Міністерство освіти і науки України
Державний університет телекомунікацій

Гніденко М.П., Вишнівський В.В., Сєрих С.О.,
Зінченко О.В., Прокопов С.В.

Конвергентна мережна інфраструктура

Навчальний посібник

Київ – 2019

УДК 004.72

Гриф надано Державним університетом телекомунікацій

Рецензенти: **Левківський К.М**., кандидат технічних наук, доцент, головний спеціаліст Інституту модернізації змісту освіти.
Приходько Ю.І., кандидат технічних наук, доцент, головний науковий співробітник Науково-методичного центру Національного університета оборони України

Гніденко М.П., Вишнівський В.В., Сєрих С.О., Зінченко О.В., Прокопов С.В.
Г 56 Конвергентна мережна інфраструктура. – Навчальний посібник. – К: ФОП Гуляєва В.М., 2019. – 180 с.
ISBN 978-617-7503-69-8

На ринку інформаційних технологій (IT) дуже динамічно просуває свої досягнення в області мережевих технологій компанія Hewlett-Packard (HP), в якості світового лідера виробництва мережевого обладнання для проектування, розгортання і експлуатації мереж на основі відкритих стандартів і конвергентної інфраструктури. Завдяки використанню мережевого обладнання компанії Hewlett-Packard (HP), можна істотно підвищити оперативність малого і середнього бізнесу, зменшити вимоги до обслуговування і знизити витрати на утримання IT-середовища.

У навчальному посібнику розглядаються питання проектування і впровадження мережевих рішень компанії Hewlett-Packard (HP) на основі таких понять як основи мережевих технологій і мережевого обладнання, інфраструктури дротових і бездротових мереж, протоколів TCP/IP, комутації та маршрутизації, адміністрування та управління мережами, безпеки мереж, усунення несправностей, оптимізації, доступності і надійності мереж. Всі питання мають прикладний характер і пояснюються на практичних прикладах.

Матеріали навчального посібника є основою для оволодіння таких відкритих стандартизованих конвергентних рішень, як: HP FlexNetwork з єдиною системою управління та моніторингу, HP Intelligent Management Center (IMC HP), а також програмно-визначених мереж SDN (Software Defined Networking).

Навчальний посібник призначено для студентів, аспірантів і викладачів, які планують підготуватися до міжнародної сертифікації рівня HPE Accredited Technical Associate (HP ATA) – Networks.

ISBN 978-617-7503-69-8

Зміст

Введення

Комп'ютерні інформаційні технології використовуються в усіх областях наукової та виробничої діяльності. Комп'ютеризації зазнали такі галузі діяльності як автоматизація процесів управління складних виробництв, системи моделювання та чисельні методи дослідження природних явищ, системи комунікацій і зв'язку, системи накопичення і зберігання знань, електронні інформаційні системи. Нові досягнення в розвитку цих систем стали можливі завдяки їх інтеграції з мережевими технологіями.

Мережеві технології сьогодні формують нове поле інформаційної культури, в якому реалізується процес розвитку сучасного суспільства. Те, наскільки швидко мережеві технології впроваджуються в усі сфери діяльності людини і те, наскільки швидко вони змінюються і розвиваються, виникає нагальна потреба йти в ногу з часом і постійно вдосконалювати свої знання в даній області.

Цей навчальний посібник є результатом досвіду викладання авторами курсів конвергентних мережевих технологій компанія Hewlett Packard Enterprise в Державному університеті телекомунікацій.

Hewlett Packard Enterprise допомагає замовникам в побудові ефективного, продуктивного і безпечного IT-середовища за допомогою поєднання традиційних підходів з новими, що дозволяє компаніям швидко реагувати на ідеї створюючи, використовуючи і розвиваючи нові рішення на основі кращого досвіду і кращих бізнес-моделей. Нові підходи допомагають вибрати і впровадити обчислювальні потужності, які можуть мати значний вплив на результативність і ефективність бізнесу, побудувати сховище, здатне «думати» в не меншій ступені, ніж зберігати, використовувати ковергентні мережі, які здійснюють обмін даними швидше і безпечніше, ніж будь-коли.

Інтенсивний розвиток і впровадження нових мережевих технологій останніми роками вимагало не тільки припливу великої кількості фахівців з розробки і проектування систем, а й істотно змінило вимоги до рівня підготовки користувачів.

Цими фактами обумовлений підвищений попит до навчальних програм і курсів з різних напрямків інформаційних технологій, що в свою чергу вимагає наявності великого числа навчально-методичного матеріалу.

Навчальний посібник пропонує матеріал по конвергентних мережевих технологій як з точки зору теоретичних основ мережевих технологій і мережевого устаткування, так і практичних рекомедацій по їх використанню. Такий підхід може бути корисний як початківців, які мають намір освоювати новий вид діяльности, так і фахівцям, яким необхідно освіжити знання і підвищити кваліфікацію.

Розділ 1:
Основи мережних технологій

Введення

На початку розвитку комп'ютерних мереж, проблема сумісності між обладнанням різних виробників була актуальною як ніколи. Існувало кілька несумісних стандартів підключення комп'ютерів, форматування даних і додатки переданих даних. Ранні моделі мережі були засновані на цих оригінальних концепціях. Дуже швидко стала очевидною потреба в загальних стандартах. Спочатку було розроблено декілька стандартів, проте з часом найбільшого поширення набули мережні стандарти на основі моделей OSI і TCP / IP.

У цьому розділі ми введемо основні поняття мереж і мережевих стандартів. Почнемо з прийнятого базового стандарту - семирівневої моделі взаємодії відкритих систем (OSI). Потім ми порівняємо модель OSI з найбільш поширеною реалізацією використовуваної в даний час, моделлю TCP/IP. Ми розглянемо практичне застосування Ethernet і бездротових технологій. Також коротко розглянемо деякі стандарти, більш високого рівня, що використовуються для реалізації адресації, основний мережевої безпеки і віртуальних локальних мереж (VLAN).

Мета

У цьому розділі ми будемо вивчати:

- Опис семиуровневой моделі OSI.
- Порівняння і зіставлення моделей OSI і TCP/IP.
- Пояснення мети і використання призначення різних методів адресації.
- Визначення загальних технологій Ethernet.
- Визначення загальних бездротових технологій.
- Пояснення основних концепцій безпеки.

Модель OSI

Міжнародна організація по стандартизації (ISO) представила модель OSI (Рисунок 1.1), як спосіб вирішення дилеми (необхідності вибору) стандартів, спричиненою використанням множинних несумісних стандартів у минулому.

Модель OSI є семирівневою моделлю, яка організовує і описує мережеві функції і інтерфейси. Модель досягла своєї нинішньої форми у 1983 році.

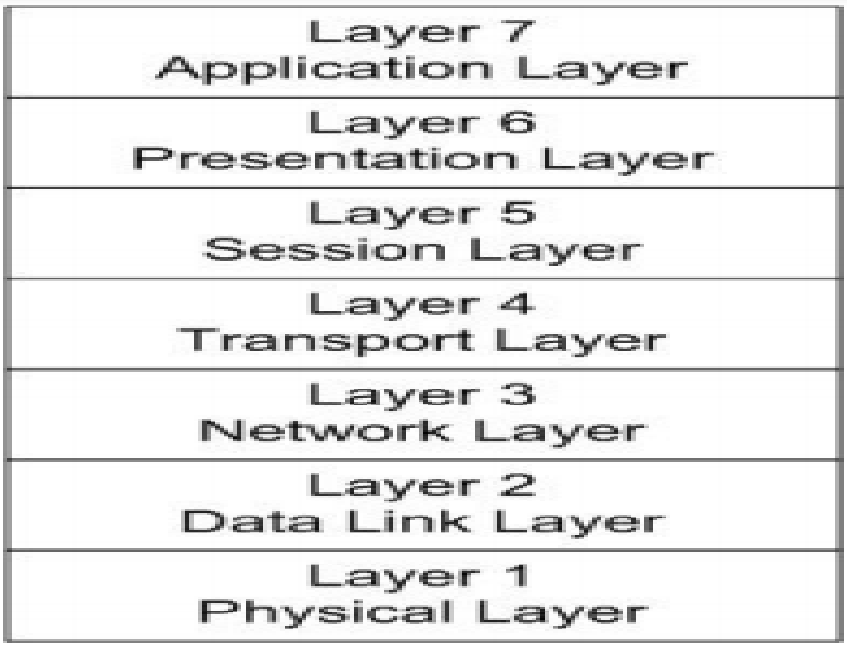


Рисунок 1.1 – Модель OSI

Модель OSI складається з наступних рівнів: фізичного, канального, мережевого, транспортного, сеансового, рівня представлення і прикладного рівня. За винятком фізичного рівня, кожен з рівнів може взаємодіяти тільки з рівнем розташованим безпосередньо вище або нижче нього. Фізичний рівень одного мережевого пристрою, може взаємодіяти з фізичним рівнем іншого мережевого пристрою.

Модель OSI забезпечує стандарти керівництва, а не суворі правила реалізації мережі. Інші організації зі стандартизації як правило, дотримуються цієї моделі, щоб забезпечити функціональну мережу. Наприклад, IEEE розробив докладні стандарти протоколів, реалізованих на рівнях 1 і 2: 802.3 (Ethernet) і 802.11 (бездротові технології).

Institute of Electrical and Electronics Engineers (институт инженеров электорехники и электроники) (IEEE) *- технічна організація, яка сприяє розвитку і публікацій стандартів.*

Протокол *- набір правил, які пристрої використовують для взаємодії. Кожен з рівнів використовує власні протоколи для забезпечення сеансу зв'язку.*

Однією з сильних сторін моделі OSI є те, що вона забезпечує загальний контекст для опису мереж і мережевих пристроїв. Стверджуючи, що пристрій працює на певному рівні, мається на увазі що пристрій включає в себе функціонал всіх попередніх рівнів. Наприклад, багато комутаторів описані на рівні 3, це означає, що пристрій реалізує функціональні можливості мережевого рівня. Також це означає що в ньому реалізована функціональність каналу передачі даних і фізичного рівня.

Комутатор (switch) - *мережеве пристрій зв'язку, що передає дані з порту джерела передачі до порту призначення.*

Рівень 1 - Фізичний рівень

Фізичний рівень відповідальний за передачу і прийом даних через середовище передачі. Інформація розглядається як неструктурований потік вихідних даних сигналу. Передача може бути здійснена на фізичному носії, наприклад по мідному дроту або оптоволокну, або ж по бездротовій мережі за допомогою радіохвиль.

 ***Середовище передачі*** *- той шлях даних, за яким здійснюється передача даних. У провідної мережі мідні кабелі використовуються найбільш часто.*

Фізичний рівень забезпечує прямий зв'язок між вузлами. Крім того, цей шар найкраще визначається і найбільш послідовно реалізується.

Вузол *- цей термін використовується для позначення точки підключення до мережі, як правило, це комп'ютер або інший мережний пристрій.*

Фізичне середовище

Фізичне середовище це шлях, по якому передаються дані. Фізичний рівень визначає тип середовища який використовується. Він також визначає, як пристрої фізично підключені до середовища, в тому числі типу роз'єму, номер телефону, і так далі.

У разі провідної мережі, потрібні певні види роз’ємів. Визначається тип носія: мідного або волоконно-оптичного кабелю. Також визначається потужність сигналу.

Опто-волоконний кабель *- кабель зі скла або пластикових волокон, який передає сигнал у вигляді світлових променів.*

Для бездротових пристроїв, для передачі і прийому задається частота. Стандарти вказують частоту, яка буде використовуватися і рекомендовані рівні передачі.

Передача даних

Технічні характеристики, вказані на фізичному рівні визначають кодування даних - як дані перетворюються в відповідну форму для передачі. Кодування даних включає в себе подання даних у вигляді 1 або 0, визначає як почати спочатку і до кінця кадру, і як дані синхронізувати.

 ***Кодування даних*** *- перетворення даних з потоку даних в інший формат. В контексті фізичного рівня, це відноситься до конвектуванню даних в формат, придатний для передачі.*

Характеристики фізичного рівня також визначають метод передачі. Дані можуть бути відправлені з використанням або цифрової або аналогової передачі. Системи передачі по оптоволокну, для прикладу, використовують цифрову передачу. У волоконно-оптичних системах передачі, наявність або відсутність світла використовується для вираження двох станів цифрової передачі: 0 або 1. Бездротова передача є аналогової передачею за самою своєю природою, тому що вона використовує радіо частоти для передачі.

 ***Цифровий сигнал*** *- сигнал з двома різними станами, представлених у вигляді значень 0 і 1 для передачі даних.*

Аналоговий сигнал *характеризується мінливою амплітудою сигналу (висота хвилі), частотою (швидше за зміни), або обох складових.*

Технологія передачі *- передача даних або в якості аналогового або цифрового сигналу.*

Рівень 2 – Канальний

Канальний рівень несе відповідальність за забезпечення того, що дані передаються між вузлами без помилок. Передача даних без помилок є кінцевою метою цього рівня, але це не завжди досягається. До сих пір, з використанням сучасних технологій передачі, більшість передач часто дуже близькі до безпомилковим. Така точність здійснюється за допомогою таких методів:

• Управління посиланнями - встановлює логічний зв'язок між вузлами і потім усуває з'єднання, коли це вже не потрібно.

• Контроль трафіку - управляє передачею кадрів і відключає вузол передачі, коли дані не доступні для відправки.

• Секвестрування - гарантує, що кадри посилаються (і виходять) послідовно.

• Підтвердження - визнає отримання кадрів, як спосіб виявлення втрачених або пошкоджених кадрів.

• Визначення меж - визначає формати кадру, і визнає ці межі на отриманих кадрах.

• Корекція помилок - перевіряє цілісність кадру.

• Управління доступом - визначає, який вузол може використовувати носій для передачі.

Кожен вузол однозначно визначений на канальному рівні через унікальну адресу яка відома як адреса управління доступом до середовища (MAC-адресу).

 ***MAC-адреса*** *- адреса, який однозначно ідентифікує вузол мережі на 2 рівні моделі OSI.*

MAC-адресу зазвичай записується як 12-значне шістнадцяткове число. Перші шість цифр ідентифікують виробника мережевого інтерфейсу. Інші цифри являють собою унікальний адреса адаптера. Це актуально як для дротових, так і для бездротових мережевих адаптерів. У деяких випадках, наприклад, коли мережі реалізовані на віртуальній машині, MAC-адресу генерується за допомогою програмного забезпечення.

Віртуальна машина *- комп'ютер в пам'яті фізичного комп'ютера, що дозволяє представляти один комп'ютер в якості кілька окремих комп'ютерів, що виконують ізольовані функції.*

Протоколи передачі низького рівня, такі як Ethernet і Token Ring, визначаються на обох рівнях - фізичному і канальному. Ці два протоколи несумісні. Вони не можуть інтерпретувати дані один одного, тому що їх кадри будуються по-різному. Вони також мають різні визначення для типів фізичних носіїв і характеристик сигналу.

Ethernet *- найбільш поширений протокол передачі низького рівня. Іноді також згадується як транспортний протокол.*

Token Ring *- ласний протокол низького канального рівня, який найбільш часто використовується в реалізації мережі IBM.*

Ви можете отримати MAC-адресу для мережевого Ethernet адаптера в Windows, виконавши команду **IPCONFIG** (Рисунок 1.2).

Рисунок 1.2 – Перегляд MAC-адресу

MAC-адреса буде вказана в конфігурації адаптера Ethernet. Він у списку фізичного адреса адаптера. В цьому випадку, адреса: 00-1F-16-F8-2E-19

Рівень 3 – Мережевий рівень

Мережевий рівень виробляє маршрутизацію в мережі можливою. Кожен вузол-мережа ідентифікується унікальною адресою, яка складається з адреси мережі і адреси вузла (Рисунок 1.3). До протоколів мережного рівня також належать логічні імена пристроїв (такі як CopyRoomPC) для мережевих адрес.

Рисунок 1.3 – Адреса IPv4

Замість того, щоб бути жорстко фіксованим для вузла, як MAC-адреса, адреса мережі визначається через конфігурації пристрою. Адреса може бути або налаштованою на вузлі або застосовуватися автоматично, коли вузол підключається до мережі.

Больш детально формат адреси IPv4 ми розглянемо подальше у цьому курсі, але, як коротеньке зауваження, адреса ідентифікує вузол і підмережу, на якій він розташований. Значення, відоме як маска підмережі визначає, які біти використовується для кожної частини адреси.

Маршрутизатор відповідаэ за пересилку трафіку між мережами. Маршрутизатор відповідаэ за те, щоб дані в такий спосіб прокладали шлях до правильного адресату. Вони також несуть відповідальність за управління фрагментацією.

Маршрутизатор (router) *- ристрій відповідає за направлення трафіку на основі мережевої адреси.*

Фрагментація *- процес розподілу мережевого пакету на пакети меншого розміру для збірки в пункті призначення.*

Фрагментація необхідна через те, що деякі маршрутизатори мають менший розмір MTU ніж інші. Коли маршрутизатор з великим MTU передає кадр до маршрутизатора з меншим MTU, він повинен розбити кадр так, щоб він міг бути зібраний після приходу до приймаючого вузла.

Максимальний блок передачі (MTU - maximum transmission unit) *- найбільший розмір пакета або кадру, з яким маршрутизатор може впоратися.*

Рівень 4 – Транспортний рівень

Транспортний рівень відповідає за безпомилкову доставку повідомлення. Конкретні функції, реалізовані відповідно до протоколу на транспортному рівні залежать від якості передачі і умов перевірок на помилки на мережевому рівні і нижче. Основні функції аналогічні тим, які передбачені для кадрів канального рівня, але на більш високому рівні. До них відносяться:

• Сегментація - розбиває повідомлення (якщо необхідно) з наступним збиранням на транспортному рівні.

• Підтвердження - використовує підтвердження, щоб забезпечити надійну доставку.

• Контроль трафіку - забезпечує передачу тільки тоді, коли є повідомлення.

• Мультиплексування - управляє передачею декількох повідомлень.

• Транспортний рівень додає інформацію заголовка, яка дозволяє зібрати повідомлення при отриманні. Це включає в себе нумерацію, якщо це не передбачено в нижніх рівнях.

Рівень 5 – Сеансовий рівень

Сеансовий рівень відповідає за встановлення та підтримку сесій між хостами, а також завершення сеансу, коли він перестає бути необхідний. Протоколи сеансового рівня також надають функції для підтримки сесії, включаючи безпеку, розпізнавання між хостами і запис сесії.

Сесія - *ряд взаємодій, які відбуваються між двома вузлами в ході підключення.*

Рівень 6 – Рівень представлення

Рівень представлення відповідає за форматування даних з прикладного рівня, так що дані можуть бути передані або так, що дані можуть бути розпізнані прикладним рівнем. Це робиться за допомогою перекладу даних, який може включати:

- Переклад символів - зазвичай ASCII або EBCDIC.
- Перетворення - у міру необхідності, в тому числі порядок бітів, форматування кінця рядка, і так далі.
- Стиснення - застосування алгоритмів стиснення даних для зменшення розмірів переданих даних.
- Шифрування - шифрування/дешифрування даних для забезпечення безпеки даних.

Американський стандартний код для обміну інформацією (ASCII - American Standard Code for Information Interchange) - *Метод кодування символів, який використовується для представлення 128 символів у вигляді 7-бітових значень. Найчастіше використовується операційною системою UNIX і деякими застарілими програмами, такими як DOS-додатки.*

Розширений двійковій-десятковий код обміну (EBCDIC - *Extended Binary Coded Decimal Interchange Code) - двійковий код для символьного кодування, розроблений IBM і, перш за все, використовується в ЕОМ.*

Навіть тоді, коли дані передаються у відкритому вигляді, шифрування даних, як правило, застосовується до будь-яких паролів, переданих між вузлами.

Рівень 7 – Прикладний рівень

Користувачі і додатки забезпечують доступ до мережевих служб через рівень додатків. Всі мережеві послуги здійснюються через рівень додатків, в тому числі:

- Дистанційний доступ до файлів і принтера.
- Спільне використання ресурсів.
- Зв'язок між процесами, що працюють на різних комп'ютерах.
- Електронні повідомлення та електронна пошта.
- Служби каталогів.
- Перегляд веб-сторінок.

Процес *– в цьому контексті, процес відноситься до випадку, коли програма виконується на комп'ютері.*

Управління мережею здійснюється також на рівні додатків. Кілька спеціалізованих протоколів управління реалізують управління мережею.

Модель TCP/IP

Transmission Control Protoco/Internet Protocol (TCP/IP) - це стек мережевих протоколів, який в даний час найчастіше використовується. Він використовується в більшості локальних і глобальних мережах і це є основним протокол підтримки в Інтернеті.

Локальна мережа (LAN) *– з'єднані комп'ютери в рамках невеликої географічної області, як правило, одного офісу або будинку.*

Глобальна мережа (WAN) *- комп'ютери, підключені в більш широкому географічному районі. Інтернет є прикладом WAN.*

Модель TCP/IP складається із чотирьох рівнів моделі DARPA. Рисунок 1.4 показує, як модель TCP/IP відображається на моделі OSI. Функціональність забезпечується за допомогою різних протоколів, реалізованих в кожному із рівнів.

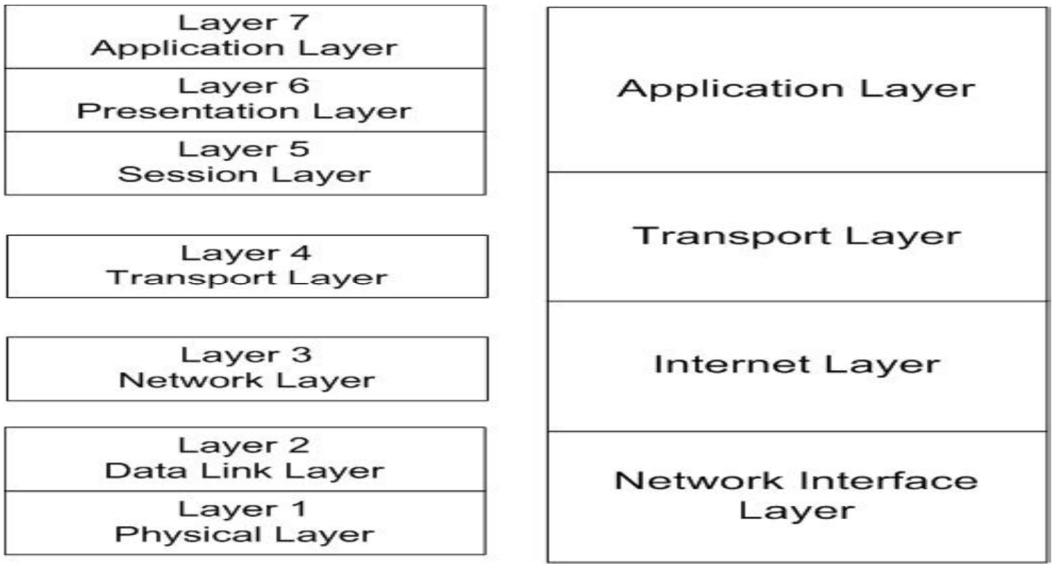


Рисунок 1.4 Модель TCP/IP

DARPA (Defense Advanced Research Projects Agency) *- проекти перспективних досліджень агентства оборони. Незалежні дослідження агентства, що фінансується Департаментом оборони США.*

Рівень Доступу до мережі

Рівень Мережевого інтерфейсу (також відомий як Рівень Доступу до мережі) реалізує більшу частину функціональності фізичного і канального впустив моделі OSI. Як і в моделі OSI, окремі вузли ідентифіковані MAC-адресами, які реалізуються на рівні мережного інтерфейсу.

 ***Хост*** *- термін використовується для позначення вузлів в TCP/IP мережі.*

Як згадувалося раніше, транспортні протоколи низького рівня, такі як 802.3 Ethernet і 802.11 бездротових мереж реалізуються на цьому рівні.

Модель TCP/IP була розроблена, щоб працювати незалежно від мережі комунікаційних технологій. Через це, вона може бути пристосована, щоб підтримувати широкий спектр протоколів, в тому числі протоколів WAN, таких як Frame Relay, на рівні Мережевого інтерфейсу. Така гнучкість дозволяє TCP/IP бути адаптованою для підтримки нових мережевих комунікаційних технологій.

 ***Frame Relay*** *– (ретрансляція кадрів) - формат передачі низького рівня призначений для підтримки зв'язку між локальними мережами і між кінцевими точками WAN.*

Рівень Мережевого інтерфейсу не підтримує послідовності і визнання певного на Канальному рівні модеді OSI. Коли модель TCP/IP була вперше розроблена, передбачалося, що зв'язок на рівні Мережного інтерфейсу буде ненадійною. Замість цього, функціональні можливості, необхідні для підтримки надійного зв'язку здійснюється на рівнях транспорту й додатків.

Рівень Інтернет

Рівень Інтернет моделі TCP/IP забезпечує ту ж функціональність, що і Мережевий рівень моделі OSI. У своїй поточній реалізації, рівень Інтернет виконаний з двох рівнів, що діють паралельно:

Рівень Інтернет-протоколу версії 4 (IPv4)

Рівень Інтернет-протоколу версії 6 (IPv6)

Обидва несуть відповідальність за адресацію хостів, мережеву адресацію, маршрутизацію і упаковку даних для передачі. Надалі, кожен з них буде обговорюватися.

Інтернет-протокол IPv4 або IPv6, несуть відповідальність за фрагментацію пакетів для передачі і збірку пакетів після отримання. Обидва протоколи забезпечують надійну доставку без встановлення з'єднання.

Основна відмінність між ними полягає в форматі адреси. IPv4, оригінальний протокол Інтернет, використовує 32-бітову адресу. Його, як правило, записують в десятковій нотації, як показано нижче: **192.168.10.42**

IPv4 як і раніше використовується в більшості випадків, але Інтернет в перспективі припиняє працювати з адресацією IPv4, оскільки вона має обмежений характер. З цієї причини був розроблений протокол IPv6, він розширює адресний простір, забезпечуючи 128-бітову адресу, представлений у вигляді серії шістнадцятирічних чисел: **fe80: d46f: 5f6c: bff1: 30db**

Мета реалізації TCP/IP, в тому числі в Інтернеті, є поступовий перехід від IPv4 до IPv6. Більшість мережевих пристроїв в даний час підтримує як IPv4, так і IPv6. Операційні системи налаштовують хости як з IPv4, так і з IPv6. Проте, адреси IPv6 в значній мірі ігноруються, оскільки вони в даний час не потрібні в більшості мережевих середовищ.

Для підтримки IPv4 або IPv6 протоколи, які реалізуються на більш високих рівнях моделі TCP/IP, не потрібно змінювати, якщо вони не дають інформації про адресу.

ARP

Один из протоколов, который выполнен на уровне Интернета и заслуживает особого упоминания, является ARP. Есть версия ARP: в IPv4, так и IPv6. В каждом случае его основная функция заключается в отображении IP-адресов в MAC-адресах.

 ***Address Resolution Protocol (ARP)*** *- протокол TCP/IP, который предназначен для разрешения IP-адресов/MAC-адресов.*

Інформацію про MAC-адреси збирають шляхом використання широкомовних передач. Щоб зменшити кількість передач, кожен хост має свій власний кеш ARP. Ви можете ввести інформацію про адресу в кеші статично, але більша частина інформації зберігається динамічно в результаті трансляції ARP.

Ви можете переглянути вміст ARP кеша, виконавши наступну команду:
arp – a

Результати будуть унікальні для кожного вузла, але список типових результатів дасть вам уявлення про те, чого очікувати в таблиці ARP.

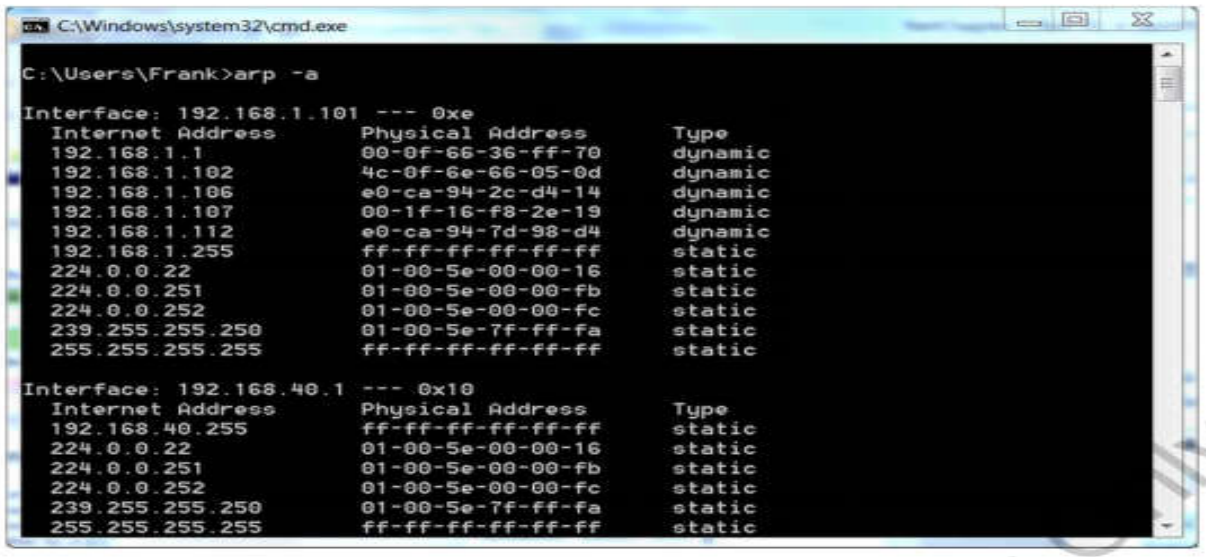


Рисунок 1.5 - Приклад таблиці ARP

Зверніть увагу, що кожен запис ідентифікує IPv4-адресу, фізичну адресу (MAC-адресу) і тип адреси: динамічний або статичний. Адреси призначаються або динамічно, або вони налаштовані як статичні адреси.

Транспортний рівень

Транспортний рівень TCP/IP (також відомий як хост-хост транспортного рівня) несе відповідальність за ту ж функціональність, що і транспортний рівень моделі OSI. Деякі функції сеансового рівня OSI також забезпечується через транспортний рівень. Транспортний рівень TCP/IP забезпечує сесії і дейтаграмні послуги для TCP/IP прикладного рівня.

Дейтаграма *- пакет даних, що містить пункт призначення і інформацію маршрутизації.*

Два основних протоколи реалізовані на рівні транспортному TCP/IP:

• транспортний протокол управління (TCP);

• протокол дейтаграм користувача (UDP).

Обидва вони можуть бути реалізовані за протоколами IPv4 і IPv6. TCP і UDP будуть детально обговорені далі, але їх швидкий огляд допоможе вам зрозуміти, що відбувається на цьому рівні.

TCP

TCP є протоколом, орієнтованим на з'єднання. Іншими словами, це забезпечує надійний зв'язок (один до одного) між двома вузлами мережі:

• Встановлення з'єднання між хостами;

• Підтвердження послідовностей пакетів, що пересилаються між хостами;

• Відновлення втрачених пакетів (через ретрансляцію).

Для забезпечення доставки даних, TCP використовується щоразу, коли це необхідно.

UDP

UDP є протоколом без встановлення з'єднання. Він може бути використаний в режимі передачі один-до-одного або один-ко-багатьох (трансляція). Оскільки UDP не вимагає з'єднання, він не гарантує надійну доставку, хоча надійний зв'язок може бути реалізований за допомогою протоколів більш високого рівня, які використовують UDP для доставки. Як правило, UDP використовується, при малих об'ємах даних (не більше одного пакета).

Прикладний рівень

Прикладний рівень відповідає за функціональні можливості, що надаються сеансовим рівнем, рівнем представлення і прикладним рівнем додатків моделі OSI. Це інтерфейс між користувачами і додатками комп'ютера і мережевих послуг, що надаються TCP/IP. Велика кількість протоколів реалізовані на цьому рівні. Деякі з найбільш відомих мають справу з обміном інформацією, включаючи HTTP, який є частиною Wide Web (WWW).

 ***Протокол передачі гіпертексту (HTTP)*** *- протокол високого рівня TCP/IP, що дозволяє використовувати веб-браузер для запиту і отримувати дані з веб-сайту.*

Прикладний рівень також включає в себе кілька протоколів управління, використовувані для таких цілей, як:

Дозвіл імен хостів в IP-адреси;

Підтримка і обмін інформацією про маршрут між маршрутизаторами;

Автоматичне надання інформації про конфігурацію мережі для хост-комп'ютера.

Протоколи, які реалізовані на прикладному рівні можуть дозволяти створювати навіть каталог пристроїв, розгорнутих в мережі. Ця можливість дозволяє адміністратора створити карту мережі.

Технології Ethernet

Ethernet представляє собою протокол зв'язку низького рівня, який реалізується на фізичному і канальному рівні моделі OSI або на рівні мережного інтерфейсу моделі TCP/IP, в залежності від контексту. Це означає, що Ethernet відповідає за визначення такої стандартної інформації, як:

- середове передачі і типи роз'ємів;
- довжина кабелю сегмента;

- передачі сигналів (стійкість і формат);
- формат кадру;
- метод доступу до мережі.

Ethernet, в даний час, є найбільш часто використовуваний стандарт обміну даними для технологій локальних мереж. Однією з причин цього є те, що Ethernet, в його нинішньому вигляді, це стандартизована технологія, заснована на стандарті IEEE 802.3. Ethernet вперше був введений в систему особистої залежності. Першими розробниками є компанія Xerox. Надалі Intel, Digital Equipment Corporation (DEC) і Xerox працювали разом, для просування Ethernet як стандарт, в порівнянні з конкуруючими технологіями, в тому числі Token Ring (IBM).

До 1980 року, Ethernet був явним переможцем. Сьогодні, рідко можна зустріти інші протоколи низького рівня, і тільки в дуже спеціалізованих мережах, наприклад на деяких системах управління виробничим процесом.

Ethernet став настільки поширеним, що більшість виробників вбудовують мережевий адаптер Ethernet (або NIC) безпосередньо в материнську плату комп'ютера для настільних і переносних комп'ютерів.

Технічні характеристики Ethernet

В оригінальних реалізаціях Ethernet використовується коаксіальний кабель. Перші стандарти коаксіального кабелю були відомі як:

10Base5 - Товстий Ethernet або Thicknet

10Base2 - Тонкий Ethernet або Thinnet

Коаксіальний кабель - *кабель з центральним металевим сердечником, який переносить сигнал, оточений ізолятором і металевою оболонкою.*

Терміни Thicknet і Thinnet позначають товщину коаксіального кабелю. Обидва стандарти підтримують швидкість передачі даних до 10 мегабіт в секунду (Mbps). Типи 10Base5 і 10Base2 використовувати різні з'єднувачі. 10Base5 використовує підключення AUX, а 10Base2 використовує роз'єм BNC.

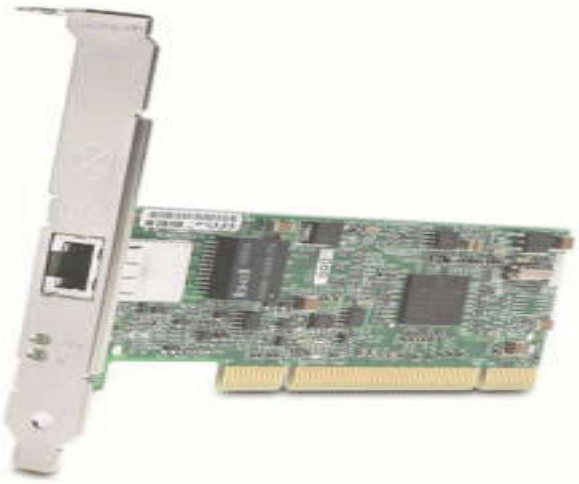


Рисунок 1.6 – Мережевий адаптер

Ви навряд чи коли-небудь стикалися з мережею, яка використовує Ethernet через коаксіальний кабель. Зараз стандартом є Ethernet по мідній кручений парі, хоча оптоволоконний кабель також використовується в високошвидкісних мережах і мережах з високим рівнем безпеки.

Тому мережеві плати Ethernet більше не поставляються з AUX або BNC з'єднувачами. Вони мають RJ-45 модульний адаптер (як показано на малюнку 1.6), волоконно-оптичний адаптер, або обидва адаптера. Нові комп'ютери мають RJ-45 з'єднувач, який вбудований в материнську плату, і вони можуть також мати оптичний з'єднувач.

Перший стандарт Ethernet який використовує виту пару був відомий як StarLAN і був обмежений швидкістю 1 Mbps. Оскільки технології покращилися, і потреби користувачів еволюціонували, утворилося безліч Ethernet стандартів. Популярні стандарти наведені в таблиці 1.1:

Табл. 1.1 - Популярні стандарти

Name	Data rate	IEEE Standard	Note
10BaseT	10 Mbps	802.3i	Requires two twisted pairs
100BaseT	100 Mbps	802.3u	Requires two twisted pairs
1000BaseT	1 Gbps	802.3ab	Requires four twisted pairs
10GBaseT	10 Gbps	802.3an	Requires four twisted pairs

Більшість комутаторів розроблені, щоб дозволити вам використовувати кросово або пряме підключення кабелю. ПІН-аут для кручений пари залежить від застосування кабелів.

У кабелі прямих підключень, пари на прийом і передачу підключаються до таких же контактам на обох кінцях, як показано на Рисунок 1.7.

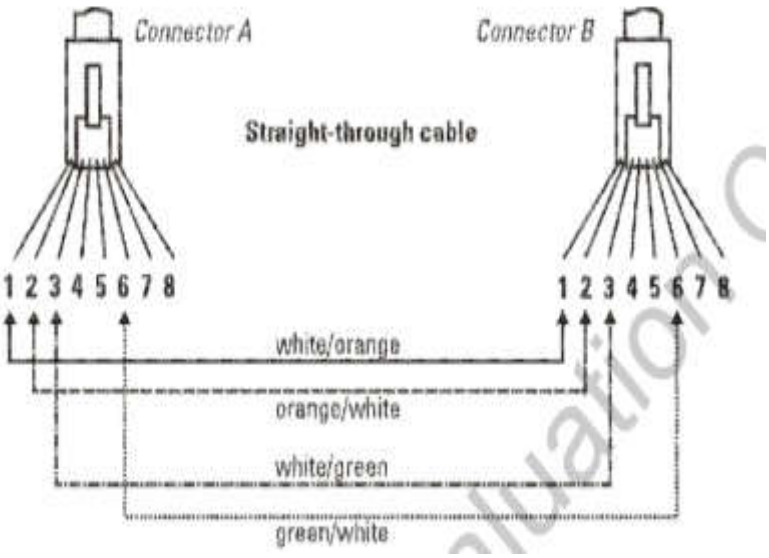


Рисунок 1.7 – Пряме подключение кабеля

При прямому підключенні кабелю, функції (прийом або передача) протилежні на кожному кінці RJ-45 (Рисунок 1.8).

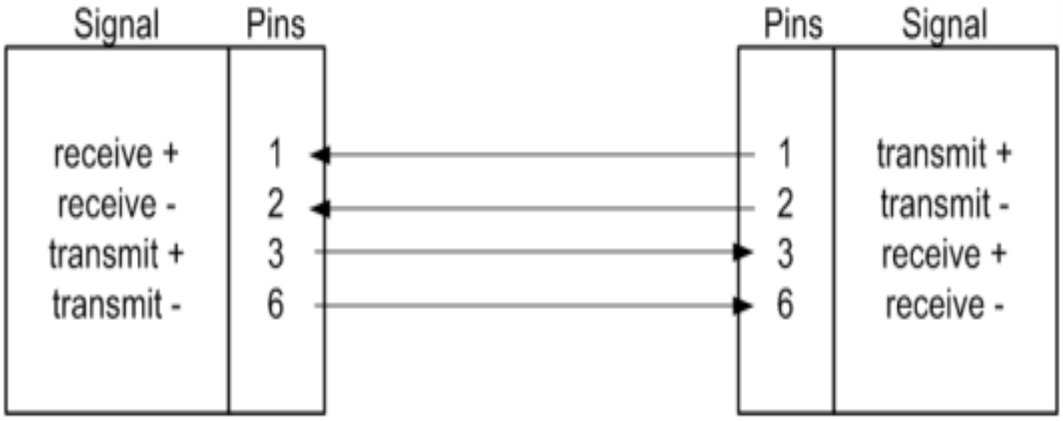


Рисунок 1.8 – Схема контактів при прямому підключенні

Пряме підключення контактів використовується з чотирма крученими парами, тобто використовуються всі вісім контактів (Рисунок 1.9).

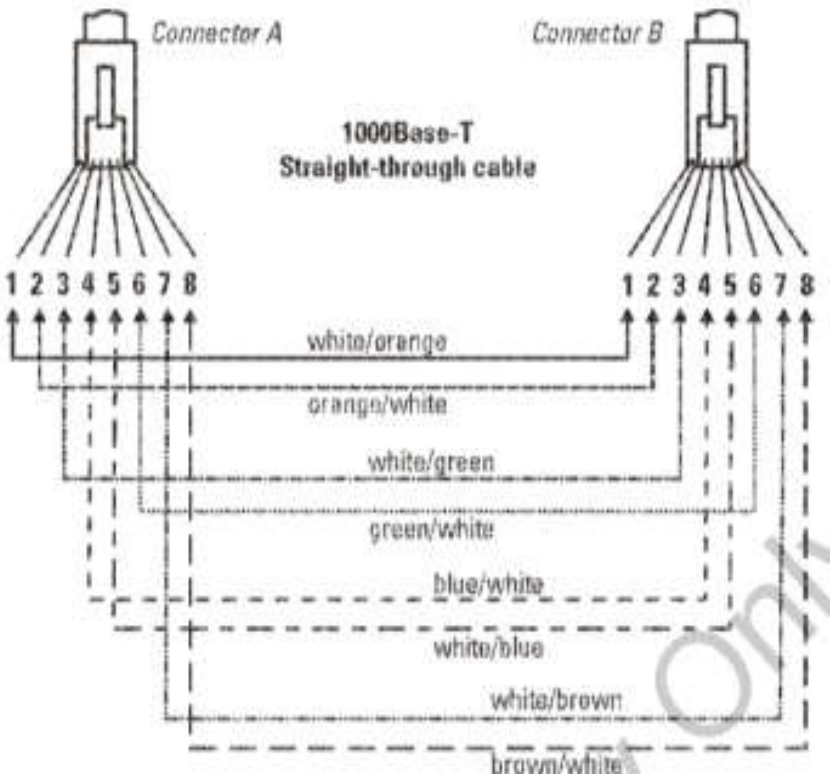


Рисунок 1.9 – Стандарт 1000BaseT с прямим подключенням кабелю

При перехресному підключенні кабелю (Рисунок 1.10) пари відправки та отримання обмінюються місцями, так що пара передачі на одному кінці підключена як пара прийому на іншому кінці.

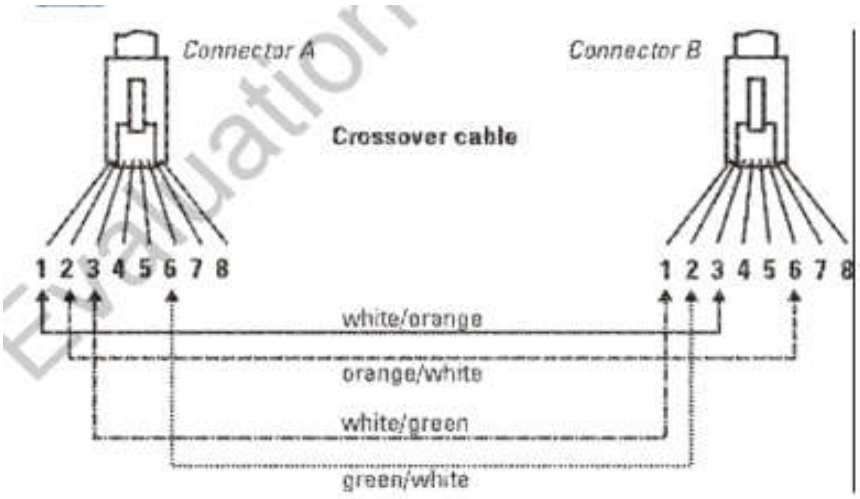


Рисунок1.10 – Перекрестное подключение

При використанні кросовера, вихід RJ-45 визначається розташуванням контактів на обох кінцях. Контакти які на одному кінці є передавальними, на іншому є приймальними (Рисунок 1.11).

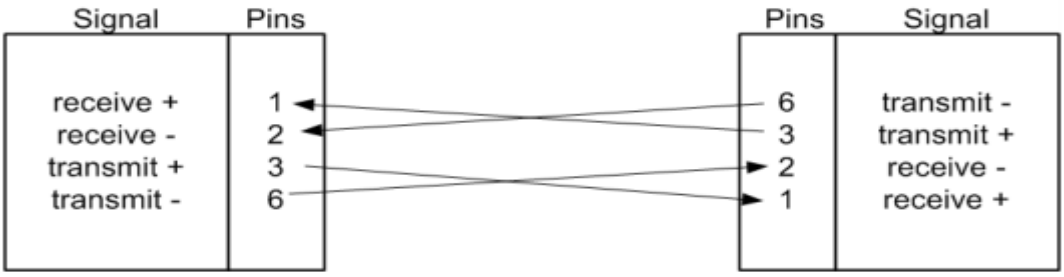


Рисунок 1.11 – Схема контактів при перехресному підключенні

Стандарти Ethernet на 40 Гбіт і 100 Гбіт знаходяться в стадії розробки.

Існують такі ж стандарти для Ethernet по оптоволоконному кабелю. Волоконно-оптичний кабель має ряд привілеїв: більш висока швидкість, стійкість до ЕМП, довжина кабельних сегментів більше 20 км в довжину.

Електромагнітні перешкоди (ЕМП) *- електромагнітне поле радіочастотного спектру, що викликає перешкоди.*

Типи трафіку Ethernet

Перш ніж ми розглянемо як управляється зв'язок Ethernet, ми зробимо швидкий огляд видів Ethernet трафіку. Є чотири основних типи трафіку:

Unicast (одноадресна) - посилається по одному конкретному хосту, ідентифікованого за певною адресою.

Broadcast (широкомовний) - посилається по всіх вузлах мережі або сегментам мережі без урахування адреси вузла.

Multicast (багатоадресну) - посилається за ідентифікованою групі хостів в групі, це ефективна група розсилки.

Anycast - посилається першому сервера в групі розподілу, а не всім членам групи.

Як правило, більша частина трафіку в мережі це одноадресний трафік, зв'язок між вузлами будується за принципом один-до-одного. У комутованій мережі, трафік фільтрують і направляють на комутатор.

Широкомовний трафік, як правило, пов'язаний з мережевою управлінською діяльністю. Всі хости можуть потенційно отримувати і, в свою чергу, обробляти трафік. ARP, наприклад, використовує широкомовну передачу для вирішення MAC-адрес.

Багатоадресний трафік схожий на широкомовний трафік, він будується на кшталт один-до-багатьох. Різниця між ними полягає в тому, що дані в багатоадресного трафіку призначені для конкретних хостів. Перевага багатоадресного трафіку перед одноадресна трафіком є те, за одну передачу передаються дані відразу декільком адресатам.

Anycast трафік також відправляється в групу розсилки, яка представляє собою набір вузлів, будь-який пристрій яких має однакову адресу призначення. Проте, трафік обробляється першим хостом прийому передачі. Anycast найбільш часто використовується в управлінні інформацію про маршрут і доступності маршрутизатора.

Зв’язок за допомогою Ethernet

Для передачі по Ethernet дані форматуються в кадри, як показано на Рисунку 1.12

Рисунок 1.12 – кадр Ethernet

Кожен кадр починається з преамбули і роздільника початку кадру. Далі слідують MAC-адреса джерела і MAC-адреса призначення. Кадр може також включати в себе тег визначення приналежності VLAN. Кадр також ідентифікує тип протоколу, вбудованого в корисне навантаження, за яким слідують корисні дані.

Стандарти для кадрів є до 1500 байт корисного навантаження, яка є частиною даних кадру Ethernet. Весь розмір кадру 1518 байт. Нові пристрої, в тому числі комутатори Gigabit Ethernet, підтримують великі кадри до 9000 байт даних.

Jumbo Frame - кадр Ethernet, що використовується з IPv4 і IPv6, має можливість переносити до 9000 байт даних.

Нездатність більшості мережевих пристроїв підтримувати Jumbo кадри затримало їх застосування в більшості мереж.

CSMA/CD

Ethernet використовує метод доступу до мережі, відомий як CSMA/CD (Carrier Sense Multiple Access with Collision Detection). З CSMA/CD, хост спочатку виявляє передає чи в даний момент інший хост. Якщо середовище вільне, він буде передавати свій кадр. Це було великою проблемою в початкових мережах Ethernet, які поділяли з'єднання коаксіального кабелю або, були підключені через концентратор.

Множинний доступ до несучої з виявленням колізій (CSMA/CD) - метод доступу до мережі, який використовується протоколом Ethernet, що підтримує загальний доступ до засобів масової передачі.

Головний недолік CSMA/CD в тому, що кілька вузлів намагаються передавати одночасно. Це відомо як колізія і призводить до пошкодження всіх кадрів, переданих в той час.

Коли відбувається колізія:

• Всі задіяні хости припиняють передачу.

• Обидва кадри відкидаються.

• Обидві станції будуть чекати протягом рандомного часу і будуть намагатися передавати, поки не передадуть кадр успішно.

Як правило, хост налаштований на максимальну кількість спроб передачі. Якщо цей показник буде досягнутий протягом одного кадру, кадр відкидається і передача даних переривається.

Сьогодні більшість мереж Ethernet побудовані із застосуванням комутаторів, так що цей загальний метод доступу до середовища не застосовується. Трафік передається через відповідний порт на комутаторі, так що інші пристрої не поділяють з'єднувальний кабель до місця призначення.

Основні мережеві пристрої

Якщо мережа стає все більше, з великою кількістю (і більш активних) хостів, колізія може стати серйозною проблемою і значно погіршити продуктивність мережі. Тим не менш, ви можете контролювати і розділяти мережевий трафік, створюючи домени колізій через пристрої зв'язку встановлені в мережі.

Домен колізій - *група Ethernet вузлів безпосередньо пов'язаних на фізичному рівні, які можуть перешкодити комунікацій один одного.*

У більшості базових конфігурацій, всі комп'ютери в мережі підключаються безпосередньо до мережі. Кожен вузол має рівний доступ до мережі. Весь трафік передається з кінця в кінець по мережі кабельного сегмента.

Коли ви сегментуєте мережу за допомогою пристроїв рівня 2 або рівня 3, необхідно створити домен колізій. За допомогою сегментування мережі за цією методикою, пристрої будуть поширювати трафік через мережу, уникаючи зіткнень. Домени колізій можуть значно поліпшити продуктивність мережі.

Традиційно, домени колізій встановлюються на основі фізичного розташування хостів. Кожен хост розташований по одній або іншій стороні пристрою. Комутатори також можуть дозволити вам створювати домени колізій

певних портів на комутаторі. Проте, комутатори пішли ще далі в запобіганні зіткнень при буферизації трафіку на порту.

Пристрої, які працюють на фізичному рівні, для запобігання колізій нічого не роблять. Найбільш поширеними пристроями цього типу є повторювачі і концентратори. Обидва пристрої передають трафік без урахування адреси призначення.

Пристрої, які працюють на канальному рівні управляють трафіком на основі MAC-адреси. Пристрої на цьому рівні включають шлюзи і комутатори рівня 2. Ці пристрої можуть пропускати або блокувати трафік на основі MAC-адреси призначення. Пристрої другого рівня, як правило, пропускають весь широкомовний трафік.

Пристрої, які працюють на мережному рівні керують трафіком на основі мережевої адреси. У разі TCP/IP, управління трафіком проводиться на основі IP-адреси. Трафік направляється, проходить, або блокується на основі адреси призначення. За замовчуванням, маршрутизатор блокує більшість (або весь) широкомовний трафік, створюючи широкомовні домени.

Безпроводові технології

Бездротові мережі працюють по повітрю, або, точніше, передача радіохвиль здійснюється по повітрю, він виступає в якості їх засобу передачі. Ця особливість дає вам можливість розгорнути мережі там, де неможливо провести кабель і забезпечує раніше неймовірну гнучкість в пошуку і підключенні до мережі.

Сучасні бездротові локальні мережі засновані на стандартах IEEE 802.11. Як і 802.3, специфікація 802.11 визначає кілька стандартів. Специфікації 802.11 часто дає прилади потенціалу для підтримки більш ніж одного стандарту одночасно. Ви частіше чуємо термін Wi-Fi, який використовується для опису мережі, заснованої на стандартах 802.11

Спочатку бездротові мережі 802.11 були розгорнуті в першу чергу як приватні мережі, або мережі всередині будинку або в офісі. За останні кілька років громадські Wireless Fidelity (Wi-Fi) мережі (гарячі точки) стали звичайним явищем. Більшість навчальних закладів, багато ресторанів (в тому числі ресторани швидкого харчування), і інші громадські місця, наприклад бібліотеки і аеропорти, дають доступ громадськості до Інтернету через їх точки доступу Wi-Fi.

Використання широкосмугового бездротового підключення до Інтернету в даний час стали дуже поширеним явищем. Ця бездротова технологія заснована на мобільних технологіях 3G (третього покоління) і 4G (четвертого покоління). Пристрої підключаються до Інтернету через бездротові мережі стільникового зв'язку. Стандарт 3G розроблений для підтримки теоретичної максимальної пропускної спроможності 100 Мбіт/с. У практичних додатках його ефективна пропускна здатність значно менше, а максимальна пропускна здатність рідко перевищує 47 Мбіт/с.

Пристрої 4G мають максимальну пропускну здатність при русі (наприклад, в транспортному засобі) 100 Мбіт/с, а при нерухомому стані їх максимальна пропускна здатність становить 1 Гбіт/с. Цей дизайн підтримує безшовну передачу, так як пристрій переміщається по географічній області, що дозволяє пристрою ніколи не втрачати з'єднання до тих пір, поки воно залишається в зоні обслуговування.

Основи комунікацій

Бездротова мережева плата складається з радіопередавача і приймача які працюють в певному діапазоні частот, в залежності від стандарту або стандартів, які підтримує бездротова мережа. Мобільні комп'ютери і більшість настільних комп'ютерів поставляються з вбудованим Wi-Fi модулем. Інші пристрої, такі як медіа-плеєри і смартфони, також в даний час широко підтримують Wi-Fi мережі, а також широкосмуговий доступ 3G або 4G.

Частота - *величина, що виражає число повторень в одиницю часу, вимірюється в герцах (Гц).*

Смартфон - *мобільний телефон, який працює на мобільній обчислювальної платформі, забезпечуючи роботу комп'ютера через телефон.*

Всі бездротові пристрої можуть приймати передачу, але чи можуть вони що-небудь робити з інформацією, що передається чи ні, залежить від конфігурації

пристрою і мережі. Більшість конфігурацій бездротової мережі 802.11 засновані на одній або більше точок доступу (AP). AP виступає в якості центральної точки доступу для бездротових хостів. Замість прямого зв'язку один з одним, хости взаємодіють через точку доступу.

Кількість і розміщення точок доступу в мережі в першу чергу залежить від кількості і розміщення бездротових пристроїв. AP також може приєднувати комп'ютери до бездротової мережі. Вони також дозволяють комп'ютерам в проводовій мережі взаємодіяти один з одним.

Стандарти безпроводових мереж

Стандарти 802.11 перелічені в таблиці.

802.11 Standard	Frequency	Maximum data rate
802.11a	5 MHz	54 Mbps
802.11b	2.4 MHz	11 Mbps
802.11g	2.4 MHz	54 Mbps
802.11n	2.4/5 MHz	Up to 600 Mbps

Швидкості передачі даних засновані на ідеальних умовах. Типові швидкості передачі даних в більшості реалізацій будуть менше, ніж максимальні. Пристрої 802.11g сумісні з пристроями стандарту 802.11b. Пристрої 802.11n сумісні з пристроями 802.11a, 802.11b, 802.11g.

Всякий раз, використовуючи смугу 2,4 МГц, існує потенціал для перешкод з іншими пристроями, що працюють на тій же частоті. Це включає в себе пристрої Bluetooth, бездротові клавіатури, бездротові миші і монітори безпеки, мікрохвильові печі.

CSMA/CA

Як і Ethernet, пристрої 802.11 передають дані в вигляді кадрів. Вони схожі на кадри даних Ethernet і виконують ту ж функцію. Вони призначені для організації даних для передачі.

Метод доступу до мережі використовується 802.11 є CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance), який працює дещо по іншому, ніж

CSMA/CD. Причина, по якій CSMA/CD не використовується є та, що передавальна станція не може знайти колізію.

Множинний доступ до несучої з уникненням колізій (CSMA/CA) - метод доступу до мережі, використовується в бездротових мережах стандарту 802.11, який дає їм змогу розділяти частотний діапазон загального середовища передачі.

При CSMA/CA, хост прослуховує протягом заданого періоду часу, щоб забезпечити наявність каналу, який він буде використовувати для передачі. У більшості реалізацій, відправляється запит про відправку сигналу (RTC) - інформування інших вузлів про свій намір передати. Хост, який посилає, чекає сигнал (CTS - clear-to-send) для початку передачі.

Основи безпеки

Безпека є постійною проблемою в майже будь-якому мережевий середовищі. З огляду на це, безпеку буде розглянута дещо пізніше протягом цього курсу. В даний час, наша дискусія обмежиться коротким введенням в концепції безпеки. Ми орієнтуємося на двох ключових областях:

Аутентифікація і ресурс доступу.

Дані і безпеку зв'язку.

У реальних додатках, ви побачите, що ці дві складові часто перетинаються і не можуть бути легко розділений.

Основи аутентифікації

Якщо ви коли-небудь заходили на комп'ютер за допомогою пароля, ви взяли участь у процесі аутентифікації. Ім'я користувача і пароль, які ви вводили, порівнюються зі збереженою інформацією. Деякі форми аутентифікації звичайно потрібні при підключенні до мережі, запуску утиліт управління, або спробі отримати доступ до ресурсів, таким як файли. Досить часто різні види діяльності вимагають різних рівнів доступу і, в свою чергу, окремий аутентифікації.

Для користувачів, аутентифікація, як правило, на грунтується на наступному:

Що ви знаєте;

Що у вас є;

Хто ви.

"Те, что ви знаєте," как правило, відноситься до паролю, PIN-коду або іншої информації, яку знаєте тільки ви. Фахівці, для забезпечення безпеки, не використовують однофакторну аутентифікацію як єдиний спосіб захисту. Паролі не складно підібрати, особливо коли користувачі вибирають прості, легкі для підбору паролі.

Персональний ідентифікаційний номер (PIN-код) - числове значення, використовується для перевірки ідентичності.

Однофакторна аутентифікація - аутентифікація на основі тільки одного типу фактору аутентифікації.

"Те, що у вас є" відноситься до якогось типу маркера фізичної безпеки, наприклад смарт-карти, посвідчення, ключа, або іншого фізичного пристрою. Ви повинні надати один з цих фізичних пристроїв, перед процедурою аутентифікації.

"Хто ви" відноситься до біометричної інформації. Сканери відбитків пальців і сітківки стають звичайним явищем в додатках середнього і високого рівня безпеки. Деякі пристрої безпеки навіть розраховані на послідовностях ДНК. Багато ноутбуки та клавіатури тепер поставляються з вбудованим сканером відбитків пальців.

Біометрична інформація - *інформація заснована на фізичних характеристиках.*

Іноді використовується четвертий фактор, який використовується для аутентифікації "то, що ви можете зробити", він базується на визнанні тебе по діяльності.

Загальний підхід до підвищення безпеки покладається на багатофакторну аутентифікацію. Наприклад, можна вимагати смарт-карту і пароль, або посвідчення і відбиток, перш ніж дозволити доступ.

Багатофакторна аутентифікація - *аутентифікація вимагає, принаймні два типи перевірки автентичності, облікових даних для виконання перевірки автентичності. Наприклад, те, що ви знаєте, (ПІН-код) і щось у вас є (смарт-карта).*

Більшість систем захисту мережі визначають, до яких ресурсів ви можете отримати доступ і які рівні доступу доступні для вас. Вам можете бути надано доступ на рівні читання/запис ваших власних файлів, що зберігаються в мережі, але обмежений доступ на читання інших файлів. Як правило, ви не будете мати доступу до більшості файлів.

Аутентифікація не обмежує користувачів. Багато сучасних мережевих активів і програм, перш ніж дозволити комп'ютерам встановити сеанс зв'язку, перевіряють комп'ютери на справжність. Бездротові мережеві точки доступу зазвичай налаштовані на вимогу перевірки автентичності хоста, перш ніж дозволити підключення.

Введення в безпеку даних

У широкому сенсі, безпека даних пов'язана з:
запобіганням впливу на дані;
запобіганням пошкодження даних.

У більшості мережевих систем використання шифрування даних відіграє центральну роль в забезпеченні безпеки.

Дані зберігаються в зашифрованому вигляді на диску. Навіть якщо неавторизований користувач (або програма) отримали доступ до місця зберігання файлу, файл як і раніше буде захищений шифруванням.

Шифрування - *процес представлення даних в нечитабельному виді з використанням алгоритму, технологій і знань, необхідних для повернення процесу назад.*

Безпека зв'язку може також запобігти несанкціонованому доступу до даних. Деякі мережеві протоколи, наприклад HTTP, FTP, передають дані в вигляді тексту. Проте, цей формат не є безпечним, оскільки дані можуть бути перехоплені третьою стороною. В правильно захищеній мережі, вживаються заходи для того, щоб дані були зашифровані для передачі, навіть коли здійснюється передача по внутрішній кабельній мережі. HTTPS і FTPS є захищеними версія цих протоколів.

Протокол передачі файлів (FTP) - *за своєю суттю небезпечний протокол передачі даних, зазвичай використовується для завантаження файлів з і на сервер в Інтернеті.*

Введення в VLAN

На початку роботи мережі, може бути організовано тільки фізичне розташування мережевих вузлів. Це обмеження було подолано з введенням VLAN. Старі мережеві проекти використовують шлюзи і маршрутизатори для створення кордонів між хостами. Сучасні комутатори забезпечують сегментацію через VLAN. VLAN виглядає як маршрутизована підмережа, так званою підмережею третього рівня, відносно до решти мережі. Кожна мережа VLAN має свій власний IP-адрес мережі з метою маршрутизації.

Статична VLAN є найпростішим типом VLAN. У цій конфігурації, порти комутатора призначені VLAN, створюючи еквівалент підмережі третього рівня. Якщо Ваш пристрій приєднаний до порту, він стає частиною локальної мережі для якої порт призначений.

Як правило, комутатор налаштований за замовчуванням як єдиний VLAN. Для створення нових мереж VLAN, ви повинні спочатку видалити порти з VLAN за замовчуванням. Ви навіть можете визначити порти з різних комутаторів як частина тієї ж VLAN.

VLAN також можуть бути створені і управлятися динамічно. Ви можете призначити порти до VLAN на основі таких факторів, як MAC-адресу підключеного комп'ютера або ім'я користувача, який використовується при вході на комп'ютер.

При використанні мереж VLAN в мережі Ethernet, кожен кадр містить у собі тег 802.1Q в кожному кадрі Ethernet, це призводить до збільшення загального розміру кадру до максимального 1522 байта. Інформація в тегу ідентифікує кадр як кадр VLAN і включає в себе інформацію ідентифікатора VLAN, щоб допомогти кадру досягти правильного призначення.

Розділ 2:
Основи мережевого обладнання

Вступ

Семирівнева модель OSI забезпечує стандартизовану структуру для мережевих пристроїв, а також їх функціональність. В цьому розділі ми разглянемо застосування на практиці моделі OSI і пристроїв що працюють на разних рівнях.

Ми звернемо увагу на певний конкретний тип пристрою – комутатор. За останні декілька років більшість комутаторов значно разширили свої можливості за рахунок добавлення функцій 2 і 3 рівнів, які в одночас поєднують властивості концентраторів, мостів, маршрутизаторів та інших пристроїв. Широке розповсюдження комутаторів в сучасних мережах робить їх одним з ключевих об'єктів досліджень.

В процесі вивчення цього курсу, Ви ознайомитеся з різними моделями комутаторів фірми Hewlett Packard. Більшість команд управління, а такж інтерфейс командного рядка є однаковими для різних комутаторів.

Мета

В цьому розділі ви дізнаєтеть, як:

- Визначити загальне призначення і використання основного мережевого обладнання, такого як: мережева карта; ретранслятор; концентратор; шлюз; комутатор; маршрутизатор.
- Побудувати карту апаратних пристроїв для будь-якого з рівнів моделі OSI.
- Разглянути процедури управління комутатором.
- Визначити інтерфейс управління.
- Описати призначення і використання журналів подій.

Загальне мережеве обладнання

Одним з критеріїв класифікації мережевого обладнання може бути рівень моделі OSI, на якому безпосередньо працює пристрій. Наприклад: Мережевий адаптер - працює на фізичному і канальному рівнях (1 і 2 рівні). Ретранслятор - працює на фізичному рівні (1 рівень). Концентратор - працює на фізичному рівні (1 рівень). Шлюз - працює на канальному рівні (2 рівень). Комутатор - традиційно працює на канальному рівні (рівень 2), а також виконує допоміжні функції на мережевому рівні (3 рівень).

Коли пристрій повідомляє, що працює на певному рівні, він реалізує функціональні можливості всіх нижчих рівнів. Наприклад, міст працює на

канальному рівні. Тим не менш, він був би марним, якщо б він не включав в себе функціонали першого рівня, які дають можливість підключатися і взаємодіяти, використовуючи мережі загального доступу.

Ми починаємо цей розділ з обговорення найпоширеніших видів мережевого обладнання, а також їх функціоналу. Це важливо, тому що ми будемо посилатися на ці пристрої протягом всього курсу.

Мережевий адаптер

На зорі мережевих технологій мережеві адаптери (мережеві плати) найбільш часто реалізовувалися в якості додаткових плат розширення. Вони були відносно дорогими і часто викликали труднощі в налагодженні. Як тільки мережеві комп'ютери стали більш поширені, в промисловості впровадили мережеві стандарти, ціни значно знизилися.

Вже через кілька років, мережі стали настільки поширеними, що настільні і портативні комп'ютери вже мають, щонайменше, один вбудований мережевий адаптер. Настільні ПК в основному мають вже вбудований Ethernet адаптер і порт RJ45. У ноутбуках вже зазвичай вбудований як дротовий, так і бездротової адаптер.

Розваги, в тому числі комп'ютерні ігри, є основною рушійною силою технічних інновацій. Багато комп'ютерів, призначені для серйозних професійних ігор, щоб відповідати потужності обробки деяких серверів.

Ви до сих пір можете купити карти розширення, які дозволять вам обладнати ваш комп'ютер додатковими дротовими або волоконно-оптичними Ethernet адаптерами. Деякі конфігурації системи вимагають кілька мережевих адаптерів. Наприклад, якщо ви плануєте використовувати ПК в якості провідного мережного маршрутизатора, вам буде потрібно як мінімум два мережевих адаптера, кожен з яких має власну мережеву адресу.

Однією з причин для встановлення нового мережевого адаптера, може виступати збільшення продуктивності мережі. Наприклад, ви можете оновити комп'ютери, побудовані на підтримку 100Base-T, таким чином, що вони зможуть підтримувати 1000BASE-T.

Також ви можете побачити мережевий адаптер у вигляді плати розширення при додаванні бездротового мережевого адаптера (Рисунок 2.1).

Рисунок 2.1 - Бездротовий адаптер

Найбільш популярним зараз способом розширення мережевої плати на ПК є підключення бездротового мережевого адаптера в USB порт (Рисунок 2.2). Як правило, встановлення полягає тільки в підключенні адаптера до комп'ютера, після чого комп'ютер сам виконає розпізнавання і налаштування.

Рисунок 2.2 – USB адаптер

Незалежно від того вбудований він або доданий, мережевий адаптер виконує ті ж функції для комп'ютера, що і інші мережеві пристрої. Мережевий адаптер має, як мінімум, MAC (Media Access Control) адресу, що використовується для ідентифікації та підключення пристрою до мережі передачі даних.

Повторювач

Повторювач, по своїй суті, є просто підсилювачем. Він працює на фізичному рівні, приймає сигнал, ретранслює його посиленням в інший сегмент кабелю. Традиційний повторювач має властивий йому недолік, який полягає в тому, що він підсилює все, що отримує. Якщо сигнал, що приймається з перешкодами, повторювач підсилює як сигнал так і шуми.

Шуми негативно впливають на корисний сигнал, так як вони можуть поглинати відбитий сигнал або вступати в інтерференцію з корисним сигналом, що негативно позначається на якості кінцевого (отриманого) сигналу.

Ретранслятори використовують для збільшення довжини сегмента мережі. Залежно від типу мережі, існують різні правила, формування кількості повторювачів між кінцевими точками, або вузлами, в мережі. На початковому етапі розвитку Ethernet, можливо було підключити до п'яти відрізків кабелю з чотирма повторювачами (Рисунок 2.3). Тільки три сегменти могли мати всі підключені пристрої, і вони повинні були бути розділені за сегментами, без подключення пристроїв.

Іноді це правило називають «5 - 4 - 3». Правило Ethernet для використання ретрансляторів: п'ять сегментів, з'єднаних чотирма повторювачами з не більше ніж трьома сегментами з підключеними до них пристроями.

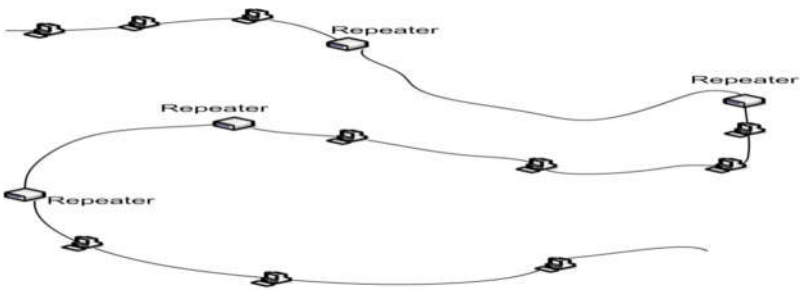


Рисунок 2.3: Правило 5-4-3

На сьогодні Ви ще можете побачити ретранслятори в сучасних мережах, але це досить таки рідкісне явище. Так як оптико-волоконний кабель несприйнятливий до електромагнітного випромінювання, на відміну від мідного кабелю, то сигнал на вході ретранслятора має кращі показники. Виходячи з цього, один з варіантів використання повторювачів в локальній мережі є розширення кабельних сегментів для волоконно-оптичних мереж.

Мережевий концентратор

Мережевий концентратор - пристрій, що працює на першому рівні моделі OSI. Концентратор являє собою центральну точку для підключення кабелів мережевих пристроїв (Рисунок 2.4). Він виконує функцію об'єднання пристроїв разом на електронному рівні, що дає їм рівний доступ до мережі. Крім того, сигнал не тільки регенерується, як у випадку зі стандартним аналоговим ретранслятором, а й посилюється. З точки зору передачі і можливих колізій, концентратор працює так само, як пристрої, що використовують коаксіальний кабель.

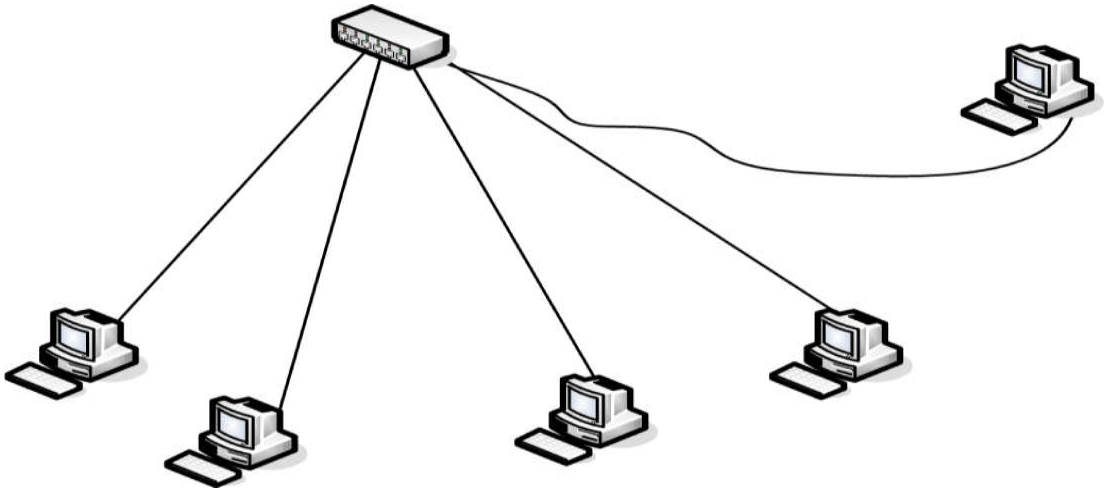


Рисунок 2.4 – Концентратор

Термін, який ми повинні пояснити в належному контексті це - порт. Ви дізналися в попередньому розділі, що порт може бути використаний разом з IP-адресою, щоб визначити кінцеву точку для передачі. Під час обговорення концентраторів і комутаторів, порт необхідний для реалізації фізичної зв'язку мережевих пристроїв.

Порт - зазвичай використовується для позначення точки підключення (як правило з'єднання RJ45) мережевих пристроїв Ethernet до концентратора або комутатора.

Більшість концентраторів мають в своєму складі порт для каскадного з'єднання зв'язку, що дозволяє розширити свою мережу шляхом підключення до інших мережевих пристроїв (Рисунок 2.5).

Порт для каскадного з'єднання забезпечує, і підтримує зв'язок з іншими мережами сполучних пристроїв.

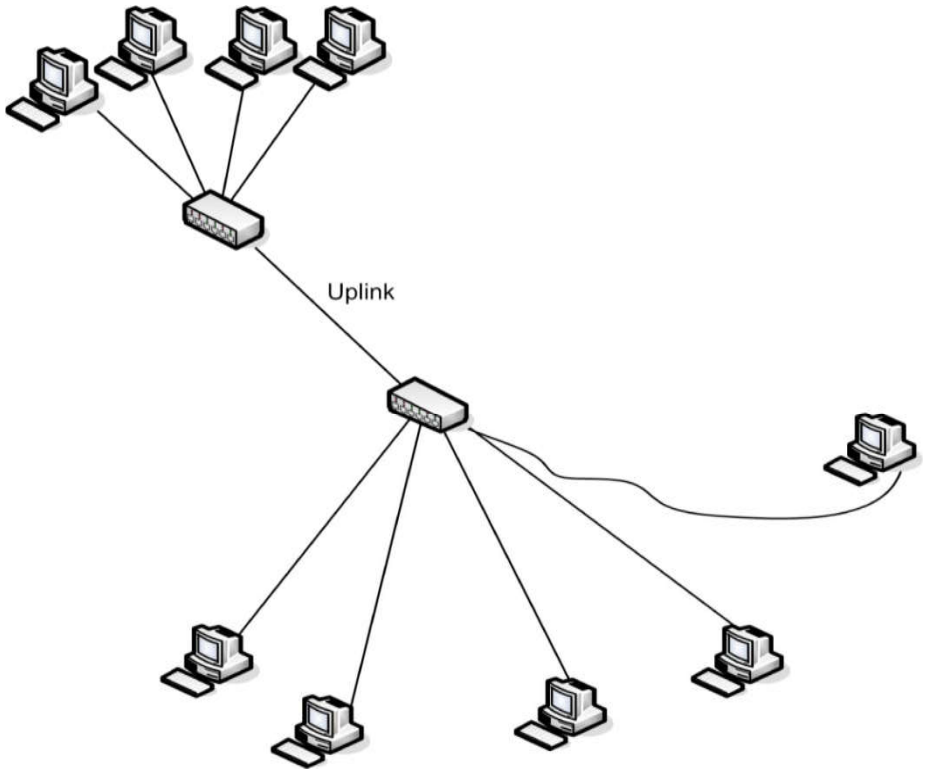


Рисунок 2.5 - Хаби з'єднані висхідною лінією порту.

Іноді ви можете побачити традиційні центри, іменовані не керованими вузлами. У такому центрі відсутня можливість, будь якої зміни параметрів вузла. На сьогоднішній день Ви рідко побачите концентратор в його класичному визначенні. Більшість сучасних концентраторів мають ряд додаткових функцій. Наприклад, концентратор виявляє швидкість, з якою працює мережевий адаптер і компенсує її, щоб дозволити комп'ютерам зв'язуватися один з одним, навіть коли комп'ютери використовують різні швидкості передачі. Деякі концентратори також підтримують функції віддаленого управління, такі, як можливість відключення порту. Наприклад, ви могли б застосувати це в разі якщо на комп'ютер, підключений до нього, не вдається відправити спотворені дані. При відключенні порту, можна ізолювати комп'ютер так, щоб він не заважав роботі мережі. Часто, це може бути зроблено віддалено, і при цьому немає необхідності фізично відключати комп'ютер.

Міст

Міст працює на другому рівні еталонної моделі взаємодії відкритих систем. Традиційно, його мета полягає в тому, щоб поєднати різні види медіа в єдину логічну мережу. Одним з варіантів використання може виступати необхідність об'єднання сегментів мережі, що працюють з різними типами кабелю (коаксіальний і вита пара) в одній підмережі з загальним мережевим адресою.

Підмережа - область мережі, що має унікальний мережеву адресу. Всі вузли в підмережі будуть мати туж саму мережеву адресу.

Міст приймає кадри від одного підключеного сегмента і визначає, чи передавати повторно кадр на інші підключені сегменти. Мостові фільтри направляють на основі MAC-адреси призначення.

Розглянемо ситуацію, в якій комп'ютер сегмента А передає кадр і пункт призначення до іншого комп'ютера в тому ж сегменті. Міст отримує кадр, але, так як адресат знаходиться на тому ж сегменті, а не в сегменті В, то виконується його знищення, а не передача на сегмент В (Рисунок 2.6). Проте, якщо міст бачить, що MAC-адреса призначення знаходиться в сегменті В, або, якщо він не визнає призначення, він пересилає кадр в сегмент В.

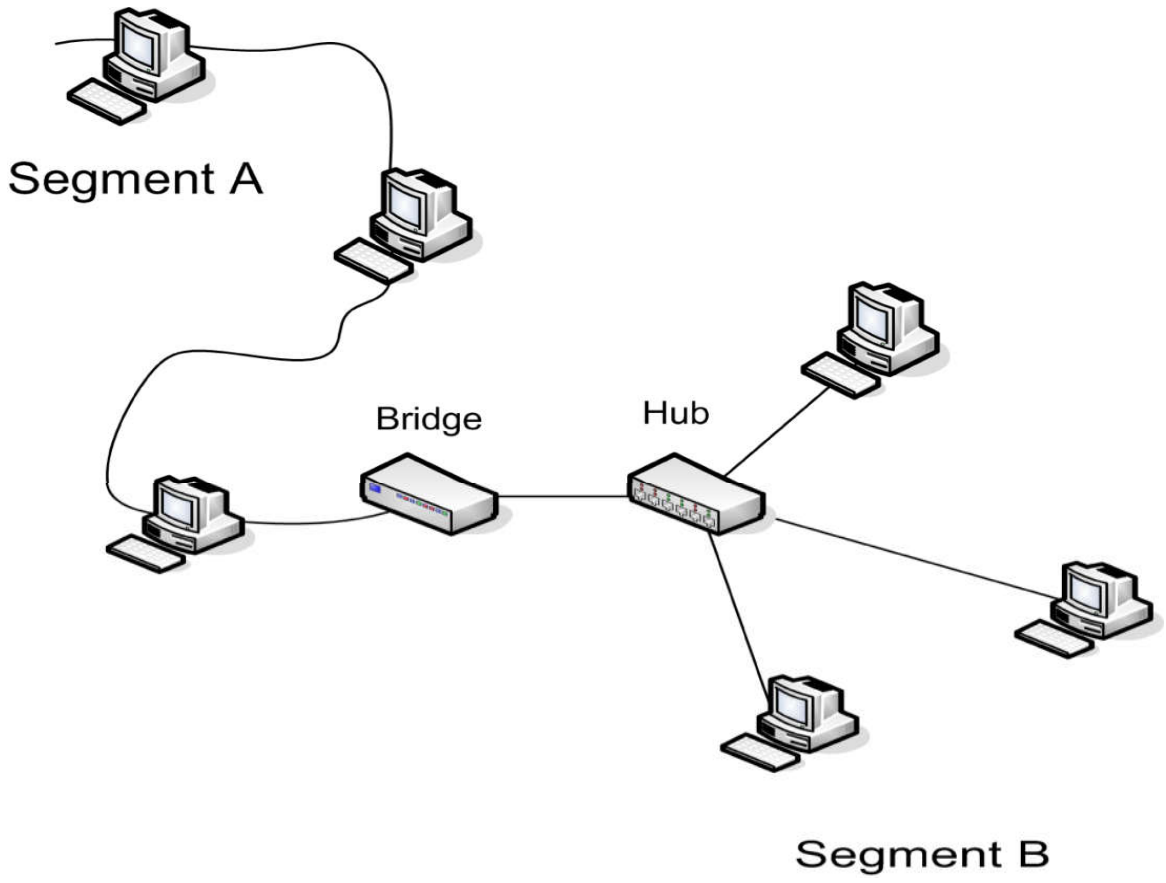


Рисунок 2.6 - Сегменти мосту

В процесі міст створює домени колізій, оскільки кадри відновлені, а не тільки проходять через міст. На рис. 2-6, дані комп'ютерів на відрізку А можуть увійти в колізію з даними інших комп'ютерів того ж сегмента, або мосту, але не з даними сегмента В.

Міст також виконує функції ретранслятора між сегментами, тому що вихідний кадр повторно передається, а сигнал - просто регенерується.

Мости допомагають керувати мережевим трафіком, але не у всіх ситуаціях. Широкомовний трафік не фільтрується мостами. На жаль, іноді пристрої невірно названі виробниками. Протягом багатьох років, пристрої, які насправді були мостами, були названі концентраторами (Рисунок 2.7).

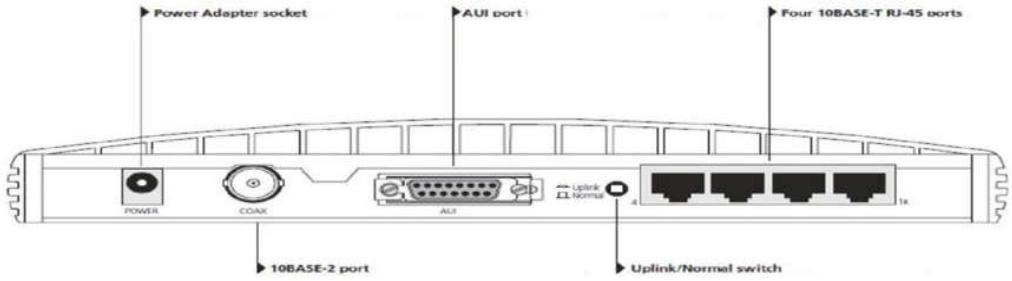


Рисунок 2.7 – Міст

Пристрій на Рисунку 2.7 є мостом. В класичному розумінні, він дозволяє підключати 10base2, 10base5 (через порт AUI) і 10Base-T сегменти мережі.

Комутатор

Комутатор швидко став популярним в сучасній мережі. Більшість сучасних комутаторів підтримують функціональність на 2 і 3 рівнях моделі OSI, що означає, що в інших пристроях часто немає необхідності, особливо в мережах малого і середнього бізнесу.

На перший погляд, багато невеликих комутатори виглядають як шлюзи. Однак всередині вони істотно відрізняються один від одного. Замість того щоб просто зв'язувати порти разом в електронному вигляді, комутатор діє як мультипортових міст. Це реалізується за допомогою буфера трафіку між портами, використовуючи технологію, відому як «store and forward» (зберегти і передати), що виключає зіткнення. Комутатор підтримує таблицю, яка відстежує MAC-адреси. Він визначає адресу призначення і перенаправляє трафік туди на основі MAC-адреси. Вона також дозволяє налаштувати віртуальні локальні мережі для управління мережевим трафіком і безпекою.

Комутатор третього рівня моделі OSI може бути налаштований для передачі трафіку з однієї підмережі в іншу. Комутатор, який включає в себе можливості третього рівня, іноді називають «routing switch» (комутатор маршрутизації).

Великі комутатори, як правило, являють собою модульні пристрої (Рисунок 2.8), які дозволяють налаштувати комутатор для ваших потреб на основі встановлених модулів. Ви можете почати з малого - одного або двох модулів, а також розширити комутатор в міру зростання мережі.

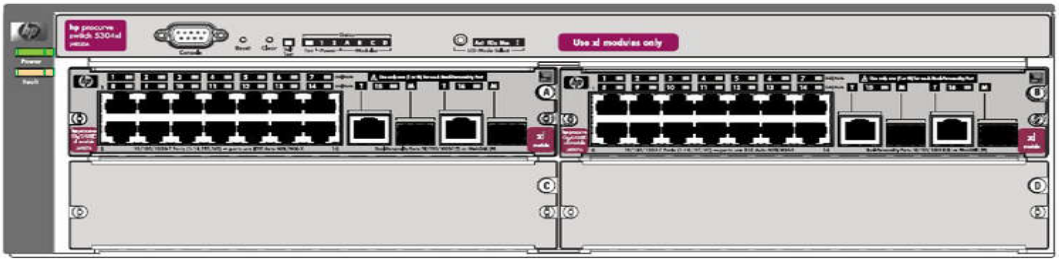


Рисунок 2.8 - Комутатор

Більшість комутаторів призначені для підтримки віддаленого управління. Це означає, що ви можете дистанційно керувати конфігураціями, а також оновити програмне забезпечення комутатора, зробити резервне копіювання інформації, управління діяльністю портів і так далі. Багато комутатори також забезпечують високий рівень безпечної зв'язку шляхом шифрування зв'язку з підключеними пристроями.

Маршрутизатор

У найпростішому вигляді, напрямна мережа побудована з двох або більше адресованих мереж 3 рівня, з'єднаних між собою маршрутизаторами (Рисунок 2.9). Кожен маршрутизатор має, принаймні, два порти (також звані інтерфейсами), кожен з яких має свій мережеву адресу. Маршрутизатор, призначені для використання по посиланнях WAN, як правило, підтримують додаткові функції, такі як здатність діяти в якості брандмауера або VPN кінцевої точки.

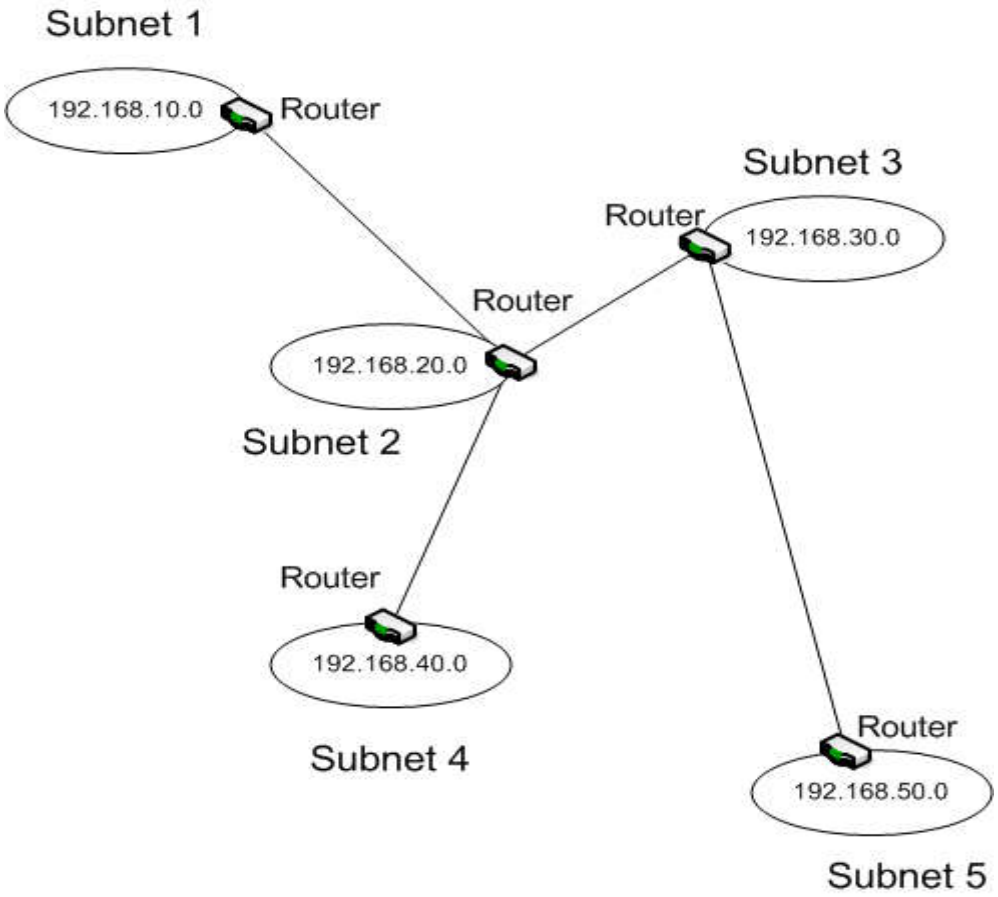


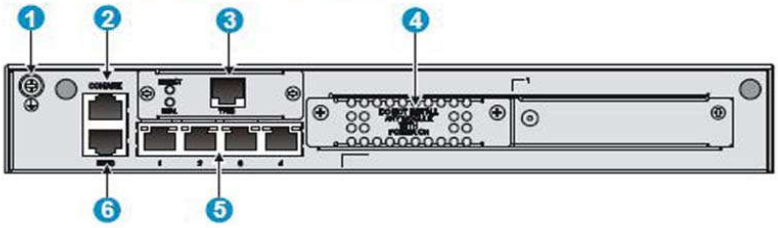
Рисунок 2.9 - Топологія мережі

У прикладі, показаному на Рисунку 2.9, маршрутизатор в підмережі 3 має три доступних порти, що дозволяє підключити до IPv4 підмережі 2, 3 і 5. Маршрутизатору в підмережі 2 буде потрібно чотири порти для підмереж 1, 2, 3 і 4.

Коли пакет приходить на маршрутизатор, він визначає адресу призначення і пересилає пакет через відповідний порт в мережі призначення для доставки. Залежно від типу маршрутизатора, його дії можуть відрізнятися. Вони залежать від інформації в пакеті, такої як адреса джерела або данні, що містяться в пакеті.

(1) Power switch	(2) Power receptacle	(3) USB port
(4) Reset button		

Figure 10 A-MSR20-12-T rear panel



(1) Grounding screw	(2) Console/AUX port	(3) T1 port TPRI0
(4) SIC/DSIC slot	(5) Ethernet LAN ports (ETH1 to ETH4)	(6) Ethernet WAN port ETH0

Рисунок 2.10 – Маршрутизатор

Маршрутизатор, який зображений на Рисунку 2.10, має п'ять портів Ethernet. Чотири з них доступні як порти LAN (позначені номером 5 на рис 2.10). Кожен порт визначає різні підмережі в локальній мережі. П'ятий порт - WAN-порт підтримує широкі зв'язки зони (марковані як номер 6 на Рисунку 2.10). Зверніть увагу, що консольний порт на цьому маршрутизаторі (позначений як № 2 на Рисунку 2.10) є з'єднання RJ45, замість послідовного порту.

Через те, що маршрутизатор включає в себе функції пристроїв нижчого рівня, наприклад, такого як міст, а також встановлює межу для доменів колізій в мережі. Інформація від пристроїв в одній підмережі не може зіткнутися з інформацією інших підмереж. Крім того, маршрутизатор обробляє кожен пакет, щоб визначити найкращий шлях доставки, так що підвищує рівень сигналу ретрансляції кожного пакета. Маршрутизатор також встановлює межу для широкомовних доменів. Маршрутизатори не поширюють широкомовний трафік, за винятком передачі DHCP/BOOTP. Більшість маршрутизаторів не проводять ці трансляції за замовчуванням, але ви маєте можливість включити цю функцію, працюючи з деякими маршрутизаторами. Як правило, маршрутизатор налаштований на режим "модуля підтримки IP-адреси", який дозволяє маршрутизатору змінити трансляцію на одноадресну для пересилання DHCP-сервера. Тому що DHCP-сервер отримує адресу DHCP-клієнта, як частину запиту, він відповідає маршрутизатору односпрямованою передачею пакета, а маршрутизатор пересилає DHCP відповідь клієнту.

DHCP/Bootp

Спеціальні трансляції, використовувані з автоматичним присвоєнням IP-адреса (DHCP) і віддаленого завантаження для пристроїв, які не мають завантажувальні файли на локальному диску (BOOTP). Багато комутаторів спроектовані таким чином, що вони можуть також бути налаштовані для роботи в якості маршрутизаторів.

Інші розповсюджені пристрої

Існують і інші мережеві пристрої, про які тут не йдеться. Нерідко мережа має один або кілька серверів, які надають особливі послуги мережі. Іноді ви будете зустрічати пристрої, розроблені спеціально, щоб дозволити внутрішнім комп'ютерам безпечно спілкуватися. Інші поширені пристрої - будуть розглянуті більш детально нижче в даному курсі. Ще один пристрій, який дійсно заслуговує на особливу увагу - безпроводова точка доступу «AP» (Access Point), іноді згадується як WAP. Як уже згадувалося в попередньому розділі, точка доступу виступає в якості центральної точки з'єднання для безпроводових пристроїв. Вона також виступає в якості шлюзу, що з'єднує безпроводові пристрої з проводовою мережею (Рисунок 2.11).

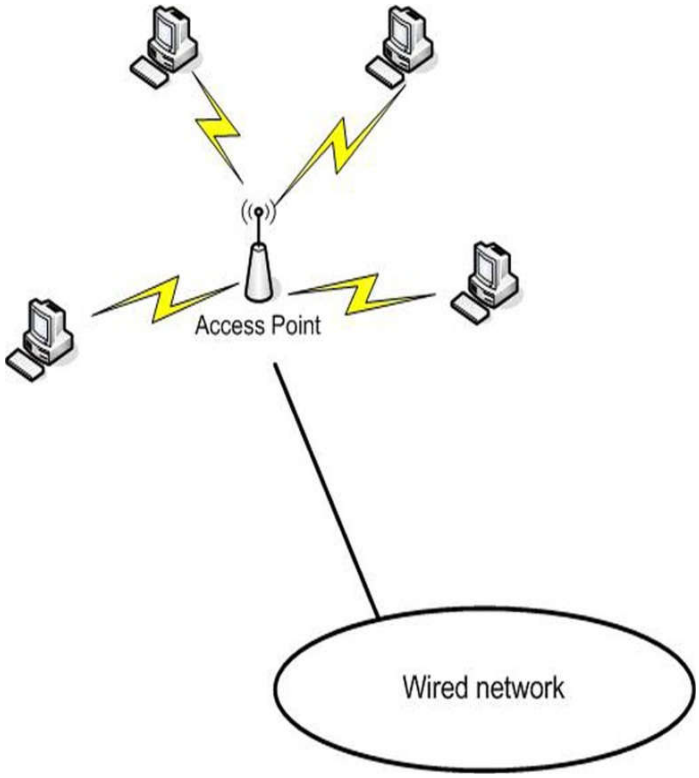


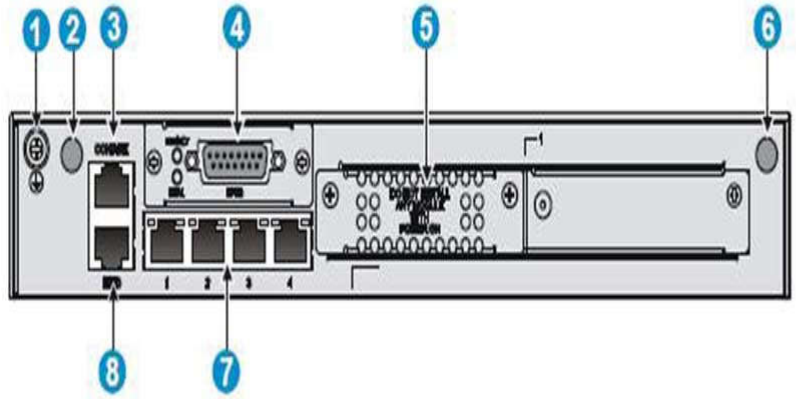
Рисунок 2.11 - Точка доступу

У більшості мереж, аутентифікація, зв'язок і безпеку для безпроводових клієнтів здійснюється через точки доступу. Як і в інших сполучних пристроях, більшість точок доступу підтримують віддалене управління, часто через веб-інтерфейс. У великої безпроводовій мережі, ймовірно, знайдуться точки доступу, керовані через центральний безпроводовий контролер, що робить непотрібним (в більшості випадків) індивідуальне налаштування і управління точкою доступу. Пристрій, що створив найбільшу революцію, як в домашньому користуванні, так і в малому бізнесі, мережі є безпроводовий маршрутизатор (Рисунок 2.12). Безпроводовий маршрутизатор поєднує в собі шлюз, маршрутизатор, комутатор і функціональність безпроводової точки доступу поряд з автоматичним присвоєнням IP-адреси, безпроводової безпеки, і, в деяких випадках, навіть інших функцій. Слід

зам'ятати, що безпроводовий маршрутизатор не проводить маршрутизацію безпроводових сигналів. Він пересилає трафік за допомогою безпроводової мережі 802.11 Wi-Fi до адресатів, які, як правило, користуються інтернетом.

(1) Power switch	(2) Power receptacle	(3) USB port
(4) Reset button		

Figure 8 A-MSR20-12-W rear panel



(1) Grounding screw	(2) Antenna port	(3) Console/AUX port
(4) E1 port EPRI0	(5) SIC/DSIC slot	(6) Antenna port
(7) Ethernet LAN ports (ETH1 to ETH4)	(8) Ethernet WAN port ETH0	

Рисунок 2.12 - Безпроводовий маршрутизатор

Зверніть увагу, що конфігурація безпроводового маршрутизатора дуже схожа на конфігурацію проводового маршрутизатора, про який вже казалося, з тими ж проводовими мережевими портами і портом WAN. Основна відмінність полягає в тому, що цей маршрутизатор також включає в себе вбудований радіомодем, а також має зовнішній порт антени. Одна з причин популярності безпроводових маршрутизаторів є те, що вони дають простий спосіб підключення до високошвидкісного інтернету (Рисунок 2.13).

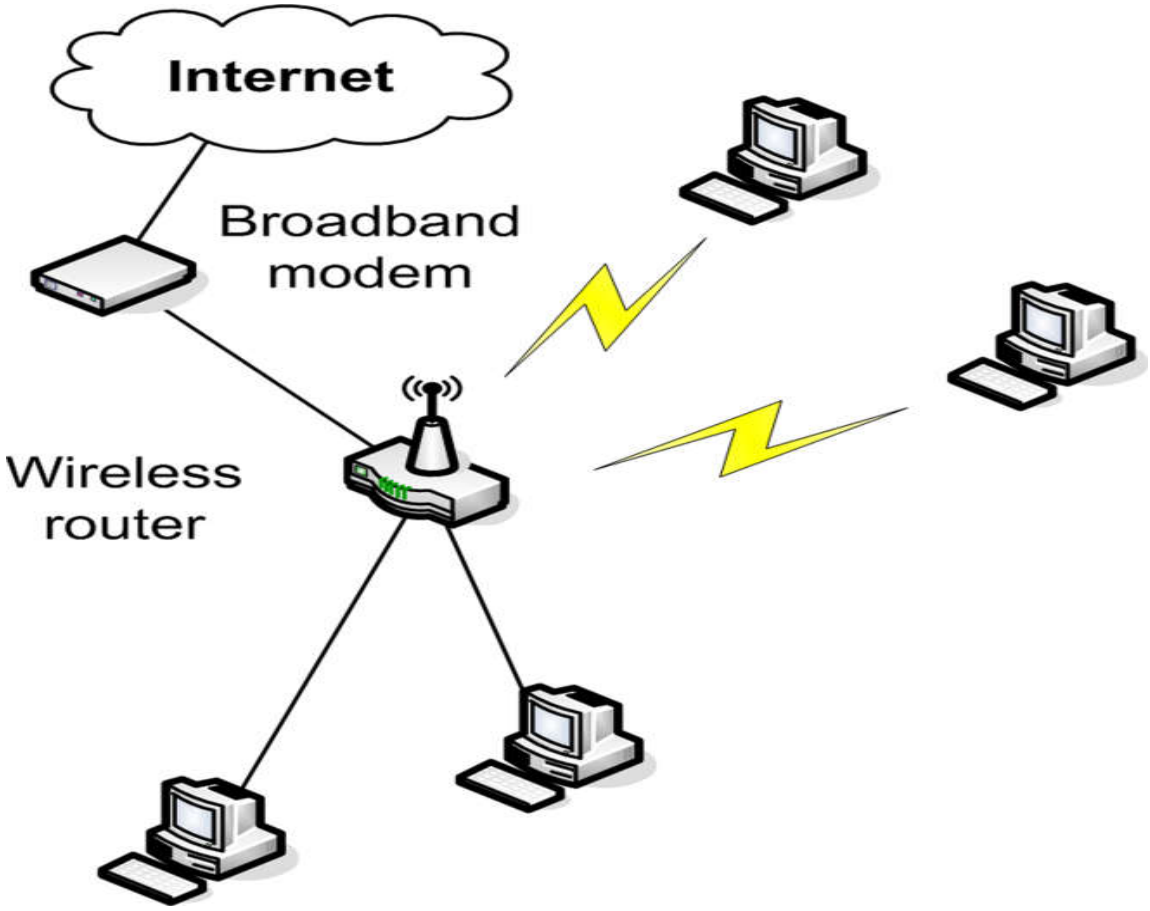


Рисунок 2.13 - Використання безпроводового маршрутизатора

В одній загальній конфігурації, високошвидкісний пристрій, як правило, DSL або кабельний модем, підключається до порту по висхідній лінії зв'язку безпровожового маршрутизатора до загального доступу за допомогою проводових клієнтів портів і безпроводових клієнтів. Безпроводовий маршрутизатор також призначений для визначення IP-адреси підключених клієнтів і управляє перетворенням адрес для доступу в інтернет. Мережеві пристрої, як правило, призначені для підтримки невеликої кількості підключених комп'ютерів. Для будинку або малого бізнесу, ви, можливо, побачите DSL модем з можливістю бездротового використання.

Модем *- скорочення від модулятор/демодулятор. Це пристрій, який перетворює цифрою сигнал в аналоговий.*

Цифрова абонентська лінія (DSL) *- технологія, яка забезпечує зв'язок цифрових даних за стандартними телефонними лініями.*

Кабельний модем *- пристрій, який забезпечує доступ в Інтернет через коаксіальні ліній кабельного телебачення.*

Сценарій: GoShop, Inc.

GoShop, Inc розробляє свою нову мережу. Мережа буде стартувати менш ніж с 20 комп'ютерів, але, як очікується, виросте з плином часу. Мережа буде розгорнута в районі, який може підтримувати дротове або бездротове підключення, але кабель ще не був прокладений. Комп'ютери клієнтів будуть працювати з ОС Windows або Linux. Всі будуть отримувати TCP/IP адреси IPv4 автоматично. Метою компанії є, виключити можливість отримувати будь-якої

доступ до мережі. Розгляньте мережеві параметри і сполучні пристрої які ви будите використовувати.

Загальні відомості про комутатор

А зараз ми розглянемо комутатор, і розберемося в особливостях управління комутатором. Для цього ми розглянемо комутатор не вдаючись у подробиці, пізніше, в цьому курсі, ми розглянемо його більш детально. *Управління комутатором розкрито більш детально в розділі 4 і наступних розділах.*

Орієнтація комутатора

Перш ніж ми розглянемо управління комутатором, ми повинні вивчити сам пристрій. Фізично, більшість комутаторів дуже схожі функціонально, але вони можуть відрізнятися кількістю портів. Деякі комутатори, особливо менш дорогі, мають фіксовані конфігурації (Рисунок 2.14).

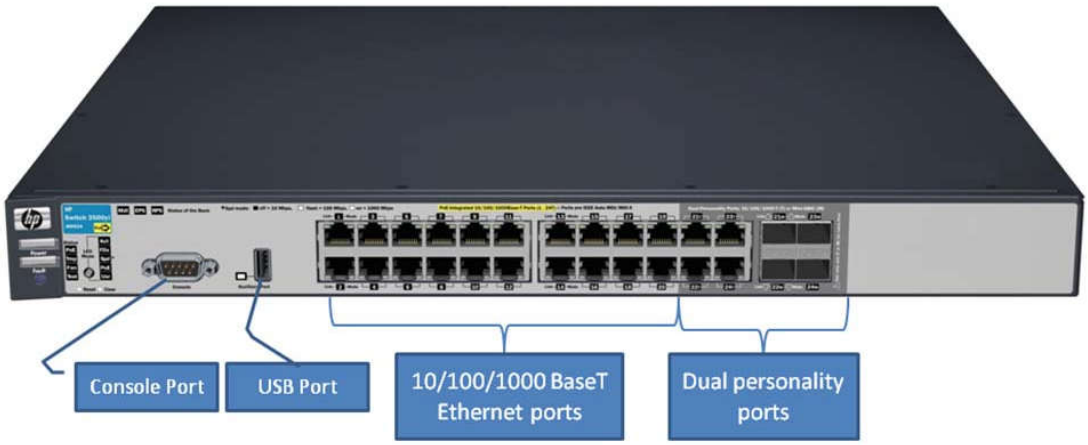


Рисунок 2.14 - HP E3500-24G-PoE yl

Консоль порт послідовного порту, може бути використаний для управління комутатором. Комутатор також має порт USB, який може використовуватися для завантаження нового програмного забезпечення або резервного копіювання конфігурації комутатора. Ця конфігурація комутатора дає вам 20 портів 10/100/1000 Base-T і 8 портів HP подвійного призначення, які підтримують міні-GBIC або 10/100/1000 Base-T, даючи вам можливість вибору типу кабелю (провідний або оптичний). Shared порт - порт подвійного призначення. Якщо трансивер вставлено як - колективний 10/100/1000 Base-T RJ-45, порт відключається.

Живлення через Ethernet (PoE)

Wired Ethernet network technology - мережева технологія, що дозволяє пристроям отримати електричний струм, який дозволяє їм працювати через кабель для передачі даних, без окремого силового кабелю.

Перетворювач інтерфейсу Gigabit (GBIC)

Приймач (трансивер) - пристрій, який поєднує в собі функціональність передавача і приймача в одному пристрої. Приймач - перетворює електричний сигнал в оптичний і оптичний в електричний.

Чотири порти на правій стороні комутатора на Рисунку 2.14 є вихідною лінією портів. Вони дозволяють розширити свою конфігурацію підключенням комутатора до інших комутаторів або інших пристроїв, таких як маршрутизатор. Higher-end switches, як правило, має модульну конструкцію (Рисунок 2.15). Ви можете змінити функціональність комутатора шляхом зміни модулів встановлених в ньому.

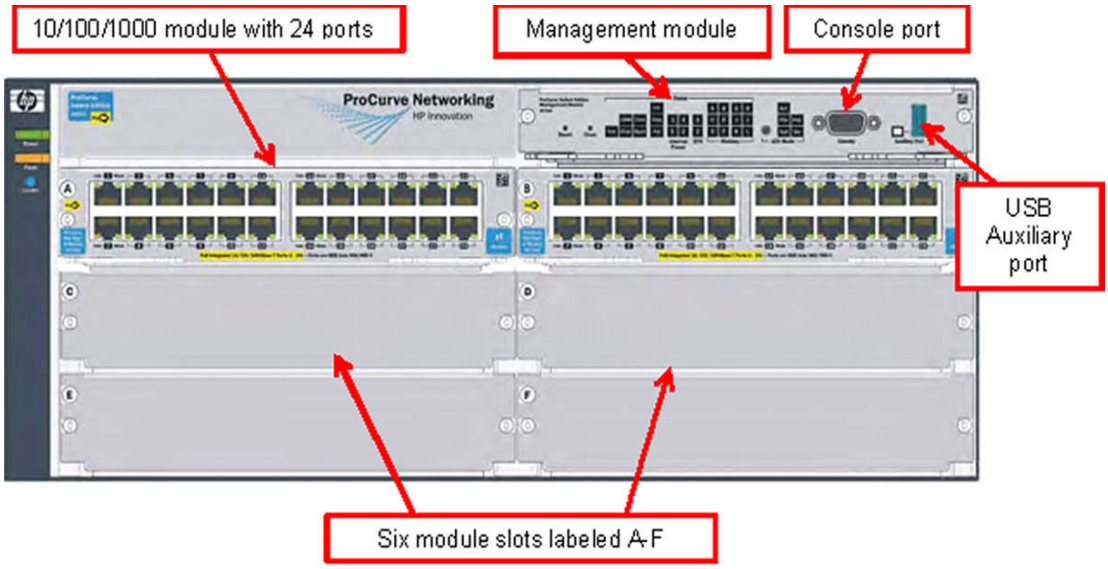


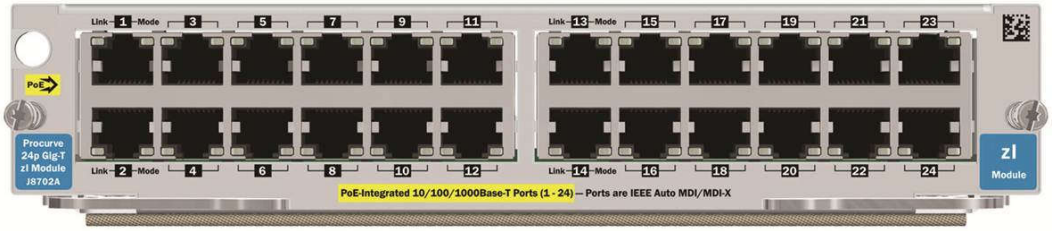
Рис. 2.15 - HP 5406zl-48G

Управління модулем здійснюється через консоль або USB порт. Також є індикатор світлодіодів, які надають інформацію про комутатор і статус встановлених модулів. Ця модель комутатора забезпечує установку до шести модулів.

Зразок на Рисунку 2.15 має тільки два встановлених модуля. Ви можете встановити додаткові модулі портів, в разі необхідності (Рисунок 2.16). Ви можете вибрати модуль для установки наявного висхідного порту, для подальшого розширення. У багатьох комутаторах, модулі мають можливість гарячої заміни.

Гаряча заміна *- відноситься до компонентів пристроїв і модулів, які можуть бути змінені без виключення пристрою. Будь-який з модулів може бути замінений, в той час, як інші будуть продовжувати роботу.*

Стандартний модуль має 24 порти з непарними номерами портів у верхньому рядку і парними номерами портів в нижньому рядку (Рисунок 2.16).



Риунок. 2.16 - Модуль з 24 портами

Порти в модулі називаються ідентифікатором слота (зазвичай буква) і номер порту. Якщо ви встановили цей модуль в слот A, порт на лівому верхньому кутку цього модуля буде порт A1, і порт на правій нижній частині буде A24.

Варіанти управління комутатором

Комутатори HP володіють трьома варіантами інтерфейсу управління:
Інтерфейс командного рядка (CLI);
Меню;
Веб-інтерфейс.

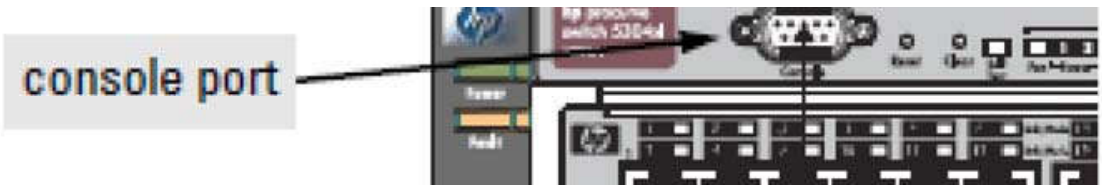
CLI є найпотужнішим, але це також самий складний у використанні тип управління. Інтерфейс меню простіше у використанні, тому що ви оберете команди з меню, а будите їх вводити. Проте, інтерфейс меню обмежує команди управління, до яких у вас є доступ, що робить його менш потужним. Веб-інтерфейс найменш потужний, але зате найпростіший у використанні. Веб-інтерфейс дає вам простий спосіб перевірити стан комутатора з будь-якої точки мережі.

CLI (Інтерфейс командного рядка)

Доступ до CLI здійснюється при підключенні до порту консолі, з ПК під управлінням емулятора терміналу або за допомогою VT-100 терміналу (Рисунок 2.17). Очевидним недоліком є те, що необхідно знаходитися в безпосередній близькості до комутатора, а також мати в наявності 9-контактний послідовний кабель. Найбільшою перевагою є те, що можна підключитися до комутатора і відкрити командний рядок, навіть якщо це не може бути досягнуто через мережу.

Наприклад, доведеться використовувати консольне підключення, якщо комутатор не має діючий IP-адреса.

Емулятор терміналу *– програма, яка дозволяє ПК емулювати функціональність послідовний терміналів. VT-100 - загальні положення послідовного терміналу.*



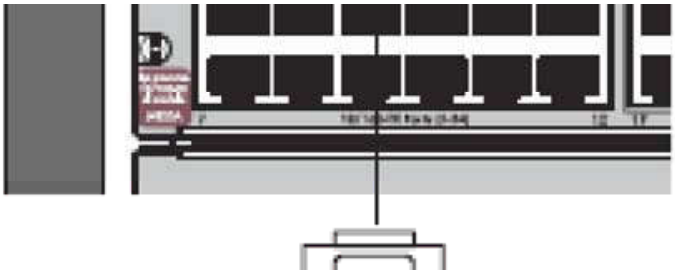


Рис. 2.17 – Підключення до порту консолі

Іншим варіантом є запуск Telnet сесії і підключення до комутатора. Для того, щоб зробити це, виконайте команду Telnet і вкажіть ім'я перемикача або IP-адреса (Рисунок 2.18). Telnet за замовчуванням, використовує порт додатку 23 для спілкування, але може бути вказаний альтернативний порт.

Переконайтеся, що студенти зрозуміли, що порт 23 - порт TCP/IP зв'язку, а не фізичний порт на комутаторі.

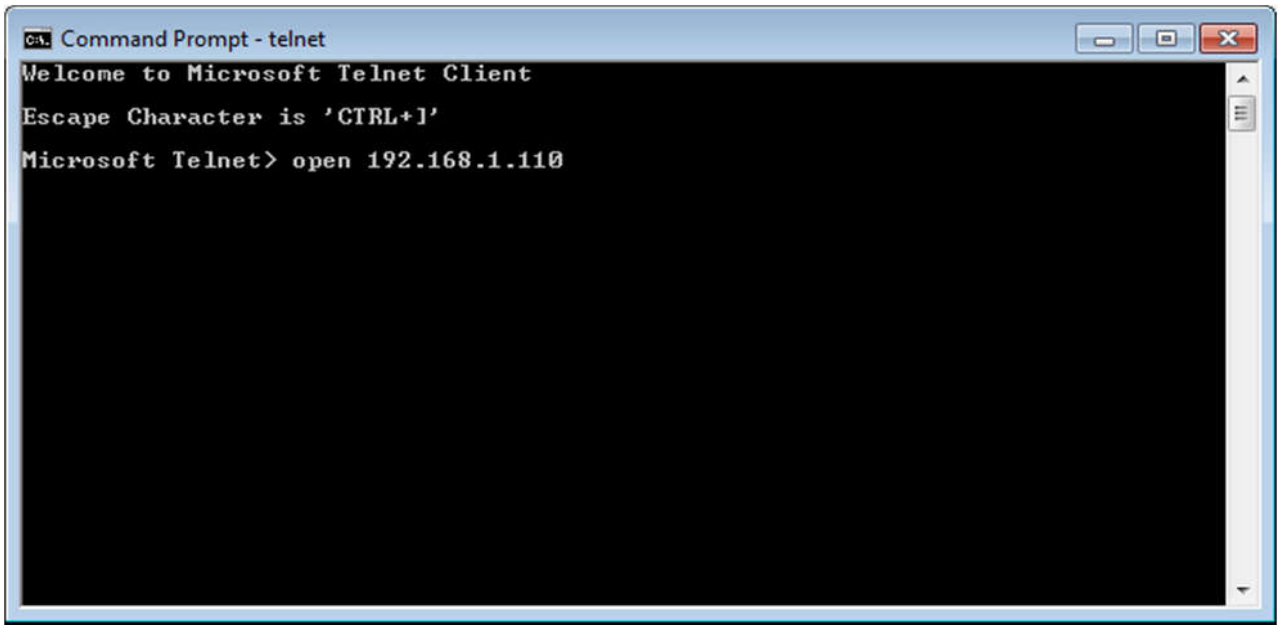


Рис. 2.18 - Підключення до комутатору по Telnet

Telnet *- застосування шару TCP/IP-утиліти / протокол, який дозволяє виконувати команди на віддаленому пристрої.*

Використання Telnet для підключення до комутатора по мережі дійсно несе невід'ємний ризик безпеки. Всі дані, що передаються під час сесії Telnet, передається у відкритому вигляді. Однією з цілей отримання доступу зловмисниками може бути перехоплення управлінської діяльності. При підключенні, комутатор відображає авторські права і повідомляє свої характеристики (Рисунок 2.19). Скріншот екрану, показаний на Рисунку 2.19, був зроблений з комутатора HP - 24G 3500yl. Ви можете побачити інші версії цих заяв. Натисніть будь-яку клавішу для продовження в командному рядку CLI.

Рис. 2.19 - Початкове підключення

Вкажіть, що оператор може переглядати, але не змінювати параметри конфігурації. За замовчуванням в рядку зазначено, що комутатор застарів.

Управління і режим оператора

За замовчуванням CLI проводить швидку перекличку номерів моделі комутатора (Рисунок 2.20). Ви спочатку підключаєте рівень управляння, який дозволяє вам виконувати всі команди, підтримувані CLI.

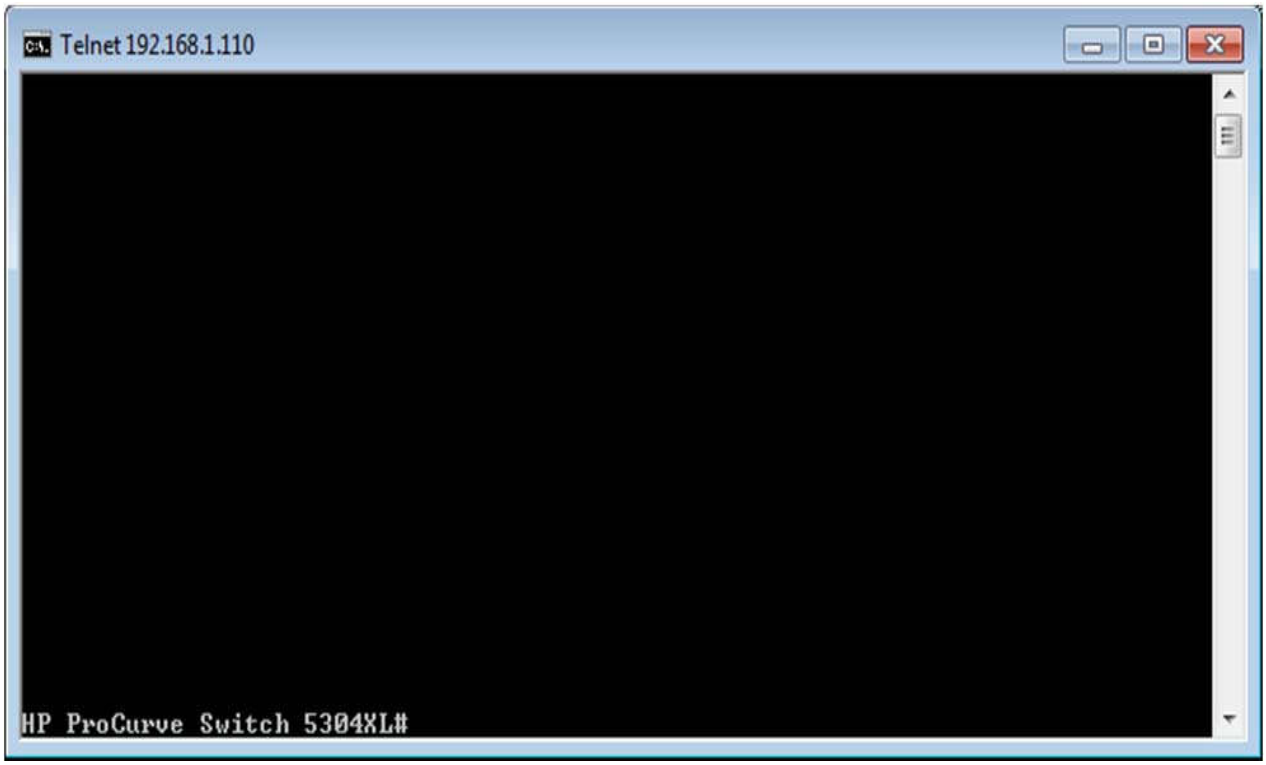


Рисунок 2.20 – Управлінняза допомогою командного рядка

У цьому випадку управляння повідомляє:

```
HP ProCurve Switch 5304#
```

Щоб виконати команду, введіть її в командний рядок і натисніть клавішу Enter. Якщо ввести «вихід» в командному рядку і натиснути клавішу Enter, то це направить Вас в рядок оператора. Зміни командного рядка для:

```
HP ProCurve Switch 5304>
```

Запустіть команду, що дозволить повернутися до рівня менеджера. Нехай студенти знають, що CLI документація включена в посібниках продукту, а також присутня в Інтернеті на веб-сайті HP. рис. 2.21 показує конфігурацію роботи застарілого модульного комутатора.

Перегляд активної конфігурації

Для перегляду інформації про конфігурацію виконайте наступну команду:

```
show running-config
```

Результат виконання команди покаже активні відомості про конфігурацію, в тому числі про тип модуля, VLAN, і інформацію порта (Рисунок 2.21).

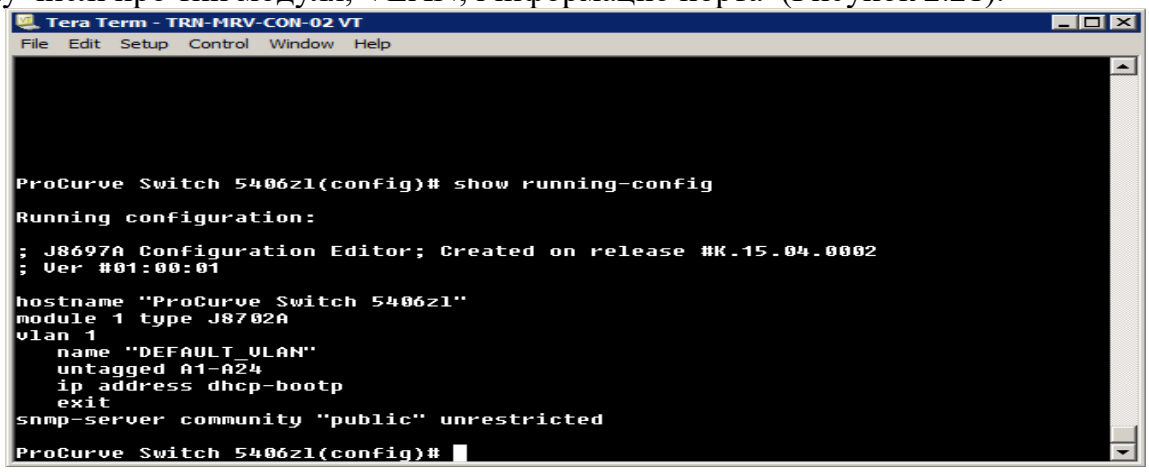


Рисунок 2.21 - Активні конфігурації

При запуску цієї команди ще раз модульний комутатор перерахує всі встановлені модулі і їх тип (Рисунок 2.22).

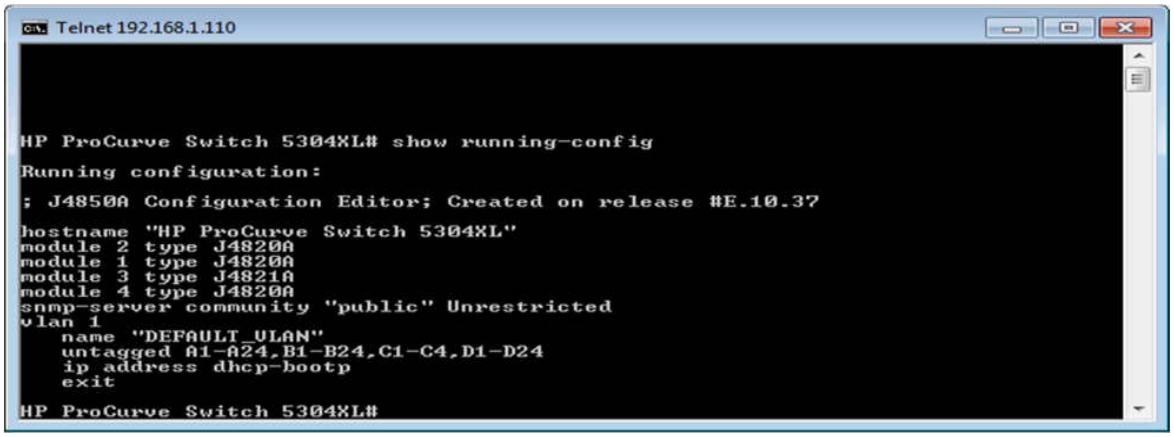


Рисунок 2.22 - Модульний комутатор

CLI має велику кількість підтримуваних команд, багато з яких мають свій набір функцій.

Отримання довідки

Однією з перших речей, яку ви повинні зробити, це переглянути список доступних команд. Для цього введіть або натисніть клавішу Tab в командному рядку (Рисунок 2.23).

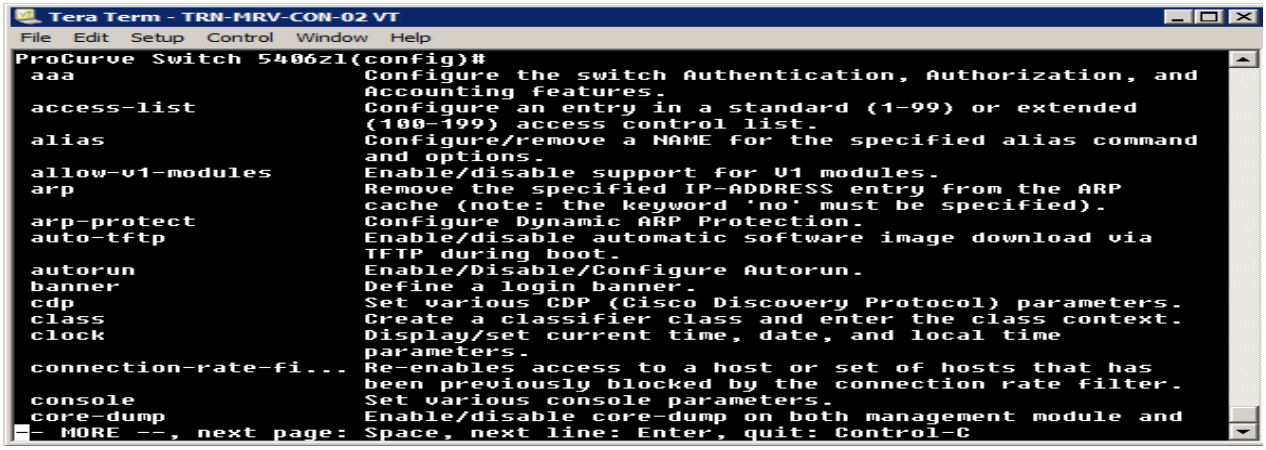


Рисунок 2.23 - Диспетчерські команди

Список доступних команд обмежений під час роботи в режимі оператора (Рисунок 2.24).

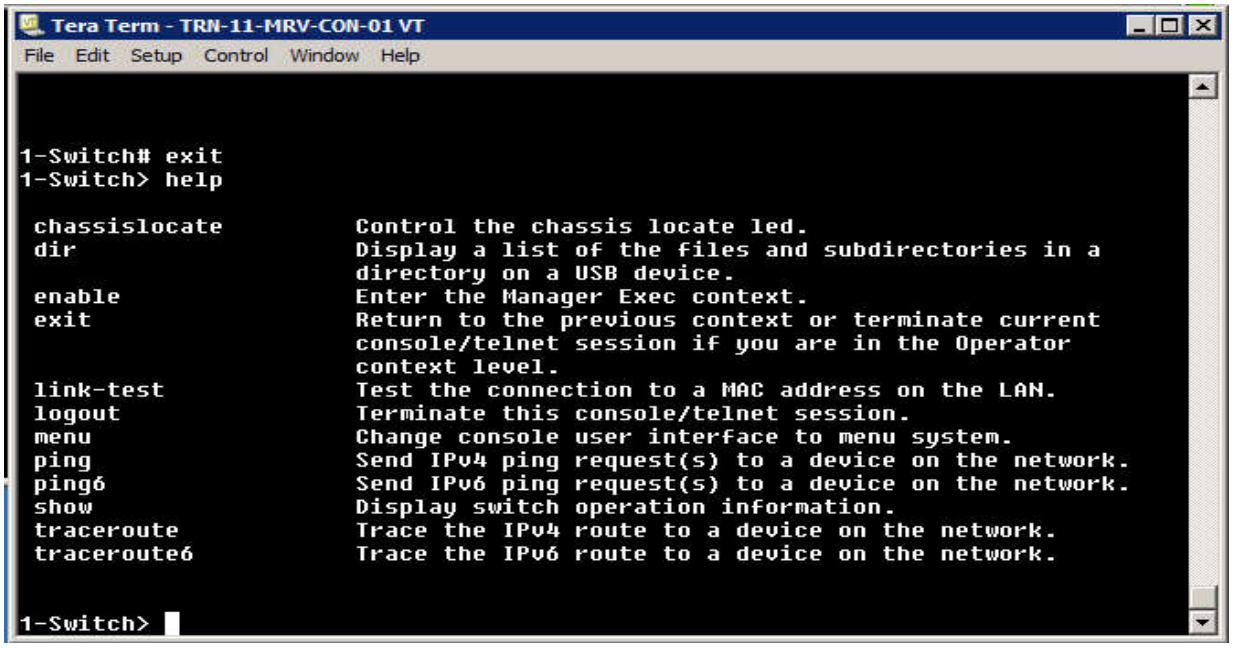


Рисунок 2.24 - Список команд оператора

Деякі команди підтримують підкоманди. Одним із прикладів цього є команди шоу, яке ви бачили раніше. Для отримання списку підтримуваних команд, шоу типу в командному рядку, а потім введіть або натисніть клавішу Tab (Рисунок 2.25).

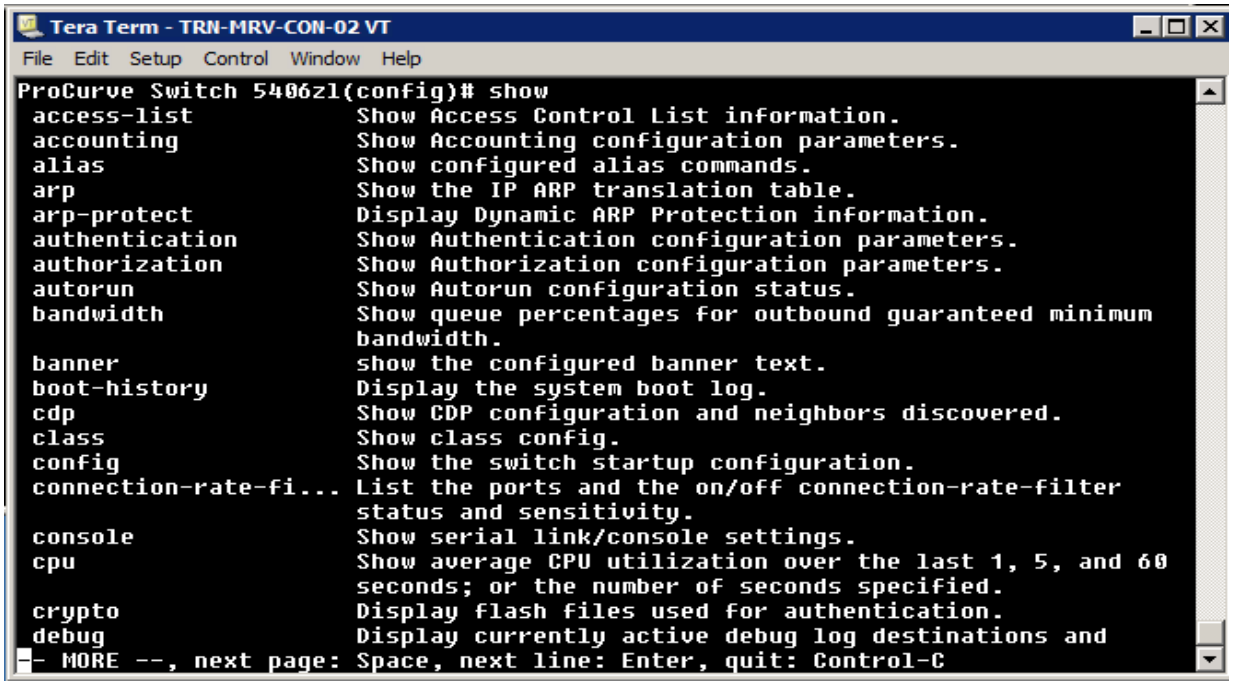


Рисунок 2.25 – Команды

Щоб дізнатися більше про будь-який з цих команд, типу шоу, ім'я команди, допомога, а потім натисніть клавішу Enter. Наприклад:

```
show arp help
```

Ця дія відображає опис команди та будь-яких додаткових опцій, якщо вони підтримуються (Рисунок 2.26).

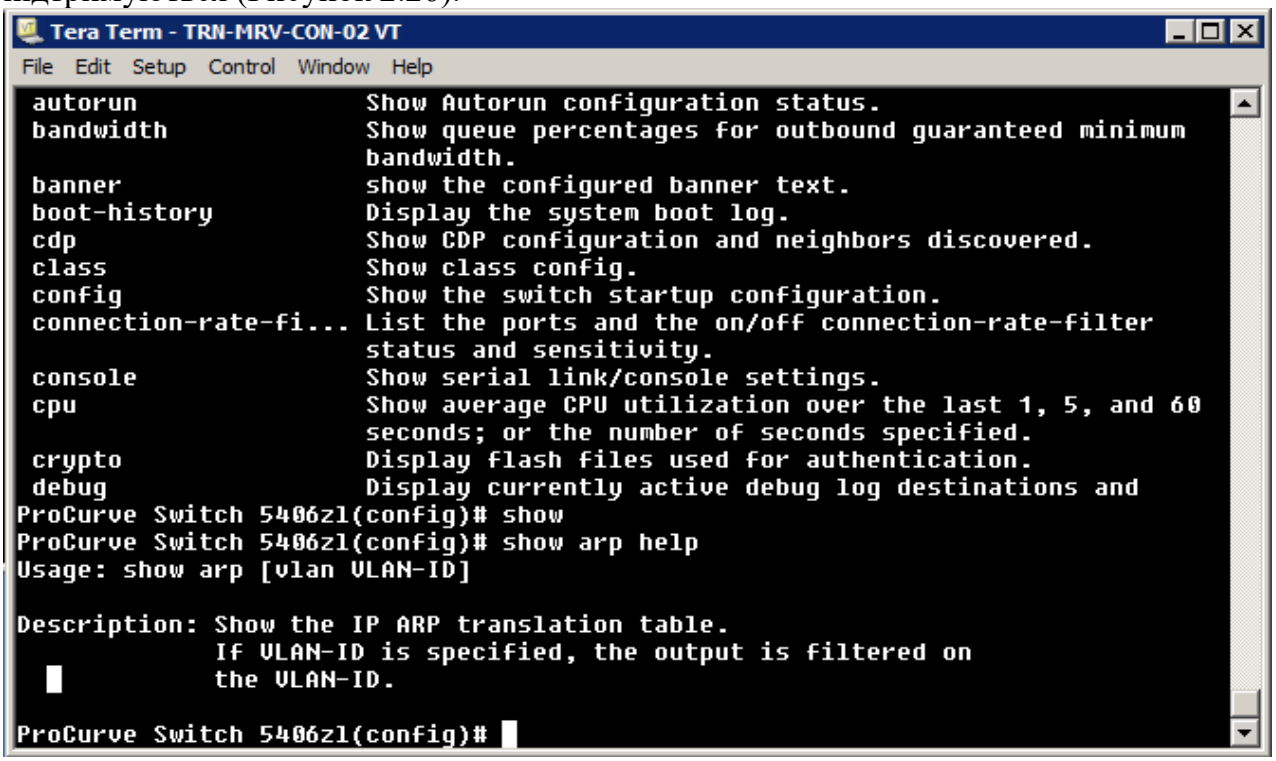


Рисунок 2.26 - Показати команду допомоги

Для більшості інших команд, ви можете просто ввести ім'я команди з подальшої підказкою, або і натисніть клавішу Enter для отримання додаткової інформації про команду і командних опцій. Наприклад, якщо ви хочете дізнатися більше про команду TraceRoute яку ви бачили раніше, ви повинні ввести:

```
traceroute help
```

Ця команда повертає список опцій команд з описами (Рисунок 2.27).

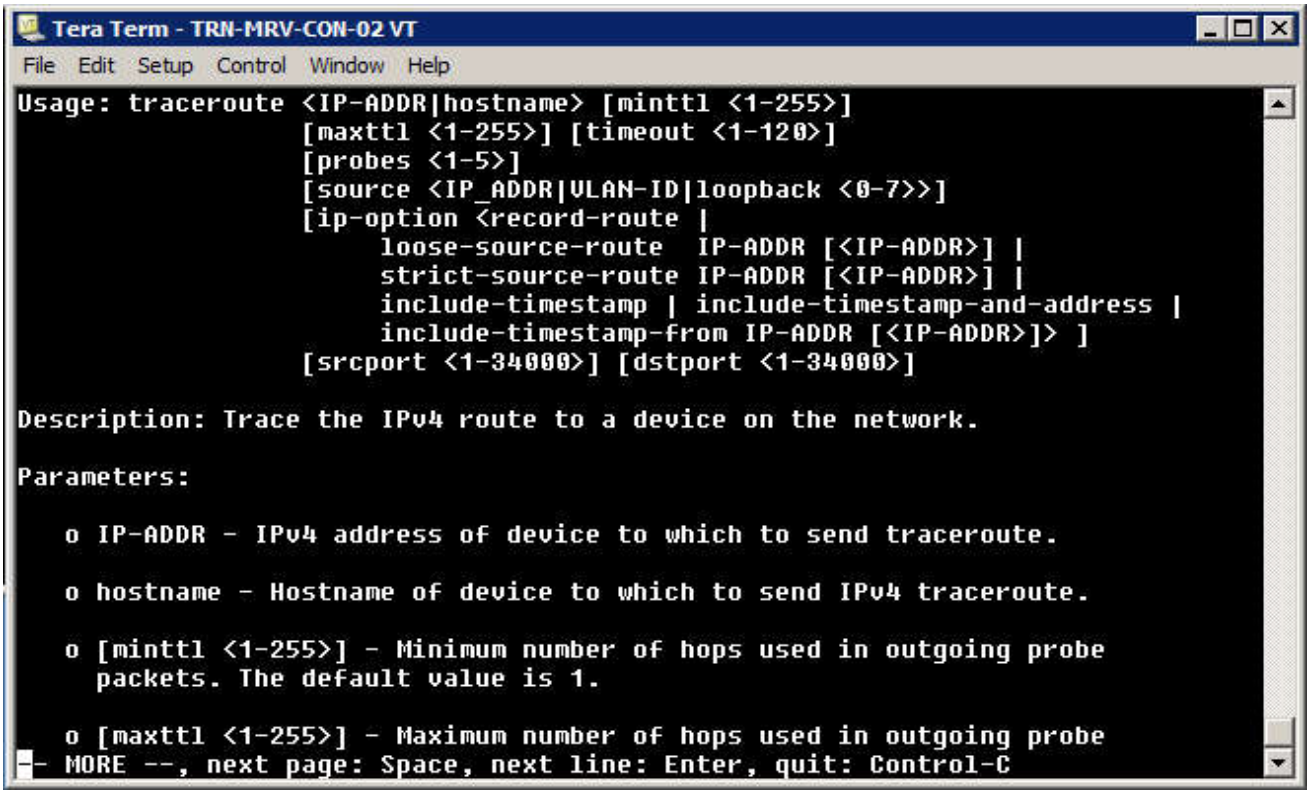


Рисунок 2.27 - Трасировка, команди допомоги

Команди контекста

Деякі команди змінюють контекст командного рядка. Наприклад, якщо ви запустите команду (config), стрімкі зміни включають в себе (конфігурацію) і ви можете виконувати команди конфігурації (Рисунок 2.28).

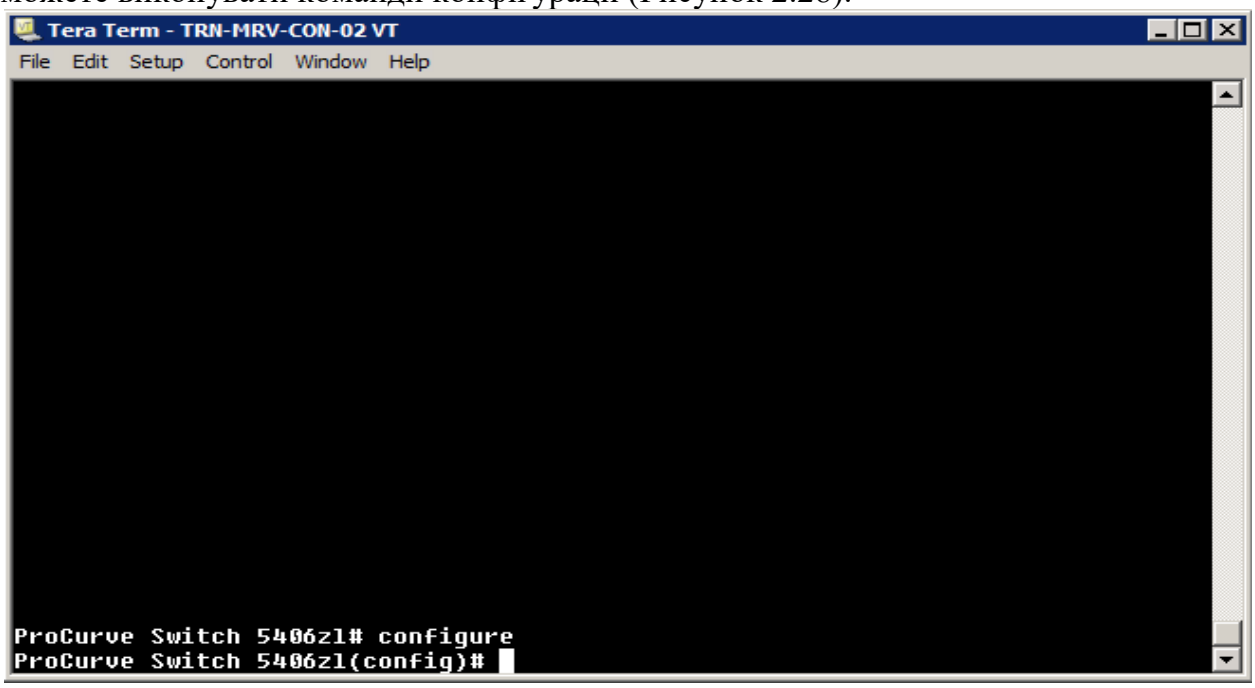


Рисунок 2.28 - Конфігурація контексту

Тепер, при введенні отримаєте список команд конфігурації (Рисунок 2.29).

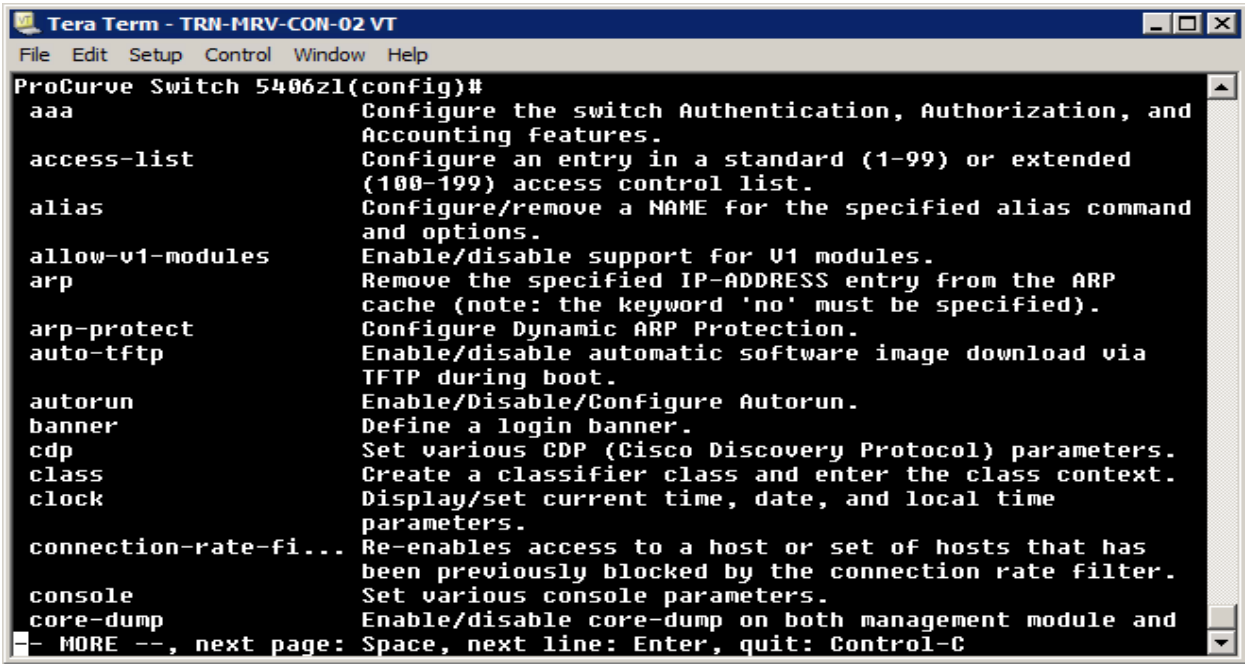


Рисунок 2.29 – Команди конфігурації

Наберіть Exit в (config) командного рядка, щоб вийти з контексту конфігурації.

Меню інтерфейс

Перш ніж ви зможете запустити інтерфейс меню, необхідно підключитися до комутатора і відкрити CLI (Рисунок 2.30). Необхідно запустити команду «Menu» в командному рядку.

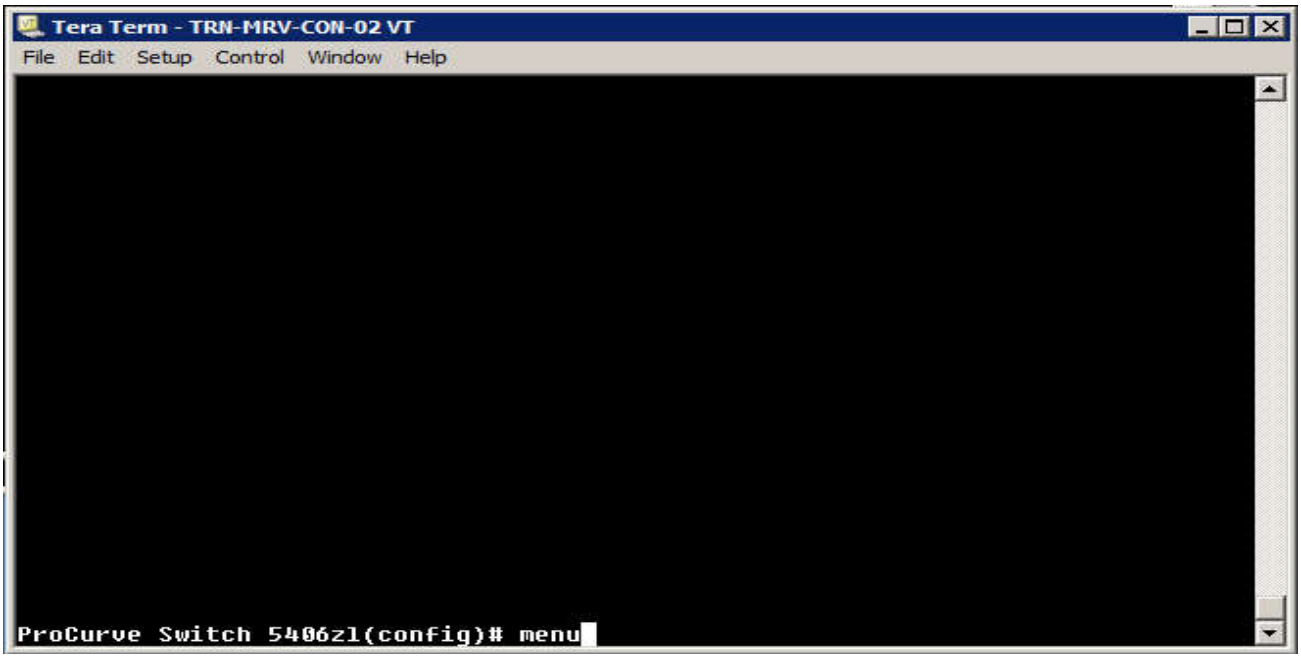


Рисунок 2.30 - Команда «Menu»

Це відкриває головне меню за замовчуванням (Рисунок 2.31). .

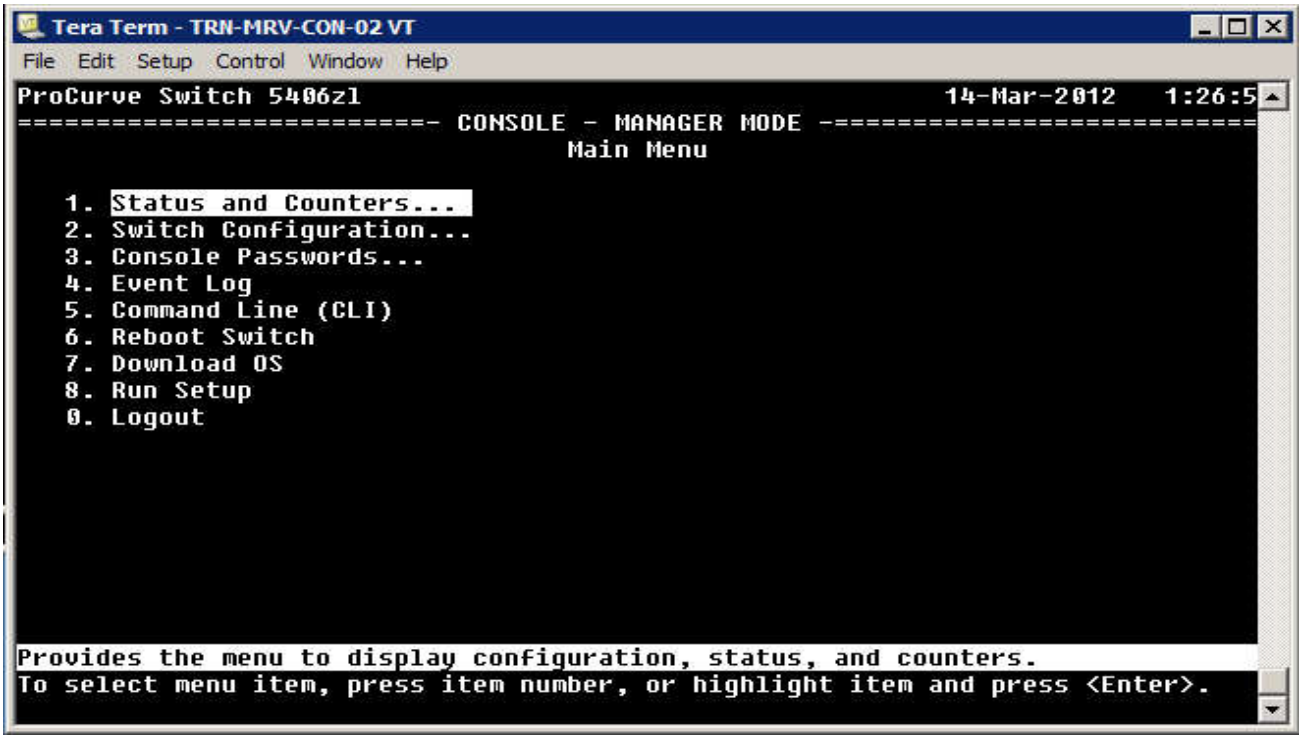


Рисунок 2.31 - Гловне меню

Натисніть номер пункту за допомогою клавіш зі стрілками, щоб вибрати пункт меню, потім натисніть клавішу Enter. Наприклад, «Status and Counters» направить вас до «Status and Counters Menu» (Рисунок 2.32).

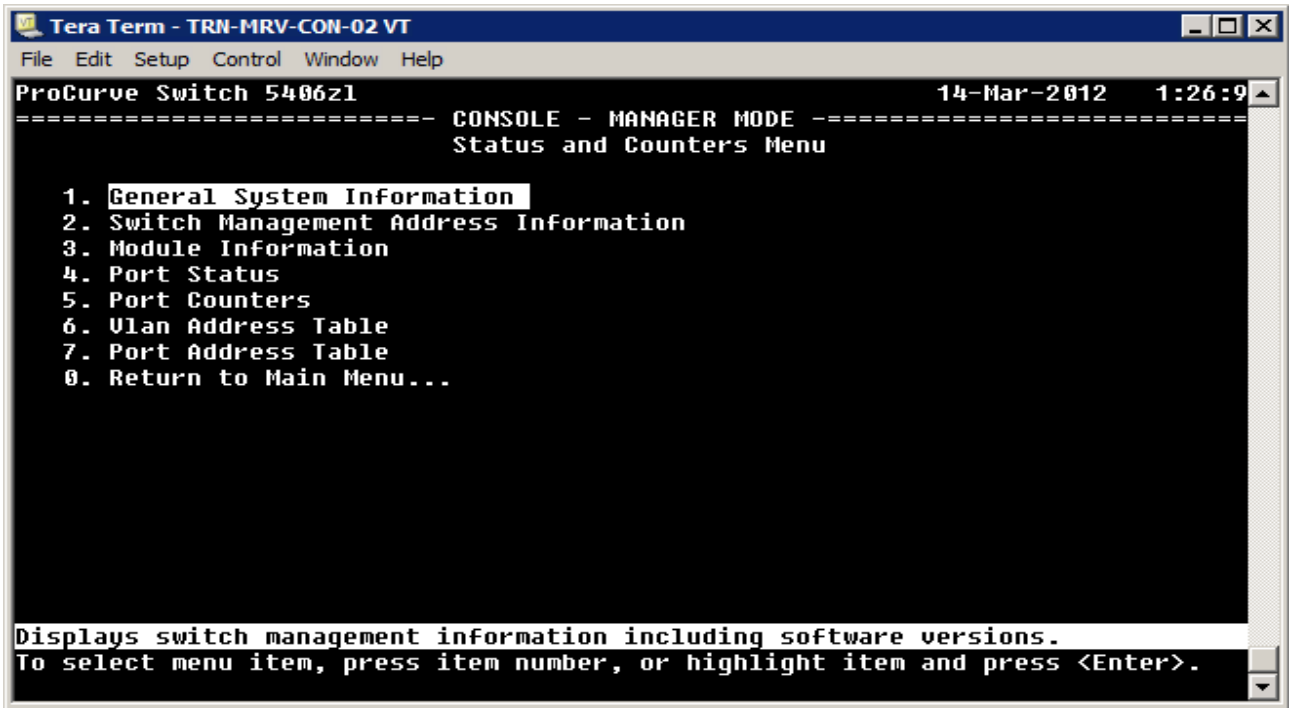


Рисунок 2.32 - Status and Counters Menu

У кожному з підменю, вибір номера 0, повертає вас до меню вищого рівня.

Звідси ви можете переглядати загальну інформацію про систему (вибір 1). Введіть «1» або натисніть клавішу «Enter», щоб вивести загальну інформацію на екран (Рисунок 2.33).

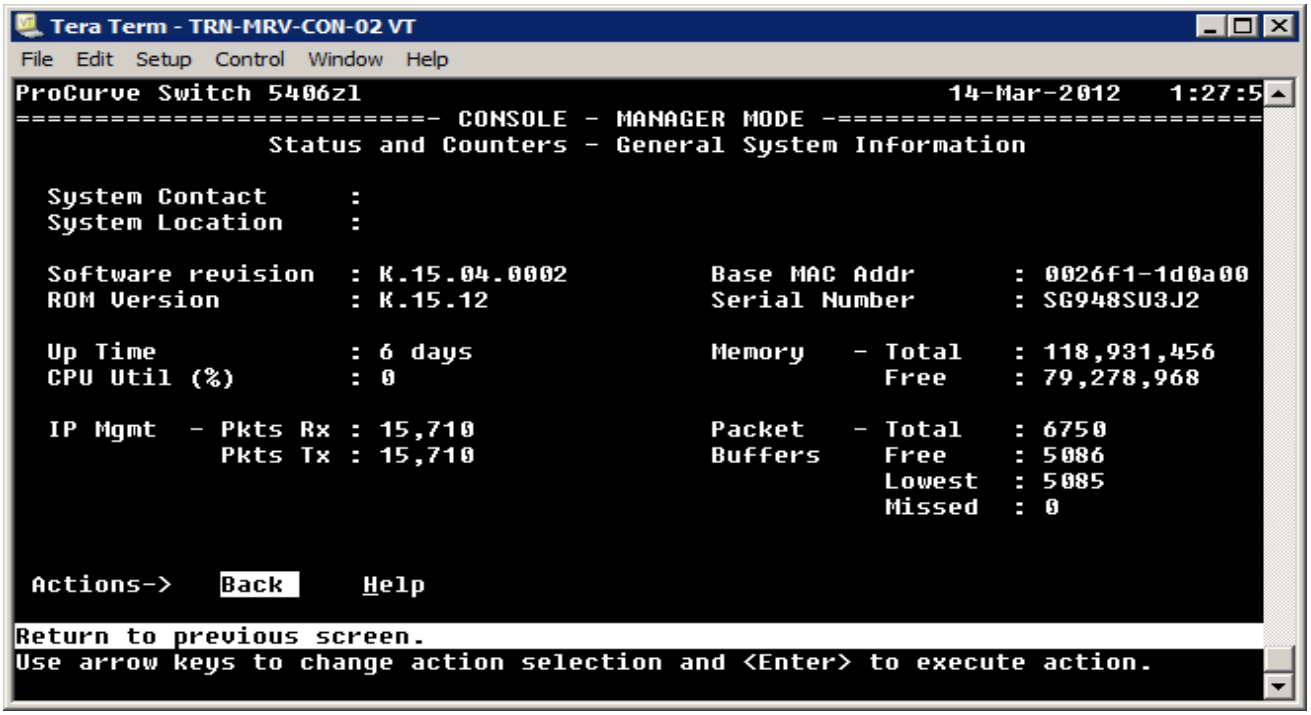


Рисунок 2.33 - Загальна інформація про систему

Для того щоб побачити інформацію про конфігурацію системи, виберіть пункт «2». Для цього перемкніть конфігурацію (Switch Configuration), на «1». Відомості про систему (System Information). Ця команда виведе на монітор інфомацію про систему (Рисунок 2.34).

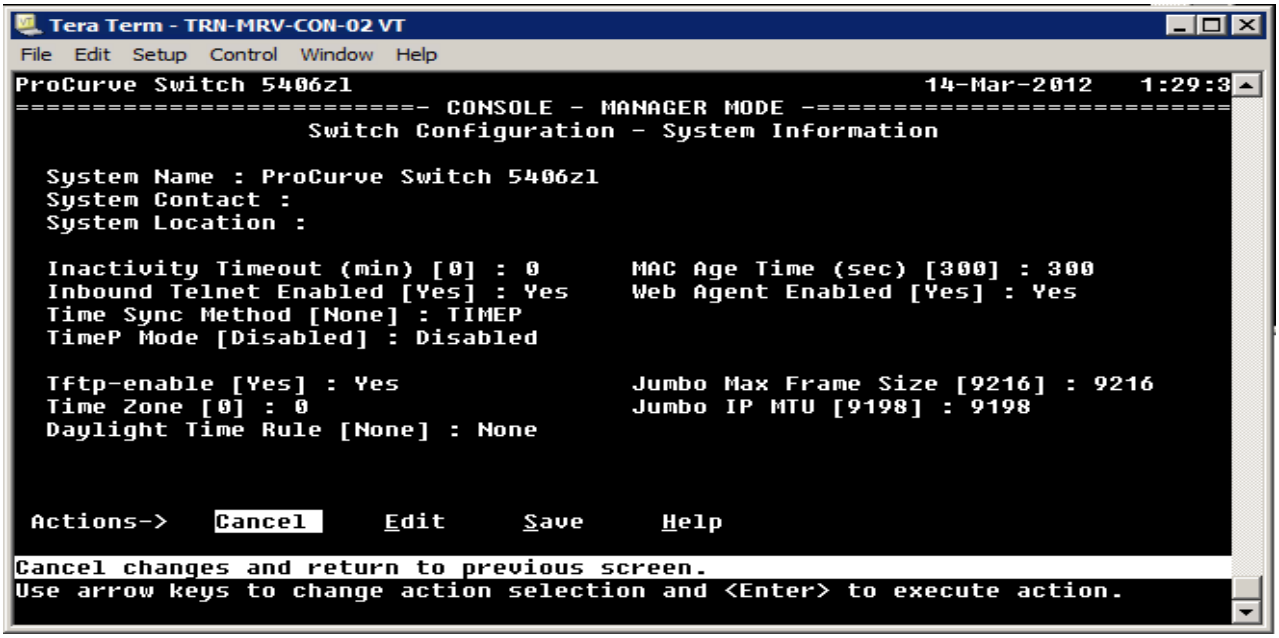


Рисунок 2.34 - Коммутатор, Сводка конфигурации (Switch Configuration Summary)

Нагадайте студентам, що для Telnet і Веб-інтерфейсу управлінням з'єднанням клієнт / хост повинен бути в тій же підмережі, що і комутатор або маршрутізарот повинні бути підключені до комутатора.

Запуск інтерфейсу меню з оператором CLI рядку, має на увазі більш обмежений вибір меню (Рисунок 2.35).

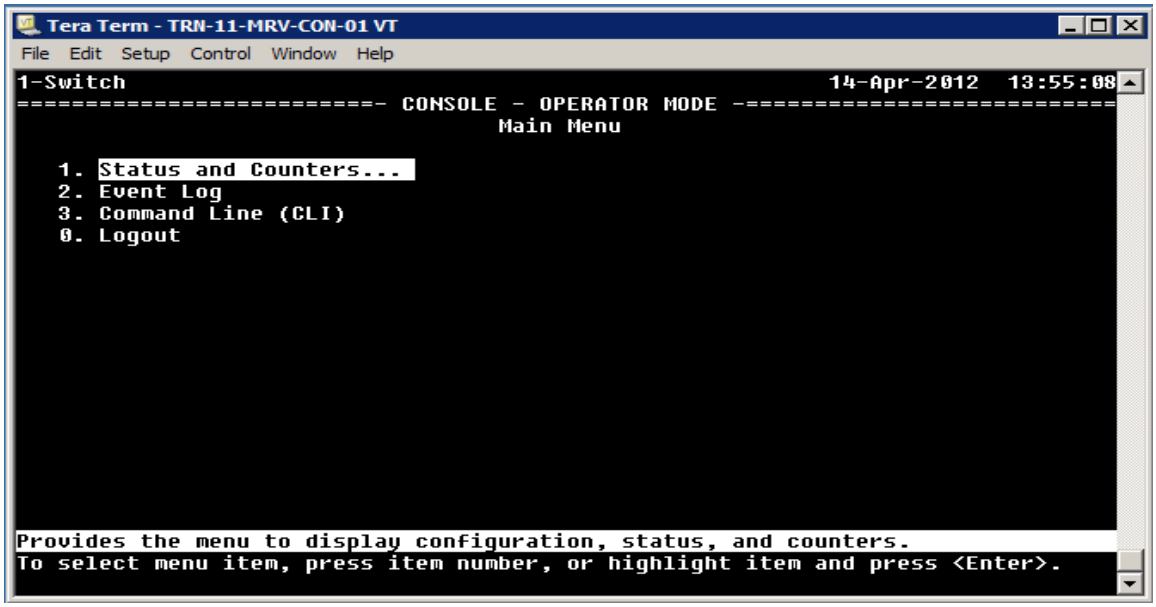


Рисунок 2.35 - Оператор Меню (Manu)

У вас є доступ до підменю «Status and Counters», можна переглянути вміст журналу подій, повернутися до CLI або вийти з вашої Telnet сесії.

Веб-інтерфейс

Для запуску веб-інтерфейсу, введіть IP-адресу комутатора в URL рядок браузера. Ваш браузер буде підключатися до комутатора і відобразить полний URL для веб-інтерфейсу комутатора, як показано на Рисунку 2.36.

Рисунок 2.36 - Подключение к веб-интерфейсу

Веб-інтерфейс відкриває сторінку Стан (Status) і відображає інформацію про стан комутатора (Рисунок 2.37). Точна поява сторінки стану залежить від моделі комутатора і рівня програмного забезпечення. На Рисунку 2.37, відображається загальна інформація про комутаторі і стан порту.

У цьому прикладі обмежєно кількість сторінок інтерфейсу, щоб дати вам загальне уявлення про те, що ви можете зробити через веб-інтерфейс.

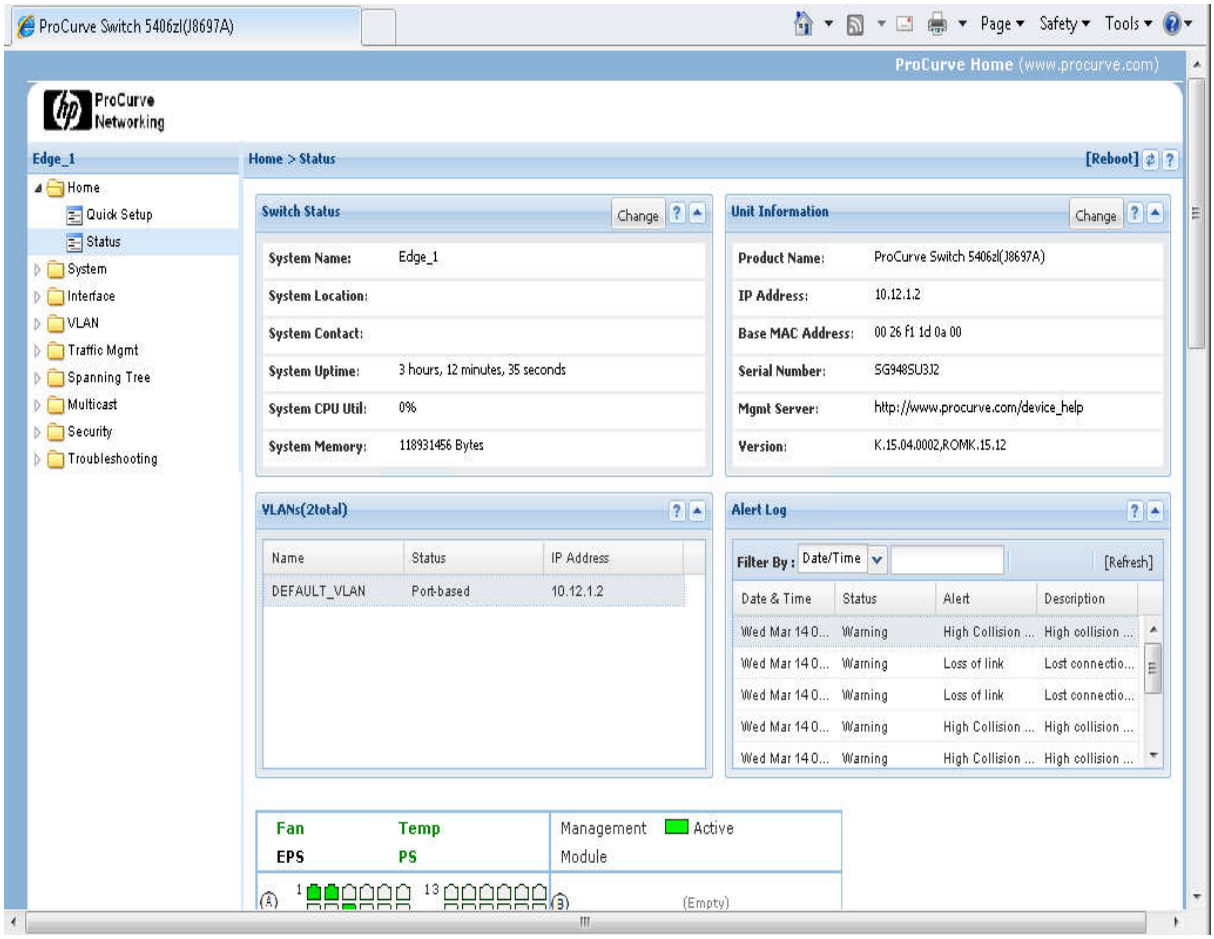


Рисунок 2.37 - Сторінка стану (Status Page)

Більш детельно про SNMP Ви дізнаєтеся в главі 10.

Виберіть «Quick Setup», щоб відкрити основні параметри налаштування комутатора (Рисунок 2.38).

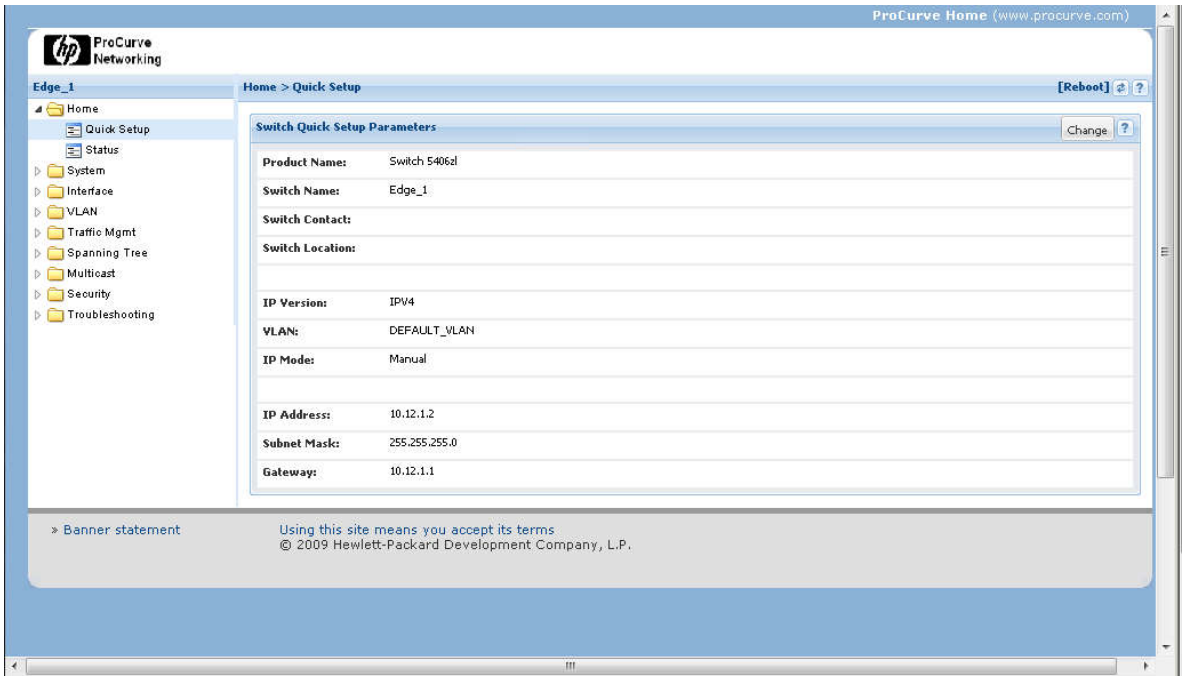


Рисунок 2.38 – Швидке налаштування (Quick Setup)

Системні параметри

Розгорніть папку «System», щоб отримати доступ до «Logging, SNMP» та виберіть «Updates / Downloads» екрани. «Logging» відображає журнал комутатора (Рисунок 2.39).

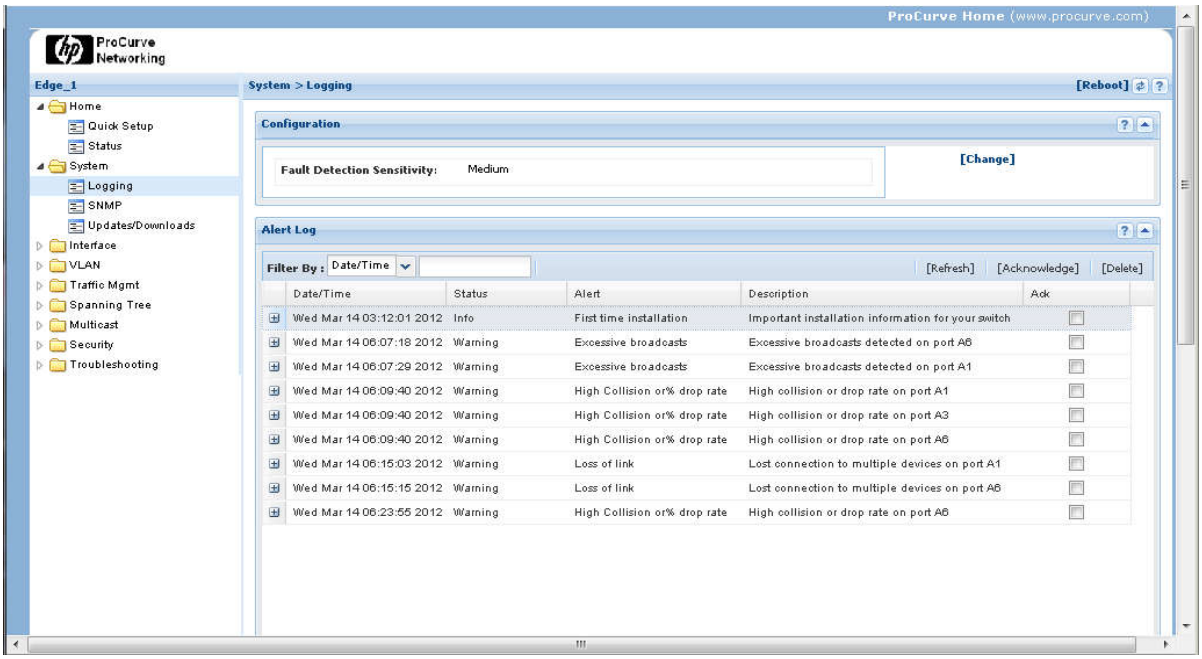


Рисунок 2.39 - Вхід на стрінку (Logging Page)

Відкрийте сторінку «Updates/Downloads» для перегляду і управління образами програмного забезпечення і конфігураційних файлів (Рисунок 2.40), які зберігаються у флеш-пам'яті комутатора. Максимальна кількість образів програмного забезпечення становить 2 одиниці, в той час, як кількість конфігурова-нних файлів досягае 3-х. Налаштування в файлах конфігурації використовуються для налаштування комутатора під час запуску.

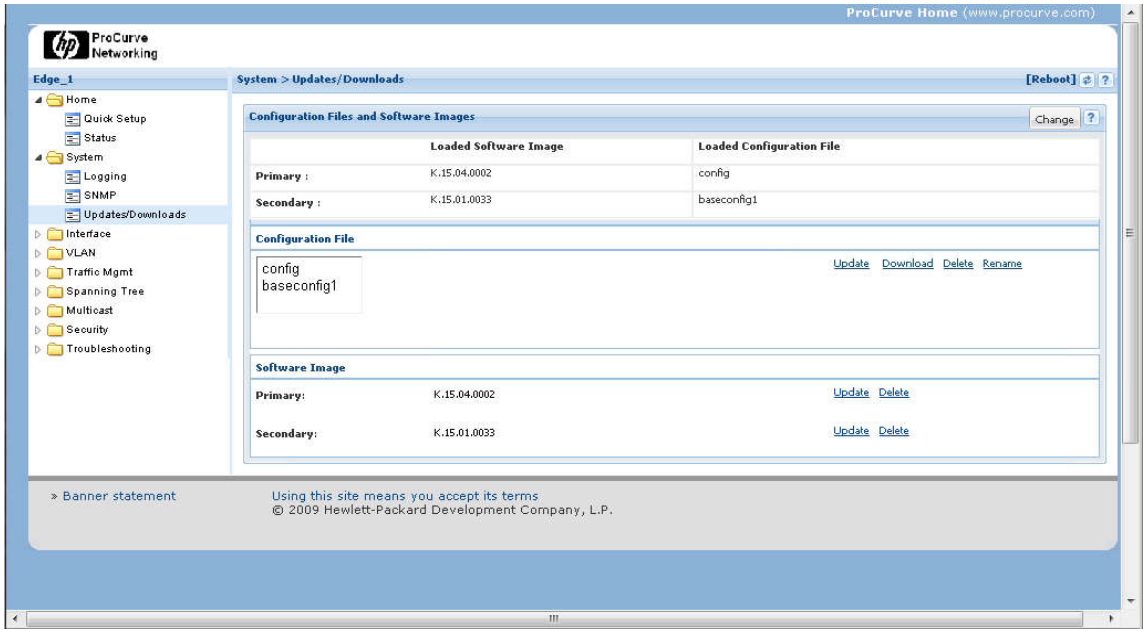


Рисунок 2.40 - Updates/Downloads

Параметри інтерфейсу

Розгорніть папку «Interface», щоб отримати доступ до сторінки «Info / Config» і «POE». Сторінка Порт «Info/Config» (Рисунок 2.41) відображає інформацію порту конфігурації і дозволяє управляти параметрами конфігурації.

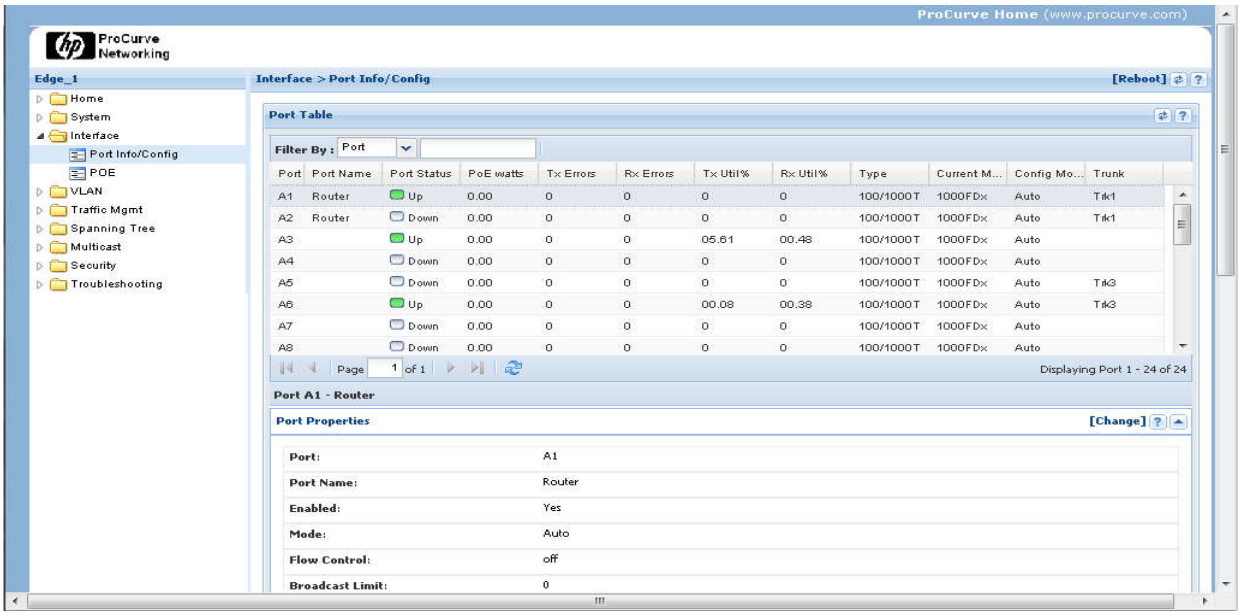


Рисунок 2.41 - Порт Info/Config

Підкресліть що пристрій, живлення якого організовано через POE (Power over Ethernet - по кручений парі) зазвичай не матиме можливості альтернативного живлення, тому POE необхідний для пристрою.

Сторінка Port Info/Config також відображає зведену статистику портів комутатора (Рисунок 2.42), які можуть вам знадобитися (перейдіть, щоб подивитися).

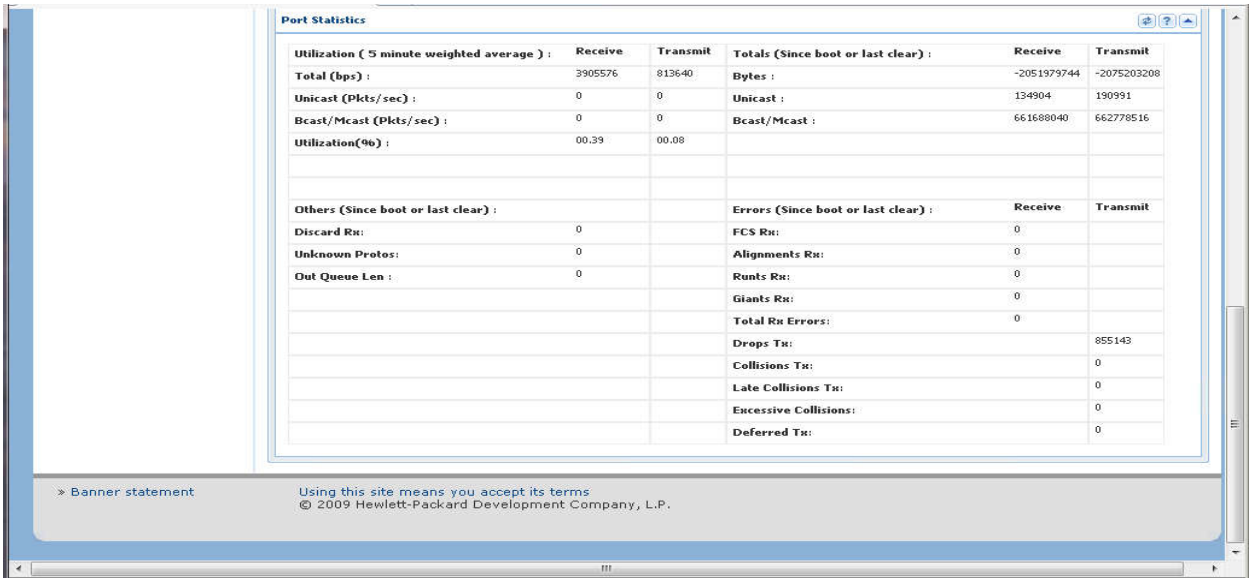


Рисунок 2.42 - статистика портів на стрінці «Port Info/Config»

Натисніть «POE» для перегляду і зміни параметрів конфігурації POE (Рисунок 2.43). Кількість доступних пристроїв POE дещо обмежена, але воно постійно зростає.

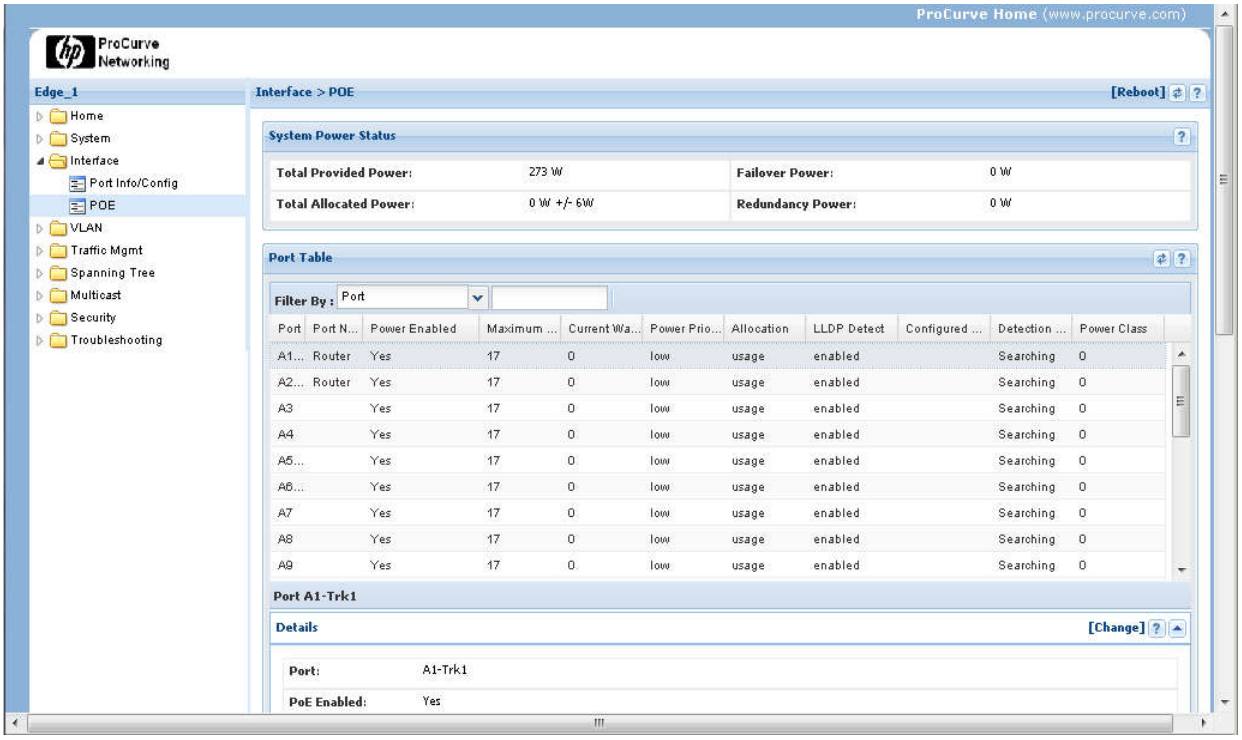


Рисунок 2.43 – POE

VLAN опції

Розгорніть «VLAN» і виберіть «VLAN Mgmt» для зміни і перегляду налаштувань параметрів VLAN (Рисунок 2.44). Виберіть VLAN з таблиці «VLAN» для перегляду властивостей, характерних для цієї VLAN.

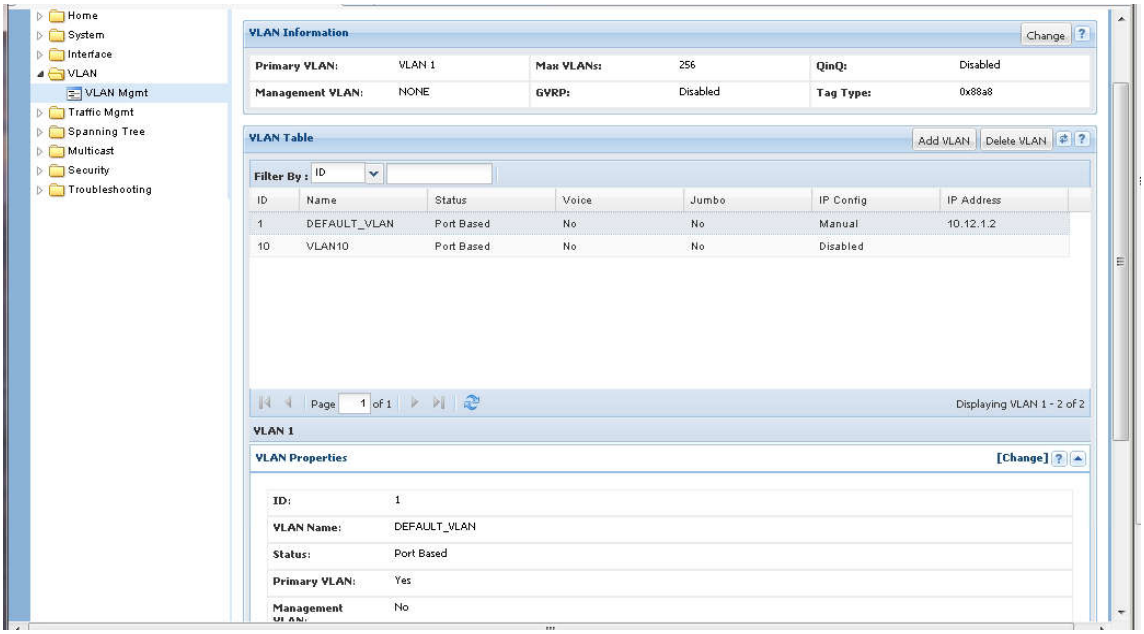


Рисунок 2.44 - Управління VLAN

Параметри безпеки

Сторінка безпеки дозволяє налаштувати параметри безпеки. За замовчуванням, комутатор не захищений. Наприклад, за замовчуванням, імена та паролі користувачів оператора і менеджера - порожні (Рисунок 2.45).

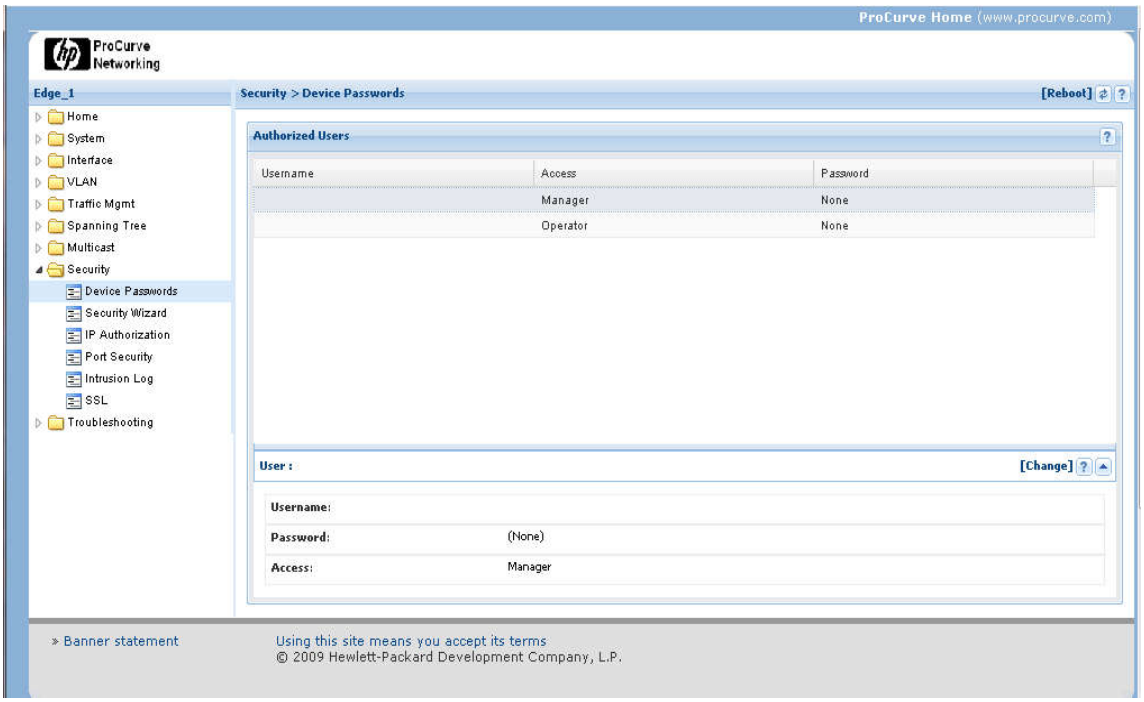


Рисунок 2.45 - Паролі пристроїв

Якщо дозволяє час обговоріть з аудиторією, чому це найкраща пропозиція з точки зору практики.

На додаток до обмеження доступу на ім'я користувача і пароля, ви можете обмежити доступ до управління комутатором за допомогою IP-адреси джерела. Таким чином, ви зможете обмежити комп'ютери, які можуть запустити сесію Telnet за допомогою комутатора.

Ми наполеглево рекомендуємо, при налаштуванні нового комутатора, насамперед виконати установку імен користувачів і паролів для оператора і управляння доступу до комутатора.

Засоби для усунення негараздів

Деякі інструменти пошуку несправностей здійснюється через веб-інтерфейс. Ping/Link Test (Рисунок 2.46) що дозволяє перевірити зв'язок з мережевими пристроями. Ви можете запускати «ping» тести по IP-адресою і «link» тести - по MAC адресу. Деякі версії веб-інтерфейсу не включають в себе сторінки для усунення неполадок. Ви також можете включити комутатор дзеркально відображення, використовуючи інтерфейс командного рядка. Налаштування комутатора віддзеркалення показана пізніше.

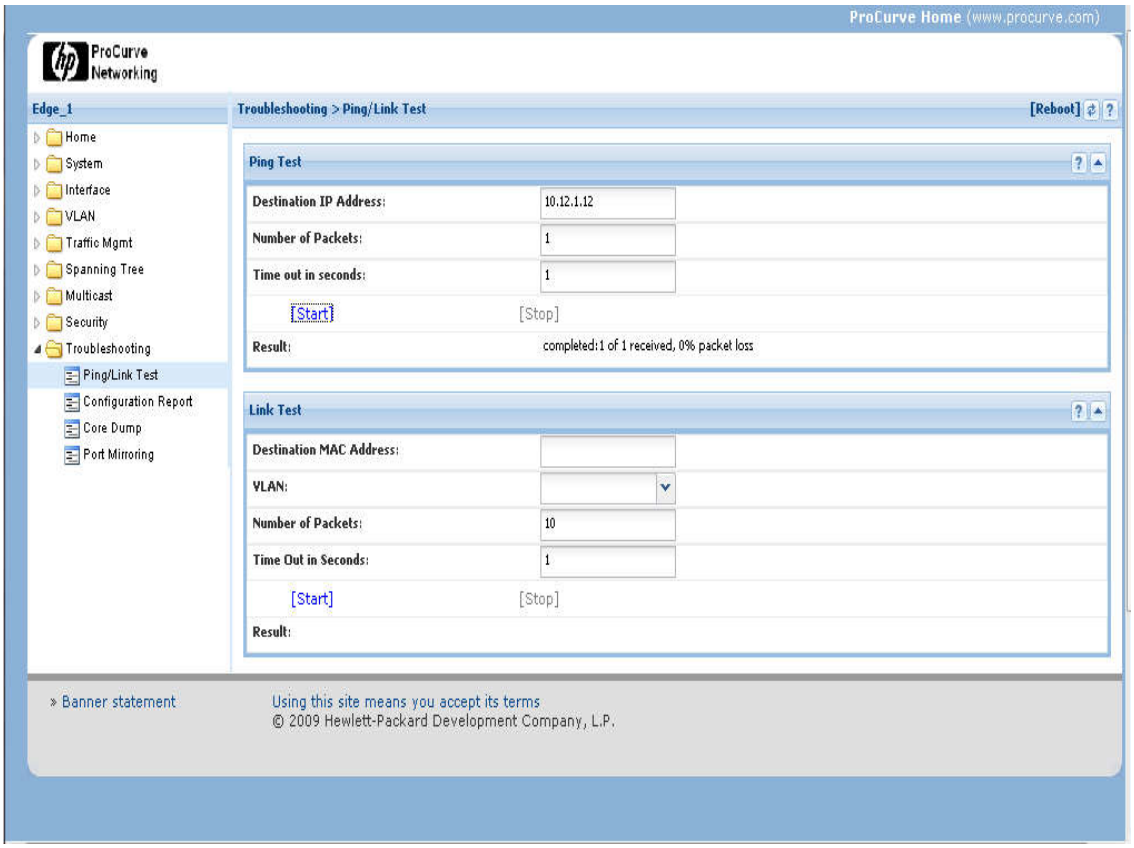


Рисунок 2.46 - Ping/Link Test

Виберіть «Configuration Report», щоб переглянути докладні налаштування комутатора (Рисунок 2.47). Сторінка «Configuration Report» відображає поточну конфігурацію.

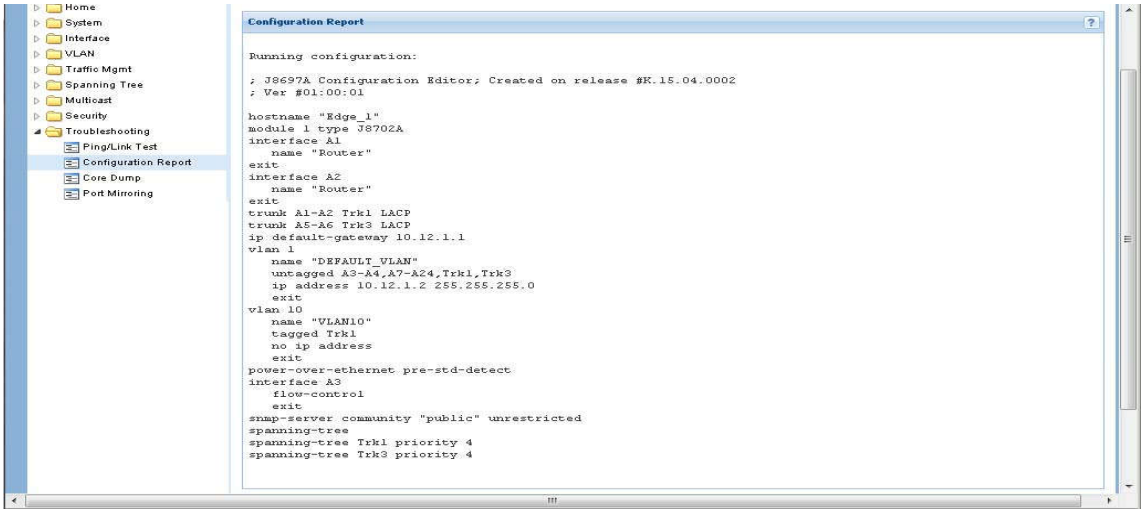


Рисунок 2.47 - Configuration Report

Сторінки з усунення несправностей також дозволяють Вам виконувати скидання установок системи або пам'яті, переключитися на аналіз. Ви також можете включити комутатор дзеркального відображення для моніторингу трафіку. Однією з переваг використання веб-інтерфейсу є те, що він дозволяє управляти комутатором з будь-якого місця мережі. Ще однією перевагою є те, що веб-інтерфейс це найпростіший інструмент управління у використанні. Найбільший

недолік в тому, що веб-інтерфейс підтримує найменшу кількість варіантів управління.

Управління комутатором

Перед тим як покинути тему комутаторів, ми витратимо трохи більше час на обговорення управління комутатором.

Switch Setup с помощью мастера безопасности Web Interface

Перше, що треба виконати для нового комутатора - це налаштувати основні параметри комутатора, особливо параметри безпеки. Розглянемо один з способір реалізації цього процеса, з допомогою Веб-майстра безпеки (Рисунок 2.48).

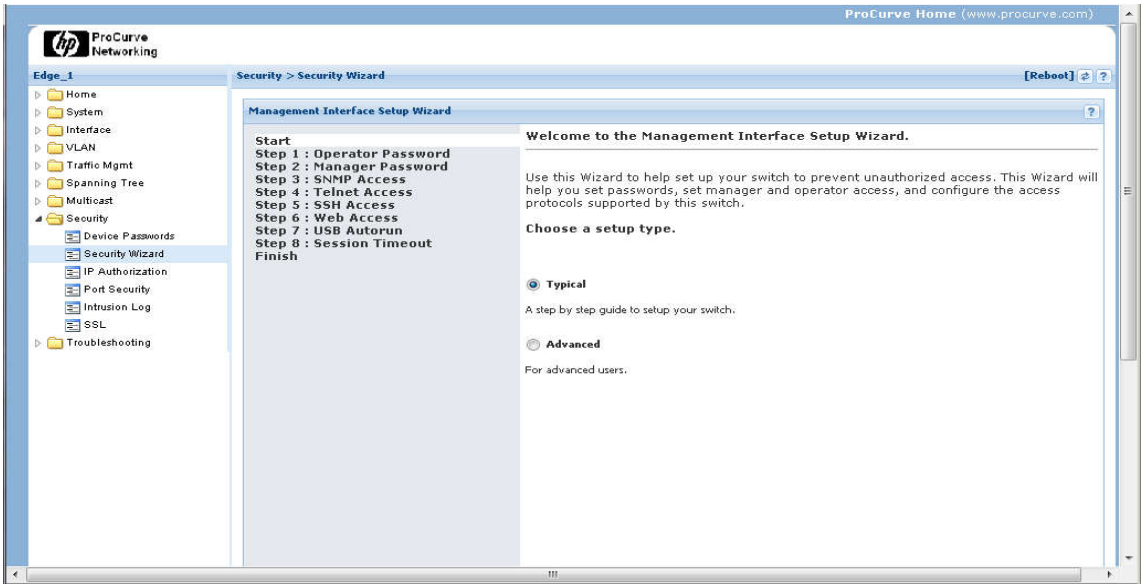


Рисунок 2.48 - Майстер безпеки

Типові налаштування конфігурації безпеки включають в себе:

пароль оператора;
пароль управління;
доступ до SNMP;
доступ до Telnet;
доступ до SSH;
веб-доступ;
USB автозапуску;
тайм-аут сесія.

Існують також інші дії, які ви, швидше за все, захочете виконати під час початкового налаштування. Одним з них є відключення DHCP/BOOTP підтримки і призначення статичної IP-адреси комутатора. При включенні DHCP/BOOTP, є шанс, що IP-адреса комутатора може змінитися. Використовуючи статичний адреса, ви можите здійснити підключення до комутатора через Telnet або веб-інтерфейс.

Налаштування комутатора за допомогою інтерфейсу командного рядка

Команда налаштування CLI дозволяє ввести основну інформацію для комутатора використовуючи інтерфейс меню (Рисунок 2.49).

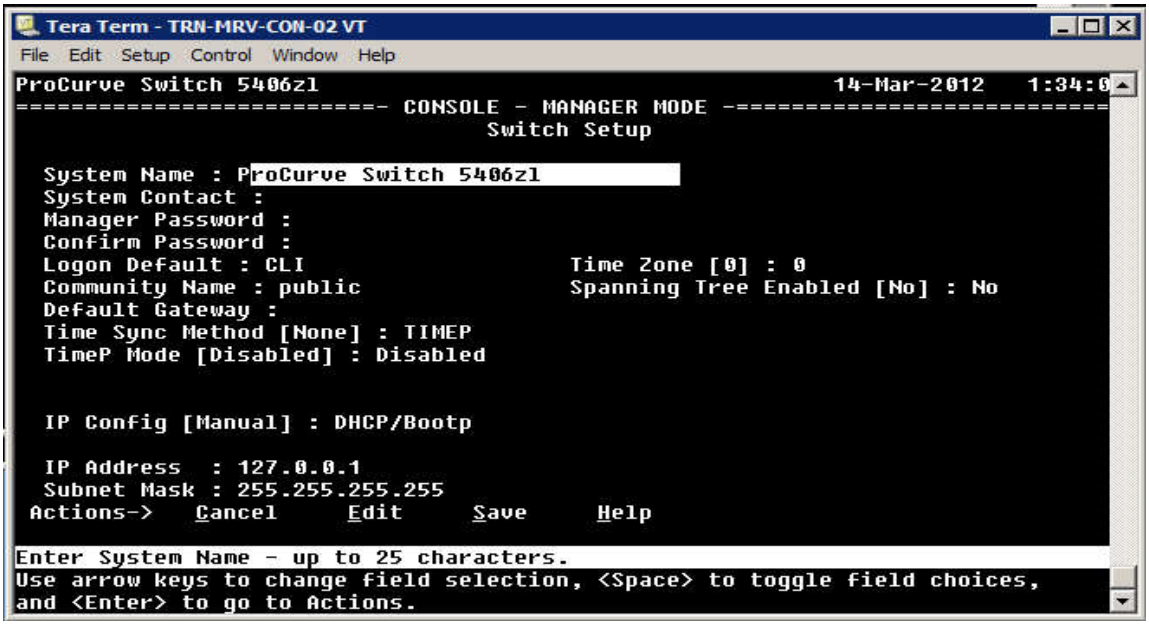


Рисунок 2.49 - Екран Switch Setup

Звідси, ви можете ввести основну інформацію установки, наприклад, як контактна особа для комутатора, управляння паролів, включити або відключити DHCP/BOOTP, а також IP-адреса. У цьому прикладі передбачається, що комутатор виконаний з можливістю назаначанія IP-адреси - автоматично.

Шлюз за замовчуванням встановлюється на маршрутизатор, на який проводиться переадресація пакетів, в разі якщо адресат знаходиться не в локальній мережі, то шлях до місця призначення - не відомий.

Один із кроків, який ви повинні виконати це визначення описового і унікального імені хоста для комутатора, який необхідно зробити в контексті конфігурації. Наприклад, якщо ви хочете назвати комутатора Switch1, вам буде потрібно запустити команду «config», щоб увійти в контекст конфігурації, а потім запустити: `hostname switch1`

При налаштуванні хоста для комутатора, його ім'я буде відображатися в командному рядку CLI замість числа моделі комутатора.

Ви також можете управляти паролями в контексті конфігурації. Наприклад, якщо ви хочете встановити ім'я користувача для доступу до менеджера як адміністратора і встановити пароль, то необхідно виконати:

```
password manager user-name admin
```

CLI запросить у вас пароль. Введіть пароль і натисніть клавішу Enter. Щоб задати ім'я користувача і пароль для доступу оператора, ви повинні використовувати ту ж саму команду «password». Для того, щоб задати ім'я користувача як технічний оператора, виконайте:

```
password operator user-name techie
```

Вас ще раз запропонують ввести пароль.

Для того щоб очистити обидва паролі, тобто залишити комутатор захищеним паролем, виконайте:

```
no password all
```

Перш ніж запустити цю команду Ви повинні бути підключені до комутатора з доступом управляння через Telnet сесію або через консоль.

Багато комутатори також мають кнопку, яку можна використовувати для очищення паролів. Натискання кнопки Clear призведе до очищення паролів, але не скине конфігурацію комутатора до налаштувань за замовчуванням.

Команди налаштування і управління

Таблиця 2.1 - Команди конфігурації, що часто застосовуються

Синтаксис команди	Опис
configure	Перехід від рівня менеджера к глобальному контексту конфігурації
hostname	Визначити ім’я хоста на комутаторі
password	Налаштування захисту паролем для рівнів конфигурації
ip address <subnet mask>	Налаштування IP-адреси для інтерфейсу
interface <int number>	Показати tagged / untagged VLAN статус портів
write memory	Зберегти зміни конфігурації
vlan <vlan-id>	Перехід від глобального контексту конфігурації в контексті конфігурації VLAN
logout	Вийти з інтерфейсу управління
show ip	Показати IP-адресу
show lldp info remote-device	Продивитися інформацію LLDP для поєднання пристроїв
show interface	Показати інформацію про порти Ethernet
exit	Віхід з рівня конфігурації. Приклад, ця команда будет рухатися із контекста конфігурації VLAN до глобального контексту конфігурації.
enable	Привілей менеджера рівня доступу

Після внесення змін в конфігурацію, ви повинні зберегти їх у флеш-пам'яті комутатора. Щоб зробити це, виконайте команду: `write memory`

Рівні доступу

Рівні доступу комутатора являють собою ієрархічну структуру (Рисунок 2.50). Рівень оператора забезпечує доступ тільки для перегляду інформації про

комутатор. Якщо ви хочете внести зміни, ви повинні бути підключені на рівні управління.

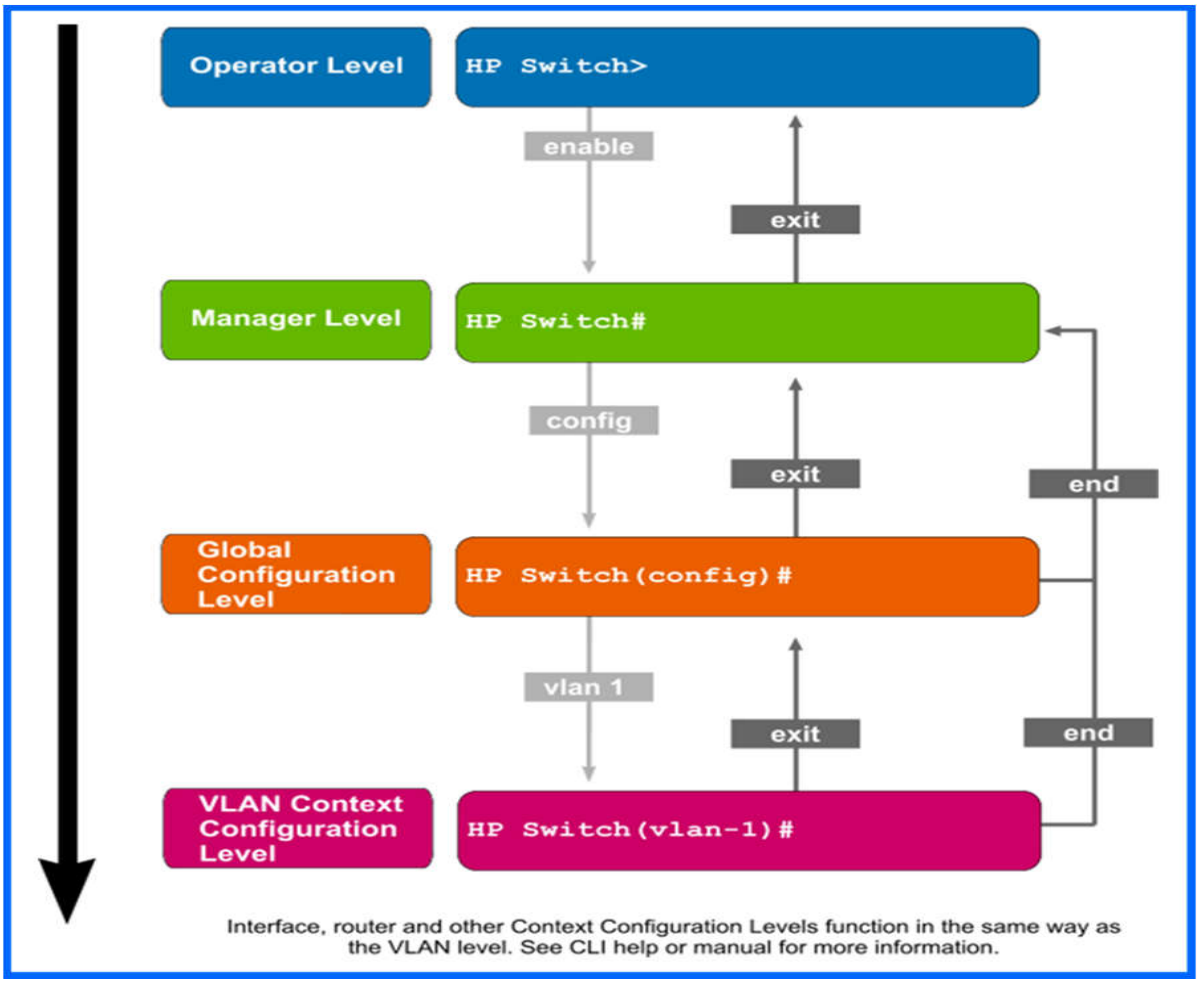


Рисунок 2.50 - Рівні доступу

Глобальний рівень конфігурації (контекст config) і VLAN рівня конфігурації контексту (VLAN контекст) дасть вам доступ до більш потужних, спеціалізованим конфігурацій і командам управління.

Приклади управління

Перед тим як перейти до наступного, ми розглянемо деякі додаткові приклади управління.

Показати приклади команд

Раніше ми розглядали використання команд «show». Команда «show» також дозволяє переглядати інформацію про різні параметри конфігурації. Наприклад щоб побачти список налаштувань VLAN, ви можете запустити:

```
show vlans
```

Щоб побачити інформацію про маршрутизації за допомогою комутатора, виконайте наступну команду:

```
show ip route
```

Ви також можете використовувати команду, щоб переглянути інформацію поділу мережевих комутаторів, що використовують протокол LLDP.

Link Layer Discovery Protocol (LLDP) - TCP / IP протокол канального рівня, який використовується пристроями для обміну служемной інформацією з місних сусідами, такий як: хто вони, їх можливості, і т. д.

Щоб побачити інформацію про місцеві портах і портових ідентифікаторів комутатора, виконайте:

```
show lldp info local-device
```

Щоб побачити інформацію про віддалених комутаторах, виконайте команду:

```
show lldp info remote-device
```

Ви можете отримати більш детальну інформацію про порти, запустивши:

```
show interface
```

Ця команда покаже список портів, переданих та отриманих пакетів, а також список пакетних помилок.

Команди глобальной конфігурації контекста

Ви дізналися вище що контекст «config» (глобальний контекст конфігурації) дає вам доступ до додаткових команд конфігурації. Звідти, ви можете ввести контекст конфігурації для конкретного порту. Якщо ви хочете, управляти портом A10, ви повинні запустити:

```
interface a10
```

Ваша підказка схожа на наступне:

```
switch1(eth-A10)#
```

Деякі з команд управління включають в себе:

```
enable
```

Включення порту (значення за замовчуванням):

```
disable
```

Відключити порт, так що він більше не може бути використаний.

```
speed-duplex
```

Визначити параметри швидкості і дуплексу для порту.

```
mdix-mode
```

Вкажіть підтримку перехресного або прямого кабелю.

```
name
```

Вкажіть ім'я порту, щоб визначити його по імені, або порт ID.

Duplex. В контексті спілкування, дуплекс означає, що користувачі, на обох кінцях, можуть відправляти і отримувати інформацію одночасноuplex.

Контекст рівня VLAN

Якщо ви хочете запустити додаткові команди управління VLAN, необхідно ввійти в віртуальну локальну мережу. При необхідності управління з рядка «config», виберете «vlan context» для VLAN. Спочатку комутатор буде налаштований з однієї VLAN, VLAN-1.

```
vlan 1
```

Ви можете переконається, що ви перебуваєте в vlan по рядку:

```
switch1(vlan-1)#
```

Використовуйте команду «IP» для конфігурації IP в VLAN, наприклад:

```
ip address 192.168.1.14/24
```

Адреса задається за допомогою безкласової междоменной маршрутизацією (CIDR). Про CIDR россказивется пізніше в цьому курсі, але пару слів, все таки,

сказати варто: після "/" визначає кількість бітів в масці підмережі номер, так / 24 еквівалентно масці підмережі:

```
255.255.255.0
```

Якщо це за замовчуванням VLAN комутатора, ви міняєте IP-адреса комутатора. Якщо Ви зайшли, щоб перевірити настройки системи в цій точці, ви побачите, що IP Config встановлений в ручний режим, а IP-адреса і маска підмережі встановлені в значення, які ви вказали.

Ви повинні зберегти ці зміни, якщо хочете, щоб вони були застосовані в наступний раз після скидання. Ви можете зберегти їх звідси, або за допомогою «write memory» в командному рядку.

Історія команд

Ви маєте доступ до недавно виконуваних команд в разі, якщо є необхідність використовувати їх знову. Використовуйте стрілки вгору і вниз для прокрутки команд. Ви можете редагувати командний рядок, якщо необхідно, натисніть клавішу «Enter», щоб виконати команду ще раз. Щоб переглянути список історії команд, запустіть:

```
show history
```

Буде відображена поточна історію командного рядка (Рисунок 2.51).

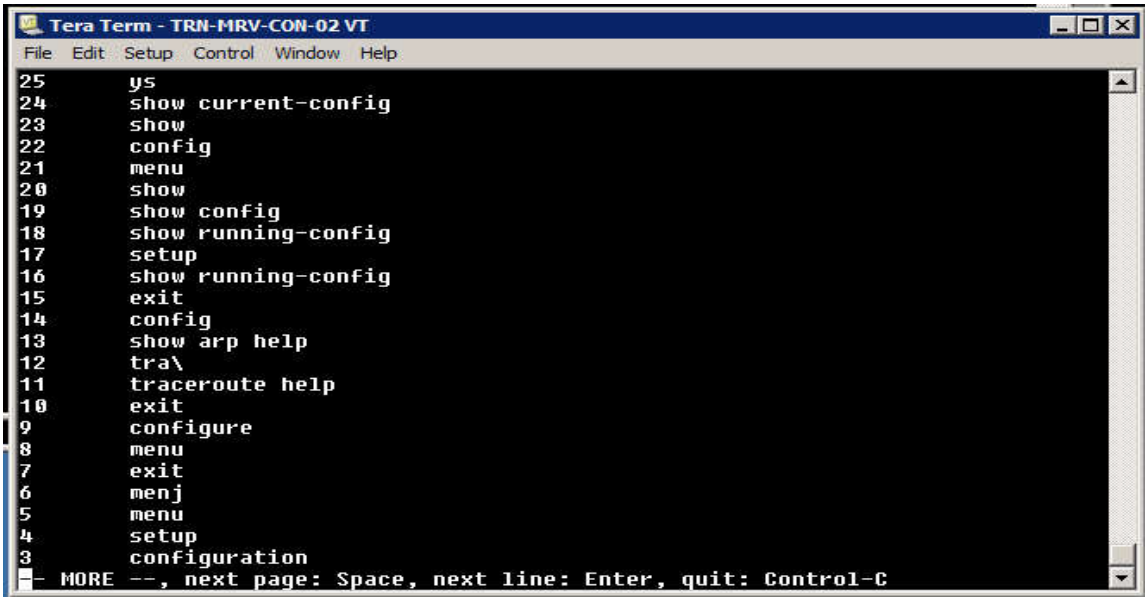


Рисунок 2.51 - Список історії команд

Ви можете виконати команду з історії команд за номером індексу. наприклад:ы можете выполнить команду из истории команд по номеру индекса.

Приклад:

```
repeat 10
```

Розділ 3:
Мережева інфраструктура

Вступ

Перш ніж ви зможете зрозуміти, як функціонує мережа в цілому, ви повинні зрозуміти, як працюють окремі мережеві пристрої. Проте, щоб отримати реальне уявлення про мережу, вам необхідно дізнатися, як ці окремі пристрої працюють разом, щоб сформувати мережеву інфраструктуру. Навіть невелика мережа може бути реалізована в різних формах.

Важливо, зрозуміти ці варіанти мережі, перш ніж розглядати мережеві пристрої більш докладно. У цьому розділі докладно розглядаються дротові та бездротові мережі. Ми досліджуємо мережі засобів масової інформації та варіанти кабельних установок, в тому числі топології і конфігурації, як для дротових, так і бездротових мереж. В процесі, ми зробимо короткий огляд на питання безпеки, пов'язані з веб-функцій.

Ми також витратимо трохи більше часу на сегментацію мережі, і поговоримо про використання периметра мережі для захисту LAN від зовнішньої мережі. Ця лекція так само включає в себе огляд на деякі додаткові технології, в тому числі трансляція адрес, міжмережеві екрани, фаєрволи і проксі-сервери.

Мета

У цьому розділі ви дізнаєтеся, як:

- Описати провідні мережеві характеристики.
- Вибрати відповідний тип кабелю для певного використання.
- Порівняти і зіставити провідні мережеві топології.
- Опис стандартів для бездротових мереж і їх реалізації.
- Порівняти і зіставити бездротові варіанти мережевої безпеки.
- Порівняти і зіставити загальні зміни бездротової мережі.
- Опис призначення і використання основних мережевих технологій:

Підмережі і VLAN.
NAT і PAT.
Брандмауери і проксі-сервери.
VPN.

Проводові мережі

Головна увага в цьому розділі приділяється відомим, добре усталеним технологія. В першу чергу ми поговоримо про конфгурації мережі (LAN конфігурація і підключення локальних мереж через Інтернет).

Незважаючи на зростаючу популярність безпроводових мереж на ділових і споживчих ринках, дротові мережі продовжують домінувати в бізнесі і промисловості. Більшість нових споруд і будівельні ремонти включають плани кабельних трас для кабельного обладнання. Ви могли б запитати себе, чому дротові мережі продовжують використовуватися. Однією з основних причин є те, що мережеві адміністратори виконують і, як правило, використовують технології, які вони вже знають. Проводові мережі були на першому місці протягом десятиліть, так що вся промисловість була створена, щоб тримати їх функціонування належним чином. Можливо, найголовнішим є той факт, що проводові локальні мережі Ethernet і раніше перевищують бездротові мережі в продуктивності і безпеки, тому перехід до безпроводової мережі не має сенсу для багатьох підприємств.

Інші причини для подальшого використання проводових мереж включають в себе:

Доступність

Багато комерційних будівлі підключені до мережі вже при будівництві. Якщо вони ще не підключені, вони, принаймні сконструйовані таким чином, що мають повне уявлення про мережу (з маршрутами для кабелів і комутаційними шафами, розробленими в будівлі).

Надійність

Компанії знають, що вони можуть розраховувати на проводові мережі. Проводове підключення засноване на вже існуючих технологіях. Більшість основних технологій існують протягом десятиліть. Після їх установки, мережеві компоненти, в тому числі кабелі і роз'єми, можуть бути недоторканими протягом багатьох років. Джерела потенційних проблем зв'язку добре відомі і, в більшості випадків їх відносно легко виправити або уникнути.

Встановлені стандарти

Компоненти, пов'язані з проводовим Ethernet слідують встановленим стандартам реалізації в основному способі всієї галузі.

Гнучкість

Більшість функцій доступні при проектуванні і розгортанні проводової мережі. Замість того, щоб створювати конфігурацію з нуля, встановлені конструкції можуть бути змінені, так, щоб задовольнити ваші потреби.

Безпечність

У багатьох сенсах, проводова мережа безпечніша за своєю природою, ніж безпроводова мережа, на крайній випадок, на місцевому рівні. Підключення через мережевий кабель і його потоки даних є більш важкими для перехоплення, ніж перехоплення радіочастотної передачі.

Перевага проводових мереж навряд чи істотно зміниться найближчим часом. Деякі мережеві потреби, такі як далекі, високошвидкісні мережеві з'єднання, просто не можуть бути задоволені поточними безпроводовими технологіями. Крім того, навіть якщо більша частина вашої мережі розгорнута в кабельній мережі, це не єдиний варіант конфігурації. Ви можете з'єднати проводові та безпроводові технології для подальшого розширення ваших варіантів мережі. Мікрохвильове з'єднання точка-точка, яке іноді використовується для з'єднання двох місць. З практичної точки зору, воно діє безпосередньо як кабель між двома точками.

Інфраструктура проводової мережі

Перш, ніж ми звернемо увагу на провідні технології передачі інформації та проводові мережеві топології, ми повинні спочатку розглянути кілька моментів про структуру проводів і проводові мережеві стандарти. Ми почнемо з введення в кабельну систему. Далі, ми звернемо увагу на стандарти Ethernet. Ми обмежимо наше обговорення 802.3 стандартами Ethernet, так як вони на сьогоднішній день є найбільш поширеними мережевими стандартами в експлуатації.

Топологія *- то, яким чином пов'язані між собою мережеві компоненти. Логічна топологія описує потоки даних в мережі, а фізична топологія описує фізичні взаємозв'язку між пристроями.*

Кабельна система *- мережеві провідні інфраструктури.*

Кабельна система

Кабельна система - це кабелі в будівлі. В загальному користуванні, вона відноситься як до мережевих так і до телекомунікаційних (телефонні) кабелям. Вона також визначать лінію поділу (або демаркіроване) між кабелями в будівлі і кабелями зовні будівлі. Місце, де кабелі входять в будівлю іноді називають точкою входу або входом об'єкта. Це те, де телефон, Інтернет і інші телекомунікаційні послуги підключаються до внутрішньої мережі.

Усередині об'єкту, конкретна реалізація кабельної системи може варіюватися, але часто бувають деякі спільні риси. Вони, як правило, мають технічне приміщення, комп'ютерне обладнання, що підтримують мережу. Там також може бути окрема кімната телекомунікаційної підтримки телефонної системи. Якщо у вас є кілька технічних приміщень і телекомунікаційних приміщень, магістральні кабелі використовуються для зв'язку між місцями. Наприклад, у вас магістральний кабель може працювати між поверхами в будівлі або між будівлями в університетському містечку.

Магістральний кабель *- мережевий кабель, який використовується в локальних мережах для ефективного з'єднання на відстані.*

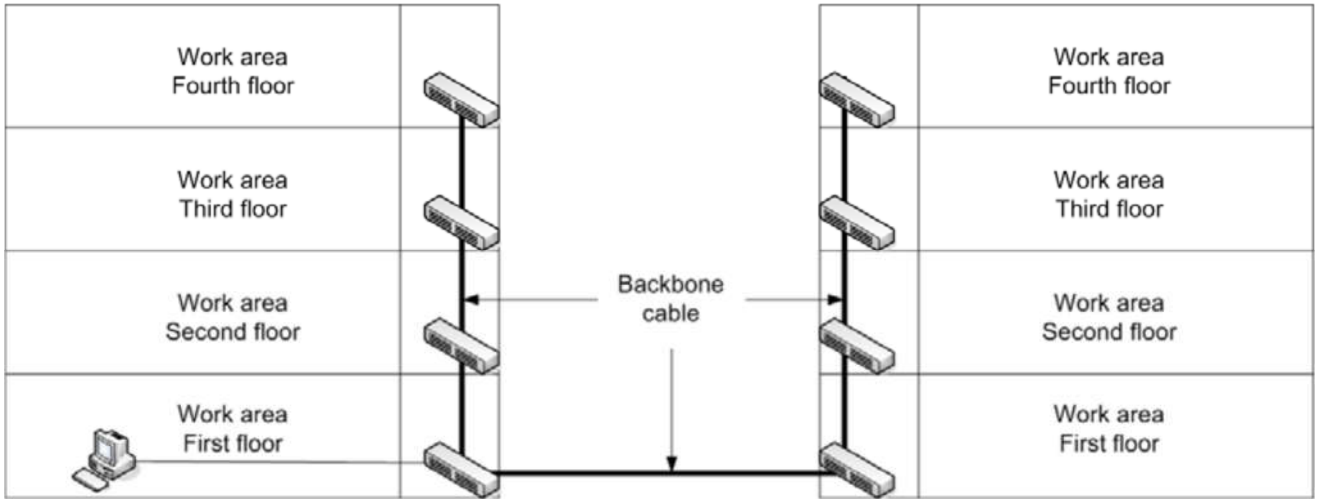


Рисунок 3.1: Магістральні дроти

У робочому середовищі, наприклад, в якості офісної площі або поверху будівлі, кабельна система складається з горизонтальних компонентів розподілу. Це починається з розподілу фреймів в кінцеві точки в технічній кімнаті, а звідти кабелі прокладаються в робоче середовище. Кабелі фізично направляються в робоче середовище за рахунок використання каналів, кабельних підвісок, і кабельних лотків. Канал являє собою пластикову або металеву трубу, яка забезпечує шлях для кабелю і фізично захищає його. Кабельні лотки і кабельні підвіски забезпечують кабелям маршрут і полегшують фізичну напругу на кабель. Площа, що прилягає і через яку прямує кабель зазвичай називають пленум (Рисунок 3.2). Площа плenуму може включати в себе простір над підвісною стелею, область під фальшполом, або відкритий простір між стінами.

Кабельний лоток *- вузький лоток який проходить через області плenуму, в якому може бути покладено кабель.*

Кабельна підвіска *- прості гачки, використовуються для зберігання кабелів в просторі і забезпечують розвантаження кабелю.*

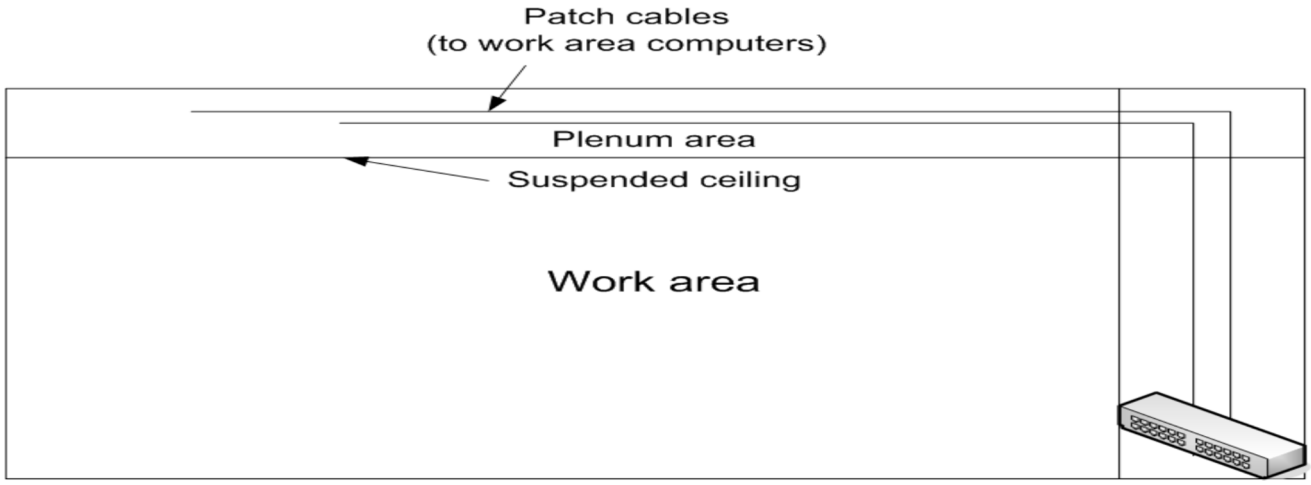


Рисунок 3.2: Приклад горизонтального прокладення

Стандарти Ethernet

Початкові стандарти Ethernet були засновані на коаксіальних кабельних спорудах.

Було два вихідних еталона: **10Base5; 10Base2**

10Base5, також відомий як товстий Ethernet або Thicknet, в першу чергу був використаний в магістральних додатках. 10Base2, також відомий як Thin Ethernet або ThinNet, був використаний для з'єднання з окремими мережевими пристроями.

Ці успадковані технології зустрічаються рідко і не використовуються в нових пристроях. Більшість мережевих пристроїв і майже всі мережеві плати навіть не підтримують роз'єми AUI і BNC використовувані в 10Base5 і 10Base2.

Стандартні технології сьогодні використовують або виту пару або оптоволоконні кабелі. Найбільш поширеними є кабелі на основі стандартів BaseT мідні кабелі. Мідні кабельні стандарти, які ви, ймовірно, побачите включають в себе: **10BaseT; 100BaseT; 1000BaseT; 10GBaseT.**

1000Base-LH - стандарт підтримує роботу на відстані до 80 км в одномодовом волоконному кабелі.

Ці стандарти засновані на використанні кручений пари (Рисунок 3.3). Кабель має кілька мідних проводів, зібраних в пари. Кожна пара буде наполовину скручений по всій довжині проводів, використовується для того, щоб зменшити шанс втручання. Підключення здійснюється через RJ-45 роз'єм.

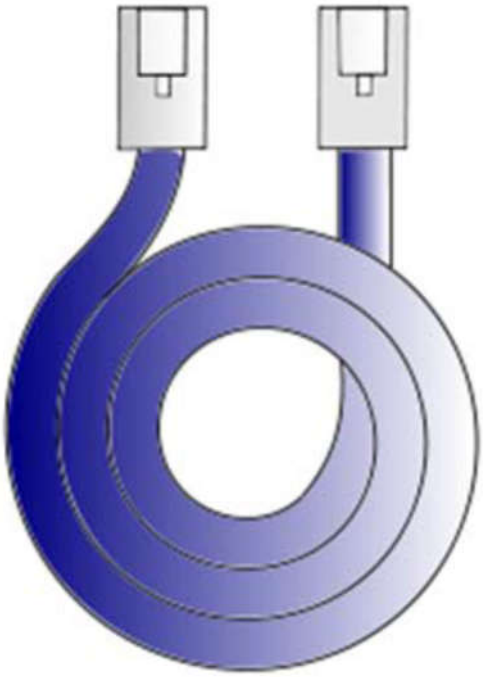


Рисунок 3.3: Вита пара

10BaseT і раніше підтримується, але як правило, служить в якості резервної системи проводки. Більшість мережевих інтерфейсів, що використовують

0BaseT як і раніше підтримується, але як правило, служить в якості резервної системи проводки. Більшість мережевих інтерфейсів використовують 10BaseT тільки в якості запасного варіанту коли основна система проводки має комунікаційні проблеми. Більшість комутаторів автоматично налаштовують швидкість передачі даних портів відповідно до максимальною швидкістю, яку підтримує як перемикачем так і підключеним пристроєм.

Є також різні стандарти Ethernet для волоконно-оптичного кабелю. Найстаршим з них є 10Base-FL. Обмежена максимальна швидкість передачі даних 10 Мбіт, стандарт підтримує кабельні відрізки до 1 км. Інші волоконні стандарти включають в себе: **1000Base-LX; 1000Base-SX; 1000Base-ZX; 10GBase-X.**

Ці всі стандарти підтримують швидкість передачі даних до 1 Гбіт, а для 10GBASE-X - 10 Гбіт. Максимальна довжина сегмента кабелю відрізняється між стандартами, максимальна довжина 10 км для найбільш поширених реалізацій. Поточні реалізації волоконно-оптичних зв'язків засновані на стандарті IEEE 802.3ah. Higherspeed стандарти, в тому числі 40 Гб і 100 Гб Ethernet, знаходяться в стадії розробки, деякі прилади, що працюють на цих швидкостях доступні в даний момент. Проте, реалізація більшості з цих високих швидкостей залежать від виробника.

Мережеві засоби масової інформації

Як уже згадувалося вище, є три основних типи провідних мережевих засобів масової інформації.

До них відносяться:

Коаксіальний кабель;

Вита пара;

Волоконно-оптичний кабель.

Вита пара може бути розділена на STP і UTP. Фізична різниця між ними полягає в тому, що дроти в кабелі STP в оточенні металевою оболонкою, що забезпечує захист від електромагнітних перешкод і радіоперешкод. Ранні використані терміни визначені нижче.

Екранована кручена пара (STP) *- дві або більше пар ізольованих мідних проводів, оточені металевим екраном і зовнішнім діелектриком.*

Неекранована кручена пара (UTP) *- дві або більше пар ізольованих мідних проводів, оточені зовнішнім діелектриком.*

Електромагнітні перешкоди (EMI) *- сигнали перешкоди, викликані випромінюванням або створенням електричного струму поперек магнітного поля (електромагнітної індукції) зовнішнього джерела.*

Вплив радіочастот (RFI) *- форма EMI, що складається з високо частотних (частоти радіохвиль) викидів.*

Коаксіальній кабель

Коаксіальний кабель, показаний на Рисунку 3.4, має центральний провідник, який несе сигнал даних. Він оточений діелектриком, а потім металевим екраном.

Рисунок 3.4: Коаксіальный кабель

Коаксіальний кабель ефективне технологічне спадщина для мереж. Він як і раніше широко використовується для кабельного телебачення і для підключення до супутникової антени або супутникового модему.

Характеристики необхідного кабелю, залежать від того, що ви використовуєте - 10base2 або 10Base5 Ethernet.

10Base2. RG58 A / U кабель. Довжина сегмента максимум близько 185 м.
10Base5. RG-11 кабель. Довжина сегмента максимум 500 м.

Максимальна довжина кабелю будь-якого типу обумовлена фізичними характеристиками кабелю і передається сигналом. Сигнал втрачає силу на відстані, це процес, відомий як ослаблення (Рисунок 3.5). Після проходження відстані, сигнал стає надійним. Це відноситься як до провідних так і до бездротових передачам.

Ослаблення - втрата сигналу (амплітуди сигналу) на відстані.

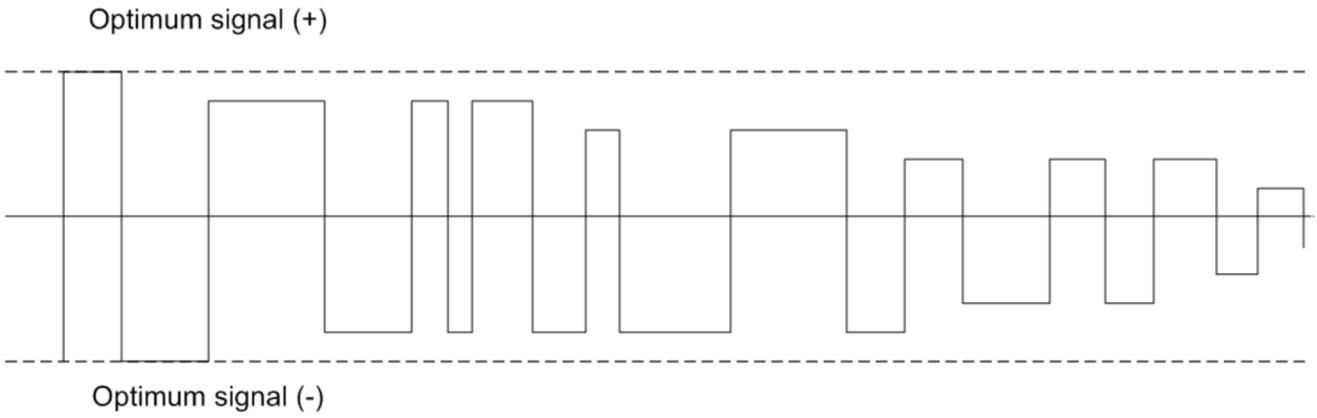


Рисунок 3.5: Ослаблення

У прикладі, пунктирні лінії показують оптимальну силу сигналу. Сигнал починається в оптимальному стані, але чим далі він проходить послабляється.

10Base2, є найбільш поширеною реалізацією, використовувалася коли обидва пристрої були підключені безпосередньо до кабелю або до ланцюга. З'єднання були реалізовані за допомогою роз'єму BNC, показаний на Рисунку 3.6. На обидва типи кабелю по їх кінцях були встановлені резистори по 50 Ом, щоб забезпечити якість сигналу.

Рисунок 3.6: BNC роз’єднувач

Є кілька причин, чому коаксіальний кабель втратив рентабельність в мережевих реалізаціях. У порівнянні з кручений парою, з ним досить важко працювати, коаксіальний кабель не є достатньо гнучким, щоб зігнути його під гострим кутом. Основні коаксіальні конфігурації також дуже складно усунути. Проблема в будь-якому місці вздовж траси кабелю, на обох кінцях або з будь-якого підключеного пристрою може викликати помилку мережі.

Вита пара

Майже всі поточні конфігурації мережі використовують виту пару. Більшість розгортання використовують UTP кабель, який легше у використанні і дешевше, ніж STP кабелю. STP кабель зазвичай використовується тільки тоді, коли екологічні чинники вимагають цього, наприклад, джерела електромагнітних завад, розташовані поблизу кабелів. Вита пара має кілька переваг у порівнянні з коаксіальним кабелем, які сприяли його швидкому впровадженню. Основними серед цих переваг були вартість та простота установки. Це було просто дешевше для розгортання мережі з допомогою кручений пари, а не коаксіальногокабелю. Крім того, більшість офісів вже створені з підтримкою кручений пари для роботи в офісі телефонних систем.

Телефонні системи використовувати більш низькі якісну виту пару, ніж мережеві системи. Телефонний кабель не повинен бути використаний для сучасних мережевих додатків, хоча телефонні системи можуть використовувати один і той же UTP кабель, який використовується для мереж передачі даних. Крос-з'єднання систем на розподіл кадрів буде зберігати інформацію і голосові дроти розділеними. Часто сьогодні, телекомунікаційний трафік здійснюється в TCP/IP-пакетів з мережевого кабелю, щоб голосові сигнали пускалися в мережі передачі даних. Це часто згадується як передача голосу по IP або VoIP.

Крос-комутаційні системи - пристрій цифрового перемикання використовується для маршрутизації телекомунікаційного трафіку.

Стандарти витої пари

Стандарти витої пари називаються кабельними категоріями. Є кілька стандартів по всьому світу, які визначають ці категорії. На додаток до категорій, перерахованих тут, є категорії, які поки не (або ніколи не були) використовуються в мережевих додатках.

Поточні категорії перераховані в таблиці 3-1.

Таблиця 3-1: категорії витих пар

Категорія	**Пропускная спроможність**	
Cat 3	16 MHz	10BaseT
Cat 5/5e	100 MHz	До Gigabit Ethernet
Cat 6	250 MHz	Замена 5e Cat

Cat 6e	500 MHz	До 10 Gigabit Ethernet
Cat 7	600 MHz	10 Gigabit Ethernet

Категоріям Cat 5e, Cat 6 і Cat 6e доступний STP або UTP кабель. Cat 7 кабелі, як правило, екрановані, а іноді і використовуются нестандартні роз'єми. Максимальна довжина кабелю, як правило, визначається як 100 м. Довші кабелі приведуть до деградації сигналів через загасання і перехресних перешкодами між парами. Ця проблема особливо видно в кабелях, які містять кілька пар. Це часто можна побачити в кабелях, що містять до 25 пар в професійних електродротах. При необхідності більш далеких передач використовують волоконно-оптичний кабель замість кручений пари.

Перехресні перешкоди - сигнал перешкоди між проводами працюють паралельно.

З'єднання витих пар

У невеликих установках, пристрої можуть підключатися безпосередньо до центральної станції або комутатора. Це не практично в середніх і великих установках. Замість цього, з'єднання зазвичай виконуються в кросі з мультипарних кабелів, які йдуть під стіною в плиті по всьому офісу. Остаточний підключення проводиться за допомогою кабелю з роз'ємом RJ-45 (Рисунок 3.7) на кожному кінці.

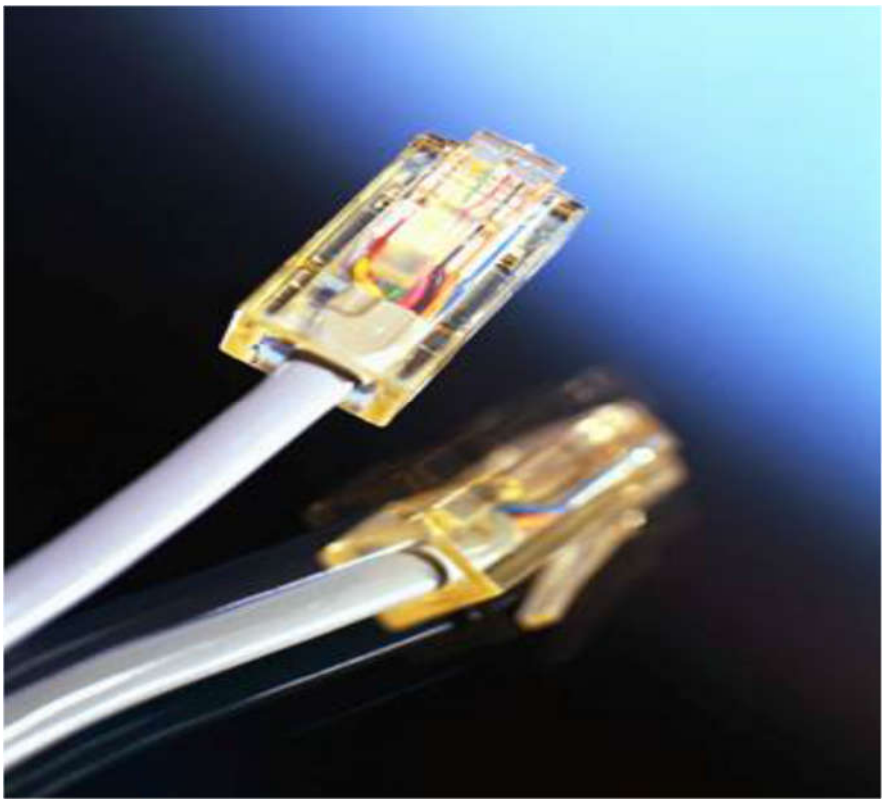


Рисунок 3.7: З'єднання RJ-45

Старі монтажні шафи іноді мають один і той же тип патч-панелей, як для телефону і так і для підтримки мережі. Ці панелі вимагають плінти, щоб створити з'єднання. У плінтах закуси дуже тісно розташовані, для того щоб проколоти окремі дроти і щоб зробити зв'язок. Вони дуже складні у використанні, і також вимагають спеціальних інструментів для підключення до панелі.

Патч-панель *- Центральна точка підключення і панель розподілу кручених пар, в тому числі телефонних систем і мережевого кабелю.*

Плінт *- традиційний спосіб підключення кручений пари всередині патч-панелі.*

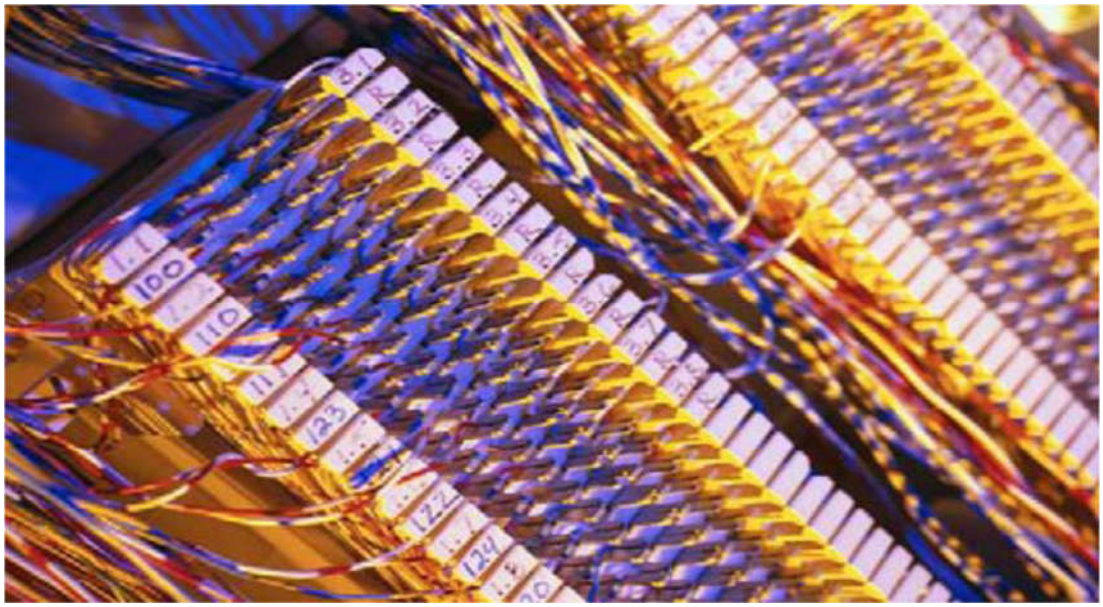


Рисунок 3.8: Плінт

У більшості сучасних мережевих установок використовуються патч-панелі з модульними роз'ємами (Рисунок 3.9). Патч кабелі прокладаються між комутатором і патч-панеллю. Звідси, проводка поширюється по всій території.

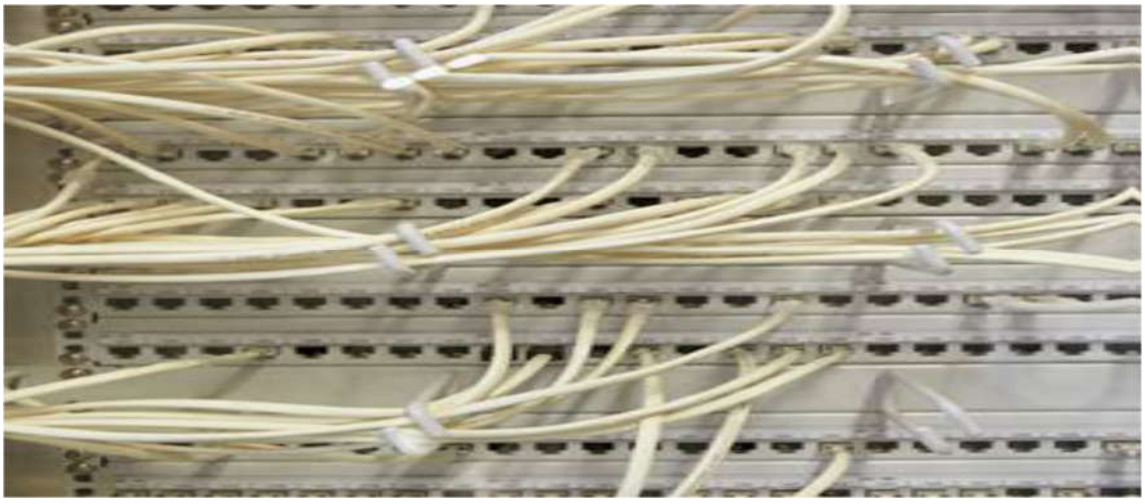


Рисунок 3.9: Модульна патч-панель

Більшість модульних патч-панелей можуть бути розширені. Це означає, що ви можете розширити свою мережу, підключивши додаткову панель розширення, замість того, щоб купувати і встановлювати повністю нову панель.

Більшість також дозволяють видалити один або кілька наборів модульних роз'ємів, щоб дати вам прямий доступ до комутаційної панелі внизу. Іноді це необхідно для усунення неполадок і ремонту або для деяких спеціальних застосувань установки.

Опто-волоконний кабель

Волоконно-оптичний кабель, як показано на Рисунку 3.10, спочатку вважається виправданим тільки в особливих випадках, особливо коли дуже довгі, дуже високі швидкості з'єднання були необхідні. Він знайшов свій шлях у багатьох конфігураціях LAN в ситуаціях, коли він краще підходить, ніж мідний кабель.

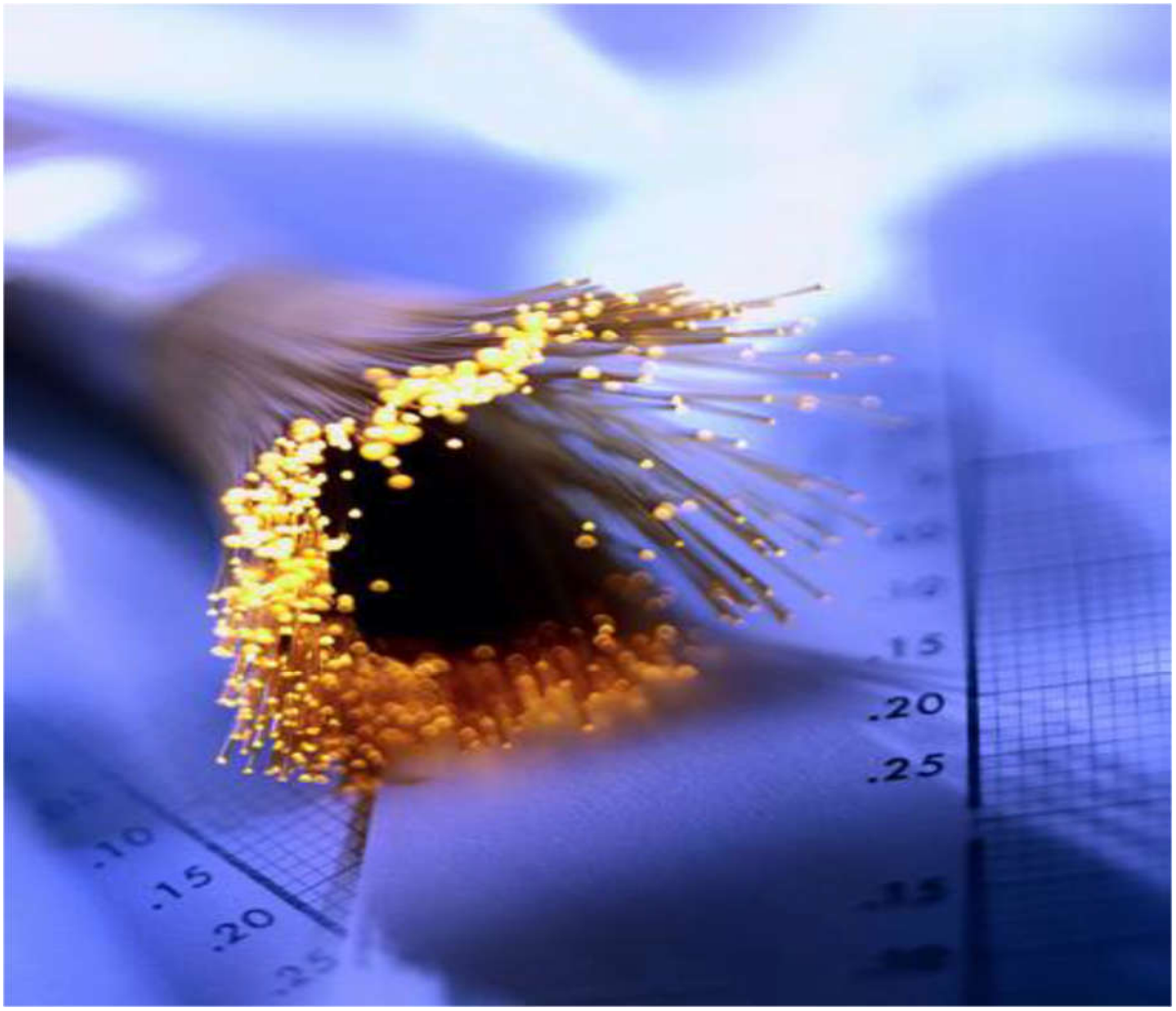


Рисунок 3.10: Волоконно-оптичний кабель

Волоконно-оптичний кабель використовується, коли EMI занадто висока, щоб використовувати мідний дріт. Досить високий рівень EMI може заважати навіть STP кабелям. Він також використовується, коли необхідно надати надійне і високошвидкісне з'єднання між мережевими пристроями. Наприклад, ви могли б

використовувати волоконно-оптичний кабель для підключення високопродуктивних серверів прямо до мережевого сховища. Волоконно-оптичний кабель також вибирається для багатьох додатків з високим рівнем безпеки. Підключення до мережі через волоконно-оптичному кабелю і перехоплення даних надзвичайно важке. Навіть тоді, коли волоконно-оптичний кабель пропускає такі спроби вони будуть легко виявлені, так як вони відразу ж обривають зв'язок в кабелі. Інший ринок, який є рушійною силою прийняття оптоволоконного кабелю для мережевих додатків є ігровий. Мережі, створені спеціально для підтримки комп'ютерних геймерів оптимізовані для максимальної продуктивності, часто потребують підтримки типових швидкостей передачі даних, що перевищують пікові швидкості передачі даних в більшості мереж SMB. Волоконно-оптична мережа не є універсальним рішенням для всіх мережевих ситуацій. Вона відносно дорога. Сам кабель досить крихкий, і його важко правильно встановити. Наприклад, деякі розгортання вимагають спеціальної підготовки, щоб правильно завершити і підключити кабель.

Використання волоконно-оптичного кабелю

Більшість комп'ютерів не мають наперед визначеної волоконно-оптичної підтримки, але є і виключення. Комп'ютери, які виступають в якості мережевих серверів мають вбудовані (або встановлені) волоконно-оптичні адаптери. Те ж саме можна сказати і про багатьох топових ігрових машинах. Волоконно-оптичні з'єднувачі приймають різні форми в залежності від того де вони конкретно применять (Рисунок 3.11). Більшість додатків використовують два волокна, один для відправки і інший для отримання. Пристрої, які використовують волоконно-оптичний кабель з'єднані в конфігурації послідовного ланцюжка, так що дані проходять через кожне пристрій по дорозі до місця призначення.

Рисунок 3.11: Волоконно-оптичний разєднувач

Одна з переваг конфігурації послідовного ланцюжка полягає в тому, що сигнал на кожному пристрої регенерується. Загасання потенційна проблема в

волоконно-оптичному кабелі, так само як і в мідній кабелі. Проте, на відміну від мідного дроту, сигнал в волоконно-оптичному кабелі оновлюється на кожному пристрої і кожної з'єднаної ланцюжком. Оптичні з'єднання зазвичай використовують SFP (або SFP+) трансивери, показані на Рисунку 3.12, як закінчення на комутаторі. Є види трансиверів, спрямовані на підтримку загальних багатомодових і одномодових волоконних стандартів.

Рисунок 3.12: HP X130 10G SFP + LC ER 40km Transceiver

Малий форм-фактор (SFP)

- підключається модульний трансивер підтримує всі мережеві інтерфейси і телекомунікаційні додатки. Замінює більш ранній інтерфейсний перетворювач Gigabit (GBIC).

Посилений малий форм-фактора (SFP +)

- поліпшена версія стандарту SFP, призначеної для підтримки 10 Гбіт додатків.

Кабельні мережеві топології

Ваша мережева топологія дещо залежить від вашого протоколу низького рівня зв'язку. Ethernet був спочатку розроблений для використання технології шини; в той час як Token Ring використовує (Не дивно) кільцеву топологію. Перш ніж намагатися розробляти або підтримувати мережі, ви повинні розуміти мережеві топології і як вони використовуються. Наша дискусія зосереджена на чотирьох загальних мережевих топологіях:

Зірка;
Шина;
Кільце;
Сітка.

Кожна топологія має свої сильні і слабкі сторони.

Зірка

У топології зірка, кожен вузол з'єднується з центральним вузлом за допомогою бездротової технології точка-точка, як показано на Рисунку 3.13. Метод доступу до мережі буде залежати від використаного протоколу низького рівня розгортання в мережі.

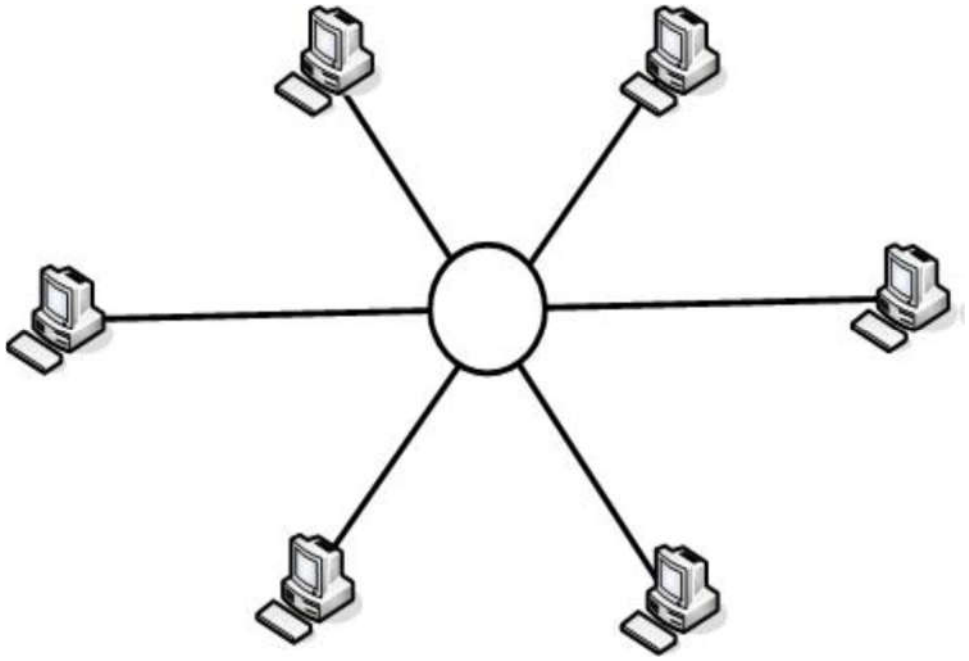


Рисунок 3.13: Топологія Зірка

Навіть якщо мережа Ethernet може виглядати як топологія зірка, це не справжня зірка, через те як проходить доступ до мережі і управління. Оригінальні стандарти Ethernet вказують топологію шини, хоча це рідко використовується на практиці.

Частою зміною топології зірка є розподілена зірка (Рисунку 3.14). У розподіленої зірки є концентратори, які з'єднані один з одним, щоб розширити мережу.

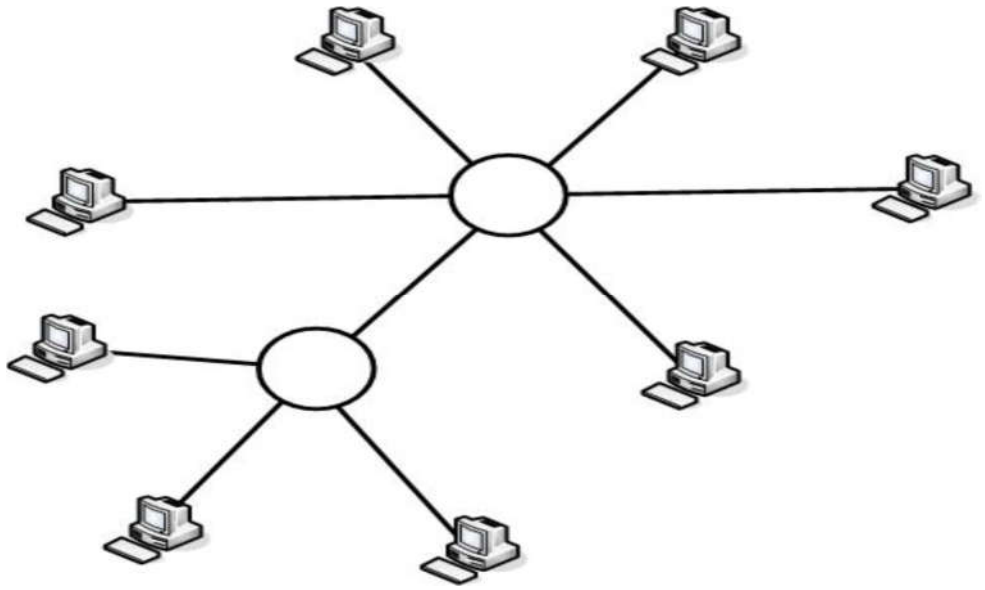


Рисунок 3-14: Топологія расподілу зірки

На справді конфігурації топології зірка дуже рідко видно в реалізаціях LAN. Проте, з'єднання точка-точка, зроблені між хостами і комутаторами виглядають як зіркоподібна топологія. Центр зірки відрізняється від комутатора Ethernet або концентратора тим що трафік управляється в центральному підключенні.

Шина

Ethernet був розроблений навколо логічної топології шини (Рисунок 3.5). Всі вузли мережі підключаються безпосередньо до мережевого кабелю. Теоретично, кожен вузол має рівний, загальний доступ до кабельного сегменту. Через обміну такими даними, можуть розвинутися черзі і повільна швидкість передачі, коли два вузла намагаються передавати інформацію одночасно. Кожен кінець кабелю сегмента припиняється резистором, щоб сигнал не відбивався назад і вперед по кабелю.

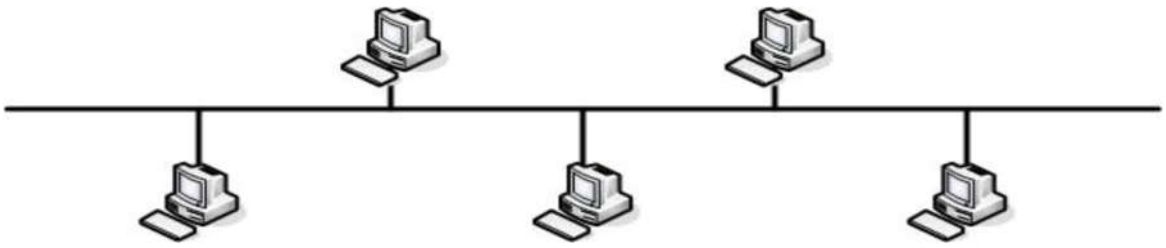


Рисунок 3.15: Топологія шини

У топології шини, при кожній передачі всі вузли отримують фактично той же самий час. Якщо передача не адресована конкретному вузлу (або адресою в ефірі), вузол буде ігнорувати передачу. Цей тип топології шини іноді називається лінійним. Одна з проблем в цій топології є те, що проблеми спілкування важко усунути. Проблеми з термінатором на будь-якому кінці, або коротку перерву або

проблема в будь-якому місці в кабельному сегменті, може викликати проблеми зв'язку по всьому сегменту.

Як згадувалося раніше, при монтажі за допомогою концентратора (або комутатора), сегмент Ethernet виглядає як фізична зірка. Концентратор має внутрішньо проводове мовлення, як на шинному підключенні в центральній точці. Концентратор виступає в якості центральної точки підключення.

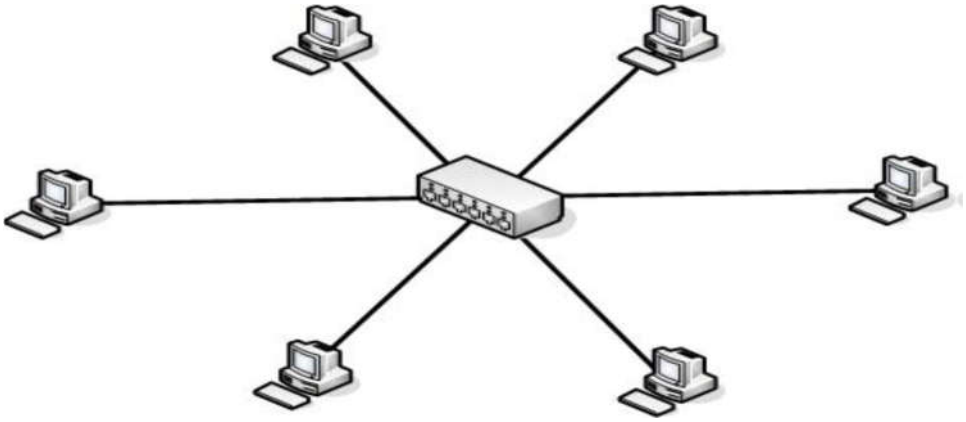


Рисунок 3.16. Подключення с хабом

Коли використовується комутатор, він компенсує одне зі слабких місць топології шини. Перемикач додає контроль трафіку по буферизації передачі в порту, тим самим уникаючи більшості зіткнень. Порти комутатора можна налаштувати так, що вони діють як єдиний сегмент кабелю для цілей адресації.

Кільце

У кільцевій топології, вихід одного вузла є входом наступного вузла в істинної шлейфової конфігурації. Кожен вузол діє як повторювач, підвищуючи сигнал при передачі до наступного вузла в ланцюжки.

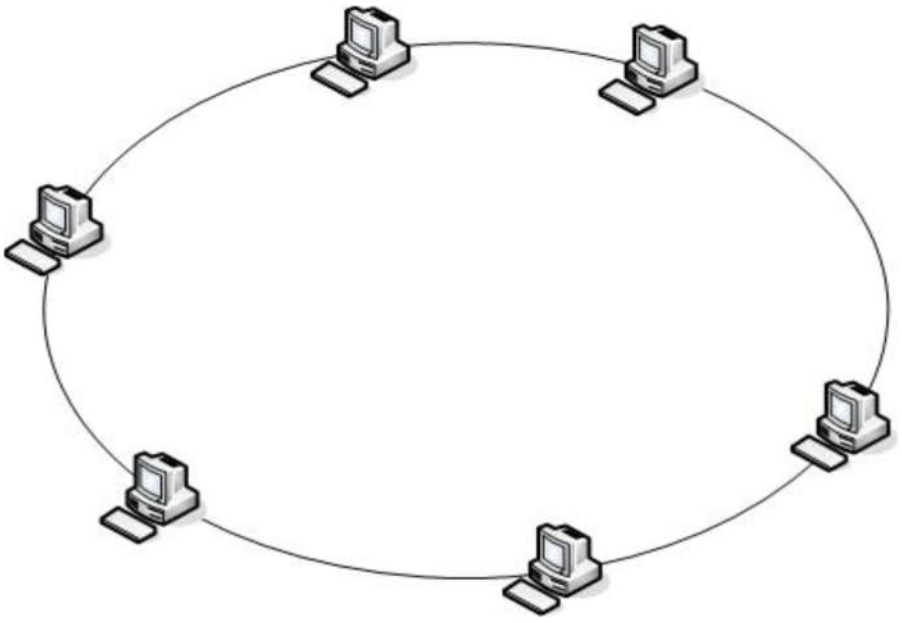


Рисунок 3.17. Топологія Кільця

Протокол від IBM Token Ring використовує кільцеву топологію. Пакет даних, відомий як маркер, передається від вузла до вузла по мережі. Вузол може завантажити маркер з даними, який передається по всьому сегменту, поки не досягне своєї мети. У цей момент, дані вивантажуються з маркера і порожній маркер і передається до наступного вузла.

Деякі топології "Кільце" використовують подвійне кільце, тобто, два кільця, які посилають сигнали в протилежних напрямках. Це дає можливість кільцю працювати так, щоб компенсувати розрив або несправний вузол до тих пір, поки проблема не буде усунена.

Сітка

У суцільній мережі (Рисунок 3.18), кожен вузол в мережі пов'язаний з кожним іншим вузлом. Ні центрального вузла в даній конфігурації, так само як немає ніякого центрального вузла в зоряній конфігурації. Вона надає кілька каналів зв'язку для передачі даних. Вона також вимагає протокол, який управляє маршрутами прийнятих даних, щоб уникнути петлі. Трафік через ці петлі, якщо він не ретельно контролюється, може привести до поломки мережі зв'язку через широкомовних штормів.

Петля - *шлях зв'язку, де дані йдуть по колу без кінцевого пункту призначення.*

Широкомовні шторми *- ситуація, в якій трансляцій неодноразово повторно відправляється, споживаючи ресурси мережі і запобігаючи доставку нормального мережевого трафіку.*

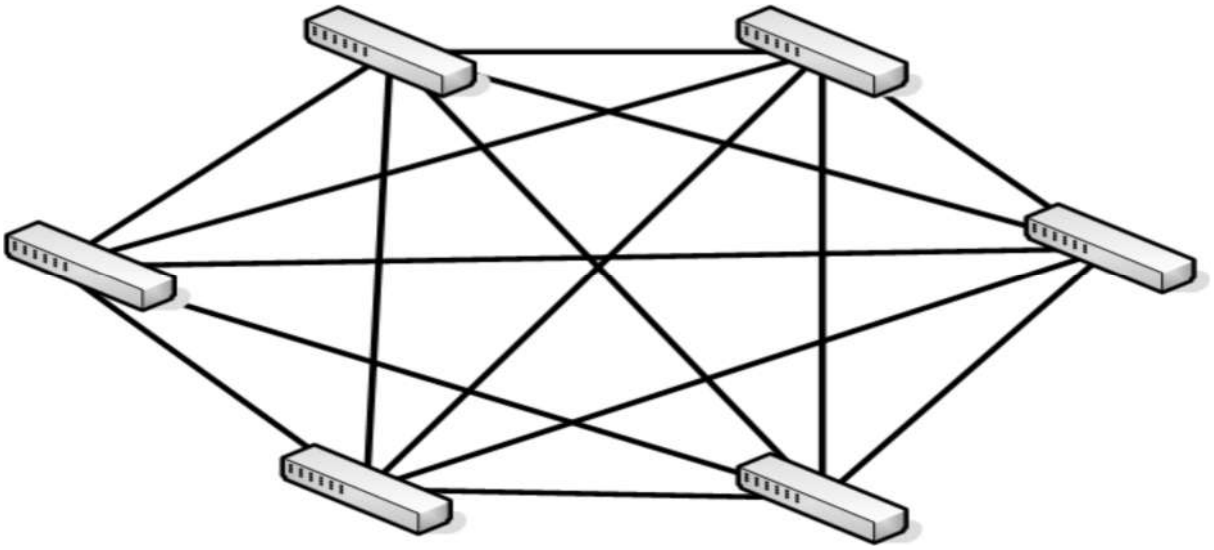


Рисунок 3.18. Топологія Сітка

Одією з переваг цієї топології є те, що вона може компенсувати невдачі. Численні з'єднання дозволяють маршрутизацію даних по всім відсутнім вузлів або розривів в сполучної кабельної системи. Найвідоміший приклад частічтой мережі є Інтернет з його незліченними зв'язками. У багатьох випадках, це більш обмежені сітки або часткове сітки (Рисунок 3.19), а не повністю підключена мережа.

Часткова сітка - топологія мережі, де деякі вузли не підключені до будь-яких інших вузлів.

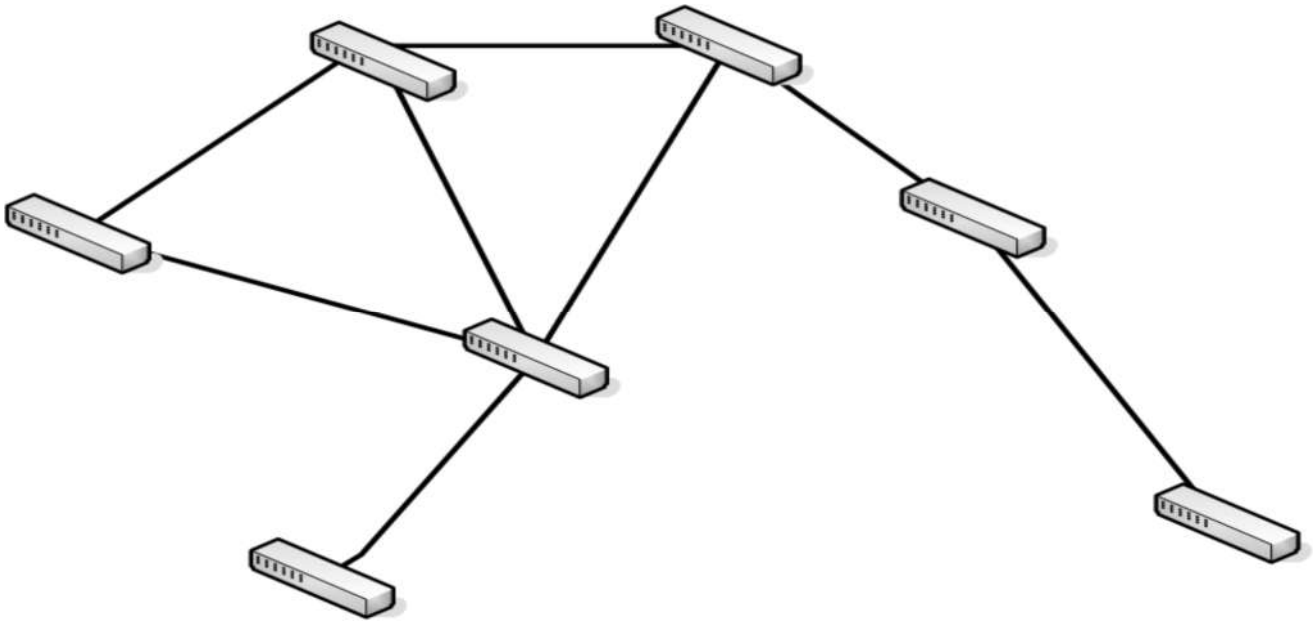


Рисунок 3.19: Часткова мережа

Навіть в часткової сітці, все ще існує можливість створення нескінченного циклу.

Огляд безпеки проводових мереж

Важливою частиною будь-якого розгортання мережі є надання належної безпеки для мережі, його комп'ютерів, і його даних. Більшість заходів безпеки реалізовані на більш високих рівнях в OSI моделі, але є деякі речі, які можна зробити в кабельній системі.

Ви повинні захистити фізичну мережу, щоб запобігти від несанкціонованого перехоплення в мережі кабельної системи. Відкритий кабель повинен бути зведений до мінімуму. Якщо ваш об'єкт має монтажну шафу, вам необхідно тримати його забезпечення на весь час. Ви також повинні періодично інвентаризувати мережі, щоб переконатися, що там не було ніяких сторонніх (і, можливо компрометуючих) змін.

Ви також повинні захищати засоби доступу до мережі від зовнішнього світу. Трохи пізніше в цій главі ми пояснимо, як реалізувати ці заходи безпеки.

Бездротова мережа

Існує велика ймовірність, що ви вже використовуєте бездротову мережу, можливо, навіть не усвідомлюючи цього. Бездротові комунікації є звичайним явищем і для стільникових телефонів системи забезпечують майже всесвітній охоплення. Системи топології мережі бездротової мережі з веж стільникового зв'язку забезпечують покриття в більшості районів.

Бездротові комп'ютерні мережі тепер стали звичайним явищем. Вони є найбільш популярним способом спілкування в будинку, тому що немає необхідності запускати фізичну кабельний систему і вони користуються популярністю в багатьох офісах, особливо з-за їх гнучкості і відносною легкістю управління. Ви навіть можете знайти публічні мережі Wi-Fi в місцях, де люди збираються, таких як бібліотеки, коледжі та ресторани (Рисунок 3.20).

Рисунок 3.20: Символ безкоштовної Wi-Fi

Wi-Fi точки доступу знаходяться навіть в найнесподіваніших місцях, наприклад в пральнях. У деяких містах навіть по всьому місту є Wi-Fi, щоб забезпечити всіх громадян безкоштовним доступом в Інтернет. Нові технології Wi-Fi і оновлені мережеві пристрої висуваються на постійній основі, постійно розширюючи можливості бездротових мереж.

Гаряча точка *- місце з бездротовим підключенням Wi-Fi.*

Ви вже познайомилися з бездротовим стандартом 802.11 раніше. Сучасні бездротові пристрої призначені для підтримки 802.11n, але в стані також підтримувати пристрої, які мають 802.11a/b/g бездротові адаптери. Таким чином, ви можете продовжувати використовувати старі бездротові пристрої без їх модернізації.

Є кілька потенційних переваг, доступних через бездротові мережі, в тому числі:

Простота розгортання;

Вимоги до обладнання мінімальні і немає, як правило, немає необхідності, щоб прокладати кабель;

Підтримка мобільних користувачів;

Мобільні користувачі або користувачі, які знаходяться в офісі, періодично можуть легко підключатися до офісної мережі;

Взаємозв'язок з проводовою мережею.

У вас є можливість підключення безпроводлвих мережевих клієнтів з проводовою мережею, даючи їм повний доступ до мережевих ресурсів.

Іноді обмеження, які потрібні, щоб використовувати безпроводову мережу є законними, а не фізичними. Наприклад, ви могли б бути налаштувати мережу в історичній будівлі і юридично заборонити робити фізичні зміни або запуск комп'ютерного кабелю.

Бездротові мережеві конфігурації

Для пристрою що використовує безпроводову мережу необхідний безпроводовий адаптер. Майже всі мобільні комп'ютери і смартфони (багато ноутбуки, планшети і т.д.) мають вбудований Wi-Fi адаптер. Багато настільних комп'ютерів мають вбудований Wi-Fi адаптер. Є також різні стилі безпроводових адаптерів які легко доступні.

Рисунок 3.21: USB Wi-Fi адаптер

Хоча можна знайти безпроводові адаптери, які встановлюються в якості розширення, вони є більш поширеним, виглядають вони як пристрої, які підключаються до вільного USB порту (Рисунок 3.21).

Існує два основні варіанти конфігурації, які підтримуються для безпроводових мереж:

Одноранговий режим;

Режим інфраструктури.

Вибір режиму залежить від ваших вимог до мережі. Робочий режим налаштовується за допомогою властивостей безпроводового адаптера.

Одноранговий режим

Одноранговий режим, також відомий як режим точка-точка, це найпростіша конфігурації для реалізації, але не підходить для більшості середовищ SMB. Насправді, однорангова іноді недоречна навіть для домашніх мереж.

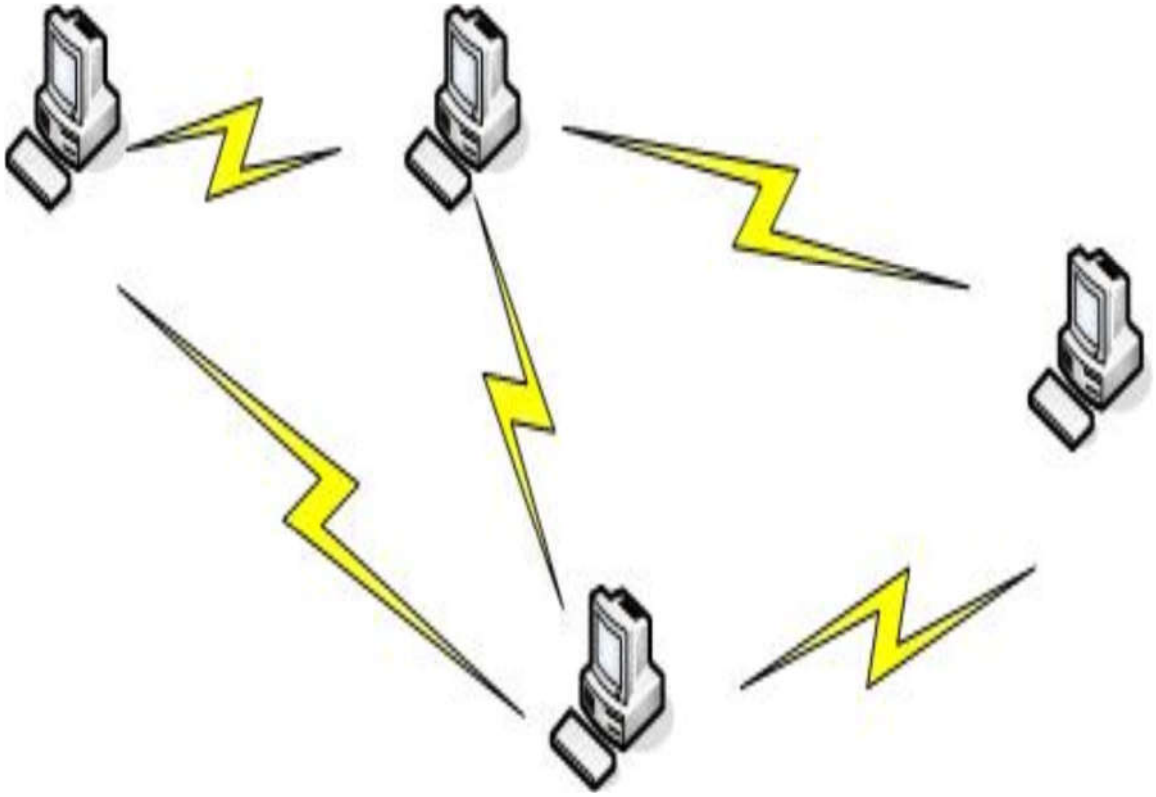


Рисунок 3.22. Режим однорангової мережі

В одноранговому режимі, бездротові пристрої безпосередньо спілкуватися один з одним. Це дає їм змогу обмінюватися файлами і іншими ресурсами один з одним, але не з іншими провідними мережевими пристроями. Тимчасова мережа обмежується не більше ніж дев'яти клієнтськими пристроями. Два пристрої повинні бути в межах діапазону покриття друг від друга, щоб спільно використовувати ресурси. Там немає організованого методу для подолання або ретрансляції даних між пристроями. Ви виявите, що ефективні конфігурації безпроводової безпеки засновані навколо використання точки доступу (AP) в якості центрального контактного пункту для бездротового зв'язку.

Точка доступу (AP) *- центральний пункт зв'язку для безпроводових мереж. Точка доступу забезпечує зв'язок між безпроводовими пристроями і може підтримувати зв'язок до проводової мережі.*

Інфраструктурний режим

У стандартній конфігурації для більшості безпроводових адаптерів, підтримується тільки інфраструктурний режим. У режимі інфраструктури безпроводові пристрої взаємодіють через AP (Рисунок 3.23), а не спілкуватися один з одним безпосередньо.

Рисунок 3.23: MSM422 точка доступу

У постійному робочому режимі вимагає принаймні одну точку доступу і один комп'ютер (або інше бездротове пристрій). Конфігурація може включати в себе кілька точок для розширення діапазону мережі. Ви також можете підключити AP до проводової мережі, щоб дати безпроводовим клієнтам доступ до проводових мережевих ресурсів (Рисунок 3-24).

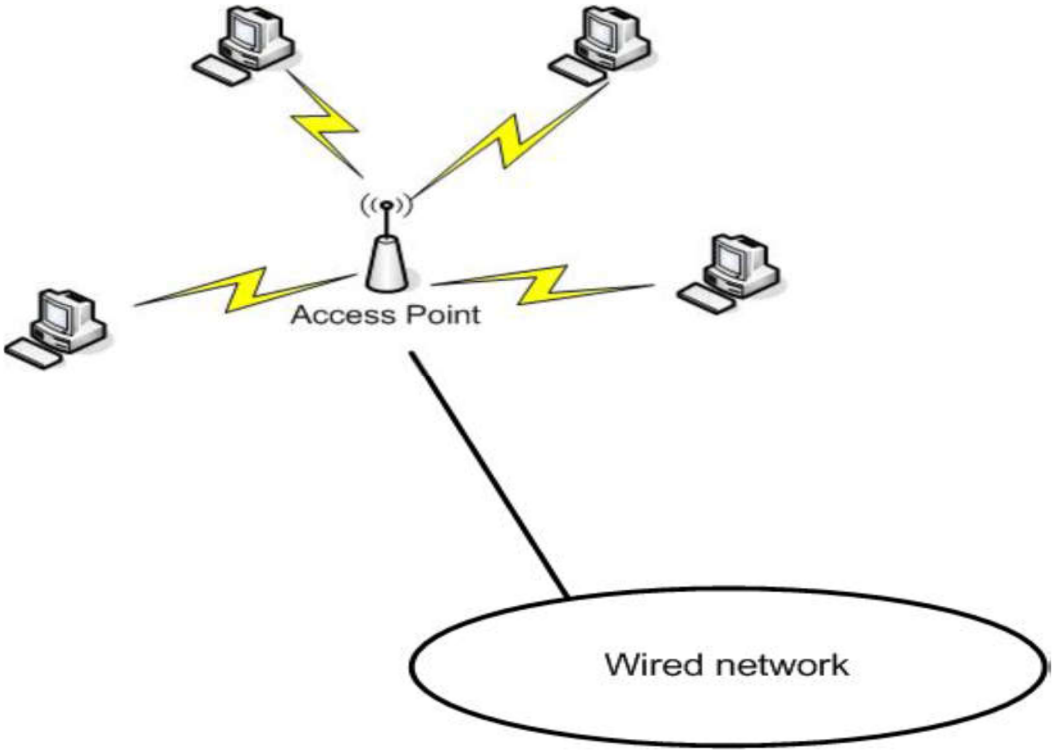


Рисунок 3.24. AP Підключення до проводової мережі

Не тільки ця конфігурація найбільш підходяща для більшості потреб малого та середнього бізнесу. Це також найпопулярніша конфігурація для домашніх мереж. Одна з основних причин по якій багато людей використовують цю конфігурацію для домашньої мережі, це те що вона дозволяє їм використовувати підключення до Інтернету з високою пропускною здатністю з їх безпроводових пристроїв.

Огляд безпеки безпроводової мережі

Головною проблемою безпроводових мереж є те, що ви могли б забезпечувати гарячу точку для незнайомців. Один із способів, який виявляє незахищені або слабо захищені бездротові мережі це вардрайвінг.

Вардрайвінг *(англ. Wardriving) - процес пошуку і злому уразливих точок доступу безпроводових мереж Wi-Fi людиною або групою осіб, оснащених переносним комп'ютером з Wi-Fi-адаптером. При цьому для просторового пошуку і локалізації точки використовується транспортний засіб (звідси і назва - бойове водіння).*

Якщо ваша мережа виявлена через вардрайвінг, ви можете стати жертвою вархакінга. Якщо так, то ви знайдете цей символ написаний крейдою на тротуарі біля вашого офісу:

Рисунок 3.25: Символ вархакінга

Вархакінг - *маркування доступних бездротових мереж крейдою.*

Це символ вказує на незахищене Wi-Fi з'єднання, відкрите запрошення для людей, щоб скористатися вашою безпроводовою мережею і, найчастіше, вашим інтернет-зв'язком. Як мінімум, це може погіршити продуктивність мережі. У

гіршому випадку, це виставить ваші мережеві ресурси зловживання і втрат. Несанкціоновані користувачі можуть вкрасти або видалити загальні дані.

Стандарти 802.11 і 802.1X визначають кілька параметрів безпеки, щоб допомогти вам захистити вашу мережу. Реалізація цих стандартів не завжди гарантує, що ваша мережа буде залишатися в безпеці, але вони будуть проходити довгий шлях до захисту. Це не заважає вархакінгу. Проте, це змінить статус вашої мережі з незахищеного Wi-Fi в захищений Wi-Fi (Рисунок 3.26).

Рисунок 3.26: Защищенный Wi-Fi

Доступні опції безпеки включають в себе:

Фільтрація MAC-адрес

Дозволяє або блокує доступ до точки доступу, заснованого на MAC-адресу комп'ютера клієнта. Це легко обійти, підробкою MAC-адрес.

Wired Equivalent Privacy (WEP)

Метод шифрування даних, що використовується для шифрування даних, що передаються між бездротовими вузлами. Шифрування легко зламуються і тому не рекомендується для використання в будь-якому додатку.

Wi-Fi Protected Access (WPA)

Тимчасова аутентифікації і шифрування стандартів призначених для заміни WEP і виправити деякі з його найбільш значущих недоліків.

Wi-Fi Protected Access 2 (WPA2)

Стандарт 802.11i, який визначається поліпшеною мережевий аутентифікації і шифрування.

Ці захисні і шіфровочние методи призначені для використання з іншими методами забезпечення безпеки мережі, наприклад, вимагаючи аутентифікація користувача для доступу до мережевих ресурсів, установка безпеки доступу до файлів та інших ресурсів, увійшовши в мережеву активність, і так далі.

Основні мережеві технології

Ми закінчимо цей розділ з короткого обговорення деяких технологій і концепцій, які мають вирішальне значення для розуміння сучасних мережевих інфраструктур. Обговорення покликане служити тільки в якості огляду предмета. Ці теми будуть розглянуті більш детально в більш пізній час протягом цього курсу.

Сегментація мережі

Ви вже розглянули деякі вводні ідеї сегментації мережі. Є кілька причин, чому ви могли б розглянути сегментації мережі, в тому числі:

Оптимізація мережі зв'язку
Поліпшення управління потоком мережевого трафіку
Підвищення безпеки управління мережею

Є два основні методи, які використовуються для сегментації мережі, підмереж і віртуальних локальних мереж (Рисунок 3-28). Один з найбільш істотних відмінностей між ними полягає в тому підмережі реалізуються на рівні 3 моделі OSI в, але VLAN, реалізуються на рівні 2.

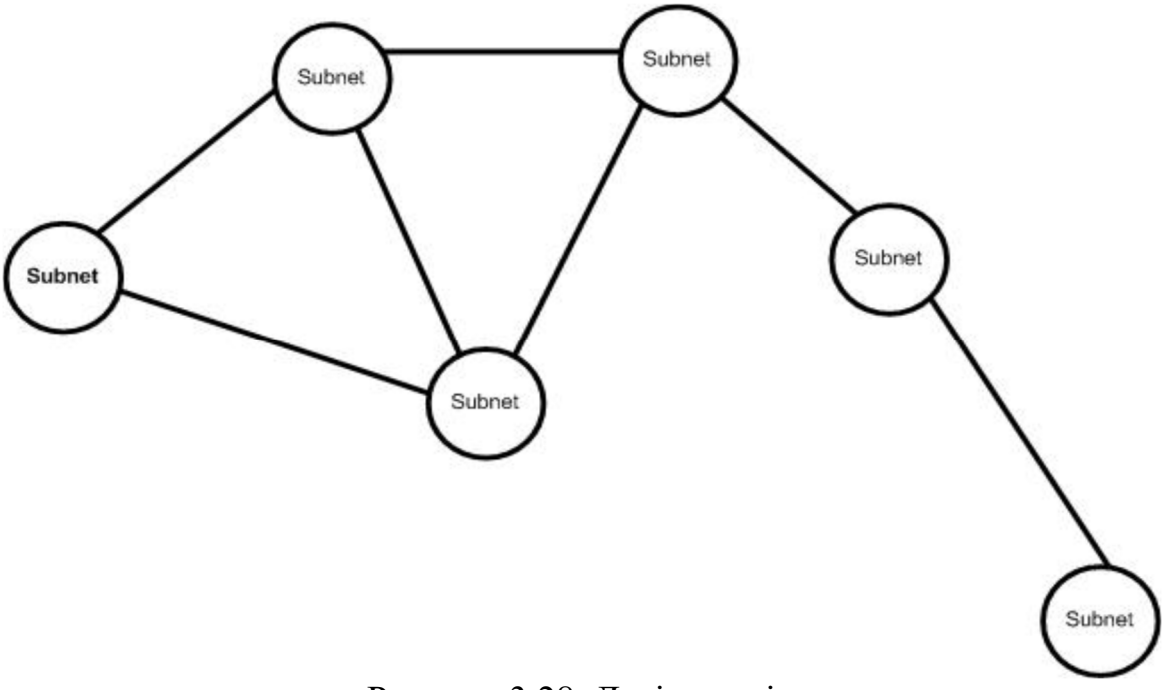


Рисунок 3.28: Декілька підмереж

Маршрутизатор і комутатори маршрутизації необхідна для використання підмереж в сегменті мережі. Кожна підмережа повинна мати різний мережеву адресу. При використанні VLAN, комутатор використовуються для сегмента

мережі, а сегментація зазвичай портом. Мережа VLAN може бути складена з портів, призначених від одного комутатора або складатися з портів, зібраних з кількох комутаторів. Кожна мережа VLAN матиме різний ідентифікаційний номер і інший присвоєний IP-адреса. Мережа VLAN може бути пов'язана з безліччю підмереж (Рисунок 3.29).

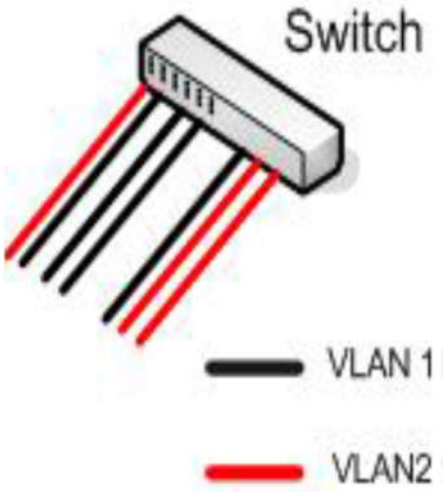


Рисунок 3.29. Комутатор с двома VLAN

Мережі VLAN стали популярним варіантом сегментації для локальних мереж. Маршрутизатор як і раніше є основним засобом сегментації більш широкої області.

Периметр мережі

Один спеціалізований тип сегментації мережі периметра. Мережевий периметр захищеної підмережі, що знаходиться між внутрішньою локальною мережею і зовнішнім світом, зокрема в Інтернеті. Термін ДМЗ іноді використовується, щоб звернутися до демілітаризованої зони або екранованої підмережі.

Екранована підмережа *- підмережа ізольована від решти мережі з трафіком в і з мережі фільтрується.*

Демілітаризована зона (ДМЗ) *- в контексті мережі, відноситься до підмережі екранованої одним або декількома міжмережевими екранами.*

Спочатку потрібно ввести поняття брандмауера. Брандмауер являє собою пристрій безпеки, яке може фільтрувати трафік в або з мережі периметра. Брандмауер може бути окремим, спеціалізованого пристроєм або, найчастіше, здійснюватися через функціональні можливості, що надаються в маршрутизаторі. Брандмауер діє по фільтрації трафіку, що дозволяє пройти в будь-якому напрямку, як показано на малюнку 3.30. Таким чином, ви можете обмежити трафік на певні види зв'язку, б блокуваті доступ потенційно небезпечних програм, і навіть встановлювати обмеження на інформацію джерела і адреса призначення.

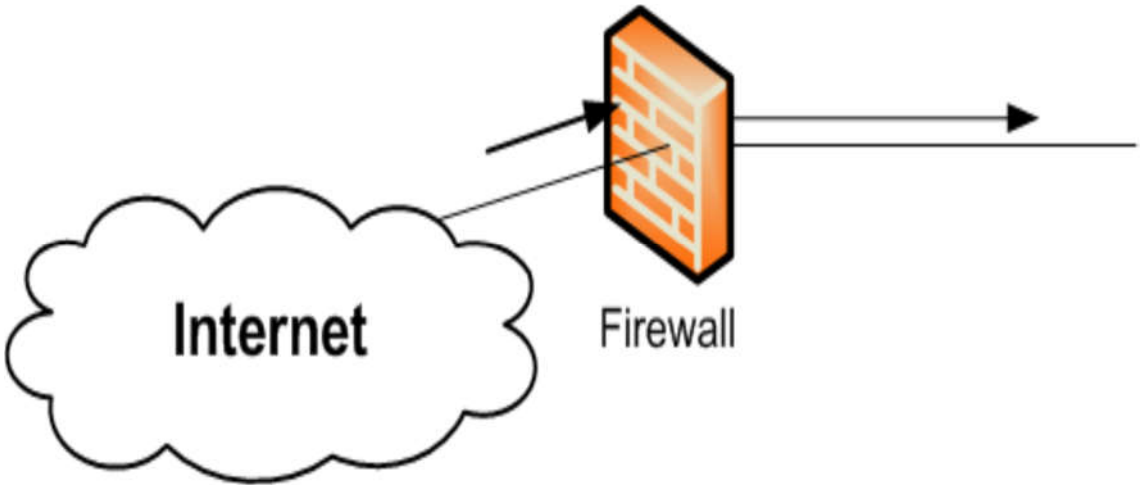
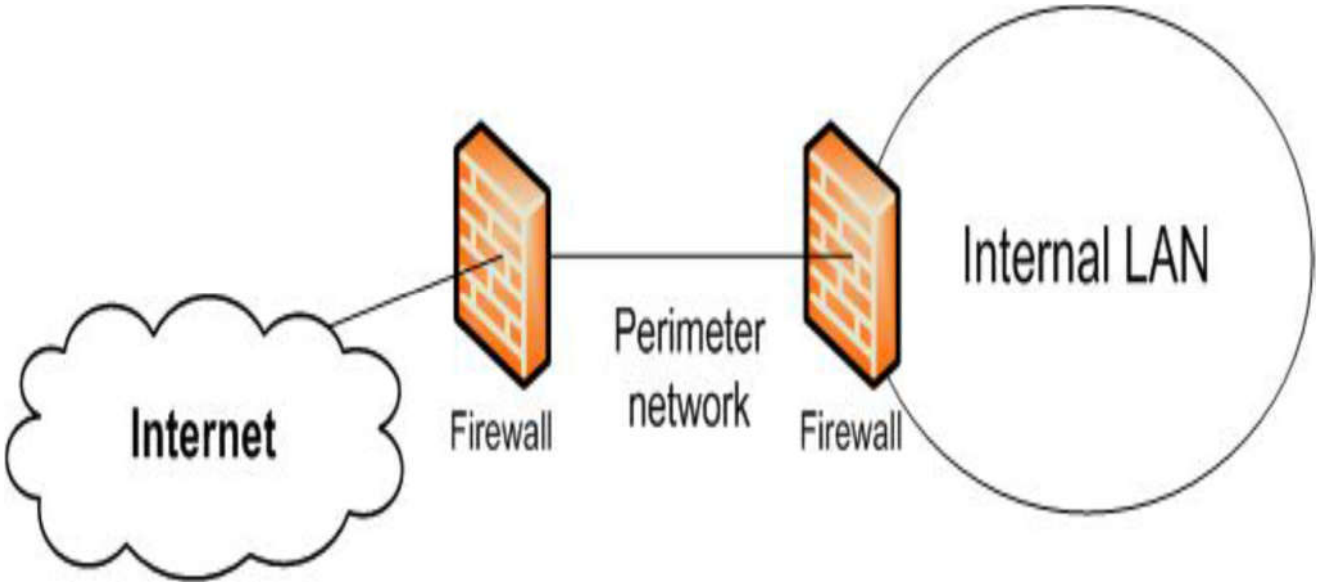


Рисунок 3.30: Брандмауєр

Особисті брандмауери, що захищають один комп'ютер, також поширені. Вони часто реалізуються за допомогою операційної системи. Персональний брандмауер фільтрує трафік в і з комп'ютера, на якому він налаштований.



Рисуно 3.31. Периметр мережі

Периметр мережі виступає в якості буфера, щоб захистити вашу мережу. Він призначений для запобігання несанкціонованого доступу в мережі, а також цілеспрямовані напади. Одна конфігурація загального мережевого периметра має периметр мережі, обмежений по обидва боки брандмауерами, як показано на Рисунку 3.31.

Основна мета мережі периметра, що вона дає вам місце, щоб розгорнути пристрої, якими ви хочете поділитися зі світом в цілому. Наприклад, якщо ви хочете мати загальнодоступний веб-сайт і розмістити на своєму веб-сервері, ви повинні розгортання веб-сервера в демілітаризованій зоні. Таким чином, ви зробили б його доступним для Інтернет, не піддаючи всю мережу для громадськості.

Скриті підмережі

Ви можете побачити внутрішні зміна мережі на мережі периметра, яке називають просто прихованою під сіткою. В цьому випадку, підмережа є частиною вашої внутрішньої мережі, але межа в підмережі захищена брандмауером, як показано на Рисунку 3.32. Брандмауер фільтрує всі передачі в і з підмережі.

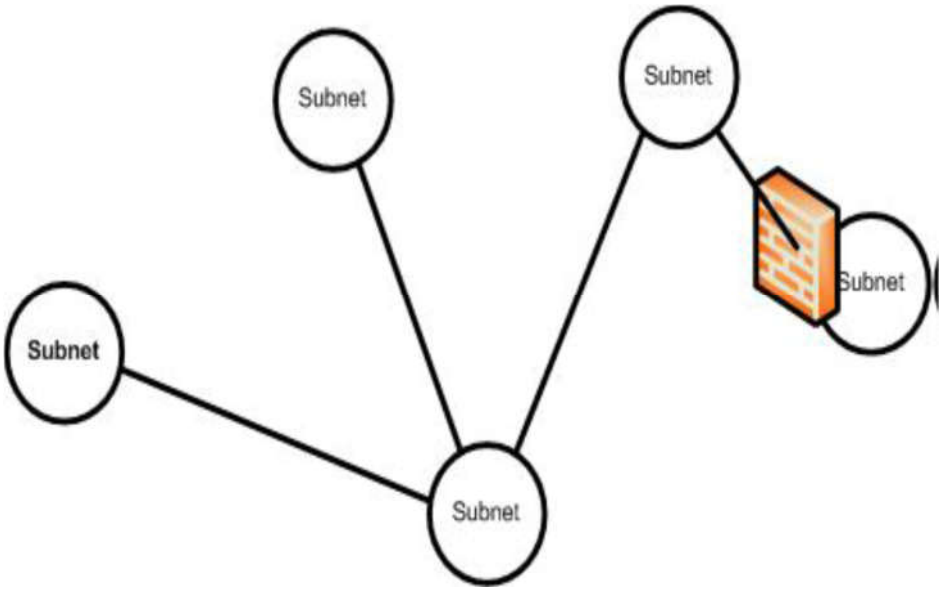


Рисунок 3.32: Скриті підмережі

Однією з причин для конфігурації вашої мережі цим способом є те, що це забезпечення додаткової безпеки для комп'ютерів, розміщених в екранованої підмережі. Вона також дозволяє вказати жорсткий контроль над користувачами (і які програми) можуть мати доступ до ресурсів в захищеній підмережі.

Проксі

Один тип спеціалізованого сервера, який ви можете знайти в мережі периметра, є проксі-сервер. Замість того, щоб дозволити клієнтським комп'ютерам внутрішньої мережі доступ до серверів безпосередньо, їх запити обробляються через проксі-сервер. Клієнти можуть отримати доступ до проксі-сервера, проходячи через наступні етапи:

Клієнт робить запит до проксі-сервера.

Проксі-сервер запитує Інтернет-ресурс і витягує результат.

Проксі-сервер передає результат запитуваний клієнтом.

Процес невидимий для користувача, щоб нічого не вказувало що вони мають доступ до Інтернету через додатковий пристрій. Використання проксі-сервера дозволяє підвищити безпеку мережі. Він також додає шар адміністративного контролю, дозволяючи вам обмежити доступ користувачів до веб-сайтам, які ви не хочете що б їх переглядали. Проксі-сервер може сканувати вихідний трафік, а також, як спосіб запобігання втрат даних або розкриття.

Проксі-сервери також допомагає зменшити обсяг трафіку між мережею та Інтернетом. Інформація витягнута з Інтернету потрапляє в буфер на проксі-сервер. Якщо інший клієнт запитує ту ж саму інформацію, то вона читається з буфера проксі-сервера, а не шукається заново в Інтернеті.

Перетворення адреси

Переклад адреси ще одна важлива технологія, коли пристрою у внутрішній мережі необхідно отримати доступ до зовнішнього світу. Чим більше інформації потенційний зловмисник зможе зібрати про вашу локальної мережі, тим легше йому або їй буде зламати вашу мережу.

Злом *- в цьому контексті, несанкціонованого доступу в мережу і до її ресурсів.*

Таким чином, ви завжди повинні приховувати IP-адреси комп'ютерів в локальній мережі. Ви також повинні часто використовувати особисті IP-адреси для конфігурації внутрішніх хостів. При використанні приватних IP-адрес, ви повинні використовувати трансляцію адреси при доступі до Інтернету.

Приватні IP-адреси *- IP діапазони адрес, які можуть бути призначені в якості внутрішніх адрес LAN, але не можуть бути використані для спілкування в Інтернеті.*

Ви можете приховати IP-адреси локальних комп'ютерів і використовувати особисті адреси у вашій мережі за допомогою мережевих адрес (NAT) сервера або мережевого порту і Address Translation (PAT або NAPT) сервер. NAT-сервер замінює дійсну адресу Інтернет на хостової адресу. Коли відповідь повертається, він спрямований на хост. NAPT або PAT сервера використовують ті ж адреси для всіх хостів IT-послуг і відстежують, які виходять хости шляхом присвоєння іншого TCP або UDP адреси порту для кожного. Використання NAT або PAT також дає вам додатковий контроль над фільтрацією порту на ваші брандмауери, тому що ви можете вказати порти, що б потенційний зловмисник не міг увійти в вашу мережу. Як з проксі-сервером, процес є прозорим для користувача.

Віртуальна приватна мережа (VPN)

VPN-призначена для забезпечення безпечної, надійної зв'язку менш безпечних засобів масової комунікації. Найбільш поширеним використання VPN є забезпечення безпечного зв'язку між двома віддаленими вузлами, використовуючи Інтернет в якості носія. З VPN, сеанс зв'язку встановлюється між двома кінцевими точками. Два найбільш поширених сценарію LAN-to-LAN зв'язок і комп'ютер-LAN зв'язок.

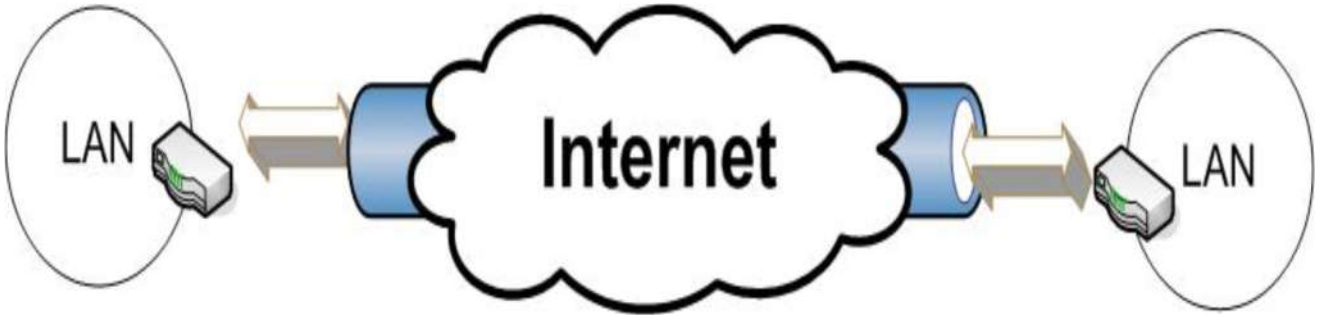


Рисунок 3.33. LAN-to-LAN VPN

У зв'язку LAN-to-LAN, ви використовуєте Інтернет в якості каналу глобальної зв'язку між локальними мережами, як показано на рис. 3-33. Цей тип з'єднання найчастіше є постійним підключенням між локальними мережами. На кожному кінці, пристрій, як правило, маршрутизатор, налаштоване як VPN кінцевої точки. Зв'язок зазвичай шифруються тільки між двома кінцевими точками.

Зв'язок комп'ютер-LAN найбільш часто використовується, щоб забезпечити видалений призначений для користувача з доступом до безпечної локальної мережі. Комп'ютер виступає в якості кінцевої точки VPN на одному кінці. Кінцева точка буде створена в кінці LAN і прийме зв'язок комп'ютера. Часто, в локальній мережі кінцева точка буде налаштована для підтримки декількох одночасних підключень VPN. Це часто встановлюється в якості з'єднання на вимогу, яка не «впаде», коли доступ в Інтернет більше не потрібно.

Ви можете знайти обидва типи кінцевих точок, налаштованих на одну локальну мережу. Наприклад, якщо SMB має віддалені офіси, а також віддалених або мобільних користувачів, він може мати точки для підтримки WAN зв'язку на віддалених місцях і кінцеві точки для підтримки окремих користувачів.

VPN, засновані на використанні протоколів тунелювання для передачі даних між кінцевими точками. Кінцеві точки повинні бути здатні взаємно аутентифікувати один одного, коли сеанс зв'язку встановлюється для забезпечення безпеки.

Тунелювання *(від англ. Tunnelling - «прокладка тунелю» в комп'ютерних мережах) - процес, в ході якого створюється захищене логічне з'єднання між двома кінцевими точками за допомогою інкапсуляції різних протоколів. Тунелювання є методом побудови мереж, при якому один мережевий протокол інкапсулюється в інший.*

Розділ 4:
Комутатори

Вступ

Раніше в цьому курсі ви вже познайомилися з комутаторами (switches), у тому числі з деякими процедурами базової конфігурації. Але зараз ми повертаємося до комутаторів, щоб детальніше розглянути їх конфігурацію і управління.

Частина нашої уваги буде приділена створенню і управлінню основної мережевої безпеки і віртуальних локальних мереж (VLAN), що є основним визначенням для використання комутатора багатьма компаніями. Також ми поглянемо по-іншому на управління і моніторинг стану порту. Глава включатиме процедури для з'єднання портів і для створення даних з високою пропускною спроможністю. Ми дізнаємося про налаштування на мережевий рівень (рівень 3), підтримку маршрутизації в комутаторі. Закріпимо наші знання обговоренням про файли конфігурації і оновлень програмного забезпечення.

У цьому розділі ми будемо використовувати CLI (Command Line Interface) і меню інтерфейсів для виконання різних завдань управління. Ми робимо так, щоб дати вам більше досвіду роботи після вивчення кожного з інтерфейсів управління.

Мета

У цій главі ви дізнаєтесь, як:
Описати розповсюджені типи перемикачів.
Налаштувати призначені для користувача мережі VLAN.
Керувати IP-адресою для VLAN.
Налаштувати і управляти мережами VLAN.
Налаштовувати і управляти портами.
Налаштовувати агрегацію портів.
Управляти оновленнями програмного забезпечення.
Керувати кількома конфігураціями комутатора.
Управління комутатором

Цей розділ присвячена процедурам управління комутатором. Специфіка в тому, що ви зможете робити, буде прямо залежати від комутатора, вони, як правило, можуть бути зосереджені в одному з трьох основних категорій:

Некеровані комутатори (Unmanaged switch)

Напівкерованих комутатори (комутатор з обмеженими можливостями управління, а також відомий як веб-керований комутатор - Web Managed Switch)

Керовані комутатори (Managed switch)

Основну увагу ми будемо приділяти керованим комутаторів, або повністю керованим комутаторів, які мають кілька інтерфейсів управління і знаходяться в широкому діапазоні параметрів, що настроюються.

Некеровані комутатори

На нижньому кінці доступних комутаторів є некеровані комутатори. Вони призначені для забезпечення зв'язку для невеликих мереж. Працюють некеровані комутатори строго на 2 рівні моделі OSI. Вони мають обмежену кількість портів, зазвичай не більше 24 (частіше 8 або 16), і не мають параметрів, що налаштовуються.

Некеровані комутатори мають явну перевагу, якщо ви хочете створити мережу для малого бізнесу. А все тому, що їм властиві не керовані параметри, так зване "plug-and-play" (це характеристика пристрою, під якою розуміють можливість користуванням пристрою відразу після підключення і без установки додаткових драйверів). Підключіть комутатор в розетку, а потім підключите мережеві пристрої до нього, і все працює. Некеровані комутатори забезпечують основні функціональні можливості, які можна було б чекати на цьому рівні, наприклад, можливість буферного трафіку, щоб уникнути зіткнення, але немає підтримки для більше просунутих функцій.

Некеровані комутатори також не надають ніякої інформації по мережі, тільки інформацію за індикаторами. Ви зможете, як правило, сказати, дивлячись на стан індикаторів, виявив чи порт підключений пристрій і чи є будь-яка діяльність на порту. Також можна сказати з якою швидкістю експлуатується порт і подивитися дуплексні настройки підключених пристроїв.

Але необхідно запам'ятати! Не можна створити VLAN на некерованому комутаторі.

Напівкеровані комутатори

Напівкеровані комутатори, також відомі як веб-керовані комутатори (Web Managed Switch), підтримують обмежені можливості управління. Однак, вони є більш просунутими пристроями, ніж некеровані комутатори та володіють додатковою функціональністю.

Як і некеровані комутатори, більшість напівкерованих комутаторів мають фіксовану фізичну конфігурацію. Більшість напівкерованих комутаторів надають функції канального рівня моделі OSI, а невелика їх кількість включають деяку функціональність на мережевому рівні, включаючи підтримку маршрутизації IP-адреси. Підтримка маршрутизації зазвичай обмежується тільки статичними маршрутами.

Статичний маршрут (static route) *- вручну налаштований маршрут із IP-адресом призначення та маршрутною інформацією.*

Як і некеровані комутатори, напівкеровані комутатори можуть бути, як правило, розгорнуті як «plug-and-play» пристрої, що використовують конфігурації радіоуправляємих комутаторів за замовчуванням. Доступ до більш просунутою функціональністю, проте, потребує наявності призначених для користувача настройках.

Напівкеровані комутатори забезпечують явні переваги перед некерованими комутаторами. Наприклад, напівкеровані комутатори мають доступ до управління через інтерфейс управління на основі браузера, який дозволяє дивитися статистику

по портам і управляти призначеними для користувача настройками. Ще однією перевагою є те, що напівкеровані комутатори включають підтримку VLAN. Ви також зможете налаштувати агрегацію каналів, щоб забезпечити дані з високою пропускною здатністю.

Агрегація каналів (link aggregation) - об'єднання декількох фізичних мережевих підключень паралельно, як один логічний шлях зв'язку, щоб забезпечити більш високу пропускну здатність і резервування.

Напівкеровані комутатори не обов'язково обмежуються веб-інтерфейсом. Більшість комутаторів цього типу також мають роз'єм RJ-45. Деякі з них також мають з'єднання USB, яке він може використовуватися для прямого підключення до комутатора. Це аналогічно з'єднанню консолі на керованих комутаторах, але також може бути використаним для виконання тих же процедур, як веб-інтерфейс.

Напівкеровані комутатори також включають обмежену підтримку SNMP. SNMP пристрої управління можуть автоматично виявити і віддалено контролювати напівкеровані комутатори. Проте, напівкеровані комутатори не підтримують дистанційне керування з пристрою управління SNMP.

Simple Network Management Protocol (SNMP) *- протокол TCP/IP для віддаленого моніторингу та управління мережевими пристроями.*

Керований комутатор

Ми вже раніше познайомилися з керованими комутаторами. Більшість з них побудовані на модульній конструкції, що дозволяє розширити їх, якщо є необхідність. Керовані комутатори підтримують функціональність на канальному рівні моделі OSI, а також забезпечують широкий спектр функціональних можливостей мережевого рівня (такі як динамічна маршрутизація).

Динамічна маршрутизація (dynamic routing) *- підтримка динамічних оновлень напрямків і маршрутів в мережі для забезпечення змін в доступних маршрутах і умов мережі.*

Керовані комутатори підтримують різні призначені для користувача налаштування управління, в тому числі:

CLI - інтерфейс командного рядка (консольний порт або по мережі);

Інтерфейс меню (консольний порт або по мережі);

Веб-інтерфейс (тільки через мережу).

Крім того, більшість керованих комутаторів можуть бути перевірені і налаштовані через SNMP і консоль управління SNMP. Це не тільки надає додаткові можливості управління. Також ви можете встановити порогові значення, такі що пристрій управління SNMP буде попереджати вас про ситуації, що можуть вимагати прямого втручання.

Такі продукти, як Pro Curve Manager (PCM) є прикладами управління SNMP консолей, які дозволяють вам бачити підключені пристрої і діяльність руху.

Більшість керованих комутаторів розроблені для роботи з протоколом SNMP. Таким чином, пристрій управління знає, яка інформація доступна на комутаторі і які види діяльності віддаленого управління він підтримує.

Management Information Base (MBI) *інформаційна база управління - сукупність інформації управління про пристрій для використання з керуванням SNMP.*

Налаштування розміщення комутатора всередині мережі

Коли ви проектуєте мережу, важливо зрозуміти, що ви можете змішувати типи комутаторів в одній локальній мережі. Ви завжди маєте некерований комутатор, а потім до нього додаєте напівкерований комутатор в мережу, і комутатор розширюється. Залежно від потреб, комутатори можна підключати безпосередньо один з одним або через маршрутизатор (комутатор мережевого рівня, виконаний у вигляді маршрутизатора, як показано на Рисунку 4.1).

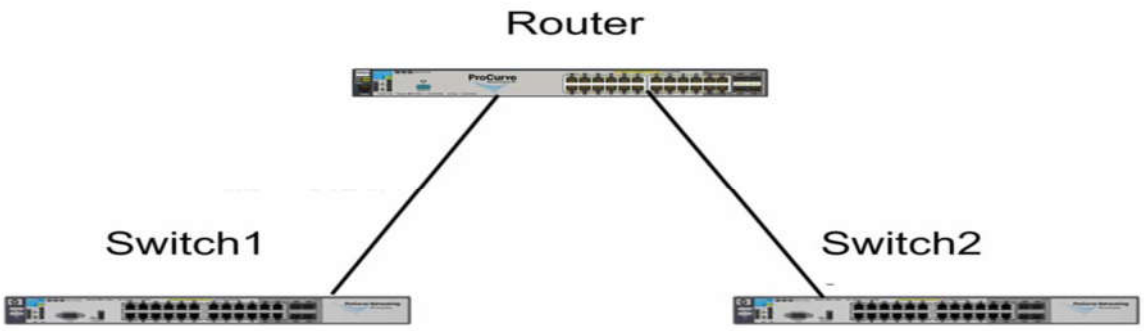


Рисунок 4.1 – Підключення комутаторів через маршрутизатор

Router (маршрутизатор), Switch1 (комутатор 1), і Switch2 (комутатор 2), імена пристроїв на Рисунку 4.1 - комутатори.

Комутатор 1 і комутатор 2 може бути реалізований на рівні 2 моделі OSI, але маршрутизатор повинен бути також і в конфігурації рівня 3 моделі OSI. Ви також можете створити таку конфігурацію для підключення до кінцевих комутаторів, використавши роутер замість комутатора 3 рівня.

Комутатор рівня 3 (Layer 3 switch) *- перемикач, який підтримує функціональність рівня 3 моделі OSI, в тому числі IP-маршрутизацію.*

Кінцевий комутатор (edge switch) *– перемикач, який здійснює перемикання на кордоні безлічі перемикачів, з'єднаних з центральним пристроєм.*

Ви можете розгорнути різні типи комутаторів в різних місцях (Рисунок 4.2). Це дозволяє використовувати тип, який найкраще підходить, а також дозволяє заощадити гроші шляхом розгортання менш дорогих комутаторів, де додаткова функціональність не потрібна.

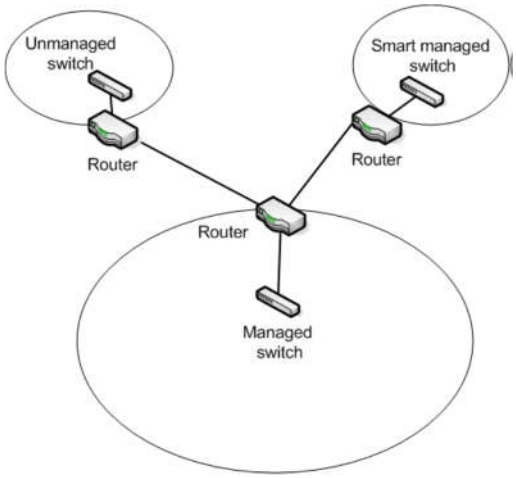


Рисунок 4.2 – Приклад розгортання

Поряд з потребами в будь-якій точці, доступність персоналу також може бути проблемою. Невеликі віддалені офіси, частіше, не мають можливості утримувати обслуговуючий персонал або мають тільки допоміжний персонал, який проходив мінімальне навчання. Проте, навіть якщо ніхто з персоналу не може забезпечити підтримку управління, ви можете використати напівкерований комутатор, адже він може бути реалізований як віддалений моніторинг, тобто можливі деякі віддалені налаштування.

Ви також можете змішувати і поєднувати різні з'єднувальні пристрої, а також розгорнути некеровані мережеві концентратори (hubs) разом з комутаторами, але це робиться в сучасній конфігурації мережі дуже не часто. Те, що ви, швидше за все, побачите - це мережа з вимикачами і бездротові точки доступу, а також деякі спеціальні розгортання додатків, які мають комутатори, вони також працюють в якості точок доступу.

Мережевий некерований концентратор (unmanaged hub) - *пристрій для об'єднання комп'ютерів в мережу Ethernet, який не вимагає і не підтримує управління. Пристрої підключені по топології "зірка", але трафік, може бути керований як в концентраторі при топології "загальна шина".*

Віртуальні мережі

Підмережі і мережі VLAN мають два шляхи, по якому можна розділити мережу для управління і контролю трафіку. Мережі VLAN допомагають поліпшити безпеку мережі шляхом поділу управління, пов'язаного з трафіком від іншого мережевого трафіку. Наприклад, якщо ця функція підтримується VoIP, ви можете використовувати VLAN для ізоляції телефонного трафіку з мережі даних трафіку.

Voice over IP (VoIP) - протокол передачі телефонних сигналів (розмов) через інтернет.

Є два типи портів (з'єднань):

Нетеговані (посилання доступу);

Теговані (агреговані з'єднання).

Нетегований порт (untagged/access link) - порт пов'язаний з будь-яким мережевим пристроєм, крім іншого комутатора.

Тегований порт (tagged/trunk link) - порт, що пов'язаний з іншим комутатором.

Більшість зв'язків - це зв'язки доступу, зв'язки на ПК і інші мережеві вузли пристрою. Теговані з'єднання також використовуються для створення зв'язку з високою пропускною спроможністю при налаштуванні віртуальної локальної мережі з комутаторами.

Віртуальну локальну мережу можна прирівняти до підмережі. І VLAN і підмережа являють собою широкомовний домен. Основна різниця між ними в тому, що VLAN реалізований на рівні 2, а підмережа реалізується на рівні 3. Крім того, має залежність від місця розташування, а VLAN реалізується на основі конфігурації порта.

Найпростіший тип статичного VLAN на основі портів

Членство в мережі VLAN залежить виключно від порту, до якого пристрій додається.

Статична визначення віртуальної локальної мережі включає в себе ідентифікатор VLAN, ім'я та пов'язані з ними порти. Ви також можете включати IP-адреса для VLAN. Це необов'язково якщо ви використовуєте SNMP для мережевого управління. У цьому випадку, ви повинні, зазвичай, визначити IP-адресу для VLAN управління, він повинен бути унікальним. Крім того, якщо включена маршрутизація на комутаторі, визначаючи IP-адреса для кожного VLAN, це дозволяє маршрутизувати трафік між VLAN.

Управління віртуальної локальної мережею (management VLAN) - це віртуальна локальна мережа позначена як VLAN, може бути використана для цілей управління комутатором.

Можна налаштувати VLAN так, що він буде складатися з портів, розташованих на різних фізичних комутаторах. Трафік між портами в тій же мережі VLAN, навіть якщо вони знаходяться на різних комутаторах, з'єднується, таким чином, що мовлення розповсюджується через мережу VLAN. Трафік між мережами VLAN направляється, так як широкомовний трафік не перетинає мереж VLAN. Ви також можете мати динамічні конфігурації VLAN на основі різних параметрів, такі що увійшли в використання пристрою або MAC-адреса.

Типи віртуальних локальних мереж

На додаток до управління трафіку шляхом створення широкомовних доменів, ще одним поширеним використанням мереж VLAN - є вміння відокремити різні типи трафіку від нормального мережевого трафіку.

На основі портів VLAN статичні типи включають в себе:

VLAN за замовчуванням.

Включає в себе всі порти комутатора, коли знаходиться в режимі за замовчуванням. Завдяки цьому VLAN здійснює як і трафік управління, так і стандартний мережевий трафік.

Первинна VLAN

Спочатку, це віртуальна локальна мережа за замовчуванням. Ви можете призначити користувальницькі VLAN в якості основного і покласти на нього відповідальність за деякі функції управління. Для комутаторів HP, первинна VLAN є єдиною VLAN на комутаторі, яка може приймати адреси що генеруються через DHCP.

Безпечна VLAN управління.

При створенні в якості призначеного для користувача VLAN, безпечне управління є ізольованою мережею спеціально для управління комутатором. Доступ до функцій управління, обмежується тільки тими портами, налаштованими як безпечні члени управління VLAN. Трафік не може бути направлений до або від цієї VLAN.

Voice VLAN.

Це віртуальна локальна мережа, яка створюється що б ізолювати VoIP трафік від інших трафіків.

Це звичайна практика, щоб видалити або перейменувати VLAN за замовчуванням в цілях безпеки. Залишивши VLAN за замовчуванням, ми можемо забезпечити шлях для несанкціонованого доступу в мережу.

Порт в VLAN може бути тегірованим або нетегірованним. Тегування побудовано на основі стандарту 802.1Q. Один порт може дозволити обробку трафіку від кількох VLAN.

Порт може бути нетегірованим для однієї віртуальної локальної мережі, і при цьому може бути тегірованим для іншої мережі (Рисунок 4.3).

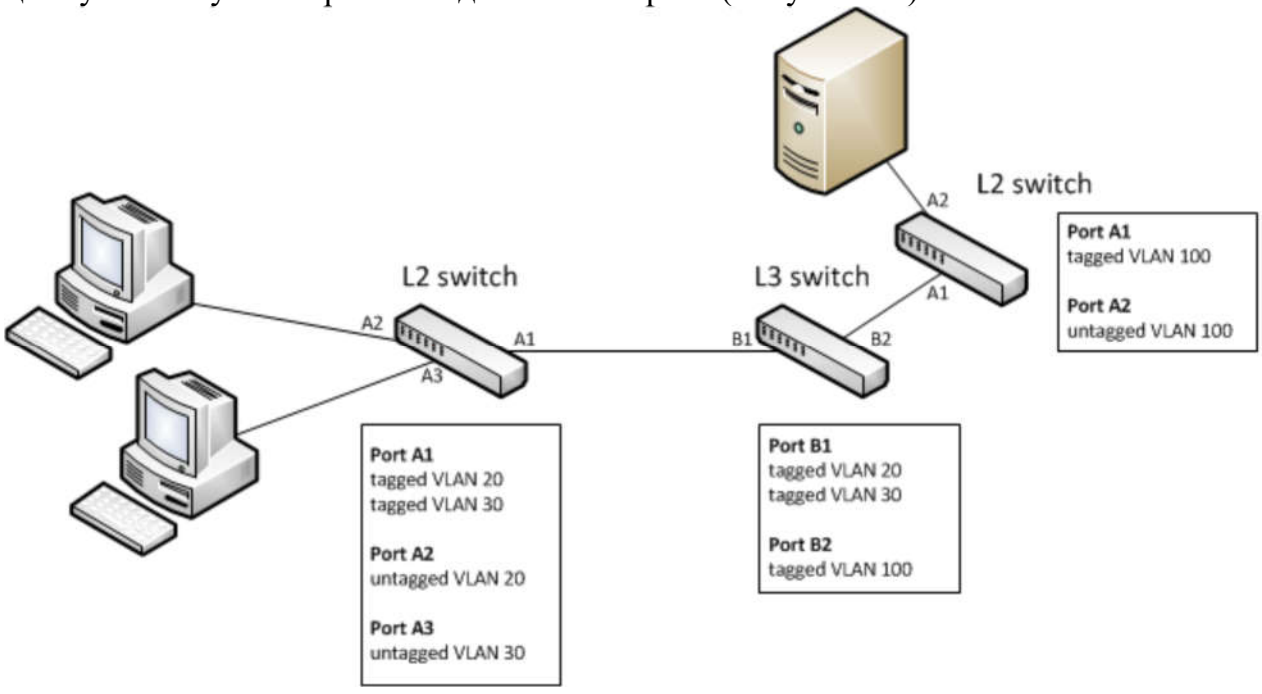


Рисунок 4.3 – Локальна мережа із тегірованими и нетегірованими портами

Як ви можете бачити, порти A1 і B1 - тегіровані порти, які несуть трафік для VLAN 20 і 30 між комутаторами L2 і L3. Порти A2 і A3 підключають клієнтські комп'ютери до VLAN, 20 і 30, відповідно, і, таким чином налаштовані як нетегіровані. Порт B2 на комутаторі L3 і порт A1 на комутаторі L2 визначають тегіровані порти, які дозволяють здійснюватися трафіку для VLAN 100 між комутатором L2 і L3. Нетегірований порт A2 на правому комутаторі L2 з'єднує сервер для VLAN 100.

802.1Q - стандарт для використання тегів VLAN з пакетами Ethernet.

Управління віртуальними локальними мережами

Якщо комутатор підтримує віртуальні локальні мережі, то в стандартній конфігурації буде одна віртуальна мережа, до якої прив'язані всі порти. Вона буде мати індекс VLAN 1. Трафік не зможе маршрутизуватися через VLAN.

Щоб налаштувати VLAN, ви повинні спочатку створити новий і видалити порти з VLAN за замовчуванням. Любий порт явно не видаляється, а залишається частиною VLAN за замовчуванням.

Основні кроки для створення призначеного для користувача VLAN:

Визначте ім'я та індекс VLAN;

Передача портів від дефолту (або інший) VLAN до нової VLAN;

Призначити IP-адреса в мережі VLAN (за бажанням).

Ви можете виконувати основні кроки для створення VLAN, використовуючи CLI (Command Line Interface) - інтерфейс меню або веб-інтерфейс. Наприклад, на Рисунок 4.4 показана сторінка веб-інтерфейс для управління VLAN.

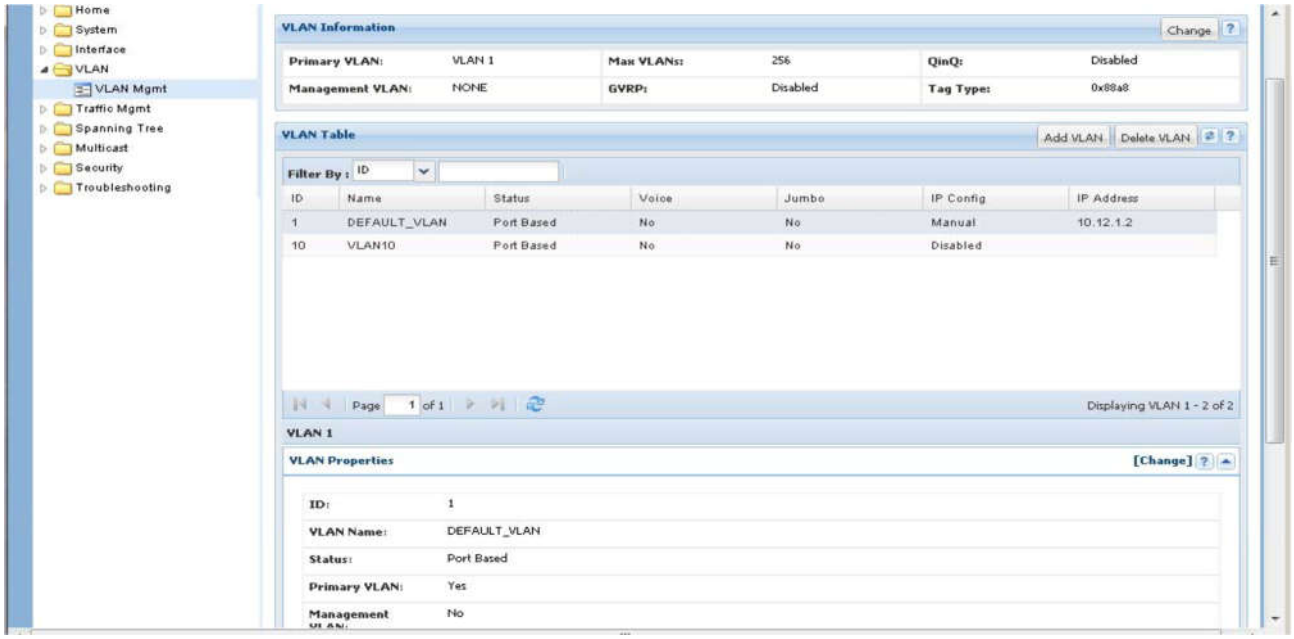


Рисунок 4.4 - Сторінка веб-інтерфейс для управління VLAN

По-перше, ми будемо використовувати інтерфейс меню, щоб пройти через процес створення VLAN, призначеного для користувача. Запустіть інтерфейс меню і виберіть 2. Switch Configuration з головного меню, щоб відкрити меню конфігурації комутатора (Рисунок 4.5).

-

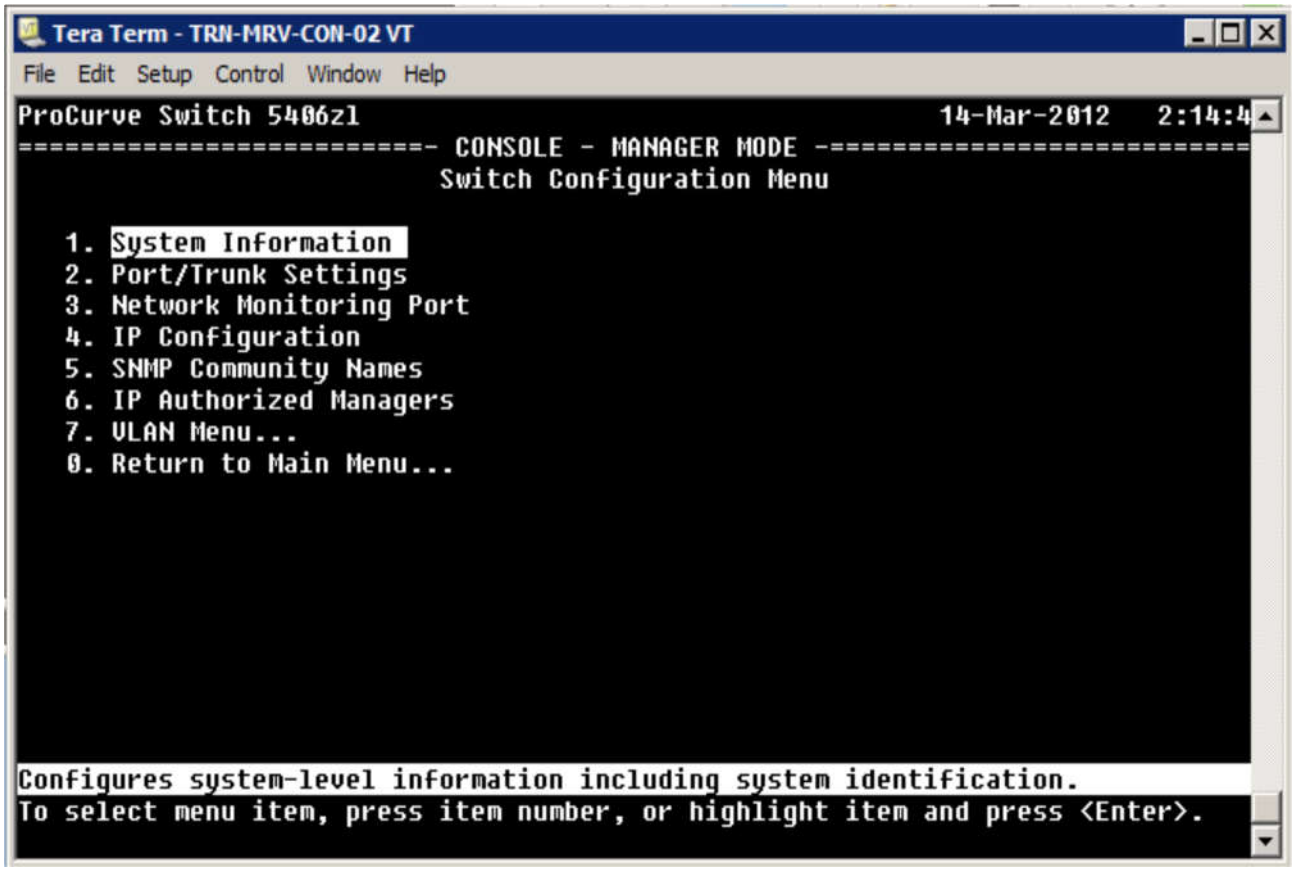


Рисунок 4.5 - Меню конфігурації комутатора

От Switch Configuration Menu, виберіть 7. VLAN меню (Рисунок 4.6).

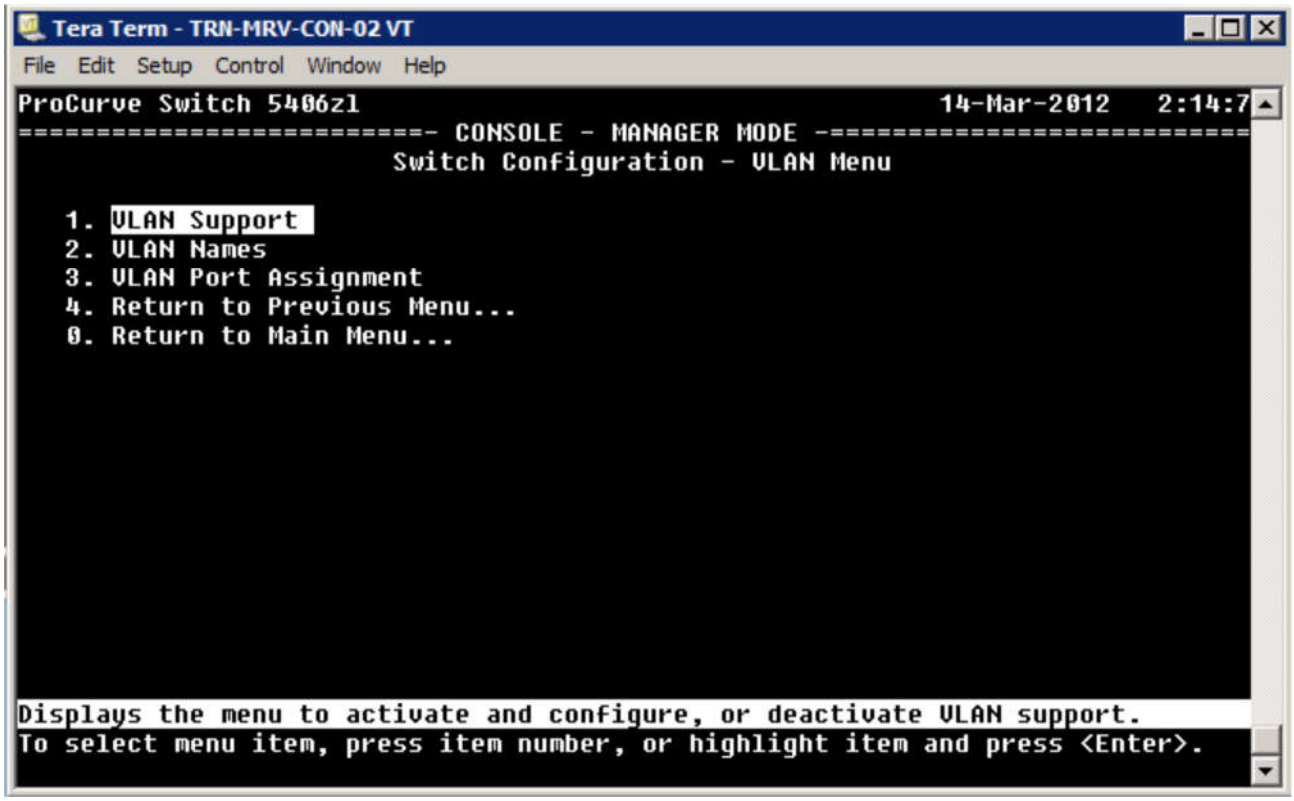


Рисунок 4.6 - VLAN меню

Ми почнемо з розгляду меню опцій команд VLAN. Тут ви можете:

Налаштовувати параметри підтримки VLAN;

Створювати і управляти іменами і ідентифікаторами VLAN;

Призначати чи видалити порти з VLAN.

Почніть з вибору пуекту1 «VLAN Support», щоб перевірити параметри конфігурацій VLAN (Рисунок 4.7).

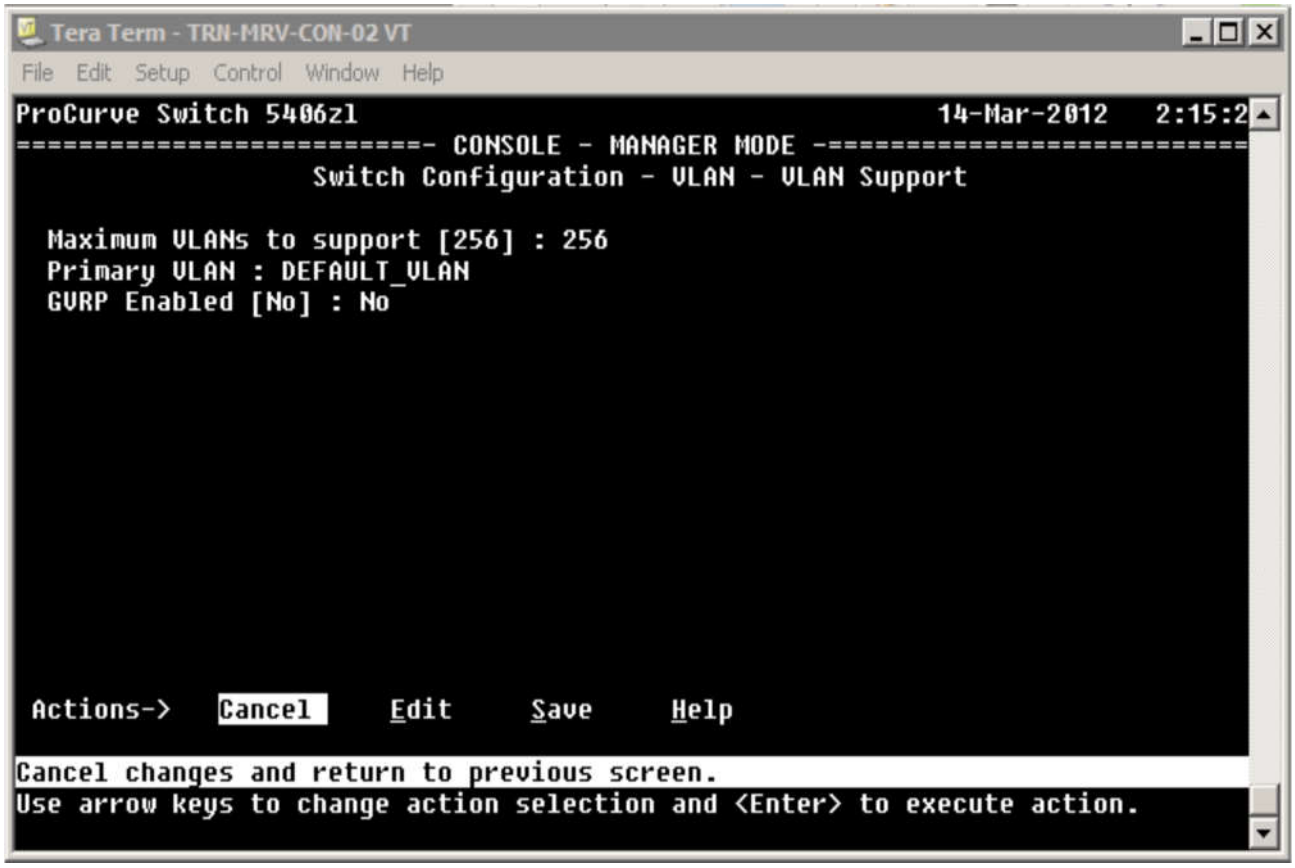


Рисунок 4.7 - Параметри конфігурації VLAN

Ви можете бачити, що цей комутатор підтримує до 256 віртуальних локальних мереж. Комутатор, в даний час, створений з конфігурацією за замовченням VLAN, тому основна VLAN також за замовчуванням (має назву DEFAULT_VLAN).

GVRP, протокол управління VLAN, за замовчуванням відключений.

Протокол реєстрації GARP VLAN (GVRP) - додаток до загального протоколу реєстрації атрибутів (GARP), який використовується в створенні та управлінні мережі VLAN.

Він динамічне створює VLAN на приймаючій стороні відповідно до VLAN, що створено статично на передавальній стороні.

Щоб створити нову VLAN, необхідно її визначити. Виберіть Cancel, щоб повернутися до VLAN Menu і виберіть пункт 2 «VLAN Names», щоб відкрити екран VLAN Names Configuration (Рисунок 1.8). За замовчуванням вибирається меню Actions. Виберіть Add з Actions меню і введіть інформацію.

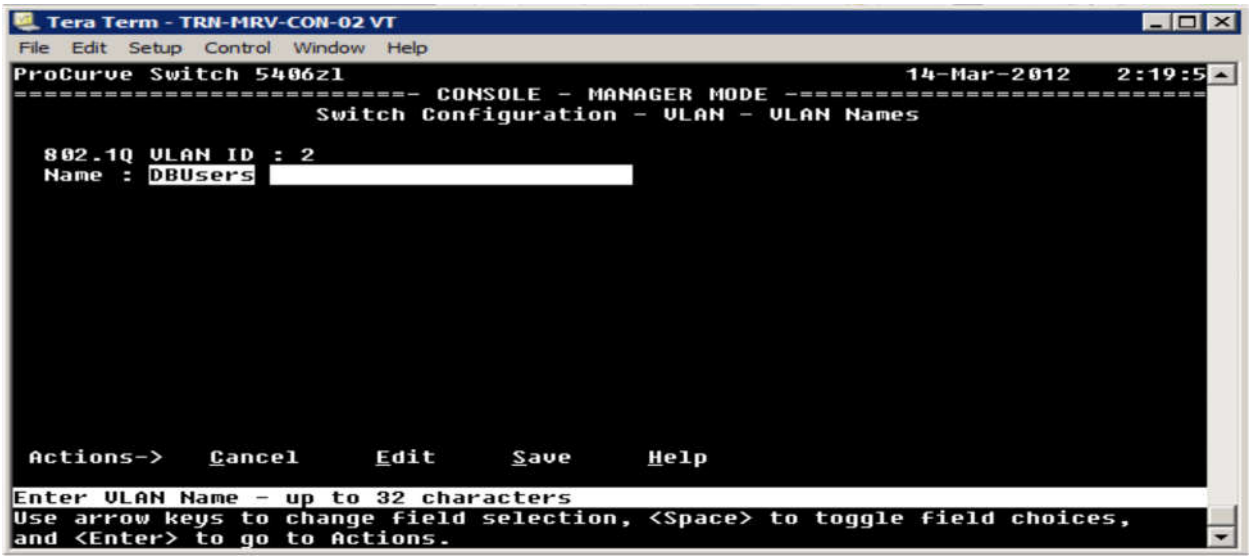


Рисунок 4.8 - Екран VLAN Names Configuration

Ви можете вказати ідентифікатор і ім'я. Звідси ви повинні натиснути клавішу Enter, щоб повернутися в Actions меню, і вибрати пункт Save, щоб зберегти нове визначення VLAN.

Тепер список імен VLAN включає в себе як DEFAULT_VLAN так і нове, яке ви, тільки що створили (Рисунок 4.9).

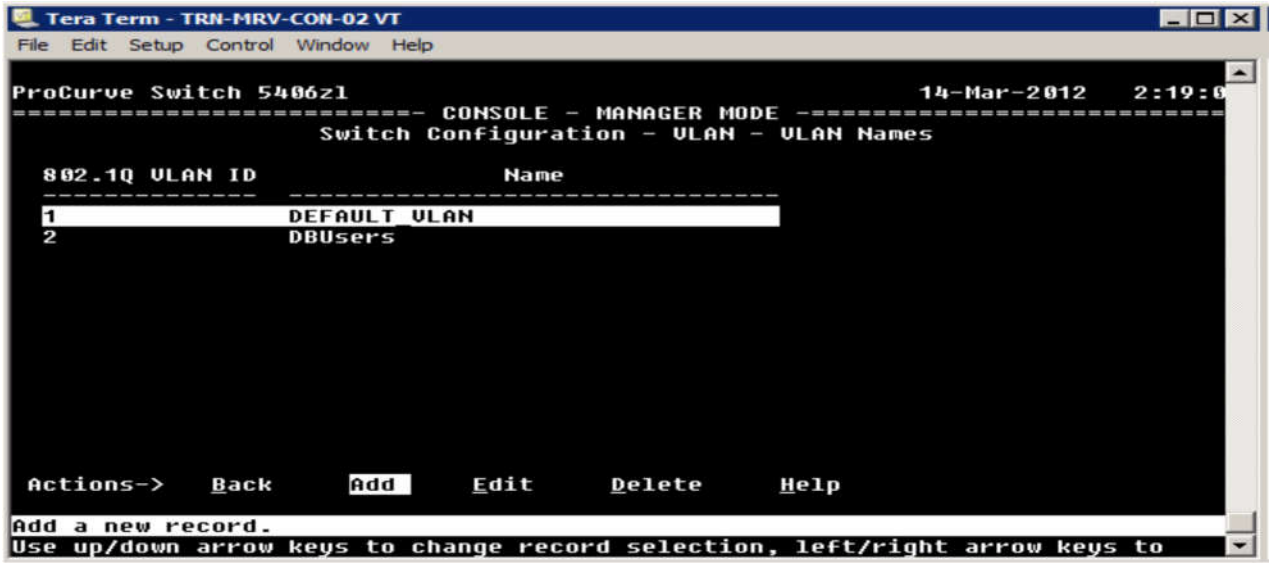


Рисунок 4.9 - Список імен VLAN

У цей момент, існує друга VLAN, що сконфігуровано на комутаторі. Проте, вона не має ніяких призначених портів, так що насправді нічого не потрібно робити. Щоб додати порти, виберіть 3. VLAN Port Assignment з меню VLAN.

Екран VLAN Port Assignment показує поточне призначення портів (Рисунок 4.10). У прикладі показано стандартні прив'язки портів, де всі вони прив'язані до стандартної VLAN (default VLAN).

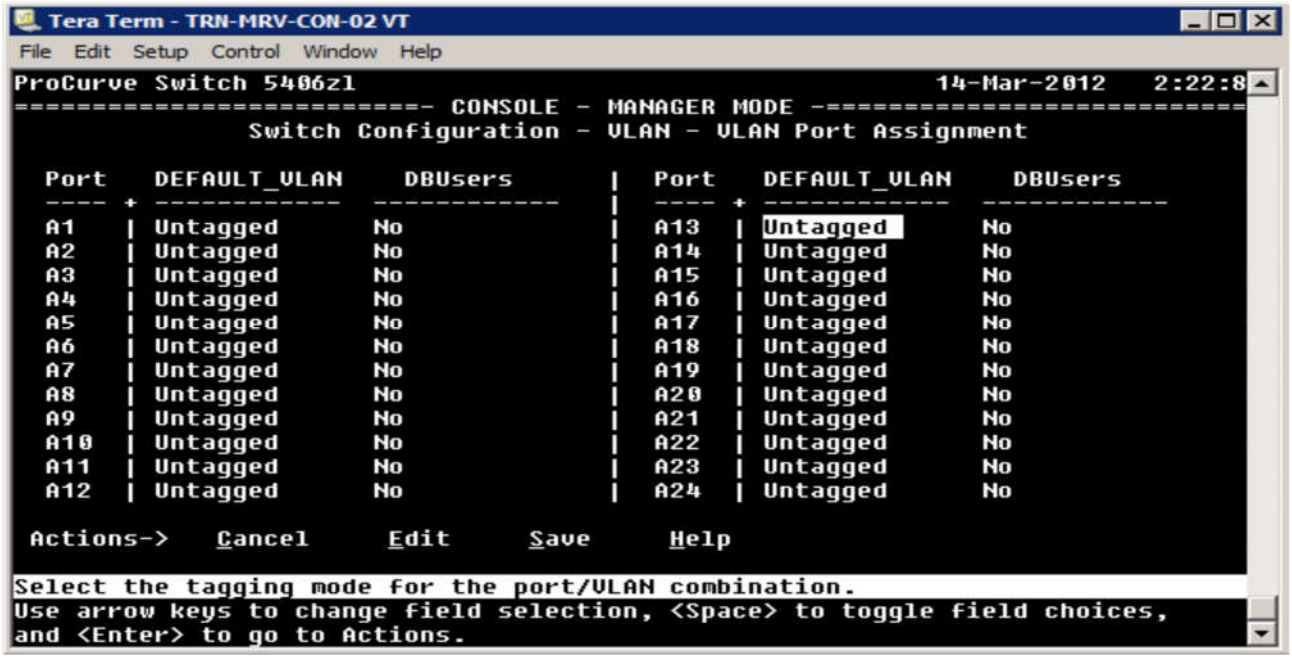


Рисунок 4.10 - Екран VLAN Port Assignment

Щоби змінити порт призначення, виберіть Edit в меню Actions та із його допомогою і клавіши із стрілкою виберіть порт, який ви бажаєте змінити (Рисунок 4.11).

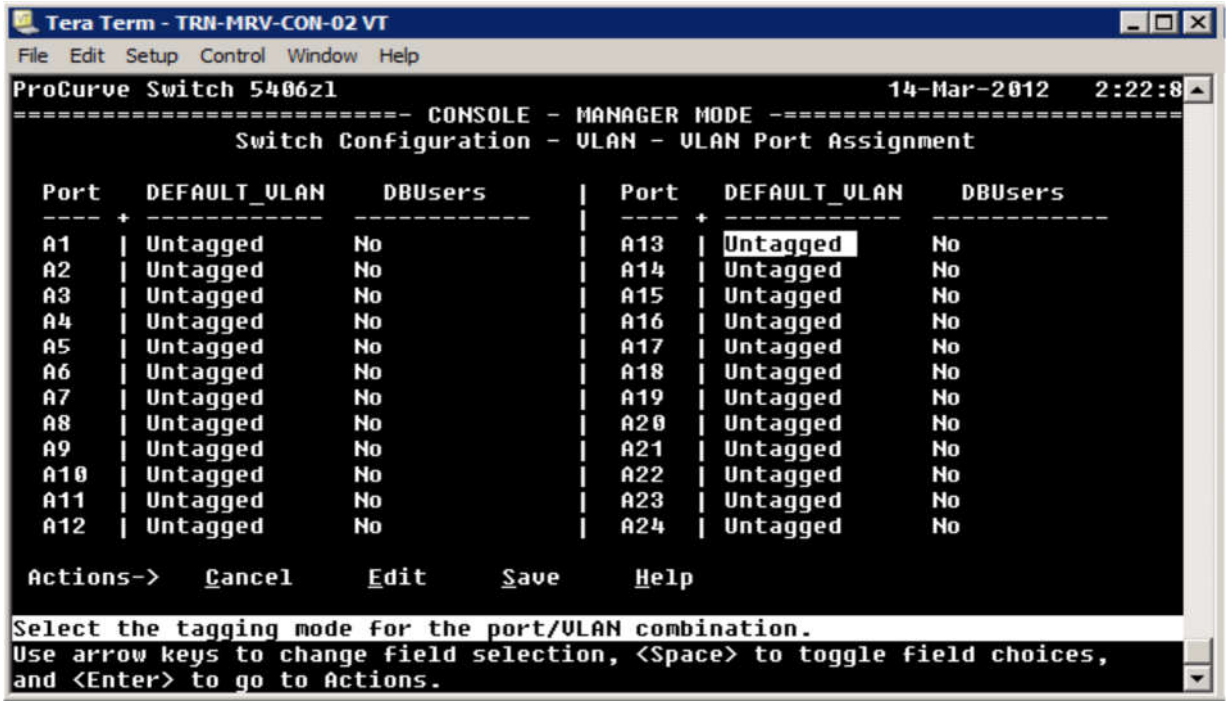


Рисунок 4.11 - Меню Actions

Що потрібно робити, якщо ви бажаєте додати порти в DBUsers VLAN?

У вибраний порт, в колонці DEFAULT_VLAN, натисніть пробіл, поки значення показує No.

Для цього порта, під DBUsers, натисніть пробіл, поки показує Untagged (Рисунок 4.12). Продовжуйте цей процес для всіх портів, які ви бажаєте додати в мережу VLAN.

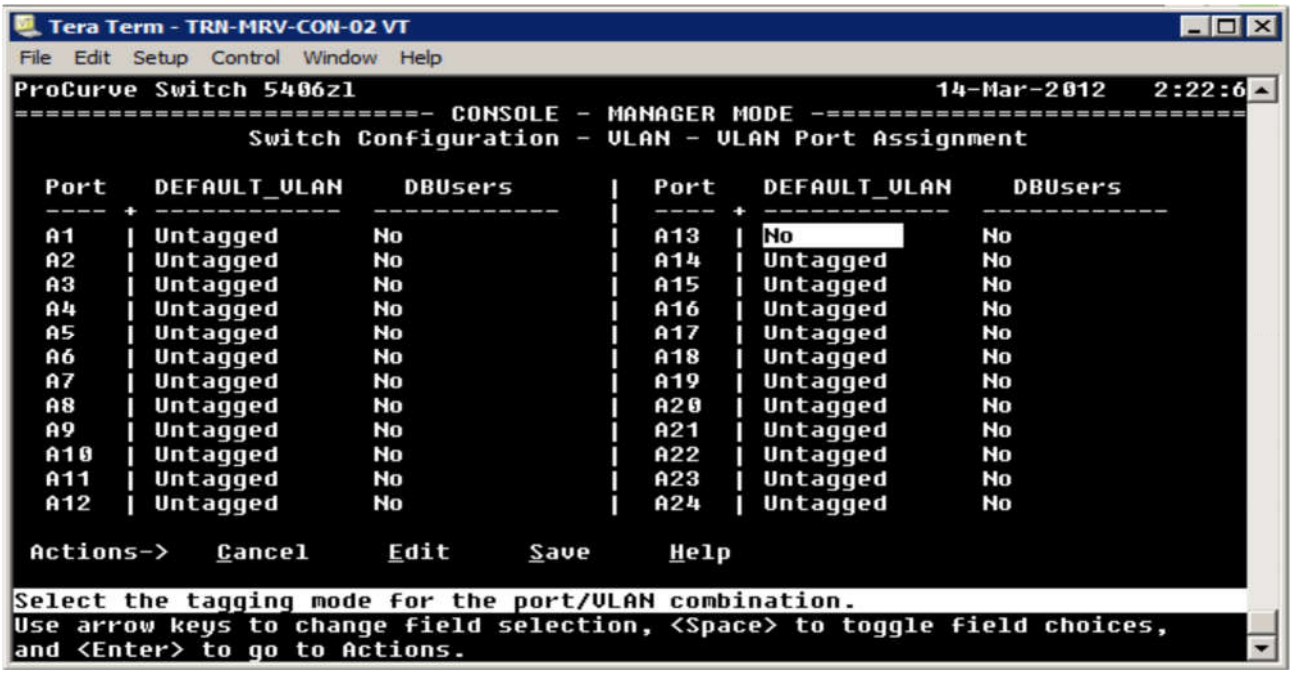


Рисунок 4.12 – Додавання портів в мережу VLAN.

Порти також можуть бути налаштовані як тегіровані або заборонені. Коли порт встановлюється як заборонений, він не вступає в VLAN, яка була динамічне створена за допомогою протоколу GVRP. Після того як ви налаштували порти, виберіть Save з меню Actions.

Раніше ми розглядали як використовувати інтерфейс командного рядка для установки IP-адреси для VLAN. Це також може бути досягнуто за допомогою меню інтерфейсу.

З VLAN Menu, виберіть пункт 4 «Return to Previous Menu;. Це приведе вас назад до Switch Configuration Menu. Звідси, виберіть пункт 4.

Тепер, коли ви знайомі з процесом, ми можемо вивчити команди консолі, що ви будете використовувати для створення і назви VLAN. Щоб створити нову мережу, виконайте команду віртуальної локальної мережі, за якою слідує ідентифікатор VLAN (Рисунок 4.13).

Рисунок 4.13 – Створення нової мережі

Це створює нову мережу і автоматично перемикається в контекст конфігурації для цієї VLAN. Як ви можете бачити на Рисунку 4.13, ви повернетеся

до оновлення в командному рядку, але ніякого додаткового зворотного зв'язку не передбачено, якщо немає помилки в заданій команді. У цьому прикладі, нова VLAN матиме ім'я за замовчуванням VLAN 2 (Рисунок 4.14).

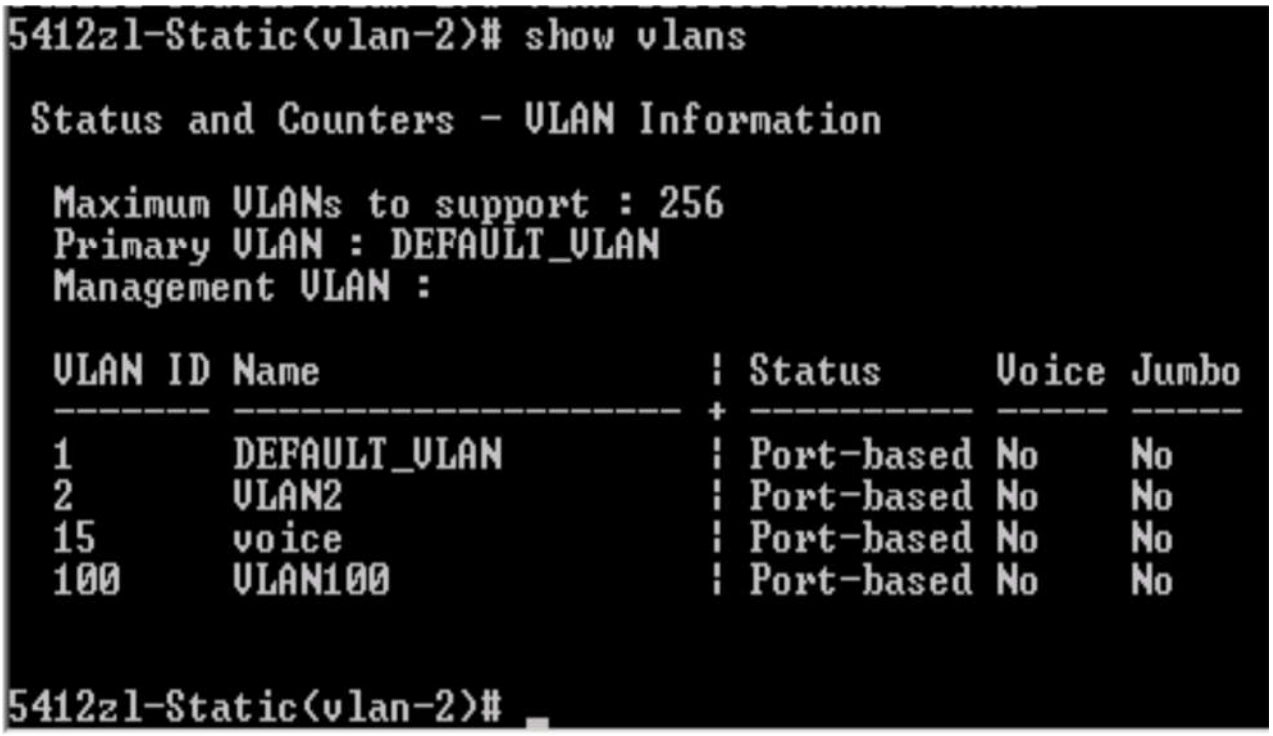


Рисунок 4.14 – Ім’я VLAN за замовченням

Якщо ви бажаєте перейменувати VLAN як DBUsers, ви повинні задати команду:

VLAN VLAN2 name DBUsers.

Якщо немає ніяких помилок, то команда не повертає жодної відповіді, а повертає дію в командний рядок.

Конфігурація IP

Конфігурація IP відключена за замовчуванням для новоствореного VLAN (Рисунок 4.15). Ви можете досягти цього, вибравши IP Configuration з головного меню. Також можете встановити настройки конфігурації IP - DHCP / BOOTP, щоб автоматично отримувати IP-адресу від DHCP-сервера, або ви можете вручну налаштовувати статичний адреса конфігурації IP.

Виділіть значення IP-Config для VLAN і натисніть пробіл, щоб прокрутити доступні варіанти.

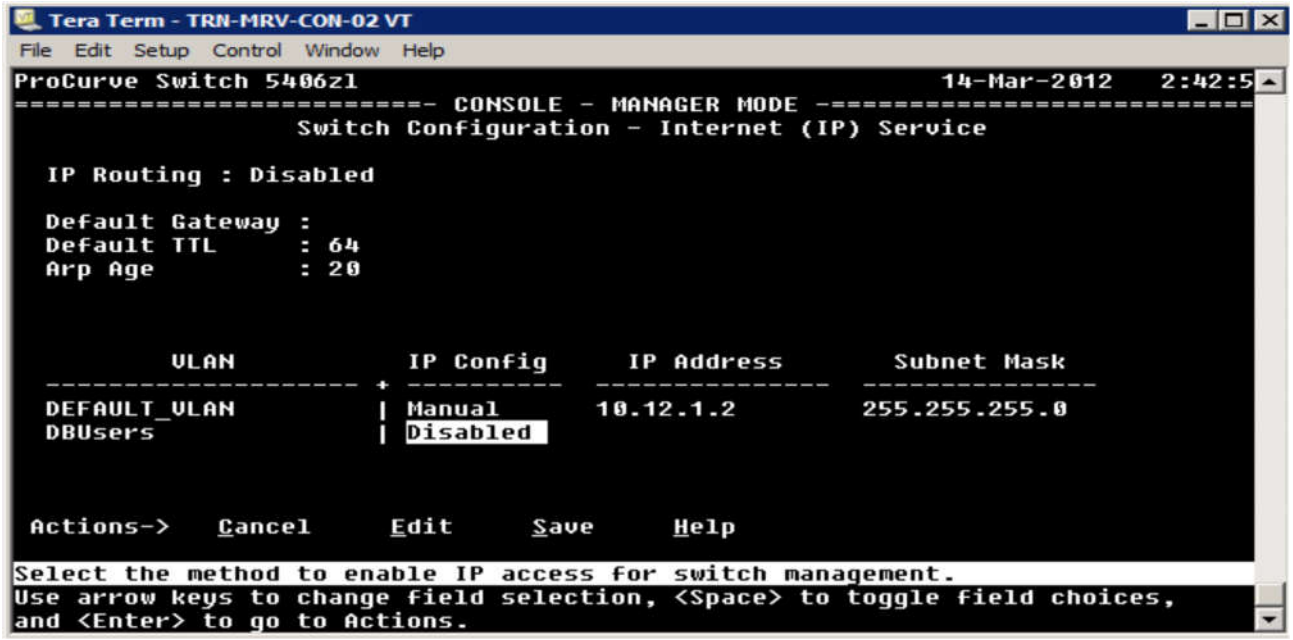


Рисунок 4.15 – Стандартна IP конфігурація

Щоб дістатися до екрану управління, виберіть Switch Configuration в головному меню, а потім виберіть IP Configuration з IP Configuration Menu.

Якщо ви хочете, щоб мережа VLAN мала відомий IP-адреса, ви можете вибрати налаштування статичної IP-адреси (Рисунок 4.16).

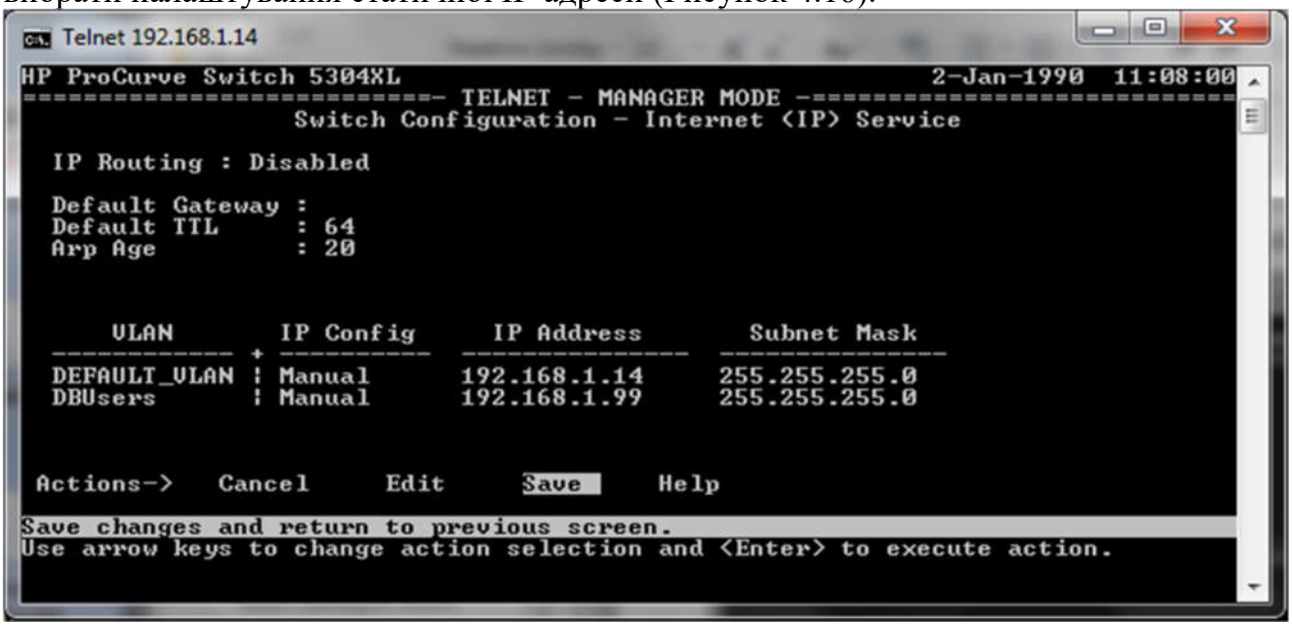


Рисунок 4.16 – Статична IP-адреса

Якщо ви повернетеся до CLI, ви можете запустити наступну команду, щоб побачити список мереж VLAN налаштованих на комутаторі разом з типом VLAN:

show vlans

В цьому випадку комутатор сконфігуровано на основі двох портів VLAN (Рисунок 4.17).

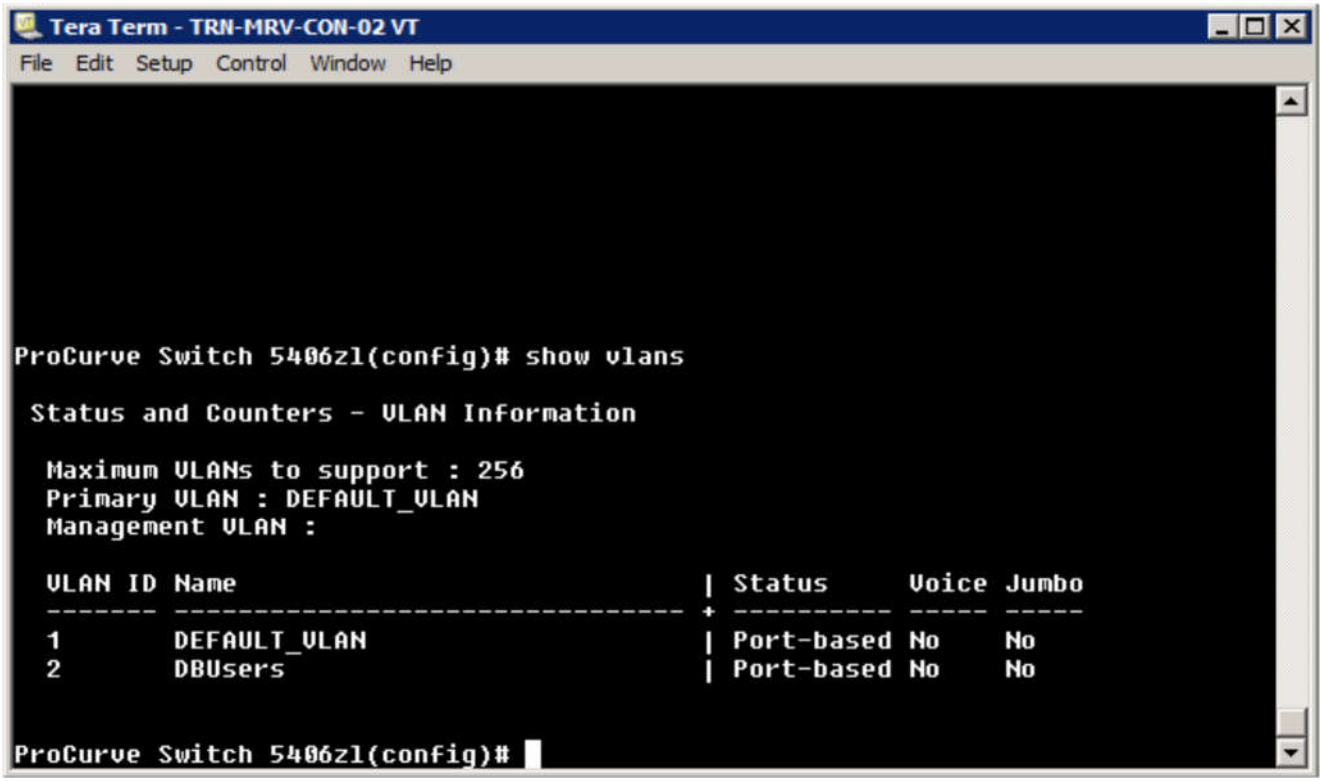


Рисунок 4.17 – Список VLAN

Зверніть увагу, що DEFAULT_VLAN ще називається первинною VLAN. Там немає визначального, що означає, що ви можете підключитися до комутатора з будь-якого порту і здійснювати діяльність з управління.

Вимоги до видалення VLAN залежить від комутатора, а іноді і від версії системного програмного забезпечення. З деяких комутаторів, ви повинні видалити всі порти з VLAN, перш ніж вона може бути видалена. З іншими, ви можете видалити VLAN, і його порти автоматично повернуться до VLAN за замовчуванням.

Керівництво портами

Керівництво портами для VLAN робиться під віртуальну локальною мережу зв'язку. Разом з тим, ви можете переглянути інформацію порту, включаючи статистичні дані та лічильники, в будь-якому контексті. Для перегляду, виконайте наступну команду:

show interface

Якщо ви хочете побачити більш детальну інформацію для одного порту, вкажіть його номер:

show interface a1

Це дасть вам статистику для зазначеного порту (Рисунок 4.18).

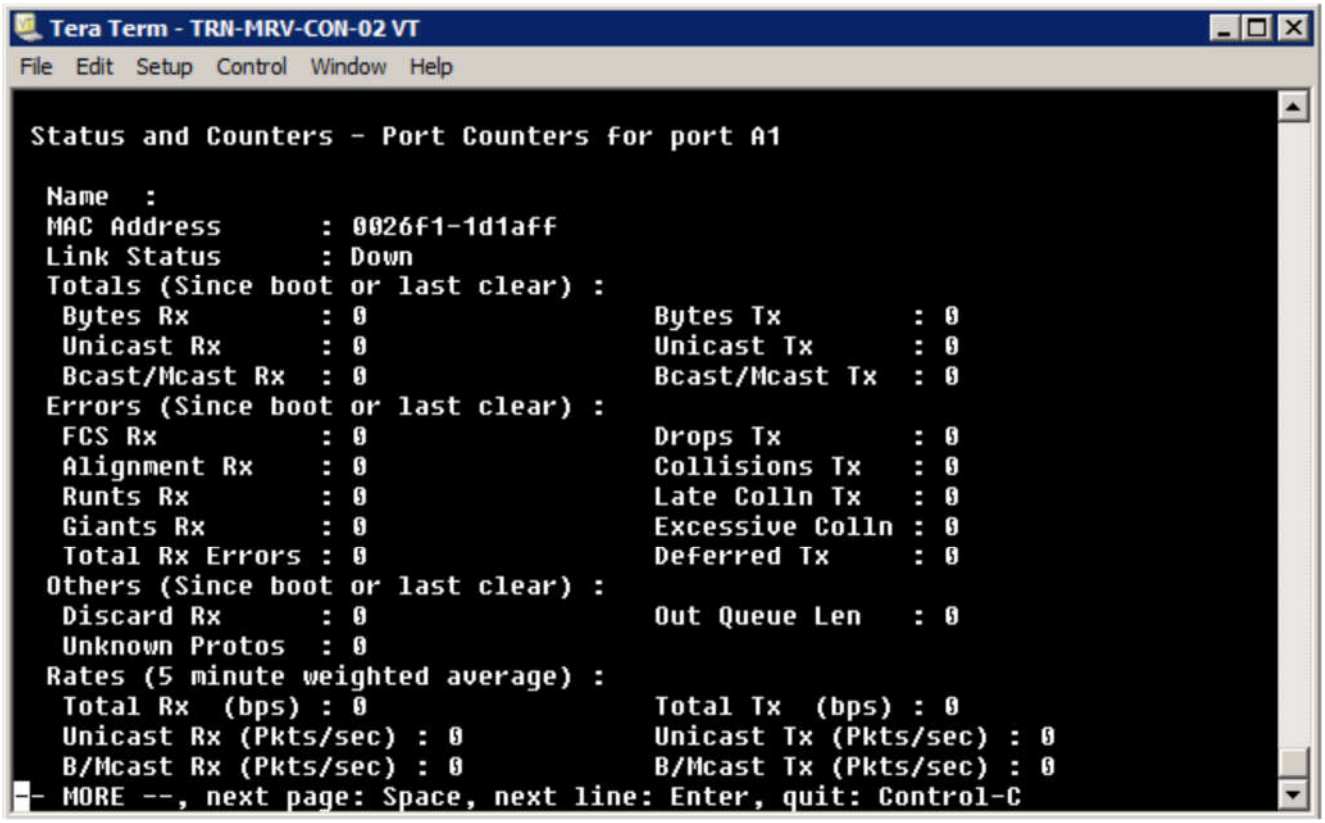


Рисунок 4.18 – Статичні порти

Надана інформація включає наступне:

1. Статус з'єднання.
2. Загальна кількість байтів, юнікаст, отримані і передані дані.
3. Швидкість приймання і передачі.

Там немає портів, які можуть бути пов'язані з новоствореною VLAN (Рисунок 4.19). Ви повинні зробити порт призначення після створення VLAN.

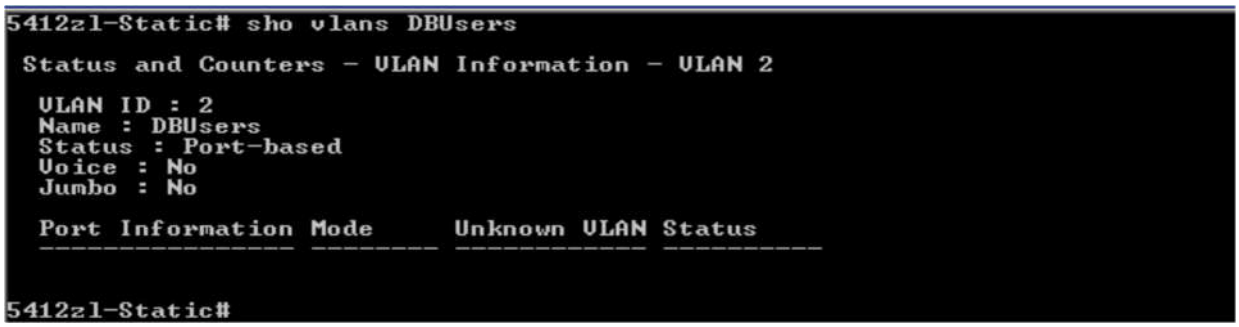


Рисунок 4.19 – Порт призначення нової VLAN

Ви повинні спочатку ввести контекст конфігурації. Потім, ви можете ввести контекст для VLAN, якою ви керуєте. Пам'ятайте, що ви повинні ввести ідентифікатор, коли ви переключаєтеся на віртуальній локальної мережі зв'язку. Для управління VLAN 2, виконайте наступне в контекстному рядку конфігурації:

5412zl-Static (config) #vlan 2

Новим командним рядком буде:
5412zl-Static (vlan-10) #

За замовчуванням, всі порти будуть налаштовані як нетеговані. Щоб налаштувати тегований порт, виконайте наступну команду:

tagged <port>

Пам'ятайте, що коли ви маєте справу з модульним комутатором, порт призначення буде виглядати наступним чином:

tagged b1

Щоб змінити маркований порт назад в нетегований порт, виконайте:

untagged <port>

Ви можете вказати один або діапазон портів, як в прикладі (Рисунок 4.20).

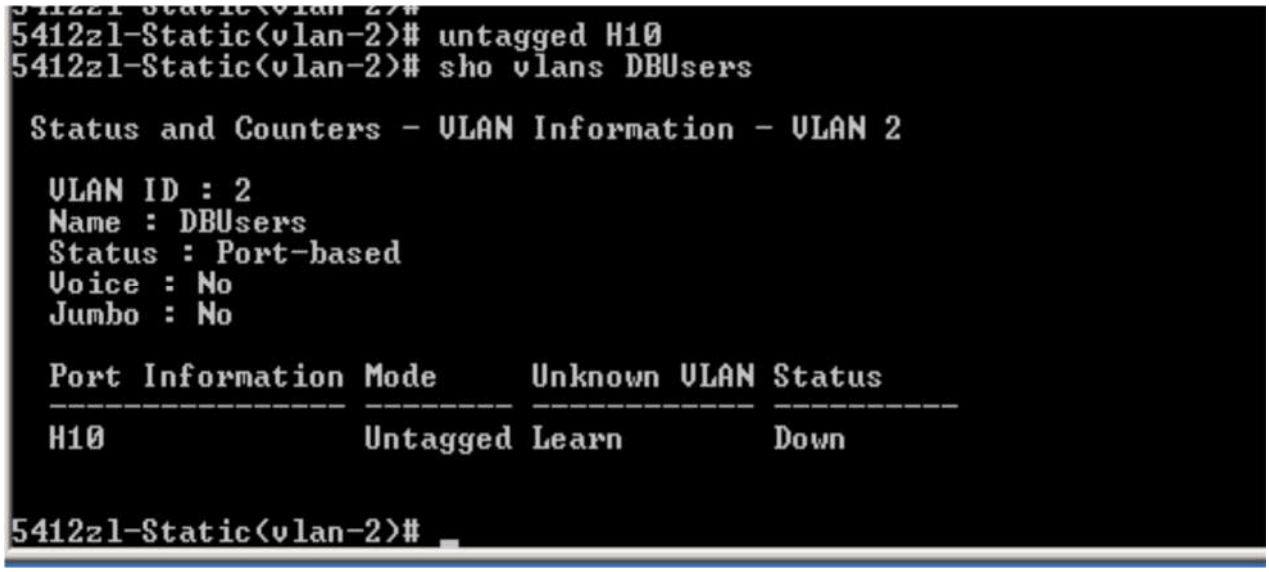


Рисунок 4.20 – Додавання портів

У цьому прикладі, також потрібно включити порт. Коли порт налаштований як тегований член VLAN, його статус (тегований або нетегований) в будь-який інший VLAN залишається незмінним.

Коли порт нетегований, він завжди буде віддалений від будь-якої іншої VLAN, в якій в даний час він тегований.

Коли ви змінюєте тегований порт на нетегованний в тій же VLAN, цей порт не стає автоматично нетегованим в інший VLAN.

В цьому випадку, якщо тегований порт повинен бути нетегованим в інший VLAN, він повинен бути вручну позначений як нетегований в цієї VLAN.

Пам'ятайте, що ви повинні записати зміни в пам'ять, щоб оновити конфігурацію запуску. В іншому випадку, всі не збережені зміни будуть втрачені, якщо ви перезавантажити комутатор.

Рівень 3. Управління

Комутатори рівня 3 підтримують широкий діапазон зміни команди підтримки маршрутизації і допомагають забезпечити доступ до послуг мережі.

Команди маршрутизатора в цьому розділі є команди на комутатор з назвою "Router". У командному рядку показується, як легше це зробити, що б побачити контекст команди.

Ми почнемо з розгляду зразка конфігурації мережі (Рисунок 4.21).

При використанні комутатора в якості маршрутизатора, як в цьому прикладі, налаштовується маршрутизатор в якості шлюзу для клієнтів і для передачі трафіку між налаштованими VLAN.

Шлюз за замовчуванням (default gateway) - роутер за замовчуванням, який використовується для передачі трафіку у разі, коли конкретний маршрут призначення ніхто не знає або не вказано.

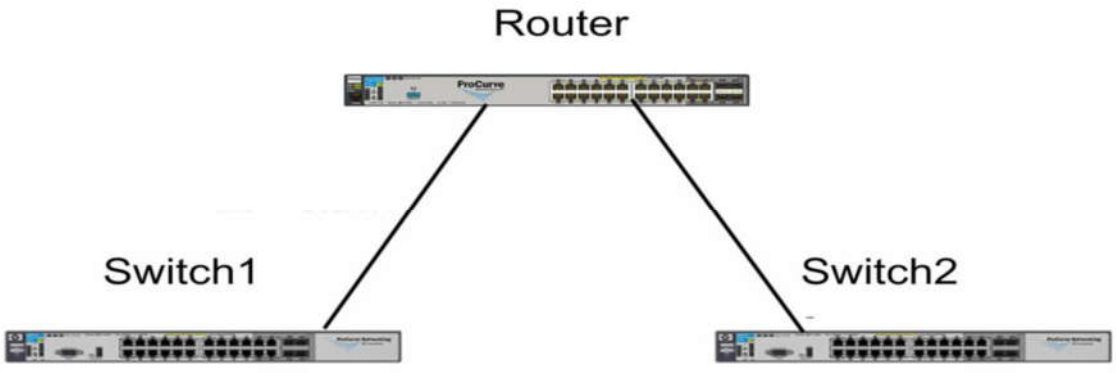


Рисунок 4.21 – Зразок конфігурації мережі

Щоб використовувати комутатор в якості маршрутизатора, необхідно спочатку включити маршрутизацію. Для цього з контексту конфігурації, виконайте наступне:

Router (config) # ip routing

Використання пінга для усунення зв'язку підтримується як і в меню інтерфейс, так і в веб-інтерфейсі.

Ви також повинні налаштувати комутатор зі шлюзом за замовчуванням для віддаленого управління по мережі VLAN, яка присвячена для управління пристроєм. Шлюз за замовчуванням повинен бути в тій же підмережі, що і IP-адресу управління комутатором. Це робиться з кінцевим комутатором в контексті конфігурації. Припускаючи, що адреса шлюзу в 192.168.10.1, виконайте наступне:

Switch1 (config) # ip default-gateway 192.168.10.1

Параметр helper-address використовується для включення комутатора, що направляє DHCP запити від всіх VLAN, до DHCP-сервера або до іншої VLAN. Наприклад, у вас може бути DHCP-сервер в мережі VLAN 100 і клієнтські комп'ютери в мережі VLAN 2, 3 і 5. Ця команда повинна бути запущена окремо для кожного VLAN, використовуючи контекст VLAN:

Router (vlan-1) # ip helper-address <ip _address>

Зверніть увагу, що в цій команді, ви повинні замінити <ip_address> з IP-адреси DHCP-сервера. Helper - address налаштований на маршрутизаторі або на

рівні 3 комутатора. Налаштування допоміжного адреси комутатора на рівні 2 не має ніякого ефекту.

Наприклад, якщо клієнти на VLAN 2 повинні орендувати IP-адреси з DHCP-сервера з адресою 10.10.5.2, виконайте наступне:

Router (vlan2) # ip helper-address 10.10.5.2

Ви можете використовувати команду пінг для перевірки комунікацій з комутатором для підключеного пристрою. Щоб перевірити підключення маршрутизатора на пристрій, підключений до одного з кінцевих комутаторів, запустіть команду, схожу на наступне:

Router # ping 192.168.1.108

Агрегація каналів

Агрегація каналів, або об'єднання портів, дозволяє створити більш високу пропускну здатність шляхом зв'язування кілька фізичних портів в один логічний канал зв'язку. HP використовує стандартний протокол, що має назву LACP, щоб управляти об'єднання портів в своїх комутаторах.

Об'єднання портів (port trunking) - відоме як агрегація каналів, це поєднання фізичних портів, щоб створити один канал зв'язку для забезпечення більш високої пропускної здатності зв'язку.

Link Aggregation Control Protocol (LACP) - протокол, який використовується для управління об'єднаних фізичних портів в якості одного каналу зв'язку.

LACP визначається в RFC 802.3ad.

Агрегування каналів іноді робиться для забезпечення більш високої пропускної здатності між маршрутизатором і пов'язаними кінцевими комутаторами. Воно також може бути використано для створення магістральної мережі з високою пропускною здатністю. Серверні операційні системи також підтримують агрегацію каналів, що дозволяє зв'язати кілька мережевих адаптерів, щоб поліпшити зв'язок з мережевими серверами.

Налаштування агрегації каналів вимагає контекст конфігурації, для цього введіть:

<Port_id, port_id> trk <id> lacp

Для введення фактичних значень потрібно виконати наступний рядок команд:

trunk a4, a5 trk2 lacp

Щоб побачити з'єднання, які налаштовані на комутаторі, виконайте наступне:

show trunk

Це поверне список з'єднань і їх асоційовані порти (Рисунок 4.22).

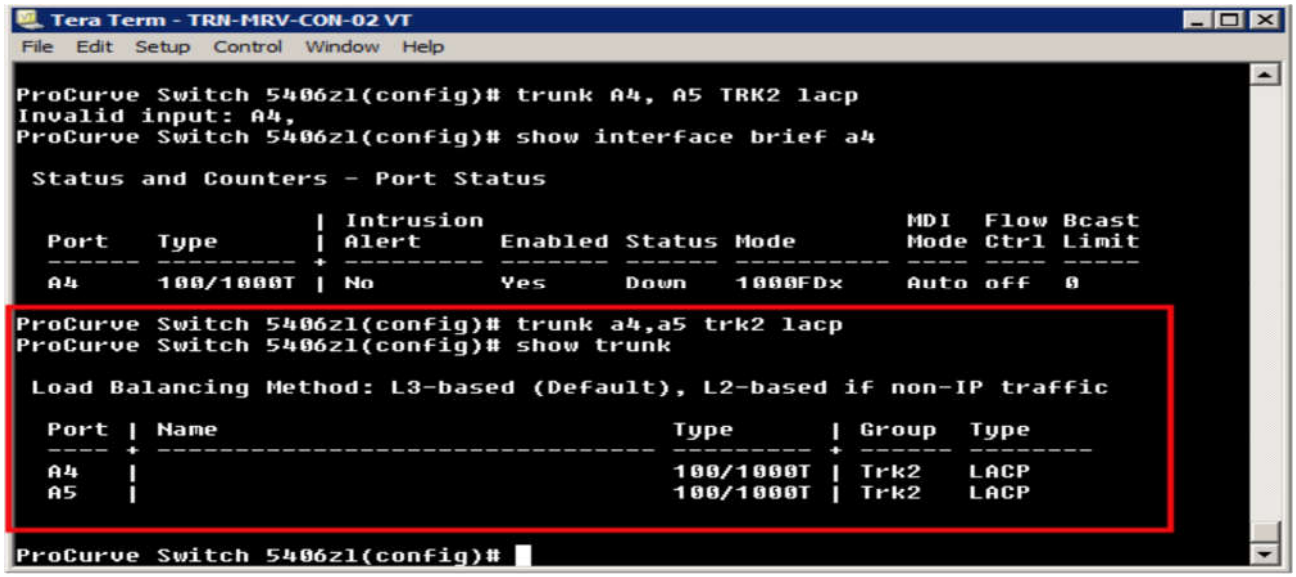


Рисунок 4.22 – Налаштування шин

Рисунок 4.22 показує команду об'єднання і результуючий список. Результати позначені як балансування навантаження, яке також згадується як розподіл навантаження. Це означає, що комутатор буде намагатися зберегти трафік між двома портами в тому ж обсязі.

Балансування навантаження (load balancing) - процес обміну трафіку в рівній мірі, коли доступні кілька фізичних ліній зв'язку.

Ви можете отримати більш детальну інформацію про сконфігуровані порти, виконавши такі дії:

show interface brief a4-a5

Це дасть вам короткий виклад інформації про порт (рис. 4.23).

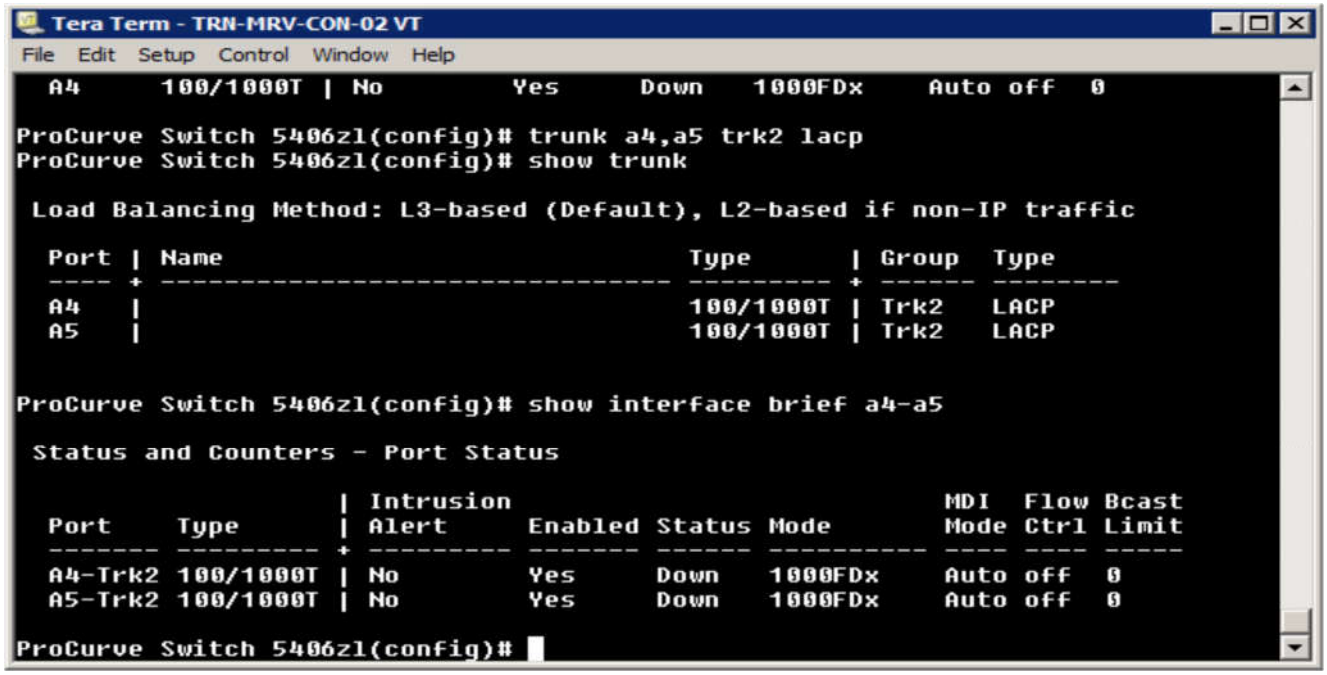


Рисунок 4.23 – Дані про стан портів

У цьому прикладі, обидва порти мають статус Down, так як комутатор не може фізично підключатися до будь-якого з портів.

Щоб зв'язати об'єднання з VLAN, виконайте наступні дії в контексті конфігурації:

vlan <id> tagged trk <id>

Наприклад, щоб зв'язати trunk 2 з VLAN 10, виконайте наступне:

vlan 10 tagged trk2

Тут маркування може стати практичною частиною вашої конфігурації. Оскільки порти TRK2 тегований, вони можуть бути частиною декількох VLAN.

Конфігурація комутаторів

До цього моменту ми мали справу з двома конфігураціями, поточною конфігурацією, яка використовується, і конфігурацією запуску зберігається у флеш-пам'яті. Зміни в конфігурації зберігаються тільки в поточній пам’яті, поки ви не виконаєте команду - write memory. Ви можете створити резервну копію конфігурації на USB або на сервері TFTP.

Разом з даними конфігурації, образи прошивки, які використовується для завантаження комутатора, зберігаються у флеш-пам'яті. Насправді, комутатор має два образи прошивки: первинні і вторинні. Вони можуть мати однакові або різні версії файлу. Можуть бути скопійовані з комутатора на будь-яку флеш-пам'ять або сервер TFTP.

Процедури, обговорені в цьому розділу, припускають наявність доступного USB порта на комутаторі.

Управління конфігурацією

Перед початком роботи з конфігураціями комутатора, ви повинні переконатися, що поточна конфігурація і конфігурація запуску однакові. Таким чином, ви починаєте з відомого базового рівня. Ви можете переглянути поточну конфігурацію, виконавши такі дії:

show running-config

Для порівняння поточної конфігурації із збереженою конфігурацією запуску, виконайте наступне:

show running-config status

Якщо вони відрізняються, пам'ятайте, що ви можете написати в пам'ять, щоб зберегти поточну конфігурацію в якості нової конфігурації запуску.

Створення резервних копій файлів конфігурації

Щоб побачити файл конфігурації або файли, що зберігаються у флеш-пам'яті комутатора, ви можете запустити наступне:

show config files

Це повертає список файлів конфігурації. За замовчуванням, комутатор буде мати одну конфігурацію. Рисунок 4.24 показує комутатор, який виконаний з двома файлами конфігурації.

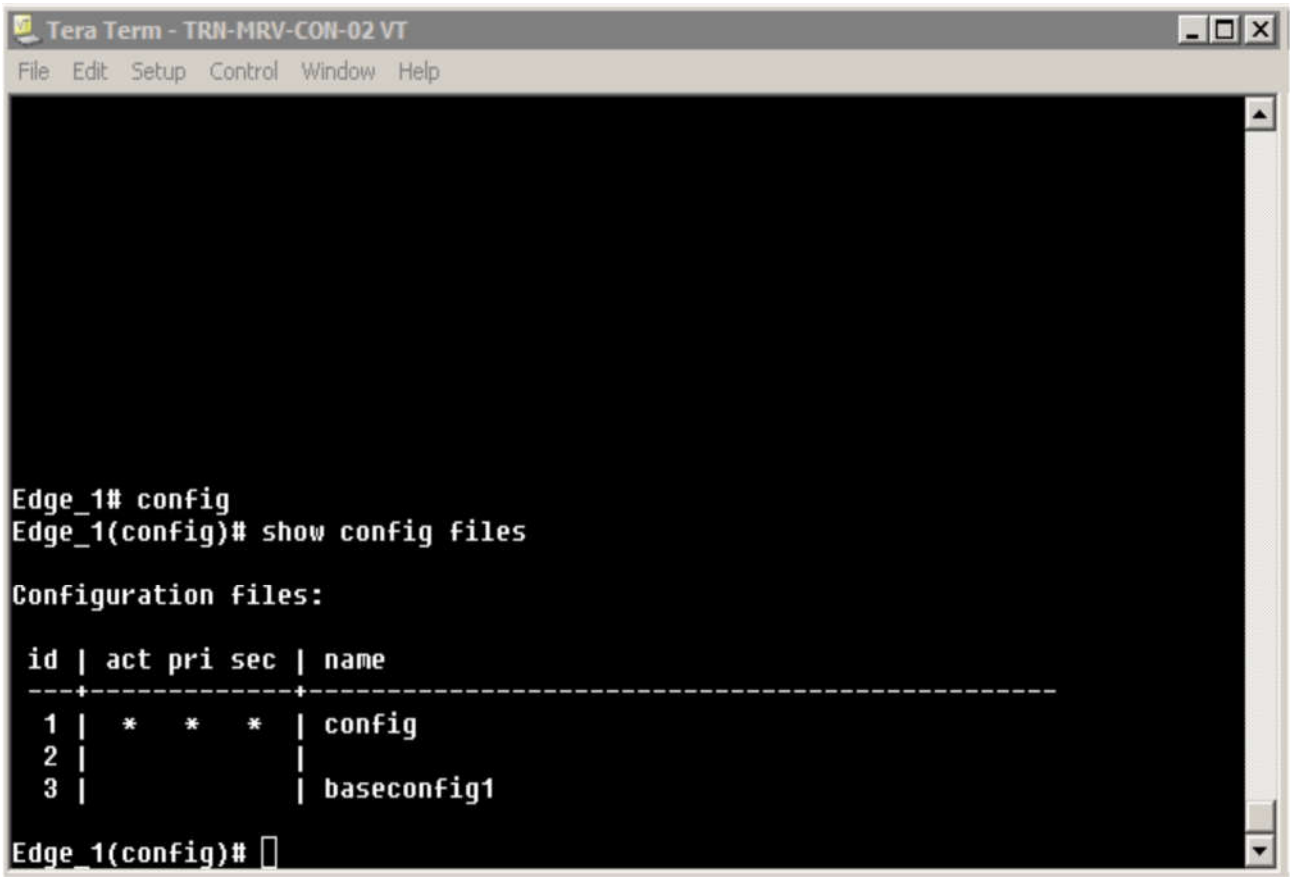


Рисунок 4.24 – Файли у флеш-пам’яті комутатора

Там може бути до трьох файлів конфігурації. Зверніть увагу, що у вас є три колонки між ідентифікатором і ім'ям конфігурації. Зірочка вказує на:

Act

Активна конфігурація, вона використовується для завантаження комутатора

Pri

Конфігурація прив'язується до первинного образу прошивки

Sec

Конфігурація прив'язується до вторинного образу прошивки.

Ви також можете подивитися на інформацію про конфігурацію, яка зберігається у файлі конфігурації за допомогою команди show config з подальшим ім'ям файлу. В цьому випадку, виконайте наступне:

show config config

Будьте обережні при вказівці конфігурації файлу. Команди не чутливі до регістру, тільки на імена. Це повертає той же тип інформації, яку ви можете побачити, якщо відобразите поточну конфігурацію (Рисунок 4.25).

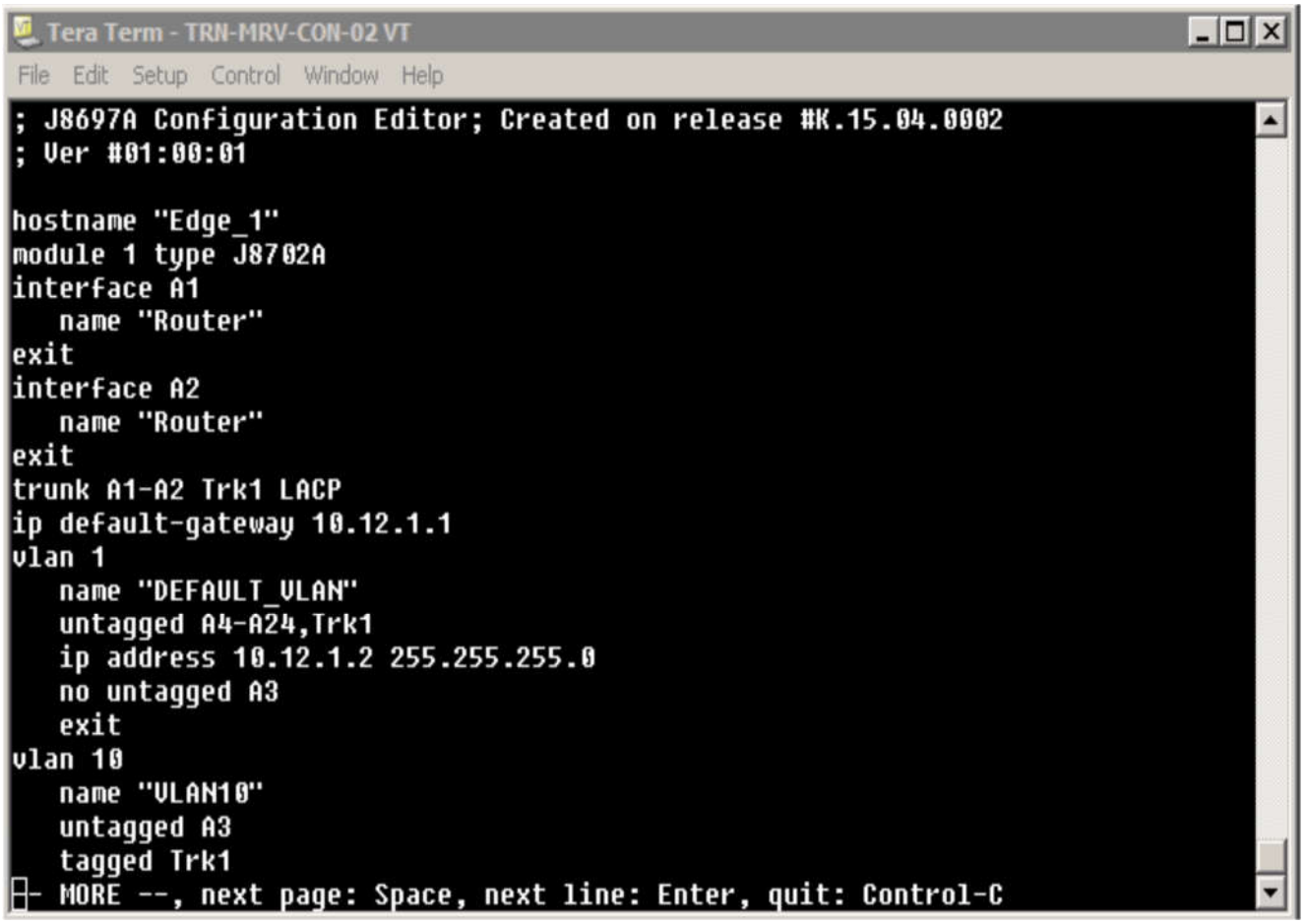


Рисунок 4.25 – Поточна конфігурація

Для резервного копіювання початкової конфігурації на флеш-накопичувач USB, виконайте наступне:

copy startup-config usb <filename>. <ext>

Коли ви виконуєте цю команду, замініть <filename> і <ext> з фактичними значеннями. наприклад:

copy startup-config usb switch1.cfg

Ви можете також проводити резервне копіювання на сервер TFTP, використовуючи наступне:

copy startup-config tftp <ip_address> <filename>. <ext>

Команда повинна бути введена як безперервна послідовність. Команда іноді може не поміщатися в текстовому рядку. Щоб ввести команду, просто продовжуйте її введення, поки не закінчите, після чого натисніть клавішу "Enter" для запуску команди.

Управління декількома файлами конфігурації

У вас також є можливість зберігання кількох конфігураційних файлів на комутаторі. Ви можете створити новий - шляхом копіювання існуючого файлу. Розглянемо наступну команду копіювання:

copy config baseconfig1 config baseconfig2

Це створює дублікат baseconfig1 з ім'ям файлу baseconfig2. Якщо подивитись конфігураційні файли, то побачимо помічені три файли (Рисунок 4.26).

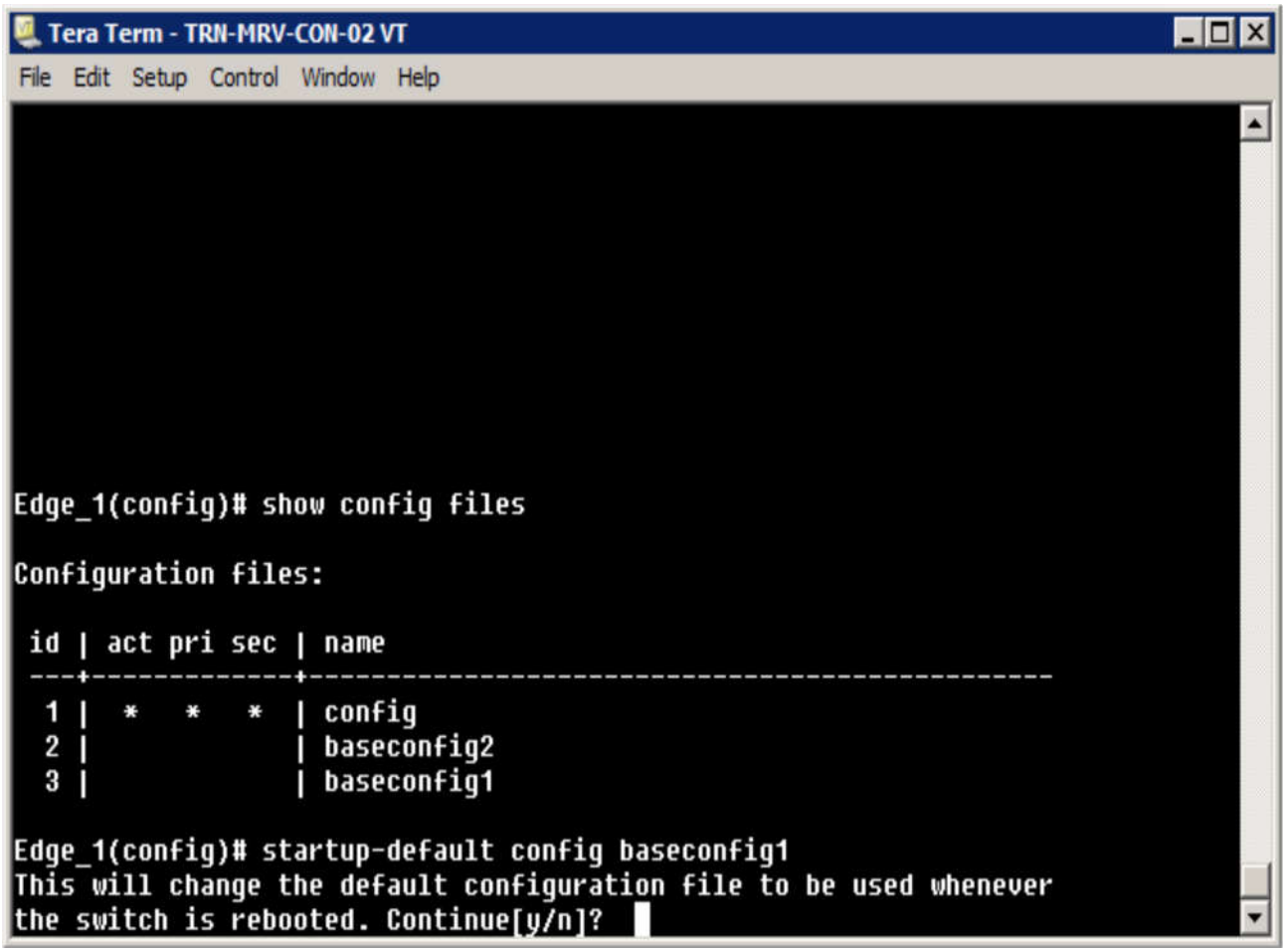


Рисунок 4.26 – Файли конфігурації

Для того, щоб новий файл конфігурації став файлом конфігурації запуску, виконайте наступне:

startup-default config <configname>

У цьому прикладі, ви би виконали наступне:

startup-default config baseconfig1

Вам буде запропоновано перевірити свою дію. Зміни не вступлять в силу до тих пір, поки комутатор не буде перезапущений.

Команда, яка показана вище, пов'язує конфігураційний файл baseconfig1 з первинним і вторинним чином прошивки (Рисунок 4.27).

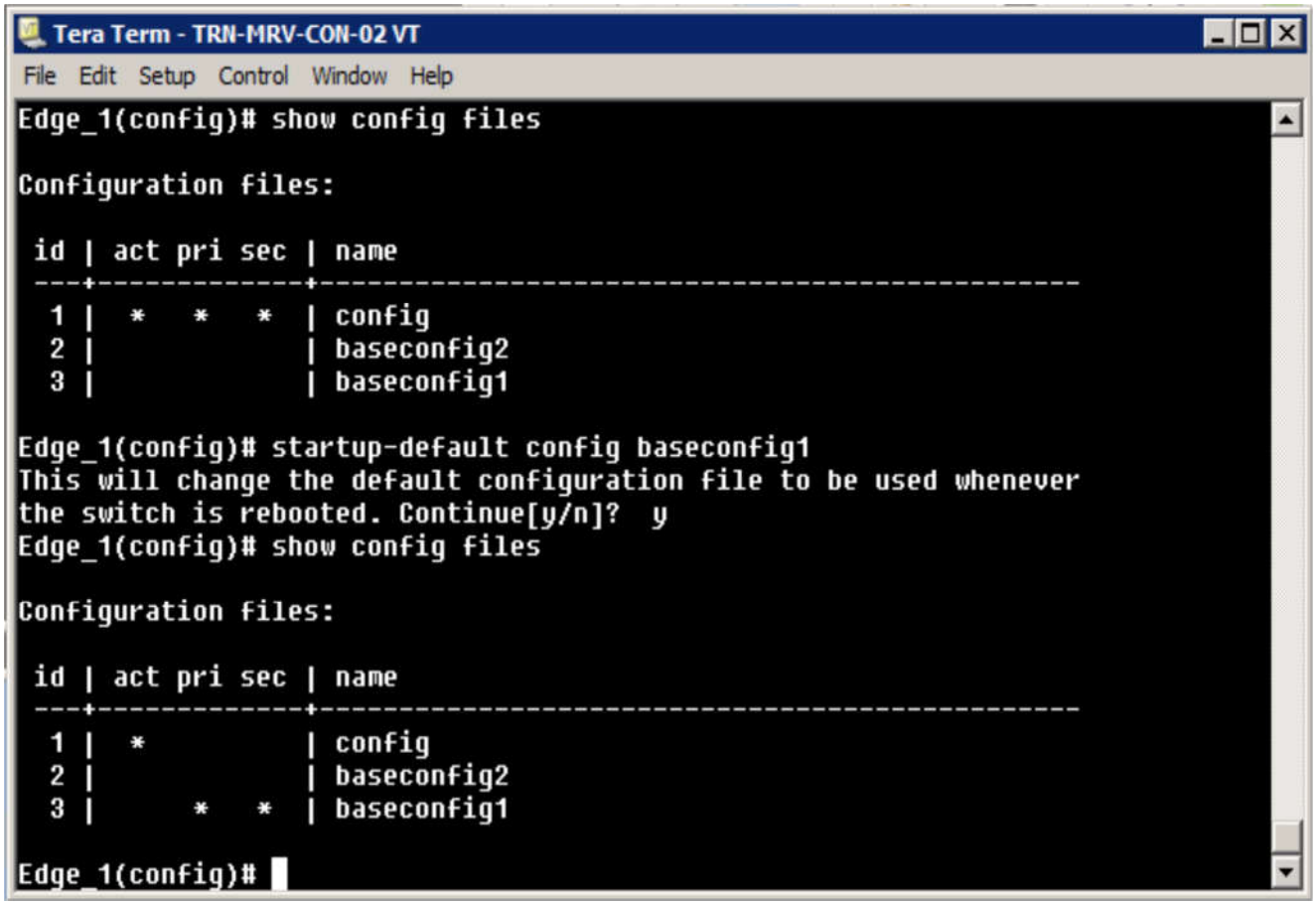


Рисунок 4.27 – Звязок із первинним і вторинним образом прошивки

У цей момент, конфігурація як і раніше є активною, тому що вона є останньою, яка використовується для завантаження комутатора. Наступного разу при завантаженні, baseconfig1 буде використовуватися в якості файлу конфігурації запуску і початкової запущеної конфігурації.

Після перезавантаження, всі зміни конфігурації, які ви внесли в робочу конфігурацію, збережуться в "baseconfig 1". Файл конфігурації буде залишатися незмінним, поки він не буде активованим.

Ви також можете пов'язати файли конфігурації з різними образами прошивки. Наприклад, ви могли б пов'язати конфігурації початкової прошивки і baseconfig1 з вторинним образом. Щоб зв'язати основний образ прошивки тільки з настройками, виконайте наступне:

startup-default primary config config

Це пов'язує конфігураційний файл з основним, в той час як baseconfig1 досі асоціюється з вторинним образом прошивки (Рисунок 4.28).

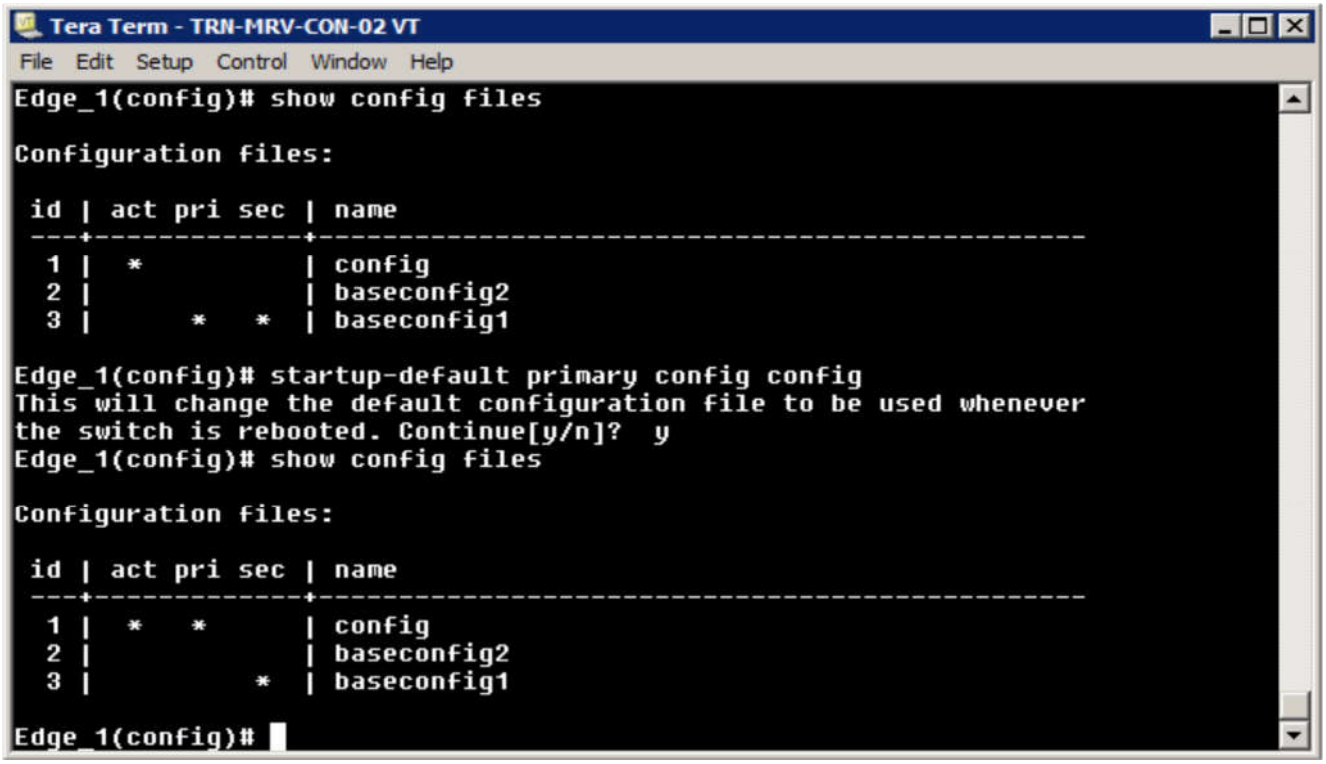


Рисунок 4.28 - Зв’язок із первинним і вторинним образом прошивки

Команда *erase* дозволяє видалити файл конфігурації з флеш-пам'яті. Наприклад, щоб видалити *baseconfig2,* виконайте наступне:

erase config baseconfig2

Це видаляє файл конфігурації і залишає відкритий файл (Рисунок 4.29).

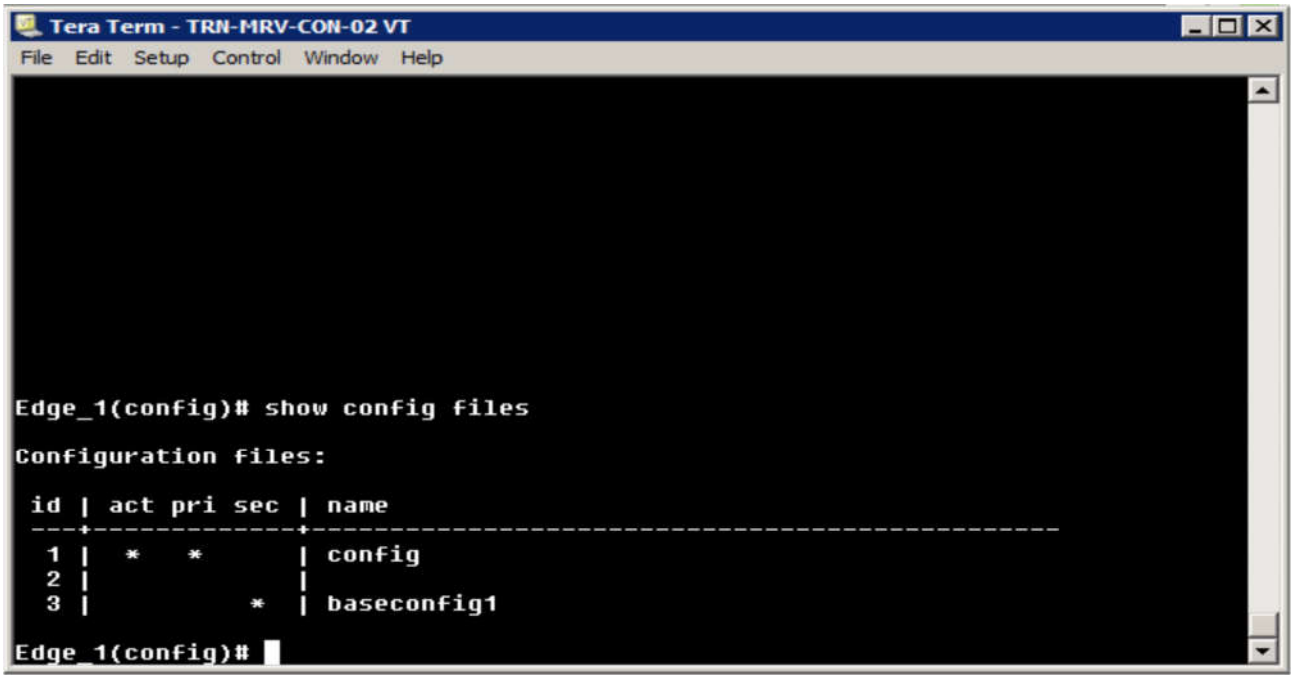


Рисунок 4.29 – Видалення образу прошивки

Якщо ви видалите активний файл конфігурації, то вам буде запропоновано замінити його на інший. У цьому випадку, ви отримаєте наступне повідомлення:

The specified configuration file "baseconfig1" is the default configuration for the primary and / or secondary boot image. If it is deleted, the current active configuration file "config" will be set as the default.

Натисніть "у, щоб мати пере конфігурований файл.

Управління програмним забезпеченням

Комутатор програмного забезпечення зберігається у флеш-пам'яті разом з файлом конфігурації запуску (Рисунок 4.30). Існує дві програмні прошивки, які визначені як первинні і вторинні. За замовчуванням, комутатор налаштований на завантаження з головним образом прошивки.

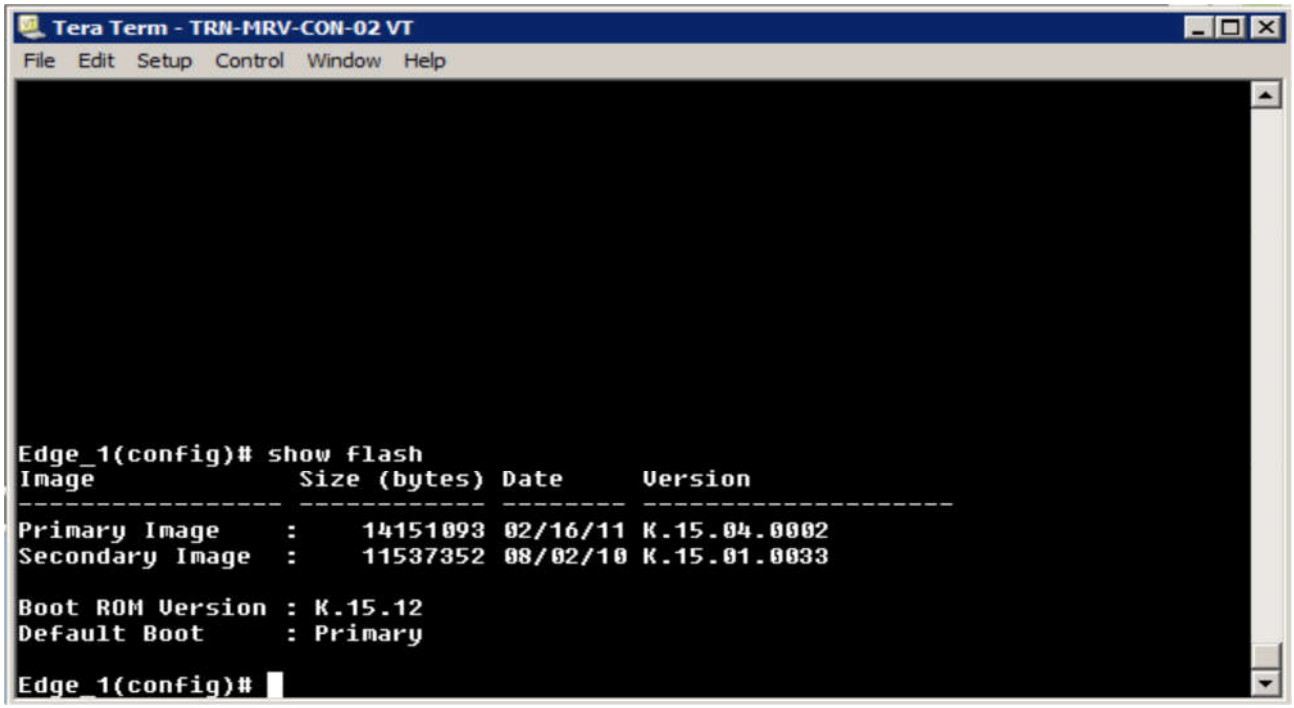


Рисунок 4.30 – Образ прошивки програмного забезпечення

В цьому випадку, є два способи версії прошивки. Чим вище номер версії, тим він вказує на більш свіжу. Основна прошивка має номер версії K.15.04.0002 і є пізнішою. Вторинна має номер версії K.15.01.0033. Прошивки кожного комутатора залежать від його серії. "K" образ прошивки є для комутаторів 3500yl, 5400zl, 6600 і 8200zl серії.

Рисунок 4.31 показує інформацію про версії для старшої моделі комутатора з більш старою версією. Розмір файлу, в даному випадку, значно менше, ніж більш нової версії.

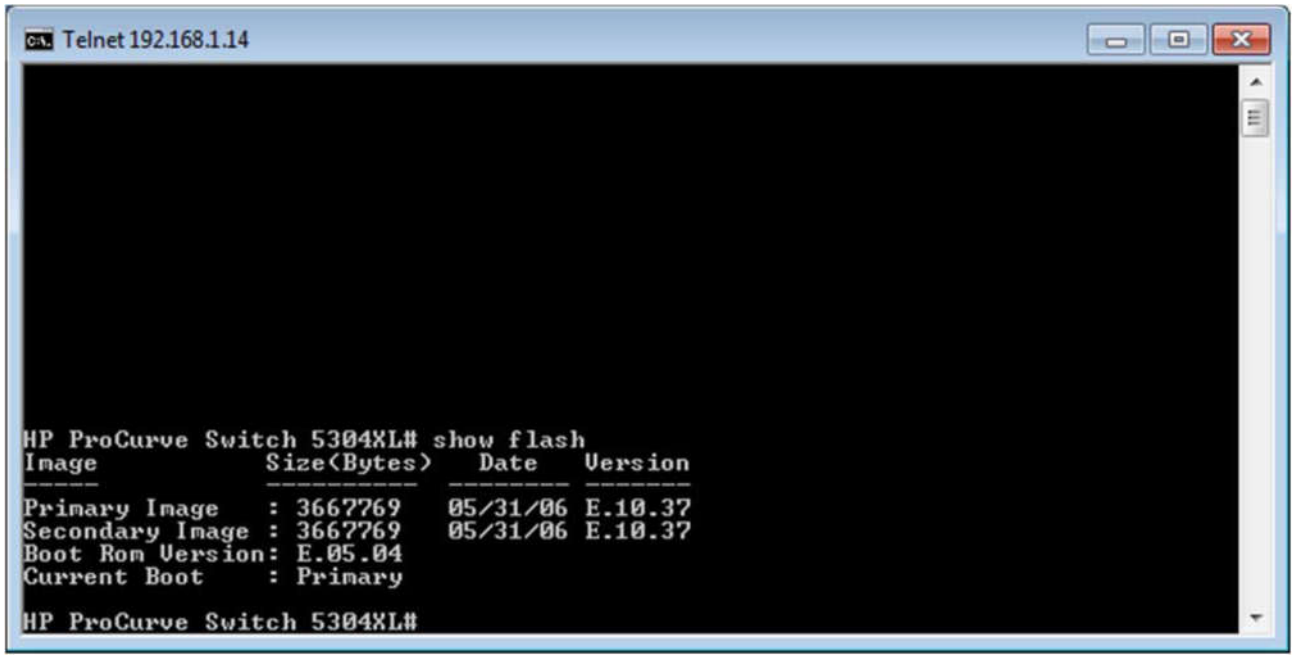


Рисунок 4.31 - Інформація про версії старшої моделі комутатора

Одним з варіантів оновлення системного ПЗ, є завантаження файлу на диску USB, а потім застосування зображення на флеш-пам'ять комутатора. Щоб скопіювати програмне забезпечення в якості вторинного образу прошивки, виконайте наступне:

copy usb flash <filename> secondary

Це залишає основну копію незмінною. Вкажіть "primary" в кінці рядка команди, якщо ви хочете скопіювати файл з диска USB на флеш-пам'ять. Це може зайняти від двох до трьох хвилин, щоб застосувати оновлене програмне забезпечення.

Після копіювання образу прошивки в флеш-пам'ять, потрібно завантажитися з цього образу прошивки, щоб перевірити, чи все працює правильно. Для одноразового запуску вторинного образу, введіть наступну команду:

boot system flash secondary

Вам буде запропоновано перевірити свою дію і зберегти конфігурацію в файл конфігурації запуску флеш-пам'яті. Коли комутатор перезавантажиться, ви втратите з'єднання управління до комутатора. Вам потрібно буде відновити зв'язок після завершення перезавантаження комутатора.

Розділ 5:
Стек протоколів TCP/IP

Введення

Мережеві протоколи були колись одним з найбільших перешкод для створення інтегрованих мережевих середовищ. Ми вже обговорювали деякі з питань представлених протоколів нижнього рівня і протоколів більш високого рівня. Проблеми, які ми бачили на більш високих рівнях були ще більш складні, ніж на низькому рівні. На більш високих рівнях було кілька конкуруючих протоколів, тому що у кожної мережевої операційної системи був свій, як правило, власний протокол.

Тепер, через кілька років, ситуація стала менш складною, і один набір протоколів став загальноприйнятим стандартом: стек протоколів Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP є набором протоколів на яких побудований інтернет, а також майже всі локальні мережі ПК. Ми обговорювали TCP/IP протягом цього курсу. Тепер ми уважно подивимося на TCP/IP. Ми розглянемо, що реалізується на кожному рівні моделі DARPA і як протоколи, які складають протокол TCP/IP працюють разом. Нашу увагу буде сконцентровано на практичних застосуваннях.

Мета

У цьому розділі ви дізнаєтеся, як:

- Визначити протоколи, реалізовані на кожному рівні Мережевий моделі DARPA
- Відповідність протоколів TCP/IP рівням моделі OSI.
- Описати призначення та іспользованте протоколів IPv4 та IPv6.
- Пояснити призначення класів адрес.
- Порівняти протоколи TCP і UDP, а також їх ролі в передачі даних.
- Зробити перелік і описати загальні прикладні протоколи.
- Ручна конфігурація TCP/IP налаштування.

Стек протоколів TCP/IP

Набір протоколів TCP/IP став стандартом для роботи в мережі. Процедури встановлення та налаштування стали стандартними, і майже будь-яке обладнання виробника може обмінюватися даними з будь-яким іншим обладнанням виробника,

принаймні з точки зору протоколу. Це домінування, а також стандартизація методів доступу до мереж 802.3 та 802.11 сприяли зростанню як корпоративних, так і домашніх мереж.

Розглянемо дві найбільш популярні операційні системи для персональних комп'ютерів: Microsoft Windows і різні версії розподілу Linux. При установці операційної системи для ПК клієнта, він буде автоматично встановлювати TCP/IP і налаштовувати його, щоб запросити IP-адреса, коли він підключається до мережі. У перші дні цих операційних систем, особливо Windows, TCP/IP був лише одним з багатьох доступних варіантів протоколів.

Переважна більшість комп'ютерних мереж використовують TCP/IP. Інтернет, який є найбільшою мережею взаємопов'язаною зі світом, також використовує TCP/IP як його єдиного протоколу. Це означає, що комп'ютер повинен працювати з протоколом TCP/IP для доступу до Інтернет.

Через домінування TCP/IP в галузі, розуміння сучасних мереж і управління мережею вимагає розуміння TCP/IP. Оскільки TCP/IP базується на повній мережній моделі, подібній семирівневій моделі OSI, він включає широкий спектр технологій і функціональності.

Модель TCP/IP

Ми почнемо з розгляду моделі TCP/IP (Рисунок 5-1). Ми коротко раніше розглядали, як моделі OSI і TCP/IP (технічно DARPA) зіставляються один з одним.

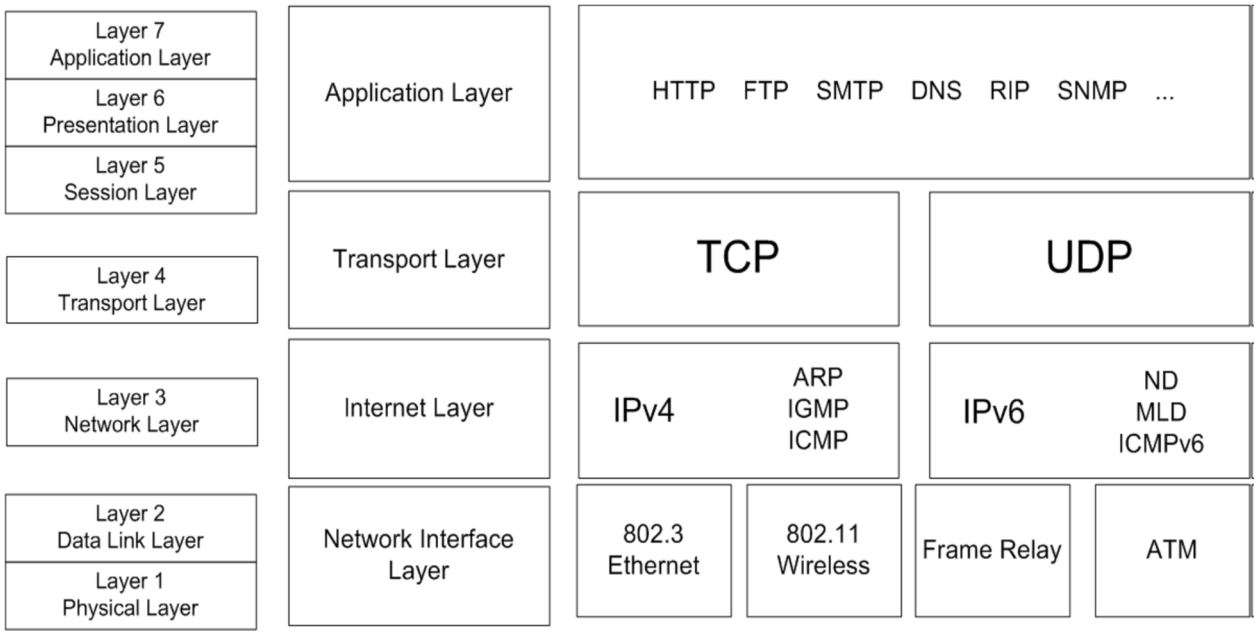


Рисунок 5.1 Модель TCP/IP

- TCP/IP Рівень доступу до мережі відповідає Канальному рівню (Data Link layer) та Фізичному рівню (Physical layer) моделі OSI.
- TCP/IP Рівень Інтернет відповідає Мережевому рівню (Network layer) моделі OSI.

- TCP/IP Транспортний рівень відповідає Транспортному рівні моделі OSI і частини функціональності Сеансового рівня моделі OSI.
- TCP/IP Прикладний рівень відповідає Сеансовому рівні, Рівню представлення та Прикладному рівню моделі OSI.

Як і в моделі OSI, кожен рівень TCP/IP пов'язується з рівнем безпосередньо над або під ним. TCP/IP не єдиний протокол, який надає цю функціональність. Проте, деякі інші протоколи, які все ще використовуються, здебільшого є пропрієтарними технологіями, що використовуються в спеціалізованих додатках, або це застарілі програми, які навряд чи будуть оновлені.

Крім того, TCP/IP є відкритим стандартом і продовжує рости і розвиватися. Технічна група з інженерної справи в Інтернеті (IETF) є органом стандартизації для Інтернету, включаючи все, що стосується комплекту протоколів TCP/IP. TCP/IP визначається через ряд документів, відомих як Запити на коментарі (RFC). Робоча група мережі пропонує RFC, які потім переходять до процесу експертної оцінки. Якщо RFC приймаються як стандарт, вони публікуються IETF.

Internet Engineering Task Force (IETF) - *Формальна частина суспільства Інтернет (ISOC) відповідальна за визначення Інтернет стандартів. Вона складається з робочих груп та обговорення групи, кожна має справу з конкретною тематичної областю.*

Запити на коментарі (RFC) - *Документи, що визначають стандарти Інтернет, в тому числі протоколу TCP/IP. RFC стає стандартом, коли формально опубліковано IETF.*

Рівень доступу до мережі

Рівень мережевого інтерфейсу також іноді називають рівнем доступу до мережі. На рівні мережевого інтерфейсу реалізуються протокол доступу до мереж низького рівня та контролю доступу до медіа. Протоколи низького рівня, що підтримуються на цьому рівні, такі як 802.3 Ethernet, 802.11 wireless, Frame Relay і режим асинхронної передачі (ATM), не є частиною протоколу TCP/IP, але є прикладами підтримуваних протоколів доступу до мережі.

Однією з переваг пакету TCP / IP є те, що вона була розроблена таким чином, щоб бути незалежною від конкретних деталей доступу до мережі. Це не безпосередньо стосується таких питань, як спосіб доступу до мережі, розмір і формат кадру, або навіть середовище передачі даних. Натомість TCP/IP призначена для зв'язку зі стандартними протоколами доступу до мережі, що дозволяє розгортати його практично в будь-якому мережевому середовищі.

MAC-адреса, яка також називається фізичною адресою, підтримується на рівні мережевого інтерфейсу. Як було описано раніше, MAC адреса записується як 12-значне шістнадцяткове число (Рисунок 5.2). Перші шість цифр ідентифікують

виробника мережевого інтерфейсу. Решта цифри представляють унікальну адресу адаптера.

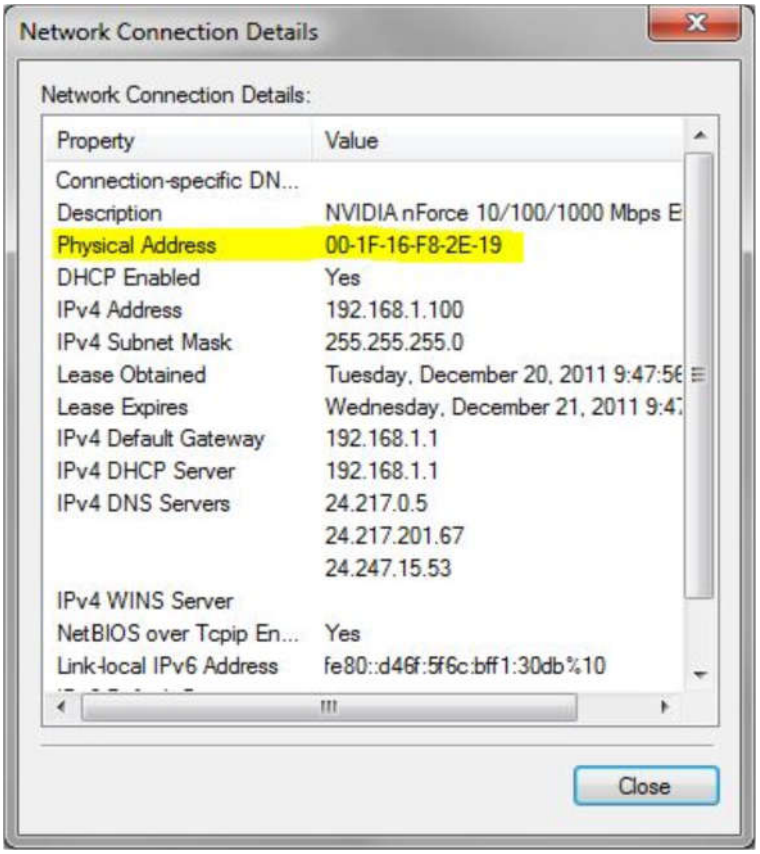


Рисунок 5.2 MAC-адрес

Модель OSI має певні можливості, яких модель TCP/IP не має. Наприклад, TCP/IP не передбачає секвенування і підтвердження на рівні доступу до мережі. Насправді, рівень Інтернет моделі TCP/IP припускає, що рівень доступу до мережі і його базової інфраструктури, ненадійні і залишає функціональність, яка необхідна для забезпечення надійного зв'язоку з верхніми рівнями за собою.

Рівень Internet

Рівень Internet моделі TCP/IP відповідає за ту жсаму функціональність, що і рівень Network моделі OSI. Його основні обов’язки містяться у наступному:

- Пакетування даних для передачі.
- Унікальна адресація хоста.
- Функції маршрутизації пакетів.

Існує два Интернет протоколи, які визначені на рівні Internet для забезпечення цієї функціональності: IPv4 и IPv6. IP-адреси налаштовуються за допомогою програмного забезпечення, а не через апаратні засоби, такі як MAC-адреси. У більшості мережевих середовищ властивості IPv4 і IPv6 налаштовуються для кожного мережного адаптера, навіть якщо IPv6 не використовується активно в мережі (рис. 5.3). Сучасні мережеві пристрої також розроблені для підтримки як IPv4 так і IPv6.

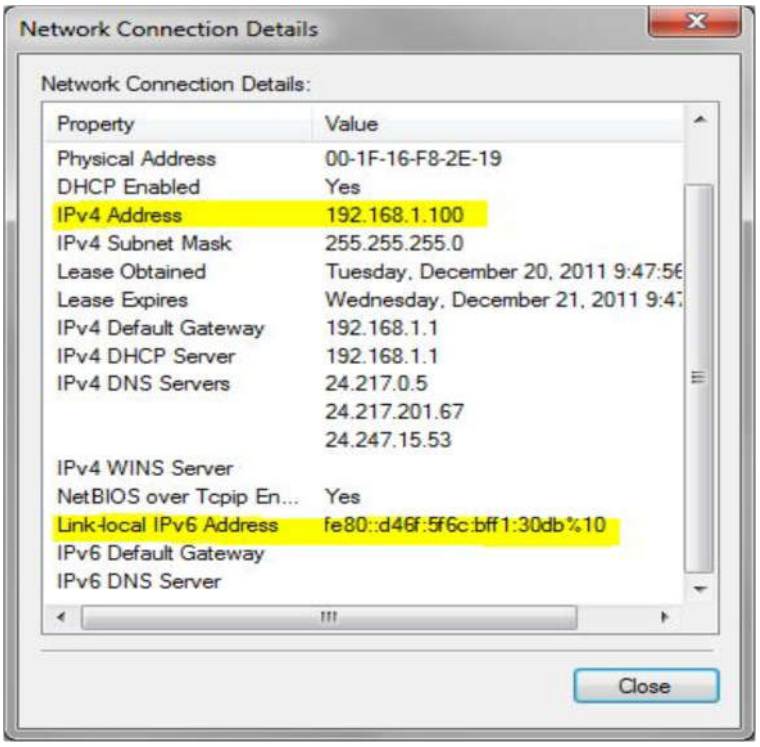


Рисунок 5.3

План, в кінцевому рахунку перейде в Інтернет, а потім в приватні мережі, на протокол IPv6 виключно. Перехід на IPv6 просувається, хоча повільно. В IPv6, MAC-адреса, згадується як адреса канального рівня.

Чому існує два інтернет-протоколи?

IPv4 був використаний протягом багатьох десятиліть. IPv4 є 32-бітовим адресою, який надає в цілому 4,294,967,296 (232) адрес. Кількість біт, що використовуються для визначення адреси мережі та адреса хоста визначається маскою підмережі, пов'язані з адресою. Кількість адрес скорочується також тому, що деякі значення адрес непридатні за визначенням, і кілька мільйонів відведено для спеціальних застосувань і не підключені до Інтернету.

Маска підмережі *– значення, яке використовується для розмежування адреси мережі і адреси хоста в IPv4- адресі.*

Для всіх практичних цілей, все IPv4-адреси, які доступні для інтернету, повинні бути вже використані. Але обхідні прийоми, такі як NAT і CIDR, допомогли зробити більш ефективне використання доступних адрес, але вони є лише відстрочкою неминучого, коли адресація IPv4 буде вичерпана.

IPv6 розширює адресний простір до 128 біт. У теорії, це робить 2128 (340 undecillion) IP-адрес, доступних в інтернет, хоча деякі із них відведені для спеціальних цілей. Перші 64 біти використовуються в якості адреси мережі. Останні 64 біта, які часто основані на MAC-адресу хоста, використовуються в

якості адреси хоста. IPv6 підтримує ту ж саме функціональність, як IPv4, з деякими додатковими функціями. Поки все рухається до можливого переходу на IPv6 і скасування IPv4, а поки буде використовуватися дві схеми адресації.

IPv4

У стандартній конфігурації TCP/IP, кожен NIC має адресу IPv4. IPv4 адреси найбільш часто написані з використанням десяткової нотації.

Кожне десяткове число представляє значення одного октету з восьми бітів, значенням від 0 до 255.

Рисунок 5.4 Адрес IPv4

Крім того, кожна адреса буде асоційована з мережевої маскою. У більшості ситуацій, мережевій карті також буде присвоєна адресу шлюзу.

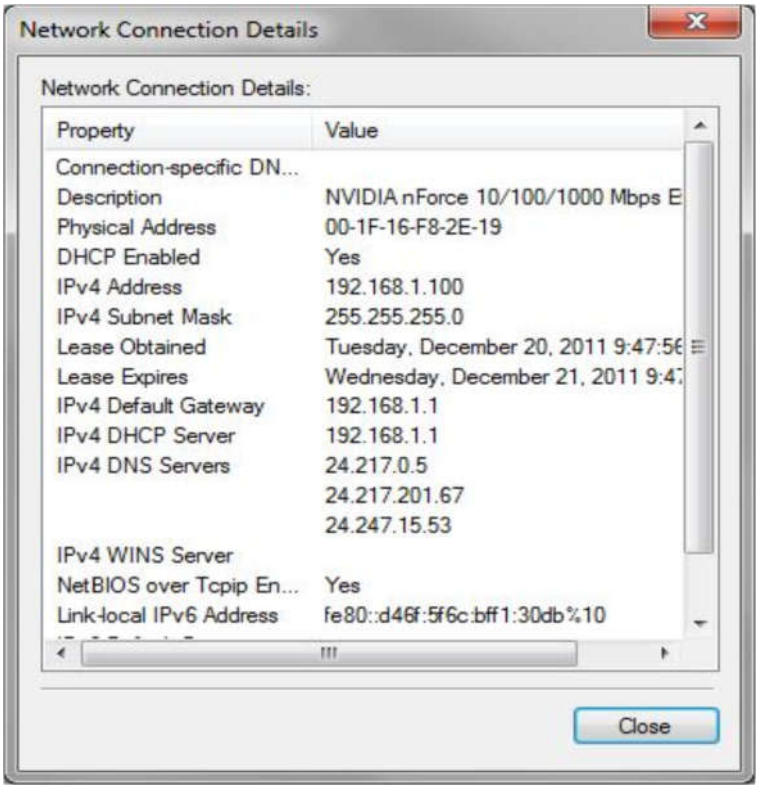


Рисунок 5.5 Параметри IP адреси

Шлюз по замочуванню *- адреса маршрутизатора або комутатора маршрутизації пакетів, на які спрямований потік, коли конкретний шлях до місця призначення не відомо.*

У цьому прикладі, IP-адреса 192.168.1.100. Маска підмережі 255.255.255.0. Значення 1 біт маски підмережі означає, що біт є частиною мережевої адреси. Значення 0 біт маски підмережі означає, що біт є частиною адреси хоста.

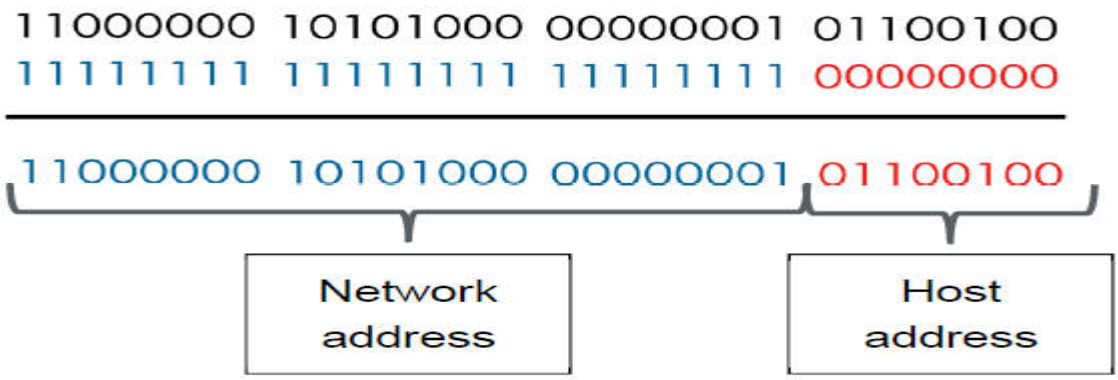


Рисунок 5.6: Адреса и маска підмережі

У цьому прикладі приведена маска підмережі за замовчуванням, яка дорівнює 255.255.255.0.

Класи адрес

Є чотири класи адрес, визначених для IPv4. Вони наведені в таблиці нижче.

Наведені значення хостів в мережі і мережевих адрес засновані на використанні маски підмережі за замовчуванням. Ви також можете використовувати маску підмережі або призначені для користувача CIDR, налаштувавши кількість бітів, виділених для мережі і адреси хоста.

Address class	First octet	Range	Default subnet mask	Available Hosts per network	Networks
Class A	01xxxxxx	0.0.0.0 to 127.255.255.255	255.0.0.0	16,777,214	128
Class B	10xxxxxx	128.0.0.0 to 191.255.255.255	255.255.0.0	65,534	16,384
Class C	110xxxxx	192.0.0.0 to 223.255.255.255	255.255.255.0	254	2,097,152
Class D (multicast)	1110xxxx	.0.0.0 to 239.255.255.255	undefined	undefined	undefined
Class E (reserved)	11110xxx	240.0.0.0 to 255.255.255.255	undefined	undefined	undefined

Особлива адреса, яка заслуговує на увагу, є TCP/IP адреса 127.0.0.1. Ця адреса використовується для пошуку та усунення несправностей місцевого TCP/IP стека.

На додаток до цих діапазонів адрес, є конкретні адреси і діапазони адрес, які зарезервовані для спеціальних цілей. Наприклад, адреса діапазону 169.254.0.0 - 169.254.255.255 зарезервовані в діапазоні APIPA. Коли хост не в змозі отримати IP-адресу від DHCP-сервера, він зазвичай буде використовувати адресу APIPA, поки проблема не буде вирішена.

Автоматичний приватний IP-адреса (APIPA) - *адреса генерується для хоста, коли він не може отримати адресу з DHCP-сервера.*

Протокол динамічної конфігурації хоста (DHCP) - *протокол, який використовується для автоматичного надання мережевих хостів з чинним IP адресою та іншою інформацією про конфігурацію.*

Публічні і приватні адреси

У кожному класі зарезервований діапазон адрес для використання в якості приватної адреси.

Приватна адреса - *діапазон адрес, відведених для використання в приватних мережах і є непридатним для використання в Інтернеті.*

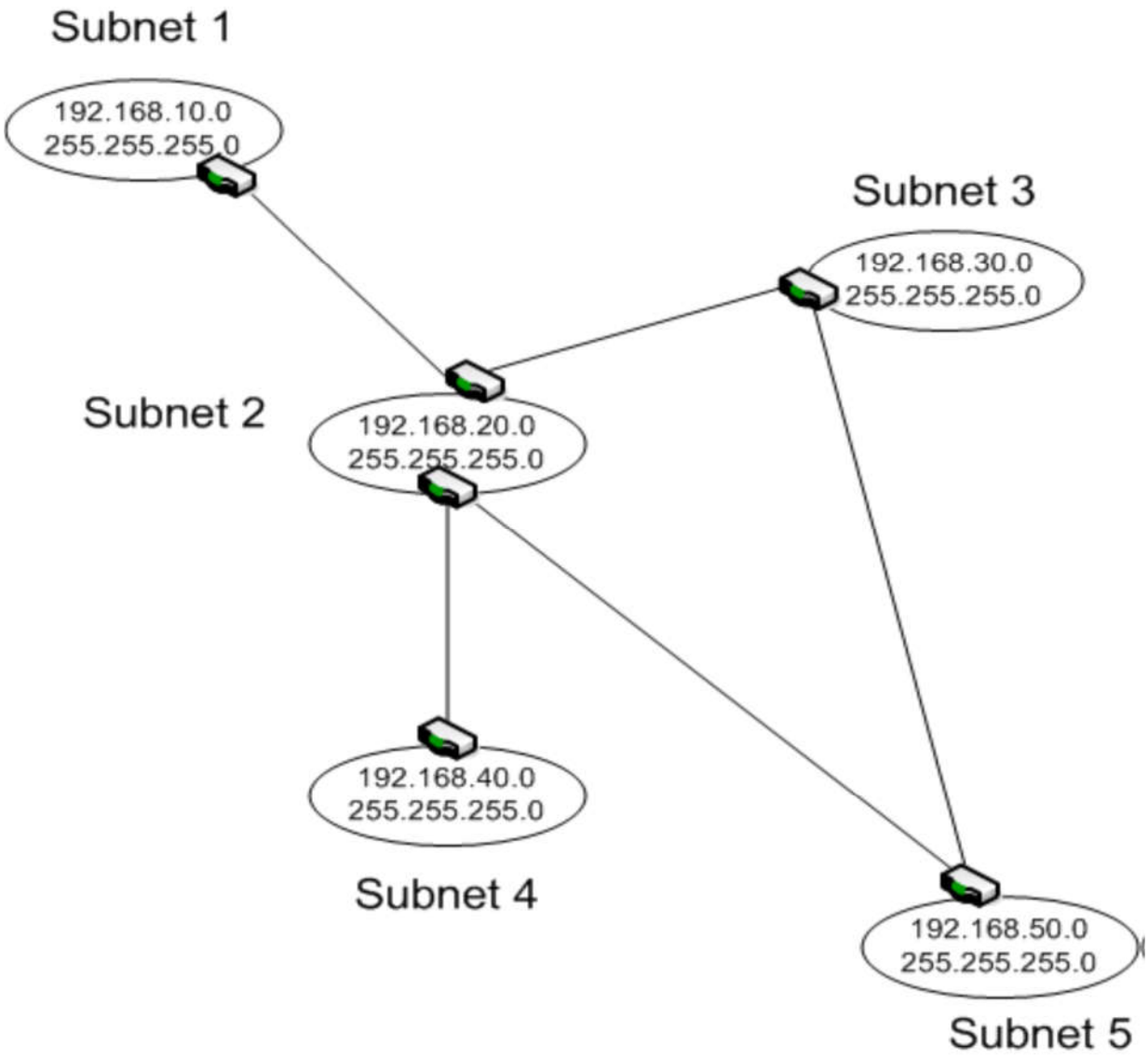
Деякі IP-адреси є публічними адресами, тому вони можуть бути використані на будь-якому з громадських мереж (Інтернет) або приватних мереж. Найчастіше, приватні мережі використовують приватні IP-адреси. Доступні приватні адреси показані в таблиці нижче.

Address class	Range
Class A	10.0.0.0 – 10.255.255.255
Class B	172.16.0.0 – 172.31.255.255
Class C	192.168.0.0 – 192.168.255.255
APIPA	169.254.0.0 – 169.254.255.255

Приватні адреси не розпізнаються в Інтернеті. Хост з приватним адресою повинен пройти через NAT пристрій для доступу в Інтернет.

Мережі і підмережі

На рисунку 5.7, кожна підмережа конфігурується адресою класу C і маскою підмережі за замовчуванням. Це означає, що в кожній підмережі, останні вісім біт IP-адреси зарезервовані для адреси хостів.



У адреси класу С за замовчуванням, є 256 хостів адрес призначення. Однак, тільки 254 з них можуть бути призначені в якості приймаючих адрес. Є два спеціальних адрес для будь-якого набору адрес вузлів:

• Всі 0

Наприклад, 192.168.40.0 з маскою підмережі 255.255.255.0 відносяться до цієї категорії. Він не може бути призначений на хості, тому що він ідентифікує мережеву адресу.

• Всі 1

Прикладом може бути 192.168.40.255 з маскою підмережі 255.255.255.0. Він використовується, щоб вказати адресу призначення для широкомовної передачі. Заповнення адреса хоста з усіма 1 фактично означає, що всі вузли в цій підмережі є дійсними адресами призначення.

За замовчуванням мережеві адреси також можна записати, використовуючи формат CIDR. Для прикладу, ви можете побачити:

Це означає, що перші 24 біта маски підмережі встановлені в "1". Якщо ми перетворимо маску підмережі 255.255.255.0 в двійковий, ми отримуємо наступне: (Рисунок 5.9):

Як ви можете бачити, ці записи еквівалентні. У будь-якому випадку, перші 24 біта маски підмережі встановлені на "1", і перші 24 біта визначають мережеву адресу.

Маска підмережі

Ви можете використовувати підмережі, щоб розділити адреса на додаткові адреси мережі з меншою кількістю хостів в адресі мережі. Ви можете зробити це шляхом зміни біт в масці підмережі на 1, починаючи з самого значного 0 біт.

Найбільший значущий біт - самий лівий біт, що представляє максимальну ступінь 2.

Щоб побачити, як ця зміна може бути зроблено, ми почнемо з наступної мережевої адреси з маскою підмережі (Рисунок 5.10).

Перші два біта останнього октету тепер встановлені в 1. Ця зміна дає два додаткових біти для визначення мережевої адреси або чотири значення адреси:

- 00000000 (0)
- 01000000 (64)
- 10000000 (128)
- 11000000 (192)

Ця послідовність чисел також залишає 6 біт для адрес хоста, що дозволяє визначити 64 унікальних адрес хостів або 62 реальних адрес (64 мін все 0 і все 1). Таблиця перераховує мережеві адреси, а також доступні та асоційовані адреси хостів.

Network address	Host address range
192.168.40.0	192.168.40.1 – 192.168.40.62
192.168.40.64	192.168.40.65 – 192.168.40.126
192.168.40.128	192.168.40.129 – 192.168.40.190
192.168.40.192	192.168.40.193 – 192.168.40.254

Ці адреси можуть бути опубліковані з використанням традиційного позначення, або з використанням CIDR позначення. Наприклад, мережева адреса може бути записана наступним чином:

Network 192.168.40.64 with a subnet mask of 255.255.255.192.

Крім того, теж саме можна записати в іншому вигляді, з використанням CIDR:

Network 192.168.40.64/26.

Можна використати ці адреси для створення мереж з використанням маршрутизатора, де кожна підмережа є підмережою відповідної адреси з маскою підмережі по замовчуванню (Рисунок 5.11).

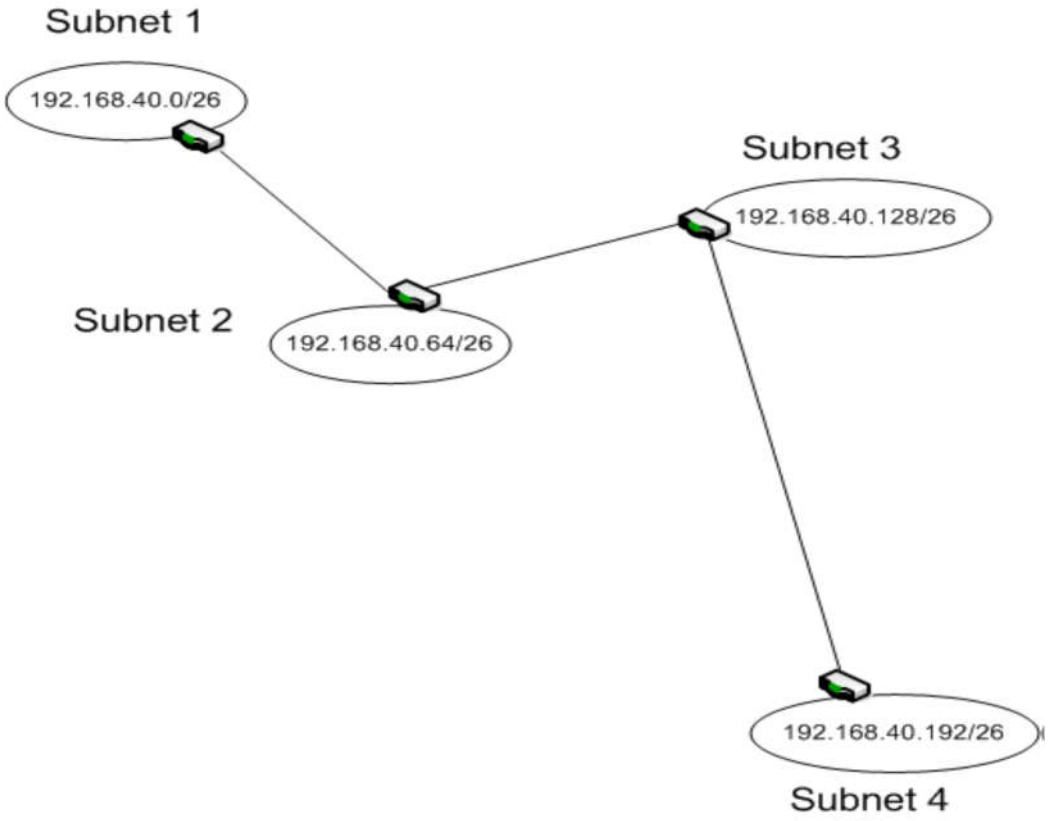


Рисунок 5.11

Якщо вам потрібно більше підмереж з однієї мережі за замовчуванням, ви повинні додати більше бітів до маски підмережі.

Наприклад, ви можете мати маску підмережі 255.255.255.240. Десяткове значення 240 дорівнює двійковому 11110000. Це означає, що у вас є чотири біти для мережних адрес і чотири для адрес вузла. Це дає вам 16 доступних мережних адрес, але лише 14 адрес на мережу, які можуть бути призначені для хостів.

Інші класи адрес можна розбити так само. Візьміть клас B 172.31.0.0, який має маску підмережі за замовчанням 255.255.0.0. Тепер припустимо, що ми змінюємо маску підмережі на 255.255.128.0, змінюючи найважливіший біт третього октету на 1. Ми розділили адресу на дві мережі (172.31.0.0 та 172.31.128.0), до 32.766 хостів (15 біт адреси хоста) кожна. З іншого боку, одна і та ж IP-адреса з маскою підмережі 255.255.255.252 дає до 16,384 мереж з одним або двома хостами в мережі.

Змінна довжина маски підмережі

Процес підмережі може стати більш складним при використанні масок підмережі змінної довжини. У кожній підмережі не потрібно використовувати одну маску підмережі одного розміру (Рисунок 5-12). Тим не менш, ви повинні переконатися, що ви не викликаєте будь-які помилки, наприклад, дублікати адрес або нерозв'язних маршрутів.

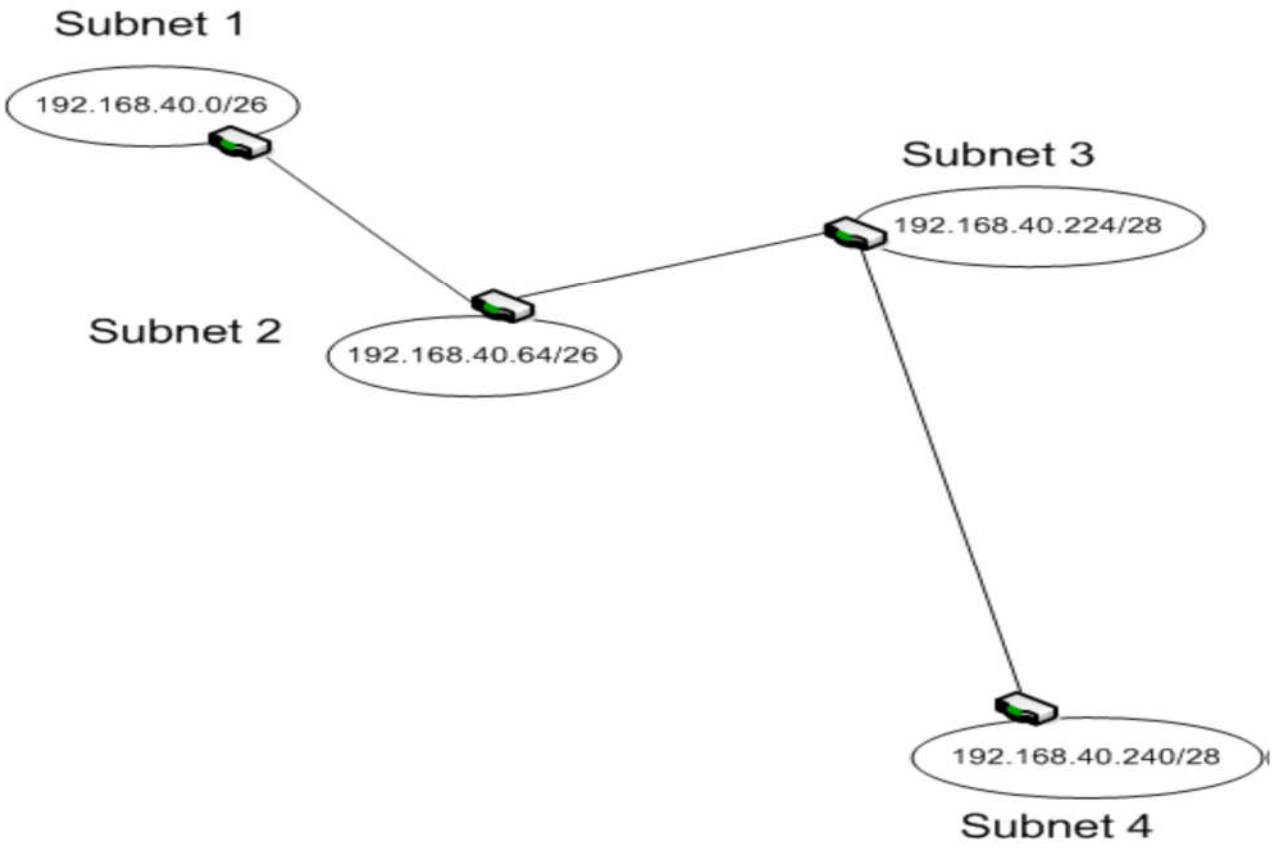


Рисунок 5.12 Змінна довжина маски підмережі

На Рисунку 5.12 дві підмережі мають маску підмережі 255.255.255.192, яка підтримує чотири мережі з 62 вузлами в мережі. Ви також маєте дві підмережі з маскою підмережі 255.255.255.240, що підтримують до 16 мереж і до 14 хостів у кожній мережі.

Однак, якщо ви не обережні, ви можете закінчити з перекриттям мереж (Рисунок 5-13), що може викликати проблеми.

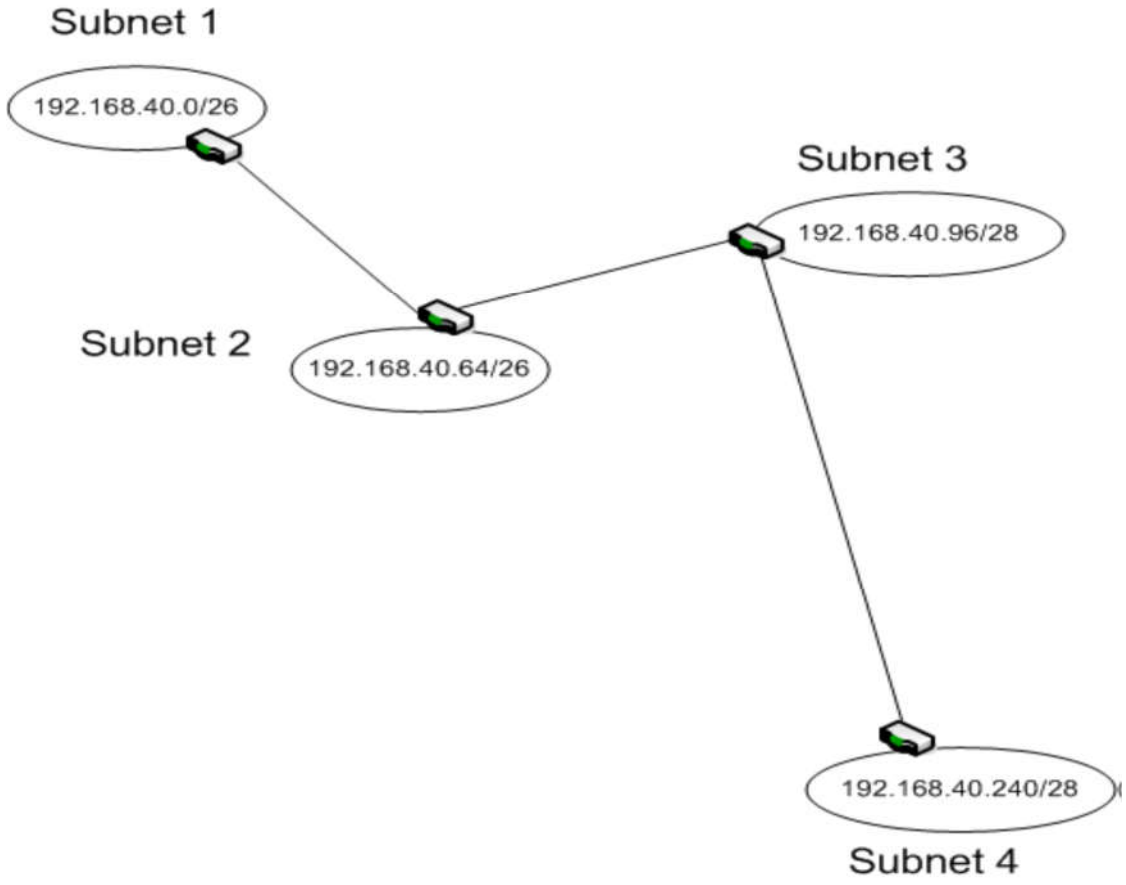


Рисунок 5.13 Помилка підмережі

На перший погляд цей приклад виглядає дуже схожим на попередній приклад. Проблема тут полягає в тому, що адреса мережі і адреси вузла є частиною області адреси, визначеної в підмережі 2.

Підмережа 2 підтримує діапазон адрес 192.168.40.65 -192.168.40.126
Підтримка мережі 3 і діапазон адрес 192.168.40.97 -192.168.40.110

Діапазон адрес підмережі 3 є частиною діапазону адрес підмережі 2. Це може привести до появи хостів з однаковими адресами IP, тобто з недозволеним станом. Це також може привести до неоднозначних напрямками маршрутизації через схожість в мережевих адресах.

Це дублювання можна побачити, коли ви пишете останній октет кожного з мережевих адрес в двійковому вигляді:

Перші два біта двійкового числа для десяткового числа 96 рівні 0 і 1, так само, як і для десяткового числа 64. Вони можуть бути інтерпретовані як дублікати мережевих адрес.

CIDR

CIDR був розроблений для забезпечення більш гнучкої системи розподілу адрес вузла, ніж це дозволено оригінальним методом IP-адреси та підмережі.

CIDR може використовуватися для документування традиційних підмереж, як і приклади, що розглядалися раніше в цьому розділі, а також для агрегування мережевих адрес в єдиний блок (процес, що спочатку називався supernetting). Це було використано для об'єднання адрес класу C для створення більшого адресного простору.

Частина мережевої адреси IP-адреси, коли використовується CIDR, часто називають мережевим префіксом. Наприклад, з мережевою адресою 192.168.22.0/24 перші три октету є префіксом мережі. Числом після діагональної косої риси є кількість бітів в префіксі мережі. Це також число бітів в адресі мережі.

Щоб побачити, як CIDR можна використовувати для створення агрегованих адрес, розглянемо наступний приклад (Рисунок 5-15). Маска підмережі має 23 біта, 8 бітів у перших двох октетах і 7 найбільш значущих бітів третього октету. Це залишає 9 бітів для адрес хоста.

Цей адресний блок CIDR буде включати в себе мережі класу C 192.168.6.0 і 192.168.7.0. Повний діапазон підтримуваних адрес хоста становить з 192.168.6.1 до 192.168.7.254.

Ось ще один приклад, цього разу з двійковими значеннями, які можуть зробити це трохи легше для розуміння. Розгляньте наступну адресу CIDR:

192.168.172.0/22

На цей раз є 22 біти мережевої адреси і 10 біт адреси хоста. Це надає йому діапазон адрес вузла з 192.168.172.1 до 192.168.175.254.

У цьому прикладі блок адреси CIDR містить адреси класу C з 192.168.172.0 до 192.168.175.0 як один суміжний блок.

Багатоадресна розсилка Рівня 3

Ви мали короткий вступ до багатоадресної передачі раніше. Перші чотири біти IP-адреси визначають адресу багатоадресної передачі. У нотації CIDR адреси групової розсилки є частиною підмережі 224.0.0.0/24. Всі члени групи багатоадресної розсилки матимуть однакову адресу групової розсилки. Хост може належати декільком групам багатоадресної передачі.

Для адресації вузлів в основному використовуються два діапазони адрес. Адреси для використання під час багатоадресної передачі в підмережі є частиною 244.0.0.0/24 з діапазоном адрес від 224.0.0.0 до 224.0.0.255. Оскільки пункти призначення, за визначенням, є частиною локальної підмережі, маршрутизатори не будуть пересилати пакети з підмережі.

Інший діапазон груп багатоадресної передачі призначений для багатоадресної передачі в глобальному масштабі адреси. Підтримуваний діапазон адрес становить з 224.0.1.0 до 238.255.255.255.

Припустимо, що ви налаштовуєте групу багатоадресної передачі з груповою адресою 224.100.100.5. Незалежно від того, де вони фізично розташовані, кожен хост, який є членом цієї групи, буде налаштований на туж саму адресу. Пакети багатоадресної передачі, адресовані 224.100.100.5, будуть перенаправлені на відповідний вузол незалежно від того, де вони знаходяться (принаймні в теорії)

Налаштування адрес клієнта

Можна налаштувати автоматичну підтримку адрес за допомогою DHCP, статичних адрес або обох. При налаштуванні областей DHCP потрібно ретельно зрівняти їх з адресами підмережі. Більшість серверів DHCP можуть підтримувати традиційні підмережі класів або CIDR.

Конфігурація клієнта спрощується при використанні DHCP. Фактично, DHCP є стандартною конфігурацією для більшості комп'ютерів Windows (Риунок 5.17). Хост намагатиметься знайти DHCP-сервер і орендувати IP-адресу.

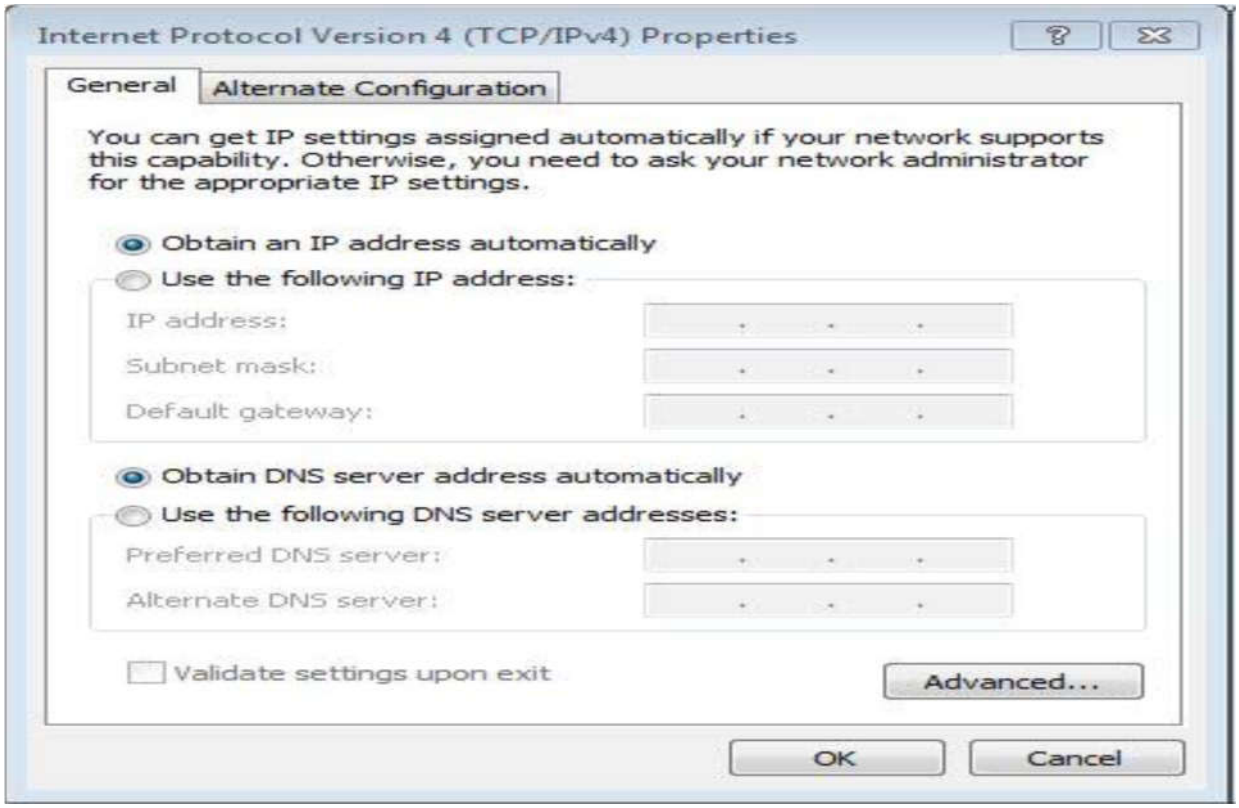


Рисунок 5.17

Вкладка "Альтернативна конфігурація" (Рисунок 5.18) визначає, як налаштовується адреса хоста, якщо він не може знайти DHCP-сервер або якщо немає доступних адрес.

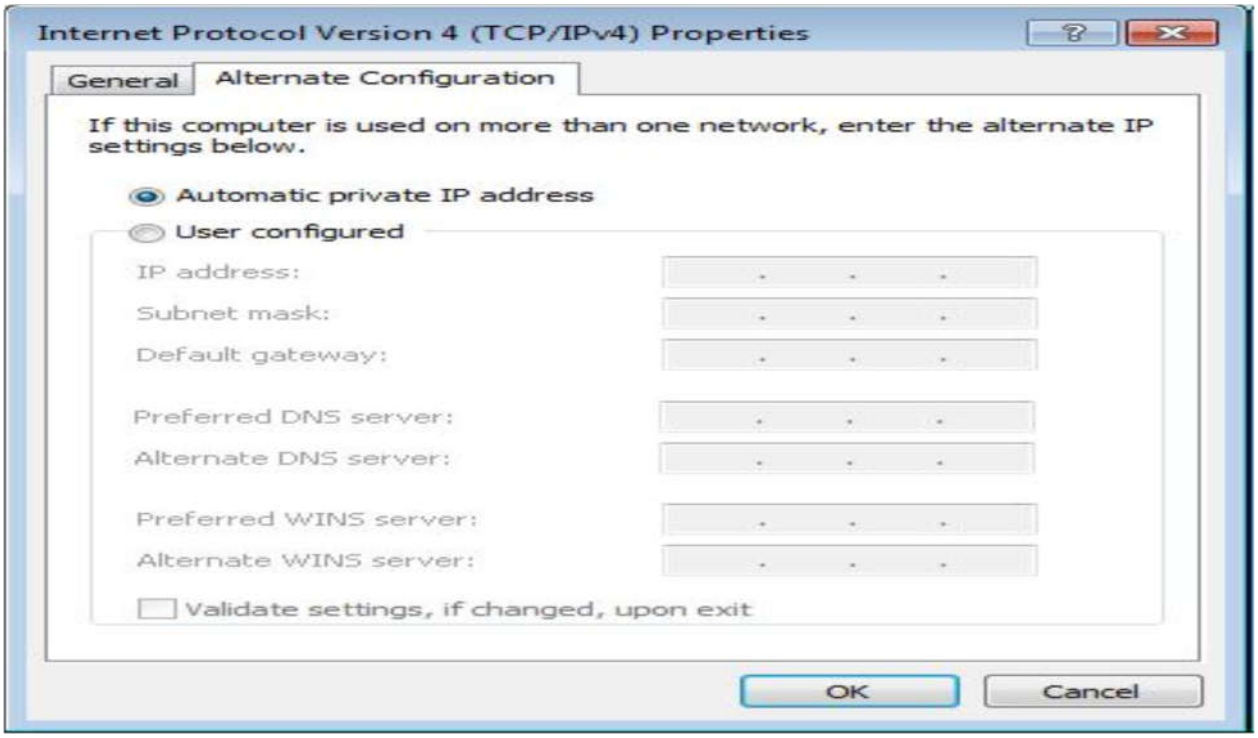


Рисунок 5.18

Якщо не вказано інший параметр, автоматично генеруються адреса APIPA. У вас є можливість налаштування також статичних параметрів адреси.

При використанні статичних IP-адрес необхідно передбачити інформацію про адресу хоста (Рисунок 5.19).

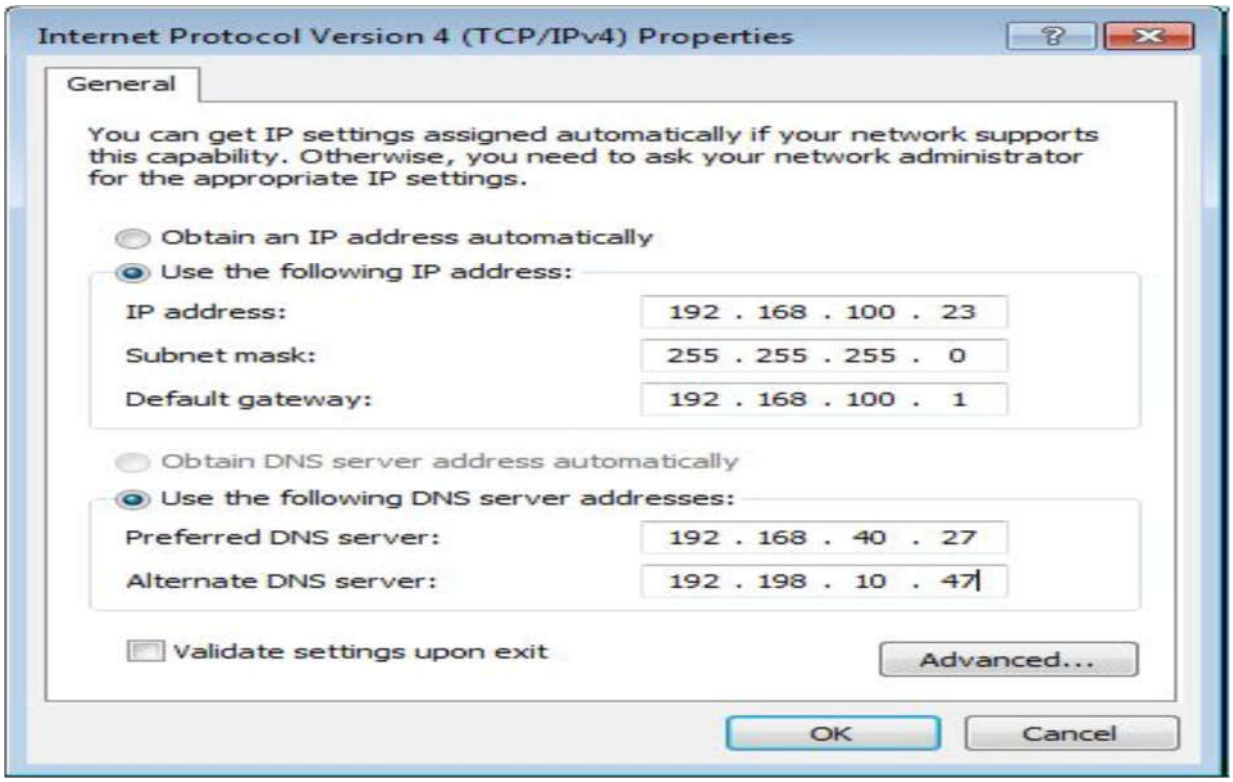


Рисунок 5.19

Як мінімум, необхідно вказати IP-адресу, маску підмережі та шлюз по замовчуванням. Якщо шлюз за промовчанням не включений, хост буде обмежено тільки для передачі даних у локальній підмережі. Крім того, якщо ви використовуєте DNS, ви повинні налаштувати адресу бажаного DNS-сервера. Якщо доступний другий DNS-сервер, налаштуйте його як альтернативний DNS-сервер.

Протоколи IPv4

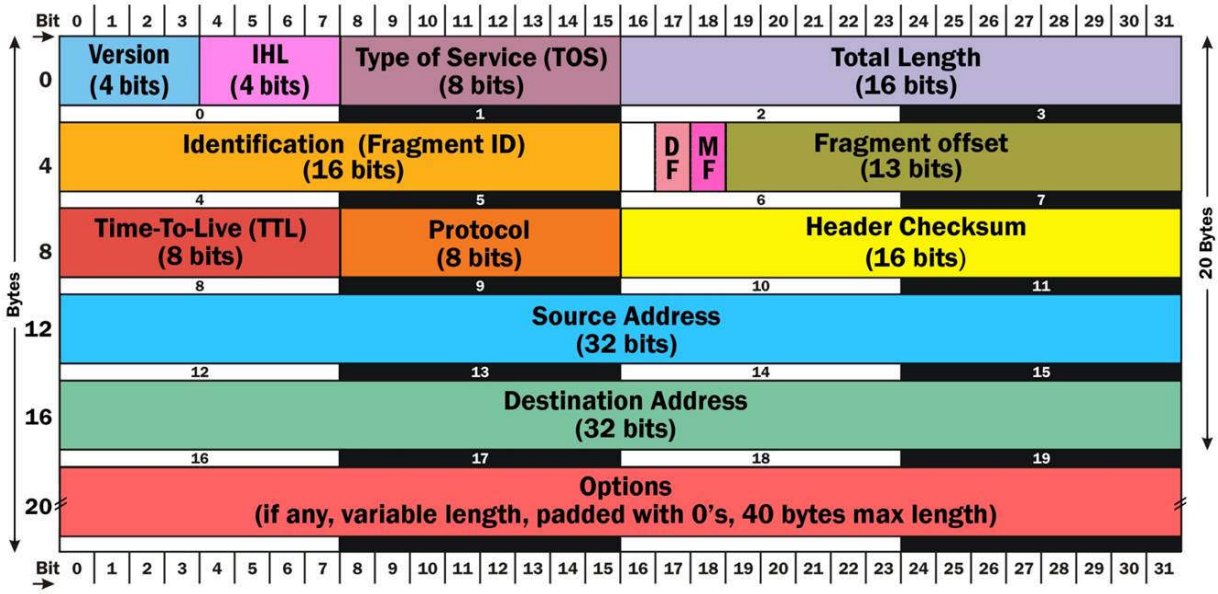
Є чотири протоколи, які визначені в якості компонентів IPv4:

- Інтернет-протоколи (IP, або IPv4)
- Протокол співставлення адрес (ARP)
- Протокол керуючих повідомлень Internet (ICMP)
- Протокол управління групами Internet (IGMP)

Кожен з цих протоколів грає важливу роль у вашій мережі TCP/IP.

IPv4

IPv4 - цей протокол відповідає за обмін даними. Він відповідає за адресацію і маршрутизацію пакетів. Це протокол без встановлення з'єднання, так що не встановлюється з'єднання між вихідним і кінцевим хостами. Це робить все можливе при доставці, але не гарантує доставку. IPv4 форматує дані у вигляді пакетів. Заголовок пакета містить інформацію, необхідну для маршрутизації пакета і збору фрагментованих пакетів. Заголовок включає в себе:



• IP-адреса джерела - хост, який ініціював пакет.

• IP-адреса призначення - хост, який отримує пакет.

• Ідентифікатор - значення використовується для ідентифікації фрагментованих пакетів (тільки якщо фрагментований).

• Протокол - протокол верхнього рівня (TCP або UDP), яким передається пакет після отримання.

• Час-Live (TTL) - кількість мережевих сегментів, які може пройти пакет, перш ніж він відкидається.

IPv4 не предусматривает восстановления ошибок. Вместо этого, восстановление после ошибки осуществляется транспортном уровне применения модели TCP/IP.

ARP

MAC-адреси хоста використовуються в остаточній доставці пакета. Проте, пакети адресуються IP адресою хоста призначення, а не його MAC-адресою. У цей момент, ARP стає залученим в процес. ARP використовується для співсиавлення IPv4 і MAC адрес. Хости кешують локальний MAC-адрес в

кеші ARP. Кешування адреси допомагає зменшити обсяг трафіку, що генерується при передачі ARP, використовуваних в процесі співсиавлення адреси. Кешування адреси створює динамічні записи кеша. Більшість реалізацій TCP/IP дозволяють також вручну помістити статичні записи кеша в кеш ARP.

ICMP

IPv4 сам по собі, не повідомляє про помилки. Замість цього, ця функціональність забезпечується через Internet Control Message протоколу (ICMP). ICMP використовується при усуненні неполадок, звітності помилки, і вирішення помилок. Утиліта для «пінг», наприклад, використовує повідомлення ICMP Echo, щоб перевірити зв'язок з віддаленим хостом. Якщо маршрутизатор не може доставити пакет в відповідний пункт призначення, він згенерує повідомлення «Місце призначення недоступно» назад на вихідний хост.

Повідомлення	**Використання**
Echo	Використовується для перевірки підключення між хостами.
Echo Reply	Надсилається у відповідь на отримане ехо-повідомлення.
Redirect	Надсилаються на відправляючі хости для визначення кращих маршрутів до пунктів призначення.
Source Quench	Надсилаються на відправляючі хости, щоб повідомити, що пакети скидаються на маршрутизатор через перевантаження.
Destination Undeliverable	Надсилаються на відправляючі хости, коли пакет не може бути доставлений до місця призначення.

Мережеві адміністратори іноді відключають здатність маршрутизатора, щоб відповісти на повідомлення Echo. Відключення відповіді на здатність маршрутизатора відповідати на повідомлення відлуння допомагає запобігти потенційного зловмисника відображення мережі.

ICMP також може бути використаний в нападі на мережі. ICMP пакети надсилаються в мережі в усталеному повені і пригнічують пристрою призначення.

IGMP

Інтернет протокол управління групами (IGMP) використовується при багатоадресній передачі. Як ви пам'ятаєте, в багатоадресній передачі, одне джерело посилає ті ж пакети на декілька хостів призначення. Це допомагає зменшити трафік, що генерується деякої високою пропускною спроможністю додатків, таких як потокове відео на кілька хостів.

IGMP використовується для управління групами багато адресної розсилки, які також називаються групами хостів. IGMP - це протокол, який використовується для реєстрації членства в групі хостів, щоб хост міг приймати багатоадресні передачі IPv4.

• Хости використовують IGMP для оголошення членства в певній групі многоадресной передачі.
• Хости використовують IGMP для оголошення, коли вони залишають групу многоадресной передачі.
• Маршрутизатор використовують протокол IGMP для опитування підмереж для отримання інформації про членів групи.

Маршрутизатор повинен підтримувати багатоадресну пересилання, щоб він міг визначити, як і куди пересилати багатоадресні розсилки.

IPv6

IPv6 - це можлива заміна IPv4 в Інтернеті. Однак перехід на IPv6 буде повільним, і IPv4 все ще буде використовуватися в майбутньому.

Оскільки адреси мережі і хоста завжди окреслюються на одному кордоні в IPv6, маски підмереж з адресами IPv6 не потрібні. Перші 64 біта завжди представляють мережеву адресу. Початкове значення також вказує тип адреси, наприклад локальний, маршрутизації або багатоадресний адреса.

Протокол IPv6

IPv6 надає всі функціональні можливості, підтримувані IPv4. Як і в разі IPv4, це виконується за допомогою набору протоколів, що складають IPv6.

- Internet Protocol (IPv6)
- Internet Control Message Protocol for IPv6 (ICMPv6)
- Neighbor Discovery (ND)
- Multicast Listener Discovery (MLD)

окладне обговорення IPv6 і його складових протоколів виходить за рамки даного курсу. Однак, ми швидко переглядаємо кожен протокол, так що ви, по крайней мере знайомі з їхньою метою.

IPv6

IPv6 виконує ту ж роль, що і IPv4, як протокол без встановлення з'єднання, що відповідає за адресацію і маршрутизацію пакетів між вузлами. Протокол IPv6 продовжує залишатися ненадійним протоколом, а надійність

забезпечується за допомогою протоколів, реалізованих на більш високих рівнях.

Вузол - *адресується об'єкт в мережі. Термін вузол часто використовується як спосіб для позначення хостів і маршрутизаторів, коли обидва підтримуються тією ж функціональністю.*

Pv4 і IPv6 відрізняються тим, що вони працюють по-різному. Одна з відмінностей є те, що в IPv6 фрагментація може відбуватися тільки на передавальному вузлі. Якщо пакет занадто великий для низхідного маршрутизатора, то інформація, як повідомляється, що відправляє хоста, може бути фрагментована.

ICMPv6

CMPv6 бере на себе роль ICMP в IPv4. Як з IPv4, IPv6, не забезпечує свою власну звітність про помилку. Замість цього він покладається на ICMPv6. Основна відмінність між ICMP і ICMPv6, що ICMPv6 підтримує додаткові повідомлення, які не підтримуються ICMP. Один з цих нових повідомлень є занадто великий пакет повідомлення, яке використовується для інформування хоста, щоб фрагментувати пакет перед відправкою. Ці нові повідомлення включають в себе повідомлення, що підтримують протоколи ND і MLD.

ND

ND занимает место ARP в IPv6 и обладает дополнительной функциональностью, которой нет у ARP. Функциональность, предоставляемая ND, зависит от того, является ли узел хостом или маршрутизатором. Вот обзор этой функциональности:

- Для всіх вузлів
  - Виконує перетворення адрес канального рівня
  - Оголошує зміни в канальному рівні, адресу вузла
  - Визначає, чи є відомий сусід, і чи є він як і раніше досягнутим
- Тільки для хостів
  - Виявляє сусідні маршрутизатори
  - Виявляє і налаштовує адресу та інші параметри
- Тільки для маршрутизаторів
  - Оголошує присутність в мережі, адресу та інші параметри
  - Повідомляє господарів більш адрес для пересилання пакетів

MLD

MLD IGMP забезпечує функціональність для IPv6. Основна відмінність між MLD і IGMP, що MLD не має свою власну структуру повідомлення. Замість цього,

MLD використовує повідомлення ICMPv6 для того, щоб маршрутизатори виявили будь-які місцеві багатоадресні вузли прослуховування для багатоадресної передачі. Повідомлення MLD описуються в таблиці нижче.

Повідомлення	**Джерело**	**Опис**
Multicast Listener . Query	Router	Запитує підмережу, щоб виявити слухачів багатоадресної розсилки
Multicast Listener Report	Host (Multicast Listener)	Надсилає у відповідь на запит Multicast Listener або на повідомлення про інтерес до прийому багатоадресного трафіку, адресованого конкретному хосту
Multicast Listener Done	Host (Multicast Listener)	Повідомляє, що слухач може бути останнім членом групи багатоадресної передачі в локальній підмережі.

Протокол динамічної конфігурації хоста (DHCP)

У той час як ми працюємо на рівні інтернету, необхідно витратити трохи часу на розмови про DHCP. У той час, як можна управляти IP-адресою за допомогою налаштування статичної адреси на кожному NIC, більшість мереж призначені для використання автоматичного призначення адрес.

Адреси надаються DHCP-сервером, налаштованим в даній адресній області. Коли хост, що потребує адресу приходить в Інтернет, він намагається знайти DHCP-сервер з доступною адресою. Замість того, щоб отримувати адресу в якості постійного призначення, хост отримує оренду на адресу, яка закінчується після певного періоду часу.

Призначення адреси відбувається через серію передач. Процес починається з DHCP клієнта, який відправляє повідомлення DHCP Discover (Рисунок 5.20). Це повідомлення надсилається в ефір, так що клієнт може спробувати знайти DHCP-сервер в мережі. На відміну від більшості інших передач, маршрутизатори можуть бути налаштовані для передачі повідомлень DHCP виявлення.

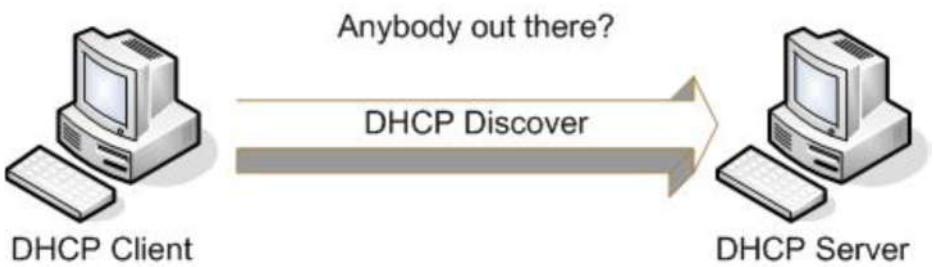


Рисунок 5.20

Будь-сервер DHCP з дійсним набором адрес відповідає повідомленням DHCP-пропозиція (Рисунок 5.21). Повідомлення включає в себе інформацію про адресу IP і може включати в себе інші параметри конфігурації.

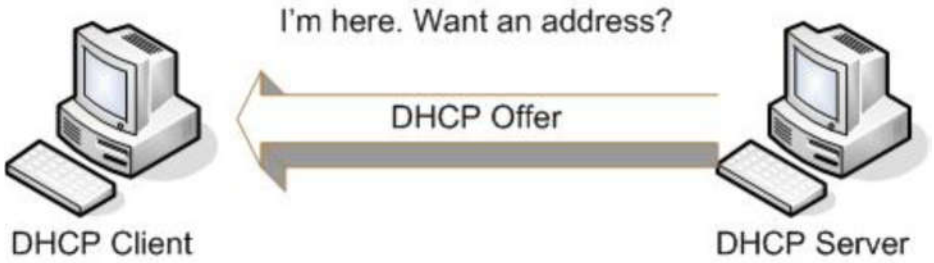


Рисунок 5-21

Клієнт вибирає пропозицію з наявних, але не налаштовує себе з цією інформацією. Замість цього, він посилає повідомлення DHCP-запит (Рисунок 5.22). Це повідомляє DHCP-сервер, який відправив пропозицію, що пропозиція була прийнята. Він також перевіряє, що адреса ще не прийнято іншим хостом і раніше доступний.

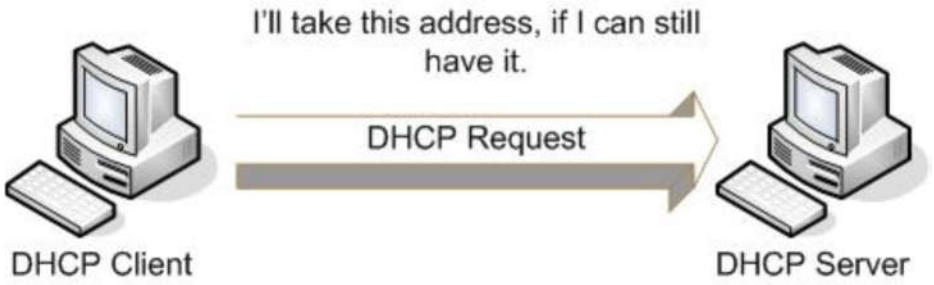


Рисунок 5.22

Якщо припустити, що адреса як і раніше доступна, DHCP-сервер посилає повідомлення DHCP ACK (Рисунок 5.23). Це підтверджує IP-адресу оренди. Тепер клієнт буде налаштовувати себе з цією інформацією.

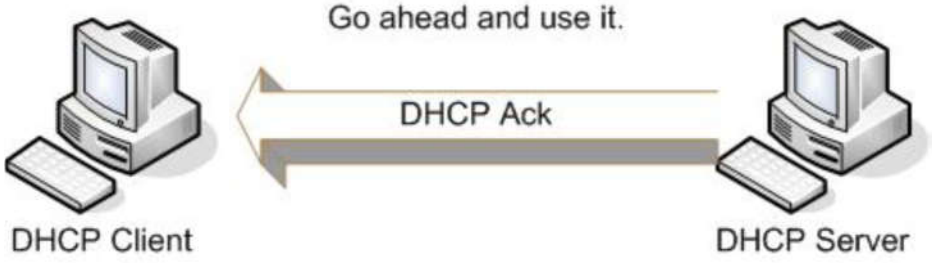


Рисунок 5.23

На додаток до IP-адресами, DHCP-сервер може також призначити адреси багато адресної розсилки. Один сервер DHCP може бути налаштований з декількома областями, що дозволяє йому забезпечити адреси та відомості про конфігурацію для вузлів на декількох підмереж.

Транспортний рівень

Транспортний рівень відповідає за сеанс і послуги дейтаграм, функціональність, що надається рівнями транспорту та сеансу в моделі OSI. Транспортний рівень може підготувати датаграми для передачі без встановлення з'єднання або з встановленням з'єднання.

На транспортному рівні визначені два протоколи. TCP - це протокол, орієнтований на встановлення з'єднання, який встановлює сеанс зв'язку між відправником і отримувачем. UDP - це протокол без встановлення з'єднання, який відправляє дані тільки в надії, що вони будуть отримані. TCP і UDP можуть передавати дейтаграми в IPv4 і IPv6 у відповідний час.

TCP

TCP відповідає за надійний зв'язок. Комунікації встановлюється як сеанс один-до-одного між двома хостами. TCP несе особливу відповідальність за:

Встановлення з'єднання між двома хостами;.

Послідовність і підтвердження пакетів;

Повторна відправка пакетів у відповідь на помилки.

Перш ніж два хоста зможуть передавати дані, вони повинні спочатку встановити з'єднання. Відправник і одержувач будуть передавати дані через серію сегментів рукопотискання. Сегменти рукопотискання встановлюють сеанс, а потім завершують сеанс.

Передача інформації

Термін сегмент використовується для позначення даних, переданих через TCP/IP. Кожен сегмент матиме номер сегмента, який використовується для ідентифікації сегмента, а також для відстеження та його визнання. Після того, як хост посилає пакет, він буде очікувати заданий час для підтвердження. Якщо підтвердження не отримане протягом цього часу, хост, який посилає пакет, буде повторно посилати пакет.

- *Підтвердження відправляється тільки після успішного отримання пакету даних. Якщо пакет не отримано, або якщо він містить будь-які помилки, підтвердження не відправляється.*

ли додаток передає дані TCP, воно повинно включати в себе IP-адреса призначення і порт призначення. Заголовок TCP пакету включає в себе як порт джерела, так і порт призначення інформації. Він також матиме порядковий номер і номер підтвердження. Обидва з них використовуються, щоб перевірити порядок даних для складання та запобігання втрати даних.

Порт - *16-бітове число, яке використовується для ідентифікації кінцевої точки зв'язку для отриманих даних. Порти використовуються як з TCP і UDP.*

Номер послідовності - *Номер першого байта в поточному сегменті даних.*

Номер підтвердження - *Номер наступного байта, який відправник очікує для одержання від свого партнера.*

UDP

UDP може використовуватися для зв'язку один-до-одного або один-до-багатьох. UDP не має з'єднання, тому він не встановлює сеанс зв'язку між відправником і отримувачем. Оскільки він не має відношення до управління сеансом, або послідовністю пакетів, або навіть успішної доставкою, накладні витрати на обробку і необхідна пропускна здатність мережі менше для трафіку UDP.

Передача інформації

Пакети даних, відправлені UDP, називаються повідомленнями. Вони включають в себе заголовок UDP і частину даних, також відому як повідомлення. Оскільки передача даних не підтверджується і не відстежується, заголовок пакета UDP включає:

• Порт джерела;
• Порт призначення;
• Контроль.

Він не включає в себе інформацію про послідовність. Значення контрольної суми використовується приймаючим комп'ютером, щоб переконатися, що дані не були пошкоджені під час передачі. Якщо виявлена помилка, то пакет просто відкидається і ігнорується.

Прикладний рівень

Прикладний рівень реалізує функціональність на рівні сеансів OSI, презентації та додатків. Він діє як інтерфейс між користувачами (і додатками) і мережевими сервісами. Він включає в себе велику кількість прикладних протоколів і сервісів прикладного рівня причому нові функціональні можливості визначаються на досить регулярній основі.

Протоколи прикладного рівня

Ми представляємо деякі з найвідоміших і найбільш часто використовуваних протоколів в цьому розділі, але ці списки протоколів ніде поруч не повні. Більшість протоколів, представлених тут, будуть обговорюватися більш докладно пізніше в

процесі. Є також деякі спеціалізовані протоколи, які ми не вирішуватиме пізніше, в ході, щоб уникнути плутанини.

Ви можете приблизно організувати протоколи додатків і служби рівня додатків в залежності від того, що вони роблять. Ці категорії включають:

Name system;
File transfer;
World Wide Web;
Email;
Management protocols.

Name system

Протокол DNS є важливою частиною практичної мережі. Він дозволяє імена комп'ютерів (наприклад www.hp.com) і IP-адреси. Хоча докладне обговорення DNS виходить за рамки даного курсу, важливо зрозуміти, що це таке і що він робить.

Система доменних імен (DNS) - *Система для підтримки бази даних імен пристроїв і виконання імені/IP адреси резолюції.*

Уявіть собі, якою помилкою було б, якщо кожен раз, коли ви намагалися отримати доступ до іншого мережевого комп'ютера або переглянути розташування в Інтернеті, вам потрібно поставити його IP-адресу. Замість цього, символічні імена дозволяють легко ідентифікувати або визнавати комп'ютер. DNS-визначається в RFCs, який встановлює стандарти Інтернету. Це ім'я системи, що використовується в Інтернеті і в більшості інших мереж.

DNS - це ієрархічна система імені. Імена комп'ютерів, як правило, складаються з трьох частин, але вони можуть мати і більш. Розглянемо приклад на Рисунку 5-24. Це відомо як повне доменне ім'я, або FQDN.

"Com" часть имени является именем домена верхнего уровня. Это имя может быть именем трех символов идентификации организационного типа или названием стран из двух букв.

Домен второго уровня, "HP" в данном случае, используется для идентификации уникальной организации.

Третий и более высокие уровни используются для идентификации отдельных устройств.

Второй и верхний уровень имен вместе, такие как hp.com, как правило, называют в качестве доменного имени. Имя должно быть зарегистрировано с организацией стандартов интернета, прежде чем он может быть использован в Интернете, чтобы идентифицировать устройства. Доменные имена верхнего уровня поддерживаются органом Internet Assigned Numbers (IANA). Второй уровень регистрации доменного имени отводится местным органам власти, которые отчитываются перед IANA.

Internet Assigned Numbers Authority (IANA) *– Организация интернет стандартов, ответственная за номер порта и имя домена регистраций.*

Бази даних об'єднань імені та IP-адрес підтримують на серверах імен, як правило, називають DNS-сервера.

Про сервер імен DNS

Сеть с помощью DNS для имен компьютеров, как правило, имеют один или несколько серверов DNS местных. DNS-сервера в Интернете предоставляют информацию о доступных публичных компьютерах. Большинство провайдеров поддерживают несколько серверов DNS, которые могут получить доступ к серверам высшего уровня с помощью в течение Интернет иерархии.

Интернет-провайдер (ISP) - *Компанія, яка надає іншим організаціям і приватним особам доступ до мережі Інтерне.*

У базі даних ім'я сервера містить записи ресурсів. Загальні ресурсні записи перераховані в таблиці нижче.

Resource record	Description
A	Associates a FQDN with an IPv4 address.
AAAA	Associates a FQDN with an IPv6 address.
NS	Indicates the computer is acting as a name server.
PTR	Maps an IP address to a FQDN for looking up a name based on IP address (reverse lookup).

CNAME	Specifies an alias for a device registered under a different FQDN.
MX	Identifies a computer acting as a mail server.
SRV	Indicates that the computer is providing a service to the network.

Кожен вузол буде мати, як мінімум, запис A. Якщо вузол підтримує IPv6, він також буде із записом AAAA. Інші записи будуть залежати від ролі комп'ютера в мережі.

File transfer protocols

Три найбільш поширених протоколу передачі файлів є: FTP, TFTP і SFTP.

Протокол передачі файлів (FTP) - *Чистий спосіб передачі текстового файлу.*

Найпростіший протокол передачі файлів (TFTP) - *Чистий метод текстового файлу передачі, використовується в основному з передачею дуже маленьких файлів.*

Безпечний протокол передачі файлів (SFTP) - *Зашифрований метод передачі даних.*

FTP

FTP використовується для копіювання файлів між комп'ютерами. Передача файлів здійснюється у вигляді звичайного тексту. Порт 20 використовується для повідомлень управління FTP і порт 21 використовується для фактичної передачі даних. FTP-сервер може або вимагати від клієнта FTP, щоб увійти перед передачею де може мати місце, або сервер може бути налаштований для анонімної передачі файлів.

Підтримуються три режими передачі файлів:

• режим ASCII;

• режим EBCDIC;

• Бінарний режим (зображення).

ASCII і EBCDIC передають дані в вигляді символьних рядків. Бінарний режим відправляє необроблені двійкові дані.

Різноманітність клієнтів FTP можна підключити з FTP-сервера. Є обидва GUI і командний рядок клієнтів FTP. Більшість веб-браузерів також можуть бути використані в якості клієнтів FTP.

TFTP

TFTP також є протоколом передачі чистого тексту. Клієнт і сервер використовують порт 69 для початкового з'єднання, а потім узгоджують номер порту, який використовується для передачі файлу. TFTP рідко використовується для інтерактивних переказів. Замість цього, він зазвичай використовується для:

• завантаження файлів для пристроїв без локального сховища;
• мережевих інсталяційних систем.

TFTP не підтримує аутентифікацію.

SFTP

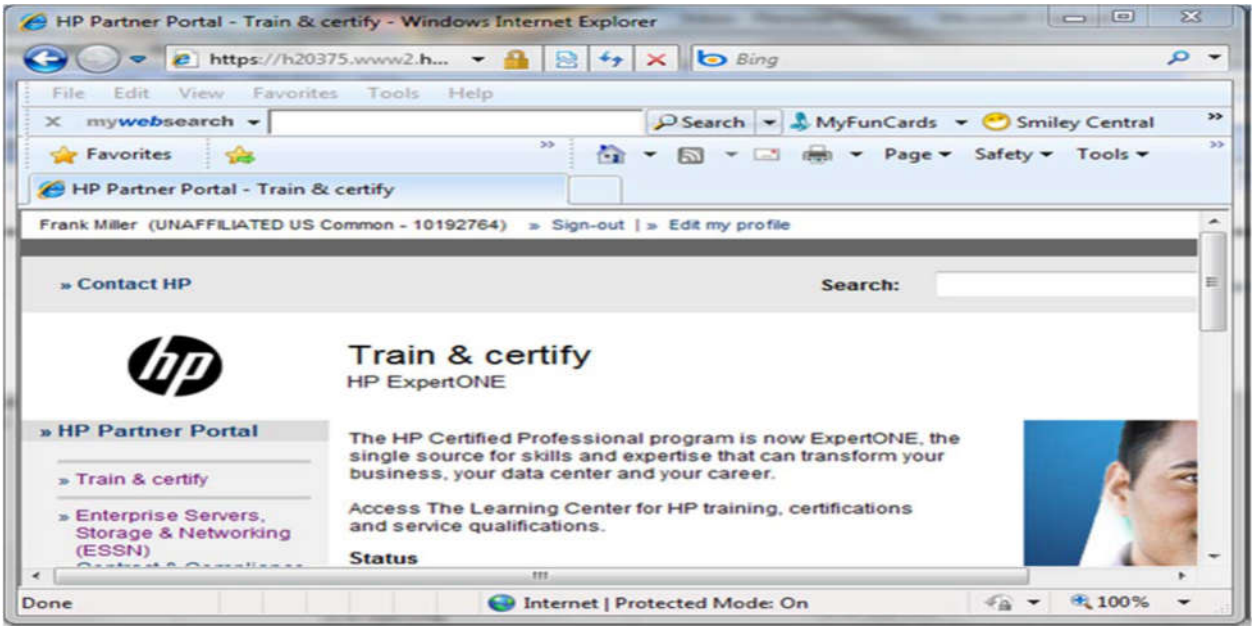
SFTP використовує SSH для забезпечення безпеки передачі файлів. Потрібна автентифікація і всі дані шифруються для передачі. Крім цієї різниці, SFTP використовується так само, як FTP для загальної передачі файлів. За замовчуванням SSH використовує порт 22.

Secure Shell (SSH) - *Протокол, який забезпечує безпечну аутентифікацію і зашифровану передачу даних для інших прикладних протоколів.*

World Wide Web

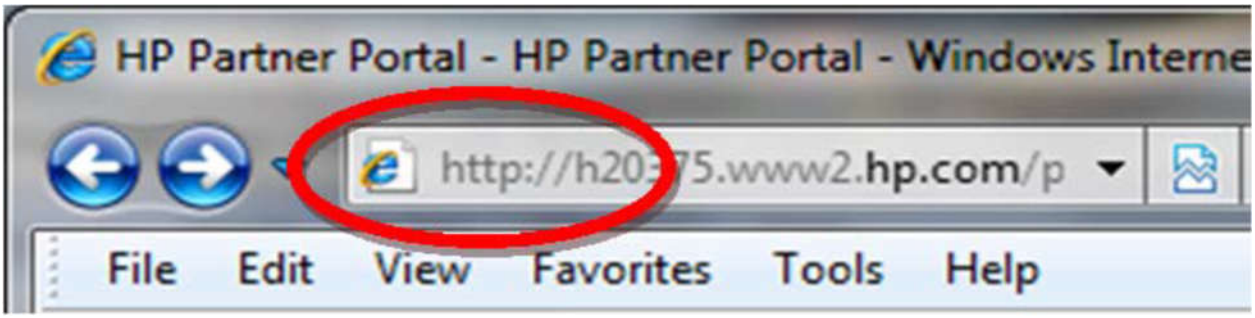
Два протоколи, які в першу чергу пов'язані з World Wide Web, є HTTP і HTTPS. Ці два протоколи дозволяють переглядати веб-сторінки - серце WWW.

Hypertext Transfer Protocol Secure *(HTTPS)* - *Протокол забезпечення безпечної веб-комунікації.*



HTTP

HTTP є протоколом, основою WWW. Він використовується для передачі команд і даних між веб-серверами і веб-клієнтами (браузерами). Якщо немає спеціальних вимог безпеки, ви будете використовувати HTTP при перегляді веб-сторінок в Інтернеті або навіть на місцевих веб-серверах, розгорнутих в приватній мережі.



Данные передаются в виде текста по умолчанию. HTTP использует порт 80 по умолчанию для всех коммуникаций.

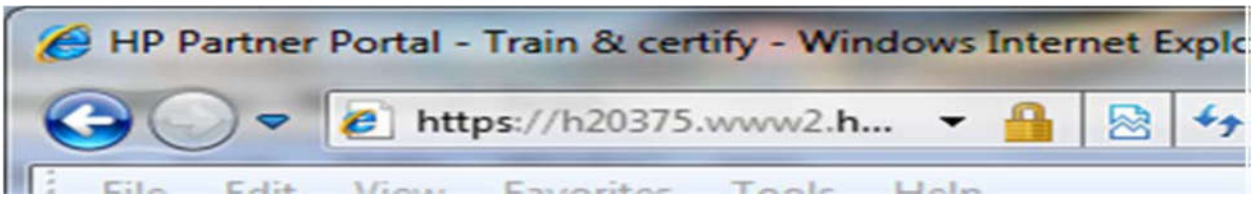
HTTPS

HTTPS використовує SSL або TLS по стандартному протоколу HTTP для забезпечення безпечного зв'язку. Всі дані, що передаються між веб-серверами і клієнтом шифруються.

Secure Sockets Layer (SSL) - *Протокол, який використовується для забезпечення безпечного зв'язку через Інтернет.*

Transport Layer Security (TLS) - *Протокол безпеки на основі і в кінцевому підсумку очікування заміни SSL для безпечного зв'язку в Інтернет.*

Ви побачите HTTPS в адресному рядку, коли за допомогою HTTPS спілкуються з веб-сайту. З багатьма веб-браузерами, ви побачите значок замка, що означає, що ви використовуєте безпечні комунікації. Веб-сервер, або окремі сторінки на веб-сервері, можуть бути налаштовані на використання клієнтського браузера, щоб використовувати HTTPS при підключенні до забезпеченим сторінок.



За замовчуванням, HTTPS використовується порт 443.

Email

Три протоколу в даний час використовуються для підтримки електронної пошти, це SMTP, POP3 та IMAP. У простих термінах, SMTP використовується при відправленні пошти. POP3 і IMAP використовуються при отриманні пошти.

Simple Message Transfer Protocol *(SMTP)* - *Протокол пошти використовується при відправленні пошти або передачі пошти між серверами.*

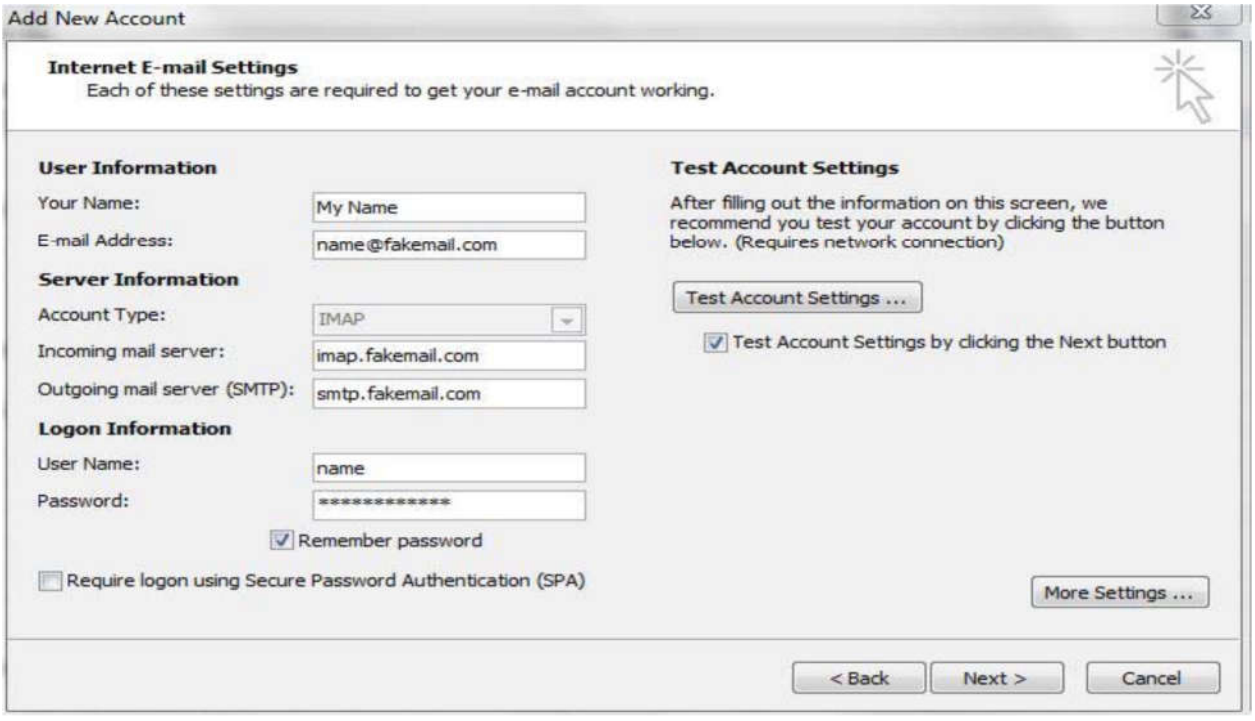
***Post Office Protocol v3 (POP3)* -** *Протокол клієнтської пошти.*

***Internet* Message Access Protocol (IMAP) -** *Протокол клієнтської пошти*.

SMTP використовується поштовими клієнтами для відправки пошти на поштовому сервері. Він також використовується при передачі повідомлень між поштовими серверами. За замовчуванням, SMTP використовує порт 25.

OP3 є одним з двох клієнтських протоколів загального користування. POP3 використовує порт 110 за замовчуванням, для безпечної передачі, які використовує порт 995. POP3 завантажує повідомлення з поштового сервера, за винятком. Після того, як вони будуть завантажені, повідомлення видаляються на сервері. POP3 підтримує тільки онлайн операції.

IMAP є більш просунутим протоколом, де клієнт підтримує більше можливостей, ніж POP3. Це означає, що IMAP також більш складний і може бути більш складним, ніж для настройки POP3. IMAP підтримує і онлайн та офлайн операції.



IMAP дає можливість завантаження повних повідомлень або тільки заголовки (залишаючи повідомлення на сервері). Коли ви завантажуєте тільки заголовки повідомлень, у вас є можливість їх перегляду і прийняття рішення, які повідомлення ви хочете завантажити. IMAP використовує порт 143.

Приклади параметрів конфігурації пошти ті ж при налаштуванні POP3 або IMAP поштових клієнтів. Відмінності між POP3 і IMAP можна побачити під час налаштування додаткових параметрів.

Більшість поштових клієнтів можуть підтримувати POP3 і IMAP. Ви можете налаштувати клієнта на сервері за допомогою сервера (або адреси за адресою), до якого протоколу клієнта користуватися.

Management protocols

Протоколи управління дозволяють збирати інформацію про вашу мережі і дистанційно керувати мережевими пристроями. Зазвичай використовуються протоколи управління включають Telnet, SSH і SNMP.

Telnet - *Інтерфейс протоколів і команд, який дозволяє запускати утиліти командного рядка і команди на віддаленому комп'ютері.*

Simple Network Management Protocol (SNMP) - *Протокол використовується як основа систем управління мережею. Ці системи управління мережею дозволяють вам контролювати і керувати мережевими пристроями.*

Telnet і SSH

Telnet дозволяє підключатися до віддаленого комп'ютера, використовуючи порт 23 за замовчуванням. Вона виступає в якості віртуального терміналу, наслідуючи німі термінали, які використовуються на початку комп'ютерних додатків. Сеанс зв'язку встановлюється з віддаленого комп'ютера. Будь-які команди, введені в командному рядку Telnet виконуються на віддаленому комп'ютері, а результат повертається.

Оскільки Telnet працює в чистому тексті, це потенційний ризик для безпеки. Для когось можна було б перехопити всі дані, які обмінюються з віддаленим хостом. Також можливо, що сеанс може бути захоплений, надаючи комусь прямий доступ до віддаленого хоста.

SSH є надійною заміною для Telnet. SSH використовує порт 22 для здійснення початкового з'єднання з віддаленим хостом. Аутентифікація необхідна при підключенні до сеансу SSH, і всі дані шифруються для передачі на кожному

кінці з'єднання. SSH використовується як безпечний інтерфейс для запуску утиліт керування на основі командних рядків і для безпечних передач файлів, запускаючи FTP в сеансі SSH.

SNMP

SNMP працює з комп'ютерами управління, централізовано керуючими мережевими пристроями. Ці комп'ютери управління використовують SNMP для збору інформації про мережеві пристрої і передають команди управління для пристроїв. SNMP може бути використаний для виконання широкого спектру завдань управління, в тому числі налаштування параметрів пристрою для підтримуваних пристроїв.

Існує центральний комп'ютер управління, і програмне забезпечення SNMP, агент, працює на кожному пристрої. Агент забезпечує інформацію про стан і конфігурацію пристрою. Він також приймає і переводить команди керування для виконання.

SNMP використовує порти 161 і 162 за замовчуванням. Безпечний SNMP використовує порти 10162 і 10161.

Є три версії SNMP в поточному використанні:

- SNMP v1

Де-факто стандартний протокол управління Інтернетом. Він є гнучким і може працювати з різними протоколами низького рівня, але вважається дещо незахищеним.

- SNMP v2

Забезпечує підвищену безпеку і функціональність управління по SNMPv1. Він також передбачає прямі менеджер-на-менеджера комунікації.

- SNMP v3

Додає аутентифікацію, цілісність повідомлень, шифрування, а також поліпшення функціональності віддаленої конфігурації.

Більшість систем управління TCP/IP підтримує всі три версії SNMP.

Інші протоколи

Є багато інших протоколів, реалізованих на рівні додатків, і список цих протоколів, неухильно зростає. Деякі з цих протоколів працюють у фоновому режимі, щоб зберегти мережу, належним чином, наприклад, працює синхронізація часу і протоколи маршрутизації. Протоколи маршрутизації обговорюються пізніше в курсі, але NTP заслуговує короткої згадки.

Network Time Protocol (NTP) - *Використовується для збереження всередині мережевих комп'ютерів синхронізованих годин.*

NTP використовує порт 123, щоб годинник комп'ютера синхронізувалися з точністю до 1 мілісекунди. У деяких випадках, ця синхронізація може бути поліпшена до частки мілісекунди. NTP підтримує ієрархічну структуру вихідних годин, з годинником вище в ієрархії, що забезпечує синхронізацію годин нижче в ієрархії. NTP використовується в додатках, де точна інформація часу має вирішальне значення, наприклад, з управлінням повітряного руху.

Протоколи і порти

Дані, що передаються з Прикладного рівня на Транспортний рівень для передачі, повинні включати номер порту призначення. Цей номер використовується приймаючим хостом для доставки даних до відповідної програми.

Номери портів від 0 до 1024 призначаються IANA як відомі порти. Є як TCP, так і UDP добре відомі порти. Під час налаштування призначених для користувача портів слід використовувати 1025 і вище. Підтримуються значення до 65535.

Добре відомі призначення портів як для TCP, так і для UDP. У багатьох випадках протокол буде мати як номер порту TCP, так і номер порту UDP (зазвичай це один і той же номер). Як згадувалося раніше в курсі, міжмережеві екрани можуть бути налаштовані на пропуск або блокування трафіку на основі номера порту джерела або призначення. Блокуючи добре відомий порт, ви ефективно блокуєте будь-який трафік, пов'язаний з цим протоколом або службою.

Розділ 6:
Маршрутизація

Вступ

Використання терміна "маршрутизація" не обмежується комп'ютерними мережами. Маршрутизація це вибір мережевого маршруту, через який надсилається інформація до кінцевої точки призначення. Це відноситься, як згадувалося в попередніх частинах, до LAN і WAN, а так само до комп'ютерних мереж, мереж електронного обміну даними, і навіть для фізичних транспортних мереж.

Нашу увагу в цьому розділі в основному буде приділено роутера (маршрутизаторів), як мережевого обладнання та ролі, яку вони грають. Ми розглянемо процес поділу мереж на підмережі і використання роутерів для забезпечення того щоб інформація дійшла до місця призначення. Ми так само коротко розглянемо, як управляється інформація про маршрути. Ми так само досліджуємо спеціалізовані роутери, в яких реалізовані додаткові можливості, як спосіб доповнення до мережевої безпеки.

Цей розділ в основному фокусується на технологіях маршрутизації заснованих на IPv4. Тим не менше, більшість тем, описаних тут, так само застосовні до IPv6. Деякі важливі обмеження будуть згадані як необхідні.

Мета

У цьому розділі ви дізнаєтеся, як:

Пояснити основи маршрутизації та обґрунтування.

Перелік та опис протоколів, що використовуються для управління маршрутом.

Визначити призначення та використання маршрутизаторів спеціального призначення:

- Firewall
- Proxy
- Multicast routers
- VPN endpoint

Обговорити процедури розгортання та підтримки маршрутизаторів.

Основи маршрутизації

Для комп'ютерних мереж, маршрутизація знаходиться на мережевому рівні моделі OSI (або на рівні Internet TCP/IP моделі). Будь який мережевий транспортний протокол, який реалізує Мережевий рівень моделі OSI, може підтримувати маршрутизацію (Рисунок 6.1).

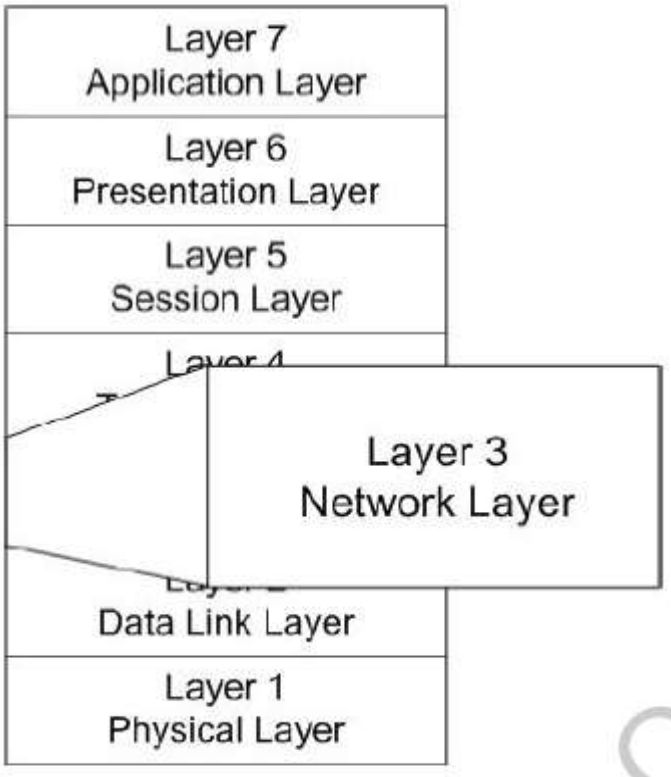


Figure 6-1: OSI Model

Рисунок 6.1: Модель OSI

Сучасне обладнання підтримує безліч функцій. Проте, для приладу, якого називають роутер (маршрутизатор), одна з функцій, яка повинна забезпечується це маршрутизація 3 рівня.

Деякі старі мережеві протоколи, такі як NetBEUI, іноді звані NetBIOS кадрами, не включали функціональність Мережевого рівня. Протягом багатьох років, терміни NetBEUI і NetBIOS помилково використовувалися як взаємозамінні для позначення мережевого протоколу.

NetBIOS Extended User Interface (NetBEUI) - *Відноситься до мереж NetBIOS, засновані на мережевих схемах, які забезпечували сесії комунікації, засновані на символічних іменах, але не включали протоколи маршрутизації.*

Network Basic Input/Output System (NetBIOS). *Зазвичай відноситься до сесійній рівню і системам символьного позначення, що визначає пристрої по 16-бітовому імені.*

NetBIOS все ще іноді розглядається як NetBIOS over TCP/IP (NBT) - NetBIOS через TCP/IP. Призначені для користувача операційні системи продовжують надавати підтримку для NetBIOS імен. Ви можете відключити підтримку NetBIOS в сучасних операційних системах сімейства Windows, шляхом зміни властивостей TCP/IP.

NetBIOS через TCP/IP (NBT). *Метод інкапсуляції пакетів NetBIOS всередині TCP або UDP пакетів для доставки по маршрутизуються мережі.*

Маршрутизатори

Коли ми говоримо, що маршрутизатор працює на Рівні 3 моделі OSI, ми маємо на увазі, що він забезпечує функціональність через рівень 3. Наприклад, на Рівні 1 він забезпечує підключення до фізичних носіїв передачі мережі. На Рівні 2 кожен з мережевих інтерфейсів маршрутизатора також має локальну або MAC-адресу (Рисунок 6-4).

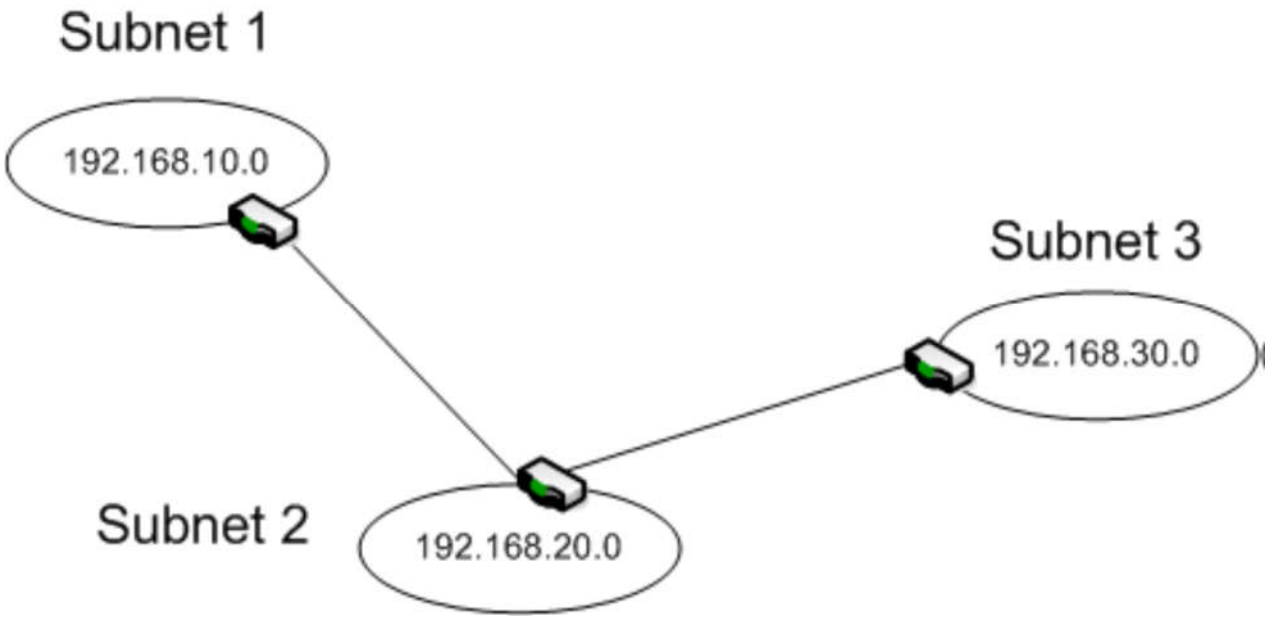


Рисунок 6.4: Проста маршрутизована мережа

Маршрутизатор (роутер) використовують, щоб розділити мережу на розділені (окремі) підмережі, кожні з унікальними мережевими адресами. Трафік проходить або не проходить в залежності від мережевої адреси. Наприклад, якщо пакет згенерований в підмережі 1 і призначений будь-якого іншого хосту з тієї ж підмережі 1, пакет не буде з неї випущений (з підмережі) її маршрутизатором.

У мережах TCP/IP, маршрутизатор так само описується як шлюз. Кожному хосту може бути призначений шлюз, який є роутером за замовчуванням, на який посилається інформація для подальшої маршрутизації.

Маршрутизатор отримує пакет, перевіряє адресу одержувача і, якщо він підходить, перепосилает пакет по його шляху. В цьому випадку, роутер поводиться як повторювач першого рівня, посилюючи (швидше за ретранслюючи) переданий сигнал і допомагаючи забезпечити найкращу зв'язність.

Використання Роутера

Зазвичай, роутери використовуються для:

- Управління мережевим трафіком

Трафік, призначений для підмережі, залишається в підмережі, таким чином, зменшуючи общесетевой трафік. Роутери так само можуть бути використані для посилки інформації по широкосмуговим маршрутами, уникаючи скупчень інформації і можливих збоїв мережі.

- Ізолювання мережевих сегментів

Роутери можуть бути використані для поліпшення безпеки в сегменті, контролюючи трафік, що знаходиться в і поза сегмента.

Багато роутерів, крім їх основних функцій, були створені з додатковим функціоналом, і можуть в мережі виконувати функції:

- NAT
- VPN
- Firewall
- Проксі-сервер

Ви так само можете зустріти роутери, які підтримують проводові та безпроводові сегменти мережі. У такій конфігурації, вони поводяться як роутери так і як мости (bridge), будучи інтерфейсом між різними середовищами передачі.

Типи роутерів

Є багато способів, за якими ви можете класифікувати роутери, наприклад функціональність і тип сервісів. На даний момент ми розглянемо найпростішу класифікацію: по установці і розгортання роутерів. Найбільш часто згадуються роутери засновані на програмному забезпеченні (software-based) і засновані на апаратному забезпеченні (hardware-based). Незважаючи на те, що ці визначення в деякій мірі не точні, вони придатні для наших цілей.

Software Router (роутери, засновані на програмному забезпеченні)

Коли ми говоримо що Роутер - Software Router - ми маємо на увазі що він розгорнуть на стандартному ПК зі спеціальним програмним забезпеченням, що забезпечує функції роутера. Наприклад, Windows Server operating systems підтримують сервіс RRAS, що дозволяє використовувати сервер як роутер.

Routing and Remote Access – RRAS. *Мережеві системи поставляються з Windows Server operating systems і дозволяють вам налаштувати сервер так, щоб він працював як роутер. RRAS так само забезпечує інші мережеві послуги.*

Одна з переваг використання сервера в якості роутера це відносно невеликі грошові витрати. Воно засноване на тому, що використовується стандартне апаратне і програмне забезпечення ПК. Ви навіть можете встановити на ПК такі сервіси як NAT і віддалений доступ.

Потенційні проблеми це - проблеми безпеки, надійності та ефективності. Так як роутер працює з операційною системою Windows server, роутер сприйнятливий до таких же ризикам, як і інші Windows комп'ютери. Це так само має вплив на потенційну надійність роутера. Крім того, оскільки він працює на операційній системі загального призначення, продуктивність значно страждає в порівнянні з пристроями, спеціально призначених для роботи в якості маршрутизаторів. В момент пікового навантаження, це може вилитися в повний збій мережі, якщо роутер не зможе забезпечити необхідну продуктивність.

Комп'ютер з RRAS можна так само налаштувати на забезпечення інших мережевих додатків і сервісів. Це не рекомендовано, так як це може вплинути на ефективність роутера, і створює потенційні проблеми безпеки.

Hardware роутер (апаратний маршрутизатор)

Hardware роутер (так само званий Dedicated - виділений) є, по суті, дуже схожим на вище описаний Software роутер. Це спеціальний комп'ютер зі спеціальним апаратним забезпеченням, яке було розроблено і оптимізовано спеціально для маршрутизації трафіку. Функціональність роутера так само забезпечується через Софт (програмне забезпечення), але Софт призначений для спеціальних цілей. Це дає виробникові можливість вирішувати проблеми, які можуть бути виявлені після випуску або поліпшити роутер за допомогою додаткового функціоналу.

Виділений роутер -
Мережевий прилад, розроблений спеціально для цілей маршрутизації.

Рисунок 6.5: HP MSR20 Series Router

Роутери сильно розрізняються в розмірах, можливості і вартості. Роутер на Рисунку 6-5 швидше за все, буде використовуватися при розгортанні SMB. Великі компанії можуть легко мати кілька роутерних стійок, що підтримують безліч LAN і WAN каналів, голосові сервіси, і інші сервіси якщо потрібно.

Додаткова функціональність залежить від моделі роутера і додаткових опцій, які були замовлені. Це звичайна ситуація коли в роутері інтегрована підтримка для VLAN і комутацію другого рівня, безліч сервісів 3-го рівня, контроль доступу, безпека передачі інформації і інтеграцію з іншими технологіями.

Маршрутизація

Маршрутизація (досить просто) - процес пересилки пакета від джерела до місця призначення через маршрутизації мережу. Посилає хост не повинен знати нічого про фізичне розташування місця призначення, тільки адреса мережі та хоста.

Інформація для маршрутизації

Роутери зберігають інформацію про шляхи в RIB або таблицях маршрутизації. Таблиця маршрутизації це зазвичай таблиця, що включає в себе відомі цього роутера підмережі, і який інтерфейс роутера повинен бути використаний, для відправки пакета в певну підмережа (Рисунок 6.6).

Routing Information Base, RIB - *База інформації маршрутизації. Таблиця, що підтримується в маршрутизаторі, який містить інформацію про маршрути і використовується для пересилки пакетів.*

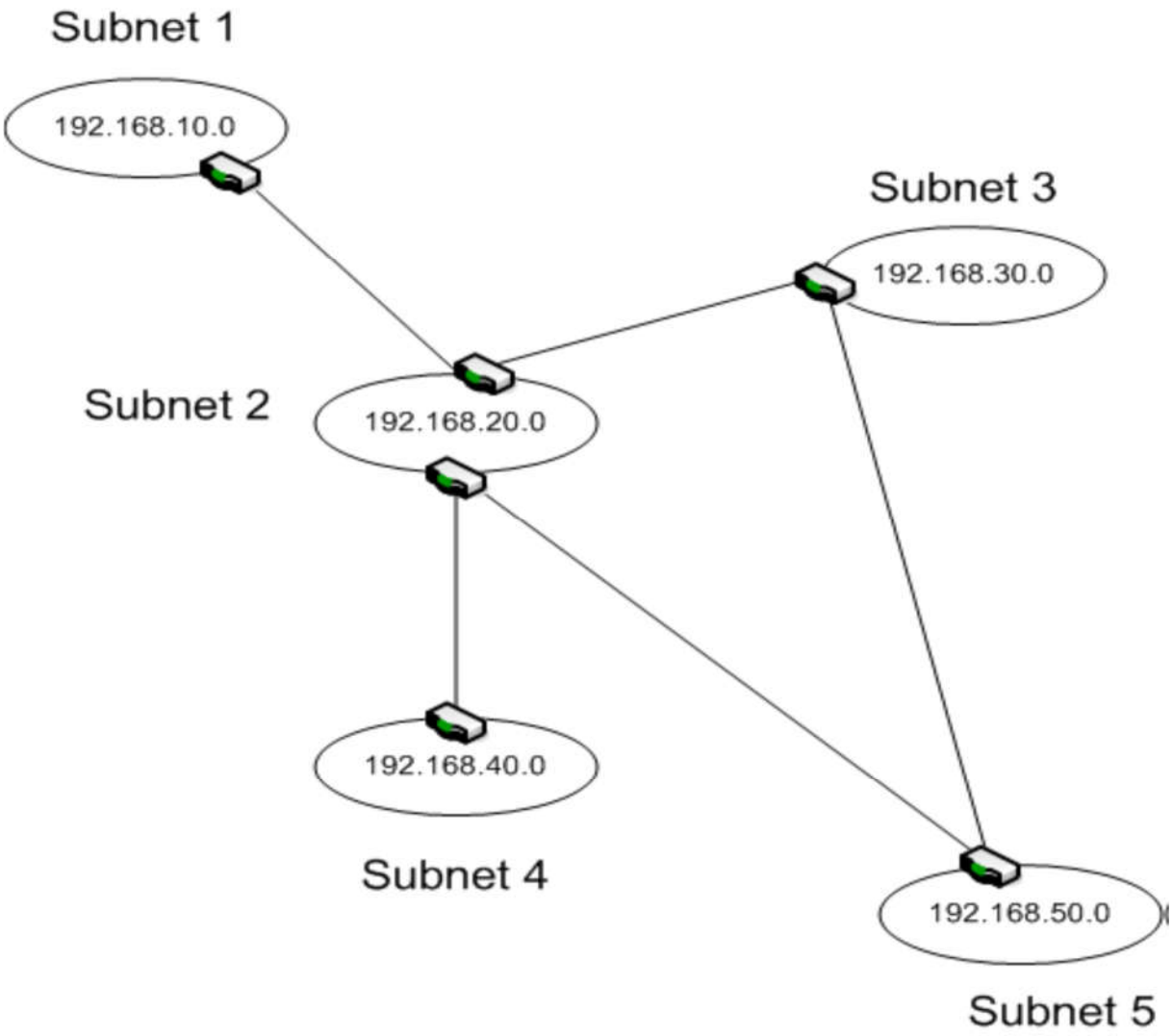


Рисунок 6.6: Приклад мережі з маршрутизацією

Інформація про маршрути може бути введена в таблицю маршрутизації за допомогою статичного ручного введення або оновлюватися динамічно. Статичні записи налаштовуються для маршрутизатора і, як правило, включаються в таблицю маршрутизації автоматично кожного разу, коли роутер перезавантажується.

Автоматичні оновлення надсилаються роутерами за допомогою спеціалізованих протоколів, які дозволяють роутера обмінюватися інформацією.

Як мінімум, таблиця маршрутизації включає наступне:

- ID адреса мережі призначення (IP адреса і маска підмережі);
- Вартість («Вага», який використовується для визначення кращого роутера);
- Наступний стрибок (наступний роутер на шляху до місця призначення).

Наступний стрибок - *Наступний роутер (шлюз) на шляху проходження пакету до місця призначення.*

Ви так само будете стикатися з записом з IP адресою мережевого інтерфейсу, через який потрібно надсилати пакет. Якщо місце призначення не буде записано в таблиці маршрутизації, пакет буде відісланий за адресою шлюзу.

У таблиці маршрутизації для шлюзу адреса і маска підмережі встановлюються 0.0.0.0

Процес маршрутизації

Хост здатний розпізнати, грунтуючись на адресу призначення, знаходиться чи ні хост призначення в тій же підмережі. Якщо немає, то хост буде посилати пакет відповідного маршрутизатора (або шлюзу за замовчуванням), який повинен перенаправити до кінцевого пункту призначення.

Точний процес маршрутизації пакета в деякій мірі залежить від типу передачі. Наприклад:

- *Unicast*
  Пакет маршрутизується до одного, унікального, місця призначення.
- *Broadcast*
  Пакет, якщо буде пропущено, відправляється в усі можливі підмережі.
  Зазвичай, роутери налаштовані не пропускати широкомовні пакети, хоча деякі будуть передавати пакети, призначені для віддаленого управління і DHCP.
- *Multicast*
  Пакет передається для групи хостів, які можливо знаходяться в різних підмережах.
- *Anycast*
  Пакет призначений групі хостів, але доставляється тільки одному хосту, зазвичай найближчого до місця відправки.

Рисунок 6.7 ілюструє процес Unicast.

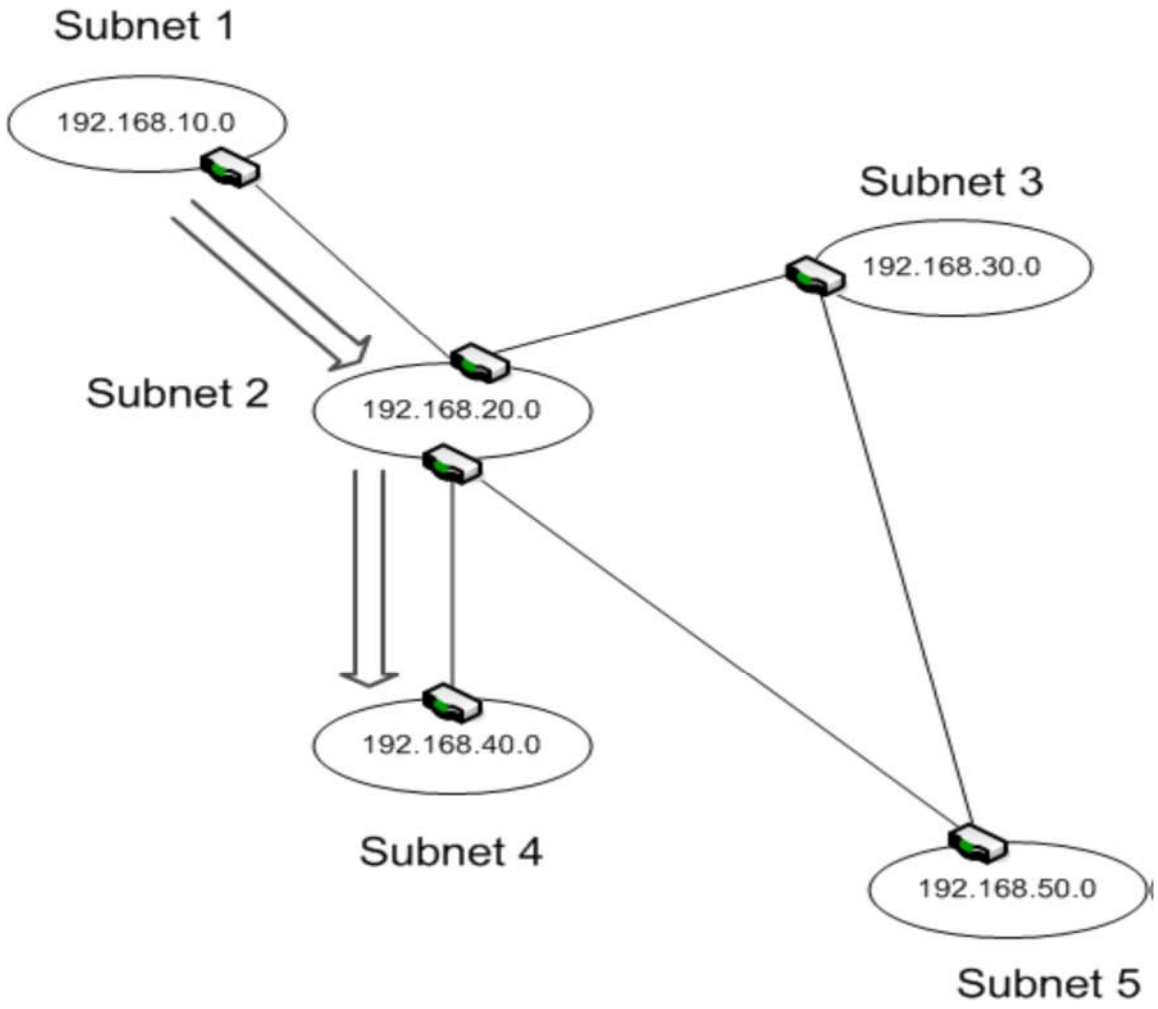


Рисунок 6.7: Приклад Unicast маршрутизації

Хост в Підмережа 1 генерує пакет з кінцевим адресою 192.168.40.115. Роутер з Підмережі 1 посилає пакет на роутер, показаний нагорі підмережі 2. Через те що є багато шляхів (навіть через одну петлю), роутер повинен прийняти рішення про найкращий маршрут. Він відправить пакет прямо на роутер, показаний знизу Підмережі 2, який в свою чергу пошле його Підмережа 4 для доставки.

Як робиться вибір кращого маршруту? У протоколах з дистанційно-векторною маршрутизацією (distance vector routing), шлях зазвичай вибираються за кількістю роутерів між джерелом і місцем призначення. У нашому прикладі пакет міг пройти через Підмережі 3 і 5, але це додало б 2 стрибки.

Distance vector routing *(дистанційно-векторна маршрутизація)*

Алгоритм маршрутизації, який будує свої розрахунки маршрутів по «вартості» (кількості стрибків) до місця призначення.

Стрибок - *Відноситься до кожного роутера, який проходить пакет на шляху до пункту призначення*

При дистанційно-векторної маршрутизації, маршрут ґрунтується на вартості, вираженої в кол-ве стрибків, до місця призначення. Ми показали дуже легкий приклад, але маршрут може стати складніше більшою мережі. Щоб полегшити процес, кожен роутер оновлює інформацію свого сусіда інформацією про кожне місце призначення, про який він знає. Роутер використовує цю інформацію для оновлення таблиці маршрутизації, і, в свою чергу, приймає рішення про кращому маршруті.

У роутера налаштований шлях за замовчуванням до іншого роутера. Він використовується, як наступний стрибок, коли місце призначення не міститься в таблиці маршрутизації RIB.

Є ймовірність того, що пакет може загубитися у великій складної мережі, що може застрягти в петлі де не зможе ніколи знайти своє місце призначення. Щоб уникнути цього, у кожного пакета налаштоване так зване значення TTL (time-to-live). Це максимальна кількість стрибків (роутерів) через які пакет може бути посланий. З проходженням кожного роутера, значення збільшується на одиницю. Коли лічильник досягає значення TTL, пакет скидається і ICMP повідомлення надсилається назад джерела показуючи, що пакет не може бути доставлений.

Повтор IPv4 адресації

IPv4 адресація була розглянута детально в попередніх частинах. Зараз, ми повторимо кілька ключових моментів, так як вони відносяться до роутера і процесу маршрутизації.

• Кожне мережеве обладнання має свою унікальну IP адресу.

• Маска підмережі використовується для визначення яка частина адреси використовується для адреси хоста, а яка для адреси підмережі.

• Хости можуть спілкуватися один з одним в одній підмережі, не проходячи через роутер.

• Трафік повинен проходити через роутер, коли пакет надсилається з однієї підмережі в іншу.

• Коли ми використовуємо DHCP/Bootp щоб дати адресу комп'ютера, будь-роутер між орендують (приймаючим IP адреса) хостом і DHCP сервером повинен бути налаштований на передання DHCP повідомлень до DHCP сервера.

• Широкомовні повідомлення можуть бути втрачені, якщо на використовуваному роутере відсутня установка мультикаст.

• Приватні IP адреси не можуть бути використані для зв'язку через Інтернет.

Ці моменти в основному стосуються IPv4 адресації, але більшість роутерів зараз підтримують як IPv4 так і IPv6.

Протоколи маршрутизації

Кожен роутер зберігає таблицю маршрутизації, або RIB, яка містить IP адреси і інформацію про маршрути. Ви можете створювати статичні записи в таблиці, але це займає багато часу і не ефективно. На додаток до сказаного, таблиця маршрутизації адаптується до змін в мережевому середовищі. Для таких випадків, у вас повинна бути інформація, яка оновлюється автоматично.

Звідки роутери отримують інформацію для маршрутизації? Вона приходить від інших роутерів, через динамічні оновлення через протоколи маршрутизації. Протоколи маршрутизації дозволяють роутера ділитися інформацією з їх таблиць з іншими маршрутизаторами.

Є два основних типи проколів маршрутизації. Протокол маршрутизації зазвичай стосується або внутрішньої маршрутизації, або зовнішньої маршрутизації.

Внутрішній протокол маршрутизації *(Interior gateway routing protocol,* ***IGRP****) - Протоколи, що розроблені для роботи з роутерами розгорнутими в LAN і WAN середовищах.*

Зовнішній протокол маршрутизації *(Exterior gateway routing protocol,* ***EGRP****) Протоколи для забезпечення інтернет маршрутів.*

Ми будемо фокусуватися на протоколах внутрішньої маршрутизації. Далі протоколи можуть бути розділені на маршрутизацію з аналізом стану каналів (link-state routing protocols) і дистанційно-векторну маршрутизацію (distance-vector routing protocols).

Протоколи маршрутизації з аналізом стану каналів
Маршрути засновані на безлічі факторів, включаючи кількість стрибків до місця призначення, а так само, смугу пропускання, скупчення трафіку, і інші чинники які зменшують ефективність.

Основнми серед внутрішніх протоколів маршрутизації є наступні – RIPv1, RIPv2, RIPng и OSPF.

Протокол інформації про маршрутизації версія 1 *(Routing Information Protocol version 1,* ***RIPv1****)*
Оригінальна версія протоколу RIP.

Протокол інформації про маршрутизації версія 2 *(Routing Information Protocol version 2,* ***RIPv2****)*
Оновлення для протоколу RIP, яке підтримує формат адреси CIDR
.
Протокол інформації про маршрутизації, нове покоління *(Routing Information Protocol, next generation,* ***RIPng****)*
Оновлення до RIP, що підтримують IPv6 адреси.

Протокол маршрутизації з визначенням найкоротшого шляху *(Open Shortest Path First,* ***OSPF)***
Загальний протокол з маршрутизацією з аналізом каналів (link-state).

Є ще інші внутрішні протоколи які використовуються, такі як IS-IS (Intermediate System-Intermediate System), але детальне обговорення цього протоколу лежить за рамками цього курсу.

RIP

RIP зазвичай досить щоб задовольнити потреби мереж середнього-малого бізнесу. Його також легко налаштувати, що робить його популярним вибором для маленьких мереж.

Є 3 версії RIP:

- RIPv1
  Оригінальна версія, розроблена для підтримки тільки безкласових мереж.
- RIPv2
  Випущений як заміна для першої версії, включає вбудовану підтримку CIDR і маски підмережі з мінливою довгою.
- RIPng
  озроблено для підтримки IPv6 маршрутизації.

RIP має деякі нерозв'язані недоліки. Як результат, повільна конвергенція, особливо у відносно великих мережах. RIP протокол так само обмежений на підтримку не більше 15 стрибків на маршруті. Це ліміт мережі, яку може підтримувати RIP.

Convergence
Конвергенція - це стан, в якому все роутери мають актуальну інформацію для маршрутизації.

RIP використовує 3 механізми, щоб запобігти розсилку неправильної інформації через мережу:

- **Split horizon** (Розщеплення горизонту)
  Коли роутер отримує оновлення інформації через інтерфейс, він не буде (інтерфейс) посилати свою інформацію назад через той же інтерфейс. Цей механізм розроблений для запобігання петель маршрутизації.

- **Route Poisoning** (Розщеплення горизонту зі зворотную забороною)
  Механізм, який використовується для визначення роутера як недосяжного. Це робиться за допомогою виставлення маршрутної метрики на значення 16 (яка позначається як недосяжна) перед тим як послати маршрут. Роутери, які отримали це повідомлення, видалять цей маршрут з їх таблиць.

- **Holddown** (Тимчасова відмова)
  Роутер запускає таймер, як тільки отримує повідомлення, що інший роутер недосяжний по цьому маршруту. Поки таймер вважає, роутер буде ігнорувати будь-які повідомлення, які будуть говорити, що роутер досяжний. Роутер може оновлювати інформацію про маршрут після того як таймер закінчиться. Таймер за замовчуванням встановлюється на 180сек для RIP.

Зараз ми ретельніше розглянемо кожну RIP версію.

RIPv1

RIPv1 має кілька недоліків, які призвели до його заміни. Серед недоліків: відсутність підтримки масок підмережі зі змінною довжиною, CIDR і IPv6 адресації. RIP використовує широкомовні повідомлення, що може надмірно споживати смугу пропускання і зменшує ефективність. Оновлення не несуть інформацію про підмережі.

RIPv2

RIPv2 додав підтримку для масок підмережі зі змінною довжиною і CIDR. Проте, RIPv2 був розроблений, щоб бути назад сумісним, так само надаючи підтримку безкласової маршрутизації і обмежуючи кількість стрибків на маршруті 15-ю. RIPv2 посилає поновлення через багатоадресну передачу на адресу 224.0.0.9, досягаючи всіх суміжних роутерів. Кожне приймаючий маршрутизатор обробляє ці оновлення, оновлює свою RIB (при необхідності), а потім відправляє нові оновлення сусідньому маршрутизатору.

RIPng

RIPng був розроблений для забезпечення distance-vector протоколу для IPv6 адрес. RIPng так само був розроблений як поліпшення RIPv2, і не завжди сумісний з роутерами, які використовують тільки RIPv1.

OSPF

SPF - це найбільш використовуваний протокол маршрутизації в великих мережах. Він дозволяє більш ефективну маршрутизації і велику ефективність зв'язку, тому що OSPF так само враховує такі параметри як смуга пропускання, підтримувана різними роутерами. OSPF так само відповідає на зміну мережевої топології, наприклад непрацюючий канал або роутер. OSPF здатний швидко обчислити і компенсувати ці та інші мінливі умови.

Спеціальні роутери

Часто буває, що роутери виконують безліч дій, щоб зберегти кількість систем, підключених до Інтернет мінімальним. Це особливо важливо, якщо вони розгорнуті в мережі периметра (perimeter network).

Firewalls (файерволи)

Є два базових типу файерволов: host-based і network-based. Host-based фаєрволи працюють на комп'ютері користувача і розроблені, щоб захищати тільки користувача. Network-based були розроблені для захисту мереж.

Фаєрволи були розроблені для захисту хоста або сегмента мережі за допомогою фільтрації трафіку, який проходить з і в фаєрвол. Це може здійснюватися через порт фільтрації, який блокує або пропускає трафік, грунтуючись на номері порту. Більш складні роутери керують трафіком, грунтуючись на адреси джерела і місця призначення і навіть залежно від змісту пакету

Конфігурація фаєрволів

Дві найбільш поширені конфігурації файрволов це network-based фаєрволи з двома мережевими адаптерами і фаєрволи з трьома мережевими адаптерами. Ми розглянемо загальні зміни периметр-мереж, щоб побачити, як вони використовуються.

На нашому першому прикладі, периметр-мережу обмежена двома фаєрволами (Рисунок 6.8). Один знаходиться між периметр-мережею і публічним інтернетом. Другий між периметр-мережею і внутрішньою мережею.

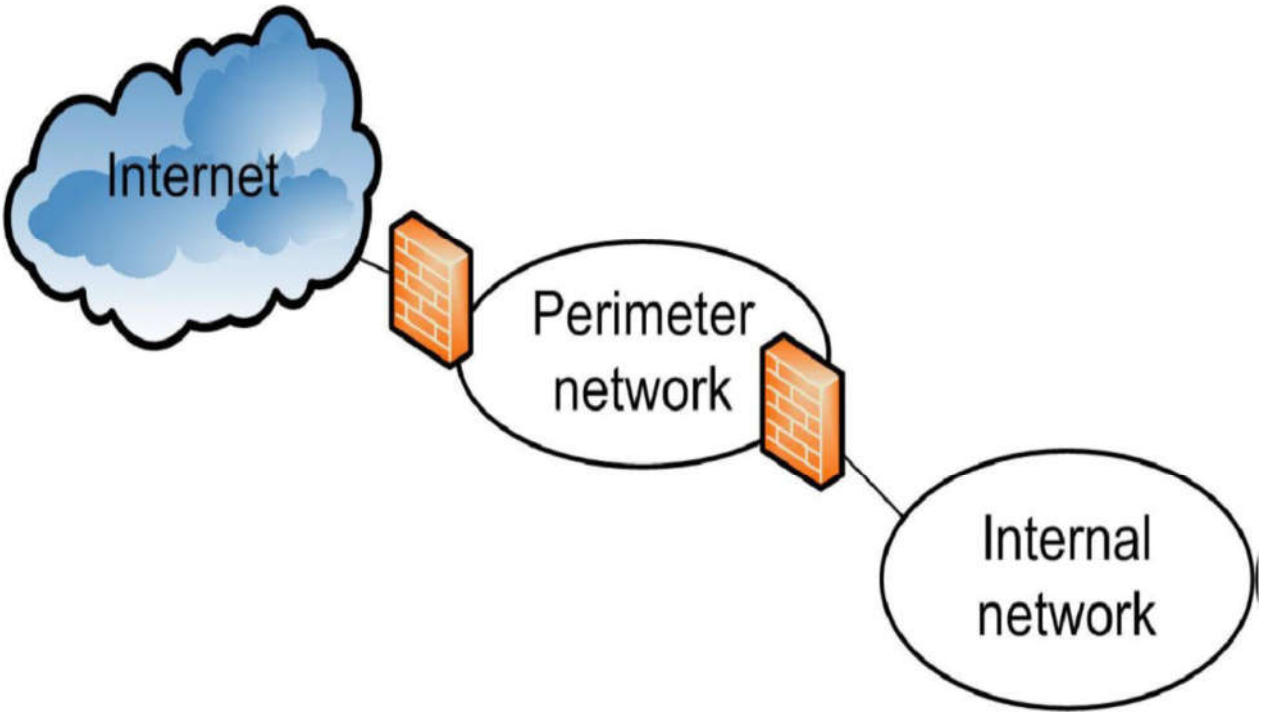


Рисунок 6.8: Периметр

Вам іноді доведеться зіткнутися з периметр-мережею з одним налаштованим файєрволом. У цьому прикладі файрвол встановлюється з трьома мережевими адаптерами.

Ви можете зустріти цю конфігурацію ще як three-prong firewall (3 файєрволи). Один з адаптерів файрволу підключений до інтернету, один до периметр-мережі і один до внутрішньої мережі. Трафік між будь-якими двома повинен пройти через брандмауер.

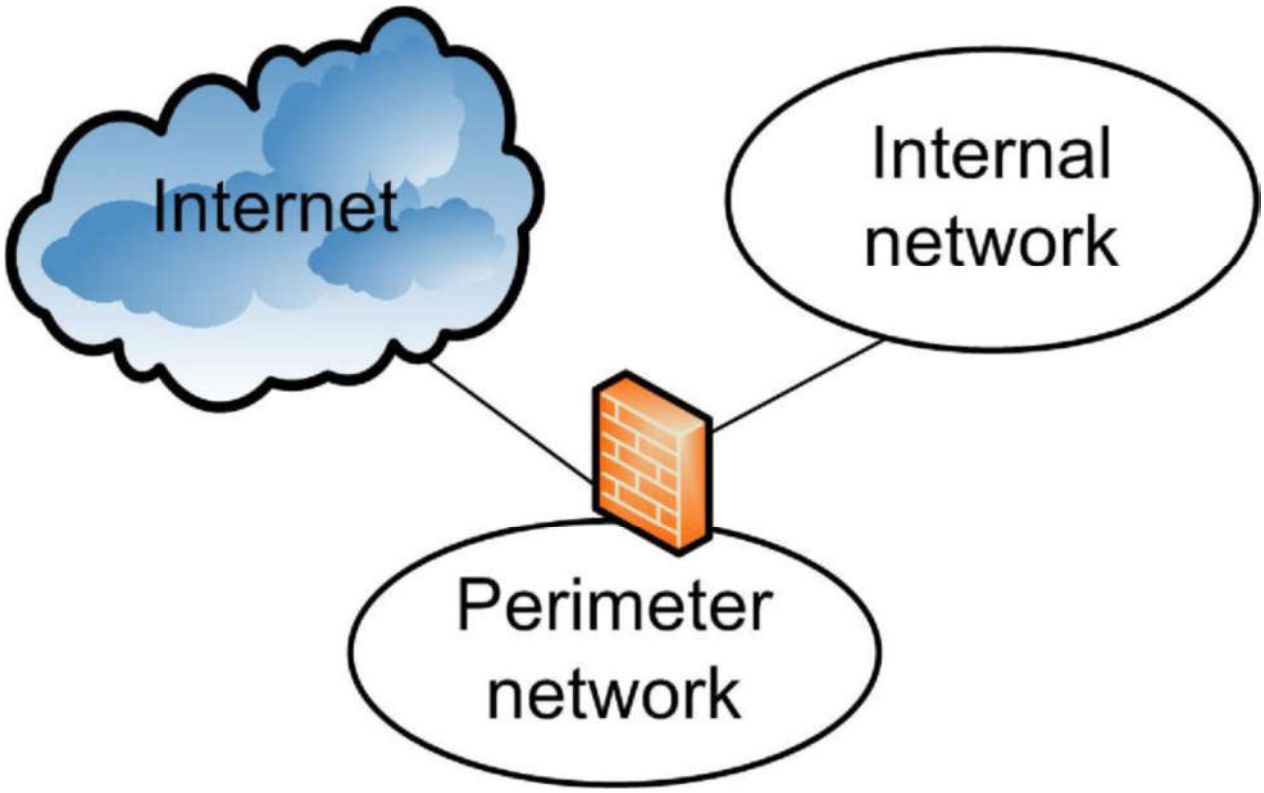


Рисунок 6.9: Альтернативная конфигурация

Ця конфігурація з одним фаєрволом іноді вважається менш захищеною, ніж використання двох фаєрволов. Є ймовірність, що фаєрвол може бути перевантажений в момент пікового навантаження. Є також більш прямий канал між внутрішньою мережею і Інтернетом, за яким набагато простіше атакувати вашу підмережа.

Проксі-сервер

Проксі-сервери (проксі) допомагають керувати доступом до мережі. Згідно з визначенням, проксі це будь-який сервер, який веде себе як посередник між хостом і іншим комп'ютером, найчастіше іншим сервером. На практиці, проксі-сервера найбільш часто використовуються для надання клієнтського доступу в Інтернет. Проксі-сервер часто реалізується на тій же апаратній платформі, що і звернений до Інтернету фаєрвол в периметр-мережі в маленьких мережах. Він може бути розгорнутий як окремий пристрій.

Основні операції проксі

Тепер, ми вивчимо базові проксі операції (Рисунок 6.10). У мережі з проксі-сервером, клієнт хоче отримати інформацію з сервера в Інтернеті. Він посилає запит проксі-сервера. Проксі фільтрує запит, грунтуючись на правилах налаштованих на сервері, і посилає його в Інтернет якщо запит задовольняє правилам.

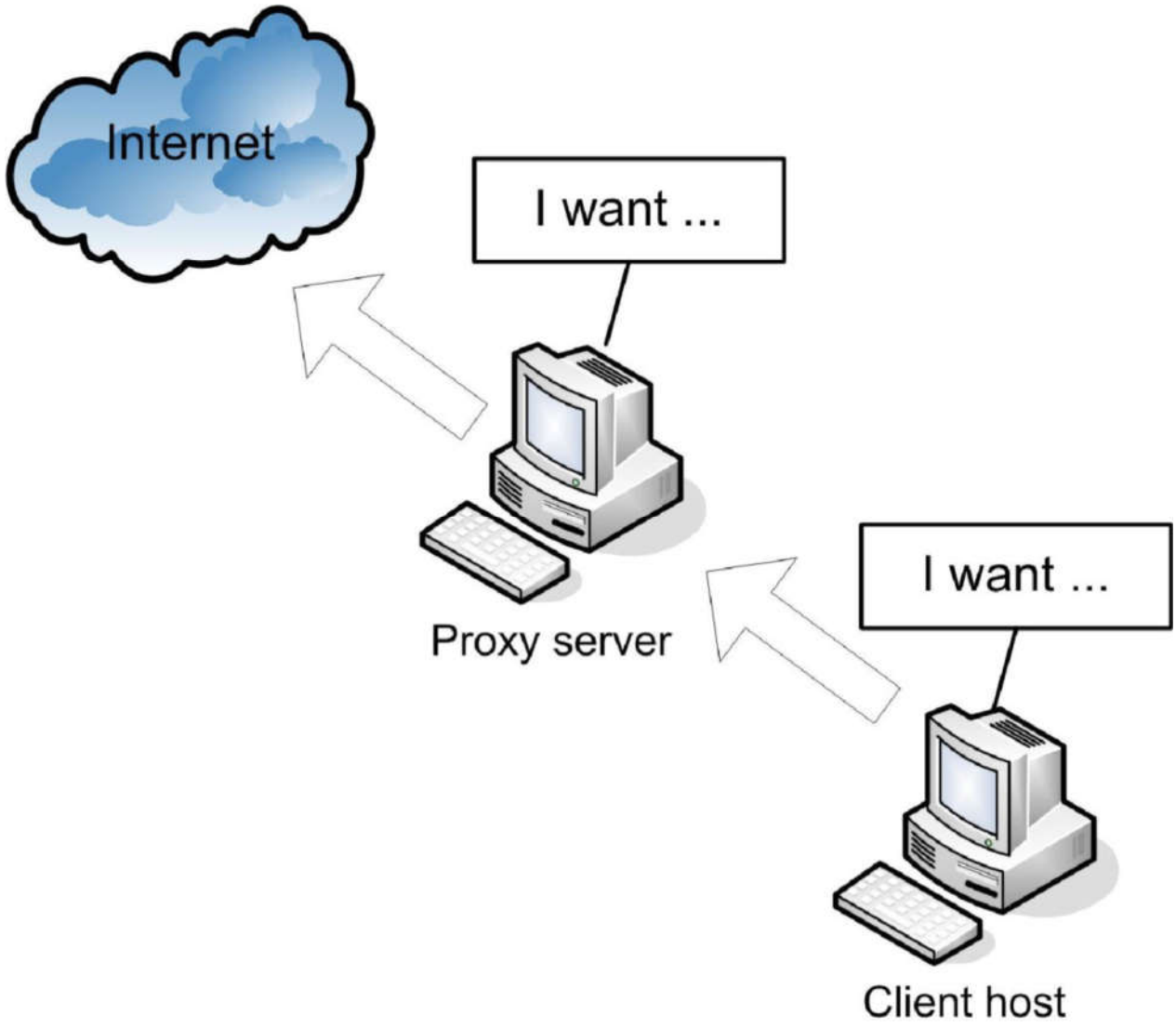


Рисунок 6.10: Інтернет запит через проксі-сервер

Фільтрація часто проводиться по серверу, який є місцем призначення, таким чином, обмежуючи Інтернет доступ по URL. Проте, можуть використовуватися і інші методи, такі як фільтрація контенту.

Фільтрація контенту
Процес фільтрації запитів заснований на інформації, що міститься в пакеті.

роцес відповіді аналогічний. Інтернет сервер посилає відповідь (Рисунок 6.11). Ще раз, він проходить через фільтр проксі-сервери, перед тим як бути доставленим клієнту.

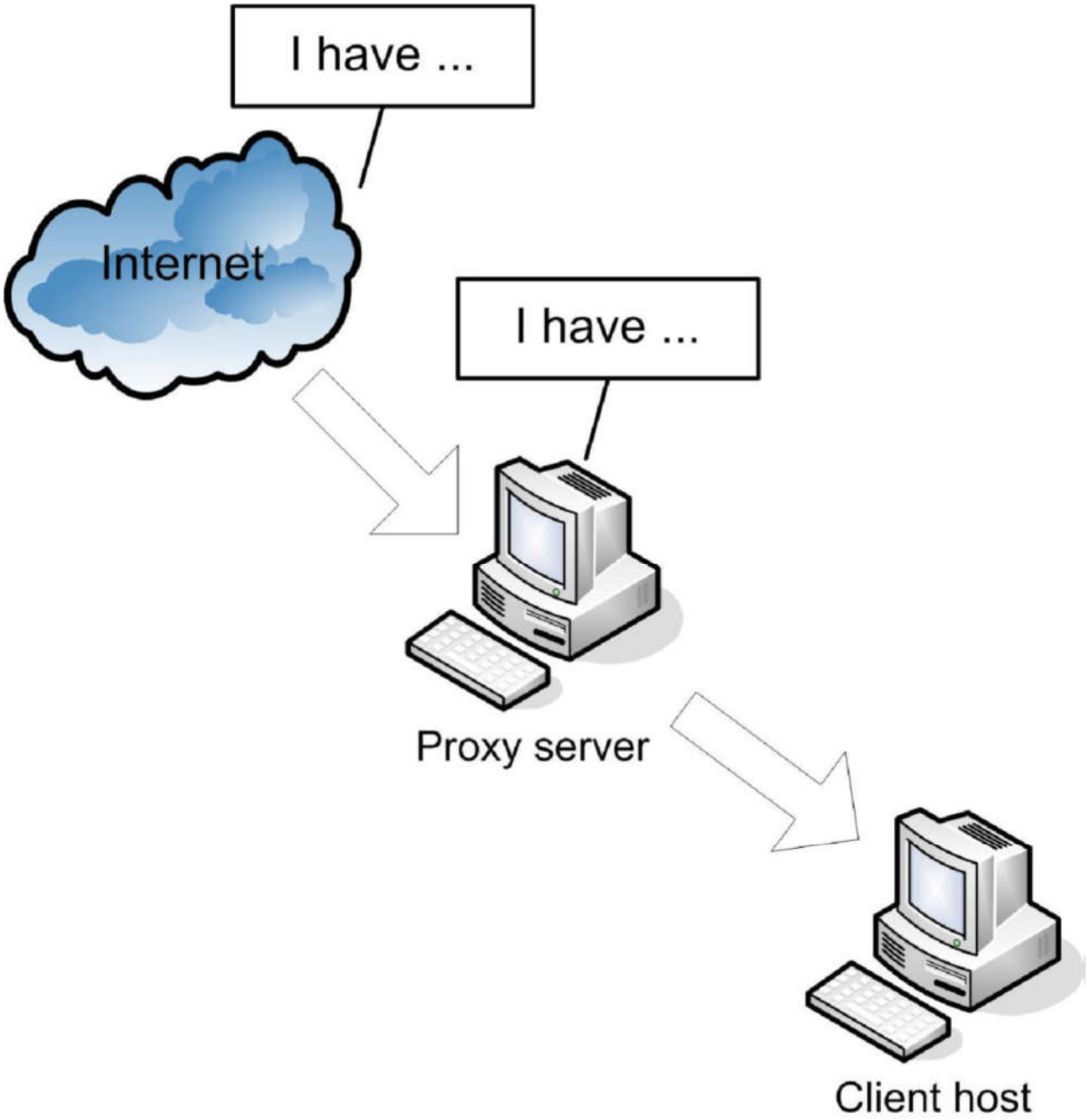


Рисунок 6.11: Інтернет відповідь через проксі-сервер

До того ж, відповідь зазвичай кешируєтся на проксі-сервері. Якщо інший клієнт (або той же), посилає той же запит, проксі відповідає йому зі свого кеша замість того щоб ще раз звертатися до Інтернету. Це допомагає зменшити трафік між вами і Інтернетом.

Типи проксі-серверів

Типи базових проксі

- Пересилаючий проксі (forwarding proxy)
  Клієнт називає специфічні послуги, до яких він хоче мати доступ. Проксі бере запити з внутрішньої мережі і пересилає їх в Інтернет.
- DNS проксі
  Спеціалізований пересилаючий проксі, який пересилає DNS запити до зовнішнього DNS сервера і повертає результат клієнтові.

- Відкритий проксі (open proxy)
  Может пересылать пакеты из внутренней сети в Интернет и наоборот.
- Зворотний проксі (Reverse proxy)
  Отримує запити з Інтернету і направляє їх у внутрішню мережу.

Коли використовується зворотний проксі, зовнішній клієнт може навіть не знати про існування внутрішньої мережі.

Зворотний проксі дає додатковий рівень безпеки для вашої мережі. Ви можете як звичайно налаштувати зворотний проксі для роботи з кодуванням/декодуванням для серверів, які це підтримують. Зворотний проксі може так само забезпечувати балансування навантаження, коли підтримується безліч веб-сервісів.

NAT

Раніше в курсі ми розглядали NAT. Функціональність NAT зазвичай реалізується на роутері в периметр-мережі, особливо в маленьких мережах.

Ми швидко згадаємо необхідність використання NAT. Так як доступні публічні IPv4 адреси стають дефіцитними, стало звичним використання приватних адрес всередині локальних мереж. Тим не менш, вони не можуть бути використані в Інтернеті, тому приватні адреси повинні бути переведені в публічні адреси для інтернет-трафіку.

Розглянемо базовий функціонал NAT (Рисунок 6.12).

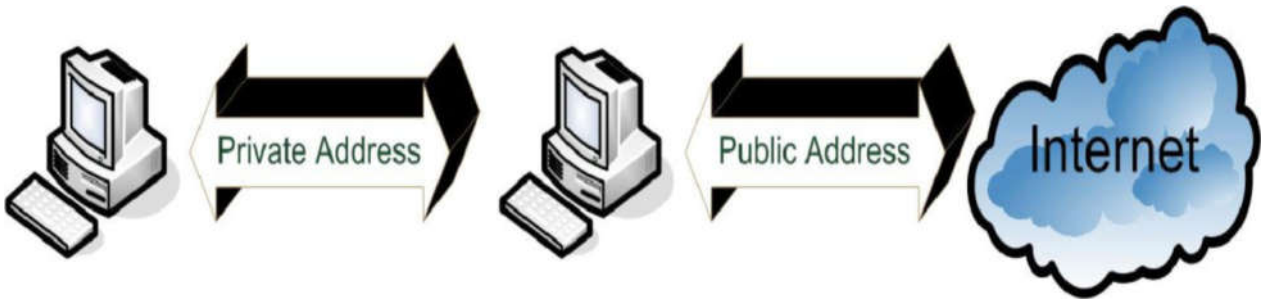


Рисунок 6.12: NAT

Пакети, що надходять з транспортного рівня TCP\IP для передачі, містять адресу джерела і місця призначення. Багато мереж використовують приватні адреси всередині мереж, але це може викликати великі проблеми. Приватний адреси не можуть бути використані в Інтернеті.

Щоб обійти це, пакети надсилатися через NAT сервер. NAT замінює IP адреса джерела публічним адресою і посилає його в Інтернет. Коли відповідь (або підтвердження) повертається назад, NAT здійснює зворотний процес. Публічний адреса замінюється оригінальним приватним адресою, і пакет надсилається оригінальному джерелу.

VPN

Ми розглядали VPN раніше в курсі. Але вони заслуговують додаткового розгляну, так як роутери використовують як кінцеві VPN точки, коли VPN

закінчується LAN. VPN можуть бути використані в LAN-to-LAN конфігураціях як захищені канали між мережами (Рисунок 6-13).

В цьому випадку, роутери використовуються як кінцеві точки на обох кінцях.

Рисунок 6-13: LAN-to-LAN VPN

Інша можливість використання VPN як підтримки віддаленого захищеного доступу в PC-LAN конфігурації (Рисунок 6-14). Роутер поводиться як кінцева точка на кінці LAN до VPN. PC налаштований як кінцева VPN точка на іншому кінці. Кінцеві LAN точки можуть бути налаштовані так, щоб підтримувати множинні одночасні віддалені з'єднання. Ви можете конфігурувати кінцеву точку в центральному офісі, щоб забезпечити віддалений доступ і до PC і до LAN.

Рисунок 6-14: PC-to-LAN VPN

У захищених VPN, кінцеві точки автентифіковані перед тим як тунелі розгортаються. Захищене з'єднання, в більшості ситуацій, забезпечується через кодування інформації. Зазвичай, VPN з'єднання прозорі для кінцевого користувача.

Найбільш поширеним тунельним протоколом є L2TP. Він має схожу функціональність з більш старим протоколом PPTP, який до цих пір використовується деякими програмами.

L2TP *(Тунельний протокол 2-го рівня, Layer 2 Tunneling Protocol) Популярний VPN тунельний протокол.*

PPTP *(Тунельний протокол точка-точка, Point-to-Point Tunneling Protocol) Старий тунельний протокол, який все ще використовується.*

L2TP популярний вибір для реалізації VPN. Проте, присутня потенційна проблема, так як L2TP сам по собі не надає підтримки для сильної аутентифікації або захисту інформації. Ви можете додати ці необхідні додатки, використовуючи IPsec разом з L2TP.

IPsec *(Internet Protocol Security)*
Набір протоколівя. щзо надають аутентифікацію і шифрування.

IPsec реалізований на Інтернет рівні TCP/IP моделі. Плюси цього додатка полягають в тому, що програми не повинні спеціально розроблятися для використання IPsec. Безпека застосовується до даних на вихід і віддаляється на зворотному шляху.

Перевага використання L2TP с IPsec полягає в забезпеченні безпеки між хостом-джерелом і хостом-місцем призначення. PPTP забезпечує безпеку тільки між двома кінцевими VPN точками.

Висновки:

У цьому розділі ви вивчили:

- Основну функціональність роутерів і їх використання.
- Software проти hardware роутерів.
- Призначення та мета таблиць маршрутизації і деталі маршруту.
- Протоколи маршрутизації та їх використання.
- Спеціалізовані роутери і їх використання.

Заключення

Завдяки виникненню і розвитку мереж передачі даних з'явився новий, високоефективний спосіб взаємодії між людьми. Комп'ютерні мережі стали проникати буквально в усі сфери людської діяльності. При цьому більшість мереж існують незалежно один від одного, вирішуючи конкретні завдання для конкретних груп користувачів. Відповідно до цих завдань вибираються ті чи інші мережеві технології і апаратне забезпечення.

Побудувати універсальну фізичну мережу світового масштабу з однотипної апаратури просто неможливо, оскільки така мережа не може задовольняти потреби всіх її потенційних користувачів. Одним потрібна високошвидкісна мережа для з'єднання машин в межах будівлі, а іншим - надійні комунікації між комп'ютерами, рознесеними на сотні кілометрів.

Щоб забезпечити ефективну роботу компанії в умовах економіки ідей, відділ IT повинен перетворитися з центру витрат до відділу, який створює додану вартість. Створення і втілення нових ідей, бізнес-моделей, рішень і методів зажадає використання нових видів програмного забезпечення або додатків, обліку нових ризиків, реалізації нових способів створення, експлуатації та використання технології, яка тепер не просто підтримує бізнес, але САМА Є бізнес.

Hewlett Packard Enterprise допомагає замовникам в побудові ефективної, продуктивної і безпечної IT-середовища за допомогою з'єднання традиційних підходів з новими, що дозволяє компаніям швидко реагувати на ідеї створюючи, використовуючи і розвиваючи нові рішення на основі кращого досвіду і промінь ших бізнес-моделей.

Hewlett Packard Enterprise допомагає вибрати і впровадити обчислювальні потужності, які можуть мати значний вплив на результати і ефективність бізнесу, побудувати сховище, здатне «думати» в не меншому ступені, ніж зберігати, використовувати мережі, здійснюють обмін даних швидше і безпечніше, ніж будь-коли.

Література

1. FRANK MILLER. Designing & Deploying Network Solutions for Small and Medium Business. Instructor Textbook Rev. 1.0. – 2014. – 602 p.

2. Designing & Deploying Network Solutions for Small and Medium Business. Student Lab Guide Rev. 1.0. – 2014. – 125 p.

3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 4-ое издание. Издательство: Питер – 2010 – 944 с.

Міністерство освіти і науки України
Державний університет
телекомунікацій

Гніденко М.П., Вишнівський В.В., Сєрих С.О.,
Зінченко О.В., Прокопов С.В.

Конвергентна мережна інфраструктура

Навчальний посібник

Формат 60х84/16. Наклад 100 прим.
Ум.-друк. арк. 10.5
Друк цифровий. Папір офсетний.Підписано до
друку 20.08.2019 р.
Замовлення № 14800

Надруковано з макету замовника
Друкарня ФОП Гуляєва В.М.
Свідоцтво суб'єкта видавничої справи ДК № 6205
Київська обл., м. Обухів, вул. Малишка, 5
044 495 0279, 050 496 0279
drukaryk.com