МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій та кібербезпеки, факультет № 4

МЕТОДИЧНІ МАТЕРІАЛИ

до лабораторних занять
з навчальної дисципліни «Мережеві технології»
вибіркових компонент
освітньо-професійної програми першого (бакалаврського) рівня вищої освіти

125 «Кібербезпека (поліцейська діяльність у кіберсфері)»

Харків 2020

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 22.10.2020 № 10

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 21.10.2020 № 6

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 22.10.2020 № 6

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки (протокол від 20.10.2020 № 19)

Розробники:
1. Доцент кафедри, к.т.н., доцент Євстрат Д. І.

Рецензенти:
1. Завідувач кафедри інформаційних технологій Харківського національного університету Повітряних Сил імені Івана Кожедуба, к.т.н., доцент Соловйова О. І.
2. Провідний науковий співробітник науково-дослідної лабораторії з проблем розвитку інформаційних технологій ХНУВС, к.т.н., доцент Мордвинцев М. В.

1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни						Література, сторінки	Вид контролю
	Всього	з них:						
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота		
Семестр № 7								
Тема № 1: Основи побудови комп'ютерних мереж.	60	12		6	12	30	Конспект лекцій. Література 7-14	
Тема №2. Локальні комп'ютерні мережі.	60	12		6	12	30	Конспект лекцій. Література 7-14	
Всього за семестр № 7:	120	24		12	24	60		Залік
Семестр № 8								
Тема №3. Глобальні комп'ютерні мережі.	90	12		6	12	60	Конспект лекцій. Література 7-17	
Тема №4. Intemet/Intranet технології.	90	12		6	12	60	Конспект лекцій. Література 7-14	
Всього за семестр № 8:	180	24		12	24	120		Екзамен
Всього по дисципліні	300	48		24	48	180		Екзамен

3. Методичні вказівки лабораторних до занять

Тема№1: Основи побудови комп'ютерних мереж.

Лабораторне заняття 1: Засоби збору первинної інформації про мережу, створення карти мережі

Навчальна мета заняття: Дослідити роботу програм для побудови карти мережі та збору інформації про неї.

Час: 2 год.

Місце проведення: комп'ютерний клас Навчальні питання:

1. **Попередній збір даних**
2. **№оТгасеРго**
3. **№оТгасе**

Література:

1. Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.
2. Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.

Методичне та матеріально-технічне забезпечення занять: Персональний комп'ютер, включений в мережу IP, Microsoft Windows.

Хід проведення заняття:

I. Порядок проведення вступу до заняття.

Вступ

Обговорювання теоретичного матеріалу:

II. Порядок проведення основної частини заняття.

Попередній збір даних

Почавши «з нуля» (наприклад, маючи лише загальні відомості про підключення до Internet) і застосовуючи різні засоби можна визначити:

1) доменні імена;
2) адреси під мереж;
3) адреси окремих комп'ютерів організації, підключених до Internet (Табл. 1). Методів збору подібної інформації дуже багато, проте всі вони зводяться до

одного - отримання інформації, що має відношення до технологій Internet, корпоративним мережам (intranet), віддаленому доступу (remote access) і екстрамережам (extranet).

Збір даних про підключення до Internet

Таблиця ***1***

Ідентифікуючі відомості за різними технологіями

Технологія	***Ідентифікуючі відомості***
Internet	- імена доменів; - адреси підмереж; - точні IP-адреси комп'ютерів, підключених до Internet; - TCP- і UDP-служби, що працюють на кожному з виявлених комп'ютерів; архітектура системи (наприклад, SPARC або X86); - механізми управління доступом і відповідні списки управління доступом (ACL — Access Control
	- List); - системи виявлення вторгнень (IDS); - реєстраційна інформація (імена користувачів і груп, системні маркери, таблиці маршрутизації, інформація про протокол SNMP)
Корпоративні мережі	- те ж, що і для Internet + - використовувані мережні протоколи (наприклад, IP, IPX, DecNET і т. д.); - імена внутрішніх доменів
Віддалений доступ	- телефонні номери, використовувані для віддаленого доступу, - а також тип АТС (аналогова чи цифрова); - тип віддаленої операційної системи; - механізм автентифікації і використовувані протоколи (IPSEC, PPTP)
Екстрамережі	- вихідні точки та вхідні з'єднання; - тип з'єднання; механізм управління доступом

Щоб зібрати інформацію, потрібно знати адресу організації або яку небудь іншу початкову точку. У Internet адресу звичайно приймає вид імені домену.

Запустіть програму whois з наступним введенням імен доменів, що Вас цікавлять:

www.microsoft.com
www.mail.ru
www.google.com
www.samsung.ru
www. anekdotov. net
www.yandex.ru
www.australia.gov. au
www.turismo.gov.ar
www.mincom.gov.ma
www.info.gov.hk
www.sar.gov.pl
www.kenya.go.ke

Програма Whois дозволяє дізнатися деяку інформацію, і вбудована в більшість версій ОС UNIX. Для її використання необхідно просто перейти у вікно терміналу або в командний рядок і ввести команду ***whois newriders.com*** (наприклад, зломщика цікавить компанія newriders).

В цьому випадку Вам надається можливість ознайомитися з програмою SmartWhoIs під Windows, результат роботи якої аналогічний результату виконання програми Whois в ОС UNIX.

Для початку збору необхідної інформації необхідно запустити програму і в поле ввести ім'я хоста, що цікавить Вас, його IP-адресу або ім'я домену і натиснути ***Enter*** або кнопку ***Запит*** (рис. 7.8).

Рис. 7.8. Поле програми SmartWhoIs під Windows

У вікні, що з'явилося, можна побачити результат виконання запиту WhoIs (рис. 7.9).

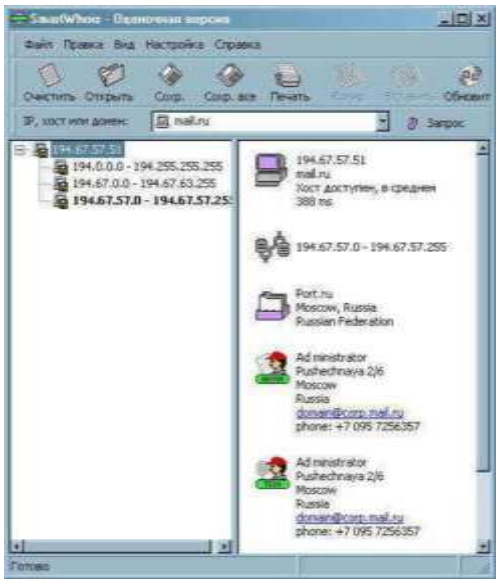


Рис. 7.9. Результат роботи програми Whols

У лівій частині екрану міститься інформація про приналежність вузла, який Вас цікавить, до мережі та її маска. У правій частині докладніша інформація про адміністраторів цього вузла або керівників цієї організації їх, поштова скринька, телефон, прізвище та ін.

VisualRoute

VisualRoute - це програмний засіб, який об'єднує інструменти Traceroute, Ping і Whois в одному зручному графічному інтерфейсі. На додаток до цього, програма надає можливість визначити географічне положення роутерів і серверів (рис. 7.10), забезпечуючи, таким чином, інформацію, яка може допомогти в ідентифікації джерела мережних вторгнень і місцеположення зловмисників.

Рис. 7.10. Результат роботи програми VisualRoute VisualRoute забезпечує трасування e-mail повідомлень, що може стати в нагоді для вирішення проблем електронної пошти та полювання за спамерами. На відміну від звичайних програм трасування, VisualRoute

визначає всі IP переходи паралельно (замість того, щоб робити це послідовно), забезпечуючи швидке отримання результату. Пакет VisualRoute Server дозволяє діставати доступ до описаної функціональності за допомогою браузера, таким чином, користувач може запитати інформацію Traceroute, знаходячись за брандмауером або з віддаленого комп'ютера.

Використовуючи функцію Ping, ви можете контролювати, що сайт «живий», а за допомогою Traceroute можна дізнатися, чи немає проблем по дорозі до нього. VisualRoute Traceroute формує три види результатів:

- загальний аналіз;
- таблицю даних (рис. 7.11);

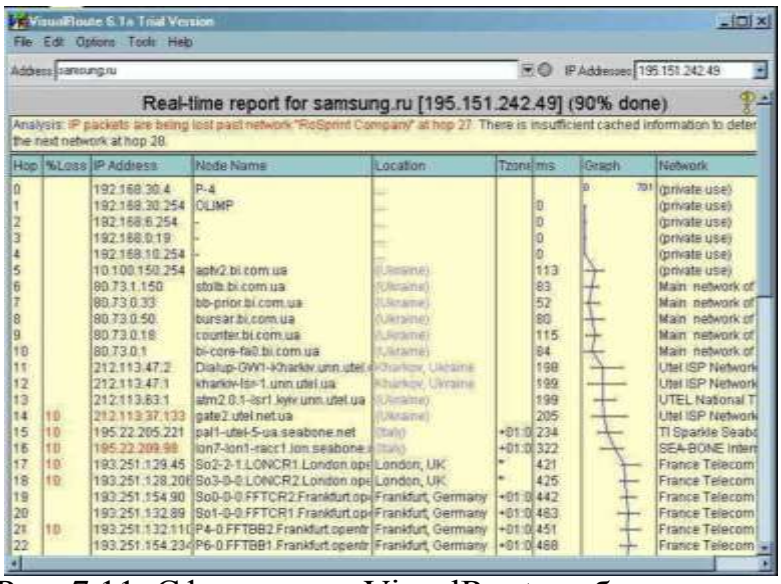


Рис. 7.11. Сформована VisualRoute таблиця даних

- географічне розташування роутинга (рис. 7.12);

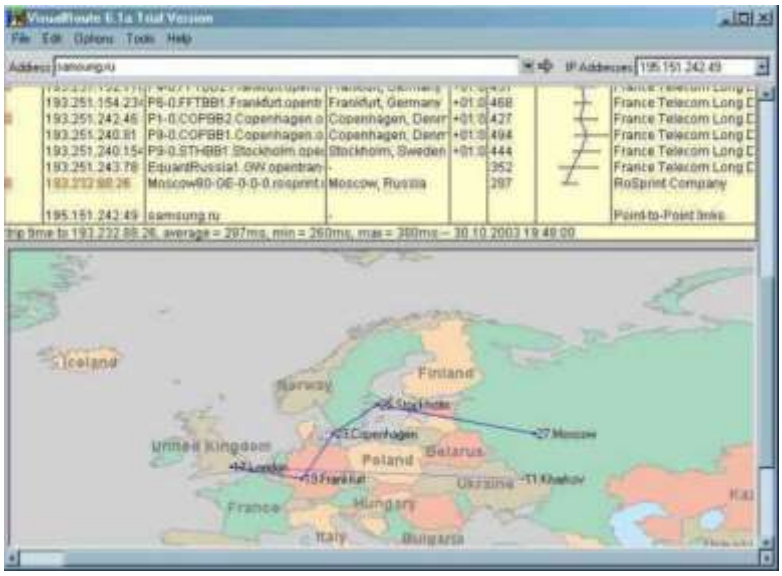


Рис. 7.12. Географічне розташування роутинга

Загальний аналіз містить короткий опис числа переходів; вказівку на місце, де відбулася проблема; тип програмного забезпечення, встановленого на сервері. Дані в табличній формі містять інформацію про кожен перехід, включаючи IP адресу, ім'я вузла, географічне положення й основні магістралі Інтернет, з якими сполучений сервер. Карта світу дає географічне уявлення маршруту, за яким відбулося з'єднання. Користувач може наближати і віддаляти картинку, переміщатися по карті. Клацнувши по вузлу мишею можна дістати доступ до контактної інформації для відправки повідомлень у разі виникнення проблем.

Для отримання наданої вище інформації необхідно запустити програму і заповнити поле Address як показано на рис. 7.13 (можливо заповнення поля Address або IP Address по вибору, залежно від відомих даних) і натиснути Enter.

Рис. 7.13. Введення адреси до відповідного вікна Visual Route Нижче буде виведена сказана вище інформація про хост, що цікавить нас, а також географічне положення роутерів і серверів.

У полі таблиці:

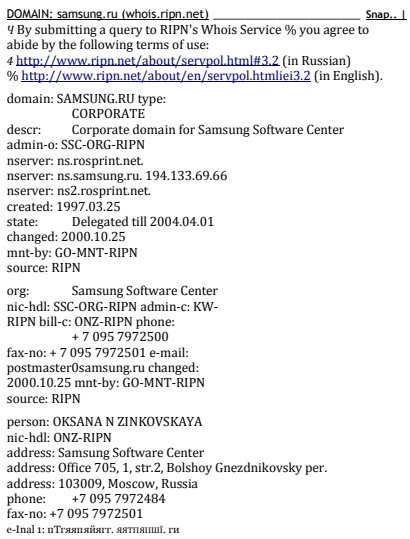
Hop показує кількість роутерів і серверів, через які проходить IP-пакет; **Node Name** - вказується інформація про DNS імена роутерів і серверів; **Location** - місцерозташування цих вузлів;

Tzone - відповідний часовий пояс;

NetWork - тип мережі.

Також в програмі є можливість виведення інформації щодо кожного з вузлів окремо. Для цього в полі Node Name клацніть один раз мишкою по імені хоста, що цікавить Вас. У результаті Ви одержите наступну інформацію (рис. 7.14.), як бачите вона дуже схожа з інформацією, що одержана за допомогою програми SmartWhois.

Для виведення інформації у файл натисніть кнопку *Snap*, розташовану в заголовку вікна (рис. 7.14).


DOMAIN: samsung.ru (whois.ripn.net) Snap.. |
Ч By submitting a query to RIPN's Whois Service % you agree to abide by the following terms of use:
4 http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.htmliei3.2 (in English).

domain: SAMSUNG.RU type: CORPORATE
descr: Corporate domain for Samsung Software Center
admin-o: SSC-ORG-RIPN
nserver: ns.rosprint.net.
nserver: ns.samsung.ru. 194.133.69.66
nserver: ns2.rosprint.net.
created: 1997.03.25
state: Delegated till 2004.04.01
changed: 2000.10.25
mnt-by: GO-MNT-RIPN
source: RIPN

org: Samsung Software Center
nic-hdl: SSC-ORG-RIPN admin-c: KW-RIPN bill-c: ONZ-RIPN phone: + 7 095 7972500
fax-no: + 7 095 7972501 e-mail: postmaster0samsung.ru changed: 2000.10.25 mnt-by: GO-MNT-RIPN
source: RIPN

person: OKSANA N ZINKOVSKAYA
nic-hdl: ONZ-RIPN
address: Samsung Software Center
address: Office 705, 1, str.2, Bolshoy Gnezdnikovsky per.
address: 103009, Moscow, Russia
phone: +7 095 7972484
fax-no: +7 095 7972501
e-Inal 1: пТтяпяйятг. яятпяшш. ги

Рис. 7.14. Інформація про домен, видана VisualRoute

VisualRoute є дуже зручним і наочним інструментальним засобом отримання інформації, необхідної ддя з'ясування інформації, на таких етапах, як: 1) з'ясування ввідної інформації; 2) з'ясування адресного простору мережі; 3) створення карти мережі.

Запустіть програму VisualRoute, задавши для пошуку імена доменів, що Вас цікавлять:

www.microsoft.com
www.mail.ru
www.google.com
www.samsung.ru
www. anekdotov. net
www.yandex.ru
www.australia.gov.au
www.turismo.gov.ar
www.mincom.gov.ma
www.info.gov.hk
www.sar.gov.pl
www.kenya.go.ke

NeoTracePro

Internet: http://www.neoworx.com/

Кожний з нас не раз бачив в кіно про хакерів або шпигунів як відбувається виявлення місцезнаходження того, хто телефонує: на екрані комп'ютера відображається карта світу, а на ній - маршрут проходження дзвінка.

Запустивши цю програму, ви зможете одержати аналогічну картину для

відстеження не телефонних номерів, а географічного розташування якого-небудь web-серверу.

NeoTrace за ім'ям сайту або поштової скриньки відображає на карті маршрут проходження трафіку з докладним переліком всіх точок ретрансляції. Після закінчення процесу можна переглянути:

- через які вузли відбувалося з'єднання;
- графік швидкості передачі даних через ці вузли;
- дізнатися, які компанії володіють ними та їх фізичні адреси;
- також програмою можна перевірити, чи реально існує яка-небудь поштова скринька.

Як видно з опису і рисунка 7.14, програма дуже схожа з програмою VisualRoute (рис. 7.15).

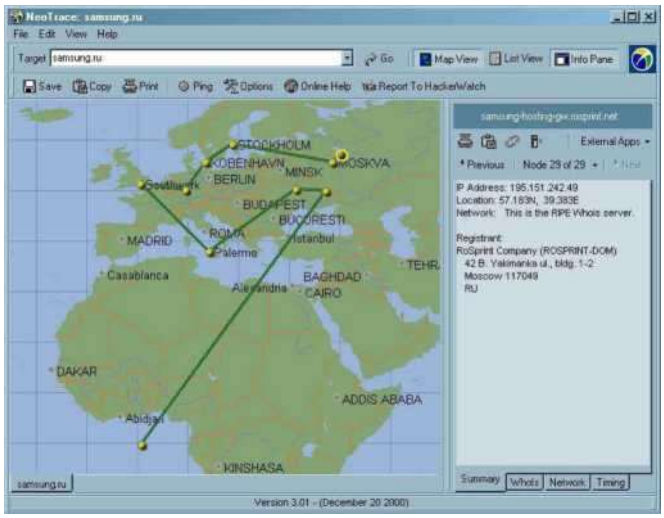


Рис. 7.15. Географічне розташування роутинга **Самостійно вивчіть можливості програми №оТгасе і зробіть відповідні висновки.**

Вирішіть завдання.

Використовуючи відомі вам засоби, визначити, чи знаходяться в одній мережі комп'ютери:

- **195.151.242.49 і 195.151.242.250;**
- **195.151.242.49 і 195.151.241.50.**

Тема№1: Основи побудови комп'ютерних мереж.

Лабораторне заняття 2: Робота з програмою Packet tracer. Основні засоби навігації програми Packet tracer.

Навчальна мета заняття: - Освоїти основні можливості програми Packet tracer на прикладі двох найпростіших топологій з використанням комутатора і концентратора.

Час: 4 год.

Місце проведення: комп'ютерний клас

Навчальні питання:

1. Представлення інтерфейсу програми Packet Tracer на прикладі простих топологій на базі концентратора.
   1.1. Створення топології і налаштування робочих станцій.
   1.2. Провірка працездатності мережі за допомогою команди Ping
2. Використання інструменту Simple PDU

Література:

1. Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.
2. Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.

Методичне та матеріально-технічне забезпечення занять:

Персональний комп'ютер, включений в мережу IP, Microsoft Windows.

Хід проведення заняття:

I. Порядок проведення вступу до заняття.

Вступ

Обговорювання теоретичного матеріалу:

II. Порядок проведення основної частини заняття.

Теоретичні відомості

Packet Tracer являє собою програму-емулятор розроблену Cisco Systems. Packet Tracer (PT) є потужним і динамічним інструментом, який відображає різні протоколи, які використовуються в мережі, або в режимі реального часу або в покроковому режимі(режимі моделювання). Це включає в себе протоколи 2 рівня моделі OSI, таких як Ethernet і PPP, 3 рівня протоколів, таких як IP, ICMP, ARP і і 4-го рівня протоколів, таких як TCP і UDP. Також можуть бути досліджені протоколи маршрутизації.

Загальний вид програми представлений на рис 1.1

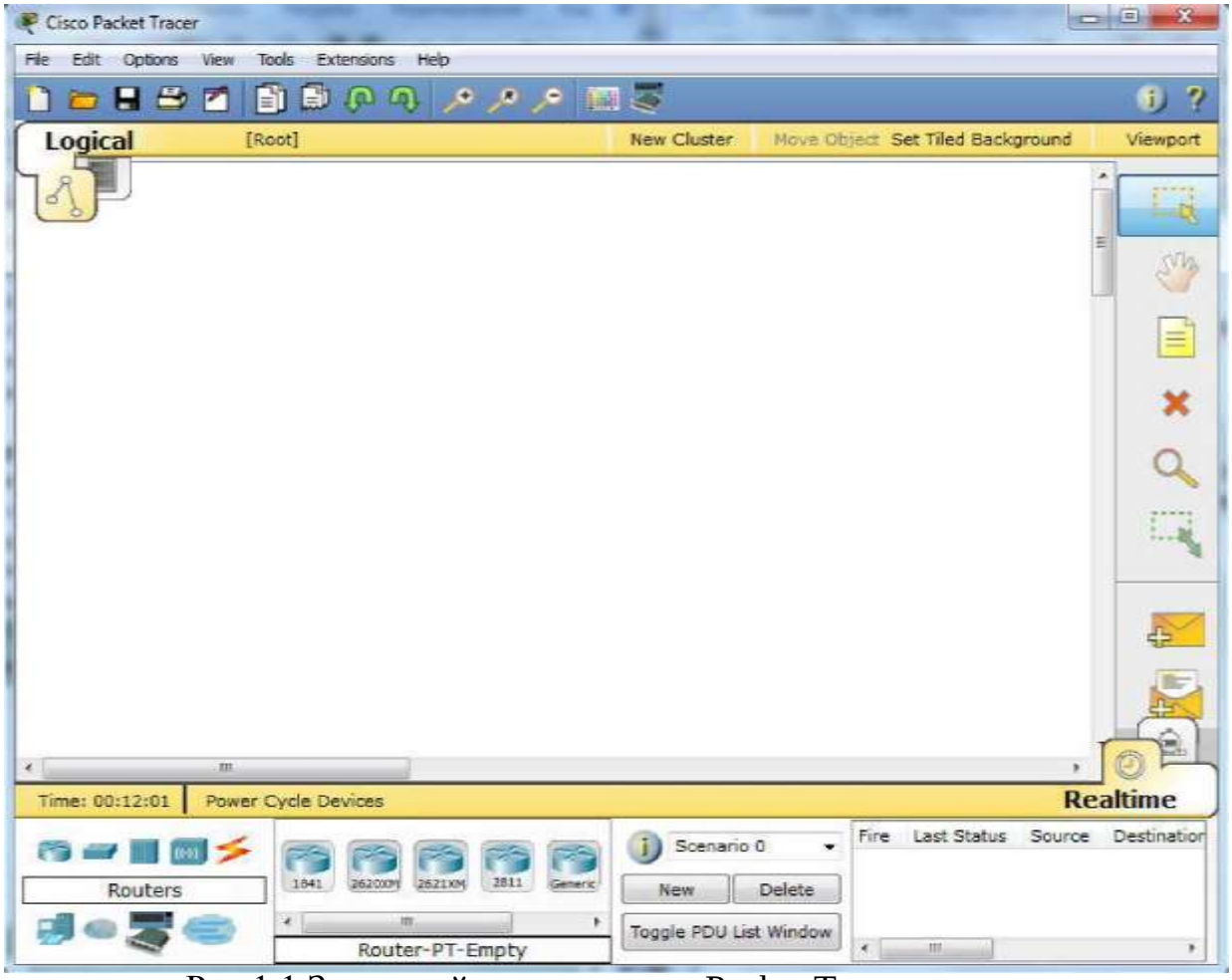


Рис 1.1 Загальний вид програми Packet Tracer

Робоче програми складається зі таких елементів:

1. Menu Bar - панель на якій знаходяться пункти меню File, Edit, Options, View, Tools, Extensions, Help.
2. Main Tool Bar - містить графічні зображення ярликів для доступу до команд меню, File, Edit, View и Tools, а також кнопку Network Information.
3. Common Tools Bar - панель, яка забезпечує доступ до найбільш використовуваних інструментів програми: Select, Move Layout, Place Note, Delete, Inspect, Add Simple PDU і Add Complex PDU.
4. Logical / Physical Workspace and Navigation Bar - панель, яка дає можливість перемикати робочу область: фізичну або логічну, а також дозволяє переміщатися між рівнями кластеру.
5. Workspace - Область, в якій відбувається створення мережі, проводяться спостереження за симуляцією і проглядається різна інформація і статистика.
6. Realtime / Simulation Bar - за допомогою закладок цієї панелі можна переключатися між режимом Realtime і режимом Simulation. Вона також містить кнопки, пов'язані з Power Cycle Devices, кнопки Play Control і перемикач Event List в режимі Simulation.

7. Network Component Box - це область, в якій вибираються пристрої та зв'язку для розміщення їх на робочому просторі. Вона містить область Device-Type Selection і область Device-Specific Selection.

8. Device-Type Selection Box - ця область містить доступні типи пристроїв та зв'язків у Packet Tracer. Область Device-Specific Selection змінюється в залежності від обраного пристрою

9. Device-Specific Selection Box - ця область використовується для вибору конкретних пристроїв і з'єднань, необхідних для будівництва в робочому просторі мережі.

10. User Created Packet Window - це вікно керує пакетами, які були створені в мережі під час симуляції сценарію.

Для створення топології необхідно вибрати пристрій з панелі Network Component, а потім з панелі Device-Type Selection вибрати тип обраного пристрою. Після цього потрібно натиснути ліву кнопку миші в полі робочої області програми (Workspace). Також можна перемістити пристрій прямо з області Device-Type Selection, але при цьому буде вибрана модель пристрою за замовчанням.

Для швидкого створення декількох екземплярів одного і того ж пристрою потрібно, утримуючи кнопку Ctrl, натиснути на пристрій в області Device-Specific Selection і відпустити кнопку Ctrl. Після цього можна кілька разів натиснути на робочій області для добавлення копій пристрою.

У Packet Tracer представлені наступні типи пристроїв:

- Маршрутизатори
- Комутатор (у тому числі і мости)
- Хаби і повторювані
- Кінцеві пристрої - ПК, сервери, принтери, IP-телефони
- Безпровідні пристрої: точки доступу і безпровідний маршрутизатор
- Решта пристрої - хмара, DSL-модем і кабельний модем.

При додаванні кожного елемента користувач має можливість дати йому ім'я та встановити необхідні параметри. Для цього необхідно натиснути на потрібний елемент лівої кнопкою миші (ЛКМ) і в діалоговому вікні пристрою перейти до вкладки Config.

Діалогове вікно властивостей кожного елемента має дві вкладки:

- Physical - містить графічний інтерфейс пристрою і дозволяє симулювати роботу з ним на фізичному рівні.
- Config - містить всі необхідні параметри для налаштування пристрою і має зручний для цього інтерфейс.

Додані елементи слід зв'язати з допомогою ліній зв’язку. Для цього необхідно вибрати вкладку Connections з панелі Network Component Box. Ми побачимо всі можливі типи з'єднань між пристроями. Виберемо відповідний тип кабелю. Вказівка миші зміниться на курсор "connection" (має вигляд роз'єму). Натиснемо на першому влаштуванні і вибрати відповідний інтерфейс, до якого потрібно виконати з'єднання, а потім натиснемо на

другий пристрій, виконавши ту ж операцію. Можна також виконати зєднання за допомогою Automatically Choose Connection Type (автоматично з'єднує елементи в мережі). Виберемо і натиснемо на кожному з пристроїв, які потрібно з'єднати. Між пристроями з'явиться кабельне з'єднання, а індикатори на кожному кінці покажуть статус з'єднання (для інтерфейсів які мають індикатор).

Рис 1.2 Типи кабелів, які можна застосувати для з’єднання в Packet Tracer

Після створення мережі її потрібно зберегти, вибравши пункт меню File -> Save або іконку Save на панелі Main Tool Bar. Файл зі збереженою топології має розширення *. pkt.

Packet Tracer дає нам можливість симулювати роботу з інтерфейсом командного рядка (ІКС) операційної системи IOS, встановленої на всіх комутаторах і маршрутизаторах компанії Cisco.

Підключившись до пристрою, ми можемо працювати з ним так, як за консоллю реального пристрою. Симулятор забезпечує підтримку практично усіх команд, доступних на реальних пристроях.

Підключення до ІКС комутатора або маршрутизаторів можна зробити, натиснувши на свій пристрій і перейшовши у вікно властивостей до вкладки CLI.

Для симуляції роботи командного рядка на кінцевому пристрої (комп'ютерів) необхідно у властивостях вибрати вкладку Desktop, а потім натиснути на ярлик Command Prompt.

Виконання роботи

1. Розглянемо представлення інтерфейсу програми Packet Tracer на прикладі простих топологій на базі концентратора.

1.1 Створення топології і налаштування робочих станцій.

- Добавити на робоче поле елементи, які вказані на Рис 1.3
- З’єднати всі пристрої в мережу Ethernet

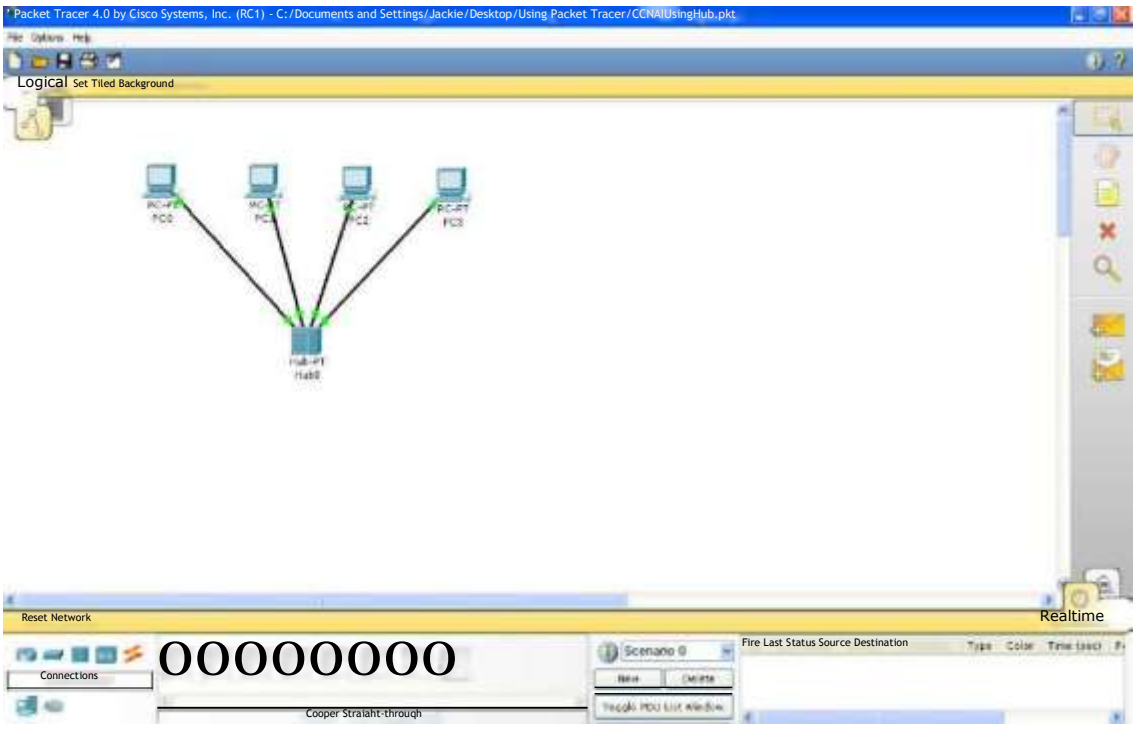


Рис 1.3 - Топологія мережі

Налаштування робочих станцій (IP-адреса, маска мережі, адреса шлюзу, якшо необхідна маршрутизація) можна виконати в зручному графічному інтерфейсі пристрою, який показано на рисунку 1.4, або використовуючи командну стрічку Command Prompt (Відкриємо властивості пристрою PC0 натиснувши на його зображення. переходимо до вкладки Desktop і симулюємо роботу run натиснувши Command Prompt.) І вводимо команду:

ipconfig 192.168.1.2 255.255.255.0

(список доступних команд в Command Prompt можна переглянути, ввівши ? і натиснути Enter)

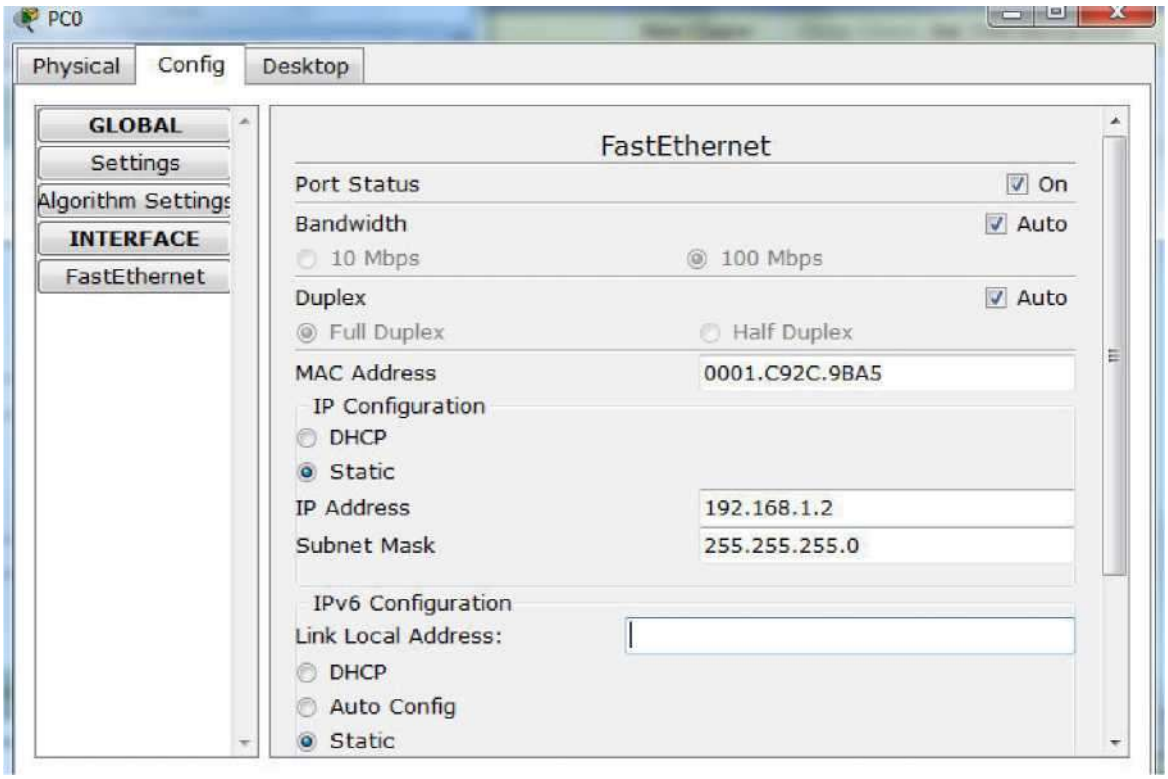


Рис 1.4- Графічний інтерфейс для налаштування пристрою PC0

Таким же шляхом настроїти всі інші робочі станції, відповідно до Таблиці 1

Таблиця 1

Устройство	IP ADRESS	SUBNET MASK
PC0	192.168.1.2	255.255.255.0
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.4	255.255.255.0
PC3	192.168.1.5	255.255.255.0

1.2 Провірка працездатності мережі за допомогою команди Ping

Слід відмітити, що в програмі присутні 2 режими роботи. За замовчуванням, програма відкривається в режимі реального часу.

Режим моделювання дозволяє переглядати послідовність подій, пов'язаних з взаємодією між двома або більше пристроями. Режим реального часу, здійснює операції з усіма послідовностями подій, що відбуваються в "реальному часі".

Для перегляду правильного налаштування №- адресу, маски підмережі, шлюзу за замовчуванням, а також MAC адреси хоста, перемістіть курсор на потрібний комп'ютер. Переконайтеся, що вибраний відповідний інструмент.

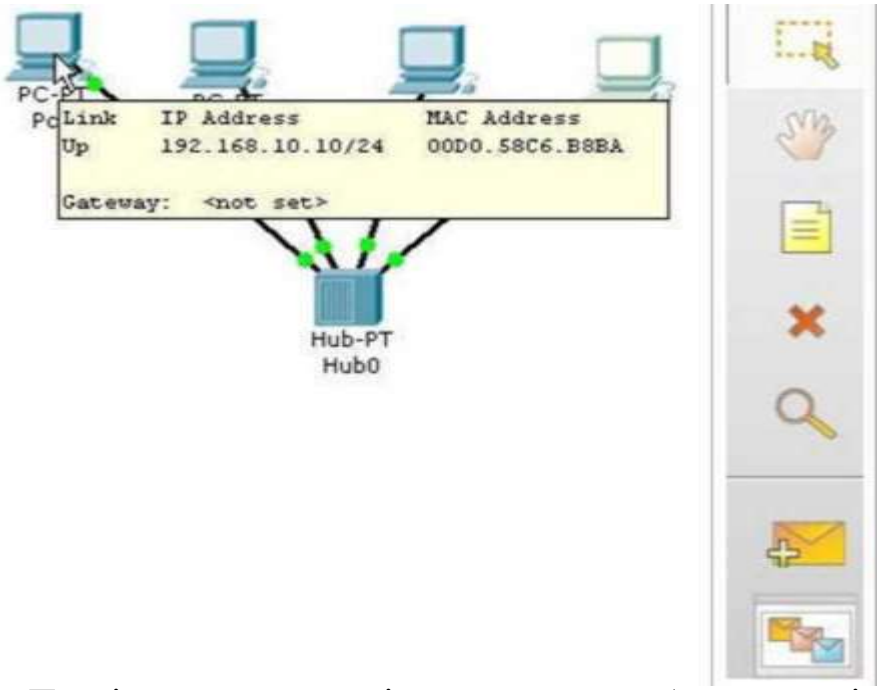


Рис 1.5 - Провірка правильності налаштувань робочих станцій

Пінг програма генерує IP пакет, який містить ICMP повідомлення з запитом відклику. Цей інструмент використовується для перевірки основних звязків 2 і 3 рівнів OSI між двома пристроями. Коли користувач вводить команду пінг, більшість операційних систем відправляє кілька (4 або 5) ICMP Echo повідомлень. Якщо пристрій призначення отримує пінг, запит, у відповідь відправляє Exo-відповідь.

Якщо все налаштовано правильно ми зможемо «пропінгувати» будь-який комп’ютер.

Для прикладу «пропінгуємо» PC0 з PC3.

Команда, яка буде вводитись на PC3: ping **192.168.1.2**

(Packet Tracer дозволяє виконати команду з командного рядка або використати засіб меню Add simple PDU.)

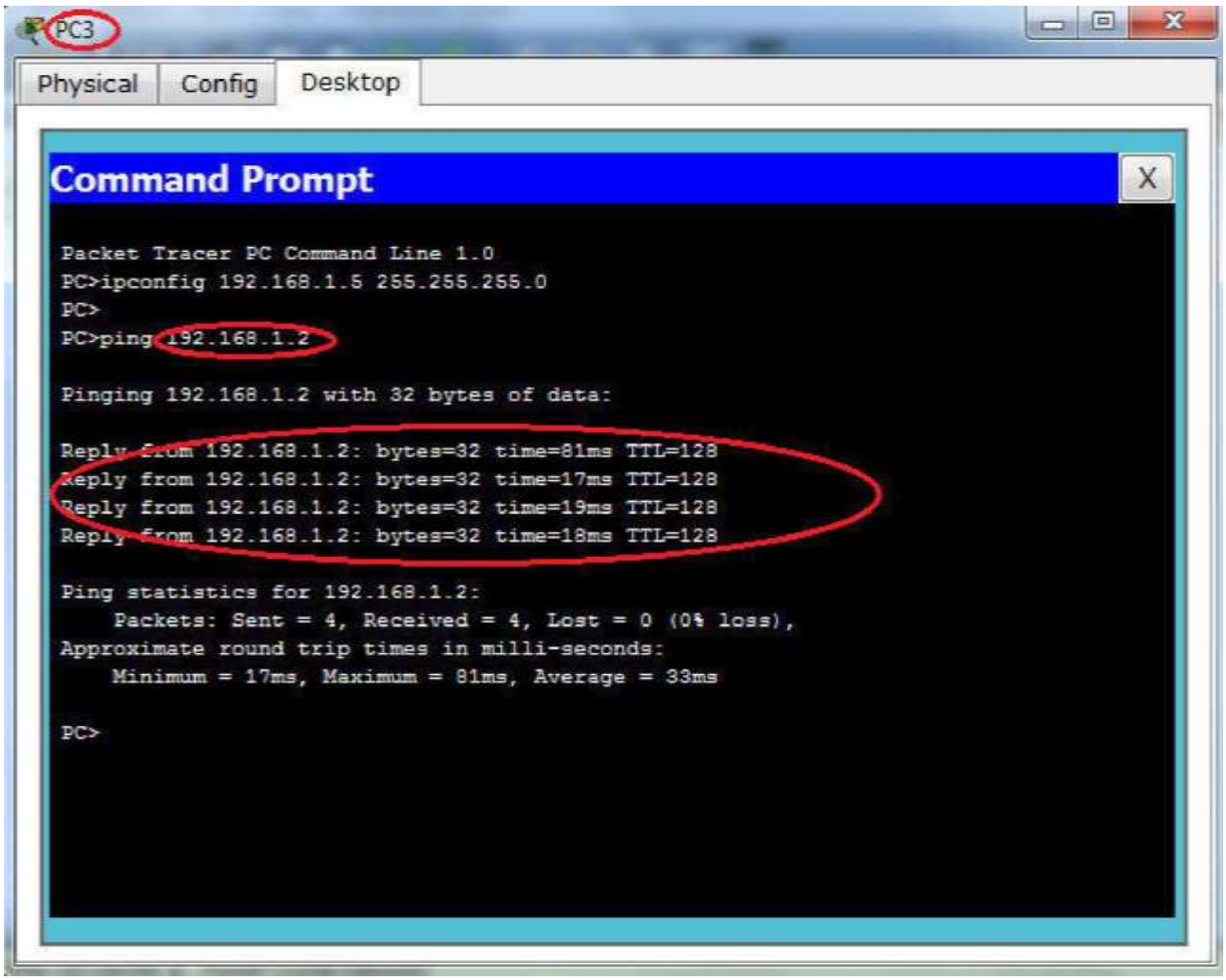
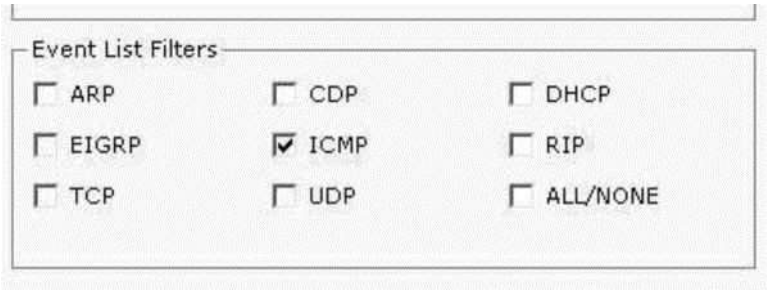


Рис 1.6 - Результат виконання команди Ping

Ping: Використання режиму моделювання.

Клацніть на вкладці Simulation Mode, яка розташована в нижньому правому куті екрану Packet Tracer. Вкладка знаходиться за вкладкою Realtime.

Для того, щоб переглянути лише "пінт", в списку подій (Event List), натисніть на All/None, щоб очистити всі протоколи, а потім натисніть на ICMP, щоб вибрати тільки цей протокол.



Перезапустіть пінг команду у вікні терміналу (Використайте вказівник «Стрілка вгору», щоб повторити останню команду).
Ви помітите, що пакети ICMP в даний час готуються відправитись з PC0 (лівій частині екрану), а також відображається в списку подій (Event List).

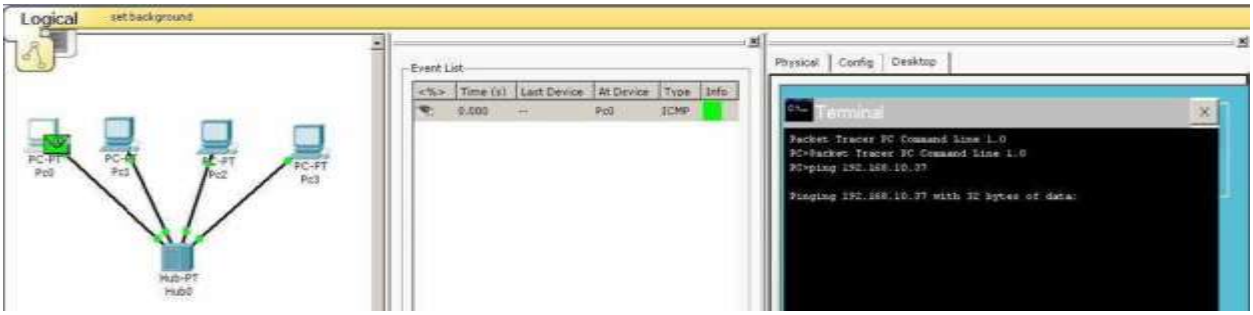


Рис 1.7 - Виконання команди Ping в режимі моделювання

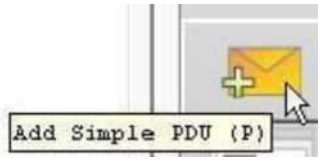
Продовжуйте натискати Capture / Forward кнопку, поки всі кадри всі кадри не будуть відправлені. Зверніть увагу, що концентратор відправляє пакети на всі порти окрім того на який поступив пакет.

Використання інструменту Simple PDU

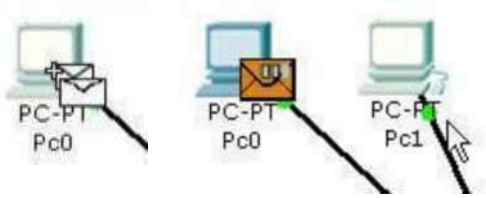
Інший метод для діагностики пристрою є використання інструменту Simple PDU. Цей інструмент виконує пінг без вводу пінг команди.

Відновіть Список подій (Event List), якщо це необхідно, натиснувши на кнопку Reset Simulation.

Виберіть інструмент Add Simple PDU з панелі інструментів:



Натисніть один раз на PC0, пристрій який відправляє пінг (ICMP Echo Request) і натисніть кнопку один раз на PC1 (призначення запиту ICMP Echo Request).



Натисніть кнопку Capture / Forward для перегляду exo-запитів і exo-відповідей.

Примітка: Цей інструмент посилає тільки один ICMP ехо-запит замість чотирьох «пінгів» як при використанні командного рядка.

Контрольні питання

1. Для чого застосовують програму Packet Tracer?
2. Які типи мережевих пристроїв і з'єднань можна використовувати в Packet Tracer?
3. Яким способом можна перейти до інтерфейсу командного рядка пристрою.
4. Яка основна функція команди Ping?
5. Як додати в топологію і налаштувати новий пристрій?

Порядок виконання та здачі роботи

1. Вивчити теоретичну і практичну частину.
2. Здати викладачеві теорію роботи шляхом відповіді на контрольні запитання.
3. Виконати в Packet Tracer практичну частину.
4. Отримайте варіант (1-12) і виконайте в Packet Tracer завдання для самостійної роботи
5. Пред'явіть викладачеві результат виконання завдання для самостійної роботи. Продемонструйте йому, що будь-який комп'ютер пінт з будь-якого комп'ютера.
6. Оформіть звіт.
7. Захистіть звіт.

Завдання для самостійної роботи

1. Побудуйте топологію виду

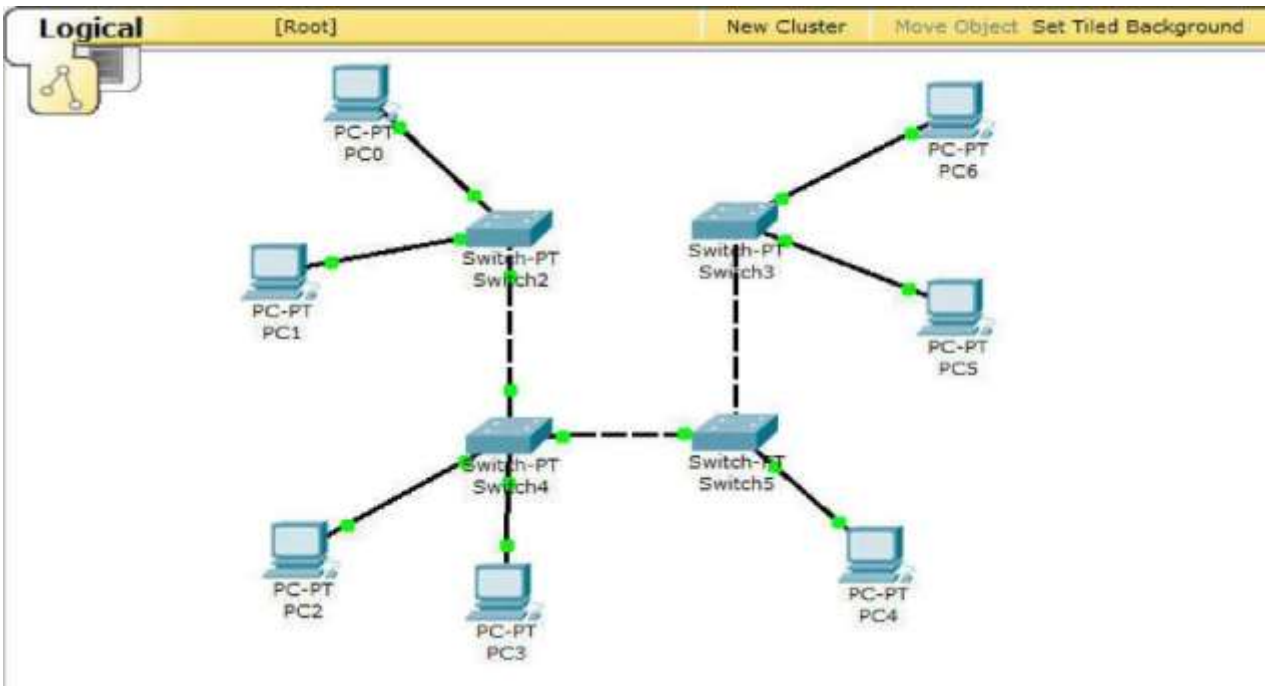


Рис 1.8

2. Налаштувати робочі станції відповідно до варіанту Таблиця 2

Устройство	IP ADDRESS	SUBNET MASK
PC1	v.1.1.1	255.255.255.0
PC2	v.1.1.2	255.255.255.0
PC3	v.1.1.3	255.255.255.0
PC4	v.1.1.4	255.255.255.0
PC5	v.1.1.5	255.255.255.0
PC6	v.1.1.6	255.255.255.0
PC7	v.1.1.7	255.255.255.0

Наприклад, для варіанта 7 (v = 7) і комп'ютера PC1 маємо IP ADDRESS 7.1.1.1

3. Провірити працездатність мережі за допомогою команди Ping

Тема№2: Локальні комп'ютерні мережі

Лабораторне заняття 3: Побудова локальних обчислювальних мереж з використанням технології *ЕШетеі*

Навчальна мета заняття: - Освоїти основні методи побудова локальних обчислювальних мереж з використанням технології Ethemet

Час: 4 год.

Місце проведення: комп'ютерний клас Навчальні питання:

1. **Огляд алгоритму роботи комутатора і створення таблиць MAC-адресів.**
2. **4 Перегляд фрейму з використанням Protocol Analyzer**

Література:

1. Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.
2. Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.

Методичне та матеріально-технічне забезпечення занять:

Персональний комп'ютер, включений в мережу IP, Microsoft Windows.

Хід проведення заняття:

I. Порядок проведення вступу до заняття.

Вступ

Обговорювання теоретичного матеріалу:

II. Порядок проведення основної частини заняття.

Лабораторна робота 2

Тема Побудова локальних обчислювальних мереж з використанням технології *Ethernet*

ГТ1
Теоретична відомості

Технологія Ethernet є найбільш поширеною на сьогоднішній день технологією локальних мереж. У широкому розумінні Ethernet - це ціле сімейство технологій, що включає різні міжнародні та фірмові стандарти, найбільш відомими серед яких є Ethernet, Fast Ethernet, Gigabit Ethernet і IEEE

Усі види стандартів Ethernet використовують метод управління доступом до середовища передачі - метод множинного доступу з контролем несучої і виявленням колізій (carrier sense multiply access with collision detection, CSMA / CD). Цей метод використовується виключно в мережах з шинної топологією (рис 2.1).

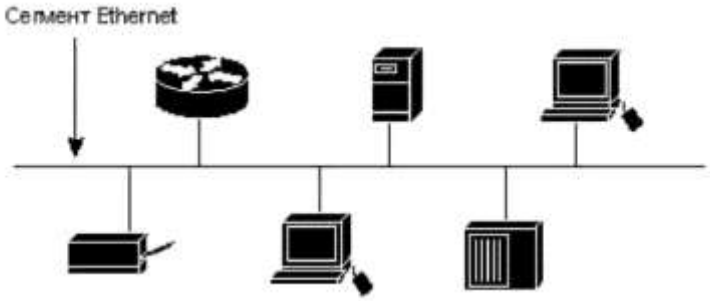


Рис 2.1 - Топологія шина

Підрівень управління доступом до середовища передачі (media access control, MAC) відповідає за формування кадру Ethernet, отримання доступу до середи передачі даних і за відправку кадру вузлу призначення. Колективна середовище Ethernet, незалежно від її фізичної природи, в будь-який момент часу знаходиться в одному з трьох станів - вільна, зайнята, колізія. Стан зайнятості відповідає нормальній передачі кадру одним з вузлів мережі. Стан колізії виникає при одночасній передачі кадрів більш ніж одним вузлом мережі. MAC-підрівень кожного вузла мережі отримує від фізичного рівня інформацію про стан розділяється середовища. Якщо вона вільна, і в MAC- підрівня є кадр для передачі, то виконується передача кадру

Фізичний рівень у процесі передачі стежить за станом середовища. Якщо за час передачі кадру колізія не виникла, то кадр вважається переданим успішно. Якщо ж за цей час була зафіксована колізія, то передача кадру припиняється, і в мережу видається спеціальна послідовність з 32 біт (так звана jam-послідовність), яка повинна допомогти однозначно розпізнати колізію усіма вузлами мережі. Після виявлення колізії вузол витримує паузу, тривалість якої вибирається випадковим чином, а потім знову намагається передати даний кадр. Це дозволяє зменшити ймовірність одночасної спроби захоплення розділяється середовища декількома вузлами при повторній передачі кадру. Інтервал, в межах якого вибирається випадкова величина, зростає з кожною спробою, так що при великому завантаженні мережі і частому виникненні колізій відбувається зниження швидкості передачі даних. При досягненні максимальної кількості спроб передачі одного кадру (як правило, 16), MAC-підрівень відкидає даний кадр і починає передачу наступного.

Для визначення точки призначення пакетів (frames) в мережі Ethernet використовується MAC-адреса. Це унікальний серійний номер привласнений кожному мережному пристрою Ethernet для ідентифікації його в мережі. MAC-адреса привласнюється адаптеру його виробником, але може бути змінений за допомогою програми. Робити це не рекомендується (тільки у разі виявлення двох пристроїв в мережі з однією MAC- адресою). При роботі мережні адаптери проглядають весь мережний трафік, що проходить через них, і шукають в кожному пакеті свою MAC-адресу. Якщо такий знаходиться, то пристрій (адаптер) декодує цей пакет. Існують також спеціальні способи по розсипці пакетів всім пристроям мережі одночасно (broadcasting). MAC-адреса має довжину 6 байт і звичайно записується в шіснадцятковому вигляді, наприклад 12:34:56:78:90:AB

Двокрапки можуть бути відсутній, але їх наявність робить число більш читаним. Кожний виробник привласнює адреси з діапазону адрес, що належить йому. Перші три байти адреси визначають виробника.

Обладнання, що використовується для побудови мереж Ethernet

Мережевий адаптер (Network Interface Card, NIC) - це периферійний пристрій комп'ютера, безпосередньо взаємодіє із середовищем передачі даних, яка прямо чи через інше комунікаційне обладнання пов'язує його з іншими комп'ютерами. Це пристрій вирішує завдання надійного обміну двійковими даними, представленими відповідними електромагнітними сигналами, по зовнішніх лініях зв'язку. Як і будь-який контролер комп'ютера, мережевий адаптер працює під управлінням драйвера операційної системи і

розподіл функцій між мережним адаптером і драйвером може змінюватися від реалізації до реалізації.

Для побудови найпростішої односегментної мережі досить мати мережеві адаптери і кабель відповідного типу. Але навіть у такому простому випадку часто використовуються додаткові пристрої - повторювані (repeater), що дозволяють подолати обмеження на максимальну довжину кабельного сегмента. Основна функція повторювана, як це випливає з його назви - повторення (і посилення) сигналів, що надходять на один з його портів, на всіх інших портах синхронно з сигналами-оригіналами. Повторювач покращує електричні характеристики сигналів та їх синхронність, і за рахунок цього з'являється можливість збільшувати загальну довжину кабелю між найбільш віддаленими в мережі станціями.

Багатопортовий повторювач часто називають концентратором (hub, concentrator), що відображає той факт, що даний пристрій реалізує не тільки функцію повторення сигналів, але й концентрує в одному центральному пристрої функції об'єднання комп'ютерів в мережу. Практично у всіх сучасних мережевих стандартах концентратор є необхідним елементом мережі, що з'єднує окремі комп'ютери в мережу.

Відрізки кабелю, що з'єднують два комп'ютери або будь-які два інших мережевих устрою, називаються фізичними сегментами. Таким чином, концентратори і повторювані, які використовуються для додавання нових фізичних сегментів, є засобом фізичної структуризації мережі.

Концентратори утворюють з окремих фізичних відрізків кабелю загальну середу передачі даних - логічний сегмент. Логічний сегмент також називають доменом колізій, оскільки при спробі одночасної передачі даних будь-яких двох комп'ютерів цього сегмента, нехай і належать різним фізичним сегментами, виникає блокування передавальної середовища. Слід особливо підкреслити, що яку б складну структуру не утворювали концентратори, наприклад, шляхом ієрархічного з'єднання, всі комп'ютери, підключені до них, утворюють єдиний логічний сегмент, в якому будь-яка пара взаємодіючих комп'ютерів повністю блокує можливість обміну даними для інших комп'ютерів.

Міст (bridge), а також його функціональний аналог - комутатор (switch, switching hub), ділить спільне середовище передачі даних на логічні сегменти. Логічний сегмент утворюється шляхом об'єднання кількох фізичних сегментів за допомогою одного або декількох концентраторів. Кожний логічний сегмент підключається до окремого порту моста / комутатора. При надходженні кадру на який-небудь з портів міст / комутатор

повторює цей кадр, але не на всіх портах, як це робить концентратор, а тільки на тому порту, до якого підключений сегмент, що містить комп'ютер-адресат.

Різниця між мостом та комутатором полягає в тому, що міст в кожен момент часу може здійснювати передачу кадрів тільки між однією парою портів, а комутатор одночасно підтримує потоки даних між всіма своїми портами. Іншими словами, міст передає кадри послідовно, а комутатор паралельно. Слід зазначити, що останнім часом локальні мости повністю витіснені комутаторами. Мости використовуються тільки для зв'язку локальних мереж з глобальними, тобто як засоби віддаленого доступу, оскільки в цьому випадку необхідність у паралельній передачі між кількома парами портів просто не виникає.

RoMMymamopfSw itch*)*

Мережевий комутатор або світч (жарт. від англ. Switch - перемикач) - пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента мережі. На відміну від концентратора, який розповсюджує трафік від одного підключеного пристрою до всіх інших, комутатор передає дані лише безпосередньо отримувачу, виняток становить широкомовний трафік (на MAC-адреса FF: FF: FF: FF: FF: FF) усіх вузлів мережі. Це підвищує продуктивність і безпеку мережі, позбавляючи інші сегменти мережі від необхідності (і можливості) обробляти дані, які їм не призначалися.

24 портовий мережевий комутатор

У загальному випадку комутатор (світч) і міст аналогічні по функціональності; різниця полягає у внутрішньому блоці: мости обробляють трафік, використовуючи центральний процесор, комутатор ж використовує комутаційну матрицю (апаратну схему для комутації пакетів). В даний час мости практично не використовуються (так як для роботи вимагають продуктивний процесор), за винятком ситуацій, коли зв'язуються сегменти

мережі з різною організацією фізичного рівня, наприклад, між xDSL, оптикою, Ethernet'ом.

Комутатор зберігає в пам'яті таблицю комутації (зберігається в асоціативної пам'яті), в якій вказується відповідність MAC-адреси вузла порту комутатора. При включенні комутатора ця таблиця порожня, і він працює в режимі навчання. У цьому режимі надходять на який-небудь порт дані передаються на всі інші порти комутатора. При цьому комутатор аналізує кадри (фрейми) і, визначивши MAC-адресу хоста-відправника, заносить його в таблицю. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, MAC-адреса якого вже є в таблиці, то цей кадр буде переданий тільки через порт, зазначений у таблиці. Якщо MAC-адреса хоста-отримувача не асоційований з яких-небудь портом комутатора, то кадр буде відправлений на всі порти. З часом комутатор будує повну таблицю для всіх своїх портів, і в результаті трафік локалізується. Варто відзначити малу латентність (затримку) і високу швидкість пересилання на кожному порту інтерфейсу.

Існує три способи комутації. Кожен з них - це комбінація таких параметрів, як час очікування і надійність передачі.

1. З проміжним зберіганням (Store and Forward). Комутатор читає всю інформацію в кадрі, перевіряє його на відсутність помилок, вибирає порт комутації і після цього посилає в нього кадр.
2. Наскрізний (cut-through). Комутатор зчитує у кадрі тільки адресу призначення і після виконує комутацію. Цей режим зменшує затримки при передачі, але в ньому немає методу виявлення помилок.
3. Бесфрагментний (fragment-free) або гібридний. Цей режим є модифікацією наскрізного режиму. Передача здійснюється після фільтрації фрагментів колізій (кадр розміром 64 байта обробляються за технологією store-and-forward, інші за технологією cut-through).

Комутатори підрозділяються на керовані й некеровані (найбільш прості). Більш складні комутатори дозволяють управляти комутацією мережному (третьому) рівні моделі OSI. Зазвичай їх іменують відповідно, наприклад Layer 3 Switch або просто, скорочено L3. Керування комутатором може здійснюватися за допомогою протоколу Web-інтерфейсу, SNMP, RMON (протокол, розроблений Cisco) і т. п. Багато керовані комутатори дозволяють виконувати додаткові функції: VLAN, QoS, агрегування, віддзеркалення. Складні комутатори можна поєднувати в один логічний пристрій - стек, з метою збільшення числа портів (наприклад, можна об'єднати 4 комутатора з

24 портами і одержати логічний комутатор з (4 * 24-6 = 90) портами, або з 96-ту портами (якщо для стекирования використовуються спеціальні порти)).

Міжмережева операційна система IOS фірми Cisco

При першому вході в IOS мережевого пристрою (розглядаємо в даній роботі саме комутатор) користувач бачить командний рядок користувацького режиму виду:

Switch>

Команди, доступні на рівні користувача є підмножиною команд, що дозволяють виводити на екран інформацію без зміни установок мережного пристрою.

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

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

Про перехід у цей режим буде свідчити поява в командному рядку запрошення у вигляді знаку #. З привілейованого рівня можна отримувати інформацію про налаштування системи та отримати доступ до режиму глобального конфігурування та інших спеціальних режимів конфігурування, включаючи режими конфігурування інтерфейсу, підінтерфейсу, лінії, мережевого пристрою, карти маршрутів і т.п. Для виходу із системи IOS необхідно набрати на клавіатурі команду exit (вихід).

Незалежно від того, як звертаються до мережевого пристрою: через консоль термінальної програми, приєднаної через нуль-модем до COM-порту мережевого пристрою, або в рамках сеансу протоколу Telnet, пристрій можна перевести в один з режимів. Нас цікавлять такі режими.

Призначений для користувача режим - це режим перегляду, в якому користувач може тільки переглядати певну інформацію про мережному пристрої, але не може нічого міняти. У цьому режимі запрошення має вигляд типу Switch>.

Привілейований режим-підтримує команди настроювання і тестування, детальну перевірку мережевого пристрою, маніпуляцію з файлами

налаштувань і доступ в режим конфігурування. У цьому режимі запрошення має вигляд типу Switch #.

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

Практична частина

1. Огляд алгоритму роботи комутатора і створення таблиць MAC-адресів

Для дослідження використаємо аналогічну топологію, що і в попередній роботі. Пристрій 1-го рівня «Хаб», був замінений на пристрій канального рівня моделі OSI Switch.

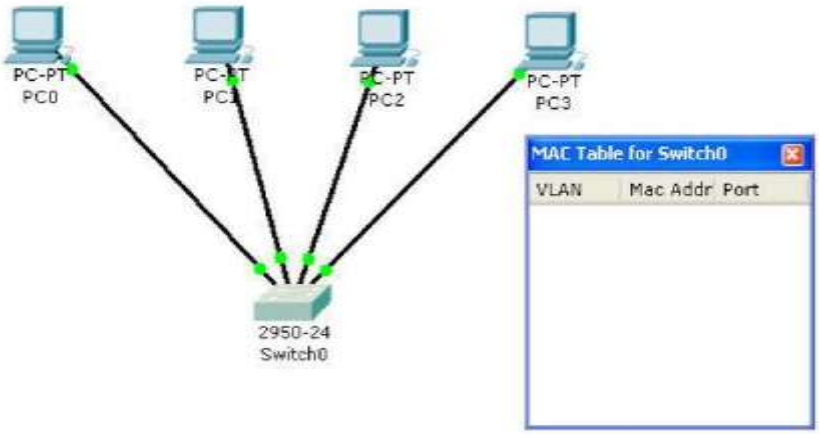
Натисніть на іконку Simulation, щоб перейти до режиму моделювання.

Перегляд таблиці МЛЄ-адресів комутатора

Використовуйте інструмент Select для перегляду IP-адресу та MAC-адреси для різних хостів.

Використовуйте інструмент Inspect для перегляду таблиць MAC-адресів комутатора

Таблиця MAC-адресів порожня, так як не було зафіксовано будь-якого джерела Ethernet MAC-адреси. Зверніть увагу, що існує також VLAN стовпчик в цій таблиці. Це питання буде вивчатися в майбутньому.



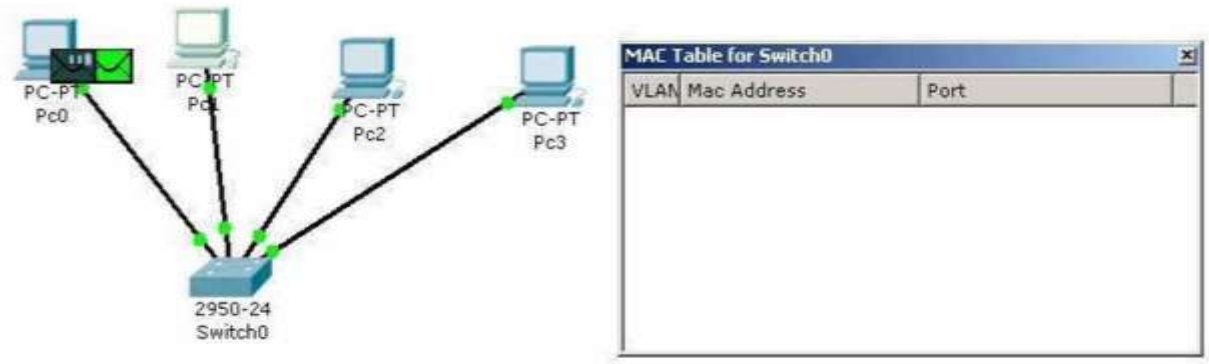
Здійснення команди Ping і перегляд таблиці MAC-адрес

Настроїти **Event List Filters** слідуючим чином:

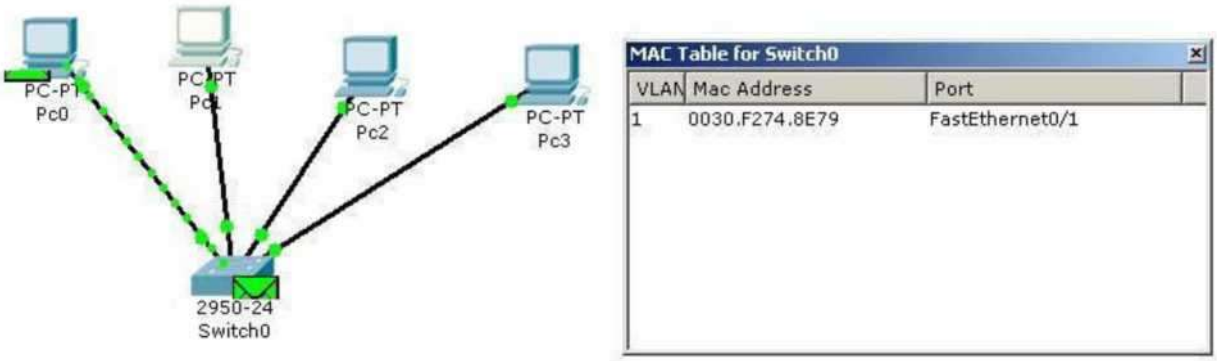
17 ARP Г	**Г CDP [7**	**Г DHCP Г**
EIGRP Г	**ICMP Г**	**RIP Г**
TCP	**UDP**	**All/None**

ARP протокол використовується, щоб дізнатися MAC-адресу, що використовується для інкапсуляції IP-пакетів в Ethemet-кадр. Пакет ARP буде передувати пакетам ICMP.

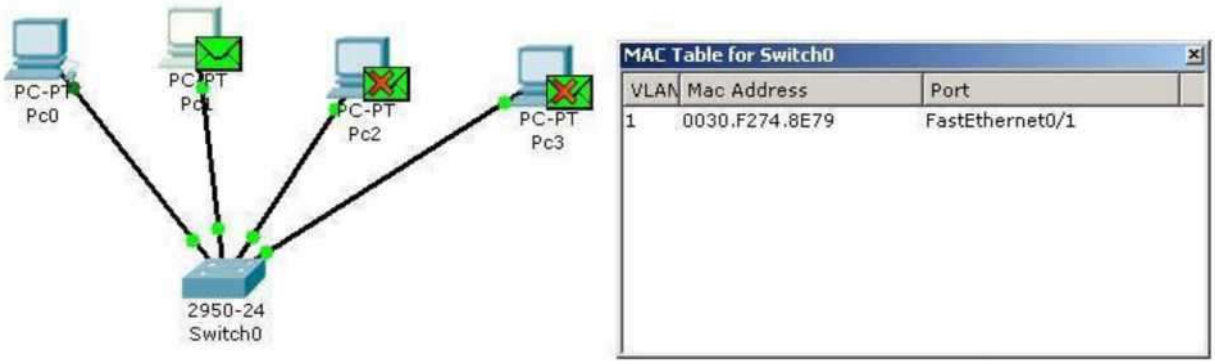
Використовуючи Simple PDU для виконати команди «пінт» від PC0 на PC1. Виберіть Додати PDU з панелі інструментів:



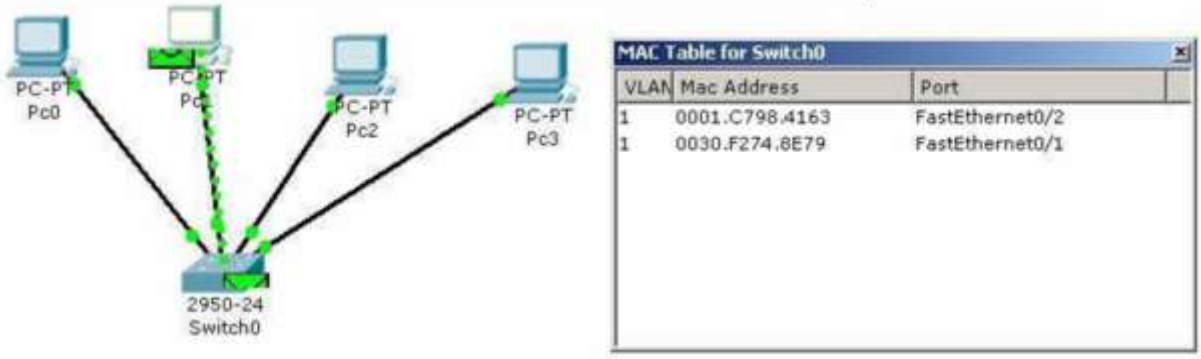
Зверніть увагу, що комутатор запам’ятовує адресу відправника.



Пакети будуть доставлені на всі інші порти, в зв’язку з тим , що в таблиці комутації Switch ще не має адрес. PC2 І PC3 відкинуть фрейм.



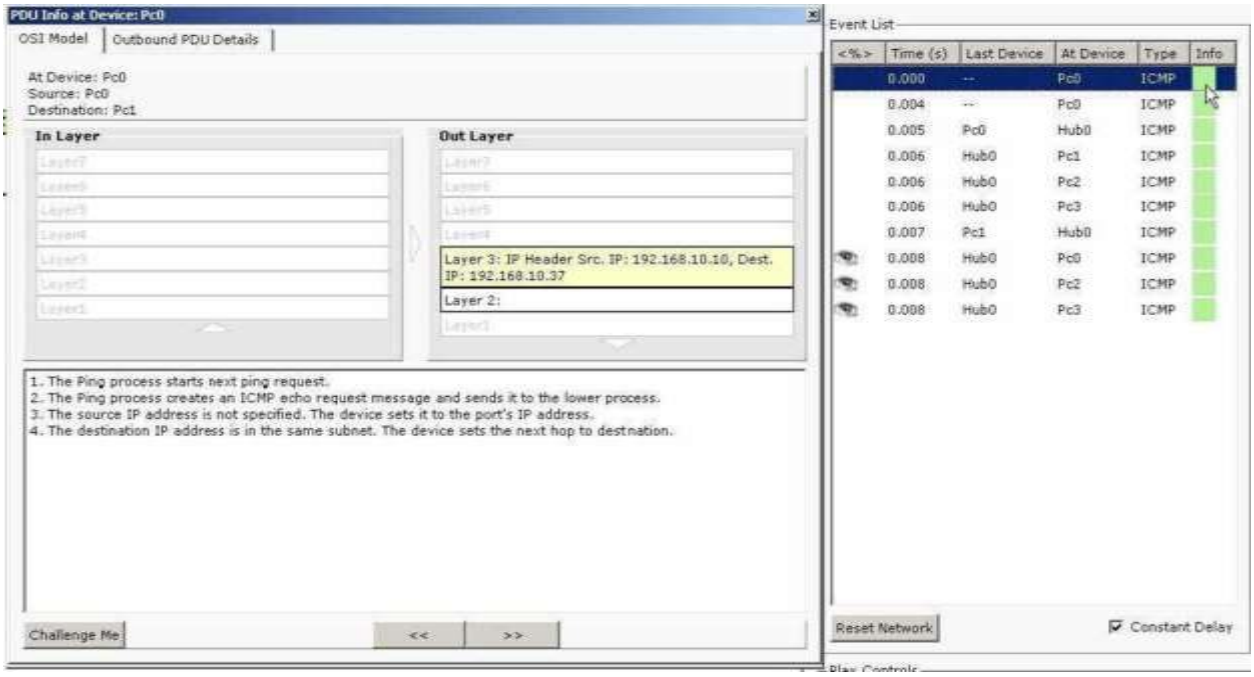
PCI повертає ARP відповідь. Switch вивчає адресу PCI

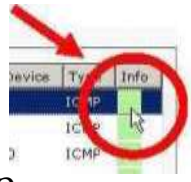


Так як MAC-адреса PC0 була вивчена раніше при відправці фрейму, комутатор відправить відповідь на порт FastEthernet port 0/1

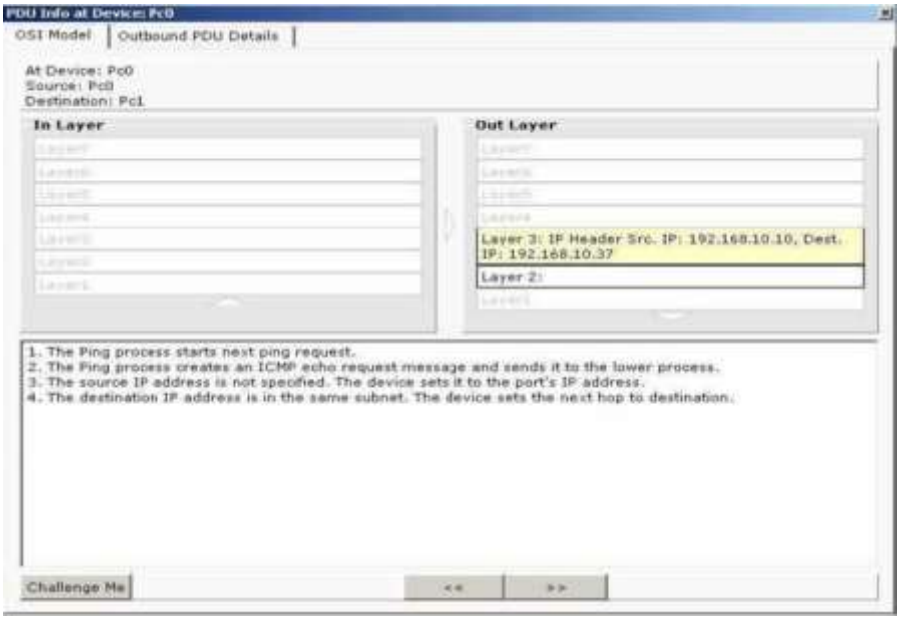
4 Перегляд фрейму з використанням Protocol Analyzer

Щоб детально вивчити фактичні протоколи, які використовуються, натисніть на кольоровій іконці в списку подій.





За замовчуванням ви побачите опис 3-го рівня моделі ОБІ з коротким описом того, що відбувається з пакетом.



Перейдіть на вкладку **Outbound PDU Details,** щоб побачити Ethernet фрейм 2-рівня, IP пакет а також ICMP повідомлення.

»■иямілииді

OSI Model [Outbound PDU Details i

-PDU Formats ----------

Ethernet II

0 _____ 4 _____8 _____14 _____19 Bytes

PREAMBLE: 1010 1010	DES" MAC: 0002.16AB.5C50	SRC MAC: 00D0.58C6.B8BA
TYPE: 0x800	DATA (VARIABLE LENGTH)	FCS: 0x0

I E

0 4 8 16 19 31 Bits

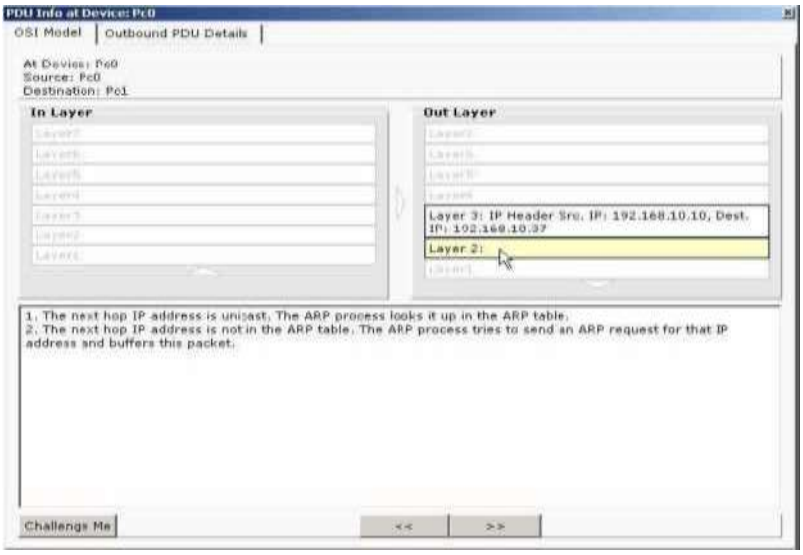
4 j IHL 1 TOS: 0x0	TL: Ox.O
ID: 0x0	0x01 FRAG OFFSET: 0x0
TTL: 32 [PRO: 0x1	CHKSUM: 0x0
SRC IP: 192.168.10.10	
DST IP: 192.168.10.37	
OPT: 0x0 _____1___ ™ ____	
DATA (VARIABLE LENGTH)	

ICMP

0 _____ 8 _____ 16_____ 31 Bits

1 TYPE: 0x8 | CODE: 0x0 | CHECKSUM: 0x0

Натисніть на Layer 2, щоб побачити короткий опис того, що відбувається на 2 рівні моделі OSI.



Контрольні запитання

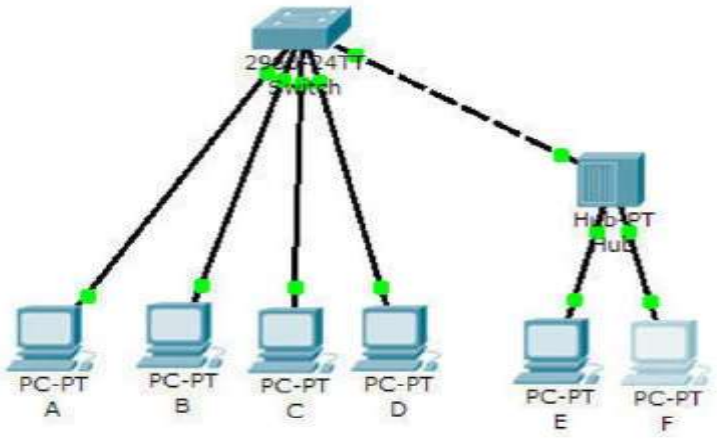
1. Технологія Ethernet. Основні принципи.
2. Що таке колізія? Причини виникнення.
3. Які існують засоби логічної структуризації мережі.
4. Основні функції мережного адаптера.
5. Функції концентратора і комутатора. В чому полягає різниця функціонування цих приладів.
6. Які існують види комутації?
7. Що таке MAC-адреса?
8. Які функції виконує протокол ARP?

Порядок виконання та здачі роботи

1. Вивчити теоретичну і практичну частину.
2. Здати викладачеві теорію роботи шляхом відповіді на контрольні запитання.
3. Виконати в Packet Tracer практичну частину.
4. Отримайте варіант (1-12) і виконайте в Packet Tracer завдання для самостійної роботи
5. Пред'явіть викладачеві результат виконання завдання для самостійної роботи.
6. Оформіть звіт.
7. Захистіть звіт.

Завдання для самостійної роботи

1. Побудуйте топологію виду



- Налаштувати мережні інтерфейси робочих станцій відповідно до таблиці

Пристрій	IP ADDRESS	SUBNET MASK
PC -A	192.168.v.1	255.255.255.0
PC - B	192.168.v.2	255.255.255.0
PC - C	192.168.v.3	255.255.255.0
PC - D	192.168.v.4	255.255.255.0
PC - E	192.168.v.5	255.255.255.0
PC - F	192.168.v.6	255.255.255.0

- Виконати команду Ping з PC -A до PC - B і дослідити заповнення таблиці комутації комутатора і ARP-таблиць робочих станцій в режимі моделювання.
- Очистити таблицю комутації через консоль командою **clear mac-address-table dynamic**
- Виконати команду Ping з PC -E до PC - F и дослідити як формується таблиця комутації світча при передачі даних через «хаб»

Тема№2: Локальні комп'ютерні мережі

Лабораторне заняття 4: Об’єднання сегментів у єдину мережу. Маршрутизація. Статична маршрутизація

Навчальна мета заняття: - Освоїти основні методи об'єднання сегментів у єдину мережу. Освоїти маршрутизацію

Час: 4 год.

Місце проведення: комп’ютерний клас Навчальні питання:

1. **Маршрутизація**
2. **Маршрутизація за замовчуванням**
3. **Команда trace**
4. **Статичні маршрути**

Література:

1. **Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.**
2. **Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.**

Методичне та матеріально-технічне забезпечення занять:

Персональний комп'ютер, включений в мережу IP, Microsoft Windows.

Хід проведення заняття:

I. Порядок проведення вступу до заняття.

Вступ

Обговорювання теоретичного матеріалу:

II. Порядок проведення основної частини заняття.

Лабораторна работа №3.

Тема. Об’єднання сегментів у єдину мережу. Маршрутизаія. Статична маршрутизация

Теоретична частина

ARP (Address Resolution Protocol)

Коли відправник визначив IP адресу приймача, він дивиться в свою ARP таблицю щоб дізнатися MAC адресу приймача. Якщо джерело виявляє, що MAC і IP адреси приймача присутні в ARP таблиці, він встановлює між ними відповідність і використовує його в ході інкапсуляції IP пакетів у фрейми канального рівня. MAC адреси фреймів канального рівня беруться з ARP таблиць. Після цього фрейм з фізичного каналу відправляється від відправника до адресата.

Якщо відправник має IP пакет для одержувача з IP-адресою АДР і ця адреса відсутня в ARP таблиці, то відправник відправляє по мережі широкомовний ARP запит наступного змісту: повідомте MAC адресу мережного інтерфейсу з IP-адресою АДР. Запит приймають всі мережеві пристрої в сегменті мережі, і тільки пристрій, що має IP-адресу АДР, реагує на нього, посилаючи відправнику інформацію про MAC адресу свого мережного інтерфейсу з IP адресою АДР. Відправник записує пару <MAC адресу, IP-адресу АДР> у свою ARP таблицю.

Маршрутизація

Протоколи маршрутизації - це правила, за якими здійснюється обмін інформацією про шляхи передачі пакетів між маршрутизаторами. Протоколи характеризуються часом збіжності, втратами і масштабованістю. В даний час використовується декілька протоколів маршрутизації. Кожен протокол має сильні і слабкі сторони.

Маршрутизатор (англ. Router) — спеціалізований мережний пристрій, що використовується для по'єднання двох або більше мереж та керує процесом маршрутизації, тобто на підставі інформації про топологію мережі і певних правил приймає рішення про пересилку пакетів мережевого рівня (рівень 3 моделі OSI) між різними сегментами мережі.

Одна з головних завдань маршрутизатора полягає у визначенні найкращого шляху до заданого адресату. Маршрутизатор визначає шляхи (маршрути) до адресатів або з статичної конфігурації, введеної адміністратором, або динамічно на підставі маршрутної інформації, отриманої від інших маршрутизаторів. Маршрутизатори обмінюються маршрутною 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. Для перегляду таблиці маршрутів слід використовувати команду show ip route. Навіть, якщо на деякому маршрутизаторі X не задавалися ніякі команди маршрутизації, тоді він все одно

будує таблицю маршрутів для безпосередньо під'єднаних до нього мереж, наприклад:. . .

C 192.168.4.0/24 is directly connected, EthernetO
10.0. 0.0/16 is subnetted, 3 subnets
C 10.3.0.0 is directly connected, Serial0
C 10.4.0.0 is directly connected, Serial1
C 10.5.0.0 is directly connected, Ethernet1

Маршрут на безпосередньо приєднані мережі відображається на інтерфейсі маршрутизатора, до якого вони приєднані. Тут / 24 позначає маску 255.255. 255.0, а / 16 - 255.255.0.0.

Таблиця маршрутів відображає мережні префікси (адреси мереж) на вихідні інтерфейси. Коли X отримує пакет, призначений для 192.168.4.46, він шукає префікс 192.168.4.0/24 в таблиці маршрутів. Згідно таблиці пакет буде спрямований на інтерфейс EthernetO. Якщо X отримає пакет для 10.3.21.5, він направить його на SerialO.

Ця таблиця показує чотири маршрути для безпосередньо приєднаних мереж. Вони мають мітку C. Маршрутизатор X відкидає всі пакети, що направляються до мереж, не зазначених у таблиці маршрутів. Для направлення пакетів до інших абонентів, треба в таблицю включити додаткові маршрути. Нові маршрути можуть бути додані двома методами:

Статична маршрутизація - адміністратор вручну визначає маршрути до мереж призначення.

Динамічна маршрутизація - маршрутизатори дотримуються правил, які 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.

Для конфігурації статичної маршрутизації в маршрутизаторах Cisco використовують дві версії команди ip route

Перша версія

ip route АдресМережі призначення МаскаМережі призначення Інтерфейс

Команда вказує маршрутизатору, що всі пакети, призначені для *Адрес Мережі призначення- МаскаМережі призначення* слід направляти на свій інтерфейс *Інтерфейс.* Якщо інтерфейс *Інтерфейс* - типу Ethernet, то фізичні (MA C) адреси вихідних пакетів будуть широкомовними (чому?).

Вторая версия

ip route АдресМережі призначення МаскаМережі призначення Адреса

Команда вказує маршрутизатора, що всі пакети, призначені для АдресМережі призначення-МаскаМережі призначення, слід спрямовувати на той свій інтерфейс, з якого можна досягти IP адреса *Адреса.* Як правило, Адреса це адреса наступного стрибка по дорозі до Адрес Мережі призначення.

Вихідний інтерфейс і фізичні адреси вихідних пакетів визначаються маршрутизатором за своїми ARP таблицями на підставі IP адреси Адреса. Наприклад

ip **route 10.6.0.0 255.255.0.0 Seriall (1)**

ip route 10.7.0.0 255.255.0.0 10.4.0.2 (2)

Перший приклад відображає мережний префікс 10.6.0.0/16 на локальний інтерфейс маршрутизатора Seriall. Наступний приклад відображає мережний префікс 10.7.0.0/16 на IP адреса 10.4.0.2 наступного стрибка по дорозі до 10.7.0. 0/16. Обидві ці команди додадуть статичні маршрути в таблицю маршрутизації (мітка S):

S 10.6.0.0 via Seriall

S 10.7.0.0 [1/0] via 10.4.0.2

Коли інтерфейс виходить з ладу, всі статичні маршрути, які відображаються на цей інтерфейс, видаляються з таблиці маршрутів. Якщо маршрутизатор не може більше знайти адресу наступного стрибка по дорозі до адресою, вказаною в статичному маршруті, то маршрут виключається з таблиці.

Зауважимо, що для мереж типу Ethernet рекомендується завжди використовувати форму (2) команди ip route. Ethernet інтерфейс на маршрутизатору як правило, з'єднаний з декількома Ethernet інтерфейсами інших пристроїв у мережі. Вказівка в команді ip route IP адреси дозволить маршрутизатору правильно сформувати фізичну адресу вихідного пакету за своїми ARP таблицями.

Маршрутизація за замовчуванням

Зовсім не обов'язково, щоб кожен маршрутизатор обслуговував маршрути до всіх можливих мереж призначення. Замість цього маршрутизатор зберігає маршрут за замовчуванням або шлюз останнього притулку (last resort). Маршрути за замовчуванням використовуються, коли маршрутизатор не може поставити у відповідність мережі призначення рядок у таблиці маршрутів. Маршрутизатор повинен використовувати маршрут за замовчуванням для відсилання пакетів іншому маршрутизатора. Наступний маршрутизатор буде мати маршрут до цієї мережі призначення або мати свій маршрут за замовчуванням до третього маршрутизатора і т.д. У кінцевому рахунку, пакет буде маршрутизувати на маршрутизатор, що має маршрут до мережі призначення.

Маршрут за замовчуванням може бути статично введений адміністратором або динамічно отриманий з протоколу маршрутизації.

Ручне завдання маршруту за замовчуванням на кожному маршрутизаторі підходить для простих мереж. У складних мережах необхідно організувати

Команда trace

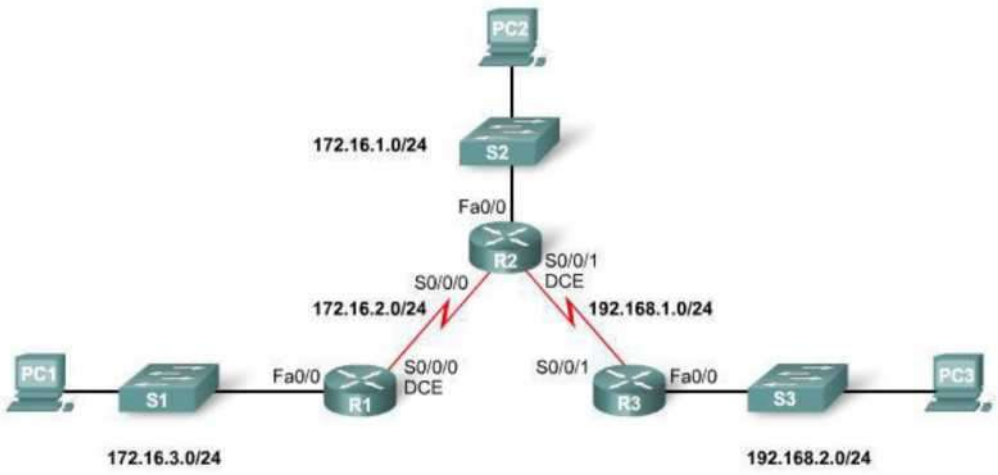
Команда trace є ідеальним способом для з'ясування того, куди відправляються дані в мережі. Ця команда використовує ту ж технологію протоколу ICMP, що і команда ping, тільки замість перевірки наскрізний зв'язку між відправником та одержувачем, вона перевіряє кожен крок на шляху. Команда trace використовує здатність маршрутизаторів генерувати повідомлення про помилку при перевищенні пакетом свого встановленого часу життя (Time To Live, TTL). Ця команда посилає декілька пакетів і виводить на екран дані про час проходження туди і назад для кожного з них. Перевага команди trace полягає в тому, що вона показує черговий досягнутий маршрутизатор на шляху до пункту призначення. Це дуже потужний засіб для локалізації відмов на шляху від відправника до одержувача. Варіанти відповідей утиліти trace

Символ	Значення
!H	Зондуючий пакет був прийнятий маршрутизатором, але не переадресований, що зазвичай буває через список доступу
P	Протокол недосяжний
N	Мережа недосяжна
U	Порт едосяжний
*	Перевищення межі очікування

Таблиця 1.

Практична частина

1. Побудуйте топологію виду:



2. Налаштуйте елементи мережі відносно адресної таблиці

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F a 0/0	172.16.3.1	255.255.255 0	N/A
	S0/0/0	172.16.2.1	255.255.255 0	N/A
R2	F a 0/0	172.16.1.1	255.255 .255 0	N/A
	S0/0/0	172.16.2.2	255.255.255.0	N/A
	S0/0/1	192.168.1.2	255.255.255 0	N/A
R3	F a 0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/1	192.168.1.1	255.255.255 0	N/A
PC1	NIC	172.16.3.10	255.255.255 0	172.16.3.1
PC2	NIC	172.16.1.10	255.255.255.0	172.16.1.1
FC3	NIC	192.168.2.10	255.255.255 0	192.168.2.1

ARP

1 Приєднайтесь до маршрутизатора Router 1 с і подивіться його ARP таблицю Router1#**show arp**

```
Rlpshcu Erp
F□toccl Iddieas                Age (ir.zIn) HEidware Addr Type Interface
Internet 172.1-e. 3.1                  -    0030.219D .B7Ü1 AREA ?E3tSthernet0/0
```

Вона містить лише один рядок про MAC адресу свого Ethernet інтерфейсу з IP адресою 172.16.3.1

2. Пропінгуйте Ethernet интерфейс маршрутизатора Router1 з PC1 ping 172.16.3.1

3 . Знову подивіться вашу ARP таблицю.

```
ÎUFShütJ EEp Frctüccl Address
Internet 172.15.3.1          Age (ir.in) Hardware Addr Type          Interface
Internet 172.15.3.10                  -   0004.9A13.D273 AAPA       FaatïthernetO/O
                             0 ÜÜEO.BÜSC.3D53 AAPA                  Faat-tiiernetO/O
```

З'явився запис про MAC адресу Ethernet інтерфейсу PC1 з IP адресою 172.16.3.2 Чому, адже ми не слали від Routerl ніяких IP пакетів? Тому, що Routerl для відповіді на пінт від PC1 повинен був знати про MAC адресу Ethernet інтерфейсу PC1 з IP адресою 172.16.3.2, і він сформував ARP пакет для її отримання.

Статичні маршрути

1. Перш за все проглянемо таблицю маршрутизації на прикладі Routerl за допомогою команди **show ip route**

Router1# **show ip route**

```
Cedes :  C - connected, 5 - static, I - IGRE, & - RIP, M - itebile, B - BGE □ - EIGRF, EX -
         EIGRE eiternsl, O - OSFF, IA. - OSEE inter area Hl - OSEE HSSA external type 1, N2
         - OSEE HSSA external type 2 El - OSEE external type 1, Eî - OSEE external type 2, S -
         E&P i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter * - candidate
         default, U - per-user static reute, Ü - ODR E - pericdic dcwnlcaded static reute          area


Gatevay ÜE last resert is net set

      172.1c.0.0/24 is subnetted, 2 subnets C    172.1£.2.0 is
directly cennected, SerialO/l/o|
C          172.1€.3-G is directly cennected, FestEthernetO/O
```

Бачимо безпосередньо приєднані мережі.

Немає маршруту до мережі 172.16.1.0/24, тобто не можливо буде здійснити зв'язок між PC1 і PC2. Додамо маршрут до мережі 172.16.1.0/24 через адресу 172.16.2.0 найближчого хопу на шляху до цієї мережі:

Router1(config)#**ip route 172.16.1.0 255.255.255.0 172.16.2.0**

(Для виконання даної команди слід перейти в режим налаштувань набравши в консолі configure і зявиться відповідно Router1(config)# **)**

Тут і далі 172.16.10.0/24 - це скорочений запис - визначення підмережі 172.16.1.0 з маскою 255.255.255.0. У масці 255.255.255.0 міститься 24 одиниці, що й позначається / 24. (більш детально структура IP-адреси і маски буде розглянута в слідкуючій роботі).

Проглянемо знов таблицю маршрутизації:

```
      172.1c.0.0/24 is subnetted, 3 subnets S
        172 .le .1.0 [1/0] via 172.15.2.1
C       172.le.2.0 is directly cennected, SerielO/l/O
C       172.1c.3.0 is directly cennected, EastEthernetO/0
",i_l
```

Як бачимо з'явився запис маршруту до мережі 172.16.1.0/24.

3. Виконаємо команду Ping з PC1 до PC 2 в режимі моделювання В командному рядку PC1 введемо ping 172.16.1.3

Як бачимо ICMP пакети доходять до місця призначення, але відповіді назад не повертаються, так як в таблиці маршрутизації R2 немає маршруту в мережу 172.16.3.0/24.

```
Gateway cf last resert is net set

      172.15.0.0/24 is sub netted, 2 subnets C   172.15.1.0 is directly
cennected, FastEthernetO/0
C          172.15.2.0 is directly cennected, SerialO/1/0
2       1Ɔ2. lcS.l. 0/24 is directly cennected. Serial0/1/1
```

Слід добавити такий маршрут:

Router2(config)#**ip route 172.16.3.0 255.255.255.0 172.16.2.0**

Ще раз виконаємо команду ping 172.16.1.3 з PC1 в режимі моделювання. Переконаємося що пакети передаються належним чином.

Виконаємо налаштування інших роутерів таким чином щоб в мережі були доступні усі мережеві пристрої із усіх хостів.

Збережіть проект в цілому і конфігурацію кожного маршрутизатора в окремий файл.

Контрольні питання

1. Як відправник дізнається MAC адресу одержувача?
2. Коли в ARP таблиці з'являються нові рядки?
3. Що таке таблиця маршрутів?
4. Якщо адміністратор не налаштовував жодних маршрутів, то що в ній буде міститись?
5. Чим статична маршрутизація відрізняється від динамічної?
6. Які дві форми завдання статичної маршрутизації ви знаєте?
7. Як у команді маршрутизації визначається мережу призначення?
8. Поясніть значення полів в командах маршрутизації.
9. Коли використовується маршрутизація за замовчуванням?
10. Як працює команда тросіровки?

Порядок виконання та здачі роботи

1. Вивчити теоретичну і практичну частину.
2. Здати викладачеві теорію роботи шляхом відповіді на контрольні запитання.
3. Виконати в Packet Tracer практичну частину.
4. Отримайте варіант і виконайте в Packet Tracer завдання для самостійної роботи.
5. Пред'явіть викладачеві результат виконання пунктів 8 і 9 завдання для самостійної роботи.
6. Оформіть звіт.
7. Захистіть звіт.

Завдання для самостійної роботи

1. Побудувати в Packet Tracer топологію, представлену на малюнку. (Рисунок 1) Використовувати необхідні маршрутизатори.

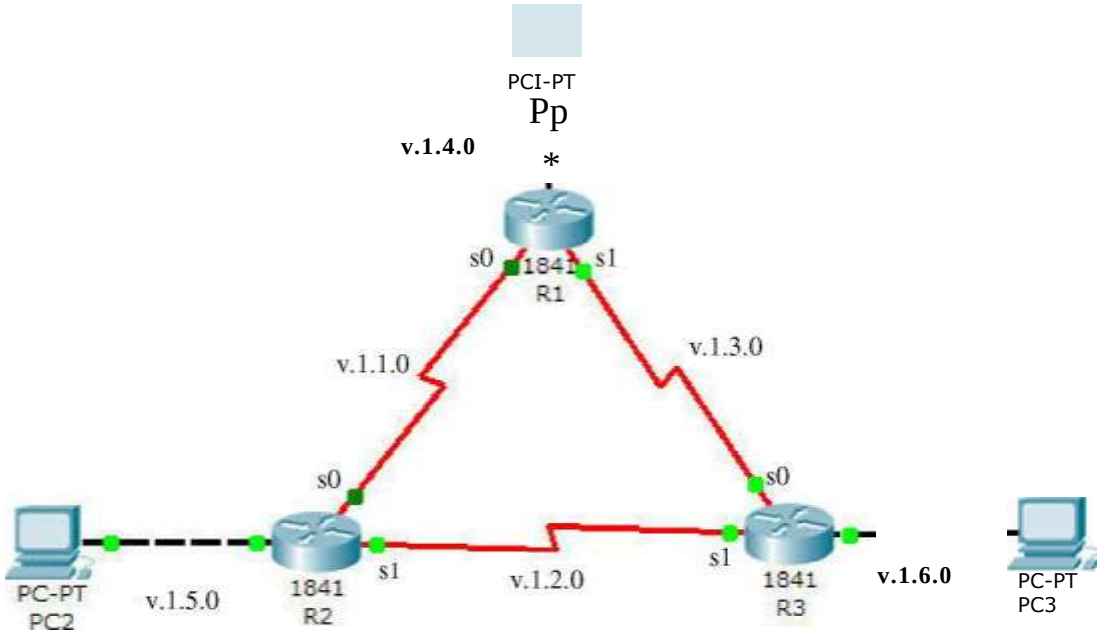


Рисунок 1 - Топологія мережі для самостійного завдання

У представленій мережі шість підмереж. Ви бачите, що кожен маршрутизатор підключений до трьох підмереж.

2. На кожному маршрутизаторі включити використовувані інтерфейси і подивитися сусідів командою show cdp neighbors. Зробити скріншоти.

3. Призначити інтерфейсам мережі адреси згідно з рисунком 1 і таблиці 1 в яких v - це номер варіанта. Всі маски 255.255.255.0. Не забудьте призначити шлюзи за замовчуванням для комп'ютерів відповідно таблиці ..

	v.1.1.0	v.1.2.0	v.1.3.0	v.1.4.0	v.1.5.0	v.1.6.0
Routerl	S0:v. 1.1.1		S1:v.1.3.1	E0:v.1.4.1		
Router2	S0:v.1.1.2	S1:v.1.2.1			E0:v.1.5.1	
Router3		S0:v.1.2.2	S1:v.1.3.2			E0:v.1.6.1
PC1				E0:v.1.4.2		
PC2					E0:v.1.5.2	
PC3						E0:v.1.6.2

4. Перевірте факт призначення адрес шляхом виконання на кожному маршрутизаторі команд show running-config і show ip interface brief. Для комп'ютерів використовуйте команду ipconfig.

5. Перевірте правильність призначення адрес шляхом виконання на кожному маршрутизаторі команд ping до безпосередніх сусідів. Наприклад, на маршрутизаторі Routerl виконайте

Routerl # ping v.1.1.2

Routerl # ping v.1.3.2

Routerl # ping v.1.4.2

6. Поставимо перед собою задачу пов'язати між собою комп'ютери PC1, PC2 і PC3. Для цього здійснимо на маршрутизаторах настройку статичної маршрутизації. У кожному маршрутизаторі пропишемо маршрути на віддалені Ethernet мережі. Для вирішення поставленого завдання маршрутизувати пакети на віддалені мережі послідовних з'єднань не треба.

У кожного маршрутизатора є по дві на віддалені Ethernet мережі. Всього треба прописати шість статичних маршрутів.

Щоб з маршрутизатора routerl досягти віддалену Ethernet мережа v.1.5.0/24, пакети можна направити на IP адреса 1.1.1.2 найближчого зовнішнього інтерфейсу на шляху в цю мережу. Це зробить команда

router1 (config) # ip route 1.1.5.0 255.255.255.0 1.1.1.2

Задайте інші п'ять команд маршрутизації.

7. На кожному маршрутизаторі подивитися таблицю маршрутизації командою show ip route. Зробити скріншоти.

8. На кожному комп'ютері зробіть скріншоти виконання команд трасування tracert інших комп'ютерів. Всього шість скріншотів. Наприклад, трасування PC1 на PC2 для варіанту 1 (v = 1)

```
PCI:fttracert 1.1.5.2


"Type escape sequence to abort. "
Tracinq the route to 1.1.5.2

  1  1.1.4.1 0 msec 16 msec 0 msec
  2  1.1.1.2 20 msec 16 msec 16 msec
  3  1.1.5.2 20 msec 16 msec *
```

11. Збережіть проект.

Зміст звіту.

Звіт готується в електронному вигляді і роздруковується. Звіт містить

1. Скріншот топології, створеної при виконанні практичної частини.
2. Скріншот топології з малюнка 1 з адресами свого варіанту
3. Таблицю 2 з адресами свого варіанту
4. Конфігурації трьох маршрутизаторів з. Txt файлів, створених при виконанні завдання для самостійної роботи.
5. Всі скріншоти, зазначені в завданні для самостійної роботи

Тема№3: Глобальні комп'ютерні мережі Лабораторне заняття 5:

Побудова корпоративної мережі

Навчальна мета заняття: - Освоїти основні методи побудови корпоративної мережі

Час: 4 год.

Місце проведення: комп'ютерний клас Навчальні питання:

1. **IP-адресація на мережному рівні. Безкласова адресація. Маски змінної довжини**
2. **Використання масок в IP-адресації - безкласова адресація**
3. **Supernetting**
4. **VLSM**
5. **Практична частина**

Література:

1. **Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.**
2. **Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.**

Методичне та матеріально-технічне забезпечення занять:

Персональний комп'ютер, включений в мережу IP, Microsoft Windows.

Хід проведення заняття:

I. Порядок проведення вступу до заняття.

Вступ

Обговорювання теоретичного матеріалу:

II. Порядок проведення основної частини заняття.

Лабораторна робота 4

Тема: Побудова корпоративної мережі.

Теоретична частина

IP-адресація на мережному рівні. Безкласова адресація. Маски змінної довжини

У стеці TCP/IP(стек протоколів - сукупність протоколів для виконання певної задачі, в данному випадку передачі данних) використовуються три типи адрес: локальні (які також називаються апаратними(MAC-адреси)), IP-адреси й символьні доменні імена.

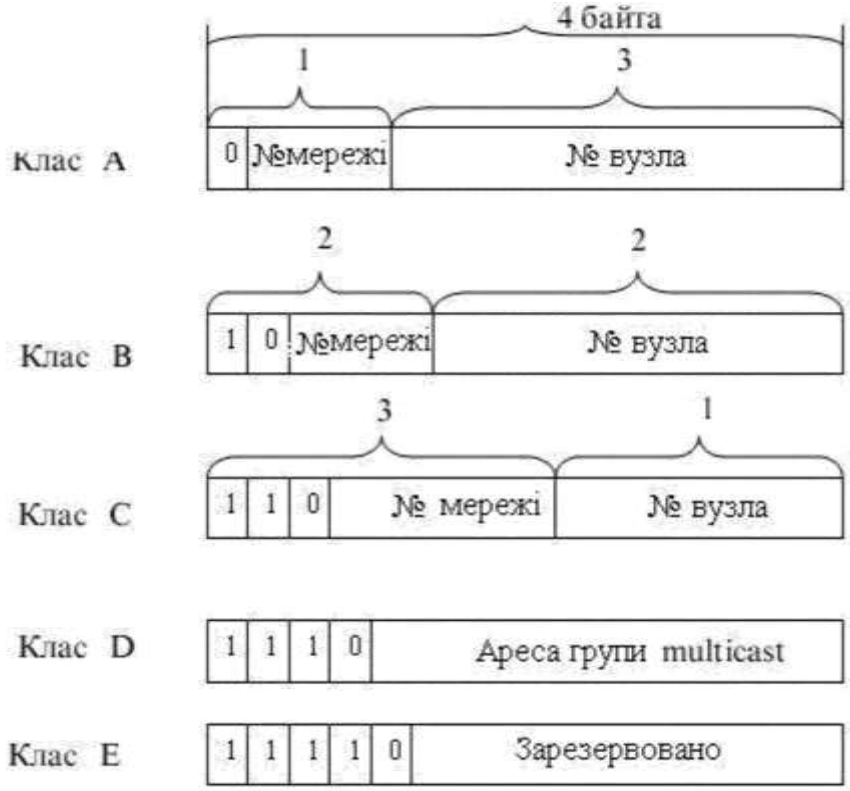
Розглянемо детальніше IP адреси

IP-адреси являють собою основний тип адрес, на підставі яких мережевий рівень передає пакети між мережами. Ці адреси складаються з 4 байт, наприклад 109.26.17.100. IP-адреса призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів. IP-адреса складається із двох частин: номера мережі й номера вузла. Номер мережі може бути обраний адміністратором довільно, або призначений за рекомендацією спеціального підрозділу Internet (Internet Network Information Center, InterNIC), якщо мережа повинна працювати як складова частина Internet. Звичайно постачальники послуг Internet одержують діапазони адрес у підрозділів InterNIC, а потім розподіляють їх між своїми абонентами. Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Маршрутизатор по визначенню входить відразу в кілька мереж. Тому кожен порт маршрутизатора має власну IP-адресу. Кінцевий вузол також може входити в кілька IP-мереж. У цьому випадку комп'ютер повинен мати кілька IP-адрес, по числу мережевих зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання.

IP-адреса має довжину 4 байти й звичайно записується у вигляді чотирьох чисел, що представляють значення кожного байта в десятковій формі й розділених точками, наприклад, 128.10.2.30 - традиційна десяткова форма представлення адреси, а 10000000 00001010 00000010 00011110 - двійкова форма представлення цієї ж адреси.

Адреса складається із двох логічних частин — номера мережі й номери вузла в мережі. Яка частина адреси відноситься до номера мережі, а яка — до номера вузла, визначається значеннями перших біт адреси. Значення цих біт є також ознаками того, до якого класу відноситься та або інша IP-адреса.

На Рис. 1 показана структура IP-адреси різних класів.



Рисі - Структура IP адреси

Якщо адреса починається з 0, то мережу відносять до класу A и номер мережі займає один байт, інші 3 байти інтерпретуються як номер вузла в мережі. Мережі класу A мають номери в діапазоні від 1 до 126. (Номер 0 не використовується, а номер 127 зарезервований для спеціальних цілей, про що буде сказано нижче.) Мереж класу A небагато, зате кількість вузлів у них може досягати 2^{24}, тобто 16 777 216 вузлів.

Якщо перші два біти адреси є 10, то мережа відноситься до класу B. У мережах класу B під номер мережі й під номер вузла виділяється по 16 біт, тобто по 2 байти. Таким чином, мережа класу B є мережею середніх розмірів з максимальним числом вузлів 2^{16}, що становить 65 536 вузлів.

Якщо адреса починається з послідовності 110, то це мережа класу C. У цьому випадку під номер мережі приділяється 24 біти, а під номер вузла — 8 біт.

Мережі цього класу найпоширеніші, число вузлів у них обмежено 2^{8}, тобто 256 вузлами.

Великі мережі одержують адреси класу A, середні - класу B, а малі - класу C.

Особливі IP-адреси

У протоколі IP існує кілька угод про особливу інтерпретацію IP-адрес.

- Якщо вся IP-адреса складається тільки із двійкових нулів, то вона позначає адресу того вузла, що згенерував цей пакет; цей режим використовується тільки в деяких повідомленнях ICMP.
- Якщо в полі номера мережі стоять тільки нулі, то за замовчуванням вважається, що вузол призначення належить тій же самій мережі, що й вузол, що відправив пакет.
- Якщо всі двійкові розряди IP-адреси рівні 1, то пакет з такою адресою призначення повинен розсилатися всім вузлам, що перебувають у тій же мережі, що й джерело цього пакета. Таке розсилання називається обмеженим широкомовним повідомленням (limited broadcast).
- Якщо в поле номера вузла призначення стоять тільки одиниці, то пакет, що має таку адреса, розсилається всім вузлам мережі із заданим номером мережі. Наприклад, пакет з адресою 192.190.21.255 доставляється всім вузлам мережі 192.190.21. 0. Таке розсилання називається широкомовним noBiaoMaeHHaM(broadcast).

При адресації необхідно враховувати ті обмеження, які вносяться особливим призначенням деяких IP-адрес. Так, ні номер мережі, ні номер вузла не може складатися тільки з одних двійкових одиниць або тільки з одних двійкових нулів. Звідси треба, що максимальна кількість вузлів, наведена в таблиці для мереж кожного класу, на практиці повинна бути зменшена на 2. Наприклад, у мережах класу С під номер вузла відводиться 8 біт, які дозволяють задавати 256 номерів: від 0 до 255. Однак на практиці максимальне число вузлів у мережі класу С не може перевищувати 254, тому що адреси 0 й 255 мають спеціальне призначення.

Використання масок в IP-адресації - безкласова адресація

Традиційна схема ділення IP-адреси на номер мережі й номер вузла засновано на понятті класу, що визначається значеннями декількох перших біт адреси. Саме тому, що перший байт адреси 185.23.44.206 потрапляє в діапазон 128-191, ми можемо сказати, що ця адреса відноситься до класу В, а значить, номером мережі є перші два байти, доповнені двома нульовими байтами - 185.23.0. 0, а номером вузла - 0.0.44.206.

А що якщо використати яку-небудь іншу ознаку, за допомогою якого можна було б більш гнучко встановлювати границю між номером мережі й номером вузла? Як такі ознаки зараз одержали широке поширення маски. Маска — це число, що використовується в парі з IP-адресою; двійковий запис маски містить одиниці в тих розрядах, які повинні в IP-адресі інтерпретуватися як номер мережі. Оскільки номер мережі є цільною частиною адреси, одиниці в масці також

повинні становити безперервну послідовність. Для стандартних класів мереж маски мають наступні значення:

клас А - 11111111. 00000000. 00000000. 00000000 (255.0.0.0);

клас В - 11111111. 11111111. 00000000. 00000000 (255.255.0.0);

клас С- 11111111.11111111.11111111.00000000(255.255.255.0).

Для запису масок використовуються й інші формати, наприклад, зручно інтерпретувати значення маски, записаної в шістнадцятковому коді: FF.FF.00.00 - маска для адрес класу В. Часто зустрічається й таке позначення 185.23.44.206/16 - цей запис говорить про те, що маска для цієї адреси містить 16 одиниць або що в указаній Ш-адресі під номер мережі відведено 16 двійкових розрядів.

Позначаючи кожну №-адресу маскою, можна відмовитися від понять класів адрес і зробити більш гнучкою систему адресації.

У масках кількість одиниць у послідовності, що визначає границю номера мережі, не обов'язково повинне бути кратним 8, щоб повторювати розподіл адреси на байти. Нехай, наприклад, для Ш-адреси 129.64.134.5 зазначено маску 255.255.128.0, тобто у двійковому виді:

IP-адреса 129.64.134.5 - 10000001. 01000000.10000110. 00000101

Маска 255.255.128.0- 11111111.11111111.10000000.00000000

Якщо ігнорувати маску, то відповідно до системи класів адреса 129.64.134.5 відноситься до класу В, а виходить, номером мережі є перші 2 байти - 129.64.0.0, а номером вузла - 0.0.134.5.

Якщо ж використовувати для визначення границі номера мережі маску, то 17 послідовних одиниць у масці, «накладені» на Ш-адресу, визначають як номер мережі у двійковому представленні число:

10000001. 01000000. 10000000. 00000000 або в десятковій формі запису - номер мережі 129.64.128.0, а номер вузла 0.0.6.5.

Механізм масок широко розповсюджений в IP-маршрутизації, причому маски можуть використовуватися для самих різних цілей. З їхньою допомогою адміністратор може структурувати свою мережу, не жадаючи від постачальника послуг додаткових номерів мереж. На основі цього ж механізму постачальники послуг можуть поєднувати адресні простори декількох мереж шляхом введення так званих «префіксів» з метою зменшення обсягу таблиць маршрутизації й підвищення за рахунок цього продуктивності маршрутизаторів.

Номера мереж призначаються або централізовано, якщо мережа є частиною Internet, або довільно, якщо мережа працює автономно. Номера вузлів й у тому й в іншому випадку адміністратор вільний призначати за своїм розсудом, не виходячи, зрозуміло, з дозволеного для цього класу мережі діапазону.

Уже порівняно давно спостерігається дефіцит IP-адрес. Дуже важко одержати адресу класу B и практично неможливо стати власником адреси класу A. При цьому слід відзначити, що дефіцит обумовлений не тільки ростом мереж, але й тим, що наявна безліч IP-адрес використовується нераціонально. Дуже часто власники мережі класу C витрачають лише невелику частину з наявних у них 254 адрес.

Якщо деяка IP-мережа створена для роботи в «автономному режимі», без зв'язку з Internet, тоді адміністратор цієї мережі вільний призначити їй довільно обраний номер. Але й у цій ситуації для того, щоб уникнути яких-небудь колізій, у стандартах Internet визначено кілька діапазонів адрес, що рекомендують для локального використання. Ці адреси не обробляються маршрутизаторами Internet ні при яких умовах. Адреси, зарезервовані для локальних потреб, обрані з різних класів: у класі A - це мережа 10.0.0.0, у класі B - це діапазон з 16 номерів мереж 172.16.0. 0 -172.31.0.0, у класі C - це діапазон з 255 мереж -192.168.0.0 - 192.168.255.0.

Для зм'якшення проблеми дефіциту адрес розробники стека TCP/IP пропонують різні підходи. Принциповим розв'язанням є перехід на нову версію IPv6, у якій різко розширюється адресний простір за рахунок використання 16-байтних адрес.

Інша технологія, що може бути використана для зняття дефіциту адрес, це трансляція адрес (Network Address Translator, NAT). Вузлам внутрішньої мережі адреси призначаються довільно (природно, відповідно до загальних правил, визначеними в стандарті), так, начебто ця мережа працює автономно. Внутрішня мережа з'єднується з Internet через деякий проміжний пристрій (маршрутизатор, міжмережевий екран). Цей проміжний пристрій отримує у своє розпорядження деяку кількість зовнішніх «нормальних» IP-адрес, погоджених з постачальником послуг або іншою організацією, що розподіляє IP-адреси. Проміжний пристрій здатний перетворювати внутрішні адреси в зовнішні, використовуючи для цього якісь таблиці відповідності. Для зовнішніх користувачів всі численні вузли внутрішньої мережі виступають під декількома зовнішніми IP-адресами. При одержанні зовнішнього запиту цей пристрій аналізує його вміст і при необхідності пересилає його у внутрішню мережу, заміняючи IP-адресу на внутрішню адресу цього вузла.

8иреггпеШ^

Зиреггпей^ - це практика використання бітової маски для групування декількох класових мереж в виді одного мережевого адресу. Биретей^ та його узагальнення маршрутів є різні імена одного процесу. Проте термін 8иреггпей^ частіше застосовується, коли агреговані мережі знаходяться під загальним адміністративним управлінням. Зиреггпеїї^ бере біти з мережевої порції маски, а виЬпеШ^ бере біти з порції маски, що відноситься до хосту. ЗиретеШ^ та його узагальнення маршрутів є інверсним поняттям по відношенню до 8иЬпеїї^.

Оскільки мережі класів А і В практично вичерпані, то організації змушені запитувати у провайдерів кілька мереж класу С. Якщо компанія отримує блок безперервних адрес в мережах класу С, то можна використовувати 8иреггпей^ і всі адреси в компанії будуть лежати в одній більшій мережі або «над мережі». Розглянемо компанію Компаніяі, якій потрібно адреси для 400 хостів. При класової адресації компанія повинна запитати у центральній інтернет служби ІпїегМС мережу класу В. Якщо компанія отримає таку мережу, то десятки тисяч адрес в ній не будуть використовуватися. Альтернативою є отримання двох мереж класу С, що дає 254 * 2 = 504 адреси для хостів. Недолік цього підходу полягає в необхідності підтримки маршрутизації для двох мереж.

При безкласовій адресній системі 8иреггпей^ дозволяє компанії Компанія 1 отримати необхідний адресний простір з мінімальною кількістю не використовуваних адрес і без збільшення розміру таблиць маршрутизації. Використовуючи CIDR, Компанія 1 запитує блок адрес у свого Інтернет провайдера, а не у центральної Інтернет служби ШегМС. Провайдер визначає потреби Компанії 1 і виділяє адресний простір зі свого адресного простору. Провайдер бере на себе управління адресним простором у своїй внутрішній безклассовой системі. Всі зовнішні Інтернет маршрутизатори містять тільки сумарні маршрути до мережі провайдера. Провайдер сам підтримує маршрути, більш специфічні для своїх клієнтів, включаючи Компанію 1. Цей підхід суттєво зменшує розміри таблиць маршрутів для всіх маршрутизаторів в Інтернеті.

Нехай Компанія 1 отримала у провайдера дві мережі класу С, адреси в яких неперервні: 207.21.54.0 і 207.21.55.0.

Таблиця 1

207.21.54.0	110001111	00010101	00110110	00000000
207.21.55.0	110001111	00010101	00110111	00000000

З таблиці видно, що адреси мають загальний 23-бітовий префікс 11001111 00010101 0011011. Доповнюючи префікс праворуч нулями 11001111 00010101 00110110 00000000, отримаємо надсеть з 23 - бітовою маскою, 207.21.54.0/23.

Провайдер представляє мережу компанії зовнішньому світу як мережу 207.21.54.0/23.

CIDR дозволяє провайдерам ефективно розподіляти і підсумовувати безперервні простори IP адрес.

VLSM

Маска змінної довжини (Variable-Length Subnet Mask (VLSM)) дозволяє організації використовувати більше однієї маски підмережі всередині одного і того ж мережевого адресного простору. Реалізацію VLSM часто називають «підмережі на підмережі».

Розглянемо підмережі, створені шляхом запозичення трьох перших біт в хостової порції адреси класу С 207.21.24.0.

Таблиця 2

Підмережа	Адреса підмережі
0	207.21.24.0/27
1	207.21.24.32/27
2	207.21.24.64/27
3	207.21.24.96/27
4	207.21.24.128/27
5	207.21.24.160/27
6	207.21.24.192/27
7	207.21.24.224/27

Ми отримали вісім підмереж, кожна з який може містити не більше 30 хостів. Кожне з'єднання через послідовний інтерфейс вимагає для себе дві адреси і окремої підмережі. Використання для цього будь-якої з підмереж / 27 призведе до втрати адрес. Для створення підмережі з двох адрес найкраще підходить 30-ти бітова маска. Це якраз те, що треба для послідовного з'єднання.

Розіб'ємо одну з підмереж 207.21.24.192/27 на вісім підмереж, використовуючи 30-ти бітову маску.

Таблиця 3

0	207.21.24.192/30
1	207.21.24.196/30
2	207.21.24.200/30
3	207.21.24.204/30
4	207.21.24.208/30
5	207.21.24.212/30
6	207.21.24.220/30
7	207.21.24.224/30

Тобто кожну з решти семи підмереж / 27 можна використовувати для адресації хостів у семи локальних мережах. Ці локальні мережі можна зв'язати в глобальну мережу за допомогою не більше ніж восьми послідовних з'єднань з наших восьми мереж.

Щоб у мережах з VLSM правильно здійснювалася маршрутизація маршрутизатори повинні обмінюватися інформацією про маски в підмережах.

Використання CIDR і VLSM не тільки запобігає порожній витраті адрес, але і сприяє агрегації маршрутів або підсумовування. Без підсумовування маршрутів Інтернет перестав би розвиватися вже в кінці 90-х років. Малюнок ілюструє як підсумовування скорочує навантаження на маршрутизатори.

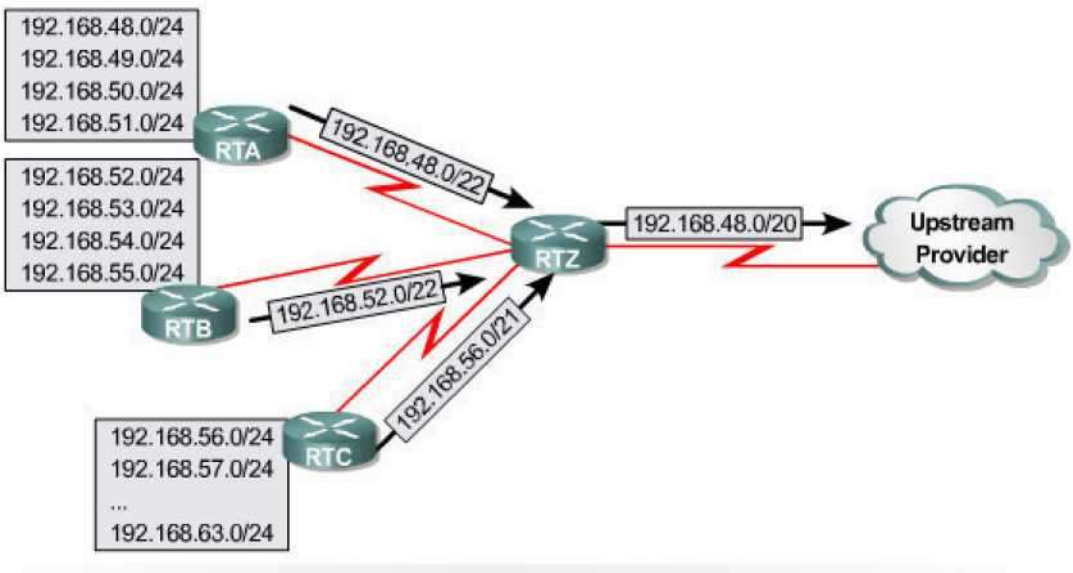


Рис2

Ця складна ієрархія мереж і підмереж підсумовується в різних точках так, що вся мережа в цілому виглядає ззовні як 192.168.48.0/20. Для правильної роботи підсумовування маршрутів слід ретельно підходити до призначення адрес: підсумовувані адреси повинні мати однакові префікси.

Практична частина

Виконуємо конфігурування VLSM і протестуємо функціонування мережі на Рис.3 з використанням статичної маршрутизації.

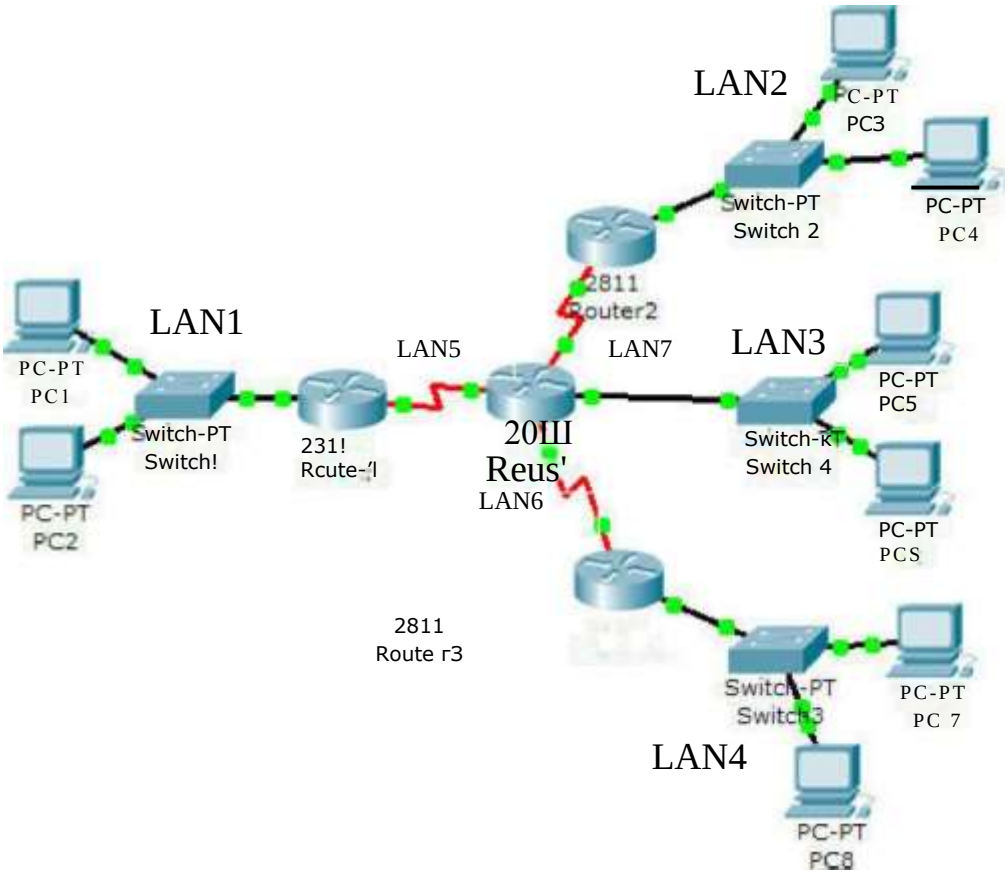


Рис 3 - Топологія мережі

Розглянемо мережу класу С 192.168.15.0/24 . Потрібно виділити потрібну кількість №- адресів відповідно до Таб 1 і зарезервувати максимальну кількість адресів для подальшого розвитку.

Таблиця 4

Назва мережі	Кількість вузлів
ЬЛШ	58
ЬЛШ	26
ЬДШ	10
ЬЛШ	10
ЬЛН5,6,7	2(кожне з’єднання)

Стандартний поділ на підмережі не буде ефективним, так як велика частина адресного простору буде простоювати, як показано в Таблиці 2

Таблиця 5

Мережа	Кількість необхідних хостів	Кількість адрес, що не використовуються при стандартному поділі на підмережі
ЬЛШ	58	4
ЬЛШ	26	36
ЬДШ	10	52
ЬЛШ	10	52
ЬЛН5,6,7	2(кожне з’єднання)	60

Для оптимізації адресного простору використаємо УЬБМ.

В першу чергу потрібно запланувати адресну схему мережі виду:

Таблиця 6

Необхідна кількість адрес	Адрес мережі	Діапазон адрес	Адреса широкомовного запиту	Мережа/префікс

Далі обчислюємо префікс для мережі з найбільшою кількістю хостів (ЬЛШ). Для адресації 58 вузлів потрібно мінімум 6 біт в порції номера вузла адреси 192.168.1.0/24., тобто префікс для даної підмережі буде мати вигляд /26.

Слідуючий крок, обчислюємо маску для слідкуючої підмережі з найбільшою кількістю вузлів ЬЛШ. Для адресації 26 вузлів достатньо 5 біт і префікс адреса мережі буде мати вигляд /27.

Таким чином формуємо адресну схему і зводимо у таблицю:

Таблиця 7

Необхідна кількість адрес	Адрес мережі	Діапазон адрес	Адреса широкомовного запиту	Мережа/префікс
LAN1	192.168.15.0	.1-.62	.63	192.168.15.0/26
LAN2	192.168.15.64	.65-.94	.95	192.168.15.64/27
LAN3				
LAN4				
LAN5				
LAN6				
LAN7				

Далі виконуємо слідуючі дії:

1. Будуємо мережу показану на Рис 3
2. Включаємо інтерфейси і провіряємо мережу командою show cdp neighbors
3. Призначити адреса інтерфейсів відповідно до таблиці. Провірити налаштування командою show ip interface brief.
4. На усіх маршрутизаторах налаштувати статичну маршрутизацію.
5. Перевірити налаштування, переглянувши таблиці маршрутизації роутерів(зробити скріншоти).

Контрольні запитання

1. Навіщо потрібна маска?
2. Що таке CIDR?
3. Що таке VLSM?
4. Як при використанні класів IP адрес в IP адресу виділяють адресу хоста і адреса підмережі?
5. Як без використання класів IP адрес в IP адресу виділяють адресу хоста і адреса підмережі?
6. Чому дорівнює число доступних адрес в підмережі?
7. По заданому викладачем числа хостів у підмережі визначте мінімальну маску.
8. Які форми запису маски ви знаєте?
9. Чому послідовне з'єднання виділяють в окрему підмережу?
10. Яку маску рекомендують використовувати для мережі послідовного з'єднання і чому?
11. Як CIDR і VLSM сприяють економному використанню адресного

простору?

12. Що таке Supemetting?

13. Що таке агрегація маршрутів і як вона сприяє зменшенню таблиць маршрутів на маршрутизаторах?

Порядок виконання та здачі роботи

1. Вивчити теоретичну і практичну частину.

2.Здати викладачеві теорію роботи шляхом відповіді на контрольні запитання.

3. Виконати в Packet Tracer практичну частину.

4. Виконайте в Packet Tracer завдання для самостійної роботи

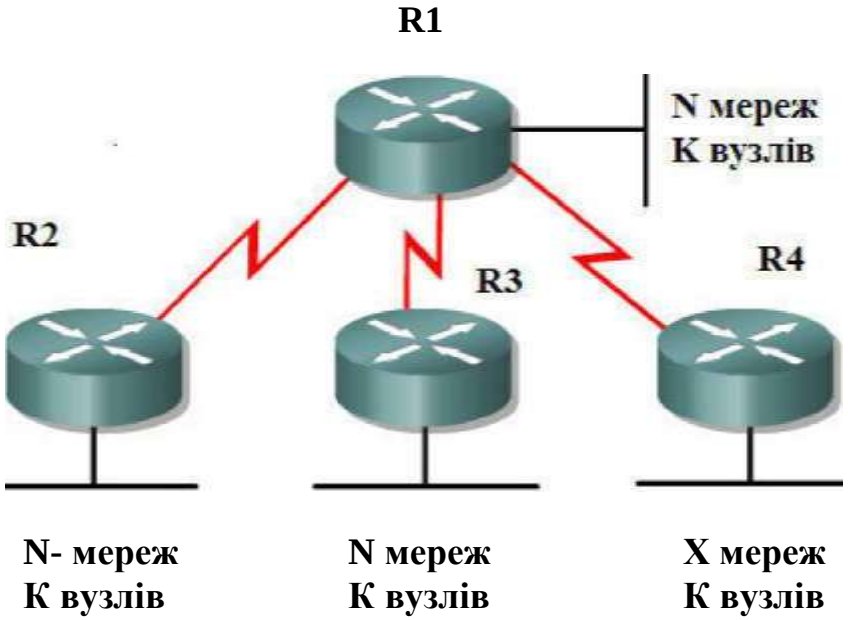
5. Пред'явіть викладачеві результат виконання пункту 9 завдання для самостійної роботи.

б.Оформіть звіт. Зміст звіту дивися нижче.

7.Захистіть звіт.

Завдання для самостійної роботи

Спроектуйте наступні мережі, відповідно до отриманого варіанту*. Див. рис.



Таблиця 8

Варіант	Адреса мережі	R1 (мережа- к-сть вузлів)	R2 (мережа- к-сть вузлів)	R3(мережа- к-сть вузлів)	R4 (мережа- к-сть вузлів)
1	192.168.10.0/24	Імережа - 28	1 мережа - 12	Імережа - 60	1 мережа - 12
2	192.168.5.0/24	Імережа - 20	Імережа - 100 2 мережа -55	Імережа -30	Імережа - 10
3	192.168.20.0/22	Імережа - 60	Імережа - 350	Імережа -200	Імережа - 40
4	192.168.20.0/23	Імережа - 45	Імережа - 150 2 мережа - 45	Імережа - 70	Імережа - 10 2мережа - 60
5	172.16.10.0/23	Імережа - 25 2мережа - 45	Імережа - 185	Імережа - 31 Імережа -22	Імережа - 64
6	192.168.20.0/22	Імережа - 80 2мережа - 60	Імережа - 250 2мережа - 120	Імережа - 90	Імережа - 120 2мережа - 45
7	172.16.10.0/24	Імережа - 25	Імережа - 22 2мережа - 12	Імережа - 48	Імережа - 50 2мережа - 12
8	172.16.10.0/23	Імережа - 75 2мережа - 12	Імережа - 120	Імережа - 55 2мережа - 40	Імережа - 31
9	192.168.11.0/22	Імережа - 70	Імережа - 75 2мережа - 140	Імережа - 12	Імережа - 250 2мережа - 60
10	192.168.1.0/24	Імережа - 25 2мережа - 16	Імережа - 75	Імережа - 22	Імережа - 30

*Варіант по списку у підгрупі

Порядок вирішення варіанту

1. У дизайнера правильно підберіть маршрутизатори з потрібним числом і типом інтерфейсів. Використовуйте многослотові пристрої, що мають можливість нарощувати число інтерфейсів.

2. Створіть топологію. Локальна мережа, представляється у вигляді комутатора з одним комп'ютером

Зробіть скріншот топології.

3. Призначте кожної підмережі правильну маску з мінімальним числом нулів. Пам'ятайте, що маска для послідовного з'єднання дорівнює / 30.

4. Визначтеся, які адреси ви будете призначати на мережеві інтерфейси маршрутизаторів і комп'ютерів.

5. У симуляторі призначте адреси на мережеві інтерфейси маршрутизаторів і комп'ютерів.

6. Перевірте правильність призначення адрес командами show ip interface brief (маршрутизатор) або ipconfig (комп'ютер).

7. Налаштуйте на кожному маршрутизаторі статичну маршрутизацію.

8. На кожному маршрутизаторі виведіть таблицю маршрутизації і зробіть скріншот.

9. Ви повинні пінгувати з будь-якого комп'ютера будь-який інший комп'ютер.

Зміст звіту

Звіт готується в електронному вигляді і роздруковується. Звіт містить:

1. Скріншот топології, створеної при виконанні практичної частини.

2. Скріншот топології вашого варіанта з адресами і масками. Скріншот схеми адресації

Тема№3: Глобальні комп'ютерні мережі

Лабораторне заняття 6: Frame relay

Навчальна мета заняття: - Освоїти основні методи побудови корпоративної мережі

Час: 4 год.

Місце проведення: комп'ютерний клас Навчальні питання:

1. **Настройка конфігурації Frame relay і статичного роутингу на роутері R1**
   - **1.1. Повірка стандартної конфігурації**
   - **1.2. Настройка фізичного інтерфейсу Frame relay на R1**
   - **1.3. Настройка під-інтерфейсів на R1**
   - **1.4. Налаштування статичної маршрутизації на R1 для зв'язку з кожним із роутерів**
   - **1.5. Налаштування Frame relay і маршрутизації за замовчуванням на Spoke-роутерах**
2. **Налаштування Cloud -pt (інтерпретація магістральної мережі)**
3. **Перевірка зв'язків**
4. **Провірка зв'язку із Spoke-LANs**

Література:

1. Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.
2. Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.

Методичне та матеріально-технічне забезпечення занять:

Персональний комп'ютер, включений в мережу IP, Microsoft Windows.

Хід проведення заняття:

I. Порядок проведення вступу до заняття.

Вступ

Обговорювання теоретичного матеріалу:

II. Порядок проведення основної частини заняття.

Лабораторна робота N6

TeMa.Frame ralay

Теоретична частина

Існують три типи послідовних каналів зв'язку:

1. Мережі з комутацією каналів: комутована телефонна мережа, ISDN.
2. Виділені або орендовані канали: DSL, кабельні модеми та канали зв'язку типу 64к, T1, T3, OC-12,
3. Мережі з комутацією пакетів: Frame Relay, X.25 і ATM.

Передача даних може здійснюватися як синхронно, так і асинхронно. Орендовані виділені канали зазвичай вимагають синхронного послідовного з'єднання.

Кожна лінія зв'язку з'єднана з послідовний портом маршрутизатора пристроєм CSU / DSU (channel service unit / data service unit - пристрій обслуговування каналу / пристрій обслуговування даних).

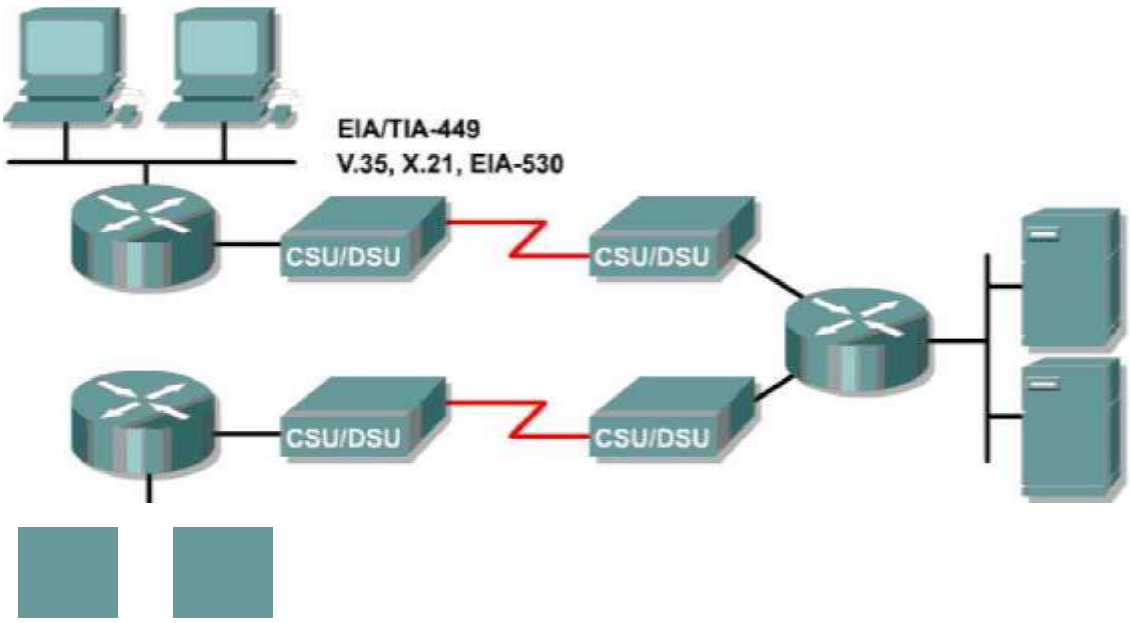


Рисунок 1

Отже, окрім власне проводів від комунікаційного провайдера, кожному з'єднанню потрібен окремий синхронний послідовний порт на маршрутизаторі і пристрій CSU / DSU. Як результат, вартість утримання декількох виділених ліній різко зростає. Тому більшість компаній знаходять побудова повно зв’язних WAN на виділених лініях занадто дорогим рішенням.

CSU / DSU є DCE (data communications equipment - обладнання передачі даних) пристроєм. DCE адаптує фізичний інтерфейс на DTE (data terminal equipment - термінальне обладнання даних) пристрої до правил передачі сигналів в несучій мережі. Прикладом DTE пристрою є маршрутизатор.

CSU / DSU забезпечує модуляцію, тимчасову синхронізацію і використовується для взаємодії з цифровою передавальної апаратурою. Важливо, що CSU / DSU використовується маршрутизатором для зв'язку з цифровим каналом таким же чином, як ПК використовує модем для зв'язку з аналоговим телефонним каналом. Тобто в зв'язці ПК-модем ПК є DTE пристроєм, а модем - DCE пристроєм.

Виділені або орендовані канали

Зазвичай послідовні з'єднання в мережах оперують з наступними швидкостями

56 kbps

64 kbps

T1 (1.544 Mbps) стандарт США

El (2.048 Mbps) європейський стандарт

E3 (34.064 Mbps) європейський стандарт

T3 (44.736 Mbps) стандарт США

DTE (маршрутизатор) пов'язаний з DCE (CSU / DSU) через синхронний послідовний порт з використанням одного з таких стандартів: EIA/TIA-232 (RS-232), EIA/TIA-449, V.35, X.21, EIA- 530.

Для з'єднання DTE (маршрутизатор, ПК) до аналогового модему (DCE (CSU / DSU)) використовується EIA/TIA-232. Випущений більше 30 років тому, він став класикою. Однак він не прийнятний на виділених лініях для швидкостей більше ніж 120 kbps.

Стандарт V.35 придатний для більш високих швидкостей (більше 2 Mbps). Він використовуються для приєднання порту маршрутизатора до T1/E1 через окреме CSU / DSU.

Сьогодні для багатьох послідовних каналів зв'язку, таких як T1, багато маршрутизаторів містять усередині себе CSU / DSU, інтегровану в інтерфейсну карту. Тобто, немає потреби в окремому DCE (CSU / DSU).

Мережі з комутацією пакетів МКП.

На відміну від орендованих ліній і з'єднань з перемиканням каналів, перемикання пакетів не покладається на виділене, точка-точка з'єднання через несучу мережу. Замість цього пакети даних маршрутизуються в несучій мережі на підставі адресації, що міститься в заголовках пакетів або фреймів.

що дозволяє провайдеру підтримувати багато споживачів на одних фізичних лініях і комутаторах.

У мережах з комутацією пакетів провайдер конфігурує свою апаратуру комутації для створення віртуальних ланцюгів (virtual circuits (VCs)) для забезпечення наскрізного зв'язку. Віртуальні ланцюги можуть бути постійними або можуть бути побудовані на вимогу. Frame Relay є типовий службою з комутації пакетів в WAN. Часто використовуються також технології ATM та X.25.

Перші МКП будувалися за протоколом X.25. Так як X.25 був спроектований для роботи на ненадійних телефонних мідних провідниках, то він забезпечує виявлення помилок

МКП це мережі з множинним доступом, що використовують спеціальне обладнання для доставки користувацького трафіку. Фізичним носієм сигналів усередині МКП є, як правило, високошвидкісні виділені канали зв'язку, найчастіше оптичні. Для забезпечення необхідного наскрізного з'єднання всередині МКП здійснюється настройка комутаційного обладнання.

МКП пропонують адміністратору мережі менший контроль, ніж з'єднання точка-точка. Проте, вартість віртуальної ланцюга в МКП менше, ніж виділеної лінії. Доступ до самої МКП, як правило, здійснюється через синхронний послідовний порт маршрутизатора за єдиною виділеної лінії T1 або T3 і дозволяє з'єднається з багатьма віддаленими сайтами. При відсутності МКП потрібна окрема виділена лінія до кожного віддаленого сайту.

Віртуальні ланцюги Frame Relay надають швидкість аж до T3, роблячи технологію перемикання пакетів високошвидкісною, ефективною, за вартістю альтернативою виділеним лініям. Єдине синхронне послідовне з'єднання до МКП може підтримувати декілька віртуальних ланцюгів в конфігураціях точка-багато точок (один-до-багатьох) і точка-точка (Рис. 2). Процес комбінування кількох передач даних в одній фізичній лінії

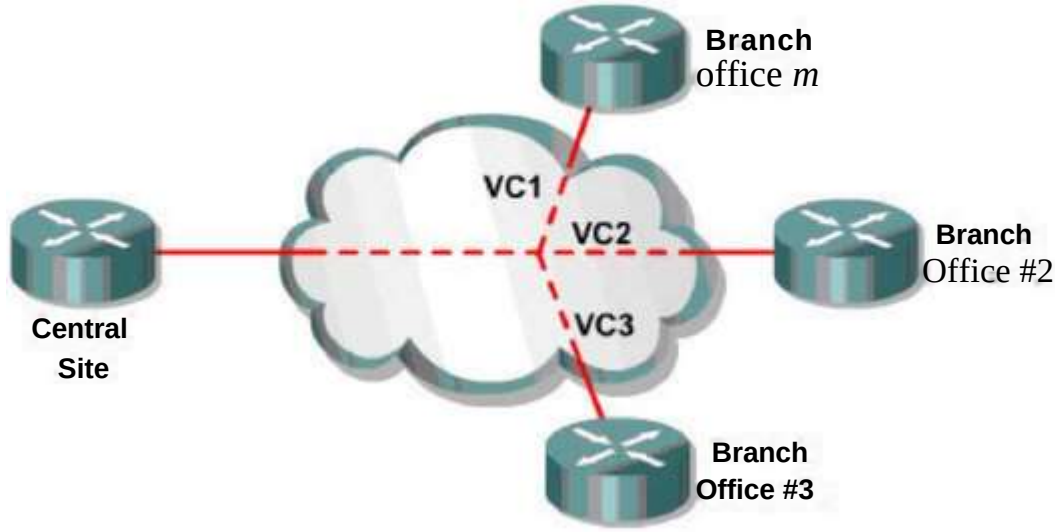


Рисунок 2

Мультиплексування стає можливим завдяки тому, що DTE (як правило маршрутизатор) інкапсулює дані в пакети МКП, що містять адреси МКП. Комутатори провайдера використовують ці адреси для визначення, як і куди доставити окремий пакет. У разі Frame Relay ці адреси називаються DLCI (Data Link Connection Identifiers). Здатність до мультиплексуванню означає, що один порт маршрутизатора разом з одним пристроєм CSU / DSU може підтримувати десятки віртуальних ланцюгів, кожна з яких веде до окремого сайту. Отже, перемикання пакетів робить доступною за ціною навіть створення повно-топології.

Frame Relay не виправляє помилок і добре пристосований для роботи на високонадійних цифрових каналах передачі.

Frame Relay не забезпечує той ступінь надійності, гнучкості та безпеки, яку надають виділені лінії, що є кращими для критично важливого трафіку та обміну великим обсягом інформації.

Іншою популярною технологією комутації пакетів є ATM (Asynchronous Transfer Mode). ATM це міжнародний стандарт для поелементної передачі, в якому інформація різних типів таких, як дані, голос і відео поміщаються в комірку фіксованої довжини в 53 байти. Фіксована довжина комірок дозволяє вести їх обробку апаратним способом, що скорочує тимчасові затримки. ATM спроектована так щоб скористатися перевагами високошвидкісних середовищ передачі E3, T3 і SONET.

Протоколи глобальних мереж

Маршрутизатори перш ніж передати IP пакети по каналу зв'язку, інкапсулюють їх у фрейми другого мережевого рівня.

Типові протоколи другого рівня глобальних мереж:

Point-to-Point Protocol (PPP) - протокол зв’язку маршрутизатор - маршрутизатор і маршрутизатор-хост для синхронних і асинхронних каналів.

Serial Line Internet Protocol (SLIP) - попередник PPP, використовуваний для послідовного з'єднання точка-точка по протоколу TCP / IP.

High-Level Data Link Control (HDLC) - є власністю Cisco і використовується для з'єднання двох пристроїв Cisco.

X.25/LAPB - це стандарт, який визначає спосіб з'єднання між DTE і DCE пристроями при віддаленому термінальному доступі і комп'ютерних комунікаціях в публічних мережах даних.

Frame Relay - високопродуктивний протокол, який використовується на багатьох мережевих інтерфейсах

Рисунок 3 показує, які протоколи зв'язку даних використовуються в кожній з трьох типів з'єднань у WAN

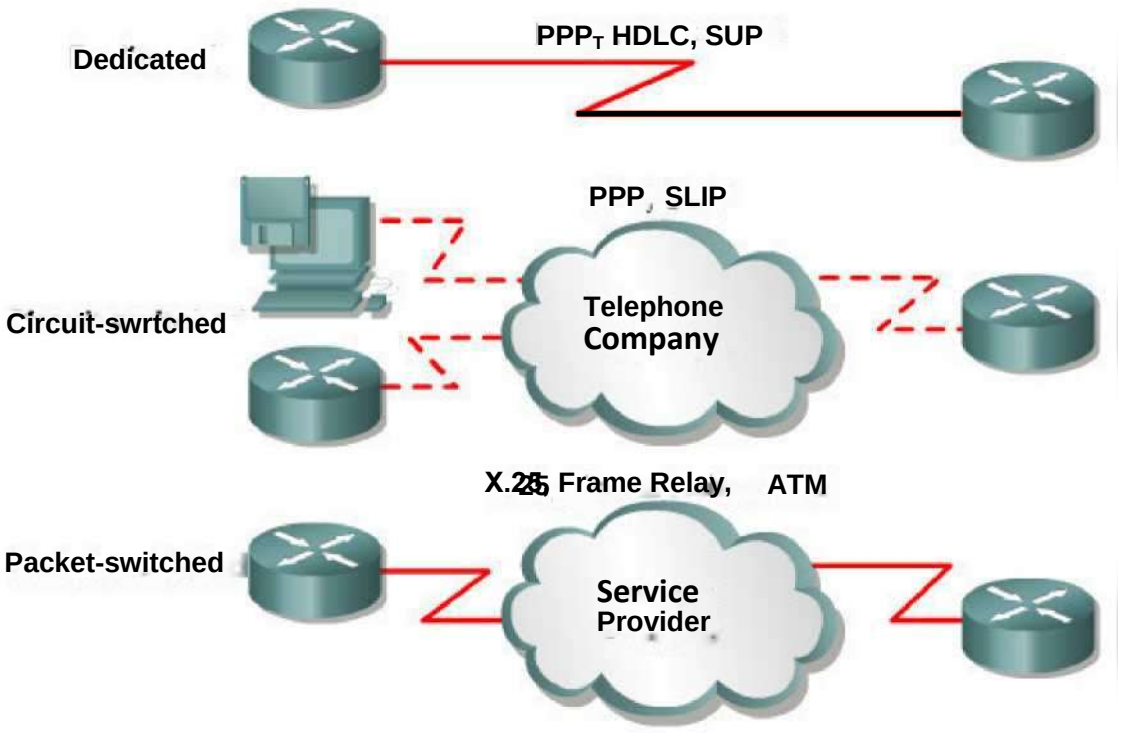


Рисунок 3

Frame Relay

В даний час Frame Relay замінює X.25 як технологія перемикання пакетів.

Стандартизований в 1990, Frame Relay спрощує функції канального

рівня і забезпечують лише перевірку на помилки, але не їх виправлення. Такий не надлишковий підхід до комутації пакетів збільшує продуктивність і ефективність. Сучасні волоконнооптичні канали зв'язку і цифрові засоби обслуговування передачі забезпечують набагато менше помилок, ніж їх мідні попередники. З цієї причини, використання як в X.25 механізмів надійності на канальному рівні тепер взагалі розцінюється як непотрібне. Виправлення помилок здійснюється у протоколах більш високого рівня, наприклад TCP.

Frame Relay - ITU і ANSI стандарт. ITU-T - International Telecommunications Union (Міжнародний Союзу телезв'язку) та ANSI - American National Standards Institute (Американський Національний Інститут Стандартів). Стандарти визначають процес для передачі даних по мережі з комутацією пакетів. Frame Relay це орієнтована на з'єднання технологія зв'язку даних, яка оптимізована, щоб забезпечити високу швидкодію і ефективність.

Сучасні мережі телекомунікацій характеризуються відносно вільною від помилок цифровою передачею і високонадійної інфраструктурою. Frame Relay покладається майже повністю на протоколи верхнього рівня, щоб виявити і виправити помилки. Frame Relay не має механізмів повторної передачі, які використовуються в X.25. Без механізмів виправлення помилки Frame Relay виграє у X.25 за швидкістю. У результаті Frame Relay прийнятний для використання там, де потрібна висока продуктивність, як у локальних мережах. Фізична мережа, на якій розгорнуто Frame Relay, може бути або громадською або приватною мережею і мати різну фізичну природу: оптика, супутникові канали зв'язку, виділені лінії.

Frame Relay визначає процес взаємозв'язку між DTE клієнта, типу маршрутизатор, і DCE провайдера. Як тільки трафік досягає комутатора провайдера, Frame Relay не визначає спосіб, за яким дані передаються в межах мережі Frame Relay. Тому, провайдер Frame Relay може використовувати різноманітні технологій, типу ATM чи PPP, щоб переміщати дані з одного кінця його мережі до іншого.

Пристрої Frame Relay

Пристрої, приєднані до глобальної мережі Frame Relay можуть бути або DTE або DCE пристроями. Пристрої DTE розглядаються як кінцеве обладнання і зазвичай розташовуються на території клієнтів - споживачів послуг Frame Relay. Прикладами DTE пристроїв є маршрутизатори і пристрої доступу FRAD (Frame Relay Access Devices). FRAD це спеціальний пристрій для зв'язку між LAN і Frame Relay.

Внутрішньомережеві пристрою DCE належать провайдера. Вони забезпечують синхронізацію і / або послуги комутації пакетів у мережі і забезпечують дійсну передачу даних в WAN.

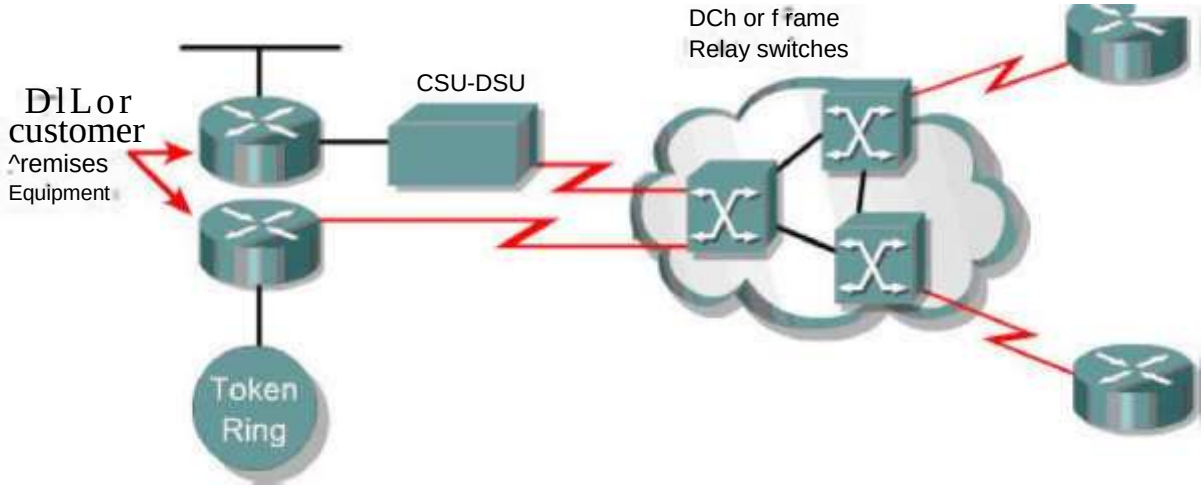


Рисунок 4

Мережа Frame Relay будується за допомогою комутаторів (switch) Frame Relay, що виступають у ролі DCE. Усередині мережі Frame Relay можуть використовуватися різні технології передачі даних, наприклад ATM. Фізичні канали зв'язку також не регламентуються - це може бути оптика, супутникові канали зв'язку, виділені лінії.

Не зважаючи на технологію всередині мережі Frame Relay, зв'язок між споживачем та провайдером Frame Relay здійснюється по протоколу Frame Relay.

Функціонування Frame Relay

Зазвичай, чим більше відстань покриває виділена лінія, тим дорожча послуга. Підтримка повнозвязного з'єднання віддалених сайтів за допомогою виділених ліній занадто накладна для багатьох організацій. З іншого боку мережі з комутацією пакетів надають спосіб мультиплексування декількох логічних передач даних по єдиному фізичному зв'язку. Єдине з'єднання до мережі з комутацією пакетів провайдера буде менш дорогим, ніж окремі виділені лінії між споживачем і кожним віддаленим сайтом. Мережі з комутацією пакетів використовують віртуальні ланцюги для доставки пакетів з кінця в кінець через поділювану інфраструктуру.

Служба у комутації пакетів, така як Frame Relay вимагає, щоб споживач підтримував тільки один канал, зазвичай T1, до центрального офісу (ЦО) провайдера. Frame Relay забезпечує величезну ефективність за вартістю, так як один кінцевий вузол може з'єднається з багатьма географічно віддаленими

вузлами, використовуючи єдину лінію T1 і один DCE (CSU / DSU) пристрій для підключення до локального ЦО.

Для комунікації між будь-якими двома вузлами провайдер послуг повинен встановити віртуальний канал між цими вузлами всередині мережі Frame Relay. Хоча оплата йде за кожну віртуальний канал, ця плата невелика. Це робить Frame Relay ідеальною технологією для створення повно-звязної топології.

Мережі Frame Relay підтримують як постійні віртуальні канали PVC (permanent virtual circuits) так і комутовані віртуальні канали SVC (switched virtual circuits). PVC - найбільш типові для Frame Relay. PVC є постійно встановленими сполуками, які використовуються, коли в мережі Frame Relay є постійний трафік між певними DTE пристроями.

SVC є тимчасовими з'єднаннями, які використовуються при наявності одиничного трафіку між DTE пристроями. Так як вони тимчасові, з'єднання SVC вимагає установки і завершення для кожного з'єднання. Більшість провайдерів підтримує тільки PVC.

Кожне з’єднання PVC і SVC ідентифікується за допомогою ідентифікатора каналу передачі даних (Data-Link Control Identifier, DLCI). DLCI схожий на телефонний номер. Різниця полягає в тому, що сфера його дії обмежується тільки локальною ділянкою мережі. Завдяки цьому різні маршрутизатори в мережі можуть повторно використовувати той самий DLCI, що дозволяє мережі підтримувати велику кількість віртуальних каналів. При отриманні фрейму комутатор аналізує ідентифікатор і доставляє фрейм на відповідний вихідний порт.

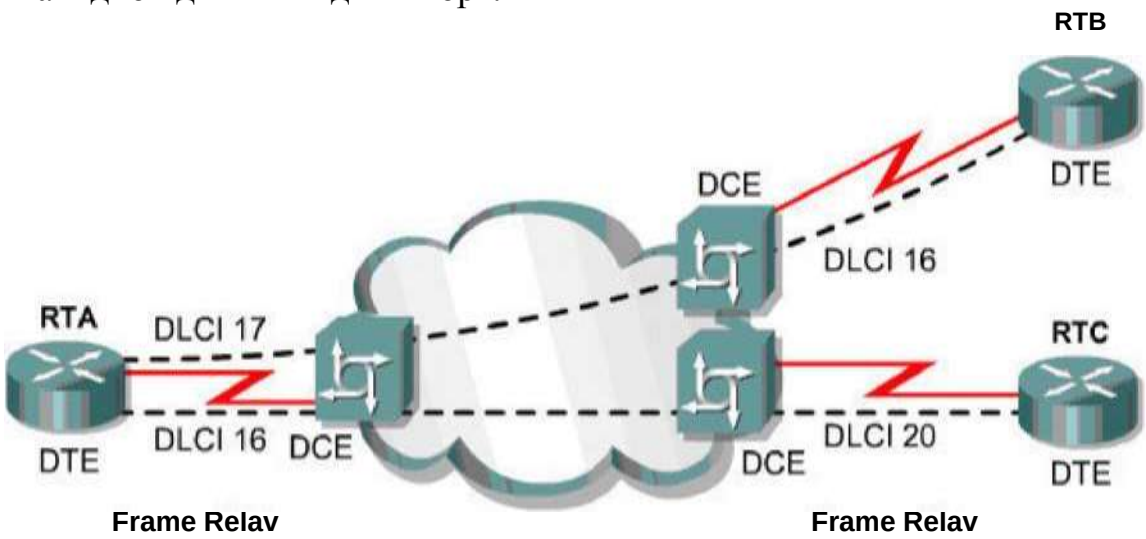


Рисунок 5

Два з'єднані віртуальним каналом пристрої DTE можуть використовувати різні значення DLCI для посилання на одне і теж з'єднання. На малюнку 5 PVC, що зв'язує маршрутизатори RTA і RTB, має DLCI рівне

17, призначений між RTA і безпосередньо з'єднаним комутатором. DLCI з номером 16 на RTB визначає той же PVC з'єднання між RTB і безпосередньо з'єднаним комутатором. Між тим, RTA використовує DLCI 16 для посилання на PVC, яке сполучається з RTC.

Для того, щоб маршрутизатор RTA знав, який PVC використовувати на третьому мережевому рівні, IP адреси повинні бути відображені у відповідності до номерів DLCI. Так на малюнку маршрутизатор RTA повинен відобразити адреси третього рівня в доступні DLCI.

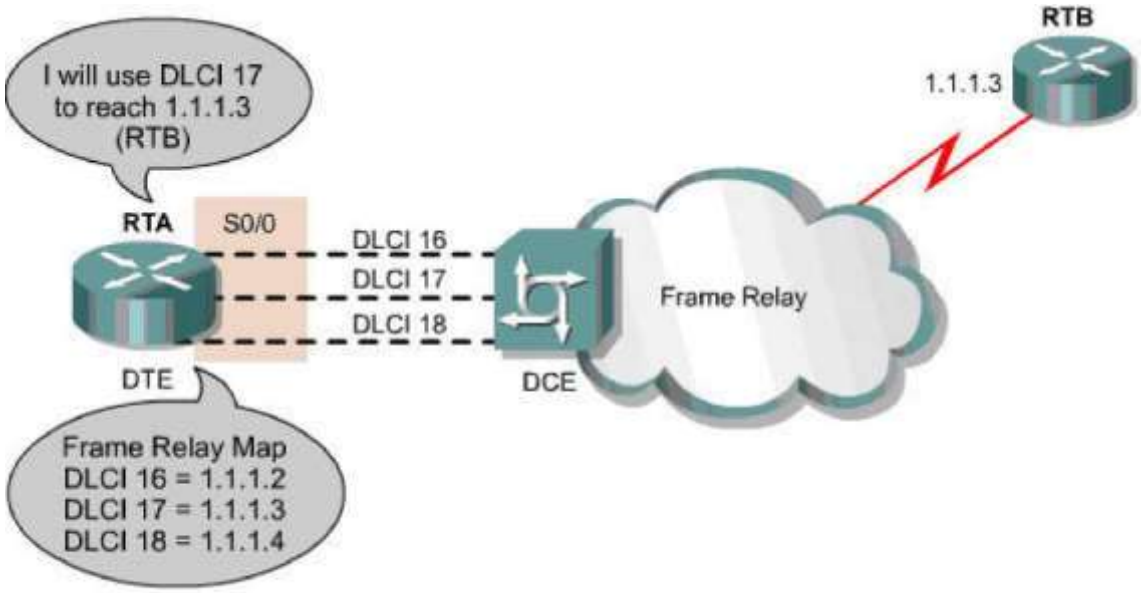


Рисунок 6

Наприклад, RTA відображає IP адресу 1.1.1.3 маршрутизатора RTB на DLCI 17. Оскільки RTA знає, який DLCI використовувати, то для досягнення одержувача слід інкапсулювати IP пакет у фрейм Frame Relay, що містить відповідний номер DLCI.

Включивши номер DLCI в заголовок Frame Relay, RTA може зв'язуватися як з RTB, так і з RTC по одній фізичній лінії. При такому статистичному мультиплексуванні смуга пропускання автоматично виділяється для активних каналів. Якщо RTA не має пакетів для посилки на RTB, то RTA може використовувати всю доступну смугу пропускання для зв'язку з RTC. При TDM (Time-division multiplexing) мультиплексуванні для кожного каналу, незалежно від наявності в каналі даних на передачу, виділяється певна смуга.

Для організації WAN провайдер послуг Frame Relay призначає своїм клієнтам номера DLCI. Зазвичай, DLCI від 0 до 15 і від 1008 до 1023 резервуються для спеціальних цілей. Клієнтам провайдер послуг призначає номери DLCI в діапазоні від 16 до 1007. Для широкомовлення можна

використовувати DLCI 1019 і 1020. Локальний інтерфейс управління Local Management Interface (LMI) використовує DLCI 1023 або 0. Деякі провайдери послуг Frame Relay можуть дозволити своїм клієнтам вибрати власні номери DLCI.

Для побудови відображення номерів DLCI в адреси третього рівня, маршрутизатор повинен спочатку знати, які VC доступні. Зазвичай процес визначення доступних VC і їх номерів DLCI здійснюється за стандартом LMI.

Як тільки маршрутизатору стали відомі номери DLCI для доступних VC, він повинен визначити які адреси третього рівня відображати на які номери DLCI. Відображення адрес може бути конфігуровано або в ручну або динамічно.

Frame Relay LMI

LMI це сигнальний стандарт між DTE пристроєм (маршрутизатором) і DCE пристроєм (комутатором Frame Relay). LMI відповідає за управління з'єднанням між пристроями, перевіряє, що дані передаються, періодично повідомляє про появу нових PVC та про знищення вже існуючих PVC.

Інверсний ARP

За допомогою прийнятних конфігураційних команд номер DLCI може бути вручну відображений на адресу третього рівня. У складних мережах побудова статичної відображення може потребувати великих зусиль, і таке відображення не пристосоване до зміни топології Frame Relay. За допомогою LMI комутатор Frame Relay може повідомити маршрутизатори про DLCI нового віртуального каналу. Це повідомлення не містить адресу 3 рівня. Станція, що отримала повідомлення буде знати про нове з'єднання, але не буде мати можливості адресувати дані одержувачу. Без нової конфігурації або механізму визначення адреси одержувача, новий віртуальний канал не може бути використаний.

Інверсний протокол визначення адреси (Inverse Address Resolution Protocol (Inverse ARP)) був розроблений для забезпечення механізму динамічного відображення DLCI на адресу третього рівня. Інверсний ARP працює багато в чому так як і ARP в LAN. Проте в ARP пристрій знає віддалений IP адрес і потребує визначення MAC адреси віддаленого пристрою. У Inverse ARP, маршрутизатор знає адресу 2 рівня, яким є DLCI, але потребує визначення віддаленої IP адреси.

Конфігурація інкапсуляції в Frame Relay

де protocol - appletalk, clns, decent, ip, xns, vines; dlci - номер DLCI; ietf | cisco - визначає тип інкапсуляції, за замовчуванням - cisco.

Опція broadcast - означає широкомовну передачу. Використовується при налаштуванні протоколів маршрутизації та дозволяє розглядати мережі з множинним доступом і без широкомовлення (якою і є Frame Relay) багато в чому таким же чином як і широкомовні мережі з множинним доступом (LAN). Наприклад

Router (config) # **interface Serial2 / 0**

Router (config-if) # **ip address 1.1.1.1 255.255.255.0**

Router (config-if) # **encapsulation frame-relay**

Router (config-if) # **frame-relay map ip 1.1.1.2 110 broadcast cisco**

Тут 1.1.1.1 локальний, а 1.1.1.2 віддалений IP адреса.

Якщо на послідовному інтерфейсі налаштовується інкапсуляція Cisco, то ця інкапсуляція застосовується до всіх VC на цьому інтерфейсі. Якщо на інтерфейсі взаємодіє обладнання Cisco і не Cisco, то слід вибірково задати інкапсуляцію IETF.

Перевірка конфігурації інтерфейсу Frame Relay

Після конфігурації Frame Relay слід перевірити, що з’єднання активні. Це здійснюється за допомогою декількох команд show:

Команда **show interfaces serial** показує інформацію про інкапсуляцію і статус протоколів першого і другого рівня, а також про широкомовний DLCI, про всі номери DLCI, що використовуються в послідовному інтерфейсі і про DLCI, що використовуються для LMI.

Команда **show frame-relay pvc** показує статус кожного налаштованого з'єднання і статистику трафіку. Команда показує статус усіх PVC, які налаштовані на маршрутизаторі.

Команда show **frame-relay map** показує елементи поточного відображення адрес та інформацію про з'єднання.

Команда **show frame-relay lmi** показує статистику трафіку LMI: число повідомлень про статус, якими обмінялися локальний маршрутизатор і комутатор Frame Relay.

Топології Frame Relay

Frame Relay дозволяє взаємодію віддалених вузлів мережі кількома способами(Рисунок 7)

Зірка, іноді називають hub and

spoke Повнозв'язна (Full mesh)

Частково пов'язана (Partial mesh)

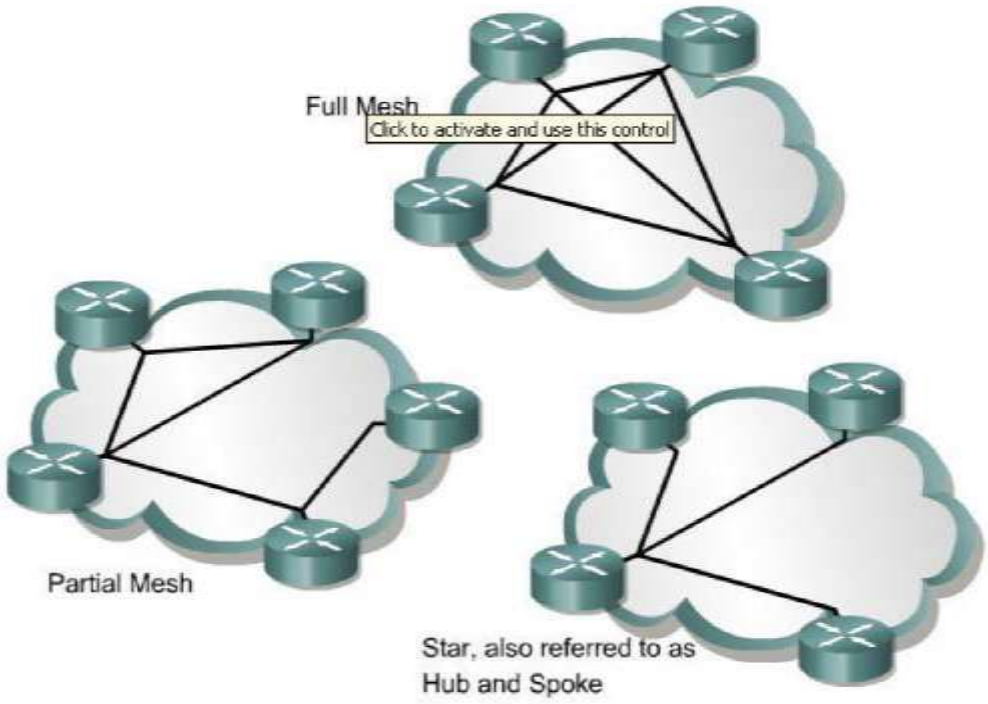


Рисунок 7

Топологія зірка найбільш популярна завдяки своїй вартісній ефективності. У цій топології віддалені вузли мережі під'єднуються до центрального вузла, який надає послуги та служби. Це найменш дорога топологія вимагає мінімального числа PVC. Зазвичай центральний маршрутизатор використовує один інтерфейс для зв'язку з багатьма PVC.

У повнозвязній топології всі маршрутизатори мають PVC до всіх маршрутизаторів. Топологія надлишкова, але надійна: якщо якесь з'єднання відключиться, маршрутизатори можуть змінити маршрут. З ростом числа вузлів вартість різко зростає.

У частково пов'язаної топології не всі вузли пов'язані безпосередньо. Наявність PVC між маршрутизаторами обумовлюється обсягом трафіку, архітектурою мережі або іншими міркуваннями.

Конфігурування підінтерфейсів для Frame Relay.

Підінтерфейси є логічний підрозділ фізичного інтерфейсу. За допомогою конфігурації підінтерфейсфв кожен PVC може бути настроєний як з'єднання точка-точка. Це дозволяє кожному підінтерфейсу діяти як орендована лінія. Це тому, що кожен підінтерфейс точка-точка розглядається як окремий фізичний інтерфейс.

У випадку з’єднання точка-точка використовується єдиний підінтерфейс для встановлення PVC з'єднання з іншим фізичним інтерфейсом або підінтерфейсом на віддаленому комп'ютері. У цьому випадку кожна пара

підінтерфейсів може перебувати в своїй власній підмережі і кожен підінтерфейс має єдиний DLCI.

Для конфігурації підінтерфейсів на фізичному інтерфейсі перш за все призначається інкапсуляція Frame Relay (cisco або ietf). Якщо фізичний інтерфейс вже має IP адресу, її треба видалити, так як кожен підінтерфейс має власну IP адресу. Якщо фізичний інтерфейс має адресу, то фрейми не будуть отримані локальними підінтерфейсами:

RTA (config) # **interface s2 / 0**

RTA (config-if) # **encapsulation frame-relay ietf**

Далі, слід налаштувати підінтерфейси, використовуючи наступні команди.

Router (config-if) # **interface serial number subinterface-number {multipoint | point-to-point}**

Наступна команда створює підінтерфейс 2 типу точка-точка на Serial 2 / 0:

RTA (config) # **interface serial s0/0.2 point-to-point**

Наступна команда створює підінтерфейс 5 типу multipoint на Serial 2 / 0:

RTA (config) # **interface serial s2/0.5 multipoint**

Зауважимо, що після введення цих команд операційна система IOS змінює рядок запрошення на config-subif, що означає режим конфігурації підінтерфейсу.

Номери підінтерфейсів можуть бути призначені в режимі конфігурації підінтерфейсу або в глобальному конфігураційному режимі в діапазоні від 1 до 4294967295. При конфігурації підінтерфейсу точка-точка, звичайною практикою є нумерувати підінтерфейси за значенням DLCI даного PVC.

Після створення підінтерфейсу слід задати IP адреса

RTA (config-subif) # **ip address 2.1.1.1 255.255.255.0**

Далі або конфігурується статичне відображення Frame Relay або використовується команда frame-relay interface-dlci для асоціації підінтерфейсу з DLCI. Ця команда потрібна для всіх підінтерфейсів точка-точка. Вона також потрібна для підінтерфейсів multipoint з дозволеним режимом інверсного ARP. Вона не вимагається для підінтерфейсів multipoint, які конфігуруються за допомогою статичних відображень маршрутів.

Один з комутаторів Frame Relay на малюнку 8 використовує LMI для інформування RTA, що доступні три активних PVC з DLCI номерами 18, 19 і 20

Коли RTA дізнається про DLCI 18, 19 і 20 на його інтерфейсі S0 / 0, роутер не знає який DLCI використовувати з яким підінтерфейсом. Це тому, що LMI не має способу повідомлення RTA про те, що DLCI 20 повинен бути

використаний з інтерфейсом S0/0.2, а не S0/0.1. Відтак кожен підінтерфейс повинен бути вручну асоційований з прийнятним номером DLCI.

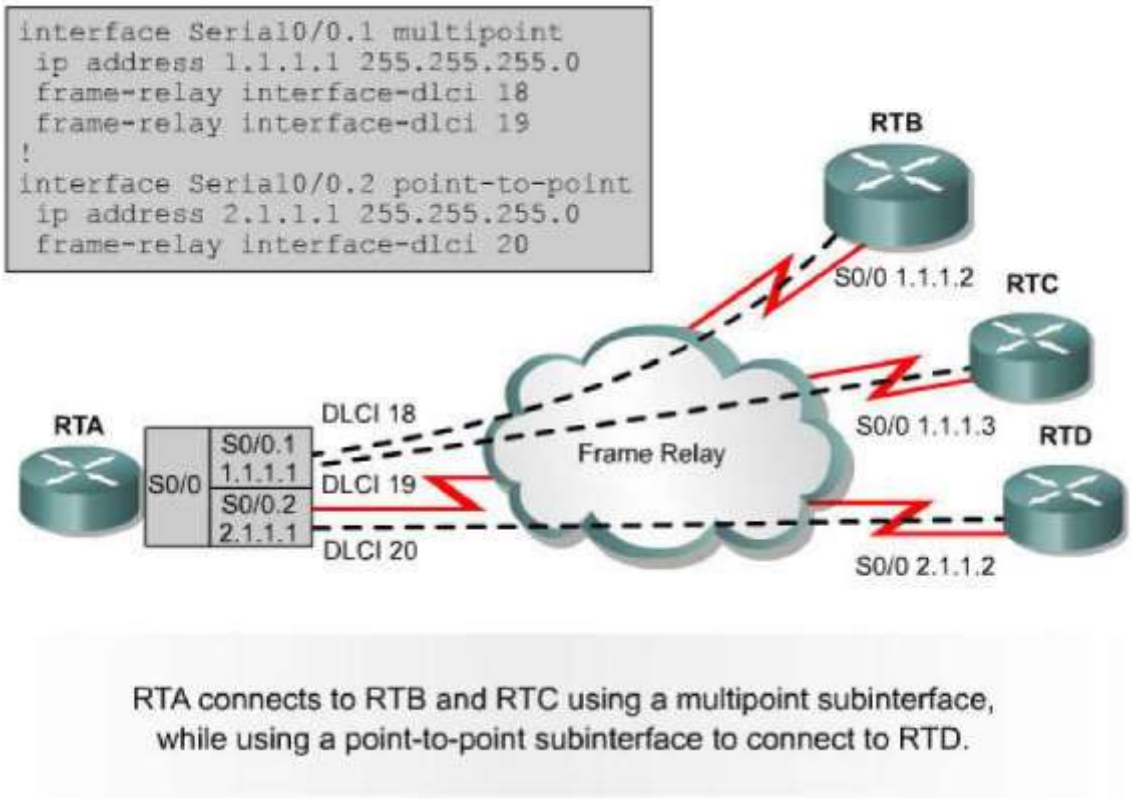


Рисунок 8

Режим multipoint підтримується симулятором не повністю і розглядатися не буде.

Практична частина

1 .В практичній роботі розглянемо невеликий фрагмент мережі з 4 роутерів, з використанням топології зірка (центральний роутер “hub-router”, до якого приєднуються інші роутери («Spoke router») через магістральну мережу (cloudO)) (Рисунок)

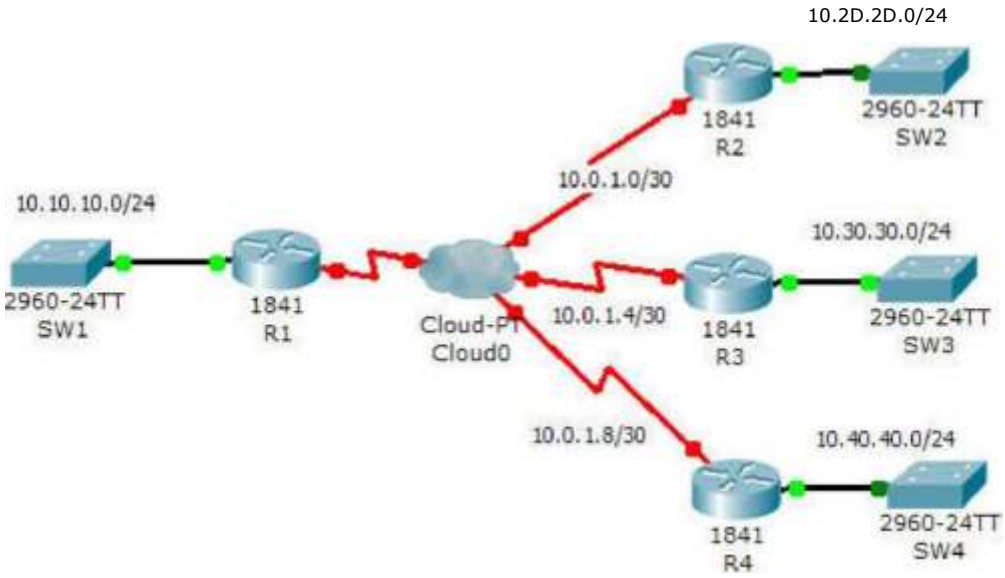


Рисунок 9

2.Настройка конфігурації Frame relay і статичного роутингу на роутері R1.

2.1 Повірка стандартної конфігурації

- виконати команду **show running-config** для повірки базових конфігурацій
- використовуючи команду **show ip route** можна проглянути таблицю маршрутизації

2.2 Настройка фізичного інтерфейсу Frame relay на R1

Для того щоб виконати конфігурацію під-інтерфейсів Frame relay, основний фізичний інтерфейс повинен бути доступним для звязку , тому проведем настройку Frame relay на інтерфейсі serial 0/0/0 роутера R1(«HUB router»). Frame relay LMI, буде настроєно автоматично

- З режиму розширеного виконання перейти в режим конфігурації
- Виконати сліуючі команди на R1 для настройки режиму Frame relay на фізичному інтерфейсі
- Rl(config)# **interface serial0/0/0**
- Rl(config-if)# **encapsulation frame-relay**
- Rl(config-if)# **no shutdown**

2.3 Настройка під-інтерфейсів на R1

Під-інтерфейси Frame relay будуть настроєні, використовуючи Frame relay point-to-point.

Виконати настройку з'єднання point-to-point до трьох роутерів через під-інтерфейси і назначити відповідні dlci номери для кожного з'єднання Frame relay відповідно до таблиці 1

Таблиця 1

S0/0/0.l02	IP: l0.0.l.l SM: 255.255.255.252	DLCI: l02
S0/0/0.l03	IP: l0.0.l.5 SM: 255.255.255.252	DLCI: l03
S0/0/0.l04	IP: l0.0.l.9 SM: 255.255.255.252	DLCI: l04

- Створити і настроїти під-інтерфейс s0/0/0.102. В режимі глобального конфігурування виконати слідуючі команди

Rl(config)# **interface Serial0/0/0.102 point-to-point** Rl(config-subif)# **ip address 10.0.1.1 255.255.255.252** Rl(config-subif)# **frame-relay interface-dlci 102**
Rl(config-subif)# **exit**

- повторити вище приведені налаштування для створення і настройки під-інтерфейсів s0/0/0.103 і s0/0/0.104

Rl(config)# **interface Serial0/0/0.103 point-to-point**
Rl(config-subif)# **ip address 10.0.1.5 255.255.255.252**
Rl(config-subif)# **frame-relay interface-dlci 103**
Rl(config-subif)# **exit**
Rl(config)# **interface Serial0/0/0.104 point-to-point**
Rl(config-subif)# **ip address 10.0.1.9 255.255.255.252**
Rl(config-subif)# **frame-relay interface-dlci 104**
Rl(config-subif)# **exit**

2.4 Налаштування статичної маршрутизації на Rl для зв'язку з кожним із роутерів

Маршрутизація може здійснюватись динамічно або статично. В даній роботі потрібно здійснити налаштування статичної маршрутизації для досягнення віддалених LAN.

- В режимі загальної конфігурації ввести такі статичні маршрути

Rl(config)# **ip route 10.20.20.0 255.255.255.0 10.0.1.2**

R1(config)# **ip route 10.30.30.0 255.255.255.0 10.0.1.6**
R1(config)# **ip route 10.40.40.0 255.255.255.0 10.0.1.10**

- Вийти з режиму конфігуруваня і виконати команду **show running-config и** для перегляду кінцевих налаштувань на **R1**

2.5 Налаштування Frame relay і маршрутизації за замовчуванням на Spoke- роутерах

Настройка Фізичного Інтерфейсу Frame relay на Spoke- роутерах В режимі загального конфігурування на R2 ввести наступні команди R2(config)# **interface serial0/0/0** R2(config-if)# **encapsulation frame-relay** R2(config-if)# **no shutdown**

Налаштування під-інтерфейсів на R2

В режимі загального конфігурування ввести наступні команди для створення і налаштування під-інтерфейсу. Назначити з'єднанню 101 DLCI номер. R2(config)# **interface Serial0/0/0.101 point-to-point** R2(config-subif)# **ip address 10.0.1.2 255.255.255.252** R2(config-subif)# **frame-relay interface-dlci 101** R2(config-subif)# **exit**

Налаштування маршрутизації за замовчуванням на R2

В режимі загального конфігурування вести слідуючі маршрути R2(config)# **ip route 0.0.0.0 0.0.0.0 10.0.1.1**

Повторити дані налаштування для роутерів 3 і 4

А) На роутері R3 виконати наступні команди
R3(config)# **interface serial0/0/0** R3(config-if)# **encapsulation frame-relay** R3(config-if)# **no shutdown**
R3(config)# **interface Serial0/0/0.101 point-to-point**
R3(config-subif)# **ip address 10.0.1.6 255.255.255.252**
R3(config-subif)# **frame-relay interface-dlci 101**
R3(config-subif)# **exit** R3(config)# **ip route 0.0.0.0 0.0.0.0 10.0.1.5**

Б) На роутері R4 виконати наступні команди
R4(config)# **interface serial0/0/0**
R4(config-if)# **encapsulation frame-relay**
R4(config-if)# **no shutdown**
R4(config)# **interface Serial0/0/0.101 point-to-point** R4(config-subif)# **ip address 10.0.1.10 255.255.255.252**

R4(config-subif)# frame-relay interface-dlci 101
R4(config-subif)# exit
R4(config)# ip route 0.0.0.0 0.0.0.0 10.0.1.9

3. Налаштування Cloud -pt (інтерпретація магістральної

На вкладці Config провести налаштування serial інтерфейсів у відповідності до того,які віртуальні канали через них проходять. Тобто слід вказати:

на вкладці Frame relay взаємозв'язки віртуальних

каналів Frame Relay

SerialO	SOtüSl	<- >	SerialO	* SOtoSI
Port	Sublink		Port	Sublink

From Port	Sublink	To Port	Sublink
SerialO	SOtoSI	Serial!	SltoSO
SerialO	S0toS2	Serial2	S2toS0
SerialO	S0toS3	Serial3	S3toS0

- В налаштуваннях портів відповідність ідентифікаторів DLCI іменам Sublink

1. Провірка зв'язків

Після закінчення налаштувань усіх роутерів виконаємо перевірку.

- Виконати команду show frame-relay map на роутері
R1 R1# show frame-relay map
Serial0/0/0.102 (up): point-to-point dlci, dlci 102, broadcast, status defined, active
Serial0/0/0.103 (up): point-to-point dlci, dlci 103, broadcast, status defined, active
Serial0/0/0.104 (up): point-to-point dlci, dlci 104, broadcast, status defined, active

Виконати команду **show frame-relay lmi**

R1# **show frame-relay lmi**
LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE = CISCO
Invalid Unnumbered info 0 Invalid Prot Disc 0
Invalid dummy Call Ref 0 Invalid Msg Type 0 Invalid
Invalid Status Message 0 Lock Shift 0 Invalid Report
Invalid Information ID 0 IE Len 0 Invalid Keep IE
Invalid Report Request 0 Len 0 Num Status msgs
Num Status Enq. Sent 26 Rcvd 26 Num Status
Num Update Status Rcvd 0 Timeouts 16

LMI Statistics for interface Serial0/0/0.102 (Frame Relay DTE) LMI TYPE = CISCO Invalid
Unnumbered info 0 Invalid Invalid Prot Disc 0
dummy Call Ref 0 Invalid Invalid Msg Type 0 Invalid
Status Message 0 Invalid Lock Shift 0 Invalid Report
Information ID 0 Invalid IE Len 0 Invalid Keep IE
Report Request 0 Num Len 0 Num Status msgs
Status Enq. Sent 0 Num Rcvd 0 Num Status
Update Status Rcvd 0 Timeouts 16

LMI Statistics for interface Serial0/0/0.103 (Frame Relay DTE) LMI TYPE = CISCO Invalid
Unnumbered info 0 Invalid Invalid Prot Disc 0
dummy Call Ref 0 Invalid Invalid Msg Type 0 Invalid
Status Message 0 Invalid Lock Shift 0 Invalid Report
Information ID 0 Invalid IE Len 0 Invalid Keep IE
Report Request 0 Num Len 0 Num Status msgs
Status Enq. Sent 0 Num Rcvd 0 Num Status
Update Status Rcvd 0 Timeouts 16

LMI Statistics for interface Serial0/0/0.104 (Frame Relay DTE) LMI TYPE = CISCO Invalid
Unnumbered info 0 Invalid Invalid Prot Disc 0
dummy Call Ref 0 Invalid Invalid Msg Type 0 Invalid
Status Message 0 Invalid Lock Shift 0 Invalid Report
Information ID 0 Invalid IE Len 0 Invalid Keep IE
Report Request 0 Num Len 0 Num Status msgs
Status Enq. Sent 0 Num Rcvd 0 Num Status
Update Status Rcvd 0 Timeouts 16

І остання команда **show frame-relay pvc**

R1# **show frame-relay pvc**
PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)
DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.102

input pkts 14055 output pkts 32795 in bytes 1096228 out bytes 6216155 dropped pkts 0 in FECN pkts 0 in BECN pkts 0 out FECN pkts 0 out BECN pkts 0 in DE pkts 0 out DE pkts 0 out bcast pkts 32795 out bcast bytes 6216155

DLCI = 103, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.103

input pkts 14055 output pkts 32795 in bytes 1096228 out bytes 6216155 dropped pkts 0 in FECN pkts 0 in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0 out bcast pkts 32795 out bcast bytes 6216155

DLCI = 104, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.104

input pkts 14055 output pkts 32795 in bytes 1096228 out bytes 6216155 dropped pkts 0 in FECN pkts 0 in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0 out bcast pkts 32795 out bcast bytes 6216155

5 Провірка зв’язку із Spoke-LANs

Виконати команду Ping з R1 на інтерфейси роутерів R2, R3, R4

Реалізація повнозвязної топології

Контрольні питання

1. Назвіть типи послідовних каналів зв'язку.
2. Де розташовується пристрій CSU / DSU і які функції він виконує?
3. Що таке DTE та DCE?
4. Як DTE пов'язаний з DCE?
5. Сформулюйте ідею мереж з комутацією пакетів МКП.
6. Що таке віртуальні канали в МКП?
7. Назвіть типи МКП?
8. Які фізичні канали зв'язку використовують МКП?
9. Які технології передачі даних використовуються в МКП?

10. У чому відмінність Frame Relay та X.25?
11. Протокол Frame Relay не виправляє помилок. Де вони тоді виправляються?
12. Що таке ATM?
13. Назвіть протоколи глобальних мереж, і для яких типів послідовних каналів зв'язку вони використовуються.
14. Чим відрізняються PVC від SVC?
15. Що таке DLCI і як воно співвідноситься з PVC?
16. Що треба зробити, щоб передати IP пакет через мережу Frame Relay?
17. Як відобразити DLCI на віддалений IP?
18. Що таке LMI?
19. Опишіть роботу протоколу Інверсний ARP.
20. Як на маршрутизаторі побачити до яких PVC він підключений?
21. Як на маршрутизаторі для інтерфейсів побачити відображення DLCI на віддалений IP?
22. Назвіть Топології Frame Relay.
23. Як здійснюється конфігурування підінтерфейсів для Frame Relay.
24. Яку роль відіграє команда frame-relay interface-dlci при конфігурування підінтерфейсів для Frame Relay.

Порядок виконання та здачі роботи

1. Вивчити теоретичну і практичну частину.
2. Здати викладачеві теорію роботи шляхом відповіді на контрольні запитання.
3. Виконати поспіль всі пункти практичної частини.
4. Створити всі скріншоти, наведені у практичній частині.
5. Показати викладачеві результат виконання пунктів 1, 2 і 3 практичної частини.
6. Виконайте в Packet Tracer завдання для самостійної роботи.
7. Показати викладачеві результат виконання пунктів 1, 2 і 3 завдання для самостійної роботи.
8. Оформіть звіт. Зміст звіту дивися нижче.
9. Захистіть звіт.

Завдання для самостійної роботи

1. Для повнозвязної топології чотирьох вузлів з локальними мережами (рисунок 10) спроектуйте Frame Relay мережу відповідно до даних в таблиці 2

Таблиця 2

R1	Fa0/0	192.168.10.1	255.255.255.0
	S0/0/0	10.10.10.1	255.255.255.0
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.10.10.2	255.255.255.0
R3	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0	10.10.10.3	255.255.255.0
R4	Fa0/0	192.168.40.1	255.255.255.0
	S0/0/0	10.10.10.4	255.255.255.0

- Для роботи мережі слід налаштувати базові статичні маршрути Frame Relay. (команда для встановлення статичного маршруту - frame-relay map ip <IP адреса мережі одержувача> ідентифікатор DLCI маршруту > broadcast)

- Для правильного функціонування мережі потрібно, щоб маршрутизатори підтримували протокол маршрутизації RIP (для цього в конфігураціях маршрутизаторів слід внести в налаштуваннях на вкладці RIP мережі які підключені до нього).

Зробіть скріншоти:

1. 4-х таблиць маршрутизації для кожного маршрутизатора.
2. Результат виконання команди **show frame-relay map** для кожного

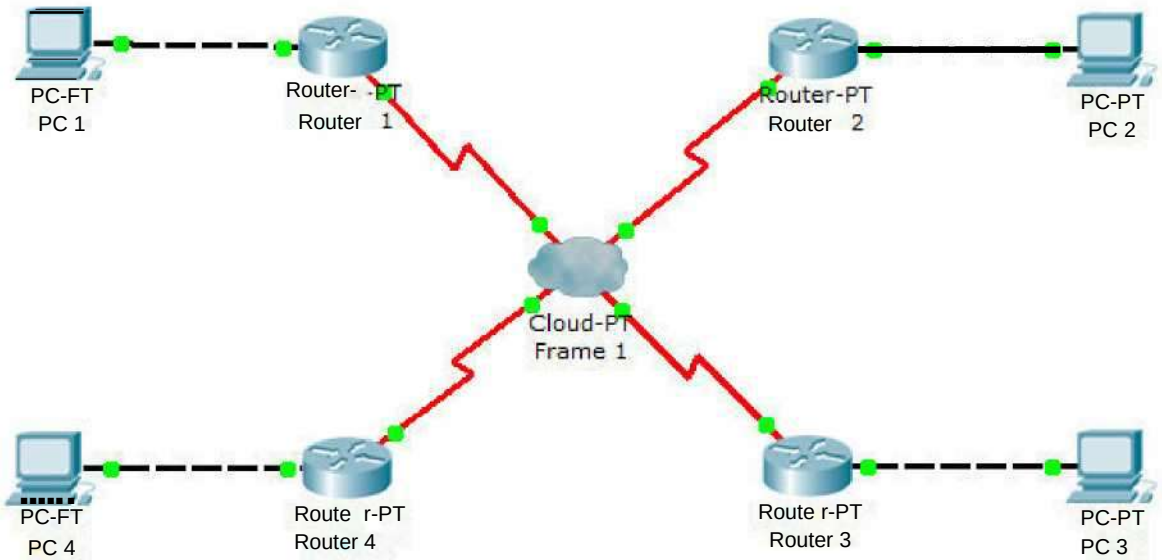


Рисунок 10

Зміст звіту.

Звіт готується в електронному вигляді і роздруковується. Звіт містить

1. Скріншоти топологій, створених при виконанні практичної частини.
2. Всі скріншоти, створені при виконанні практичної частини.
3. Конфігурації всіх маршрутизаторів з конфігураційних. Ш файлів, створених при виконанні практичної частини.
6. Конфігурацію маршрутизаторів з конфігураційних. Ш файлів, створених при виконанні завдань для самостійної роботи.
7. Всі скріншоти, зазначені в завданні для самостійної роботи.

Тема№3: Internet/Intranet технології

Лабораторне заняття 7: Віртуальні локальні мережі VLAN

Навчальна мета заняття: - Освоїти основні методи побудови віртуальні локальні мережі VLAN **Час: 4 год.**

Місце проведення: комп'ютерний клас Навчальні питання:

1. Конфігурування статичних VLAN
2. Розробка топології №1 (Рис.5)
3. Розробка топології №2 (Рис6)
4. Використання транзитних ліній, задля заощадження портів.

Література:

1. Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.
2. Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.
3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Текст] // Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286.
4. Закон України "Про інформацію" [Текст] // Відомості Верховної Ради України (ВВР), 1992, N 48, ст.650.

Методичне та матеріально-технічне забезпечення занять:

Персональний комп'ютер, включений в мережу IP, Microsoft Windows.

Хід проведення заняття:

I. Порядок проведення вступу до заняття.

Вступ

Обговорювання теоретичного матеріалу:

II. Порядок проведення основної частини заняття.

Лабораторна работа 7

Віртуальні локальні мережі VLAN

Теоретична частина.

Локальні мережі в даний час прийнято будувати на підставі технології комутованого Ethernet, прагнучи мінімізувати число концентраторів (хабів-hab) і використовувати переважно комутатори (свічі - switch). У комутаторі між приймачем і передавачем на час з'єднання утворюється віртуальний канал (virtual circuit) точка-точка. Така мережа може бути розглянута як сукупність незалежних пар приймач-передавач, кожна з яких використовує всю смугу пропускання. Комутатор дозволяє здійснювати паралельну передачу інформації. Комутація зменшує ймовірність переповнення в мережах Ethernet.

Якщо комутатору необхідно передати пакет на якийсь вихідний порт, і цей порт зайнятий, то пакет поміщається в буферну пам'ять. Це дозволяє узгодити швидкості передавачів і приймачів пакетів.

Для відправки фрейму через комутатор використовуються два методи:

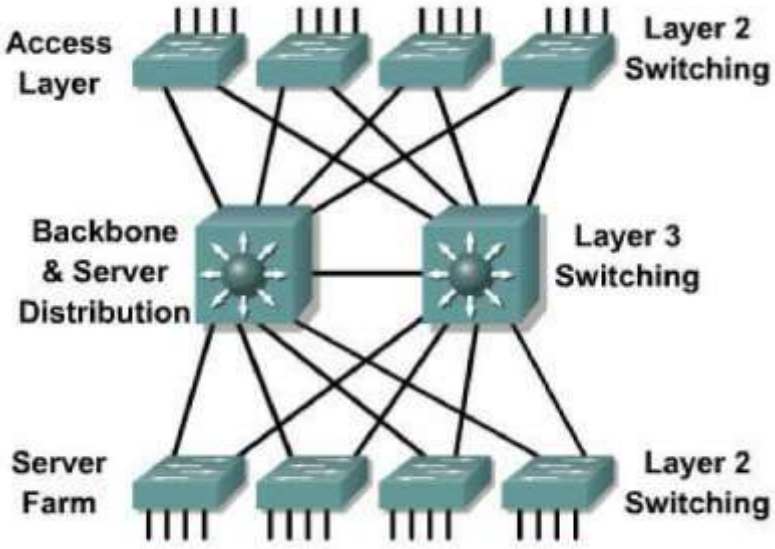
Відправлення з проміжним зберіганням (store-and-forward). Пакет повинен бути прийнятий повністю до того як буде розпочато його відправка.

Наскрізний метод (cut-through). Комутатор приймає початок пакета, зчитує в ньому адресу пункту призначення і починає відправляти пакет ще до його повного отримання.

Віртуальне з'єднання між портами комутатора зберігається протягом передачі одного пакета, тобто для кожного пакету віртуальне з'єднання організується наново на основі міститься в цьому пакеті адреси одержувача. Оскільки пакет передається тільки в той порт, до якого підключений адресат, інші пристрої підключені до комутатора, не отримають цей пакет. У комутаторах Ethernet передача даних між будь-якими парами портів відбувається незалежно і, отже, для кожного віртуального з'єднання виділяється вся смуга каналу.

При передачі широкомовного пакета, в комутаторі утворюється спектр каналів за принципом один до багатьох. Прикладами джерел широкомовного трафіку є ARP і маршрутизуючі протоколи.

Комутатори можна з'єднувати один з одним. При цьому група попарно прямо або непрямо пов'язаних комутаторів утворює один логічний комутатор з теоретично довільним числом портів. Тобто комутатори дозволяють створювати теоретично як завгодно велику локальну мережу. Правильне з'єднання комутаторів, тобто вибір топології мережі становить одну з найважливіших задач проектування локальних мереж.



Рекомендується здійснювати з’єднання комутаторів по рівням (Рисунок 1): серверний рівень, рівень розподілу(йІ8їгіЬиїіоп), рівень доступу(асеезз). Рядові комп’ютери підключаються до рівня доступу, а сервери відповідно до серверного рівня.

Головною перешкодою для створення великих локальних мереж за допомогою одних тільки комутаторів є нелінійний зростання обсягу широкомовного трафіку зі зростанням числа пристроїв у мережі. При числі пристроїв в мережі більше, ніж 2000 (за іншими оцінками 500, за третіми 4000 - все залежить від топології мережі і класу вирішуваних завдань) обсяг широкомовного трафіку різко зростає. Додавання нових пристроїв різко знижує продуктивність мережі.

Наприклад. Якщо в мережі з кількох тисяч пристроїв один з комп'ютерів A вперше здійснює IP з'єднання з іншим комп'ютером B у цій мережі, то він повинен заздалегідь послати до всіх пристроїв мережі широкомовний ARP запит для визначення MAC адреси комп'ютера B.

Локальна мережа, створена за допомогою одних тільки комутаторів представляє один домен широкомовлення. Зменшити домен широкомовлення можна, фізично розділивши локальну мережу на незалежні підмережі (незалежні групи попарно пов'язаних комутаторів) і з'єднати їх в єдине ціле з використанням маршрутизаторів. Таке завдання можна вирішити тільки на етапі побудови мережі, але не в момент її експлуатації. Тут на допомогу приходять віртуальні локальні мережі VLAN (virtual local area network).

Віртуальна локальна мережа VLAN являє собою сукупність портів одного або більше комутаторів.

VLAN дозволяють логічно розбити вихідну локальну мережу на кілька незалежних локальних мереж без фізичного обриву мережевих з'єднань. Для цього адміністратор мережі повинен на кожному комутаторі призначити, які його порти відносяться до яких VLAN. За замовчуванням всі порти комутатора відносяться до однієї VLAN з номером 1. Максимальне число VLAN в комутаторі дорівнює загальній кількості його портів. Правильна розбивка локальної мережі на VLAN становить одну з найважливіших задач проектування.

VLAN ведуть себе так само, як і фізично розділені локальні мережі. Тобто після розбивки мережі на VLAN ми отримаємо кілька локальних мереж, які далі необхідно об'єднати в єдине ціле за допомогою маршрутизації на третьому мережевому рівні.

Концепція VLAN, крім вирішення проблеми з широкомовним трафіком дає також ряд додаткових переваг: формування локальних мереж не за місцем розташування найближчого комутатора, а за належністю комп'ютерів до вирішення тієї чи іншої виробничої задачі; створення мережі за типом споживаного обчислювального ресурсу і необхідної серверної послуги (файл - сервер, сервер баз даних). VLAN дозволяють вести різну політику безпеки для різних віртуальних мереж; переводити комп'ютер з однієї мережі в іншу без здійснення фізичного переміщення або пере підключення.

Для обміну інформацією про VLAN комутатори використовують магістральний (транковий) протокол. Для здійснення обміну інформацією про VLAN між комутаторами ви повинні створити магістральні порти. Магістральний порт це порт, який використовується для передачі інформації про VLAN в інші мережеві пристрої, приєднані до цього порту. Звичайні порти не розповсюджують інформацію про VLAN, але будь-який порт може бути налаштований для прийому / передачі інформації про VLAN. Ви повинні активізувати магістральний протокол на потрібних портах, так як він вимкнений за умовчанням.

Порт комутатора працює або в режимі доступу або в магістральному режимі. Відповідно зв'язок, з'єднаний з портом є або зв'язком доступу або магістральним зв'язком. У режимі доступу порт належить тільки одній VLAN. Порт доступу приєднується до кінцевого пристрою: ПК, робочої станції, сервера, хабу. Фрейми, що проходять через порт доступу, є звичайними Ethernet фреймами.

Магістральні зв'язки здатні підтримувати декілька VLAN. VLAN на різних комутаторах зв'язуються через магістральний протокол. Магістральні порти не належать певній VLAN і використовуються для приєднання до інших комутаторів, маршрутизаторів або серверів, що мають мережеві адаптери з можливістю для підключення до багатьох VLAN.

Магістралі можуть розширити VLAN по всій мережі. Для магістральних цілей призначають високошвидкісні порти комутаторів: Gigabit Ethernet і 10Gigabit.

Для мультиплексування трафіку VLAN існують спеціальні протоколи, що дозволяють приймачам портів визначити, якій VLAN належить пакет. Для зв'язку між пристроями Cisco використовується протокол Inter-Switch Link (ISL). При наявності в мережі обладнання декількох виробників застосовується протокол IEEE 802.1Q

Без магістральних зв'язків для підтримки VLAN повинно бути організовано по одному зв'язку доступу для кожної VLAN. Такий підхід дорогий і неефективний, тому магістральні зв'язку абсолютно необхідні при проектуванні локальних мереж.

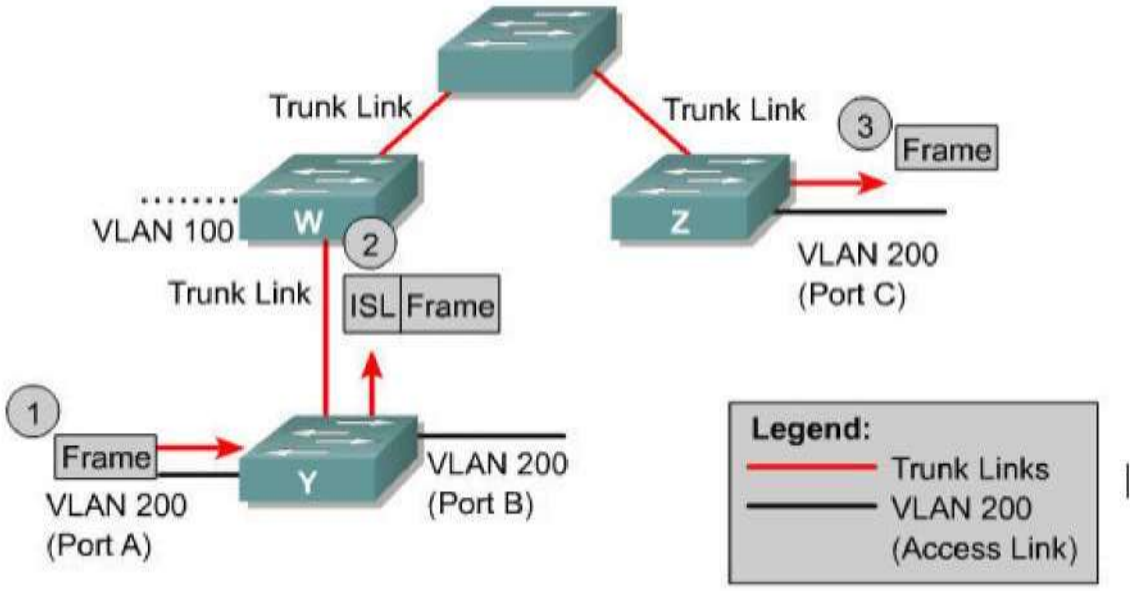


Рисунок 3

На рисунку 3 порти A і B на комутаторі Y визначені як лінії доступу на однієї і тієї же VLAN 200. За визначенням вони можуть належати тільки одній VLAN і не можуть отримувати ethemet фрейми, які містять ідентифікатор VLAN. Наприклад, коли Y отримує трафік від порту A до порту B, то він не додає ISL заголовокок в ethernet фрейми.

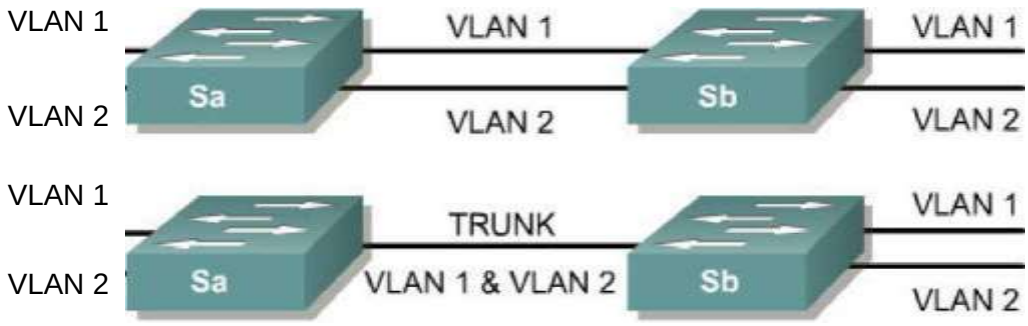
Порт C на комутаторі Z також є портом доступу і також належить до VLAN 200. Якщо порт A пересилає фрейм у порт C, то відбувається наступне:

1. Комутатор Y отримує фрейм і, зіставляючи номер порту призначення з номером VLAN, визначає його як трафік, спрямований до VLAN 200 на іншому комутаторі,
2. Комутатор Y додає до фрейму ISL заголовок з номером VLAN і пересилає фрейм через проміжний комутатор на магістральний зв'язок.
3. Цей процес повторюється на кожному комутаторі по шляху фрейму до кінцевого порту C.
4. Комутатор Z отримує фрейм, видаляє ISL заголовок і направляє фрейм на порт C.

Якщо порт знаходиться в магістральному режимі, то він може бути налаштований або для транспорту всіх VLAN або обмеженої множини VLAN. Магістральні зв'язку використовуються для зв'язку комутаторів з іншими комутаторами, маршрутизаторами або з серверами, що мають підтримку VLAN.

Згідно базової термінології магістраль це зв'язок точка-точка, що підтримує кілька VLAN. Метою магістралі є збереження номерів портів при створенні зв'язку між двома пристроями, що утворюють VLAN.

Верхня фігура на малюнку 4 показує спосіб створення VLAN шляхом використання двох фізичних зв'язків між комутаторами (по одній на кожну VLAN). Це рішення погано масштабується: при додаванні третьї VLAN треба пожертвувати ще двома портами. Це рішення неефективне і в сенсі розподілу навантаження: малий трафік на деяких лініях зв'язку може не коштувати того, що цей зв'язок є окремим пучком віртуальних зв'язків через один фізичний зв'язок. На нижній фігурі одна фізична зв'язок здатна нести трафік для будь-якої VLAN. Для досягнення цього комутатор Sa так оформляє фрейми, що Sb знає, на яку VLAN вони направляється. Для такого оформлення пакетів використовуються або стандарт IEEE 802.1Q або Cisco протокол ISL (Inter-Switch Link).



Для великих мереж ручна конфігурація VLAN стає вельми трудомістким завданням. Cisco VLAN Trunk Protocol (VTP) служить для автоматичного обміну інформацією про VLAN через магістральні порти. Перевагою використання VTP є те, що ви можете контролювати додавання, видалення або зміна мереж VLAN з комутаторів на якому створені VTP сервера. Після налаштування ваших комутаторів як VTP серверів, інші комутатори вашої мережі можуть бути налаштовані як клієнти, які тільки отримують VLAN інформацію. Недоліком є непотрібний трафік, створюваний на магістральний портах для пристроїв, яким можливо не потрібна ця інформація.

Якщо ваша мережа буде містити багато комутаторів, що містять багато віртуальних мереж, розташованих у різних комутаторах, можливо, має сенс використовувати VTP. Якщо ваша мережа залишається досить статичної, і VLAN не будуть додаватися або змінюватися по відношенню до початкової конфігурації, то краще використовувати статичне визначення віртуальних мереж.

У топології локальних мереж можливі цикли (петлі). Наприклад, вже три комутатора з'єднаних один з одним по колу утворюють цикл в топології. Петлі призводять до неоднозначності при визначенні шляху від джерела пакетів до приймача. Для вирішення цієї серйозної проблеми був розроблений протокол сполучного дерева STP (spanning tree protocol). Для графа топології кожної VLAN, яка визначена в мережі, будується мінімальне покриваюче дерево (граф без циклів) з вершиною в деякому комутаторі. Для фізичної реалізації таких дерев STP переводить надлишкові порти в стан блокування. Розрахунок дерев проводиться паралельно на всіх комутаторах. Далі пакети у VLAN йдуть тільки по шляхах, визначених у побудованих покриваючих деревах. При зміні топології, активації / зупинці портів відбувається перерахунок покривають дерев.

Для створення топографії сполучного дерева існують спеціальні фрейми, звані модулями даних мостового протоколу (bridge protocol data units, BPDU). Ці фрейми відправляються і приймаються всіма комутаторами в мережі через рівні проміжки часу.

Конфігурування статичних VLAN

1. Статичні VLAN це сукупність портів на комутаторів, які вручну призначаються командою IOS при конфігуруванні інтерфейсу.

Для створення порожньої VLAN с номером № VLAN на комутаторах Cisco серії 2950 використовуються команди

Switch # vlan database

Switch (vlan) # vlan № VLAN

Switch (vlan) # exit Наприклад, команди Switch # vlan database Switch (vlan) # vlan 33 Switch (vlan) # exit

Які створять порожню VLAN з номером 33 і система дасть VLAN ім'я VLAN0033.

Зауважимо, що команди виконуються не в режимі конфігурації.

Команда switchport mode використовується для установки інтерфейсу в динамічний режим, режими доступу або режим магістралі (trunk).

Switch (config-if) # switchport mode [access | dynamic | trunk]

Хоча режим доступу є режимом за замовчуванням, але в ряді випадків пристрій, приєднаний до порту комутатора, може перевести його в магістральний режим. Тому рекомендується всі немагістральні порти переводити в режим доступу командою *switchport mode access.*

Для статичного переміщення поточного інтерфейсу під VLAN використовуються команди

Switch (config-if) # switchport mode access Switch (config-if) # switchport access vlan № number

де № number - число - номер VLAN.

Команда *interface range* визначає діапазон інтерфейсів для наступних конфігурацій. Наприклад, порти з першого по шостий можуть бути поміщені в VLAN 10 командами Switch (config) # interface range fa0 / 1 - 6 Switch (config-if-range) # switchport access vlan 10

Після налаштування VLAN перевірте налаштування командами *show running-config, show vlan і show vlan brief.*

При налаштуванні VLAN пам'ятаєте, що за замовчуванням всі порти знаходяться у VLAN 1.

Для створення або конфігурування магістралі VLAN ви повинні налаштувати порт як магістральний

Switch (config-if) # switchport mode trunk

За замовчуванням остання команда визначає порт як магістральний для всіх VLAN в мережі. Однак існують ситуації, коли магістраль не повинна підтримувати всі VLAN. Типовою є ситуація з придушенням широкомовлення. Широкомовлення надсилається на кожен порт у VLAN. Магістральний зв'язок виступає як член VLAN і повинна пропускати всі широкомовлення. Якщо на іншому кінці магістралі немає портів потрібної VLAN, то смуга пропускання і процесорний час пристроїв витрачається даремно.

Якщо VLAN не використовується на іншому кінці магістралі, немає потреби дозволяти цю VLAN на цій магістралі. За замовчуванням магістральні порти приймають і передають трафік з усіх VLAN в мережі. Для скорочення магістрального трафіку використовуйте команду

Switch (config-if) # switchport trunk allowed vlan vlan-list Наприклад, команда

Switch (config-if) # switchport trunk allowed vlan 3 Switch (config-if) # switchport trunk allowed vlan 6-10

дозволяє на магістралі VLAN 3 та потім VLAN з 6 по 10. Про те, які VLAN дозволені на магістралі можна подивитися командою *show running-config.*

Для видалення великої кількості VLANs з магістралі простіше спочатку видалити всі VLAN, а потім вибірково дозволяти.

Найпростіший спосіб перевести зв'язок в режим доступу це задати на інтерфейсах з його двох сторін по команді

SwitchA (config-if) # switchport mode access

Найпростіший спосіб перевести зв'язок в режим транкінгу це задати на інтерфейсах з його двох сторін по команді

SwitchA (config-if) # switchport mode trunk

Практична частина

1. Зберіть топологію зображену на рисунку 5. Комутатори з'єднайте двома GigabitEthernet (gi1 / 1 і gi1 / 2) зєднаннями. Комп'ютери підключіть до інтерфейсів згідно з таблицею 1. Призначте комп'ютерам адреси, згідно з таблицею 1. Всі комп'ютери входять в одну підмережу 172.16.0.0 255.255.0.0. Маршрути за замовчуванням на комп'ютерах не встановлюйте. Пропінгуйте мережу.

Організуємо в нашій мережі дві VLAN. Комп'ютери 20_1 і 20_2 помістимо у VLAN з номером 20, а комп'ютери 30_1 і 30_2 помістимо у VLAN з номером 30.

Switch1 (conf) # interface fa0 / 2 Switch1
(conf-if) # switchport access vlan 20
Switch1 (conf-if) # interface fa0 / 3
Switch1 (conf-if) # switchport access vlan
30 Switch2 (conf) # interface fa0 / 2
Switch2 (conf-if) # switchport access vlan
20 Switch2 (conf-if) # interface fa0 / 3
Switch2 (conf-if) # switchport access vlan
20

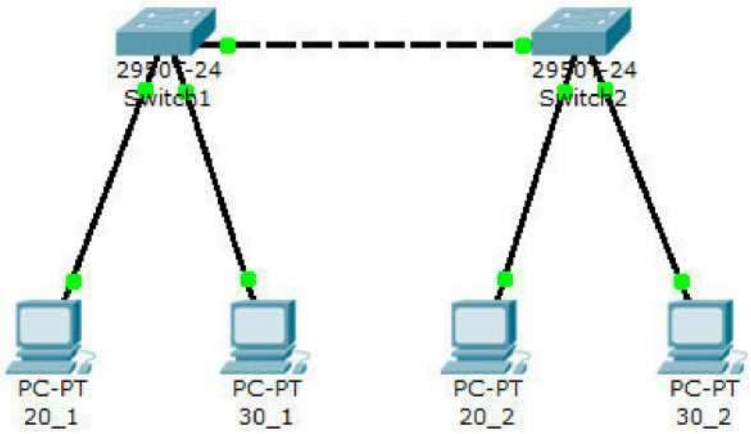


Рисунок 5

Компьютер	Switchl	Switch2	Адрес
20_1	Fa0/2		172.16.20.1/16
30_1	Fa0/3		172.16.30.2/16
20_2		Fa0/2	172.16.20.1/16
30_2		Fa0/3	172.16.30.2/16
	Gil/1	Gil/1	

На обох комутаторах провірте результати створення VLAN, наприклад

Switch1# sh vl name 20

```
VLAN Name                Status    Fort3

20 20                    active    FaO/2

VLAN Type SAID 20        MTU    Parent  RingNo  BridgeNo  Stp  BrdgMode   Transl  Trans2

enet 100020              1500   -     -        -         -    -          0       0
```

1

```
Switchl#sh vl br

VLAN Name                                Status     Forts
-------------------------------------------------------------------------------
1 default                                active     Fa.0/1, FaO/4, Fa0/5f FaO/6
                                                    FaO/7, FaO/3, FaO/9, FaO/10
                                                    Fa.0/11  FaO/12, FaO/1.3, FaO/14
                                                    FaO/15,  FaO/16, FaO/17, FaO/13
                                                    FaO/19,  Fa0/20, FaO/21, FaO/22
                                                    FaO/23,  FaO/24
20 20                                    active     FaO/2
30    30                                 active     FaO/3
1002  fddi-default                       active
1003  token-ring-default                 active
1004  fddinet-default                    active
1005  trnet-default                      active
```

Так як немає обміну інформацією про VLAN між комутаторами, то комп'ютери зможуть пінгувати лише самі себе.

Організуємо магістралі (транкінг) на комутаторах. Для цього використовуємо ***GigabitEthernet*** порт

Switch1(conf)#interface gi1/1

Switchl (conf-if)#switchport trunk allowed vlan add 20

Switchl (conf-if)#switchport trunk allowed vlan add 30

Switch1 (conf-if)#no shutdown

Switch2 (conf)#interface gi1/1

Switch2 (conf-if)#switchport trunk allowed vlan add 20

Switch2 (conf-if)#switchport trunk allowed vlan add 30

Switch2 (conf-if)#no shut

Тепер комп'ютери в межах однієї VLAN повинні пінгуватись, на відміну від комп'ютерів у різних VLANs.

Зберегти конфігурації комутаторів.

2. Зберегти топологію попереднього завдання в окремому файлі. В новій топології з'єднаємо маршрутизатор двома зв'язками з інтерфейсами fa0/1 комутаторів(Рисунок 6).

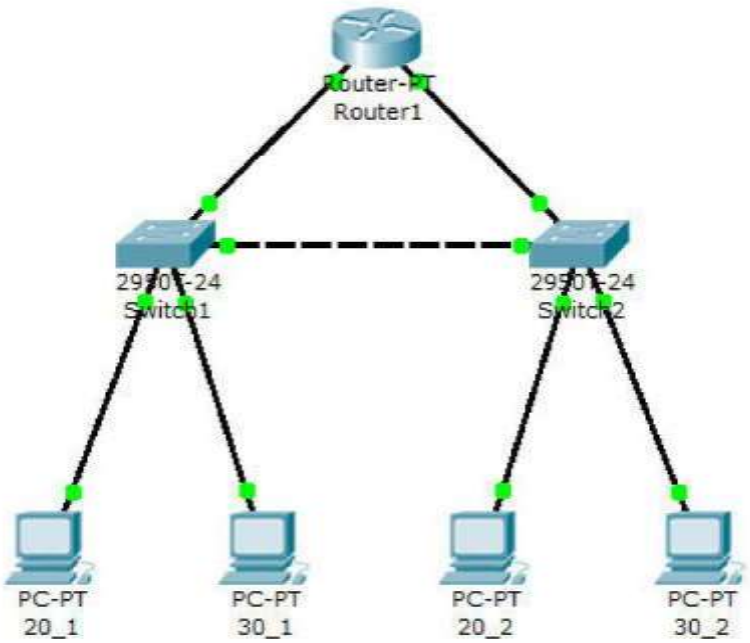


Рисунок 6

Поставимо задачу об’єднання віртуальних мереж за допомогою маршрутизатора. Для цього слід розбити існуючу мережу 172.16.0.0/16 на дві під мережі 172.16.20.0/24 і 172.16.30.1/24. Для цього просто поміняємо маски в комп’ютерів на 255.255.255.0.

Тепер комп’ютери пінгуються в межах відповідних VLANs і в межах відповідної під мережі.

Введемо на комутаторах інтерфейси, під’єднанні до маршрутизатора у віртуальні мережі.

Switch1(conf)#interface fa0/1 Switch1(conf-if)#switchport access vlan 20

Switch2(conf)#interface fa0/1 Switch2(conf-if)#switchport access vlan 30 Настроим IP адреса на маршрутизаторе

Router(conf)#interface fa0/0

Router(conf-if)#ip address 172.16.20.254 255.255.255.0

Router(conf-if)#no shutdown

Router(conf-if)#interface fa1/0

Router(conf-if)#ip address 172.16.30.254 255.255.255.0

Router(conf-if)#no shutdown

Тепер маршрутизатор маршрутизує дві мережі 172.16.20.0/24 і 172.16.30.1/24. Додамо на наших комп'ютерах маршрутизацію за замовчуванням на інтерфейси маршрутизатора.

Host	Gateway
20_1	172.16.20.254
20_2	172.16.20.254

30_1	172.16.30.254
30_2	172.16.30.254

Тепер з усіх пристроїв нашої мережі ми можемо пінгувати всі наші № адреси.

3. Покажемо, як з використанням транзитних ліній, ми можемо заощадити порти. Змінимо топологію, прокинувши магістраль gi1 / 2 від комутаторів до інтерфейсу fa0 / 0 маршрутизатора (малюнок 7). Завантажимо топологію в симулятор. Завантажимо по черзі в кожен пристрій, крім маршрутизатора, збережені конфігурації. Зауважимо, що у конфігурації комутатора Switch2 установка магістралі на §I1 / 2 не потрібна, хоча вона і не заважає.

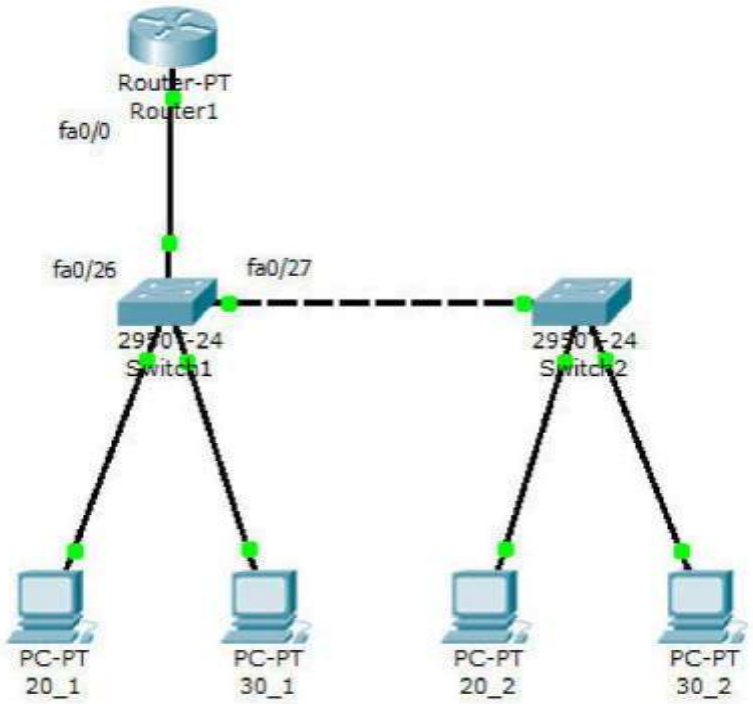


Рисунок 7

На маршрутизаторі розіб'ємо інтерфейс fa0 / 0 на два підінтерфейси fa0/0.20 і fa0/0.30. Визначимо на них інкапсуляцію dot1q і помістимо їх у віртуальні мережі 20 і 30, відповідно.

Router(conf)#interface FastEthernet0/0.20
Router(conf-subif)#encapsulation dot1q 20 Router(conf-subif)#ip address 172.16.20.254 255.255.255.0
Router(conf-subif)#interface FastEthernet0/0.30
Router(conf-subif)#encapsulation dot1q 30 Router(conf-subif)#ip address 172.16.30.254 255.255.255.0
Проглянемо таблицю маршрутів Router#show ip route

```
C       172.16.20.0 is directly connected, Fa3tEthernet0/0.20
C       172.16.30.0 is directly connected, FastEthernetO/O.30
```

Перевірте, що з кожного пристрою ви можете пінгувати всі адреси в мережі. Виконайте на Router команду розширеного пінту від адреси 172.16.20.1 комп'ютера 20_1 з VLAN 20, підключеного до комутатора Switch1 до адреси 172.16.30.2 комп'ютера 30_2 з VLAN 30, підключеного до комутатора Switch2.

```
Routerttping
Protocol [ip]:
Target IP address: 172.16.30.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended camnands [n] :y
Source address or interface:172.16.20.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [OxABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n] :

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.2, timeout is 2 seconds:

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Контрольні питання

1. Чому вважають за краще будувати локальні мережі за допомогою комутаторів, а не концентраторів?
2. Які існують методи для відправки фрейму через комутатор?
3. Як комутатор дізнається MAC адреси підключених пристроїв?
4. Де і як у комутаторі зберігаються адреси підключених пристроїв?
5. Що таке віртуальне з'єднання і як довго воно існує?
6. Наскільки велику локальну мережу можна створити за допомогою комутаторів?
7. Як прийнято будувати великі локальні мережі?
8. Що є головною перешкодою для створення великих локальних мереж за допомогою одних тільки комутаторів?
9. Що таке домен широкомовлення?
10. Як зменшити домен широкомовлення?
11. Що таке VLAN?
12. Які проблеми локальних мереж вирішує VLAN?
13. Як в локальній мережі організувати обмін інформацією у VLAN?
14. У яких режимах працюють порти комутатора?
15. Якій VLAN належить магістральний порт?
16. Як поширити одну VLAN на кілька комутаторів?
17. Чи можна організувати кілька VLAN на декількох комутаторах без використання магістралей?
18. Навіщо потрібні протоколи ISL і IEEE 802.1Q?
19. Навіщо потрібні магістралі в в локальній мережі?

20. Які завдання вирішує VTP?
21. Які завдання вирішує STP?
22. Якими командами можна організувати VLAN?
23. Якою командою перевести порт в режим доступу і в режим магістралі?
24. Якою командою можна отримати інформацію про VLAN?
25. У локальній мережі є одинадцять VLAN. Скільки маршрутизаторів треба для об'єднання всіх 11 VLAN в єдине ціле?

Завдання для самостійної роботи

Повторити усі пункти практичної частини для IP мережі підприємства, відповідно варіантів:

Вар.	Мережа	Вар.	Сеть	Вар.	Сеть
1	2.1.0.0/16	5	6.1.0.0/16	9	10.1.0.0/16
2	3.1.0.0/16	6	7.1.0.0/16	10	11.1.0.0/16
3	4.1.0.0/16	7	8.1.0.0/16	11	12.1.0.0/16
4	5.1.0.0/16	8	9.1.0.0/16	12	13.1.0.0/16

Створити такі ж скріншоти, як і у практичній частині.

Порядок виконання та здачі роботи

1. Вивчити теоретичну і практичну частину.
2. Здати викладачеві теорію роботи шляхом відповіді на контрольні запитання.
3. Виконати в Packet Tracer практичну частину.
4. Виконайте в Packet Tracer завдання для самостійної роботи.
5. Для свого варіанту пред'явіть викладачеві можливість виконати розширений пінг між будь-якими адресами для топологій на малюнках 6 і 7.
6. Оформіть звіт. Зміст звіту дивися нижче.
7. Захистіть звіт.

При конфігуруванні послідовного інтерфейсу маршрутизатора для підключення до Frame Relay повинна бути визначена інкапсуляція Frame Relay. Є дві можливі інкапсуляції - ietf і cisco. На пристроях cisco за замовчуванням використовується інкапсуляція cisco. Метод cisco є власністю компанії і не може бути використаний, якщо маршрутизатор cisco з'єднаний по мережі Frame Relay з обладнанням іншого виробника.

Для базової конфігурації Frame Relay в Cisco IOS версії старше 11.1, використовує інверсне ARP і автовизначення типу LMI, слід лише задати адресу третього рівня і встановити інкапсуляцію в Frame Relay

Router (config-if) # **encapsulation frame-relay {cisco | ietf}**

Якщо використовується Cisco IOS версії 11.1 або раніше, то необхідно задати тип LMI

Router (config-if) # **frame-relay lmi-type {ansi | cisco | q933a}**

Важливо пам'ятати, що провайдер Frame Relay послуг створює віртуальний канал всередині мережі Frame Relay, що сполучає два віддалених мережевих пристрої користувача, як правило, маршрутизатора. Як тільки маршрутизатор і комутатор Frame Relay, до якого він підключений, завершують обмін інформацією LMI, мережа Frame Relay має все необхідне для створення віртуального каналу з віддаленим маршрутизатором.

Конфігурація відображень Frame Relay

Якщо використовується динамічне відображення адрес, то для кожного активного PVC служба інверсного ARP маршрутизатора запитує IP адреса у маршрутизатора наступного кроку. Як тільки запитуючий маршрутизатор одержує відгук інверсного ARP, він оновлює таблицю відображення адрес третього рівня в номери DLCI. Для пристроїв cisco динамічне відображення адрес включено за замовчуванням. Якщо обладнання Frame Relay підтримує інверсне ARP і автовизначення типу LMI, то динамічне відображення адрес має місце автоматично. Отже, не потрібно статичного відображення адрес.

Якщо обладнання не підтримує інверсне ARP і автовизначення типу LMI, то статичне відображення має бути налагоджене вручну за допомогою команди frame-relay map. Як тільки для даної DLCI задається статичне відображення, на цьому служба інверсного ARP відключається.

Для конфігурації статичного відображення використовується наступний синтаксис

Router (config-if) # **frame-relay map protocol protocol-address dlci [broadcast] [ietf | cisco],**

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Закон України “Про Національну програму інформатизації” [Текст] // Відомості Верховної Ради України (ВВР), 1998, N 27-28, ст.181.
2. Закон України "Про електронні документи та електронний документообіг” [Текст] // Відомості Верховної Ради України (ВВР), 2003, N 36, ст.275.
3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Текст] // Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286.
4. Закон України "Про інформацію" [Текст] // Відомості Верховної Ради України (ВВР), 1992, N 48, ст.650.
5. Закон України “Про Концепцію Національної програми інформатизації” [Текст] // Відомості Верховної Ради України (ВВР), 1998, N 27-28, ст.182.
6. Указ Президента України „Про першочергові завдання щодо впровадження новітніх інформаційних технологій” [Текст]// Урядовий кур'єр 2005, N207 від 01.11.2005.
7. Кобзев, І.В. Технології локальних та глобальних мереж / [Текст]: Навчальний посібник // І.В. Кобзев, І.В. Магдаліна, С.В. Калякін. - Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2010. - 280 с.
8. Галкін В.А., Григор'єв Ю.А. Телекомунікації й мережі: [Текст]: Учеб. Посібник для вузів.-М.: Изд-У МГТУ їм. Н.Э.Баумана, 2003.-608 с.: іл.
9. Кулаков Ю.О., Луцький Г.М. [Текст]: Комп’ютерні мережі. Підручник. - К.: Юніор, 2003. - 400 с.
10. Под редакцией Л.Мелиховой. Интернет. Энциклопедия- СПб: Питер, 2001.528с. ил.
11. Уэнделл Одом. Компьютерные сети. Первый шаг = Computer Networking Firststep. — М.: «Вильямс», 2005. — С. 432.
12. Болілий В.О., Котяк В.В. Комп'ютерні мережі. Навчальний посібник. - Кіровоград: ЦОП Авангард, 2008.- 146с.
13. Олифер В.Г., Олифер Н.А. Компьютерные сети принципы, технологии, протоколы. - СПб: Питер, 2000.-672с.
14. Кулаков Ю.А., Омельянский С.В. Компьютерные сети. Выбор, установка, использование и администрирование.- К.: Юниор, 1999.- 544с.
15. Гук М. Аппаратные средства локальных сетей. Энциклопедия.- СПб: Питер, 2000.- 576 с.
16. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации - СПб.: Питер, 2002.

Допоміжна

17. Новиков Ю.В., Кондратенко С.В. Локальные сети: архитектура, алгоритмы, проектирование. - М.: ЭКОМ, 2001. - 312 с.

18.Інформатика: Комп’ютерна техніка. Комп’ютерні технології: Підручник для студентів вищих навчальних закладів / За ред. Пушкаря. - К.: Видавничій центр «Академія», 2002. - 704 с. ISBN 966-580-135-X

19. Вуль В.А., Электронные издания. - М.. -СПб.: Издательство «Петербургский институт печати», 2001. - 308 с., илл. ISBN 5-93422-015-2

20. Капелюх С.А. Электронная почта. Самоучитель. - СПб.: БХВ-Петербург, 2006. - 144 с.: ил. ISBN 5-94157-813-X

21. Вирусы и средства борьбы с ними. ЗАО «Лаборатория Касперского»., Учебный курс. М. - 2005

22. Мюллер С. Модернизация и ремонт ПК, 16-е издание.: Пер. с англ. - М.: Издательский дом “Вильямс”, 2006. - 1328 с.: ил. ISBN 5-8459-0819-1

23. Microsoft. Комп'ютерні мережі. Учбовий курс/Пер. з англ. - М.: Видавничий відділ “Російська редакція” ТОО “Channel Trading Ltd.”. - 1998. - 696 с.

24. Високопродуктивні мережі. Енциклопедія користувача: Пер. з англ./Марк А. Спортак і ін. - К.: Видавництво «Діасофт», 1998. - 432 с.

25. Скляров А.Я., Пономаренко л.А., Щелкунов в.І., Інструментальні засоби проектування, імітаційного моделювання і аналізу комп'ютерних мереж. Навчальний посібник. - До: Нук. Думання, 2002. - 508 с.