Міністерство освіти і науки України
Західноукраїнський національний університет
Факультет комп’ютерних інформаційних технологій

Методичні вказівки до проведення лабораторних занять з дисципліни «Комп'ютерні мережі»

для студентів
освітнього ступеня бакалавр
спеціальності 123 «Комп’ютерна інженерія».

2023

Мельник Г.М. Методичні вказівки до проведення лабораторних занять з дисципліни «Комп'ютерні мережі» для студентів спеціальності 123 «Комп’ютерна інженерія» Тернопіль: ЗУНУ, 2023. 78 с.

Укладачі: Г.М. Мельник, к.т.н., доцент

Відповідальний за випуск: Дубчак Л. О, к.т.н., доцент

Рецензенти: Трембач Р.Б. - к.т.н., доцент кафедри автоматизації технологічних процесів та виробництв Тернопільського національного технічного університету ім. Івана Пулюя;
Биковий П.Є., к.т.н., доцент кафедри інформаційно-обчислювальних систем та управління Тернопільського національного економічного університету.

Методичні рекомендації затверджено на засіданні кафедри «Комп’ютерна інженерія»
протокол № 7 від 30 січня 2023 р.

ЗМІСТ

ЛАБОРАТОРНА РОБОТА 1
ВИВЧЕННЯ МЕРЕЖНИХ ЗАСОБІВ ОПЕРАЦІЙНИХ СИСТЕМ

Мета роботи: Ознайомитися із вбудованими інструментальними засобами операційних систем налагодження зв'язності й діагностики мережі.

ТЕОРЕТИЧНІ ВІДОМОСТІ.

1.1 Інтерфейс командного рядка CLI

Windows також має інтерфейс командного рядка (CLI, «консоль»), cmd.exe, для управління системою командами з консолі або запуску сценаріїв, званих «командними файлами» (з розширеннями cmd), заснованими на «пакетних» (batch) файлах MS-DOS. Синтаксис Windows CLI не дуже добре задокументований у вбудованій системі допомоги. Докладнішу загальну інформацію можна отримати, набравши в командному рядку «help» для отримання загальних відомостей про доступні команди і «ім'я команди /?».

Інтерфейс командного рядка доступний як у вигляді вікна, так і в повноекранному вигляді (перемикання між ними здійснюється натисненням Alt+Enter), вигляд, що віддається перевага, можна вказати у відповідному діалозі настройки, разом з такими параметрами, як розмір і тип шрифтів і т. д. При роботі в даному режимі користувач може викликати попередні команди (так, клавіша «вгору» повертає попередню команду), використовувати автодоповнення імен файлів і каталогів, а також команд. Багато дій з управління операційною системою можна виконати, використовуючи інтерфейс CLI. Найважливішими з них є команди:

– «**net**» з підкомандами, що дозволяє управляти локальними користувачами і групами («net user /?» і inet localgroup /?"), аккаунтами, загальним доступом до ресурсів на ПК («net share /?») і в мережі («net view /?») і т. д.

– Команди перегляду і управління процесами «**tasklist** /?» і «**taskkill** /?»

– Команда управління дозволами файлів " **cacls** /? ", що дозволяє переглядати і змінювати права доступу до файлів і тек (у Home Edition – це єдина можливість гнучко змінювати має рацію, оскільки відповідний графічний інструмент доступний тільки в безпечному режимі)

– а також команди, аналогічні командам «Командної мови» DOS, дозволяють копіювати, переміщати і видаляти файли і каталоги і т. д.

– **ping** – це службова комп'ютерна програма, призначена для перевірки з'єднань в мережах на основі TCP/IP.

Утиліта Ping.

Утиліта Ping відправляє запити Echo-Request протоколу ICMP зазначеному вузлу мережі й фіксує відповіді (ICMP Echo-Reply). Час між відправленням запиту й одержанням відповіді (RTT, від англ. Round Trip Time) дозволяє визначати *двосторонні затримки* (RTT) у маршруті й частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв.

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

Програма ping є одним з основних діагностичних засобів у мережах TCP/IP і входить у поставку всіх сучасних мережевих операційних систем. Функціональність ping також реалізована в деяких вбудованих ОС маршрутизаторів, доступ до результатів виконання ping для таких пристроїв за протоколом SNMP визначається RFC 2925 (Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations).

Практичне застосування:

– можна взнати IP-адресу по доменному імені;
– можна перевірити, чи є зв'язок з сервером;
– перевірити якість каналу, подивившись, скільки пакетів не дійшло або час відклику.

Термін пінг зазвичай використовується для опису передачі будь-якого повідомлення або сигналу з метою виявлення і тестування мережевих послуг або функцій. Наприклад, пінг може бути надіслано за допомогою User Datagram Protocol (UDP) до пристрою, розташованого за транслятор мережевих адрес (NAT), щоб порт обов'язковими для NAT по тайм-ауту та видалення відображення. Інші приклади короткі або порожні миттєві повідомлення, електронну пошту, голосову пошту, або пропущених викликів, повідомлення, щоб вказати, доступність. У різних мережевих багатокористувацьких ігор, ping

відеоігри виконує аналогічні функції, як ping програми для Інтернет-трафіку. Ігровий сервер вимірює час, необхідний для гри пакет для досягнення клієнта і відповідь буде отримана. Цей час прийому-передачі, як правило, називають, як ping гравця.

Утиліта tracert

Tracert - це службова комп'ютерна програма, призначена для визначення маршрутів прямування даних в мережах TCP / IP. Traceroute може використовувати різні протоколи передачі даних в залежності від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE. Комп'ютери, зі встановленою операційною системою Windows використовують ICMP протокол, при цьому маршрутизатори Cisco - протокол UDP.

1.4 **Утиліта ipconfig**

Ipconfig - утиліта командного рядка для управління мережевими інтерфейсами (налаштування, перевірка).

В операційних системах Microsoft Windows ipconfig - це утиліта командного рядка для виводу деталей поточного з'єднання і управління клієнтськими сервісами DHCP і DNS. Також є подібні графічні утиліти з назвами winipcfg і wntipcfg (остання передувала ipconfig). Утиліта ipconfig дозволяє визначати, які значення конфігурації були отримані за допомогою DHCP, APIPA або іншої служби IP-конфігурування або задані адміністратором вручну.

Часто в операційних системах Linux і UNIX деталі з'єднання відслідковуються декількома утилітами, головною серед них є ifconfig. Тим не менш, ipconfig поряд з ifconfig присутній в Mac OS X, там ipconfig команда сервісу як оболонка до агента IPConfiguration і може використовуватися для контролю BootP і DHCP клієнта з CLI.

Утиліта netstat

Утиліта netstat визначення кількості *відкритих сесій*. Також показує вміст різних структур даних, пов'язаних з мережею, в різних форматах в залежності від зазначених опцій.

Використання

Перша форма команди показує список *активних сокетів* (sockets) для кожного протоколу. Друга форма вибирає одну з декількох інших мережевих структур даних. Третя форма показує динамічну статистику пересилання пакетів по сконфігурованим мережевим інтерфейсами; аргумент інтервал задає, скільки секунд збирається інформація між послідовними показами. Значення за замовчуванням для аргументу система - / unix; для аргументу core як значення за замовчуванням використовується / dev / kmem.

Функція ARP. Визначення параметрів канального рівня.

Опис протоколу було опубліковано в листопаді 1982 року в RFC 826. ARP був спроектований для випадку передачі IP-пакетів через сегмент Ethernet. При цьому загальний принцип, запропонований для ARP, може, і був використаний і для мереж інших типів.

Існують такі типи повідомлень ARP: запит ARP (ARP request) і відповідь ARP (ARP reply). Система-відправник за допомогою запиту ARP запитує фізичну адресу системи-одержувача. Відповідь (фізичну адресу вузла-одержувача) приходить у вигляді відповіді ARP.

Перед тим як передати пакет мережевого рівня через сегмент Ethernet, мережевий стек перевіряє кеш ARP, щоб з'ясувати, не зареєстрована в ньому вже потрібна інформація про вузол-одержувачі. Якщо такого запису в кеші ARP ні, то виконується широкомовна запит ARP. Цей запит для пристроїв в мережі має наступний зміст: «Хто-небудь знає фізичну адресу пристрою, який володіє таким IP-адресою?» Коли одержувач з цим IP-адресою прийме цей пакет, то повинен буде відповісти: «Так, це мій IP-адресу . Мій фізичний адресу наступний: ... »Після цього відправник оновить свій кеш ARP і буде здатний передати інформацію одержувачу. Нижче наведено приклад запиту і відповіді ARP. <См. внизу сторінки>

Записи в кеші ARP можуть бути статичними і динамічними. Приклад, даний вище, описує динамічну запис кеша. Можна також створювати статичні записи в таблиці ARP. Це можна зробити за допомогою команди:

arp-s <IP-адрес> <MAC-адрес>

Записи в таблиці ARP, створені динамічно, залишаються в кеші протягом 2-х хвилин. Якщо протягом цих двох хвилин сталася повторна передача даних за цією адресою, то час зберігання запису в кеші продовжується ще на 2 хвилини. Ця процедура може повторюватися до тих пір, поки запис в кеші проіснує до 10 хвилин. Після цього запис буде видалена з кеша, і буде відправлений повторний запит

ARP.

ХІД РОБОТИ

1. Виконати команду “Пуск” → “Виконати” → “**cmd”** і натиснути ОК. (Командний режим: будь-яка команда виконана із ключем „/?” – надає всі ключі із їх описами). Виконати в ньому команду “**ipconfig”** з ключем /all. Визначити ім’я комп’ютера, опис мережевої карти, фізичний адрес комп’ютера (MAC-адрес), IP адрес комп’ютера, маску півмережі, основний шлюз та сервер ДНС.
2. Запустити в командному вікні команду **„ping”** з IP адресом сусіднього комп’ютера лабораторії, і визначити затримку між комп’ютерами. Змінити розмір пакета та час затримки і повторити команду. Виконати команду трасування шляху до серверів університету (проксі, поштовий, веб, фтп) при допомозі команди **“tracert”.**
3. Запустити в командному рядку команду **“netstat”** із ключами „-aon”, переглянути всі номера tcp/udp портів на яких працюють служби ОС, визначити номера портів, які використовують програми для під’єднання до зовнішніх серверів (веб,фтп,пошта тощо). Виконати команду **“tasklist”**, яка виводить всі запущені процеси і по параметру PID визначити процеси, які слухають на портах.
4. Виконати команду **“route print”** і переглянути таблицю маршрутизації ОС, додати запис в таблицю маршрутизаці при допомозі команди **“route add”**, а потім видалити цей запис командою **“route del”.**
5. Виконати команду **“arp”** із різними ключами і переглянути таблиці відповідності MAC та IP адрес.
6. При допомозі командного режиму відіслати повідомлення на сусідній комп’ютер, за допомогою команди net send 10.xx.xx.xx.
7. Створити у редакторі (наприклад блокнот) файл із розширенням **.cmd** і помістити у нього всі команди (ping, tracert, ipconfig, route, netstat, tasklist). Цей командний файл має питати IP-адресу, яка буде пінгуватись і проходити трасування, а також автоматично вибирати і виводити імена служб які слухають на портах tcp/udp. Також командний файл має виводити результат виконання в файл звіту.
8. Результати оформити в звіт і роздрукувати.

ЗМІСТ ЗВІТУ

3.1. Тема та мета лабораторної роботи;
3.2. Хід роботи із копіями екрану;
3.3. Висновки.

КОНТРОЛЬНІ ЗАПИТАННЯ.

4.1. Призначення команди ping;
4.2. Призначення команди tracert;
4.3. Призначення команди ipconfig;
4.4. Призначення команди route;
4.5. Призначення команди netstat;
4.6. Призначення команди tasklist;
4.7 Адресація вузлів мережі для стеку протоколів TCP/IP

ЛАБОРАТОРНА РОБОТА № 2.

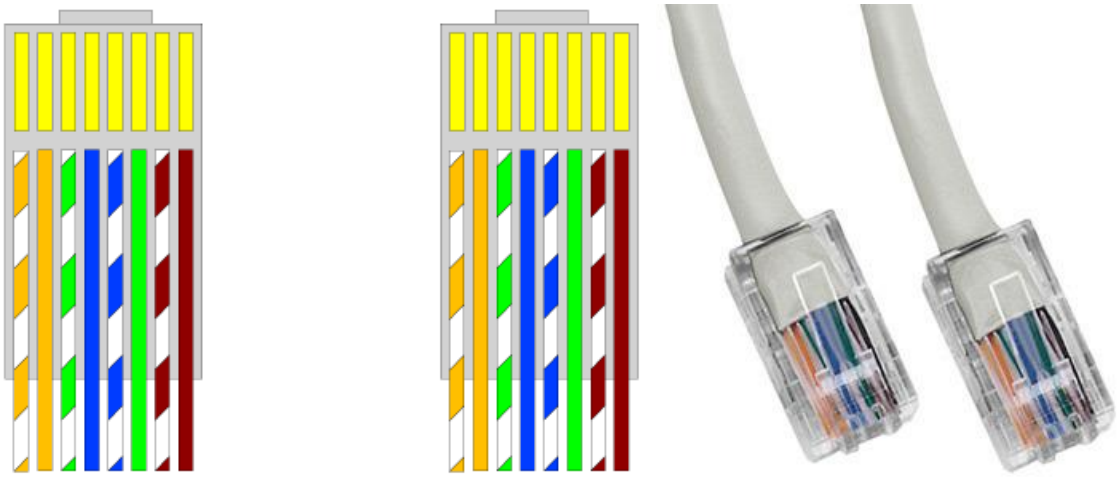
Створення мережі між двома комп'ютерами.

Мета: створити, налаштувати та перевірити мережу між двома комп'ютерами

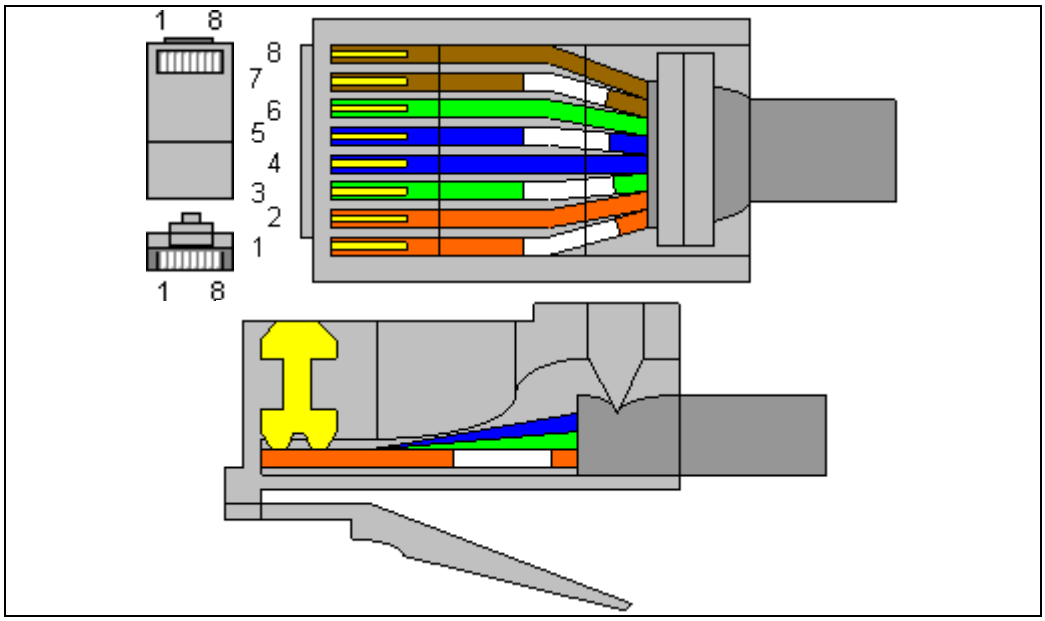
1 ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1 Прямий (Straight-through) порядок обтиску витої пари

1. Прямий (Straight-through) порядок обтиску кручений пари, яка веде від робочої станції до концентратора. Нижче представлений варіант прямого кабелю 568B-568B. Зараз в основному тільки ці кабелі використовуються в якості всіляких пасивне. Є ще варіант 568A-568A. Обидва варіанти описані в таблиці.

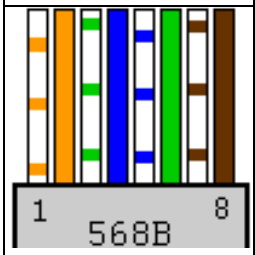
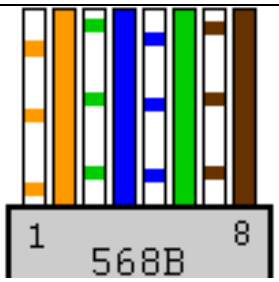


Для стандарту Ethernet 100Base-T використовуються чотири жили (помаранчева і зелена пара), а решту чотири зарезервовані для стандарту Gigabit Ethernet (1000Base-T). Є два варіанти розведення 568A або 568B. Найчастіше використовується варіант 568B, як було зазначено раніше.



Зовнішній вигляд і будова коннектора RJ-45 з нумерацією роз'ємів

Розведення кабелю для з'єднання комп'ютера з мережевим обладнанням (патч-корду) представлена в таблиці, на малюнках зображений зовнішній вигляд кабелю, підготовленого до вставки в коннектор (обидва коннектора обжимаються однаково):

EIA/TIA-568B	перший	колір провода	другий	EIA/TIA-568B	перший	колір провода	другий
	1	біло-оранжевий (TX+)	1		1	біло-оранжевий (TX+)	1
	2	оранжевий (TX-)	2		2	оранжевий (TX-)	2
	3	біло-зелений (RX+)	3		3	біло-зелений (RX+)	3
	4	синій	4		4	синій	4
	5	біло-синій	5		5	біло-синій	5
	6	зелений (RX-)	6		6	зелений (RX-)	6
	7	біло-коричневий	7		7	біло-коричневий	7
	8	коричневий	8		8	коричневий	8

1.2 Crossover cable

2. Кросовер (перехресний, кроссоверним, crossover) порядок обтиску витої пари. Застосовується в разі, коли потрібно з'єднати між собою 2 концентратора, що не мають перемикання uplink / normal, а також для прямого з'єднання 2-х комп'ютерів. Часто кроссоверний кабель не потрібен, тому що сучасні пристрої автоматично визначають, чи потрібно зробити кросовер. Нижче представлена картинка одного з варіантів обтискача кросовера: перший коннектор обжатий як 568B, другий як 568A (Рисунок 1.2.1)

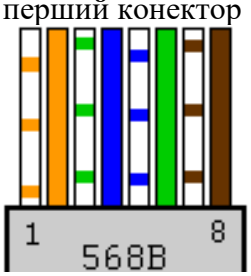
EIA/TIA-568B	перший	колір провода	другий	колір провода	EIA/TIA-568A
перший конектор 	1	біло-оранжевий (TX+)	3	біло-зелений (RX+)	другий конектор 
	2	оранжевий (TX-)	6	зелений (RX-)	
	3	біло-зелений (RX+)	1	біло-оранжевий (TX+)	
	4	синій	4	синій	
	5	біло-синій	5	біло-синій	
	6	зелений (RX-)	2	оранжевий (TX-)	
	7	біло-коричневий	7	біло-коричневий	
	8	коричневий	8	коричневий	

Рисунок 1.2.1

1.3 Зєднання двох комп’ютерів в средовищі Packet Tracer

На рисунку 1.3.1. представлено Головне вікно Cisco Packet Tracer, розділене на області.
Пояснення
1. Головне меню програми з наступним змістом:

- Файл - містить операції відкриття / збереження документів;
- Виправлення - стандартні операції "копіювати / вирізати, скасувати / повторити";
- Настройки;
- Вид - масштаб робочої області і панелі інструментів;
- Інструменти - колірна палітра і кінцеві пристрої;
- Розширення - майстер проектів;
- Допомога;

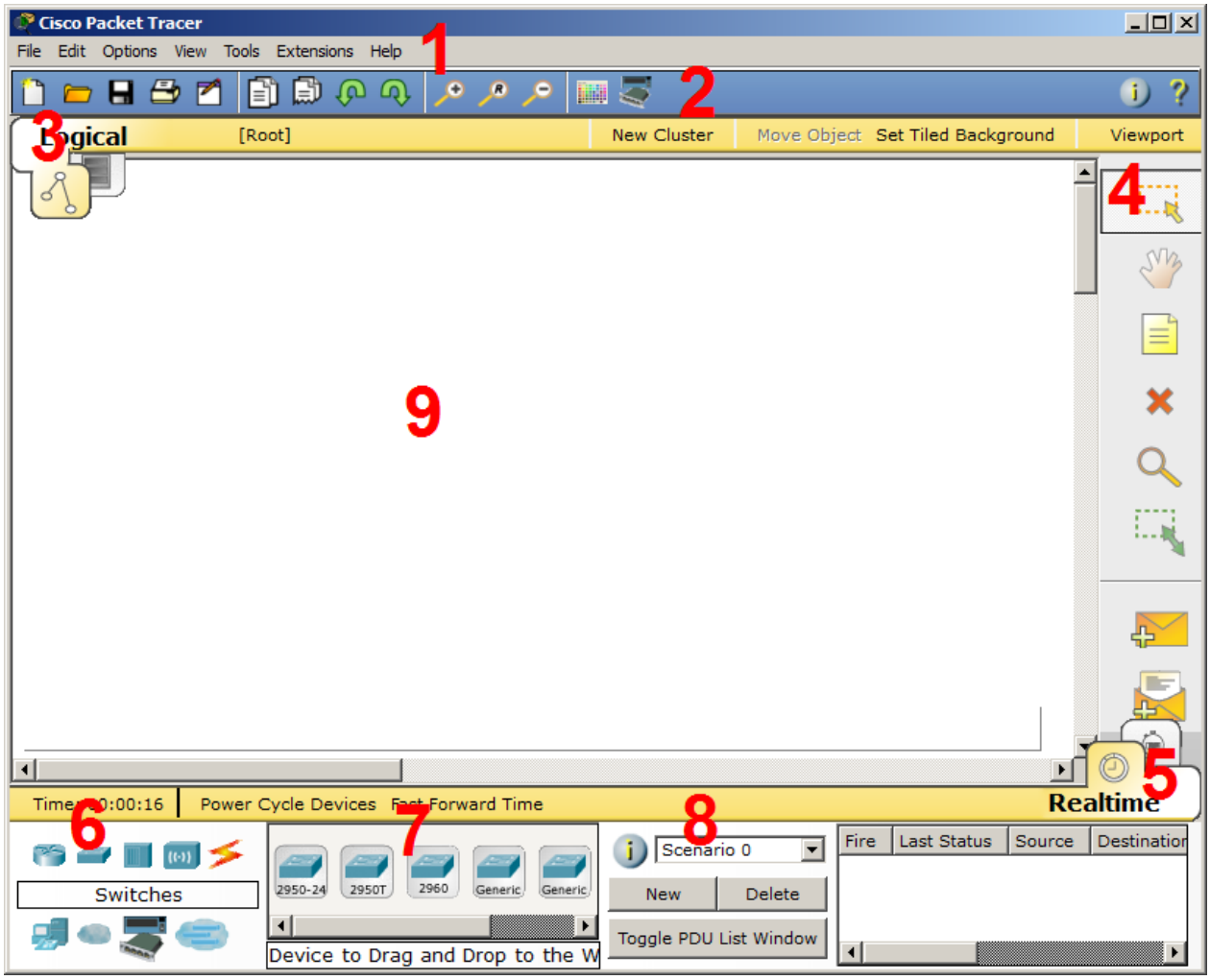


Рис. 1.3.1. Інтерфейс програми Cisco Packet Tracer.

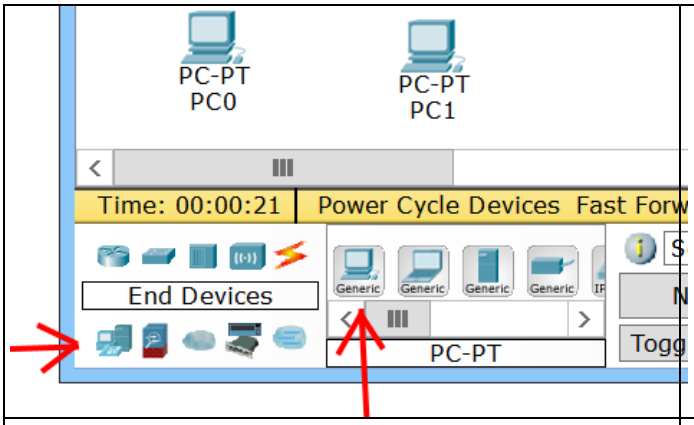
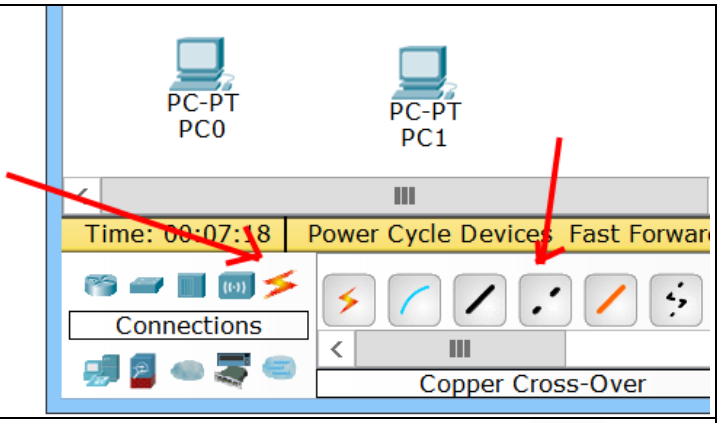
2. Панель інструментів, частина яких просто дублює пункти меню;
3. Перемикач між логічного і зниження фізичної організацією;
4. Ще одна панель інструментів, містить інструменти виділення, видалення, переміщення, масштабування об'єктів, а так само формування довільних пакетів;
5. Перемикач між реальним режимом (Real-Time) і режимом симуляції (Simulation);
6. Панель з групами кінцевих пристроїв і ліній зв'язку;
7. Самі кінцеві пристрої, тут містяться всілякі комутатори, вузли, точки доступу, провідники.
8. Панель створення призначених для користувача сценаріїв;
9. Робочий простір.

Приклад виконання роботи

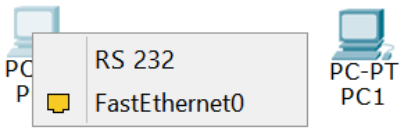
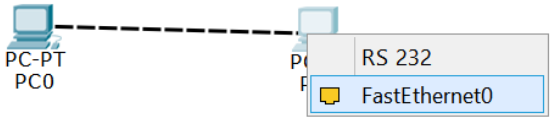
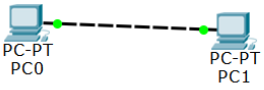
Що потрібно для організації найпростішої мережі?

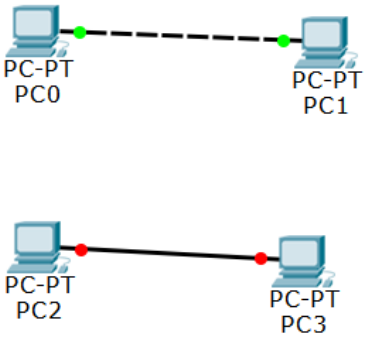
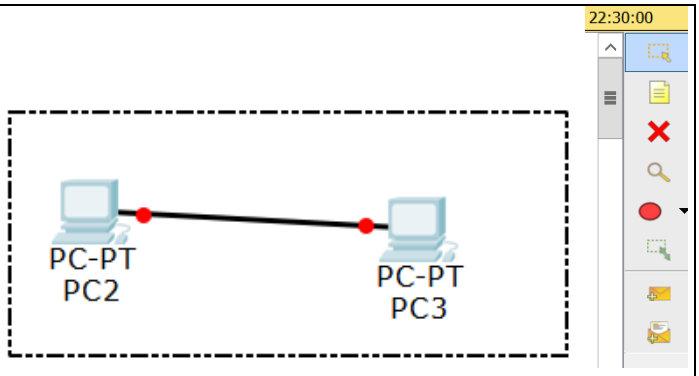
1. Два комп'ютери
2. Патч-Корд

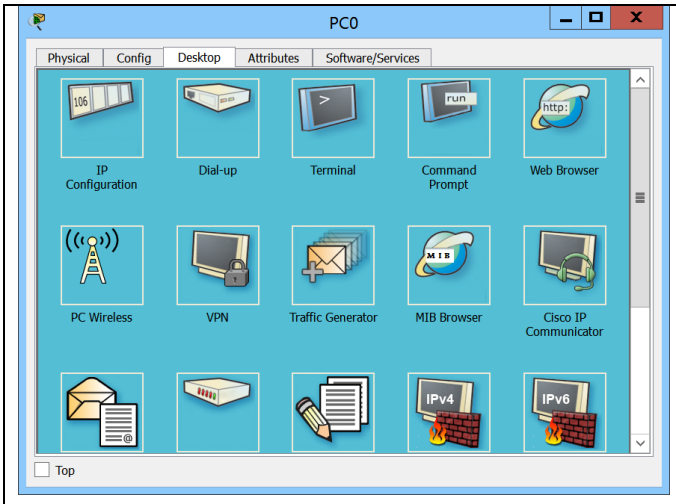
У випадку відсутності патч-корду його необхідно зробити із відрізку витої пари і двох конекторів RJ45. Прямий кабель (стандарт А, стандарт В) з'єднує комп'ютер-комутатор, комутатор-маршрутизатор. Кросовер кабель з'єднує комп'ютер-комп'ютер, комутатор-комутатор, маршрутизатор-маршрутизатор. Тобто, кросовер кабель використовується для одного рівня моделі OSI.

	
1) Переходимо в Packet Tracer, і в групі **end devices (Конечные устройства)** вибираємо комп'ютер Generic. І перетягуємо один і другий в робочий простір.	2) Переходимо на вкладку Connnections  Packet Tracer зобов'язує нас використовувати кросовер кабель для одного рівня OSI. Тому вибираємо кросовер кабель  .

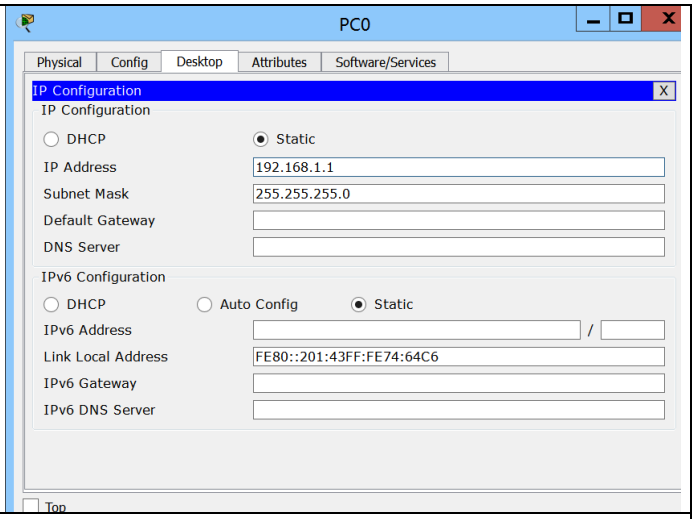
Кожен компютер в програмі представлений як і реальний своїми компонентами та засобами операціної системи. Якщо клацнути на нього зявиться вікно із зміни його компонентів Physical, Config, програмами налаштування Desktop. Крім того якщо в даний час обрано певний тип кабелю, то клацнувши певний присрій зявиться меню де потрібно вибрати певний інтерфейс до якого підключати кабель.

		
3) Клацаємо на значку кабелю  , потім клацаємо на перший комп'ютер і вибираємо інтерфейс FastEthernet0	4) клацаємо на другий комп'ютер і вибираємо інтерфейс FastEthernet0.	5) Кінці кабелю позначились зеленим, що означає що інтерфейс працює (link up).

	
6) Для порівняння можемо спробувати з'єднати два інших комп'ютера прямим кабелем  і побачити що лінки не піднялись.	7) Щоб видалити два нижні комп'ютера виділяємо їх і нажимаємо Delete або клацаємо кнопку  на панелі справа

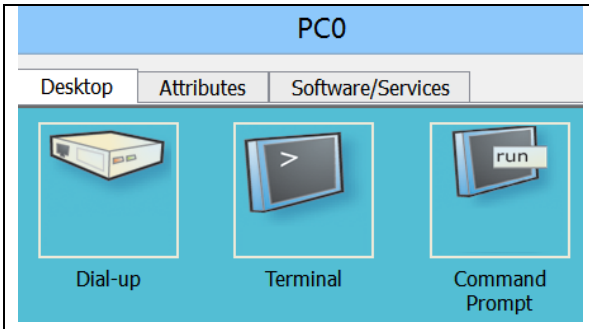


8) Переходимо до налаштування комп'ютера PC0. Одним кліком відкриваємо його налаштування .

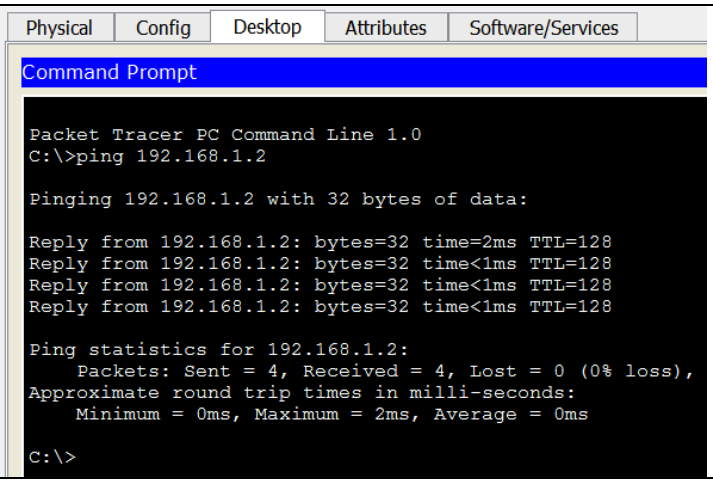


9) Переходимо на вкладку Desktop в ярлик «IP Configuration» і прописуємо IP адресу і маску 192.168.1.1 і 255.255.255.0.

10) Для другого комп'ютера прописуємо адресу 192.168.1.2 і туж саму маску. Тепер нам необхідно перевірити з'єднання на третьому мережевому рівні.



11) На першому комп'ютері в налаштуваннях вибираємо ярлик командної стрічки Desktop -> Command Prompt.



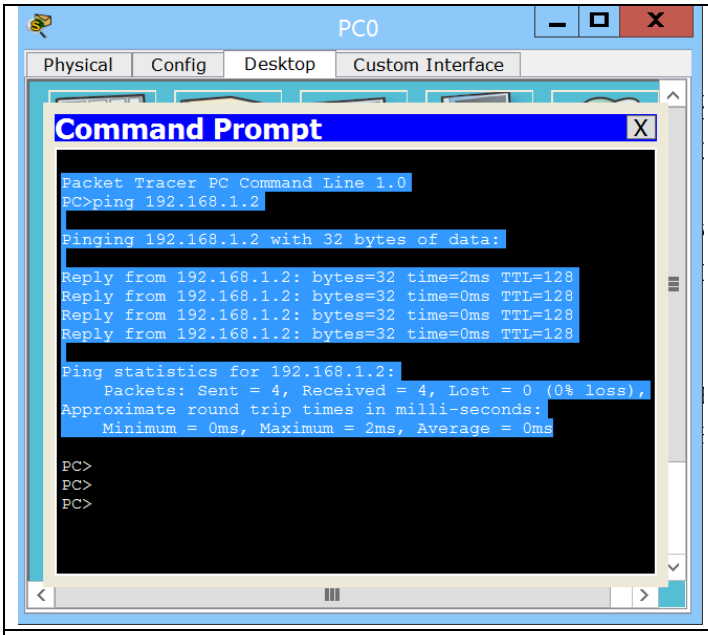
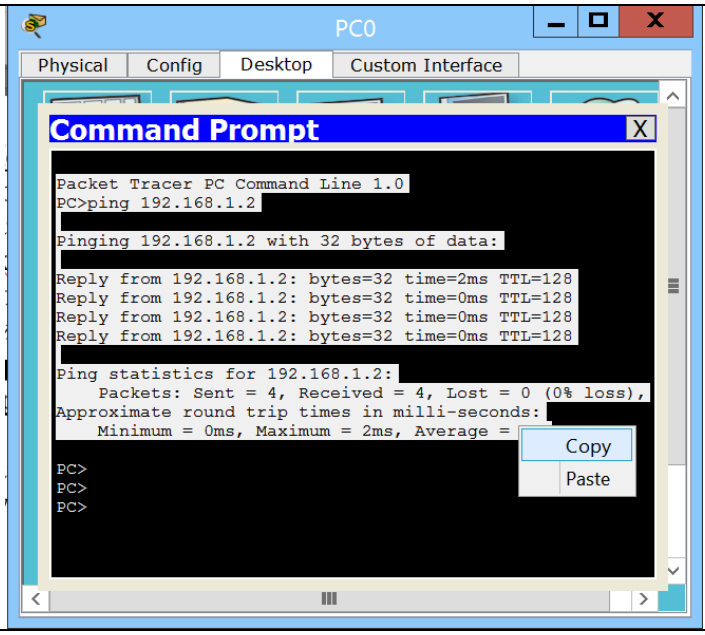
12)Набираємо команду ping і вказуємо IP адресу другого комп'ютера. Тиснемо Enter. В результаті отримуємо успішну відповідь що було послано 4 пакети по 32 байти кожен яких повернувся за менше ніж 2 мс.

Мережева команда

Команда **ping** використовує датаграму ECHO_REQUEST протоколу ICMP, щоб викликати відповідь ICMP ECHO_RESPONSE вказаного хоста або мережевого шлюзу. Якщо хост відповідає, **ping** видає повідомлення, що хост живий (**хост is alive**), в стандартний вихідний потік і завершує роботу. В іншому випадку, після **таймаут** секунд вона видає повідомлення, що від хоста відповіді немає (**no answer from хост**). **Стандартне** значення тайм-ауту - 20 секунд.

Примітка

Із вікна Desktop -> Command prompt (крок 12) текст для звіту і аналізу потрібно копіювати і скопіювати натиснувши праву кнопку і клацнувши Copy із меню. Показано нижче.

	
виділити текст мишкою розтягнувши лівою кнопкою	клацнути праву кнопку і потім клацнути Copy із меню

2 ХІД РОБОТИ

1. Об’єднайте 2 комп’ютери і налаштуйте на двох комп’ютерах мережеві інтерфейси, присвоївши їм відповідні IP-адреси, згідно номеру варіанту (НВ) по шаблону для 1-го ПК - 192.168.НВ.НВ, для 2-го ПК - 192.168.НВ.НВ+1 із маскою 255.255.255.0

Номером варіанту є порядковий номер студента в списку групи!

2. Запустіть команду пінг між комп’ютерами. Скопіюйте результат виконання в звіт.
3. Збережіть проект розробленої схеми в Packet Tracer
4.

3. ЗМІСТ ЗВІТУ

1. Титульна сторінка. Тема та мета лабораторної роботи.
2. Хід виконання лабораторної роботи та копії екранів. Схема мережі.
3. Висновки по виконаній роботі.
4. Файл звіту з лабораторної роботи називати по схемі прізвище_№групи_№лабораторної, наприклад «іваненко_КІ31_2.doc». Аналогічно називати і файл проекту Packet Tracer.

.

ЛАБОРАТОРНА РОБОТА №3.
ВИВЧЕННЯ УСТАТКУВАННЯ ЛОКАЛЬНИХ МЕРЕЖ

Мета: Вивчення специфіки ієрархічної організації мережі Ethernet в середовищі Cisco Packet Tracer

ТЕОРЕТИЧНІ ВІДОМОСТІ

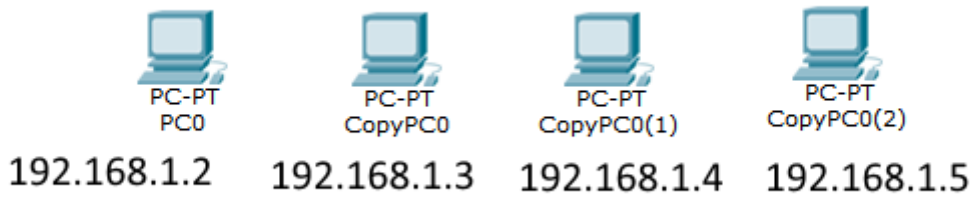
Побудова мережі Проста мережа на основі комутатора

Для того щоб з'єднати більше двох комп'ютерів потрібне мережеве обладнання – спеціалізований пристрій. Для Ethernet є два варіанти – це мережевий концентратор (хаб, hub) або комутатор. Концентратор функціонує на першому рівні моделі OSI. Комутатор (switch) функціонує на другому рівні моделі OSI (L2). Концентратор має цілий ряд недоліків – відсутність безпеки, низька швидкість та інші проблеми. Практично не застосовується сьогодні. Різницю ви можете знати з лекційного матеріалу.

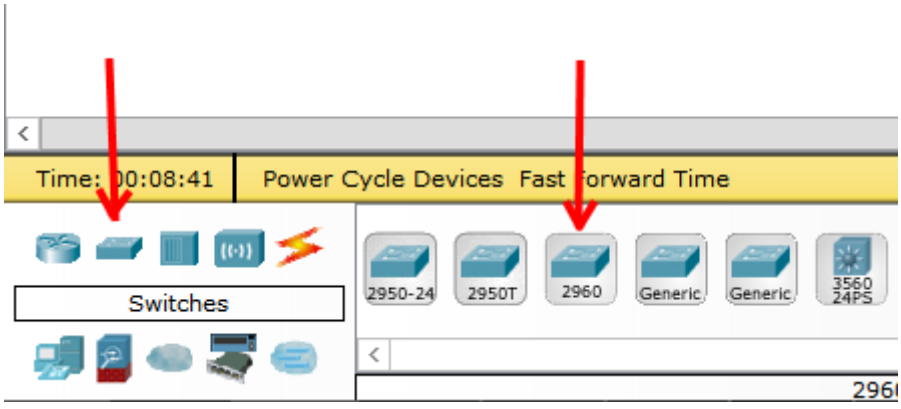
Концентратор відправляє пакети на всі порти. Комутатор відправляє пакети тільки на певні порти на основі MAC адреси отримувача. MAC адреси комп'ютерів комутатор вивчає пасивно спостерігаючи за трафіком.

Створюємо мережу. Розміщуємо компютер End devices -> Generic. Налаштовуємо IP адресу 192.168.1.2. Щоб швидше налаштовувати компюетри затскаємо на клавіатурі Ctrl і перетягуємо із першого компюетра його копію.

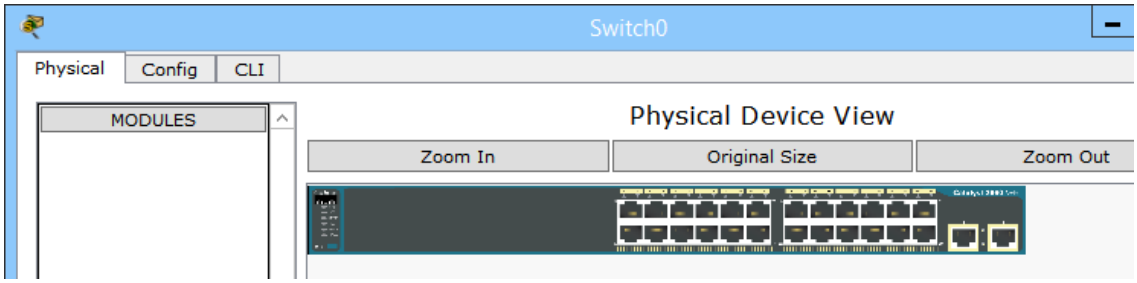
Далі копіюємо ще два рази і виправляємо IP адреси як показано на рисунку. Для кожно комп'ютера просто збільшуємо його номер на одиницю.



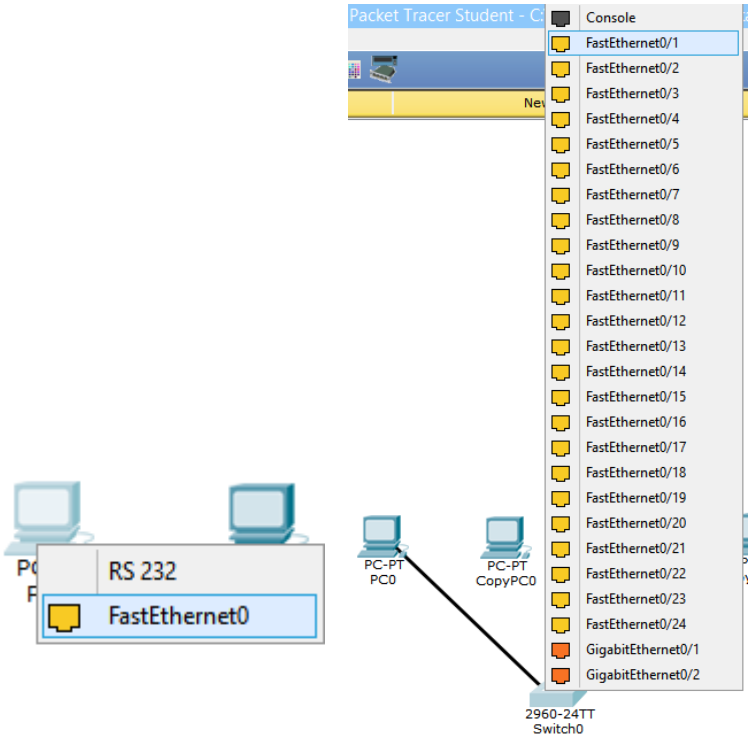
Преходимо в катеорію Switches і вибираємо комутатор 2960



Якщо клацнути комутатор то ми побачимо закладку із фізичним виглядом. Пристрій має 24 порта Fast Etprenet і 2 порта Gigabit Ethernet



Тепер прямим кабелем підключаємо кожен комп'ютер до комутатора. Всі порти комутатора пронумеровані. Кожен порт має номер *N* після знаку дробу (слеш): FastEthernet0/*N*. Під'єднаємо послідовно кожен комп'ютер в порти починаючи з FastEthernet0/1 до FastEthernet0/4.

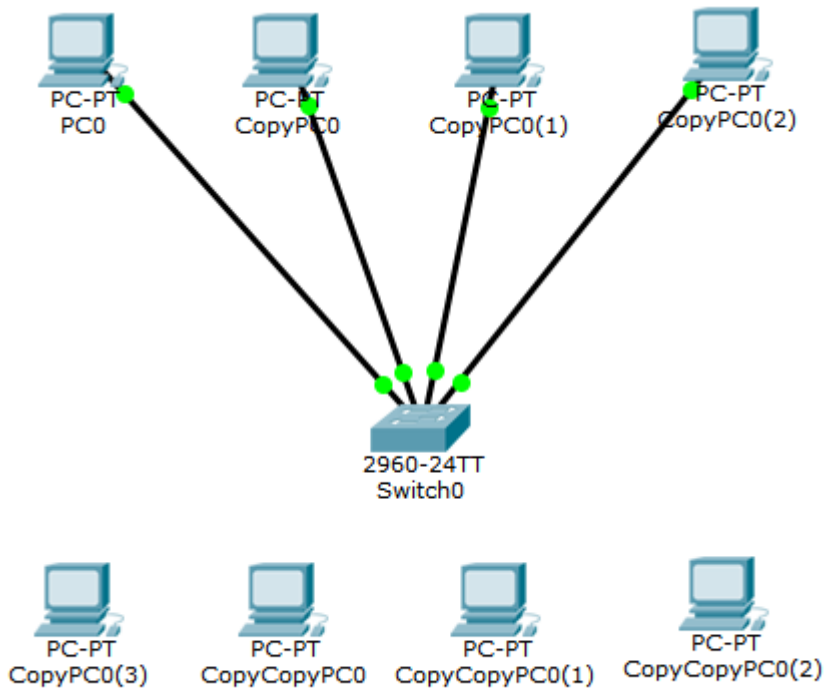


На комп'ютерах лінки зразу загорілись зеленим, а на комутаторі для цього потрібен час. Як тільки всі лінки загорілись мережа готова до роботи. З допомогою команди ping можна перевірити чи пересилаються пакети. На першому комп'ютері PC0 пінгуємо адресу 192.168.1.4 і інші. Отримаємо

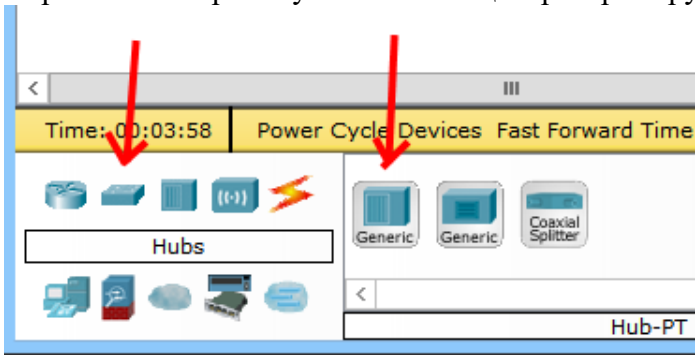
```
PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
```

```
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

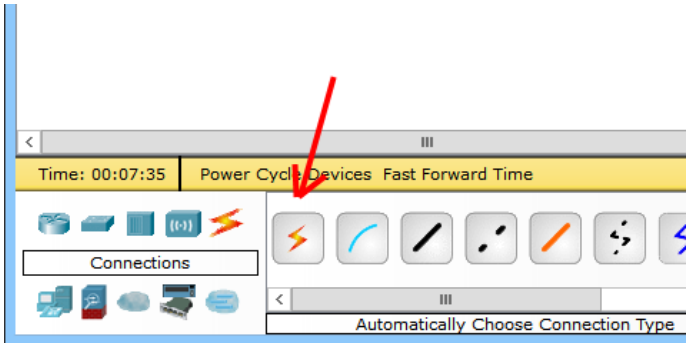
Щоб порівняти із роботою концентратора скопіюємо і вставимо комп'ютери нижче в робочу область через Crtl+C, Ctrl+V.



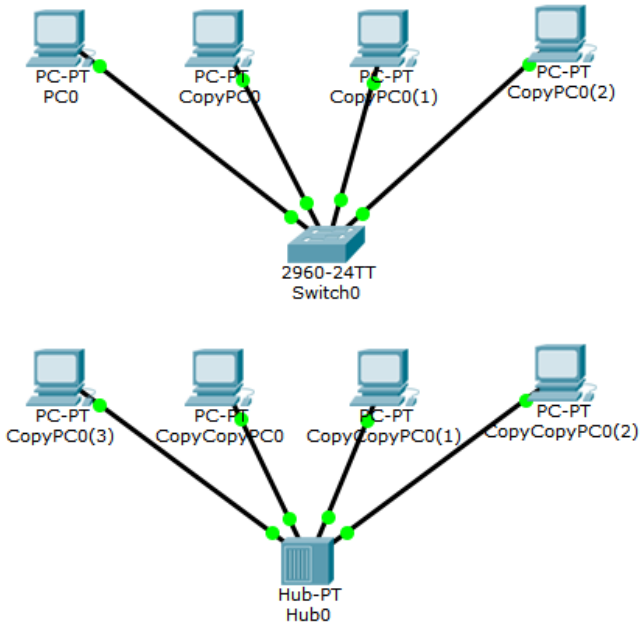
Перетягнемо в робочу область концентратор із групи Hubs -> Generic



З'єднуємо кожен компюетр із концентратором прямим кабеле або з автоматичним вибором кабеля якщо клацати кнопку блискави.

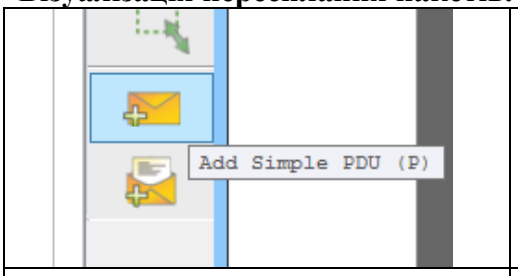
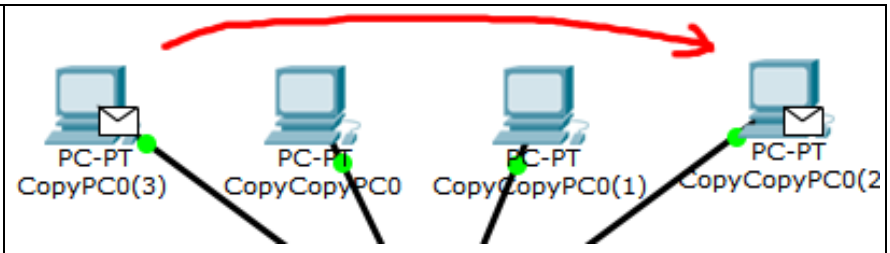


Отримаємо дві мережі

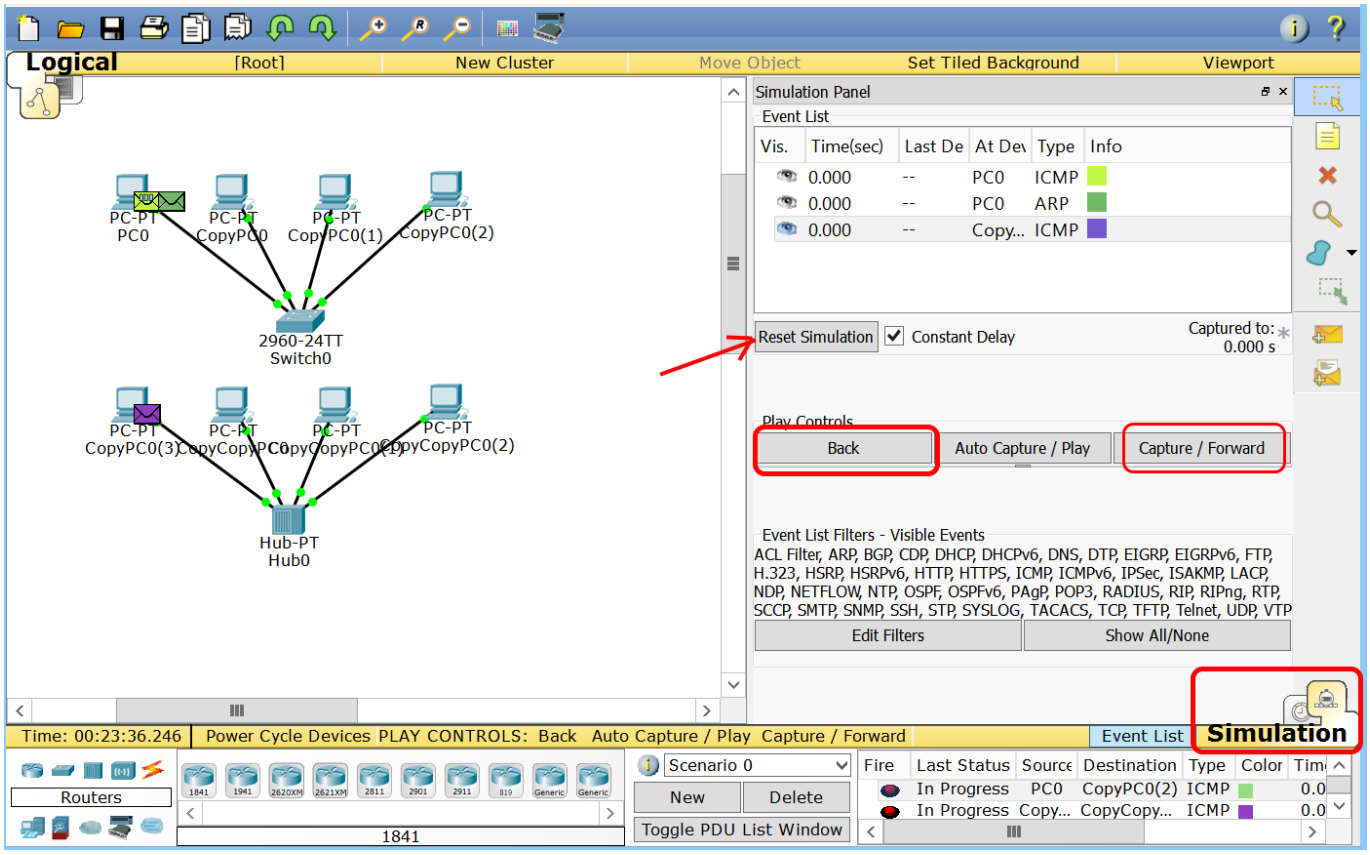


З допомогою команди ping можна перевірити і зв'язок в цій мережі.

Візуалізація пересилання пакетів.

	
Клацнемо кнопку пересилання пакетів Add simple PDU.	Після цього потрібно спочатку клацнути на комп’ютер відправник а потім комп’ютер приймач.

Преключаємся в режим Simulation. Нажимаєм Reset Simulation. Нажимаємо Capture/Forward і спостерігаємо як пакет передається від вузла до пристрою. Нажимаємо Capture/Forward другий раз і бачимо як пакт пердається від пристрою до отримувача.



Як бачимо від концентратора пакет передається всім трьом компютерам, хоча отримувач тільки один. Ми бачимо різницю в роботі між комутатором і концентратором. Можна натиснути Capture/Forward ще два рази і побачаити як передається відповідь. Якщо клацнутина іконку листа, то можна подивитись внутрішню структуру пакету

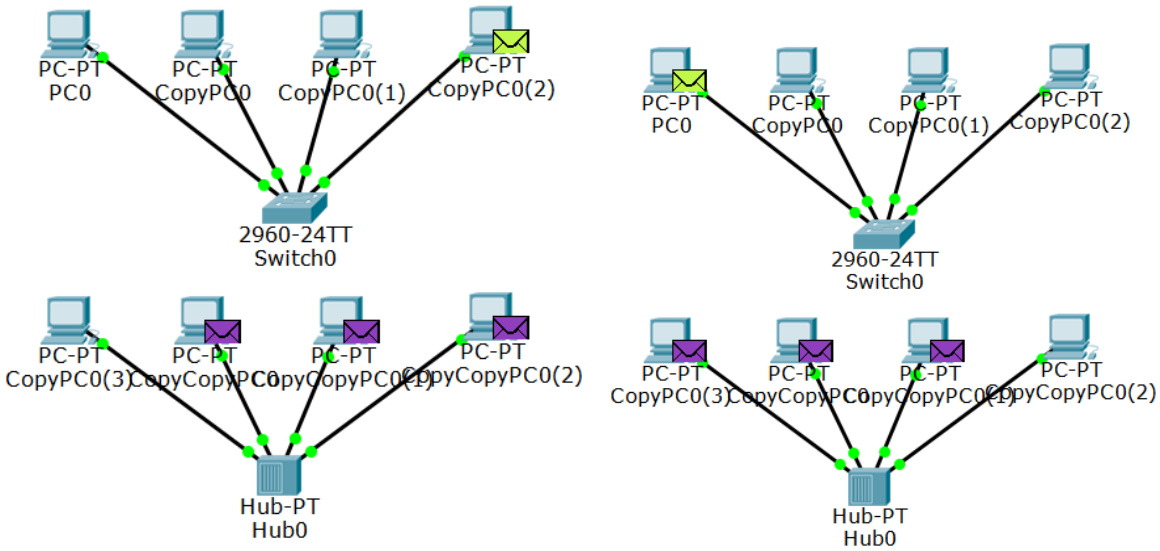


Рисунок 3.1 - Передача повідомлень від джерела жо отримувача і назад

2 ХІД РОБОТИ

1. Побудуйте дві мережі на основі концентратор і комутатора по зразку. Налаштуйте на комп'ютерах мережеві інтерфейси, присвоївши їм відповідні IP-адреси, згідно номеру варіанту (НВ) по шаблону

для 1-го ПК - 192.168.НВ.НВ,
для 2-го ПК - 192.168.НВ.НВ+1
для 3-го ПК - 192.168.НВ.НВ+2
для 4-го ПК - 192.168.НВ.НВ+3

із маскою 255.255.255.0,

Номером варіанту є порядковий номер студента в списку групи!

2. Запустіть команду пінг щоб перевірити зв'язок від першого комп’ютера до трьох інших. Скопіюйте результат виконання в звіт.

3. Збережіть проект розробленої схеми в Packet Tracer

3. ЗМІСТ ЗВІТУ

1. Титульна сторінка. Тема та мета лабораторної роботи.
2. Номер варіанту
3. Хід виконання лабораторної роботи та копії екранів. Схема мережі.
4. Висновки по виконаній роботі.

ЛАБОРАТОРНА РОБОТА № 4
РОЗПОДІЛ АДРЕСНОГО ПРОСТОРУ IP ЗАСОБАМИ МАСКУВАННЯ

Мета: Набути навички розподілу адресного простору

1. ТЕОРЕТИЧНІ ВІДОМОСТІ

Стек протоколів TCP/IP тісно пов'язаний з мережею Internet, її історією і сучасністю. Створений він був в 1969 році, коли для мережі ARPANET знадобився ряд стандартів для об'єднання в єдину мережу комп'ютерів з різною архітектурою і операційними системами. На базі цих стандартів і був розроблений набір протоколів, що отримали назву TCP/IP.

Разом із зростанням Internet протокол TCP/IP завойовував позиції і в інших мережах. На сьогоднішній день цей мережний протокол використовується як для зв'язку комп'ютерів всесвітньої мережі, так і в переважній більшості корпоративних мереж.

В наші дні використовується версія протоколу IP, відома як IPv4. Далі розглянуто стандартну схему адресації і новіші методи раціонального використання адресного простору, введені в результаті виявлених недоліків в реалізації протоколу IP.

1.1 Адресний простір протоколу IP

Згідно специфікації протоколу, кожному вузлу, приєднаному до IP-мережі, привласнюється унікальний номер. Вузол може бути комп'ютером, маршрутизатором, міжмережевим екраном тощо. Якщо один вузол має декілька фізичних підключень до мережі, то кожному підключенню повинен бути привласнений свій унікальний номер.

Цей номер, або по-іншому IP-адреса, має довжину в чотири октети, і складається з двох частин. Перша частина визначає мережу, до якої належить вузол, а друга – унікальна адреса самого вузла усередині мережі.

Номер мережі			Номер вузла
11011100	11010111	00001110	00010110

В класичній реалізації протоколу першу частину адреси називали "мережним префіксом", оскільки вона однозначно визначала мережу. Проте в сучасній реалізації це вже не так і мережу ідентифікують іншим чином, мова про що піде нижче.

Класова адресна схема протоколу IP

Спочатку весь адресний простір розділили на п'ять класів: A, B, C, D і E. Така схема отримала назву "класової". Кожний клас однозначно ідентифікувався першими бітами лівого байта адреси. Самі ж класи відрізнялися розмірами мережної і вузлової частин. Знаючи клас адреси, ви могли визначити межу між його мережною і вузловою частинами. Крім того, така схема давала змогу при маршрутизації не передавати разом з пакетом інформацію про довжину мережній частині IP-адреси.

Клас A				
Номер біту	0	8	16	24 31
Адреса	0.....	.....	.....	.....
Мережева частина				
Клас B				
Номер біту	0	8	16	24 31
Адреса	10.....	.....	.....	.....
Мережева частина				
Клас C				
Номер біту	0	8	16	24 31
Адреса	110.....	.....	.....	.....
Мережева частина				
Клас D				
Номер біту	0	8	16	24 31
Адреса	1110....	.....	.....	.....
Клас E				
Номер біту	0	8	16	24 31
Адреса	1111....	.....	.....	.....

Клас A орієнтований на дуже великі мережі. Всі адреси, що належать цьому класу, мають 8-бітовий мережний префікс, на що вказує перший біт лівого байта адреси встановлений в нуль. Відповідно, на ідентифікацію вузла відведено 24 біти і кожна мережева “вісімка” може містити до 224-2 вузлів. Дві адреси необхідно відняти, оскільки адреси, що містять в правому октеті всі нулі (ідентифікує вказану мережу) і всі одиниці (широкомовна адреса) використовуються для службової цілі і не можуть бути надані вузлам.

Самих же мереж “вісімок” може бути 27-2. Знову віднімаємо двійку, але це вже дві службові мережі: 127/8 і 0/8 (по-старому: 127.0.0.0 і 0.0.0.0).

Нарешті, можна помітити, що клас A містить всього 27 * 224 = 231 адрес, або половину всіх можливих IP-адрес.

Клас B призначений для мереж великого і середнього розмірів. Адреси цього класу ідентифікуються двома старшими бітами, рівними відповідно 1 і 0. Мережний префікс класу складається з шістнадцяти біт або перших двох октетів адреси.

Оскільки два перші біти мережного префікса зайнято визначаючим клас ключем, то можна задати лише 214 різних мереж. Вузлів же в кожній мережі можна визначити до 216-2.

В деяких джерелах, для визначення кількості можливих мереж використовується формула 2x-2 для всіх класів, а не тільки для A. Це зв’язано з певними причинами, які детальніше будуть викладені нижче. На сьогоднішній день немає ніякої необхідності зменшувати кількість можливих мереж на дві.

Провівши обчислення, аналогічні приведеним для класу A, ми побачимо, що клас B займає четвертину адресного простору протоколу IP.

Нарешті, клас мереж, що використовується, – клас C – має 24 бітовий мережний префікс, визначається старшими бітами, встановленими в 110, і може ідентифікувати до 221 мереж. Відповідно, клас дає можливість адресувати до 28-2 вузлів. Займає восьму частину адресного простору протоколу TCP/IP.

Останні два класи займають восьму частину, що залишилася, в адресному просторі і призначені для службового (клас D) і експериментального (клас E) використання. Для класу D старші чотири біти адреси встановлено в 1110, для класу E – 1111. Сьогодні клас D використовується для групової передачі інформації.

Оскільки довгі послідовності з одиниць і нулів важко запам’ятати, IP адреси звичайно записують в десятковій формі. Для цього кожний октет адреси представляється у вигляді десяткового числа. Між собою октети відділяються крапкою. Іноді октети позначаються як w.x.y.z і називаються “z-октет”, “y-октет”, “x-октет” і “w-октет”.

Представлення IP-адреси у вигляді чотирьох десяткових чисел розділених крапками і називається “точково-десяткова нотація”.

Октет	W	X	Y	Z
Номер біту	0	8	16	24 31
Адреса	11011100 220	11010111 215	00001110 14	00010110 22
Точково-десятковий формат	220.215.14.22			

Підсумуємо інформацію про класи мереж в таблиці:

Клас	Кількість мереж	Кількість вузлів	Десятковий діапазон	
A	27 – 2 (126)	224 – 2 (2 147 483 648)	1.xxx.xxx.xxx	- 126.xxx.xxx.xxx
B	214 (16 384)	216 – 2 (65 534)	128.0.xxx.xxx	- 191.255.xxx.xxx
C	221 (2 097 152)	28 – 2 (254)	192.0.0.xxx	- 223.255.255.xxx
D	-	-	224.0.0.xxx	- 239.255.255.xxx
E	-	-	240.0.0.xxx	- 254.255.255.xxx

Зарезервовані адреси

Як вже наголошувалося, в адресній схемі протоколу виділяють особливі IP-адреси.

Якщо біти всіх октетів адреси рівні нулю, то він позначає адресу того вузла, який згенерував даний пакет. Це використовується в обмежених випадках, наприклад в деяких повідомленнях протоколу IP.

Якщо біти мережного префікса рівні нулю, тоді вважається, що вузол призначення належить тій же мережі, що і джерело пакету.

Коли біти всіх октетів адреси призначення рівні двійковій одиниці, пакет доставляється всім вузлам, що належать тій же мережі, що і відправник пакету. Така розсилка називається обмеженим широкомовленням.

Нарешті, якщо в бітах адреси, відповідних вузлу призначення, стоять одиниці, то такий пакет розсилається всім вузлам вказаної мережі. Це називається широкомовленням.

Спеціальне значення має, так само, адреси мережі 127/8. Вони використовуються для тестування програм і взаємодії процесів в межах однієї машини. Пакети, відправлені на цей інтерфейс, обробляються локально, як вхідні. Тому адреси з цієї мережі не можна привласнювати фізичним мережним інтерфейсам.

1.2 Організація підмереж

Дуже рідко в локальну обчислювальну мережу входить більше 100-200 вузлів: навіть якщо взяти мережу з великою кількістю вузлів, багато мережних середовищ накладають обмеження, наприклад, в 1024 вузли. Виходячи з цього, доцільність використовування мереж класу A і B сумнівна. Та і використовування класу C для мереж, що складаються з 20-30 вузлів, теж є марнотратством.

Для вирішення цих проблем в дворівневу ієрархію IP-адрес (мережа – вузол) була введена нова складова – підмережа. Ідея полягає в “запозиченні” декількох бітів з вузлової частини адреси для визначення підмережі.

Повний префікс мережі, що складається з мережного префікса і номера підмережі, отримав назву розширеного мережного префікса. Двійкове число, і його десятковий еквівалент, що містить одиниці в розрядах, що відносяться до розширеного мережного префікса, а в решті розрядів – нулі, назвали маскою під мережі:

		Мережевий префікс		підмережа	вузол
IP адреса	144.144.19.22	10010000	10010000	00010011	00010110
Маска	255.255.255.0	11111111	11111111	11111111	00000000
		Розширений мережений префікс			

Але маску в десятковому вигляді зручно використовувати лише тоді, коли розширений мережний префікс закінчується на межі октетів, в інших випадках її розшифрувати складніше. Припустимо, що ми хотіли б для підмережі використовувати не 8 бітів, а 10. Тоді в останньому (z-ом) октеті ми мали б не нулі, а число 11000000. В десятковому вигляді одержуємо 255.255.255.192. Очевидно, що такий вигляд не дуже зручний. У наш час частіше використовують позначення виду "/xx", де xx – кількість біт в розширеному мережному префіксі. Таким чином, замість вказівки: "144.144.19.22 з маскою 255.255.255.192", ми можемо записати: 144.144.19.22/26. Як видно, такий вигляд компактніший і зрозуміліший.

Маска підмережі змінної довжини VLSM (Variable Length Subnet Mask)

Проте незабаром стало ясно, що підмережі, не дивлячись на всі їх переваги, мають і недоліки. Так, визначивши одного разу маску підмережі, доводиться використовувати підмережі фіксованих розмірів. Скажімо, у нас є мережа 144.144.0.0/16 з розширеним префіксом /23:

		Мережевий префікс		Підмережа	Вузол
144.144.0.0/23	<-->	10010000	10010000	0000000	0 00000000
		Розширений мережевий префікс			

Така схема дає змогу створити 27 підмереж розміром в 29 вузлів кожна. Це підходить до випадку, коли є багато підмереж з великою кількістю вузлів. Але якщо серед цих мереж є такі, кількість вузлів в яких знаходиться в межах ста, то в кожній з них пропадатиме близько 400 адрес.

Рішення полягає в тому, що б для однієї мережі вказувати більше одного розширеного мережного префікса. Про таку мережу говорять, що це *мережа з маскою підмережі змінної довжини* (VLSM).

Дійсно, якщо для мережі 144.144.0.0/16 використовувати розширений мережний префікс /25, то це більше б підходило мережам розмірами близько ста вузлів. Якщо припуститися використовування обох масок, то це б значно збільшило гнучкість застосування підмереж.

Загальна схема розбиття мережі на підмережі з масками змінної довжини така: мережа ділиться на підмережі максимально необхідного розміру. Потім деякі підмережі діляться на дрібніші, і рекурсивно далі, до тих пір, поки це необхідно.

Крім того, технологія VLSM, шляхом приховування частини підмереж, дає можливість зменшити об'єм даних, що передаються маршрутизаторами. Так, якщо мережа 12/8 конфігурується з розширеним мережним префіксом /16, після чого мережі 12.1/16 і 12.2/16 розбиваються на підмережі /20, то маршрутизатору в мережі 12.1 немає чого знати про підмережі 12.2 з префіксом /20, йому достатньо знати маршрут на мережі 12.1/16.

1.3 Безкласова міждоменна маршрутизація CIDR (Classless Inter-Domain Routing)

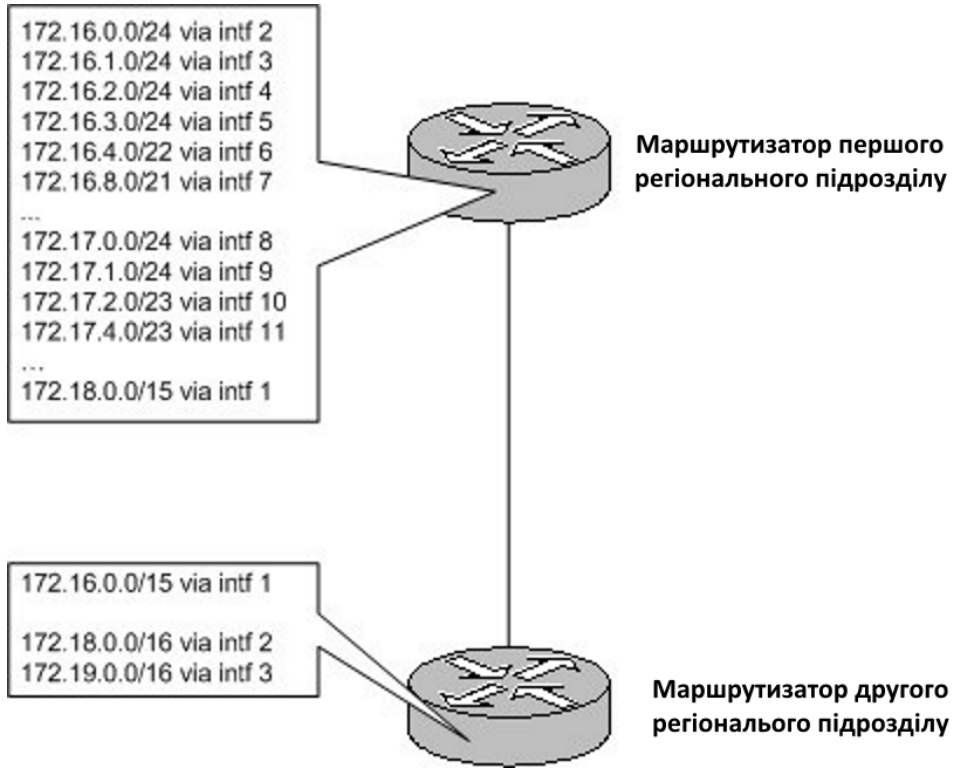
Як рішення проблеми обмеження в 4 мільярди адрес були запропоновані два підходи. Перше рішення –впровадження ***протоколу безкласової маршрутизації*** **(*CIDR*)**, до якого пізніше приєдналася система *NAT*.

Довгострокове рішення – це протокол IP наступної версії. Він позначається, як *IPv6:* довжина адреси збільшена до 16-ти байтів (128 біт)

Технологія CIDR дає змогу піти від класової схеми адресації, ефективно використовувати адресний простір протоколу IP. Крім того, CIDR агрегує маршрутні записи. Одним записом в таблиці маршрутизатора описуються шляхи до багатьох мереж.

Суть технології CIDR полягає в тому, що кожному постачальнику послуг Internet (або, для корпоративних мереж, якому-небудь структурно-територіальному підрозділу) повинен бути призначений нерозривний діапазон IP-адрес. При цьому вводиться поняття узагальненого мережного префікса, що визначає загальну частину всіх призначених адрес. Відповідно, маршрутизація на магістральних каналах може реалізовуватися на основі узагальненого мережного префікса. Результатом є агрегація маршрутних записів, зменшення розміру таблиць маршрутних записів і збільшення швидкості обробки пакетів.

Припустимо, центральний офіс компанії виділяє одному своєму регіональному підрозділу мережі 172.16.0.0/16 і 172.17.0.0/16, а іншому – 172.18.0.0/16 і 172.19.0.0/16. У кожного регіонального підрозділу є свої обласні філіали і з отриманого адресного блоку їм виділяються підмережі різних розмірів. Використовування технології безкласової маршрутизації дає змогу за допомогою всього одному запису на маршрутизаторі другого підрозділу адресувати всі мережі і підмережі першого підрозділу. Для цього указується маршрут до мережі 172.16.0.0 з узагальненим мережним префіксом 15. Він повинен вказувати на маршрутизатор першого регіонального підрозділу.



За своєю суттю технологія CIDR споріднена з VLSM. Тільки якщо у випадку з VLSM є можливість рекурсивного розподілу на підмережі, невидимі ззовні, то CIDR рекурсивно адресує цілі адресні блоки.

Використовування CIDR дало змогу розділити Internet на адресні домени, усередині яких передається інформація виключно про внутрішні мережі. Зовні домена використовується тільки загальний префікс мереж. В результаті багатьом мережам відповідає один маршрутний запис.

1.4 Приклади розбиття мережі на підмережі

Проектування адресної схеми вимагає від фахівця ретельного опрацьовування багатьох чинників, обліку можливого зростання і розвитку мережі. Почнемо з прикладу розбиття мережі на підмережі. При будь-якому плануванні потрібно знати, скільки підмереж необхідні сьогодні і можуть знадобитися завтра, скільки вузлів знаходиться в найбільшій підмережі сьогодні і скільки може бути в майбутньому.

Крім того, слід розробити хоча б схематичну топологію мережі з вказівкою всіх маршрутизаторів і шлюзів. Доброю практикою є резервування ресурсів на майбутнє. Так, якщо в найбільшій підмережі знаходиться 60 вузлів, не слід виділяти підмережу розмірністю в 26 - 2 (=62) вузли!

Приклад 1

Організації виділений блок адрес 220.215.14.0/24. Розбити блок на 4 підмережі, найбільшу з яких налічує 50 вузлів. Врахувати можливе зростання в 10%.

На першому етапі необхідне число підмереж ми округляємо у велику сторону до найближчого ступеня числа 2. Оскільки в даному прикладі число необхідних підмереж рівно 4, округляти не потрібно. Визначимо кількість біт, потрібних для організації 4 підмереж. Для цього представимо 4 у вигляді ступеня двійки: 4 = 22 . Ступінь – це і є кількість біт, що відводяться для номера підмережі. Оскільки мережний префікс блоку рівний 24, то розширений мережний префікс буде рівний 24 + 2 = 26.

		Мережевий префікс			Підмережа	Вузол
		0	8	16	24 25	31
220.215.14.0/26	<—>	10010000	10010000	00001110	0 0	000000
		Розширений мережений префікс				

32 - 26 = 6 біт, що залишилися використовуватимуться для номера вузла. Перевіримо, скільки вузлів можна адресувати 6-у бітами: 26 - 2 = 62 вузли. Чи достатньо це для 10% зростання? 10% від 50 вузлів – це 5 вузлів, а 55 вузлів менше можливих 62-х. Отже, два біти для номера підмережі нас влаштовують.

Наступним етапом буде знаходження підмереж. Для цього двійкове представлення номера підмережі, починаючи з нулем, підставляється в біти, відведені для номера підмережі.

Основна мережа	11011100	11010111	00001110	00	000000	220.215.14. 0/24
Підмережа 0(00)	11011100	11010111	00001110	00	000000	220.215.14. 0/26
Підмережа 1(01)	11011100	11010111	00001110	01	000000	220.215.14. 64/26
Підмережа 2(10)	11011100	11010111	00001110	10	000000	220.215.14.128/26
Підмережа 3(11)	11011100	11010111	00001110	11	000000	220.215.14.192/26
	Розширений мережевий префікс					

Для перевірки правильності наших обчислень, слід пам’ятати просте правило: десяткові номери підмереж повинні бути кратними номеру першої підмережі. З цього правила можна вивести й інше, що спрощує розрахунок підмереж: достатньо обчислити адресу першої підмережі, а адреси подальших визначаються множенням адреси першої на відповідний номер підмережі. В нашому прикладі ми легко могли встановити адресу третьої підмережі, просто помноживши 64 * 3 = 192.

Як вже згадувалося, окрім адреси підмережі, в якій всі біти вузлової частини рівні нулю, є ще одна службова адреса – широкомовна. Особливість широкомовної адреси полягає в тому, що всі біти вузлової частини рівні одиниці. Розрахуємо широкомовні адреси наших підмереж:

	підмережа		
ШМА підмережі 0 (00)	11011100.11011100.00001110.00	111111	220.215.14.63/26
ШМА підмережі 0 (01)	11011100.11011100.00001110.01	111111	220.215.14.127/26
ШМА підмережі 0 (10)	11011100.11011100.00001110.10	111111	220.215.14.191/26
ШМА підмережі 0 (11)	11011100.11011100.00001110.11	111111	220.215.14.255/26
	Розширений мережевий префікс	Вузлова частина = все 1	

Легко помітити, що широкомовною адресою є найбільша адреса підмережі. Тепер, отримавши адреси підмереж і їх широкомовні адреси, ми можемо побудувати таблицю адрес, що використовуються:

№ підмережі	Найменша адреса підмережі	Найбільша адреса підмережі
0	220.215.14.1	- 220.215.14.62
1	220.215.14.65	- 220.215.14.126
2	220.215.14.129	- 220.215.14.190
3	220.215.14.193	- 220.215.14.254

Це і є розбиття, що задовольняє умові.

Приклад 2

В першому прикладі всі підмережі були однакового розміру – по 6 розрядів. Часто зручніше мати підмережі різного розміру. Припустимо, одна підмережа потрібна для задання адрес двох маршрутизаторів, зв'язаних по схемі "точка-точка". В цьому випадку використовується всього лише дві адреси.

Розглянемо тепер випадок, коли компанії виділений блок адрес 144.144.0.0/16. Потрібно розбити адресний простір на три частини, виділити адреси для двох пар маршрутизаторів і залишити деякий резерв.

Розділимо мережу 144.144.0.0/16 на чотири рівні частини, виділивши два біти для номера підмережі:

Октет	W	X	Y		Z	
Підмережа 0(00)	10010000	10010000	00	000000	00000000	144.144.0.0/18
Підмережа 1(01)	10010000	10010000	01	000000	00000000	144.144.64.0/18
Підмережа 2(10)	10010000	10010000	10	000000	00000000	144.144.128.0/18
Підмережа 3(11)	10010000	10010000	11	000000	00000000	144.144.192.0/18

Усередині третьої підмережі виділимо дві підмережі розміром на чотири адреси:

		Підмережа № 3				№ вузла	
Підмережа 0(0)	10010000	10010000	11	000000	000000	00	144.144.192.0/30
Підмережа 1(1)	10010000	10010000	11	000000	000001	00	144.144.192.4/30
				Номер підмережі			

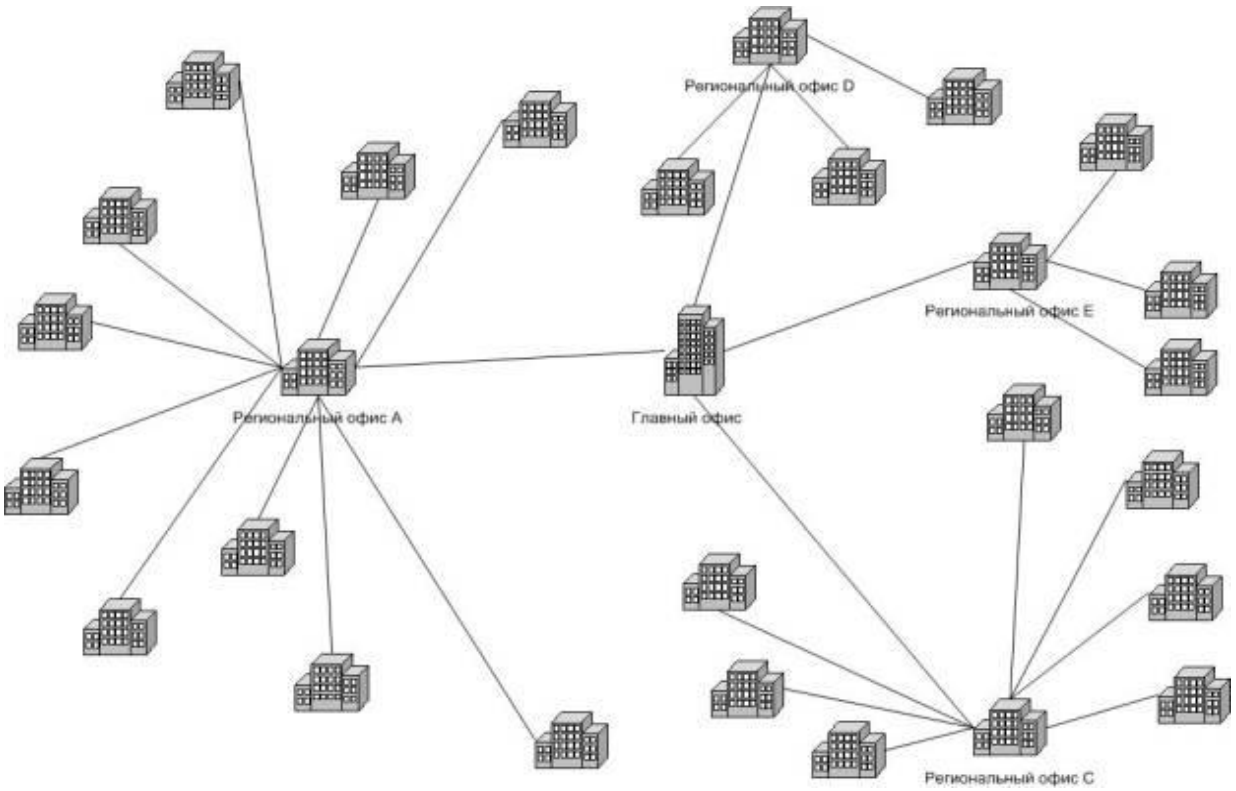
Отримані дві мережі використовуватимемо для адресації інтерфейсів маршрутизаторів. Адресний простір, що залишився, буде резервом, з якого можна буде виділяти адресні блоки по потребі. З адрес, що залишилися, можна, наприклад, утворити 62 мережі розмірності класу С і ще декілька, розміром трохи менше.

Приклад 3

Компанія організує корпоративну мережу. Схема розташування філіалів і канали, що зв'язують їх, приведено на наступному рисунку.

Є чотири регіональні офіси, зв'язані каналами з центральним офісом. До регіональних офісів, у свою чергу, підключені обласні філіали даного регіону.

Вирішено використовувати мережу 10/8 для корпоративної мережі. Вимагається скласти схему IP-адресації компанії. Умовимося відразу вибирати спосіб адресації кращий з погляду маршрутизації.



Для визначення розмірів регіональних офісів, складемо таблицю кількості підключених обласних філіалів до кожного регіонального офісу:

Регіональний офіс	Підключено обласних філіалів	Процент
A	10	36%
C	7	25%
D	3	11%
E	3	11%

Відповідно до цієї таблиці розділимо адресний простір таким чином (зразу ж вкажемо послідовні діапазони адресного простору):

Регіональний офіс	Процент адресного простору	Діапазон адрес	Блок виділених адрес
A	25%	10.0 -63.x.x	10.0.0.0/10
C	25%	10.64 -127.x.x	10.64.0.0/10
D	12,5%	10.128-159.x.x	10.128.0.0/11
E	12,5%	10.160-191.x.x	10.160.0.0/11
Резерв	25%	10.192-255.x.x	10.192.0.0/10

Розглянуто приклади використання різних масок підмережі для однієї і тієї ж мережі 10/8. Чому використовували для кожного офісу нерозривний адресний простір? Для того, що б на центральному маршрутизаторі, шлях до всіх підмереж (читай: обласних офісів даного регіону) вказувався одним рядком.

Для повноти схеми, залишається визначити, як краще адресувати районні офіси. На мій погляд, достатньо віддати кожному офісу одну мережу /16. Цього буде достатньо навіть для дуже великих офісів. Надлишок мереж поміщається в резерв.

2. ХІД РОБОТИ

Завдання 1:

За допомогою бази даних RIPE (http://www.ripe.net/db/whois/whois.html) дізнатись про власників IP адрес, розмірності (для обрахунку розмірності використовувати IP-калькулятор http://jodies.de/ipcalc) сіток відповідно до варіанту.

1. 193.193.206.193
2. 217.196.166.125
3. 193.25.48.91
4. 195.67.251.82
5. 193.195.64.110
6. 192.168.1.254
7. 217.196.166.38
8. 217.196.166.97
9. 217.196.166.98
10. 172.14.0.1

Завдання 2:

За допомогою http://jodies.de/ipcalc поділити мережу класу "С" 217.196.160.0/21 (217.196.160.0/255.255.248.0) на підмережі для таких філій:

1 філія - 683 ПК
2 філія - 112 ПК
3 філія - 57 ПК
4 філія - 117
5 філія - 28 ПК
6 філія - 22 ПК

Можна використати кілька підсіток для однієї філії, але при цьому необхідно мінімізувати їхню кількість.

3. ЗМІСТ ЗВІТУ

3.1 Тема та мета лабораторної роботи.
3.2 Хід виконання лабораторної роботи згідно завдань 1 і 2.
3.3 Інформація про власника IP-адреси згідно варіанту та результат поділу мережі на під мережі.
3.4 Висновки по виконаній роботі.

4. КОНТРОЛЬНІ ЗАПИТАННЯ

4.1 Структура IP-адреси.
4.2 Класи мереж.
4.3 Зарезервовані адреси.
4.4 Маска підмережі змінної довжини VLSM.
4.5 Проблеми класичної схеми IP-адресації.
4.6 Безкласова міждоменна маршрутизація CIDR.

ЛАБОРАТОРНА РОБОТА №5
ПОБУДОВА ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ

Мета: Налаштувати віртуальні локальні мережі

ТЕОРЕТИЧНІ ВІДОМОСТІ

Вивчення принципів роботи різних типів VLAN, конфігурування VLAN з використанням симулятора "Packet Tracer CISCO".

Функціональні можливості сучасних комутаторів дозволяють організовувати віртуальні мережі (VLAN) для створення гнучкої мережної інфраструктури. Багато в чому це пов'язане з тим, що конфігурування комутаторів для організації Vlan-Мереж досить непроста справа, особливо якщо інфраструктура мережі включає кілька комутаторів.

Конфігурування VLAN може значно відрізнятися в комутаторів від різних фірм. При створенні локальної мережі на основі комутаторів, незважаючи на можливість використання користувацьких фільтрів по обмеженню трафіка, усі вузли мережі являють собою єдиний широкомовний домен, тобто широкомовний трафік передається всім вузлам мережі. Таким чином, комутатор споконвічно не обмежує широкомовний трафік, а самі мережі, побудовані по зазначеному принципу, йменуються плоскими.

Віртуальні мережі утворюють групу вузлів мережі, у якій увесь трафік, включаючи й широкомовний, повністю ізольований на канальному рівні від інших вузлів мережі. Це означає, що передача кадрів між вузлами мережі, що ставляться до різних віртуальних мереж, на підставі адреси канального рівня неможлива (хоча віртуальні мережі можуть взаємодіяти один з одним на мережному рівні з використанням маршрутизаторів).

Ізолювання окремих вузлів мережі на канальному рівні з використанням технології віртуальних мереж дозволяє вирішувати одночасно кілька завдань. По-перше, віртуальні мережі сприяють підвищенню продуктивності мережі, локалізуючи широкомовний трафік у межах віртуальної мережі й створюючи бар'єр на шляху широкомовного шторму. Комутатори пересилають широкомовні пакети (а також пакети із груповими й невідомими адресами) усередині віртуальної мережі, але не між віртуальними мережами. По-друге, ізоляція віртуальних мереж друг від друга на канальному рівні дозволяє підвищити безпеку мережі, роблячи частину ресурсів для певних категорій користувачів недоступної.

Типи віртуальних мереж

У локальних мережах використовуються п'ять типів основних критеріїв, на підставі яких може бути визначена приналежність (членство) того або іншого компонента до віртуальної мережі. Ці критерії визначають і номенклатуру VLAN

- VLAN типу 1- визначають членство по фізичному підключенню (порт)
- VLAN типу 2- визначають членство по MAC адресі
- VLAN типу 3- визначають членство по типу протоколу (ISL або 802.1Q) рівня
- VLAN Динамічні.
- VLAN Асиметричні.

1. Віртуальні мережі на основі групування портів (статичні VLAN на основі портів)

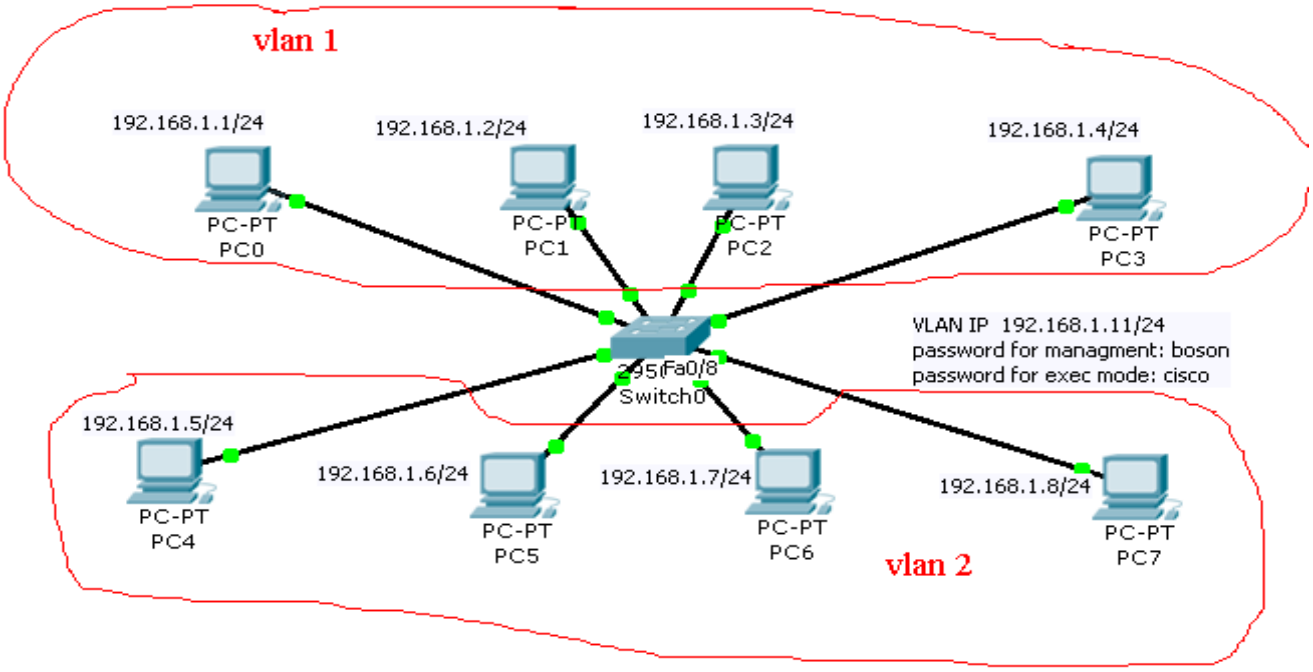


Рисунок 5.1 – Схема мережі

Віртуальні мережі на основі угруповання портів (Port-based) звичайно реалізуються в так званих Smart-Комутаторах або в керованих комутаторах. Даний спосіб створення віртуальних мереж досить простий і, як правило, не викликає проблем. Кожний порт комутатора приписується до тієї або іншій віртуальній мережі, тобто порти групуються у віртуальні мережі. Розв'язок про просування мережного пакета в цій мережі ґрунтується на Mac-Адресі одержувача й асоційованого з ним порту. За замовчуванням усі порти на комутаторі належать однієї VLAN, звичайно номер VLAN 1, ім'я цього VLAN “default”. З метою безпеки вилучене керування по IP мережі дозволяється тільки з VLAN 1.

Технологія створення віртуальних мереж на основі угруповання портів знаходить застосування у випадках використання одного комутатора або використання стека комутаторів з єдиним керуванням. Однак якщо мережа досить велика й побудована на декількох комутаторах, то можливості по організації віртуальних мереж на основі угруповання портів мають істотні обмеження. Насамперед, ця технологія погано масштабується й у більшості випадків обмежується лише одним комутатором.

ХІД РОБОТИ

Створити схему представлену на рисунку 5.1 , для чого:

- помістити на робоче поле 6 робочих станцій і один комутатор.
- з'єднати їх за допомогою ethernet кабелів.
- присвоїти кожній станції IP адресу, відповідно до рисунку 1
- перевірити наявні VLAN на комутаторі за допомогою наступних команд

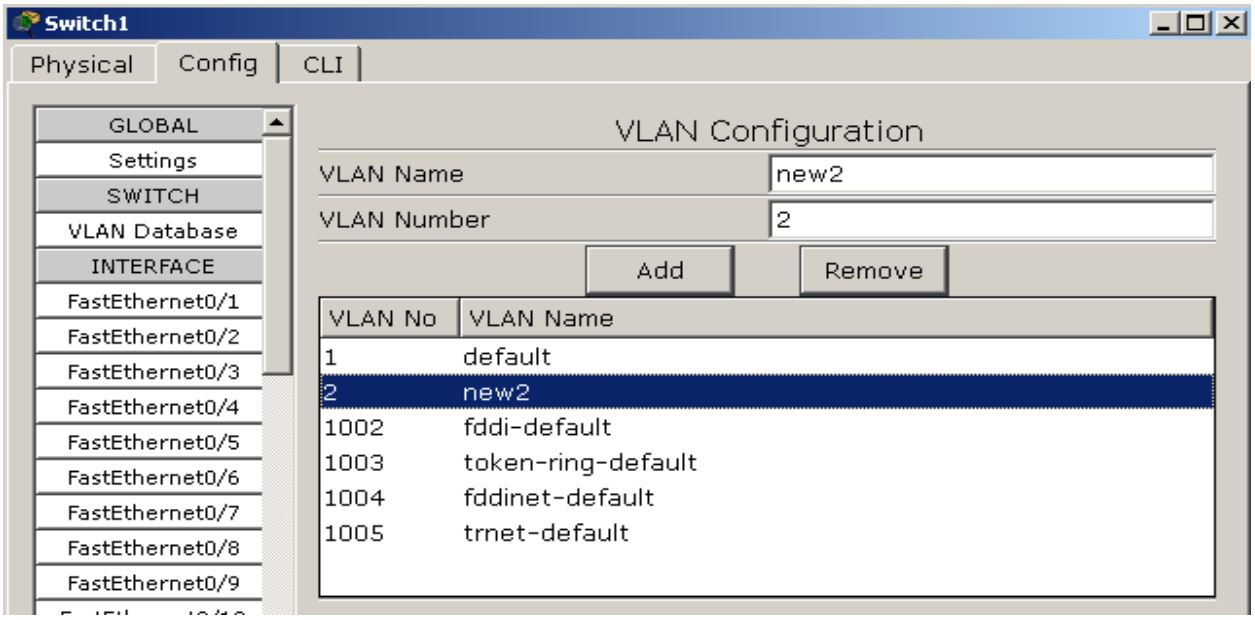
```
switch>show vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
```

```
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 enet  101002     1500  -      -      -        -    -        0      0
1003 enet  101003     1500  -      -      -        -    -        0      0
1004 enet  101004     1500  -      -      -        -    -        0      0
1005 enet  101005     1500  -      -      -        -    -        0      0
```

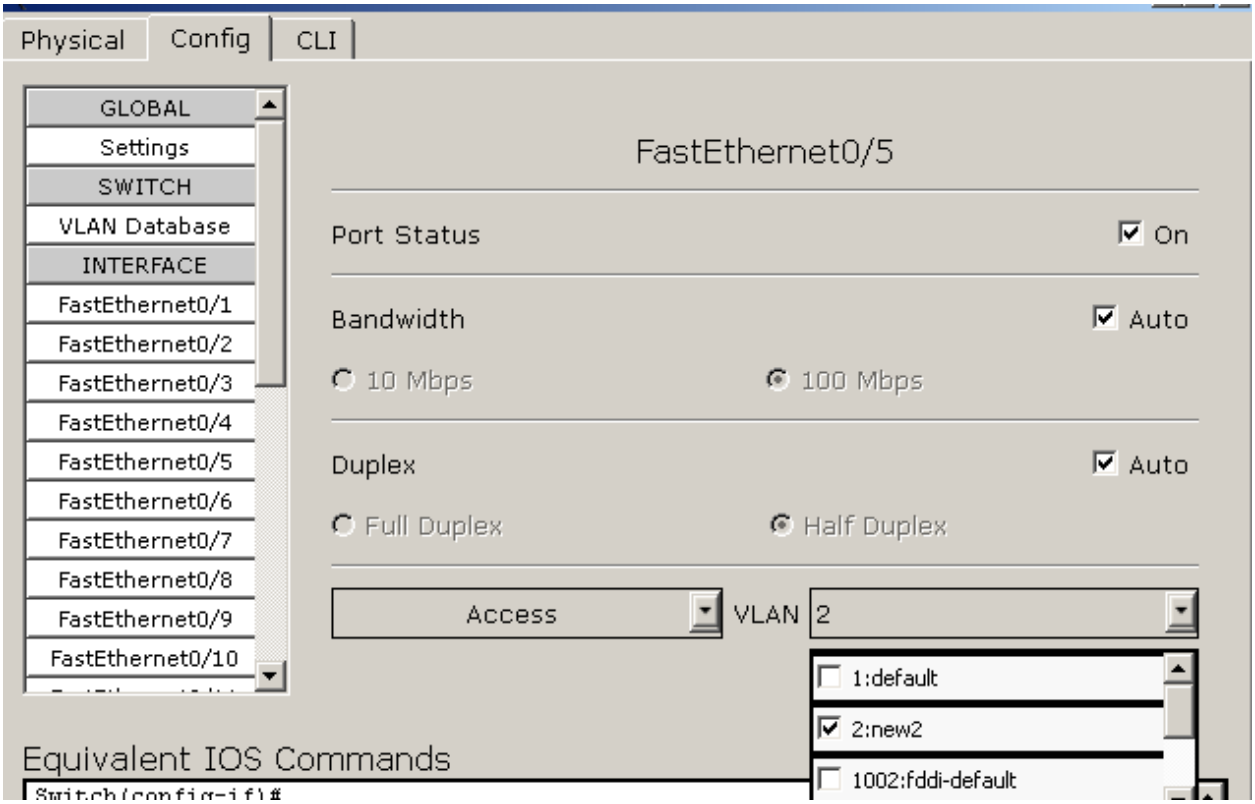
У вікні конфігурації комутатора і в CLI створіть VLAN 2, назвати "new2".

Режим CLI

```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name new2
Switch(config-vlan)#exit
Switch(config)#
Режим ‘Config’
```



Налаштувати VLAN 2, відповідно до рисунку 1. У VLAN 2 входять PC4, PC5, PC6, PC7.



CLI

```
Switch(config)#
Switch(config)#interface FastEthernet0/5
Switch(config-if)#
Switch(config-if)#switchport access vlan 2
Switch(config-if)#
```

Надати IP адресу інтерфейсу управління, пароль для входу у віддалений режим управління, пароль для переходу в exec режим.

```
switch>enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.11 255.255.255.0
Switch(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
Switch(config-if)#line vtp 0 4
Switch(config-if)#exit
Switch(config)#line vty 0 4
Switch(config-line)#login
Login disabled on line 1, until 'password' is set
% Login disabled on line 2, until 'password' is set
% Login disabled on line 3, until 'password' is set
% Login disabled on line 4, until 'password' is set
% Login disabled on line 5, until 'password' is set
Switch(config-line)#password boson
Switch(config-line)#exit
Switch(config)#enable password cisco
Switch(config)#exit
```

Перевірити доступність станцій приналежних різним VLAN, наприклад PC1 і PC5, перевірте доступність станцій приналежних до одній VLAN, наприклад PC0 і PC2, результати занесіть у звіт.

Перевірити доступ до інтерфейсу керування SWITCH по протоколу telnet с робочих станцій вхідних у різні VLAN, результати занесіть у звіт.

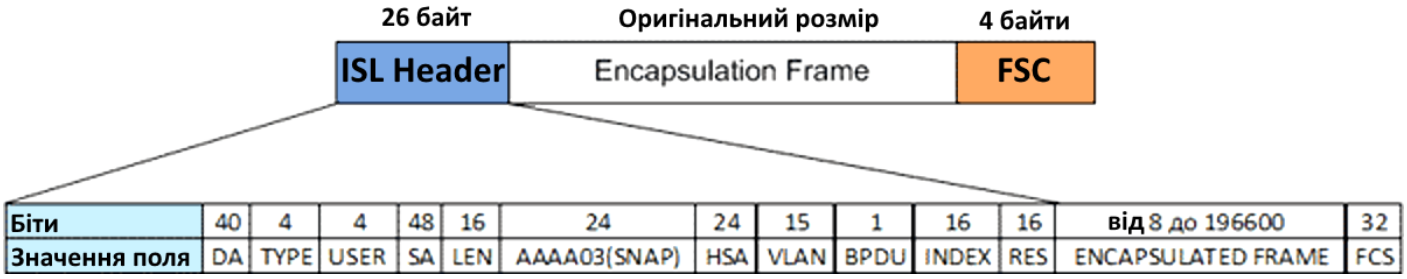
2. Віртуальні мережі на основі інкапсуляція ISL і 802.1Q

Для переносу трафіка приналежного декільком VLAN між комутаторами по тому самому лінку використовуються магістральні канали або транки. Устаткування може визначити до якого VLAN належить трафік по його ідентифікатору VLAN.

Ідентифікатор VLAN це мітка яка інкапсулюється в дані. Для перенесення даних від декількох VLAN по магістральних каналах використовуються два типи інкапсуляції ISL і 802.1Q.

ISL – це протокол розроблений Cisco для з'єднання комутаторів один з одним і підтримки інформації про VLAN у трафік, що проходить через них. ISL виконує утворення груп VLAN у єдиний магістральний канал на повній швидкості з'єднання Ethernet у повнодуплексному або напівдуплексному режимі. ISL працює в середовищі крапка-крапка й може підтримувати аж до 1000 VLAN. При ISL інкапсуляції до оригінального фрейму додається заголовок ISL, оригінальний пакет залишається в незмінному виді, а також наприкінці фрейму додається нова контрольна сума - FCS (Frame Check Sequence). Контрольна сума оригінального пакета залишається БЕЗ змін. Потім отриманий кадр передається в магістральний канал. На прийомній стороні, заголовок ISL віддаляється й кадр пересилається в призначений VLAN.

Формат кадра ISL:



Біти	40	4	4	48	16	24	24	15	1	16	16	від 8 до 196600	32
Значення поля	DA	TYPE	USER	SA	LEN	AAAA03(SNAP)	HSA	VLAN	BPDU	INDEX	RES	ENCAPSULATED FRAME	FCS

Рисунок 5.2 - Формат кадра ISL

Поля кадру

DA - Destianation Address (адреса одержувача), тут використовується мультикаст-адреса, що і є сигналом для одержувача, що кадр инкапсулирован за допомогою ISL. Використовуються адреси "0x01-00-0C-00-00" або "0x03-00-0c-00-00."

TYPE - поле типу, 4 біта, указує протокол 2го рівня, инкапсулированный у пакет. Можливі варіанти:

- 0000 - Ethernet
- 0001 - Token-Ring
- 0010 - FDDI
- 0011 – ATM

USER - користувацькі дані, використовуються для розширення значення поля типу. Для Ethernet-Кадрів у цім полі записується пріоритет кадра при проходженні через комутатор:

- XX00 - Normal Priority
- XX01 - Priority 1
- XX10 - Priority 2
- XX11 - Highest Priority

SA - Source Address, адреса джерела. Установлюється Mac-Адреса порту каталиста, що відправив даний кадр. Одержувачем дане поле може ігноруватися.
LEN - Length, довжина. Зберігає довжину пакета цілком, у байтах, крім полів DA, TYPE, USER, SA, LEN, FCS. У підсумку виходить довжина все кадра разом з інкапсуляцією мінус 18 байт.

AAAA03 (SNAP) - Subnetwork Access Protocol (SNAP) and Logical Link Control (LLC) - поле містить константу 0xaaaa03

HSA - High Bits of Source Address, містить старші біти (3байта = 24 біта) виробника (код виробника) поля SA (адреса комутатора-відправника), містить постійне значення 0x00-00-0C (код Cisco).

VLAN - Destination Virtual LAN ID, номер влана одержувача. 15-бітове поле, часто згадується як "колір" ("color") фрейму.

BPDU - Bridge Protocol Data Unit and Cisco Discovery Protocol Indicator, індикатор пакета BPDU і CDP. Установлюється в 1 при передачі инкапсулированных пакетів VTP і CDP.

INDX - Index, індекс. Вказується індекс порту-відправника на комутаторі. Використовується тільки для діагностичних цілей, може бути встановлене в будь-яке значення відправником (іншим девайсом).16-бітове значення, ігнорується одержувачем.

RES - Reserved for Token Ring and Fiber Distributed Data Interface (FDDI), резервне поле для протоколів TR і FDDI. 16 біт. Для пакетів протоколу Ethernet повинні бути всі нулі, для протоколу TR у даному полі розміщаються значення полів AC (Access Control) FC (Frame Control) оригінального фрейму. Для протоколу FDDI поле FC розміщається в молодших бітах даного поля (приклад: FC = 0x12 -> RES = 0x0012)

ENCAPSULATED FRAME - оригінальний фрейм (до інкапсуляції). Даний фрейм включається свою власну CRC - оригінальне, не змінене значення. Дане значення має сенс ТІЛЬКИ після деинкапсуляции. Довжина инкапсулированного фрейму може бути від 1 до 24575 байт для Ethernet, Token Ring, FDDI пакетів. Після одержання фрейму й деинкапсуляции пристрій-одержувач використовує инкапсулированный фрейм без змін, відповідно до номера влана-получателя.

FCS - Frame Check Sequence, поле контрольної суми. 4 байта. Створюється пристроєм-відправником Isl-Кадра, рекалькулируется комутатором-одержувачем для контролю цілісності передачі. При обчисленні даного поля використовуються поля DA, SA, Length/Type, Data створеного пакета. Обчислюється ПІСЛЯ приєднання заголовка ISL, контрольна сума додається в кінець фрейму. Обчислення даного поля НЕ має відносини до поля FCS оригінального фрейму (неинкапсулированного).

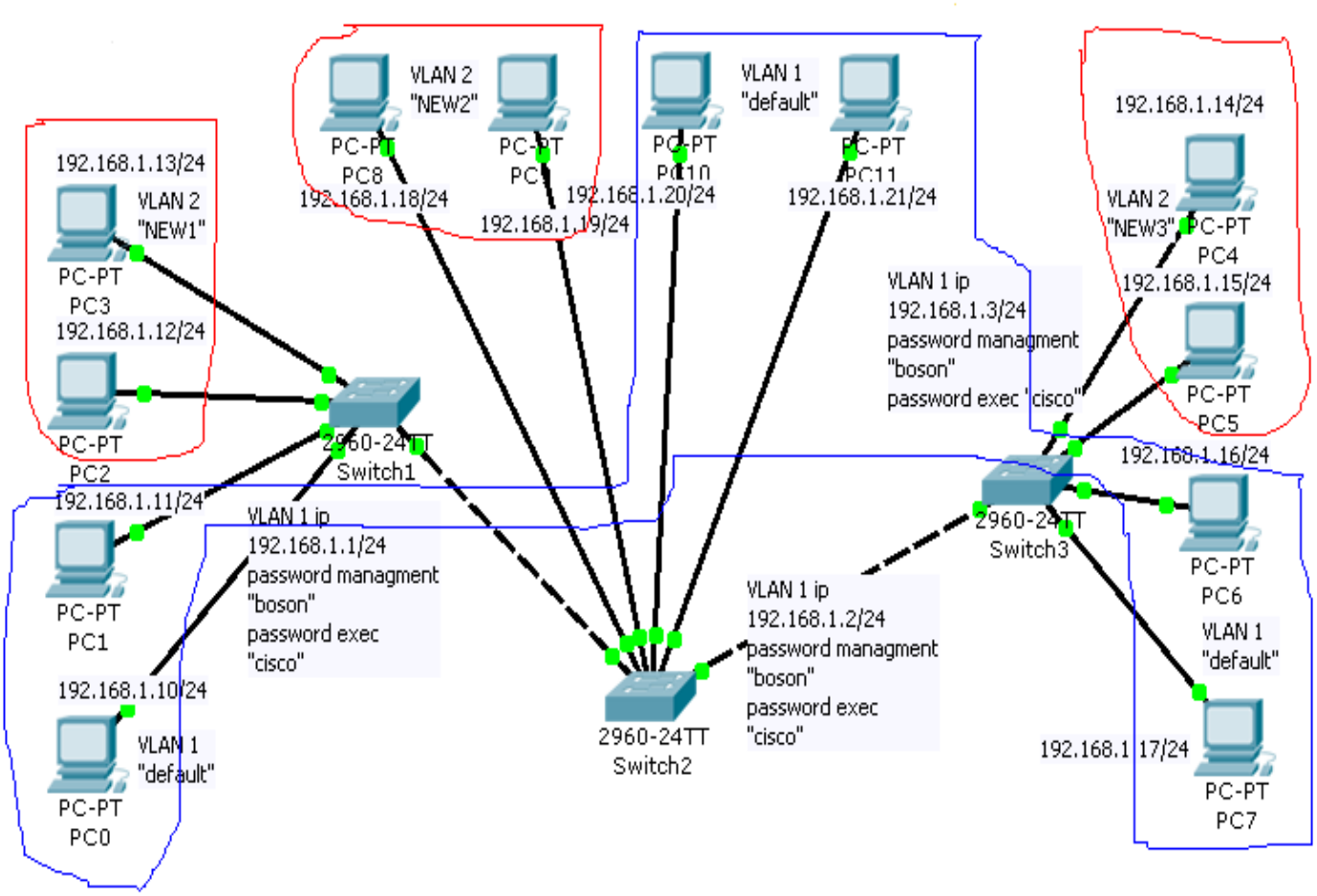


Рисунок 5.3 - Схема

Створити схему на рисунку 5.3.

Надати робочим станціям IP адреси відповідно до рис 5.3

Створити VLAN на комутаторах відповідно до рис 5.3

Налаштувати IP адреси для VLAN 1 на кожному комутаторі відповідно до рис 3, які будуть використовуватися для віддаленого керування (telnet CLI). Призначите пароль для дистанційного доступу до керування й для входу в режим exec кожного комутатора.

Створити VLAN у відповідності зі схемою

Призначитт цим VLAN відповідні порти

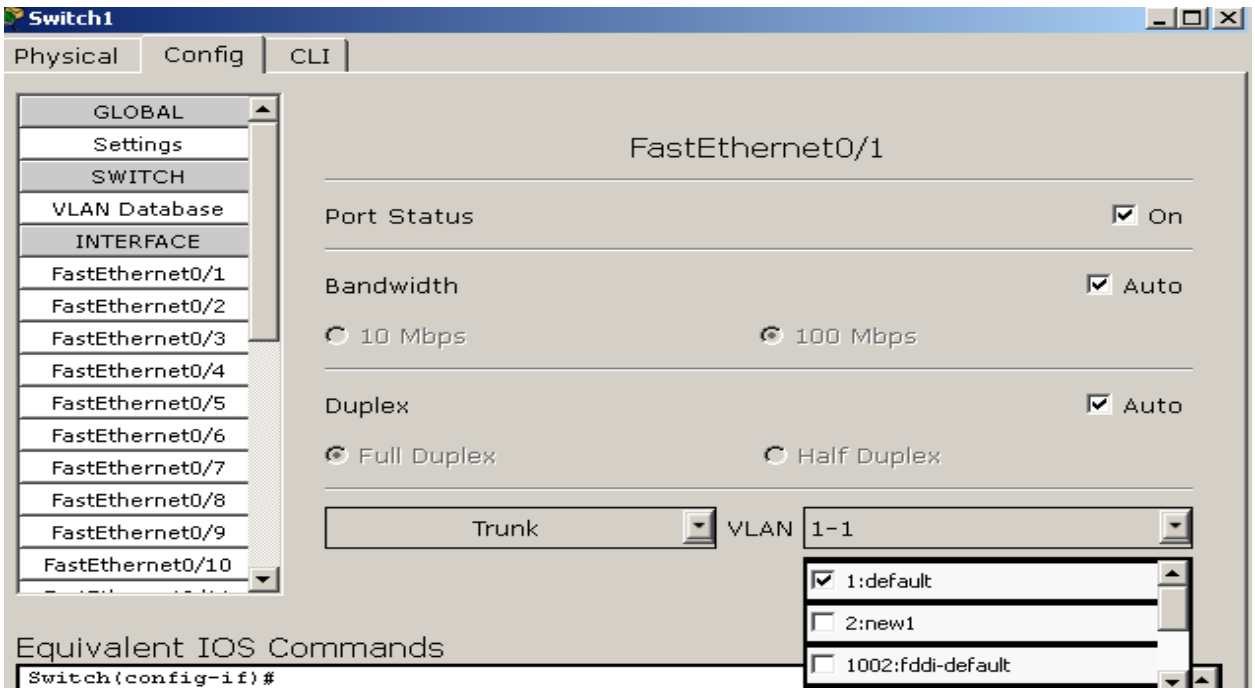
Для зв'язку двох комутаторів з настроєними однаковими VLAN порти, через які вони зв'язані, повинні бути настроєні на switchport mode trunk із вказівкою номером VLAN інформація про яких повинна переноситься. Trunk дозволяє через один з'єднуючий комутатори кабель передавати дані про всі працюючі VLAN, у той же час розділяючи їх друг від друга. Це спосіб передачі трафіка про декілька VLAN по каналу зв'язку типу крапка-крапка між двома пристроями. Ethernet транкінг може бути реалізовано двома способами: ISL (Власний протокол Cisco і 802.1Q не підтримуються комутаторами 2940 і 2950 серій).

Створити транк який буде переносити трафік від VLAN1 через єдиний канали між Sw1, Sw2 і Sw3. Це можна зробити в режимі “config” і CLI.

Настроювання з'єднання trunk для перенесення даних про VLAN 1 між комутаторами в CLI

```
Switch>enable
Password:
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 1
Switch(config-if)#exit
```

Настроювання з'єднання trunk для перенесення даних про VLAN 1 між комутаторами вкладка “config”



Після виконання всіх настроювань у системі буде працювати 4 VLAN

Перевірити доступність робочих станцій у відповідності зі схемою рис 5.3.

Перевірити доступ до керування комутаторами з робочої станції PC7.

Зберегти схему, продемонструйте викладачеві

Одержати завдання створення схеми з індивідуальними настроюваннями, збережіть цю схему й прикладіть її до звіту.

Розглянуті приклади віртуальних мереж ставилися до так званих статичних віртуальних мереж (Static VLAN), у яких усі порти настроюються вручну, при розвиненій мережній інфраструктурі є досить рутинною справою. Крім того, при кожному переміщенні користувачів у межах мережі доводиться робити перенастроювання мережі з метою збереження їх членства в заданих віртуальних мережах. Існує й альтернативний спосіб конфігурування віртуальних мереж, а створювані при цьому мережі називаються динамічними віртуальними мережами (Dynamic VLAN). У таких мережах користувачі можуть автоматично реєструватися в мережі VLAN, для чого служить спеціальний протокол реєстрації GVRP (GARP VLAN Registration Protocol). Цей протокол визначає спосіб, за допомогою якого комутатори обмінюються інформацією про мережу VLAN, щоб автоматично зареєструвати членів VLAN на портах у всій мережі.

Усі комутатори, що підтримують функцію GVRP, можуть динамічно одержувати від інших комутаторів (і, отже, передавати іншим комутаторам) інформацію VLAN про реєстрацію, що включає дані про елементи поточної VLAN, про порт, через який можна здійснювати доступ до елементів VLAN і т.д. Для зв'язку одного комутатора з іншим у протоколі GVRP використовується повідомлення GVRP BPDU (GVRP Bridge Protocol Data Units). Будь-який пристрій з підтримкою протоколу GVPR повідомлення, що одержує таке, може динамічно приєднувати до тієї мережі VLAN, про яку воно сповіщене.

ЗМІСТ ЗВІТУ

1. Титульний аркуш.
2. Конфігурація комутаторів (Running config для кожного комутатора) відповідно до завдання по створенню VLAN, отриманим від викладача
3. Схему мережі й вихідне завдання.
4. Висновки.

КОНТРОЛЬНІ ПИТАННЯ

1. У чому полягають переваги мережі, побудованої з використанням технології VLAN?
2. Які Вам відомі способи побудови VLAN? Які гідності й недоліки властиві кожному їх цих способів? При відповіді на це питання слід указати область можливого застосування кожного зі способів побудови VLAN.
3. Які Вам відомі способи побудови розподілених віртуальних мереж? Які гідності й недоліки властиві кожному їх цих способів?
4. Який формат має мітка VLAN IEEE 802.1Q? У чому полягає призначення кожного з компонентів мітки

ЛАБОРАТОРНА РОБОТА №6
ПОБУДОВА ОПТОВОЛОКОННИХ СЕГМЕНТІВ МЕРЕЖІ

Мета: Побудувати оптоволоконні сегменти мережі

ТЕОРЕТИЧНІ ВІДОМОСТІ

Структури систем оптоволоконного зв'язку

Основний структурний елемент системи оптоволоконного зв'язку - одноканальна СОЗ. Її називають симплексною, якщо по ній передають один оптичний сигнал в одному напрямку (рис. 6.1, а). Волокно в складі симплексної СОЗ може передавати два оптичних сигналу у зустрічних напрямках. У ній на обох сторонах повинні бути оптичні волоконні з'єднувачів і спрямовані відгалужувачі. Таку лінію ми умовно назвемо напівдуплексною. Повнодуплексною лінією називають пару симплексних ліній, що працюють на зустрічних напрямках між однією парою кореспондентів.

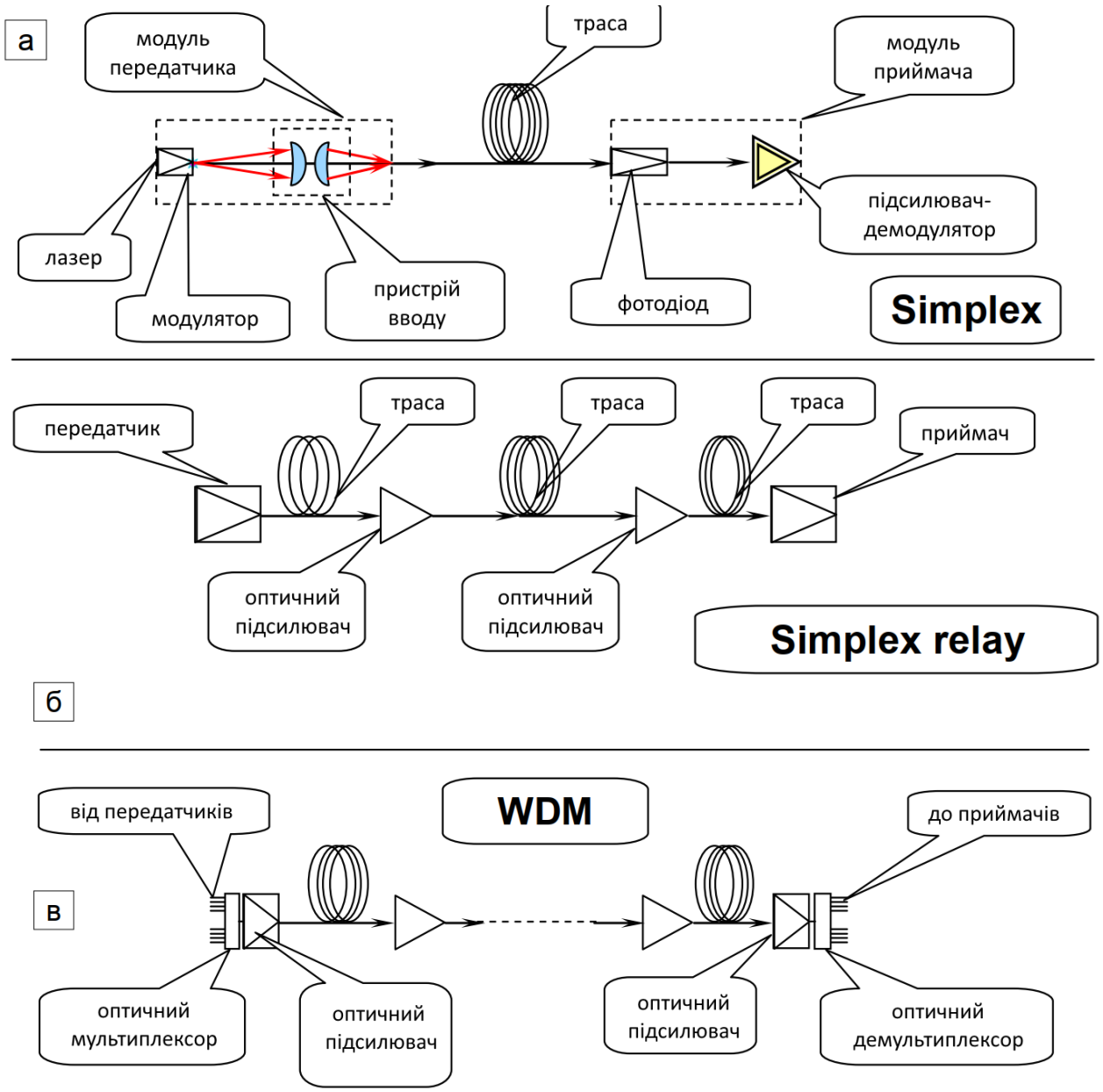


Рисунок 6.1 Структури типових волоконно-оптичних ліній зв'язку:
а - симплексна однопрогонова, розгорнута схема;
б - симплексна багатопрогонова, з проміжними підсилювачами;
в - мультиплексна багатопрогонова, WDM, з проміжними оптичними підсилювачами. Протяжні траси умовно показані у вигляді котушок

Через один канал СОЗ можна передавати один або кілька незалежних інформаційних потоків, фізично об'єднаних в загальний груповий потік даних в передавачі і поділюваних на приймальній стороні відповідно до встановленого протоколом зв'язку, як і в дротяних лініях зв'язку Ethernet і ін.

Одноканальна симплексна СОЗ містить:
1) випромінювач оптичного діапазону, переважно лазер;
2) модулятор, змінює амплітуду, частоту або фазу коливань відповідно до переданої інформації;
3) пристрій введення випромінювання в оптичне волокно;
4) власне волоконну лінію;
5) приймач, найчастіше з швидкодіючим фотодіодом.

Оптичний бюджет СОЗ, або орієнтовний загасання оптичної лінії - це прогнозована сума втрат оптичного сигналу на всіх компонентах СОЗ. Оптичний бюджет СОЗ розраховується в основному на етапі проектування лінії і підбору каналоутворюючого обладнання.

Про проектування лінії СОЗ обчислюється кількість окремих відрізків, кількість з'єднань. Кожне з'єднання вносить втрати в силу сигналу. Допуски на максимальну втрату сигналу вимірюються в децибелах дБ.

Наприклад, Втрати на кожному зварному з'єднанні для магістральної СОЗ не повинні перевищувати 0,03 - 0,05 дБ. (Для мережі доступу 0,1 - 0,15 дБ). Відповідно, обчислюємо втрати на зварних з'єднаннях, помноживши їх кількість (наприклад 21) на втрати в кожному з них :

$$\mathbf{А_{зв} = 21 * 0,05 = 1,05\ дБ.}$$

Втрати на рознімних 2-х (конекторних) з'єднаннях розраховуємо аналогічно, враховуючи значення втрат на кожному з них рівне 0,2 - 0,4 дБ

$$\mathbf{А_{кон} = 2 * 0,4 = 0,8\ дБ.}$$

В самому оптичному волокні проходять втрати потужності сигналу. Втрати світла в волокні описуються величиною, яку називають *кілометричним згасанням* або *погонними втратами* (тобто величина показує *втрати* на одиницю довжини) і виражаються в дБ/км. Погонні втрати для різних довжин хвилі світла в оптичному волокні складають:

$$\mathbf{А_{пог\ 1310} = 0,33\ дБ/км;}$$
$$\mathbf{А_{пог\ 1550} = 0,22\ дБ/км}$$

Втрати в волокні при довжині лінії, наприклад, в 100 км складуть:

$$А_{л\ 1310} = 0,33\ дБ/км * 100\ км = 33\ дБ;$$
$$А_{л\ 1550} = 0,22\ дБ/км * 100\ км = 22\ дБ$$

Якщо в лінії є інші компоненти (мультиплексори, демультиплексори, сплітери і т. д.) то втрати на них теж варто враховувати. Якщо інших компонентів лінія не включає, то її бюджет становитиме:

$$\mathbf{Бюджет\ СОЗ = А_{сум} = А_{л} + А_{зв} + А_{кон}}$$

Звичайно вимірювання втрат у СОЗ проводиться:

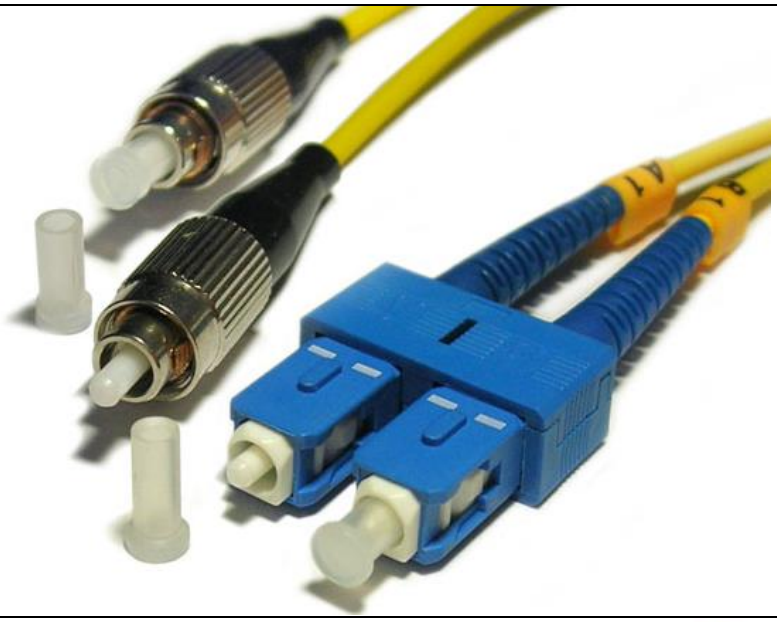
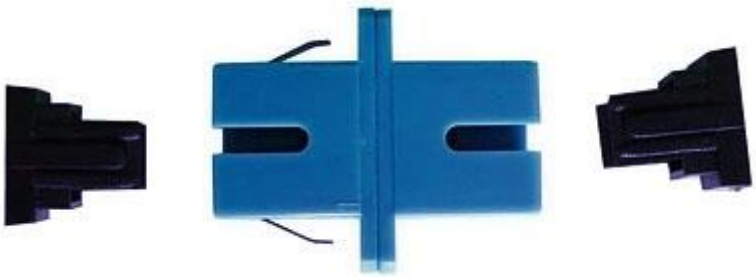
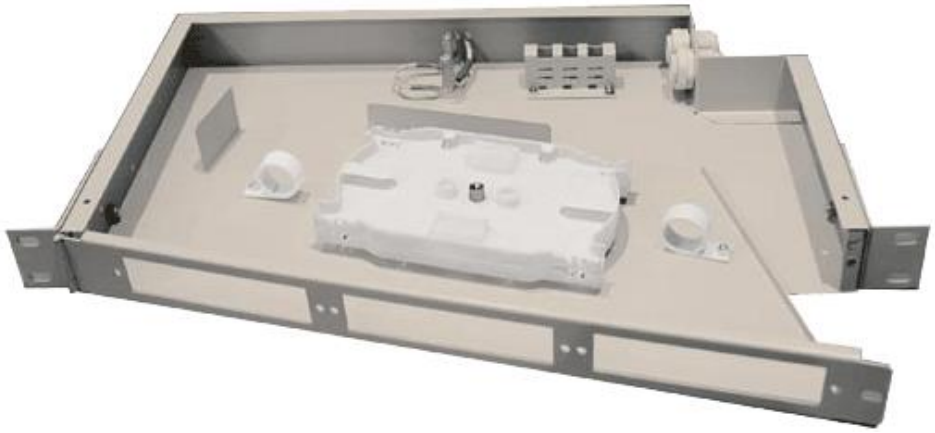
- під час будівництва,
- при експлуатації,
- при обслуговуванні.

Пасивне обладнання

PON. пасивна оптоволоконна мережа

Пасивне мережеве обладнання: кабель (коаксіальний і вита пара (UTP / STP)), вилка / розетка (RG58, RJ45, RJ11, GG45), оптичний пігтейл або патчкорд і т.д.

Пасивне мережеве обладнання **СОЗ**:

Патчкорди оптичні оконечений з обох сторін відрізок волоконно-оптичного кабелю з конекторами певного типу. ОП використовуються для з'єднання телекомунікаційного обладнання з кросс-панелями і кросування окремих волокон між собою. Розрізняють сполучні патчкорди - оконечені однаковими типами конекторів і перехідні патчкорди - оконечені різними типами конекторів.	
Пігтейли оптичні використовується для окінцювання волоконно-оптичних кабелів. Пігтейл є оконечений з одного боку відрізок волоконно-оптичного кабелю з конектором певного типу. Пігтейл з'єднується з волоконно-оптичним кабелем шляхом зварювання або за допомогою механічного з'єднувача.	
Оптичні адаптери призначені для організації роз'ємного оптичного з'єднання. Залежно конструкції конектора розрізняють кілька типів оптичних адаптерів: LC, SC, FC, ST, SC / APC, FC / APC.	
Патч-панелі Комутаційна панель (кросс-панель, патч-панель) - одна із складових частин структурованої кабельної системи (СКС). Являє собою панель з безліччю сполучних роз'ємів, розташованих на лицьовій стороні панелі. На тильній стороні панелі знаходяться контакти, призначені для фіксованого з'єднання з кабелями, і сполучені з роз'ємами електрично.	 Оптичний бокс CROSVER FOB-19/ 1-016 /16-2-24 призначений для монтажу в 19-дюймові стійку і застосовується для окінцювання оптичних кабелів методом зварювання з використанням пігтейлів.

ТВ-розгалужувачі (Optical Coupler Module) Зварні (FBT) подільники або Couplers Спліттер PON, також називають оптичним подільником і перехідником - головний елемент PON. Спліттер ділить одне оптоволокно на кілька, не допускаючи ситуації, коли у кінцевих споживачів пропускна здатність використовується лише частково; сплітери і коплери дешевше активного обладнання, яке використовується в стандартних оптоволоконних мережах.	 Коуплер 1х4  Коуплер 1х8 всередині
Оптичний циркулятор – це пасивний багатопортовий оптичний пристрій реалізований таким чином, що світло, яке потрапляє в один оптичний порт, виходить з наступного	

Бокс FTTH / PON Оптичні бокси призначені для з'єднання і комутації абонентських оптичних кабелів з магістральними. Бокс надає місце для технологічного запасу кабелю і захищає місця пайки від механічних пошкоджень.	 Для виготовлення боксів використовують пластик, що має стійкість до УФ випромінювання, має ступінь захисту IP65. За необхідності, в корпусі встановлюють оптичні дільники і замок для захисту від несанкціонованого доступу.

Принципи, способи та засоби з'єднання оптоволокна

Одна з головних вимог при роботі з оптоволоконними кабелями - уважне ставлення до всіх етапів процесу монтажу кабельної системи: укладання, оброблення, з'єднання й окінцювання.

Помилка дорогого коштує - це витрати на пошук місця ушкодження й заміна ділянки кабелю. Заміна ушкодженого ділянки не тільки збільшує працезатрати, але й знижує якість усієї системи: кожний сполучний елемент, кожна спайка вносить свої викривлення в переданий сигнал, зменшує відстань передачі сигналу, вимагає збільшення оптичного бюджету системи. Для фахівців, які тільки починають свою роботу з монтажу оптоволокна, рекомендується придбати готовий комплект основних інструментів і матеріалів, необхідних для проведення робіт: тара, дозатори, розподільники, видаткові матеріали й захисні засоби. Через деякий час, коли ви одержите початкові навички роботи з оптоволоконним кабелем і сформуєте переваги в різноманітності використовуваних інструментів і матеріалів, ви зможете комбінувати набір " під себе".

Рисунок 6.3 - Набір інструментів та матеріалів

Оброблення волоконно-оптичного кабелю

Волоконно-Оптичний кабель являє собою кілька оптичних волокон, які разом з армуючими нитками укладені в захисну полімерну оболонку. Для захисту від агресивних зовнішніх впливів кабель поміщають у броньовий захист із гофрованої алюмінієвої або сталевої захисної стрічки або зі сталевого дроту. Через те, що оптичне волокно в достатньому ступені чутливо до осьових і радіальних

деформацій, для його розрізування непридатні недорогі кабелерізи, які використовуються для роботи з мідними кабелями. Рекомендується використовувати інструмент, леза якого розраховані на різання стали.

Початковий етап оброблення волоконно-оптичних кабелів - видалення верхнього шару захисних і броньових покривів, виконується тими ж інструментами, що й оброблення звичайних кабелів. Полімерна ізоляція й фольга розкриваються різаками, а сталевий дріт викусується бокорізами. Рекомендується застосовувати кабельні ножі: вони дозволяють знімати полімерне покриття з кабелю діаметром від 4 до 35 мм, і при цьому кабельний ніж має спеціальну насадку, що обмежує глибину розрізу оболонки, що виключає ушкодження оптоволоконних жил.

Рисунок 6.4 - Стрипер буферного слою Jonard JIC-125

Але в подальшій роботі без спеціальних інструментів однаково не обійтися:

- ножиці або гострозубці з керамічними лезами - використовуються для видалення армуючих ниток з кевлара. Звичайні ножиці ці тонкі, гнучкі й міцні волокна не ріжуть, а видавлюють або гнуть;
- стрипери - призначені для зняття буферного шару. Їхнє застосування знижує ризик ушкодження оптичного волокна: у першу чергу через те, що його робочі поверхні мають фіксоване настроювання;
- сколювач оптичних волокон - застосовується для відсікання зайвого відрізка волокна під кутом 90 гради. Сколювачі бувають ручні й автоматичні. При підготовці оптоволокна для наступного зварювання або з'єднання волокон за допомогою сплайса рекомендується використовувати автоматичні сколювачі, які дозволяють одержати чистий і рівний відкол без дефектів під кутом 90±0,5 гради. Наприклад, відкол з кутом більш 2 град. може привести до збільшення втрат у з'єднанні до 1 дБ, що при *оптичному загальному бюджеті* системи в 15-25 дБ - найчастіше недозволенна розкіш;
- мікроскопи дозволяють діагностувати рознімання оптичних волокон на якість полірування жили, наявність тріщин, подряпин;
- кримпери призначені для обтискача наконечників, рознімань і контактів.

Способи з'єднання волоконно-оптичного кабелю

Широко застосовуються три способи монтажу оптоволокна:

- зварювання оптичних волокон;
- з'єднання за допомогою механічних рознімань;
- з'єднання за допомогою сплайса.

Зварювання оптичних волокон

Здійснюється за допомогою спеціальних зварювальних апаратів і звичайно виконується в три етапи:

- підготовка й зачищення кабелю, одержання якісного торця;
- зварювання зварювальним апаратом;
- тестування й оцінка якості з'єднання.

Зварювальний апарат здійснює з'єднання оптоволокна з гарними параметрами місця з'єднання просто й швидко. Сучасні зварювальні апарати дозволяють знизити втрати в місці з'єднання до 0,04 дБ і менше. Апарат автоматично виконує всі необхідні операції: юстирує оптоволокна, розплавляє кінці оптоволокон, зварює їх. Найбільш функціональні (але й, на жаль, більш дорогі) моделі також перевіряють якість з'єднання. Після чого місце зварювання захищають, звичайно за допомогою *термоусаджувальної трубки*.

З'єднання за допомогою механічних рознімань

Зварювання оптичного волокна також використовується при оконцюванні волокна конекторами. Для цих цілей використовуються готові волоконно-оптичні перемички - *пігтейли* (англ. pigtail - гнучкий провідник). **Пігтейл** звичайно виготовляється в заводських умовах, він являє собою відрізок оптоволоконного кабелю, який має з однієї сторони оптичний коннектор. Волокно оптичного кабелю зварюється з волокном пігтейла, а вже за допомогою конектора його підключають до встаткування.

З'єднання за допомогою сплайса

Сплайс - пристрій для зрощування волоконно-оптичного кабелю без застосування зварювання. У сплайс через спеціальні напрямні назустріч один одному вводяться підготовлені кінці оптичних волокон і фіксуються в ньому. Для зменшення внесених втрат стик між волокнами поміщають у спеціальний (імерсійний) гель, який найчастіше перебуває усередині сплайса.

Рисунок 6.5 - Автоматичний зварювальний апарат Fujikura FSM-60S

Пігтейл

Технологія з'єднання за допомогою сплайса містить у собі кілька етапів:

- оброблення волоконно-оптичного кабелю;
- обробка торців;

- виконання з'єднання;
- тестування й оцінка якості з'єднання;
- нанесення захисних покриттів, відновлення захисної оболонки й броні.

Застосування сплайсів полегшує процес зрощування оптоволокна, але робота з ними вимагає практичних навичок. Внесені втрати при цьому методі з'єднання волокон менше, ніж при використанні пари волоконно-оптичних вилок і адаптера, але все-таки можуть становити 0,1 дБ і вище. Згідно з вимогами стандартів на СКС IS0 11801, TIA EIA 568B внесені втрати в сплайсі не повинні перевищувати 0,3 дБ. Для цього в ході монтажу проводиться коректування положення волокон відносно один одного, у процесі робіт також необхідно проводити постійний вимір *втрат* на місці з'єднання.

Крім того, слід брати до уваги той факт, що згодом втрати в місці з'єднання за допомогою сплайса можуть збільшитися через зсув волокон у просторі або висихання імерсійного гелю.

Практикум №1 по монтажу оптоволокна

Приклад створення пігтейлу №1 «Fiber Optic Pigtail» за посиланням
https://www.youtube.com/watch?v=pgRbLIE0zao

Приклад створення *патчкорда* оптоволокна стандарту SC/PC connector №2 за посиланням https://www.youtube.com/watch?v=Gc-MP0rBkjY

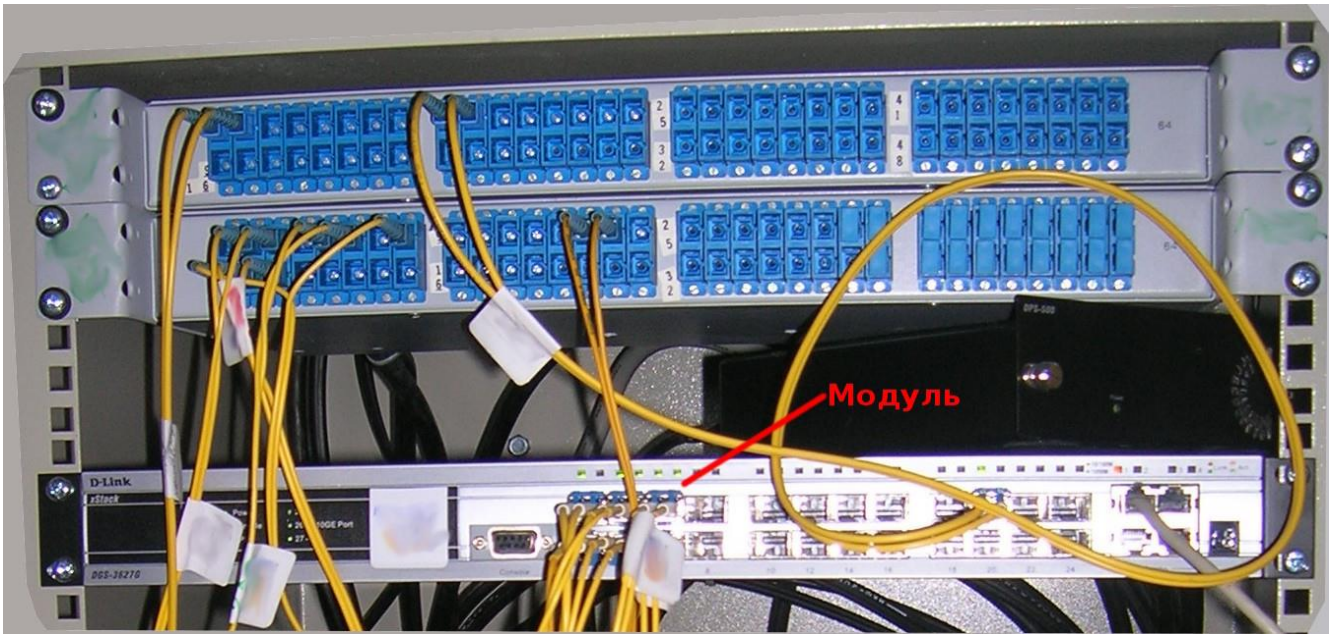
Приклад *зварювання* оптоволокна №2 «Зварювання оптоволокна апаратом DVP-740» за посиланням
https://www.youtube.com/watch?v=LK0TW_gwbng

Приклад зварювання оптоволокна №3 «Зварювальний апарат для оптоволокна EasySplicer Mark 2» за посиланням
https://www.youtube.com/watch?v=IeTvJXZxXm4

Активне мережеве обладнання СОЗ в локальні мережі

Для організації з'єднання необхідне встаткування - оптичний трансівер. Розглянемо основні характеристики оптичних модулів для приймання/передачі інформації та основні моменти, пов'язані з їхнім використанням.

Мережне встаткування для передачі даних у мережах Ethernet, що надає можливість підключення через оптичне волокно, має оптичні порти. У них установлюються оптичні модулі, у які вже може підключатися волокно. У кожний модуль вбудований оптичний передавач (лазер) і приймач (фотоприймач). При класичній передачі даних з їхнім використанням передбачається використовувати два оптичні волокна — одне для приймання, інше для передачі. На зображенні знизу представлений комутатор з оптичними портами й установленими модулями.



У верхній частині– оптична патч-панель.
В нижній частині комутатор з оптичними модулями

Періодично виникають питання, який же оптичний прийомомопередатчик потрібний у конкретній ситуації. Оптичні модулі різняться формфактором (GBIC, SFP, X2...), типом технології («прямі», CWDM, WDM, DWDM...), потужністю (у дицебелах), розніманнями (FC, LC, SC).

При роботі з OTN (оптична транспортна мережа) існують два основних типи систем мультиплексування з поділом по довжині хвилі (WDM):

мультиплексування з широким діапазоном довжин хвиль (CWDM)

мультиплексування з щільним спектром довжин хвиль (DWDM).

Як дві сучасні технології WDM, вони обидва використовуються **для збільшення смуги пропускання** волокна шляхом об'єднання оптичних сигналів різних довжин хвиль на одній нитки волокна.

Термінологія:

CWDM (Coarse Wavelength Division Multiplexing) - мультиплексування з грубим поділом по довжині хвилі.

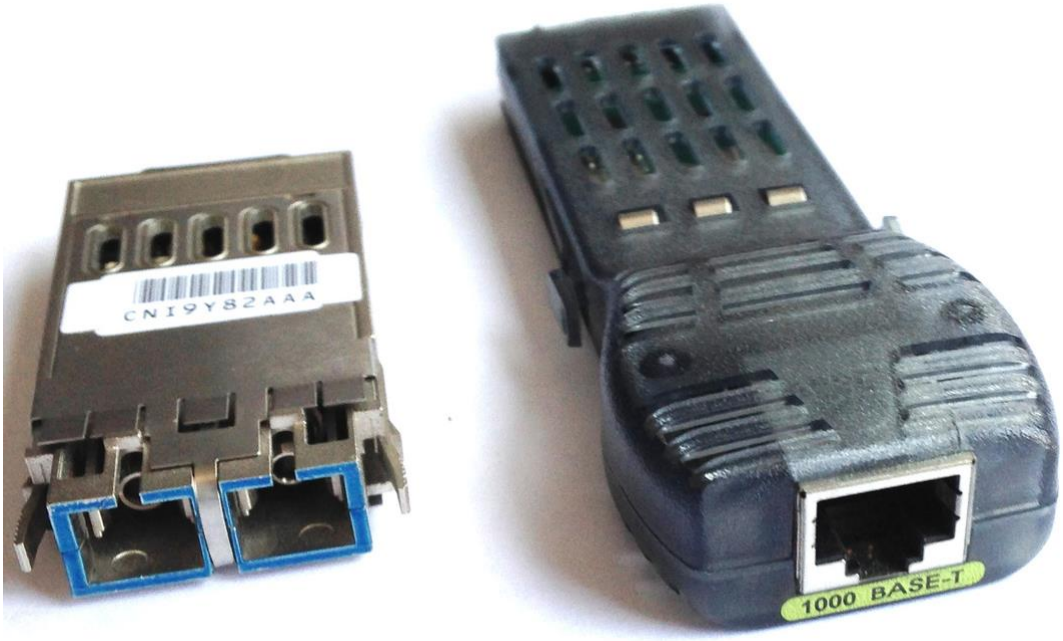
DWDM (Dense Wavelength Division Multiplexing) - мультиплексування з щільним поділом по довжині хвилі.

Основна відмінність CWDM та DWDM - рознесення довжин хвиль каналів.

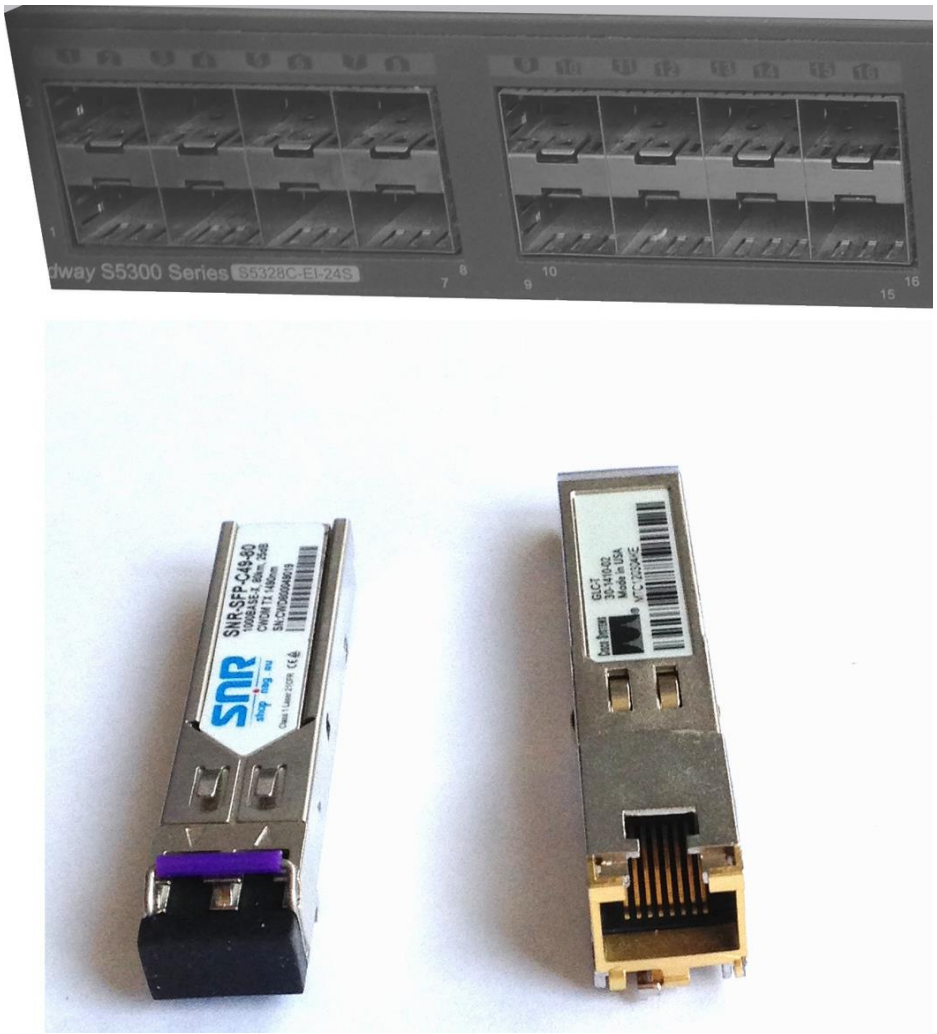
У першу чергу модулі *різняться* своїми формфакторами

GBIC Gigabit Interface Converter, активно використовувався в 2000-х. Найперший промислово стандартизований формат модулів. Дуже часто застосовувався при передачі через багатомодові волокна. Зараз же практично не використовується в силу своїх розмірів.

На зображенні нижче два GBIC-Модуля 1000Base-LX і 1000Base-T:



SFP (анг. Small Form-factor Pluggable), спадкоємець GBIC. Найпоширеніший на сьогоднішній день формат, набагато зручніше в силу менших розмірів. Такий формфактор дозволив значно збільшити щільність портів на мережному встаткуванні. Завдяки таким розмірам стало можливо реалізувати до 52 оптичних портів на одному пристрої розміром в один юніт (unit). Використовується для передачі даних на швидкостях 100Mbits, 1000Mbits. На зображенні знизу комутатор з оптичними портами й пари модулів 1000Base-LX і 1000Base-T.



Модулі SFP використовуються для приєднання плати мережевого пристрою (комутатора, маршрутизатора або подібного пристрою) до оптоволокна або неекранованої крученої пари, виступають у ролі мережевого кабелю.

Стандарт: IEEE802.3z

Різновиди SFP-модулів і їх позначення:

850 нм 550 м MMF -SX

1310 нм 10 км SMF -LX

1550 нм (40 км -XD, 80 км -ZX, 120 км -EX таEZX) і DWDM.

SFP+ Enhanced Small Form-factor Pluggable. Мають ідентичний SFP розмір. Схожий розмір дозволив зробити встаткування з портами, що підтримують звичайні SFP і SFP+. Такі порти можуть працювати в режимах 1000Base/10GBase. Лише далекобійні CWDM-Модулі мають більшу довжину через радіатор. Використовуються для передачі даних на швидкостях 10 Gbits. Малі розміри додали деякі особливості — для далекобійних модулів бувають випадки занадто сильного нагрівання. Тому для передачі більш ніж на 80 км таких модулів поки немає. На ілюстрації знизу два модулі SFP+:

CWDM і звичайний 10GEBase-LR:

XFP 10 Gigabit Small Form Factor Pluggable. Також, як і SFP+, використовуються для передачі даних на швидкостях 10 Gbits. Але на відміну від попередніх, дещо ширше. Збільшений розмір дозволив використовувати їх для передачі на більшу відстань в порівнянні з SFP+. Знизу показано додаткову мережеву плату для Huawei із установленими XFP і пари таких модулів.

ХІД РОБОТИ

1) Записати етапи зварювання оптоволокна.

КОНТРОЛЬНІ ПИТАННЯ

1. Що таке бюджет СОЗ?
2. Принципи передачі сигналу в оптичних лініях?
3. Активне обладнання?
4. Пасивне обладнання?
5. Які основні етапи зварювання оптоволокна?
6. Які важливі етапи процесу пропущені у відео-практикумі №3?

ЛАБОРАТОРНА РОБОТА 7.
НАЛАШТУВАННЯ МЕРЕЖЕВИХ СЕРВІСІВ.

Мета роботи: Налаштувати мережеві сервіси

ТЕОРЕТИЧНІ ВІДОМОСТІ

Емулятор Cisco Packet Tracer дозволяє проводити настройку таких мережевих сервісів, як: HTTP, DHCP, TFTP, DNS, NTP, EMAIL, FTP в складі сервера мережі. Розглянемо настойку деяких з них.

Створіть наступну схему мережі, представлену на рисунку 7.1:

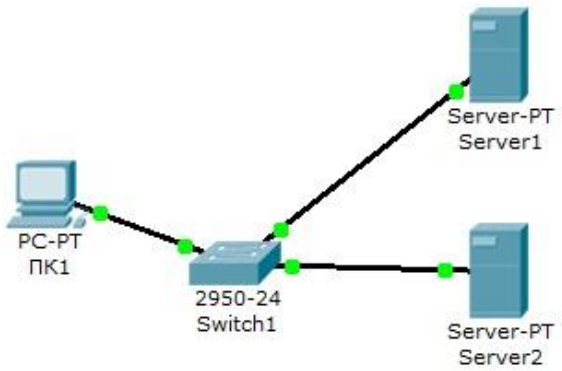


Рисунок 7.1 – Схема мережі

ХІД РОБОТИ

Налаштувати мережу таким чином:

1 - Server1 - DNS і Web сервер;

2 - Server2 - DHCP сервер;

3 - Комп'ютер ПК1 отримує параметри протоколу TCP / IP в DHCP сервера і відкриває сайт www.ukr.net на Server1.

Етап 1.

Задайте параметри протоколу TCP / IP на ПК1 і серверах.

Увійдіть в конфігурацію ПК1 і встановіть налаштування IP через DHCP сервер Рисунок 3.2.

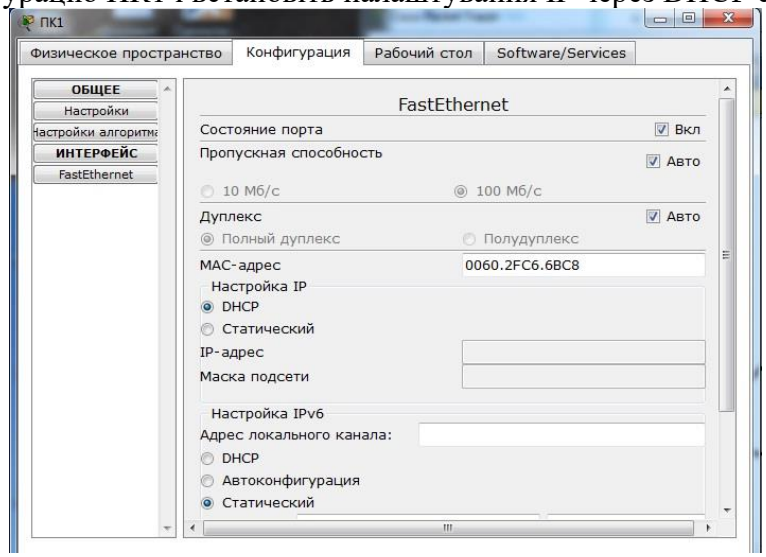


Рисунок 7.2 – Налаштування IP на ПК1.

Задайте в конфігурації серверів наступні настройки IP:

Server1: IP адреса - 10.0.0.1, маска підмережі - 255.0.0.0

Server2: IP адреса - 10.0.0.2, маска підмережі - 255.0.0.0

Етап 2. Налаштуйте службу DNS на Server1.

Для цього в конфігурації Server1 увійдіть вкладку DNS і задайте дві ресурсні записи в прямій зоні DNS:

1 - в ресурсному записі типу A зв'яжіть доменне ім'я комп'ютера з його IP адресою Рисунок 7.3 і натисніть кнопку ДОДАТИ:

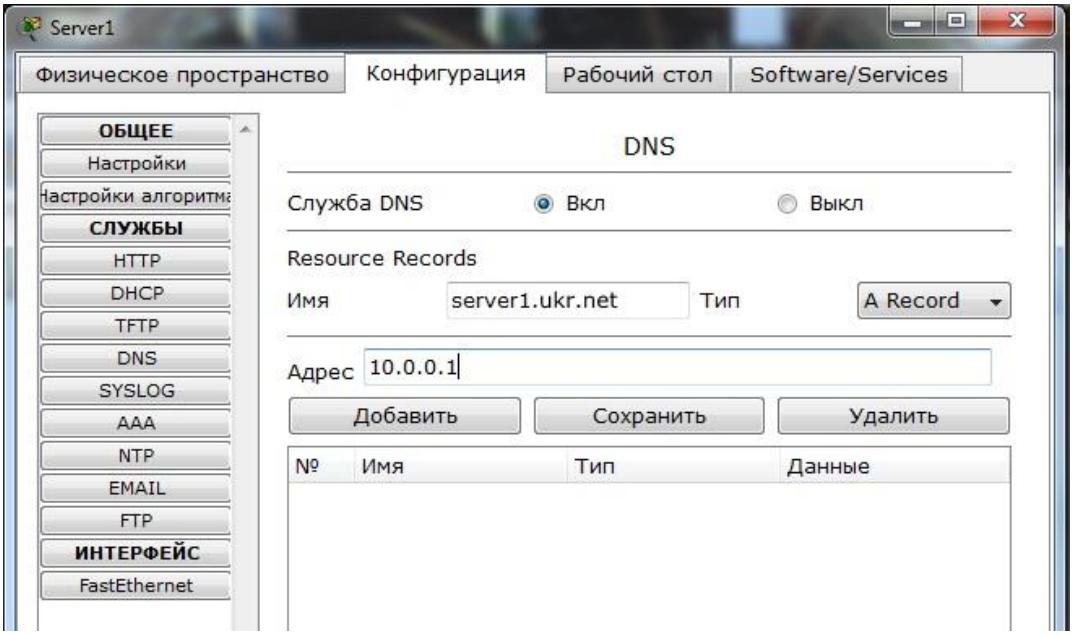


Рисунок 7.3 – Введення ресурсної записи типу A

2 - в ресурсної записи типу CNAME зв'яжіть псевдонім сайту з комп'ютером (рисунок 6.4):

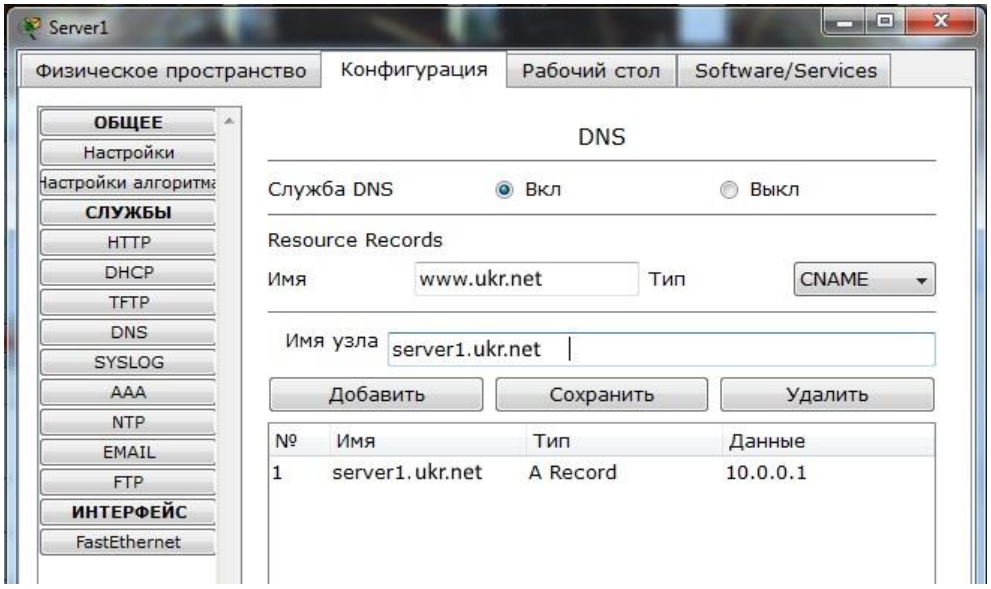


Рисунок 7.4 – Введення ресурсної записи типу CNAME

У конфігурації Server1 водите на вкладку HTTP і задайте стартову сторінку сайту www.ukr.net (Рисунок 7.5):

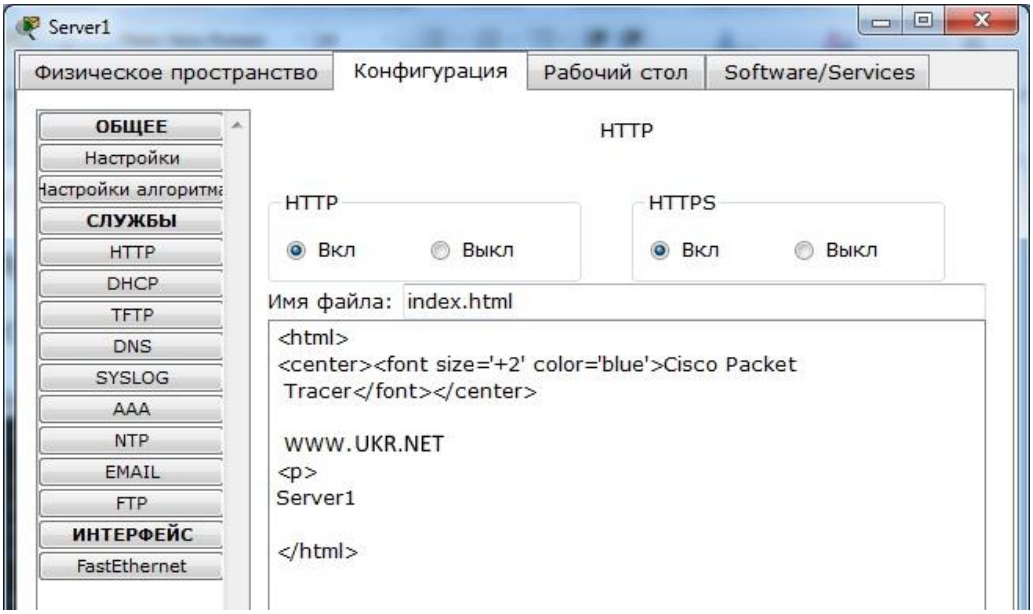


Рисунок 7.5 – Стартова сторінка сайту.

Увімкніть командний рядок на Server1 і перевірте роботу служби DNS. Для перевірки прямий зони DNS сервера введіть команду

```
SERVER> nslookup www.ukr.net
```

Якщо все правильно, то ви отримаєте відгук із зазначенням повного доменного імені DNS сервера в мережі і його IP адреса.

Етап 3. Налаштуйте DHCP службу на Server2.

Для цього увійдіть в конфігурацію Server2 і на вкладці DHCP налаштуйте службу (Рисунок 7.7):

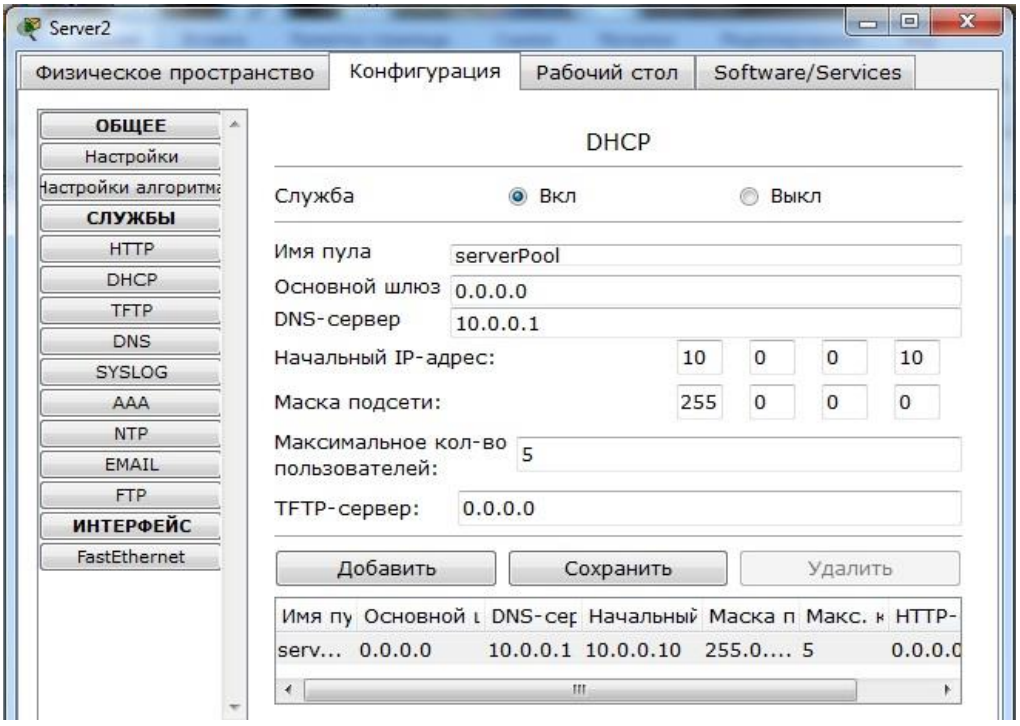


Рисунок 7.7 – Налаштування DHCP сервера.

Етап 3. Перевірка роботи клієнта.

Увійдіть в конфігурації хоста ПК1 на робочий стіл і в командному рядку налаштуйте протокол

TCP / IP.

командою

```
PC> ipconfig / release
```

скиньте старі параметри IP адреси, а командою:

```
PC> ipconfig / renew
```

Отримаєте нові параметри з DHCP сервера (Рисунок 7.8):

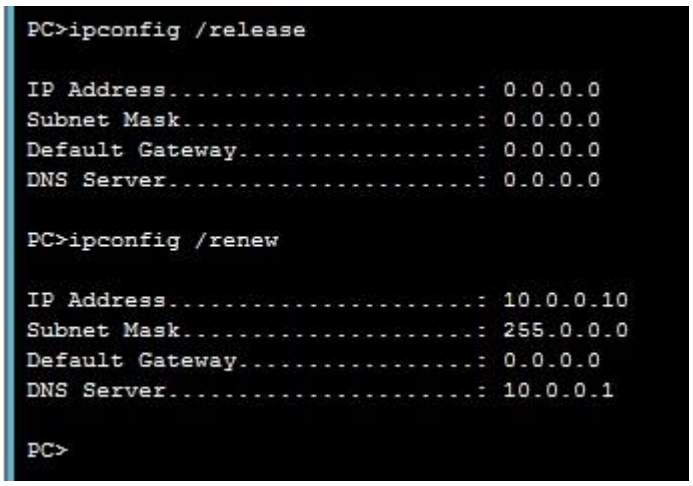


Рисунок 7.8 – Конфігурація протокол TCP / IP клієнта.

Перевірка роботи клієнта. Відкрийте сайт www.ukr.net в браузері на клієнті

ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Короткі теоретичні відомості.
3. Хід виконання роботи згідно з варіантом.
4. Висновки по виконаній роботі.

КОНТРОЛЬНІ ПИТАННЯ.

1. Що таке рекурсивний запит DNS і яка схема його роботи?
2. Вкажіть призначення типів ресурсних записів в прямій і зворотній зонах DNS.
3. Як на DNS сервері налаштовується пересилання пакетів на інші DNS сервера?
4. Опишіть роботу служби DHCP.
5. Як налаштовується клієнт DHCP?
6. Вкажіть розташування папки з контентом Web вузла і FTP сервера.
7. Як визначається склад зворотних зон DNS сервера в корпоративній мережі.
8. Продемонструйте настройку служба DNS в Cisco Paket Tracer?
9. Продемонструйте настройку служба DHCP в Cisco Paket Tracer?
10. Продемонструйте настройку служба FTP в Cisco Paket Tracer?

ЛАБОРАТОРНА РОБОТА 8.
НАЛАШТУВАННЯ СТАТИЧНОЇ МАРШРУТИЗАЦІЇ

Мета: налаштування статичної маршрутизації в Cisco Packet Tracer

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. Основні команди операційної системи Cisco IOS

Для настройки мережевого обладнання в вашому розпорядженні є різноманітні команди операційної системи Cisco IOS.

При вході в мережеве пристрій командний рядок має вигляд:

```
Switch>
```

Команди, доступні на призначеному для користувача рівні є підмножиною команд, доступних в привілейованому режимі. Ці команди дозволяють виводити на екран інформацію без зміни установок мережевого пристрою.

Щоб отримати доступ до повного набору команд, необхідно спочатку активізувати привілейований режим.

```
Press ENTER to start.
Switch>
Switch> enable
Switch #
```

Вихід з привілейованого режиму:

```
Switch # disable
Switch>
```

Про перехід в привілейований режим буде свідчити поява в командному рядку запрошення у вигляді знака #.

З привілейованого рівня можна отримувати інформацію про налаштування системи і отримати доступ до режиму глобального конфігурування та інших спеціальних режимів конфігурації, включаючи режими конфігурації інтерфейсу, под'інтерфейса, лінії, мережевого пристрою, карти маршрутів і т.п.

Для виходу з системи IOS необхідно набрати на клавіатурі команду exit (вихід):

```
Switch> exit
```

Можлива робота в наступних режимах:

- Призначений для користувача режим - це режим перегляду, у якому користувач може тільки переглядати певну інформацію про мережевому пристрої, але не може нічого міняти. В цьому режимі запрошення має вигляд:

```
Switch>
```

- Привілейований режим-підтримує команди настройки і тестування, детальну перевірку мережевого пристрою, маніпуляцію з файлами і доступ в режим конфігурації. В цьому режимі запрошення має вигляд:

```
 Switch #
```

- Режим глобального конфігурування - реалізує потужні однорядкові команди, які вирішують завдання конфігурації. В тому режимі запрошення має вигляд:

```
Switch (config) #
```

Команди в будь-якому режимі IOS розпізнає по першим унікальним символам. При натисканні табуляції IOS сам доповнить команду до повного імені.

При введенні в командному рядку будь-якого режиму імені команди і знака питання (?) На екран виводяться коментарі до команди. При введенні одного знака результатом буде список всіх команд режиму. На екран може виводитися багато екранів рядків, тому іноді в нижній частині екрана буде з'являтися підказка - More -. Для продовження слід натиснути enter або пробіл.

Команди режиму глобального конфігурування визначають поведінку системи в цілому. Крім цього, команди режиму глобального конфігурування включають команди переходу в інші режими конфігурації, які використовуються для створення конфігурацій, які потребують багаторядкових команд. Для входу в режим глобального конфігурування використовується команда привілейованого режиму configure. При введенні цієї команди слід вказати джерело команд конфігурації:

- terminal (термінал),
- memory (незалежна пам'ять або файл),
- network (сервер tftp (Trivial ftp -упрощённий ftp) в мережі).

За замовчуванням команди вводяться з терміналу консолі, наприклад:

```
Switch (config) # (commands)
Switch (config) #exit
Switch #
```

Команди для активізації приватного виду конфігурації повинні передувати командами глобального конфігурування. Так для конфігурації інтерфейсу, на можливість якої вказує запрошення

```
Switch (config-if) #
```

спочатку вводиться глобальна команда для визначення типу інтерфейсу і номера його порту:

```
Switch # conf t
Switch (config) #interface type port
Switch (config-if) # (commands)
Switch (config-if) #exit
Switch (config) #exit
```

Основні команди мережевого пристрою

1. Увійти в мережевий пристрій Router1

Router>

2. Побачити список всіх доступних команд в цьому режимі. Введіть команду, яка використовується для перегляду всіх доступних команд:

```
Router>?
```

Клавішу Enter натискати не треба.

3. Тепер увійдіть в привілейований режим

Router> enable

```
Router #
```

4. Перегляньте список доступних команд в привілейованому режимі

```
Router #?
```

5. Перейдемо в режим конфігурації

```
Router # config terminal
Router (config) #
```

6. Ім'я хоста мережевого пристрою використовується для локальної ідентифікації.

Коли ви входите в мережеве пристрій, ви бачите Ім'я хоста перед символом режиму (">" або "#"). Це ім'я може бути використано для визначення місця знаходження.

Встановіть "Router1" як ім'я вашого, мережевого пристрою.

```
Router (config) #hostname Router1
Router1 (config) #
```

7. Пароль доступу дозволяє вам контролювати доступ в привілейований

режим. Це дуже важливий пароль, тому що в привілейованому режимі можна вносити конфігураційні зміни. Встановіть пароль доступу "parol".

```
Router1 (config) #enable password parol
```

1. Давайте спробуємо цей пароль. Вийдіть з мережевого пристрою і спробуйте зайти в привілейований режим.

2.

```
Router1> en
Password: *****
Router1 #
```

Тут знаки: ***** - це ваш введення пароля. Ці знаки на екрані не помітні.

Основні Show команди.

Перейдіть в призначений для користувача режим командою disable. Введіть команду для перегляду всіх доступних show команд.

```
Router1> show?
```

1. Команда show version використовується для отримання типу платформи мережевого пристрою, версії операційної системи, імені файлу образу операційної системи, час роботи системи, обсяг пам'яті, кількість інтерфейсів і конфігураційний регістр.

2. Перегляд часу:

```
Router1> show clock
```

3. У флеш-пам'яті мережного пристрою зберігається файл-образ операційної системи Cisco IOS. На відміну від оперативної пам'яті, в реальних пристроях флеш пам'ять зберігає файл-образ навіть при збої живлення.

```
 Router1> show flash
```

4. ІКС мережевого пристрою за умовчанням сохраняет10 останніх введених команд

```
Router1> show history
```

5. Дві команди дозволять вам повернутися до командам, введеним раніше. Натисніть на стрілку вгору або <ctrl> P.

6. Дві команди дозволять вам перейти до наступної команді, збереженої в буфері.

Натисніть на стрілку вниз або <ctrl> N

7. Можна побачити список хостів і IP-Адреси всіх їх інтерфейсів

```
Router1> show hosts
```

8. Наступна команда виведе детальну інформацію про кожного інтерфейсі

```
Router1> show interfaces
```

9. Наступна команда виведе інформацію про кожну telnet сесії:

```
Router1> show sessions
```

10. Наступна команда показує конфігураційні параметри терміналу:

```
Router1> show terminal
```

11. Показати список всіх користувачів, приєднаних до пристрою по термінальним лініях:

```
Router1> show users
```

12. Команда показує стан контролерів інтерфейсів

```
Router1> show controllers
```

13. Перейти в привілейований режим.

```
Router1> en
```

14. Введіть команду для перегляду всіх доступних show команд.

```
Router1 # show?
```

Привілейований режим включає в себе всі show команди призначеного для користувача режиму і ряд нових.

15. Подивимося активну конфігурацію в пам'яті мережного пристрою. Необхідний привілейований режим. Активна конфігурація автоматично не зберігається і буде втрачена в разі збою електроживлення. Щоб зберегти настройки роутера використовуйте наступні команди:

збереження поточної конфігурації:

```
Router # write memory
```

або

```
Router # copy run start
```

Перегляд збереженої конфігурації:

```
Router # Show configuration
```

або

```
Router1 # show running-config
```

У рядку more, натисніть на клавішу пробіл для перегляду наступної сторінки інформації.

16. Наступна команда дозволить вам побачити поточний стан протоколів третього рівня:

```
Router # show protocols
```

Введення в конфігурацію інтерфейсів.

Розглянемо команди настройки інтерфейсів мережевого пристрою.

На мережевому пристрої Router1 увійдемо в режим конфігурації:

```
Router1 # conf t
Router1 (config) #
```

2. Тепер ми хочемо налаштувати Ethernet інтерфейс. Для цього ми повинні зайти в режим конфігурації інтерфейсу:

```
Router1 (config) #interface FastEthernet0 / 0
Router1 (config-if) #
```

3. Подивимося всі доступні в цьому режимі команди:

```
Router1 (config-if) #?
```

Для виходу в режим глобальної конфігурації наберіть exit. Знову увійдіть в режим конфігурації інтерфейсу:

```
Router1 (config) #int fa0 / 0
```

Ми використовували скорочене ім'я інтерфейсу.

4. Для кожної команди ми можемо виконати протилежну команду, поставивши перед нею слово no. Наступна команда включає цей інтерфейс:

```
Router1 (config-if) #no shutdown
```

5. Додамо до інтерфейсу опис:

```
Router1 (config-if) #description Ethernet interface on Router 1
```

Щоб побачити опис цього інтерфейсу, перейдіть в привілейований режим і виконайте команду show interface:

```
Router1 (config-if) #end
Router1 # show interface
```

6. Тепер приєднаєтеся до інших мережних пристроїв Router 2 і поміняйте ім'я його хоста на Router2:

```
Router # conf t
Router (config) #hostname Router2
```

Увійдемо на інтерфейс FastEthernet 0/0:

```
  Router2 (config) #interface fa0 / 0
```

Увімкніть інтерфейс:

```
Router2 (config-if) #no shutdown
```

Тепер, коли інтерфейси на двох кінцях нашого Ethernet з'єднання включені на екрані з'явиться повідомлення про зміну стану інтерфейсу на активну.

7. Перейдемо до конфігурації послідовних інтерфейсів. Зайдемо на Router1.

Перевіримо, яким пристроєм виступає наш маршрутизатор для послідовної лінії зв'язку: кінцевим пристроєм DTE (data terminal equipment), яким пристроєм зв'язку DCE (data circuit):

```
Router1 # show controllers fa0 / 1
```

Якщо бачимо повідомлення:

```
DCE cable
```

то наш маршрутизатор є пристроєм зв'язку та він повинен задавати частоту синхронізації тактових імпульсів, використовуваних при передачі даних. Частота береться з певного ряду частот.

```
Router1 # conf t
Router1 (config) #int fa0 / 1
Router1 (config-if) #clock rate?
```

Виберемо частоту 64000

```
Router1 (config-if) #clock rate 64000
```

і включаємо інтерфейс

```
Router1 (config-if) #no shut
```

2 Протоколи маршрутизації

Протоколи маршрутизації - це правила, за якими здійснюється обмін інформацією про шляхи передачі пакетів між маршрутизаторами. Протоколи характеризуються часом збіжності, втратами і масштабованість. В даний час використовується кілька протоколів маршрутизації.

Одна з головних завдань маршрутизатора полягає у визначенні найкращого шляху до заданого адресату. Маршрутизатор визначає шляхи (маршрути) до адресатів або зі статичної конфігурації, введеної адміністратором, або динамічно на підставі маршрутної інформації, отриманої від інших маршрутизаторів. Маршрутизаторіобмінюються маршрутної інформацією за допомогою протоколів маршрутизації.

Маршрутизатор зберігає таблиці маршрутів в оперативній пам'яті. Таблиця маршрутів це список найкращих відомих доступних маршрутів. Маршрутизатор використовує цю таблицю для прийняття рішення куди направляти пакет.

У разі статичної маршрутизації адміністратор вручну визначає маршрути до мереж призначення.

У разі динамічної маршрутизації - маршрутизатори дотримуються правил, що визначаються протоколами маршрутизації для обміну інформацією про маршрути і вибору кращого шляху.

Статичні маршрути не змінюються самим маршрутизатором. Динамічні маршрути змінюються самим маршрутизатором автоматично при отриманні інформації про зміну маршрутів від сусідніх маршрутизаторів. Статична маршрутизація споживає мало обчислювальних ресурсів і корисна в мережах, які не мають кількох шляхів до адресата призначення. Якщо від маршрутизатора до маршрутизатора є тільки один шлях, то часто використовують статичну маршрутизацію.

Проведемо налаштування статичної маршрутизації за допомогою графічних майстрів інтерфейсу Cisco Packet Tracer.

Створіть схему мережі, представлену на рисунку 8.1.

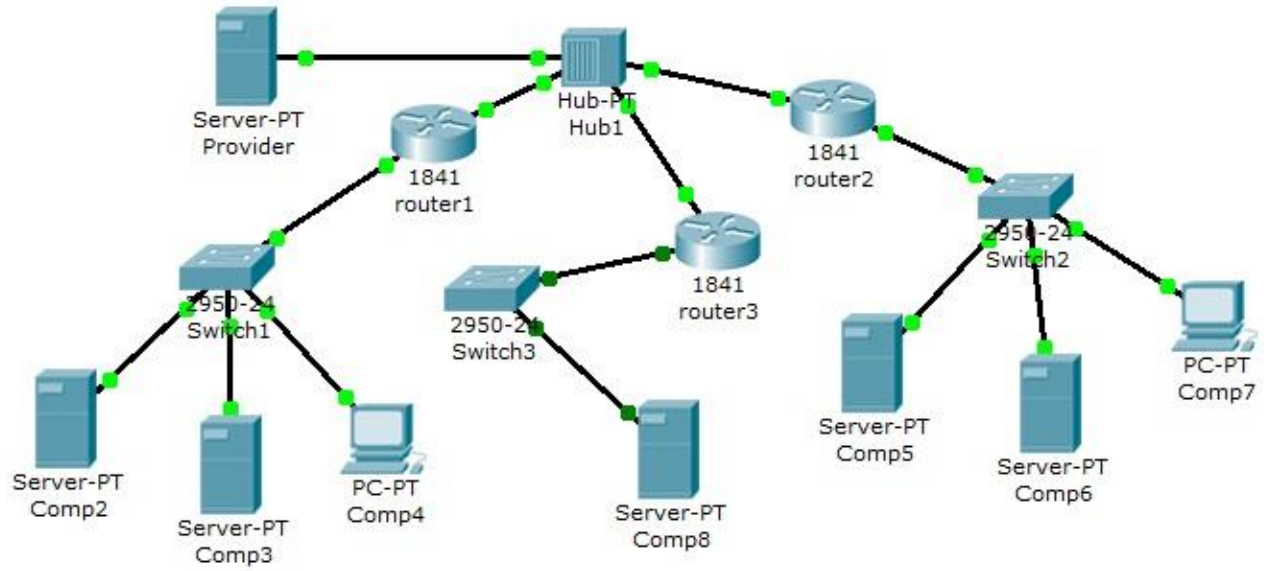


Рисунок 8.1 – Схема мережі.

На даній схемі представлена корпоративна мережа, що складається з наступних компонентів:
Мережа 1 - на Switch1 замикається мережу першої організації (таблиця 8.1):

Таблиця 8.1 – Мережа першої організації.

Комп'ютер	IP адреса	функції
Comp2	192.168.1.2/24	DNS і HTTP сервер
Comp3	192.168.1.3/24	DHCP сервер
Comp4	Отримано з DHCP сервера	клієнт мережі

В даній мережі на Comp2 встановлений DNS і Web сервер з сайтом організації.
На Comp3 встановлений DHCP сервер. Комп'ютер Comp4 отримує з DHCP сервера IP адреса, адреса DNS сервера провайдера (сервер Provider) і шлюз. Шлюз в мережі - 192.168.1.1/24.

Мережа 2 - на Switch2 замикається мережу іншої організації (таблиця 8.2):

Таблиця 8.2 – Мережа другий організації.

комп'ютер	IP адреса	функції
Comp5	10.0.0.5/8	DNS і HTTP сервер
Comp6	10.0.0.6/8	DHCP сервер
Comp7	Отримано з DHCP сервера	клієнт мережі

В даній мережі на Comp5 встановлений DNS і Web сервер з сайтом організації.
На Comp4 встановлений DHCP сервер. Комп'ютер Comp7 отримує з DHCP сервера IP адреса, адреса DNS сервера провайдера (сервер Provider) і шлюз. Шлюз в мережі - 10.0.0.1/8.
Мережа 3 - на Hub1 замикається міська мережа 200.200.200.0/24. У мережі встановлено DNS сервер провайдера (комьютер Provaider з IP адресою -200.200.200.10 / 24), що містить дані по всім сайтам мережі (Comp2, Comp5, Comp8).
Мережа 4 - маршрутизатор Router3 виводить міську мережу в інтернет через комутатор Switch3 (мережа 210.210.210.0/24). На Comp8 (IP адреса 210.210.210.8/24, шлюз 210.210.210.3/24.) Встановлено DNS і Web сервер з сайтом.
Маршрутизатор мають по два інтерфейси:
Router1 - 192.168.1.1/24 і 200.200.200.1/24.
Router2 - 10.0.0.1/8 і 200.200.200.2/24.

Router3 - 210.210.210.3/24 і 200.200.200.3/24.

ХІД РОБОТИ

Завдання 1.

Налаштувати

1 - мережі організацій;

2 - DNS сервер провайдера;

3 - статичні таблиці маршрутизації на роутерах;

4 - перевірити роботу мережі - на кожному з комп'ютерів - Comp4, Comp7 і Comp8. З кожного з них повинні відкриватися все три сайти корпоративної мережі.

У попередніх лабораторних роботах розглядалася настройка мережевих служб і DNS сервера. Приступимо до налаштування статичної маршрутизації на роутерах. Оскільки на представленій схемі чотири мережі, то таблиці маршрутизації як мінімум повинні містити записи до кожної з цих мереж - тобто чотири записи. На роутерах Cisco в таблицях маршрутизації як правило, не прописуються шляхи до мереж, до яких під'єднані інтерфейси роутера. Тому на кожному маршрутизаторі необхідно внести по два записи.

Налаштуйте перший маршрутизатор.

Для цього увійдіть в конфігурацію маршрутизатора і в інтерфейсах встановіть IP адресу і маску підмережі. Потім в розділі маршрутизації відкрийте вкладку СТАТИЧНА, внесіть дані (Рисунок 9.2) і натисніть кнопку ДОДАТИ:

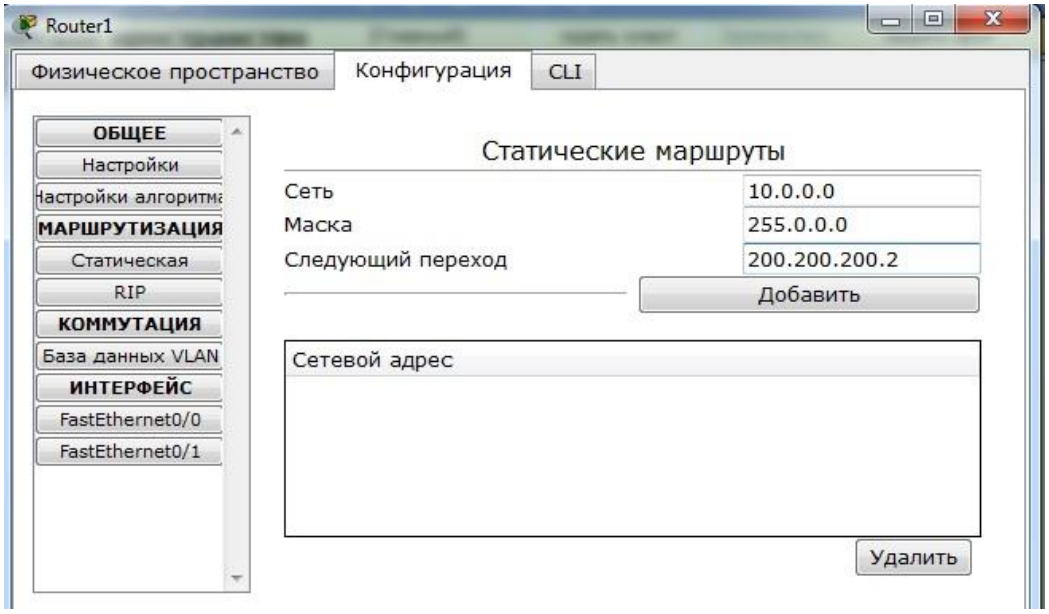


Рисунок 8.2 – Дані для мережі 10.0.0.0/8.

В результаті у вас повинні з'явитися два записи в таблиці маршрутизації (Рисунок 9.3):

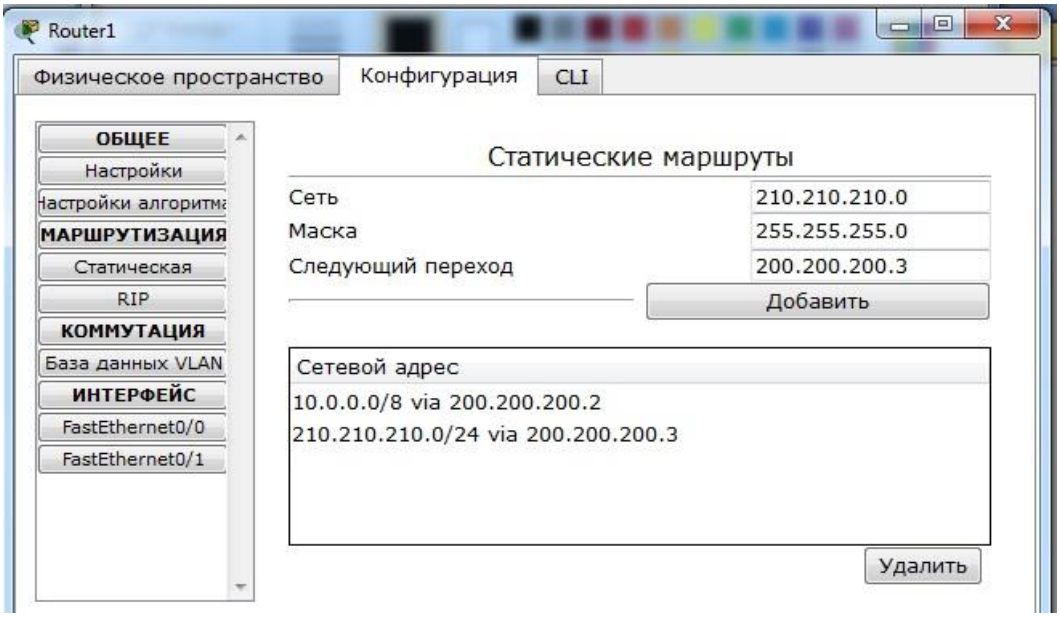


Рисунок 8.3 – Формування статичної таблиці маршрутизації.

Щоб подивитися повну настройку таблиці маршрутизації, виберіть в бічному графічному меню інструмент ПЕРЕВІРКА (піктограма лупи), клацніть у схемі на роутері і виберіть у спадному меню пункт ТАБЛИЦЯ МАРШРУТИЗАЦІЇ.

Після налаштування всіх роутерів у вашій мережі стануть доступні IP адреси будь-якого комп'ютера і ви зможете відкрити будь-який сайт з комп'ютерів Comp4, Comp7 і Comp8.

Завдання 2

Виконайте самостійно наступну роботу, схема мережі для якої представлена на рисунку 8.4.

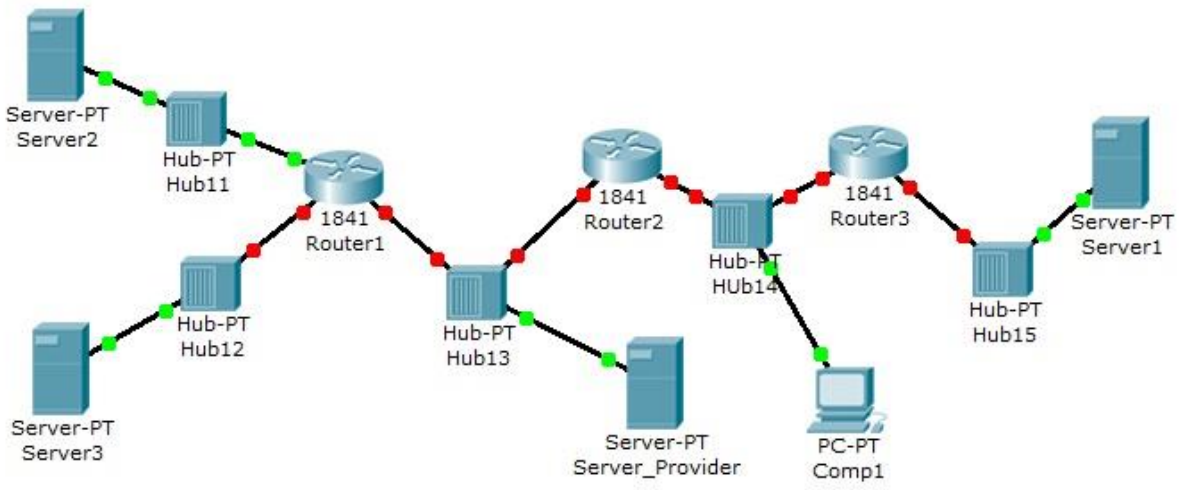


Рисунок 8.4 – Схема мережі.

П'ять концентраторів представляють наступні п'ять мереж:

Hub11 - мережа 11.0.0.0
Hub12 - мережа 12.0.0.0
Hub13 - мережа 13.0.0.0
Hub14 - мережа 14.0.0.0
Hub15 - мережа 15.0.0.0

Router 1 має додатковий мережевий інтерфейс, який додається з модуля WIC-1ENET при вимкненому маршрутизаторі.

У мережі три Web вузла на Server1, Server2 і Server3.

Сервера і комп'ютер мають довільні IP адреси зі шлюзами своїх роутерів.

Інтерфейси роутерів визначаються мережею на концентраторі і номером роутера.

Наприклад для Router3: 15.0.0.3 і 14.0.0.3

Задача:

комп'ютер Comp1 повинен відкрити всі три сайти на серверах корпоративної мережі. В налаштуваннях Comp1 як DNS сервера вказано DNS сервер провайдера на Server_Provider.

Послідовність виконання.

Корпоративна мережа 15.0.0.0/8 розбита на десять підмереж, з них в даний момент задіяно шість підмереж в шести різних підрозділах організації. Пристрої мережі:

- три маршрутизатора;
- шість комутаторів (по одному в кожному відділі на підмережа);
- один комп'ютер в кожній мережі.

Розрахунки.

1 - розрахуйте параметри підмереж і задайте на комп'ютерах IP адресу, маску і шлюз в кожній окремій підмережі;

2 - створіть довільну топологію мережі, з'єднавши маршрутизатори з підмережами в будь-якому порядку. При цьому з'єднайте маршрутизатори між собою довільно - безпосередньо, через штатні комутатори підрозділу або додаткові комутатори;

3 - перевірте працездатність корпоративної мережі командою PING - всі комп'ютери повинні бути доступні.

ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Хід виконання роботи згідно з варіантом.
3. Висновки по виконаній роботі.

КОНТРОЛЬНІ ПИТАННЯ.

1. Якою командою можна подивитися поточні настройки маршрутизатора?
2. Якими командами налаштовується мережевий інтерфейс маршрутизатора.
3. Перерахуйте основні режими конфігурації при налаштуванні маршрутизатора.
4. Як подивитися таблицю маршрутизації на маршрутизаторі?
5. Які команди формують таблицю маршрутизації?
6. Якими командами налаштовується взаємодія між VLAN?

ЛАБОРАТОРНА РОБОТА 9
НАЛАШТУВАННЯ ПРОТОКОЛУ RIP

Мета: навчитись налаштовувати протокол RIP

ТЕОРЕТИЧНІ ВІДОМОСТІ

Статична маршрутизація не підходить для великих, складних мереж тому, що зазвичай мережі включають надлишкові зв'язку, багато протоколів і змішані топології.

Маршрутизатор в складних мережах повинні швидко адаптуватися до змін топології і вибирати кращий маршрут з багатьох кандидатів.

IP мережі мають ієрархічну структуру. З точки зору маршрутизації мережу розглядається як сукупність автономних систем. В автономних підсистемах великих мереж для маршрутизації на інші автономні системи широко використовуються маршрути за замовчуванням.

Динамічна маршрутизація може бути здійснена з використанням одного і більше протоколів. Ці протоколи часто групуються відповідно до того, де вони використовуються. Протоколи для роботи всередині автономних систем називають внутрішніми протоколами шлюзів (interior gateway protocols (IGP)), а протоколи для роботи між автономними системами називають зовнішніми протоколами шлюзів (exterior gateway protocols (EGP)). До протоколів IGP відносяться RIP, RIP v2, IGRP, EIGRP, OSPF і IS-IS. Протоколи EGP3 і BGP4 відносяться до EGP. Всі ці протоколи можуть бути розділені на два класи: дистанційно-векторні протоколи і протоколи стану зв'язку.

Дистанційно-векторна маршрутизація.

Маршрутизатор використовують метрики для оцінки або вимірювання маршрутів. Коли від маршрутизатора до мережі призначення існує багато маршрутів, і всі вони використовують один протокол маршрутизації, то маршрут з найменшою метрикою розглядається як кращий. Якщо використовуються різні протоколи маршрутизації, то для вибору маршруту використовується адміністративні відстані, які призначаються маршрутам операційною системою маршрутизатора. RIP використовує в якості метрики кількість переходів (хопов).

Дистанційно-векторна маршрутизація базується на алгоритмі Белмана-Форда. Через певні моменти часу маршрутизатор передає сусіднім маршрутизаторам всю свою таблицю маршрутизації. Такі прості протоколи як RIP і IGRP просто поширюють інформацію про таблиці маршрутів через все інтерфейси маршрутизатора в широкомовному режимі без уточнення точної адреси конкретного сусіднього маршрутизатора.

Сусідній маршрутизатор, отримуючи широкомовлення, порівнює інформацію зі своєю поточною таблицею маршрутів. У неї додаються маршрути до нових мереж або маршрути до відомих мереж з кращого метрикою. Відбувається видалення неіснуючих маршрутів. Маршрутизатор додає свої власні значення до метрик отриманих маршрутів. Нова таблиця маршрутизації знову поширюється по сусідніх маршрутизаторів.

Завдання 1

Створіть схему, представлену на рисунку 9.1.

На схемі представлені наступні три мережі:

Switch1 - мережа 10.11.0.0/16.
Switch2 - мережа 10.12.0.0/16.
Мережа для роутерів - 10.10.0.0/16.

Введіть на пристроях наступну адресацію:

Маршрутизатор мають по два інтерфейси:

Router1 - 10.11.0.1/16 і 10.10.0.1/16.
Router2 - 10.10.0.2/16 і 10.12.0.1/16.
ПК11 - 10.11.0.11/16.
ПК12 - 10.12.0.12/16.

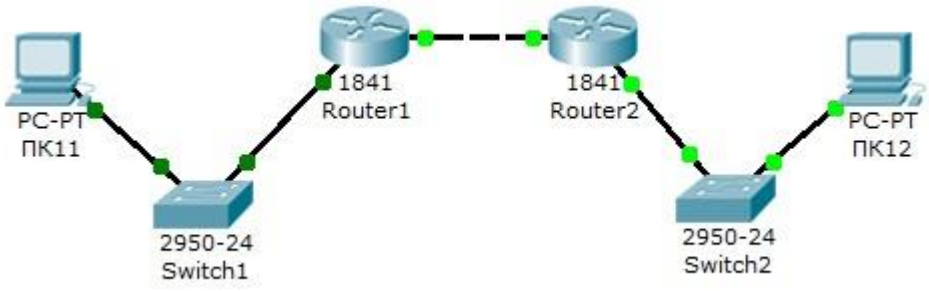


Рисунок 9.1 – Схема мережі.

Проведемо настройку протоколу RIP на маршрутизаторі Router1.

Увійдіть в конфігурації в консоль роутера і виконайте наступні настройки (при введенні команд маску підмережі можна не вказувати, тому що вона буде братися автоматично з налаштувань інтерфейсу роутера):

Увійдіть в привілейований режим:

```
Router1>en
```

Увійдіть в режим конфігурації:

```
Router1> #conf t
```

Увійдіть в режим конфігурації протоколу RIP:

```
Router1 (config) #router rip
```

Підключіть клієнтську мережу до роутера:

```
Router1 (config-router) #network 10.11.0.0
```

Підключіть другу мережу до роутера:

```
Router1 (config-router) #network 10.10.0.0
```

Задайте використання другої версії протокол RIP:

```
Router1 (config-router) #version 2
```

Вийдіть з режиму конфігурації протоколу RIP:

```
Router1 (config-router) #exit
```

Вийдіть з консолі налаштувань:

```
Router1 (config) #exit
```

Збережіть налаштування в пам'ять маршрутизатора:

```
Router1> #write memory
```

Аналогічно проведіть настройку протоколу RIP на маршрутизаторі Router2.

Перевірте зв'язок між комп'ютерами ПК11 і ПК12 командою ping.

Якщо зв'язок є - все налаштування зроблені вірно.

Приклад 2 Налаштування протоколу RIP в корпоративній мережі

Протоколи маршрутизації пропонують кращу масштабованість і збіжність у порівнянні з дистанційно-векторними протоколами. Робота протоколів базується на алгоритмі Дейкстри, який часто називають алгоритмом «найкоротший шлях - першим» (shortest path first SPF)). Найбільш типовим представником є протокол OSPF (Open Shortest Path First).

Маршрутизатор бере до розгляду стан зв'язку інтерфейсів інших маршрутизаторів в мережі. Маршрутизатор будує повну базу даних всіх станів зв'язку в своїй області, тобто має достатньо інформації для створення свого відображення мережі. Кожен маршрутизатор потім самостійно виконує SPF-алгоритм на своєму власному відображенні мережі або базі даних станів зв'язку для визначення кращого шляху, який заноситься в таблицю маршрутів. Ці шляхи до інших мереж формують дерево з вершиною в вигляді локального маршрутизатора.

Маршрутизатор сповіщають про стан своїх зв'язків всім маршрутизаторів в області. Таке повідомлення називають LSA (link-state advertisements).

На відміну від дистанційно-векторних маршрутизаторів, маршрутизатори стану зв'язку можуть формувати спеціальні відносини зі своїми сусідами.

Має місце початковий наплив LSA пакетів для побудови бази даних станів зв'язку. Далі оновлення маршрутів проводиться тільки при зміні станів зв'язку або, якщо стан не змінився протягом певного інтервалу часу. Якщо стан зв'язку змінилося, то часткове оновлення пересилається негайно. Воно містить тільки стану зв'язків, які змінилися, а не всю таблицю маршрутів.

Адміністратор, який дбає про використання ліній зв'язку, знаходить ці часткові і рідкісні поновлення ефективною альтернативою дистанційно-векторної маршрутизації, яка передає всю таблицю маршрутів через регулярні проміжки часу. Протоколи стану зв'язку мають більш швидку збіжність і краще використання смуги пропускання в порівнянні з дистанційно-векторними протоколами. Вони перевершують дистанційно-векторні протоколи для мереж будь-яких розмірів, проте мають два головні недоліки: підвищені вимоги до обчислювальної потужності маршрутизаторів і складне адміністрування.

ХІД РОБОТИ

Завдання №2. Створіть схему, представлену на рисунку 9.2.

У чотирьох мережах: 11.0.0.0/8, 12.0.0.0/8, 13.0.0.0/8 і 14.0.0.0/8 встановлені комп'ютери з адресами:

Comp1 - 11.0.0.11, маска 255.0.0.0
Comp2 - 12.0.0.12, маска 255.0.0.0
Comp3 - 13.0.0.13, маска 255.0.0.0
Comp4 - 14.0.0.14, маска 255.0.0.0

Між ними знаходиться корпоративна мережа з шістьма маршрутизаторами. На маршрутизаторах задані наступні інтерфейси.

Таблиця 9.1 – Інтерфейси маршрутизаторів

маршрутизатор	інтерфейс 1	інтерфейс 2	інтерфейс 3
Router1	11.0.0.1/8	21.0.0.1/8	31.0.0.1/8
Router2	21.0.0.2/8	51.0.0.2/8	
Router3	12.0.0.3/8	61.0.0.3/8	51.0.0.3/8
Router4	31.0.0.4/8	81.0.0.4/8	13.0.0.4/8
Router6	61.0.0.6/8	81.0.0.6/8	14.0.0.6/8

Налаштувати маршрутизацію по протоколу RIP на кожному з маршрутизаторів. Для цього:

1 - налаштувати всі маршрутизатори, як це було показано в прикладі 1 вище;

2 - перевірити налаштування маршрутизаторів по таблиці маршрутизації.

Щоб переконатися в тому, що маршрутизатор дійсно правильно сконфігурували і працює коректно, перегляньте таблицю RIP роутера, використовуючи команду show наступним чином:

```
Router #show ip route rip
```

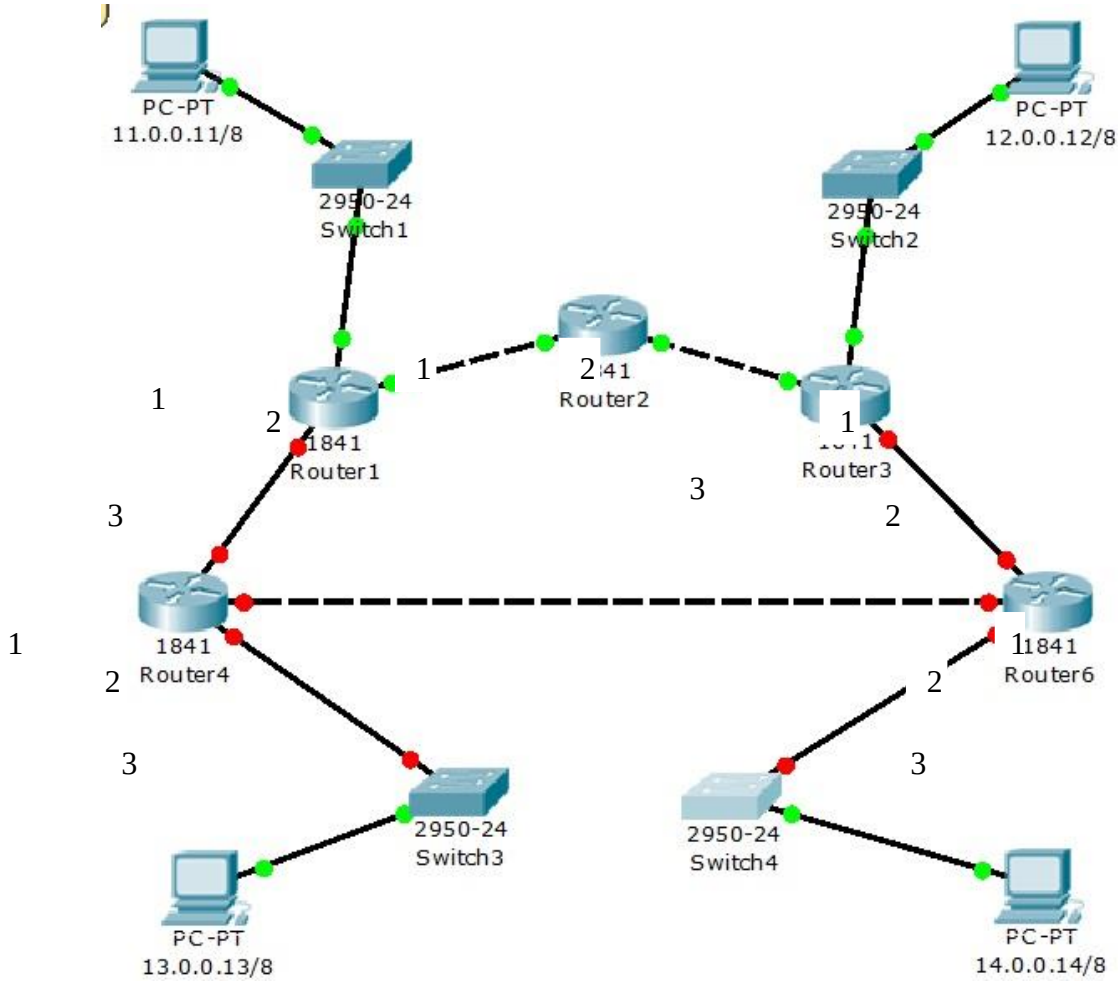


Рисунок 9.2 – Схема мережі.

Наприклад для шостого маршрутизатора Router6 таблиця буде мати такий вигляд (рис.9.3):

```
Router6>en
Router6#show ip route rip
R    11.0.0.0/8 [120/2] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    12.0.0.0/8 [120/1] via 61.0.0.3, 00:00:08, Ethernet0/0/0
R    13.0.0.0/8 [120/1] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    21.0.0.0/8 [120/2] via 61.0.0.3, 00:00:08, Ethernet0/0/0
                [120/2] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    31.0.0.0/8 [120/1] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    51.0.0.0/8 [120/1] via 61.0.0.3, 00:00:08, Ethernet0/0/0
Router6#
```

Рисунок 9.3 – Таблиця маршрутизації RIP

Дана таблиця показує, що до мережі 21.0.0.0 є два шляхи: через Router4 (мережа 81.0.0.0) і через Router3 (мережа 61.0.0.0).

Проведіть діагностику мережі:

1 - перевірте, чи правильно встановлена за допомогою команд ping і tracert в консолі кождого комп'ютера;

2 - проведіть ту ж діагностику мережі при вимкненому маршрутизаторе Router6.

3 - перевірте зв'язок між комп'ютерами з адресами 12.0.0.12 і 13.0.0.13.

Кількість проміжних роутерів при проходженні пакета по мережі при включеному і вимкненому маршрутизаторі 6 повинно бути різним. При включеному Router6 має бути на одиницю менше, ніж при вимкненому.

Завдання №3.

Створіть схему, представлену на рисунку 9.4.

Завдання.

1. Налаштуйте корпоративну мережу з використанням протоколу RIP.
2. Перевірте зв'язок між комп'ютерами Comp1 і Comp3 за допомогою команд ping і tracert при включеному і вимкненому п'ятому маршрутизаторі.
3. Перевірте зв'язок між комп'ютерами ПК0 і Comp1 за допомогою команд ping і tracert при включеному і вимкненому другому маршрутизаторі.

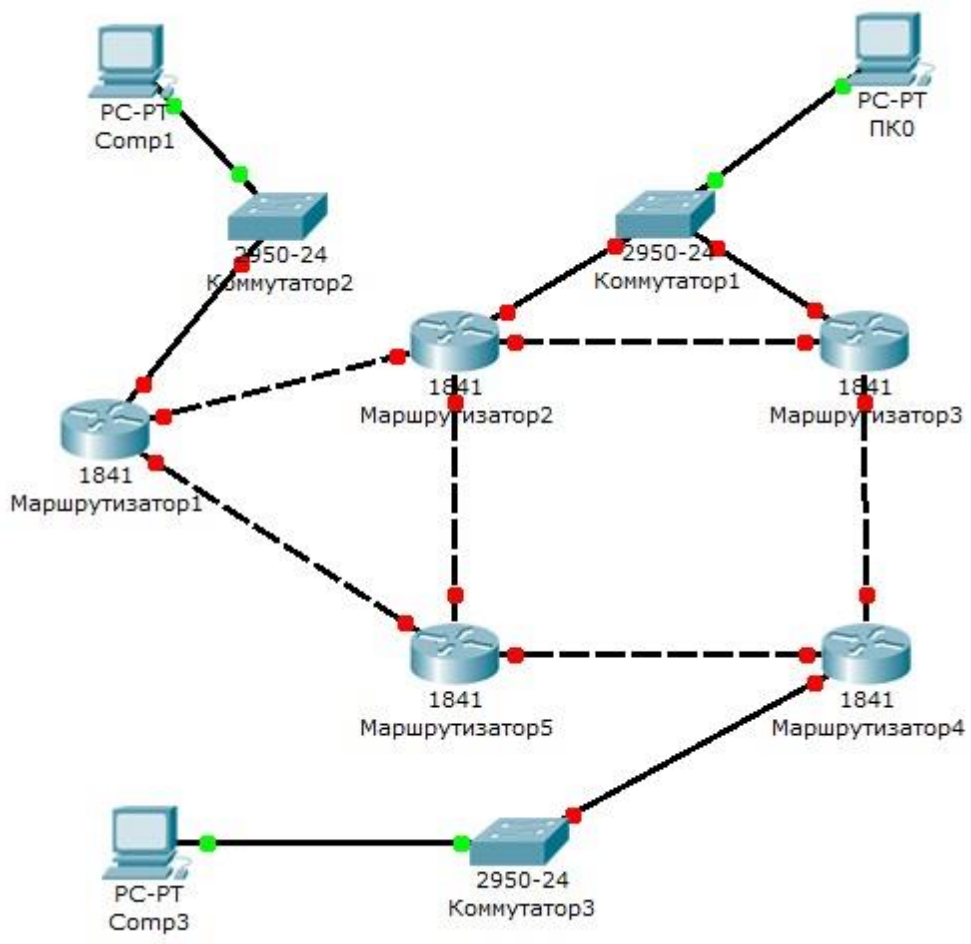


Рисунок 9.4 – Схема мережі.

ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
3. Хід виконання роботи згідно з варіантом.
4. Висновки по виконаній роботі.

КОНТРОЛЬНІ ПИТАННЯ

1. У чому переваги статичної маршрутизації?
2. Дайте характеристику параметрам статичної таблиці маршрутизації?
3. Які етапи при установці пристрою притаманні маршрутизаторів компанії Cisco, але відсутні у комутаторів?
4. Яку із зазначених нижче команд можна зустріти в інтерфейсі командного рядка маршрутизатора, але не комутатора?

- команда cloc rate;

- команда ip address маска адреса;
- команда ip address dhcp;
- команда interface vlan 1

5. Чим відрізняються інтерфейси командного рядка маршрутизатора і комутатора компанії Cisco?
6. Яка із зазначених нижче команд не покаже настройки IP-адрес і масок в своєму пристрої?

- show running-config;
- show protocol тип номер;
- show ip interface brief;
- show version

7. Перерахуйте основні функції маршрутизатора відповідно до рівнів моделі OSI.

ЛАБОРАТОРНА РОБОТА №10.
НАЛАШТУВАННЯ ПРОТОКОЛУ OSPF.

Мета: навчитись налаштовувати протокол OSPF

ТЕОРЕТИЧНІ ВІДОМОСТІ

OSPF (англ. Open Shortest Path First) – протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology), що використовує для знаходження найкоротшого шляху Алгоритм Дейкстри (Dijkstra's algorithm).

Протокол OSPF був розроблений IETF в 1988 році. Остання версія протоколу представлена в RFC 2328. Протокол OSPF являє собою протокол внутрішнього шлюзу (Interior Gateway Protocol – IGP). Протокол OSPF поширює інформацію про доступні маршрути між маршрутизаторами однієї автономної системи.

Протоколи маршрутизації пропонують кращу масштабованість і збіжність у порівнянні з дистанційно-векторними протоколами. Робота протоколів базується на алгоритмі Дейкстри, який часто називають алгоритмом «найкоротший шлях - першим» (shortest path first SPF)). Найбільш типовим представником є протокол OSPF (Open Shortest Path First).

Властивості OSPF:

- висока швидкість збіжності;
- підтримка мережних масок змінної довжини VLSM;
- відсутність обмежень досяжності;
- оптимальне використання пропускної здатності мережі;
- оптимальний вибір шляху маршрутизації.

Згідно з RFC 2328 є незапатентований тобто відкритий для громадськості протокол, таким же, як є протокол RIP. Але OSPF на відміну від RIP, має значно більшу швидкість збіжності (рекалькуляції таблиці маршрутизації), немає обмеження на довжину шляху 15-ма хопами (англ. hop, укр. стрибок), враховує пропускну здатність мережі при виборі маршруту. Все це робить OSPF потужним, масштабованим протоколом маршрутизації.

ХІД РОБОТИ

Створіть схему, представлену на рисунку 10.1.

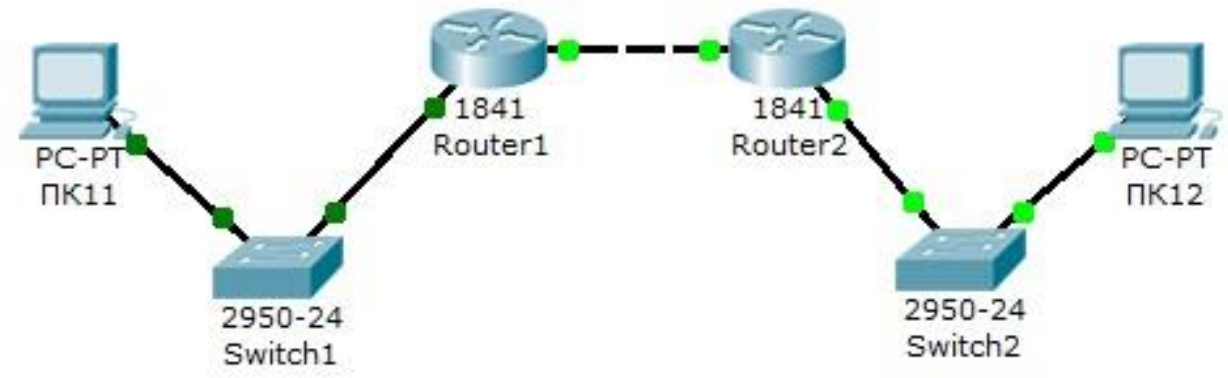


Рисунок 10.1 – Схема мережі.

На схемі представлені наступні три мережі:
Switch1 - мережа 10.11.0.0/16.
Switch2 - мережа 10.12.0.0/16.
Мережа для маршрутизаторів - 10.10.0.0/16.

Введіть на пристроях наступну адресацію. Маршрутизатор мають по два інтерфейси:

Router1 - 10.11.0.1/16 і 10.10.0.1/16.
Router2 - 10.10.0.2/16 і 10.12.0.1/16.
ПК11 - 10.11.0.11/16.
ПК12 - 10.12.0.12/16.

Візьміть схему мережі, представлену на рис 6.1.

Проведемо настройку протоколу OSPF на маршрутизаторі Router1.

Увійдіть в конфігурації в консоль роутера і виконайте наступні настройки (при введенні команд маску підмережі можна не вказувати, тому що вона буде братися автоматично з налаштувань інтерфейсу роутера):

Увійдіть в привілейований режим:

```
Switch>en
```

Увійдіть в режим конфігурації:

```
Switch1 #conf t
```

Увійдіть в режим конфігурації протоколу OSPF:

```
Router1 (config) #router ospf 1
```

У команді router ospf <ідентіфікатор_процесса> під ідентифікатором процесу розуміється унікальне числове значення для кожного процесу роутінга на маршрутизаторі. Дане значення повинно бути більше в інтервалі від 1 до 65535. У OSPF процесам на роутерах однієї зони прийнято присвоювати один і той же ідентифікатор.

Підключіть клієнтську мережу до роутера:

```
Router1 (config-router) #network 10.11.0.0
```

Підключіть другу мережу до роутера:

```
Router1 (config-router) #network 10.10.0.0
```

Задайте використання другої версії протокол OSPF:

```
Router1 (config-router) #version 2
```

Вийдіть з режиму конфігурації протоколу OSPF:

```
Router1 (config-router) #exit
```

Вийдіть з консолі налаштувань:

```
Router1 (config) #exit
```

Збережіть налаштування в пам'ять маршрутизатора:

```
Switch1 #write memory
```

Аналогічно проведіть настройку протоколу OSPF на маршрутизаторі Router2.

ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Короткі теоретичні відомості.
3. Хід виконання роботи згідно з варіантом.
4. Висновки по виконаній роботі.

КОНТРОЛЬНІ ПИТАННЯ

1. У чому відмінність між топологічної і дистанційно-векторної маршрутизацією?
2. Опишіть схему роботи протоколу RIP.

3. Опишіть схему роботи протоколу OSPF.
4. Перерахуйте основні етапи установки маршрутизатора.
5. Опишіть чотири етапи завантаження маршрутизатора.
6. Які із зазначених нижче протоколів працюють по дистанційно-векторному алгоритмі і які їхні основні відмінності?
   - RIP;
   - IGRP;
   - EIGRP;
   - OSPF
7. Дайте характеристику класів протоколів маршрутизації.
8. Наведіть класифікацію протоколів маршрутизації на основі алгоритмів їх роботи.
9. Зробіть порівняння класових і безкласових протоколів маршрутизації.
10. Зробіть порівняння протоколів маршрутизації внутрішнього шлюзу.
11. Опишіть етапи настройки протоколу маршрутизації RIP-2.

ЛАБОРАТОРНА РОБОТА №11
БЕЗДРОТОВІ СЕНСОРНІ МЕРЕЖІ

Мета: Навчитись налаштовувати бездротові сенсорні мережі

ТЕОРЕТИЧНІ ВІДОМОСТІ

Імітаційне моделювання має важливе значення для вивчення БСМ, будучи розповсюдженим способом для тестування нових додатків і протоколів у даній області. Є два ключові аспекти в моделюванні БСМ: правильність імітаційної моделі й придатність конкретних інструментів для реалізації даної моделі. Фундаментальною проблемою є вибір між точністю моделі й продуктивністю з масштабованістю.

Моделювання починається з опису реальної системи. Такий опис являє собою імітаційну модель, побудовану на основі розуміння величин, атрибутів, подій, каналів і т.д. Тому, розроблювач моделі описує ці структури моделювання в термінах сутностей і їх відносин і реалізує поведінку цих суб'єктів і реакцію на події. Системи моделювання БСМ чітко відокремлюють реалізацію процесу моделювання від опису моделі й екземплярів досліджуваної системи [6,8]:

– ядро процесу моделювання й основних об'єктів моделі поставляються у вигляді набору програмних бібліотек мовою програмування високого рівня, як правило, Java або C ++;

– деякі види скриптових мов програмування (TCL, наприклад) або мови розмітки (XML, наприклад), як правило, використовуються для опису моделі, тобто встановлення (оголошення) відносин між суб'єктами. Ці засоби дозволяють однаковий і ефективний підхід до опису моделі і її конфігурації;

– крім того, деякі бібліотеки часто включають підтримки графічного представлення або збору статистичних даних і аналізу.

Таким чином, система моделювання звичайно складається з базової бібліотеки для моделювання, бібліотеки допоміжних засобів, і системи опису й конфігурації моделей. Сама форма розгортання пакета залежить від реалізації. Деякі пакети надають засоби, які переводять опис моделей в об'єкти мови реалізації моделювання. Інші забезпечують візуальний інтерфейс.

Система імітаційного моделювання Castalia.

Castalia є подійно-дискретним симулятором. Написаний на C++. Castalia поширюється за некомерційною ліцензією, для використовуватися в навчальних закладах або некомерційних дослідницьких організаціях, а також під комерційною ліцензією. Цей симулятор підтримує написання модулів користувачем. Вона заснована на платформі OMNet++ і може бути використана дослідниками й розроблювачами, які прагнуть спробувати свої алгоритми й / або протоколи в реалістичному середовищі бездротового каналу з розширеної радіо моделлю, з реалістичною поведінкою вузла. Castalia також може бути використана для оцінки різних характеристик платформи для конкретних додатків, тому що вона дуже гнучка в настроюванні й може імітувати широкий діапазон платформ. Основними рисами Castalia є :

1) удосконалена модель каналу на основі емпіричних даних вимірів:
   – модель системи враховує втрати в каналі передачі даних, а не просто з'єднань між вузлами;
   – комплексна модель для зміни втрат у каналі;
   – повністю підтримує рухливість вузлів;
   – перешкоди враховуються вже на рівні прийнятого сигналу, а не у вигляді окремої функції.

2) удосконалена модель радіо заснована на реальних малопотужних радіо пристроях зв'язку:
   – імовірність одержання залежить від SINR, розміру пакета, типу модуляції. Модуляції PSK, FSK підтримуються, користувацькі модуляції можуть бути визначені шляхом завдання SNR-BER кривій;
   – кілька рівнів потужності передачі з індивідуальними варіаціями можуть задаватися;

– стани з різним енергоспоживанням і затримками перемикання між ними підтримуються;
– реалістичне моделювання RSSI несучої.
– Розширене моделювання вимірювальних пристроїв:
– дуже гнучка фізична модель процесу виміру;
– підтримка шумів, зсувів і споживання енергії для вимірювального пристрою.

3) MAC протоколи доступні.

4) призначена для адаптації й розширення.

Чим Castalia не є це орієнтованою на конкретну платформу. Castalia забезпечує загальний надійний і реалістичний спосіб перевірки алгоритму перш ніж перейти до реалізації на конкретній платформі.

Бібліотека OMNet заснована на поняттях модулів і повідомлень. Простий модуль є основною одиницею виконання (рисунок 2.2). Він приймає повідомлення від інших модулів або безпосередньо, і відповідно до повідомлення, він виконує частину коду. Цей код може зберігати стан, який змінюється при прийманні повідомлень і може відправити нові повідомлення. Є також складені модулі. Складений модуль просто спосіб побудови простих і / або інших композитних модулів.

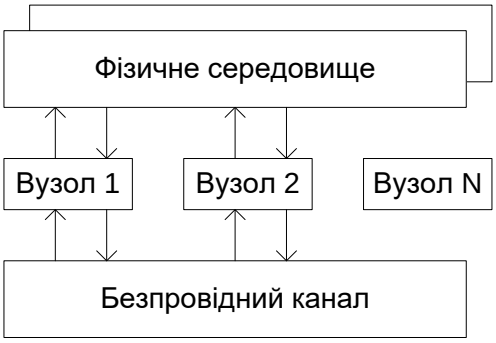


Рисунок 2.2 - Структура модулів в ситемі Castalia

Вузли не з'єднуються один з одним прямо, а через модуль бездротового каналу. Стрілки означають передачу повідомлень від одного модуля до іншого. Коли вузол має пакет для відправлення, то він переходить у бездротовій канал, який потім вирішує, які вузли повинні одержувати пакет. Вузли також зв'язані через фізичні процеси, які вони контролюють. Для кожного фізичного процесу є один модуль. Вузли взаємодіють із фізичним процесом у просторі й часі (шляхом відправлення повідомлення на відповідний модуль), щоб одержати показання датчиків. Там може бути кілька фізичних процесів, що представляють кілька датчиків.

Модуль вузла є складеним. На рисунку 2.3 показана внутрішня структура вузла. Суцільні стрілки означають передачу повідомлень і пунктирні стрілки означають просто викликувані функції. Наприклад, більшість із модулів викликають функції менеджера ресурсів, щоб сигналізувати, що енергія витрачена. Castalia пропонує підтримку для створення користувацьких протоколів і додатків, визначаючи відповідні абстрактні класи. Усі існуючі модулі, що добре настроюється по багатьом параметрам.

Опис модулів здійснюється з використанням мови OMNet++ NED. За допомогою цієї мови можемо визначити модулі, параметри модуля й інтерфейс, можливу структуру підмодуля (якщо це композитний модуль). Сам код модуля пишеться мовою C++.

ХІД РОБОТИ

1. Встановити і OMNeT, і Castalia.

Починаючи з Castalia 3.0, ми маємо два скрипти, які допомагають запускати симуляції та інтерпретувати результати. Вони називаються Castalia та CastaliaResults відповідно. Починаючи з версії 3.1, ми також маємо CastaliaPlot для створення графіків. Всі вони знаходяться у каталозі Castalia/bin/.

Виконавчий файл симулятора називається CastaliaBin і знаходиться в Castalia/, але вам не потрібно викликати його безпосередньо.

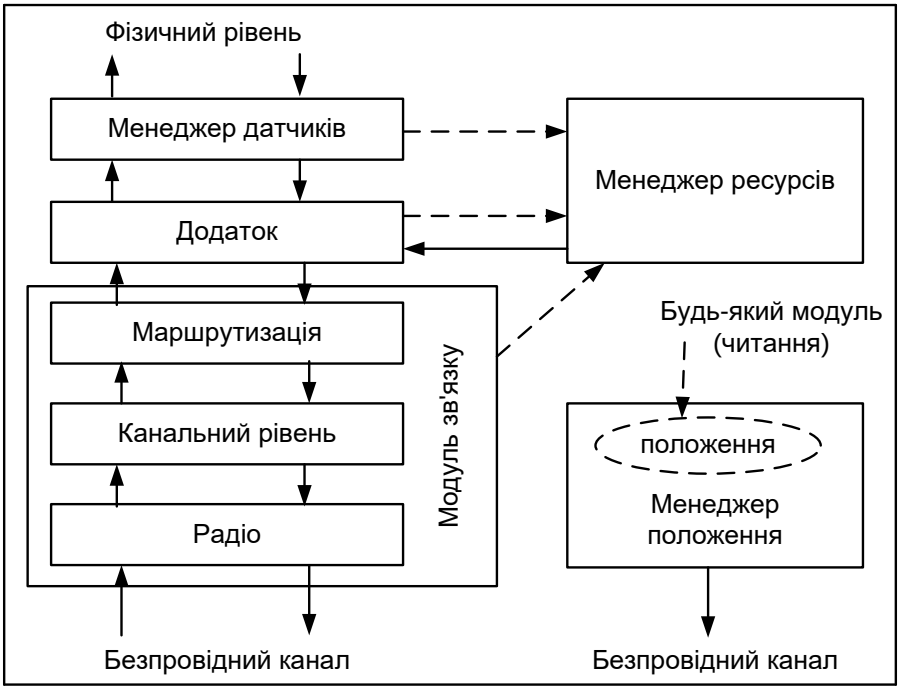


Рисунок 2.3 - Структура модуля вузла БСМ

Запуск симуляції. Перейти до каталогу Castalia/Simulations/radioTest. Він повинен містити один файл: omnetpp.ini. Це конфігураційний файл, який визначає наш сценарій(и) моделювання. Запустимо вхідний сценарій без аргументів і подивимося, що ми отримаємо:

```
~/Castalia/Simulations/radioTest$ ../../bin/Castalia
List of available input files and configurations:
* omnetpp.ini
     General
     InterferenceTest1
     InterferenceTest2
     CSinterruptTest
     varyInterferenceModel
```

Запущений без аргументів, скрипт шукає у поточному каталозі допустимі конфігураційні файли файлів конфігурації. Якщо він знаходить файл, він аналізує його і виводить назву конфігурацій, що містяться у ньому (про конфігурації ми поговоримо пізніше).

Запустити моделювання

```
~/Castalia/Simulations/radioTest$ ../../bin/Castalia -c General
Running configuration 1/1
```

В результаті будуть створені файли

```
~/Castalia/Simulations/radioTest$ ls
100806-222319.txt Castalia-Trace.txt omnetpp.ini
```

Створено 2 нових файли: 100806-222319.txt - стандартний вихідний файл Castalia, його ім'я має вигляд YYMMDD-HHMMSS.txt. Можете відкрити його для читання (він придатний для читання людиною). Зазвичай цей файл обробляється за допомогою CastaliaResults.

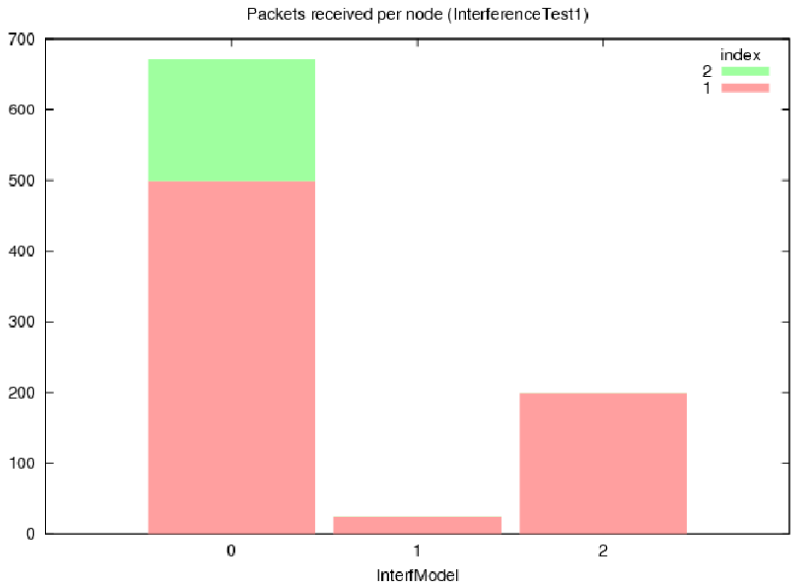
Інший створений файл - це файл трасування з назвою Castalia-Trace.txt. Він містить трасування всіх подій, які ви попросили записати, "увімкнувши" деякі параметрів у файлі omnetpp.ini

Ми створили імітаційні сценарії RadioTest, щоб побачити результати реалістичного моделювання, а також побачити деякі функції Castalia в дії. Перший сценарій (конфігурація General конфігурація, яку ми щойно запустили) тестує прийом, коли приймач (вузол 0) рухається через зону двох передавачів (вузли 1 і 2). Передавачі розміщені на достатній відстані, щоб між ними не було інтерференції між ними. Приймач рухається по прямій лінії вперед і назад, і коли він наближається до кожного з двох передавачів, він повинен отримати їхні пакети

Можжна автоматично будувати графіки прямо з CastaliaResults, використовуючи скрипт CastaliaPlot. Відобразимо пакети, отримані кожним вузлом для Interference Test 1, варіюючи модель завад .

```
radioTest$ CastaliaResults -i 101209-235427.txt -s packets -n -f Test1 |
CastaliaPlot -o interfTest1-app-varyModel.png -s stacked
```

Отриманий графік



КОНТРОЛЬНІ ПИТАННЯ

1. Призначення і функції безпровідних сенсорних мереж?
2. Основні характеристики вузлів БСМ?
3. Які алгоритми маршрутизації використовуються в БСМ?

ЛАБОРАТОРНА РОБОТА №12
ІНТЕРНЕТ РЕЧЕЙ ТА КІБЕРФІЗИЧНІ СИСТЕМИ

Мета: Ознайомитись із будовою мереж

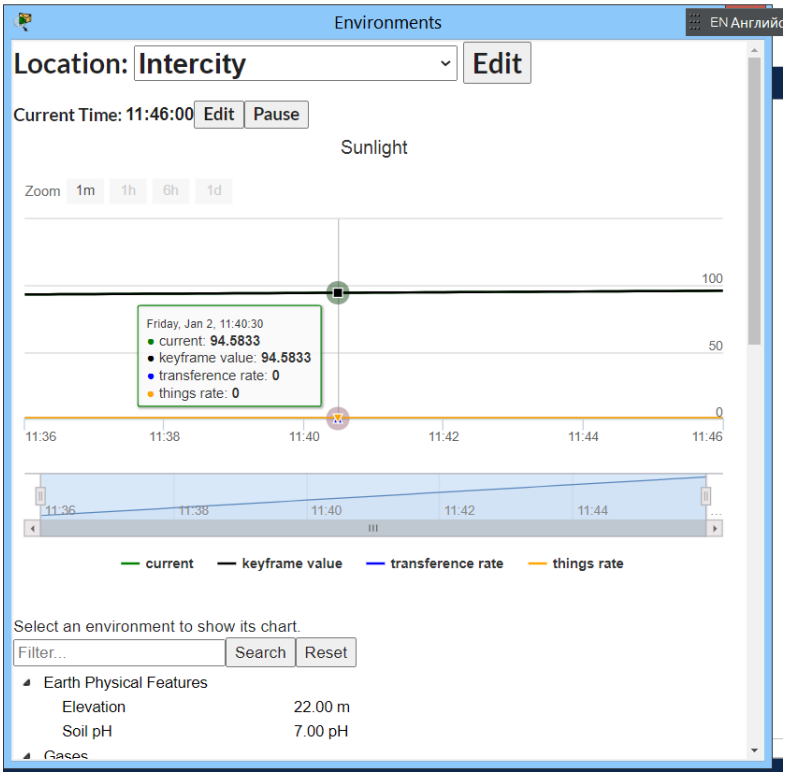
ТЕОРЕТИЧНІ ВІДОМОСТІ

The sun charges the solar panel which sends electricity to the battery for power storage and distribution A power meter connected between them reads and display the amount of power being captured by the solar panel. Because all devices are connected (IoT capabilities) they register themselves with a registration server, allowing a user to monitor the entire system from a web browser (running In the PC).

Ціллю лабораторної є побудова джерело живлення на основі сонячної енергії.

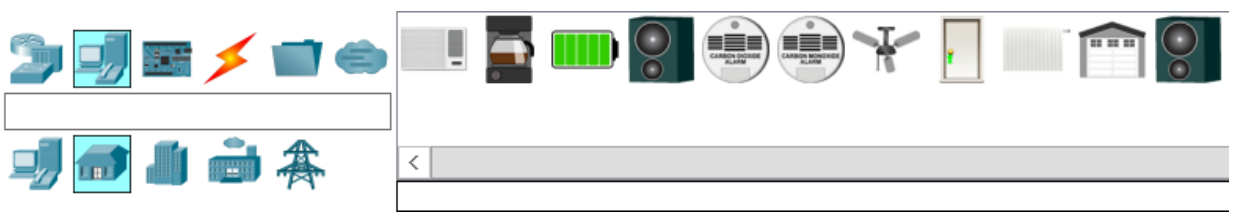
Сонце заряджає сонячну панель, яка відправляє електроенергію до акумулятора для зберігання та розподілу енергії. Лічильник електроенергії, підключений між ними, зчитує та відображає кількість енергії, яку вловлює сонячна панель. Оскільки всі пристрої підключені (можливості Інтернету речей), вони реєструються на реєстраційному сервері, що дозволяє користувачеві контролювати всю систему з веб-браузера (запущеного на комп'ютері).

Потрібно зауважити що в режимі реального часу Packet Tracer імітує вплив зовнішнього середовища зокрема, і сонячну енергію. Тому потрібно звернути увагу на годинник реального часу та праметри середовища.



Представлення кінцевих пристроїв IoT.

У лівому нижньому кутку вікна Packet Tracer вибрати групу [End Devices] (Кінцеві пристрої) у верхньому рядку, а потім вибрати піктограму [Home] (Дім) у нижньому рядку поля Device-Type Selection (Вибір типу пристрою).



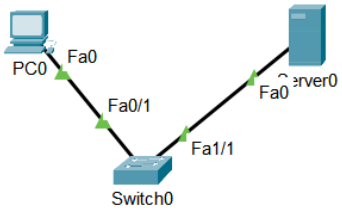
У нижній частині вікна Packet Tracer у полі Device-Specific Selection (Вибір конкретного пристрою) відображається безліч доступних пристроїв IoT для розумного будинку. При наведенні курсора на кожен пристрій в нижній частині поля Device-Specific Selection (Вибір конкретного пристрою) відображається описове ім'я цього пристрою. Детально розгляньте пристрій кожного типу.

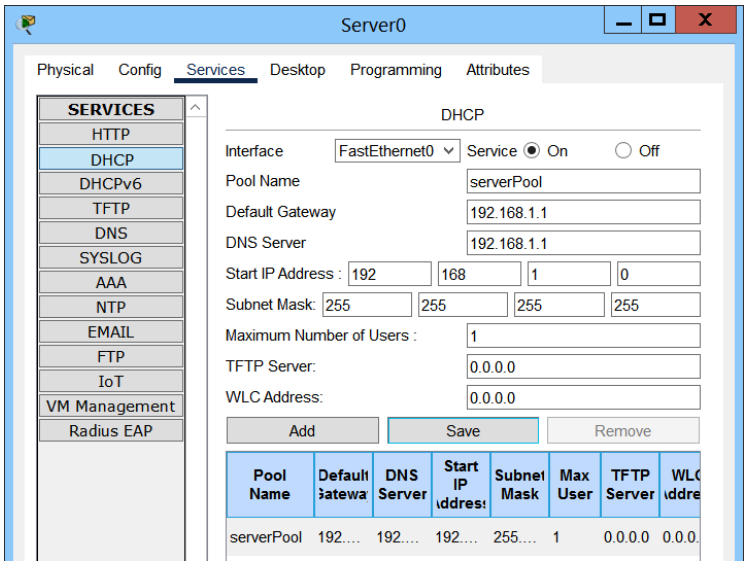
Вибрати групу кінцевих пристроїв Power Grid і переглянути пристрої цієї групи.

ХІД РОБОТИ

1 Додавання та підключення необхідних пристроїв

Створити мережу з комп'ютера PC, комутатора PT-Switch та сервера Server. Сервер потрібно налаштувати для динамічного призначення IP.





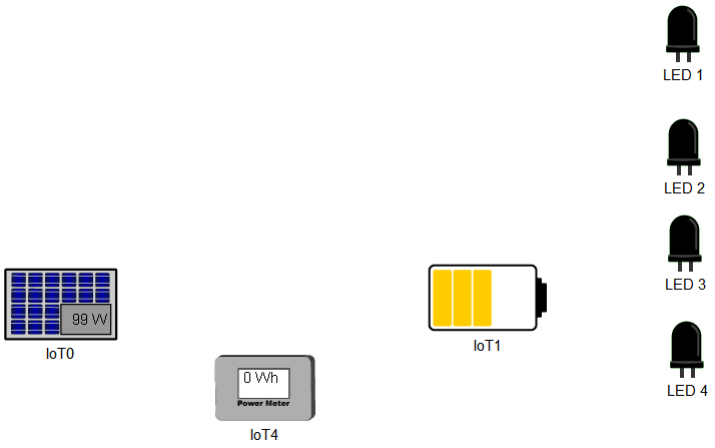
Додати в мережу чотири світлодіоди, сонячну панель, акумулятор, лічильник електроенергії. В залежності від версії Packet Tracer пристрої можуть бути в групах – End devices → «Home», «Power Grid», Components → Actuators. Додайте наступні пристрої, знайшовши і перетягнувши їх до робочого простору Packet Tracer.

Пристрій сонячна панель PT-Solar Panel;

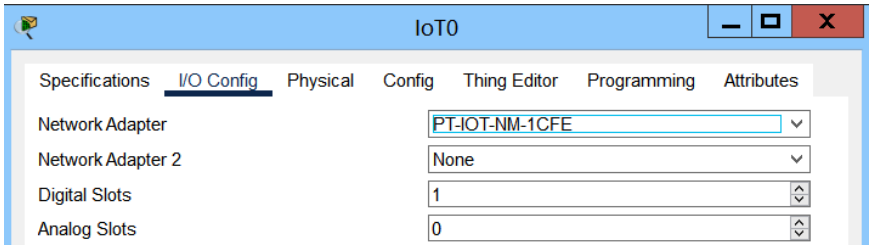
Пристрій акумулятор PT-Battery;

Пристрій лічильник електроенергії PT-Power Meter;

Пристрій LED.



! IoT пристрій може мати до двох мережевих інтерфейсів. Якщо в IoT пристрою відсутній інтерфейс кабельного Ethernet потрібно натиснути кнопку Advanced в параметрах пристрою, що перейти в детальний режим налаштувань. В детальному режимі на вкладці I/O config можна змінити тип мережевого адаптера з бездротового PT-IOT-NM-1W на інтерфейс PT-IOT-NM-1CFE.



За допомогою IoT кабелів підключіть сонячну панель та акумулятор до лічильника електроенергії відповідно до таблиці нижче. Спеціальний кабель IoT в розділі Connections-Підключення.

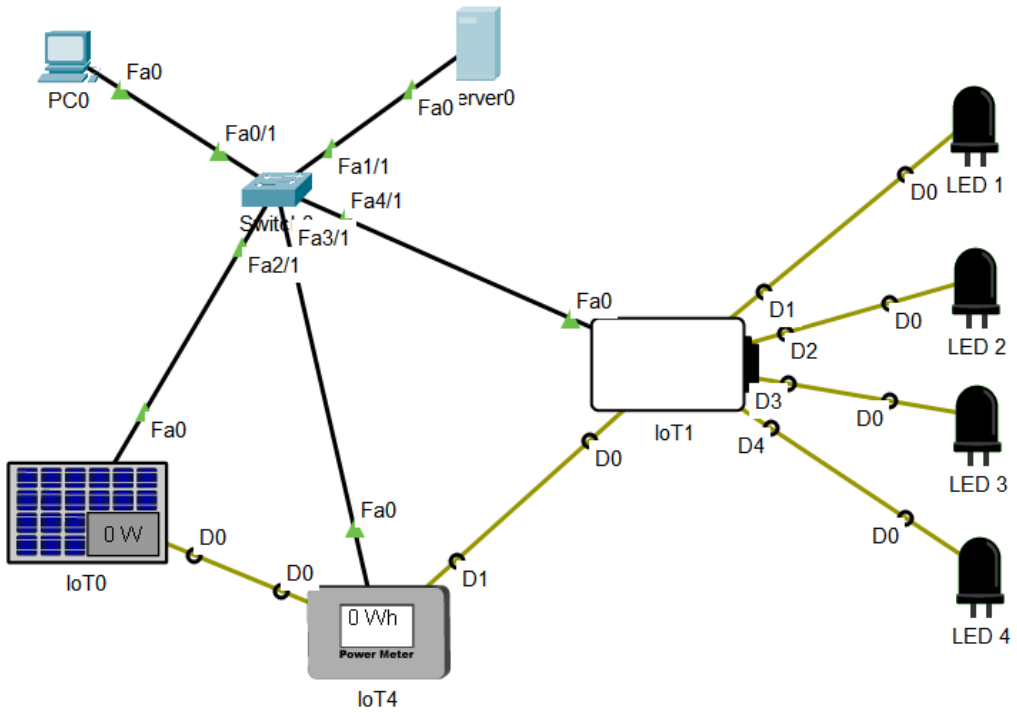
Використовуйте таблицю, щоб знайти правильні порти

Пристрій	Порт	Пристрій	Порт
Solar Panel	D0	Power Meter	D0
Battery	D0	Power Meter	D1

За допомогою спеціальних кабелів IoT (IoT Custom Cables в групі Підключення) підключіть світлодіоди до батареї Battery відповідно до таблиці нижче.

Device	Battery Port
LED1	D1
LED2	D2
LED3	D3
LED4	D4

Підключити комутатор до IoT пристроїв.



2 Налаштування пристроїв

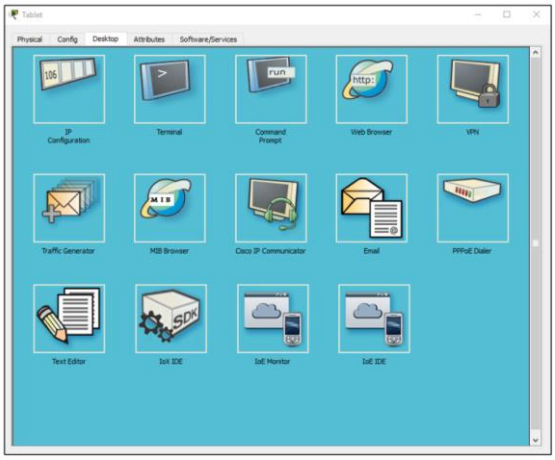
Коли пристрої правильно підключені, їх потрібно налаштувати. Оскільки система покладається на IP-мережу, пристрої повинні бути налаштовані з правильною IP-адресою. Оскільки сервер налаштований на роботу в якості DHCP-сервера, пристрої IoT повинні бути налаштовані як DHCP-клієнти.

Для кожного пристрою в Config tab » FastEthernet0 і вибрати DHCP в IP Configuration

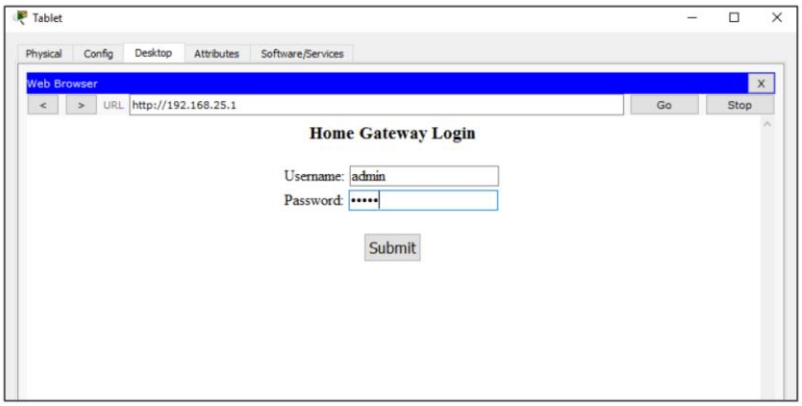
Кожен пристрій потрібно зареєструвати на сервері.

Налаштування клієнта. Вибрати вкладку Desktop (Робочий стіл) і піктограму Web Browser (Веб-браузер).

У вікні Web Browser (Веб-браузер) введіть у полі URL-адреси IP-адресу домашнього шлюзу 192.168.25.1 і натисніть Go (Перейти). На екрані Home Gateway Login (Вхід у домашній шлюз) введіть admin як ім'я користувача і пароль, після чого натисніть кнопку Submit (Відправити).



Після підключення до веб-інтерфейсу домашнього шлюзу відкриється список усіх підключених пристроїв IoT.



ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
3. Схема мережі
4. Висновки по роботі.