації, зібраної на кроці 1, мережевий адміністратор повинен вибрати бажану реалізацію OSPF - для однієї області або для декількох областей. У разі вибору параметра OSPF для декількох областей, мережевий адміністратор, визначаючи параметри OSPF, повинен врахувати ряд особливостей, щоб включити наступне:

План IP-адресації. Управління можливостями розгортання OSPF і масштабуванням цього розгортання. Повинен бути створений детальний план IP-адресації з даними про IP-підмережі. Хороший план IP-адресації повинен передбачати використання архітектури та об'єднання в рамках OSPF для декількох областей. Цей план спрощує масштабування мережі, а також оптимізує роботу OSPF і поширення пакетів LSA.

Області OSPF. Поділ мережі OSPF на області зменшує розмір бази даних станів каналів і обмежує поширення оновлень станів каналів при зміні топології. Маршрутизатор, які повинні бути ABR і ASBR, необхідно визначити як маршрутизатори, які повинні виконувати операції об'єднання і перерозподілу.

Топологія мережі. Вона складається з каналів, що з'єднують мережеве обладнання та належать різним областям OSPF в схемі OSPF для декількох

областей. Топологія мережі важлива для визначення основних і резервних каналів. Основні і резервні канали визначаються за допомогою зміни вартості OSPF для інтерфейсів. Якщо застосовується OSPF для декількох областей, детальний план топології мережі також повинен використовуватися для визначення різних областей OSPF, маршрутизаторів ABR і ASBR, а також точок об'єднання і перерозподілу.

Крок 3. Налаштуйте реалізацію мережі OSPF для декількох областей, виходячи із заданих параметрів.

Крок 4. Перевірте реалізацію мережі OSPF для декількох областей, виходячи із заданих параметрів.

Налаштування OSPF для декількох областей

На рис. 1 показана схема топології OSPF для декількох областей. У наведеному прикладі:

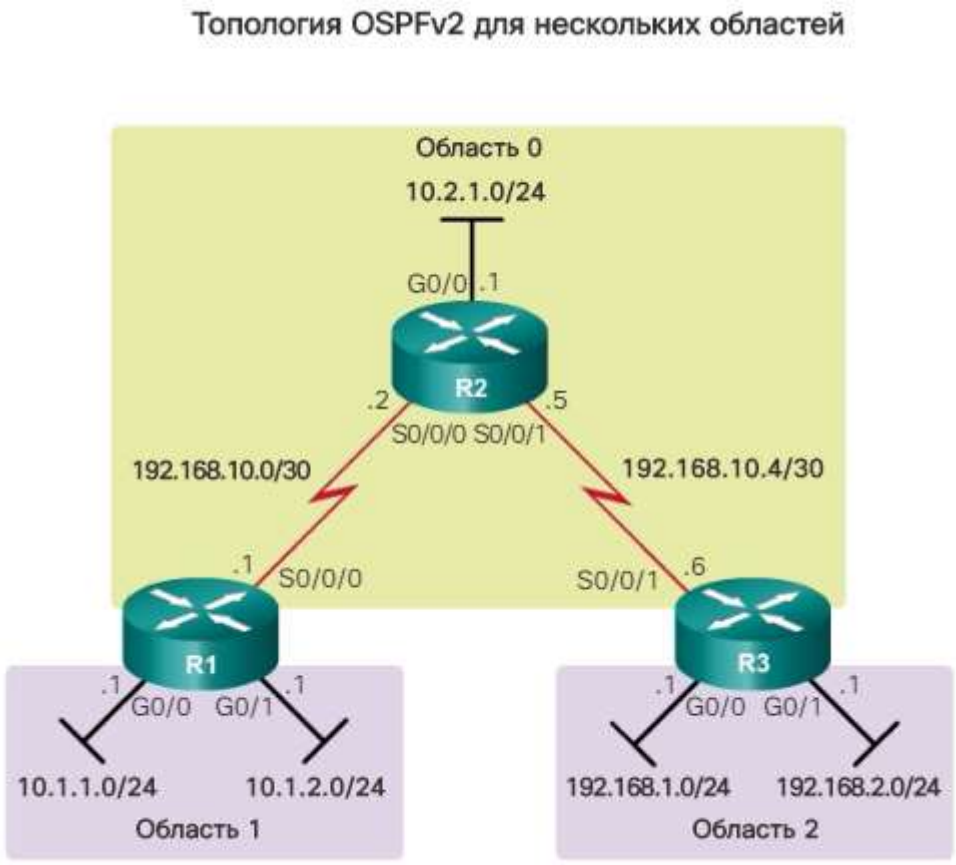


Рис. 5.5.14

Маршрутизатор R1 є ABR, оскільки у нього є інтерфейси в області 1 і інтерфейс в області 0.

Маршрутизатор R2 є внутрішнім магістральним маршрутизатором, так як всі його інтерфейси знаходяться в області 0.

Маршрутизатор R3 є маршрутизатором ABR, оскільки у нього є інтерфейси в області 2 і інтерфейс в області 0.

При реалізації цієї мережі OSPF для декількох областей не потрібні ніякі спеціальні команди. Маршрутизатор стає ABR, коли для нього задано дві інструкції network в різних областях.

Як показано на рис. 2, маршрутизатора R1 призначений ідентифікатор 1.1.1.1. У цьому прикладі протокол OSPF включений на двох інтерфейсах

локальної мережі в області 1. Послідовний інтерфейс підключений до області 0 протоколу OSPF. Оскільки у маршрутизатора R2 є інтерфейси, підключені до двох різних областях, він є ABR.

Настройка OSPF для нескольких областей на маршрутизаторе R1

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.1.1.1 0.0.0.0 area 1
R1(config-router)# network 10.1.2.1 0.0.0.0 area 1
R1(config-router)# network 192.168.10.1 0.0.0.0 area 0
R1(config-router)# end
R1#
```

Рис. 5.5.15

Використовуйте інструмент перевірки синтаксису на рис. 3, щоб налаштувати OSPF для декількох областей на маршрутизаторах R2 і R3. У цьому інструменті перевірки синтаксису використовуйте для маршрутизатора R2 шаблонну маску мережевого адреси інтерфейсу. У разі маршрутизатора R3 використовуйте для всіх мереж шаблонну маску 0.0.0.0.

Закінчивши настройку маршрутизаторів R2 і R3, зверніть увагу на інформаційні повідомлення про відносини суміжності з маршрутизатором R1 (1.1.1.1).

Закінчивши настройку маршрутизатора R3, зверніть увагу на інформаційні повідомлення про відносини суміжності з маршрутизаторами R1 (1.1.1.1) і R2 (2.2.2.2). Також зверніть увагу, як схема IP-адресації, яка використовується для ідентифікатора маршрутизатора, спрощує визначення сусіднього маршрутизатора.

Примітка. Зворотні шаблонні маски, які використовуються для настройки маршрутизаторів R2 і R3, навмисно визначені як різні, щоб показати два варіанти введення інструкцій network. Спосіб, який використовується для маршрутизатора R3, є більш простим, оскільки шаблонна маска завжди дорівнює 0.0.0.0, і її обчислення не потрібно.

Налаштування OSPFv3 для кількох областей

Аналогічно OSPFv2, реалізація топології OSPFv3 для декількох областей відрізняється простотою (рис. 1). Ніякі особливі команди не потрібні. Маршрутизатор стає ABR, коли у нього є два інтерфейси в різних областях.

Топология OSPFv3 для нескольких областей

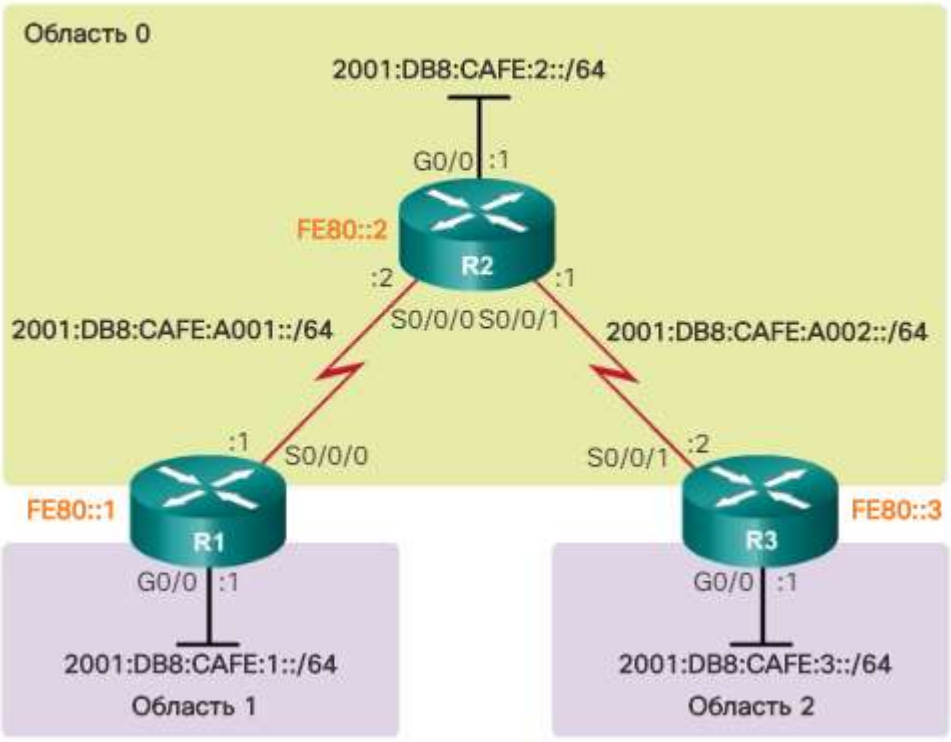


Рис. 5.5.16

У прикладі, показаному на рис. 2, маршрутизатора R1 призначений ідентифікатор 1.1.1.1. У цьому прикладі також включений протокол OSPF для двох інтерфейсів локальної мережі в області 1 і для послідовного інтерфейсу в області 0. Оскільки у маршрутизатора R1 є інтерфейси, підключені до двох різних областях, він стають ABR.

Настройка OSPFv3 для нескольких областей на маршрутизаторе R1

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# exit
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 ospf 10 area 1
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)# end
R1#
```

Рис. 5.5.17

Використовуйте інструмент перевірки синтаксису на рис. 3, щоб налаштувати OSPFv3 для кількох областей на маршрутизаторах R2 і R3.

Закінчивши настройку маршрутизатора R2, зверніть увагу на повідомлення про наявність відносин суміжності з маршрутизатором R1 (1.1.1.1).

Закінчивши настройку маршрутизатора R3, зверніть увагу на повідомлення про наявність відносин суміжності з маршрутизатором R2 (2.2.2.2).

Тема 6.2.2 Об’єднання маршрутів OSPF

Об'єднання маршрутів OSPF

Об'єднання допомагає зменшити розмір таблиць маршрутизації. Воно дозволяє об'єднати кілька маршрутів в одне оголошення, яке потім може бути поширене в магістральної області.

Зазвичай в кожній області створюються пакети LSA типу 1 і типу 2, що перетворюються в пакети LSA типу 3, які відправляються в інші області. Якщо в області 1 оголошується 30 мереж, то в магістральну область буде відправлено 30 пакетів LSA типу 3. При використанні об'єднання маршрутів маршрутизатор ABR об'єднує 30 мереж в одному з двох оголошень.

На рис. 1 маршрутизатор R1 об'єднує всі оголошення мереж в один сумарний пакет LSA. Замість пересилання окремих пакетів LSA для кожного маршруту в області 1 маршрутизатор R1 пересилає сумарний пакет LSA маршрутизатора ядра C1. C1, в свою чергу, пересилає сумарний пакет LSA маршрутизаторів R2 і R3. Маршрутизатор R2 і R3 потім пересилають цей пакет своїм відповідним внутрішнім маршрутизаторів.

Рис. 5.5.18

Об'єднання також підвищує стійкість мережі, скорочуючи розсилку непотрібних пакетів LSA. Об'єднання маршрутів безпосередньо впливає на використання процесом маршрутизації OSPF ресурсів пропускної здатності, ЦП і пам'яті. Без об'єднання маршрутів кожен пакет LSA для конкретного

каналу передається в магістраль OSPF і за її межі, приводячи до непотрібного мережевого трафіку і збільшуючи накладні витрати маршрутизатора.

Виникає відмова мережевого каналу маршрутизатора R1a, показаного на рис. 2. Маршрутизатор R1a відправляє пакет LSA маршрутизатора R1. Але R1 не поширюється оновлення, так як на ньому налаштований об'єднаний маршрут. Лавинна розсилка пакетів LSA для конкретного каналу за межі області не відбувається.

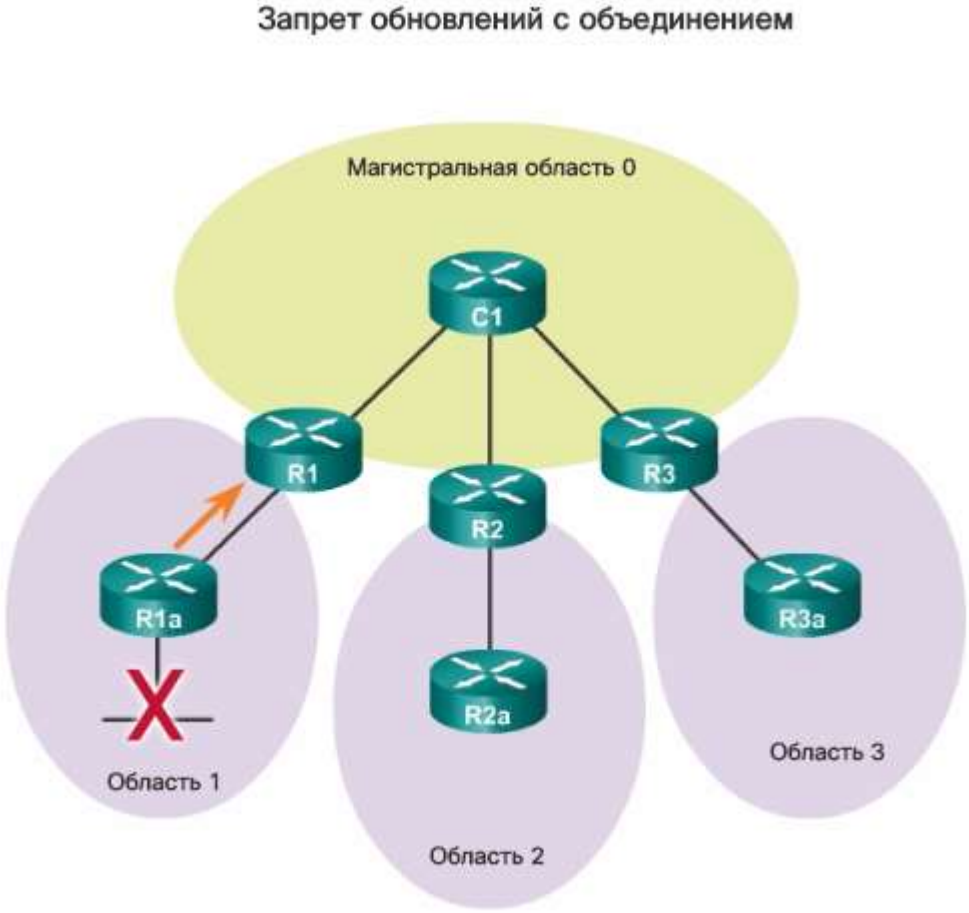


Рис. 5.5.19

Об'єднання міжобласних і зовнішніх маршрутів

У OSPF об'єднання можна налаштувати тільки на маршрутизаторах ABR або ASBR. Замість оголошення безлічі окремих мереж маршрутизатори ABR і ASBR оголошують об'єднаний маршрут. Маршрутизатор ABR об'єднують пакети LSA типу 3, а маршрутизатори ASBR об'єднують пакети LSA типу 5.

За замовчуванням сумарні (LSA типу 3) і зовнішні (LSA типу 5) пакети LSA не містять об'єднаних (агрегованих) маршрутів, тобто за замовчуванням сумарні пакети LSA не об'єднує.

Як показано на рис. 1 і 2, об'єднання маршрутів може бути налаштоване таким чином.

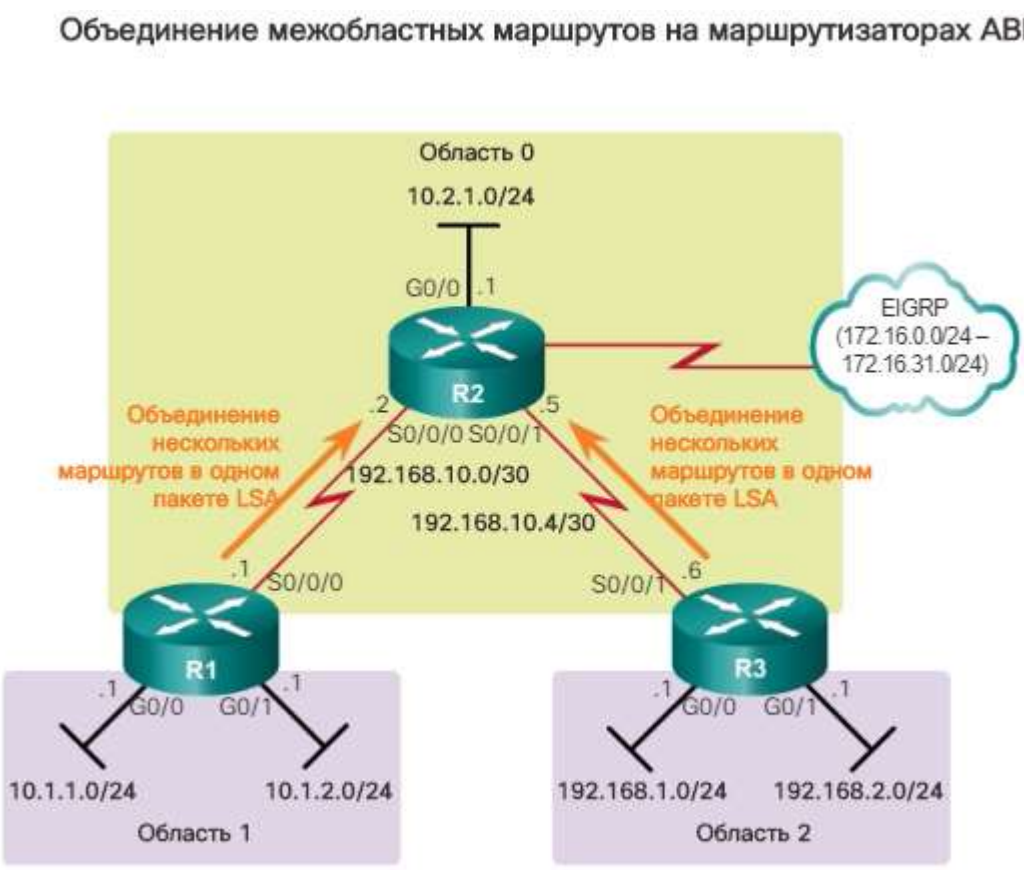


Рис. 5.5.20

Об'єднання міжобласних маршрутів. Об'єднання міжобласних маршрутів виконується на маршрутизаторах ABR і застосовується до маршрутів всередині кожної області. Воно не застосовується до зовнішніх маршрутах, поширюваним в OSPF за допомогою перерозподілу. Для ефективного об'єднання міжобласних маршрутів мережеві адреси всередині областей повинні призначатися послідовно, щоб ці адреси можна було об'єднати в мінімальне число зведених адрес.

Об'єднання зовнішніх маршрутів. Об'єднання зовнішніх маршрутів відноситься тільки до зовнішніх маршрутами, які вводяться в OSPF за допомогою перерозподілу маршрутів. Крім того, важливо забезпечити безперервність діапазонів схильних до об'єднання зовнішніх адрес. Як правило, зовнішні маршрути об'єднуються тільки маршрутизаторами ASBR. Як показано на рис. 2, зовнішні маршрути EIGRP об'єднуються ASBR-маршрутизатором R2 в один пакет LSA і відправляються маршрутизаторів R1 і R3.

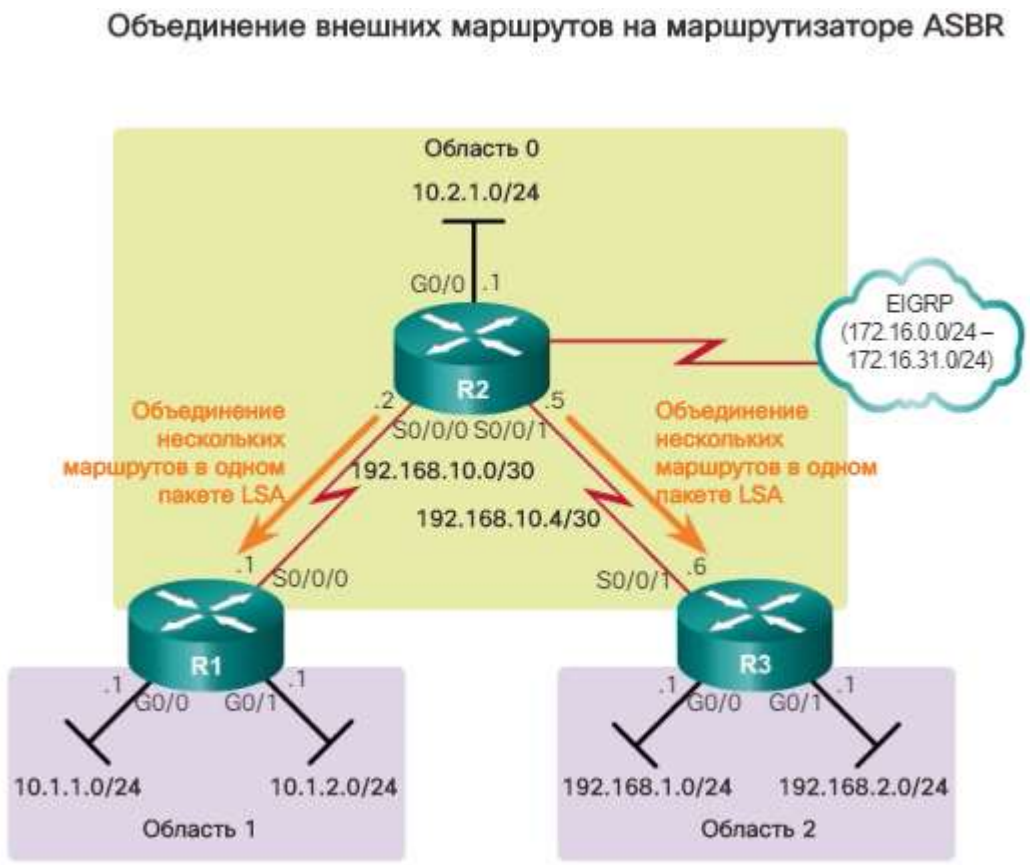


Рис. 5.5.21

Примітка. Об'єднання зовнішніх маршрутів налаштовується на граничних маршрутизаторах автономних систем (ASBR) за допомогою команди режиму конфігурації маршрутизатора summary-address address mask.

Об'єднання міжобласних маршрутів

Протокол OSPF не виконує об'єднання автоматично. Об'єднання міжобласних маршрутів необхідно вручну налаштувати на маршрутизаторах ABR.

Об'єднання внутрішніх маршрутів може виконуватися тільки маршрутизаторами ABR. Якщо на маршрутизаторі ABR включено об'єднання, цей маршрутизатор відправляє в магістраль один пакет LSA типу 3, що описує об'єднаний маршрут. Кілька маршрутів в області об'єднання в одному пакеті LSA.

Об'єднаний маршрут створюється, якщо хоча б одна підмережа в області потрапляє в діапазон об'єднаних адрес. Метрика об'єднаного маршруту дорівнює мінімальній вартості всіх підмереж в діапазоні об'єднаних адрес.

Примітка. Маршрутизатор ABR може об'єднувати тільки маршрути, що знаходяться в областях, підключених до ABR.

Топологія OSPF для декількох областей показана на рис. 1. Проаналізуємо таблиці маршрутизації R1 і R3, щоб побачити результат об'єднання.

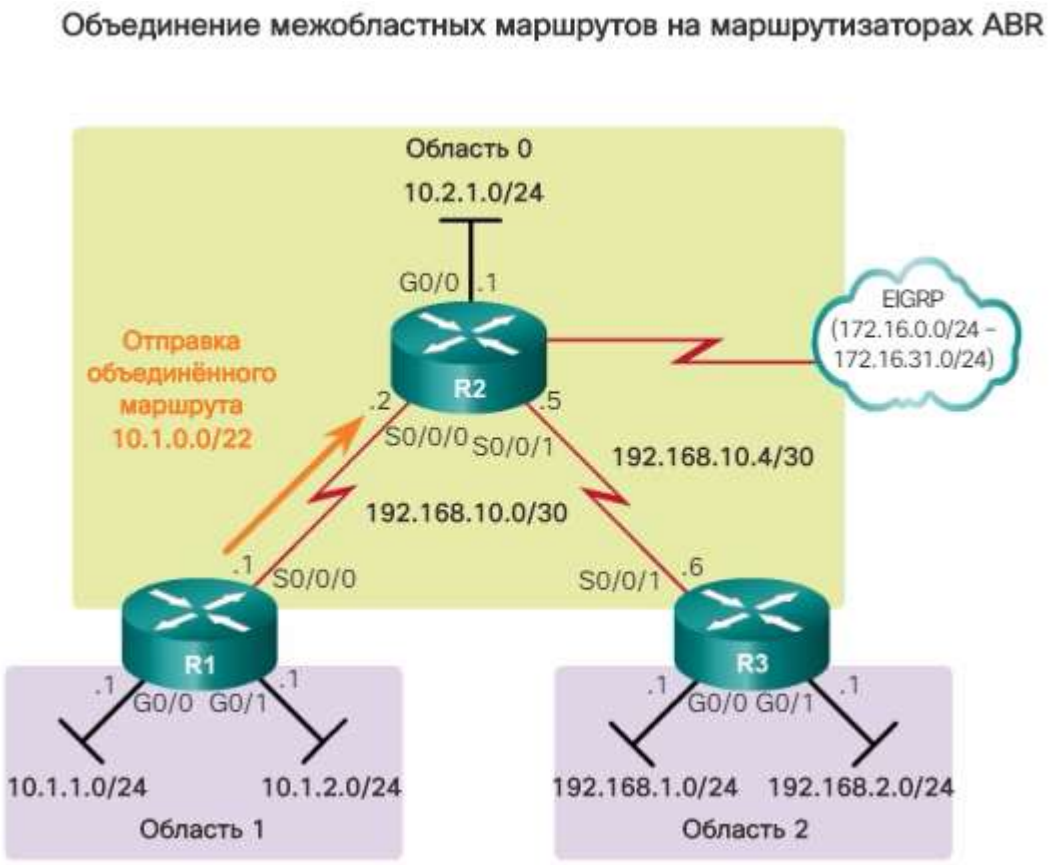


Рис. 5.5.22

На рис. показана таблиця маршрутизації для маршрутизатора R1 перед налаштуванням об'єднання, а на рис. 3 - таблиця маршрутизації для маршрутизатора R3. Зверніть увагу, що у R3 є дві міжобласних записи до мереж R1 області 1.

Перед объединением проверьте таблицу маршрутизации для маршрутизатора R1

```
R1# show ip route ospf | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O        10.2.1.0/24 [110/648] via 192.168.10.2, 00:00:49,
         Serial0/0/0
O IA  192.168.1.0/24 [110/1295] via 192.168.10.2, 00:00:49,
      Serial0/0/0
O IA  192.168.2.0/24 [110/1295] via 192.168.10.2, 00:00:49,
      Serial0/0/0
      192.168.10.0/24 is variably subnetted, 3 subnets, 2
      masks
O        192.168.10.4/30 [110/1294] via 192.168.10.2,
         00:00:49, Serial0/0/0
R1#
```

Рис. 5.5.23

Перед объединением проверьте таблицу маршрутизации для маршрутизатора R3

```
R3# show ip route ospf | begin Gateway
Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 3 subnets
O IA     10.1.1.0 [110/1295] via 192.168.10.5, 00:27:14, Serial0/0/1
O IA     10.1.2.0 [110/1295] via 192.168.10.5, 00:27:14, Serial0/0/1
O        10.2.1.0 [110/648] via 192.168.10.5, 00:27:57, Serial0/0/1
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
O        192.168.10.0/30 [110/1294] via 192.168.10.5, 00:27:57,
         Serial0/0/1
R3#
```

Рис. 5.5.24

Розрахунок об'єднаного маршруту

На малюнку показано, що об'єднання мереж в один сумарний адресу і одну сумарну маску здійснюється в 3 етапи.

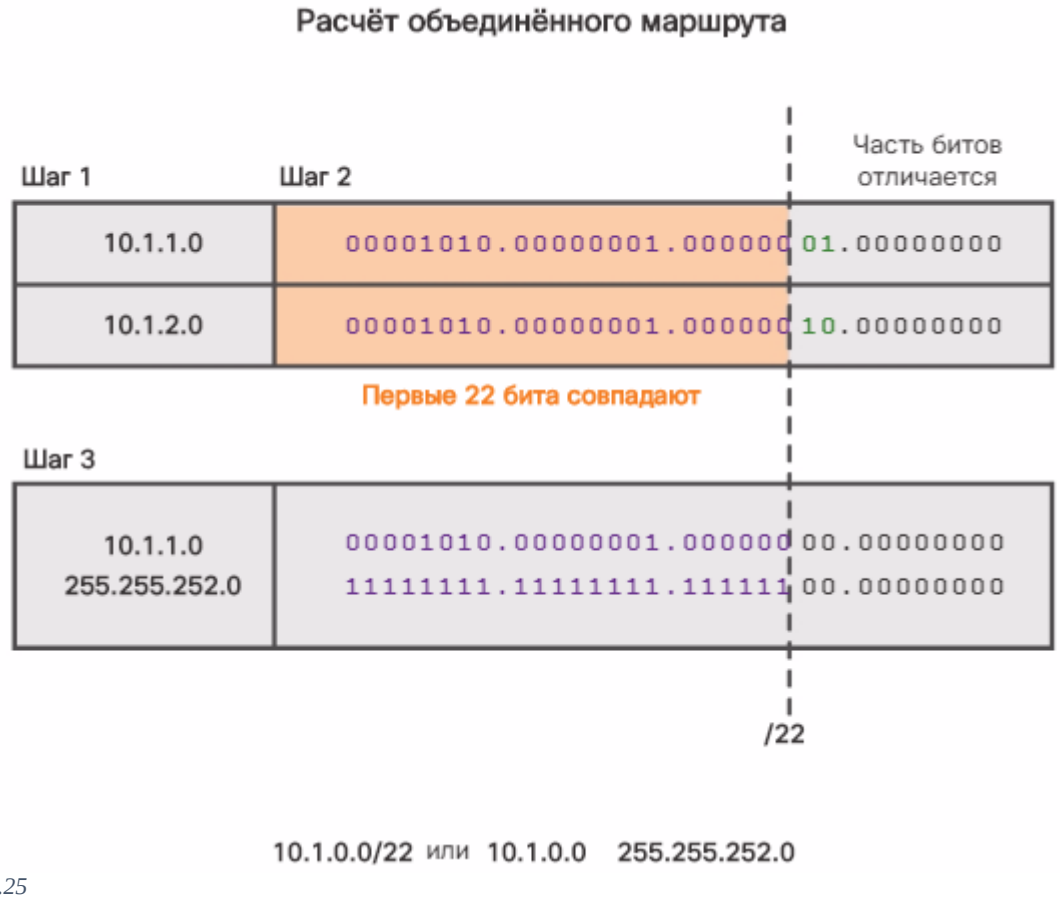


Рис. 5.5.25

Крок 1. Перерахуйте мережі в довічним форматі. У цьому прикладі дві мережі області 1 (10.1.1.0/24 і 10.1.2.0/24) перераховані в довічним форматі.

Крок 2. Підрахуйте число крайніх лівих збігаються бітів для визначення маски об'єднаного маршруту. Як зазначено, збігаються 22 крайніх перших лівих біта. Як результат вийде префікс / 22 або маска підмережі 255.255.252.0.

Крок 3. Скопіюйте збігаються біти і додайте нульові біти, щоб визначити об'єднаний мережеву адресу (префікс). У цьому прикладі збігаються біти з нулями в кінці дають адресу мережі 10.1.0.0/22. Цей об'єднаний адреса об'єднує чотири мережі: 10.1.0.0/24, 10.1.1.0/24, 10.1.2.0/24 і 10.1.3.0/24.

У прикладі об'єднаний адреса відповідає чотирьом мереж, хоча в наявності є тільки дві мережі.

Налаштування об'єднання міжобласних маршрутів

На рис. 1 для демонстрації ефективності об'єднання маршрутів на маршрутизаторі R1 налаштоване об'єднання внутрішніх маршрутів області 1.

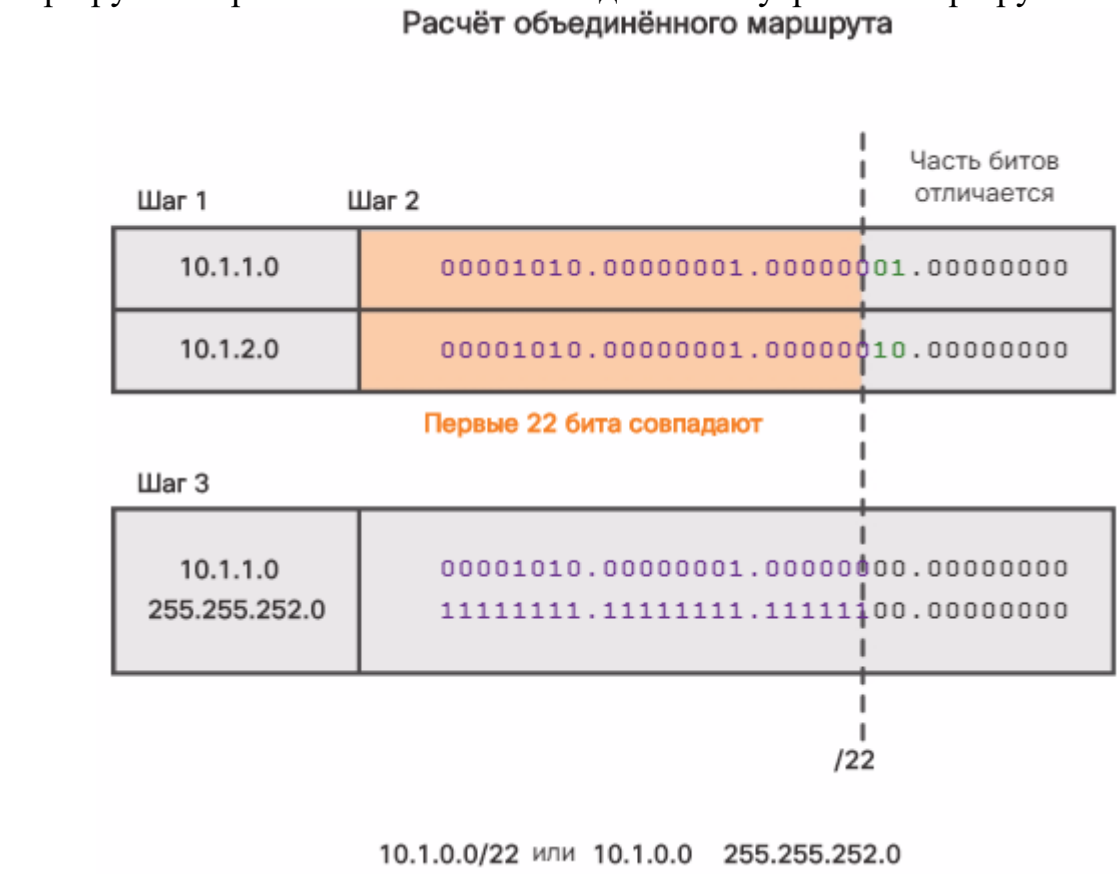


Рис. 5.5.26

Щоб вручну налаштувати об'єднання міжобласних маршрутів на граничному маршрутизаторі ABR, використовуйте команду режиму конфігурації маршрутизатора area area-id range address mask. Команда вказує маршрутизатору ABR об'єднувати маршрути для конкретної області перед їх передачею в іншу область, використовуючи магістраль, в зведених пакетах LSA типу 3.

Примітка. У OSPFv3 команда є ідентичною за винятком вказівки мережевого адреси IPv6. Синтаксис команд для OSPFv3: area area-id range prefix / prefix-length.

На рис. 2 два внутрішніх маршруту області 1 об'єднуються на маршрутизаторі R1 в один загальний міжобласний маршрут OSPF. В об'єднаному маршруті 10.1.0.0/22 фактично об'єднані адреси чотирьох мереж, з 10.1.0.0/24 до 10.1.3.0/24.

Объединение маршрутов области 1 на маршрутизаторе R1

```
R1(config)# router ospf 10
R1(config-router)# area 1 range 10.1.0.0 255.255.252.0
R1(config-router)#
```

Рис. 5.5.27

Рис. 2

На рис. 3 показана таблиця маршрутизації IPv4 для маршрутизатора R1. Зверніть увагу на появу нового запису з вихідним інтерфейсом Null0. Під час налаштування об'єднання вручну для запобігання петель маршрутизації Cisco IOS автоматично створює фіктивний об'єднаний маршрут до інтерфейсу Null0. Пакет, який надійшов інтерфейсу Null, відкидається.

Проверьте таблицу маршрутизации R1 после объединения

```
R1# show ip route ospf | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
O        10.1.0.0/22 is a summary, 00:00:09, Null0
O        10.2.1.0/24 [110/648] via 192.168.10.2, 00:00:09,Serial0/0/0
O IA  192.168.1.0/24 [110/1295] via 192.168.10.2, 00:00:09,Serial0/0/0
O IA  192.168.2.0/24 [110/1295] via 192.168.10.2, 00:00:09,Serial0/0/0
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
        192.168.10.4/30 [110/1294] via 192.168.10.2,00:00:09, Serial0/0/0
R1#
```

Рис. 5.5.28

Наприклад, нехай маршрутизатор R1 отримав пакет для вузла 10.1.0.10. Хоча цей пакет відповідає об'єднаному маршруту R1, у маршрутизатора R1 відсутня дійсний маршрут в області 1. Тому R1 виконає в таблиці маршрутизації пошук наступного найдовшого збігу, яким виявиться запис Null0. Пакет буде пересланий на інтерфейс Null0 і відкинутий. Це запобіжить пересилання маршрутизатором пакета маршрутизатора за замовчуванням і можливого створення петлі маршрутизації.

На рис. 4 показана оновлена таблиця маршрутизації для маршрутизатора R3. Зверніть увагу, що тепер тільки одна міжобласна запис вказує на об'єднаний маршрут 10.1.0.0/22. Хоча в цьому прикладі таблиця маршрутизації

скорочується тільки на одну запис, об'єднання може бути реалізовано для об'єднання декількох мереж. Це зменшить розмір таблиць маршрутизації.

Проверьте таблицу маршрутизации R1 после объединения

```
R3# show ip route ospf | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O IA     10.1.0.0/22 [110/1295] via 192.168.10.5, 00:00:06,Serial0/0/1
O        10.2.1.0/24 [110/648] via 192.168.10.5, 00:29:23,Serial0/0/1
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
O        192.168.10.0/30 [110/1294] via 192.168.10.5,00:29:23,
Serial0/0/1
R3#
```

Рис. 4

Використовуйте для об'єднання маршрутів області 2 на маршрутизаторі R3 на рис. 5 інструмент перевірки синтаксису.

Тема 6.2.3 Перевірка OSPF для декількох областей

Перевірка OSPF для декількох областей

Щоб перевірити топологію OSPF для декількох областей, показану на малюнку, можна використовувати ті ж команди перевірки, що і в разі OSPF з однією областю:

show ip ospf neighbor

show ip ospf

show ip ospf interface

До командам, що дозволяє перевірити конкретні дані для декількох областей, відносяться наступні:

show ip protocols

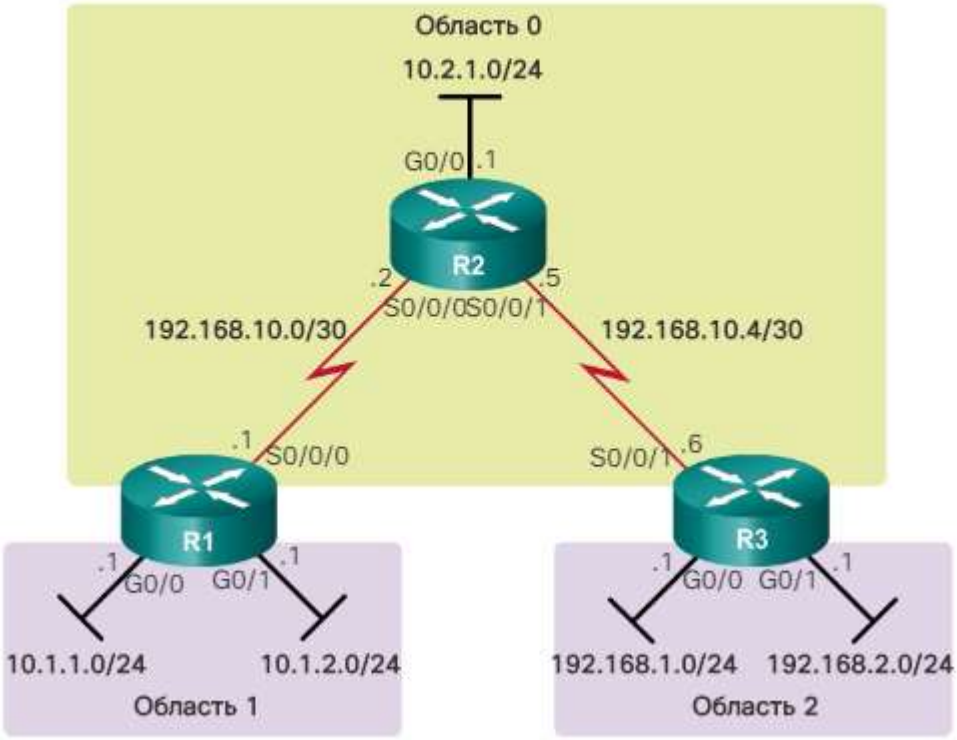
show ip ospf interface brief

show ip route ospf

show ip ospf database

Примітка. Для отримання еквівалентної команди OSPFv3 просто замініть ip на ipv6.

Топология OSPF для нескольких областей



Перевірка загальних параметрів OSPF для декількох областей

Для перевірки стану OSPF використовуйте команду show ip protocols. Результат команди показує, які протоколи маршрутизації налаштовані на маршрутизаторі. Він також містить конкретні дані протоколу маршрутизації, такі як ідентифікатор маршрутизатора, число областей для маршрутизатора та мережі, що входять в конфігурацію протоколу маршрутизації.

На рис. 1 показані параметри OSPF для маршрутизатора R1. Зверніть увагу, що результат команди містить дві області. Розділ Routing for Networks (Маршрутизація для мереж) визначає мережі і відповідні області.

Проверка состояния OSPF для нескольких областей на маршрутизаторе R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  It is an area border router
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.1.1 0.0.0.0 area 1
    10.1.2.1 0.0.0.0 area 1
    192.168.10.1 0.0.0.0 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      02:20:36
    2.2.2.2              110      02:20:39
  Distance: (default is 110)

R1#
```

Рис. 5.5.29

Використовуйте команду show ip ospf interface brief, щоб вивести коротку інформацію, що відноситься до OSPF, для інтерфейсів з підтримкою OSPF. Ця команда відображає корисну інформацію, таку як ідентифікатор процесу OSPF, якому призначений інтерфейс, область, в яку входять інтерфейси, а також вартість інтерфейсу.

На рис. 2 показані результати перевірки інтерфейсів з підтримкою OSPF і області, до яких відносяться ці інтерфейси.

Проверка интерфейсов с включенной поддержкой OSPF на маршрутизаторе R1

```
R1# show ip ospf interface brief
Interface  PID   Area  IP Address/Mask    Cost  State Nbrs  F/C
Se0/0/0    10    0     192.168.10.1/30    64    P2P   1/1
Gi0/1      10    1     10.1.2.1/24        1     DR    0/0
Gi0/0      10    1     10.1.1.1/24        1     DR    0/0
R1#
```

Рис. 5.5.30

Найбільш поширеною командою, використовуваної з метою перевірки конфігурації OSPF для декількох областей, є команда show ip route. Додайте параметр ospf, щоб вивести тільки дані, що відносяться до OSPF.

На рис. 1 показана таблиця маршрутизації для маршрутизатора R1. Зверніть увагу, як записи O IA в таблиці маршрутизації визначають мережі, відомості про яких отримані з інших областей. Зокрема, O позначає маршрути OSPF, а IA позначає міжобласні маршрути, показуючи, що джерело маршруту знаходиться в іншій області. Пам'ятайте, що маршрутизатор R1 знаходиться в області 0, а підмережі 192.168.1.0 і 192.168.2.0 підключені до маршрутизатора R3 в області 2. Запис [110/1295] в таблиці маршрутизації являє адміністративну дистанцію, призначену OSPF (110), і сукупну вартість маршрутів (вартість +1295).

Проверка маршрутов OSPF для нескольких областей на маршрутизаторе R1

```
R1# show ip route ospf | begin Gateway
Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O    10.2.1.0/24 [110/648] via 192.168.10.2, 00:26:03,
                                            Serial0/0/0
O IA 192.168.1.0/24 [110/1295] via 192.168.10.2, 00:26:03,
                                            Serial0/0/0
O IA 192.168.2.0/24 [110/1295] via 192.168.10.2, 00:26:03,
                                            Serial0/0/0
    192.168.10.0/24 is variably subnetted,3 subnets,2 masks
O    192.168.10.4/30 [110/1294] via 192.168.10.2, 00:26:03,
                                            Serial0/0/0
R1#
```

Рис. 5.5.31

Перевірка бази LSDB протоколу OSPF для декількох областей

Використовуйте команду show ip ospf database для перевірки вмісту бази даних LSDB.

Для команди show ip ospf database є безліч параметрів.

Наприклад, на рис. 1 показано вміст бази LSDB маршрутизатора R1. Зверніть увагу, що на маршрутизаторі R1 є повідомлення для області 0 і області 1, оскільки маршрутизатор ABR повинен вести окрему базу LSDB для кожної області, до якої він належить. У розділі Router Link States (Стани каналів маршрутизатора) результатів для області 0 визначені 3 маршрутизатора. Розділ Summary Net Link States (Стани об'єднаних мережевих каналів) визначає мережі, відомості про яких отримані з інших областей, і сусідній маршрутизатор, який оголосив відповідну мережу.

Проверка базы данных LSDB протокола OSPF на маршрутизаторе R1

```
R1# show ip ospf database
            OSPF Router with ID (1.1.1.1) (Process ID 10)

                Router Link States (Area 0)
Link ID         ADV Router      Age  Seq#       Checksum  Link count
1.1.1.1         1.1.1.1         725  0x80000005 0x00F9B0  2
2.2.2.2         2.2.2.2         695  0x80000007 0x003DB1  5
3.3.3.3         3.3.3.3         681  0x80000005 0x00FF91  2
                Summary Net Link States (Area 0)
Link ID         ADV Router      Age  Seq#       Checksum
10.1.1.0        1.1.1.1         725  0x80000006 0x00D155
10.1.2.0        1.1.1.1         725  0x80000005 0x00C85E
192.168.1.0     3.3.3.3         681  0x80000006 0x00724E
192.168.2.0     3.3.3.3         681  0x80000005 0x006957

                Router Link States (Area 1)
Link ID         ADV Router      Age  Seq#       Checksum  Link count
1.1.1.1         1.1.1.1         725  0x80000006 0x007D7C  2
                Summary Net Link States (Area 1)
Link ID         ADV Router      Age  Seq#       Checksum
10.2.1.0        1.1.1.1         725  0x80000005 0x004A9C
192.168.1.0     1.1.1.1         725  0x80000005 0x00B593
192.168.2.0     1.1.1.1         725  0x80000005 0x00AA9D
192.168.10.0    1.1.1.1         725  0x80000005 0x00B3D0
192.168.10.4    1.1.1.1         725  0x80000005 0x000E32
R1#
```

Рис. 5.5.32

Як і у випадку з OSPFv2, для перевірки роботи OSPFv3 передбачені аналогічні команди. Див. Довідкову топологію OSPFv3 на рис. 1.

Топология OSPFv3

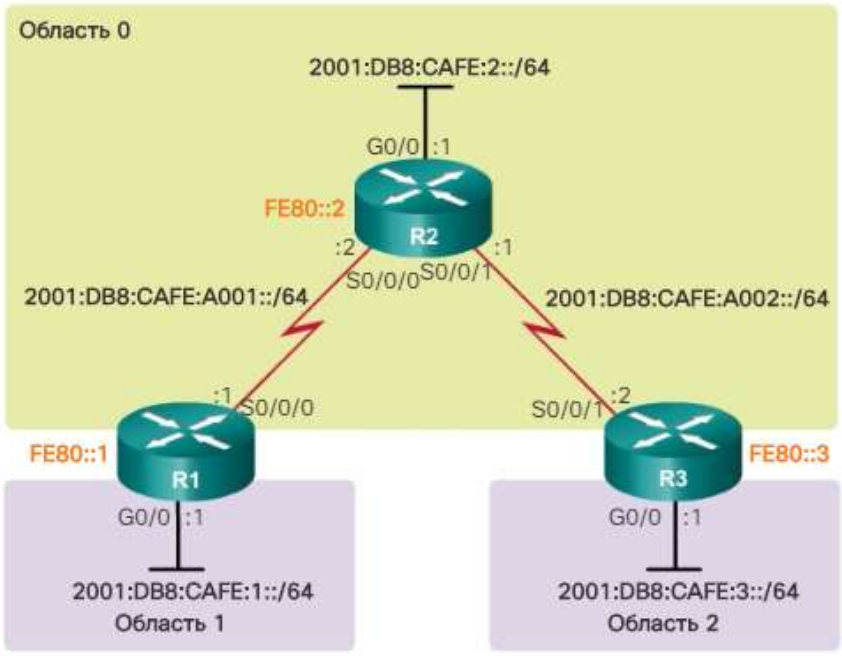


Рис. 5.5.33

На рис. 2 показані параметри OSPFv3 для маршрутизатора R1. Зверніть увагу - тепер команда підтверджує наявність двох областей. Вона також показує всі інтерфейси, доступні для відповідної області.

Проверка состояния OSPFv3 для нескольких областей на маршрутизаторе R1

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Area border router
  Number of areas: 2 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/0
  Interfaces (Area 1):
    GigabitEthernet0/0
  Redistribution:
    None
R1#
```

Рис. 5.5.34

На рис. показані результати перевірки інтерфейсів з підтримкою OSPFv3 і області, до яких відносяться ці інтерфейси.

Проверка интерфейсов с включенной поддержкой OSPFv3 на маршрутизаторе R1

```
R1# show ipv6 ospf interface brief
Interface    PID    Area         Intf ID    Cost  State Nbrs F/C
Se0/0/0      10     0            6          647   P2P   1/1
Gi0/0        10     1            3          1     DR    0/0
R1#
```

Рис. 5.5.35

На рис. показана таблиця маршрутизації для маршрутизатора R1. Зверніть увагу, як в таблиці маршрутизації IPv6 показуються записи OI, щоб вказати мережі, відомості про яких отримані з інших областей. Зокрема, O позначає маршрути OSPF, а I позначає міжобласні маршрути, показуючи, що джерело маршруту знаходиться в іншій області. Пам'ятайте, що R1 знаходиться в області 0, а підмережа 2001: DB8: CAFE3 :: / 64 підключена до R3 в області 2. Запис [110/1295] в таблиці маршрутизації являє адміністративну дистанцію, призначену OSPF (110), і сукупну вартість маршрутів (вартість +1295).

Проверка маршрутов для нескольких областей на маршрутизаторе R1

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static
route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D -
       EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF
       ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:DB8:CAFE:2::/64 [110/648]
     via FE80::2, Serial0/0/0
OI  2001:DB8:CAFE:3::/64 [110/1295]
     via FE80::2, Serial0/0/0
O   2001:DB8:CAFE:A002::/64 [110/1294]
     via FE80::2, Serial0/0/0
R1#
```

Рис. 5.5.36

На рис. показано вміст бази LSDB маршрутизатора R1. Ця команда виводить інформацію подібно аналогічної команді для OSPFv2. Але база LSDB для OSPFv3 містить додаткові типи пакетів LSA, недоступні в OSPFv2.

Проверка базы данных LSDB протокола OSPF на маршрутизаторе R1

```
R1# show ipv6 ospf database

        OSPFv3 Router with ID (1.1.1.1) (Process ID 10)

                Router Link States (Area 0)

ADV Router   Age    Seq#       Fragment ID  Link count Bits
 1.1.1.1     1617   0x80000002 0            1          B
 2.2.2.2     1484   0x80000002 0            2          None
 3.3.3.3     14     0x80000001 0            1          B

             Inter Area Prefix Link States (Area 0)

ADV Router   Age     Seq#        Prefix
 1.1.1.1     1833    0x80000001  2001:DB8:CAFE:1::/64
 3.3.3.3     1476    0x80000001  2001:DB8:CAFE:3::/64

             Link (Type-8) Link States (Area 0)

ADV Router   Age     Seq#        Link ID    Interface
 1.1.1.1     1843    0x80000001  6          Se0/0/0
 2.2.2.2     1619    0x80000001  6          Se0/0/0

             Intra Area Prefix Link States (Area 0)
```

Рис. 5.5.37

Використання OSPF для однієї області доцільно для невеликих мереж, а для мереж значних розмірів краще вибирати OSPF для декількох областей. OSPF для декількох областей вирішує проблеми великих таблиць маршрутизації, великих баз даних станів каналів і частих обчислень для алгоритму SPF, як показано на рис. 1 і 2.

Преимущества OSPF для нескольких областей

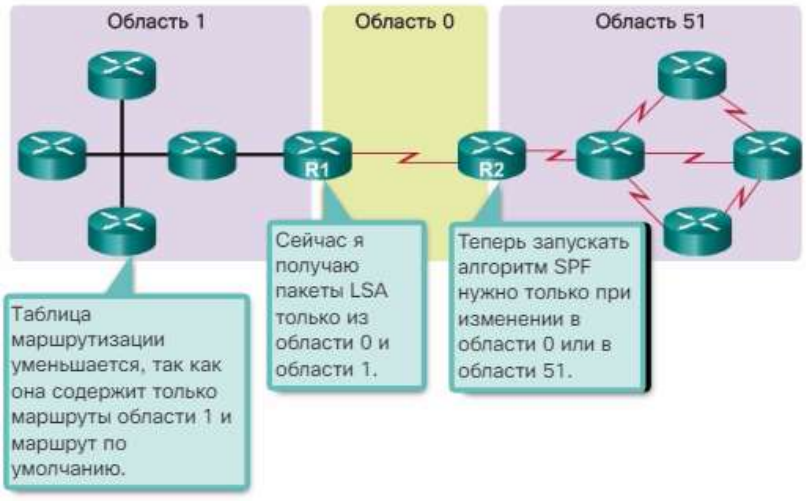


Рис. 5.5.38

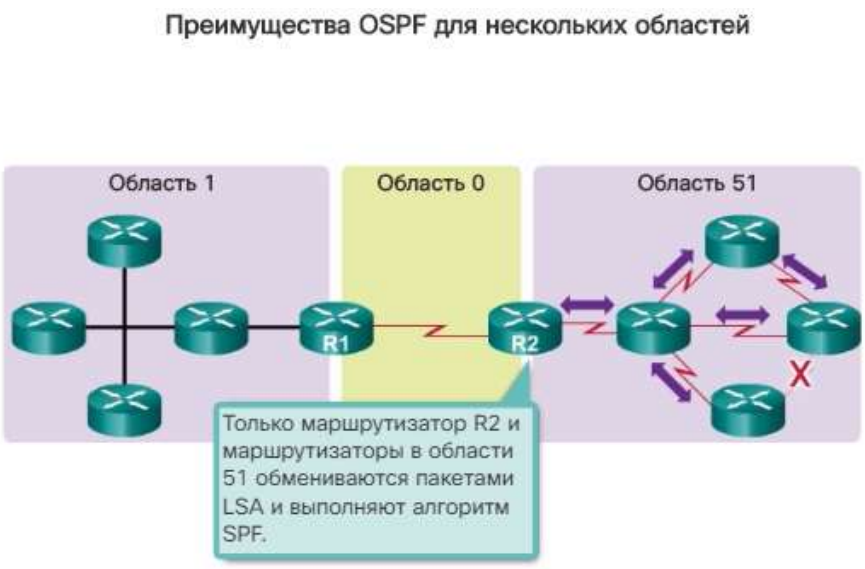


Рис. 5.5.39

Головна область називається магістральної областю (областю 0), а всі інші області повинні підключатися до магістральної області. Маршрутизація між областями виконується і в цьому випадку, але багато операцій маршрутизації, такі як повторний розрахунок бази даних, виконуються всередині області.

Існує чотири різних типів маршрутизаторів OSPF: внутрішній маршрутизатор, магістральний маршрутизатор, граничний маршрутизатор області (ABR) і граничний маршрутизатор автономної системи (ASBR). Маршрутизатор може ставитися до декількох типів маршрутизаторів.

Оголошення станів каналів (пакети LSA) є структурними елементами OSPF. У цьому розділі розглядаються пакети LSA типів 1-5. Пакети LSA типу 1 називаються записами про стан каналів маршрутизатора. Пакети LSA типу 2 називаються записами про стан каналів мережі; вони розсилаються маршрутизатором DR. Пакети LSA типу 3 називаються сумарними записами про стан каналів. Ці пакети створюються і поширюються маршрутизаторами ABR. Об'єднаний пакет LSA типу 4 створюється маршрутизатором ABR, тільки коли в області є маршрутизатор ASBR. Анонси про зовнішні маршрутах LSA типу 5 описують маршрути до мереж, що знаходяться поза автономної системи OSPF. Пакети LSA типу 5 створюються маршрутизатором ASBR і розсилаються по всій автономній системі.

Маршрути OSPF в таблиці маршрутизації IPv4 визначаються за допомогою наступних дескрипторів: O, O IA, O E1 або O E2. Кожен маршрутизатор застосовує алгоритм SPF до бази LSDB, щоб створити дерево SPF. Дерево SPF використовується для визначення оптимальних шляхів.

При реалізації мережі OSPF для декількох областей не потрібні ніякі спеціальні команди. Маршрутизатор стає ABR, коли для нього задано дві інструкції network в різних областях.

Приклад конфігурації OSPF для декількох областей:

R1 (config) # router ospf 10
R1 (config-router) # router-id 1.1.1.1
R1 (config-router) # network 10.1.1.1 0.0.0.0 area 1
R1 (config-router) # network 10.1.2.1 0.0.0.0 area 1
R1 (config-router) # network 192.168.10.1 0.0.0.0 area 0

Протокол OSPF не виконує об'єднання автоматично. У OSPF об'єднання можна налаштувати тільки на маршрутизаторах ABR або ASBR. Об'єднання міжобласних маршрутів, яке необхідно налаштовувати вручну, виконується на маршрутизаторах ABR і застосовується до маршрутів в межах кожної області. Щоб вручну налаштувати об'єднання міжобласних маршрутів на граничному маршрутизаторі ABR, використовуйте команду режиму конфігурації маршрутизатора area area-id range address mask.

Об'єднання зовнішніх маршрутів застосовується до зовнішніх маршрутах, поширюваним в OSPF за допомогою перерозподілу маршрутів. Як правило, зовнішні маршрути об'єднуються тільки маршрутизаторами ASBR. Примітка. Об'єднання зовнішніх маршрутів налаштовується на граничних маршрутизаторах автономних систем (ASBR) за допомогою команди режиму конфігурації маршрутизатора summary-address address mask.

Нижче наведені команди, використовувані для перевірки конфігурації OSPF:

show ip ospf neighbor
show ip ospf
show ip ospf interface
show ip protocols
show ip ospf interface brief
show ip route ospf
show ip ospf database

5.6 Огляд роботи протоколу EIGRP та основні його характеристики

Протокол EIGRP (Enhanced Interior Gateway Routing Protocol) - це вдосконалений протокол маршрутизації на базі векторів відстані, розроблений компанією Cisco Systems. Як випливає з назви цього протоколу, EIGRP це засіб оптимізації іншого протоколу маршрутизації Cisco - протоколу внутрішньої маршрутизації (IGRP). IGRP - це старіший протокол маршрутизації на основі класів і векторів відстані, який вважається застарілим починаючи з випуску IOS 12.3.

Протокол EIGRP - це протокол маршрутизації на базі векторів відстані, що включає можливості протоколів маршрутизації з урахуванням стану каналу. EIGRP підходить для безлічі різних топологій і середовищ. У якісно спроектованої мережі EIGRP може масштабироваться, щоб інтегрувати різні топології, і може забезпечити дуже короткий час збіжності з мінімальним мережевим трафіком.

У цьому розділі описуються протокол EIGRP і основні команди конфігурації, що включають даний протокол на маршрутизаторі Cisco IOS. У ній також описаний принцип роботи протоколу маршрутизації і приведені додаткові відомості про вибір оптимального шляху протоколом EIGRP.

Спочатку EIGRP з'явився в 1992 році як пропріетарний протокол, доступний тільки на пристроях Cisco. У 2013 р компанія Cisco представила організації IETF опис основних функцій EIGRP як відкритого стандарту у вигляді інформаційного документа RFC. Це означає, що інші постачальники мережевих рішень тепер можуть реалізовувати EIGRP в своєму обладнанні для взаємодії з маршрутизаторами Cisco і інших виробників, що підтримують протокол EIGRP. Але додаткові функції EIGRP, наприклад тупикова мережа EIGRP, необхідні для розгортання динамічної многоточечной віртуальної приватної мережі (DMVPN), не будуть представлені в IETF. Компанія Cisco продовжить підтримку EIGRP у вигляді інформаційного документа RFC.

Протокол EIGRP включає можливості як протоколів маршрутизації з урахуванням стану каналів, так і протоколів на базі векторів відстані. Але EIGRP як і раніше заснований на ключовому принципі протоколу маршрутизації на основі векторів відстані, в рамках якого інформація про решту мережі надходить від безпосередньо підключених сусідніх маршрутизаторів.

EIGRP - це вдосконалений протокол маршрутизації на основі векторів відстані, що підтримує функції, відсутні в інших протоколах маршрутизації на основі векторів відстаней, таких як RIP і IGRP.

Алгоритм дифузійного поновлення (DUAL)

Центром протоколу маршрутизації EIGRP є обчислювальний алгоритм дифузійного поновлення DUAL (Diffusing Update Algorithm), керуючий цим протоколом. Алгоритм DUAL гарантує наявність маршрутів без петель і резервних маршрутів для всього домену маршрутизації. Використовуючи DUAL, протокол EIGRP зберігає всі доступні резервні маршрути до мереж призначення, що дозволяє при необхідності швидко перемикатися на запасні маршрути.

Встановлення відносин суміжності з сусідніми пристроями

EIGRP встановлює відносини з безпосередньо підключеними маршрутизаторами, на яких також включена підтримка EIGRP. Відносини суміжності з сусідніми пристроями використовуються для відстеження статусу цих сусідніх пристроїв.

Надійний транспортний протокол (Reliable Transport Protocol, RTP)

Надійний транспортний протокол (RTP) є унікальним для EIGRP, забезпечуючи доставку пакетів EIGRP сусіднім маршрутизаторам. RTP і відстеження відносин суміжності з сусідніми пристроями створюють основу для роботи алгоритму DUAL.

Часткові і обмежені поновлення

Для оновлень протоколу EIGRP використовуються терміни «часткове» і «обмежене». На відміну від RIP, EIGRP не надсилає періодичних оновлень, і записи маршрутів не застарівають. Термін «часткове» означає, що оновлення містить тільки дані про зміни маршрутів, наприклад про новий каналі або про канал, який став недоступним. Термін «обмежене» відноситься до поширення часткових оновлень, які відправляються тільки тим маршрутизаторам, на роботу яких впливають ці зміни. Це знижує вимоги до пропускної спроможності, необхідної для передачі оновлень EIGRP.

Розподіл навантаження з рівної і нерівній вартістю

EIGRP підтримує розподіл навантаження з рівною вартістю і розподіл навантаження з нерівній вартістю, що дозволяє адміністраторам краще розподіляти потік трафіку в керованих мережах.

Примітка. У частині застарілої документації для визначення EIGRP використовується термін «гібридний протокол маршрутизації». Але цей термін вводить в оману, оскільки протокол EIGRP не є гібридом між протоколом на основі векторів відстані і протоколом маршрутизації з урахуванням стану каналів. EIGRP є виключно протоколом маршрутизації на основі векторів відстані, тому компанія Cisco більше не використовує цей термін для позначення даного протоколу.

Типы протоколов маршрутизации

	Протоколы внутренней маршрутизации				Протоколы внешней маршрутизации
	Протоколы маршрутизации на основе векторов расстояния		Протоколы маршрутизации на основе состояния каналов		Вектор пути
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	протокол RIPng	EIGRP для IPv6	OSPFv3	IS-IS для IPv6	BGP-4 для IPv6

Рис. 5.6.1

Протоколозалежні модулі

EIGRP підтримує можливість маршрутизації ряду інших протоколів, в тому числі IPv4 і IPv6, використовуючи протоколозавісімие модулі (protocol-dependent module, PDM). Хоча тепер це і застаріло, EIGRP також використовує модулі PDM для маршрутизації протоколів мережевого рівня IPX компанії Novell і AppleTalk компанії Apple Computer.

Модулі PDM відповідають за завдання, пов'язані з конкретним протоколом мережевого рівня. Прикладом є модуль EIGRP, який використовується для передачі і отримання пакетів EIGRP, інкапсульованих в IPv4. Цей модуль також відповідає за аналіз пакетів і EIGRP і передачу в алгоритм DUAL нових отриманих даних. EIGRP використовує алгоритм DUAL для прийняття рішень про маршрутизації, але результати зберігаються в таблиці маршрутизації IPv4.

Модулі PDM відповідають за конкретні завдання маршрутизації для кожного протоколу мережевого рівня, в числі яких:

- ведення для маршрутизаторів EIGRP таблиць сусідніх пристроїв і топології, що відносяться до цього сімейства протоколів;
- створення пакетів конкретного протоколу та їх перетворення для алгоритму DUAL;
- забезпечення взаємодії між алгоритмом DUAL і таблицею маршрутизації конкретного протоколу;
- обчислення метрики і передача цих відомостей в алгоритм DUAL;
- реалізація списків фільтрації і доступу;
- виконання функцій перерозподілу між EIGRP і іншими протоколами маршрутизації;
- перерозподіл маршрутів, отриманих іншими протоколами маршрутизації.

Виявивши нове сусіднє пристрій, маршрутизатор вносить запис, що містить адресу і інтерфейс сусіднього пристрою, в таблицю сусідніх пристроїв. Для кожного модуля, що залежить від протоколу, наприклад для IPv4, ведеться одна таблиця сусідніх пристроїв. Для протоколу EIGRP також ведеться таблиця топології. Таблиця топології містить всі мережі призначення, оголошені сусідніми маршрутизаторами. Таблиця топології також ведеться окремо для кожного PDM.

Рис. 5.6.2

Надійний транспортний протокол (Reliable Transport Protocol, RTP)

Протокол EIGRP використовує надійний транспортний протокол (RTP) для доставки і отримання пакетів EIGRP. EIGRP був розроблений як протокол маршрутизації, незалежний від мережевого рівня. Через цю архітектури EIGRP не може використовувати служби UDP або TCP. Це дозволяє використовувати EIGRP і для протоколів, що не входять в сімейство протоколів TCP / IP, таких як IPX і AppleTalk. На малюнку показаний принцип роботи RTP.

Хоча в назву RTP входить слово «надійний», цей протокол забезпечує як надійну, так і ненадійну доставку пакетів EIGRP, аналогічно TCP і UDP, відповідно. Надійний пакет RTP вимагає, щоб відправник повертав одержувачу підтвердження. Для ненадійного пакета RTP підтвердження не потрібно. Наприклад, пакет поновлення EIGRP відправляється по RTP надійним чином і вимагає підтвердження. Пакет вітання EIGRP також відправляється по RTP, але ненадійним чином. Це означає, що пакети вітання EIGRP не вимагають підтвердження.

RTP може відправляти пакети EIGRP, використовуючи одноадресних передачу або групову розсилку.

В пакетах групового розсилання EIGRP для IPv4 використовується зарезервований IPv4-адрес групової розсилки 224.0.0.10.

Пакети групового розсилання EIGRP для IPv6 відправляються на зарезервований IPv6-адреса FF02 :: A.

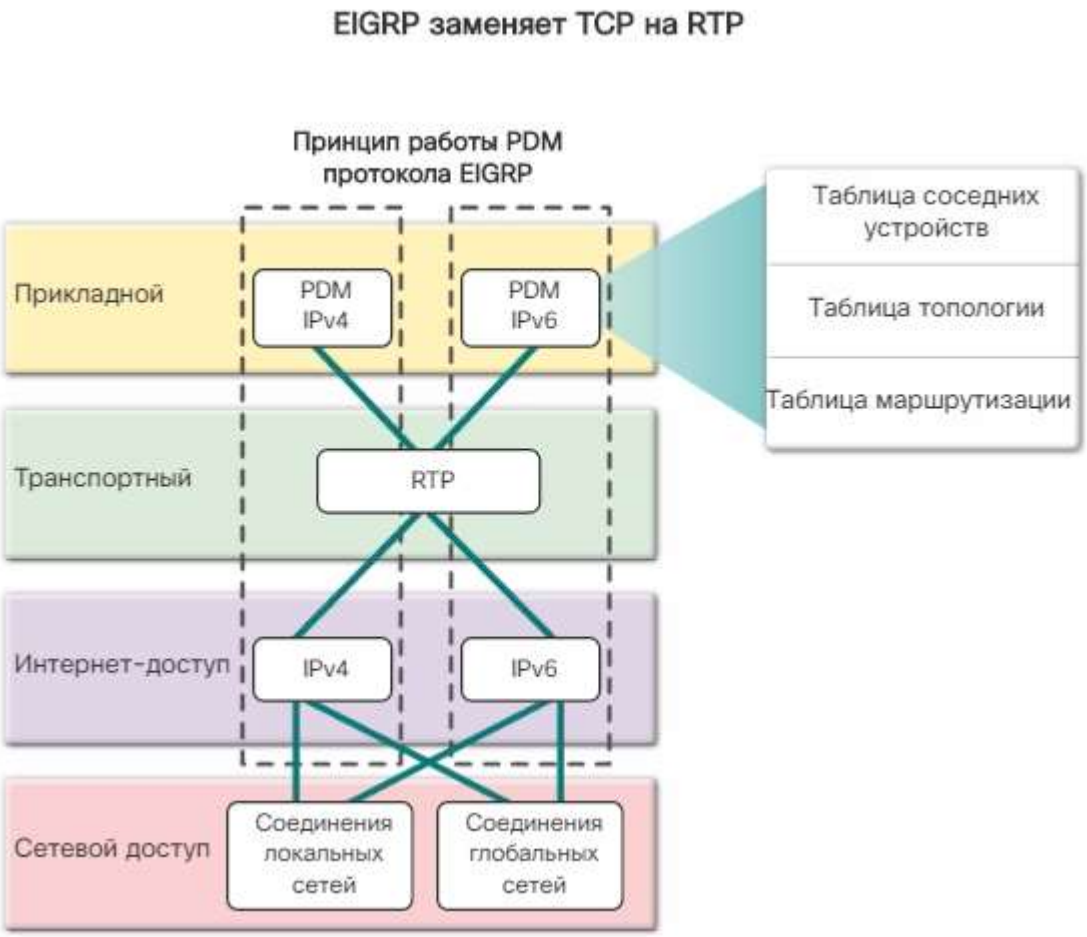


Рис. 5.6.3

Аутентифікація

Як і для інших протоколів маршрутизації, для EIGRP може бути налаштована аутентифікація. Для кожного з протоколів RIPv2, EIGRP, OSPF, IS-IS і BGP може бути налаштована аутентифікація відповідної інформації про маршрути.

Рекомендується використовувати аутентифікацію переданої інформації про маршрути. Це гарантує, що маршрутизатори будуть приймати інформацію про маршрути від інших маршрутизаторів, тільки якщо на цих маршрутизаторах налаштовані однакові пароль або параметри аутентифікації.

Примітка. Аутентифікація не забезпечує шифрування оновлень маршрутизації EIGRP.

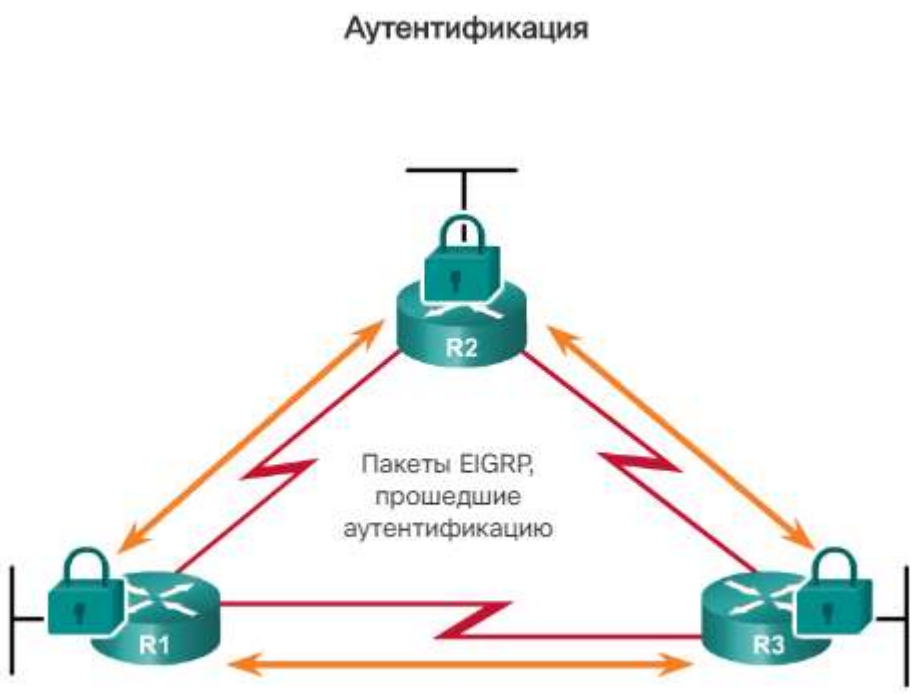


Рис. 5.6.4

Протокол EIGRP використовує п'ять різних типів пакетів, деякі з яких використовуються парами. Пакети EIGRP передаються за допомогою яких надійної, або ненадійною доставки RTP і можуть бути відправлені як одноадресні пакети, як пакети групової розсилки, а іноді і як пакети обох видів. Типи пакетів EIGRP також називаються форматами пакетів EIGRP або повідомленнями EIGRP.

Як показано на рис. 1, до п'яти типам пакетів EIGRP відносяться наступні типи:

Рис. 5.6.5

Пакети вітання EIGRP

EIGRP використовує невеликі пакети вітання в безпосередньо підключених каналах для виявлення інших маршрутизаторів з підтримкою EIGRP. Пакети вітання використовуються маршрутизаторами для створення відносин суміжності з сусідніми пристроями EIGRP.

Пакети вітання EIGRP відправляються як групові розсилки IPv4 або IPv6, використовуючи ненадійну доставку RTP. Це означає, що абонент не надсилає у відповідь пакет підтвердження.

Зарезервованим адресою групової розсилки EIGRP для IPv4 є 224.0.0.10.

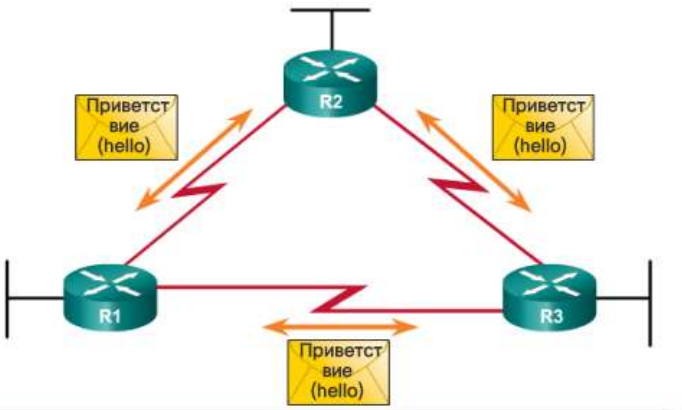
Зарезервованим адресою групової розсилки EIGRP для IPv6 є FF02 :: A.

За допомогою пакетів вітання маршрутизатори EIGRP виявляють сусідні пристрої і встановлюють відносини суміжності з сусідніми маршрутизаторами. У більшості мереж пакети вітання EIGRP відправляються як пакети групової розсилки кожні 5 секунд. Але в багатоточкових, нешироковещательнимі мережах з множинним доступом (nonbroadcast multiple access, NBMA), таких як X.25, Frame Relay і інтерфейси ATM (Asynchronous Transfer Mode) з каналами доступу T1 (1,544 Мбіт / с) або менш швидкісними, пакети вітання передаються як одноадресні пакети кожні 60 секунд.

У EIGRP пакети вітання також використовуються для підтримки встановлених відносин суміжності. Маршрутизатор EIGRP вважає, що поки надходять пакети вітання від сусіднього маршрутизатора, сусідній маршрутизатор і його маршрути залишаються працездатними.

Протокол EIGRP використовує таймер утримання, щоб визначити максимальний час очікування маршрутизатором отримання наступного пакета вітання, перш ніж відповідний сусідній маршрутизатор буде оголошений недоступним. За замовчуванням час утримання одно триразовому інтервалу передачі пакета вітання, або 15 з в більшості мереж і 180 з в низькошвидкісних мережах NBMA. Після закінчення часу утримання EIGRP оголошує маршрут неактивним, а алгоритм DUAL виконує пошук нового шляху, відправляючи відповідні запити.

Значения по умолчанию для интервалов приветствия и времени удержания для EIGRP



Пропускная способность	Пример канала	Интервал приветствия по умолчанию	Время удержания по умолчанию
1,544 Мбит/с	Многоточечный Frame Relay	60 секунд	180 секунд
Более 1,544 Мбит/с	T1, Ethernet	5 секунд	15 секунд

Рис. 5.6.6

EIGRP передає пакети оновлень, щоб поширити інформацію про маршрутах. Пакети оновлень відправляються тільки в разі потреби. Оновлення EIGRP містять тільки необхідну інформацію про маршрути і відправляються тільки тим маршрутизаторам, яким ці оновлення потрібні.

На відміну від RIP, EIGRP (інший протокол маршрутизації на основі векторів відстані) залишають поза передачею періодичних оновлень, і записи маршрутизації не втрачають актуальності. Замість цього EIGRP передає інкрементні поновлення тільки при зміні стану мережі призначення. Це може відбуватися, коли нова мережа стає доступною, коли існуюча мережа стає недоступною або коли виникають зміни метрики маршрутизації існуючої мережі.

Для оновлень протоколу EIGRP використовуються терміни часткове і обмежене. Термін «часткове» означає, що оновлення містить тільки дані про зміни маршрутів. Термін «обмежене» відноситься до поширення часткових оновлень, які відправляються тільки тим маршрутизаторам, на роботу яких впливають ці зміни.

Передаючи тільки ту інформацію про маршрути, яка необхідна, і тільки тим маршрутизаторам, яким вона необхідна, протокол EIGRP знижує вимоги до пропускної спроможності, необхідної для передачі оновлень EIGRP.

Для пакетів оновлень EIGRP використовується надійна доставка, тобто відправляє маршрутизатор вимагає підтвердження. Пакети оновлень відправляються як пакети групової розсилки, коли вони потрібні декільком маршрутизаторів, або як одноадресні, якщо вони потрібні тільки одного маршрутизатора. На малюнку, оскільки використовуються канали «точка-точка», поновлення відправляються як одноадресні.

При використанні надійної доставки EIGRP передає пакети підтверджень (ACK). Підтвердження EIGRP є пакет вітання EIGRP без даних. RTP використовує надійну передачу для пакетів оновлень, запитів і відповідей EIGRP. Пакети підтверджень EIGRP завжди відправляються як одноадресні пакети з ненадійною доставкою. Сенс ненадійною доставки полягає в тому, щоб уникнути нескінченного циклу підтверджень.

На малюнку маршрутизатор R2 втратив підключення до локальної мережі, підключеної до його інтерфейсу Gigabit Ethernet. Маршрутизатор R2 негайно посилає маршрутизаторів R1 і R3 оновлення, що повідомляє про відмовив маршруті. Маршрутизатор R1 і R3 відповідають підтвердженням, щоб повідомити маршрутизатора R2 про отримання ними оновлення.

Примітка. В деякій документації пакети вітання та підтвердження розглядаються як один тип пакетів EIGRP.

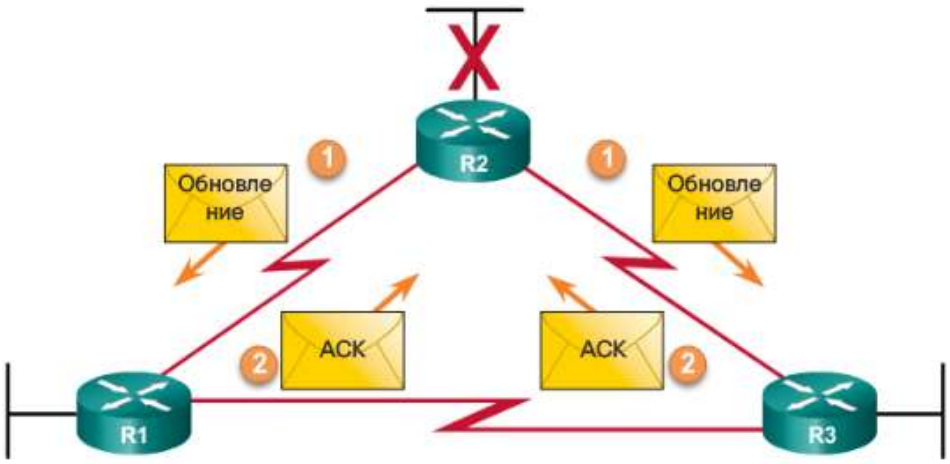


Рис. 5.6.7

Алгоритм DUAL використовує пакети запитів для пошуку мереж і виконання інших завдань. Для запитів і відповідей використовується надійна доставка. Для запитів може використовуватися групова розсилка або одноадресная передача, а відповіді завжди передаються у вигляді одноадресних пакетів.

На малюнку маршрутизатор R2 втратив підключення до локальної мережі і відправляє всім сусіднім пристроїв EIGRP запити пошуку всіх можливих маршрутів до цієї локальної мережі. Оскільки для запитів використовується надійна доставка, який одержує маршрутизатор повинен передати підтвердження EIGRP. Це підтвердження повідомляє відправнику про отримання адресатом повідомлення запиту. Щоб спростити цей приклад, підтвердження на малюнку були опущені.

Пакети відповідей EIGRP

Відповідь повинні відправити всі сусідні пристрої, незалежно від наявності у них маршруту до відключеною мережі. Оскільки для відповідей також використовується надійна доставка, маршрутизатори, такі як R2, повинні відправляти підтвердження.

Причина, по якій маршрутизатор R2 відправляє запит про мережі, яка, як йому стало відомо, відмовила, може здатися неочевидній. Фактично не працює тільки інтерфейс маршрутизатора R2, який підключений до цієї мережі. Інший маршрутизатор може бути підключений до цієї ж локальної мережі, надаючи альтернативний шлях до неї. Тому маршрутизатор R2 відправляє запит пошуку такого маршрутизатора, перш ніж повністю видалити мережу зі своєї таблиці топології.

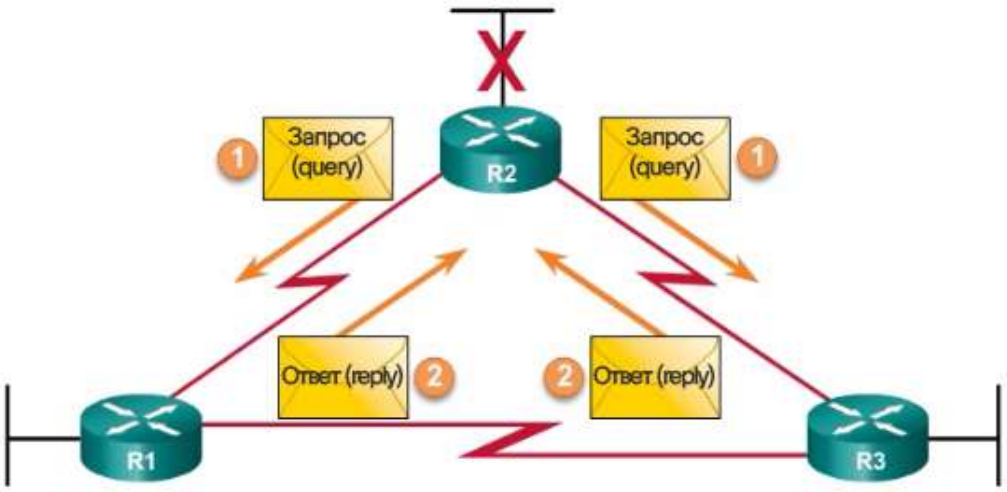


Рис. 5.6.8

Інкапсуляція повідомлень EIGRP

Частина даних повідомлення EIGRP инкапсулируется в пакет. Це поле даних називається «тип, довжина, значення» (type, length, value, TLV). Типами TLV, що відносяться до цього курсу, є параметри EIGRP, внутрішні маршрути IP і зовнішні маршрути IP.

У кожен пакет EIGRP, незалежно від типу, додається заголовок пакета EIGRP. Потім заголовок пакета EIGRP і TLV инкапсулируются в пакет IPv4. У заголовку пакета IPv4 поле протоколу встановлюється рівним значенню 88, визначаючи EIGRP, а адреса призначення IPv4 встановлюється рівним адресою групової розсилки 224.0.0.10. Якщо пакет EIGRP инкапсулируется в кадр Ethernet, MAC-адресу призначення також є адресою групової розсилки, 01-00-5E-00-00-0A.

Заголовок пакета EIGRP і TLV

Кожне повідомлення EIGRP містить заголовок, як показано на рис. 1. До важливих полях відносяться поле Opcode (код операції) і поле Autonomous System Number (номер автономної системи). Поле Opcode визначає тип пакета EIGRP наступним чином:

- оновлення
- Запит (query)
- Відповідь (reply)
- Привітання (hello)

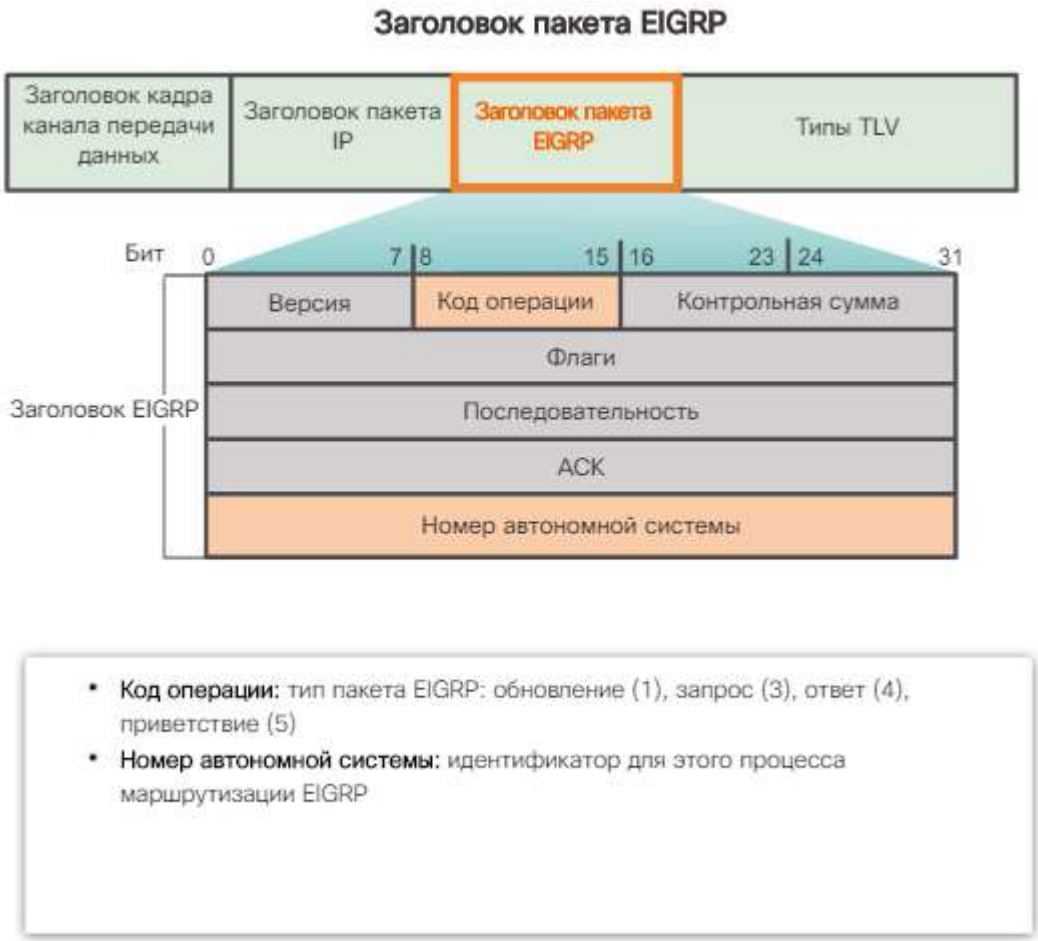


Рис. 5.6.9

Номер автономної системи визначає процес маршрутизації EIGRP. На відміну від RIP, в мережі можуть працювати кілька примірників EIGRP. Номер автономної системи використовується для відстеження кожного працюючого процесу EIGRP.

На рис. 2 показано поле TLV параметра EIGRP. Повідомлення параметра EIGRP містить вагу, який використовується EIGRP для своєї складовою метрики. За умовчанням як ваги враховуються тільки пропускна здатність і затримка. Обидва цих параметра використовуються з однаковою вагою. Тому обидва поля (K1 для пропускної здатності і K3 для затримки) встановлені рівними одиниці (1). Інші значення K встановлені рівними нулю (0).

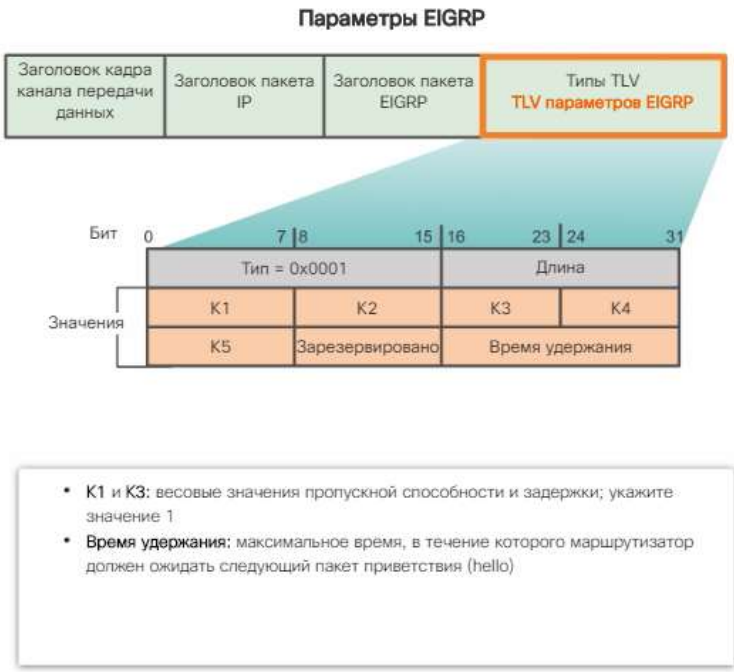


Рис. 5.6.10

Час утримання - це час, протягом якого сусідній маршрутизатор EIGRP, який отримав це повідомлення, повинен чекати, перш ніж вважати оголошує маршрутизатор недоступним.

На рис. 3 показано поле TLV внутрішніх маршрутів IP. Внутрішнє повідомлення IP використовується для оголошення маршрутів EIGRP в межах автономної системи. До важливих полях відносяться поля метрик (затримка і пропускна здатність), поле маски підмережі (довжина префікса) і поле призначення.

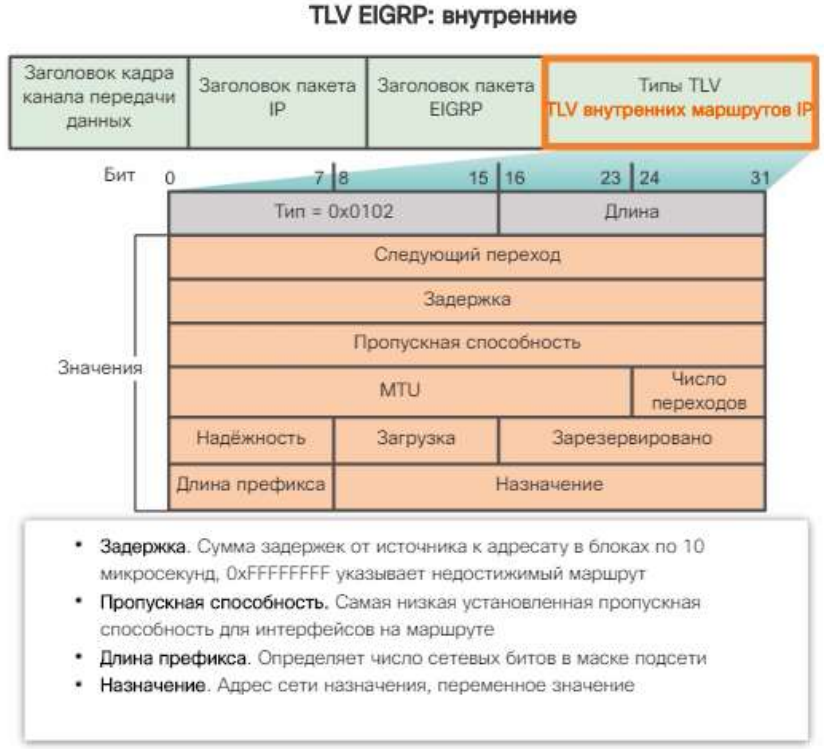


Рис. 5.6.11

Затримка розраховується як сума затримок від джерела до адресата в блоках по 10 мікросекунд. Пропускна здатність - це найнижча встановлена пропускна здатність для інтерфейсів на маршруті.

Маска підмережі визначається як довжина префікса або число бітів мережі в масці підмережі. Наприклад, довжина префікса для маски підмережі 255.255.255.0 дорівнює 24, оскільки число бітів мережі дорівнює 24.

Адреса мережі призначення зберігається в поле Destination (призначення). Хоча на цьому малюнку показано тільки 24 біта, це поле залежить від значення мережевої частини 32-бітного мережевого адреси. Наприклад, мережева частина 10.1.0.0/16 дорівнює 10.1, тому в поле Destination (призначення) зберігаються перші 16 біт. Оскільки мінімальна довжина цього поля дорівнює 24 бітам, решта поля заповнюється нулями. Якщо адреса мережі довше 24 біт (наприклад, 192.168.1.32/27), поле Destination (призначення) розширюється для інших 32 біт (всього 56 біт) і невикористовувані біти заповнюються нулями.

На рис. 4 показано поле TLV зовнішніх маршрутів IP. Зовнішнє повідомлення IP використовується при імпорті зовнішніх маршрутів в процес маршрутизації EIGRP. У даному розділі EIGRP буде імпортуватися або перерозподілятися статичний маршрут за замовчуванням. Зверніть увагу, що нижня половина TLV зовнішніх маршрутів IP містить всі поля, використовувані TLV внутрішніх IP.

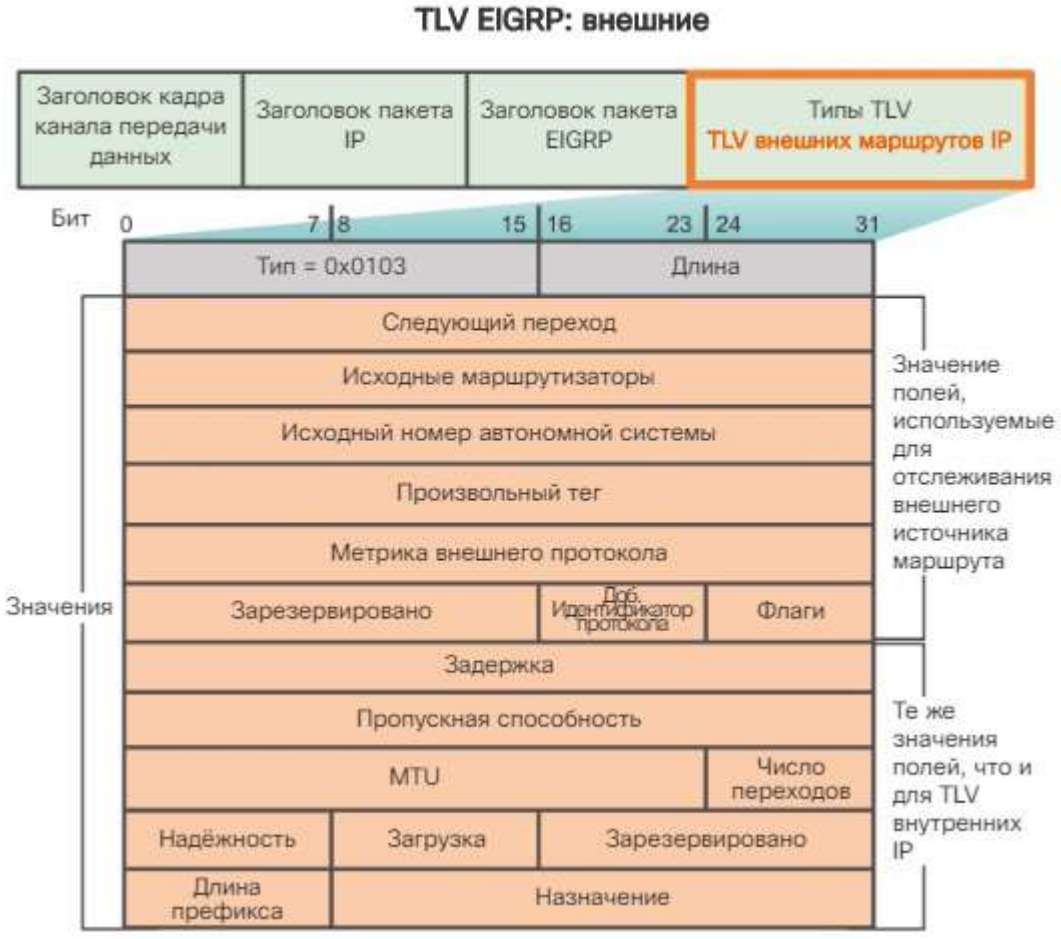


Рис. 5.6.12

Примітка. Максимальний розмір пакета (MTU) не є метрикою використовуваної EIGRP. MTU включається в оновлення маршрутів, але не використовується для визначення метрики маршрутизації.

На рис. 1 показана топологія, яка в цьому курсі для настройки EIGRP для IPv4. Типи послідовних інтерфейсів і пов'язаних з ними пропускних спроможностей не обов'язково відображають найбільш поширені типи

підключень, що застосовуються в сучасних мережах. Пропускні спроможності послідовних каналів, використовуваних в цій топології, були обрані, щоб допомогти пояснити розрахунок метрик протоколу маршрутизації і процес вибору оптимального шляху.

EIGRP для топологии IPv4

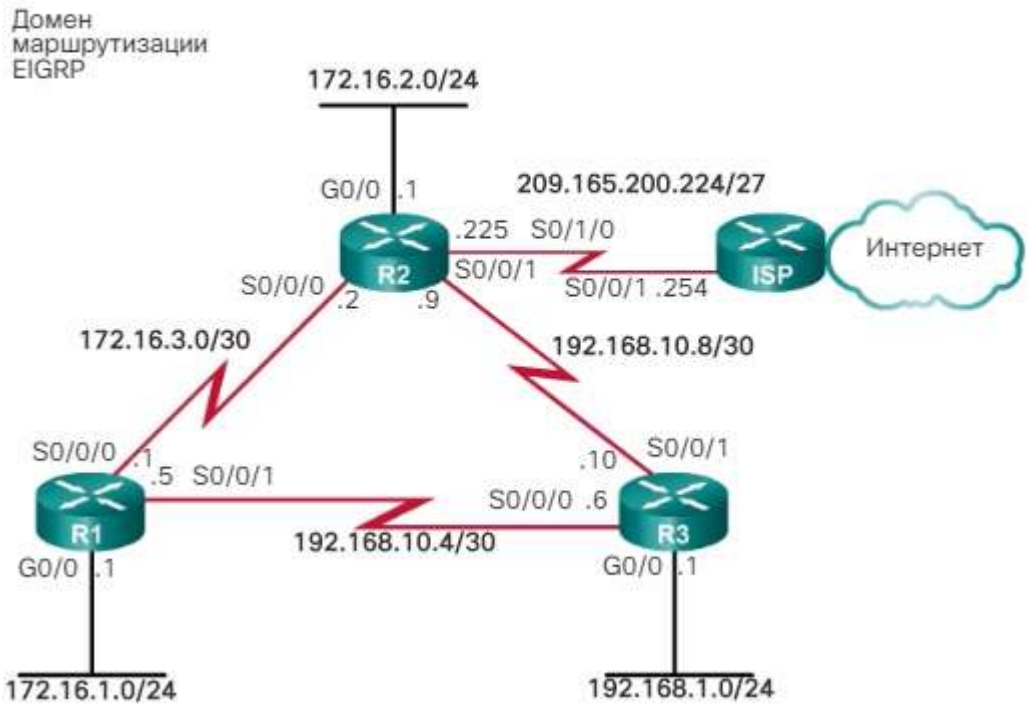


Рис. 5.6.13

Для маршрутизаторів в цій топології задана початкова конфігурація, в тому числі адреси інтерфейсів. В даний час на жодному з маршрутизаторів не настроєна статична або динамічна маршрутизація.

На рис. 2, 3 і 4 показані конфігурації інтерфейсів для трьох маршрутизаторів EIGRP в цій топології. Тільки маршрутизатори R1, R2 і R3 є частиною домену маршрутизації EIGRP. Маршрутизатор ISP використовується в якості шлюзу домену маршрутизації в Інтернет.

Конфигурация интерфейса для маршрутизатора R1

```
R1# show running-config
 <выходные данные опущены>
!
interface GigabitEthernet0/0
 ip address 172.16.1.1 255.255.255.0
!
interface Serial0/0/0
 ip address 172.16.3.1 255.255.255.252
clock rate 64000
!
interface Serial0/0/1
 ip address 192.168.10.5 255.255.255.252
```

Рис. 5.6.14

Конфигурация интерфейса для маршрутизатора R2

```
R2# show running-config
 <выходные данные опущены>
!
interface GigabitEthernet0/0
 ip address 172.16.2.1 255.255.255.0
!
interface Serial0/0/0
 ip address 172.16.3.2 255.255.255.252
!
interface Serial0/0/1
 ip address 192.168.10.9 255.255.255.252
 clock rate 64000
!
interface Serial0/1/0
 ip address 209.165.200.225 255.255.255.224
```

Рис. 5.6.15

Конфигурация интерфейса для маршрутизатора R3

```
R3# show running-config
 <выходные данные опущены>
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
 ip address 192.168.10.6 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 192.168.10.10 255.255.255.252
```

Рис. 5.6.16

Номери автономних систем

EIGRP використовує команду router eigrp autonomous-system, щоб запустити процес EIGRP. Номер автономної системи, що використовується в конфігурації EIGRP, не пов'язаний з глобально призначеними номерами автономних систем IANA, використовуваними зовнішніми протоколами маршрутизації.

Отже, в чому різниця між глобально призначеним номером автономної системи IANA і номером автономної системи EIGRP?

Глобально призначений номер автономної системи IANA - це сукупність мереж з адміністративним управлінням однієї організацією, що реалізує загальну політику маршрутизації до Інтернету. На малюнку адміністративне управління всіма компаніями A, B, C і D здійснює інтернет-провайдер ISP1. ISP1 забезпечує загальну політику маршрутизації для всіх цих компаній при оголошенні маршрутів до ISP2.

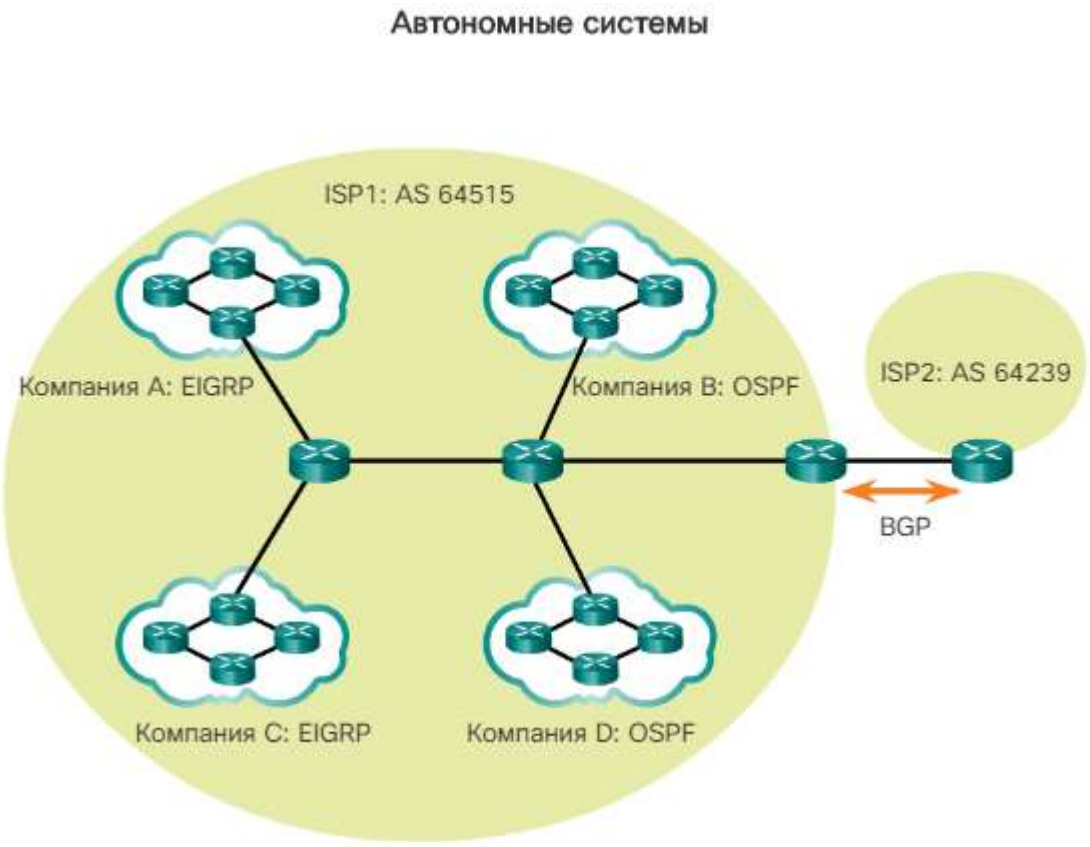


Рис. 5.6.17

Рекомендації по створенню, вибору і реєстрації автономної системи описані в документі RFC 1930. Глобальні номери автономних систем призначаються IANA, тим же органом, який призначає простір IP-адрес. Локальний регіональний реєстр Інтернету (RIR) несе відповідальність за призначення організації номера автономної системи зі свого блоку призначених номерів автономних систем. До 2007 р номера автономних систем були шестнадцатіразрядного числами в діапазоні від 0 до 65 535. Сьогодні призначаються 32-бітові номера автономних систем, що збільшує кількість доступних номерів автономних систем більш ніж до 4 мільярдів.

Зазвичай номер автономної системи потрібно інтернет-провайдерам (ISP), магістральних інтернет-провайдерам і великим установам, підключеним до інших організацій. Ці інтернет-провайдери та великі організації використовують для поширення інформації про маршрутах протокол зовнішньої маршрутизації BGP. BGP - це єдиний протокол маршрутизації, який використовує в своїй конфігурації фактичний номер автономної системи.

Переважній більшості компаній і організацій з IP-мережами номер автономної системи не потрібно, тому що вони управляються більш великою організацією, такий як інтернет-провайдер. Ці компанії використовують для маршрутизації пакетів в своїх мережах протоколи внутрішньої маршрутизації, такі як протоколи RIP, EIGRP, OSPF і IS-IS. Кожна з них є однією з багатьох незалежних і окремих мереж всередині автономної системи інтернет-провайдера. Інтернет-провайдер відповідає за маршрутизацію пакетів всередині своєї автономної системи і між іншими автономними системами.

Номер автономної системи, що використовується в конфігурації EIGRP, важливий тільки для домену маршрутизації EIGRP. Він грає роль

ідентифікатора процесу, щоб допомогти маршрутизаторів відстежувати стан декількох працюючих екземплярів EIGRP. Це необхідно, оскільки в мережі може працювати декілька екземплярів EIGRP. Для кожного примірника EIGRP можна налаштувати підтримку оновлень маршрутизації для різних мереж і обмін цими оновленнями.

Команда маршрутизатора EIGRP

В Cisco IOS входять процеси підтримки і настройки різних типів протоколів динамічної маршрутизації. Команда режиму глобальної конфігурації маршрутизатора router використовується для початку конфігурації будь-якого протоколу динамічної маршрутизації. На рис. 1 показана топологія, яка використовується для демонстрації цієї команди.

EIGRP для топологии IPv4

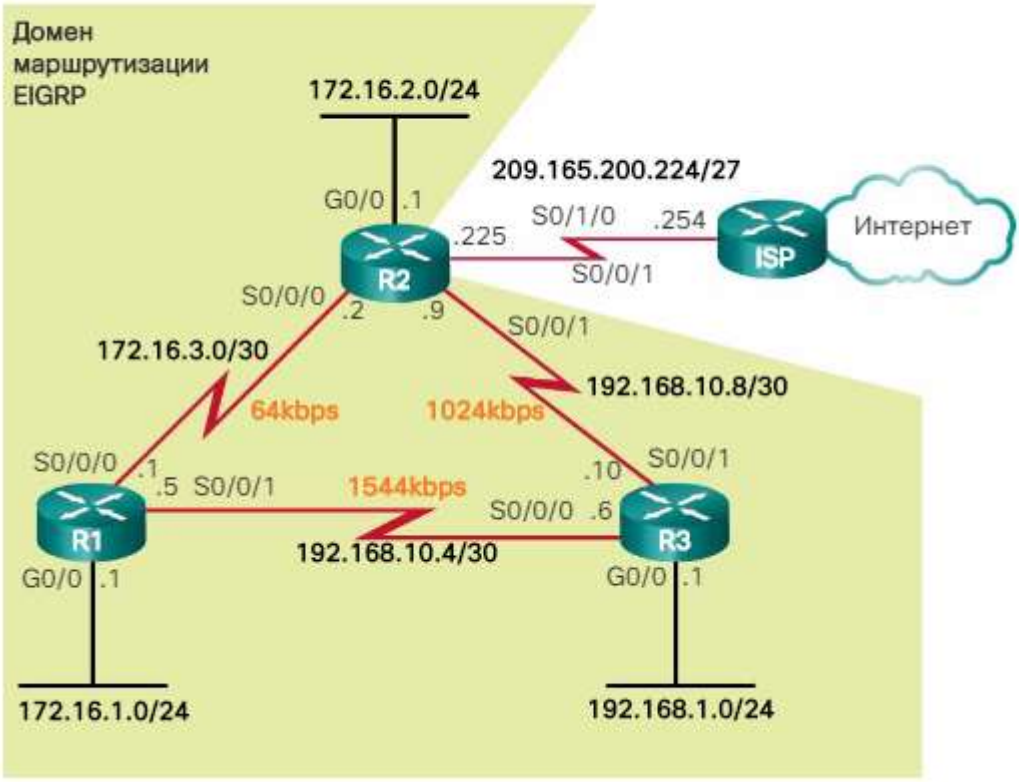


Рис. 5.6.18

Як показано на рис. 2, команда режиму глобальної конфігурації маршрутизатора router зі знаком питання (?) Після неї виводить список всіх доступних протоколів маршрутизації, підтримуваних конкретним випуском IOS, що працює на маршрутизаторі.

Команда конфигурации маршрутизатора

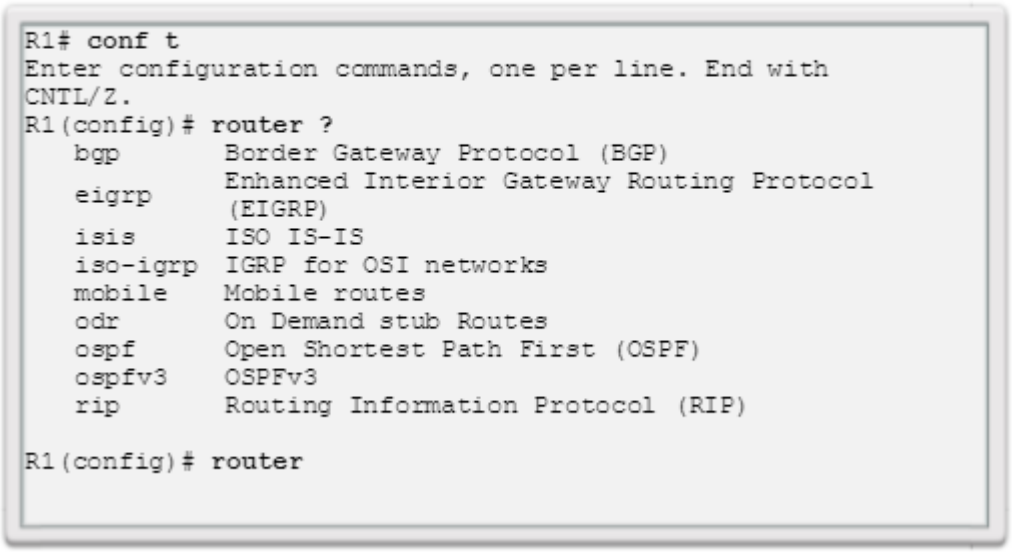


Рис. 5.6.19

Щоб увійти в режим конфігурації і налаштувати EIGRP, використовується наступна команда режиму глобальної конфігурації:

Router (config) # router eigrp autonomous-system

Аргументу autonomous-system може бути призначено будь-Шестнадцатіразрядное значення від 1 до 65 535. Всі маршрутизатори в домені маршрутизації EIGRP повинні використовувати один номер автономної системи.

На рис. 3 показана конфігурація процесу EIGRP на маршрутизаторах R1, R2 і R3. Зверніть увагу, що запрошення змінюється з запрошення режиму глобальної конфігурації на запрошення режиму конфігурації маршрутизатора.

У цьому прикладі 1 визначає цей конкретний процес EIGRP, що працює на цьому маршрутизаторі. Для створення відносин суміжності з сусідніми пристроями EIGRP вимагає, щоб для всіх маршрутизаторів, що знаходяться в одному домені маршрутизації, було поставлено одне і той же номер автономної системи. На рис. 3 цей же протокол EIGRP включений на всіх трьох маршрутизаторах, використовуючи однаковий номер автономної системи 1.

Команда конфигурации маршрутизатора для R1, R2 и R3

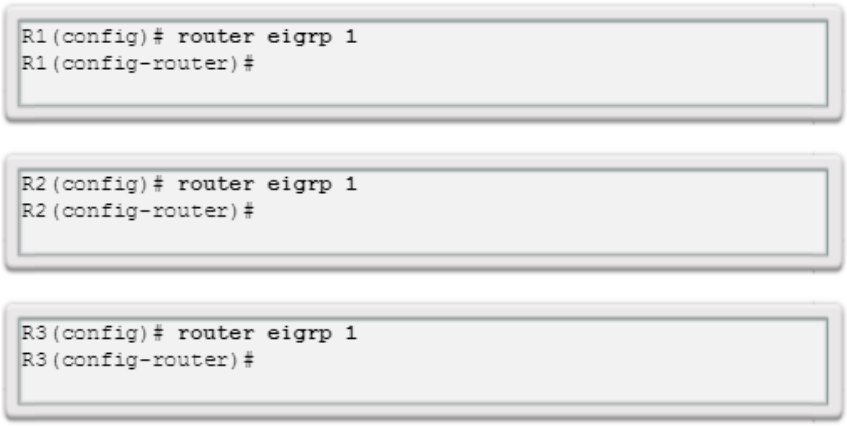


Рис. 5.6.20

Примітка. І для EIGRP, і для OSPF може підтримуватися кілька примірників кожного протоколу маршрутизації, хоча цей тип реалізації кількох протоколів маршрутизації звичайно не потрібно і не рекомендується.

Команда router eigrp autonomous-system працює програмне забезпечення власне процес EIGRP. Маршрутизатор не починає відправляти оновлення. Навпаки, ця команда тільки надає доступ до налаштування параметрів EIGRP.

Щоб відключити і повністю видалити з пристрою настройки EIGRP, використовуйте команду режиму глобальної конфігурації маршрутизатора no router eigrp autonomous-system, яка зупиняє процес EIGRP і видаляє всі існуючі налаштування маршрутизатора EIGRP.

Ідентифікатор маршрутизатора EIGRP

Визначення ідентифікатора маршрутизатора

Ідентифікатор маршрутизатора EIGRP використовується, щоб унікальним чином ідентифікувати кожен маршрутизатор в домені маршрутизації EIGRP. Ідентифікатор маршрутизатора використовується і в EIGRP, і в OSPF, хоча роль ідентифікатора маршрутизатора в OSPF набагато важливіше.

У реалізаціях EIGRP для IPv4 використання ідентифікатора маршрутизатора не так очевидно. EIGRP для IPv4 використовує 32-бітовий ідентифікатор маршрутизатора для визначення вихідного маршрутизатора з метою перерозподілу зовнішніх маршрутів. Необхідність ідентифікатора маршрутизатора стає очевиднішим під час обговорення EIGRP для IPv6. Хоча ідентифікатор маршрутизатора необхідний для перерозподілу, відомості про перерозподіл EIGRP не розглядаються в цьому навчальному курсі. Для цього курсу необхідно тільки зрозуміти, що таке ідентифікатор маршрутизатора і як він виходить.

Маршрутизатор Cisco створюють ідентифікатори маршрутизаторів на основі трьох критеріїв в наступному порядку:

1. Використовуйте адресу IPv4, налаштований за допомогою команди режиму конфігурації маршрутизатора eigrp router-id.

2. Якщо ідентифікатор маршрутизатора не заданий, маршрутизатор вибирає найвищий IPv4-адресу будь-якого з його інтерфейсів loopback.

3. Якщо інтерфейси loopback не налаштовані, маршрутизатор вибирає найвищий активний IPv4-адресу будь-якого зі своїх фізичних інтерфейсів.

Якщо адміністратор не визначив ідентифікатор маршрутизатора явно за допомогою команди eigrp router-id, EIGRP створює власний ідентифікатор маршрутизатора, використовуючи IPv4-адрес або інтерфейсу loopback, або фізичного інтерфейсу. Loopback-адреса - це віртуальний інтерфейс, який після настройки автоматично опиняється у включеному стані. Цей інтерфейс не потрібно включати для EIGRP, тобто його не потрібно додавати ні в одну з команд мережі EIGRP. Але інтерфейс повинен перебувати в активному стані (up / up).

За допомогою вищеописаних критеріїв на рис. показані ідентифікатори маршрутизаторів EIGRP за замовчуванням, які визначаються найвищими активними IPv4-адресами маршрутизаторів.

Топология с идентификаторами маршрутизаторов EIGRP по умолчанию

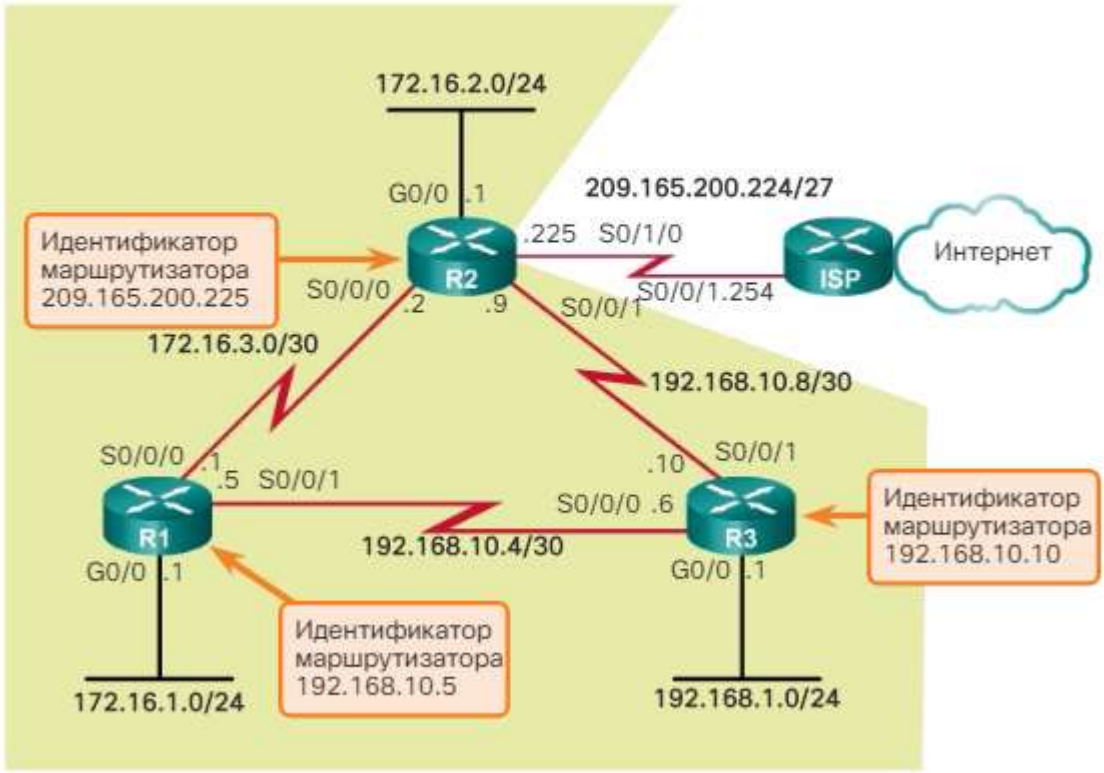


Рис. 5.6.21

Примітка. Щоб налаштувати ідентифікатор маршрутизатора для EIGRP, використовується команда eigrp router-id. Деякі випуски IOS допускають використання команди router-id (ідентифікатор маршрутизатора) без попереднього вказівки eigrp. Але в поточній конфігурації, незалежно від використаної команди, показується eigrp router-id.

Налаштування ідентифікатора маршрутизатора EIGRP

Команда eigrp router-id

Для настройки ідентифікатора маршрутизатора EIGRP використовується команда eigrp router-id, що володіє пріоритетом над усіма IPv4-адресами інтерфейсів loopback або фізичних інтерфейсів. Використовується наступний синтаксис цієї команди:

Router (config) # router eigrp autonomous-system

Router (config-router) # eigrp router-id ipv4-address

Примітка. IPv4-адреса, що використовується для відображення ідентифікатора маршрутизатора, фактично є будь-яким 32-бітових числом, представленим в десятковому форматі з розділовими точками.

В якості ідентифікатора маршрутизатора може бути налаштований будь-яку адресу IPv4 з двома винятками: 0.0.0.0 і 255.255.255.255. Ідентифікатор маршрутизатора повинен бути 32-бітових числом, унікальним в домені маршрутизації EIGRP. В іншому випадку можливі конфлікти маршрутизації.

На рис. 1 показана настройка ідентифікаторів маршрутизаторів EIGRP для маршрутизаторів R1 і R2 за допомогою команди router eigrp autonomous-system.

Настройка идентификаторов для маршрутизаторов R1 и R2

```
R1(config)# router eigrp 1
R1(config-router)# eigrp router-id 1.1.1.1
R1(config-router)#
```

```
R2(config)# router eigrp 1
R2(config-router)# eigrp router-id 2.2.2.2
R2(config-router)#
```

Рис. 5.6.22

Loopback-адреса, що використовується в якості ідентифікатора маршрутизатора

Іншим варіантом задати ідентифікатор маршрутизатора EIGRP є використання IPv4-адреси інтерфейсу loopback. Перевагою використання інтерфейсу loopback замість IPv4-адреси фізичної інтерфейсу є те, що, на відміну від фізичних інтерфейсів, цей інтерфейс ніколи не відмовляє. Не потрібні ні кабелі, ні суміжні пристрої, від яких залежало б включене стан інтерфейсу loopback. Таким чином, використання loopback-адреси в якості ідентифікатора маршрутизатора може забезпечити більш узгоджений ідентифікатор маршрутизатора, ніж використання адреси інтерфейсу.

Якщо команда eigrp router-id не використовується, а інтерфейси loopback налаштовані, EIGRP вибирає найвищий IPv4-адресу будь-якого з інтерфейсів loopback маршрутизатора. Для включення і налаштування інтерфейсу loopback використовуються наступні команди:

Router (config) # interface loopback number

Router (config-if) # IP-address ipv4-address subnet-mask

Примітка. Ідентифікатор маршрутизатора EIGRP не змінюється, поки процес EIGRP не буде видалений командою no router eigrp або поки ідентифікатор маршрутизатора НЕ буде вручну змінений командою eigrp router-id.

Перевірка процесу EIGRP

На рис. 2 показаний результат команди show ip protocols для маршрутизатора R1, в тому числі його ідентифікатор маршрутизатора Команда show ip protocols виводить на екран параметри і поточний стан всіх активних процесів протоколів маршрутизації, включаючи і EIGRP, і OSPF. Команда show ip protocols виводить різні типи результатів для кожного з протоколів маршрутизації.

Проверка идентификатора маршрутизатора R1

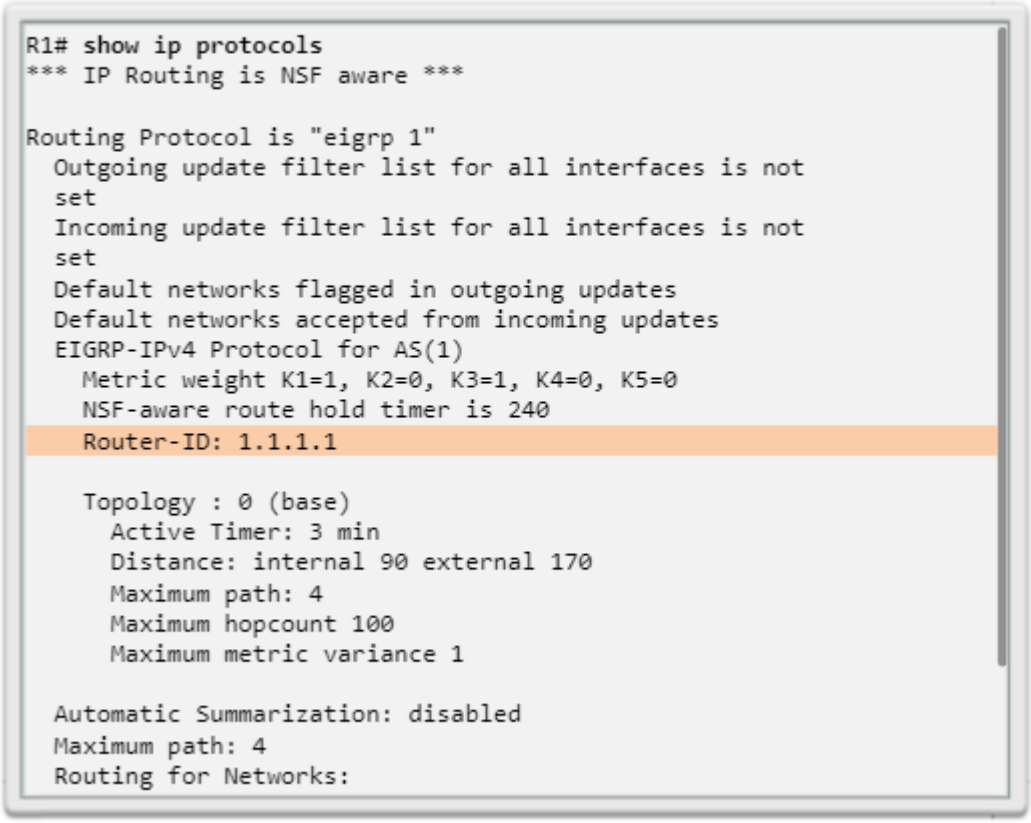


Рис. 5.6.23

Використовуйте засіб перевірки синтаксису Syntax Checker (див. Рис. 3) для настройки і перевірки ідентифікатора маршрутизатора R3.

Примітка. Ідентифікатор маршрутизатора EIGRP не змінюється, поки процес EIGRP не буде видалений командою no router eigrp або поки ідентифікатор маршрутизатора НЕ буде вручну змінений командою eigrp router-id.

Перевірка процесу EIGRP

На рис. показаний результат команди show ip protocols для маршрутизатора R1, в тому числі його ідентифікатор маршрутизатора Команда show ip protocols виводить на екран параметри і поточний стан всіх активних процесів протоколів маршрутизації, включаючи і EIGRP, і OSPF. Команда show ip protocols виводить різні типи результатів для кожного з протоколів маршрутизації.

Команда network

Режим конфігурації маршрутизатора EIGRP забезпечує настройку протоколу маршрутизації EIGRP. На рис. 1 показано, що у всіх маршрутизаторів R1, R2 і R3 є мережі, які повинні бути включені в один домен маршрутизації EIGRP. Щоб включити маршрутизацію EIGRP для інтерфейсу, використовуйте команду в режимі конфігурації маршрутизатора network і введіть для кожної безпосередньо підключеної мережі класовий адреса мережі.

EIGRP для топологии IPv4

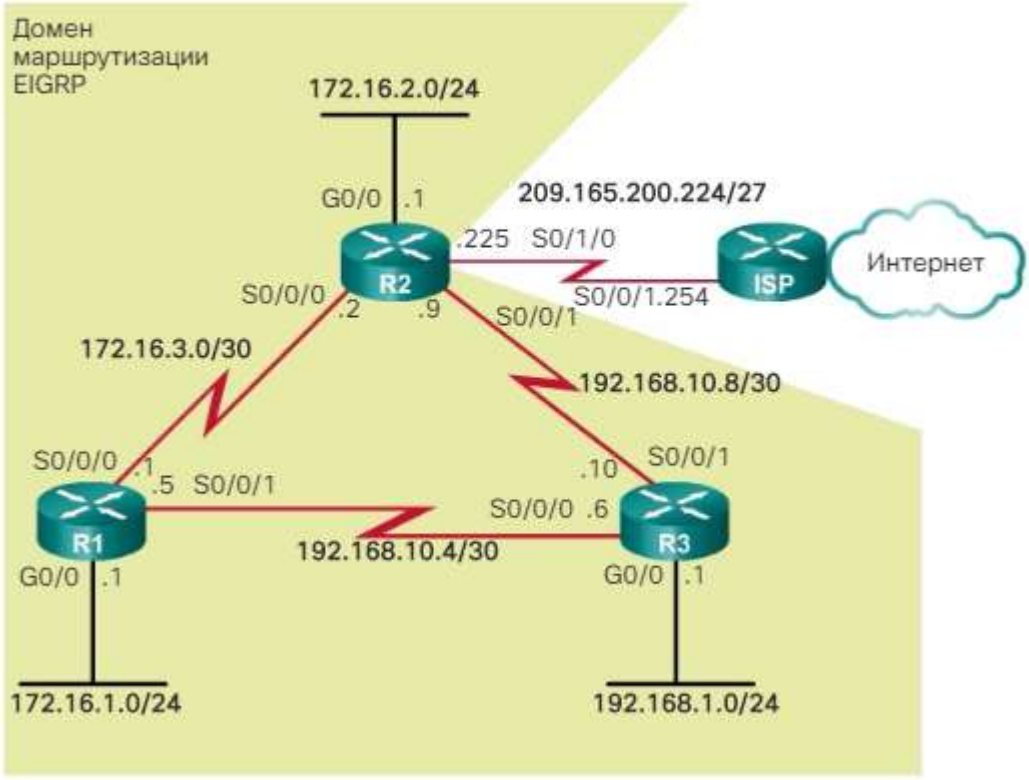


Рис. 5.6.24

Команда network працює так само, як і для інших протоколів маршрутизації IGP. Команда network в EIGRP:

Включає для будь-якого інтерфейсу цього маршрутизатора, відповідного мережевою адресою команди режиму конфігурації маршрутизатора network, відправлення та одержання оновлень EIGRP.

Мережа інтерфейсів включається в оновлення маршрутизації EIGRP.

Router (config-router) # network ipv4-network-address

Аргумент ipv4-network-address - це класовий мережевий IPv4-адрес цього інтерфейсу. На рис. 2 показані команди network, налаштовані для маршрутизатора R1. На малюнку єдина класова інструкція network, network 172.16.0.0, використовується на маршрутизаторі R1 для додавання обох інтерфейсів в підмережі 172.16.1.0/24 і 172.16.3.0/30. Зверніть увагу, що використовується тільки класовий адреса мережі.

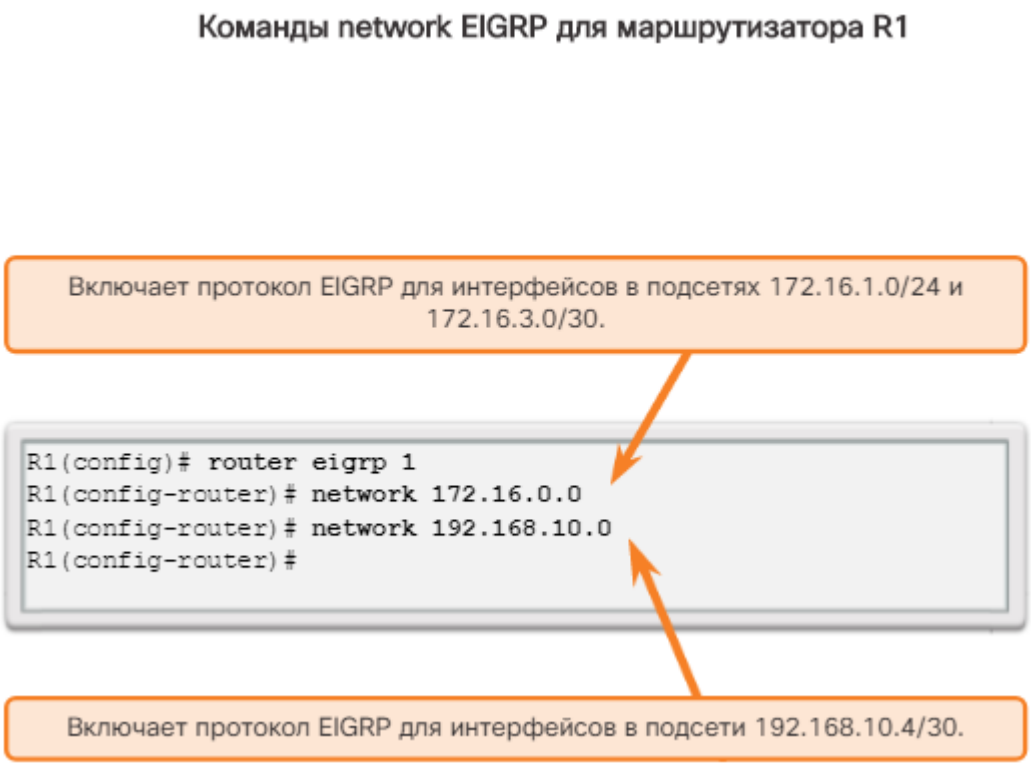


Рис. 5.6.25

На рис. 3 показана команда network, яка використовується, щоб включити EIGRP на інтерфейсах маршрутизатора R2 для підмереж 172.16.1.0/24 і 172.16.2.0/24. Якщо EIGRP налаштований на інтерфейсі S0 / 0/0 маршрутизатора R2, алгоритм DUAL виводить на консоль повідомлення з повідомленням про встановлення для цього інтерфейсу відносини суміжності з іншим маршрутизатором EIGRP. Це нове ставлення суміжності виникає автоматично, так як обидва маршрутизатора, R1 і R2, використовують один і той же номер автономної системи eigrp 1, і обидва маршрутизатора тепер відправляють поновлення для своїх інтерфейсів в мережі 172.16.0.0.

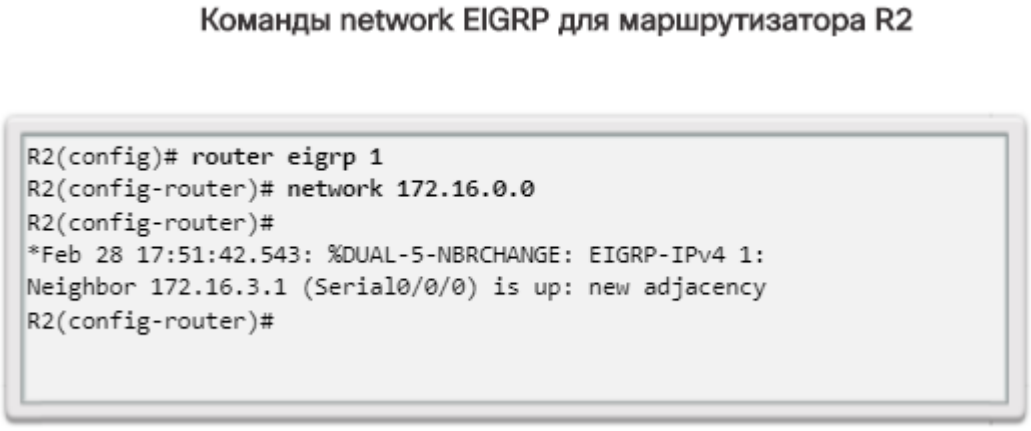


Рис. 5.6.26

За замовчуванням включена команда режиму конфігурації маршрутизатора eigrp log-neighbor-changes. Ця команда використовується для наступних цілей.

Виведення на екран всіх змін для відносин суміжності з сусідніми пристроями EIGRP.

Перевірка відносин суміжності з сусідніми пристроями при конфігурації EIGRP.

Видача рекомендацій адміністратору мережі після видалення відносин суміжності з сусідніми пристроями EIGRP.

Команда network і шаблонна маска

За замовчуванням, використання команди network і мережевого адреси IPv4, наприклад 172.16.0.0, включає EIGRP для всіх інтерфейсів маршрутизатора, що належать цьому класовому адресою мережі. Але можливі ситуації, коли адміністратор мережі не хоче включати EIGRP для всіх інтерфейсів. Як приклад розглянемо ситуацію на малюнку номер 1, де адміністратору потрібно включити EIGRP на маршрутизатор R2, але тільки для підмережі 192.168.10.8 255.255.255.252 на інтерфейсі S0 / 0/1.

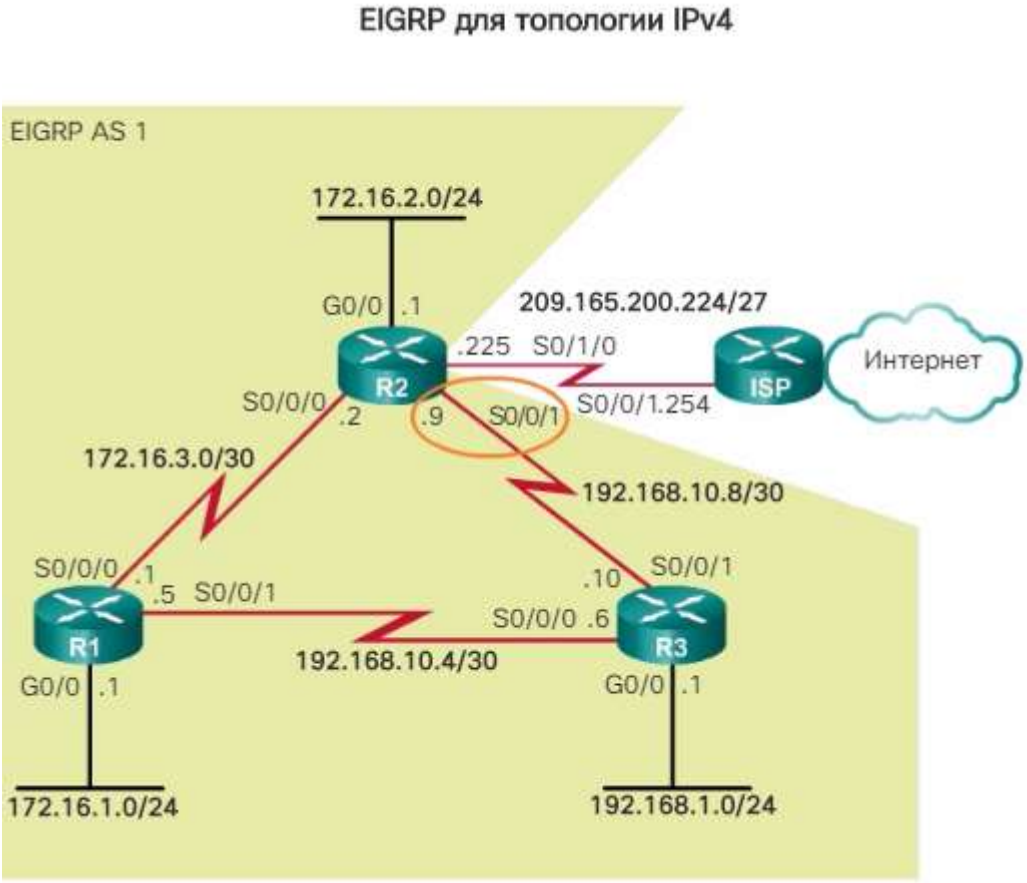


Рис. 5.6.27

Щоб налаштувати EIGRP для оголошення тільки конкретних підмереж, використовуйте з командою network параметр групової маски wildcard-mask:

Router (config-router) # network network-address [wildcard-mask]

Уявіть групову маску як звернення маски підмережі. Зверненням маски підмережі 255.255.255.252 є 0.0.0.3. Для розрахунку звернення маски підмережі відніміть маску підмережі з 255.255.255.255 наступним чином:

255.255.255.255

- 255.255.255.252

---

0. 0.0.0.3 Групова маска

На рис. показано продовження налаштування мережі EIGRP для маршрутизатора R2. Конкретно, команда network 192.168.10.8 0.0.0.3 включає протокол EIGRP на інтерфейсі S0 / 0/1, що входить в підмережа 192.168.10.8 255.255.255.252.

Команда network с шаблонной маской

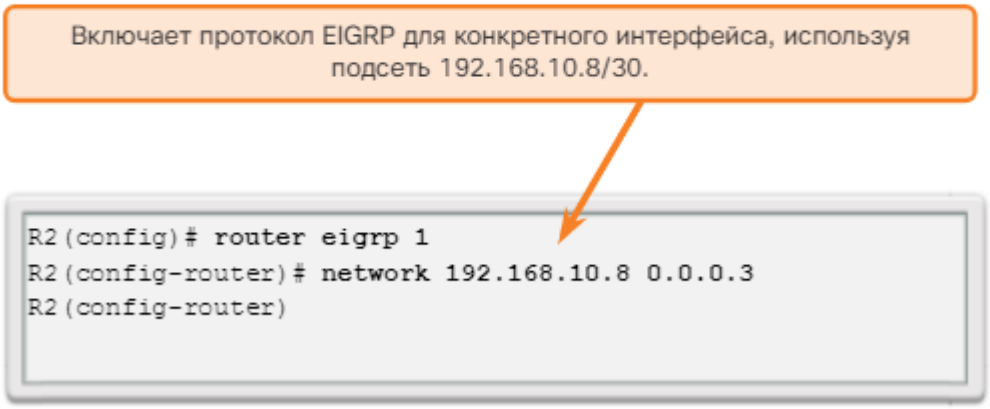


Рис. 5.6.28

Деякі випуски IOS також дозволяють вводити маску підмережі замість групової маски. На рис. 3 наведено приклад налаштування того ж інтерфейсу S0 / 0/1 маршрутизатора R2, але в цей раз за допомогою маски підмережі в команді network. Але якщо використовується маска підмережі, IOS перетворює команду в конфігурації в формат wildcard-mask. Для перевірки можна використовувати результат команди show running-config, показаний на рис. 3.

Альтернативная конфигурация команды network с использованием маски подсети

```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.10.8 255.255.255.252
R2(config-router)# end
R2# show running-config | section eigrp 1
router eigrp 1
 network 172.16.0.0
 network 192.168.10.8 0.0.0.3
 eigrp router-id 2.2.2.2
R2#
```

Рис. 5.6.29

Після включення в мережі EIGRP нового інтерфейсу протокол EIGRP намагається створити відносини суміжності з усіма сусідніми маршрутизаторами для відправки та отримання оновлень EIGRP.

Іноді може знадобитися або виявиться вигідніше додати в оновлення маршрутів EIGRP безпосередньо підключену мережу, але заборонити для цього інтерфейсу створення відносин суміжності з сусідніми пристроями. Для заборони відносин суміжності з сусідніми пристроями можна використовувати команду passive-interface. Існують дві основні причини включення команди passive-interface:

придушити небажаний трафік оновлення, наприклад, коли інтерфейс є інтерфейсом локальної мережі без інших підключених маршрутизаторів;

поліпшити елементи безпеки, наприклад забороняючи невідомим стороннім пристроям маршрутизації отримувати оновлення EIGRP.

На рис. 1 показано, що у інтерфейсів GigabitEthernet 0/0 маршрутизаторів R1, R2 і R3 відсутні сусідні маршрутизатори.

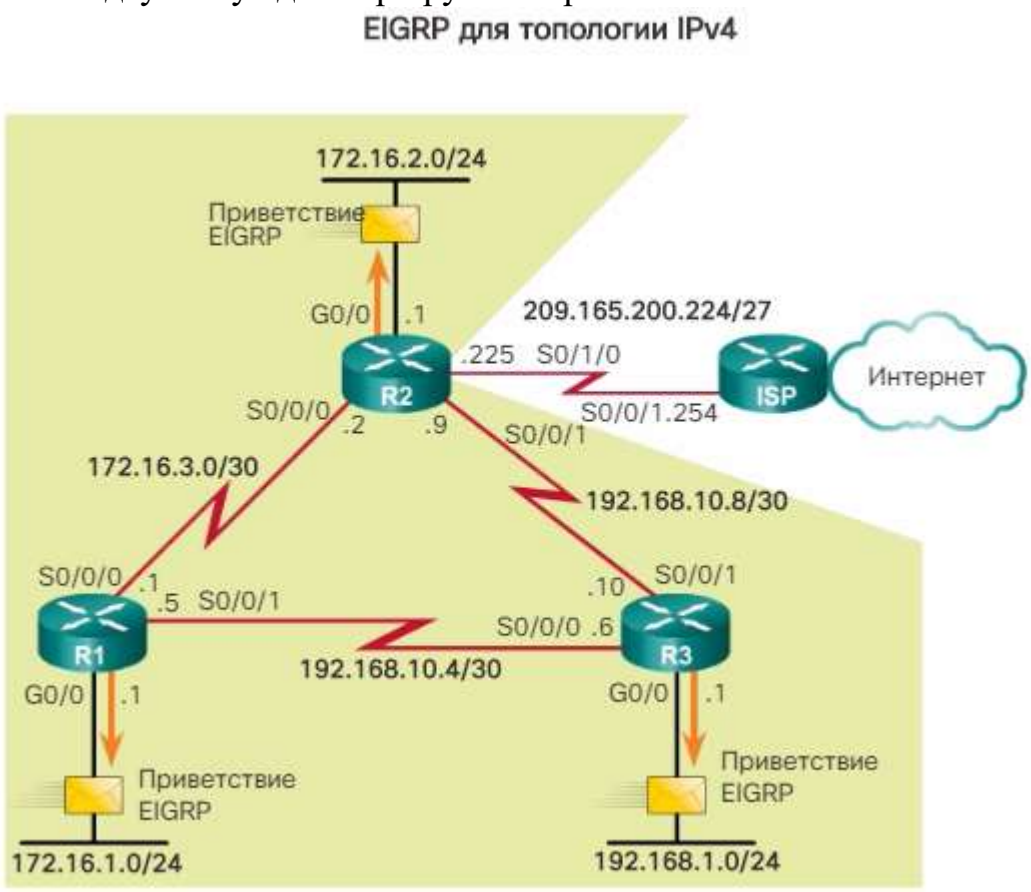


Рис. 5.6.30

Команда режиму конфігурації маршрутизатора passive-interface відключає для цих інтерфейсів передачу та отримання пакетів вітання EIGRP.

Router (config) # router eigrp as-number

Router (config-router) # passive-interface interface-type interface-number

На рис. 2 показана команда passive-interface, налаштована для придушення пакетів вітання в локальних мережах для маршрутизаторів R1 і R3. Маршрутизатор R2 налаштовується за допомогою засобу перевірки синтаксису.

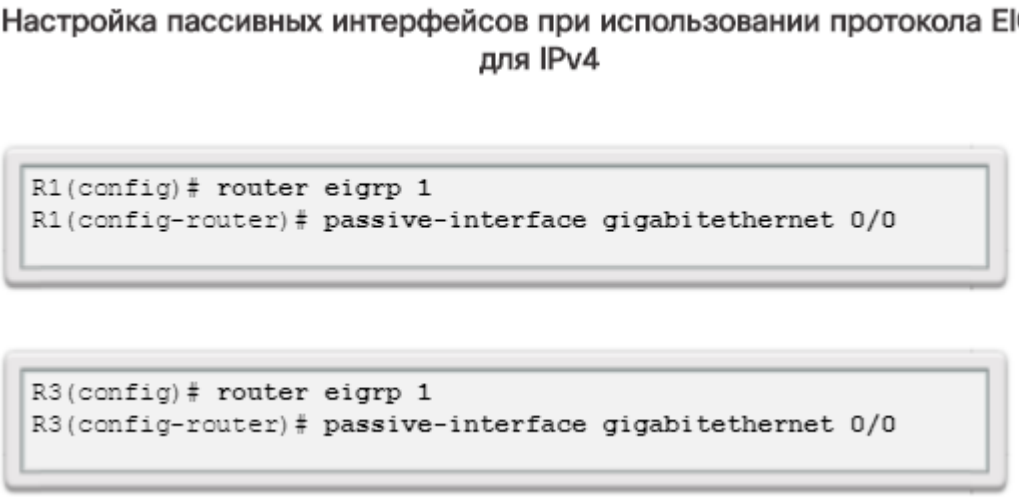


Рис. 5.6.31

Без відносин суміжності з сусідніми пристроями EIGRP не може обмінюватися маршрутами з сусіднім маршрутизатором. Таким чином, команда passive-interface забороняє обмін маршрутами для інтерфейсу. Хоча EIGRP не надсилає і не отримує оновлення маршрутизації через інтерфейс, налаштований за допомогою команди passive-interface, адреса цього інтерфейсу все ще міститься в оновленнях маршрутизації, що відправляються через інші, непассівние інтерфейси.

Примітка. Щоб налаштувати всі інтерфейси як пасивні, використовуйте команду passive-interface default. Щоб відключити інтерфейс як пасивний, використовуйте команду no passive-interface interface-type interface-number.

Прикладом використання пасивного інтерфейсу для підвищення безпеки є ситуація, коли необхідно підключити мережу до мережі сторонньої організації, управління якою недоступно локальному адміністратору, такий як мережу інтернет-провайдера. В цьому випадку адміністратору локальної мережі потрібно оголошувати канал інтерфейсу через власну мережу, але небажано, щоб стороння організація обмінювалася оновленнями маршрутизації з локальним пристроєм маршрутизації, так як це становить небезпеку.

Перевірка пасивного інтерфейсу

Щоб перевірити, чи налаштований інтерфейс маршрутизатора як пасивний, використовуйте команду привілейованого режиму show ip protocols, як показано на рис. 3. Зверніть увагу, що хоча інтерфейс GigabitEthernet 0/0 маршрутизатора R3 є пасивним інтерфейсом, EIGRP як і раніше додає мережеву адресу інтерфейсу мережі 192.168.1.0 в свої відновлення маршрутизації.

Проверка пассивных интерфейсов при использовании протокола EIGRP для IPv4

```
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
<выходные данные опущены>
Routing for Networks:
    192.168.1.0
    192.168.10.4/30
    192.168.10.8/30
  Passive Interface(s):
    GigabitEthernet0/0

  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.10.5          90      01:37:57
    192.168.10.9          90      01:37:57
  Distance: internal 90 external 170
R3#
```

Рис. 5.6.32

Щоб протокол EIGRP міг відправляти і приймати будь-які оновлення, маршрутизатори повинні налаштувати відносини суміжності зі своїми сусідніми пристроями. Маршрутизатор EIGRP встановлюють відносини суміжності з сусідніми маршрутизаторами, обмінюючись пакетами вітання EIGRP.

Використовуйте команду show ip eigrp neighbors для перегляду таблиці сусідніх вузлів і перевірки, чи встановлені відносини суміжності з сусідніми маршрутизаторами протоколом EIGRP. Для кожного маршрутизатора повинен бути виведений IPv4-адрес сусіднього маршрутизатора і інтерфейс, використовуваний маршрутизатором для зв'язку з цим сусіднім пристроєм EIGRP. Відповідно до цієї топології, таблиця сусідів кожного маршрутизатора містить два сусідніх пристрою.

Результат команди show ip eigrp neighbors містить наступні дані.

Стовпець H. Містить списки сусідніх пристроїв в порядку отримання відомостей про них.

Address. IPv4-адрес сусіднього пристрою.

Interface. Локальний інтерфейс, через який було отримано цей пакет вітання.

Hold. Поточний час утримання. Після отримання пакета вітання для цього значення встановлюється максимальне для цього інтерфейсу час утримання, після чого починається зворотний відлік. При досягненні нуля сусіднє пристрій вважається несправним.

Uptime. Час, що минув з моменту додавання цього сусіднього пристрою в таблицю сусідніх пристроїв.

Smooth Round Trip Timer (SRTT) (час плавного проходження сигналу в прямому і зворотному напрямках) і Retransmission Timeout (RTO) (тайм-аут повторної передачі). Використовується RTP для управління пакетами надійного протоколу EIGRP.

Queue Count. Лічильник черзі. Повинен бути завжди рівним нулю. Якщо це значення не дорівнює нулю, то якісь пакети EIGRP очікують відправки.

Sequence Number. Порядковий номер, який використовується для відстеження пакетів оновлень, запитів і відповідей.

Команда show ip eigrp neighbors дуже корисна для перевірки і усунення проблем EIGRP. Якщо після встановлення відносин суміжності з сусідніми маршрутизаторами сусіднє пристрій відсутній у списку, за допомогою команди show ip interface brief перевірте локальний інтерфейс, щоб переконатися в його активації. Якщо інтерфейс активний, спробуйте відправити луна-запит ping на IPv4-адрес сусіднього пристрою. Якщо цей луна-запит не проходить, то інтерфейс сусіднього пристрою відключений і її потрібно активувати. Якщо луна-запит ping виконується успішно, але EIGRP як і раніше не бачить маршрутизатор як сусіднє пристрій, проаналізуйте наступні конфігурації.

Налаштовані обидва маршрутизатора з використанням одного і того ж номера автономної системи EIGRP?

Чи включена безпосередньо підключена мережа в інструкції network EIGRP?

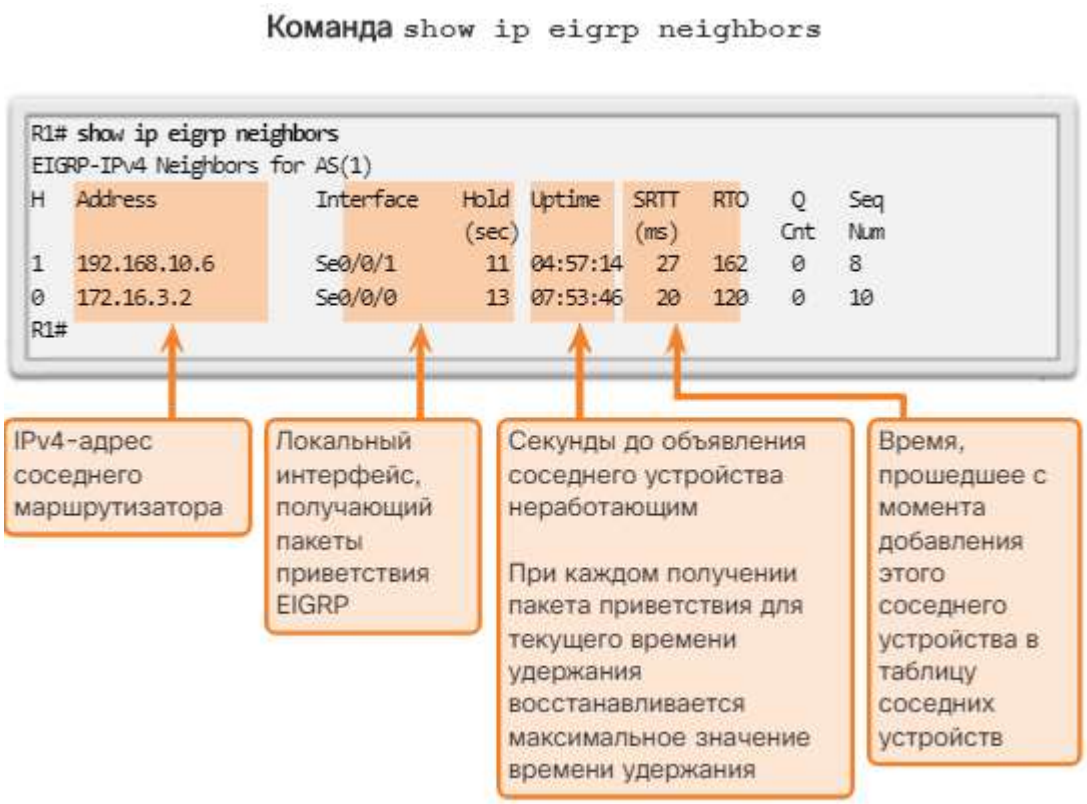


Рис. 5.6.33

Перевірка EIGRP. Команда show ip protocols

Команда show ip protocols виводить параметри і іншу інформацію про поточний стан всіх активних процесів протоколів маршрутизації IPv4, налаштованих на маршрутизаторі. Команда show ip protocols виводить різні типи результатів для кожного з протоколів маршрутизації.

Результат на рис. 1 містить ряд параметрів EIGRP, в тому числі такі.

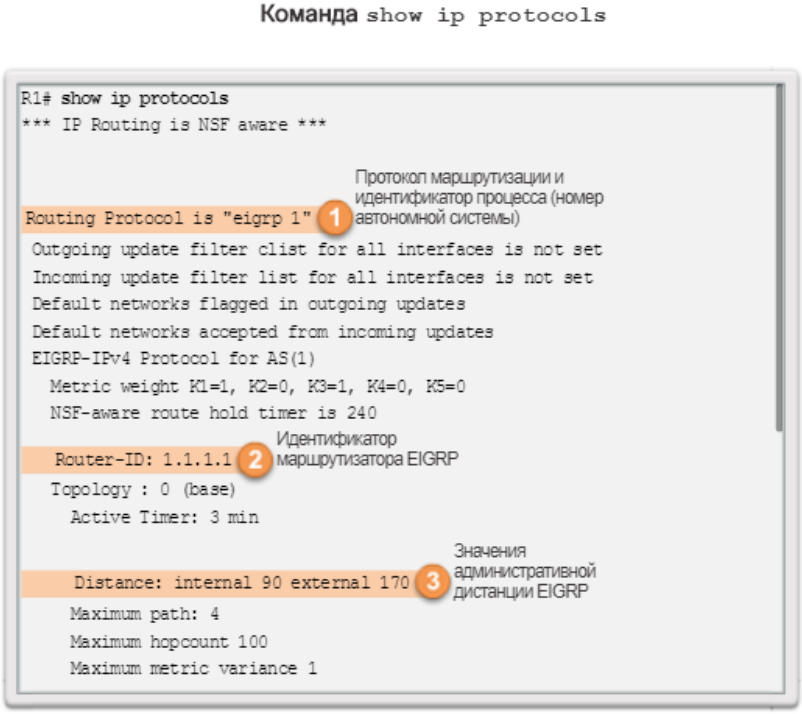


Рис. 5.6.34

1. EIGRP є активним протоколом динамічної маршрутизації на маршрутизаторі R1, налаштованому з використанням номера автономної системи 1.

2. Ідентифікатор EIGRP маршрутизатора R1 дорівнює 1.1.1.1.

3. Адміністративними дистанціями EIGRP для маршрутизатора R1 є внутрішнє AD 90 і зовнішнє AD 170 (значення за замовчуванням).

4. За замовчуванням протокол EIGRP не об'єднує мережі автоматично. Підмережі включені в оновлення маршрутизації.

5. Відносини суміжності EIGRP з сусідніми пристроями, встановлені маршрутизатором R1 з іншими маршрутизаторами, використовуються для отримання оновлень маршрутизації EIGRP.

Примітка. Для випусків, що передують IOS 15, автоматичне об'єднання EIGRP включено за замовчуванням.

Результат команди show ip protocols корисний при налагодженні операцій маршрутизації. Інформація в поле Routing Information Sources (Джерела даних про маршрути) може допомогти визначити маршрутизатор, підозрюваний в наданні неправильної інформації про маршрути. В поле Routing Information Sources (Джерела даних про маршрути) перераховані всі джерела маршрутизації EIGRP, використовувані Cisco IOS для побудови таблиці маршрутизації IPv4. Для кожного джерела зверніть увагу на наступне:

IPv4-адрес

адміністративна дистанція

Час отримання останнього оновлення від цього джерела

Як показано на рис. 2, EIGRP за замовчуванням використовує значення AD 90 для внутрішніх маршрутів і 170 для маршрутів, імпортованих із зовнішнього джерела, таких як маршрути за замовчуванням. У порівнянні з іншими IGP протокол EIGRP є найкращим для Cisco IOS, так як його адміністративна дистанція виявляється найменшою. EIGRP використовує третє значення AD, рівне 5, для сумарних маршрутів.

Административная дистанция по умолчанию

Источник маршрута	Административная дистанция
Подключенный	0
Статический	1
Объединённый маршрут EIGRP	5
Внешний BGP	20
Внутренний EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
Внешний EIGRP	170
Внутренний BGP	200

Рис. 5.6.35

Перевірка EIGRP. Аналіз таблиці маршрутизації IPv4

Іншим способом перевірити правильність налаштувань EIGRP і інших функцій маршрутизатора є аналіз таблиць маршрутизації IPv4 за допомогою команди show ip route. Як і в разі будь-якого протоколу динамічної маршрутизації, мережевий адміністратор повинен перевірити дані таблиці маршрутизації, щоб переконатися, що вони заповнені очікуваним чином, відповідно до введених конфігураціями. З цієї причини важливо добре розуміти команди конфігурації протоколу маршрутизації, а також роботу протоколу маршрутизації і процеси, які використовуються протоколом маршрутизації для побудови таблиці IP-маршрутизації.

Зверніть увагу, що в цьому курсі використовуються результати, що виводяться Cisco IOS 15. Для випусків, що передують IOS 15, автоматичне об'єднання EIGRP включено за замовчуванням. Стан автоматичного об'єднання може змінити інформацію, що відображається в таблиці маршрутизації IPv4. Якщо використовується попередній випуск IOS, то автоматичне об'єднання можна відключити, використовуючи команду режиму конфігурації маршрутизатора no auto-summary:

Router (config-router) # no auto-summary

На рис. 1 показана топологія для маршрутизаторів R1, R2 і R3.

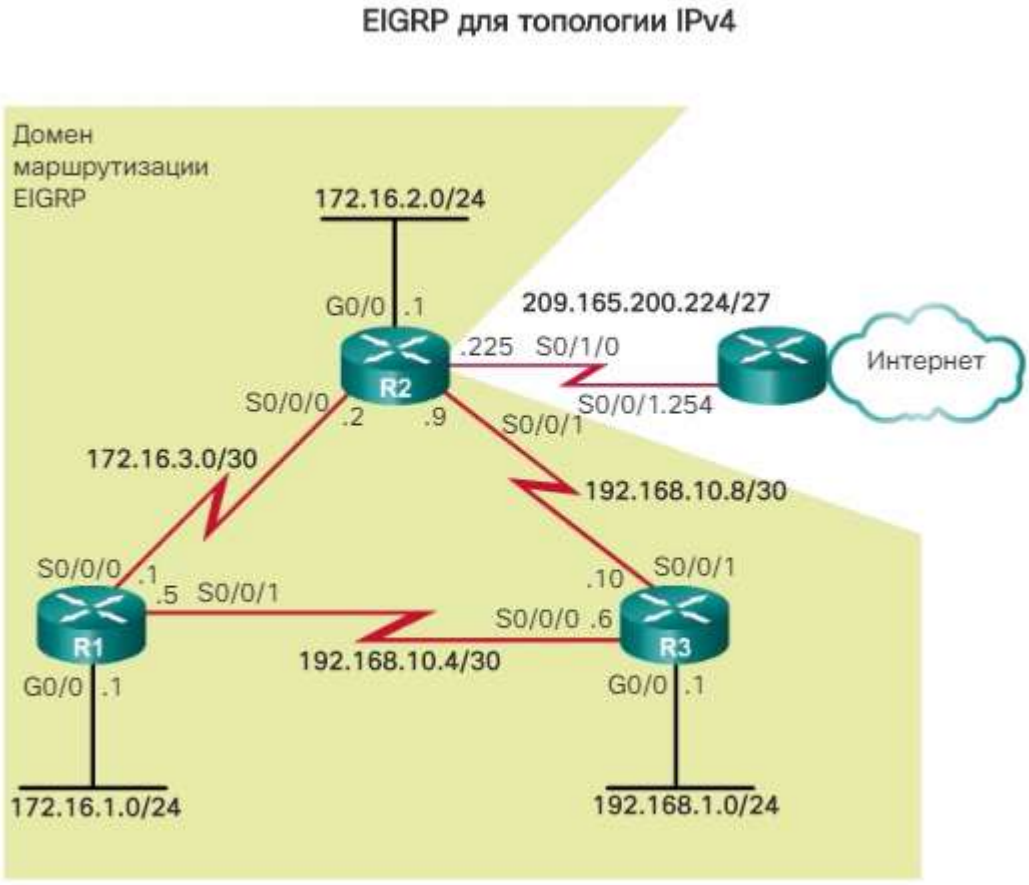
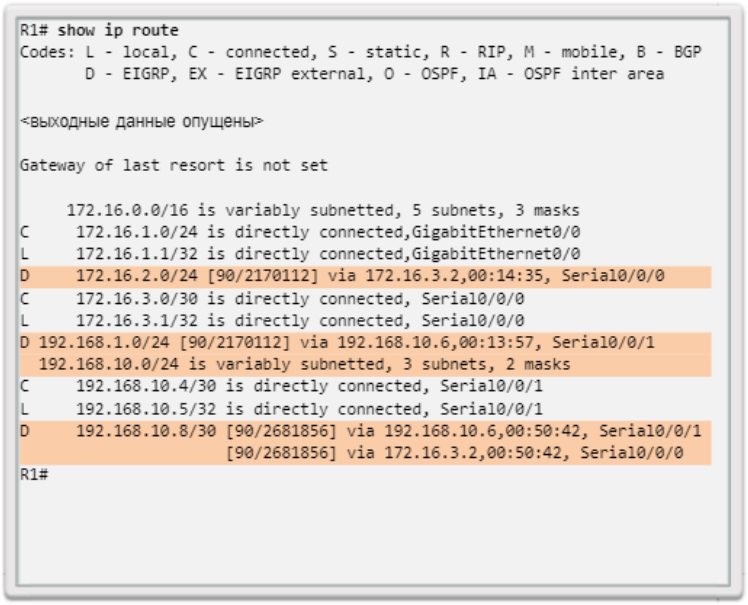


Рис. 5.6.36

На рис. для аналізу таблиці маршрутизації IPv4 використовується команда show ip route. Маршрути EIGRP в таблиці маршрутизації позначаються D. Буква D використана для подання EIGRP, оскільки протокол використовує алгоритм DUAL.

Таблица маршрутизации IPv4 маршрутизатора R1



```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

<выходные данные опущены>

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C     172.16.1.0/24 is directly connected,GigabitEthernet0/0
L     172.16.1.1/32 is directly connected,GigabitEthernet0/0
D     172.16.2.0/24 [90/2170112] via 172.16.3.2,00:14:35, Serial0/0/0
C     172.16.3.0/30 is directly connected, Serial0/0/0
L     172.16.3.1/32 is directly connected, Serial0/0/0
D 192.168.1.0/24 [90/2170112] via 192.168.10.6,00:13:57, Serial0/0/1
  192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C     192.168.10.4/30 is directly connected, Serial0/0/1
L     192.168.10.5/32 is directly connected, Serial0/0/1
D     192.168.10.8/30 [90/2681856] via 192.168.10.6,00:50:42, Serial0/0/1
                      [90/2681856] via 172.16.3.2,00:50:42, Serial0/0/0
R1#
```

Рис. 5.6.37

Команда show ip route перевіряє, чи з'явилися маршрути, отримані сусідніми пристроями EIGRP, в таблиці маршрутизації IPv4. Команда show ip route виводить всю таблицю маршрутизації, в тому числі віддалені мережі, які визначаються динамічно, безпосередньо підключені маршрути і статичні маршрути. З цієї причини ця команда зазвичай є першою командою, яка використовується для перевірки збіжності. Після правильного налаштування маршрутизації на всіх маршрутизаторах команда show ip route показує, що кожен маршрутизатор містить повну таблицю маршрутизації, з маршрутами до всіх мереж в топології.

Зверніть увагу, що маршрутизатор R1 додав в таблицю маршрутизації IPv4 маршрути до трьох віддаленим мереж IPv4:

мережу 172.16.2.0/24, отримана від маршрутизатора R2 через інтерфейс Serial0 / 0/0;

мережу 192.168.1.0/24, отримана від маршрутизатора R2 через інтерфейс Serial0 / 0/1;

мережу 192.168.10.8/30, отримана як від маршрутизатора R2 через інтерфейс Serial0 / 0/0, так і від маршрутизатора R3 через інтерфейс Serial0 / 0/1.

У маршрутизатора R1 є два маршрути до мережі 192.168.10.8/30, оскільки вартість або метрика досягнення цієї мережі однакова або дорівнює для обох використовуваних маршрутизаторів. Ці маршрути називаються маршрутами дорівнює вартості. Маршрутизатор R1 використовує обидва маршрути для досягнення цієї мережі, що називається розподілом навантаження. Метрика EIGRP розглядається нижче в цьому розділі.

На рис. 3 показана таблиця маршрутизації для маршрутизатора R2. Зверніть увагу на аналогічні відображаються результати, в тому числі маршрут дорівнює вартості для мережі 192.168.10.4/30.

Таблица маршрутизации IPv4 маршрутизатора R2

```
R2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

<выходные данные опущены>

Gateway of last resort is not set

 172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
D   172.16.1.0/24 [90/2170112] via 172.16.3.1, 00:11:05, Serial0/0/0
C   172.16.2.0/24 is directly connected, GigabitEthernet0/0
L   172.16.2.1/32 is directly connected, GigabitEthernet0/0
C   172.16.3.0/30 is directly connected, Serial0/0/0
L   172.16.3.2/32 is directly connected, Serial0/0/0
D  192.168.1.0/24 [90/2170112] via 192.168.10.10, 00:15:16,Serial0/0/1
  192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D   192.168.10.4/30 [90/2681856] via 192.168.10.10, 00:52:00,Serial0/0/1
                    [90/2681856] via 172.16.3.1, 00:52:00,Serial0/0/0
C   192.168.10.8/30 is directly connected, Serial0/0/1
L   192.168.10.9/32 is directly connected, Serial0/0/1
  209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.165.200.224/27 is directly connected, Loopback209
L   209.165.200.225/32 is directly connected, Loopback209
R2#
```

Рис. 5.6.38

На рис. показана таблиця маршрутизації для маршрутизатора R3. Аналогічно результатами для маршрутизаторів R1 і R2, дані про віддалених мережах отримані за допомогою EIGRP, в тому числі маршрут дорівнює вартості для мережі 172.16.3.0/30.

Таблица маршрутизации IPv4 маршрутизатора R3

```
R3# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

<выходные данные опущены>

Gateway of last resort is not set

 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D    172.16.1.0/24 [90/2170112] via 192.168.10.5, 00:12:00, Serial0/0/0
D    172.16.2.0/24 [90/2170112] via 192.168.10.9, 00:16:49, Serial0/0/1
D    172.16.3.0/30 [90/2681856] via 192.168.10.9, 00:52:55, Serial0/0/1
                   [90/2681856] via 192.168.10.5, 00:52:55, Serial0/0/0
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
  192.168.10.0/24 is variably subnetted, 4 subnets, 2 masks
C    192.168.10.4/30 is directly connected, Serial0/0/0
L    192.168.10.6/32 is directly connected, Serial0/0/0
C    192.168.10.8/30 is directly connected, Serial0/0/1
L    192.168.10.10/32 is directly connected, Serial0/0/1
R3#
```

Рис. 5.6.39

Ставлення суміжності з сусідніми пристроями EIGRP

Мета будь-якого протоколу динамічної маршрутизації - отримати відомості про віддалених мережах від інших маршрутизаторів і домогтися збіжності в домені маршрутизації. Перш ніж маршрутизатори зможуть обмінюватися пакетами оновлень EIGRP, протокол EIGRP спочатку повинен виявити свої сусідні пристрої. Сусідні пристрої EIGRP - це інші маршрутизатори, що використовують протокол EIGRP в безпосередньо підключені мережі.

EIGRP використовує пакети вітання для формування і підтримки відносин суміжності з сусідніми маршрутизаторами. Щоб два маршрутизатора EIGRP стали сусідніми пристроями, у цих двох маршрутизаторів повинен збігатися ряд параметрів. Наприклад, два маршрутизатора EIGRP повинні використовувати однакові параметри метрик EIGRP, а також для них повинен бути налаштований один і той же номер автономної системи.

Кожен маршрутизатор EIGRP веде таблицю сусідніх пристроїв, що містить для загальних каналів список маршрутизаторів, які встановили відносини суміжності EIGRP з цим маршрутизатором. Таблиця сусідів використовується для відстеження статусу цих сусідніх пристроїв EIGRP.

На малюнку показані два маршрутизатора EIGRP, які обмінюються початковими пакетами вітання EIGRP. Отримавши пакет вітання на свій інтерфейс, маршрутизатор з увімкненим протоколом EIGRP додає відповідний маршрутизатор в свою таблицю сусідніх пристроїв.

Рис. 5.6.40

1. Новий маршрутизатор (R1) активується в каналі і відправляє пакети вітання EIGRP через всі свої інтерфейси, для яких налаштований протокол EIGRP.

2. Маршрутизатор R2 отримує пакет вітання на інтерфейс з включеним протоколом EIGRP. Маршрутизатор R2 відповідає пакетом оновлень EIGRP, що містить всі маршрути, що знаходяться в його таблиці маршрутизації, за винятком маршрутів, отриманих через цей інтерфейс (правило поділу горизонту). Але ставлення суміжності з сусіднім пристроєм не встановлюється, поки маршрутизатор R2 також не відправить пакет вітання EIGRP до маршрутизатора R1.

3. Ставлення суміжності встановлюється після того, як обидва маршрутизатора обміняються пакетами вітання. Маршрутизатор R1 і R2 оновлюють свої таблиці сусідів EIGRP, додаючи суміжний маршрутизатор в якості сусіднього пристрою.

Таблиця топології EIGRP

Оновлення EIGRP містять мережі, доступні з маршрутизатора, що відправляє оновлення. Оскільки оновленнями EIGRP обмінюються сусідні пристрої, який одержує маршрутизатор додає ці записи в свою таблицю топології EIGRP.

Кожен маршрутизатор EIGRP веде таблицю топології для кожного налаштованого маршрутизації протоколу, такого як IPv4 і IPv6. Таблиця топології містить записи маршрутів для кожної мережі призначення, отриманих маршрутизатором від своїх безпосередньо підключених сусідніх пристроїв EIGRP.

На малюнку показано продовження процесу первісного виявлення маршруту, описаного на попередній сторінці. Тепер відображається оновлення таблиці топології.

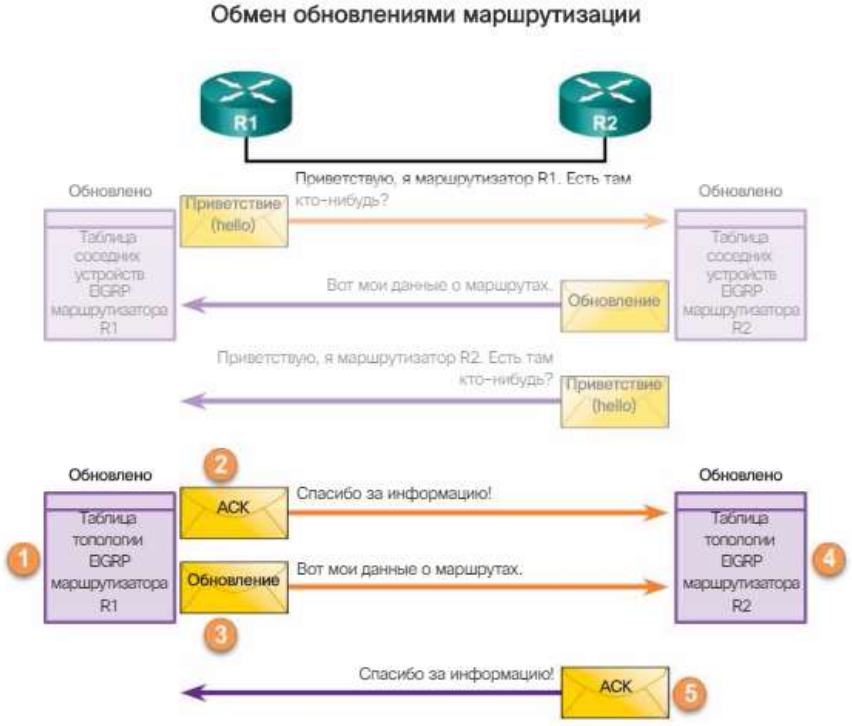


Рис. 5.6.41

Отримавши оновлення маршрутизації EIGRP, маршрутизатор додає дані про маршрути в свою таблицю топології EIGRP і відповідає підтвердженням EIGRP.

1. Маршрутизатор R1 отримує поновлення EIGRP від сусіднього маршрутизатора R2 і додає відомості про маршрутах, оголошених сусіднім пристроєм, включаючи метрику для кожного місця призначення. Маршрутизатор R1 додає все записи поновлення в свою таблицю топології. Таблиця топології містить всі призначення, оголошені сусідніми (суміжними маршрутизаторами) і вартість (метрику) досягнення кожної мережі.

2. Для пакетів оновлень EIGRP використовується надійна доставка, тому маршрутизатор R1 відправляє пакет підтвердження EIGRP, повідомляє маршрутизатора R2 про отримання оновлення.

3. Маршрутизатор R1 відправляє маршрутизатора R2 оновлення EIGRP, оголошує відомі маршрутизатора маршрути, за винятком отриманих від маршрутизатора R2 (правило поділу горизонту).

4. Маршрутизатор R2 отримує оновлення EIGRP від сусіднього маршрутизатора R1 і додає відповідну інформацію в свою таблицю топології.

5. Маршрутизатор R2 відповідає на пакет поновлення EIGRP від маршрутизатора R1 підтвердженням EIGRP.

Збіжність EIGRP

На малюнку показані заключні кроки процесу первісного виявлення маршруту.

Рис. 5.6.42

1. Отримавши пакети оновлень EIGRP від маршрутизатора R2, маршрутизатор R1 оновлює свою таблицю IP-маршрутизації, використовуючи дані в таблиці топології і додаючи оптимальний шлях до кожного місця призначення, включаючи метрику і маршрутизатор наступного переходу.

2. Аналогічно маршрутизатора R1, маршрутизатор R2 оновлює свою таблицю IP-маршрутизації, додаючи оптимальні маршрути до кожної мережі.

З цього моменту протокол EIGRP вважається що зійшов на обох маршрутизаторах.

За замовчуванням протокол EIGRP використовує для розрахунку пріоритетного шляху до мережі в свою складову метриці наступні значення.

Bandwidth (пропускна здатність). Найнижча пропускна здатність серед усіх вихідних інтерфейсів на маршруті від джерела до місця призначення.

Delay (затримка). Сума всіх затримок інтерфейсів уздовж маршруту (в десятках мікросекунд).

Можна використовувати такі значення, але це не рекомендується, оскільки їх використання зазвичай призводить до частих повторних розрахунками таблиці топології:

Reliability (надійність). Являє найгіршу надійність маршруту між відправником і отримувачем, засновану на повідомленнях перевірки активності (keepalive).

Load (завантаження) являє гіршу навантаження для каналу між джерелом і місцем призначення, яка обчислюється на основі швидкості передачі пакета і налаштованої пропускної здатності інтерфейсу.

Примітка. Хоча MTU міститься в оновленнях таблиці маршрутизації, ця метрика маршрутизації не використовується протоколом EIGRP.

складова метрика

На рис. 1 показана формула для складовою метрики, використовуваної EIGRP. Формула містить значення від K1 до K5, звані вагами метрик EIGRP. K1 і K3 представляють пропускну здатність і затримку, відповідно. K2 представляє навантаження, а K4 і K5 - надійність. За замовчуванням значення K1 і K3 встановлені рівними 1, а значення K2, K4 і K5 - рівними 0. У результаті для розрахунку складовою метрики за замовчуванням використовуються тільки значення пропускної здатності і затримки. EIGRP для IPv4 і EIGRP для IPv6 використовують для складовою метрики одну і ту ж формулу.

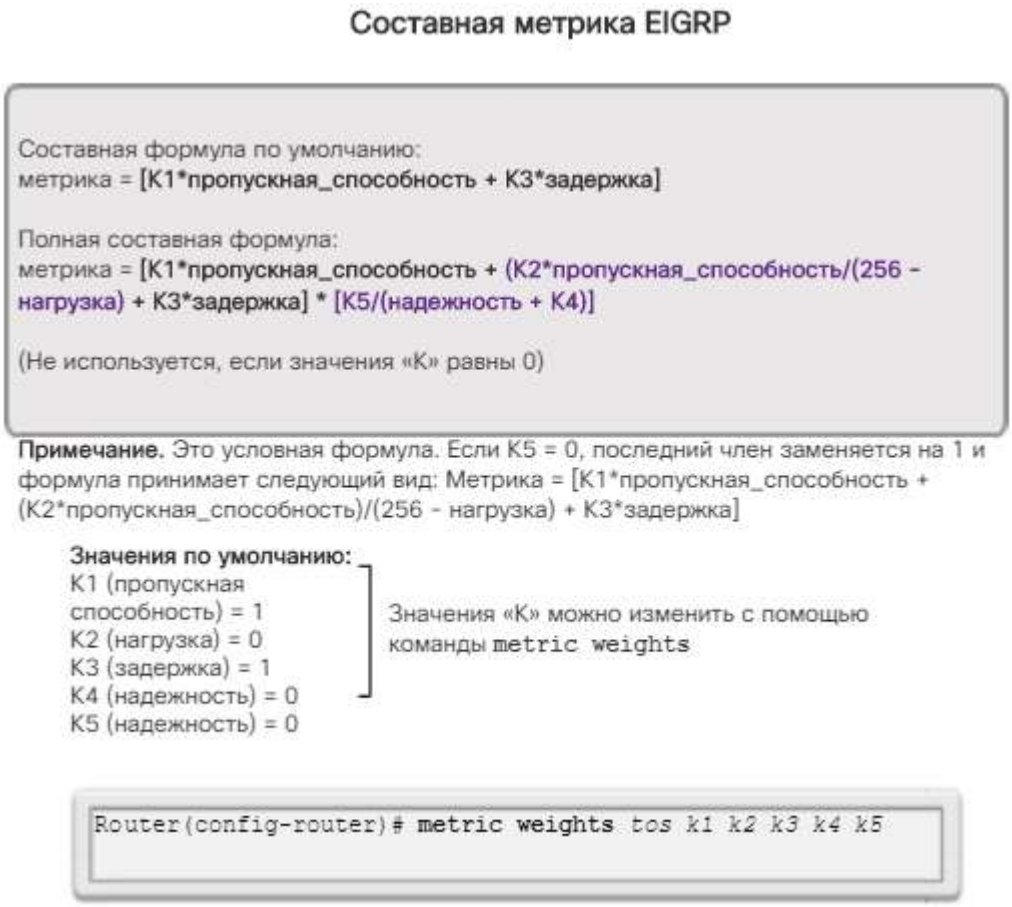


Рис. 5.6.43

Спосіб розрахунку метрики (значення k) і номер автономної системи EIGRP на сусідніх вузлах протоколу EIGRP повинні збігатися. Якщо вони не збігаються, маршрутизатори не створюють відносини суміжності.

Значення k за замовчуванням можна змінити, використовуючи команду режиму конфігурації маршрутизатора metric weights:

Router (config-router) # metric weights tos k1 k2 k3 k4 k5

Примітка. Змінювати значення ваг метрик, metric weights, зазвичай не рекомендується, і в рамках даного курсу подібні зміни не розглядаються. Але їх відповідність важливо для формування відносин суміжності з сусідніми пристроями. Якщо на одному маршрутизаторі ваги метрик змінені, а на іншому маршрутизаторе - немає, то відносини суміжності не можуть бути сформовані.

Перевірка Значення k

Для проверка значення k використовується команда show ip protocols. На рис. 2 показаний результат цієї команди для маршрутизатора R1. Зверніть увагу, що значення k для маршрутизатора R1 встановлені рівними значенням за замовчуванням.

Проверка коэффициентов K метрики

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight k1=1, k2=0, k3=1, k4=0, k5=0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1
<выходные данные опущены>
R1#
```

Рис. 5.6.44

Аналіз значень інтерфейсу

Аналіз значень метрик

Команда show interfaces інформує вас про інтерфейс, включаючи параметри, які використовуються для розрахунку метрики EIGRP. На малюнку приведена команда show interfaces для інтерфейсу Serial 0/0/0 маршрутизатора R1.

Команда `show interfaces`

```
R1# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  <выходные данные опущены>
R1#

R1# show interfaces gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
(bia fc99.4775.c3e0)
  Internet address is 172.16.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  <выходные данные опущены>
R1#
```

Рис. 5.6.45

BW. Пропускна здатність інтерфейсу (в кбіт / с).

DLY. Затримка інтерфейсу (в мікросекундах).

Reliability. Надійність інтерфейсу в частках від 255 (255/255 відповідає стовідсоткової надійності), що розраховується як експоненціальне середнє за п'ять хвилин. За замовчуванням протокол EIGRP не використовує це значення при обчисленні своєї метрики.

Txload, Rxload. Завантаження на передачу і прийом для інтерфейсу даних в частках від 255 (255/255 відповідає повному завантаженні), що розраховується як експоненціальне середнє за 5 хвилин. За замовчуванням протокол EIGRP не використовує це значення при обчисленні своєї метрики.

Примітка. В рамках даного курсу пропускна здатність вказується в кбіт / с. Але в результатах для маршрутизатора пропускна здатність відображається з використанням скорочення "Kbit / sec». У результатах для маршрутизатора затримка також відображається як «usec» (мкс). В рамках даного курсу затримка вказується в мікросекундах.

Метрика пропускної здатності

Метрика пропускної здатності - це статична значення, яке використовується деякими протоколами маршрутизації, такими як EIGRP і OSPF, для розрахунку своєї метрики маршрутизації. Пропускна здатність відображається в кілобітах в секунду (kb / s). Для більшості послідовних інтерфейсів використовується значення пропускної здатності за замовчуванням, рівне 1544 кбіт / с або 1 544 000 біт / с (1,544 Мбіт / с). Це значення пропускної здатності каналу T1. Але для деяких послідовних інтерфейсів використовується інше значення пропускної здатності за замовчуванням. На рис. 1 показана топологія, яка в цьому розділі. Типи послідовних інтерфейсів і значення їх пропускної здатності не обов'язково є показниками найбільш поширених типів з'єднань, що застосовуються в сучасних мережах.

EIGRP для топологии IPv4

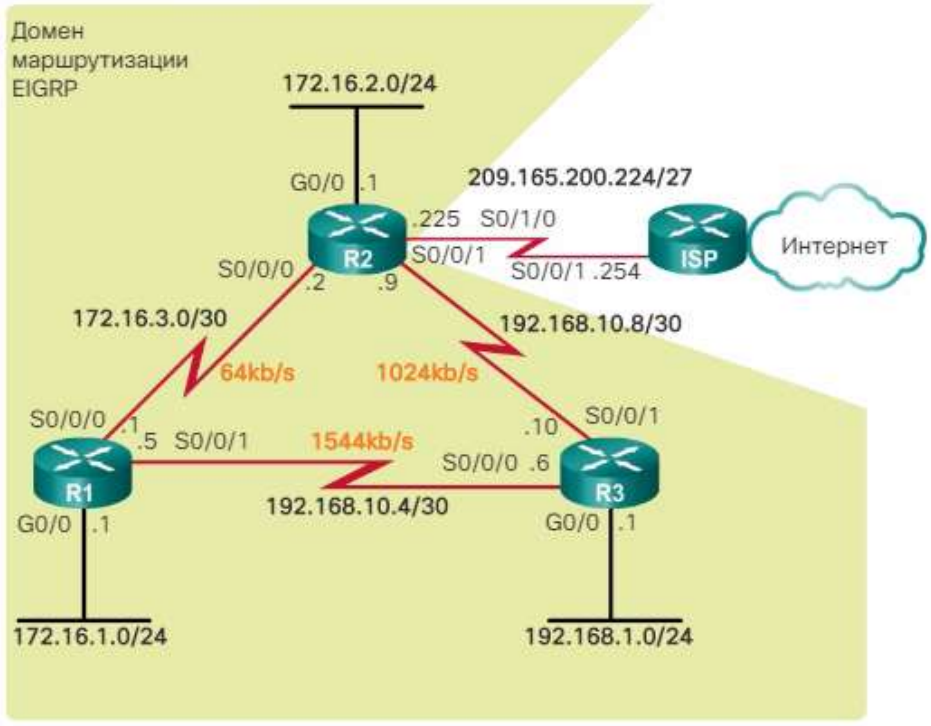


Рис. 5.6.46

Завжди перевіряйте пропускну здатність, використовуючи команду show interfaces.

Значення пропускної здатності за замовчуванням може відповідати або не відповідати фактичної фізичної пропускної здатності інтерфейсу. Якщо значення фактичної пропускної здатності каналу відрізняється від значення пропускної здатності за замовчуванням, то значення пропускної здатності потрібно змінити.

Налаштування параметра пропускної здатності

Для більшості послідовних каналів пропускна здатність за замовчуванням дорівнює +1544 Кбіт / с. Оскільки і EIGRP, і OSPF використовують пропускну здатність для розрахунку метрики за замовчуванням, правильне значення пропускної здатності дуже важливо для точності даних про маршрутах.

Для зміни метрики пропускної здатності використовуйте наступну команду режиму конфігурації інтерфейсу:

Router (config-if) # bandwidth kilobits-bandwidth-value

Для відновлення значення пропускної здатності за замовчуванням використовується команда no bandwidth.

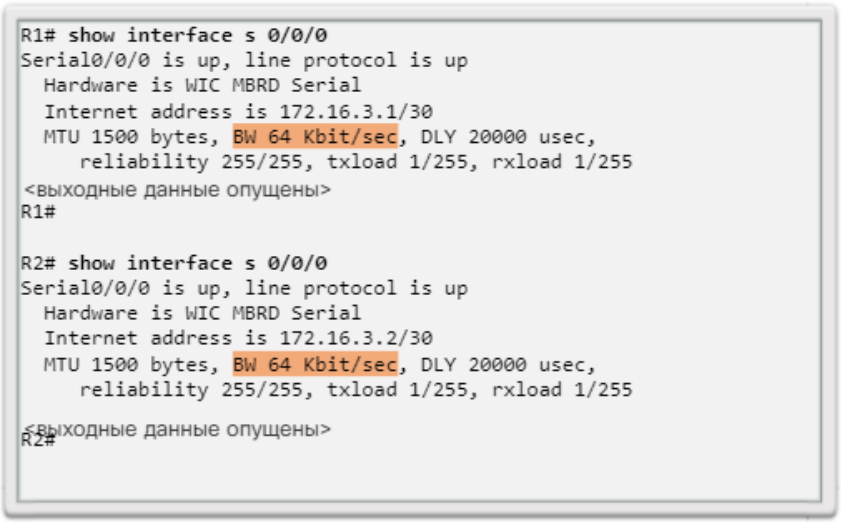
На рис. 2 пропускна здатність каналу між маршрутизаторами R1 і R2 дорівнює 64 кбіт / с, а пропускна здатність каналу між маршрутизаторами R2 і R3 дорівнює 1024 кбіт / с. На малюнку показані конфігурації, які використовуються на всіх трьох маршрутизаторах для зміни пропускної здатності відповідних послідовних інтерфейсів.

Рис. 5.6.47

Перевірка параметра пропускної здатності

Для перевірки нових параметрів пропускної здатності використовуйте команду show interfaces, як показано на рис. 3. Для забезпечення правильної маршрутизації в обох напрямках важливо змінити пропускну здатність на обох сторонах каналу.

Проверка значения пропускной способности



Для обеспечения правильной маршрутизации в обоих направлениях важно, чтобы параметры пропускной способности совпадали с обеих сторон канала.

Рис. 5.6.48

Зміна значення пропускної здатності не змінює фактичну пропускну здатність каналу. Команда bandwidth змінює тільки метрику пропускної здатності, яка використовується протоколом маршрутизації, таким як EIGRP і OSPF.

Метрика затримки

Затримка - це міра часу, необхідного для проходження пакета по маршруту. Метрика затримки (DLY) є статичним значенням, що залежать від типу каналу, до якого підключений інтерфейс. Даний параметр виражається в мікросекундах. Затримка не вимірюються динамічно. Іншими словами, в дійсності маршрутизатор не відслідковує, скільки часу потрібно пакету, щоб досягти місця призначення. Значення затримки, подібно значенням пропускної здатності, є значенням за замовчуванням, яке може бути змінено мережевим адміністратором.

При використанні цього значення для визначення метрики EIGRP затримка є сумою затримок для всіх інтерфейсів уздовж маршруту (вимірюється в десятках мікросекунд).

У таблиці на рис. 1 показані значення затримок за замовчуванням для різних інтерфейсів. Значення за замовчуванням дорівнює 20 000 мікросекунд для послідовних інтерфейсів і 10 мікросекунд для інтерфейсів гигабитного Ethernet.

Значения задержки для интерфейсов

Среда передачи данных	Задержка
Ethernet	1000
Fast Ethernet	100
гигабитный Ethernet	10
16M Token Ring	630
FDDI	100
T1 (последовательный по умолчанию)	20000
DS0 (64 Кб/с)	20000
1024 Кб/с	20000
56 кбит/с	20000

Рис. 5.6.49

Щоб перевірити значення затримки для інтерфейсу, як показано на рис. 2, використовуйте команду show interfaces. Хоча у інтерфейсу з різними пропускними здатностями може бути однакове значення затримки за замовчуванням, компанія Cisco не рекомендує змінювати параметр затримки, поки у Адміністратора не з'явиться вагома причина для подібної дії.

Проверка значения задержки

```
R1# show interfaces s 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
 <выходные данные опущены>
R1#

R1# show interfaces g 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
(bia fc99.4775.c3e0)
  Internet address is 172.16.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
 <выходные данные опущены>
R1#
```

Рис. 5.6.50

Спосіб обчислення метрики EIGRP

Незважаючи на те, що EIGRP автоматично обчислює метрику таблиці маршрутизації, яка використовується для вибору найкращого маршруту, важливо, щоб мережевий адміністратор знав, як визначаються ці метрики.

На малюнку показана складова метрика, яка використовується EIGRP. Використовуючи значення за замовчуванням для K1 і K3, розрахунок можна

спростити до найнижчої (або мінімальної) пропускної здатності плюс сума всіх затримок.

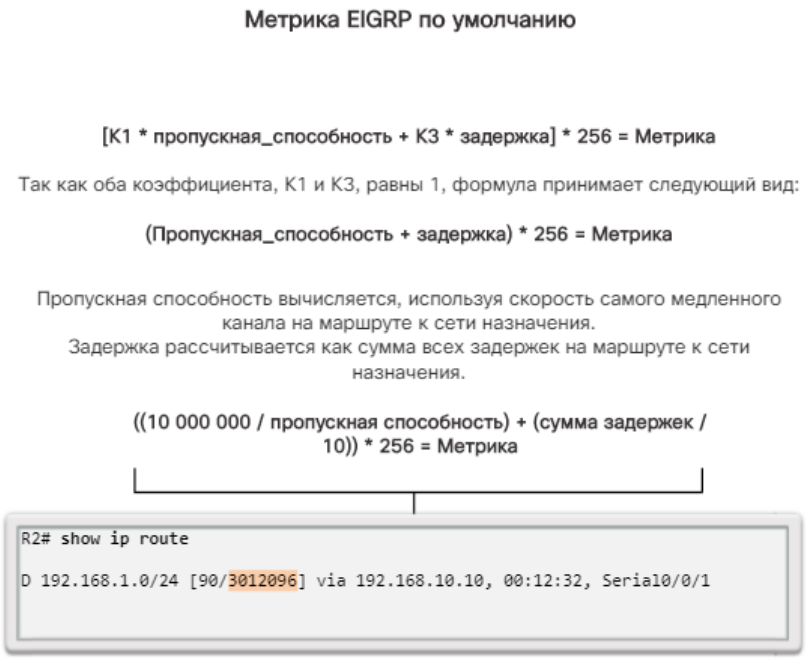


Рис. 5.6.51

Іншими словами, проаналізувавши значення пропускної здатності і затримки для всіх вихідних інтерфейсів маршруту, можна визначити метрику EIGRP наступним чином:

Крок 1. Визначте канал з найнижчою пропускною спроможністю. Використовуйте це значення для розрахунку пропускної здатності (10 000 000 / пропускна здатність).

Крок 2. Визначте значення затримки для кожного вихідного інтерфейсу на маршруті до місця призначення. Складіть значення затримки і розділіть суму на 10 (сума затримок / 10).

Крок 3. Складіть обчислені значення для пропускної здатності і затримки, а потім помножте результат на 256, щоб отримати метрику EIGRP.

Результат для таблиці маршрутизації маршрутизатора R2 показує, що метрика EIGRP маршруту до 192.168.1.0/24 дорівнює 3 012 096.

Розрахунок метрики EIGRP

На рис. 1 показана топологія з трьох маршрутизаторів. Даний приклад демонструє, як протокол EIGRP визначає метрику, що відображається в таблиці маршрутизації маршрутизатора R2 для мережі 192.168.1.0/24.

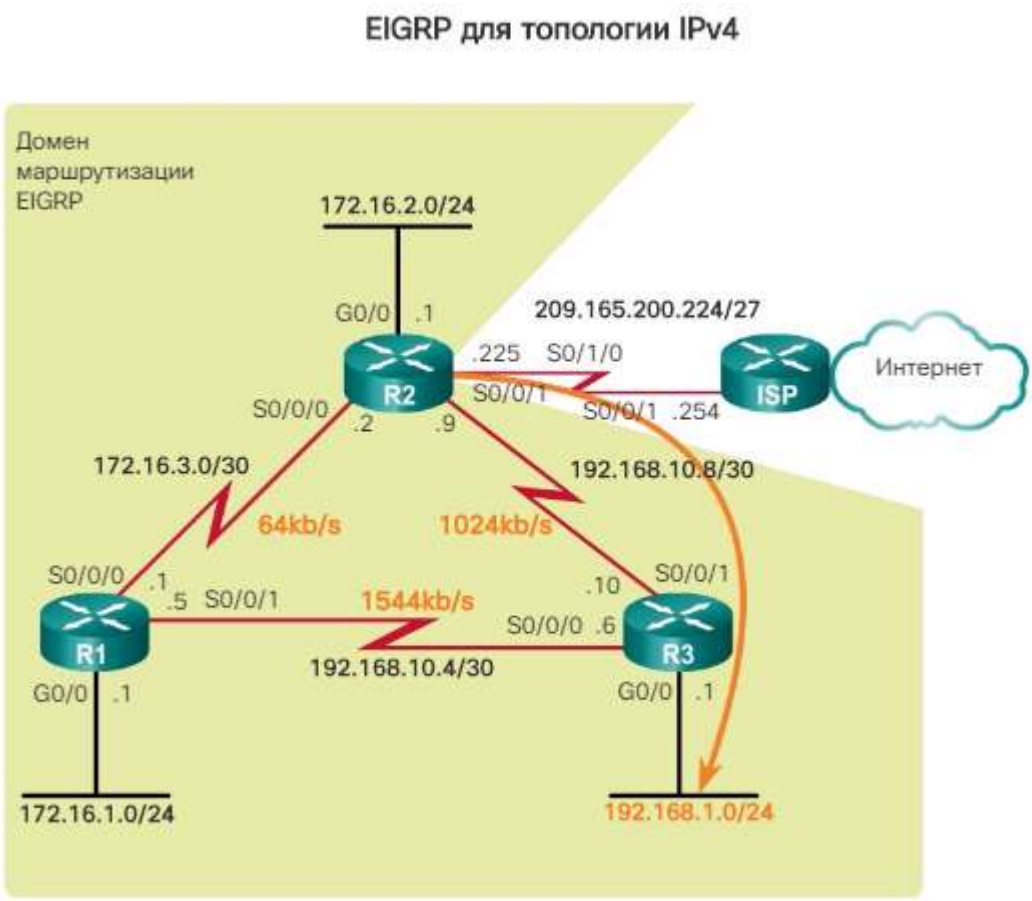


Рис. 5.6.52

Протокол EIGRP використовує при обчисленні своєї метрики найнижчу пропускну здатність. Найнижча пропускна здатність може бути визначена шляхом аналізу кожного інтерфейсу між маршрутизатором R2 і мережею призначення 192.168.1.0. Пропускна здатність інтерфейсу Serial 0/0/1 маршрутизатора R2 рівна 1 024 кбіт / с. Пропускна здатність інтерфейсу GigabitEthernet 0/0 маршрутизатора R3 дорівнює 1 000 000 кбіт / с. Тому найнижча пропускна здатність дорівнює 1024 кбіт / с, і саме це значення використовується при розрахунку метрики.

EIGRP ділить еталонне значення пропускної здатності довідки 10 000 000 на значення пропускної здатності інтерфейсу в кбіт / с. При цьому значенням більшої пропускної спроможності відповідає менша метрика, а значенням меншою пропускної здатності - велика метрика. 10 000 000 ділиться на 1024. Якщо результат не є цілим числом, значення округляється в бік більш низького значення. В даному випадку 10 000 000 розділити на 1 024 одно 9765,625. 0,625 відкидається для отримання значення пропускної здатності в складовою метриці, рівного 9765, як показано на рис. 2.

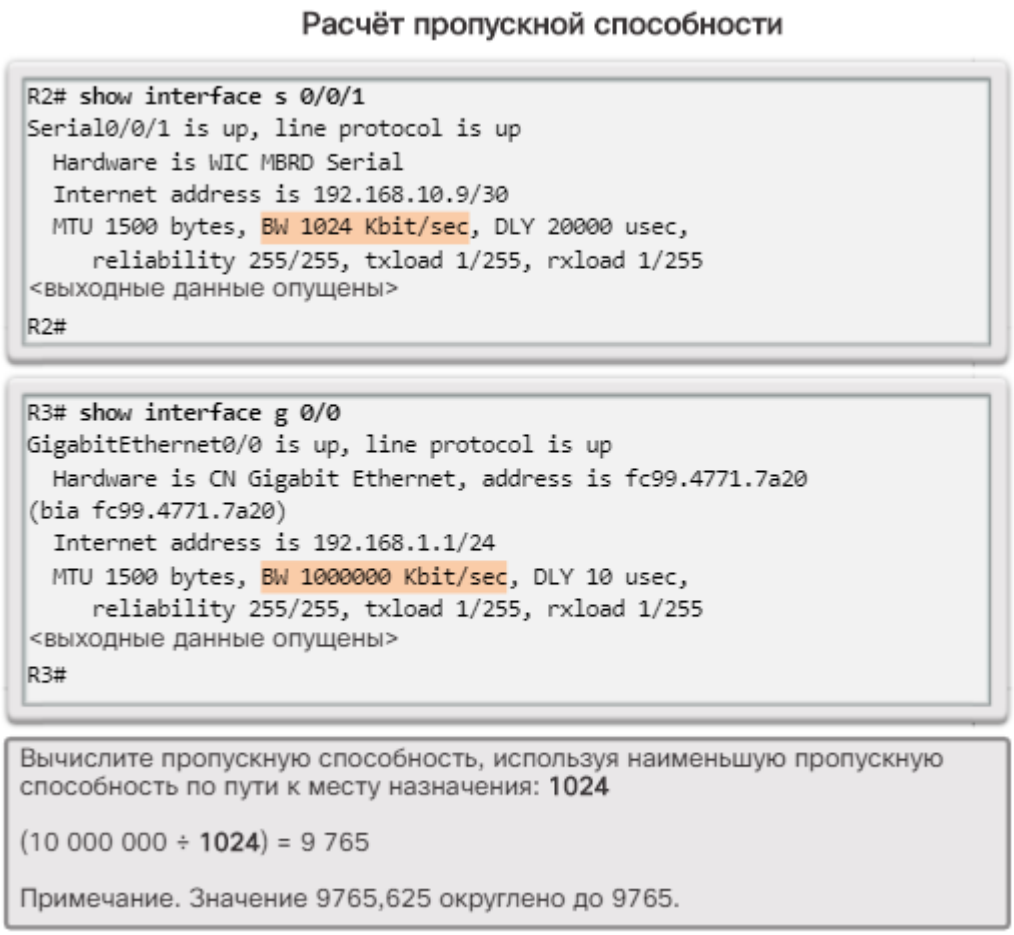


Рис. 5.6.53

Ті ж вихідні інтерфейси використовуються для визначення значення затримки.

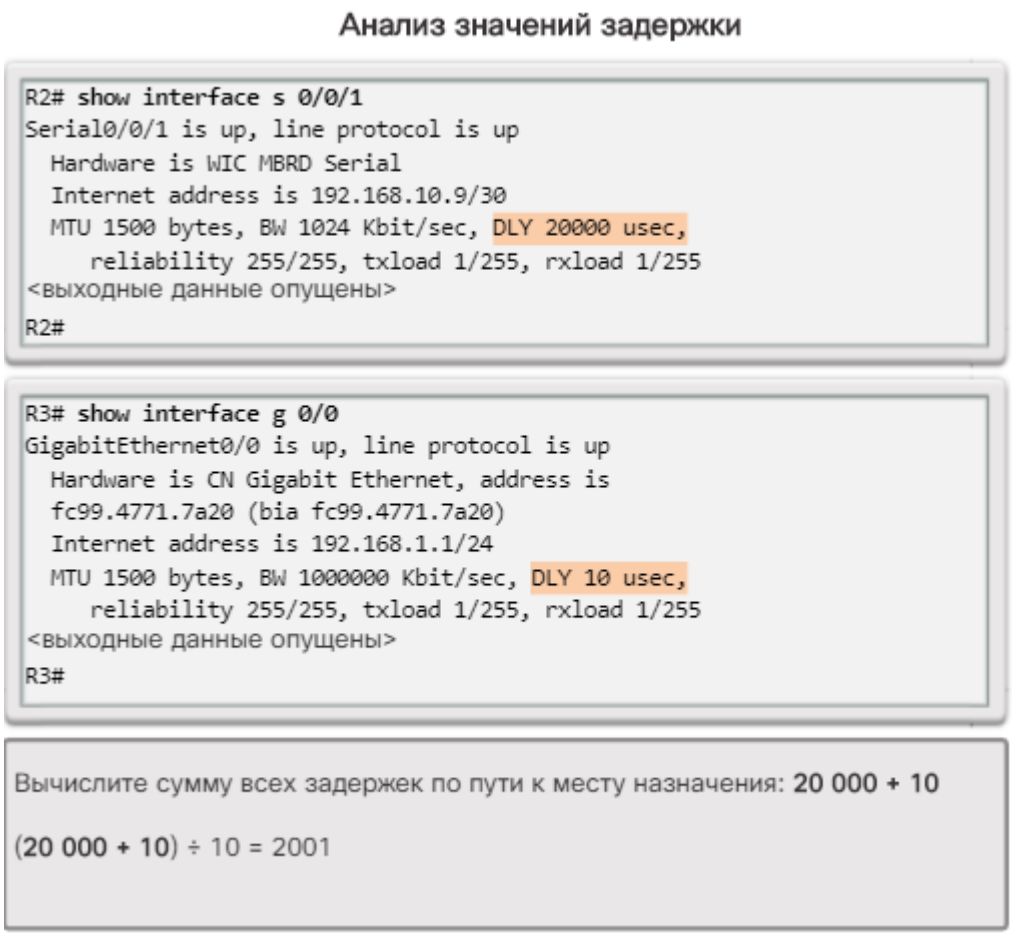


Рис. 5.6.54

Протокол EIGRP використовує суму всіх затримок на маршруті до місця призначення. Затримка для інтерфейсу Serial 0/0/1 маршрутизатора R2 дорівнює 20 000 мікросекунд. Затримка для інтерфейсу Gigabit 0/0 маршрутизатора R3 дорівнює 10 мікросекунд. Сума цих затримок ділиться на 10. У цьому прикладі (20 000 + 10) / 10 дає значення 2001 для значення затримки в складовою метриці.

Розрахунок метрики

Використовуйте розраховані значення пропускної здатності і затримки у формулі метрики. Це дає метрику 3 012 096, як показано на рис. 4. Дане значення відповідає значенню, показаному в таблиці маршрутизації для маршрутизатора R2.

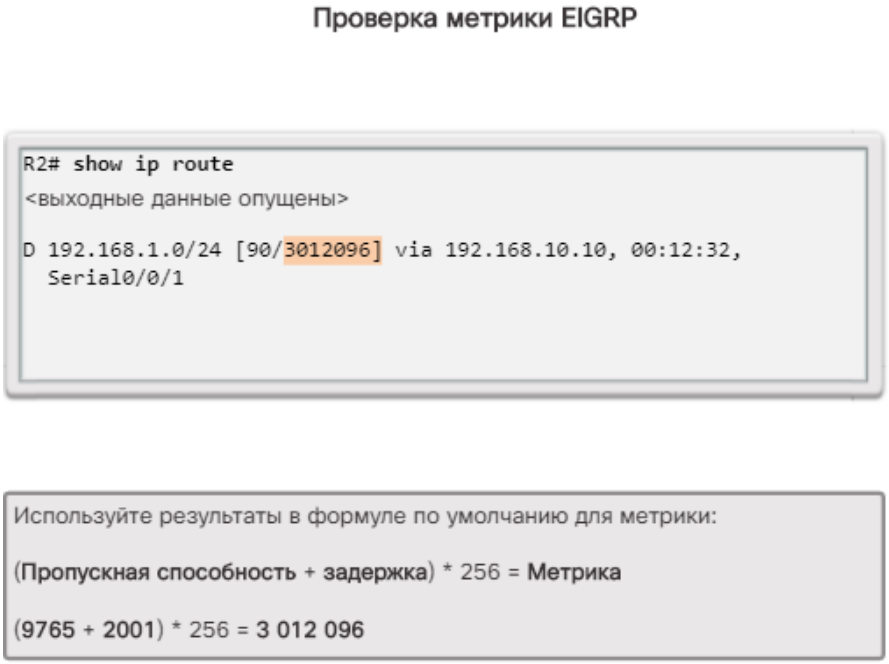


Рис. 5.6.55

Основні ідеї алгоритму DUAL

Протокол EIGRP використовує алгоритм дифузійного поновлення (DUAL) для отримання оптимального маршруту без петель і резервних маршрутів без петель.

Алгоритм DUAL використовує ряд термінів, детально описані в даному розділі:

- наступник
- Допустима відстань (FD)
- Можливий наступник (FS)
- Повідомлене відстань (RD) або оголошене відстань (AD)
- Можливе умова або умова здійсненності (FC)

Ці терміни і поняття знаходяться в центрі механізму запобігання петель алгоритму DUAL.

Знайомство з DUAL

EIGRP використовує алгоритм збіжності DUAL. Збіжність необхідна для запобігання в мережі петель маршрутизації.

Петлі маршрутизації, навіть тимчасові, можуть негативно позначитися на продуктивності мережі. Протоколи маршрутизації на основі векторів відстані, такі як RIP, запобігають появі петель маршрутизації, використовуючи таймери утримання і правило поділу горизонту. Хоча в EIGRP використовуються обидва цих методу, цей протокол використовує їх трохи інакше - основним способом, за допомогою якого EIGRP запобігає утворенню петель, є алгоритм DUAL.

Щоб переглянути принципи роботи алгоритму DUAL, натисніть «Відтворення» на малюнку.

Алгоритм DUAL використовується, щоб усунути петлі для кожного екземпляра при розрахунку маршруту. Це дозволяє одночасно синхронізувати всі маршрутизатори, які беруть участь у зміні топології. Маршрутизатор, не порушені змінами топології, не беруть участі в повторному розрахунку. Цей

метод дозволяє EIGRP скоротити часи збіжності в порівнянні з іншими протоколами маршрутизації на основі векторів відстані.

При прийнятті рішень для всіх обчислень маршрутів застосовується кінцевий автомат (FSM) алгоритму DUAL. Кінцевий автомат - це модель технологічного процесу, аналогічна блок-схемі, яка складається з таких компонентів:

Кінцеве число етапів (станів)

Перехід між цими етапами

операції

Кінцевий автомат алгоритму DUAL відстежує всі маршрути, використовує метрики EIGRP для вибору ефективних маршрутів без петель і визначення маршрутів з найменшою вартістю, які будуть занесені в таблицю маршрутизації.

Повторний розрахунок за алгоритмом DUAL може зажадати інтенсивної роботи процесора. EIGRP по можливості дозволяє уникнути повторного розрахунку, підтримуючи список резервних маршрутів, які алгоритм DUAL вже визначив як маршрути без петель. У разі відмови основного маршруту в таблицю маршрутизації негайно додається кращий резервний маршрут.

Наступник і можливу відстань

На рис. 1 представлена топологія для вивчення даної теми. Наступник - це сусідній маршрутизатор, який використовується для пересилання пакетів і забезпечує маршрут з найменшою вартістю до мережі призначення. IP-адреса наступника показаний в записи таблиці маршрутизації відразу ж після слова «via».

EIGRP для топологии IPv4

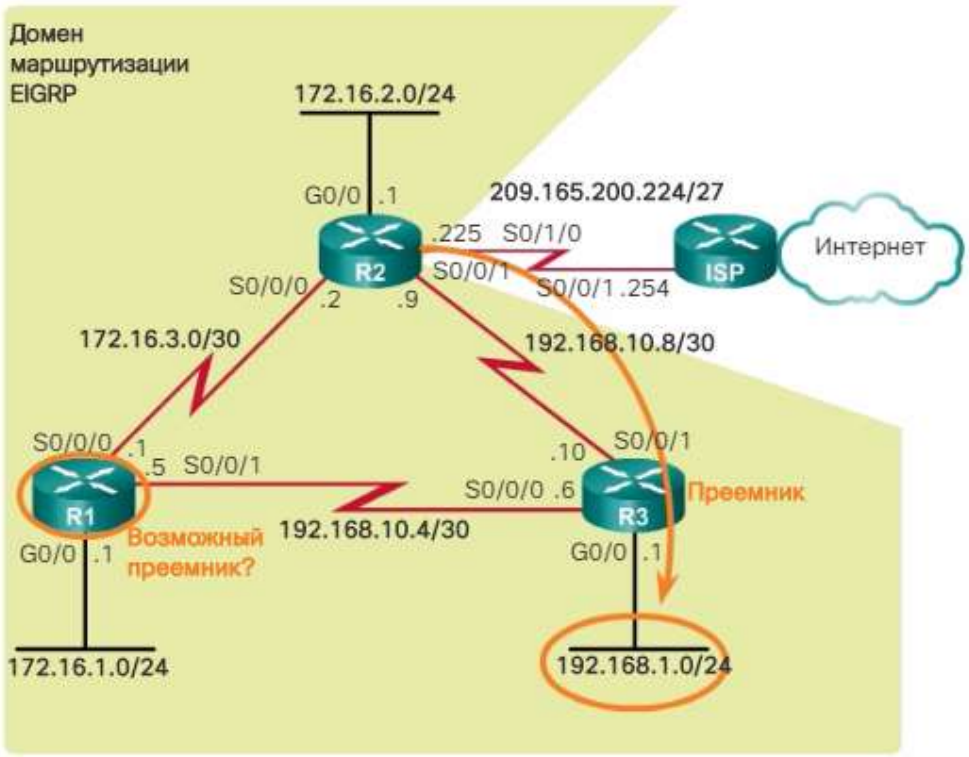


Рис. 5.6.56

FD (допустима відстань) - це мінімальна з обчислених метрик досягнення мережі призначення. Допустима відстань - це метрика, наведена в запису таблиці маршрутизації в дужках під другим номером. Як для інших протоколів маршрутизації, цей параметр також називається метрикою маршруту.

Аналізуючи таблицю маршрутизації для маршрутизатора R2 на рис. 2, зверніть увагу, що оптимальний маршрут EIGRP для мережі 192.168.1.0/24 проходить через маршрутизатор R3, і що можливе відстань дорівнює 3 012 096. Саме ця метрика була розрахована в попередньому розділі.

Рис. 5.6.57

Можливі наступники, умова здійсненності і оголошене відстань

Алгоритм DUAL може швидко сходитися після зміни топології, оскільки він може використовувати резервні маршрути до інших мереж без повторних обчислень за алгоритмом DUAL. Ці резервні шляху називаються можливими наступниками (Feasible Successor, FS).

FS (можливий наступник) - це сусідній маршрутизатор, у якого є резервний маршрут без петель до тієї ж мережі, що і у наступника, і який задовольняє умові здійсненності (Feasibility Condition, FC). Наступником маршрутизатора R2 для мережі 192.168.1.0/24 є маршрутизатор R3, що забезпечує оптимальний шлях або мінімальну метрику для мережі призначення. Зверніть увагу на рис. 1, що маршрутизатор R1 надає альтернативний шлях, але чи є він можливим наступником? Щоб маршрутизатор R1 міг бути можливим наступником для маршрутизатора R2, спочатку R1 повинен відповідати умові здійсненності (FC).

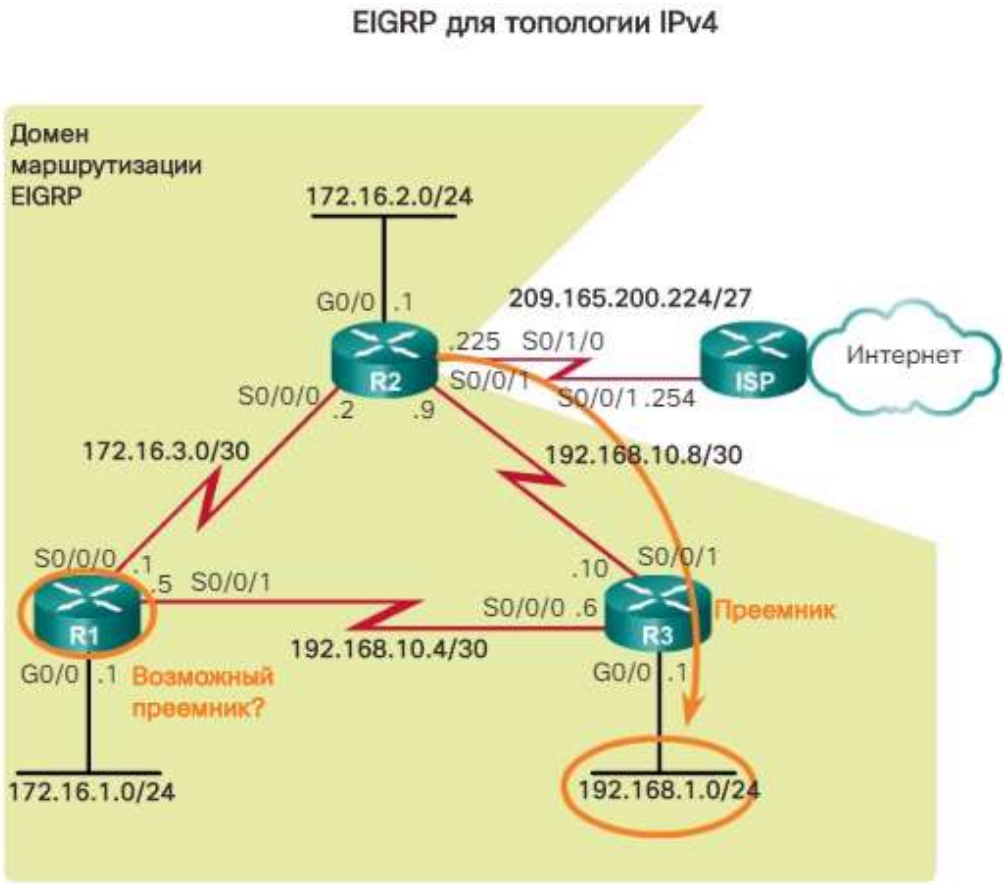


Рис. 5.6.58

Умова здійсненності виконується, коли оголошене відстань (RD) сусіднього пристрою для мережі менше, ніж можливу відстань локального маршрутизатора до цієї ж мережі призначення. Якщо оголошене відстань виявляється менше, воно являє маршрут без петель маршрутизації. Оголошене відстань являє собою просто можливу відстань сусіднього пристрою EIGRP для тієї ж мережі призначення. Оголошене відстань - це метрика, повідомляється маршрутизатором сусіднього пристрою про вартість свого маршруту до цієї мережі.

На рис. можливу відстань маршрутизатора R1 до мережі 192.168.1.0/24 дорівнює 2 170 112.

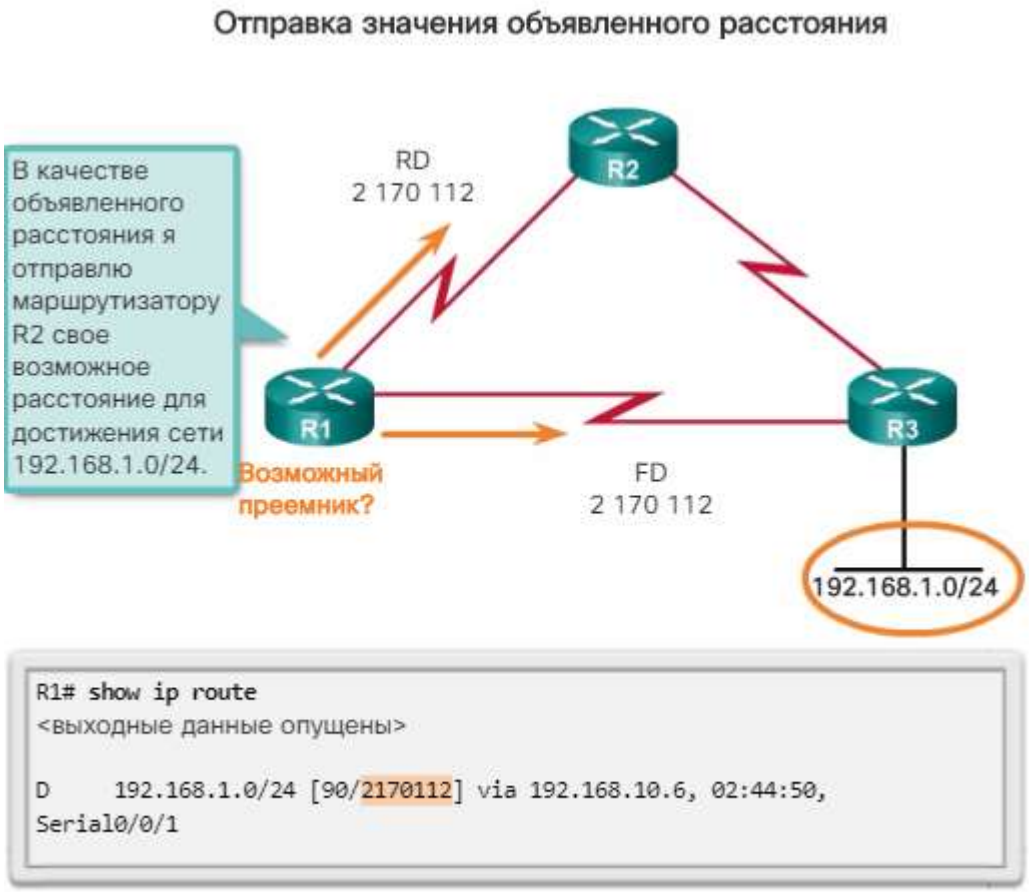


Рис. 5.6.59

Маршрутизатор R1 повідомляє маршрутизатора R2, що його допустима відстань до мережі 192.168.1.0/24 дорівнює 2 170 112.

З точки зору маршрутизатора R2 2 170 112 - це RD маршрутизатора R1.

Маршрутизатор R2 використовує цю інформацію, щоб визначити, чи виконується умова здійсненності для маршрутизатора R1 і чи може цей маршрутизатор тому бути можливим наступником.

Як показано на рис. 3, оскільки RD маршрутизатора R1 (2 170 112) менше, ніж власне допустима відстань маршрутизатора R2 (3 012 096), для маршрутизатора R1 виконується умова здійсненності.

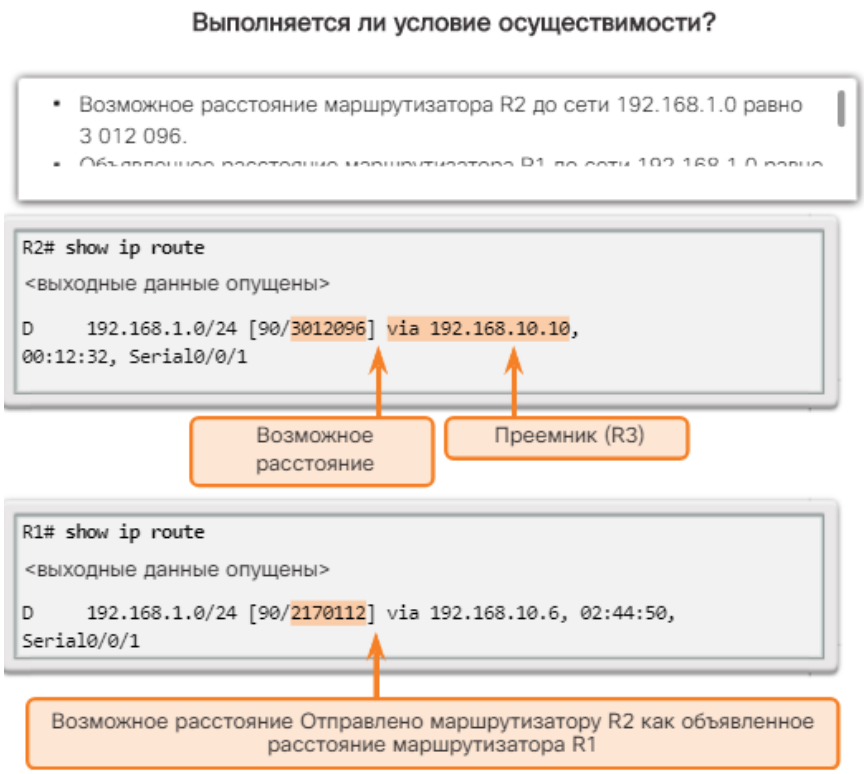


Рис. 5.6.60

Рис. 3

Тепер маршрутизатор R1 є можливим наступником до мережі 192.168.1.0/24 для маршрутизатора R2.

У разі відмови маршруту R2 до мережі 192.168.1.0/24 через R3 (наступник) маршрутизатор R2 негайно вставляє в таблицю маршрутизації маршрут через маршрутизатор R1 (можливий наступник). Маршрутизатор R1 стане новим наступником для маршруту від маршрутизатора R2 до цієї мережі.

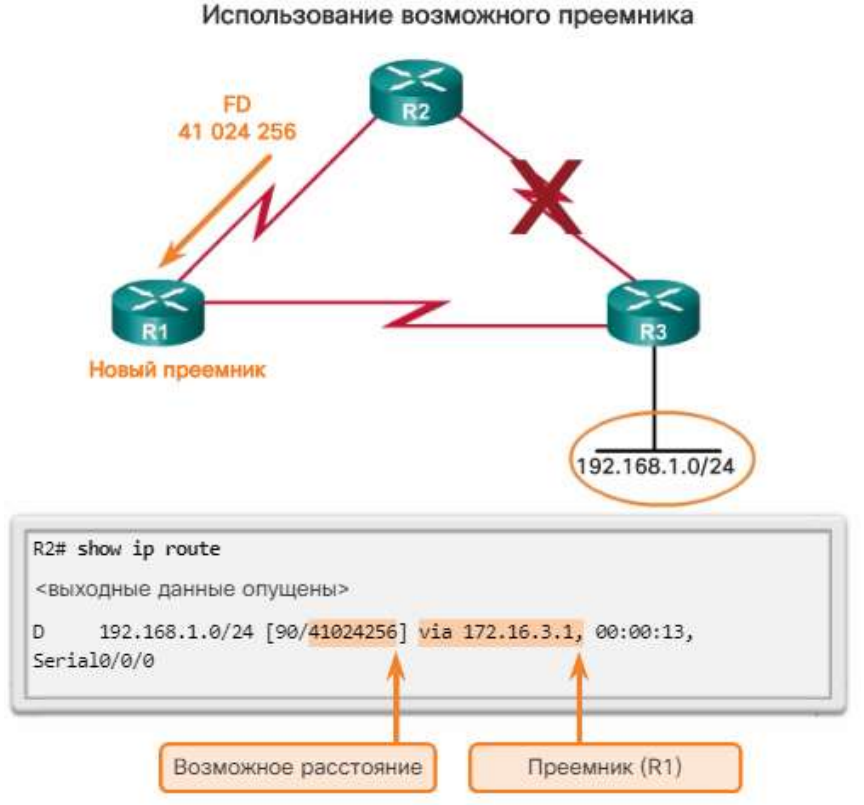


Рис. 5.6.61

Таблиця топології. Команда show ip eigrp topology

Вже згадана топологія приведена на рис. 1.

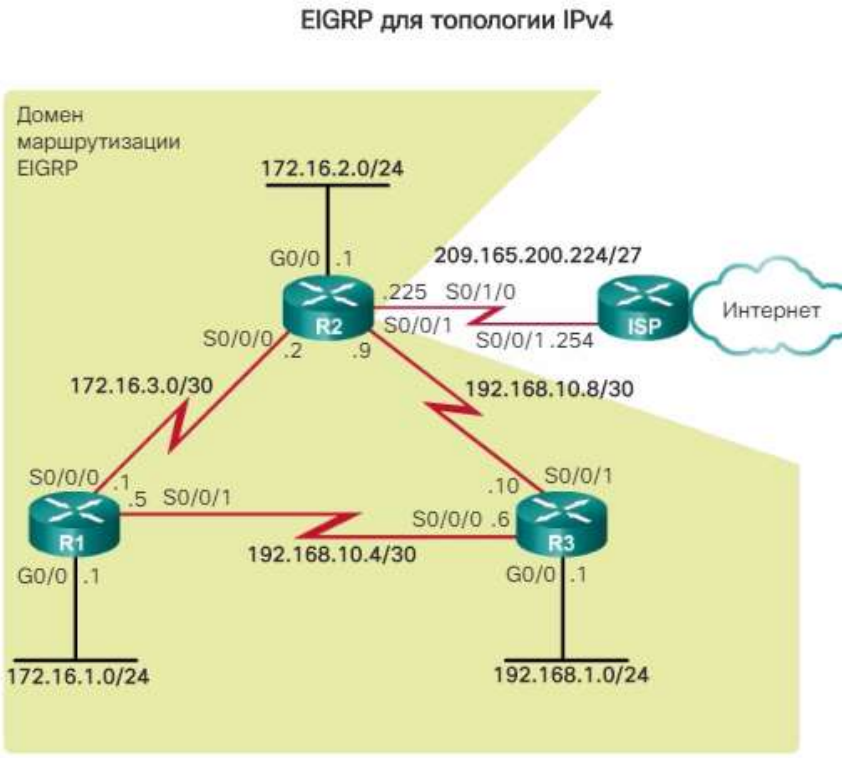


Рис. 5.6.62

Таблиця топології EIGRP містить всі маршрути, відомі всім сусіднім пристроїв EIGRP. Дізнавшись маршрути EIGRP від сусідніх пристроїв, маршрутизатор додає ці маршрути в свою таблицю топології EIGRP.

Як показано на рис. 2, використовуйте команду show ip eigrp topology для перегляду таблиці топології. Таблиця топології містить список всіх наступників і всіх можливих наступників, обчислених алгоритмом DUAL для мережі призначення. У таблицю IP-маршрутизації додається тільки наступник.

Таблица топологии маршрутизатора R2

```
R2# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(1)/ID(2.2.2.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.16.2.0/24, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/0
P 192.168.10.4/30, 1 successors, FD is 3523840
        via 192.168.10.10 (3523840/2169856), Serial0/0/1
        via 172.16.3.1 (41024000/2169856), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 3012096
        via 192.168.10.10 (3012096/2816), Serial0/0/1
        via 172.16.3.1 (41024256/2170112), Serial0/0/0
P 172.16.3.0/30, 1 successors, FD is 40512000
        via Connected, Serial0/0/0
P 172.16.1.0/24, 1 successors, FD is 3524096
        via 192.168.10.10 (3524096/2170112), Serial0/0/1
        via 172.16.3.1 (40512256/2816), Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
        via Connected, Serial0/0/1

R2#
```

Рис. 5.6.63

Таблиця топології. Команда show ip eigrp topology (продовження)

Як показано на рис. 1, перший рядок в таблиці топології містить наступний ознака:

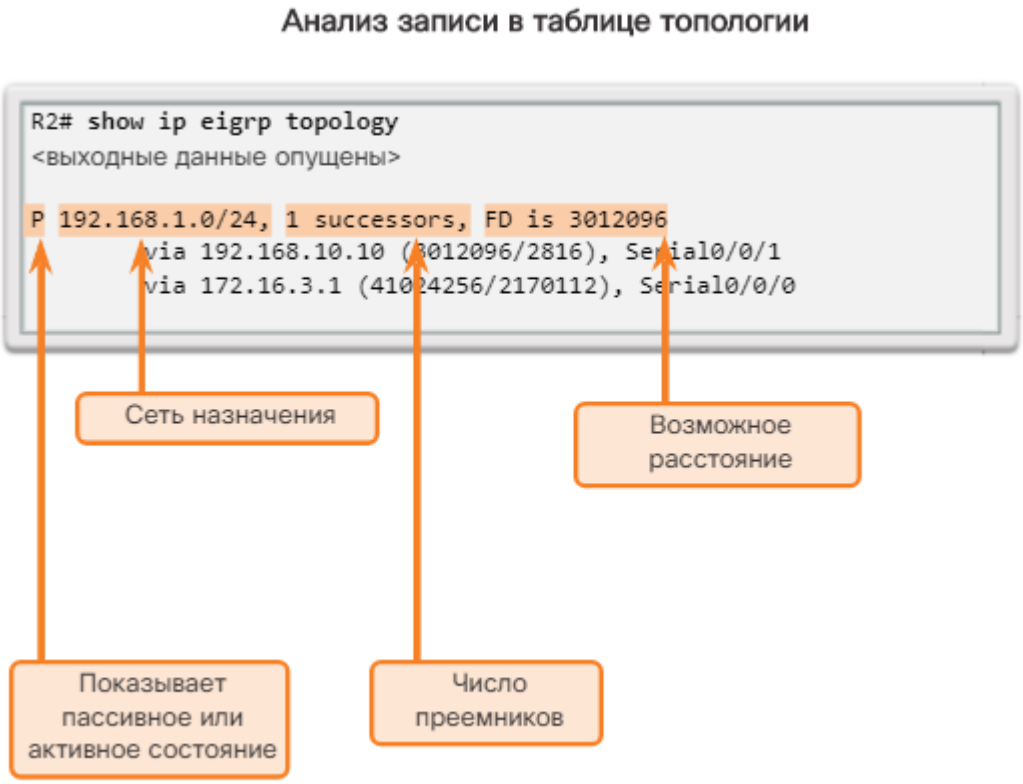


Рис. 5.6.64

P. Маршрут в пасивному стані. Коли алгоритм DUAL не виконує дифузійні обчислення для визначення шляху до мережі, маршрут знаходиться в стабільному режимі, що називається пасивним станом. Якщо алгоритм DUAL виконує повторне обчислення або пошук нового шляху, то маршрут знаходиться в активному стані і позначається значком A. В стабільному домені маршрутизації всі маршрути в таблиці топології повинні знаходитися в пасивному стані.

192.168.1.0/24. Мережа призначення, яка також знаходиться в таблиці маршрутизації.

1 successors. Показує кількість наступників для цієї мережі. Якщо до цієї мережі веде кілька шляхів з однаковою вартістю, то і наступників теж буде кілька.

FD is 3012096. Допустима відстань, метрика EIGRP для досягнення мережі призначення. Це метрика, який показується в таблиці IP-маршрутизації.

Як показано на рис., в першій вкладеної записи в результаті міститься наступник:

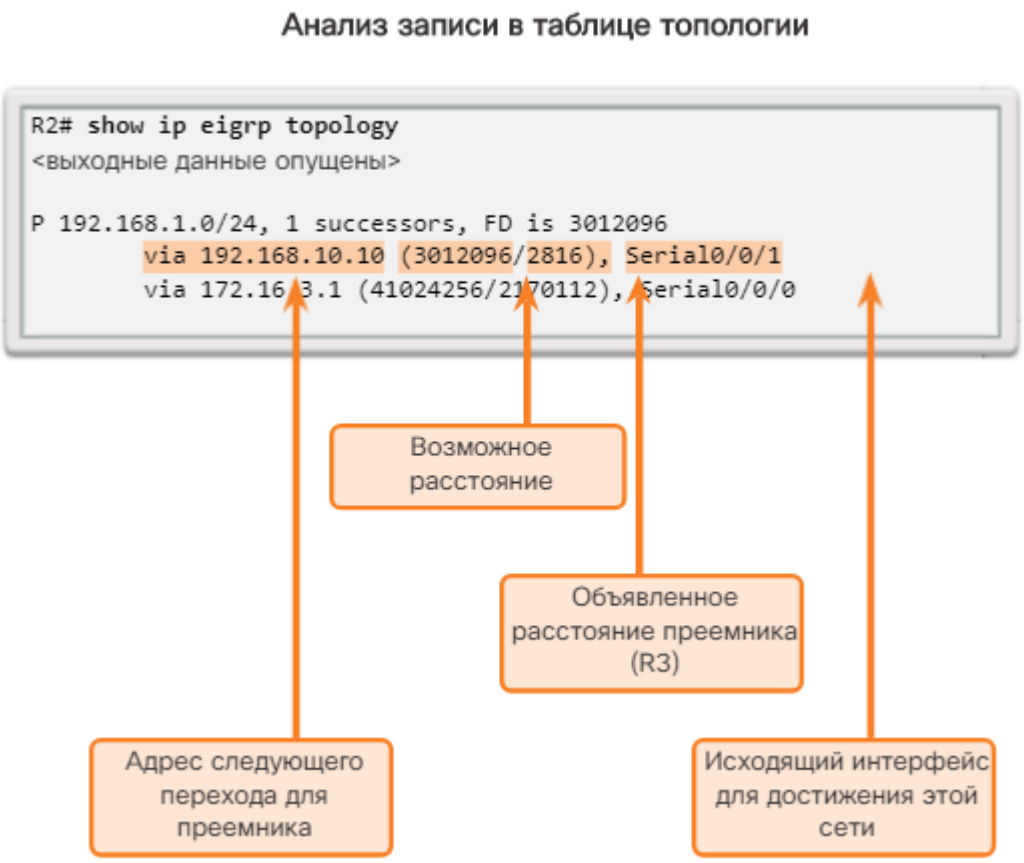


Рис. 5.6.65

via 192.168.10.10. Адреса наступного переходу наступника, маршрутизатор R3. Ця адреса вказана в таблиці маршрутизації.

3012096. Допустима відстань для мережі 192.168.1.0/24. Це метрика, який показується в таблиці IP-маршрутизації.

2816. RD наступника і вартість досягнення цієї мережі для маршрутизатора R3.

Serial 0/0/1. Вихідний інтерфейс, використовуваний для досягнення цієї мережі, також наводиться в таблиці маршрутизації.

Як показано на рис. 3, друга вкладена запис вказує можливого наступника, маршрутизатор R1 (якщо немає другого запису, можливі наступники відсутні):

Рис. 5.6.66

via 172.16.3.1. Адреса наступного переходу для можливого наступника, маршрутизатор R1.

41024256. Нове допустима відстань до мережі 192.168.1.0/24 для маршрутизатора R2, якщо маршрутизатор R1 став новим спадкоємцем і буде новою метрикою, яка відображається в таблиці IP-маршрутизації.

2170112. RD для можливого наступника або метрика маршрутизатора R1 для досягнення цієї мережі. Для виконання умови здійсненності відстань RD повинно бути менше поточного допустимого відстані, еквівалент 3 012 096.

Serial 0/0/0. Це вихідний інтерфейс, використовуваний для досягнення можливого наступника, якщо цей маршрутизатор стає наступником.

Таблиця топології. Відсутність можливого наступника

Щоб зрозуміти, як в алгоритмі DUAL використовуються наступники і можливі наступники, проаналізуйте таблицю маршрутизації R1, вважаючи, що мережа зійшлася.

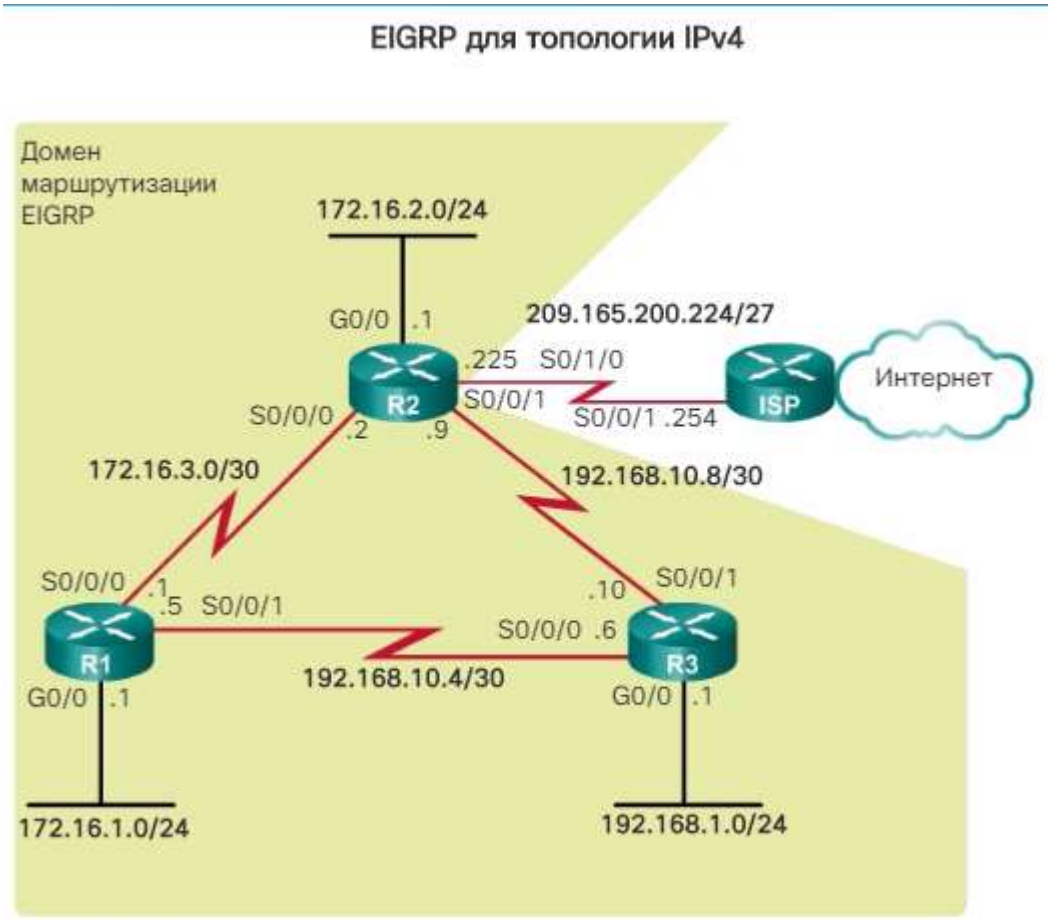


Рис. 5.6.67

На рис. показана частина результатів команди show ip route для маршрутизатора R1. Маршрут до 192.168.1.0/24 показує, що наступником є маршрутизатор R3 через мережу 192.168.10.6 з допустимим відстанню, рівним 2 170 112.

Рис. 5.6.68

Таблиця IP-маршрутизації містить тільки оптимальний маршрут, наступник. Щоб зрозуміти, чи існують можливі наступники, необхідно проаналізувати таблицю топології EIGRP. У таблиці топології на рис. 3 показаний тільки наступник 192.168.10.6, яким є маршрутизатор R3. Можливі наступники відсутні. Якщо поглянути на фактичну фізичну топологію або

схему мережі, очевидно наявність резервного маршруту до мережі 192.168.1.0/24 через маршрутизатор R2. Маршрутизатор R2 не є можливим наступником, так як для нього не виконується умова здійсненності. Хоча, згідно з топології, очевидно, що R2 є резервним маршрутом, у EIGRP відсутня схема топології мережі. EIGRP є протоколом маршрутизації на основі векторів відстаней і отримує інформацію про віддалених мережах від своїх сусідніх пристроїв.

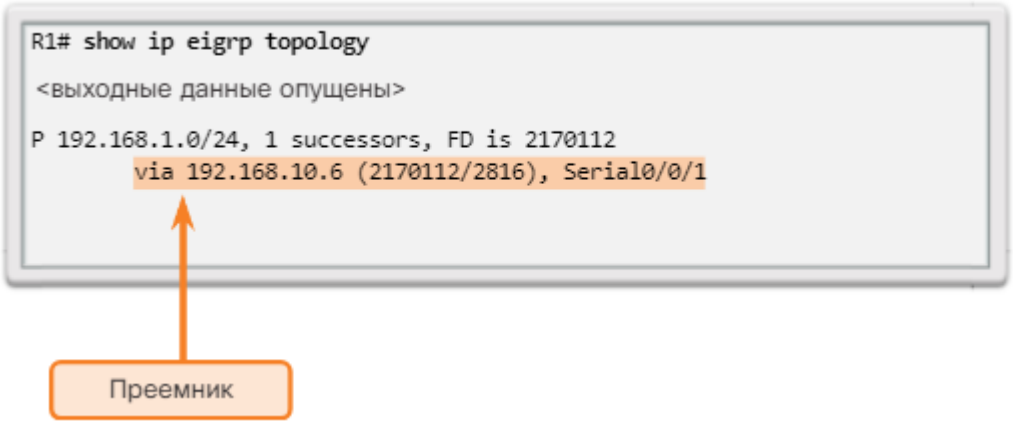


Рис. 5.6.69

Алгоритм DUAL не зберігає маршрут через маршрутизатор R2 в таблиці топології. Всі канали можна переглянути за допомогою команди show ip eigrp topology all-links. Ця команда виводить для каналів відомості про те, чи виконується для них умова здійсненності чи ні.

Як показано на рис. 4, команда show ip eigrp topology all-links виводить всі доступні шляхи до мережі, в тому числі наступники, можливі наступники і навіть маршрути, які не є можливими наступниками. Допустима відстань маршрутизатора R1 для мережі 192.168.1.024/ дорівнює 2 170 112 через наступника R3. Щоб маршрутизатор R2 вважався можливим наступником, для нього має виконуватися умова здійсненності. Відстань RD від маршрутизатора R2 до маршрутизатора R1 для досягнення мережі 192.168.1.0/24 має бути менше поточного допустимого відстані маршрутизатора R1. Згідно малюнку, відстань RD маршрутизатора R2 дорівнює 3 012 096, що більше ніж поточний допустима відстань маршрутизатора R1, що дорівнює 2 170 112.

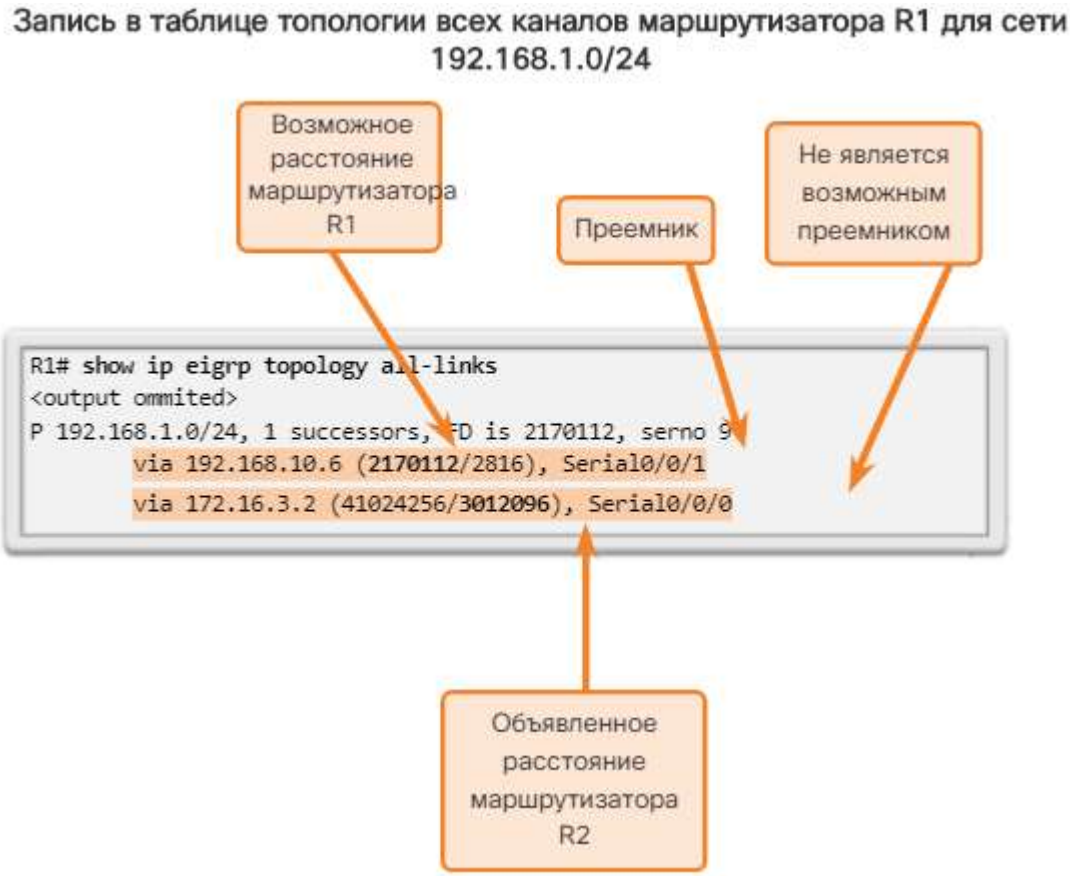


Рис. 5.6.70

Навіть якщо маршрутизатор R2 виглядає як можливий резервний шлях до мережі 192.168.1.0/24, маршрутизатора R1 невідомо, що всередині цього шляху немає можливих петель. Протокол EIGRP - це протокол маршрутизації на основі векторів відстані, без можливості переглянути повну, без петель, топологічну схему мережі. Щоб гарантувати відсутність петель для маршруту, що забезпечується сусіднім пристроєм, алгоритм DUAL перевіряє, чи задовольняє метрика сусіднього маршрутизатора умові здійсненності. Завдяки тому, що відстань RD сусіднього пристрою менше власного допустимого відстані маршрутизатора, цей маршрутизатор може вважати, що сусідній маршрутизатор не є частиною маршруту, оголошеного самим цим маршрутизатором, що дозволяє повністю усунути можливість появи петель.

Маршрутизатор R2 може використовуватися в якості наступника в разі відмови маршрутизатора R3. Але при цьому збільшується затримка його додавання в таблицю маршрутизації. Перш ніж маршрутизатор R2 можна буде використовувати в якості наступника, алгоритм DUAL повинен скористатися додатковими функціями.

Центральним компонентом протоколу EIGRP є алгоритм DUAL і його механізм розрахунку маршрутів EIGRP. Ця технологія називається кінцевим автоматом (Finite State Machine, FSM) DUAL. Цей кінцевий автомат містить всю логіку, використовувану для розрахунку і порівняння маршрутів в мережі EIGRP. На малюнку показаний спрощений випуск кінцевого автомата DUAL.

Кінцевий автомат - це абстрактна машина, а не механічний пристрій з рухомими частинами. Кінцеві автомати визначають набір можливих станів, події, що викликають перехід у такий стан, і події, які є результатом цих станів. Конструктори використовують кінцеві автомати, щоб описати, як пристрій,

комп'ютерна програма або алгоритм маршрутизації реагують на набір вхідних подій.

Кінцеві автомати не розглядаються в даному курсі. Але відповідна концепція використовується для аналізу результатів роботи кінцевого автомата EIGRP, одержуваних за допомогою команди debug eigrp fsm. Використовуйте цю команду, щоб переглянути дії алгоритму DUAL в разі видалення маршруту з таблиці маршрутизації.

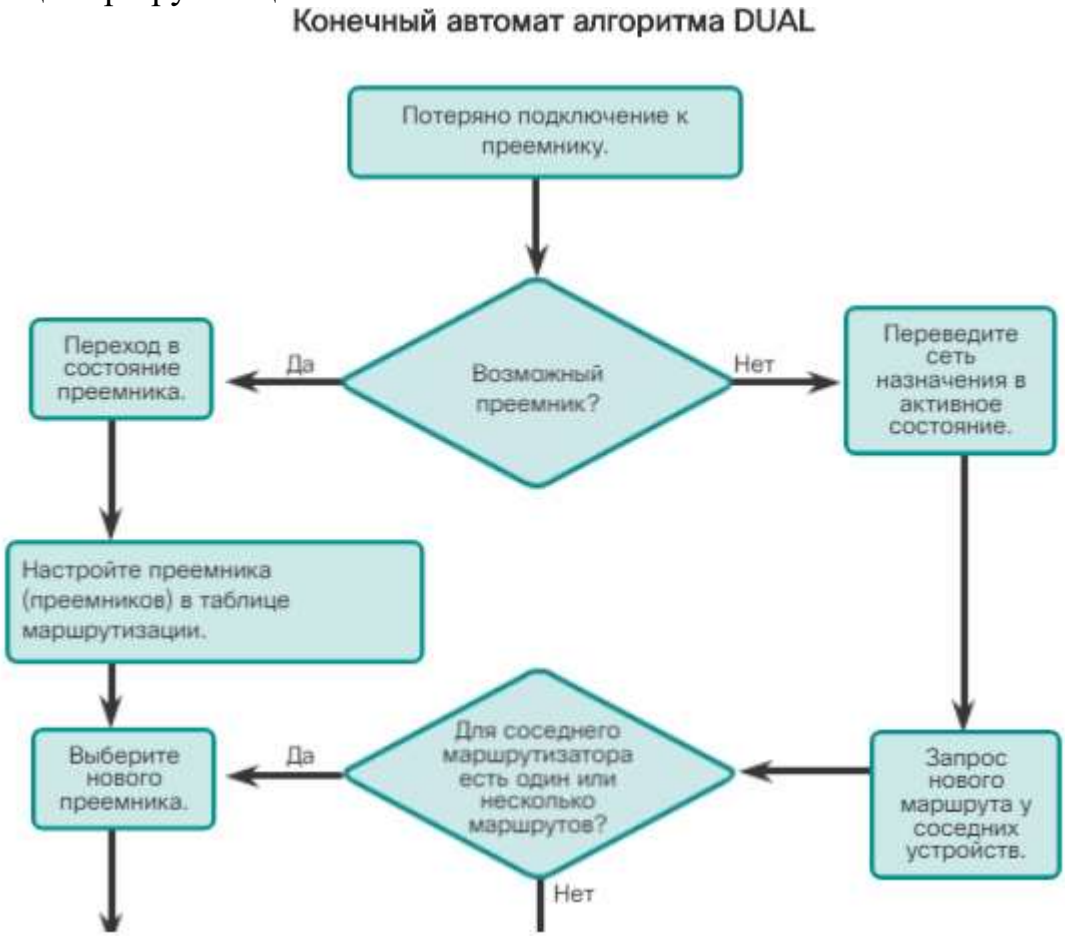


Рис. 5.6.71

Алгоритм DUAL. можливий наступник

Маршрутизатор R2 в даний час використовує маршрутизатор R3 в якості наступника для мережі 192.168.1.0/24. Крім того, маршрутизатор R2 в даний вказує маршрутизатор R1 в якості можливого наступника (FS.

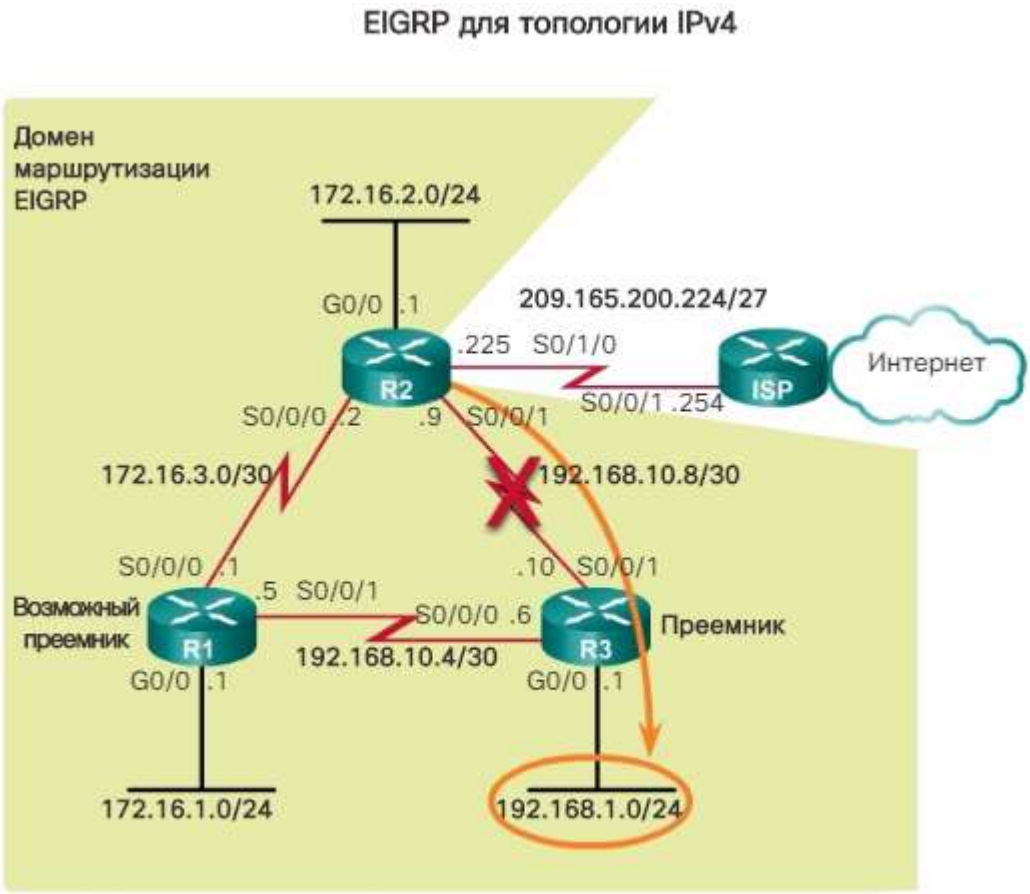


Рис. 5.6.72

Результат команди show ip eigrp topology для маршрутизатора R2 на рис. 2 підтверджує, що маршрутизатор R3 є наступником, а маршрутизатор R1 - можливий наступник для мережі 192.168.1.0/24. Щоб зрозуміти, як алгоритм DUAL може використовувати можливого наступника, коли шлях, який використовує наступника, стає недоступним, імітується відмову каналу між маршрутизаторами R2 і R3.

Запись таблицы топологии маршрутизатора R2 для сети 192.168.1.0/24

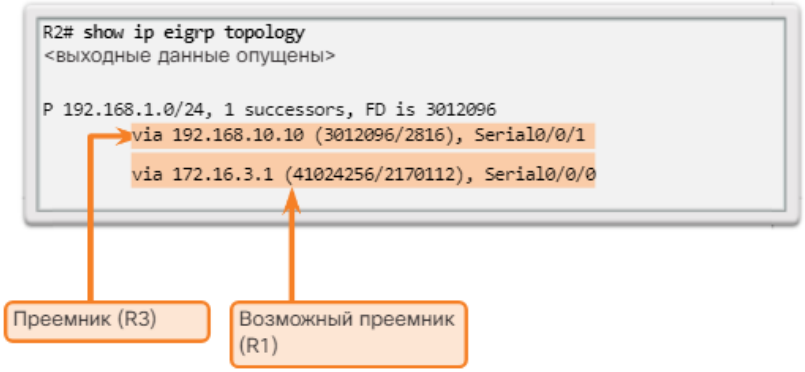


Рис. 5.6.73

Перед імітацією відмови необхідно виконати налагодження DUAL, використовуючи команду debug eigrp fsm на маршрутизаторі R2, як показано на

рис. 3. Відмова каналу імітується за допомогою видачі команди shutdown для інтерфейсу Serial 0/0/1 маршрутизатора R2.

Отладка конечного автомата

```
R2# debug eigrp fsm
EIGRP Finite State Machine debugging is on
R2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# interface s 0/0/1
R2(config-if)# shutdown
<выходные данные опущены>
EIGRP-IPv4(1):Find FS for dest 192.168.1.0/24. FD is 3012096,
RD is 3012096 on tid 0
DUAL: AS(1) Removing dest 172.16.1.0/24, nexthop 192.168.10.10

DUAL: AS(1) RT installed 172.16.1.0/24 via 172.16.3.1
<выходные данные опущены>
R2(config-if)# end
R2# undebug all
```

Рис. 5.6.74

Результат команди debug показує дії, що виконуються алгоритмом DUAL в разі відмови каналу. Маршрутизатор R2 повинен повідомити всім сусіднім пристроїв EIGRP про що відмовив каналі, а також оновити свої таблиці маршрутизації і топології. У цьому прикладі показана тільки частина результатів команди debug. Зокрема, зверніть увагу, що кінцевий автомат алгоритму DUAL шукає і знаходить можливого наступника для маршруту в таблиці топології EIGRP.

Тепер маршрутизатор R1, колишній можливий наступник, стає наступником і поміщається в таблицю маршрутизації в якості нового кращого маршруту до мережі 192.168.1.0/24, як показано на рис. 4. У разі можливого наступника це зміна в таблиці маршрутизації відбувається практично миттєво.

Запись таблицы маршрутизации маршрутизатора R2 для сети 192.168.1.0/24

```
R2# show ip route
<выходные данные опущены>

D 192.168.1.0/24 [90/41024256] via 172.16.3.1, 00:15:51,
Serial0/0/0
```

Новый преемник (R1)

Рис. 5.6.75

Як показано на рис. 5, в таблиці топології маршрутизатора R2 в якості наступника тепер показується маршрутизатор R1, а нові можливі наступники відсутні. Якщо канал між маршрутизаторами R2 і R3 знову стає активним, то маршрутизатор R3 знову стає наступником, а маршрутизатор R1 знову стає можливим наступником (FS).

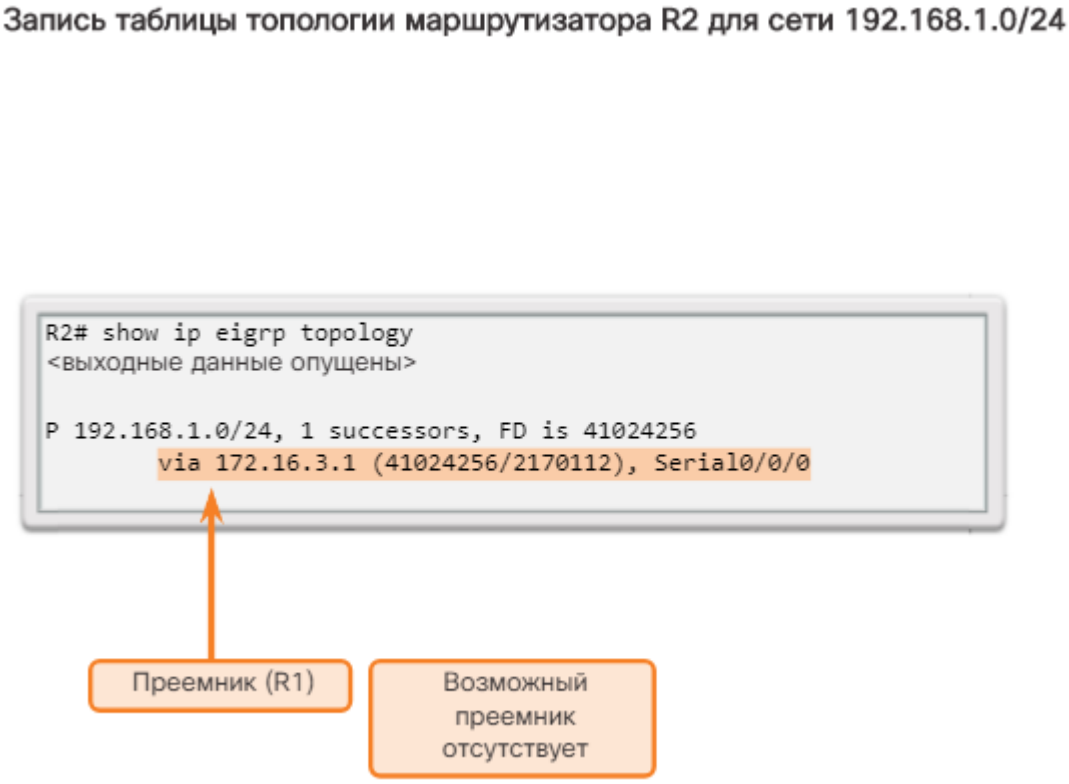


Рис. 5.6.76

Алгоритм DUAL. Відсутність можливого наступника

Іноді шлях до наступника відмовляє, а можливі наступники відсутні. В цьому випадку у алгоритму DUAL відсутня гарантований резервний маршрут без петель до мережі, тому в таблиці топології відсутня шлях, який є можливим наступником. При відсутності можливого наступника в таблиці топології алгоритм DUAL переводить мережу в активний стан. Алгоритм DUAL активно запрошувати сусідні маршрутизатори для визначення нового наступника.

Маршрутизатор R1 в даний час використовує маршрутизатор R3 в якості наступника для мережі 192.168.1.0/24, як показано на рис. 1. Але для маршрутизатора R1 маршрутизатор R2 НЕ позначений як наступника, оскільки він не задовольняє умові здійсненності. Щоб зрозуміти, як алгоритм DUAL виконує пошук нового наступника за відсутності можливого наступника, імітується відмову каналу між маршрутизаторами R1 і R3.

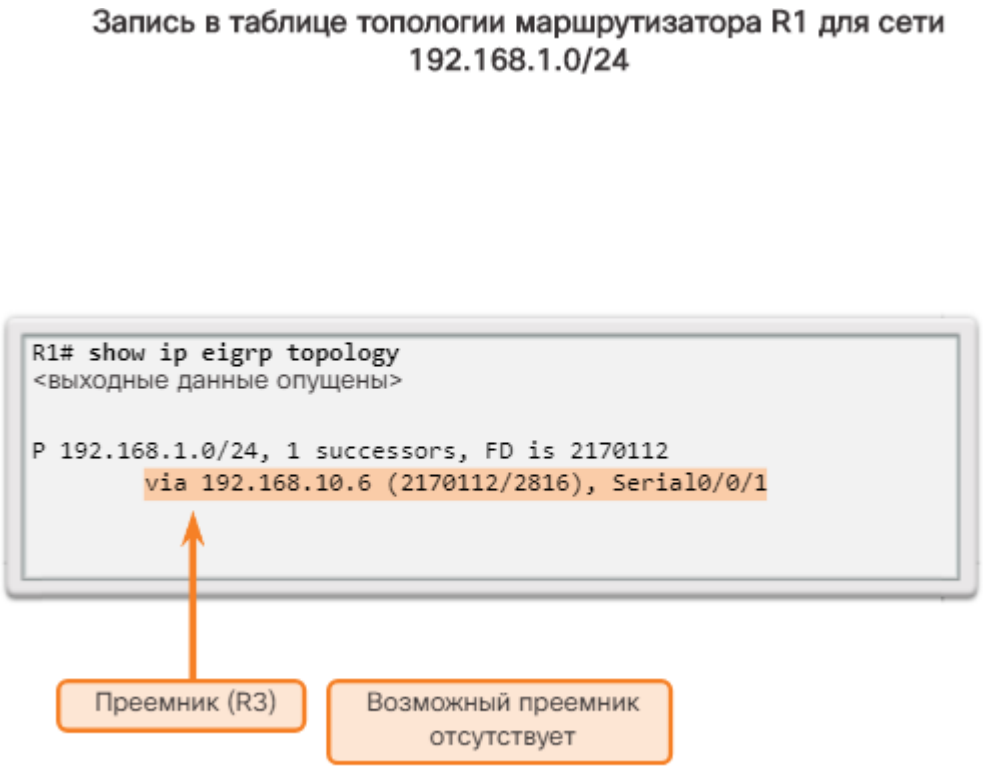


Рис. 5.6.77

Перед імітацією відмови каналу на маршрутизаторі R1 за допомогою команди debug eigrp fsm включається налагодження алгоритму DUAL, як показано на рис. 2. Відмова каналу імітується за допомогою видачі команди shutdown для інтерфейсу Serial 0/0/1 маршрутизатора R1.

Коли наступник стає недоступним, а можливі наступники відсутні, алгоритм DUAL переводить маршрут в активний стан. Алгоритм DUAL відправляє запити EIGRP, запитуючи у іншихмаршрутизаторів маршрут до мережі. Інші маршрутизатори повертають відповіді EIGRP, дозволяючи відправнику EIGRP дізнатися, чи є у цих маршрутизаторів шлях до запитуваної мережі. Якщо жоден з відповідей EIGRP не містить шлях до цієї мережі, у відправника запиту відсутня маршрут до цієї мережі.

Вибрані результати команди debug на рис. 2 показують мережу 192.168.1.0/24, перекладену в активний стан, і запити EIGRP, відправлені іншим сусіднім пристроїв. Маршрутизатор R2 відповідає, повідомляючи шлях до цієї мережі, який стає новим наступником і поміщається в таблицю маршрутизації.

Отладка конечного автомата

```
R1# debug eigrp fsm
EIGRP Finite State Machine debugging is on
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface s 0/0/1
R1(config-if)# shutdown
<выходные данные опущены>
EIGRP-IPv4(1): Find FS for dest 192.168.1.0/24. FD is 2170112,
RD is 2170112
DUAL: AS(1) Dest 192.168.1.0/24 entering active state for tid
0.
EIGRP-IPv4(1): dest(192.168.1.0/24) active
EIGRP-IPv4(1): rcvreply: 192.168.1.0/24 via 172.16.3.2 metric
41024256/3012096 EIGRP-IPv4(1): reply count is 1
EIGRP-IPv4(1): Find FS for dest 192.168.1.0/24. FD is
72057594037927935, RD is 72057594037927935
DUAL: AS(1) Removing dest 192.168.1.0/24, nexthop 192.168.10.6
DUAL: AS(1) RT installed 192.168.1.0/24 via 172.16.3.2

<выходные данные опущены>
R1(config-if)# end
R1# undebug all
```

Рис. 5.6.78

Якщо відправник запитів EIGRP отримує відповіді EIGRP, що містять шлях до запитуваної мережі, кращий шлях додається в якості нового наступника і додається в таблицю маршрутизації. Цей процес займає більше часу, ніж у випадку, коли таблиця топології алгоритму DUAL містить можливого наступника і алгоритм DUAL може швидко додати новий маршрут в таблицю маршрутизації. На рис. 3 зверніть увагу, що у маршрутизатора R1 з'являється новий маршрут до 192.168.1.0/24. Новим наступником EIGRP є маршрутизатор R2.

Запись в таблице маршрутизации маршрутизатора R1 для 192.168.1.0/24

```
R1# show ip route
<выходные данные опущены>

D     192.168.1.0/24 [90/41024256] via 172.16.3.2, 00:05:25,
      Serial0/0/0
```

Новый преемник (R2)

Рис. 5.6.79

На рис. показано, що таблиця топології для маршрутизатора R1 тепер містить маршрутизатор R2 в якості наступника і не містить нових можливих наступників. Якщо канал між маршрутизаторами R1 і R3 знову стає активним,

то маршрутизатор R3 також знову стає наступником. Але маршрутизатор R2 все ще не є можливим наступником, оскільки для нього не виконується умова здійсненності.

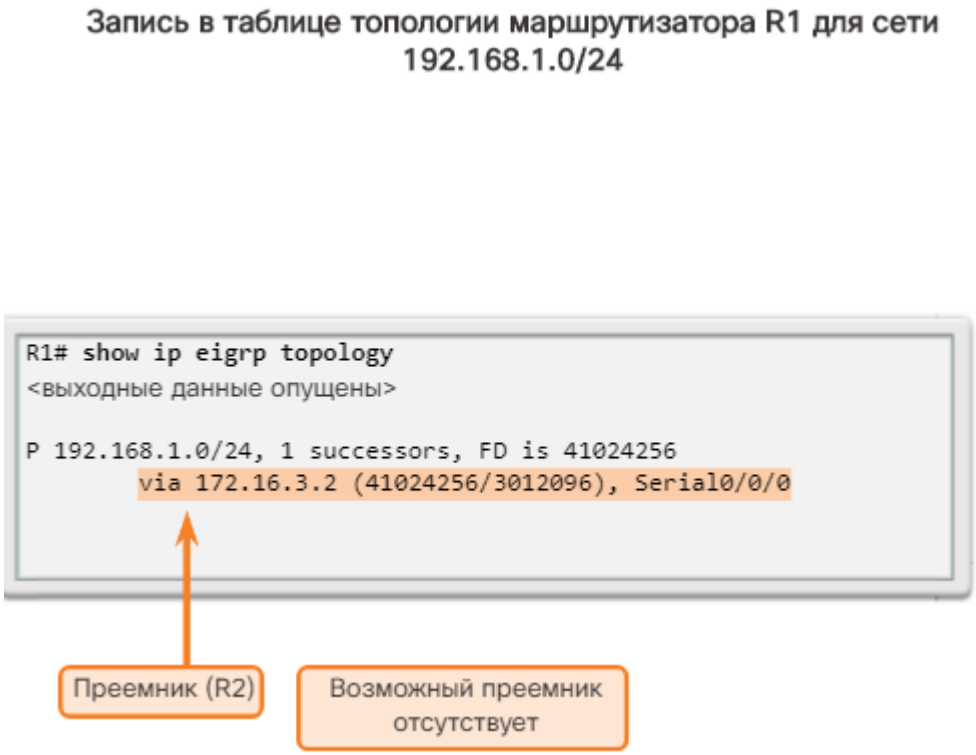


Рис. 5.6.80

Аналогічно своєму аналогу для IPv4, протокол EIGRP для IPv6 обмінюється даними про маршрути, щоб заповнити таблицю маршрутизації IPv6 префіксами віддалених мереж. EIGRP для IPv6 з'явився в Cisco IOS, випуск 12.4 (6) T.

Примітка. В IPv6 мережевою адресою називається префікс, а маска підмережі називається довжиною префікса.

EIGRP для IPv4 виконується на основі мережевого рівня IPv4, взаємодіючи з іншими IPv4-вузлами EIGRP і оголошуючи лише маршрути IPv4. EIGRP для IPv6 виконує ті ж функції, що і EIGRP для IPv4, але в якості транспорту мережевого рівня використовує IPv6, взаємодіючи з іншими IPv6-вузлами EIGRP і оголошуючи маршрути IPv6.

EIGRP для IPv6 також використовує алгоритм DUAL як механізм обчислень, що гарантує побудову шляхів без петель і резервних шляхів для всього домену маршрутизації.

Як і всі протоколи маршрутизації IPv6, протокол EIGRP для IPv6 використовує процеси, незалежні від його аналога для IPv4. Процеси та операції по суті є точно такими ж, як і для протоколу маршрутизації IPv4, але вони виконуються незалежно. Кожен з протоколів, EIGRP для IPv4 і EIGRP для IPv6, використовує окремі таблиці сусідніх пристроїв EIGRP, таблиці топології IP EIGRP і таблиці IP-маршрутизації, як показано на малюнку. EIGRP для IPv6 є окремим модулем, що залежать від протоколу (PDM).

Команди налаштування і перевірки EIGRP для IPv6 дуже схожі на команди, які використовуються в EIGRP для IPv4. Ці команди описані нижче в даному розділі.

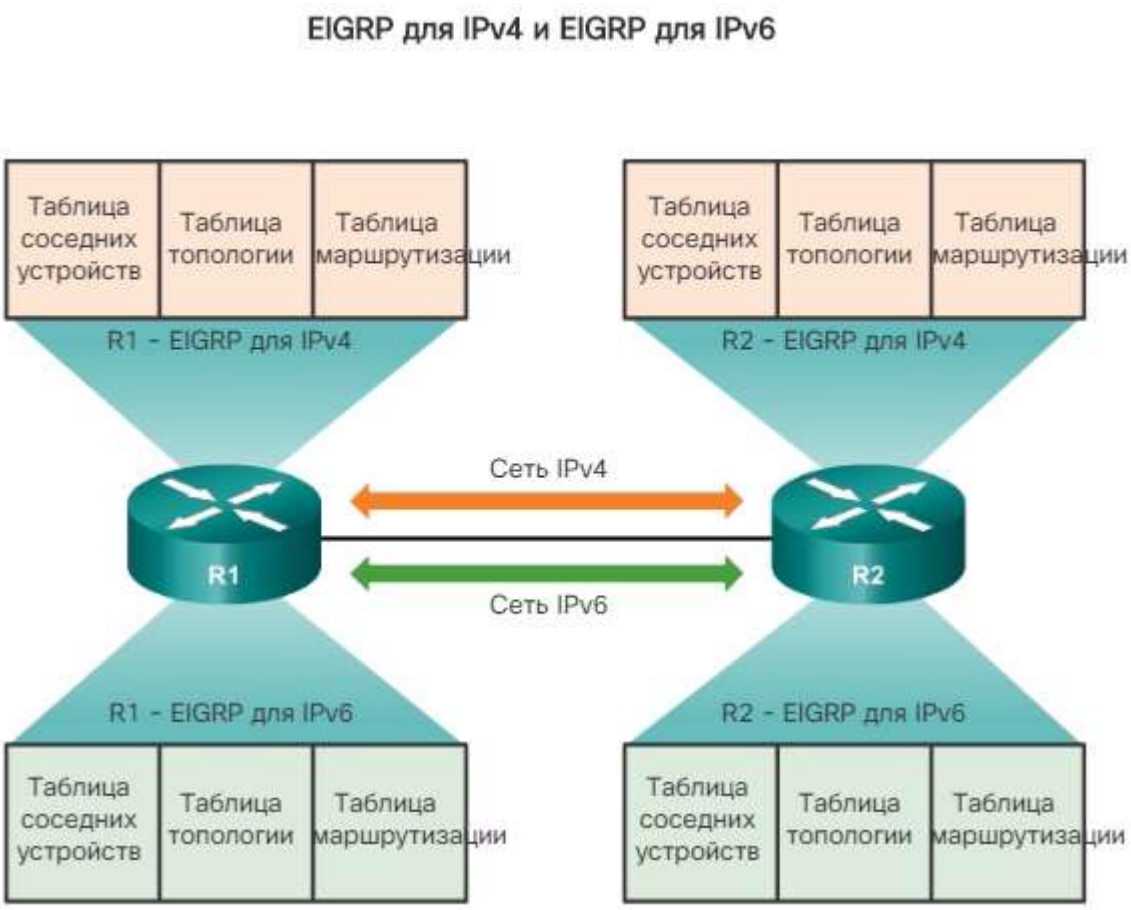


Рис. 5.6.81

Порівняння EIGRP для IPv4 і IPv6

Нижче показано порівняння основних функцій EIGRP для IPv4 і EIGRP для IPv6:

Оголошені маршрути. EIGRP для IPv4 оголошує мережі IPv4, а EIGRP для IPv6 оголошує префікси IPv6.

Вектор відстані. Обидва протоколу EIGRP, для IPv4 і для IPv6, є вдосконаленими протоколами маршрутизації на основі векторів відстані. Обидва протоколу використовують одні і ті ж адміністративні дистанції.

Технологія збіжності. Обидва протоколу EIGRP, для IPv4 і для IPv6, використовують алгоритм DUAL. Обидва протоколу використовують одні і ті ж методи і процеси DUAL, в числі яких наступники, можливі наступники, допустима відстань і RD.

Метрика. Обидва протоколу EIGRP, для IPv4 і для IPv6, використовують у своїй складовою метриці пропускну здатність, затримку, надійність і завантаження. Обидва протоколу маршрутизації застосовують одну і ту ж складову метрику, використовуючи за замовчуванням тільки пропускну здатність і затримку.

Транспортний протокол. Надійний транспортний протокол (Reliable Transport Protocol, RTP) відповідає за гарантовану доставку пакетів EIGRP всім сусіднім пристроїв для обох протоколів, EIGRP для IPv4 і для IPv6.

Повідомлення оновлень. Обидва протоколу EIGRP, для IPv4 і для IPv6, відправляють інкрементні поновлення в разі зміни стану місця призначення. Для оновлення обох протоколів застосовуються терміни «часткове» і «обмежене».

Механізм виявлення сусідніх пристроїв. Обидва протоколу EIGRP, для IPv4 і для IPv6, використовують простий механізм привітань для отримання відомостей про сусідні маршрутизатори та створення відносин суміжності.

Адреси джерела і призначення. EIGRP для IPv4 відправляє повідомлення на адресу групового розсилання 224.0.0.10. В якості адреси джерела в цих повідомленнях використовується IPv4-адрес вихідного інтерфейсу. EIGRP для IPv6 передає свої повідомлення на адресу групового розсилання FF02 :: A. Як джерело повідомлень EIGRP для IPv6 використовується локальний IPv6-адреса каналу вихідного інтерфейсу.

Аутентифікація. EIGRP для IPv4 може використовувати або аутентифікацію без шифрування, або аутентифікацію MD5. У EIGRP для IPv6 використовується MD5.

Ідентифікатор маршрутизатора. Обидва протоколу EIGRP, для IPv4 і для IPv6, використовують 32-бітове число для ідентифікатора маршрутизатора EIGRP. 32-бітний ідентифікатор маршрутизатора представлений в десятковому форматі з розділовими точками і зазвичай називається IPv4-адресою. Якщо у маршрутизатора EIGRP для IPv6 не налаштований IPv4-адрес, для настройки 32-бітного ідентифікатора маршрутизатора необхідно використовувати команду eigrp router-id. Процес визначення ідентифікатора маршрутизатора однаковий для обох протоколів EIGRP, для IPv4 і для IPv6.

Сравнение EIGRP для IPv4 и IPv6

	EIGRP для IPv4	EIGRP для IPv6
Объявленные маршруты	Сети IPV4	Префиксы IPv6
Вектор расстояния	Да	Да
Технология сходимости	DUAL	DUAL
Метрика	Пропускная способность и задержка по умолчанию, надежность и нагрузка дополнительно	Пропускная способность и задержка по умолчанию, надежность и нагрузка дополнительно
Транспортный протокол	RTP	RTP
Сообщения обновлений	Инкрементные, частичные и ограниченные обновления	Инкрементные, частичные и ограниченные обновления
Обнаружение соседних устройств	Пакеты приветствия	Пакеты приветствия
Адреса источника и назначения	IPv4-адрес источника и IPv4-адрес групповой рассылки 224.0.0.10 в качестве адреса	Локальный IPv6-адрес канала в качестве адреса источника и IPv6-адрес

Рис. 5.6.82

Локальні IPv6-адреси каналу

Маршрутизатор, на яких працює протокол динамічної маршрутизації, такий як EIGRP, обмінюються повідомленнями з сусідніми пристроями, що

знаходяться в тій же підмережі або підключеними до цього ж каналу. Маршрутизаторів потрібно обмінюватися повідомленнями протоколу маршрутизації тільки зі своїми безпосередньо підключеними сусідами. Ці повідомлення завжди відправляються з IP-адреси маршрутизатора-джерела, що виконує пересилку.

Локальні IPv6-адреси каналу ідеально підходять для цієї мети. Локальний IPv6-адреса каналу забезпечує обмін даними з іншими пристроями, які використовують IPv6, по одному і тому ж каналу і тільки по цьому каналу (підмережі). Пакети з link-local адресою джерела або призначення не можуть бути спрямовані за межі того каналу, в якому створено пакет.

Повідомлення EIGRP для IPv6 відправляються з використанням наступних параметрів:

IPv6-адреса джерела. Це локальний IPv6-адреса каналу вихідного інтерфейсу.

IPv6-адреса призначення. Коли пакет потрібно відправити на адресу групового розсилання, він відправляється по IPv6-адресу FF02 :: A, який є адресою всіх маршрутизаторів EIGRP в області дії локального каналу. Якщо пакет може бути відправлений як пакет з індивідуальним адресою, він відправляється на локальну адресу каналу сусіднього маршрутизатора.

Примітка. Локальні IPv6-адреси каналів знаходяться в діапазоні FE80 :: / 10. / 10 означає, що перші 10 біт - це 1111 1110 10xx xxxx, що призводить до того, що перший гекстет знаходиться в діапазоні від 1111 1110 1000 0000 (FE80) до 1111 1110 1011 1111 (FEBF).

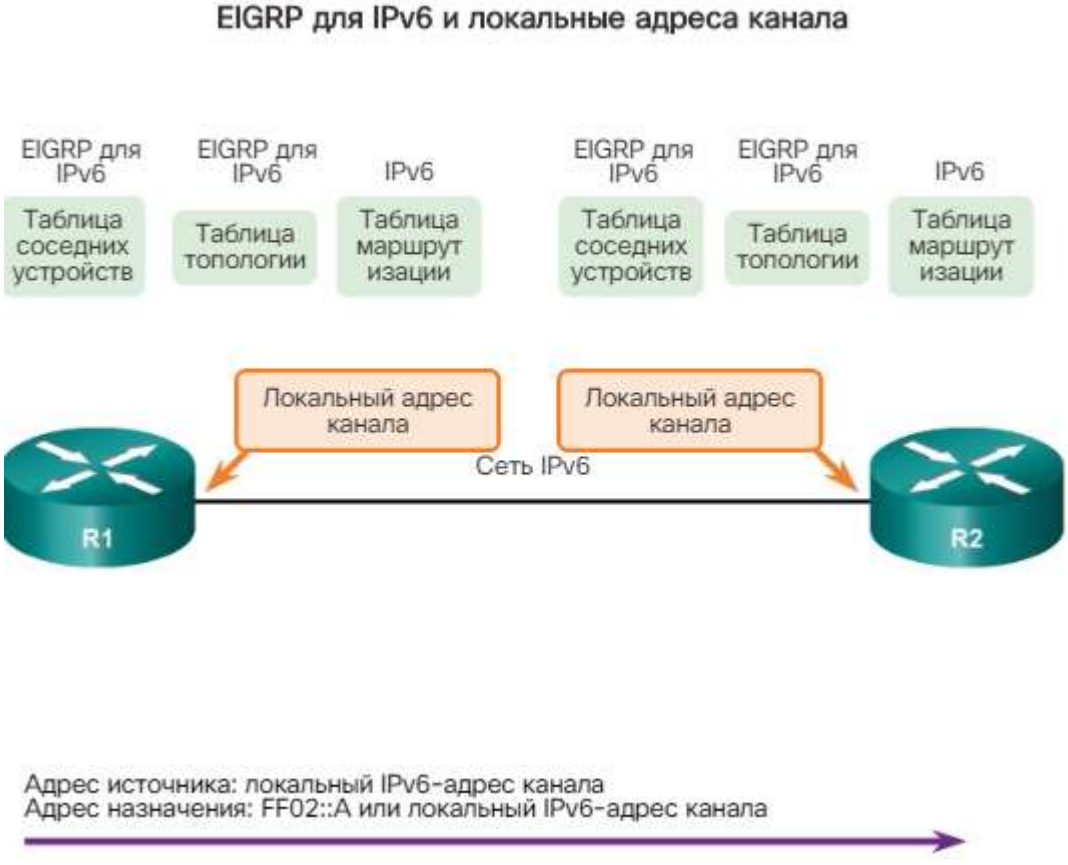


Рис. 5.6.83

На рис. показана топологія мережі, яка використовується в даному прикладі з налаштування EIGRP для IPv6. Якщо мережа працює в двухстековом

режимі, використовуючи IPv4 і IPv6 на всіх пристроях, на всіх маршрутизаторах можна налаштувати обидва протоколи EIGRP, для IPv4 і для IPv6. Але в даному розділі розглядається тільки EIGRP для IPv6.

EIGRP для топологии IPv6

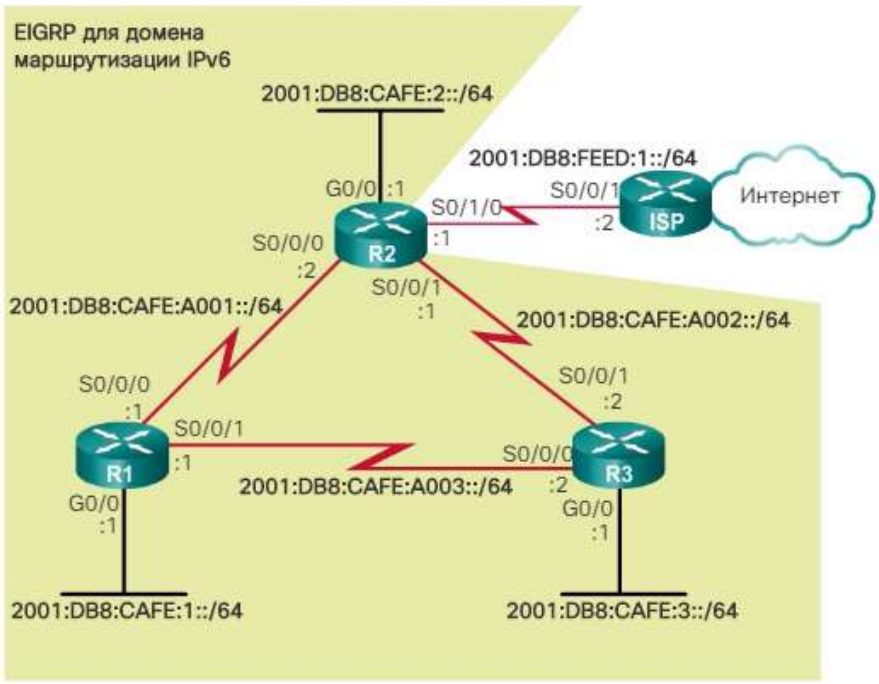


Рис. 5.6.84

Для кожного маршрутизатора налаштовані тільки глобальні індивідуальні адреси IPv6.

На рис. 2, 3 і 4 показані початкові конфігурації інтерфейсів на кожному маршрутизаторі. Зверніть увагу на значення пропускних спроможностей інтерфейсів з попередньої конфігурації EIGRP для IPv4. Оскільки протоколи EIGRP для IPv4 і для IPv6 використовують одні і ті ж метрики, зміна параметрів пропускної здатності впливає на обидва протоколи маршрутизації.

Запуск режима конфигурации интерфейса для маршрутизатора R1

```
R1# show running-config
<выходные данные опущены>
!
interface GigabitEthernet0/0
 ipv6 address 2001:DB8:CAFE:1::1/64
!
interface Serial0/0/0
 ipv6 address 2001:DB8:CAFE:A001::1/64
 clock rate 64000
!
interface Serial0/0/1
 ipv6 address 2001:DB8:CAFE:A003::1/64
```

Рис. 5.6.85

Запуск режима конфигурации интерфейса для маршрутизатора R2

```
R2# show running-config
<выходные данные опущены>
!
interface GigabitEthernet0/0
 ipv6 address 2001:DB8:CAFE:2::1/64
!
interface Serial0/0/0
 ipv6 address 2001:DB8:CAFE:A001::2/64
!
interface Serial0/0/1
 ipv6 address 2001:DB8:CAFE:A002::1/64
 clock rate 64000
!
interface Serial0/1/0
 ipv6 address 2001:DB8:FEED:1::1/64
```

Рис. 5.6.86

Запуск режима конфигурации интерфейса для маршрутизатора R3

```
R3# show running-config
<выходные данные опущены>
!
interface GigabitEthernet0/0
 ipv6 address 2001:DB8:CAFE:3::1/64
!
interface Serial0/0/0
 ipv6 address 2001:DB8:CAFE:A003::2/64
 clock rate 64000
!
interface Serial0/0/1
 ipv6 address 2001:DB8:CAFE:A002::2/64
```

Рис. 5.6.87

Локальні адреси каналів (link-local) створюються автоматично, коли інтерфейсу призначається глобальний індивідуальний IPv6-адреса. Глобальні індивідуальні адреси для інтерфейсу не потрібні, на відміну від локальних IPv6-адрес каналів, які є обов'язковими.

Якщо не використовується ручне налаштування, маршрутизатори Cisco створюють локальну адресу каналу, використовуючи префікс FE80 :: / 10 і процес EUI-64, як показано на рис. 1. EUI-64 передбачає використання 48-бітного MAC-адреси Ethernet, вставку FFFE в центрі і перемикання сьомого біта. Для послідовних інтерфейсів в пристроях Cisco використовується MAC-адресу інтерфейсу Ethernet. Маршрутизатор з декількома послідовними інтерфейсами може призначити всім інтерфейсам IPv6 однакові локальні адреси каналів, оскільки локальні адреси каналів потрібні тільки в рамках локального з'єднання.

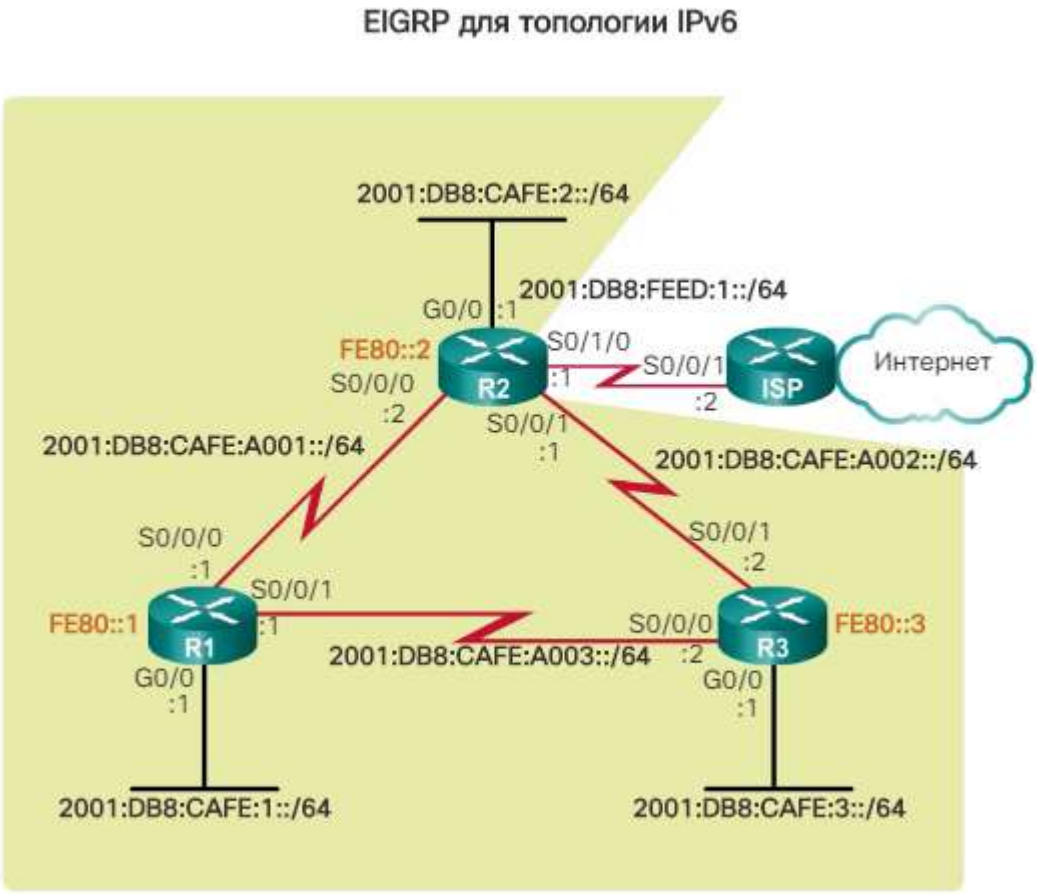


Рис. 5.6.88

Локальні адреси каналів, створені за допомогою формату EUI-64 або, в деяких випадках, випадкових ідентифікаторів інтерфейсів, ускладнюють розпізнавання і запам'ятовування цих адрес. Так як протоколи маршрутизації IPv6 використовують локальні IPv6-адреси каналів для індивідуальної адресації і відомостей про адресу наступного переходу в таблиці маршрутизації, рекомендується, щоб ця адреса був зроблений легко впізнаваним. Налаштування локальної адреси вручну дозволяє створювати адреси, які легко розпізнати і запам'ятати.

Локальні адреси каналів можна налаштовувати вручну за допомогою команди, аналогічної що використовувалася для створення глобальних індивідуальних IPv6-адрес, але з іншими параметрами:

Router (config-if) # ipv6 address link-local-address link-local

Для локального адреси каналу використовується префікс в діапазоні від FE80 до FEBF. Якщо адреса починається з цього гекстета (16-бітний сегмент), за адресою має слідувати ключове слово link-local.

На рис. 2 показана конфігурація локального адреси каналу за допомогою команди режиму конфігурації інтерфейсу ipv6 address. Локальний адреса каналу FE80 :: 1 використовується для вказівки на те, що він належить маршрутизатора R1. Такий же локальний адресу каналу IPv6 налаштований на всіх інтерфейсах маршрутизатора R1. FE80 :: 1 можна налаштувати на кожному каналі, оскільки він повинен бути унікальним тільки на даному каналі.

Настройка локальных адресов канала на маршрутизаторе R1

```
R1(config)# interface s 0/0/0
R1(config-if)# ipv6 address fe80::1 ?
  link-local  Use link-local address

R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface s 0/0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface g 0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)#
```

Рис. 5.6.89

Подібно маршрутизатора R1 на рис. 3, для всіх інтерфейсів маршрутизатора R2 налаштований локальний IPv6-адреса каналу FE80 :: 2.

Настройка локальных адресов канала на маршрутизаторе R2

```
R2(config)# interface s 0/0/0
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# exit
R2(config)# interface s 0/0/1
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# exit
R2(config)# interface s 0/1/0
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# exit
R2(config)# interface g 0/0
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)#
```

Рис. 5.6.90

Як показано на рис. 5, команда show ipv6 interface brief використовується для перевірки локальних IPv6-адрес каналів і глобальних індивідуальних адрес для всіх інтерфейсів.

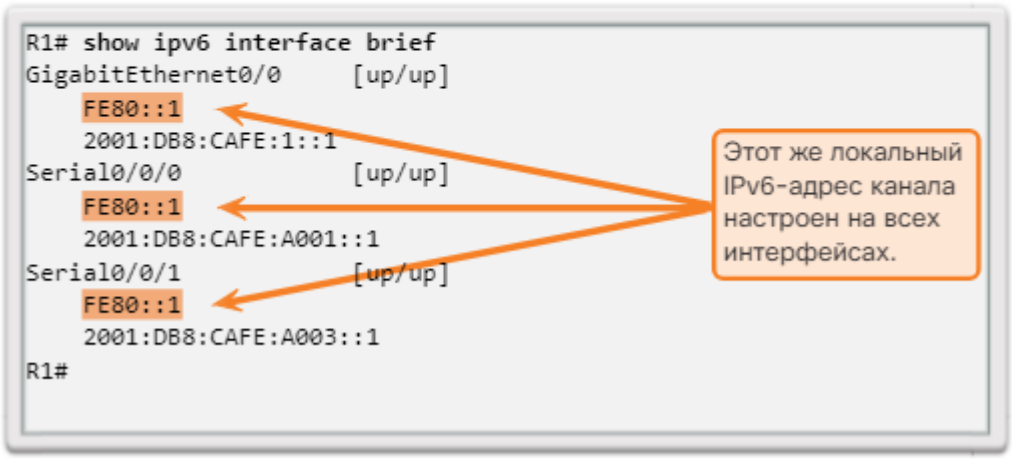


Рис. 5.6.91

Команда режиму глобальної конфігурації ipv6 unicast-routing включає маршрутизацію IPv6 на маршрутизаторі. Дана команда повинна бути виконана перед налаштуванням будь-якого протоколу маршрутизації IPv6. Команда потрібно не для настройки IPv6-адрес на інтерфейсах, а для включення маршрутизатора в якості маршрутизатора IPv6.

EIGRP для IPv6

Щоб перейти в режим конфігурації маршрутизатора для EIGRP для IPv6, використовується наступна команда режиму глобальної конфігурації:

Router (config) # ipv6 router eigrp autonomous-system

Аналогічно EIGRP для IPv4, значення autonomous-system (автономна система) має бути однаковим на всіх маршрутизаторах в домені маршрутизації. На рис. 1 процес маршрутизації EIGRP для IPv6 не може бути налаштований, поки маршрутизація IPv6 не буде активована за допомогою команди режиму глобальної конфігурації ipv6 unicast-routing.

```
R1(config)# ipv6 router eigrp 2
% IPv6 routing not enabled
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 router eigrp 2
R1(config-rtr)#
```

Рис. 5.6.92

Як показано на рис., для настройки ідентифікатора маршрутизатора використовується команда eigrp router-id. EIGRP для IPv6 використовує для ідентифікатора маршрутизатора 32-бітове значення. З метою отримання цього значення протокол EIGRP для IPv6 використовує той же процес, що і EIGRP для IPv4. Команда eigrp router-id має пріоритет над усіма IPv4-адресами інтерфейсів loopback або фізичних інтерфейсів. Якщо у маршрутизатора EIGRP

для IPv6 немає активних інтерфейсів з IPv4-адресою, буде потрібно команда eigrp router-id.

```
R1(config)# ipv6 router eigrp 2
R1(config-rtr)# eigrp router-id 1.0.0.0
R1(config-rtr)#
```

Рис. 5.6.93

Ідентифікатор маршрутизатора повинен бути 32-бітових числом, унікальним в IP-домені маршрутизації EIGRP. В іншому випадку можливі конфлікти маршрутизації.

Примітка. Щоб налаштувати ідентифікатор маршрутизатора для EIGRP, використовується команда eigrp router-id. Деякі випуски IOS допускають використання команди router-id (ідентифікатор маршрутизатора) без попереднього вказівки eigrp. Але в поточній конфігурації, незалежно від використаної команди, показується eigrp router-id.

За замовчуванням процес EIGRP для IPv6 знаходиться в відключеному стані. Щоб включити процес EIGRP для IPv6, потрібно команда no shutdown, як показано на рис. 3. У разі EIGRP для IPv4 ця команда не потрібно. Хоча EIGRP для IPv6 включений, обмін відносинами суміжності і оновленнями маршрутизації з сусідніми пристроями неможливий, поки на відповідних інтерфейсах не включений протокол EIGRP.

```
R1(config)# ipv6 router eigrp 2
R1(config-rtr)# eigrp router-id 1.0.0.0
R1(config-rtr)# no shutdown
R1(config-rtr)#
```

Рис. 5.6.94

Маршрутизатора для створення відносин суміжності з сусідніми пристроями потрібно як команда no shutdown, так і ідентифікатор маршрутизатора.

На рис. показана повна конфігурація EIGRP для IPv6 для маршрутизатора R2.

```
R2(config)# ipv6 unicast-routing
R2(config)# ipv6 router eigrp 2
R2(config-rtr)# eigrp router-id 2.0.0.0
R2(config-rtr)# no shutdown
R2(config-rtr)#
```

Рис. 5.6.95

EIGRP для IPv6 використовує інший спосіб включення інтерфейсу для EIGRP. Замість використання команди режиму конфігурації маршрутизатора network для завдання відповідних адрес інтерфейсів, EIGRP для IPv6 налаштовується прямо на інтерфейсі.

Щоб включити EIGRP для IPv6 на інтерфейсі, використовуйте наступну команду режиму конфігурації інтерфейсу:

Router (config-if) # ipv6 eigrp autonomous-system

Значення autonomous-system (автономна система) має збігатися з номером автономної системи, що використовуються для включення процесу маршрутизації EIGRP. Подібно команді network, використовуваної в EIGRP для IPv4, команда ipv6 eigrp interface виконує наступне:

включає інтерфейс для створення відносин суміжності і обміну оновленнями EIGRP для IPv6;

додає префікс (мережа) цього інтерфейсу в оновлення маршрутизації EIGRP для IPv6.

Це повідомлення показує, що маршрутизатор R2 тепер створив відношення суміжності EIGRP-IPv6 з сусіднім пристроєм по локальній адресі каналу FE80 :: 1. Оскільки на всіх трьох маршрутизаторах налаштовані статичні локальні адреси каналів, легко визначити, що це відношення суміжності з маршрутизатором R1 (FE80 :: 1).

Та ж команда passive-interface, що використовувалась для IPv4, застосовується і для настройки пасивного інтерфейсу в EIGRP для IPv6. Як показано на рис. 3, для перевірки конфігурації використовується команда show ipv6 protocols.

Настройка и проверка EIGRP для IPv6 с пассивным интерфейсом

```
R1(config)# ipv6 router eigrp 2
R1(config-rtr)# passive-interface gigabitethernet 0/0
R1(config-rtr)# end

R1# show ipv6 protocols

IPv6 Routing Protocol is "eigrp 2"
EIGRP-IPv6 Protocol for AS(2)
<выходные данные опущены>

  Interfaces:
    Serial0/0/0
    Serial0/0/1
    GigabitEthernet0/0 (passive)
  Redistribution:
    None
R1#
```

Рис. 5.6.96

Аналогічно EIGRP для IPv4, перед обміном будь-якими оновленнями EIGRP для IPv6 маршрутизатори повинні налаштувати свої відносини суміжності з сусідніми пристроями.

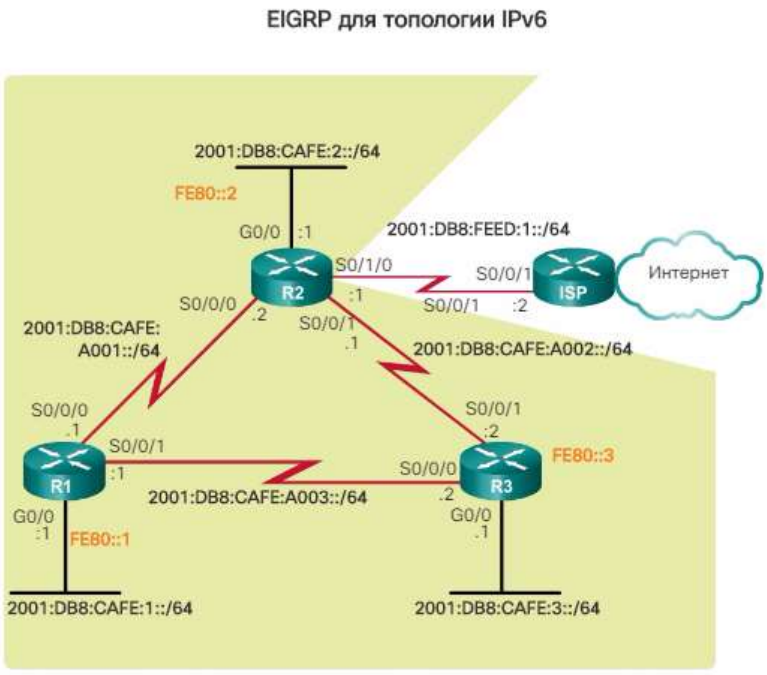


Рис. 5.6.97

Використовуйте команду show ipv6 eigrp neighbors для перегляду таблиці сусідніх вузлів і перевірки встановлення протоколом EIGRP для IPv6 відносин суміжності зі своїми сусідніми маршрутизаторами. Результат, показаний на рис. 2, містить локальний IPv6-адреса каналу для суміжного сусіднього пристрою і інтерфейс, використовуваний маршрутизатором для досягнення цього сусіда EIGRP. Використання зрозумілих локальних адрес каналів спрощує розпізнавання сусідніх пристроїв - маршрутизатора R2 з адресою FE80 :: 2 і маршрутизатора R3 з адресою FE80 :: 3.

Рис. 5.6.98

Результат команди show ipv6 eigrp neighbors містить наступні дані:

Стовпець H. Містить списки сусідніх пристроїв в порядку отримання відомостей про них.

Address. Локальний IPv6-адреса каналу для сусіднього пристрою.

Interface. Локальний інтерфейс, через який було отримано цей пакет вітання.

Hold. Поточний час утримання. Після отримання пакета вітання для цього значення встановлюється максимальне для цього інтерфейсу час утримання, після чого починається зворотний відлік. При досягненні нуля сусіднє пристрій вважається несправним.

Uptime. Час, що минув з моменту додавання цього сусіднього пристрою в таблицю сусідніх пристроїв.

SRTT і RTO. Використовуються протоколом RTP для управління надійної доставкою пакетів EIGRP.

Queue Count. Лічильник черзі. Повинен бути завжди рівним нулю. Якщо він більше нуля, існують пакети EIGRP, які очікують свого надсилання.

Sequence Number. Порядковий номер, який використовується для відстеження пакетів оновлень, запитів і відповідей.

Команда show ipv6 eigrp neighbors корисна для перевірки і усунення проблем EIGRP для IPv6. Якщо очікуване сусіднє пристрій відсутній у списку, переконайтеся, що обидва інтерфейсу знаходяться в робочому стані (up / up), використовуючи команду show ipv6 interface brief. У разі EIGRP для IPv6 пред'являються ті ж вимоги до встановлення відносин суміжності з сусідніми пристроями, як і в разі EIGRP для IPv4. Якщо інтерфейси на обох сторонах каналу активні, перевірте наступні параметри.

Налаштовані обидва маршрутизатора з використанням одного і того ж номера автономної системи EIGRP?

Заданий для інтерфейсу, на якому включений протокол EIGRP для IPv6, правильний номер автономної системи?

Перевірка EIGRP для IPv6. Команда show ip protocols

Команда show ipv6 protocols виводить параметри і іншу інформацію про стан усіх активних процесів протоколів маршрутизації IPv6, налаштованих в даний момент на маршрутизаторі. Команда show ipv6 protocols виводить різні типи результатів для кожного з протоколів маршрутизації IPv6.

Результат, показаний на малюнку, містить дещо раніше обговорювалися параметрів EIGRP для IPv6, в тому числі такі.

1. EIGRP для IPv6 є активним протоколом динамічної маршрутизації на маршрутизаторі R1, налаштованим з використанням номера автономної системи 2.

2. Для обчислення складовою метрики EIGRP використовується ряд значень k. За замовчуванням K1 і K3 рівні 1, а K2, K4 і K5 за замовчуванням рівні 0.

3. Ідентифікатор маршрутизатора R1 протоколу EIGRP для IPv6 дорівнює 1.0.0.0.

4. Аналогічно EIGRP для IPv4, адміністративні дистанції в разі EIGRP для IPv6 визначаються наступним чином: внутрішнє AD одно 90, а зовнішнє AD одно 170 (значення за замовчуванням).

5. На інтерфейсах включена підтримка протоколу EIGRP для IPv6.

Результат команди show ipv6 protocols корисний при налагодженні операцій маршрутизації. У розділі Interfaces показується, для яких інтерфейсів

включена підтримка EIGRP для IPv6. Це корисно при перевірці того, що протокол EIGRP включений на всіх відповідних інтерфейсах, з правильно заданим номером автономної системи.

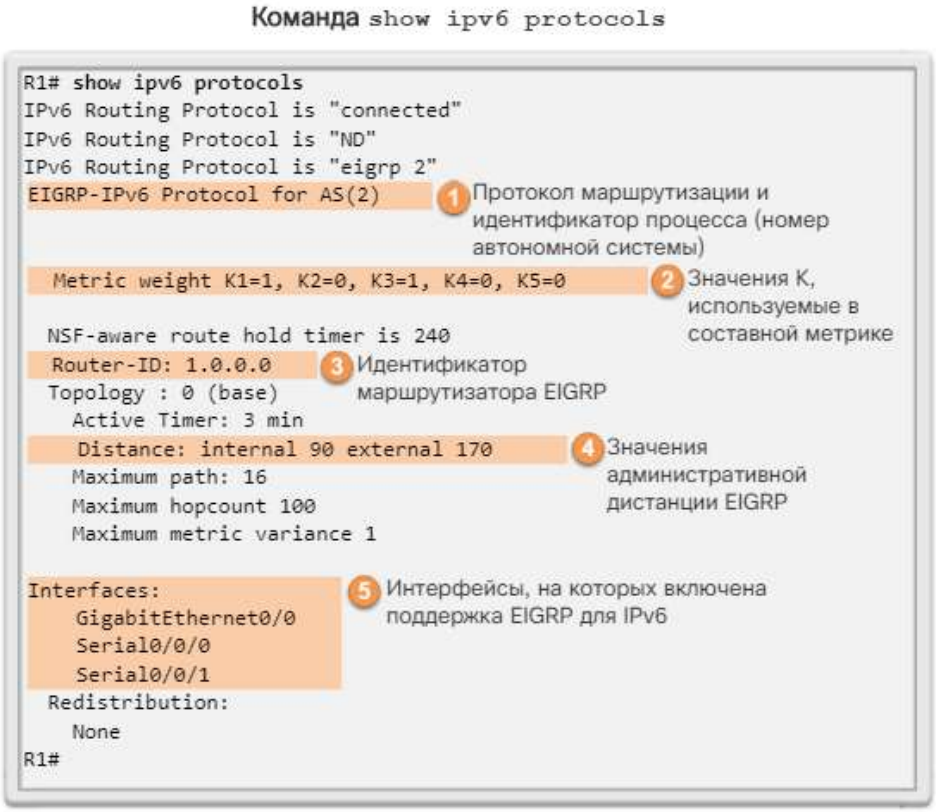


Рис. 5.6.99

Перевірка EIGRP для IPv6: аналіз таблиці маршрутизації IPv6

Як і в разі будь-якого протоколу маршрутизації, мета полягає в тому, щоб заповнити таблицю IP-маршрутизації маршрутами до віддалених мереж і оптимальними шляхами для досягнення цих мереж. Як і в разі IPv4, важливо проаналізувати таблицю маршрутизації IPv6 і визначити, чи заповнено вона правильними маршрутами.

Для перегляду таблиці маршрутизації IPv6 використовується команда show ipv6 route. Маршрути EIGRP для IPv6 в таблиці маршрутизації позначені кодом D, так само, як і їх аналоги для IPv4.

На рис. 1 показано, що маршрутизатор R1 помістив в свою таблицю маршрутизації IPv6 три маршрути EIGRP до віддалених мереж IPv6:

Анализ таблицы маршрутизации IPv6 маршрутизатора R1

```
R1# show ipv6 route
 <выходные данные опущены>
C   2001:DB8:CAFE:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:CAFE:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
D   2001:DB8:CAFE:2::/64 [90/3524096]
     via FE80::3, Serial0/0/1
D   2001:DB8:CAFE:3::/64 [90/2170112]
     via FE80::3, Serial0/0/1
C   2001:DB8:CAFE:A001::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:CAFE:A001::1/128 [0/0]
     via Serial0/0/0, receive
D   2001:DB8:CAFE:A002::/64 [90/3523840]
     via FE80::3, Serial0/0/1
C   2001:DB8:CAFE:A003::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:CAFE:A003::1/128 [0/0]
     via Serial0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

Рис. 5.6.100

2001: DB8: CAFE: 2 :: / 64 через маршрутизатор R3 (FE80 :: 3), використовуючи його інтерфейс Serial 0/0/1

2001: DB8: CAFE: 3 :: / 64 через маршрутизатор R3 (FE80 :: 3), використовуючи його інтерфейс Serial 0/0/1

2001: DB8: CAFE: A002 :: / 64 через маршрутизатор R3 (FE80 :: 3), використовуючи його інтерфейс Serial 0/0/1

Всі три маршрути використовують маршрутизатор R3 в якості маршрутизатора наступного переходу (наступник). Зверніть увагу, що таблиця маршрутизації в якості адреси наступного переходу використовує локальну адресу каналу. Оскільки для всіх інтерфейсів кожного маршрутизатора налаштовані унікальні і помітні локальні адреси каналу, легко виявити, що маршрутизатором наступного переходу через FE80 :: 3 є маршрутизатор R3.

На рис. показана таблиця маршрутизації IPv6 для маршрутизатора R2.

Анализ таблицы маршрутизации IPv6 маршрутизатора R2

```
R2# show ipv6 route
 <выходные данные опущены>
D   2001:DB8:CAFE:1::/64 [90/3524096]
     via FE80::3, Serial0/0/1
C   2001:DB8:CAFE:2::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:CAFE:2::1/128 [0/0]
     via GigabitEthernet0/0, receive
D   2001:DB8:CAFE:3::/64 [90/3012096]
     via FE80::3, Serial0/0/1
C   2001:DB8:CAFE:A001::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:CAFE:A001::2/128 [0/0]
     via Serial0/0/0, receive
C   2001:DB8:CAFE:A002::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:CAFE:A002::1/128 [0/0]
     via Serial0/0/1, receive
D   2001:DB8:CAFE:A003::/64 [90/3523840]
     via FE80::3, Serial0/0/1
C   2001:DB8:FEED:1::/64 [0/0]
     via Loopback6, directly connected
L   2001:DB8:FEED:1::1/128 [0/0]
     via Loopback6, receive
L   FF00::/8 [0/0]
```

Рис. 5.6.101

На рис. показана таблиця маршрутизації для маршрутизатора R3. Зверніть увагу, що у маршрутизатора R3 два шляхи з рівною вартістю до мережі 2001: DB8: CAFE: A001 :: / 64. Один шлях через маршрутизатор R1 з адресою FE80 :: 1, а інший шлях через маршрутизатор R2 з адресою FE80 :: 2.

Анализ таблицы маршрутизации IPv6 маршрутизатора R3

```
R3# show ipv6 route
 <выходные данные опущены>
D   2001:DB8:CAFE:1::/64 [90/2170112]
     via FE80::1, Serial0/0/0
D   2001:DB8:CAFE:2::/64 [90/3012096]
     via FE80::2, Serial0/0/1
C   2001:DB8:CAFE:3::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:CAFE:3::1/128 [0/0]
     via GigabitEthernet0/0, receive
D   2001:DB8:CAFE:A001::/64 [90/41024000]
     via FE80::1, Serial0/0/0
     via FE80::2, Serial0/0/1
C   2001:DB8:CAFE:A002::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:CAFE:A002::2/128 [0/0]
     via Serial0/0/1, receive
C   2001:DB8:CAFE:A003::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:CAFE:A003::2/128 [0/0]
     via Serial0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R3#
```

Рис. 5.6.102

EIGRP (Enhanced Interior Gateway Routing Protocol) - це безкласовий протокол маршрутизації на основі векторів відстані. EIGRP це засіб оптимізації іншого протоколу маршрутизації Cisco - IGRP (Interior Gateway Routing Protocol). Спочатку EIGRP з'явився в 1992 році як власний протокол компанії

Cisco, доступний тільки на пристроях Cisco. У 2013 р компанія Cisco представила організації IETF основні функції EIGRP у вигляді відкритого стандарту.

Протокол EIGRP використовує для алгоритму DUAL в таблиці маршрутизації позначення джерела «D». За замовчуванням EIGRP застосовує адміністративну дистанцію 90 для внутрішніх маршрутів і 170 для маршрутів, імпортованих із зовнішнього джерела, таких як маршрути за замовчуванням.

EIGRP - це вдосконалений протокол маршрутизації на основі векторів відстані, що підтримує функції, відсутні в інших протоколах маршрутизації на основі векторів відстаней, таких як RIP. До цих функцій належать: алгоритм дифузного поновлення DUAL, встановлення відносин суміжності з сусідніми пристроями, надійний транспортний протокол RTP, часткові і обмежені поновлення, а також розподіл навантаження з рівної і нерівній вартістю.

Протокол EIGRP використовує залежні модулі протоколів PDM, що надають можливість підтримки різних протоколів 3-го рівня, включаючи IPv4 і IPv6. Протокол EIGRP використовує надійний транспортний протокол (RTP) в якості протоколу транспортного рівня для доставки пакетів EIGRP. Протокол EIGRP використовує надійну передачу для оновлень, запитів і відповідей EIGRP, а для привітань і підтверджень EIGRP використовується ненадійна доставка. Надійний RTP означає необхідність повернення підтвердження EIGRP.

Перед відправкою оновлень EIGRP маршрутизатор спочатку повинен виявити свої сусідні пристрої. Це робиться за допомогою пакетів вітання EIGRP. Щоб два маршрутизатора могли стати сусідніми пристроями, значення вітань і утримання не зобов'язані збігатися. Використовуйте команду show ip eigrp neighbors для перегляду таблиці сусідніх пристроїв і перевірки встановлення протоколом EIGRP відносин суміжності зі своїми сусідніми маршрутизаторами.

На відміну від протоколу маршрутизації, EIGRP не надсилає періодичні оновлення. EIGRP відправляє часткові або обмежені поновлення, що містять тільки зміни маршрутів, і тільки тим маршрутизаторам, на роботу яких впливають зміни. Для визначення найкращого маршруту протокол EIGRP використовує складову метрику, що враховує пропускну здатність, затримку, надійність і завантаження. За замовчуванням використовуються тільки пропускна здатність і затримка.

Центром EIGRP служить алгоритм дифузного поновлення DUAL (Diffusing Update Algorithm). Для визначення оптимального маршруту і можливих резервних шляхів до кожної мережі призначення використовується кінцевий автомат алгоритму DUAL. Наступником є сусідній маршрутизатор, який використовується для пересилки пакету по маршруту з найменшими витратами до мережі призначення. Допустима відстань (FD) - це найменша обчислена метрика досягнення мережі призначення через наступника. Можливий наступник (FS) - це сусідній маршрутизатор, що забезпечує резервний маршрут без петель до тієї ж мережі, що і наступник, і при цьому відповідний умові здійсненності. Умова здійсненності (FC) виконується, коли оголошене відстань (RD) сусіднього пристрою для мережі менше, ніж можливу відстань локального маршрутизатора до цієї ж мережі призначення. Оголошене

відстань - це просто можливу відстань сусіднього пристрою EIGRP до мережі призначення.

Для настройки EIGRP використовується команда router eigrp autonomous-system. Значення autonomous-system (автономна система) фактично є ідентифікатором процесу і має бути однаковим на всіх маршрутизаторах в домені маршрутизації EIGRP. Команда network аналогічна команді, використовуваної з протоколом маршрутизації. Мережа - це класовий мережеву адресу безпосередньо підключених інтерфейсів маршрутизатора. Шаблонна маска - це додатковий параметр, який може бути використаний для включення тільки конкретних інтерфейсів.

EIGRP - це гнучкий протокол маршрутизації, який підтримує точну настройку різними способами. До двох найважливіших можливостям точного налаштування відносяться функція об'єднання маршрутів і функція розподілу навантаження. Інші можливості настройки включають в себе поширення таймерів точної настройки за замовчуванням і реалізацію аутентифікації між сусідніми пристроями EIGRP для забезпечення безпеки.

Інтерактивне завдання. EIGRP. Назад у майбутнє

У цьому розділі ви навчитеся підтримувати роботу мереж EIGRP і налаштовувати їх відповідно до індивідуальних потреб. У цьому розділі будуть вивчені такі поняття EIGRP:

- Автоматичне об'єднання
- Розподіл навантаження
- Маршрути за замовчуванням
- Таймери утримання (hold-down timer)
- Аутентифікація

Разом з однокурсником запишіть 10 питань на закріплення матеріалу про протокол EIGRP, пройденого в попередньому розділі. Три з цих питань повинні бути пов'язані з елементами з наведеного вище списку. В ідеалі повинні бути створені питання наступних типів: з вибором правильного варіанта, істина / неправда або заповнення порожніх полів. При створенні ваших запитань не забудьте записати розділ навчального курсу і номера сторінок використовуваних матеріалів, щоб ви могли до них повернутися для перевірки відповідей.

Збережіть свою роботу, а потім запропонуйте відповісти на створені питання іншій групі або всьому класу.

Щоб точніше налаштувати розширені можливості EIGRP, спочатку треба зробити базову настройку протоколу.

На рис. представлені мережеві топології, використовувані для цього розділу.

EIGRP для топологии IPv4

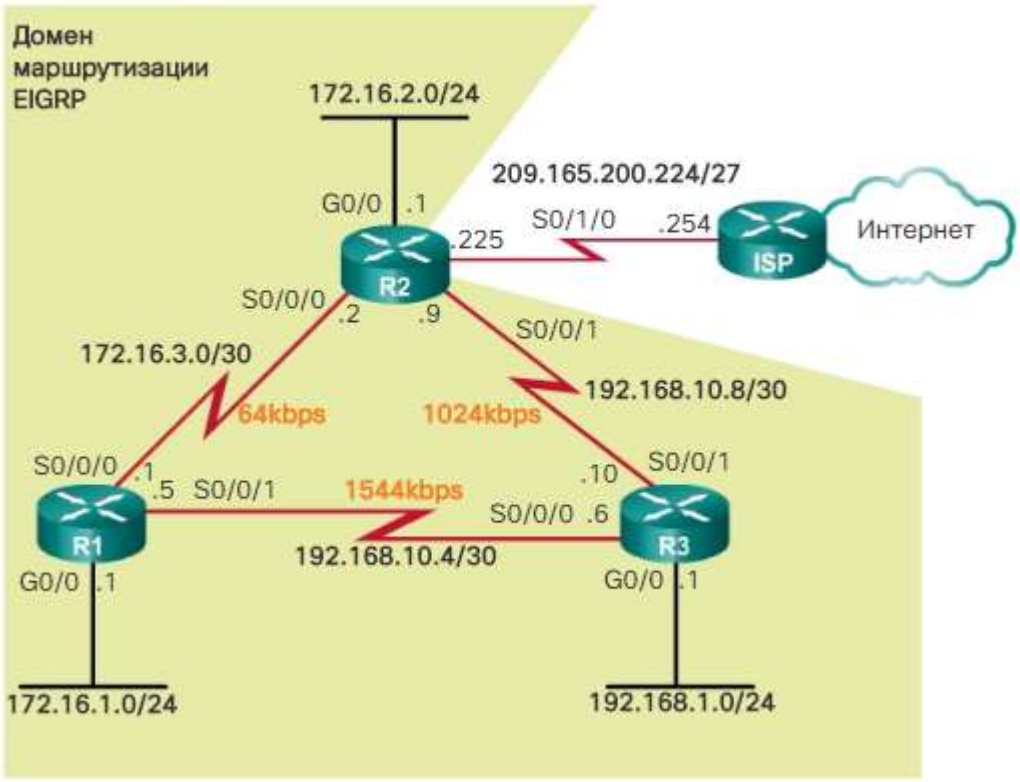


Рис. 5.6.103

На рис показані конфігурації інтерфейсу IPv4 і реалізації EIGRP на маршрутизаторах R1, R2 і R3 відповідно.

Запуск интерфейса IPv4 и протокола EIGRP для конфигурации IPv4 маршрутизатора R1

```
R1# show running-config
<выходные данные опущены>
version 15.2
!
interface GigabitEthernet0/0
 ip address 172.16.1.1 255.255.255.0
!
interface Serial0/0/0
 bandwidth 64
 ip address 172.16.3.1 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 192.168.10.5 255.255.255.252
!
router eigrp 1
 network 172.16.0.0
 network 192.168.10.0
 eigrp router-id 1.1.1.1
```

Рис. 5.6.104

Запуск интерфейса IPv4 и протокола EIGRP для конфигурации IPv4 маршрутизатора R2

```
R2# show running-config
<выходные данные опущены>
version 15.2
!
interface GigabitEthernet0/0
 ip address 172.16.2.1 255.255.255.0
!
interface Serial0/0/0
 bandwidth 64
 ip address 172.16.3.2 255.255.255.252
!
interface Serial0/0/1
 bandwidth 1024
 ip address 192.168.10.9 255.255.255.252
 clock rate 64000
!
interface Serial0/1/0
 ip address 209.165.200.225 255.255.255.224
!
router eigrp 1
 network 172.16.0.0
 network 192.168.10.8 0.0.0.3
 eigrp router-id 2.2.2.2
```

Рис. 5.6.105

Запуск интерфейса IPv4 и протокола EIGRP для конфигурации IPv4 маршрутизатора R3

```
R3# show running-config
<выходные данные опущены>
version 15.2
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
 ip address 192.168.10.6 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 bandwidth 1024
 ip address 192.168.10.10 255.255.255.252
!
router eigrp 1
 network 192.168.1.0
 network 192.168.10.4 0.0.0.3
 network 192.168.10.8 0.0.0.3
 eigrp router-id 3.3.3.3
```

Рис. 5.6.106

Типи послідовних інтерфейсів і значення їх пропускної здатності не обов'язково є показниками найбільш поширених типів з'єднань, що застосовуються в сучасних мережах. Значення пропускної здатності

послідовних каналів, які використовуються в рамках даної топології, допомагають пояснити розрахунок метрик протоколу маршрутизації і процес вибору оптимального шляху.

Зверніть увагу, що команди bandwidth на послідовних інтерфейсах використовувалися в цілях зміни пропускної здатності за замовчуванням, яка становила +1544 кбіт / с.

В цьому розділі маршрутизатор ISP використовується в якості шлюзу домену маршрутизації в мережу Інтернет. Всі три маршрутизатора працюють під управлінням Cisco IOS, випуск 15.2.

Включення і відключення автоматичного об'єднання маршрутів - це один з найбільш поширених способів точного налаштування EIGRP. Об'єднання маршрутів дозволяє маршрутизаторів групувати мережі і оголошувати їх як одну велику групу, використовуючи один об'єднаний маршрут. З огляду на швидке розширення мереж можливість об'єднання маршрутів має критичне значення.

Граничний маршрутизатор знаходиться на кордоні мережі. Цей маршрутизатор повинен оголошувати всі мережі, що містяться в його таблиці маршрутизації, маршрутизатора підключається мережі або маршрутизатора інтернет-провайдера (ISP). Така збіжність може привести до появи дуже великих таблиць маршрутизації. Уявіть, якби в таблиці одного маршрутизатора містилося 10 різних мереж, і він повинен був би оголошувати всі ці 10 записів про маршрутах підключати до нього маршрутизатора. Що, якби цей підключається маршрутизатор теж містив 10 мереж, і мав би оголосити маршрутизатора ISP вже 20 маршрутів? Якби кожен корпоративний маршрутизатор дотримувався цього правила, то таблиці маршрутизації ISP були б просто величезні.

Об'єднання скорочує кількість записів в оновленнях маршрутизації і локальних таблицях маршрутизації. Ця функція також зменшує використання пропускної здатності для оновлень маршрутизації, приводячи до прискорення пошуку в таблицях маршрутизації.

Щоб обмежити кількість оголошень і розмір таблиць маршрутизації, такі протоколи маршрутизації, як EIGRP, використовують автоматичне об'єднання на кордонах класів. Це означає, що EIGRP пізнає підмережі, як мережі класу A, B або C, і створює в таблиці маршрутизації тільки один запис для об'єднаного маршруту. В результаті весь трафік, призначений для підмереж, надходить по цьому єдиному шляху.

На малюнку наводиться приклад роботи автоматичного об'єднання. Маршрутизатор R1 і R2 налаштовані за допомогою EIGRP для IPv4 з автоматичним об'єднанням. У таблиці маршрутизатора R1 містяться три підмережі: 172.16.1.0/24, 172.16.2.0/24 і 172.16.3.0/24. При архітектурі класової адресації мережі всі ці підмережі розглядаються як частина великої мережі класу B, 172.16.0.0/16. Оскільки на маршрутизаторі R1 протокол EIGRP налаштовується для автоматичного об'єднання, то при відправленні свого відновлення маршрутизації на R2 він об'єднує три підмережі / 24 в єдину мережу 172.16.0.0/16, що скорочує кількість відправлених оголошень маршрутизації і записів в таблиці маршрутизації IPv4 маршрутизатора R2.

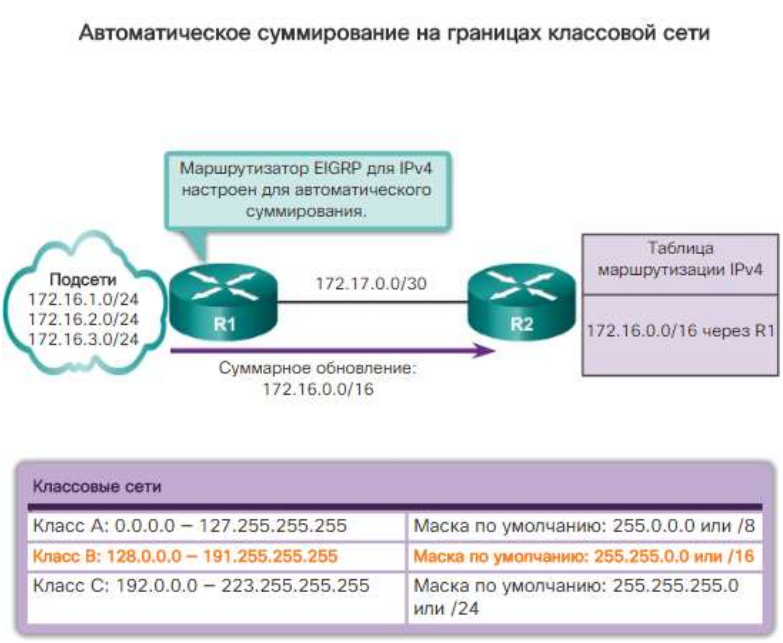


Рис. 5.6.107

Весь трафік, призначений для цих трьох підмереж, проходить по одному шляху. Маршрутизатор R2 не підтримує маршрути до конкретних подсетям і не отримує відомості про подсетях. У корпоративної мережі обраний шлях до сумарного маршруту може не бути оптимальним для трафіку, призначеного для тієї чи іншої окремої підмережі. Маршрутизатор можуть знайти оптимальні маршрути до кожної з окремих підмереж, тільки отримавши від сусідніх пристроїв відомості про ці подсетях. В цьому випадку автоматичне об'єднання слід відключити. При відключенні об'єднання відомості про підмережі містять про 615бновленія.

Налаштування автоматичного об'єднання EIGRP

Автоматичне об'єднання EIGRP для IPv4 за замовчуванням вимкнено, починаючи з випусків Cisco IOS 15.0 (1) M і 12.2 (33). До цього функція автоматичного об'єднання за замовчуванням була включена. Це означало, що протокол EIGRP виконував автоматичне об'єднання кожен раз, коли топологія EIGRP перетинала кордон між двома основними класовими мережами.

На рис. 1 в вихідних даних команди show ip protocols на маршрутизаторі R1 зазначено, що автоматичне об'єднання EIGRP відключено. Цей маршрутизатор працює під управлінням IOS 15,2, тому автоматичне об'єднання EIGRP відключено за замовчуванням. На рис. 2 показана поточна таблиця маршрутизації маршрутизатора R3. Зверніть увагу, що таблиця маршрутизації IPv4 для R3 містить всі мережі і підмережі в рамках домена маршрутизації EIGRP.

Проверка отключения автоматического объединения

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
<выходные данные опущены>


  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.0
  <выходные данные опущены>
```

Рис. 5.6.108

Проверка отключения функции автоматического объединения маршрутов

```
R3# show ip route eigrp
<выходные данные опущены>


 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D 172.16.1.0/24 [90/2170112] via 192.168.10.5, 02:21:10, Serial0/0/0
D 172.16.2.0/24 [90/3012096] via 192.168.10.9, 02:21:10, Serial0/0/1
D 172.16.3.0/30 [90/41024000] via 192.168.10.9, 02:21:10, Serial0/0/1
                [90/41024000] via 192.168.10.5, 02:21:10, Serial0/0/0
R3#
```

Рис. 5.6.109

Щоб увімкнути автоматичне об'єднання для EIGRP, використовуйте команду auto-summary в режимі конфігурації маршрутизатора.

Настройка автоматического объединения

```
R1(config)# router eigrp 1
R1(config-router)# auto-summary
R1(config-router)#
*Mar  9 19:40:19.342: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.10.6 (Serial0/0/1) is resync: summary configured
*Mar  9 19:40:19.342: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.10.6 (Serial0/0/1) is resync: summary up, remove components
*Mar  9 19:41:03.630: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.10.6 (Serial0/0/1) is resync: peer graceful-restart
```

```
R2(config)# router eigrp 1
R2(config-router)# auto-summary
R2(config-router)#
```

Рис. 5.6.110

R1 (config) # router eigrp as-number

R1 (config-router) # auto-summary

Щоб вимкнути функцію автоматичного об'єднання використовуйте цю команду, додавши no.

Перевірка автоматичного об'єднання. Команда show ip protocols

На рис. 1 зверніть увагу, що домен маршрутизації EIGRP містить три класові мережі:

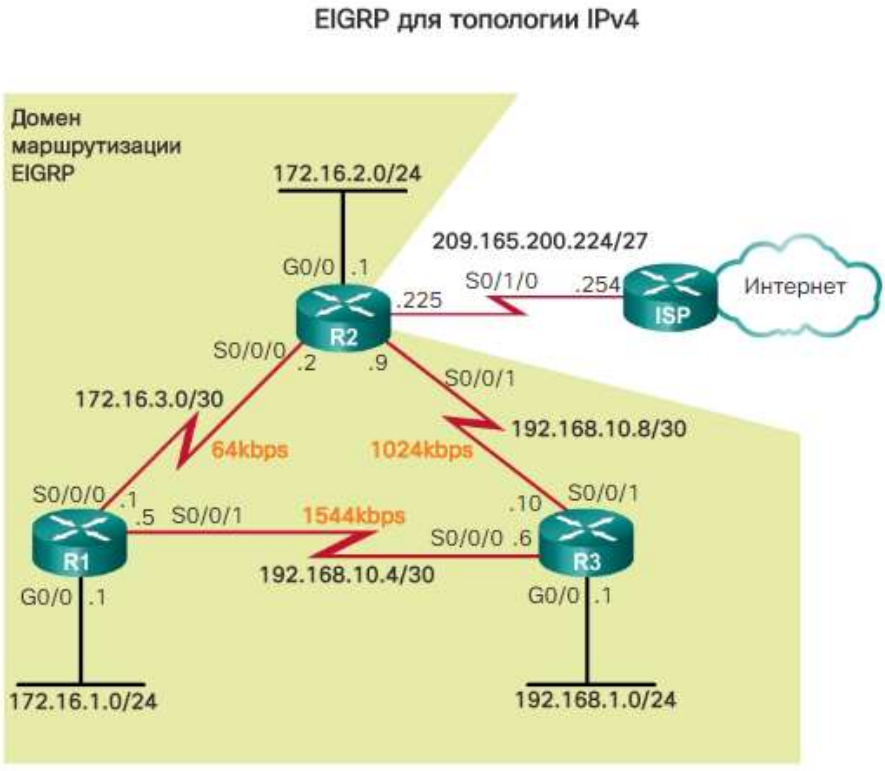


Рис. 5.6.111

Мережа класу B 172.16.0.0/16, що складається з підмереж 172.16.1.0/24, 172.16.2.0/24 і 172.16.3.0/30.

Мережа класу C 192.168.10.0/24, що складається з підмереж 192.168.10.4/30 і 192.168.10.8/30.

Мережа класу C 192.168.1.0/24, яка не містить підмереж.

З вихідних даних команди show ip protocols, виконаної на R1 (рис. 2), видно, що в даний час автоматичне об'єднання включено. Також в вихідних даних вказані мережі, які об'єднані, і відповідні інтерфейси. Зверніть увагу, що в своїх оновленнях маршрутизації EIGRP маршрутизатор R1 об'єднує дві мережі:

Проверка включения автоматического суммирования

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
<выходные данные опущены>

Automatic Summarization: enabled
    192.168.10.0/24 for Gi0/0, Se0/0/0
      Summarizing 2 components with metric 2169856
    172.16.0.0/16 for Se0/0/1
      Summarizing 3 components with metric 2816
<выходные данные опущены>
```

Рис. 5.6.112

Мережа 192.168.10.0/24, відправлена з інтерфейсів GigabitEthernet 0/0 і Serial 0/0/0

Мережа 172.16.0.0/16, відправлена з інтерфейсу Serial 0/0/1

У таблиці маршрутизації IPv4 маршрутизатора R1 містяться підмережі 192.168.10.4/30 і 192.168.10.8/30.

Як показано на рис. 3, маршрутизатор R1 об'єднує підмережі 192.168.10.4/30 і 192.168.10.8/30. Він пересилає об'єднаний адреса 192.168.10.0/24 своїм сусіднім пристроїв по інтерфейсів Serial 0/0/0 і GigabitEthernet 0/0. Оскільки маршрутизатор R1 не має сусідніх пристроїв EIGRP на інтерфейсі GigabitEthernet 0/0, оновлення об'єднаної маршрутизації отримує тільки маршрутизатор R2.

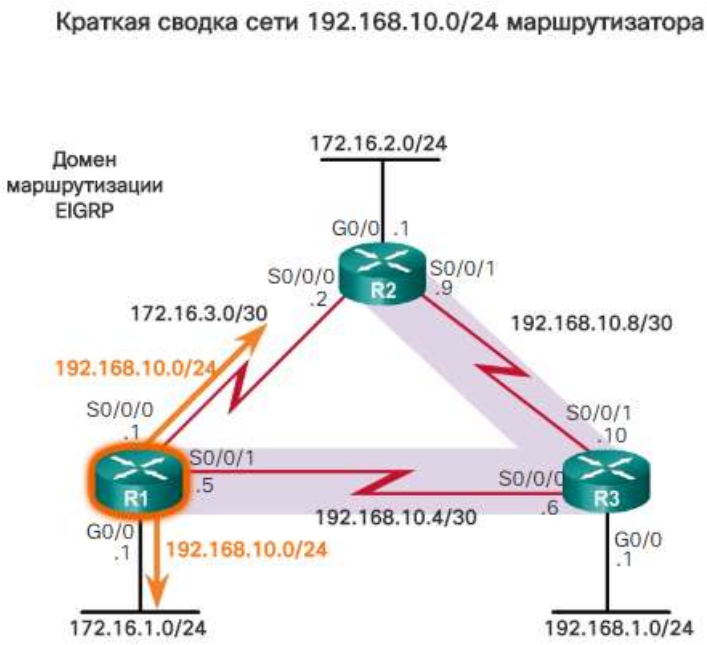


Рис. 5.6.113

Як показано на рис. 4, в таблиці маршрутизації IPv4 маршрутизатора R1 також містяться підмережі 172.16.1.0/24, 172.16.2.0/24 і 172.16.3.0/30. Маршрутизатор R3 вибирає R1 в якості наступника до мережі 172.16.0.0/16, оскільки він характерний найменшим реальним відстанню. Інтерфейс S0 / 0/0 маршрутизатора R3, підключений до R1, використовує пропускну здатність за замовчуванням 1544 кбіт / с. Канал між маршрутизаторами R3 і R2 має більш високу протяжністю, оскільки інтерфейс S0 / 0/1 маршрутизатора R3 налаштований з більш низькою пропускною спроможністю - +1024 кбіт / с.

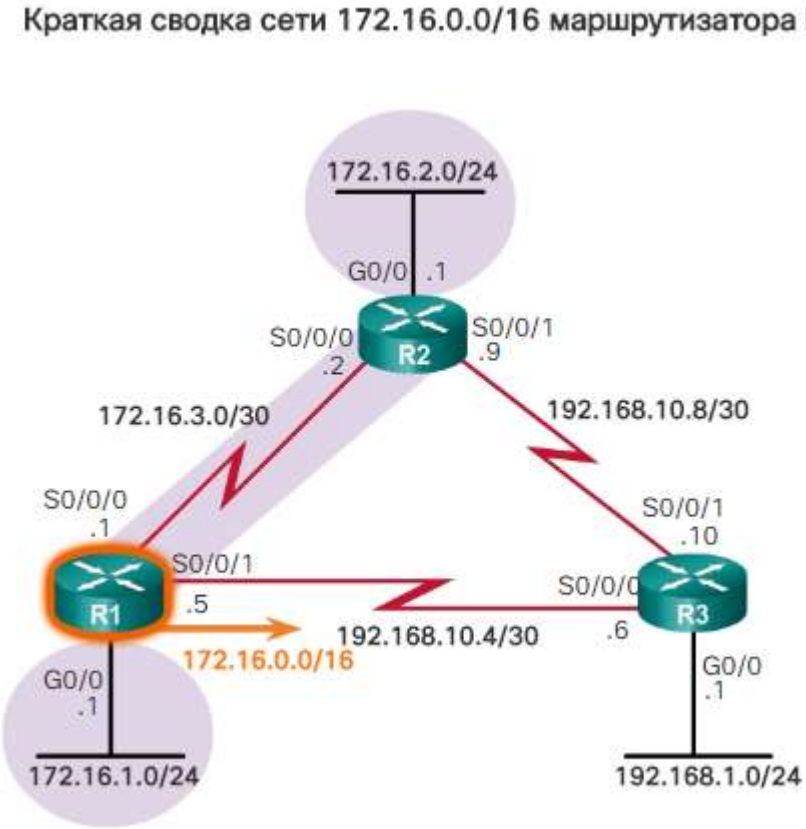


Рис. 5.6.114

Зверніть увагу, що об'єднане оновлення 172.16.0.0/16 не надсилається через інтерфейси GigabitEthernet 0/0 і Serial 0/0/0 маршрутизатора R1. Це пояснюється тим, що ці два інтерфейси входять в одну і ту ж мережу класу B - 172.16.0.0/16. Оновлення маршрутизації 172.16.1.0/24 відправляється від маршрутизатора R1 на R2 без об'єднаного маршруту. Об'єднані поновлення відправляються тільки через інтерфейси в різних основних класових мережах.

На рис. маршрутизатори R1 і R2 відправляють об'єднане оновлення маршрутизації EIGRP 172.16.0.0/16 маршрутизатора R3. Таблиці маршрутизації R1 і R2 містять підмережі мережі 172.16.0.0/16, тому обидва маршрутизатора відправляють маршрутизатора R3 об'єднане оголошення по інший основний класової мережі.

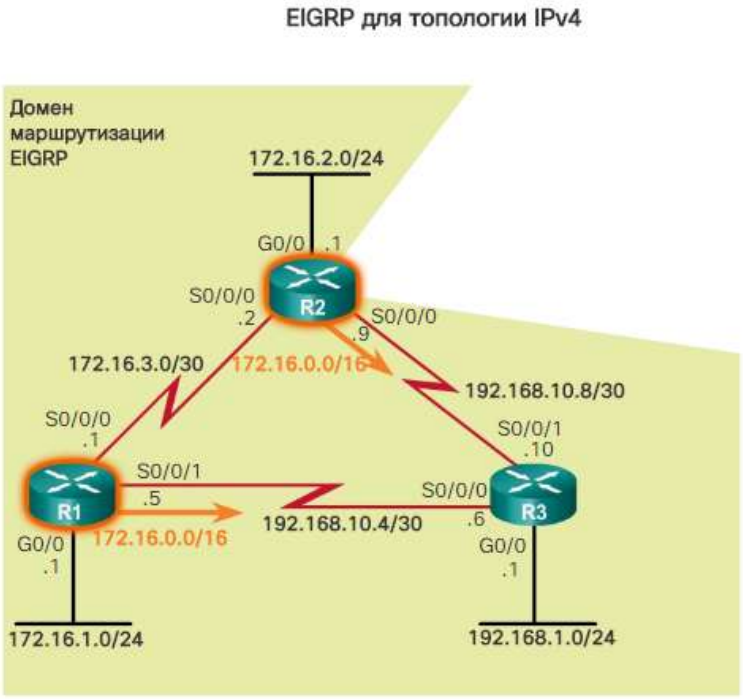


Рис. 5.6.115

На рис. представлені вихідні дані команди show ip eigrp topology all-links, виконаної для перегляду заповненої таблиці топології EIGRP маршрутизатора R3. Це підтверджує, що R3 отримав об'єднаний маршрут 172.16.0.0/16, як від R1 за адресою 192.168.10.5, так і від R2 - за адресою 192.168.10.9. Перший запис через 192.168.10.5 - це наступник, а друга 192.168.10.9 - можливий наступник. Маршрутизатор R1 є наступником, оскільки його канал з пропускною спроможністю 1544 Кбіт / с з маршрутизатором R3 забезпечує кращу вартість EIGRP до 172.16.0.0/16, ніж маршрутизатор R2, який використовує більш повільний канал з пропускною спроможністю 1024 Кбіт / с.

Проверка объединённого маршрута в таблице топологии

```
R3# show ip eigrp topology all-links

P 172.16.0.0/16, 1 successors, FD is 2170112, serno 9
        via 192.168.10.5 (2170112/2816), Serial0/0/0
        via 192.168.10.9 (3012096/2816), Serial0/0/1

<выходные данные опущены>
```

Рис. 5.6.116

Параметр all-links показує всі отримані поновлення, незалежно від того, чи стає маршрут можливим наступником (FS) чи ні. У цьому випадку маршрутизатор R2 стає можливим наступником. Маршрутизатор R2 стає можливим наступником, оскільки його оголошене відстань (RD) становить 2 816, що менше допустимої відстані (FD); 2 170 112 через маршрутизатор R1.

Перевірте таблицю маршрутизації, щоб переконатися, що був отриманий об'єднаний маршрут.

На рис. 1 показана таблиця маршрутизації R3 перед автоматичним об'єднанням, а потім після автоматичного об'єднання, включеного за допомогою команди auto-summary. Зверніть увагу, що при включеному автоматичному об'єднанні таблиця маршрутизації R3 містить тільки один мережевий адресу класу B - 172.16.0.0/16. Наступник або маршрутизатор наступного переходу - це R1 через 192.168.10.5.

Проверка объединённого маршрута в таблице маршрутизации

Автоматическое объединение отключено

```
R3# show ip route eigrp
<выходные данные опущены>

 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D    172.16.1.0/24 [90/2170112] via 192.168.10.5,
                   02:21:10, Serial0/0/0
D    172.16.2.0/24 [90/3012096] via 192.168.10.9,
                     02:21:10, Serial0/0/1
D    172.16.3.0/30 [90/41024000] via 192.168.10.9,
                   02:21:10, Serial0/0/1
```

Автоматическое объединение включено

```
R3# show ip route eigrp
<выходные данные опущены>

D     172.16.0.0/16 [90/2170112] via 192.168.10.5, 00:12:05,
      Serial0/0/0
      192.168.10.0/24 is variably subnetted, 5 subnets, 3
      masks
D        192.168.10.0/24 is a summary, 00:11:43, Null0
R3#
```

Рис. 5.6.117

Примітка. Автоматичне об'єднання є додатковою функцією EIGRP для IPv4. Класова адресація не існує в IPv6, тому автоматичне об'єднання у випадку з EIGRP для IPv6 не потрібно.

При включенні автоматичного об'єднання необхідно враховувати специфіку нульового інтерфейсу (Null). На рис. 2 показана таблиця маршрутизації маршрутизатора R1. Зверніть увагу, що дві виділених записи використовують вихідний інтерфейс Null0. EIGRP автоматично включив в інтерфейс Null0 об'єднаний маршрут для двох класових мереж - 192.168.10.0/24 і 172.16.0.0/16.

Объединённые маршруты Null0 на маршрутизаторе R1

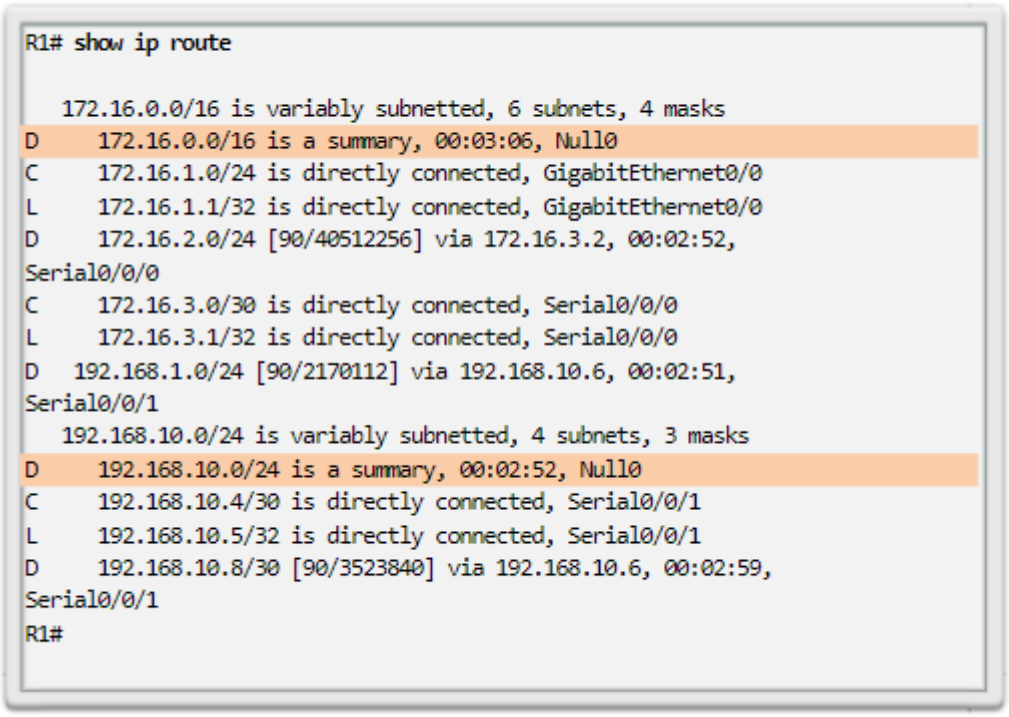


Рис. 5.6.118

Інтерфейс Null0 - це віртуальний інтерфейс IOS, який є маршрутом в нікуди. Його також нерідко називають «бітопріемніком». Пакети, які відповідають маршруту з вихідним інтерфейсом Null0, відкидаються.

EIGRP для IPv4 автоматично включає в себе об'єднаний маршрут Null0 за таких умов:

Принаймні одна підмережа була отримана через EIGRP.

Були виконані дві або більше команд network режиму конфігурації маршрутизатора EIGRP.

Включено автоматичне об'єднання.

Мета об'єднаного маршруту Null0 полягає в запобіганні петель маршрутизації для призначень, які включені в об'єднання, але не містяться в таблиці маршрутизації.

На малюнку зображений випадок, при якому може виникнути петля маршрутизації:

1. R1 використовує маршрут за замовчуванням 0.0.0.0/0 через маршрутизатор інтернету-провайдера, ISP.

2. Маршрутизатор R1 відправляє маршрутизатора R2 оновлення маршрутизації, що містить маршрут за замовчуванням.

3. R2 додає маршрут по замовчуванню від маршрутизатора R1 в свою таблицю маршрутизації IPv4.

4. Таблиця маршрутизації R2 містить підмережі 172.16.1.0/24, 172.16.2.0/24 і 172.16.3.0/24.

5. Маршрутизатор R2 відправляє маршрутизатора R1 об'єднане оновлення для мережі 172.16.0.0/16.

6. R1 встановлює об'єднаний маршрут для 172.16.0.0/16 через маршрутизатор R2.

7. R1 отримує пакет для 172.16.4.10. Оскільки у маршрутизатора R1 є маршрут для 172.16.0.0/16 через маршрутизатор R2, він пересилає пакет маршрутизатора R2.

8. R2 отримує від маршрутизатора R1 пакет з адресою призначення 172.16.4.10. Пакет не відповідає жодному конкретному маршруту, тому, використовуючи маршрут за замовчуванням в своїй таблиці маршрутизації, R2 пересилає пакет назад на R1.

9. Пакет для 172.16.4.10 передається по петлі між R1 і R2, поки не закінчиться його час життя (TTL), після чого пакет відкидається.

Рис. 5.6.119

Об'єднаний маршрут (продовження)

EIGRP використовує інтерфейс Null0 для запобігання подібних петель маршрутизації. На малюнку представлений випадок, при якому маршрут Null0 запобігає появі петлі маршрутизації, проілюстровану в попередньому прикладі:

1. R1 використовує маршрут за замовчуванням 0.0.0.0/0 через маршрутизатор інтернету-провайдера, ISP.

2. Маршрутизатор R1 відправляє маршрутизатора R2 оновлення маршрутизації, що містить маршрут за замовчуванням.

3. R2 додає маршрут по замовчуванню від маршрутизатора R1 в свою таблицю маршрутизації IPv4.

4. Таблиця маршрутизації R2 містить підмережі 172.16.1.0/24, 172.16.2.0/24 і 172.16.3.0/24.

5. R2 додає об'єднаний маршрут 172.16.0.0/16 до Null0 в свою таблицю маршрутизації.

6. Маршрутизатор R2 відправляє маршрутизатора R1 об'єднане оновлення для мережі 172.16.0.0/16.

7. R1 встановлює об'єднаний маршрут для 172.16.0.0/16 через маршрутизатор R2.

8. R1 отримує пакет для 172.16.4.10. Оскільки у маршрутизатора R1 є маршрут для 172.16.0.0/16 через маршрутизатор R2, він пересилає пакет маршрутизатора R2.

9. R2 отримує від маршрутизатора R1 пакет з адресою призначення 172.16.4.10. IP-адреса призначення цього пакета не потрапляє в яку-небудь конкретну підмережу мережі 172.16.0.0, але потрапляє в діапазон 172.16.0.0/16 об'єднаного маршруту в Null0. Пакет відкидається з використанням маршруту Null0.

Об'єднаний маршрут на R2 для мережі 172.16.0.0/16 в інтерфейс Null0 відкидає всі пакети, адреса призначення яких починається на 172.16.x.x, але не входить в одну з підмереж: 172.16.1.0/24, 172.16.2.0/24, або 172.16.3.0/24.

Навіть якщо в таблиці маршрутизації R2 міститься маршрут за замовчуванням 0.0.0.0/0, маршрут Null0 є більш точним збігом.

Примітка. Об'єднаний маршрут Null0 видаляється після відключення автоматичного об'єднання за допомогою команди режиму конфігурації маршрутизатора no auto-summary.

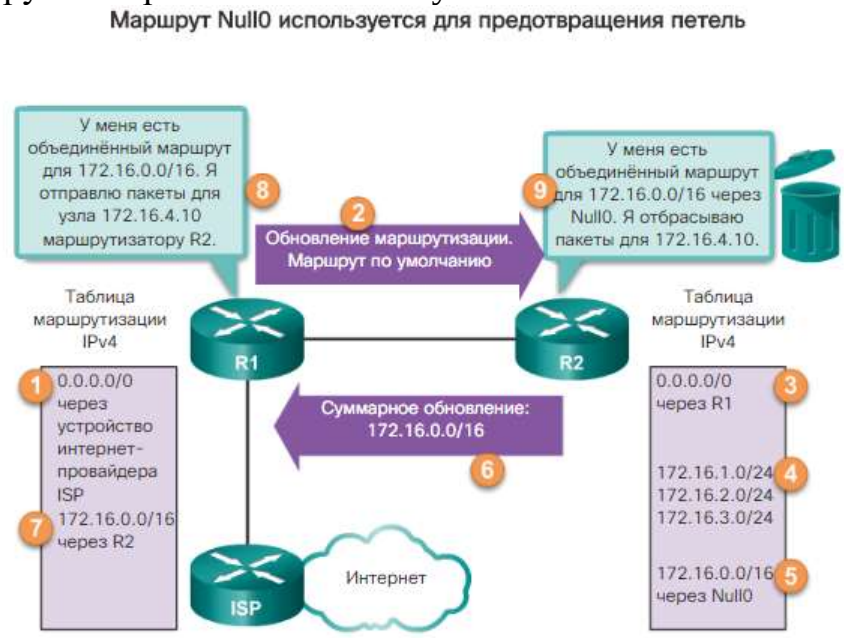


Рис. 5.6.120

EIGRP можна налаштувати для об'єднання маршрутів, як при включеному, так і вимкненому автоматичному об'єднанні (auto-summary). Оскільки протокол EIGRP - протокол безкласової маршрутизації, в оновленнях маршрутизації якого містяться маски підмережі, об'єднання вручну може включати маршрути

Суперсети. Не забувайте, що об'єднана мережа - це об'єднання декількох мережевих адрес основний класової мережі.

На рис. 1 показані дві мережі, які додані в маршрутизатор R3 за допомогою інтерфейсів loopback: 192.168.2.0/24 і 192.168.3.0/24. Хоча інтерфейси loopback - це віртуальні інтерфейси, в даному прикладі вони використовуються для подання фізичних мереж.

EIGRP для топологии IPv4

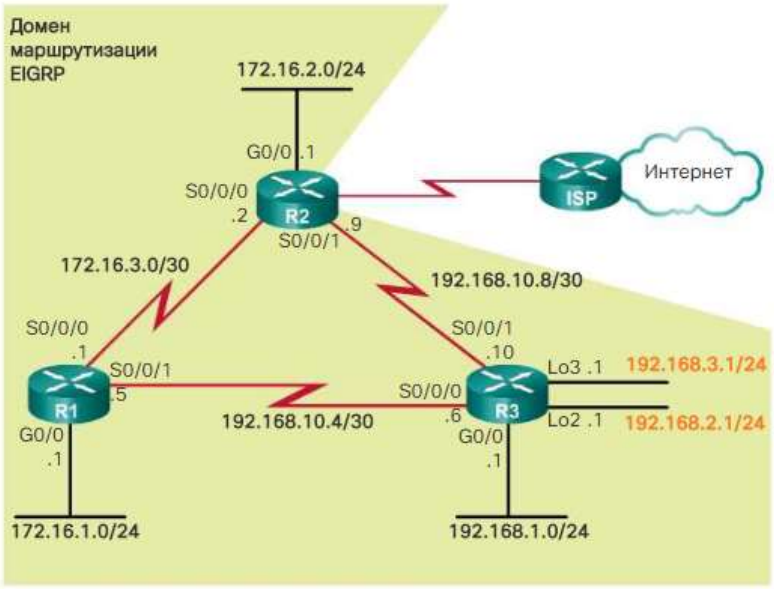


Рис. 5.6.121

На рис. представлені команди для налаштування на маршрутизаторі R3 двох інтерфейсів loopback, а також конфігурація для включення обох інтерфейсів для EIGRP.

Настройка интерфейсов loopback на маршрутизаторе R3

```
R3(config)# interface loopback 2
R3(config-if)# ip add 192.168.2.1 255.255.255.0
R3(config-if)# exit
R3(config)# interface loopback 3
R3(config-if)# ip add 192.168.3.1 255.255.255.0
R3(config-if)# exit
R3(config)# router eigrp 1
R3(config-router)# network 192.168.2.0
R3(config-router)# network 192.168.3.0
R3(config-router)#
```

Рис. 5.6.122

Щоб переконатися, що маршрутизатор R3 відправив пакети оновлень EIGRP на R1 і R2, таблиці маршрутизації слід перевірити на обох маршрутизаторах.

На рис. 3 показані тільки відповідні маршрути. У таблицях маршрутизації на R1 і R2 показані ці додаткові мережі: 192.168.2.0/24 і 192.168.3.0/24. Замість того щоб відправляти три окремі мережі, маршрутизатор R3 може об'єднати мережі 192.168.1.0/24, 192.168.2.0/24 і 192.168.3.0/24 в єдиний маршрут.

Проверка дополнительных маршрутов на R1 и R2

```
R1# show ip route
<выходные данные опущены>

D 192.168.1.0/24 [90/2170112] via 192.168.10.6, 00:47:39,Serial0/0/1
D 192.168.2.0/24 [90/2297856] via 192.168.10.6, 00:08:09,Serial0/0/1
D 192.168.3.0/24 [90/2297856] via 192.168.10.6, 00:08:04,Serial0/0/1
R1#
```

```
R2# show ip route
<выходные данные опущены>

D 192.168.1.0/24 [90/3012096] via 192.168.10.10, 00:47:58,Serial0/0/1
D 192.168.2.0/24 [90/3139840] via 192.168.10.10, 00:08:28,Serial0/0/1
D 192.168.3.0/24 [90/3139840] via 192.168.10.10, 00:08:23,Serial0/0/1
R2#
```

Рис. 5.6.123

Визначення об'єднаного маршруту EIGRP

На рис. 1 показані два об'єднаних маршруту, які були вручну налаштовані на маршрутизаторі R3. Ці об'єднані маршрути відправлені сусіднім пристроїв EIGRP маршрутизатора R3 через інтерфейси Serial 0/0/0 і Serial 0/0/1.

EIGRP для топологии IPv4

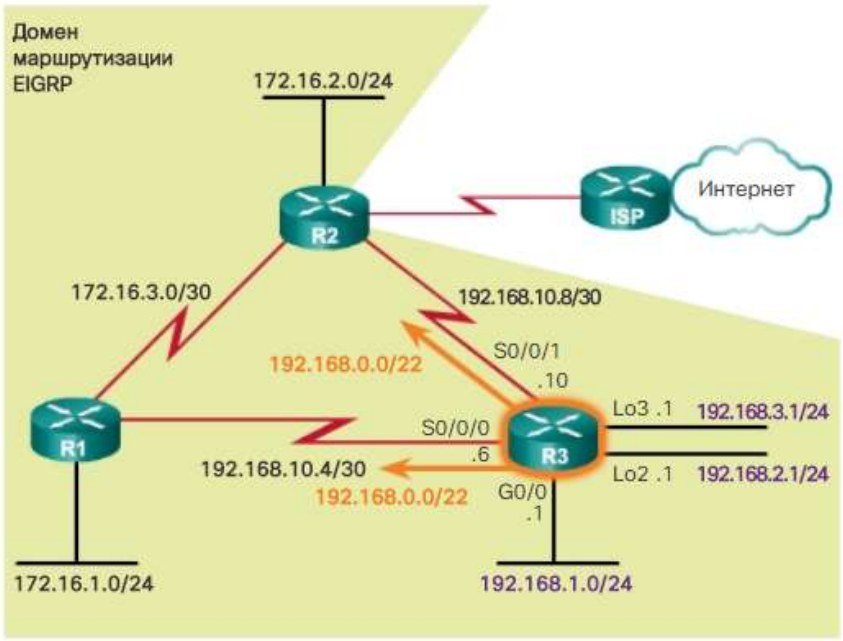


Рис. 5.6.124

Як показано на рис. для визначення об'єднання цих трьох мереж використовується той же метод, що і для визначення об'єднаних статичних маршрутів:

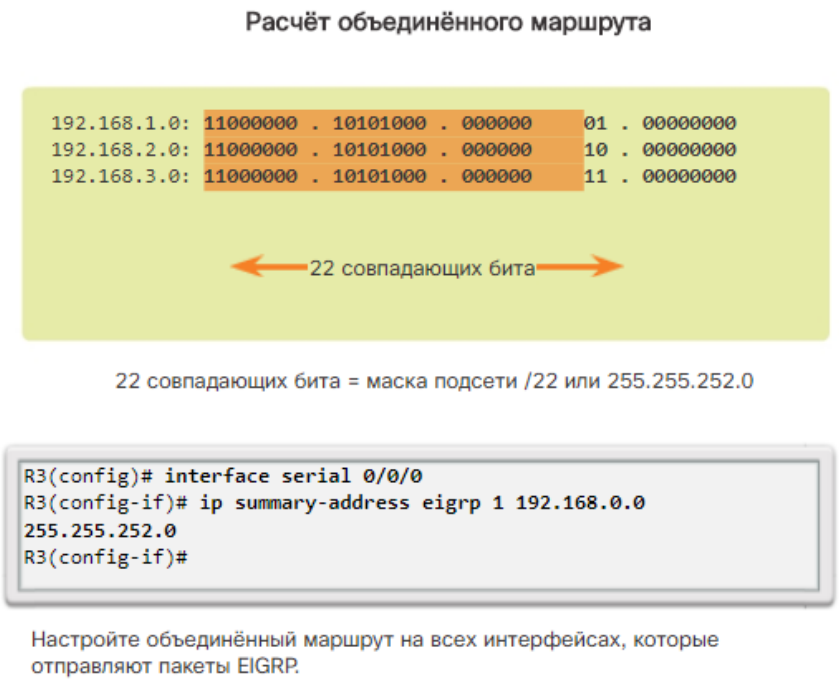


Рис. 5.6.125

Крок 1. У довічним форматі запишіть мережі, які слід об'єднати.

Крок 2. Щоб знайти маску підмережі для об'єднання, почніть з крайнього зліва біта.

Крок 3. Зліва направо знайдіть все біти, які послідовно збігаються.

Крок 4. Дійшовши до колонки з незбіжними битами, зупиниться. Це межа об'єднання.

Крок 5. Підрахуйте кількість крайніх зліва співпадаючих бітів. У наведеному прикладі їх 22. Це число використовується для визначення маски підмережі для об'єднаного маршруту: / 22 або 255.255.252.0.

Крок 6. Для того щоб отримати мережеву адресу для об'єднання, скопіюйте збігаються 22 біта і додайте все біти 0 в кінець, щоб отримати 32 біта.

В результаті отримуємо об'єднаний мережеву адресу і маску для 192.168.0.0/22.

Налаштування об'єднання EIGRP вручну

Щоб налаштувати об'єднання EIGRP вручну на конкретному інтерфейсі EIGRP, використовуйте наступну команду режиму конфігурації інтерфейсу:

Router (config-if) # ip summary-address eigrp as-number network-address subnet-mask

На рис. 2 показана конфігурація для поширення об'єднаного вручну маршруту на інтерфейсі Serial 0/0/0 маршрутизатора R3. Оскільки R3 має два сусідніх пристрої EIGRP, об'єднання EIGRP вручну слід налаштувати як на інтерфейсі Serial 0/0/0, так і на Serial 0/0/1.

На малюнку показано, що після настройки об'єднаного маршруту таблиці маршрутизації на R1 і R2 більше не містять окремі мережі 192.168.1.0/24, 192.168.2.0/24 і 192.168.3.0/24. Зате вони містять один об'єднаний маршрут 192.168.0.0/22. Об'єднані маршрути дозволяють скоротити кількість записів в таблицях маршрутизації і підвищити ефективність пошуку в таблиці маршрутизації. При об'єднанні маршрутів вручну також потрібно менше

пропускної здатності для оновлень маршрутизації, оскільки замість декількох окремих маршрутів можна відправити тільки один.

Проверка получения объединённого маршрута на маршрутизаторах R1 и R2

```
R1# show ip route
<выходные данные опущены>
D 192.168.0.0/22 [90/2170112] via 192.168.10.6, 01:53:19,
Serial0/0/1
R1#
```

```
R2# show ip route
<выходные данные опущены>
D 192.168.0.0/22 [90/3012096] via 192.168.10.10, 01:53:33,
Serial0/0/1
R2#
```

Рис. 5.6.126

EIGRP для IPv6. Об'єднання маршрутів вручну

На відміну від автоматичного об'єднання, об'єднання вручну можна використовувати також для EIGRP IPv6.

На рис. представлена топологія EIGRP IPv6 з чотирма loopback-адресами, налаштованими на маршрутизаторі R3. Ці віртуальні адреси використовуються для подання фізичних мереж в таблиці маршрутизації IPv6 маршрутизатора R3. Ці мережі можна об'єднати вручну в EIGRP для IPv6.

EIGRP для топологии IPv6

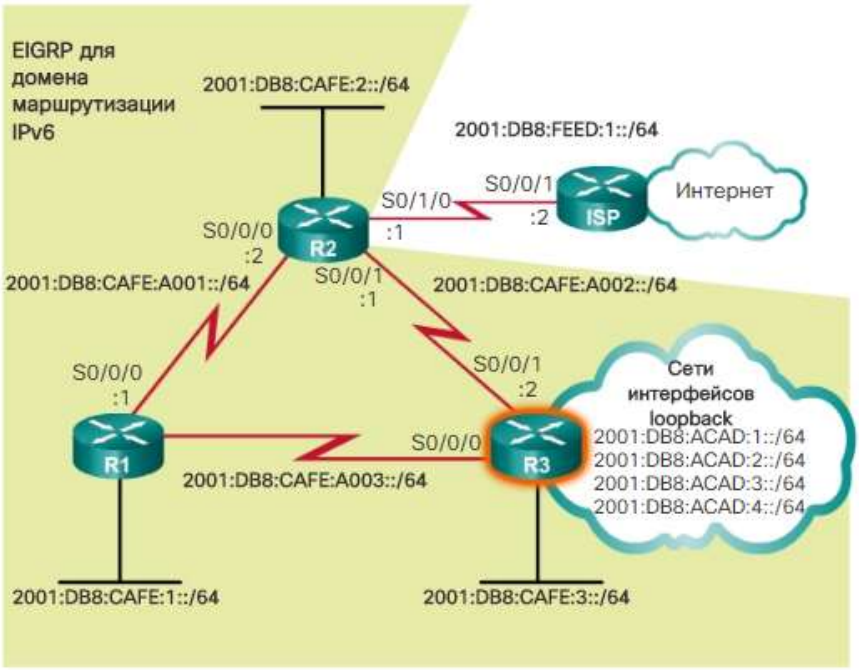


Рис. 5.6.127

На рис. 2 представлена конфігурація loopback-адрес IPv6 на маршрутизаторі R3. Тільки чотири loopback-адреси представлені в топології і налаштовані на R3, однак для цього прикладу допускається, що всі підмережі 2001: DB8: ACAD :: / 48 досяжні через R3.

Настройка интерфейсов loopback IPv6 на маршрутизаторе R3

```
R3(config)# interface loopback 11
R3(config-if)# ipv6 address 2001:db8:acad:1::1/64
R3(config-if)# ipv6 eigrp 2
R3(config-if)# exit
R3(config)# interface loopback 12
R3(config-if)# ipv6 address 2001:db8:acad:2::1/64
R3(config-if)# ipv6 eigrp 2
R3(config-if)# exit
R3(config)# interface loopback 13
R3(config-if)# ipv6 address 2001:db8:acad:3::1/64
R3(config-if)# ipv6 eigrp 2
R3(config-if)# exit
R3(config)# interface loopback 14
R3(config-if)# ipv6 address 2001:db8:acad:4::1/64
R3(config-if)# ipv6 eigrp 2
```

Рис. 5.6.128

Щоб налаштувати об'єднання EIGRP вручну для IPv6 на конкретному інтерфейсі EIGRP, використовуйте наступну команду режиму конфігурації інтерфейсу:

Router (config-if) # ipv6 summary-address eigrp as-number prefix / prefix-length

На рис. представлена конфігурація для поширення маршруту EIGRP, об'єднаного вручну для IPv6, на маршрутизатори R1 і R2 для префікса 2001: DB8: ACAD :: 48 /. Як і у випадку з EIGRP для IPv4, маршрутизатор R3 включає об'єднаний маршрут в інтерфейс null0 з метою запобігання петлі.

Настройка объединения IPv6 вручную на маршрутизаторе R3

```
R3(config)# interface serial 0/0/0
R3(config-if)# ipv6 summary-address eigrp 2 2001:db8:acad::/48
R3(config-if)# exit
R3(config)# interface serial 0/0/1
R3(config-if)# ipv6 summary-address eigrp 2 2001:db8:acad::/48
R3(config-if)# end

R3# show ipv6 route

D   2001:DB8:ACAD::/48 [5/128256]
     via Null0, directly connected

<выходные данные опущены>
```

Рис. 5.6.129

Щоб переконатися в отриманні об'єднаного вручну маршруту, слід вивчити таблиці іншихмаршрутизаторів в рамках домена маршрутизації. На рис. 4 показаний маршрут 2001: DB8: ACAD :: 48 / в таблиці маршрутизації IPv6 на R1.

Проверка протокола EIGRP для объединённого вручную маршрута IPv6

```
R1#  show ipv6 route | include 2001:DB8:ACAD::
D   2001:DB8:ACAD::/48 [90/2297856]
R1#
```

Рис. 5.6.130

Використання статичного маршруту до 0.0.0.0/0 як маршрут за замовчуванням не залежить від протоколу маршрутизації. Статичний маршрут за замовчуванням з «чотирьох нулів» можна використовувати з будь-яким з підтримуваних протоколів маршрутизації. Як правило, статичний маршрут за замовчуванням налаштовують на маршрутизаторі, який підключений до мережі поза домену маршрутизації EIGRP, наприклад до ISP.

На рис. 1 маршрутизатор R2 є шлюзовим маршрутизатором, що підключає домен маршрутизації EIGRP до Інтернету. Коли статичний маршрут за замовчуванням налаштований, необхідно поширити цей маршрут по всьому домену EIGRP, як показано на рис. 2.

Распространение маршрута по умолчанию

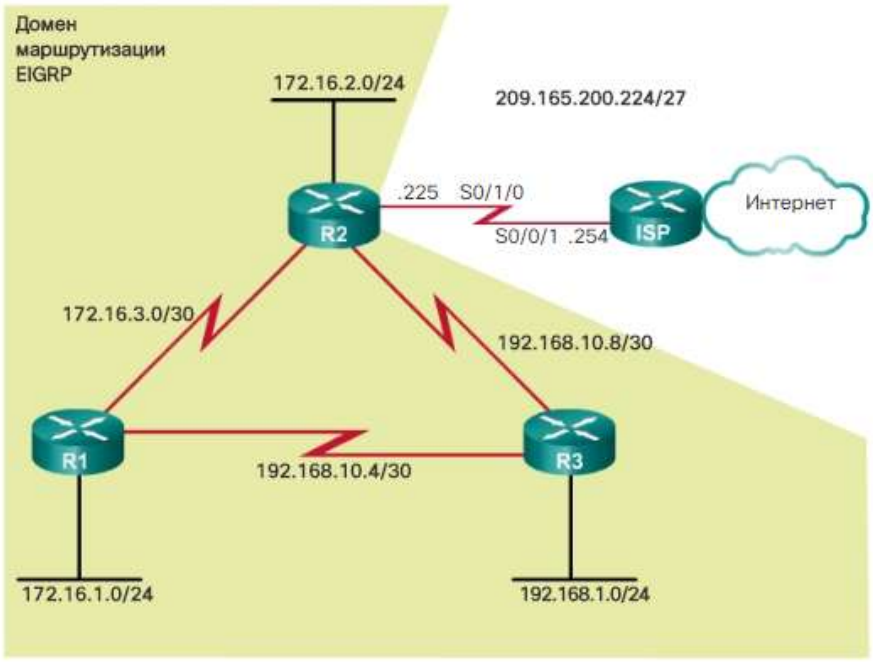


Рис. 5.6.131

EIGRP для топологии IPv4

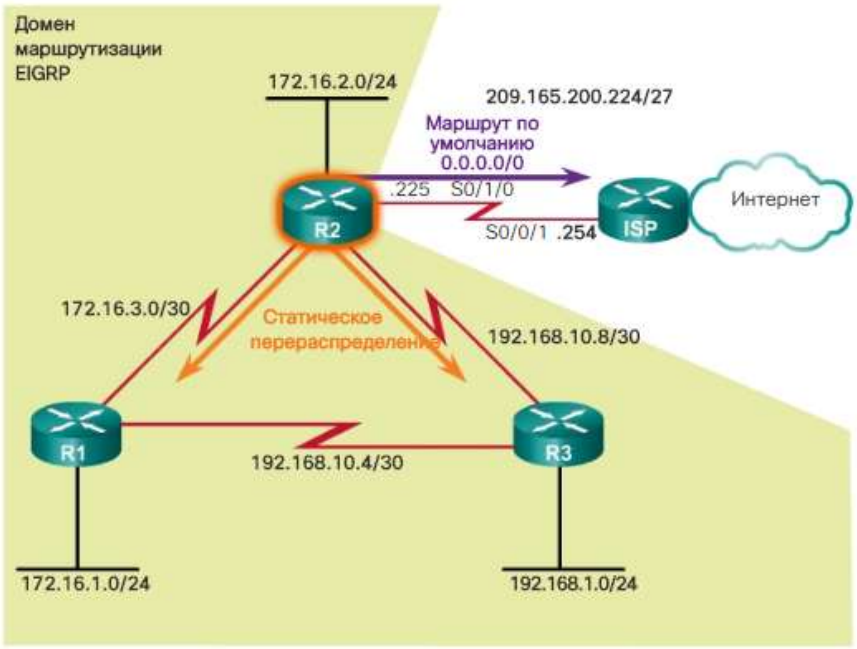


Рис. 5.6.132

Поширити статичний маршрут за замовчуванням в домені маршрутизації EIGRP можна за допомогою команди redistribute static. Завдяки команді redistribute static EIGRP включає статичні маршрути в оновлення EIGRP, що відправляються на інші маршрутизатори. На рис. 3 представлена конфігурація статичного маршруту за замовчуванням і команда redistribute static, виконана на маршрутизаторі R2.

Настройка и распространение статического маршрута по умолчанию маршрутизатора R2

```
R2(config)# ip route 0.0.0.0 0.0.0.0 serial 0/1/0
R2(config)# router eigrp 1
R2(config-router)# redistribute static
```

Рис. 5.6.133

На рис. підтверджується, що маршрут за замовчуванням був отриманий маршрутизатором R2 і доданий в його таблицю маршрутизації IPv4.

Статический маршрут по умолчанию маршрутизатора R2

```
R2# show ip route | include 0.0.0.0
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S* 0.0.0.0/0 is directly connected, Serial0/1/0
R2#
```

Рис. 5.6.134

На рис. 5 команда show ip protocols дозволяє переконатися, що R2 перерозподіляє статичні маршрути по домену маршрутизації EIGRP.

Перераспределение статических маршрутов в EIGRP

```
R2# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: static
  EIGRP-IPv4 Protocol for AS(1)
<выходные данные опущены>
```

Рис. 5.6.135

Перевірка розповсюджуваного маршруту за замовчуванням

На малюнку показана частина таблиць маршрутизації IPv4 для маршрутизаторів R1 і R3.

Проверка маршрутов по умолчанию на маршрутизаторах R1 и R3

```
R1# show ip route | include 0.0.0.0
Gateway of last resort is 192.168.10.6 to network 0.0.0.0
D*EX 0.0.0.0/0 [170/3651840] via 192.168.10.6, 00:25:23,
Serial0/0/1
R1#
```

```
R3# show ip route | include 0.0.0.0
Gateway of last resort is 192.168.10.9 to network 0.0.0.0
D*EX 0.0.0.0/0 [170/3139840] via 192.168.10.9, 00:27:17,
Serial0/0/1
R3#
```

Рис. 5.6.136

У таблицях маршрутизації R1 і R3 зверніть увагу на джерело маршрутизації і значення адміністративної дистанції для нового маршруту за замовчуванням, отриманого через протокол EIGRP. Запис для маршруту за замовчуванням, отриманого через EIGRP, характеризується наступними символами:

D - цей маршрут був отриманий через оновлення маршрутизації EIGRP.

- маршрут є кандидатом на маршрут за замовчуванням.

EX - маршрут є зовнішнім маршрутом EIGRP, тобто в даному випадку статичним маршрутом за межами домену маршрутизації EIGRP.

170 - це адміністративна дистанція зовнішнього маршруту EIGRP.

Зверніть увагу, що маршрутизатор R1 вибирає R3 в якості наступника до маршруту за замовчуванням, оскільки він має найменшу реальне відстань. Маршрути за замовчуванням забезпечують шлях за замовчуванням за межі домену маршрутизації і, як об'єднані маршрути, дозволяють скоротити кількість записів в таблиці маршрутизації.

Як ви пам'ятаєте, EIGRP створює окремі таблиці для IPv4 і IPv6, тому маршрут за замовчуванням IPv6 слід поширювати окремо, як показано на рис. 1.

EIGRP для топологии IPv6

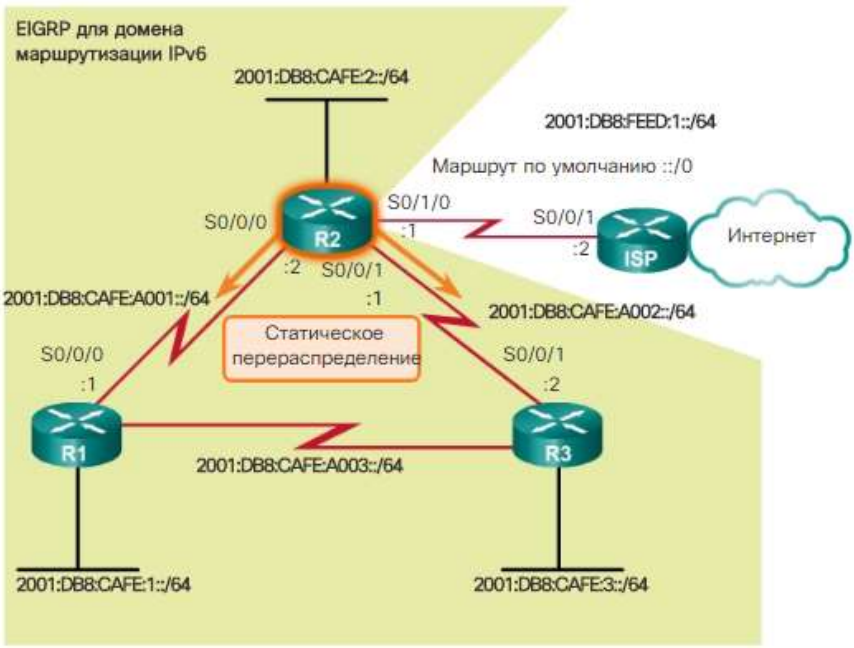


Рис. 5.6.137

Як і у випадку з EIGRP для IPv4, статичний маршрут за замовчуванням налаштовується на шлюзовому маршрутизаторі (R2), як показано на рис. 2:

Настройка и распространение статического маршрута по умолчанию IPv6 маршрутизатора R2

```
R2(config)# ipv6 route ::/0 serial 0/1/0
R2(config)# ipv6 router eigrp 2
R2(config-rtr)# redistribute static
```

Рис. 5.6.138

R2 (config) # ipv6 route :: / 0 serial 0/1/0

Префікс :: / 0 і довжина префікса еквівалентні адресою 0.0.0.0 0.0.0.0 і масці підмережі, використовуваним в IPv4. Обидва адреси складаються з нулів і довжини префікса / 0.

Статичний маршрут за замовчуванням IPv6 перерозподілено в домен EIGRP для IPv6 за допомогою тієї ж команди redistribute static, яка використовувалася в EIGRP для IPv4.

Примітка. У деяких випусках IOS перед перерозподілом статичного маршруту потрібно додати до команди redistribute static метричні параметри EIGRP.

Щоб перевірити поширення статичного маршруту за замовчуванням IPv6, слід вивчити таблицю маршрутизації IPv6 на R1 за допомогою команди show ipv6 route, як показано на рис. 3. Зверніть увагу, що наступником або адресою наступного переходу є маршрутизатор R3, а не R2. Це пояснюється тим, що маршрутизатор R3 забезпечує оптимальний маршрут до R2 по меншій вартості, ніж R1.

Проверка маршрута по умолчанию на маршрутизаторах R1 и R3

```
R1# show ipv6 route
IPv6 Routing Table - default - 12 entries
Codes: C - Connected, L - Local, S - Static,
       U - Per-user Static route
   B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
   IA - ISIS interarea, IS - ISIS summary, D - EIGRP,
      EX - EIGRP external
   ND - ND Default, NDp - ND Prefix, DCE - Destination,
      NDr - Redirect
   O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1,
      OE2 - OSPF ext 2
   ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
EX ::/0 [170/3523840]
   via FE80::3, Serial0/0/1
```

Рис. 5.6.139

За замовчуванням протокол EIGRP використовує не більше 50% пропускної здатності інтерфейсу для передачі інформації EIGRP. Завдяки цьому процес EIGRP не "зловживає» ресурсами каналу, і наявної пропускної здатності досить для маршрутизації звичайного трафіку.

Використовуйте команду ip bandwidth-percent eigrp для настройки відсотка пропускної здатності, який буде використовуватися протоколом EIGRP на інтерфейсі.

Router (config-if) # ip bandwidth-percent eigrp as-number percent

На рис. 1 маршрутизатори R1 і R2 спільно використовують повільний канал з пропускною спроможністю 64 Кбіт / с. На рис. 2 показана конфігурація для обмеження пропускної здатності, використовуваної протоколом EIGRP. При розрахунку процентного кількості пропускної здатності, яку може використовувати протокол EIGRP, команда ip bandwidth-percent eigrp використовує налаштовану пропускну здатність. В даному прикладі EIGRP може використовувати не більше 40% пропускної здатності каналу. Тому для передачі трафіку пакетів EIGRP цей протокол ніколи не використовує більше 25,6 кбіт / с від наявної пропускної здатності каналу.

EIGRP для топологии IPv4

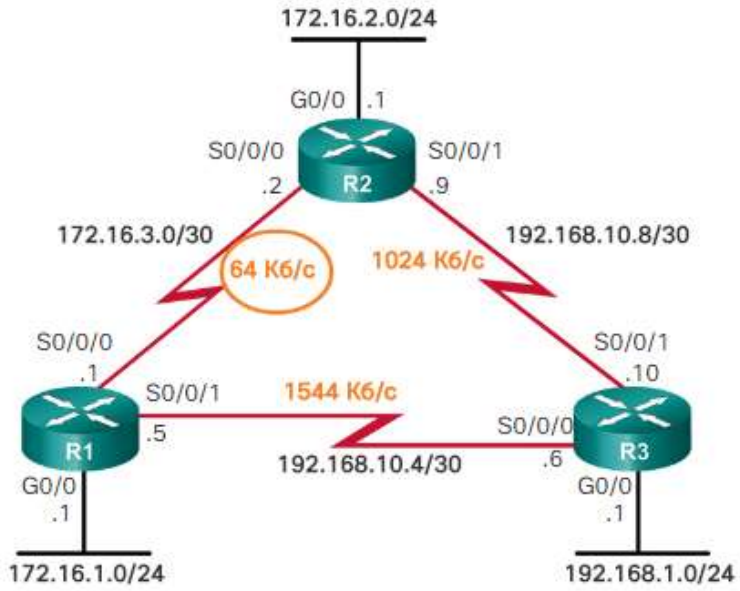


Рис. 5.6.140

Настройка использования пропускной способности с EIGRP для IPv4

```
R1(config)# interface serial 0/0/0
R1(config-if)# ip bandwidth-percent eigrp 1 40
R1(config-if)#
```

```
R2(config)# interface serial 0/0/0
R2(config-if)# ip bandwidth-percent eigrp 1 40
R2(config-if)#
```

Рис. 5.6.141

Для відновлення значення за замовчуванням використовуйте версію no цієї команди.

Щоб встановити необхідний відсоток співвідношення пропускної спроможності, яка може використовуватися EIGRP для IPv6 на інтерфейсі, використовуйте команду ipv6 bandwidth-percent eigrp в режимі конфігурації інтерфейсу. Для відновлення значення за замовчуванням використовуйте версію no цієї команди.

Router (config-if) # ipv6 bandwidth-percent eigrp as-number percent

На рис. 4 представлена конфігурація інтерфейсів між маршрутизаторами R1 і R2 для обмеження пропускної здатності, використовуваної протоколом EIGRP для IPv6.

Настройка использования пропускной способности с EIGRP для IPv6

```
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 bandwidth-percent eigrp 2 40
R1(config-if)#
```

```
R2(config)# interface serial 0/0/0
R2(config-if)# ipv6 bandwidth-percent eigrp 2 40
R2(config-if)#
```

Рис. 5.6.142

Інтервали вітання та очікування з EIGRP для IPv4

EIGRP використовує легкий протокол вітання (Hello) для встановлення і моніторингу підключення його сусіднього пристрою. Час очікування повідомляє маршрутизатора максимальний час, протягом якого він повинен очікувати наступний пакет вітання (hello), перш ніж оголосити дане сусіднє пристрій недоступним.

Інтервали вітання та очікування налаштовуються на інтерфейсах окремо і не повинні збігатися з інтервалами іншихмаршрутизаторів EIGRP при встановленні або підтримці відносин суміжності. Для настройки інтервалів вітання використовується наступна команда:

Router (config-if) # ip hello-interval eigrp as-number seconds

Якщо інтервал вітання (hello) змінився, переконайтеся, що значення часу очікування одно або більше значення інтервалу вітання. В іншому випадку відносини суміжності сусідніх пристроїв будуть порушені після певного періоду, і до наступного інтервалу вітання. Для настройки інтервалів вітання використовується наступна команда:

Router (config-if) # ip hold-time eigrp as-number seconds

Значення seconds як для інтервалу вітання (hello), так і для часу очікування, може бути налаштоване в діапазоні від 1 до 65 535.

На рис. 1 представлена конфігурація маршрутизатора R1 для використання 50-секундного інтервалу вітання та 150-секундного часу очікування. Для відновлення стандартних налаштувань слід використовувати no перед командою.

Настройка протокола EIGRP для интервалов приветствия (hello) и удержания (hold) IPv4

```
R1(config)# interface s0/0/0
R1(config-if)# ip hello-interval eigrp 1 50
R1(config-if)# ip hold-time eigrp 1 150
```

Значения по умолчанию для интервалов приветствия и времени удержания для EIGRP

Пропускная способность	Пример канала	Интервал приветствия по умолчанию	Время удержания по умолчанию
1,544 Мбит/сек	Многоточечный Frame Relay	60 секунд	180 секунд
Более 1,544 Мбит/сек	T1, Ethernet	5 секунд	15 секунд

Рис. 5.6.143

Для формування відносин суміжності між двома маршрутизаторами інтервал вітання (hello) і час очікування (hold) не повинні збігатися.

У EIGRP для IPv6 використовуються ті ж інтервали вітання (hello) і таймери очікування (hold), що і в EIGRP для IPv4. Команди режиму конфігурації інтерфейсу аналогічні тим, що використовуються для IPv4:

Router (config-if) # ipv6 hello-interval eigrp as-number seconds

Router (config-if) # ipv6 hold-time eigrp as-number seconds

На рис. 3 представлені конфігурації інтервалу вітання (hello) і таймера очікування (hold) для маршрутизаторів R1 і R2 з EIGRP для IPv6.

Настройка протокола EIGRP для интервалов приветствия (hello) и удержания (hold) IPv6

```
R1(config)# inter serial 0/0/0
R1(config-if)# ipv6 hello-interval eigrp 2 50
R1(config-if)# ipv6 hold-time eigrp 2 150
```

```
R2(config)# inter serial 0/0/0
R2(config-if)# ipv6 hello-interval eigrp 2 50
R2(config-if)# ipv6 hold-time eigrp 2 150
```

Рис. 5.6.144

Розподіл навантаження з рівною вартістю - це здатність маршрутизатора розподіляти вихідний трафік, використовуючи всі інтерфейси з такою ж метрикою, що і у адреси призначення. При розподілі навантаження сегменти мережі і пропускна здатність використовуються ефективніше. Для IP в Cisco IOS застосовується розподіл навантаження з використанням до чотирьох шляхів з рівною вартістю за замовчуванням.

На рис. 1 представлена мережева топологія EIGRP для IPv4. У цій топології маршрутизатор R3 має два маршрути EIGRP з рівною вартістю до мережі між R1 і R2, 172.16.3.0/30. Один маршрут лежить через маршрутизатор

R1 за адресою 192.168.10.4/30, а інший маршрут через маршрутизатор R2 за адресою 192.168.10.8/30.

EIGRP для топологии IPv4

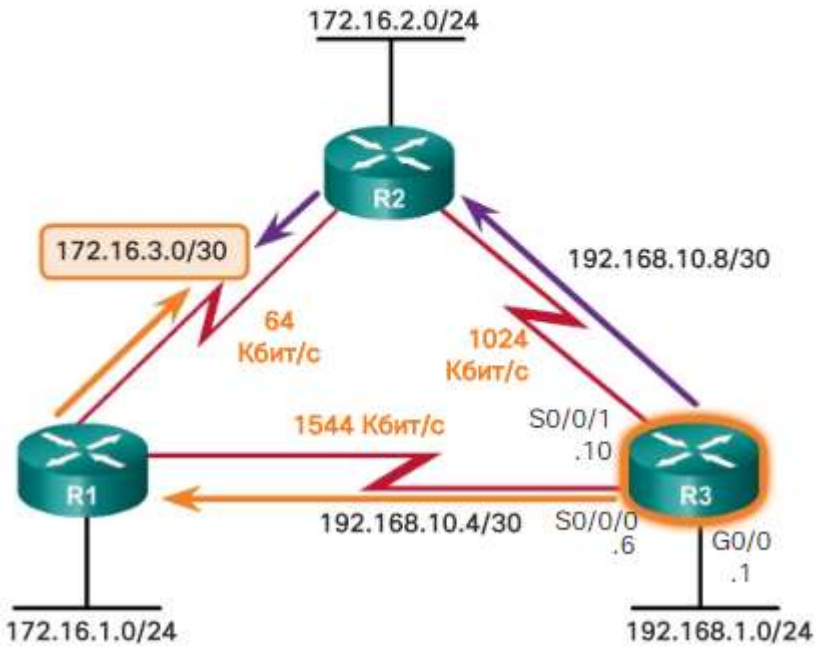


Рис. 5.6.145

Команду show ip protocols можна використовувати для перевірки кількості шляхів з рівною вартістю, налаштованих на маршрутизаторі на даний момент. У вихідних даних на рис. 2 видно, що маршрутизатор R3 використовує чотири шляхи з рівною вартістю за замовчуванням.

Максимальное количество путей маршрутизатора R3

```
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 3.3.3.3
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Address Summarization:
    192.168.0.0/22 for Se0/0/0, Se0/0/1
      Summarizing 3 components with metric 2816
  Maximum path: 4

<выходные данные опущены>
```

Рис. 5.6.146

У таблиці маршрутизації містяться обидва цих маршруту. На рис. 3 показано, що маршрутизатор R3 має два маршрути EIGRP з рівною вартістю для мережі 172.16.3.0/30. Один маршрут лежить через маршрутизатор R1 за

адресою 192.168.10.5, а інший маршрут через маршрутизатор R2 за адресою 192.168.10.9. З топології на рис. 1 може здатися, що шлях через R1 є більш оптимальним, оскільки маршрутизатори R3 і R1 з'єднані каналом з пропускною спроможністю 1 544 кбіт / с, а пропускна здатність на каналі до R2 становить лише 1024 кбіт / с. Однак EIGRP використовує тільки саму повільну пропускну здатність з наявних, і це канал 64 кбіт / с між маршрутизаторами R1 і R2. На обох шляхах канал з пропускною спроможністю 64 Кбіт / с є найповільнішим, через що ці шляхи є рівними.

Таблица маршрутизации IPv4 маршрутизатора R3

```
R3# show ip route eigrp
<выходные данные опущены>

Gateway of last resort is 192.168.10.9 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/3139840] via 192.168.10.9, 00:14:24,
Serial0/0/1
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D        172.16.1.0/24 [90/2170112] via 192.168.10.5,
         00:14:28, Serial0/0/0
D        172.16.2.0/24 [90/3012096] via 192.168.10.9,
         00:14:24, Serial0/0/1
D        172.16.3.0/30 [90/41024000] via 192.168.10.9,
         00:14:24, Serial0/0/1
              [90/41024000] via 192.168.10.5, 00:14:24,
               Serial0/0/0
D     192.168.0.0/22 is a summary, 00:14:40, Null0
R3#
```

Рис. 5.6.147

Коли пакет проходить комутацію, то в процесі розподілу навантаження через колії з рівною вартістю бере участь кожен пакет. Коли пакети проходять швидку комутацію, то розподіл навантаження через колії з рівною вартістю виконується на рівні пунктів призначення. Метод комутації CEF (Cisco Express Forwarding) виконує розподіл навантаження як для пакетів, так і для місць призначень.

Cisco IOS за замовчуванням дозволяє використовувати в розподілі навантаження до чотирьох шляхів, проте ця кількість можна змінити. Завдяки команді режиму конфігурації маршрутизатора maximum-paths таблиця маршрутизації може містити до 32 маршрутів з рівною вартістю.

Router (config-router) # maximum-paths value

Аргумент value вказує кількість маршрутів, які може містити таблиця для розподілу навантаження. Якщо це значення налаштоване на 1, то розподіл навантаження відключається.

На рис. 1 представлена мережева топологія EIGRP для IPv6. Послідовні канали в топології мають ту ж пропускну здатність, що використовується в топології EIGRP для IPv4.

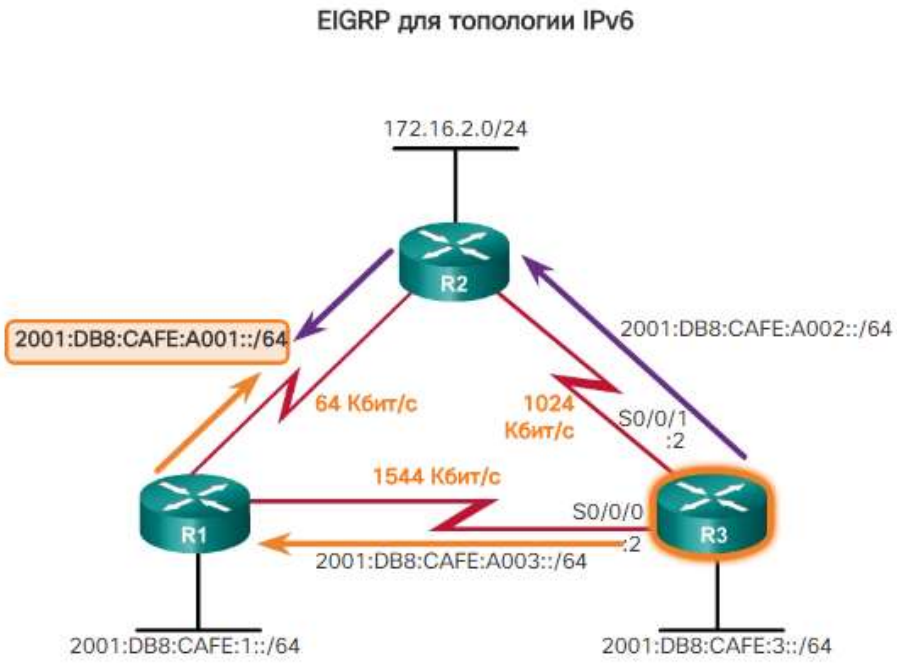


Рис. 5.6.148

Як і в попередньому випадку для IPv4, маршрутизатор R3 має два маршрути EIGRP з рівною вартістю для мережі між маршрутизаторами R1 і R2, 2001: DB8: CAFE: A001 :: / 64. Один маршрут проходить через маршрутизатор R1 за адресою FE80 :: 1, а інший маршрут - через маршрутизатор R2 за адресою FE80 :: 2.

На рис. 2 показано, що в таблицях маршрутизації IPv6 і IPv4 містяться рівні метрики для мереж 2001: DB8: CAFE: A001 :: / 64 і 172.16.3.0/30. Це пояснюється тим, що складова метрика EIGRP для IPv6 і для IPv4 однакова.

Таблица маршрутизации IPv6 маршрутизатора R3

```
R3# show ipv6 route eigrp
 <выходные данные опущены>

EX   ::/0 [170/3011840]
     via FE80::2, Serial0/0/1
D    2001:DB8:ACAD::/48 [5/128256]
     via Null0, directly connected
D    2001:DB8:CAFE:1::/64 [90/2170112]
     via FE80::1, Serial0/0/0
D    2001:DB8:CAFE:2::/64 [90/3012096]
     via FE80::2, Serial0/0/1
D    2001:DB8:CAFE:A001::/64 [90/41024000]
     via FE80::2, Serial0/0/1
     via FE80::1, Serial0/0/0
R3#
```

Рис. 5.6.149

Розподіл навантаження з нерівній вартістю

Крім того, EIGRP для IPv4 і IPv6 може розподіляти трафік по декількох маршрутах з різними метриками. Це називається розподілом навантаження з нерівній вартістю. Якщо налаштувати значення за допомогою команди variance в режимі конфігурації маршрутизатора, EIGRP додасть в локальну таблицю маршрутизації кілька беспетлевого маршрутів з нерівній вартістю.

Щоб маршрут, отриманий через EIGRP, міг бути доданий в локальну таблицю маршрутизації, він повинен відповідати двом критеріям:

Маршрут повинен бути беспетлевого, бути можливим наступником або мати оголошене відстань, яке менше сумарного відстані.

Метрика маршруту повинна бути менше метрики оптимального маршруту (наступника), помноженої на відхилення, налаштоване на маршрутизаторі.

Наприклад, якщо коефіцієнт відхилення налаштований на 1, то в локальну таблицю маршрутизації додаються тільки маршрути з тієї ж метрикою, що і у кращого маршруту. Якщо коефіцієнт відхилення налаштований на 2, то в локальну таблицю маршрутизації буде встановлений будь-який маршрут, отриманий через EIGRP, з метрикою в 2 рази менше, ніж метрика кращого маршруту.

Щоб контролювати розподіл трафіку за маршрутами в тому випадку, коли до одного і того ж місця призначення є кілька маршрутів з різною вартістю, використовуйте команду traf fi c-share balanced. В цьому випадку трафік буде розподілятися пропорційно процентному співвідношенню вартостей.

Мережеві адміністратори повинні знати, що маршрутизатори схильні до ризику атак так само, як і пристрої кінцевих користувачів. Будь-який користувач з аналізатором пакетів, наприклад програмою Wireshark, може прочитати дані, поширювані між маршрутизаторами. Як правило, системи маршрутизації піддаються атакам через порушення безпеки рівноправних пристроїв або фальсифікацію відомостей про маршрутах.

Порушення безпеки рівноправних пристроїв - це найменш небезпечна загроза з двох згаданих, оскільки протоколи маршрутизації самі відновлюють свою систему безпеки, завдяки чому загроза зникає незабаром після самої атаки.

Фальсифікація відомостей маршрутизації - це більш небезпечний вид атаки, метою якої є відомості, що передаються протоколом маршрутизації. До наслідків фальсифікації даних про маршрути відносяться:

- перенаправлення трафіку для створення петель маршрутизації
- перенаправлення трафіку для відстеження незахищеного каналу
- перенаправлення трафіку з метою його видалення.

Для захисту відомостей про маршрути в мережі використовується аутентифікація пакетів протоколу маршрутизації за допомогою алгоритму Message Digest 5 (MD5). Алгоритм MD5 дозволяє маршрутизаторів порівнювати підписи, які повинні бути однаковими, для підтвердження, що вони отримані від надійного джерела.

Така система складається з трьох компонентів:

- алгоритм шифрування, який є загальновідомим

- ключ, який використовується в алгоритмі шифрування; цей ключ можуть знати тільки маршрутизатори, аутентифицирующей свої пакети
- вміст самого пакета.

Як правило, автор відомостей про маршрутах створює підпис, використовуючи ключ і дані маршрутизації, які він збирається відправити, як шифрованих даних. Потім маршрутизатор, який одержує відомості маршрутизації, може повторити цей процес, використовуючи той же ключ і ті ж дані маршрутизації, які він отримав. Якщо підпис, яку створює одержувач, збігається з підписом відправника, то оновлення успішно аутентифицироваться і визнається надійним.

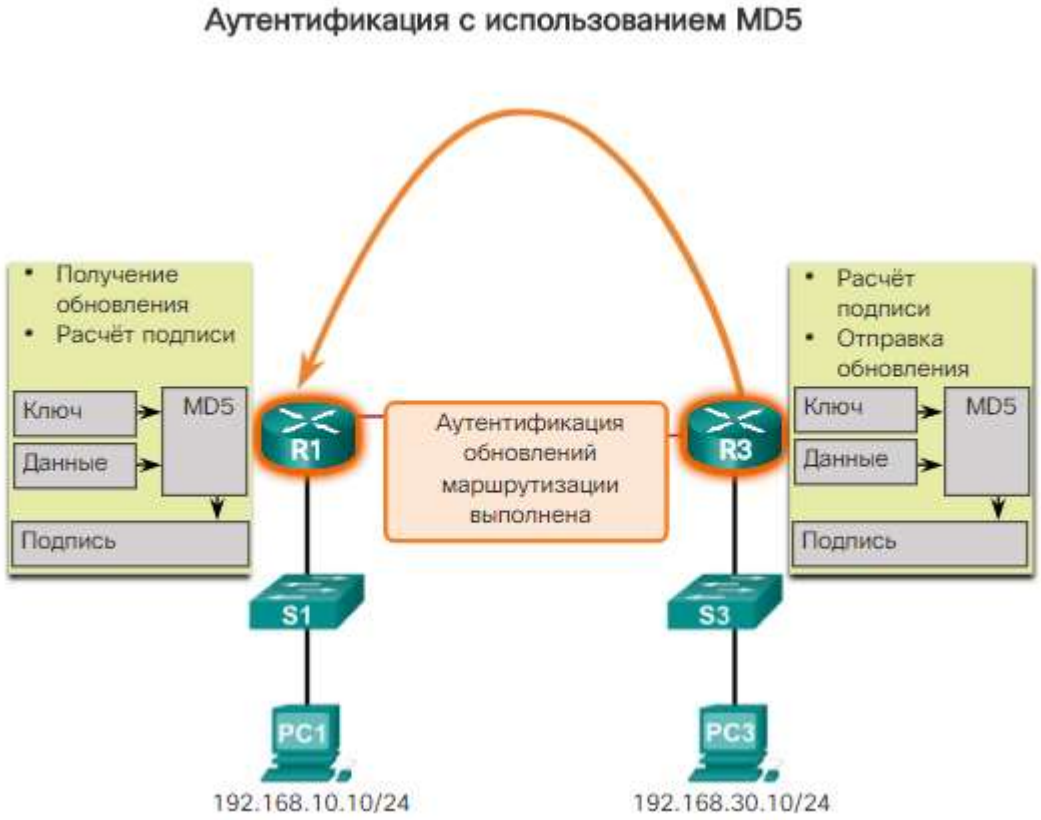


Рис. 5.6.150

Різні форми аутентифікації MD5 підтримуються протоколами RIPv2, EIGRP, OSPF, IS-IS і BGP.

Повідомлення аутентифікації EIGRP гарантує, що маршрутизатори приймають повідомлення маршрутизації тільки від інших маршрутизаторів, яким відомий один і той же попередньо узгоджений ключ. Якщо без налаштованої аутентифікації сторонній користувач додає до мережі іншого маршрутизатор з іншими або неправильними відомостями маршрутизації, то можуть виникнути пошкодження в таблицях маршрутизації на допустимих маршрутизаторах або атака відмови в обслуговуванні (DoS). Таким чином, настройка аутентифікації на повідомленнях EIGRP, що відправляються між маршрутизаторами, запобіжить навмисне чи випадкове додавання іншого маршрутизатора до мережі і виникнення пов'язаних з цим додаванням неполадок.

EIGRP підтримує аутентифікацію протоколу маршрутизації за допомогою MD5. Налаштування аутентифікації повідомлень EIGRP складається з двох

кроків: створення ланцюжка ключів і ключа і настройка аутентифікації EIGRP для використання ланцюжка ключів і ключа.

Крок 1. Створення ланцюжка ключів і ключа

Для аутентифікації потрібно ключ в ланцюжку ключів. Перед включенням аутентифікації створіть ланцюжок ключів і, по крайней мере, один ключ.

a. У режимі глобальної конфігурації створіть ланцюжок ключів. Незважаючи на те, що можна налаштувати кілька ключів, в даному розділі розглядається створення тільки одного ключа.

Router (config) # key chain name-of-chain

b. Вкажіть ідентифікатор ключа. Ідентифікатор ключа - це номер, який використовується для визначення ключ аутентифікації в ланцюжку ключів. Діапазон ключів варіюється від 0 до 2 147 483 647. Рекомендується призначати однаковий ідентифікатор ключа на всіх маршрутизаторах в конфігурації.

Router (config-keychain) # key key-id

c. Визначте значення ключа. Значення ключа повинно збігатися з паролем. На маршрутизаторах, які обмінюються ключами аутентифікації, має бути налагоджене однакове значення ключа.

Router (config-keychain-key) # key-string key-string-text

Крок 2. Налаштування аутентифікації EIGRP за допомогою ланцюжка ключів і ключа

Налаштуйте EIGRP для настройки аутентифікації повідомлень з наперед заданим ключем. Виконайте цю конфігурацію на всіх інтерфейсах, налаштованих для EIGRP.

a. У режимі глобальної конфігурації вкажіть інтерфейс, на якому буде налаштована аутентифікація повідомлень EIGRP.

Router (config) # interface type number

b. Увімкніть аутентифікацію повідомлень EIGRP. Ключове слово md5 означає, що для аутентифікації буде використовуватися хеш MD5.

Router (config-if) # ip authentication mode eigrp as-number md5

c. Визначте ланцюжок ключів, яка буде використовуватися для аутентифікації. Аргумент name-of-chain визначає ланцюжок ключів, створену на кроці 1.

Router (config-if) # ip authentication key-chain eigrp as-number name-of-chain

Each key has its own key ID, which is stored locally. Поєднання ключового ідентифікатора і інтерфейсу, пов'язаного з повідомленням, однозначно визначає алгоритм аутентифікації і використовуваний ключ аутентифікації MD5. Для створення унікальної підписи ланцюжок ключів і оновлення маршрутизації обробляються за допомогою алгоритму MD5.

Аутентификация EIGRP с использованием MD5

Шаг 1. Создание цепочки ключей и ключа

```
Router(config)# key chain name-of-chain
Router(config-keychain)# key key-id
Router(config-keychain-key)# key-string key-string-text
```

Шаг 2. Настройка аутентификации EIGRP с помощью цепочки ключей и ключа

```
Router(config)# interface type number
Router(config-if)# ip authentication mode eigrp as-number md5
Router(config-if)# ip authentication key-chain eigrp as-number
name-of-chain
```

Рис. 5.6.151

Приклад аутентифікації EIGRP

Для аутентифікації оновлень маршрутизації EIGRP-інтерфейси необхідно налаштувати на підтримку аутентифікації. На рис. 1 представлені топологія IPv4 і інтерфейси, налаштовані з аутентифікацією.

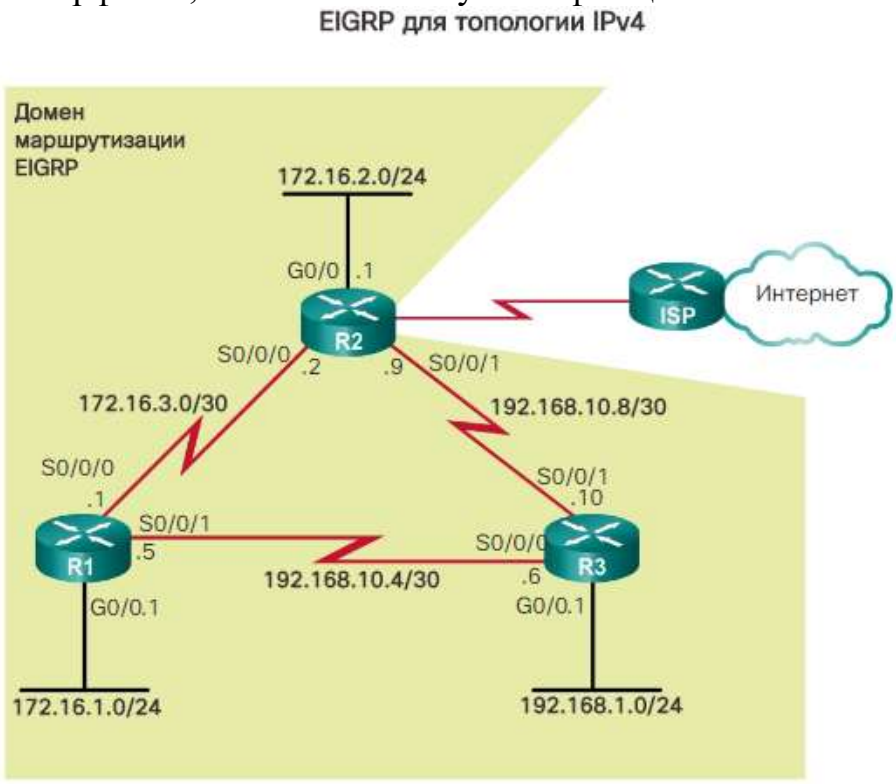


Рис. 5.6.152

На рис. представлена конфігурація для маршрутизатора R1 з використанням ланцюжка ключів EIGRP_KEY і рядок ключів cisco123. Після настройки маршрутизатора R1 інші маршрутизатори отримують аутентифіковані відновлення маршрутизації. Відносини суміжності втрачаються до тих пір, поки аутентифікація протоколу маршрутизації ще не встановлено на сусідніх пристроях.

Настройка аутентификации MD5 для EIGRP на маршрутизаторе R1

```
R1(config)# key chain EIGRP_KEY
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string cisco123
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip authentication mode eigrp 1 md5
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY
R1(config-if)# exit
R1(config)# interface serial 0/0/1
R1(config-if)# ip authentication mode eigrp 1 md5
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY
R1(config-if)# end
R1#
```

Рис. 5.6.153

На рис. представлена аналогічна конфігурація для маршрутизатора R2. Зверніть увагу, що одна і та ж рядок ключа, cisco123, використовується для аутентифікації відомостей з маршрутизатором R1 і, в кінцевому рахунку, R3.

Настройка аутентификации MD5 для EIGRP на маршрутизаторе R2

```
R2(config)# key chain EIGRP_KEY
R2(config-keychain)# key 1
R2(config-keychain-key)# key-string cisco123
R2(config-keychain-key)# exit
R2(config-keychain)# exit
R2(config)# interface serial 0/0/0
R2(config-if)# ip authentication mode eigrp 1 md5
R2(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config-if)# ip authentication mode eigrp 1 md5
R2(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY
R2(config-if)# end
R2#
```

Рис. 5.6.154

Алгоритми і конфігурація для аутентифікації EIGRP для повідомлень IPv6 мало чим відрізняється від IPv4. Єдина відмінність полягає в тому, що в командах режиму конфігурації використовується ipv6, а не ip.

Router (config-if) # ipv6 authentication mode eigrp as-number md5

Router (config-if) # ipv6 authentication key-chain eigrp as-number name-of-chain

На рис. 5 представлені команди для конфігурації EIGRP для аутентифікації IPv6 на маршрутизаторі R1 за допомогою ланцюжка ключів EIGRP_IPV6_KEY і рядки ключів cisco123. Аналогічні настройки знадобиться ввести на маршрутизаторах R2 і R3.

Настройка аутентификации MD5 для IPv6 на маршрутизаторе R1

```
R1(config)# key chain EIGRP_IPV6_KEY
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string cisco123
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 authentication mode eigrp 2 md5
R1(config-if)# ipv6 authentication key-chain eigrp 2
               EIGRP_IPV6_KEY
R1(config-if)# exit
R1(config)# interface serial 0/0/1
R1(config-if)# ipv6 authentication mode eigrp 2 md5
R1(config-if)# ipv6 authentication key-chain eigrp 2
               EIGRP_IPV6_KEY
R1(config-if)#
```

Рис. 5.6.155

Після настройки аутентифікації повідомлень EIGRP на одному маршрутизаторі все суміжні сусідні пристрої, на яких ще не була налаштована аутентифікація, перестануть бути сусідніми пристроями EIGRP. Наприклад, якщо інтерфейс Serial 0/0/0 маршрутизатора R1 був налаштований для аутентифікації MD5 на відміну від маршрутизатора R2, то на маршрутизаторі R1 з'явиться наступне повідомлення IOS:

% DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.3.2 (Serial0 / 0/0) is down: authentication mode changed

Відносини суміжності відновляться після настройки суміжного інтерфейсу Serial 0/0/0 на маршрутизаторі R2, а на маршрутизаторі R1 з'явиться наступне повідомлення IOS:

% DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.3.2 (Serial0 / 0/0) is up: new adjacency

Аналогічні повідомлення з'являться на маршрутизаторі R2.

Відносини суміжності формуються тільки в тому випадку, якщо аутентифікація налаштована на обох підключених пристроїв.

EIGRP для топологии IPv4

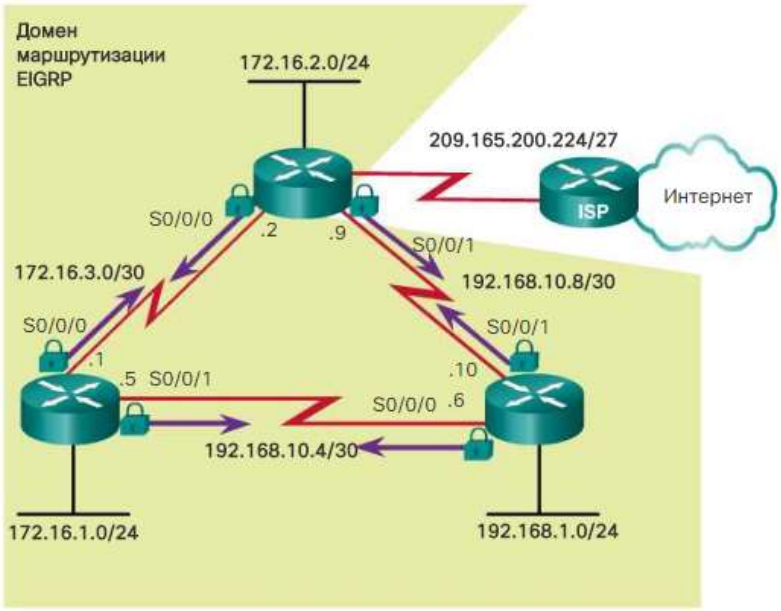


Рис. 5.6.156

Для перевірки відносин суміжності EIGRP після настройки аутентифікації використовуйте для кожного маршрутизатора команду show ip eigrp neighbors. На рис. 2 показано, що після настройки аутентифікації EIGRP на всіх трьох маршрутизаторах між ними відновлені відносини суміжності.

Проверка аутентификации MD5 для EIGRP на маршрутизаторе R1

```
R1# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address      Interface  Hold Uptime   SRTT   RTO  Q  Seq
                          (sec)         (ms)       Cnt Num
1 172.16.3.2   Se0/0/0     140 03:28:12  96   2340  0  23
0 192.168.10.6 Se0/0/1      14 03:28:27  49    294  0  24
R1#
```

```
R2# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address      Interface Hold Uptime   SRTT   RTO  Q  Seq
                         (sec)         (ms)       Cnt Num
1 172.16.3.1   Se0/0/0    136 00:22:50 1046  5000  0  32
0 192.168.10.10Se0/0/1     10 07:51:37   62   372  0  35
R2#
```

```
R3# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address      Interface Hold Uptime   SRTT   RTO  Q  Seq
                         (sec)         (ms)       Cnt Num
0 192.168.10.5 Se0/0/0    14 00:21:26  1297  5000  0  33
1 192.168.10.9 Se0/0/1    14 07:51:50    43   258  0  36
R3#
```

Рис. 5.6.157

Основні команди, які застосовуються для пошуку і усунення неполадок в EIGRP

Як правило, протокол EIGRP використовується в великих корпоративних мережах. Адміністратор повинен вміти знаходити і усувати неполадки, пов'язані з обміном інформацією про маршрути. Особливо це стосується адміністраторів, які задіяні в реалізації і обслуговуванні великих комутованих

корпоративних мереж, що використовують EIGRP в якості протоколу внутрішніх шлюзів (IGP). Для усунення неполадок в мережі EIGRP необхідно знати наступні команди.

Команда show ip eigrp neighbors використовується для того, щоб переконатися, що маршрутизатор розпізнає свої сусідні пристрої. У вихідних даних на рис. 1 представлені два успішно встановлених відносини суміжності між сусідніми пристроями EIGRP на маршрутизатор R1.

Таблица соседних устройств EIGRP маршрутизатора R1

```
R1# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address       Interface  Hold Uptime    SRTT  RTO  Q  Seq
                              (sec)          (ms)     Cnt Num
1 172.16.3.2    Se0/0/0     140 03:28:12   96  2340  0  23
0 192.168.10.6  Se0/0/1      14 03:28:27   49   294  0  24
R1#
```

Рис. 5.6.158

На рис. команда show ip route дозволяє переконатися, що маршрутизатор отримав відомості про маршрут до віддаленої мережі через EIGRP. Вихідні дані вказують, що маршрутизатор R1 дізнався близько чотирьох віддалених мереж через EIGRP.

Таблица маршрутизации IPv4 маршрутизатора R1

```
R1# show ip route eigrp

Gateway of last resort is 192.168.10.6 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/3651840] via 192.168.10.6, 05:32:02,
      Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
D        172.16.2.0/24 [90/3524096] via 192.168.10.6, 05:32:02,
         Serial0/0/1
D     192.168.0.0/22 [90/2170112] via 192.168.10.6, 05:32:02,
      Serial0/0/1
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D        192.168.10.8/30 [90/3523840] via 192.168.10.6,
         05:32:02,Serial0/0/1
R1#
```

Рис. 5.6.159

На рис. показані вихідні дані команди show ip protocols. Дана команда дозволяє переконатися, що EIGRP відображає поточні значення для різних властивостей всіх активних протоколів маршрутизації.

Процессы протоколов маршрутизации R1

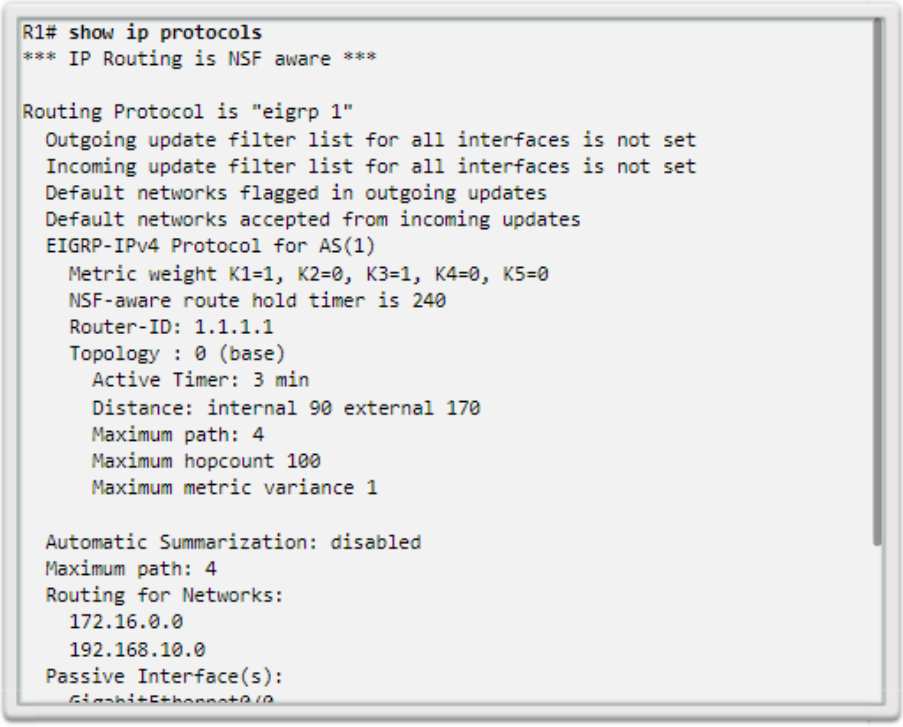


Рис. 5.6.160

EIGRP для IPv6

Аналогічні команди і критерії пошуку та усунення несправностей застосовуються і в EIGRP для IPv6.

Нижче наведені відповідні команди, які використовуються для EIGRP для IPv6:

- Router # show ipv6 eigrp neighbors
- Router # show ipv6 route
- Router # show ipv6 protocols

Компоненти

На малюнку зображена схема діагностики неполадок з підключенням EIGRP.

Рис. 5.6.161

Після настройки EIGRP насамперед слід протестувати підключення до віддаленої мережі. Якщо луна-запит був невдалим, підтвердіть відносини суміжності між сусідами EIGRP. Відносини суміжності сусідніх пристроїв можуть не сформуватися з наступних причин:

Відсутня дає змогу пристроям обмінюватися.

На двох маршрутизаторах не збігаються номери автономної системи EIGRP (ідентифікатори процесу).

Для роботи процесу EIGRP не включені потрібні інтерфейси.

Інтерфейс налаштований як пасивного.

Формуванню відносин суміжності можуть перешкоджати і інші, більш складні неполадки. Наприклад, неправильно налаштована аутентифікація EIGRP або неспівпадаючі значення коефіцієнтів K, які використовує протокол EIGRP для розрахунку метрики.

Якщо між двома маршрутизаторами сформувалися відносини суміжності EIGRP, але підключення як і раніше не встановлено, то проблема може полягати в маршрутизації. До неполадок, які перешкоджають встановленню підключення для EIGRP, відносяться наступні:

У віддалених Маршрутизатор не оголошуються відповідні мережі.

Оголошення про віддалених мережах блокуються пасивним інтерфейсом або неправильно налаштованим ACL-списком.

Автоматичне об'єднання може привести до непослідовної маршрутизації в «розірваної» мережі.

Якщо в таблиці маршрутизації знаходяться всі необхідні маршрути, але трафік слід по неправильному шляху, перевірте значення пропускної здатності на інтерфейсі.

Підключення 3-го рівня

Обов'язковою умовою для встановлення відносин суміжності між двома маршрутизаторами з прямим підключенням є доступність на 3-му рівні. Вивчивши вихідні дані команди show ip interface brief, мережевий адміністратор може переконатися, що як протокол, так і самі підключаються інтерфейси включені. Підключення IPv4 між двома пристроями можна перевірити за допомогою exo-запиту, відправленого від одного маршрутизатора на інший маршрутизатор з прямим підключенням. На малюнку представлені вихідні дані команди show ip interface brief для маршрутизатора R1. Маршрутизатор R1 підключений до маршрутизатора R2, луна-запити відправляються успішно.

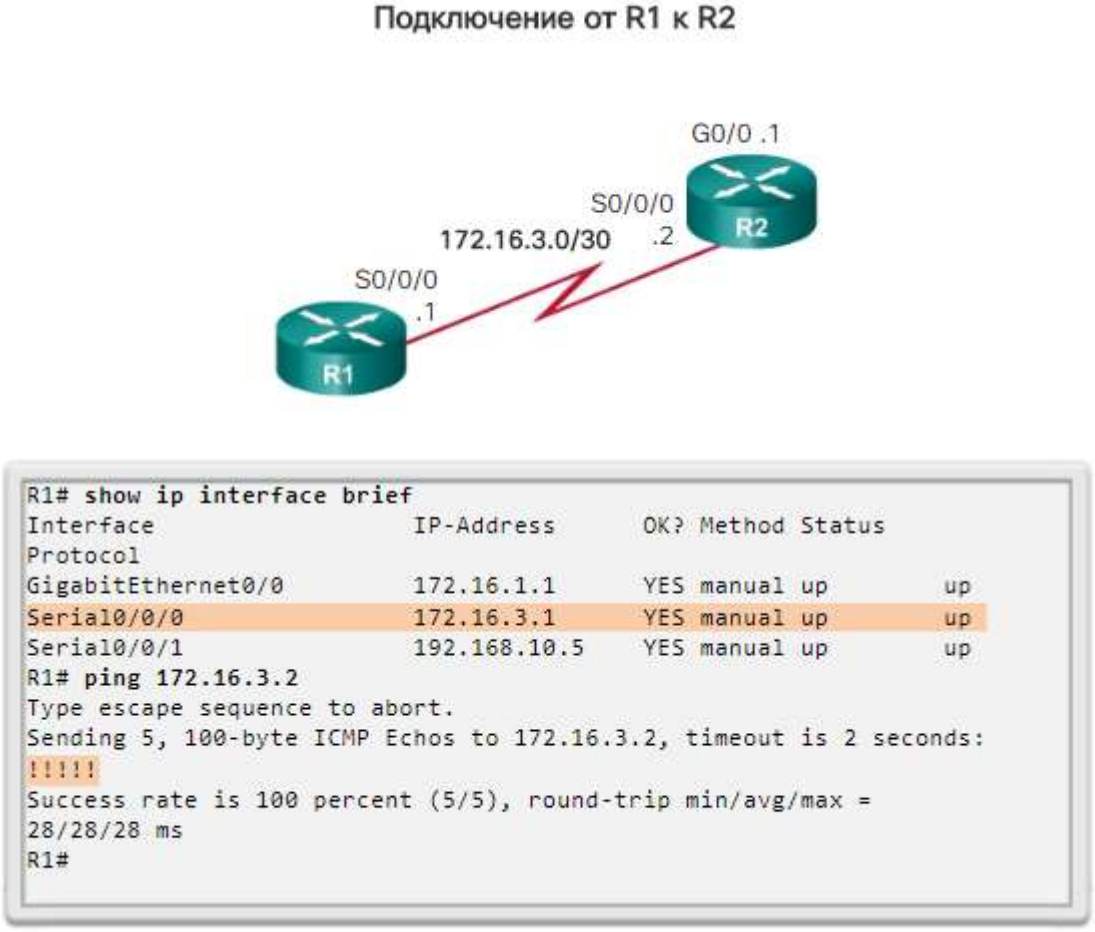


Рис. 5.6.162

Якщо луна-запит був відправлений невдало, перевірте кабелі та переконайтеся, що інтерфейси на підключених пристроях підключені до загальної підмережі. Повідомлення журналу про те, що сусідні вузли EIGRP not on common subnet (не перебувають в загальній мережі) означає, що на одному з двох сусідніх інтерфейсів EIGRP налаштований невірний IPv4-адрес.

EIGRP для IPv6

Аналогічні команди і критерії пошуку та усунення несправностей застосовуються і в EIGRP для IPv6.

У випадку з EIGRP для IPv6 використовується еквівалентна команда show ipv6 interface brief.

При пошуку і усунення неполадок в мережі EIGRP насамперед рекомендується переконатися, що на всіх маршрутизаторах, які знаходяться в рамках мережі EIGRP, налаштований однаковий номер автономної системи. Команда router eigrp as-number, після якої слід номер автономної системи,

запускає процес EIGRP. Значення аргументу as-number має бути однаковим для всіх маршрутизаторів, які знаходяться в одному і тому ж домені маршрутизації протоколу EIGRP.

На рис. 1 показано, що на всіх маршрутизаторах повинен бути налаштований номер автономної системи 1.

EIGRP для топологии IPv4

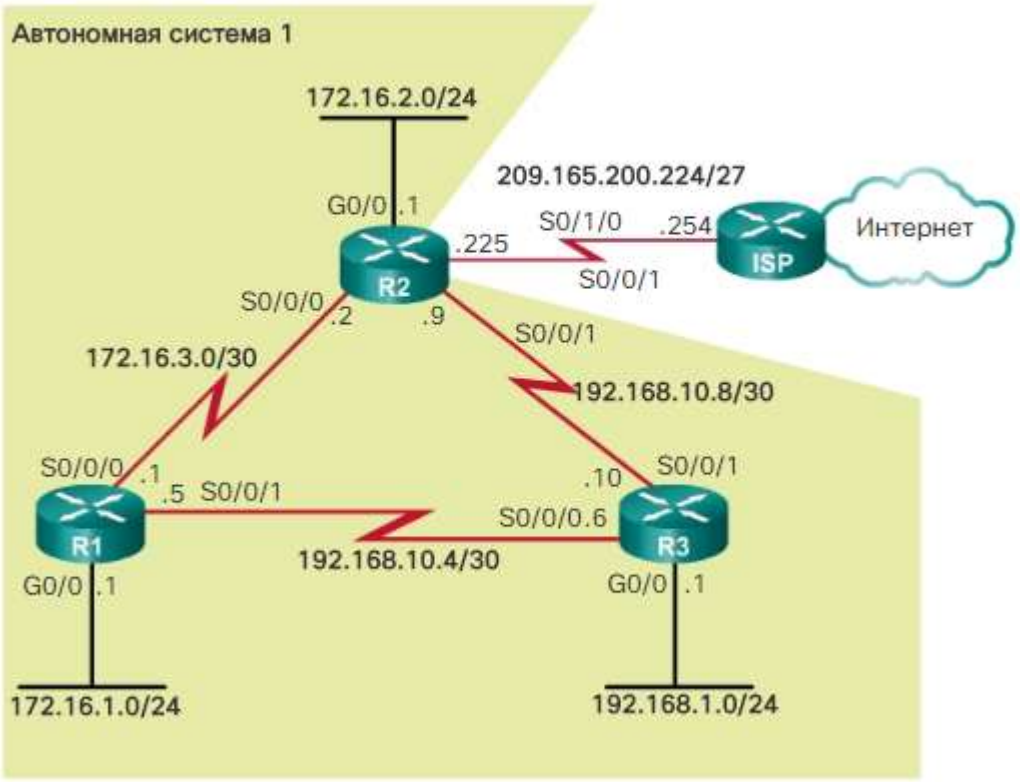


Рис. 5.6.163

На рис. команда show ip protocols дозволяє переконатися, що маршрутизатори R1, R2 і R3 використовують один і той же номер автономної системи.

Запуск интерфейса IPv4 и протокола EIGRP для конфигурации IPv4

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
<выходные данные опущены>
```

```
R2# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is  "eigrp 1"
<выходные данные опущены>
```

```
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is  "eigrp 1"
<выходные данные опущены>
```

Рис. 5.6.164

Аналогічні команди і критерії пошуку та усунення несправностей застосовуються і в EIGRP для IPv6.

Нижче наведені відповідні команди, які використовуються для EIGRP для IPv6:

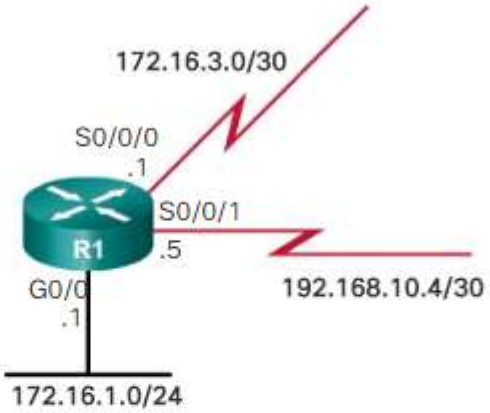
- Router (config) # ipv6 router eigrp as-number
- Router # show ipv6 protocols

Примітка. Інформація з верхньої частини вихідних даних «IP Routing is NSF aware» відноситься до безперервної пересилання (Nonstop Forwarding, NSF). Ця функція дозволяє рівноправним вузлів EIGRP несправного маршрутизатора зберегти відомості про маршрутах, які були їм оголошені, а також далі використовувати ці відомості, поки несправний маршрутизатор не буде поновлено і не зможе обмінюватися відомостями про маршрутах.

Крім перевірки номера автономної системи, необхідно переконатися, що всі інтерфейси підключені до мережі EIGRP. Команда network, виконана для процесу маршрутизації EIGRP, дозволяє визначити, які інтерфейси маршрутизатора братимуть участь в процесі EIGRP. Ця команда застосовується до адресою класової мережі інтерфейсу або, якщо включена шаблонна маска, до адресою підмережі.

На рис. 1 команда show ip eigrp interfaces відображає, які інтерфейси налаштовані для EIGRP на маршрутизатор R1. Якщо підключення інтерфейси не налаштовані для EIGRP, то сусідні пристрої не зможуть сформувати відносини суміжності.

Интерфейсы IPv4 EIGRP




```
R1# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(1)
                Xmit Queue   PeerQ        Mean   Pacing Time   Mult
Interface  Peers Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow
Gi0/1        0       0/0         0/0          0        0/0
Se0/0/0      1       0/0         0/0       1295        0/23
Se0/0/1      1       0/0         0/0       1044        0/15
R1#
```

Рис. 5.6.165

На рис. в розділі «Routing for Networks» вихідних даних команди show ip protocols вказані налаштовані мережі; всі інтерфейси цих мереж беруть участь в процесі EIGRP.

Процессы протоколов маршрутизации R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"

<выходные данные опущены>

Routing for Networks:
    172.16.0.0
    192.168.10.0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.10.6          90      00:42:31
    172.16.3.2            90      00:42:31
  Distance: internal 90 external 170

R1#
```

Рис. 5.6.166

Якщо в цьому розділі немає потрібної мережі, використовуйте команду show running-config, щоб переконатися, що була налаштована вірна команда network.

У вихідних даних команди show running-config на рис. 3 підтверджується, що всі інтерфейси з цими адресами або підмережа зазначених адрес налаштовані для EIGRP.

Объявляемые сети IPv4 по протоколу EIGRP маршрутизатора R1

```
R1# show running-config | section eigrp 1
router eigrp 1
 network 172.16.0.0
 network 192.168.10.0
 passive-interface GigabitEthernet0/0
 eigrp router-id 1.1.1.1
R1#
```

Рис. 5.6.167

Аналогічні команди і критерії пошуку та усунення несправностей застосовуються і в EIGRP для IPv6.

Нижче наведені відповідні команди, які використовуються для EIGRP для IPv6:

- Router # show ipv6 protocols
- Router # show ipv6 eigrp interfaces

У таблицях маршрутизації можуть не відбиватися вірні маршрути через команди passive-interface. Якщо мережа працює з EIGRP, то команда passive-interface припиняє передачу як вихідних, так і вхідних оновлень маршрутизації. З цієї причини маршрутизатори не зможуть стати сусідніми пристроями.

Щоб перевірити, чи налаштований інтерфейс маршрутизатора в якості пасивного, виконайте команду show ip protocols в привілейованому режимі. На рис. 1 показано, що інтерфейс GigabitEthernet 0/0 маршрутизатора R2 налаштований як пасивного, оскільки на цьому каналі немає сусідніх пристроїв.

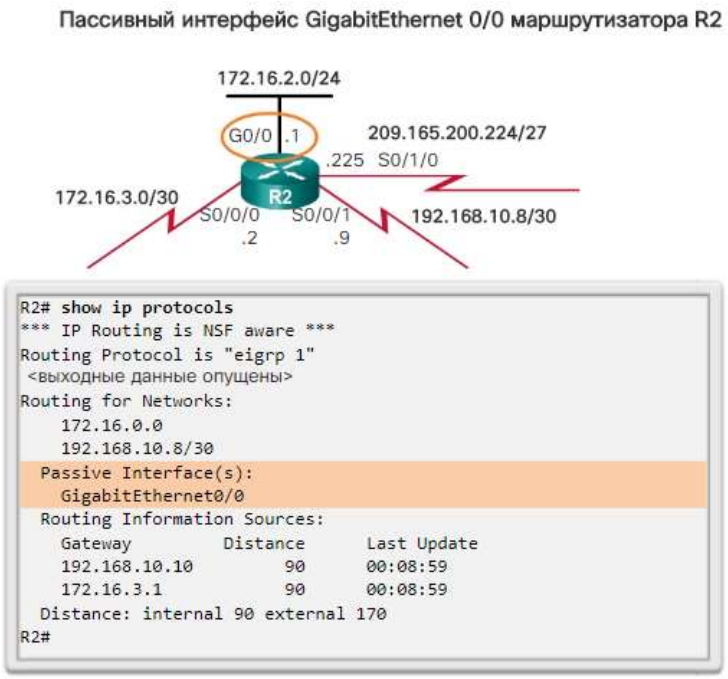
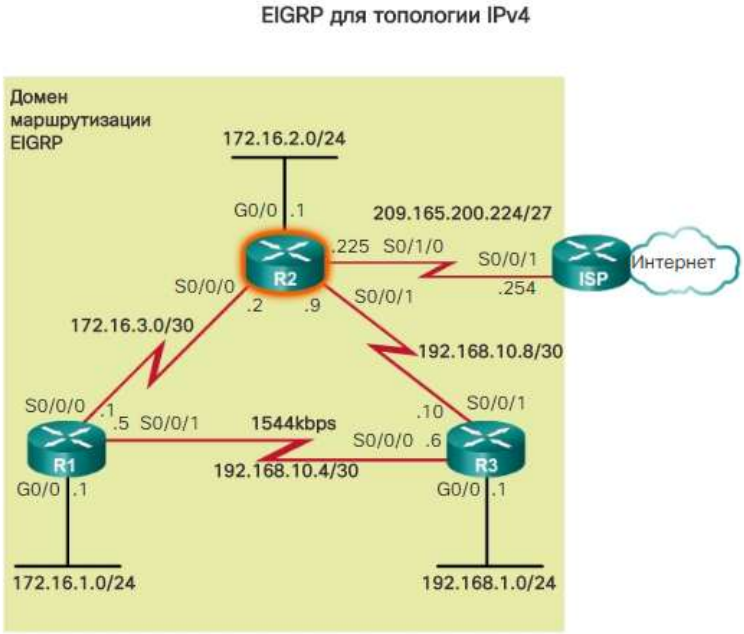


Рис. 5.6.168

Пасивний інтерфейс може бути не тільки налаштований на інтерфейсах, які не мають сусідніх пристроїв, він також може бути включений в цілях забезпечення безпеки. На рис. зверніть увагу, що зафарбовування домену маршрутизації EIGRP відрізняється від попередніх топологій. Тепер мережа 209.165.200.224/27 включена в оновлення EIGRP маршрутизатора R2. Однак з міркувань безпеки мережевий адміністратор не хоче, щоб між маршрутизаторами R2 і ISP сформувалися відносини суміжності EIGRP.



На рис. показано додавання команди network для мережі 209.165.200.224/27 на маршрутизаторі R2. Тепер R2 оголошує цю мережу іншим маршрутизаторів в домені маршрутизації EIGRP.

Настройка сети к ISP в качестве пассивного интерфейса

```
R2(config)# router eigrp 1
R2(config-router)# network 209.165.200.0
R2(config-router)# passive-interface serial 0/1/0
R2(config-router)# end
R2# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address      Interface  Hold Uptime   SRTT  RTO  Q  Seq
                            (sec)       (ms)      Cnt Num
1   172.16.3.1     Se0/0/0   175 01:09:18   80  2340 0  16
0   192.168.10.10  Se0/0/1   11 01:09:33  1037  5000 0  17
R2#
```

Рис. 5.6.169

Команда режиму конфігурації маршрутизатора passive-interface налаштовується на інтерфейсі Serial 0/1/0 для того, щоб поновлення EIGRP маршрутизатора R2 ненадіслані на маршрутизатор ISP. Виконання команди show ip eigrp neighbors на маршрутизаторі R2 дозволяє підтвердити, що R2 не встановив відносини суміжності з ISP.

На рис. 4 показано, що в таблиці маршрутизації IPv4 маршрутизатора R1 міститься маршрут EIGRP до мережі 209.165.200.224/27 (в таблиці маршрутизації IPv4 маршрутизатора R3 теж міститься маршрут EIGRP до цієї мережі). Однак маршрутизатори R2 і ISP не пов'язані відносинами суміжності.

Проверка сети, распространяемой как маршрут EIGRP

```
R1# show ip route | include 209.165.200.224
D          209.165.200.224 [90/3651840] via 192.168.10.6,
00:06:02, Serial0/0/1
R1#
```

Рис. 5.6.170

EIGRP для IPv6

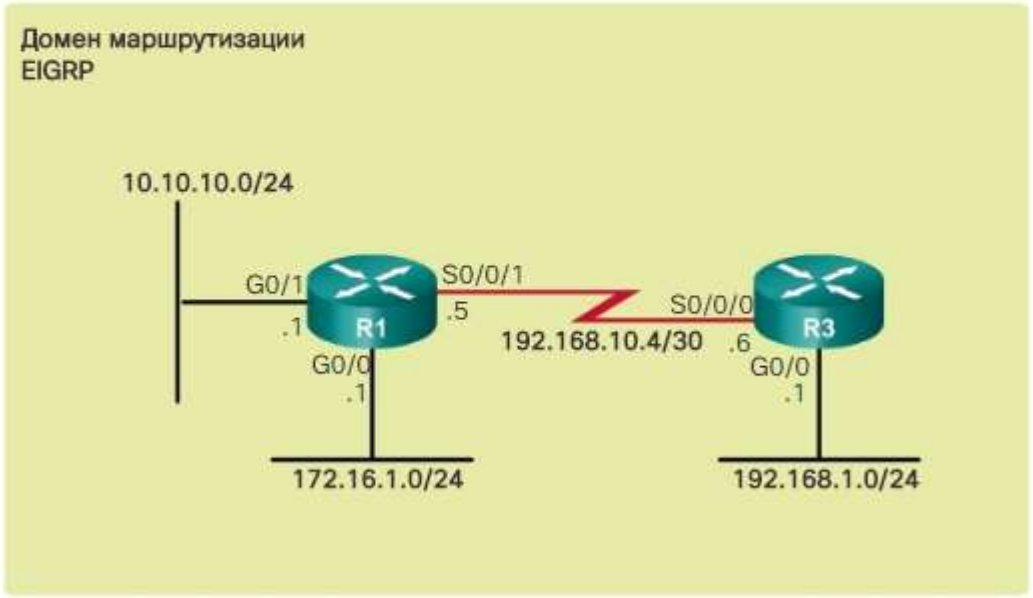
Аналогічні команди і критерії пошуку та усунення несправностей застосовуються і в EIGRP для IPv6.

Нижче наведені відповідні команди, які використовуються для EIGRP для IPv6:

- Router # show ipv6 protocols
- Router (config-rtr) # passive-interface type number

На рис. 1 показано, що тепер інтерфейс GigabitEthernet 0/1 маршрутизатора R1 налаштований з адресою 10.10.10.1/24 і включений.

EIGRP для топологии IPv4



Маршрутизатор R1 і R3 як і раніше пов'язані відносинами суміжності один з одним, але луна-тестування від маршрутизатора R3 до інтерфейсу G0 / 1 маршрутизатора R1 за адресою 10.10.10.1 пройшло невдало. На рис. 2 показано невдале тестування підключення між R3 і мережею призначення 10.10.10.0/24.

Маршрутизатор R3 не может подключиться к сети 10.10.10.0/24

```
R3# ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
R3#
```

Рис. 5.6.171

На рис. зображено, як виконання команди show ip protocols на маршрутизаторі R1 показує, що мережа 10.10.10.0/24 не оголосить сусіднім пристроїв EIGRP.

Обновления 10.10.100/24 маршрутизатора R1

```
R1# show ip protocols | begin Routing for Networks
  Routing for Networks:
    172.16.0.0
    192.168.10.0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.10.6           90      01:34:19
    172.16.3.2             90      01:34:19
  Distance: internal 90 external 170

R1#
```

Рис. 5.6.172

Як показано на рис. процес EIGRP на маршрутизатор R1 повинен включати в себе оголошення мережі 10.10.10.0/24.

Настройка сети

```
R1(config)# router eigrp 1
R1(config-router)# network 10.0.0.0
```

Рис. 5.6.173

На рис. показано, що тепер в таблиці маршрутизації R3 міститься маршрут до мережі 10.10.10.0/24, а доступ до неї перевірений за допомогою ехо-тестування інтерфейсу GigabitEthernet 0/1 маршрутизатора R1.

Проверка сети, распространяемой как маршрут EIGRP

```
R3# show ip route | include 10.10.10.0
D      10.10.10.0 [90/2172416] via 192.168.10.5, 00:04:14,
       Serial0/0/0
R3#
R3# ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent(5/5), round-trip min/avg/max =
24/27/28 ms
R3#
```

Рис. 5.6.174

Аналогічні команди і критерії пошуку та усунення несправностей застосовуються і в EIGRP для IPv6.

Нижче наведені відповідні команди, які використовуються для EIGRP для IPv6:

- Router # show ipv6 protocols
- Router # show ipv6 route
- Router (config-rtr) # network ipv6-prefix / prefix-length

Примітка. Інша форма відсутності маршруту може виникнути через те, що маршрутизатор фільтрує вхідні та вихідні відновлення маршрутизації. ACL-списки забезпечують фільтрацію по різних протоколах, і їх вплив на обмін повідомленнями протоколу маршрутизації може привести до того, що маршрути будуть відсутні в таблицях. Команда show ip protocols дозволяє побачити, застосовані чи до EIGRP будь-які списки ACL.

Автоматичне об'єднання EIGRP - це ще одна проблема, яка може ускладнити роботу мережевого адміністратора.

На рис. 1 представлена інша топологія мережі, ніж використовувалася раніше в цій главі. Між R1 і R3 немає підключення. Мережевий адреса локальної мережі маршрутизатора R1 - 10.10.10.0/24, а адреса локальної мережі R3 - 10.20.20.0/24. Обидва ці маршрутизатора підключені до R2 по послідовних каналах з пропускною спроможністю +1024 кбіт / с.

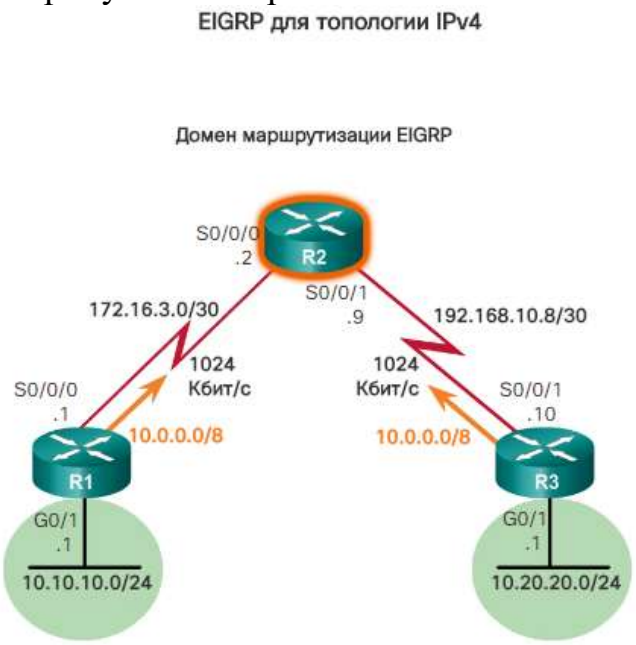


Рис. 5.6.175

Як показано на рис. локальні мережі та послідовні інтерфейси маршрутизаторів R1 і R3 налаштовані для EIGRP. Обидва маршрутизатора виконують автоматичне об'єднання EIGRP.

Настройки EIGRP для маршрутизатора R1 и R3

```
R1(config)# router eigrp 1
R1(config-router)# network 10.0.0.0
R1(config-router)# network 172.16.0.0
R1(config-router)# auto-summary
```

```
R3(config)# router eigrp 1
R3(config-router)# network 10.0.0.0
R3(config-router)# network 192.168.10.0
R3(config-router)# auto-summary
```

Рис. 5.6.176

EIGRP для IPv4 можна налаштувати на автоматичне об'єднання маршрутів на кордонах класів. За наявності не суміжних мереж автоматичне об'єднання може привести до непослідовної маршрутизації.

На рис. ми бачимо, що таблиця маршрутизації R2 не отримала індивідуальні маршрути для підмереж 10.10.10.0/24 і 10.20.20.0/24. При відправленні пакетів оновлень EIGRP на R2, маршрутизатори R1 і R3 автоматично об'єднали ці підмережі з класової кордоном 10.0.0.0/8. В результаті в таблиці маршрутизації R2 містяться два маршрути з рівною вартістю до 10.0.0.0/8, через що можуть виникнути неточності в маршрутизації і втрата пакетів. Будуть пакети пересилатися через потрібний інтерфейс чи ні, залежить від використовуваного типу розподілу (по пакетам, за призначенням або CEF).

Непоследовательная пересылка данных от R2

```
R2# show ip route
<выходные данные опущены>

      10.0.0.0/8 is subnetted, 1 subnets
D        10.0.0.0 [90/3014400] via 192.168.10.10, 00:02:06,
                   Serial0/0/1
                  [90/3014400] via 172.16.3.1, 00:02:06,
                   Serial0/0/0
```

Рис. 5.6.177

На рис. виконання команди show ip protocols дозволяє переконатися, що автоматичне об'єднання виконується як на маршрутизаторі R1, так і на R3.

Проверка состояния автоматического объединения

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"

  Automatic Summarization: enabled
    10.0.0.0/8 for Se0/0/0
      Summarizing 1 component with metric 28160

<выходные данные опущены>
```

```
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"

  Automatic Summarization: enabled
    10.0.0.0/8 for Se0/0/1
      Summarizing 1 component with metric 28160

<выходные данные опущены>
```

Рис. 5.6.178

Зверніть увагу, що обидва маршрутизатора об'єднують мережу 10.0.0.0/8 з використанням однакових метрик.

В Cisco 15 і пізніших випусках 12.2 (33) команда auto-summary відключена за замовчуванням. У старіших випусках ОС автоматичне об'єднання включено за замовчуванням. Щоб відключити автоматичне об'єднання, введіть команду no auto-summary в режимі конфігурації router EIGRP.

З метою виправлення цієї проблеми автоматичне об'єднання відключено на R1 і R3:

- R1 (config) # router eigrp 1
- R1 (config-router) # no auto-summary
- R3 (config) # router eigrp 1
- R3 (config-router) # no auto-summary

Як показано на рис. 5, після відключення автоматичного об'єднання на маршрутизаторах R1 і R3 в таблиці маршрутизації R2 зазначено, що індивідуальні підмережі 10.10.10.0/24 і 10.20.20.0/24 були отримані від маршрутизаторів R1 і R3 відповідно. Тепер точна маршрутизація і підключення до обох подсетям відновлено.

Все сети доступны с маршрутизатора R2

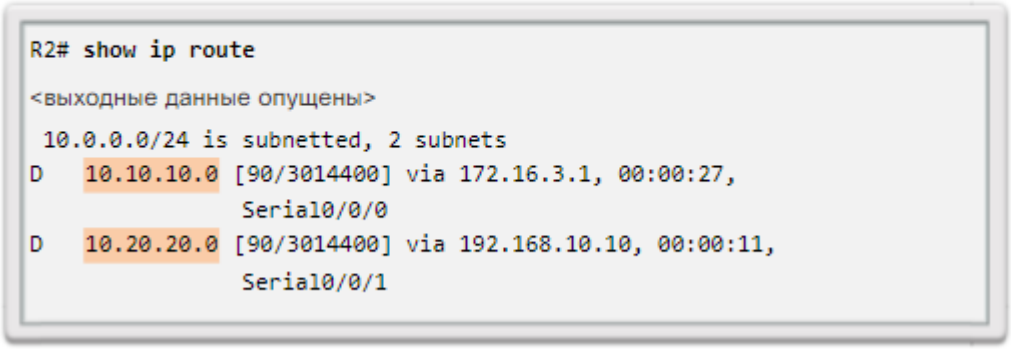


Рис. 5.6.179

EIGRP для IPv6

В IPv6 класових мереж не існує, тому EIGRP для IPv6 не підтримує автоматичне об'єднання. Об'єднання EIGRP має бути виконано вручну.

Протокол маршрутизації EIGRP досить широко використовується у великих корпоративних мережах. Мережевий інженер, який займається налаштуванням і обслуговуванням великих комутованих корпоративних мереж, що використовують EIGRP, повинен вміти налаштовувати функції EIGRP і усувати будь-які виникаючі неполадки.

Об'єднання скорочує кількість записів в оновленнях маршрутизації і локальних таблицях маршрутизації. Ця функція також зменшує використання пропускної здатності для оновлень маршрутизації, приводячи до прискорення пошуку в таблицях маршрутизації. Автоматичне об'єднання EIGRP для IPv4 за замовчуванням вимкнено, починаючи з випусків Cisco IOS 15.0 (1) M і 12.2 (33). До цього функція автоматичного об'єднання за замовчуванням була включена. Щоб увімкнути автоматичне об'єднання для EIGRP, використовуйте команду auto-summary в режимі конфігурації маршрутизатора. Для перевірки стану автоматичного об'єднання використовуйте команду show ip protocols. Перевірте таблицю маршрутизації, щоб переконатися, що автоматичне об'єднання функціонує.

Протокол EIGRP автоматично включає об'єднані маршрути в інтерфейс Null0 для запобігання петель маршрутизації, які включені в об'єднання, але не містяться в таблиці маршрутизації. Інтерфейс Null0 - це віртуальний інтерфейс IOS, тобто маршрут в нікуди, який часто називають «бітопріемніком». Пакети, відповідні маршруту з вихідним інтерфейсом Null0, відкидаються.

Щоб налаштувати об'єднання EIGRP вручну на конкретному інтерфейсі EIGRP, використовуйте наступну команду режиму конфігурації інтерфейсу:

Router (config-if) # ip summary-address eigrp as-number network-address subnet-mask

Щоб налаштувати об'єднання EIGRP вручну для IPv6 на конкретному інтерфейсі EIGRP, використовуйте наступну команду режиму конфігурації інтерфейсу:

Router (config-if) # ipv6 summary-address eigrp as-number prefix / prefix-length

Поширити статичний маршрут за замовчуванням в домені маршрутизації EIGRP можна за допомогою команди redistribute static. Завдяки цій команді EIGRP включає даний статичний маршрут в свої поновлення EIGRP, що відправляються на інші маршрутизатори. Виконання команди show ip protocols дозволяє переконатися, що статичні маршрути в домені маршрутизації EIGRP піддаються перерозподілу.

Використовуйте команду ip bandwidth-percent eigrp as-number percent в режимі конфігурації інтерфейсу для налаштування відсотка пропускної здатності, який буде використовуватися протоколом EIGRP на інтерфейсі.

Щоб встановити необхідний відсоток співвідношення пропускної спроможності, яка може використовуватися EIGRP для IPv6 на інтерфейсі, використовуйте команду ipv6 bandwidth-percent eigrp в режимі конфігурації інтерфейсу. Для відновлення значення за замовчуванням використовуйте версію no цієї команди.

Інтервали вітання та очікування налаштовуються на інтерфейсах окремо і не повинні збігатися з інтервалами іншихмаршрутизаторів EIGRP при встановленні або підтримці відносин суміжності.

Для IP в Cisco IOS застосовується розподіл навантаження з використанням до чотирьох шляхів з рівною вартістю за замовчуванням. Завдяки команді режиму конфігурації маршрутизатора maximum-paths таблиця маршрутизації може містити до 32 маршрутів з рівною вартістю.

EIGRP підтримує аутентифікацію протоколу маршрутизації за допомогою MD5. Алгоритми і конфігурація для аутентифікації EIGRP для повідомлень IPv4 мало чим відрізняється від IPv6. Єдина відмінність полягає в тому, що в командах режиму конфігурації використовується ip, а не ipv6.

Router (config-if) # ipv6 authentication mode eigrp as-number md5

Router (config-if) # ipv6 authentication key-chain eigrp as-number name-of-chain

Для перевірки відносин суміжності EIGRP після настройки аутентифікації використовуйте для кожного маршрутизатора команду show ip eigrp neighbors.

Команда show ip protocols використовується для того, щоб переконатися, що маршрутизатор отримав відомості про маршрутах EIGRP. Команда show ip protocols використовується для того, щоб переконатися, що EIGRP відображає значення, налаштовані на даний момент.

Список рекомендованої літератури

1. Буров Є. Комп’ютерні мережі. 2 - ге оновлене і доповн. вид. – Львів: БаК, 2003. – 584 с.
2. Буров Є.В. Комп’ютерні мережі: Підручник. – Львів: “Магнолія плюс”, 2006. – 264 с.
3. Галкин В.А., Григорьев Ю.А. Телекоммуникации и сети: Учеб. пособие для вузов. –М.: Изд-во МГТУ имени Н.Э. Баумана, 2003. –608 с.
4. Гук М. Аппаратные средства локальных сетей. Энциклопедия. – СПб.: Питер, 2002. –573 с.
5. Дж. Бони. Руководство по Cisco IOS. –СПб.: Питер; М.: Издательство «Русская Редакция», 2008. —784 с.
6. Димарцио Д. Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. / пер. с англ. –СПб: Символ-Плюс, 2003. –512 с.
7. Досталек Л., Кабелова А. TCP/IP и DNS в теории и на практике. Полное руководство / Пер. с чеш. Рус. изд. под ред. М.В. Финкова и А.В. Анисимова.
8. Серия «Полное руководство». –СПб.: Наука и Техника, 2006. –608 с.
9. Кларк, Кеннеди, Гамильтон, Кевин. Принципы коммутации в локальних сетях Cisco. Пер. с англ. –М.: Издательский дом «Вильямс», 2003. –976 с.
10. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі. Підручник / За ред. Ю.С. Ковтанюка. –К.: Юніор, 2003. –400 с.
11. Леинванд Аллан, Пински Брюс. Конфигурирование маршрутизаторов Cisco, 2-е изд. : Пер. с англ. -М.: Издательский дом «Вильямс», 2001. –368 с.
12. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. –СПб.: Питер, 2001. –672 с.
13. Олифер В.Г., Олифер Н.А. Компьютерные сети.Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. –СПб.: Питер, 2005. –958 с.
14. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. –4-е изд. –СПб.: Питер, 2012. –944 с.
15. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. –СПб.: Питер, 2002. –544 с.
16. Олифер В.Г., Олифер Н.А. Сетевые операционные системы: Учебник для вузов. 2-е изд. –СПб.: Питер, 2007. –672 с.
17. Паркер Т., Сиян К. TCP/IP. Для профессионалов. 3 - е изд. – СПб.: Питер, 2004. – 859 с.
18. Росляков А.В. Сети доступа. Учебное пособие для вузов. –М.: Горячая линия Телеком, 2008. –96 с.
19. Таненбаум Э. Компьютерные сети. 4-е изд. –СПб.: Питер, 2003. –848 с.
20. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1. – 2-е изд. / пер. с англ. – М.:
21. ООО «И.Д. Вильямс», 2011. –572 с.
22. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2. –2-е изд. / пер. с англ. –М.: ООО «И.Д. Вильямс», 2011. –736 с.

23. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822. –3-е изд. / пер. с англ. –
24. М.: ООО «И.Д. Вильямс», 2013. –720 с.
25. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 640-816. – 3-е изд. / пер. с англ. – М.: ООО «И.Д. Вильямс», 2013. –752 с.
26. Филимонов А.Ю. Построение мультисервисных сетей Ethernet. –СПб.: БХВПетербург, 2007. –592 с.
27. Хабракен Д. Как работать с маршрутизаторами Cisco. Пер. с англ. – М.:ДМК-Пресс, 2005. –320 с.
28. Хьюкаби Дэвид, Мак - Квери Стив. Руководство Cisco по конфигурированию комм у т а-торов Catalyst. : Пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 560 с.
29. Дэвид Хьюкаби, Стив Мак-Квери, Эндрю Уайтейкер. Маршрутизаторы Cisco. Руководство по конфигурированию. 2-е изд. / пер. с англ. – М.: ООО «И.Д. Вильямс», 2012. –736 с.
30. Амато, Вито. Основы организации сетей Cisco, том 1, испр. изд.: Пер. с англ. –М.: Издательский дом «Вильямс», 2004. –512 с.
31. Амато, Вито. Основы организации сетей Cisco, том 2, испр. изд.: Пер. с англ. –М.: Издательский дом «Вильямс», 2004. –464 с.
32. Буассо и др. Введение в технологию ATM: Пер. с англ. / М. Буассо, М. Деманж, Ж.–М. Мюнье. Под ред. В.О. Шварцмана. –М.: Радио и связь, 1997. –128 с.
33. Шиндер,Дебра, Литтлджон. Основы компьютерных сетей: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. –656 с.
34. Куин Ляем, Рассел Ричард. Fast Ethernet. – К.: Издательская группа BHV, 1998. – 448 с.
35. Назаров С.В. Администрирование локальных сетей Windows NT/ 20 00/.NET: Учеб. п о-собие. – 2 - е изд., перераб. и доп. – М.: Финансы и статистика, 2003. – 480 с.
36. Хилл, Брайан. Полный справочник по Cisco. Пер. с англ. –М.: Издательский дом «Вильямс», 2006. –1088 с.
37. Спортак Марк и др. Компьютерные сети. Книга 1. High-perf ormance Networking. Энциклопедия пользователя. –К.: Изд-во “ДиаСофт”, 1998. – 432 с.
38. Спортак Марк и др. Компьютерные сети. Книга 2. Networking Essentials. Энциклопедия пользователя. –К.: Изд-во “ДиаСофт”, 1999. – 432 с.
39. Найк Дилип. Стандарты и протоколы Интернета /Пер с англ. –М.: Издатель-ский отдел «Русская редакция» ТОО «Channel Trading Ltd.», 1999. –384 с.
40. Сидни Фейт. TCP/IP: Архитектура, протоколы, реализация (включая IP вер-сии 6 и IP Security), 2-е издание. –М.: Издательство «ЛОРИ», 2000. – 424 с.
41. Комп’ютерні мережі: Методичні рекомендації для підготовки та проведення практичних, лабораторних занять і самостійної роботи

студентів. Частина 1. Підг. А.А. Єфіменко. –Житомир: ЖВІ НАУ, 2008. – 80 с.
42. Інформаційно-комунікаційні системи: методичні рекомендації для підготовки та проведення практичних і лабораторних занять. підг. А.А. Єфіменко. –Жи-томир: ЖВІ НАУ, 2012. –100 с.
43. ABRAMSON, N.: “Internet Access Using VSATs,” IEEE Commun. Magazine, vol. 38, pp. 60–68,July 2000.
44. AHMADI, S.: ‘‘An Overview of Next-Generation Mobile WiMAX Technology,’’ IEEE Commun.Magazine, vol. 47, pp. 84–88, June 2009.
45. ALLMAN, M., and PAXSON, V.: ‘‘On Estimating End-to-End Network Path Properties,’’ Proc.SIGCOMM ’99 Conf., ACM, pp. 263–274, 1999.
46. ANDERSON, C.: The Long Tail: Why the Future of Business is Selling Less of More, rev. upd. ed.,New York: Hyperion, 2008a.
47. ANDERSON, R.J.: Security Engineering: A Guide to Building Dependable Distributed Systems, 2nded., New York: John Wiley & Sons, 2008b.
48. ANDERSON, R.J.: “Free Speech Online and Office,” Computer, vol. 25, pp. 28–30, June 2002.
49. ANDERSON, R.J.: ‘‘The Eternity Service,’’ Proc. Pragocrypt Conf., CTU Publishing House, pp.242–252, 1996.
50. ANDREWS, J., GHOSH, A., and MUHAMED, R.: Fundamentals of WiMAX: Understanding Broadband Wireless Networking, Upper Saddle River, NJ: Pearson Education, 2007.
51. ASTELY, D., DAHLMAN, E., FURUSKAR, A., JADING, Y., LINDSTROM, M., and PARKVALL, S.: ‘‘LTE: The Evolution of Mobile Broadband,’’ IEEE Commun. Magazine, vol. 47, pp. 44–51, Apr. 2009.
52. BALLARDIE, T., FRANCIS, P., and CROWCROFT, J.: “Core Based Trees (CBT),” Proc. SIGCOMM‘ 93 Conf., ACM, pp. 85-95, 1993.
53. BARAN, P.: ‘‘On Distributed Communications: I. Introduction to Distributed CommunicationNetworks,’’ Memorandum RM-420-PR, Rand Corporation, Aug. 1964.
54. BELLAMY, J.: Digital Telephony, 3rd ed., New Ytfrk: Wiley, 2000.
55. BELLMAN, R.E.: Dynamic Programming, Princeton, NJ: Princeton University Press, 1957.
56. BELLOVIN, S.: ‘‘The Security Flag in the IPv4 Header,’’ RFC 3514, Apr. 2003.
57. BELSNES, D.: “Flow Control in the Packet Switching Networks,” Communications Networks, Uxbridge, England: Online, pp. 349–361, 1975.
58. BENNET, C.H., and BRASSARD, G.: “Quantum Cryptography: Public Key Distribution and Coin Tossing,” Int’l Conf. on Computer Systems and Signal Processing, pp. 175–179, 1984.
59. BERESFORD, A., and STAJANO, F.: ‘‘Location Privacy in Pervasive Computing,’’ IEEE Pervasive Computing, vol. 2, pp. 46–55, Jan. 2003.
60. BERGHEL, H.L.: “Cyber Privacy in the New Millennium,” Computer, vol. 34, pp. 132–134, Jan. 2001.

61. BERNERS-LEE, T., CAILLIAU, A., LOUTONEN, A., NIELSEN, H.F., and SECRET, A.: “The World Wide Web,” Commun. of the ACM, vol. 37, pp. 76–82, Aug. 1994.
62. BERTSEKAS, D., and GALLAGER, R.: Data Networks, 2nd ed., Englewood Cliffs, NJ: Prentice Hall, 1992.
63. BHATTI, S.N., and CROWCROFT, J.: “QoS Sensitive Flows: Issues in IP Packet Handling,” IEEE Internet Computing, vol. 4, pp. 48–57, July–Aug. 2000.
64. BIHAM, E., and SHAMIR, A.: “Differential Cryptanalysis of the Data Encryption Standard,” Proc. 17th Ann. Int’l Cryptology Conf., Berlin: Springer-Verlag LNCS 1294, pp. 513–525, 1997.
65. BIRD, R., GOPAL, I., HERZBERG, A., JANSON, P.A., KUTTEN, S., MOLVA, R., and YUNG, M.: “Systematic Design of a Family of Attack-Resistant Authentication Protocols,” IEEE J. on Selected Areas in Commun., vol. 11, pp. 679–693, June 1993.
66. BIRRELL, A.D., and NELSON, B.J.: “Implementing Remote Procedure Calls,” ACM Trans, on Computer Systems, vol. 2, pp. 39–59, Feb. 1984.
67. BIRYUKOV, A., SHAMIR, A., and WAGNER, D.: “Real Time Cryptanalysis of A5/1 on a PC,” Proc. Seventh Int’l Workshop on Fast Software Encryption, Berlin: Springer-Verlag LNCS 1978, p. 1, 2000.
68. BLAZE, M., and BELLOVIN, S.: “Tapping on My Network Door,” Commun. of the ACM, vol. 43, p. 136, Oct. 2000.936
69. BOGGS, D., MOGUL, J., and KENT, C.: ‘‘Measured Capacity of an Ethernet: Myths and Reality,’’ Proc. SIGCOMM ’88 Conf., ACM, pp. 222–234, 1988.
70. BORISOV, N., GOLDBERG, I., and WAGNER, D.: “Intercepting Mobile Communications: The Insecurity of 802.11,” Seventh Int’l Conf. on Mobile Computing and Networking, ACM, pp. 180–188, 2001.
71. BRADEN, R.: ‘‘Requirements for Internet Hosts—Communication Layers,’’ RFC 1122, Oct. 1989.
72. BRADEN, R., BORMAN, D., and PARTRIDGE, C.: ‘‘Computing the Internet Checksum,’’ RFC 1071, Sept. 1988.
73. BRANDENBURG, K.: ‘‘MP3 and AAC Explained,’’ Proc. 17th Intl. Conf.: High-Quality Audio Coding, Audio Engineering Society, pp. 99–110, Aug. 1999.
74. BRAY, T., PAOLI, J., SPERBERG-MCQUEEN, C., MALER, E., YERGEAU, F., and COWAN, J.: ‘‘Extensible Markup Language (XML) 1.1 (Second Edition),’’ W3C Recommendation, Sept. 2006.
75. BRESLAU, L., CAO, P., FAN, L., PHILLIPS, G., and SHENKER, S.: ‘‘Web Caching and Zipf-like Distributions: Evidence and Implications,’’ Proc. INFOCOM Conf., IEEE, pp. 126–134, 1999.
76. BURLEIGH, S., HOOKE, A., TORGERSON, L., FALL, K., CERF, V., DURST, B., SCOTT, K., and WEISS, H.: ‘‘Delay-Tolerant Networking: An Approach to Interplanetary Internet,’’ IEEE Commun. Magazine, vol. 41, pp. 128–136, June 2003.
77. BURNETT, S., and PAINE, S.: RSA Security’s Official Guide to Cryptography, Berkeley, CA: Osborne/McGraw-Hill, 2001.
78. BUSH, V.: ‘‘As We May Think,’’ Atlantic Monthly, vol. 176, pp. 101–108, July 1945.

79. CAPETANAKIS, J.I.: “Tree Algorithms for Packet Broadcast Channels,” IEEE Trans, on Information Theory, vol. IT-25, pp. 505–515, Sept. 1979.
80. CASTAGNOLI, G., BRAUER, S., and HERRMANN, M.: ‘‘Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits,’’ IEEE Trans. on Commun., vol. 41, pp. 883–892, June 1993.
81. CERF, V., and KAHN, R.: “A Protocol for Packet Network Interconnection,” IEEE Trans, on Commun., vol. COM-22, pp. 637–648, Way 1974.
82. CHANG, F., DEAN, J., GHEMAWAT, S., HSIEH, W., WALLACH, D., BURROWS, M., CHANDRA,
83. T., FIKES, A., and GRUBER, R.: ‘‘Bigtable: A Distributed Storage System for Structured Data,’’ Proc. OSDI 2006 Symp., USENIX, pp. 15–29, 2006.
84. CHASE, J.S., GALLATIN, A.J., and YOCUM, K.G.: “End System Optimizations for High-Speed TCP,” IEEE Commun. Magazine, vol. 39, pp. 68–75, April 2001.
85. CHEN, S., and NAHRSTEDT, K.: ‘‘An Overview of QoS Routing for Next-Generation Networks,’’ IEEE Network Magazine, vol. 12, pp. 64–69, Nov./Dec. 1998.
86. CHIU, D., and JAIN, R.: ‘‘Analysis of the Increase and Decrease Algorithms for Congestion Avoidance in Computer Networks,’’ Comput. Netw. ISDN Syst., vol. 17, pp. 1–4, June 1989.
87. CISCO: ‘‘Cisco Visual Networking Index: Forecast and Methodology, 2009–2014,’’ Cisco Systems Inc., June 2010.
88. CLARK, D.D.: “The Design Philosophy of the DARPA Internet Protocols,” Proc. SIGCOMM ’88 Conf., ACM, pp. 106–114, 1988.
89. CLARK, D.D.: “Window and Acknowledgement Strategy in TCP,” RFC 813, July 1982.
90. CLARK, D.D., JACOBSON, V., ROMKEY, J., and SAL WEN, H.: “An Analysis of TCP Processing Overhead,” IEEE Commun. Magazine, vol. 27, pp. 23–29, June 1989.
91. CLARK, D.D., SHENKER, S., and ZHANG, L.: ‘‘Supporting Real-Time Applications in an Integrated Services Packet Network,’’ Proc. SIGCOMM ’92 Conf., ACM, pp. 14–26, 1992.
92. CLARKE, A.C.: “Extra-Terrestrial Relays,” Wireless World, 1945.
93. CLARKE, I., MILLER, S.G., HONG, T.W., SANDBERG, O., and WILEY, B.: “Protecting Free Expression
94. Online with Freenet,” IEEE Internet Computing, vol. 6, pp. 40–49, Jan.-Feb. 2002.
95. COHEN, B.: ‘‘Incentives Build Robustness in BitTorrent,’’ Proc. First Workshop on Economics of Peer-to-Peer Systems, June 2003.
96. COMER, D.E.: The Internet Book, 4th ed., Englewood Cliffs, NJ: Prentice Hall, 2007.
97. COMER, D.E.: Internetworking with TCP/IP, vol. 1, 5th ed., Englewood Cliffs, NJ: Prentice Hall, 2005.
98. CRAVER, S.A., WU, M., LIU, B., STUBBLEFIELD, A., SWARTZLANDER, B., WALLACH, D.W., DEAN, D., and FELTEN, E.W.: “Reading Between the Lines: Lessons from the SDMI Challenge,” Proc. 10th USENIX Security Symp., USENIX, 2001.

99. CROVELLA, M., and KRISHNAMURTHY, B.: Internet Measurement, New York: John Wiley & Sons, 2006.
100. DAEMEN, J., and RIJMEN, V.: The Design of Rijndael, Berlin: Springer-Verlag, 2002.
101. DALAL, Y., and METCLFE, R.: ‘‘Reverse Path Forwarding of Broadcast Packets,’’ Commun. of the ACM, vol. 21, pp. 1040–1048, Dec. 1978.
102. DAVIE, B., and FARREL, A.: MPLS: Next Steps, San Francisco: Morgan Kaufmann, 2008.
103. DAVIE, B., and REKHTER, Y.: MPLS Technology and Applications, San Francisco: Morgan Kaufmann, 2000.
104. DAVIES, J.: Understanding IPv6, 2nd ed., Redmond, WA: Microsoft Press, 2008.
105. DAY, J.D.: “The (Un)Revised OSI Reference Model,” Computer Commun. Rev., vol. 25, pp. 39-55, Oct. 1995.
106. DAY, J.D., and ZIMMERMANN, H.: “The OSI Reference Model,” Proc. of the IEEE, vol. 71, pp. 1334–1340, Dec. 1983.
107. DECANDIA, G., HASTORIN, D., JAMPANI, M., KAKULAPATI, G., LAKSHMAN, A., PILCHIN, A., SIVASUBRAMANIAN, S., VOSSHALL, P., and VOGELS, W.: ‘‘Dynamo: Amazon’s Highly Available Key-value Store,’’ Proc. 19th Symp. on Operating Systems Prin., ACM, pp. 205–220, Dec. 2007.
108. DEERING, S.E.: “SIP: Simple Internet Protocol,” IEEE Network Magazine, vol. 7, pp. 16-28, May/June 1993.
109. DEERING, S., and CHERITON, D.: ‘‘Multicast Routing in Datagram Networks and Extended LANs,’’ ACM Trans. on Computer Systems, vol. 8, pp. 85–110, May 1990.
110. DEMERS, A., KESHAV, S., and SHENKER, S.: “Analysis and Simulation of a Fair Queue-ing Algorithm,” Internetwork: Research and Experience, vol. 1, pp. 3–26, Sept. 1990.
111. DENNING, D.E., and SACCO, G.M.: “Timestamps in Key Distribution Protocols,” Commun. of the ACM, vol. 24, pp. 533–536, Aug. 1981.
112. DEVARAPALLI, V., WAKIKAWA, R., PETRESCU, A., and THUBERT, P.: ‘‘Network Mobility (NEMO) Basic Support Protocol,’’ RFC 3963, Jan. 2005.
113. DIFFIE, W., and HELLMAN, M.E.: ‘‘Exhaustive Cryptanalysis of the NBS Data Encryption Standard,’’ IEEE Computer, vol. 10, pp. 74–84, June 1977.
114. DIFFIE, W., and HELLMAN, M.E.: “New Directions in Cryptography,” IEEE Trans, on Information Theory, vol. IT-2, pp. 644–654, Nov. 1976.
115. DIJKSTRA, E.W.: “A Note on Two Problems in Connexion with Graphs,” Numer. Math., vol. 1, pp. 269–271, Oct. 1959.
116. DILLEY, J., MAGGS, B., PARIKH, J., PROKOP, H., SITARAMAN, R., and WHEIL, B.: ‘‘Globally Distributed Content Delivery,’’ IEEE Internet Computing, vol. 6, pp. 50–58, 2002.
117. DINGLEDINE, R., MATHEWSON, N., SYVERSON, P.: ‘‘Tor: The Second-Generation Onion Router,’’ Proc. 13th USENIX Security Symp., USENIX, pp. 303–320, Aug. 2004.
118. DONAHOO, M., and CALVERT, K.: TCP/IP Sockets in C, 2nd ed., San Francisco: Morgan Kaufmann, 2009.

119. DONAHOO, M., and CALVERT, K.: TCP/IP Sockets in Java, 2nd ed., San Francisco: Morgan Kaufmann, 2008.
120. DONALDSON, G., and JONES, D.: “Cable Television Broadband Network Architectures,” IEEE Commun. Magazine, vol. 39, pp. 122–126, June 2001.
121. DORFMAN, R.: “Detection of Defective Members of a Large Population,” Annals Math. Statistics, vol. 14, pp. 436–440, 1943.
122. DUTCHER, B.: The NAT Handbook, New York: John Wiley&Sons, 2001.938
123. DUTTA-ROY, A.: “An Overview of Cable Modem Technology and Market Perspectives,” IEEE Commun. Magazine, vol. 39, pp. 81–88, June 2001.
124. EDELMAN, B., OSTROVSKY, M., and SCHWARZ, M.: ‘‘Internet Advertising and the Generalized Second-Price Auction: Selling Billions of Dollars Worth of Keywords,’’ American Economic Review, vol. 97, pp. 242–259, Mar. 2007.
125. EL GAMAL, T.: “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” IEEE Trans, on Information Theory, vol. IT-1, pp. 469–472, July 1985.
126. EPCGLOBAL: EPC Radio-Frequency Identity Protocols Class– Generation–UHF RFID Protocol for Communication at 860-MHz to 960-MHz Version 1.2.0, Brussels: EPCglobal Inc., Oct. 2008.
127. FALL, K.: ‘‘A Delay-Tolerant Network Architecture for Challenged Internets,’’ Proc. SIGCOMM 2003 Conf., ACM, pp. 27–34, Aug. 2003.
128. FALOUTSOS, M., FALOUTSOS, P., and FALOUTSOS, C.: ‘‘On Power-Law Relationships of the Internet Topology,’’ Proc. SIGCOMM ’99 Conf., ACM, pp. 251–262, 1999.
129. FARRELL, S., and CAHILL, V.: Delay- and Disruption-Tolerant Networking, London: Artech House, 2007.
130. FELLOWS, D., and JONES, D.: ‘‘DOCSIS Cable Modem Technology,’’ IEEE Commun. Magazine, vol. 39, pp. 202–209, Mar. 2001.
131. FENNER, B., HANDLEY, M., HOLBROOK, H., and KOUVELAS, I.: ‘‘Protocol Independent MulticastSparse Mode (PIM-SM),’’ RFC 4601, Aug. 2006.
132. FERGUSON, N., SCHNEIER, B., and KOHNO, T.: Cryptography Engineering: Design Principles and Practical Applications, New York: John Wiley & Sons, 2010.
133. FLANAGAN, D.: JavaScript: The Definitive Guide, 6th ed., Sebastopol, CA: O’Reilly, 2010.
134. FLETCHER, J.: ‘‘An Arithmetic Checksum for Serial Transmissions,’’ IEEE Trans. on Commun., vol. COM–0, pp. 247–252, Jan. 1982.
135. FLOYD, S., HANDLEY, M., PADHYE, J., and WIDMER, J.: ‘‘Equation-Based Congestion Control for Unicast Applications,’’ Proc. SIGCOMM 2000 Conf., ACM, pp. 43–56, Aug. 2000.
136. FLOYD, S., and JACOBSON, V.: “Random Early Detection for Congestion Avoidance,” IEEE/ACM Trans, on Networking, vol. 1, pp. 397–413, Aug. 1993.
137. FLUHRER, S., MANTIN, I., and SHAMIR, A.: ‘‘Weakness in the Key Scheduling Algorithm of RC4,’’ Proc. Eighth Ann. Workshop on Selected Areas in Cryptography, Berlin: Springer-Verlag LNCS 2259, pp. 1–24, 2001.

138. FORD, B.: ‘‘Structured Streams: A New Transport Abstraction,’’ Proc. SIGCOMM 2007 Conf., ACM, pp. 361–372, 2007.
139. FORD, L.R., Jr., and FULKERSON, D.R.: Flows in Networks, Princeton, NJ: Princeton University Press, 1962.
140. FORD, W., and BAUM, M.S.: Secure Electronic Commerce, Upper Saddle River, NJ: Prentice Hall, 2000.
141. FOULI, K., and MALER, M.: ‘‘The Road to Carrier-Grade Ethernet,’’ IEEE Commun.
142. Magazine, vol. 47, pp. S30–S38, Mar. 2009.
143. FOX, A., GRIBBLE, S., BREWER, E., and AMIR, E.: ‘‘Adapting to Network and Client Variability via On-Demand Dynamic Distillation,’’ SIGOPS Oper. Syst. Rev., vol. 30, pp. 160–170, Dec. 1996.
144. FRANCIS, P.: “A Near-Term Architecture for Deploying Pip,” IEEE Network Magazine, vol. 7, pp. 30–37, May/June 1993.
145. FRASER, A.G.: ‘‘Towards a Universal Data Transport System,’’ IEEE J. on Selected Areas in Commun., vol. 5, pp. 803–816, Nov. 1983.
146. FRIDRICH, J.: Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge: Cambridge University Press, 2009.
147. FULLER, V., and LI, T.: ‘‘Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan,’’ RFC 4632, Aug. 2006.9.2. Алфавитный список литературы 939
148. GALLAGHER, R.G.: ‘‘A Minimum Delay Routing Algorithm Using Distributed Computation,’’ IEEE Trans. on Commun., vol. COM–5, pp. 73–85, Jan. 1977.
149. GALLAGHER, R.G.: ‘‘Low-Density Parity Check Codes,’’ IRE Trans. on Information Theory, vol. 8, pp. 21–28, Jan. 1962.
150. GARFINKEL, S., with SPAFFORD, G.: Web Security, Privacy, and Commerce, Sebastopol, CA: O’Reilly, 2002.
151. GAST, M.: 802.11 Wireless Networks: The Definitive Guide, 2nd ed., Sebastopol, CA: O’Reilly, 2005.
152. GERSHENFELD, N., and KRIKORIAN, R., and COHEN, D.: ‘‘The Internet of Things,’’ Scientific American, vol. 291, pp. 76–81, Oct. 2004.
153. GILDER, G.: ‘‘Metcalfe’s Law and Legacy,’’ Forbes ASAP, Sepy. 13, 1993.
154. GOODE, B.: ‘‘Voice over Internet Protocol,’’ Proc. of the IEEE, vol. 90, pp. 1495–1517, Sept. 2002.
155. GORALSKI, W.J.: SONET, 2nd ed., New York: McGraw-Hill, 2002.
156. GRAYSON, M., SHATZKAMER, K., and WAINNER, S.: IP Design for Mobile Networks, Indianapolis, IN: Cisco Press, 2009.
157. GROBE, K., and ELBERS, J.: ‘‘PON in Adolescence: From TDMA to WDM-PON,’’ IEEE Commun. Magazine, vol. 46, pp. 26–34, Jan. 2008.
158. GROSS, G., KAYCEE, M., LIN, A., MALIS, A., and STEPHENS, J.: ‘‘The PPP Over AAL5,’’ RFC 2364, July 1998.
159. HA, S., RHEE, I., and LISONG, X.: ‘‘CUBIC: A New TCP-Friendly High-Speed TCP Variant,’’ SIGOPS Oper. Syst. Rev., vol. 42, pp. 64–74, June 2008.
160. HAFNER, K., and LYON, M.: Where Wizards Stay Up Late, New York: Simon & Schuster, 1998.

161. HALPERIN, D., HEYDT-BENJAMIN, T., RANSFORD, B., CLARK, S., DEFEND, B., MORGAN, W., FU, K., KOHNO, T., and MAISEL, W.: ‘‘Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses,’’ IEEE Symp. on Security and Privacy, pp. 129–142, May 2008.
162. HALPERIN, D., HU, W., SHETH, A., and WETHERALL, D.: ‘‘802.11 with Multiple Antennas for Dummies,’’ Computer Commun. Rev., vol. 40, pp. 19–25, Jan. 2010.
163. HAMMING, R.W.: “Error Detecting and Error Correcting Codes,” Bell System Tech. J., vol. 29, pp. 147–160, April 1950.
164. HARTE, L., KELLOGG, S., DREHER, R., and SCHAFFNIT, T.: The Comprehensive Guide to Wireless Technology, Fuquay-Varina, NC: APDG Publishing, 2000.
165. HAWLEY, G.T.: “Historical Perspectives on the U.S. Telephone Loop,” IEEE Commun. Magazine, vol. 29, pp. 24–28, March 1991.
166. HECHT, J.: “Understanding Fiber Optics,” Upper Saddle River, NJ: Prentice Hall, 2005.
167. HELD, G.: A Practical Guide to Content Delivery Networks, 2nd ed., Boca Raton, FL: CRC Press, 2010.
168. HEUSSE, M., ROUSSEAU, F., BERGER-SABBATEL, G., DUDA, A.: ‘‘Performance Anomaly of 802.11b,’’ Proc. INFOCOM Conf., IEEE, pp. 836–843, 2003.
169. HIERTZ, G., DENTENEER, D., STIBOR, L., ZANG, Y., COSTA, X., and WALKE, B.: ‘‘The IEEE 802.11 Universe,’’ IEEE Commun. Magazine, vol. 48, pp. 62–70, Jan. 2010.
170. HOE, J.: ‘‘Improving the Start-up Behavior of a Congestion Control Scheme for TCP,’’ Proc. SIGCOMM ’96 Conf., ACM, pp. 270–280, 1996.
171. HU, Y., and LI, V.O.K.:‘‘Satellite-Based Internet: A Tutorial,’’ IEEE Commun. Magazine, vol. 30, pp. 154–162, Mar. 2001.
172. HUITEMA, C.: Routing in the Internet, 2nd ed., Englewood Cliffs, NJ: Prentice Hall, 1999.
173. HULL, B., BYCHKOVSKY, V., CHEN, K., GORACZKO, M., MIU, A., SHIH, E., ZHANG, Y., BALAKRISHNAN, H., and MADDEN, S.: ‘‘CarTel: A Distributed Mobile Sensor Computing System,’’ Proc. Sensys 2006 Conf., ACM, pp. 125–138, Nov. 2006.
174. HUNTER, D., RAFTER, J., FAWCETT, J., VAN DER LIST, E., AYERS, D., DUCKETT, J., WATT, A., and MCKINNON, L.: Beginning XML, 4th ed., New Jersey: Wrox, 2007.940
175. IRMER, T.: “Shaping Future Telecommunications: The Challenge of Global Standardization,” IEEE Commun. Magazine, vol. 32, pp. 20–28, Jan. 1994.
176. ITU (INTERNATIONAL TELECOMMUNICATION UNION): ITU Internet Reports 2005: The Internet of Things, Geneva: ITU, Nov. 2005.
177. ITU (INTERNATIONAL TELECOMMUNICATION UNION): Measuring the Information Society: The ICT Development Index, Geneva: ITU, Mar. 2009.
178. JACOBSON, V.: ‘‘Compressing TCP/IP Headers for Low-Speed Serial Links,’’ RFC 1144, Feb. 1990.

179. JACOBSON, V.: “Congestion Avoidance and Control,” Proc. SIGCOMM ‘88 Conf., ACM, pp. 314–329, 1988.
180. JAIN, R., and ROUTHIER, S.: ‘‘Packet Trains—Measurements and a New Model for Computer Network Traffic,’’ IEEE J. on Selected Areas in Commun., vol. 6, pp. 986–995, Sept. 1986.
181. JAKOBSSON, M., and WETZEL, S.: “Security Weaknesses in Bluetooth,” Topics in Cryp-tology: CTRSA 2001, Berlin: Springer-Verlag LNCS 2020, pp. 176–191, 2001.
182. JOEL, A.: “Telecommunications and the IEEE Communications Society,” IEEE Commun. Magazine, 50th Anniversary Issue, pp. 6-14 and 162–167, May 2002.
183. JOHNSON, D., PERKINS, C., and ARKKO, J.: ‘‘Mobility Support in IPv6,’’ RFC 3775, June 2004.
184. JOHNSON, D.B., MALTZ, D., and BROCH, J.: ‘‘DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks,’’ Ad Hoc Networking, Boston: Addison-Wesley, pp. 139–172, 2001.
185. JUANG, P., OKI, H., WANG, Y., MARTONOSI, M., PEH, L., and RUBENSTEIN, D.: ‘‘Energy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet,’’ SIGOPS Oper. Syst. Rev., vol. 36, pp. 96–107, Oct. 2002.
186. KAHN, D.: The Codebreakers, 2nd ed., New York: Macmillan, 1995.
187. KAMOUN, F., and KLEINROCK, L.: “Stochastic Performance Evaluation of Hierarchical Routing for Large Networks,” Computer Networks, vol. 3, pp. 337–353, Nov. 1979.
188. KARN, P.: “MACA—A New Channel Access Protocol for Packet Radio,” ARRL/CRRL Amateur Radio Ninth Computer Networking Conf., pp. 134–140, 1990.
189. KARN, P., and PARTRIDGE, C.: ‘‘Improving Round-Trip Estimates in Reliable Transport Protocols,’’ Proc. SIGCOMM ’87 Conf., ACM, pp. 2–7, 1987.
190. KARP, B., and KUNG, H.T.: ‘‘GPSR: Greedy Perimeter Stateless Routing for Wireless Networks,’’ Proc. MOBICOM 2000 Conf., ACM, pp. 243–254, 2000.
191. KASIM, A.: Delivering Carrier Ethernet, New York: McGraw-Hill, 2007.
192. KATABI, D., HANDLEY, M., and ROHRS, C.: ‘‘Internet Congestion Control for Future High Bandwidth-Delay Product Environments,’’ Proc. SIGCOMM 2002 Conf., ACM, pp. 89–102, 2002.
193. KATZ, D., and FORD, P.S.: “TUBA: Replacing IP with CLNP,” IEEE Network Magazine, vol. 7, pp. 38–47, May/June 1993.
194. KAUFMAN, C., PERLMAN, R., and SPECINER, M.: Network Security, 2nd ed., Engle-wood Cliffs, NJ: Prentice Hall, 2002.
195. KENT, C., and MOGUL, J.: ‘‘Fragmentation Considered Harmful,’’ Proc. SIGCOMM ’87 Conf., ACM, pp. 390–401, 1987.
196. KERCKHOFF, A.: “La Cryptographic Militaire,” J. des Sciences Militaires, vol. 9, pp. 5–38, Jan. 1883 and pp. 161–191, Feb. 1883.
197. KHANNA, A., and ZINKY, J.: ‘‘The Revised ARPANET Routing Metric,’’ Proc. SIGCOMM ’89 Conf., ACM, pp. 45–56, 1989.

198. KIPNIS, J.: “Beating the System: Abuses of the Standards Adoptions Process,” IEEE Commun. Magazine, vol. 38, pp. 102–105, July 2000.
199. KLEINROCK, L.: ‘‘Power and Other Deterministic Rules of Thumb for Probabilistic Problems in Computer Communications,’’ Proc. Intl. Conf. on Commun., pp. 43.1.1–43.1.10, June 1979.
200. KLEINROCK, L., and TOBAGI, F.: “Random Access Techniques for Data Transmission over PacketSwitched Radio Channels,” Proc. Nat. Computer Conf., pp. 187-201, 1975.
201. KOHLER, E., HANDLEY, H., and FLOYD, S.: ‘‘Designing DCCP: Congestion Control without Reliability,’’ Proc. SIGCOMM 2006 Conf., ACM, pp. 27–38, 2006.
202. KOODLI, R., and PERKINS, C.E.: Mobile Inter-networking with IPv6, New York: John Wiley & Sons, 2007.
203. KOOPMAN, P.: ‘‘32-Bit Cyclic Redundancy Codes for Internet Applications,’’ Proc. Intl. Conf. on Dependable Systems and Networks., IEEE, pp. 459–472, 2002.
204. KRISHNAMURTHY, B., and REXFORD, J.: Web Protocols and Practice, Boston: Addison-Wesley, 2001.
205. KUMAR, S., PAAR, C., PELZL, J., PFEIFFER, G., and SCHIMMLER, M.: ‘‘Breaking Ciphers with COPACOBANA: A Cost-Optimized Parallel Code Breaker,’’ Proc. 8th Cryptographic Hardware and Embedded Systems Wksp., IACR, pp. 101–118, Oct. 2006.
206. LABOVITZ, C., AHUJA, A., BOSE, A., and JAHANIAN, F.: ‘‘Delayed Internet Routing Convergence,’’ IEEE/ACM Trans. on Networking, vol. 9, pp. 293–306, June 2001.
207. LAM, C.K.M., and TAN, B.C.Y.: “The Internet Is Changing the Music Industry,” Commun. of the ACM, vol. 44, pp. 62–66, Aug. 2001.
208. LAOUTARIS, N., SMARAGDAKIS, G., RODRIGUEZ, P., and SUNDARAM, R.: ‘‘Delay Tolerant Bulk Data Transfers on the Internet,’’ Proc. SIGMETRICS 2009 Conf., ACM, pp. 229–238, June 2009.
209. LARMO, A., LINDSTROM, M., MEYER, M., PELLETIER, G., TORSNER, J., and WIEMANN, H.: ‘‘The LTE Link-Layer Design,’’ IEEE Commun. Magazine, vol. 47, pp. 52–59, Apr. 2009.
210. LEE, J.S., and MILLER, L.E.: CDMA Systems Engineering Handbook, London: Artech House, 1998.
211. LELAND, W., TAQQU, M., WILLINGER, W., and WILSON, D.: ‘‘On the Self-Similar Nature of Ethernet Traffic,’’ IEEE/ACM Trans. on Networking, vol. 2, pp. 1–15, Feb. 1994.
212. LEMON, J.: ‘‘Resisting SYN Flood DOS Attacks with a SYN Cache,’’ Proc. BSDCon Conf., USENIX,
213. pp. 88–98, 2002.
214. LEVY, S.: ‘‘Crypto Rebels,’’ Wired, pp. 54–61, May/June 1993.
215. LEWIS, M.: Comparing, Designing, and Deploying VPNs, Indianapolis, IN: Cisco Press, 2006.
216. LI, M., AGRAWAL, D., GANESAN, D., and VENKATARAMANI, A.: ‘‘Block-Switched Networks: A New Paradigm for Wireless Transport,’’ Proc. NSDI 2009 Conf., USENIX, pp. 423–436, 2009.

217. LIN, S., and COSTELLO, D.: Error Control Coding, 2nd ed., Upper Saddle River, NJ: Pearson Education, 2004.
218. LUBACZ, J., MAZURCZYK, W., and SZCZYPIORSKI, K.: ‘‘Vice over IP,’’ IEEE Spectrum, pp. 42–47, Feb. 2010.
219. MACEDONIA, M.R.: ‘‘Distributed File Sharing,’’ IEEE Computer, vol. 33, pp. 99–101, 2000.
220. MADHAVAN, J., KO, D., LOT, L., GANGPATHY, V., RASMUSSEN, A., and HALEVY, A.: ‘‘Google’s Deep Web Crawl,’’ Proc. VLDB 2008 Conf., VLDB Endowment, pp. 1241–1252, 2008.
221. MAHAJAN, R., RODRIG, M., WETHERALL, D., and ZAHORJAN, J.: ‘‘Analyzing the MAC-Level Behavior of Wireless Networks in the Wild,’’ Proc. SIGCOMM 2006 Conf., ACM, pp. 75–86, 2006.
222. MALIS, A., and SIMPSON, W.: ‘‘PPP over SONET/SDH,’’ RFC 2615, June 1999.
223. MASSEY, J.L.: ‘‘Shift-Register Synthesis and BCH Decoding,’’ IEEE Trans. on Information Theory, vol. IT–5, pp. 122–127, Jan. 1969.
224. MATSUI, M.: ‘‘Linear Cryptanalysis Method for DES Cipher,’’ Advances in Cryptology— Eurocrypt 1993 Proceedings, Berlin: Springer-Verlag LNCS 765, pp. 386–397, 1994.
225. MAUFER, T.A.: IP Fundamentals, Upper Saddle River, NJ: Prentice Hall, 1999.
226. MAYMOUNKOV, P., and MAZIERES, D.: ‘‘Kademlia: A Peer-to-Peer Information System Based on the XOR Metric,’’ Proc. First Intl. Wksp. on Peer-to-Peer Systems, Berlin: Springer-Verlag LNCS 2429, pp. 53–65, 2002.
227. MAZIERES, D., and KAASHOEK, M.F.: ‘‘The Design, Implementation, and Operation of an Email Pseudonym Server,’’ Proc. Fifth Conf. on Computer and Commun. Security, ACM, pp. 27–36,1998.
228. MCAFEE LABS: McAfee Threat Reports: First Quarter 2010, McAfee Inc., 2010.
229. MENEZES, A.J., and VANSTONE, S.A.: ‘‘Elliptic Curve Cryptosystems and Their Implementation,’’ Journal of Cryptology, vol. 6, pp. 209–224, 1993.
230. MERKLE, R.C., and HELLMAN, M.: ‘‘Hiding and Signatures in Trapdoor Knapsacks,’’ IEEE Trans. on Information Theory, vol. IT–4, pp. 525–530, Sept. 1978.
231. METCALFE, R.M.: ‘‘Computer/Network Interface Design: Lessons from Arpanet and Ethernet,’’ IEEE J. on Selected Areas in Commun., vol. 11, pp. 173–179, Feb. 1993.
232. METCALFE, R.M., and BOGGS, D.R.: “Ethernet: Distributed Packet Switching for Local Computer Networks,” Commun. of the ACM, vol. 19, pp. 395–404, July 1976.
233. METZ, C.: “Interconnecting ISP Networks,” IEEE Internet Computing, vol. 5, pp. 74–80, Mar.-Apr. 2001.
234. MISHRA, P.P., KANAKIA, H., and TRIPATHI, S.: ‘‘On Hop by Hop Rate-Based Congestion Control,’’ IEEE/ACM Trans. on Networking, vol. 4, pp. 224–239, Apr. 1996.
235. MOGUL, J.C.: “IP Network Performance,” in Internet System Handbook, D.C. Lynch and M.T. Rose (eds.), Boston: Addison-Wesley, pp. 575–675, 1993.

236. MOGUL, J., and DEERING, S.: ‘‘Path MTU Discovery,’’ RFC 1191, Nov. 1990.
237. MOGUL, J., and MINSHALL, G.: ‘‘Rethinking the Nagle Algorithm,’’ Comput. Commun. Rev., vol. 31, pp. 6–20, Jan. 2001.
238. MOY, J.: “Multicast Routing Extensions for OSPF” Commun. of the ACM, vol. 37, pp. 61–66, AUg. 1994.
239. MULLINS, J.: “Making Unbreakable Code,” IEEE Spectrum, pp. 40-45, May 2002.
240. NAGLE, J.: “On Packet Switches with Infinite Storage,” IEEE Trans, on Commun., vol. COM-5, pp. 435–438, Apr. 1987.
241. NAGLE, J.: “Congestion Control in TCP/IP Internetworks,” Computer Commun. Rev., vol. 14, pp. 11–17, Oct. 1984.
242. NAUGHTON, J.: “A Brief History of the Future,” Woodstock, NY: Overlook Press, 2000. NEEDHAM, R.M., and SCHROEDER, M.D.: “Using Encryption for Authentication in Large Networks of Computers,” Commun. of the ACM, vol. 21, pp. 993–999, Dec. 1978.
243. NEEDHAM, R.M., and SCHROEDER, M.D.: ‘‘Authentication Revisited,’’ Operating Systems Rev., vol. 21, p. 7, Jan. 1987.
244. NELAKUDITI, S., and ZHANG, Z.-L.: “A Localized Adaptive Proportioning Approach to QoS Routing,” IEEE Commun. Magazine vol. 40, pp. 66–71, June 2002.
245. NEUMAN, C., and TS’O, T.: ‘‘Kerberos: An Authentication Service for Computer Networks,’’ IEEE Commun. Mag., vol. 32, pp. 33–38, Sept. 1994.
246. NICHOLS, R.K., and LEKKAS, P.C.: Wireless Security, New York: McGraw-Hill, 2002.
247. NIST: “Secure Hash Algorithm,” U.S. Government Federal Information Processing Standardise, 1993.
248. NONNENMACHER, J., BIERSACK, E., and TOWSLEY, D.: ‘‘Parity-Based Loss Recovery for Reliable Multicast Transmission,’’ Proc. SIGCOMM ’97 Conf., ACM, pp. 289–300, 1997.
249. NUCCI, A., and PAPAGIANNAKI, D.: Design, Measurement and Management of Large- Scale IP Networks, Cambridge: Cambridge University Press, 2008.
250. NUGENT, R., MUNAKANA, R., CHIN, A., COELHO, R., and PUIG-SUARI, J.: ‘‘The CubeSat: The PicoSatellite Standard for Research and Education,’’ Proc. SPACE 2008 Conf., AIAA, 2008.
251. ORAN, D.: ‘‘OSI IS-IS Intra-domain Routing Protocol,’’ RFC 1142, Feb. 1990.
252. OTWAY, D., and REES, O.: “Efficient and Timely Mutual Authentication,” Operating Systems Rev., pp. 8–10, Jan. 1987.
253. PADHYE, J., FIROIU, V., TOWSLEY, D., and KUROSE, J.: ‘‘Modeling TCP Throughput: A Simple Model and Its Empirical Validation,’’ Proc. SIGCOMM ’98 Conf., ACM, pp. 303–314, 1998.
254. PALAIS, J.C.: Fiber Optic Commun., 5rd ed., Englewood Cliffs, NJ: Prentice Hall, 2004.

255. PARAMESWARAN, M., SUSARLA, A., and WHINSTON, A.B.: “P2P Networking: An InformationSharing Alternative,” Computer, vol. 34, pp. 31–38, July 2001.
256. PAREKH, A., and GALLAGHER, R.: ‘‘A Generalized Processor Sharing Approach to Flow Control in Integrated Services Networks: The Multiple-Node Case,’’ IEEE/ACM Trans. on Networking, vol. 2, pp. 137–150, Apr. 1994.
257. PAREKH, A., and GALLAGHER, R.: ‘‘A Generalized Processor Sharing Approach to Flow Control in Integrated Services Networks: The Single-Node Case,’’ IEEE/ACM Trans. on Networking, vol. 1, pp. 344–357, June 1993.
258. PARTRIDGE, C., HUGHES, J., and STONE, J.: “Performance of Checksums and CRCs over Real Data,” Proc. SIGCOMM ‘95 Conf., ACM, pp. 68–76, 1995.
259. PARTRIDGE, C., MENDEZ, T., and MILLIKEN, W.: ‘‘Host Anycasting Service,’’ RFC 1546, Nov. 1993.
260. PAXSON, V., and FLOYD, S.: ‘‘Wide-Area Traffic: The Failure of Poisson Modeling,’’ IEEE/ACM Trans. on Networking, vol. 3, pp. 226–244, June 1995.
261. PERKINS, C.: ‘‘IP Mobility Support for IPv4,’’ RFC 3344, Aug. 2002.
262. PERKINS, C.E.: RTP: Audio and Video for the Internet, Boston: Addison-Wesley, 2003. PERKINS, C.E. (ed.): Ad Hoc Networking, Boston: Addison-Wesley, 2001.
263. PERKINS, C.E.: Mobile IP Design Principles and Practices, Upper Saddle River, NJ: Prentice Hall, 1998.
264. PERKINS, C.E., and ROYER, E.: ‘‘The Ad Hoc On-Demand Distance-Vector Protocol,’’ in Ad Hoc Networking, edited by C. Perkins, Boston: Addison-Wesley, 2001.
265. PERLMAN, R.: Interconnections, 2nd ed., Boston: Addison-Wesley, 2000.
266. PERLMAN, R.: Network Layer Protocols with Byzantine Robustness, Ph.D. thesis, M.I.T., 1988.
267. PERLMAN, R.: ‘‘An Algorithm for the Distributed Computation of a Spanning Tree in an Extended LAN,’’ Proc. SIGCOMM ’85 Conf., ACM, pp. 44–53, 1985.
268. PERLMAN, R., and KAUFMAN, C.: “Key Exchange in IPsec,” IEEE Internet Computing, vol. 4, pp. 50–56, Nov.–Dec. 2000.
269. PETERSON, W.W., and BROWN, D.T.: “Cyclic Codes for Error Detection,” Proc. IRE, vol. 49, pp. 228–235, Jan. 1961.
270. PIATEK, M., KOHNO, T., and KRISHNAMURTHY, A.: ‘‘Challenges and Directions for Monitoring
271. P2P File Sharing Networks—or Why My Printer Received a DMCA Takedown Notice,’’ 3rd Workshop on Hot Topics in Security, USENIX, July 2008.
272. PIATEK, M., ISDAL, T., ANDERSON, T., KRISHNAMURTHY, A., and VENKATARAMANI, V.: ‘‘Do Incentives Build Robustness in BitTorrent?,’’ Proc. NSDI 2007 Conf., USENIX, pp. 1–14, 2007.
273. PISCITELLO, D.M., and CHAPIN, A.L.: Open Systems Networking: TCP/IP and OSI, Boston: Addison-Wesley, 1993.

274. PIVA, A., BARTOLINI, F., and BARNI, M.: “Managing Copyrights in Open Networks,” IEEE Internet Computing, vol. 6, pp. 18–26, May– 2002.
275. POSTEL, J.: ‘‘Internet Control Message Protocols,’’ RFC 792, Sept. 1981.
276. RABIN, J., and MCCATHIENEVILE, C.: ‘‘Mobile Web Best Practices 1.0,’’ W3C Recommendation, July 2008.
277. RAMAKRISHNAM, K.K., FLOYD, S., and BLACK, D.: ‘‘The Addition of Explicit Congestion Notification (ECN) to IP,’’ RFC 3168, Sept. 2001.
278. RAMAKRISHNAN, K.K., and JAIN, R.: ‘‘A Binary Feedback Scheme for Congestion Avoidance in Computer Networks with a Connectionless Network Layer,’’ Proc. SIGCOMM ’88 Conf., ACM, pp. 303–313, 1988.
279. RAMASWAMI, R., KUMAR, S., and SASAKI, G.: Optical Networks: A Practical Perspective, 3rd ed., San Francisco: Morgan Kaufmann, 2009.
280. RATNASAMY, S., FRANCIS, P., HANDLEY, M., KARP, R., and SHENKER, S.: “A Scalable ContentAddressable Network,” Proc. SIGCOMM 2001 Conf, ACM, pp. 1161–172, 2001.
281. RIEBACK, M., CRISPO, B., and TANENBAUM, A.: ‘‘Is Your Cat Infected with a Computer Virus?,’’ Proc. IEEE Percom, pp. 169–179, Mar. 2006.
282. RIVEST, R.L.: “The MD5 Message-Digest Algorithm,” RFC 1320, Apr. 1992.944 Глава 9. Рекомендации для чтения и библиография
283. RIVEST, R.L., SHAMIR, A., and ADLEMAN, L.: “On a Method for Obtaining Digital Signatures and Public Key Cryptosystems,” Commun. of the ACM, vol. 21, pp. 120–126, Feb. 1978.
284. ROBERTS, L.G.: “Extensions of Packet Communication Technology to a Hand Held Personal Terminal,” Proc. Spring Joint Computer Conference, AFIPS, pp. 295–298, 1972.
285. ROBERTS, L.G.: “Multiple Computer Networks and Intercomputer Communication,” Proc. First Symp. on Operating Systems Prin., ACM, pp. 3.1–3.6, 1967.
286. ROSE, M.T.: The Simple Book, Englewood Cliffs, NJ: Prentice Hall, 1994.
287. ROSE, M.T.: The Internet Message, Englewood Cliffs, NJ: Prentice Hall, 1993.
288. ROWSTRON, A., and DRUSCHEL, P.: “Pastry: Scalable, Distributed Object Location and Routing for Large-Scale Peer-to-Peer Storage Utility,” Proc. 18th Int’l Conf. on Distributed Systems
289. Platforms, London: Springer-Verlag LNCS 2218, pp. 329–350, 2001.
290. RUIZ-SANCHEZ, M.A., BIERSACK, E.W., and DABBOUS, W.: “Survey and Taxonomy of IP Address Lookup Algorithms,” IEEE Network Magazine, vol. 15, pp. 8–23, March-April 2001.
291. SALTZER, J.H., REED, D.P., and CLARK, D.D.: ‘‘End-to-End Arguments in System Design,’’ ACM Trans. on Computer Systems, vol. 2, pp. 277–288, Nov. 1984.
292. SAMPLE, A., YEAGER, D., POWLEDGE, P., MAMISHEV, A., and SMITH, J.: ‘‘Design of an RFIDBased Battery-Free Programmable Sensing Platform,’’ IEEE Trans. on Instrumentation and Measurement, vol. 57, pp. 2608–2615, Nov. 2008.

293. SAROIU, S., GUMMADI, K., and GRIBBLE, S.: ‘‘Measuring and Analyzing the Characteristics of Napster & Gnutella Hosts,’’ Multim. Syst., vol. 9,, pp. 170–184, Aug. 2003.
294. SALTZER, J.H., REED, D.P., and CLARK, D.D.: “End-to-End Arguments in System Design,” ACM Trans, on Computer Systems, vol. 2, pp. 277-288, Nov. 1984.
295. SCHALLER, R.: ‘‘Moore’s Law: Past, Present and Future,’’ IEEE Spectrum, vol. 34, pp. 52–59, June 1997.
296. SCHNEIER, B.: Secrets and Lies, New York: John Wiley&Sons, 2004.
297. SCHNEIER, B.: E-Mail Security, New York: John Wiley&Sons, 1995.
298. SCHNORR, C.P.: “Efficient Signature Generation for Smart Cards,” Journal of Cryptol-ogy, vol. 4, pp. 161–174, 1991.
299. SCHOLTZ, R.A.: “The Origins of Spread-Spectrum Communications,” IEEE Trans, on Commun., vol. COM–0, pp. 822–854, May 1982.
300. SCHWARTZ, M., and ABRAMSON, N.: ‘‘The AlohaNet: Surfing for Wireless Data,’’ IEEE Commun. Magazine, vol. 47, pp. 21–25, Dec. 2009.
301. SEIFERT, R., and EDWARDS, J.: The All-New Switch Book, NY: John Wiley, 2008.
302. SENN, J.A.: ‘‘The Emergence of M-Commerce,’’ IEEE Computer, vol. 33, pp. 148–150, Dec. 2000.
303. SERJANTOV, A.: “Anonymizing Censorship Resistant Systems,” Proc. First Int’l Workshop on Peerto-Peer Systems, London: Springer-Verlag LNCS 2429, pp. 111–120, 2002.
304. SHACHAM, N., and MCKENNY, P.: ‘‘Packet Recovery in High-Speed Networks Using Coding and Buffer Management,’’ Proc. INFOCOM Conf., IEEE, pp. 124–131, June 1990.
305. SHAIKH, A., REXFORD, J., and SHIN, K.: ‘‘Load-Sensitive Routing of Long-Lived IP Flows,’’ Proc. SIGCOMM ’99 Conf., ACM, pp. 215–226, Sept. 1999.
306. SHALUNOV, S., and CARLSON, R.: ‘‘Detecting Duplex Mismatch on Ethernet,’’ Passive and Active Network Measurement, Berlin: Springer-Verlag LNCS 3431, pp. 3135–3148, 2005.
307. SHANNON, C.: “A Mathematical Theory of Communication,” Bell System Tech. J., vol. 27, pp.
308. 379–423, July 1948; and pp. 623–656, Oct. 1948.
309. SHEPARD, S.: SONET/SDH Demystified, New York: McGraw-Hill, 2001.
310. SHREEDHAR, M., and VARGHESE, G.: “Efficient Fair Queueing Using Deficit Round Robin,” Proc.
311. SIGCOMM ‘95 Conf., ACM, pp. 231–243, 1995.
312. SIMPSON, W.: Video Over IP, 2nd ed., Burlington, MA: Focal Press, 2008.
313. SIMPSON, W.: ‘‘PPP in HDLC-like Framing,’’ RFC 1662, July 1994b.
314. SIMPSON, W.: ‘‘The Point-to-Point Protocol (PPP),’’ RFC 1661, July 1994.
315. SIU, K., and JAIN, R.: ‘‘A Brief Overview of ATM: Protocol Layers, LAN Emulation, and Traffic,’’ ACM Computer Communications Review, vol. 25, pp. 6–20, Apr. 1995.
316. SKOUDIS, E. and LISTON, T.: Counter Hack Reloaded, 2nd ed., Upper Saddle River, NJ: Prentice Hall, 2006.

317. SMITH, O.K., and ALEXANDER, R.C.: Fumbling the Future, New York: William Morrow, 1988.
318. SNOEREN, A.C., and BALAKRISHNAN, H.: “An End-to-End Approach to Host Mobility,” Intel Conf. on Mobile Computing and Networking, ACM, pp. 155–166, 2000.
319. SOBEL, D.L.: “Will Carnivore Devour Online Privacy,” Computer, vol. 34, pp. 87–88, May 2001.
320. SOTIROV, A., STEVENS, M., APPELBAUM, J., LENSTRA, A., MOLNAR, D., OSVIK, D., and DE
321. WEGER, B.: ‘‘MD5 Considered Harmful Today,’’ Proc. 25th Chaos Communication Congress, Verlag Art d’Ameublement, 2008.
322. SOUTHEY, R.: The Doctors, London: Longman, Brown, Green and Longmans, 1848.
323. SPURGEON, C.E.: Ethernet: The Definitive Guide, Sebastopol, CA: O’Reilly, 2000.
324. STALLINGS, W.: Data and Computer Communications, 9th ed., Upper Saddle River, NJ: Pearson Education, 2010.
325. STEVENS, W.R.: TCP/IP Illustrated, TheProtocols, Boston: Addison-Wesley, 1994.
326. STINSON, D.R.: Cryptography Theory and Practice, 2nd ed., Boca Raton, FL: CRC Press, 2002.
327. STOICA, I., MORRIS, R., KARGER, D., KAASHOEK, M.F., and BALAKRISHNAN, H.: “Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications,” Proc. SIGCOMM 2001 Conf., ACM, pp. 149–160, 2001.
328. STUBBLEFIELD, A., IOANNIDIS, J., and RUBIN, A.D.: “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP,” Proc Network and Distributed Systems Security Symp., ISOC, pp. 1–11,2002.
329. STUTTARD, D., and PINTO, M.: The Web Application Hacker’s Handbook, New York John Wiley & Sons, 2007.
330. SU, S.: The UMTS Air Interface in RF Engineering, New York: McGraw-Hill, 2007.
331. SULLIVAN, G., and WIEGAND, T.: ‘‘Tree Algorithms for Packet Broadcast Channels,’ Proc. of the IEEE, vol. 93, pp. 18–31, Jan. 2005.
332. SUNSHINE, C.A., and DALAL, Y.K.: “Connection Management in Transport Protocols,” Computer Networks, vol. 2, pp. 454–473, 1978.
333. TAN, K., SONG, J., ZHANG, Q., and SRIDHARN, M.: ‘‘A Compound TCP Approach for High-Speed and Long Distance Networks,’’ Proc. INFOCOM Conf., IEEE, pp. 1–12, 2006.
334. TANENBAUM, A.S., and VAN STEEN, M.: Distributed Systems: Principles and Paradigms, Upper Saddle River, NJ: Prentice Hall, 2007.
335. TOMLINSON, R.S.: “Selecting Sequence Numbers,” Proc. SIGCOMM/SIGOPS Interprocess Commun. Workshop, ACM, pp. 11–23, 1975.
336. TUCHMAN, W.: “Hellman Presents No Shortcut Solutions to DES,” IEEE Spectrum, vol. 16, pp. 40–41, July 1979.

337. TURNER, J.S.: “New Directions in Communications (or Which Way to the Information Age),” IEEE Commun. Magazine, vol. 24, pp 8–15, Oct. 1986.
338. UNGERBOECK, G.: ‘‘Trellis-Coded Modulation with Redundant Signal Sets Part I: Introduction,’’ IEEE Commun. Magazine, vol. 25, pp. 5–11, Feb. 1987.
339. VALADE, J.,: PHP & MySQL for Dummies, 5th ed., New York: John Wiley & Sons, 2009.
340. VARGHESE, G.: Network Algorithmics, San Francisco: Morgan Kaufmann, 2004.
341. VARGHESE, G., and LAUCK, T.: “Hashed and Hierarchical Timing Wheels: Data Structures for the Efficient Implementation of a Timer Facility,” Proc. llth Symp. on Operating Systems Prin., ACM, pp. 25–38, 1987.
342. VERIZON BUSINESS: 2009 Data Breach Investigations Report, Verizon, 2009.
343. VITERBI, A.: CDMA: Principles of Spread Spectrum Communication, Englewood Cliffs, NJ: Prentice Hall, 1995.
344. VON AHN, L., BLUM, B., and LANGFORD, J.: ‘‘Telling Humans and Computers Apart Automatically,’’ Commun. of the ACM, vol. 47, pp. 56–60, Feb. 2004.
345. WAITZMAN, D., PARTRIDGE, C., and DEERING, S.: ‘‘Distance Vector Multicast Routing Protocol,’’ RFC 1075, Nov. 1988.
346. WALDMAN, M., RUBIN, A.D., and CRANOR, L.F.: “Publius: A Robust, Tamper-Evident, Censorship-Resistant, Web Publishing System,” Proc. Ninth USEN1X Security Symp., USENIX, pp. 59–72, 2000.
347. WANG, Z., and CROWCROFT, J.: ‘‘SEAL Detects Cell Misordering,’’ IEEE Network Magazine, vol. 6, pp. 8–9, July 1992.
348. WANT, R.: RFID Explained, San Rafael, CA: Morgan Claypool, 2006.
349. WARNEKE, B., LAST, M., LIEBOWITZ, B., and PISTER, K.S.J.: “Smart Dust: Communicating with a Cubic Millimeter Computer,” Computer, vol. 34, pp. 44–51, Jan. 2001.
350. WAYNER, P.: Disappearing Cryptography: Information Hiding, Steganography, and Watermarking, 3nded., San Francisco: Morgan Kaufmann, 2008.
351. WEI, D., CHENG, J., LOW, S., and HEGDE, S.: ‘‘FAST TCP: Motivation, Architecture, Algorithms, Performance,’’ IEEE/ACM Trans. on Networking, vol. 14, pp. 1246–1259, Dec. 2006.
352. WEISER, M.: ‘‘The Computer for the Twenty-First Century,’’ Scientific American, vol. 265, pp. 94–104, Sept. 1991.
353. WELBOURNE, E., BATTLE, L., COLE, G., GOULD, K., RECTOR, K., RAYMER, S., BALAZINSKA, M., and BORRIELLO, G.: ‘‘Building the Internet of Things Using RFID,’’ IEEE Internet Computing, vol. 13, pp. 48–55, May 2009.
354. WITTENBURG, N.: Understanding Voice Over IP Technology, Clifton Park, NY: Delmar Cengage Learning, 2009.
355. WOLMAN, A., VOELKER, G., SHARMA, N., CARDWELL, N., KARLIN, A., and LEVY, H.: ‘‘On the Scale and Performance of Cooperative Web Proxy Caching,’’ Proc. 17th Symp. on Operating Systems Prin., ACM, pp. 16–31, 1999.

356. WOOD, L., IVANCIC, W., EDDY, W., STEWART, D., NORTHAM, J., JACKSON, C., and DA SILVA CURIEL, A.: ‘‘Use of the Delay-Tolerant Networking Bundle Protocol from Space,’’ Proc. 59th Int’l Astronautical Congress, Int’l Astronautical Federation, pp. 3123–3133, 2008.
357. WU, T.: ‘‘Network Neutrality, Broadband Discrimination,’’ Journal on Telecom. and High-Tech. Law, vol. 2, pp. 141–179, 2003.
358. WYLIE, J., BIGRIGG, M.W., STRUNK, J.D., GANGER, G.R., KILICCOTE, H., and KHOSLA, P.K.: “Survivable Information Storage Systems,” Computer, vol. 33, pp. 61–68, Aug. 2000.
359. YU, T., HARTMAN, S., and RAEBURN, K.: ‘‘The Perils of Unauthenticated Encryption: Kerberos Version 4,’’ Proc. NDSS Symposium, Internet Society, Feb. 2004.
360. YUVAL, G.: “How to Swindle Rabin,” Cryptologia, vol. 3, pp. 187–190, July 1979.
361. ZACKS, M.: “Antiterrorist Legislation Expands Electronic Snooping,” IEEE Internet Computing, vol. 5, pp. 8–9, Nov.-Dec. 2001.
362. ZHANG, Y., BRESLAU, L., PAXSON, V., and SHENKER, S.: ‘‘On the Characteristics and Origins of Internet Flow Rates,’’ Proc. SIGCOMM 2002 Conf., ACM, pp. 309–322, 2002.
363. ZHAO, B., LING, H., STRIBLING, J., RHEA, S., JOSEPH, A., and KUBIATOWICZ, J.: ‘‘Tapestry: A Resilient Global-Scale Overlay for Service Deployment,’’ IEEE J. on Selected Areas in Commun., vol. 22, pp. 41–53, Jan. 2004.
364. ZIMMERMANN, P.R.: The Official PGP User’s Guide, Cambridge, MA: M.I.T. Press, 1995a.
365. ZIMMERMANN, P.R.: PGP: Source Code and Internals, Cambridge, MA: M.I.T. Press, 1995b.
366. ZIPF, G.K.: Human Behavior and the Principle of Least Effort: An Introduction to Human Ecology, Boston: Addison-Wesley, 1949.
367. ZIV, J., and LEMPEL, Z.: “A Universal Algorithm for Sequential Data Compression,” IEEE Trans, on Information Theory, vol. IT-3, pp. 337–343, May 1977.