МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Л.М. Олещенко

ОРГАНІЗАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

ЛАБОРАТОРНИЙ ПРАКТИКУМ

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського як навчальний посібник для студентів, які навчаються за спеціальністю 121 «Інженерія програмного забезпечення», спеціалізацією «Програмне забезпечення комп'ютерних та інформаційно-пошукових систем»

Київ
КПІ ім. Ігоря Сікорського
2018

Рецензенти: *Бідюк, П. І.*, д-р техн. наук, проф.
Стеценко, І. В., д-р техн. наук, проф.

Відповідальний редактор *Заболотня, Т. М.*, канд. техн. наук, доц.

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол № 7 від 29.03.2018 р.)
за поданням Вченої ради факультету прикладної математики
(протокол № 8 від 26.03.2018 р.)

Електронне мережне навчальне видання

Олещенко Любов Михайлівна, канд. техн. наук

ОРГАНІЗАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

ЛАБОРАТОРНИЙ ПРАКТИКУМ

Організація комп'ютерних мереж: лабораторний практикум [Електронний ресурс] : навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення», спеціалізації «Програмне забезпечення комп'ютерних та інформаційно-пошукових систем» / Л.М. Олещенко ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 4,68 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 137 с.

Навчальний посібник розроблено для отримання студентами практичних навичок з проектування та налаштування комп'ютерних мереж. Навчальне видання призначене для студентів, які навчаються за спеціальністю 121 Інженерія програмного забезпечення, спеціалізацією «Програмне забезпечення комп'ютерних та інформаційно-пошукових систем» факультету прикладної математики КПІ ім. Ігоря Сікорського.

ЗМІСТ

ВСТУП

Учбова дисципліна "Організація комп’ютерних мереж" є нормативною і входить до складу циклу професійно-орієнтованих дисциплін навчального плану підготовки бакалаврів, що навчаються за спеціальністю 121 «Інженерія програмного забезпечення» спеціалізації «Програмне забезпечення комп’ютерних та інформаційно- пошукових систем».

Предмет дисципліни – теоретичні і практичні основи в області організації комп'ютерних мереж. Мета дисципліни – забезпечити знання теоретичних і практичних основ з організації та функціонування комп'ютерних мереж, уміння застосовувати в професійній діяльності розподілені дані, програми і ресурси мереж.

Метою лабораторного практикуму є отримання практичних навичок з проектування та обслуговування комп’ютерних мереж передачі даних. Вивчення курсу допомагає забезпечити необхідний рівень знань з мережевого апаратного та програмного забезпечення, мережевих операційних систем та їх компонент.

У даному навчальному посібнику студенти ознайомляться з правилами проектування локальних мереж, стандартами передачі даних, алгоритмами роботи та функціональними можливостями мережевих пристроїв. Навчальний посібник складається з 9 розділів, кожен з яких присвячений виконанню певної лабораторної роботи з дисципліни «Організація комп’ютерних мереж».

В кожному розділі надаються теоретичні відомості з певної теми, завдання на лабораторну роботу цієї теми, вказівки щодо виконання завдання, а також наводяться вимоги до оформлення звіту з виконаної лабораторної роботи, контрольні питання для самоперевірки та список рекомендованої літератури.

Лабораторні роботи з дисципліни «Організація комп’ютерних мереж» розраховані на 36 академічних годин аудиторних занять.

ЛАБОРАТОРНА РОБОТА № 1. МЕРЕЖЕВІ ПРИСТРОЇ І ЗАСОБИ КОМУНІКАЦІЙ. СЕРЕДОВИЩЕ МОДЕЛЮВАННЯ CISCO PACKET TRACER

Мета роботи*:* ознайомитися з основними мережевими пристроями та засобами передавання даних комп'ютерних мереж з використанням середовища моделювання Cisco Packet Tracer, навчитися додавати у симуляторі нові пристрої, створювати з'єднання, налаштовувати вузли та перевіряти підключення.

Теоретичні відомості

В якості засобів комунікації найчастіше використовуються вита пара, коаксіальний кабель та оптоволоконні лінії. При виборі типу кабелю враховують наступні показники:

- Вартість монтажу і обслуговування;
- Швидкість передачі інформації;
- Обмеження на величину відстані передачі інформації;
- Безпека передачі даних.

Головною проблемою при проектуванні комп'ютерних мереж є одночасне забезпечення даних показників. Наприклад, найвища швидкість передачі даних обмежена максимально можливою відстанню передачі даних, при якій ще забезпечується необхідний рівень захисту даних. Простота розширення кабельної системи впливають на її вартість і безпеку передачі даних.

Мережеві пристрої

Мережева карта (мережева плата, мережевий адаптер, Ethernet-адаптер, NIC (англ. *network interface card*)) відповідає за передачу інформації між одиницями мережі. Будь-яка мережева карта складається з роз'єму для мережевого провідника та мікропроцесора, що кодує/декодує мережеві пакети та з допоміжних програмно-апаратних комплексів і служб. Кожна мережева карта має свою фізичну **MAC-адресу** (англ. *Media Access Control*) – унікальний ідентифікатор пристрою. Це ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж. У випадку з мережами типу Ethernet це унікальний ідентифікатор (номер) мережевої карти. Формат MAC-адреси – 6 пар цифр і букв, що зазвичай розділяються дефісом або двокрапкою. Наприклад: **00: 1D: 72: 1F: AC: 95** або: **00-3D-42-3F-CC-95.**

Рис.1.1 Мережева карта

Мережеве середовище

У сучасних мережах використовуються головним чином три типи середовищ, що зв'язують пристрої і забезпечують шлях, по якому передаються дані. До таких типів середовищ відносяться:

- **металеві дроти усередині кабелю;**
- **скляні або пластикові волокна (оптоволоконний кабель);**
- **радіозв'язок.**

Кодування сигналу, яке потрібне для передачі, здійснюється по-різному залежно від типу середовища.

У металевих дротах дані кодуються у вигляді електричних імпульсів, що відповідають певним шаблонам.

Передача в **оптоволоконних мережах відбувається у вигляді імпульсів світла, в діапазоні інфрачервоного випромінювання або видимого світла.**

При **безпровідній передачі для опису різних значень бітів використовуються шаблони електромагнітного випромінювання**.

Мідні кабелі

У мережевих технологіях існують три основні типи мідних кабелів:

- **коаксіальний кабель;**
- **неекранована вита пара (UTP);**
- **екранована вита пара (STP).**

Ці кабелі використовуються для з'єднання вузлів в локальній мережі і пристроїв мережевої інфраструктури, таких як комутатори, маршрутизатори і точки безпровідного доступу. Кожен тип з'єднання і відповідні пристрої мають певні вимоги до кабелів, передбачені стандартами фізичного рівня.

Коаксіальний кабель

Коаксіальний кабель має середню ціну, добре завадозахищений і застосовується для зв'язку на великі відстані (декілька кілометрів). Коаксіальний кабель називається так тому, що **два провідники в ньому використовують одну і ту ж вісь.**

Коаксіальний кабель складається з таких елементів:

- мідний провідник для передачі електричних сигналів;
- мідний провідник, оточений ізоляцією з еластичного пластика;
- ізолюючий матеріал, оточений мідним обплетенням або металевою фольгою.

Цей екран знижує кількість зовнішніх електромагнітних завад. Увесь кабель покритий кабельною оболонкою для захисту від невеликих фізичних ушкоджень.

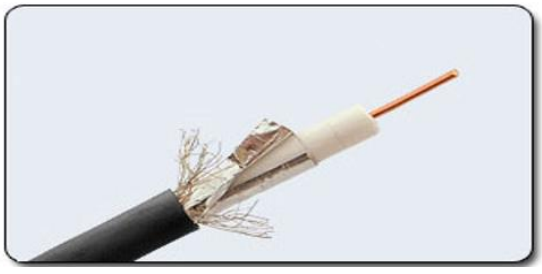


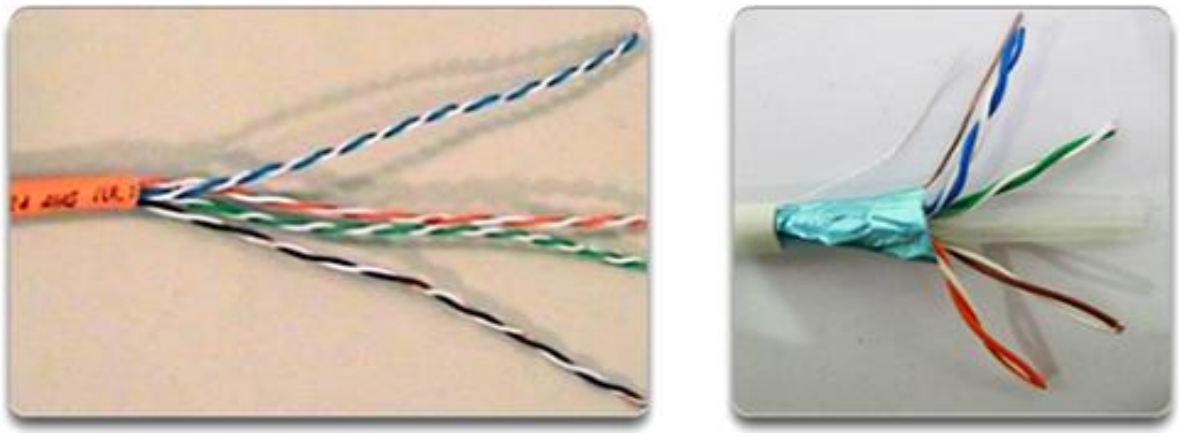
Рис.1.2. Коаксіальний кабель

Швидкість передачі інформації від 1 до 10 Мбіт/с, в деяких випадках може досягати 50 Мбіт/с. Коаксіальний кабель використовується для основної і широкосмугової передачі інформації.

Вита пара

Найбільш дешевим кабельним з'єднанням є вите двожильне дротяне з'єднання "вита пара" (англ. *twisted pair*). Підтримує передачу даних на відстань до 100 метрів. На більших відстанях сигнал через загасання не розпізнається; якщо передача даних на більшу відстань все-таки необхідна, потрібно скористатися повторювачем, або задіяти коаксіальний кабель. Перевагами є низька ціна і безпроблемна установка.

Неекранована вита пара складається з восьми дротів. Кожен дріт ізольований окремо; усі вісім дротів зібрано в чотири звиті пари. Завивка дротів запобігає перехресним перешкодам, що наводяться сусідніми парами і зовнішніми джерелами. Усі чотири пари поміщені в загальну оболонку.



а) неекранована вита пара (UTP) *б) екранована вита пара (STP)*

Рис.1.3 Вита пара

Для підвищення завадозахищеності інформації часто використовують **екрановану виту пару**, тобто виту пару, поміщену в екрануючу оболонку, подібно до екрану коаксіального кабелю. Це збільшує вартість витої пари і наближає її ціну до ціни коаксіального кабелю.

Вита пара витіснила коаксіальний кабель завдяки кільком явним перевагам. Кабель "витої пари" складається з восьми окремих дротів, що робить його гнучкішим ніж коаксіальний і, відповідно, полегшує його укладання. Мінімальний набір устаткування для мережі з витою парою включає такі елементи:

- мережеві адаптери (за числом об'єднуваних в мережу комп'ютерів);
- UTP-роз’ єми RJ-45;
- відрізки кабелю з роз'ємами RJ-45 на обох кінцях (за числом об'єднуваних комп'ютерів);
- комутатор, що має стільки UTP-портів з роз'ємами RJ-45, скільки необхідно об'єднати комп'ютерів.

Категорії кабелю

Існує декілька категорій кабелю вита пара, які нумеруються від **CAT 1** до **CAT 8.2**. Кабель вищої категорії зазвичай містить більше пар дротів і кожна пара має більше витків на одиницю довжини.

Категорії неекранованої витої пари описуються в стандарті EIA/TIA 568.

Оптоволоконні лінії

Найбільш дорогими є оптопровідники, або скловолоконні кабелі.

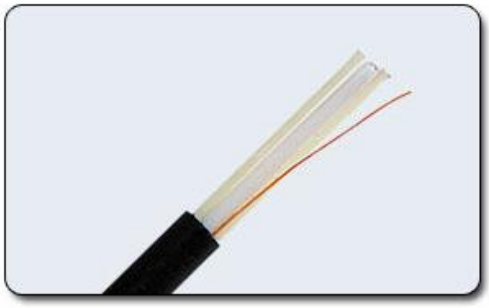


Рис.1.4 Оптоволокно

Допустиме віддалення більше 50 км. Зовнішня дія перешкод практично відсутня. На даний момент це найбільш дороге з'єднання. Застосовується там, де виникають електромагнітні поля перешкод або потрібна передача інформації на дуже великі відстані без використання повторювачів. Вони мають протипідслуховуючі властивості, оскільки техніка відгалужень в оптоволоконних кабелях дуже складна. Передача інформації йде по двох оптоволоконних кабелях, що передають сигнали в різні боки. Іноді використовуються двопровідні оптоволоконні кабелі, що містять два кабелі, в загальній зовнішній оболонці, але частіше – два поодинокі кабелі. Всупереч поширеній думці, вартість оптоволоконного кабелю не дуже висока (вона близька до вартості тонкого коаксіального кабеля). Правда, в цілому апаратура в даному випадку виявляється помітно дорожчою, оскільки вимагає використання дорогих оптоволоконних трансиверів.

Основними перевагами передачі даних по волоконно-оптичних лініях зв'язку є:

- Висока швидкість передачі даних – 3ГГц, в той час, як для мідного кабелю це значення складає не більше 500 Мгц.
- Нечутливість до електромагнітних завад.
- Відсутність електромагнітного випромінювання при передачі даних.
- Забезпечення гальванічної розв'язки між передавачем і приймачем даних.

Волоконно-оптичний кабель складається з наступних компонентів: оптичне волокно, оптичний екран, захисний екран.

Власне середовище передачі – оптичне волокно є скляною або пластмасовою жилою, товщина якої залежно від призначення кабелю може змінюватися в межах від одиниць до сотень мікрон.

Кабелі з діаметром волокна 10 мікрон називаються **одномодовими** за назвою режиму випромінювання передавального елементу – лазера. Кабелі з діаметром волокна 60 і більше мікрон називаються **багатомодовими.**

Одномодові волоконно-оптичні кабелі (*Single Mode Fiber* – SMF) складніші у виготовленні і експлуатації, проте, вони здатні забезпечувати велику дальність поширення інформаційного сигналу. Дешевші у виготовленні і зручніші в експлуатації багатомодові (*Multi Mode Fiber* – MMF) кабелі забезпечують меншу дальність поширення інформаційного сигналу.

Особливості безпровідного середовища

За допомогою надвисоких частот безпровідні середовища передачі даних переносять електромагнітні сигнали, які представляють біти передаваної інформації.

На відміну від мідних і оптоволоконних кабелів, безпровідна мережа в якості мережевого середовища не обмежується провідниками. Безпровідне середовище передачі даних характеризується найбільшою мобільністю. Кількість пристроїв безпровідного зв'язку постійно зростає. Саме тому безпровідна мережа стала середовищем для домашніх мереж. Також популярність безпровідних мереж швидко збільшується завдяки зростаючій пропускній спроможності мережі.

Проте безпровідна мережа має деякі **проблемні області:**

- **Зона покриття**. Безпровідні технології передачі даних добре працюють у відкритих просторах. Проте деякі конструкційні матеріали, що використовуються в будівлях, а також умови місцевості можуть обмежити зону покриття.

- **Перешкоди**. Безпровідна мережа сприйнятлива до перехресних перешкод, і її функціонування може бути порушене звичайними пристроями, наприклад, безпровідними телефонами, телевізійними приймачами, деякими типами флуоресцентних ламп, мікрохвильовими печами і іншими безпровідними комунікаціями.

- **Безпека.** Покриття безпровідного зв'язку не обмежується умовами доступу до середовища. Тому доступ до передачі можуть дістати неавторизовані користувачі і пристрої. Отже, засоби забезпечення мережевої безпеки є основною складовою адміністрування безпровідної мережі.

До безпровідних мереж застосовуються три стандарти передачі даних.

Стандарт IEEE 802.11: технологія безпровідних локальних мереж (WLAN), яка найчастіше називається Wi - Fi, використовує конкуруючу або недетерміновану систему з множинним доступом (CSMA/CA).

Стандарт IEEE 802.15: стандарт безпровідної персональної мережі, відомий, як Bluetooth; для передачі даних на відстанях від 1 до 100 метрів вимагає близького розташування двох пристроїв.

Стандарт IEEE 802.16: відомий як протокол широкосмугового радіозв'язку (WiMAX); використовує топологію "точка-точка" для забезпечення безпровідного широкосмугового доступу.

Хоча популярність безпровідних мереж для підключення настільних комп'ютерів зростає, мідні і оптоволоконні кабелі є найбільш популярним мережевим середовищем передачі даних на фізичному рівні. Існує ряд принципів побудови мереж на основі вище розглянутих компонентів. Такі принципи ще називають топологіями.

Топології комп’ютерних мереж

Топологія "зірка"

Це топологія мережі з явно виділеним центром, до якого підключаються всі інші абоненти. Обмін інформацією йде винятково через центральний комп'ютер, на який лягає більше навантаження, тому нічим іншим, крім мережі, він, як правило, займатися не може. Мережеве устаткування центрального абонента повинно бути істотно складнішим, ніж устаткування периферійних абонентів. Центральний комп'ютер найпотужніший, на нього покладають всі функції по керуванню обміном. Ніякі конфлікти в мережі з топологією «зірка» в принципі неможливі, тому що керування повністю централізоване.

Якщо говорити про стійкість зірки до відмов комп'ютерів, то вихід з ладу периферійного комп'ютера або його мережевого устаткування ніяк не відбивається на функціонуванні мережі, проте будь-яка відмова центрального комп'ютера робить мережу повністю непрацездатною. У зв'язку із цим повинні прийматися спеціальні заходи щодо підвищення надійності центрального комп'ютера і його мережевого обладнання.

Пропускна спроможність мережі визначається обчислювальною потужністю вузла і гарантується для кожної робочої станції. Колізій (зіткнень) даних не виникає.

Кабельне з'єднання досить просте, оскільки кожна робоча станція пов'язана з вузлом. Витрати на прокладення кабелів високі, особливо коли центральний вузол географічно розташований не в центрі топології.

При розширенні мережі не можуть бути використані раніше виконані кабельні зв'язки: до нового робочого місця необхідно прокладати окремий кабель з центру мережі.

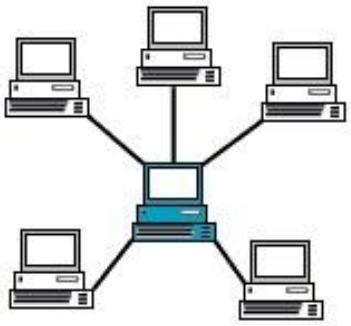


Рис. 1.5. Топологія "зірка"

Топологія «зірка» є найбільш швидкодіючою з усіх топологій комп’ютерних мереж, оскільки передача даних між робочими станціями проходить через центральний вузол (при його хорошій продуктивності) по окремих лініях, використовуваних тільки цими робочими станціями. Частота запитів передачі інформації від однієї станції до іншої невисока в порівнянні з тією, що досягається в інших топологіях.

Центральний вузол управління – файловий сервер реалізує оптимальний механізм захисту проти несанкціонованого доступу до інформації. Уся мережа може управлятися з її центру.

Топологія «кільце»

При кільцевій топології мережі робочі станції пов'язані одна з іншою по колу, тобто робоча станція 1 з робочою станцією 2, робоча станція 3 з робочою станцією 4 і так далі. Остання робоча станція пов'язана з першою. Комунікаційний зв'язок замикається в кільце. Прокладення кабелів від однієї робочої станції до іншої може бути досить складним і дорогим, особливо якщо географічне розташування робочих станцій далеко від форми кільця (наприклад, лінія).

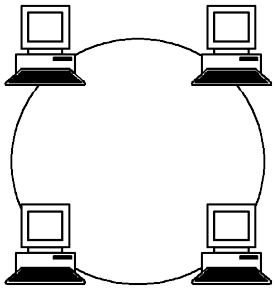


Рис. 1.6. Топологія "кільце"

Повідомлення циркулюють регулярно по колу. Робоча станція посилає за певною кінцевою адресою інформацію, заздалегідь отримавши з кільця запит. Пересилка повідомлень є дуже ефективною, оскільки більшість повідомлень можна відправляти по кабельній системі одне за іншим. Дуже просто можна зробити кільцевий запит на усі станції. Тривалість передачі інформації збільшується пропорційно кількості робочих станцій, що входять в обчислювальну мережу.

Основна проблема при кільцевій топології полягає в тому, що кожна робоча станція повинна брати активну участь в пересилці інформації, і у разі виходу з ладу хоч би однієї з них уся мережа не функціонує. Підключення нової робочої станції вимагає коротко термінового виключення мережі, оскільки під час установки кільце має бути розімкнене. Обмеження на протяжність обчислювальної мережі не існує, оскільки воно визначається виключно відстанню між двома робочими станціями.

Топологія «шина»

При шинній топології середовище передачі інформації представляється у формі комунікаційного шляху, доступного дня усіх робочих станцій, до якого вони усі мають бути підключені. Усі робочі станції можуть безпосередньо вступати в контакт з будь-якою робочою станцією, наявною в мережі.

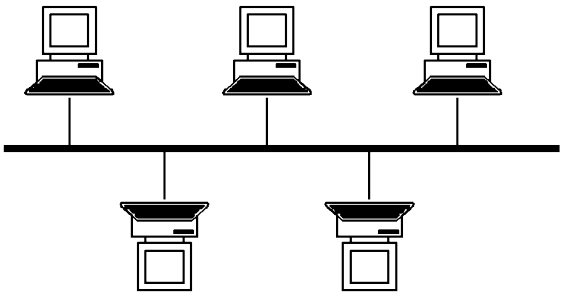


Рис. 1.7. Топологія "шина"

Робочі станції у будь-який час, без переривання роботи усієї мережі, можуть бути підключені до неї або відключені. Функціонування мережі не залежить від стану окремої робочої станції. Завдяки тому, що робочі станції можна підключати без переривання мережевих процесів і комунікаційного середовища, дуже легко прослуховувати інформацію.

Основні характеристики трьох найбільш типових топологій мереж передачі даних приведені в таблиці 1.1.

Табл.1.1. Основні характеристики топологій комп'ютерних мереж

ХАРАКТЕРИСТИКИ	**ТОПОЛОГІЇ КОМП'ЮТЕРНИХ МЕРЕЖ**		
	Зірка	**Кільце**	**Шина**
Вартість розширення	Незначна	Середня	Середня
Приєднання абонентів	Пасивне	Активне	Пасивне
Захист від відмов	Незначна	Незначна	Висока
Розмір системи	Довільний	Довільний	Обмежений
Захищеність від прослуховування	Хороша	Хороша	Незначна

ХАРАКТЕРИСТИКИ	ТОПОЛОГІЇ КОМП'ЮТЕРНИХ МЕРЕЖ		
	Зірка	**Кільце**	**Шина**
Вартість підключення	Незначна	Незначна	Висока
Поведінка системи при високих навантаженнях	Хороше	Задовільне	Погане
Можливість роботи в реальному режимі часу	Дуже хороша	Хороша	Погана
Розводка кабелю	Хороша	Задовільна	Хороша
Обслуговування	Дуже хороше	Середнє	Середнє

Топологія «дерево»

Комбінована, або деревовидна структура утворюється у вигляді комбінацій вище названих топологій комп'ютерних мереж. Основа дерева мережі (корінь) розташовується в точці, в якій збираються комунікаційні лінії інформації (гілки дерева).

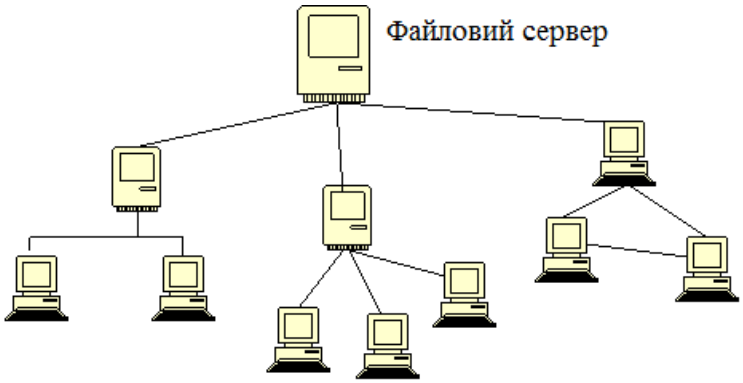


Рис. 1.8. Деревовидна структура мережі

Мережі з деревовидною структурою застосовуються там, де неможливе безпосереднє застосування базових мережевих структур в чистому вигляді. Для підключення великого числа робочих станцій відповідно до адаптерних плат застосовують мережеві підсилювачі і комутатори.

Знайомство з середовищем моделювання Cisco Packet Tracer

Середовище моделювання Packet Tracer дає можливість створювати мережеві топології з широкого спектру маршрутизаторів і комутаторів, робочих станцій і мережевих з'єднань типу Ethernet, Serial, ISDN. Ця функція може бути виконана як для навчання, так і для роботи, наприклад, щоб виконати налаштування мережі ще на етапі планування або щоб створити копію робочої мережі з метою усунення несправності. Для запуску Cisco Packet Tracer необхідно запустити виконуваний файл **PacketTracer.exe.** Загальний вигляд програми зображено на рис.1.9.

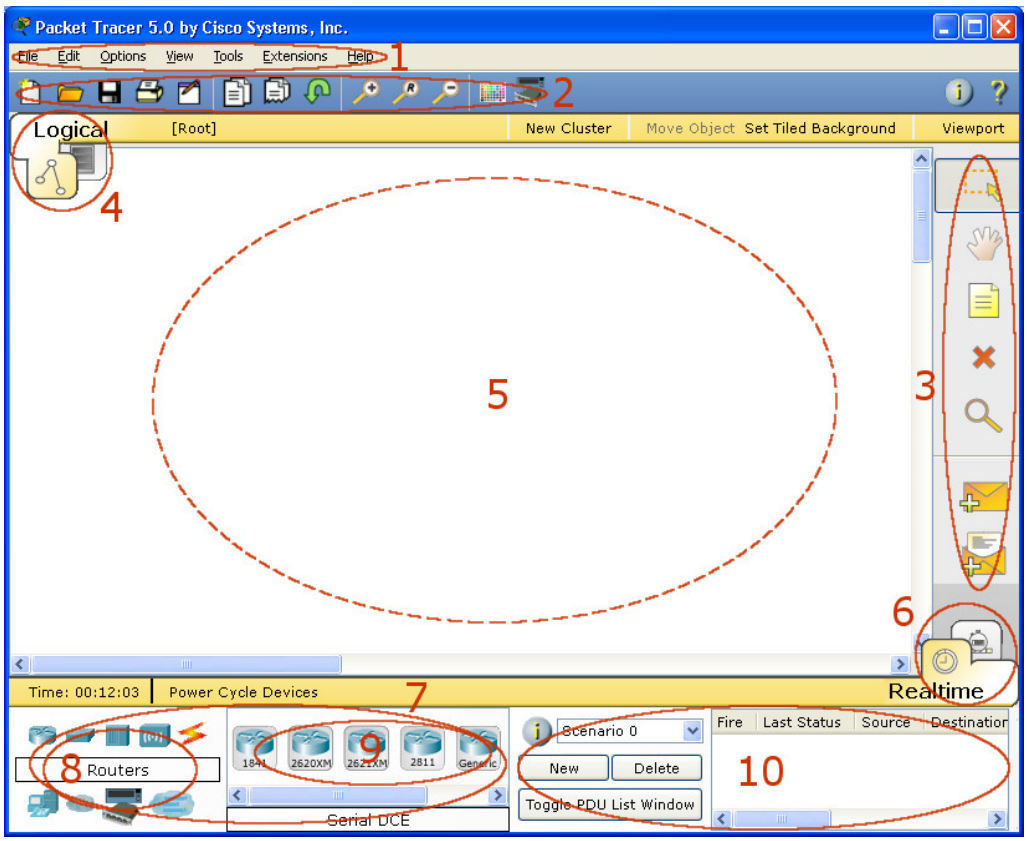


Рис.1.9. Загальний вигляд програми Packet Tracer

Робоча зона вікна програми складається з наступних елементів:

1. **Menu Bar** – панель, яка містить меню File, Edit, Options, View, Tools, Extensions, Help.
2. **Main Tool Bar** містить графічні зображення ярликів для доступу до команд меню File, Edit, View і 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 кластера.
5. **Workspace** – область, в якій відбувається створення мережі, проводяться спостереження за симуляцією, є видимою різна інформація та статистика.
6. **Realtime/Simulation Bar** – за допомогою закладок цієї панелі можна перемикатися між режимом Realtime і режимом Simulation. Вона також містить кнопки, що відносяться до Power Cycle Devices, кнопки Play Control та перемикач Event List в режимі Simulation.
7. **Network Component Box** – область, в якій вибираються пристрої і зв'язки для розміщення їх на робочому просторі. Вона містить область Device - Type Selection і область Device - Specific Selection.
8. **Device - Type Selection Box** – область містить доступні типи пристроїв і зв'язків в Packet Tracer. Область Device - Specific Selection змінюється залежно від вибраного пристрою.
9. **Device - Specific Selection Box** – область використовується для вибору конкретних пристроїв і з'єднань, необхідних для побудови в робочому просторі мережі.
10. **User Created Packet Window** – це вікно управляє 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 вибраного пристрою. Після цього треба 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 замовчуванням.

Для швидкого створення декількох екземплярів одного і того ж пристрою треба, 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 додавання копій пристрою.

У Packet Tracer представлені наступні типи пристроїв :

- маршрутизатори;
- комутатори;
- кінцеві пристрої – ПК, сервери, принтери, IP -телефони;
- безпровідні пристрої: точки доступу і безпровідні маршрутизатори;
- інші пристрої - хмара, DSL -модем і кабельний модем тощо.

Додамо необхідні елементи в робочу область програми так, як показано на рис.1.10.

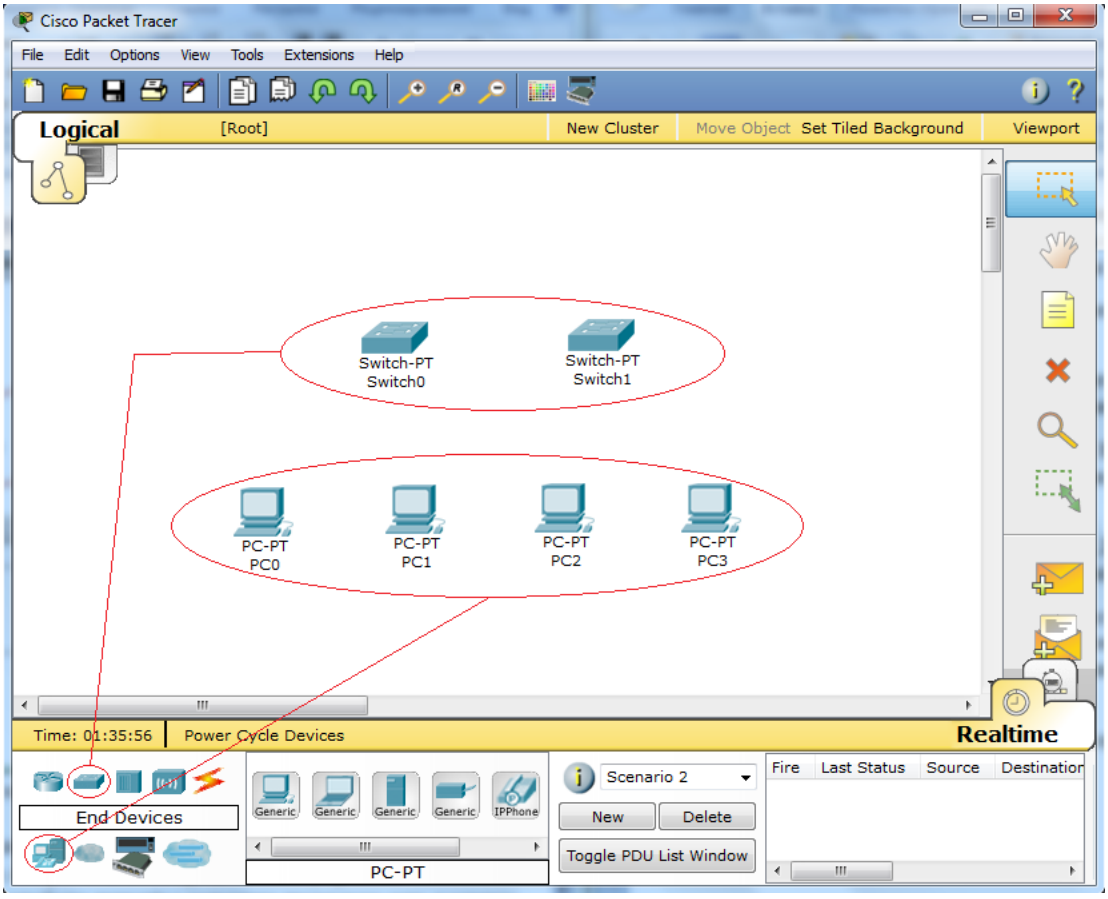


Рис.1.10. Додавання елементів мережі

При додаванні кожного елементу користувач має можливість дати йому ім'я і встановити необхідні параметри. Для цього необхідно натиснути на потрібний елемент лівою кнопкою миші і в діалоговому вікні пристрою перейти до вкладки **Config**.

Діалогове вікно властивостей кожного елементу має дві вкладки: **Physical** – містить графічний інтерфейс пристрою і дозволяє симулювати роботу з ним на фізичному рівні. **Config** – містить усі необхідні параметри для налаштування пристрою і має зручний для цього інтерфейс.

Залежно від пристрою, властивості можуть мати додаткову вкладку для управління роботою вибраного елементу: **Desktop** (якщо вибраний кінцевий пристрій) або **CLI** (якщо вибраний маршрутизатор) і так далі. Для видалення непотрібних пристроїв з робочої області програми використовується кнопка **Delete** (Del). Зв'яжемо додані елементи ми за допомогою сполучних зв'язків. Для цього необхідно вибрати вкладку **Connections** з панелі **Network Component Box**. Ми побачимо усі можливі типи з'єднань між пристроями. Виберемо відповідний тип кабелю. Покажчик миші зміниться на курсор "connection" (має вигляд роз'єму). Натиснемо на першому пристрої і виберемо відповідний інтерфейс, з яким треба виконати з'єднання, а потім натиснемо на другий пристрій, виконавши ту ж операцію. Можна також з'єднати за допомогою **Automatically Choose Connection Type** (автоматично сполучає елементи в мережі). Виберемо і натиснемо на кожному з пристроїв, які треба з'єднати. Між пристроями з'явиться кабельне з'єднання, а індикатори на кожному кінці покажуть статус з'єднання (для інтерфейсів, які мають індикатор).

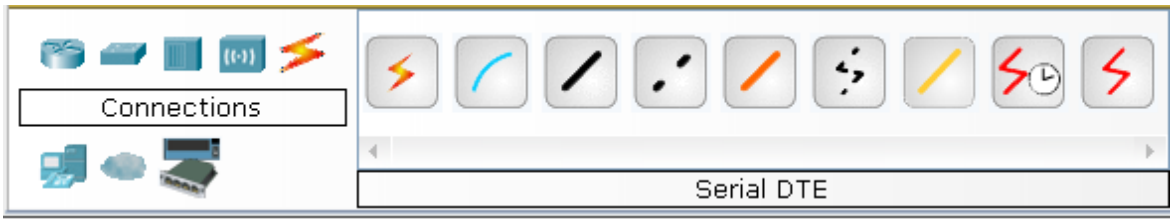


Рис.1.11. Підтримувані в Packet Tracer типи кабелів

Packet Tracer підтримує широкий діапазон мережевих з'єднань (див. таблицю 1.2). Кожен тип кабелю може бути сполучений лише з певними типами інтерфейсів.

Табл.1.2. Типи з'єднань в Packet Tracer

Тип кабелю	Опис
Console	Консольне з'єднання може бути виконане між ПК і маршрутизаторами або комутаторами. Мають бути виконані вимоги для роботи консольного сеансу з ПК: швидкість з'єднання з обох боків має бути однакова.
Copper Straight - through	Цей тип кабелю є стандартним середовищем передачі Ethernet для з'єднання пристроїв, який функціонує на різних рівнях OSI. Він має бути сполучений з наступними типами портів: мідний 10 Мбіт/с (Ethernet), мідний 100 Мбіт/с (Fast Ethernet) і мідний 1000 Мбіт/с (Gigabit Ethernet).
Copper Cross - over	Цей тип кабелю є середовищем передачі Ethernet для з'єднання пристроїв, які функціонують на однакових рівнях OSI. Він може бути сполучений з наступними типами портів : мідний 10 Мбіт/с (Ethernet), мідний 100 Мбіт/с (Fast Ethernet) і мідний 1000 Мбіт/с (Gigabit Ethernet).
Fiber	Оптоволоконне середовище використовується для з'єднання між оптичними портами (100 Мбіт/с або 1000 Мбіт/с).
Phone	З'єднання через телефонну лінію може бути здійснене тільки між пристроями, що мають модемні порти. Стандартне представлення модемного з'єднання – це кінцевий пристрій (наприклад, ПК), що додзвонюється в мережеву хмару.

Coaxial	Коаксіальне середовище використовується для з'єднання між коаксіальними портами, такі як кабельний модем, сполучений з хмарою.
Serial DCE and DTE	З'єднання через послідовні порти, часто використовуються для зв'язків WAN. Для налаштування таких з'єднань необхідно встановити синхронізацію на стороні DCE - пристрою. Сторону DCE можна визначити по маленькій іконці "годинника" поряд з портом. При виборі типу з'єднання Serial DCE, перший пристрій, до якого застосовується з'єднання, стає DCE -пристроєм, а друге – автоматично стане стороною DTE. Можливе і зворотне розташування сторін, якщо вибраний тип з'єднання Serial DTE.

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

Packet Tracer дає нам можливість симулювати роботу з інтерфейсом командного рядка (**CLI – Command Line Interface**) операційної системи IOS, встановленої на усіх комутаторах і маршрутизаторах Cisco. Підключившись до пристрою, ми можемо працювати з ним так, як ми працюємо з консоллю реального пристрою. Симулятор забезпечує підтримку практично усіх команд, доступних на реальних пристроях.

Підключення до CLI комутаторів або маршрутизаторів можна провести, натиснувши на необхідний пристрій і перейшовши у вікно властивостей до вкладки CLI.

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

Робота з файлами в симуляторі

Packet Tracer дає можливість користувачеві зберігати конфігурацію пристроїв, таких як маршрутизатори або комутатори, в текстових файлах. Для цього необхідно перейти до властивостей необхідного пристрою і у вкладці **Config** натиснути на кнопку **"Export"** для експорту конфігурації **Startup Config** або **Running Config**. Так отримаємо діалогове вікно для збереження необхідної конфігурації у файл, який матиме розширення *.txt . Текст файлу з конфігурацією пристрою **running, - config.txt** (ім'я за замовчуванням), аналогічний тексту інформації отриманої при використанні команди **show running - config** в IOS -пристроях.

Конфігурація кожного пристрою зберігається в окремому текстовому файлі. Користувач також має можливість змінювати конфігурацію в збереженому файлі вручну за допомогою довільного текстового редактора. Для надання пристрою збережених або відредагованих налаштувань треба у вкладці **Config** натиснути кнопку **"Load."**. для завантаження необхідної конфігурації **Stàrtup Config** або кнопку **"Merge"** для завантаження конфігурації **Running Config**.

Розмір реальних мереж значно перевищує розмір більшості мереж, з якими ми будем працювати у рамках цього курсу. Щоб побачити мережу в повному масштабі, потрібно буде змінити розмір вікна Packet Tracer. При необхідності за допомогою інструментів масштабування можна налаштувати розмір вікна Packet Tracer.

Доступ до розділів довідки Packet Tracer, учбових відеороликів і інтерактивних матеріалів

Доступ до розділів довідки програми Packet Tracer можна отримати двома способами:

1) клацнути знак питання в правому верхньому кутку меню панелі інструментів;

2) відкрити меню **Help** і вибрати команду **Contents**.

Щоб відкрити учбові відеоролики Packet Tracer, виберіть меню **Help > Tutorials**. У цих відеоматеріалах наочно представлена інформація з розділів Help, а також продемонстровані різні можливості програмного забезпечення Packet Tracer. Прогляньте відеоролик **Interface Overview** (Огляд інтерфейсу) у розділі **Getting Started** (Початок роботи) навчальних посібників.

Прогляньте відеоролик **Simulation Environment** (Середовище моделювання) у розділі **Realtime and Simulation Modes** (Режими реального часу і моделювання).

Знайдіть навчальний посібник "**Configuring Devices Using the Desktop Tab**" (Налаштування пристроїв за допомогою вкладки "Desktop"). Подивіться першу частину навчального посібника і дайте відповідь на наступне питання: які дані можна налаштувати у вікні "IP Configuration"? Вибравши DHCP або Статична адреса, можна налаштувати IP - адресу, маску підмережі, шлюз за замовчуванням та DNS -сервер.

Перемикання між режимами реального часу і моделювання

Знайдіть слово **Realtime** в правому нижньому кутку інтерфейсу Packet Tracer. У режимі реального часу (Realtime) мережа завжди діє як реальна незалежно від того, чи працюєте ви з нею або ні. Налаштування застосовуються в реальному часі, і мережа реагує на них в режимі, близькому до реального часу.

Клацніть вкладку безпосередньо за вкладкою **Realtime**, щоб перейти в режим **Simulation** (Моделювання). У режимі моделювання мережа відображається з нижчою швидкістю, дозволяючи спостерігати за шляхами отримання даних і перевіряти пакети даних. Відкрийте панель моделювання і натисніть кнопку **Auto capture/Play** (Автоматичне захоплення/відтворення). Тепер ви повинні бачити пакети даних, представлені конвертами різного кольору, які рухаються між пристроями.

Натисніть кнопку **Auto capture/Play** ще раз, щоб припинити моделювання.

Натисніть кнопку **Capture/Forward**, щоб включити покрокове моделювання. Натисніть кнопку ще кілька разів, щоб побачити процес у дії. У топології мережі ліворуч клацніть один з конвертів на проміжному пристрої і вивчите його вміст.

Перемикання між логічним і фізичним представленням

Знайдіть слово **Logical** в лівому верхньому куті інтерфейсу Packet Tracer. Зараз ви знаходитеся в робочій області Logical; її ви будете її використовуватие найчастіше при роботі з мережами (побудова мереж, налаштування, вивчення і усунення неполадок в них тощо).

Клацніть вкладку під областю **Logical**, щоб перемкнутися на робочу область **Physical** (Фізична). Робоча область **Physical** містить фізичні розміри логічної топології мережі. Вона дозволяє оцінити масштаб і розташування елементів (наприклад, як мережа може виглядати в реальному середовищі).

Вказівки щодо виконання завдання

Додамо на робочу область середовища моделювання два комутатори Switch-PT. За замовчуванням вони мають імена Switch0 та Switch1. Додамо в робоче поле чотири комп'ютери з іменами за замовчуванням PC0, PC1, PC2, PC3. З'єднаємо пристрої в мережу Ethernet, як показано на рис.1.12. Збережемо створену топологію, натиснувши кнопку **Save** (у меню **File -> Save**).

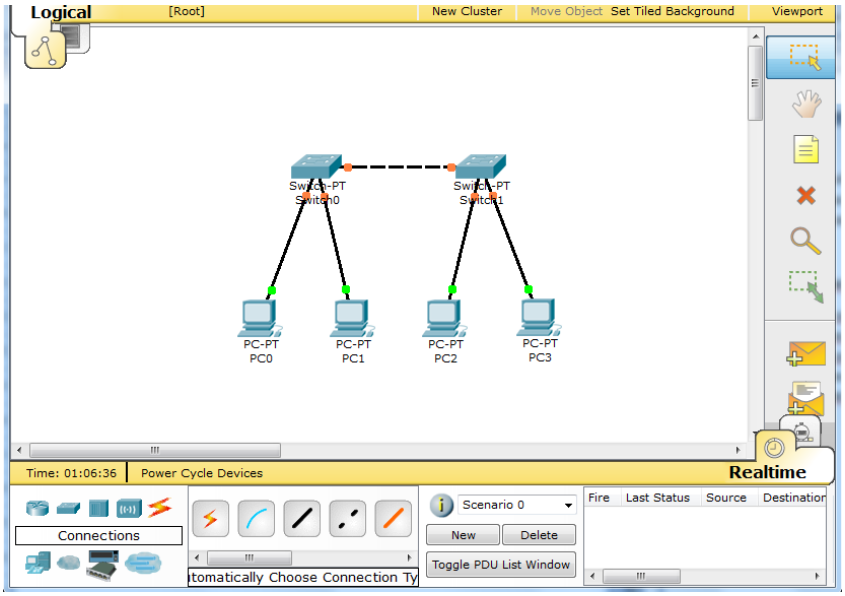


Рис.1.12. Модель простої мережі, що складається з двох комутаторів та чотирьох вузлів

Відкриємо властивості пристрою PC0, натиснувши на його зображення. Перейдемо до вкладки **Desktop** і симулюємо роботу **run**, натиснувши **Command Prompt**.

Список команд отримаємо, якщо введемо "**?**" і натиснемо Enter. Для конфігурації комп'ютера скористаємося командою **ipconfig** з командного рядка, наприклад:

ipconfig 192.168.1.2 255.255.255.0

IP адресу і маску мережі також можна вводити в зручному графічному інтерфейсі пристрою (рис.1.13). Поле DEFAULT GATEWAY – адреси шлюзу, поки що не потрібні, оскільки створювана мережа не вимагає маршрутизації.

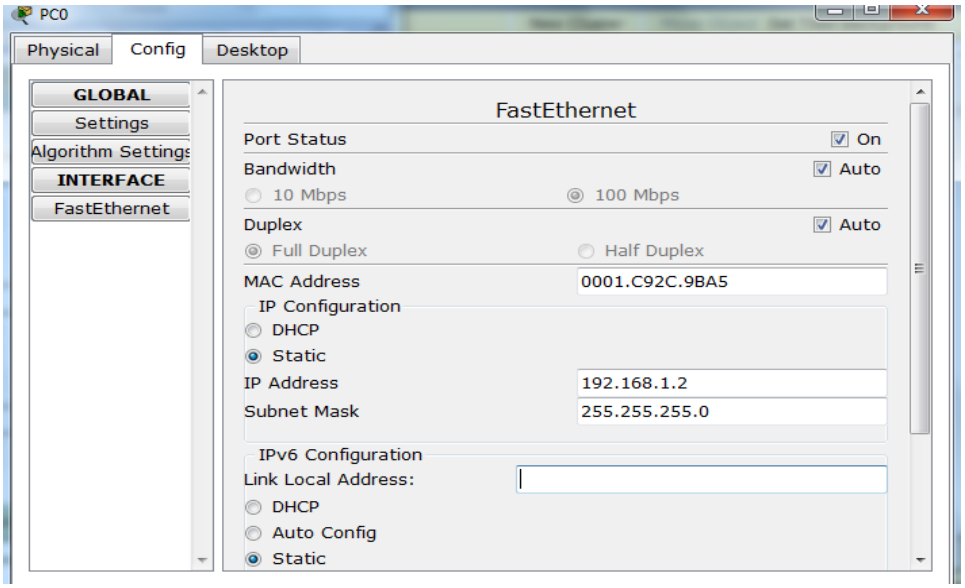


Рис.1.13. Налаштування вузла

Аналогічно налаштовуємо кожен комп'ютер.

Пристрій	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

На кожному комп'ютері подивимося призначені адреси командою **ipconfig** без параметрів.

У Packet Tracer передбачений режим моделювання, в якому детально описується і показується, як працює утиліта **ping**. Тому необхідно перейти в цей режим, натиснувши на однойменний значок в нижньому лівому кутку робочої області, або по комбінації клавіш Shift+S. Відкриється "Панель моделювання", в якій відображуватимуться усі події, пов'язані з виконання **ping** -процесу.

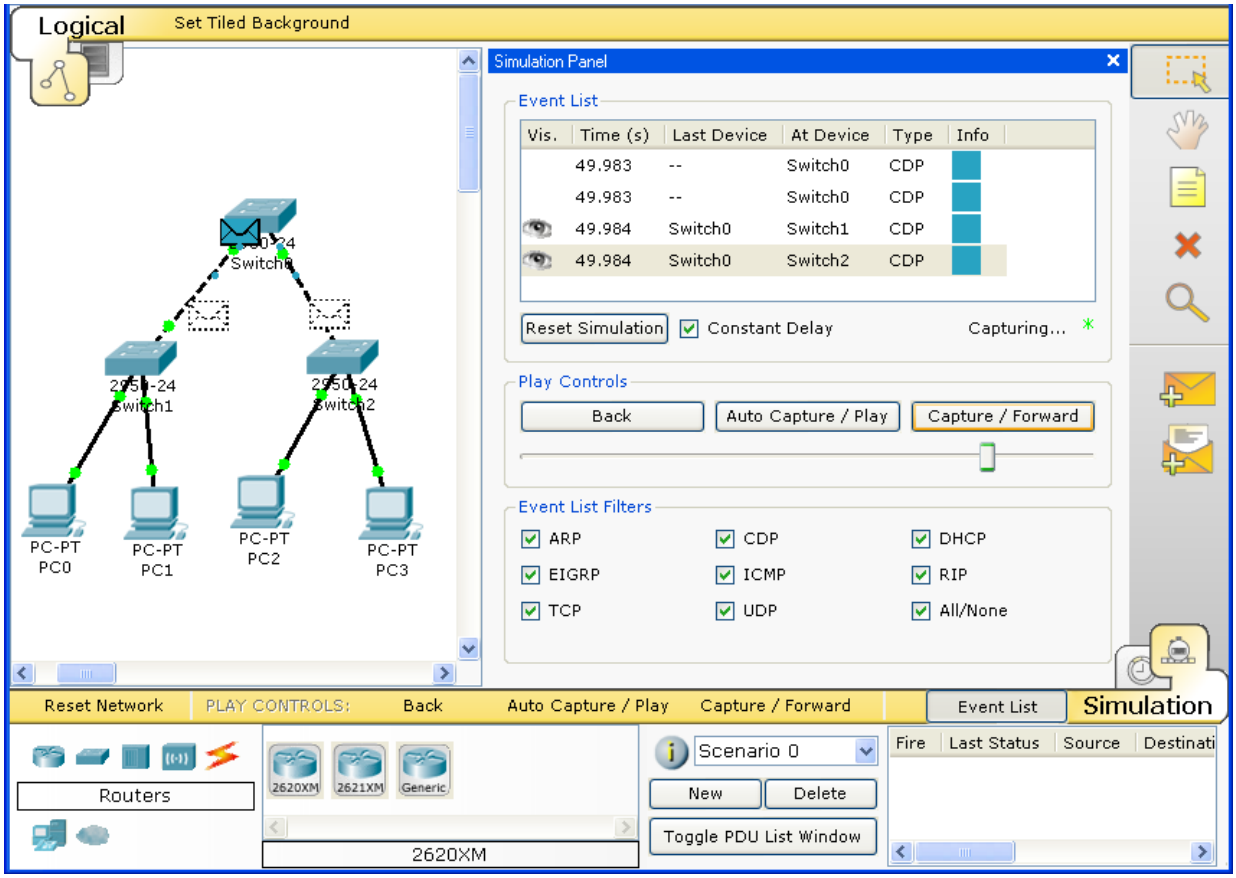


Рис.1.14. Панель моделювання в Packet Tracer

Тепер необхідно повторити запуск **ping**-процесу. Після його запуску можна згорнути "Панель моделювання", щоб на схемі спроектованої мережі спостерігати за відправкою/прийманням пакетів. Кнопка "Автоматично" має на увазі моделювання усього **ping**-процесу в єдиному процесі, тоді як "Покроково" дозволяє відображувати його покроково. Щоб упізнати інформацію, яку несе в собі пакет, його структуру, досить натиснути правою кнопкою миші на кольоровий квадрат в графі "Інформація".

Моделювання припиняється або при завершенні **ping**-процесу, або при закритті вікна "Редагування" відповідної робочої станції.

Якщо усе зроблено правильно, ми зможемо пропінгувати будь-який ПК з будь-якого комп'ютера. Наприклад, зайдемо на комп'ютер PC3 і пропінгуємо комп'ютер PC0. Ми повинні побачити звіт про пінг подібний до рис.1.15.

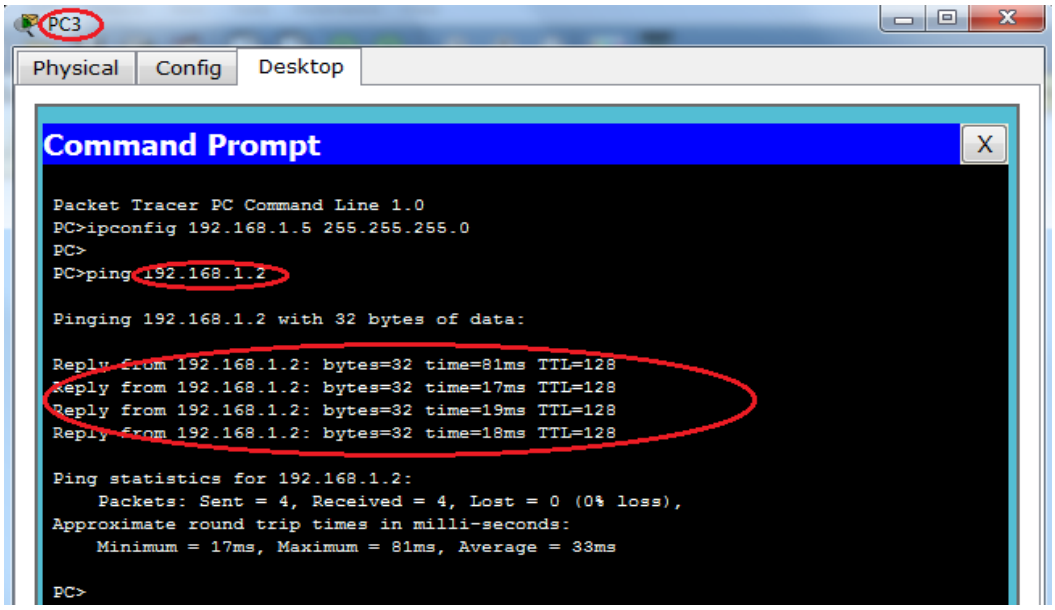


*Рис.1.15. Виконання команди **ping** у командному рядку*

У "Режимі симуляції" можна не лише відстежувати використовувані протоколи, але і побачити, на якому з семи рівнів моделі OSI цей протокол задіяний (рис.1.16).

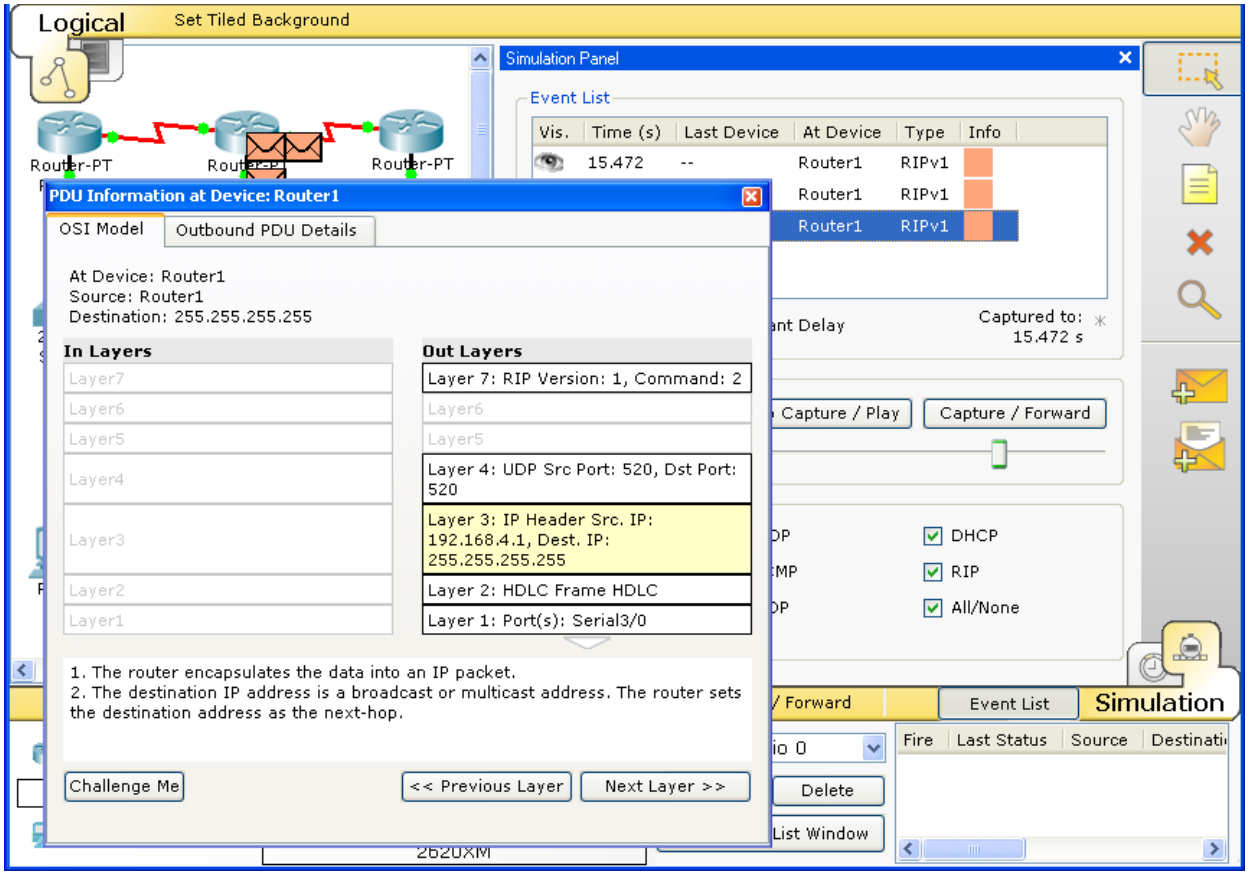


Рис.1.16. Аналіз семирівневої моделі OSI в Cisco Packet Tracer

Завдання для лабораторної роботи:

1. Створіть топологію мережі, зображену на рис. 1.17.

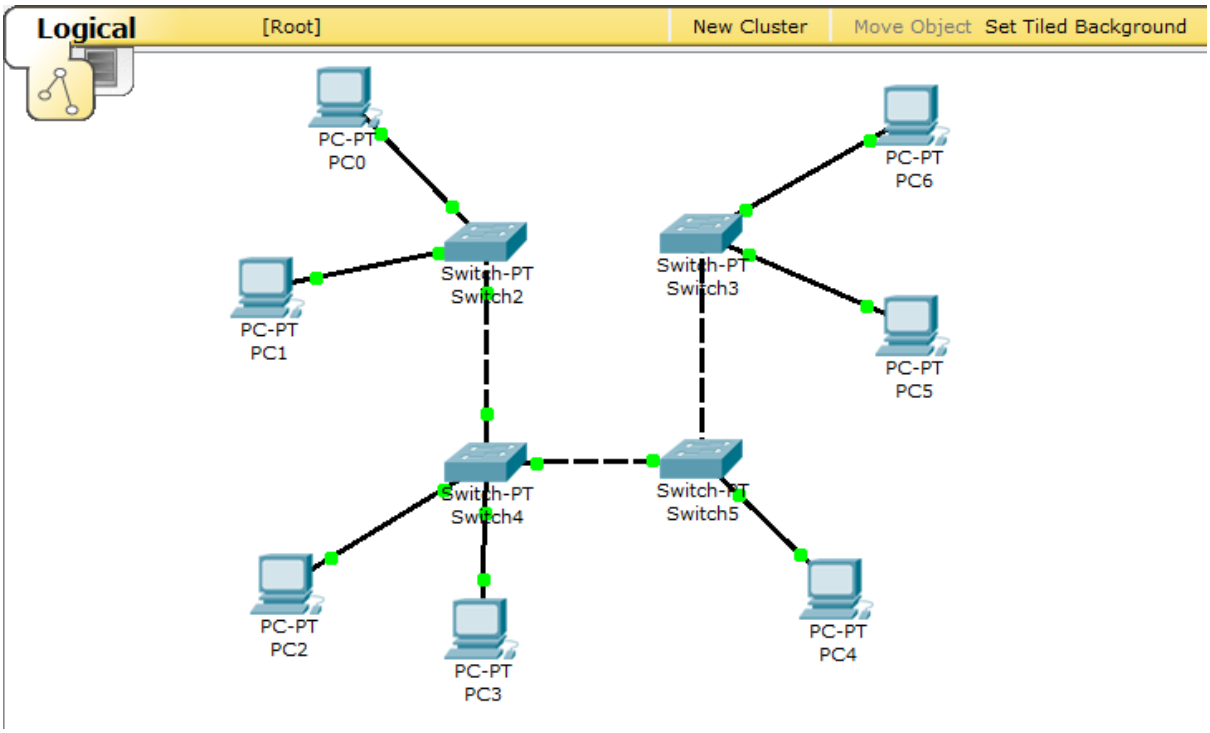


Рис. 1.17. Топологія мережі для дослідження

2. Призначте комп'ютерам адреси, згідно з варіантом по списку v за таблицею:

Пристрій	IP ADDRESS	SUBNET MASK
PC0	v*10. v.1.1	255.255.255.0, якщо v%2==0 255.255.0.0, якщо v%2==1
PC1	v*10. v.1.2	
PC2	v*10. v.1.3	
PC3	v*10. v.1.4	
PC4	v*10. v.1.5	
PC5	v*10. v.1.6	
PC6	v*10. v.1.7	

Наприклад, для варіанту 5 (v=5) і комп'ютера PC0 маємо IP ADDRESS 50.5.1.1, маска 255.255.0.0. Якщо зроблено усе правильно, ви зможете пропінгувати будь-який комп'ютер з будь-кого іншого комп'ютера.

3. Виконайте утиліту **ping**, згідно таблиці:

Варіант v%	Пінг з	Пінг в
1	PC1	PC6
2	PC2	PC7
3	PC3	PC1
4	PC4	PC2
5	PC5	PC3

6	PC6	PC4
7	PC7	PC5
8	PC7	PC5
9	PC1	PC6
10	PC2	PC7
11	PC3	PC1
12	PC4	PC2
13	PC5	PC3
14	PC6	PC4
15	PC1	PC6
16	PC2	PC7
17	PC3	PC1
18	PC4	PC2
19	PC5	PC3
20	PC6	PC4
21	PC7	PC5
22	PC1	PC6
23	PC2	PC7
24	PC3	PC1
25	PC4	PC2

4. У "Режимі симуляції" відстежте рух пакетів і використовувані протоколи.

а) У "Режим симуляції" розглянути і пояснити процес обміну даними по протоколу ICMP між пристроями (виконавши команду **ping** з одного комп'ютера на інший), пояснити роль протоколу ARP в цьому процесі. Детальне пояснення включити в звіт.

б) Переконатися в досяжності усіх об'єктів мережі по протоколу IP.

Вимоги до оформлення звіту

Звіт має включати:

1. Титульний аркуш.
2. Індивідуальне завдання на лабораторну роботу (скріншот топології мережі згідно та адресація вузлів згідно варіанту).
3. Хід роботи. Цей розділ складається з послідовного опису значущих виконуваних кроків (з вказівкою їх суті), пояснення роботи команди **ping** і вмісту протоколів.
4. Висновки.

Питання для самоперевірки

1. Для чого використовується мережева карта?
2. Що таке MAC-адреса, яку вона має форму запису?
3. Які типи мережевого середовища ви знаєте?
4. Які є типи мідних кабелів?
5. Яка будова і особливості використання коаксіального кабелю?
6. Яка будова і особливості використання витої пари? Які є типи витої пари?
7. Яка будова і особливості використання оптоволоконних ліній?
8. Які основні характеристики безпровідного середовища?
9. Які ви знаєте безпровідні стандарти передачі даних?
10. Які типи топологій мереж ви знаєте?
11. Які особливості топології "зірка"?
12. Які особливості топології «кільце»?
13. Які особливості топології «шина»?
14. Які особливості топології «дерево»?

15. Назвіть основні порівняльні характеристики топологій комп'ютерних мереж.
16. Які типи мережевих з'єднань в Packet Tracer ви знаєте?
17. Які особливості мережевого з'єднання через послідовні порти?
18. Як відбувається перемикання між логічним і фізичним представленням в Packet Tracer?
19. Яке призначення утиліти **ipconfig**?
20. Яке призначення утиліти **ping**?
21. Яке призначення протоколу ICMP?
22. Яке призначення протоколу ARP?

Рекомендована література

1. Топології комп'ютерних мереж // Електронний ресурс. Режим доступу: http://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6
2. Бездротові технології передачі даних WI-FI, BLUETOOTH ТА ZIGBEE // Електронний ресурс. Режим доступу: http://radap.kpi.ua/radiotechnique/article/viewFile/502/487-radap.pdf
3. Комп'ютерні мережі та телекомунікації: навч. посіб. / В. А. Ткаченко, О. В. Касілов, В. А. Рябик. – Харків : НТУ "ХПІ", 2011. – 224 с.
4. Городецька, О. С. Комп'ютерні мережі. Навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. − Вінниця : ВНТУ, 2015. − 128 с.
5. Еталонна модель OSI // Електронний ресурс. Режим доступу: http://bourabai.kz/lan/03.html
6. Протокол ICMP // Електронний ресурс. Режим доступу: http://iptcp.net/protokol-icmp.html
7. ARP // Електронний ресурс. Режим доступу: https://uk.wikipedia.org/wiki/ARP

ЛАБОРАТОРНА РОБОТА №2. ВІДСТЕЖУВАННЯ МАРШРУТУ ДО ВІДДАЛЕНОГО СЕРВЕРУ З КОМАНДНОГО РЯДКА, ПРОГРАМНИМИ ТА ВЕБ-ЗАСОБАМИ

Мета роботи: навчитися перевіряти можливість з'єднання з віддаленим сервером, навчитися визначати маршрути до віддаленого серверу, використовуючи командний рядок та різні програмні та веб-засоби.

Теоретичні відомості

Програмне забезпечення для трасування маршруту – це утиліта, що містить списки мереж, по яким повинні пройти дані від відправляючого кінцевого пристрою користувача до віддаленої мережі призначення.

Для запуску процесу трасування в командний рядок необхідно ввести наступне:

tracert <destination network name or end device address>

(для операційних систем сімейства Microsoft Windows)

або

traceroute <destination network name or end device address>

(для Unix подібних систем)

Утиліти трасування маршруту дозволяють визначати шляхи або маршрути, а також обчислювати час затримки в IP - мережі. Для виконання цієї функції існує декілька засобів.

Інструмент **traceroute** (або **tracert**) використовується для пошуку та усунення неполадок в мережі. Він відображає список пройдених маршрутизаторів і дозволяє визначити, який шлях використовувався для досягнення пункту призначення в одній мережі або під час переходу між кількома мережами. Кожен маршрутизатор – це точка з'єднання двох мереж, через яку пересилаються пакети даних. Кількість маршрутизаторів є кількістю "переходів", здійснених даними на шляху від джерела до місця призначення.

Список, що відображується, допоможе визначити, які проблеми з потоком даних виникають при спробі доступу до якого-небудь сервісу, наприклад веб-сайту. Також список може бути використаний при виконанні завантаження даних. Якщо один і той же файл доступний на декількох веб-сайтах (дзеркалах), можна перевірити маршрут для кожного дзеркала і вибрати найбільш швидкий варіант.

Два трасування маршруту, виконані між одними і тими ж вузлами джерела і адресата, але в різний час, можуть дати різні результати. Це може бути пов'язано з "повнозв'язним" характером взаємно підключених мереж, що складаються з можливостей Інтернету і протоколів Інтернету вибирати різні кабельні канали для відправки пакетів. Засоби трасування маршруту з використанням командного рядка зазвичай закладені в операційну систему кінцевого пристрою (вузла).

Інші інструменти, такі як **VisualRoute™**, є пропрієтарними програмами і дозволяють отримувати детальнішу інформацію. **VisualRoute** формує графічне відображення маршруту, використовуючи доступну інформацію в мережі.

Для виконання цієї лабораторної роботи використовується програма **VisualRoute**. Якщо на вашому комп'ютері програма VisualRoute не встановлена, завантажите її за посиланням:

http://www.visualroute.com/download.html

Якщо із завантаженням або установкою програми **VisualRoute** виникнуть проблеми, переконайтеся, що виконується завантаження **Lite Edition**.

VisualRoute Lite Edition	Windows XP\2003\Vista\7	4.0Mb	Download
	Mac OS X (dmg) 10.3+, universal binary	2.0Mb	Download

Вказівки щодо виконання завдання

Для виконання лабораторної роботи використовується один ПК (Windows 7, Vista або XP з виходом в Інтернет). Використовуючи інтернет-підключення і три різні утиліти трасування маршруту, необхідно відстежити шлях проходження пакетів даних через інтернет до мереж призначення. Для цього використовується комп'ютер, підключення до Інтернету і доступ до командного рядка. Спочатку використаємо утиліту "**tracert**", вбудовану в ОС Windows, потім **веб-засоби** для трасування маршруту (http://www.subnetonline.com/pages/network-tools/online-traceroute.php) і, нарешті, програму **VisualRoute**.

Примітка. Безкоштовні програми, такі як **VisualRoute**, швидко застарівають. Якщо на момент виконання цієї лабораторної роботи версія **VisualRoute Lite Edition** не доступна, відкрийте будь-яку пошукову систему і введіть в поле пошуку "завантажити visual traceroute tool".

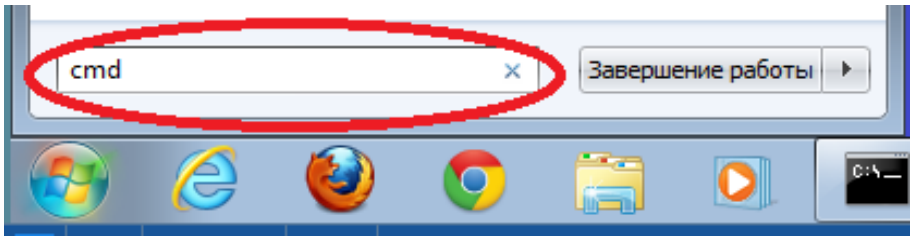
У деяких учбових закладах ехо-відповіді ICMP (Internet Control Message Protocol), які використовуються ехо-запитами за допомогою команди **ping** і командами трасування, відключені. Перш ніж починати виконувати це завдання, перевірте відсутність місцевих обмежень, пов'язаних з датаграмами ICMP. Ця робота припускає, що датаграми ICMP не обмежені якими-небудь місцевими політиками безпеки.

Перевірка підключення до мережі за допомогою ехо-запиту за допомогою команди ping

Перевіримо, чи доступний віддалений сервер. Для трасування маршруту до віддаленої мережі використовуваний ПК має бути підключений до Інтернету.

Спочатку скористаємося ехо-запитом за допомогою команди **ping**. **Ехо-запит за допомогою команди ping – це засіб для перевірки доступності вузла**. Пакети інформації пересилаються віддаленому вузлу з вимогою відповіді. Локальний ПК визначає, чи отримана відповідь для кожного пакету, і розраховує, який час зайняла пересилка цих пакетів по мережі. Назва «ехо-запит» прийшла з області активної гідролокації, де вона означала звуковий сигнал, що відправляється під воду і відбивається від дна або інших кораблів.

Натисніть кнопку *Пуск* на екрані комп'ютера, введіть команду **cmd** в поле *Знайти програми і файли* і натисніть клавішу ВВЕДЕННЯ.



У командному рядку введіть **ping www.cisco.com.**

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

У першому рядку отриманих даних відображується повне доменне ім'я (FQDN) **e144.dscb.akamaiedge.net**. Потім слідує IP-адреса **23.1.48.170**. Веб-вузли компанії Cisco, що містять одну і ту ж інформацію, розміщуються на різних серверах (так званих дзеркалах) по всьому світу. Це означає, що ім'я FQDN і IP-адреса відрізнятимуться залежно від вашого місцезнаходження.

Візьмемо частину отриманих результатів:

```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

З неї видно, що були відправлені чотири ехо-запити за допомогою команди **ping**, на кожний з яких була отримана відповідь. Відповідь поступила на усі ехо-запити за допомогою команди **ping**, значить, втрат пакетів немає (0 % втрат). В середньому для передачі пакетів по мережі потрібно 54 мс (мілісекунди).

Примітка. Якщо час очікування першого пакету ICMP витік, це може статися через те, що ПК перетворить адресу призначення. Цього не станеться, якщо ехо-запит за допомогою команди **ping** повториться при кешуванні адреси.

Від втрати пакетів або повільного мережевого підключення в першу чергу страждає якість потокового відео і онлайн-ігр. Щоб визначити швидкість інтернет-підключення точніше, можна відправити не 4 ехо-запити за допомогою команди **ping**, передбачених за замовчуванням, а 100. Для цього використовується вказана нижче команда.

```
C:\>ping -n 100 www.cisco.com
```

Результат виглядатиме таким чином.

```
Ping statistics for 23.45.0.170:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 53ms, Average = 49ms
```

Тепер розглянемо випадок, коли усі ехо-запити за допомогою команди **ping** були відправлені з комп'ютера, розташованого в США на веб-сайти регіонального інтернет-реєстратора (RIR), розташовані в різних частинах світу.

Африка:
C:\> **ping www.afrinic.net**

```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

Австралія:
C:\> **ping www.apnic.net**

```
C:\>ping www.apnic.net

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

Європа:
C:\> **ping www.ripe.net**

```
C:\>ping www.ripe.net

Pinging www.ripe.net [193.0.6.139] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.0.6.139:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Південна Америка:
C:\> **ping lacnic.net**

```
C:\>ping www.lacnic.net

Pinging www.lacnic.net [200.3.14.147] with 32 bytes of data:
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=157ms TTL=51

Ping statistics for 200.3.14.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 157ms, Maximum = 158ms, Average = 157ms
```

Коли дані передаються за допомогою команди **ping** в межах одного континенту (Північної Америки), в порівнянні з ситуацією, коли дані з Північної Америки пересилаються на інші континенти, середній час ехо-запиту (у мілісекундах) значно збільшується. У даному випадку ехо-запити за допомогою команди **ping**, відправлені на європейський веб-сайт з США не були успішними.

Відстежування маршруту до віддаленого сервера за допомогою утиліти "traceroute"

Визначимо, який маршрут з усього інтернет-трафіку спрямований до віддаленого сервера. Перевіривши досяжність за допомогою утиліти **ping**, варто уважніше розглянути кожен сегмент мережі, через який проходять дані. Для цього скористаємося утилітою **tracert**.

У командному рядку введіть **tracert www.cisco.com.**

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

Збережіть результати, отримані після введення команди **tracert**, в текстовий файл, виконавши вказані нижче дії.

3) Натисніть правою кнопкою миші на рядок заголовка вікна командного рядка і виберіть параметри Змінити > Виділити усе.

4) Ще раз натисніть правою кнопкою миші на рядок заголовка вікна командного рядка і виберіть параметри Змінити > Копіювати.

5) Відкрийте Блокнот Windows. Для цього натисніть кнопку Пуск і виберіть Усі програми > Стандартні > Блокнот.

6) Щоб вставити дані в Блокнот, виберіть в меню Правка команду Вставити.

7) У меню Файл виберіть команду Зберегти як і збережете файл Блокнота на робочий стіл з назвою tracert1.txt.

Запустите утиліту **tracert** для кожного веб-сайту призначення і збережіть отримані результати в послідовно пронумеровані файли.

C:\> **tracert www.afrinic.net**

C:\> **tracert www.lacnic.net**

Інтерпретуйте дані, отримані за допомогою утиліти **tracert**.

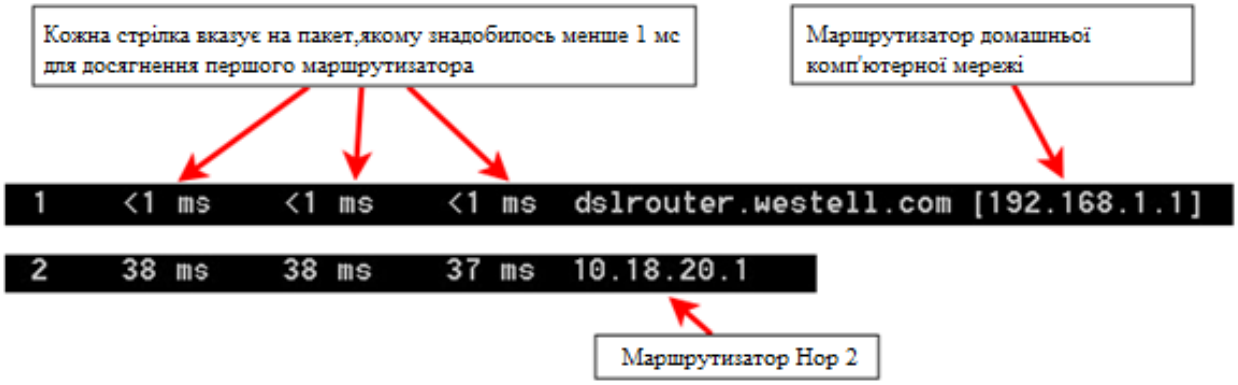
Залежно від зони охоплення вашого інтернет-провайдера і розташування вузлів джерела і призначення, відстежені маршрути можуть перетинати багато переходів і мереж. Кожен перехід – це один маршрутизатор. Маршрутизатор є особливим комп'ютером, який використовується для перенаправлення трафіку через Інтернет. Уявіть, що ви відправилися в поїздку по автодорогах декількох країн. Під час своєї подорожі ви

постійно потрапляєте на розвилки, де треба вибирати один з декількох напрямів. Тепер уявіть собі, що на кожній такій розвилці є пристрій, який вказує правильний шлях до кінцевої мети вашої подорожі. Те ж саме робить маршрутизатор для пакетів у мережі.

Оскільки комп'ютери використовують мову цифр, а не слів, маршрутизаторам привласнюються унікальні IP -адреси (номери у форматі x.x.x.x). **Утиліта tracert показує, по якому шляху проходить пакет даних до кінцевого пункту призначення.** Крім того, за допомогою утиліти **tracert** можна визначити, з якою швидкістю проходить трафік через кожен сегмент мережі. Кожному маршрутизатору на шляхи проходження даних вирушають три пакети, час відповіді на які вимірюється в мілісекундах. Використовуючи цю інформацію, проаналізуйте результати, отримані за допомогою утиліти **tracert** при відправці пакетів до **www.cisco.com**. Нижче представлений увесь маршрут трасування.

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

Деталізуємо отримані дані.



У наведеному прикладі пакети, відправлені утилітою **tracert**, пересилаються з ПК джерела на основний шлюз локального маршрутизатора (перехід 1: 192.168.1.1), а потім на маршрутизатор в точці підключення (POP) до інтернет-провайдера (перехід 2: 10.18.20.1). У кожного провайдера є багато маршрутизаторів POP. Вони відмічають межі мережі інтернет-провайдера і служать точками підключення до Інтернету для клієнтів. Пакети передаються по мережі компанії Verizon, перетинають два переходи і потрапляють в маршрутизатор, що належнить alter.net. Це може означати, що пакети досягли іншого інтернет-провайдера. Цей момент дуже важливий, оскільки при пересилці пакетів від одного до іншого провайдера можливі втрати, а також важливо пам'ятати, що не усі

інтернет-провайдери здатні забезпечити однакову швидкість передачі даних. Як визначити, чи являється alter.net тим же самим або іншим інтернет-провайдером?

Існує інтернет-сервіс **whois**, за допомогою якого можна розпізнати власника доменного імені. Сервіс **whois** доступний за адресою http://whois.domaintools.com/. Згідно інформації, отриманої за допомогою whois, домен alter.net також належить компанії Verizon.

```
Registrant:
        Verizon Business Global LLC
        Verizon Business Global LLC
        One Verizon Way
         Basking Ridge NJ 07920
        US
         domainlegalcontact@verizon.com +1.7033513164 Fax: +1.7033513669

    Domain Name: alter.net
```

Таким чином, інтернет-трафік починається на домашньому ПК і проходить через домашній маршрутизатор (перехід 1). Потім він підключається до інтернет-провайдера і передається по його мережі (переходи 2-7), поки не досягне віддаленого сервера (перехід 8). Це досить нетиповий приклад, у якому від початку до кінця задіяний тільки один провайдер. Як видно з наступних прикладів, найчастіше в пересилці даних беруть участь два і більше інтернет-провайдерів. Тепер розглянемо приклад з пересилкою інтернет-трафіку через декілька інтернет-провайдерів. Нижче представлені результати використання утиліти **tracert** до вузла www.afrinic.net.

```
C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    39 ms    38 ms    37 ms  10.18.20.1
  3    40 ms    38 ms    39 ms  G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4    44 ms    43 ms    43 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    42 ms  0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6    43 ms    71 ms    43 ms  0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7    47 ms    47 ms    47 ms  te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8    43 ms    55 ms    43 ms  vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9    52 ms    51 ms    51 ms  ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

 10   130 ms   132 ms   132 ms  ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11   139 ms   145 ms   140 ms  ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
 12   148 ms   140 ms   152 ms  ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
 13   144 ms   144 ms   146 ms  ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
 14   151 ms   150 ms   150 ms  ae-23-23.ebr2.London1.Level3.net [4.69.148.193]

 15   150 ms   150 ms   150 ms  ae-58-223.csw2.London1.Level3.net [4.69.153.138]

 16   156 ms   156 ms   156 ms  ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
 17   157 ms   159 ms   160 ms  195.50.124.34
 18   353 ms   340 ms   341 ms  168.209.201.74
 19   333 ms   333 ms   332 ms  csw4-pkl-gi1-1.ip.isnet.net [196.26.0.101]
 20   331 ms   331 ms   331 ms  196.37.155.180
 21   318 ms   316 ms   318 ms  fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22   332 ms   334 ms   332 ms  196.216.2.136

Trace complete.
```

Що відбувається в переході 7? Чи є **level3.net** тим же самим інтернет-провайдером, що і в переходах 2-6? Щоб відповісти на це питання, скористаємося сервісом **whois**, звідки визначаємо, що інтернет-трафік проходить від вузла **alter.net** до вузла **level3.net**. Сервіс **whois** повідомляє, що це – окрема компанія або інший інтернет-провайдер.

Що відбувається у переході 18? За допомогою сервісу **whois** виконаємо пошук за адресою 168.209.201.74. Час переходу по одному каналу в мережі збільшується з 159 до 340 мс. Це може означати, що трафік перейшов з магістральної мережі рівня 3 в іншу мережу. За допомогою сервісу **whois** встановлюємо, що IP-адреса 168.209.201.74 належить Африканському мережевому інформаційному центру.

Введемо команду **tracert www.lacnic.net.**

```
C:\>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.147]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    38 ms    38 ms    39 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    42 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    82 ms    47 ms    47 ms  0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6    46 ms    47 ms    56 ms  204.255.168.194
  7   157 ms   158 ms   157 ms  ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8   156 ms   157 ms   157 ms  xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

  9   161 ms   161 ms   161 ms  xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]

 10   158 ms   157 ms   157 ms  ae0-0.ar3.nu.registro.br [200.160.0.249]
 11   176 ms   176 ms   170 ms  gw02.lacnic.registro.br [200.160.0.213]
 12   158 ms   158 ms   158 ms  200.3.12.36
 13   157 ms   158 ms   157 ms  200.3.14.147

Trace complete.
```

Ми бачимо, що у переході час проходження пакету по мережі може збільшувася більш ніж в чотири рази - з ~40 до ~180 мс.

Відстежування маршруту до віддаленого сервера за допомогою програмних і веб-засобів

Скористаємося веб-засобом для трасування маршруту. За допомогою сайту http://www.subnetonline.com/pages/network-tools/online-tracepath.php відстежимо маршрут до веб-сайтів www.cisco.com та www.afrinic.net.

www.cisco.com:

TracePath Output :

1:	pera.subnetonline.com (141.138.203.105)	0.157ms pmtu 1500
1:	gw - v130.xl - is.net (141.138.203.1)	1.168ms
2:	rt - eu01 - v2.xl - is.net (79.170.92.19)	0.566ms
3:	akamai.telecity4.nl - ix.net (193.239.116.226)	1.196ms

www.afrinic.net:
TracePath Output :

```
 1:  pera.subnetonline.com (141.138.203.105)                          0.175ms pmtu 1500
 1:  gw - v130.xl - is.net (141.138.203.1)                            0.920ms
 2:  rt - eu01 - v2.xl - is.net (79.170.92.19)                        0.556ms
 3:  xl - internetservices.nikhef.openpeering.nl (217.170.0.225)      10.679ms
 4:  r22.amstnl02.nl.bb.gin.ntt.net (195.69.144.36)       asymm       54.412ms
 5:  ae - 5.r23.londen03.uk.bb.gin.ntt.net (129.250.5.197)            49.349ms
 6:  ae - 2.r02.londen03.uk.bb.gin.ntt.net (129.250.5.41)   asymm     78.842ms
 7:  dimensiondata - 0.r02.londen03.uk.bb.gin.ntt.net (83.231.235.222)   18.080ms
 8:  168.209.201.74 (168.209.201.74)                                  196.375ms
 9:  csw4 - pkl - gi1 - 1.ip.isnet.net (196.26.0.101)         asymm    10 186.855ms
10:  196.37.155.180 (196.37.155.180)                                  185.661ms
11:  fa1 - 0-1.ar02.jnb.afrinic.net (196.216.3.132)                   197.912ms
```

У даному прикладі трасування маршруту за допомогою командного рядка завершилося на сервері в Кембріджі, штат Массачусетс. Трасування маршруту з веб-сайту в Нідерландах привело до сервера-дзеркала в тій же країні. Домен cisco.com розміщується на декількох веб-сайтах (дзеркалах), розташованих по всьому світу. Це зроблено для того, щоб максимально скоротити час доступу до сайту з будь-якої точки світу.

Порівняємо результати трасування маршруту в Африку з частини 1 з результатами трасування того ж маршруту через веб-інтерфейс. Яка між ними різниця? Маршрут по Європі забезпечується іншим інтернет-провайдером.

В Інтернеті існує не один, а ціла множина магістральних каналів. Усі вони з'єднуються в точках взаємообміну. Швидкодія мережі одного інтернет-провайдера може відрізнятися від швидкодії мережі іншого.

У деяких результатах трасування маршруту можна побачити вираз "**asymm**" – це скорочення від слова **asymmetric**, тобто "асиметричний". Воно означає, що тестовий пакет досяг пункту призначення по одному шляху, а повернувся по іншому. Уявіть, що ви поїхали на машині в місто Чернігів. По дорозі ви виявили, що створено проблеми на дорозі і рух надзвичайно ускладнений. Додому ви вирішили повернутися іншою дорогою, тобто вибрали асиметричний шлях.

Робота з програмою VisualRoute Lite Edition

VisualRoute – це пропрієтарна програма, що дозволяє відобразити результати трасування маршруту наочно.

Якщо програма VisualRoute Lite Edition на комп'ютері не встановлена, завантажите її за наступним посиланням:

http://www.visualroute.com/download.html

Якщо із завантаженням або установкою програми VisualRoute виникнуть проблеми, переконайтеся, що виконується завантаження Lite Edition.

За допомогою програми VisualRoute 2010 Lite Edition відстежите маршрути до www.cisco.com. Збережіть отримані IP -адреси у файлі Блокнота.

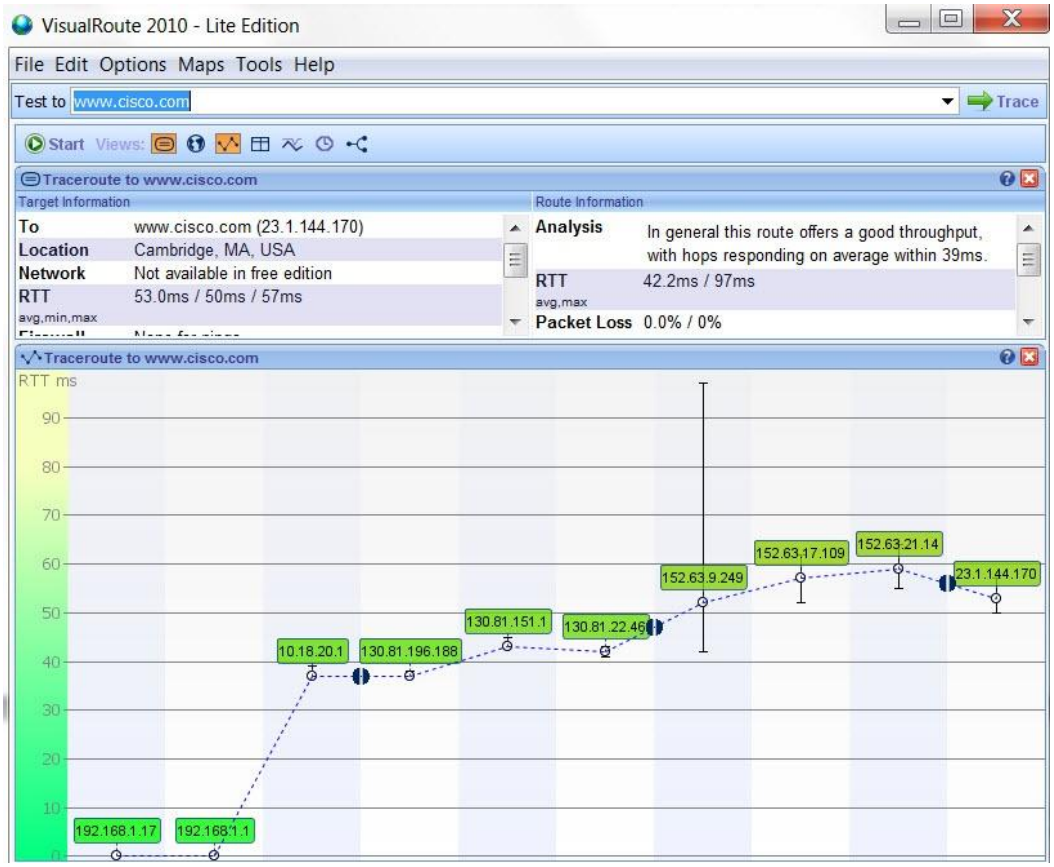


Рис.2.1. Вікно програми VisualRoute Lite Edition

Порівняння результатів трасування

Порівняємо результати трасування маршруту до www.cisco.com, щоб перевірити, чи усі інструменти для трасування використовували одні і ті ж маршрути до www.cisco.com, чи різні. Перерахуємо адреси на маршруті до www.cisco.com, отримані за допомогою утиліти **tracert**:

192.168.1.1 > 10.18.20.1 > 130.81.196.190 > 130.81.22.46 > 152.63.1.57 > 152.63.17.109 > 152.63.21.14 > 23.1.144.170.

Перерахуємо адреси на маршруті до www.cisco.com, отримані за допомогою веб-сервісу **subnetonline.com:**

141.138.203.105 > 141.138.203.1 > 79.170.92.19 > 19.239.116.226

Перерахуємо адреси на маршруті до www.cisco.com, отримані за допомогою програми **VisualRoute Lite Edition:**

192.168.1.17 > 192.168.1.1 > 10.18.20.1 130.81.196.188 > 130.81.151.1 130.81.22.46 > 152.63.9.249 > 152.63.17.109 > 152.63.21.14 > 231.144.170

Трасування маршруту, виконані між одними і тими ж вузлами джерела і призначення, але в різний час, можуть дати різні результати. Це може бути пов'язано з "повнозв'язним" характером взаємно підключених мереж, що складаються з можливостей Інтернету і протоколів Інтернету вибирати різні кабельні канали для відправки пакетів.

Завдання для лабораторної роботи:

Необхідно перевірити можливість з’єднання до віддаленого серверу (згідно варіанту) за допомогою утиліти **ping**, скористатися трьома різними засобами для трасування маршруту (утиліта **tracert**, веб-інтерфейс і програма **VisualRoute**). Порівняти та пояснити результати трасування, як це було наведено у вказівках до виконання завдання.

.

Варіант	Віддалений сервер
1	www.intc.com
2	www.facebook.com
3	www.dlinkmea.com
4	www.java.com
5	www.netacad.com
6	www.intel.com
7	www.yahoo.com
8	www.ibm.com
9	www.linkedin.com
10	www.google.com
11	www.av-intel.com
12	www.agri-intel.com
13	www.gmail.com
14	www.cisco.com
15	www.jossandmain.com
16	www.repmusicldn.com
17	www.scopus.com
18	www.bbc.com
19	www.telegram.org
20	www.oracle.com
21	www.phyton.com
22	www.apple.com
23	www.travelandleisure.com
24	www.ford.com
25	www.gokcecan.com

Вимоги до оформлення звіту

Звіт має включати:

1. Титульний аркуш.
1. Індивідуальне завдання на лабораторну роботу (скріншот завдання згідно варіанту).
2. Хід роботи (послідовний опис виконуваних кроків (з скріншотами виконання), пояснення роботи команди утиліт, програмних та веб-засобів трасування маршруту на віддалений сервер, порівняння результатів трасування).
3. Висновки.

Питання для самоперевірки

1. Для чого використовуються утиліти **ping**, **tracert** та **traceroute**?
2. Які ви знаєте програмні засоби та веб-ресурси для трасування маршруту до віддаленого серверу?
3. Чому результати трасування різними засобами можуть відрізнятися?
4. Що означає вираз "**asymm**"в результатах трасування маршруту?

Рекомендована література

1.CNA R&S ITN // Електронний ресурс. режим доступу: http://static-course-assets.s3.amazonaws.com
2. VisualRoute // Електронний ресурс. Режим доступу: http://www.visualroute.com
3. Tracepath // Електронний ресурс. Режим доступу: http://www.subnetonline.com/pages/network-tools/online-tracepath.php

ЛАБОРАТОРНА РОБОТА №3. НАВІГАЦІЯ ПО IOS. СТВОРЕННЯ БАЗОВОЇ КОНФІГУРАЦІЇ КОМУТАТОРА

Мета: навчитися користовуватися операційною системою Cisco IOS для налаштування основних параметрів мережевих пристроїв, використовуючи команди користувацького, привілейованого режимів та режиму глобальної конфігурації.

Теоретичні відомості

Мережева операційна система – це операційна система (ОС) з вбудованими можливостями для роботи в комп'ютерних мережах.

Операційна система мережевої взаємодії Cisco (IOS) – це загальний термін для групи мережевих операційних систем, що використовуються на мережевих пристроях Cisco.

При використанні інтерфейсу командного рядка (CLI) відбувається безпосереднє звернення до системи в текстовому режимі методом введення команд з клавіатури в командний рядок. Система виконує команду, виводячи вихідні дані в текстовому форматі.

Функції операційної системи IOS:

- забезпечення безпеки мережі;
- IP -адресація віртуальних та фізичних інтерфейсів;
- можливість налаштування інтерфейсу для оптимізації підключення відповідного середовища передачі даних;
- налаштування технологій якості обслуговування (QoS);
- підтримка мережевих протоколів;
- підтримка протоколів маршрутизації;
- підтримка фільтрації зв'язку;
- підтримка мережевих протоколів авторизації;
- наявність в системі мережевих служб, які дозволяють віддаленим користувачам використовувати ресурси комп'ютера тощо.

Кожна функція або служба має відповідний набір команд конфігурації, які дозволяють мережевому фахівцеві її активувати.

Доступ до пристрою Cisco IOS (найбільш поширені методи):

- консоль;
- Telnet або SSH;
- порт AUX.

Для початкової конфігурації комутатора слід використовувати підключення консолі, оскільки параметри IP-адресації ще не налагоджені, а протоколи, які використовуються для віддаленого підключення, не налаштовані.

Рівень доступу до CLI може бути призначений або для звичайних користувачів (**режим користувача**), або для адміністраторів (**привілейований режим**). З рівня адміністратора можна потрапити в режим конфігурації, який внутрішньо ділиться на режими **глобальної конфігурації, канальної конфігурації, конфігурації інтерфейсу** і, при необхідності, на інші режими. Адміністратор дізнається про поточний режим з командного рядка, де символ > означає рівень призначеного для користувацького доступу, символ # показує рівень привілейованого доступу, а додаткові ключові слова в дужках – режим конфігурації і можливі підрежими.

Команда **enable** використовується для надання доступу до повного контролю пристрою, **configure terminal** – запуск редактора конфігурації для прийняття змін з

терміналу, **hostname** – привласнення пристрою імені, **service password - encryption** – захист усіх введених в конфігурації паролів, **line con 0** – вхід конфігурації каналу або "сокет" з позначенням CONSOLE 0 на пристрої, **line vty 0 4** – налаштування п'яти віртуальних віддалених сесій, які забезпечують віддалене управління пристроєм по мережі, **password** – налаштування пароля, який використовуватиметься при підключенні до пристрою, **login** – запит пароля при спробі доступу; призначається командою "**password**", **exit** – вихід з поточного режиму і перехід у вище стоячий режим, **enable secret** – призначення пароля (секретної фрази), що відміняє дії команди "enable", **banner** – повідомлення, яке бачить користувач при спробі доступу до пристрою, **interface Vlan 1** – вхід в режим конфігурації інтерфейсу Vlan1, **description** – створення текстового коментаря для інтерфейсу, який допоможе адміністраторові визначити мету і місце розташування інтерфейсу, **ip address** – привласнення інтерфейсу цифрової IP –адреси, **no shutdown** – відміна команди "shutdown" з наступною активацією інтерфейсу, **end** - вихід з режиму конфігурації.

Розглянемо приклад мережі, що складається з таких пристроїв (рис.3.1):

- 1 маршрутизатор (серія Cisco 1941 з програмним забезпеченням Cisco IOS версії 15.2(4));
- 1 комутатор (серія Cisco 2960, з програмним забезпеченням Cisco IOS версії 15.0(2));
- 2 ПК (Windows 7, Vista і XP з програмою емуляції терміналу, наприклад Tera Term);
- консольні кабелі для налаштування пристроїв Cisco IOS через консольні порти.

Рис.3.1. Мережа з комутатором та маршрутизатором, які підключені через консольний кабель до вузлів

Підключення до маршрутизатора

Підключимо консоль до маршрутизатора і увійдемо до привілейованого режиму (команда **enable**).

Router> enable
Router#

Видалимо файл завантажувальної конфігурації з NVRAM. Введемо команду **erase startup - config**, щоб видалити завантажувальну конфігурацію з NVRAM.

Router# erase startup - config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#

Перезавантаження маршрутизатора

Запустимо команду **reload**, щоб видалити з пам'яті попередню конфігурацію. По запиту перезавантаження натиснем клавішу ВВЕДЕННЯ, щоб підтвердити перезавантаження. Щоб перервати перезавантаження, натиснем будь-яку клавішу.

Router# reload

Proceed with reload? [confirm]

**Nov 29 18:28:09.923: %SYS - 5 - RELOAD: Reload requested by console. Reload Reason : Reload Command.

Примітка. Можливо, з'явиться запит про збереження поточної конфігурації перед перезавантаженням маршрутизатора. Щоб відповісти, введіть **no** і натисніть клавішу ВВЕДЕННЯ.

System configuration has been modified. Save? [yes/no]: no

Після перезавантаження маршрутизатора з'явиться запит про вхід в діалогове вікно початкової конфігурації. Введіть no і натисніть клавішу ВВЕДЕННЯ.

Would you like to enter the initial configuration dialog? [yes/no]: no

Програма запропонує припинити процес автоустановки. Дайте відповідь yes і натисніть клавішу ВВЕДЕННЯ.

Would you like to terminate autoinstall? [yes]: yes

Router>

Ініціалізація і перезавантаження комутатора

Підключимося до комутатора.

Підключимо консоль до комутатора і увійдемо до привілейованого режиму.

Switch> enable

Switch#

Визначимо, чи були створені віртуальні локальні мережі (VLAN).

Скористаємося командою **show flash**, щоб визначити, чи були створені мережі VLAN на комутаторі.

Switch# show flash

Видалимо файл віртуальної локальної мережі (VLAN). Якщо файл **vlan.dat** виявлений у флеш-пам’яті, видалимо цей файл.

Switch# delete vlan.dat

Delete filename [vlan.dat]?

Буде запропоновано перевірити ім'я файлу. На цьому етапі можна змінити ім'я файлу або натиснути клавішу ВВЕДЕННЯ, якщо ім'я введене вірно.

При запиті видалення цього файлу натисніть клавішу ВВЕДЕННЯ, щоб підтвердити видалення. (Щоб відмінити видалення, натисніть будь-яку іншу кнопку.)

Delete flash:/vlan.dat? [confirm]

Switch#

Видалимо файл завантажувальної конфігурації.

Введемо команду **erase startup - config**, щоб видалити файл завантажувальної конфігурації з NVRAM. При необхідності видалення файлу конфігурації натисніть клавішу ВВЕДЕННЯ, щоб підтвердити видалення. (Щоб відмінити операцію, натисніть будь-яку іншу кнопку.)

Switch# erase startup - config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete

Switch#

Перезавантажимо комутатор, щоб видалити з пам'яті усю інформацію про попередню конфігурацію. При необхідності перезавантаження комутатора натисніть клавішу ВВЕДЕННЯ, щоб продовжити перезавантаження. (Щоб відмінити перезавантаження, натисніть будь-яку іншу клавішу.)

Switch# reload

Proceed with reload? [confirm]

Примітка. Можливо, з'явиться запит про збереження поточної конфігурації перед перезавантаженням комутатора. Введіть no і натисніть клавішу ВВЕДЕННЯ.

System configuration has been modified. Save? [yes/no]: no

Після перезавантаження комутатора з'явиться запит про вхід в діалогове вікно початкової конфігурації. Введіть **no** у вікні запиту і натисніть клавішу ВВЕДЕННЯ.

Would you like to enter the initial configuration dialog? [yes/no]: no

Switch>

Розглянемо мережу, що складається з двох вузлів ПК-А і ПК-В, підкючених до комутаторів S1 та S2 (рис.3.2):

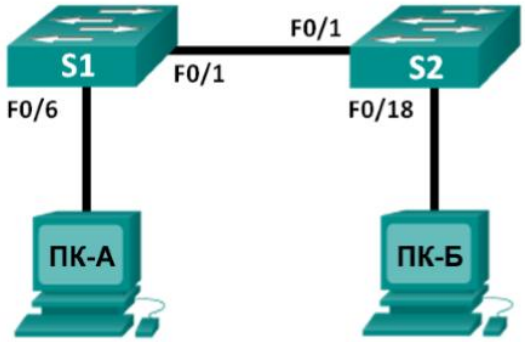


Рис.3.2. Мережа з двома комутаторами, які підключені до вузлів ПК-А та ПК-В

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
S1	VLAN 1	Не доступна	Не доступна	Не доступний
S2	VLAN 1	Не доступна	Не доступна	Не доступний
ПК-А	Мережевий адаптер	192.168.1.10	255.255.255.0	Не доступний
ПК-В	Мережевий адаптер	192.168.1.11	255.255.255.0	Не доступний

Необхідно налаштувати основні параметри мережевих пристроїв, включаючи ім'я вузла, локальні паролі і банер входу в систему.

Налаштування мережі Ethernet

Необхідно включити усі пристрої. Комутатори не мають кнопок включення і включаються при підключенні шнура живлення. З'єднаємо два комутатори. Підключимо один кінець кабелю Ethernet до роз'єму F0/1 на комутаторі S1, а інший - до роз'єму F0/1 на комутаторі S2. Лампочки роз'ємів F0/1 на обох комутаторах спалахнуть жовтим, а потім зеленим кольором. Це означає, що комутатори підключені правильно.

Під'єднаємо комп'ютери до відповідних комутаторів. Підключимо один кінець другого кабелю Ethernet до порту мережевого адаптера ПК-А. Інший кінець кабелю підключимо до роз'єму F0/6 на комутаторі S1. Після підключення ПК до комутатора лампочка роз'єму F0/6 спалахне спочатку жовтим, а потім зеленим кольором, що означає, що ПК-А підключений правильно.

Підключимо один кінець останнього кабелю Ethernet до порту мережевого адаптера ПК-Б. Підключимо інший кінець кабелю до роз'єму F0/18 на комутаторі S2. Після підключення ПК до комутатора лампочка роз'єму F0/18 спалахне спочатку жовтим, а потім зеленим кольором, що означає, що ПК-Б підключений правильно.

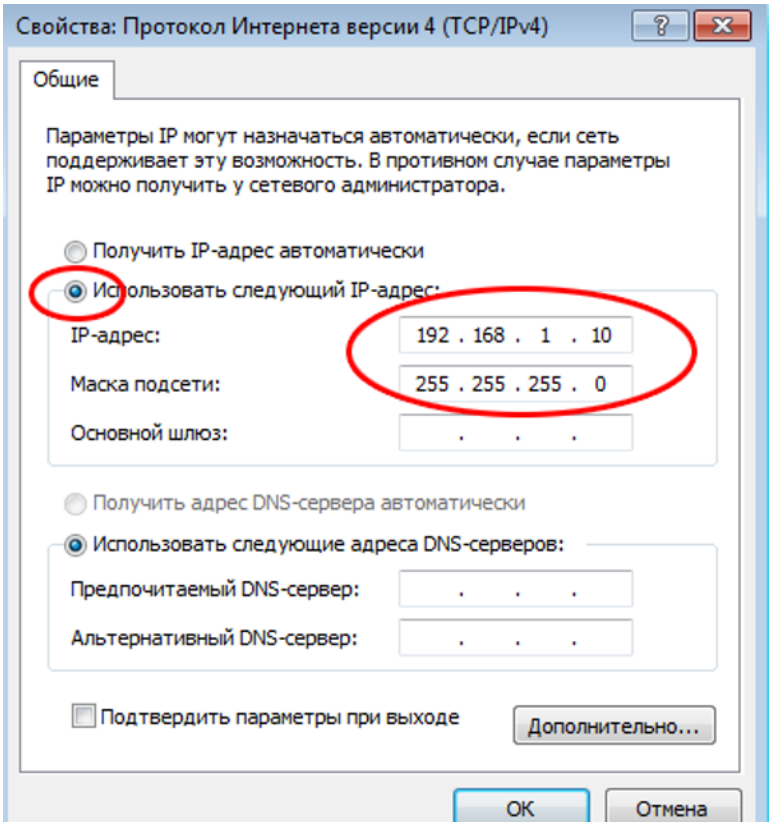
Після підведення кабелів до мережевих пристроїв ретельно перевіримо з'єднання, щоб згодом скоротити час пошуку і усунути неполадки з мережевим підключенням.

Далі необхідно налаштувати статичну IP -адресу на комп'ютерах. У ОС Windows натискаємо кнопку **Пуск**, потім **Панель управління.**

У розділі **"Мережа і Інтернет"** натискаємо на посилання **Перегляд стану мережі і завдань.** У лівій частині вікна **"Центр управління мережами і загальним доступом"** натискаємо на посилання **Зміна параметрів адаптера.**

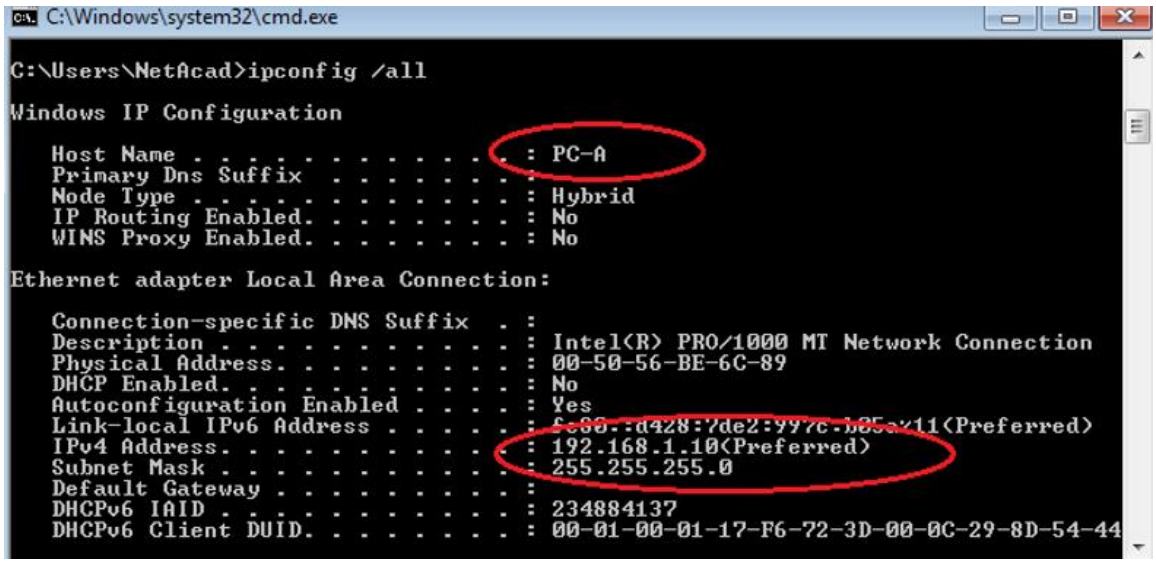
У вікні **"Мережеві підключення"** відображуються доступні інтерфейси ПК. Натискаємо правою кнопкою миші на значок **Підключення по локальній мережі** та вибираємо пункт **Властивості.** Вибираємо опцію **Протокол Інтернету версії 4 (TCP/IPv4)** і натискаємо кнопку **Властивості.**

Щоб налаштувати IP -адресу, маску підмережі і шлюз за замовчуванням вручну, встановлюємо перемикач **Використовувати наступну IP -адресу.**

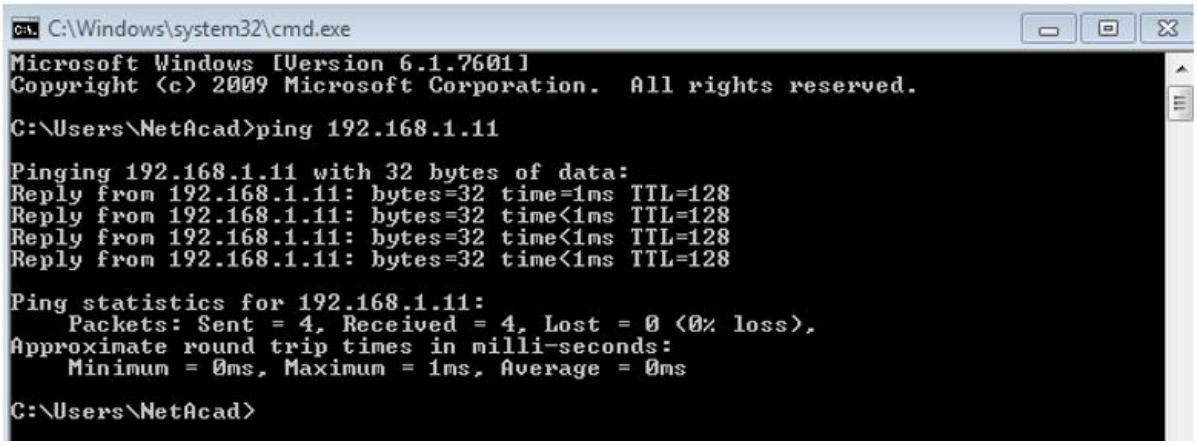


У розглянутому вище прикладі введені IP -адреса і маска підмережі для ПК-А. Шлюз за замовчуванням не вказаний, оскільки до мережі не підключений жоден маршрутизатор. Вказавши усі дані IP, натискаємо кнопку OK. Натискаємо кнопку OK у вікні **"Властивості підключення по локальній мережі"**, щоб присвоїти IP -адресу адаптеру локальної мережі. Повторюємо перелічені вище дії, щоб ввести дані IP -адреси для ПК-Б.

Для перевірки налаштувань і з'єднання ПК використовується вікно командного рядка (**cmd.exe**). На ПК-А натискаємо кнопку **Пуск**, вводимо **cmd** в рядку **Знайти програми і файли** і натискаємо клавішу ВВЕДЕННЯ. У вікні **cmd.exe** можна вводити команди відразу в комп'ютер і тут же переглядати їх результати. Перевіряємо налаштування ПК за допомогою команди **ipconfig /all**. Ця команда відображує ім'я ПК і відомості про IPv4 -адресу.

4. 

Вводимо **ping** 192.168.1.11 і натискаємо клавішу ВВЕДЕННЯ.

5. 

6. Налаштування і перевірка основних параметрів комутатора

Увійдіть до привілейованого режиму. Привілейований режим дає доступ до усіх команд комутатора. До привілейованого набору команд відносяться ті, які містяться в призначеному для користувача режимі, а також команда **configure**, за допомогою якої виконується доступ до інших командних режимів.

Перейдіть в привілейований режим, ввівши команду **enable**.

Switch>enable

Switch#

Запрошення в командному рядку зміниться з Switch > на Switch #, що вказує на привілейований режим.

Увійдіть до режиму конфігурації. Для входу в режим конфігурації використовуйте команду **configuration terminal (conf t).**

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch (config)#

7. Присвоєння імені комутатору

За допомогою команди **hostname** змініть ім'я комутатора на S1.

Switch(config)# hostname S1

S1(config)#

8. Заборона небажаного пошуку в DNS

Відключимо пошук в DNS, щоб запобігти спробам комутатора перетворювати введені команди таким чином, неначе вони є іменами вузлів.

S1(config)# no ip domain - lookup

S1(config)#

Введіть локальні паролі. Для запобігання несанкціонованому доступу до комутатора необхідно настроїти паролі.

9. S1(config)# enable secret class
10. S1(config)# line con 0
11. S1(config - line)# password cisco
12. S1(config - line)# login
13. S1(config - line)# exit
14. S1(config)#

15. Повідомлення дня (MOTD)

16. Банер входу в систему або повідомлення дня (MOTD), попереджає про те, що будь-які спроби несанкціонованого доступу до комутатора заборонені. Для використання команди **banner motd** необхідні розмежувачі, щоб можна було розпізнати вміст баннерного повідомлення. Розмежувальним символом може бути будь-який символ, якого немає в цьому повідомленні. З цієї причини часто використовуються такі символи, як #.
17. S1(config)# banner motd # Enter TEXT message.End with the character '#'. Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. #
18. S1(config)# exit
19. S1#
20. Збережіть конфігурацію. За допомогою команди **copy** збережіть поточну конфігурацію у файл завантажувальної конфігурації, який зберігається в незалежній пам'яті (NVRAM).
21. S1# copy running - config startup - config Destination filename [startup - config]? [Enter] Building configuration.. [OK]
22. S1#

Відобразіть поточну конфігурацію. Команда **show running - config** відображує усю поточну конфігурацію посторінкового. Для перегортування сторінок використовуйте клавішу ПРОПУСК.

S1# show running - config

Building configuration..

Current configuration: 1409 bytes ! ! !

…

version 15.0

…

service timestamps log datetimemsec no service password – encryption

!

hostname S1

!

boot - start - marker boot - end – marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

23. !
24. noip domain - lookup
25. !
26. <outputomitted>
27. !
28. bannermotd ^ Unauthorized access is strictly prohibited and prosecuted to the full extent of the law. ^ !
29. line con 0
30. password cisco
31. login

За допомогою команди **show version** відобразіть версію IOS комутатора, а також іншу корисну інформацію. Тут для перегортування даних також використовується клавіша ПРОПУСК.

S1# show version

Cisco IOS Software, C2960 Software (C2960 - LANBASEK9 - M), Version 15.0(2) SE, RELEASE SOFTWARE (fc1)

Technical Support : http://www.cisco.com/techsupport

Compiled Sat 28 - Jul -12 00:29 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader

BOOTLDR: C2960 Boot Loader (C2960 - HBOOT - M)

Version 12.2(53r) SEY3, RELEASE SOFTWARE (fc1)

S1 uptime is 1 hour, 38 minutes System returned to ROM by power - on System image file is "flash:/c2960 - lanbasek9 - mz.150-2.SE.bin"

…

Для перевірки стану підключених інтерфейсів використовуйте команду show ip interface brief. Для перегортування списку використовуйте клавішу ПРОПУСК.

S1# show ip interface brief

Ініціалізація і перезавантаження комутатора

Підключіть консоль до комутатора і увійдіть до привілейованого режиму.

Switch>enable

Switch#

Визначте, чи були створені віртуальні локальні мережі (VLAN). Скористайтеся командою **show flash**, щоб визначити, чи були створені мережі VLAN на комутаторі. Switch# show flash

Видаліть файл віртуальної локальної мережі (VLAN). Якщо файл **vlan.dat** виявлений у флеш-пам’яті, видалите цей файл.

Switch# delete vlan.dat

Delete filename [vlan.dat]?

Буде запропоновано перевірити ім'я файлу. На цьому етапі можна змінити ім'я файлу або натиснути клавішу ВВЕДЕННЯ, якщо ім'я введене вірно. При запиті видалення цього файлу натисніть клавішу ВВЕДЕННЯ, щоб підтвердити видалення. (Щоб відмінити видалення, натисніть будь-яку іншу кнопку.) Delete flash:/vlan.dat? [confirm]

Видаліть файл завантажувальної конфігурації. Введіть команду **erase startup - config**, щоб видалити файл завантажувальної конфігурації з NVRAM. При необхідності видалення файлу конфігурації натисніть клавішу ВВЕДЕННЯ, щоб підтвердити видалення. (Щоб відмінити операцію, натисніть будь-яку іншу кнопку.)

Switch# erase startup – config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete

Switch#

Перезавантажте комутатор, щоб видалити з пам'яті усю інформацію про попередню конфігурацію. При необхідності перезавантаження комутатора натисніть клавішу ВВЕДЕННЯ, щоб продовжити перезавантаження. (Щоб відмінити перезавантаження, натисніть будь-яку іншу клавішу.)

Switch# reload

Proceed with reload? [confirm]

Налаштування основних параметрів комутатора

Комутатори Cisco мають особливий інтерфейс, який називається **віртуальним інтерфейсом комутатора (SVI)**. На SVI інтерфейсі можна конфігурувати IP -адресу, яку зазвичай називають **адресою управління**. Вона дозволяє дістати віддалений доступ до комутатора для відображення і налаштування параметрів. Необхідно створити просту мережу, використовуючи кабель локальної мережі Ethernet і дістати доступ до комутатора Cisco, використовуючи консоль і методи віддаленого доступу. Налаштувати основні параметри комутатора та IP -адресацію, використати IP -адресу управління для віддаленого доступу до комутатора.

Топологія складається з одного комутатора і одного вузла, що використовує тільки порти Ethernet і консолі. Мережевому адміністраторові необхідно налаштувати основні параметри комутатора (такі як ім'я вузла) і IP -адресу для SVI. Призначення IP адреси на комутаторі – це лише перший крок. Необхідно вибрати спосіб управління комутатором. Два найбільш поширених методу управління – це Telnet і SSH, проте протокол Telnet не є надійним, оскільки уся інформація, що передається між двома пристроями, вирушає у вигляді простого тексту. Аналізатор пакетів може легко перехопити, а також прочитати паролі та інші важливі дані. Якщо в незалежній пам'яті (NVRAM) комутатора немає збережених файлів конфігурації, скориставшись командою Switch>, ви перейдете в призначений для користувача режим. Увійдіть до привілейованого режиму.

Switch> enable

Switch#

Перевірте чистий файл конфігурації за допомогою команди привілейованого режиму **show running - config**. Якщо файл конфігурації був раніше збережений, його треба видалити. Залежно від моделі комутатора і версії IOS конфігурація може виглядати по-різному. При цьому налагоджених раніше паролів або IP -адреси на комутаторі бути не повинно. Увійдіть до режиму глобальної конфігурації і призначте ім'я вузла комутатора.

Switch# configure terminal

Switch(config)# hostname S1

S1(config)# .

Налаштуйте пароль доступу до комутатора.

S1(config)# enable secret class

S1(config)#.

Забороніть небажані пошуки в службі доменних імен (DNS).

S1(config)# no ip domain - lookup

S1(config)# .

Налаштуйте повідомлення дня (MOTD), яке відображуватиметься перед входом в систему.

S1(config)# banner motd # Enter Text message. End with the character '#'.

Unauthorized access is strictly prohibited. #

Перевірте налаштування доступу, перемикаючись між режимами.

S1(config)# exit

S1#

S1# exit

Unauthorized access is strictly prohibited.

S1>

Примітка. Поєднання клавіш **Ctrl-Z** використовується для прямого переходу з режиму глобальної конфігурації в привілейований режим.

Поверніться з призначеного для користувача режиму в привілейований.

S1> enable

Password: class

S1#

Примітка. Пароль не відображуватиметься на екрані в процесі введення.

Увійдіть до режиму глобальної конфігурації і настройте IP -адресу SVI для дозволу віддаленого управління комутатором.

S1# config t

S1##00# interface vlan 1

S1(config - if)# ip address 192.168.1.2 255.255.255.0

S1(config - if)# no shut

S1(config - if)# exit

S1(config)#

Обмежте доступ до порту консолі. Конфігурація за умовчанням не вимагає пароля при консольних підключеннях.

S1(config)# line con 0

S1(config - line)# password cisco

S1(config - line)# login

S1(config - line)# exit

S1(config)#

Налаштування мережевих пристроїв в Packet Tracer

Запустимо Packet Tracer та додамо в робочу область комутатор та вузол PC1 (рис.3.3).

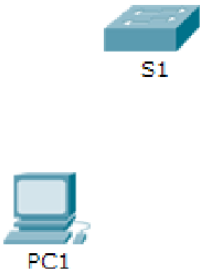


Рис.3.3. Комутатор та комп'ютер в Packet Tracer

Підключимо PC1 до S1 за допомогою консольного кабелю. Інструкції:

- Клацніть значок **Connections** (у вигляді блискавки) в лівому нижньому кутку вікна Packet Tracer.
- Виберіть ясно-блакитний консольний кабель, клацнувши по ньому. Покажчик миші набере вигляду роз'єму із звисаючим кінцем кабелю.
- Клацніть PC1. У вікні буде показаний варіант для підключення RS - 232.
- Перетягніть інший кінець консольного підключення до комутатора S1 і клацніть комутатор, щоб відкрити список підключень.
- Виберіть консольний порт, щоб завершити підключення.
- Встановіть сеанс термінального зв'язку з комутатором S1.
- Клацніть PC1 та відкрийте вкладку **Desktop** (Робочий стіл).
- Клацніть значок **Terminal**. Перевірте правильність параметрів за замовчуванням, встановлених для порту.
- Натисніть кнопку OK.

- У вікні, що з'явилося, може бути показані декілька повідомлень. У якій-небудь частині вікна повинне з'явитися повідомлення Press RETURN to get started! (Натисніть клавішу ВВЕДЕННЯ, щоб почати роботу). Натисніть клавішу ВВЕДЕННЯ. На екрані повинно з'явитися запрошення S1> .

Вивчення довідки по IOS на комутаторі

У IOS доступна довідка з команд залежно від рівня роботи. В даний момент відображується запрошення для **режиму користувача**, і пристрій чекає введення команд. Найпростіший спосіб виклику довідки – ввести знак (?) питання в запрошенні, щоб отримати список команд.

S1> ?

У командному рядку введіть t зі знаком питання у кінці (?).

S1> t

Відобразяться команди:

telnet
terminal
traceroute

У командному рядку введіть te зі знаком питання у кінці (?).

S1> te

Відобразяться команди:

telnet
terminal

Такий тип довідки називається **контекстною**; у ній надаються додаткові відомості при розширенні команд.

Вивчення режимів введення

Перейдемо до привілейованого режиму.
У командному рядку введіть знак (?) питання.
S1> ?

Введіть en і натисніть клавішу TAB.

S1> en<Tab>

Що відображується після натиснення клавіші TAB? (enable). Це завершення команди або завершенням клавішею TAB. Після введення частини команди за допомогою клавіші TAB можна завершити введення цієї команди. Якщо введених символів вистачає для унікального визначення команди (наприклад, як у випадку з командою enable), частина, що залишилася, буде введена автоматично.

Що станеться, якщо ввести te<Tab> у командному рядку? У "te" недостатньо символів для унікального визначення команди, тому ці ж символи відображуватимуться і далі, пропонуючи користувачеві ввести додаткові символи для унікального визначення команди. З "te" починається декілька команд.

Введіть команду **enable** і натисніть клавішу ВВЕДЕННЯ. Як змінився рядок запрошення? Він змінився з S1> на S1#, показуючи **привілейований режим введення**.

Введіть в рядку знак (?) питання. S1# ? Раніше вже використовувалася одна команда, яка почалася з букви "c" в призначеному для користувача режимі. Скільки команд показано тепер, коли включений привілейований режим?

clear
clock
configure
connect
copy

Перехід в режим глобальної конфігурації

Однією з команд, що доступних в привілейованому режимі і починаються з букви "c", є **configure**. Введіть команду повністю або тільки її частину, достатню для завершення, клавішею TAB, а потім натисніть клавішу ВВЕДЕННЯ.

S1# configure

Яке відобразилося повідомлення? Configuring from terminal, memory, or network [terminal]? Натисніть клавішу ВВЕДЕННЯ, щоб прийняти параметр за замовчуванням, узятий у квадратні дужки [terminal]. Як змінився рядок запрошення?

S1(config)#

Такий режим називається **режимом глобальної конфігурації**. А тепер поверніться в привілейований режим, ввівши команду **exit** або **end**, або натиснувши поєднання клавіш **Ctrl - Z.**

S1(config)#

exit S1#

Налаштування годинника

Використовуйте команду **clock**, щоб детальніше вивчити довідку і синтаксис команди. Введіть **show clock** в привілейованому режимі.

S1# show clock

Яка інформація відображується? Який рік відображується? (Після запису "UTC Mon Mar 1 1993" відображені дані в годиннику, хвилинах і секундах з моменту запуску пристрою. Рік – 1993). Використовуйте контекстну довідку і команду clock, щоб встановити поточний час на комутаторі.

Введіть команду **clock** і натисніть клавішу ВВЕДЕННЯ.

S1# clock<ENTER>

Яка інформація відображується? IOS видала повідомлення % Incomplete command, яке означає, що для команди **clock** потрібно додаткові параметри. У довідці можна отримати додаткові відомості про час, якщо ввести після команди пропуск і знак (?) питання.

S1# clock ?

Яка інформація відображується? (set Set the time and date). Налаштуйте час за допомогою команди **clock**. Продовжуйте вивчення команди, виконуючи по одній дії за один раз.

S1# clock set ?

Яка проситься інформація? (hh: mm: ss Current Time). Які відобразяться відомості, якщо ввести тільки команду **clock**, не виконуючи запит довідки за допомогою знаку питання? (% Incomplete command). На основі даних, запрошених за допомогою команди **clock set ?**, введіть час 15:00, використовуючи 24-годинний формат. Перевірте, чи потрібні додаткові параметри.

S1# clock set 15:00:00 ?

Вихідні дані містять запит на отримання додаткових відомостей : <1-31> Day of the month MONTH Month of the year. Спробуйте встановити дату 01/31/2035, використовуючи запрошений формат. Для цього може потрібно запросити додаткову довідку. Після закінчення виконаєте команду **show clock**, щоб відобразити параметри годинника. Виведення команди повинне мати наступний вигляд:

S1# show clock

**15:0:4.869 UTC Tue Jan 31 2035

Якщо ваші вихідні дані відрізняються, спробуйте виконати наступну команду:

S1# clock set 15:00:00 31 Jan 2035

IOS виводить різні дані для неправильних або неповних команд. Продовжуйте працювати з командою **clock**, щоб вивчити додаткові повідомлення, які можуть з'явитися в ході навчання роботи з IOS. Введіть наступну команду і запишіть повідомлення:

S1# cl
Які повернені дані? (% Ambiguous command: "cl")
S1# clock
Які повернені дані? (% Incomplete command)
S1# clock set 25:00:00
Які повернені дані?
S1#clock set 25:00:00
(^ % % Invalid input detected at '^' marker)
S1# clock set 15:00:00 32 Які повернені дані?
S1#clock set 15:00:00
(32 % % Invalid input detected at '^' marker).

Налаштування початкових параметрів комутатора в Packet Tracer

Створимо в Packet Tracer модель мережі, зображеної на рис. 3.4.

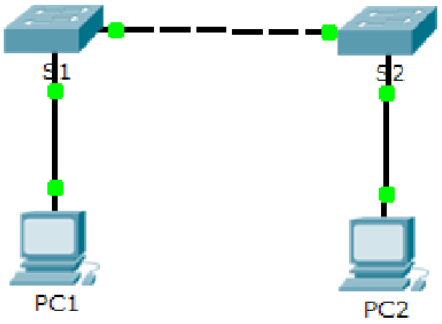


Рис.3.4. Мережа з двома комутаторами S1 та S2, які підключені до вузлів PC1 та PC2

Конфігурація S1

Необхідно забезпечити безпеку доступу до інтерфейсу командного рядка (CLI) і портів консолі за допомогою зашифрованих і текстових паролів.

Вхід в привілейований режим

У привілейованому режимі доступні усі команди комутатора. Але у зв'язку з тим, що багатьма з привілейованих команд задаються робочі параметри, привілейований доступ має бути захищений паролем щоб уникнути несанкціонованого використання. До привілейованого набору команд відносяться ті, які містяться в призначеному для користувача режимі, а також команда **configure**, за допомогою якої виконується доступ до інших командних режимів. Клацніть S1 і відкрийте вкладку CLI. Натисніть клавішу ВВЕДЕННЯ. Перейдіть в привілейований режим, виконавши команду **enable.**

Switch> enable
Switch#

Проглянете поточну конфігурацію комутатора. Виконаєте команду **show running - config.**

Switch# show running - config
Скільки у маршрутизатора інтерфейсів FastEthernet? (24)
Скільки у маршрутизатора інтерфейсів Gigabit Ethernet? (2)
Який діапазон значень, що відображуються в vty -лініях? (0 -15)
Яка команда відображує поточний вміст NVRAM? (show startup – configuration)
Чому комутатор відповідає повідомленням «startup - config is not present»? (Він відображує це повідомлення, оскільки цей файл конфігурації не був збережений в NVRAM. На даний момент він розташований в ОЗП).

Створення базової конфігурації комутатора

Для налаштування параметрів комутатора, можливо, потрібно буде перемикатися між режимами налаштування. Зверніть увагу, як змінюється рядок запрошення при переході по розділах комутатора. Задамо ім'я комутатору S1.

Switch# configure terminal
Switch(config)# hostname S1
S1(config)# exit
S1#

Безпечний доступ до консолі

Для забезпечення безпечного доступу до консолі перейдіть в режим **config - line** і встановіть для консолі пароль letmein.

S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# line console 0
S1(config - line)# password letmein
S1(config - line)# login
S1(config - line)# exit
S1(config)# exit
%%SYS - 5 - CONFIG_I : Configured from console by console
S1#

Для чого потрібна команда **login**? (Щоб працював процес перевірки пароля, потрібно обидві команди: login і password).

Переконайтеся, що доступ до консолі захищений паролем. Вийдіть з привілейованого режиму, щоб переконатися, що для консольного порту встановлений пароль.

S1# exit
Switch con0 is now available Press RETURN to get started. User Access Verification Password:
S1>

Примітка. Якщо комутатор не виводить запит на введення пароля, значить, ви не налаштували параметр login.

Безпечний доступ в привілейований режим

Встановіть для **enable** пароль c1$c0. Цей пароль обмежує доступ до привілейованого режиму.

Примітка. Символ 0 в c1$c0 - це цифра нуль, а не буква "O". Цей пароль не буде дійсним, поки ви його не зашифруєте його в наступному кроці.

S1> enable
S1# configure terminal
S1(config)# enable password c1$c0
S1(config)# exit
%%SYS - 5 - CONFIG_I : Configured from console by console
S1#

Переконайтеся, що доступ до привілейованого режиму захищений паролем. Виконаєте команду **exit** ще раз, щоб вийти з комутатора. Натисніть клавішу <ВВЕДЕННЯ>, після чого вам буде запропоновано ввести пароль: User Access Verification Password:

Перший пароль відноситься до консолі, який був заданий для line con 0. Введіть цей пароль, щоб повернутися в призначений для користувача режим. Введіть команду для доступу до привілейованого режиму. Введіть другий пароль, який був заданий для

обмеження доступу до привілейованого режиму. Перевірте конфігурацію, вивчивши вміст файлу running - configuration:

S1# show running - configuration

Зверніть увагу, що паролі для консолі та привілейованого режиму відображуються у вигляді звичайного тексту. Це може представляти ризик для системи безпеки, якщо за вашими діями спостерігають із-за спини.

Налаштування зашифрованого пароля для доступу до привілейованого режиму

Пароль для **enable** треба замінити на новий зашифрований пароль за допомогою команди **enable secret**. Встановіть для команди "enable" пароль itsasecret.

S1# config t
S1(config)# enable secret itsasecret
S1(config)# exit
S1#

Примітка. Пароль enable secret перевизначає пароль enable. Якщо для комутатора задано обидва паролі, для переходу в привілейований режим треба ввести пароль enable secret.

Переконайтеся в тому, що пароль "enable secret" доданий у файл конфігурації. Введіть команду **show running - config** ще раз, щоб перевірити новий пароль enable secret.

Примітка. Команду show running - config можна скоротити до

S1# show run

Що відображується при виведенні пароля enable secret? (1mERr$ILwq/b7kc.7X/ejA4Aosn0) Чому пароль enable secret відображується не так, як заданий пароль? (Пароль "enable secret" відображується в зашифрованому виді, а пароль "enable password" – у вигляді звичайного тексту).

Шифрування паролів для консолі і привілейованого режиму

Пароль enable secret зашифрований, а паролі enable і console зберігаються у вигляді звичайного тексту. Зашифруємо усі відкриті паролі за допомогою команди **service password - encryption.**

S1# config t
S1(config)# service password - encryption
S1(config)# exit

Якщо встановити на комутаторі інші паролі, вони зберігатимуться у файлі конфігурації у вигляді звичайного тексту або в зашифрованому виді? (Ця команда служби шифрування паролів шифрує усі поточні і наступні паролі).

Налаштування банера MOTD

У набір команд Cisco IOS входить команда, яка дозволяє настроїти повідомлення, яке показуватиметься усім, хто входить в систему на комутаторі. Це повідомлення називається **щоденним банером (MOTD).**

Текст банера треба взяти в подвійні лапки або використовувати роздільник, відмінний від будь-якого символу в рядку MOTD.

S1# config t
S1(config)# banner motd "This is a secure system. Authorized Access Only"!
S1(config)# exit %%SYS - 5 - CONFIG_I : Configured from console by console
S1#

Повідомлення показуватиметься, коли хтось входить в систему на комутаторі через консольний порт. Кожен комутатор повинен мати повідомлення, що застерігає неавторизованих користувачів про те, що доступ заборонений. Але його також можна використовувати для відправки повідомлень мережевих фахівців (наприклад, про заплановане відключення системи або до кого звертатися за діставанням доступу).

Збереження файлів конфігурації в NVRAM

Перевірте правильність конфігурації за допомогою команди "show run". Збережіть файл конфігурації. Ви завершили базове налаштування комутатора. Тепер виконайте резервне копіювання файлу конфігурації в NVRAM і перевірте, щоб внесені зміни не загубилися після перезавантаження системи та відключення живлення.

S1# copy running - config startup - config

Destination filename [startup - config]?[Enter] Building configuration.. [OK]

Яка найкоротша версія команди copy running - config startup - config? (cop r s).

Вивчите початковий файл конфігурації. Яка команда відображує вміст NVRAM? (show startup – configuration). Чи усі внесені зміни були записані у файл? (Так, після запуску running - configuration він залишився без змін).

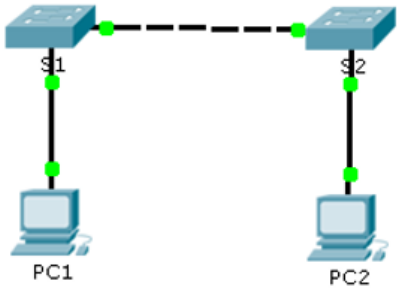
Конфігурація S2

Ви завершили налаштування комутатора S1. Налаштуйте для комутатора S2 наступні параметри. Ім'я пристрою: S2. Захистіть доступ до консолі паролем letmein. Встановіть для привілейованого режиму пароль c1$c0 і задайте пароль "enable secret" для itsasecret. Введіть наступне повідомлення для користувачів, що виконують вхід в систему на комутаторі: Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law. Зашифруйте усі відкриті паролі. Перевірте правильність конфігурації. Збережіть файл конфігурації, щоб запобігти його втраті у разі відключення живлення комутатора.

```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#line console 0
S2(config - line)#password letmein
S2(config - line)#login
S2(config - line)#enable password c1$c0
S2(config)#enable secret itsasecret
S2(config)#banner motd $any text here$
S2(config)#service password - encryption
S2(config)#do wr
```

Завдання до лабораторної роботи

Створити в симуляторі Packet Tracer мережу заданої топології згідно наступного сценарію. Ваш менеджер попросив вас, як нового фахівця з обслуговування локальних мереж, продемонструвати навички конфігурації невеликої локальної мережі. Вам належить провести налаштування початкових параметрів на двох комутаторах з операційною системою Cisco IOS, а також налаштувати параметри IP-адресації для встановлення наскрізного з'єднання. Необхідно використовувати два комутатори і два вузли (ПК) в активній мережі з кабельним підключенням.



Таблиця адресації

Пристрій	Інтерфейс	Адреса	Маска підмережі
S1 Name	VLAN 1	S1 Add	255.255.255.0
S2 Name	VLAN 1	S2 Add	255.255.255.0
PC1 Name	Мережевий адаптер	PC1 Add	255.255.255.0
PC2 Name	Мережевий адаптер	PC2 Add	255.255.255.0

Необхідно:

- Налаштувати імена вузлів і IP -адреси на двох комутаторах IOS за допомогою інтерфейсу командного рядка (CLI).
- Обмежити доступ до конфігурацій пристроїв за допомогою команд Cisco IOS.
- Використати команди IOS для збереження поточної конфігурації.
- Налаштувати IP -адреси на двух вузлах.
- Перевірити зв'язок між двома кінцевими пристроями (ПК). Вказівки:
- Використати консольне підключення для доступу до кожного комутатора.
- Присвоїте комутаторам імена, для деяких варіантів [[SN]] і [[SN+1]] де N – номер варіанту студента, наприклад, для 8-го варіанту назви комутаторів будуть S8 та S9.
- Використати пароль для входу в консоль і привілейований режим.
- Заборонити небажані пошуки в DNS.
- Зашифрувати усі відкриті паролі.
- Додате слово WARNING в банер MOTD.
- Налаштувати адресацію для усіх пристроїв відповідно до таблиці адресації.
- Зберегти налаштування. Перевірити поточну конфігурацію комутаторів.
- Перевірите наявність підключення між усіма пристроями.

Варіант 1

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	128.107.20.10	255.255.255.0
S N+1	VLAN 1	128.107.20.15	255.255.255.0
User - 1	Мережевий адаптер	128.107.20.25	255.255.255.0
User - 2	Мережевий адаптер	128.107.20.30	255.255.255.0

Варіант 2

Пристрій	Інтерфейс	Адреса	Маска підмережі
Room - 145	VLAN 1	172.16.5.35	255.255.255.0
Room - 146	VLAN 1	172.16.5.40	255.255.255.0
Manager	Мережевий адаптер	172.16.5.50	255.255.255.0
Reception	Мережевий адаптер	172.16.5.60	255.255.255.0

Варіант 3

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	10.10.10.100	255.255.255.0
S N+1	VLAN 1	10.10.10.150	255.255.255.0
User - 1	Мережевий адаптер	10.10.10.4	255.255.255.0
User - 2	Мережевий адаптер	10.10.10.5	255.255.255.0

Варіант 4

Пристрій	Інтерфейс	Адреса	Маска підмережі
Class – A	VLAN 1	128.107.20.1	255.255.255.0
Class - B	VLAN 1	128.107.20.10	255.255.255.0
Student – 1	Мережевий адаптер	128.107.20.20	255.255.255.0
Student - 2	Мережевий адаптер	128.107.20.30	255.255.255.0

Варіант 5

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	172.16.5.30	255.255.255.0
S N+1	VLAN 1	172.16.5.45	255.255.255.0
Manager	Мережевий адаптер	172.16.5.60	255.255.255.0
Reception	Мережевий адаптер	172.16.5.70	255.255.255.0

Варіант 6

Пристрій	Інтерфейс	Адреса	Маска підмережі
ASw – 1	VLAN 1	10.10.10.100	255.255.255.0
ASw - 2	VLAN 1	10.10.10.120	255.255.255.0
User - 1	Мережевий адаптер	10.10.10.3	255.255.255.0
User - 2	Мережевий адаптер	10.10.10.4	255.255.255.0

Варіант 7

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	128.107.20.10	255.255.255.0
S N+1	VLAN 1	128.107.20.20	255.255.255.0
Student – 1	Мережевий адаптер	128.107.20.30	255.255.255.0
Student - 2	Мережевий адаптер	128.107.20.40	255.255.255.0

Варіант 8

Пристрій	Інтерфейс	Адреса	Маска підмережі
Room – 5	VLAN 1	172.16.5.30	255.255.255.0
Room - 6	VLAN 1	172.16.5.40	255.255.255.0
Manager	Мережевий адаптер	172.16.5.50	255.255.255.0
Reception	Мережевий адаптер	172.16.5.60	255.255.255.0

Варіант 9

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	10.10.10.100	255.255.255.0
S N+1	VLAN 1	10.10.10.150	255.255.255.0
User - 1	Мережевий адаптер	10.10.10.5	255.255.255.0
User - 2	Мережевий адаптер	10.10.10.6	255.255.255.0

Варіант 10

Пристрій	Інтерфейс	Адреса	Маска підмережі
Class – 1	VLAN 1	128.107.20.10	255.255.255.0
Class - 2	VLAN 1	128.107.20.25	255.255.255.0
Student – 1	Мережевий адаптер	128.107.20.30	255.255.255.0
Student - 2	Мережевий адаптер	128.107.20.40	255.255.255.0

Варіант 11

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	172.16.5.35	255.255.255.0
S N+1	VLAN 1	172.16.5.45	255.255.255.0
Manager	Мережевий адаптер	172.16.5.50	255.255.255.0
Reception	Мережевий адаптер	172.16.5.60	255.255.255.0

Варіант 12

Пристрій	Інтерфейс	Адреса	Маска підмережі
Sw – 1	VLAN 1	10.10.10.100	255.255.255.0
Sw – 2	VLAN 1	10.10.10.120	255.255.255.0
User - 01	Мережевий адаптер	10.10.10.5	255.255.255.0
User - 02	Мережевий адаптер	10.10.10.6	255.255.255.0

Варіант 13

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	128.107.20.10	255.255.255.0
S N+1	VLAN 1	128.107.20.20	255.255.255.0
Student – 01	Мережевий адаптер	128.107.20.30	255.255.255.0
Student - 02	Мережевий адаптер	128.107.20.40	255.255.255.0

Варіант 14

Пристрій	Інтерфейс	Адреса	Маска підмережі
Room – 3	VLAN 1	172.16.5.35	255.255.255.0
Room - 4	VLAN 1	172.16.5.40	255.255.255.0
Manager	Мережевий адаптер	172.16.5.60	255.255.255.0
Reception	Мережевий адаптер	172.16.5.70	255.255.255.0

Варіант 15

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	10.10.10.100	255.255.255.0
S N+1	VLAN 1	10.10.10.150	255.255.255.0
User - 1	Мережевий адаптер	10.10.10.3	255.255.255.0
User - 2	Мережевий адаптер	10.10.10.4	255.255.255.0

Варіант 16

Пристрій	Інтерфейс	Адреса	Маска підмережі
Class – 1	VLAN 1	172.16.5.25	255.255.255.0
Class - 2	VLAN 1	172.16.5.45	255.255.255.0
Student – 1	Мережевий адаптер	172.16.5.80	255.255.255.0
Student - 2	Мережевий адаптер	172.16.5.90	255.255.255.0

Варіант 17

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	128.107.20.30	255.255.255.0
S N+1	VLAN 1	128.107.20.40	255.255.255.0
Manager	Мережевий адаптер	128.107.20.55	255.255.255.0
Reception	Мережевий адаптер	128.107.20.65	255.255.255.0

Варіант 18

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	192.168.10.5	255.255.255.0
S N+1	VLAN 1	192.168.10.6	255.255.255.0
User - 1	Мережевий адаптер	192.168.10.25	255.255.255.0
User - 2	Мережевий адаптер	192.168.10.35	255.255.255.0

Варіант 19

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	10.10.15.100	255.255.255.0
S N+1	VLAN 1	10.10.15.120	255.255.255.0
Student – 1	Мережевий адаптер	10.10.15.3	255.255.255.0
Student - 2	Мережевий адаптер	10.10.15.4	255.255.255.0

Варіант 20

Пристрій	Інтерфейс	Адреса	Маска підмережі
Room – 10	VLAN 1	172.16.10.25	255.255.255.0
Room - 20	VLAN 1	172.16.10.45	255.255.255.0
Manager	Мережевий адаптер	172.16.10.80	255.255.255.0
Reception	Мережевий адаптер	172.16.10.90	255.255.255.0

Варіант 21

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	192.168.20.5	255.255.255.0
S N+1	VLAN 1	192.168.20.6	255.255.255.0
User - 01	Мережевий адаптер	192.168.20.35	255.255.255.0
User - 02	Мережевий адаптер	192.168.20.45	255.255.255.0

Варіант 22

Пристрій	Інтерфейс	Адреса	Маска підмережі
Class – A	VLAN 1	107.20.30.10	255.255.255.0
Class - B	VLAN 1	107.20.30.20	255.255.255.0
Student – A	Мережевий адаптер	107.20.30.40	255.255.255.0
Student - B	Мережевий адаптер	128.107.30.50	255.255.255.0

Варіант 23

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	172.16.5.20	255.255.255.0
S N+1	VLAN 1	172.16.5.30	255.255.255.0
Manager	Мережевий адаптер	172.16.5.80	255.255.255.0
Reception	Мережевий адаптер	172.16.5.90	255.255.255.0

Варіант 24

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	192.168.30.5	255.255.255.0
S N+1	VLAN 1	192.168.30.6	255.255.255.0
User - 1	Мережевий адаптер	192.168.30.70	255.255.255.0
User - 2	Мережевий адаптер	192.168.30.80	255.255.255.0

Варіант 25

Пристрій	Інтерфейс	Адреса	Маска підмережі
S N	VLAN 1	10.10.10.100	255.255.255.0
S N+1	VLAN 1	10.10.10.120	255.255.255.0
Student - 1	Мережевий адаптер	10.10.10.3	255.255.255.0
Student - 2	Мережевий адаптер	10.10.10.4	255.255.255.0

Вимоги до оформлення звіту

Звіт має включати:

1. Титульний аркуш.
2. Індивідуальне завдання на лабораторну роботу (скріншот завдання згідно варіанту).
3. Хід роботи (послідовний опис виконуваних кроків (з скріншотами виконання) та пояснення команд).
4. Висновки.

Питання для самоперевірки

1. Які основні функції мережевої операційної системи?
2. Які режими роботи операційної системи Cisco IOS ви знаєте?
3. Як відбувається перехід в привілейований режим?
4. Як відбувається перехід в режим глобальної конфігурації?
5. Чому для початкової конфігурації комутатора слід використовувати підключення консолі? Чому не можна підключитися до комутатора по протоколу Telnet або SSH?
6. Яким чином команди об'єднуються в підгрупи або режими? Як адміністратор дізнається, який режим він використовує в поточний момент?
7. Для чого використовуються команди **enable** та **configure terminal**?
8. Яка команда використовується для привласнення імені пристрою?
9. Для чого використовується команда **service password - encryption** ?
10. Для чого використовуються команди **line con 0** та **line vty 0 4**?
11. Для чого використовується команда **no shutdown**?
12. Для чого використовується віртуальний інтерфейс комутатора?
13. Як налаштовується поточний час на комутаторі?
14. Як переглянути поточну конфігурацію комутатора?
15. Які засоби захисту комутатора від несанкціонованого доступу ви знаєте? Як налаштувати банерне повідомлення на комутаторі?

Рекомендована література

1. CNA R&S ITN // Електронний ресурс. режим доступу: http://static-course-assets.s3.amazonaws.com
2. Cisco IOS Command Modes // Електронний ресурс. Режим доступу: www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf019.html
3. Початкове налаштування комутатора Cisco Catalyst 2960 на базі Cisco IOS // Електронний ресурс. Режим доступу: supportforums.cisco.com/ru/document/147811

ЛАБОРАТОРНА РОБОТА №4. ЗБІР ТА АНАЛІЗ ДАНИХ ПРОТОКОЛУ ICMP ЗА ДОПОМОГОЮ ПРОГРАМИ WIRESHARK

Мета: навчитися використовувати програму Wireshark для збору та аналізу даних протоколу ICMP, для перехоплення IP -адрес пакетів даних ICMP і MAC-адрес Ethernet – кадрів з локальних та віддалених вузлів.

Теоретичні відомості

Wireshark – це програма для аналізу протоколів (аналізатор пакетів), яка використовується для пошуку і усунення неполадок в мережі, аналізу, розробки програмного забезпечення і протоколів. У міру руху потоків даних по мережі аналізатор перехоплює кожен протокольний блок даних (PDU), після чого розшифровує або аналізує його зміст згідно з відповідним документом RFC або іншими специфікаціями.

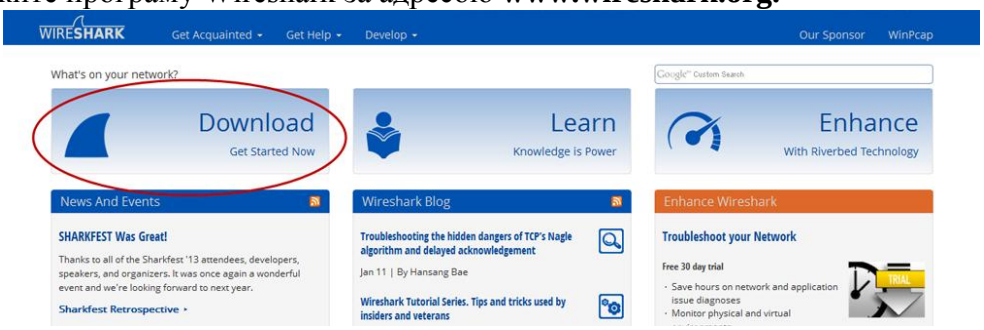
Для виконання лабораторної роботи використовується один ПК (Windows 7, Vista або XP з виходом в Інтернет), додаткові ПК в локальній мережі необхідні для відповідей на ехо-запити (команда **ping)** на інші комп'ютери в локальній мережі.

Порядок установки Wireshark і знімки екрану можуть відрізнятися залежно від версії програми. У цій лабораторній роботі наведено використання Wireshark версії 1.8.3 для Windows 7 (64-розрядна версія).

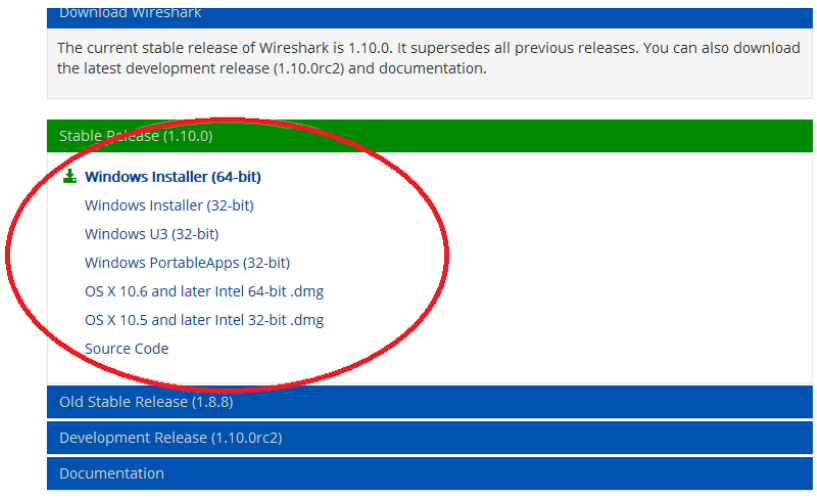
Завантаження і установка програми Wireshark

Програма Wireshark є стандартним аналізатором пакетів, який використовують мережеві інженери. Версії цієї програми з відкритим початковим кодом доступні для різних операційних систем, включаючи Windows, Mac і Linux.

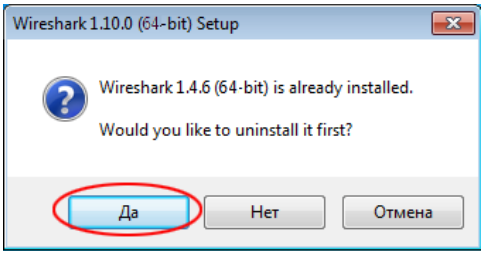
Завантажите програму Wireshark за адресою **www.wireshark.org.**



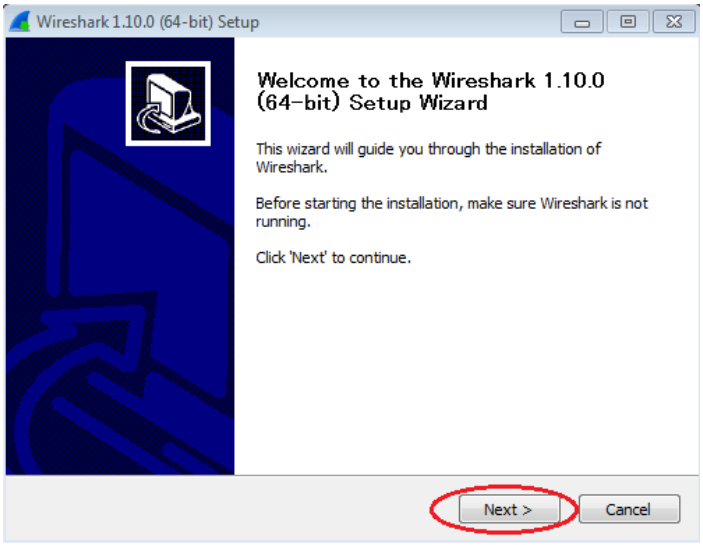
Виберіть версію програми відповідно до архітектури і операційної системи вашого ПК. Наприклад, якщо ваш ПК працює під управлінням 64-розрядною ОС Windows, виберіть Windows Installer (64 - bit).



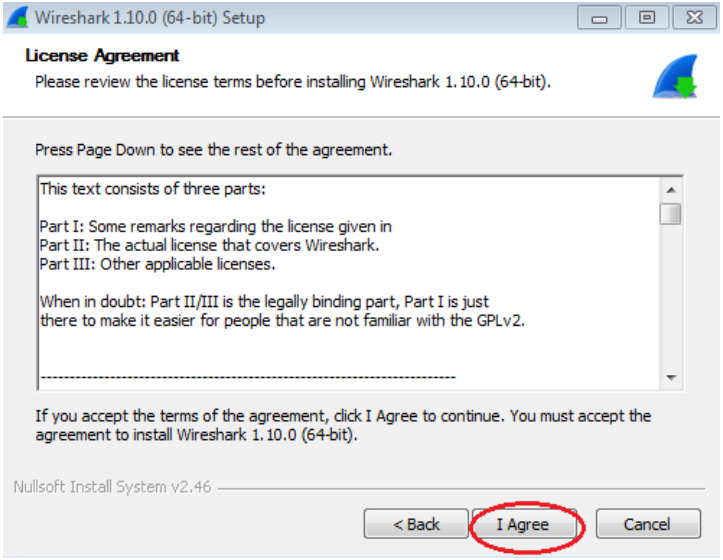
Відразу після цього почнеться завантаження. Місцезнаходження завантаженого файлу залежить від браузеру і операційної системи, якими ви користуєтеся. Завантажений файл називається **Wireshark - win64 - x.x.x.exe**, де "x" відповідає номеру версії. Двічі натисніть на файл, щоб почати установку. Дайте відповідь на усі повідомлення безпеки, які з'являться на екрані. Якщо на вашому ПК вже є копія Wireshark, перед установкою програми з'явиться запит на видалення старої версії. Рекомендується видалити стару версію програми перед установкою нової. Щоб видалити попередню версію програми Wireshark, натисніть кнопку **Так**.



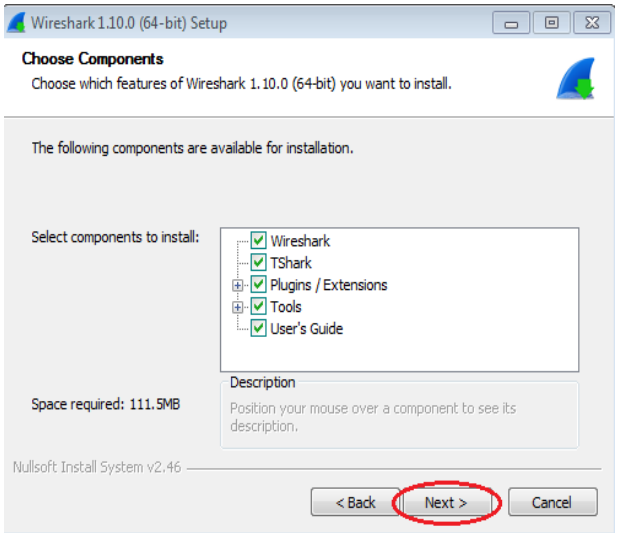
Якщо програма Wireshark встановлюється уперше або попередня версія була видалена, відкриється майстер установки програми Wireshark. Натисніть кнопку **Next** (Далі).

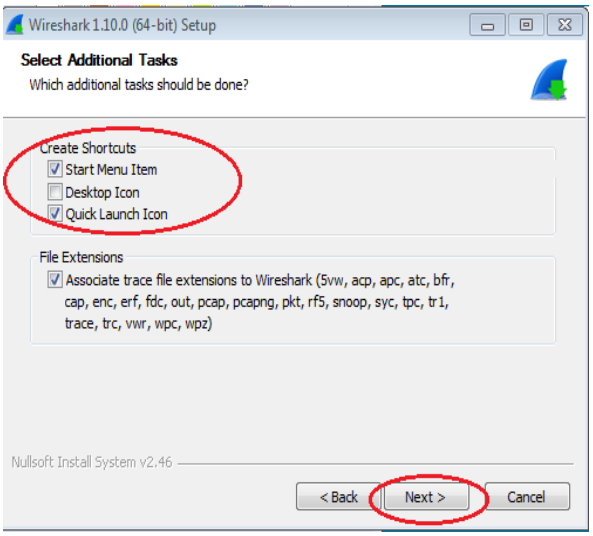


Виконайте інструкції по установці. Коли відкриється вікно "**License Agreement**" (Ліцензійна угода), натисніть кнопку **I accept** (Прийняти).

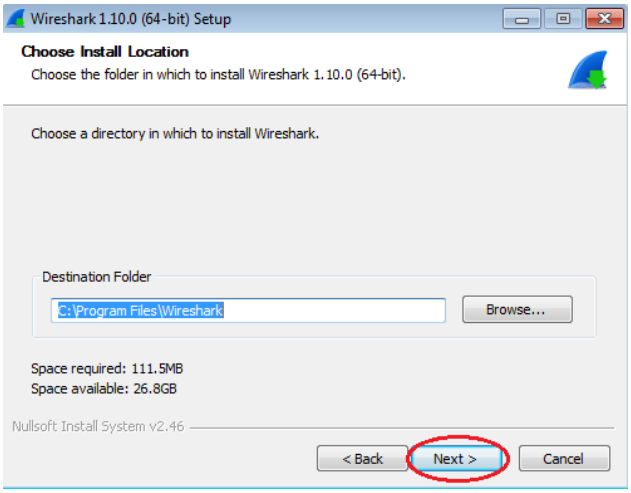


При виборі компонентів залиште налаштування за замовчуванням і натисніть кнопку **Next** (Далі). Виберіть бажані ярлики і натисніть кнопку **Next** (Далі).

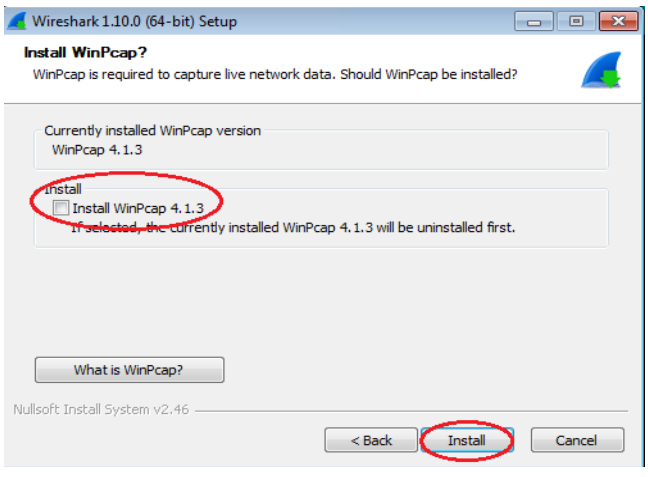




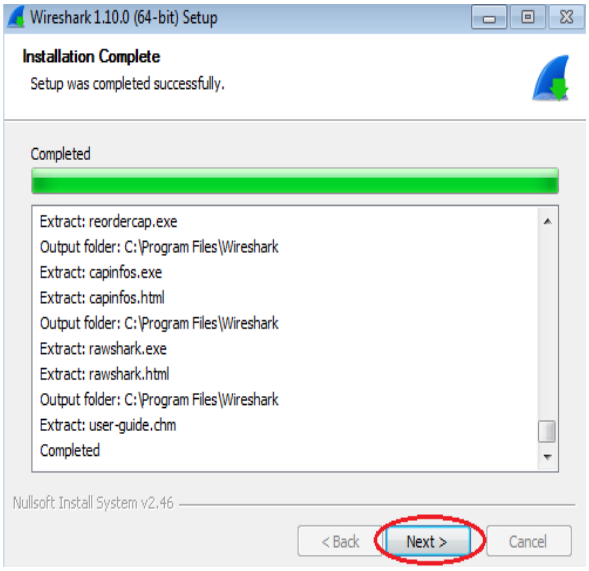
Якщо дисковий простір обмежений, директорію установки можна змінити, інакше, залиште адресу, вказану за замовчуванням.

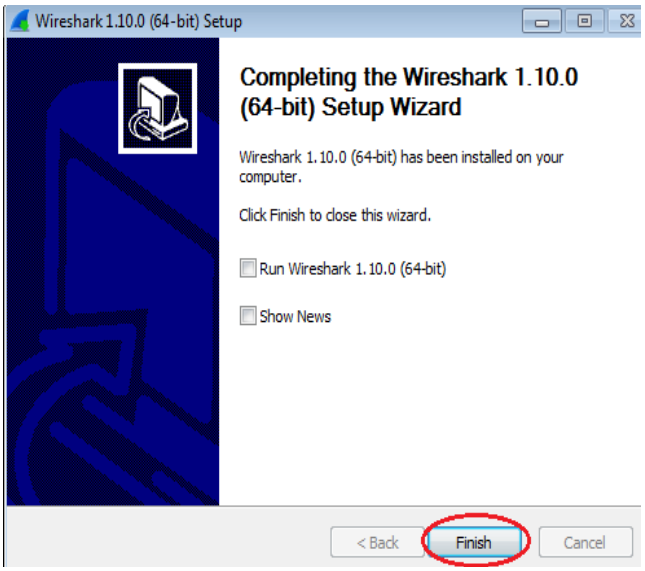


Для збору мережевих даних на ваш ПК необхідно встановити програму **WinPcap**. Якщо встановлена версія WinPcap старша за версію, що додається до програми Wireshark, необхідно встановити новішу версію, натиснувши на прапорець поряд з варіантом **Install WinPcap x.x.x** (Встановити WinPcap x.x.x). Якщо установка пройшла успішно, закрийте майстер установки WinPcap.



Після цього почнеться установка програми Wireshark. Статус установки відображатиметься в окремому вікні. Після закінчення установки натисніть кнопку **Next.** Для завершення процесу установки програми Wireshark натисніть **Finish** (Готово).



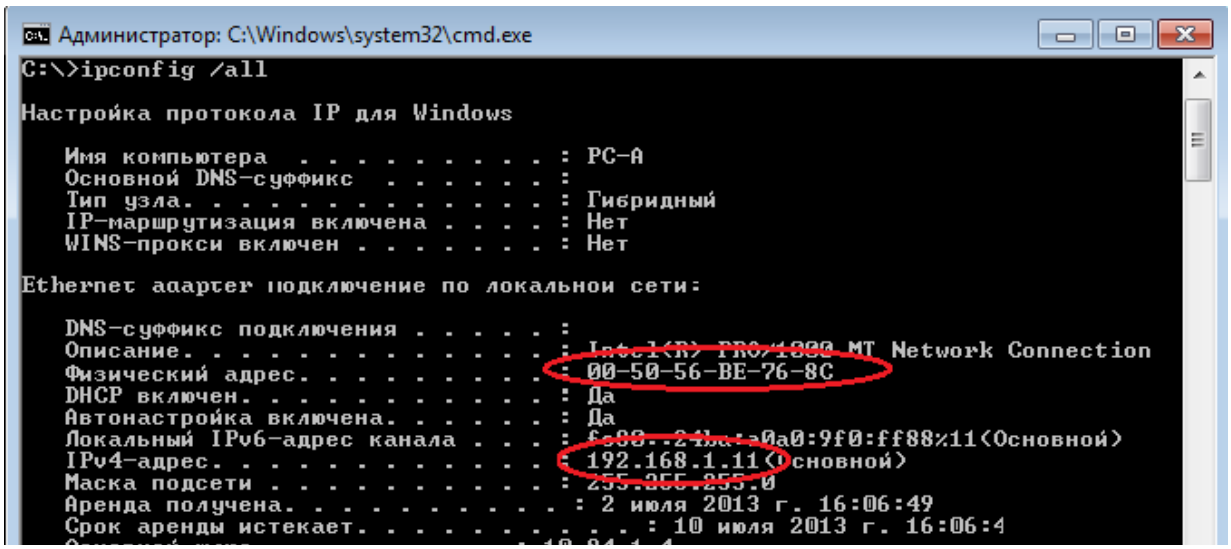


Вказівки щодо виконання завдання

Збір і аналіз даних протоколу ICMP по локальних вузлах в програмі Wireshark

Відправте ехо-запит за допомогою команди **ping** на інший ПК в локальній мережі і перехопіть ICMP -запити і відгуки в програмі Wireshark. При цьому знайдіть необхідну інформацію в зібраних кадрах. Цей аналіз допоможе зрозуміти, як використовуються заголовки пакетів для передачі даних за місцем призначення.

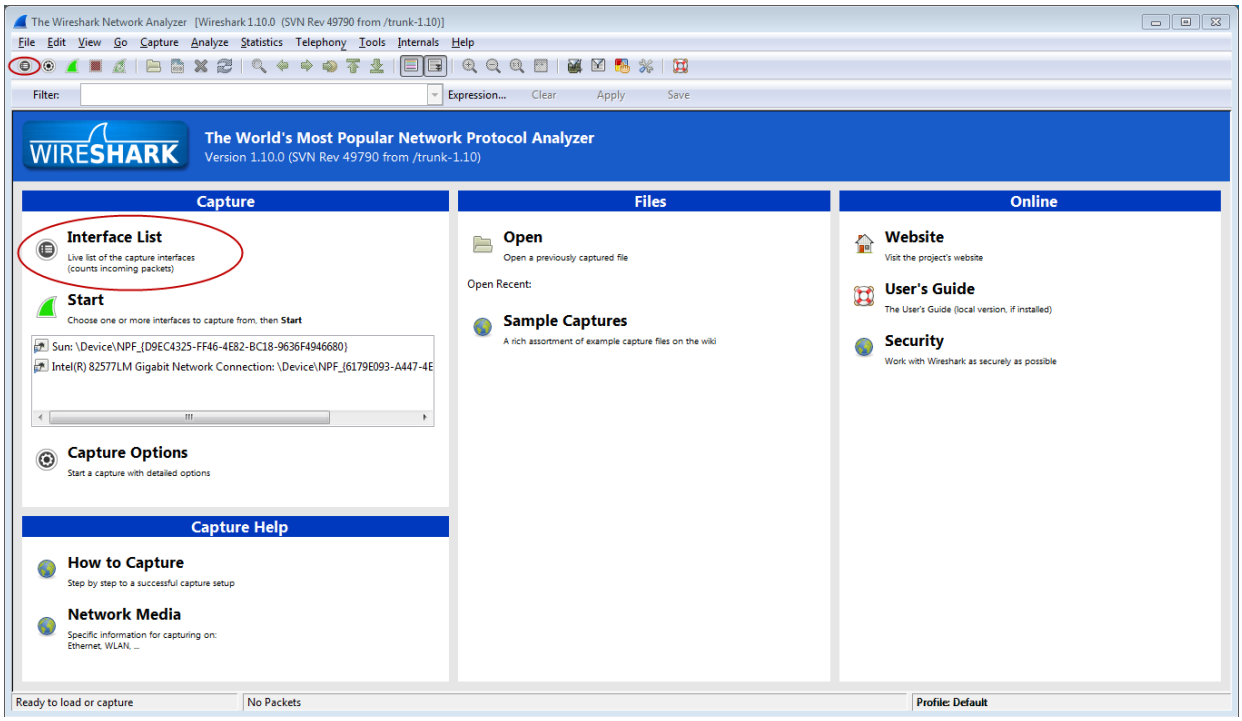
Визначіть адреси інтерфейсів нашого ПК. У цій лабораторній роботі необхідно дізнатись IP –адресу свого комп'ютера і фізичну адресу мережевого адаптера (MAC – адресу). Відкрийте вікно командного рядка, введіть команду **ipconfig /all** і натисніть клавішу ВВЕДЕННЯ. Запишіть IP -адресу інтерфейсу ПК і MAC-адресу.



Обміняйтеся IP -адресами з колегою, але поки що не повідомляйте йому свою MAC-адресу. Запустіть програму Wireshark і почніть перехоплення даних.

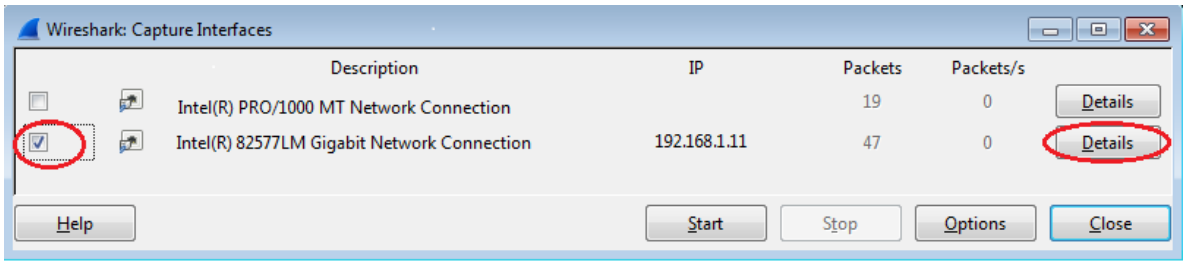
На своєму ПК натисніть кнопку Пуск / Wireshark.

Запустивши програму Wireshark, натисніть на параметр **Interface list** (Список інтерфейсів).

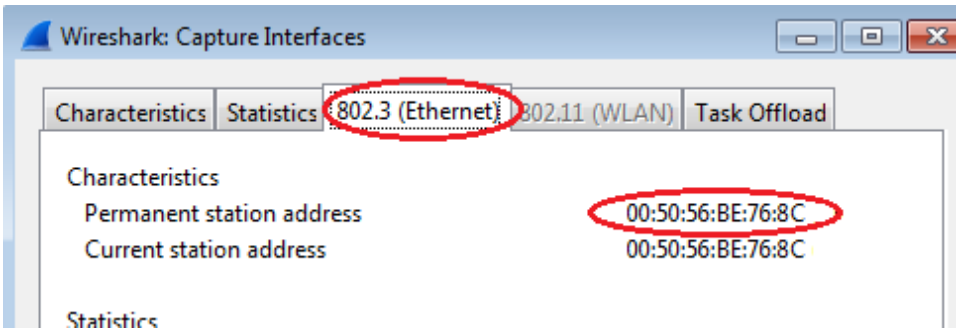


Список інтерфейсів можна також відкрити, натиснувши на значок першого інтерфейсу у ряді значків.

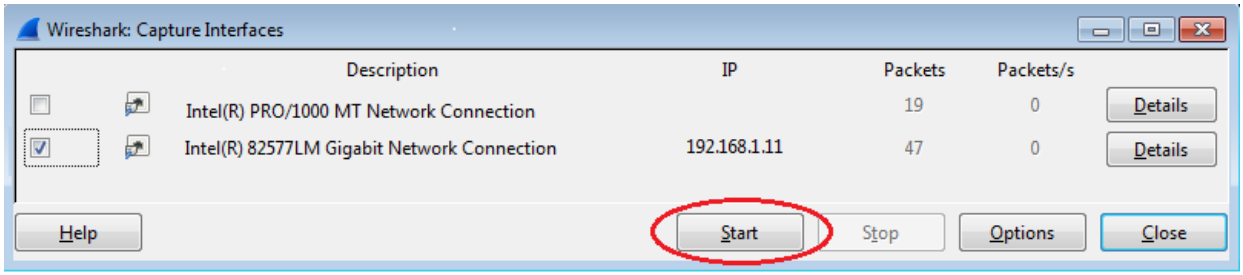
У вікні "**Capture Interfaces**" (Перехоплення інтерфейсів) програми **Wireshark** встановіть прапорець поряд з інтерфейсом, підключеним до вашої локальної мережі.



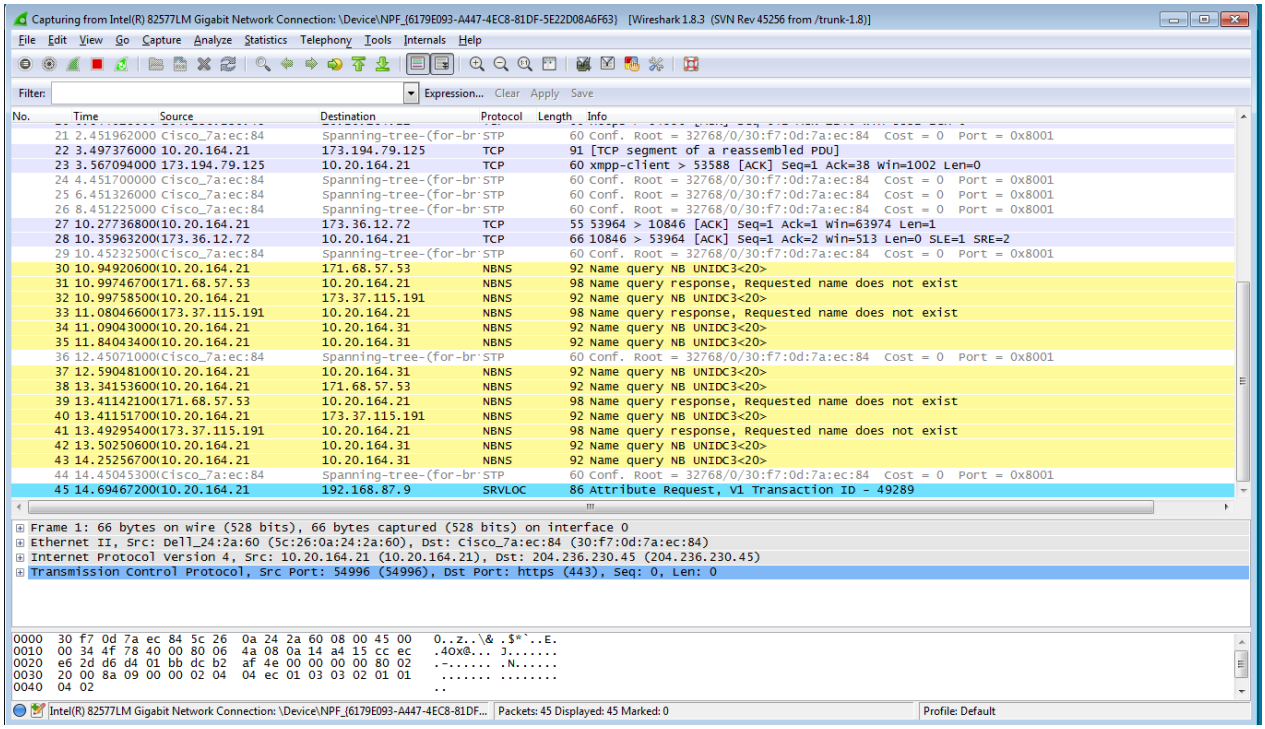
Якщо перераховано декілька інтерфейсів і ви не упевнені в тому, якою з них треба вибрати, натисніть кнопку **Details** (Детальніше) і відкрийте вкладку 802.3 (Ethernet). Переконаєтеся в тому, що MAC -адреса відповідає результату, який ви отримали раніше. Переконавшись в правильності інтерфейсу, закрийте вікно інформації.



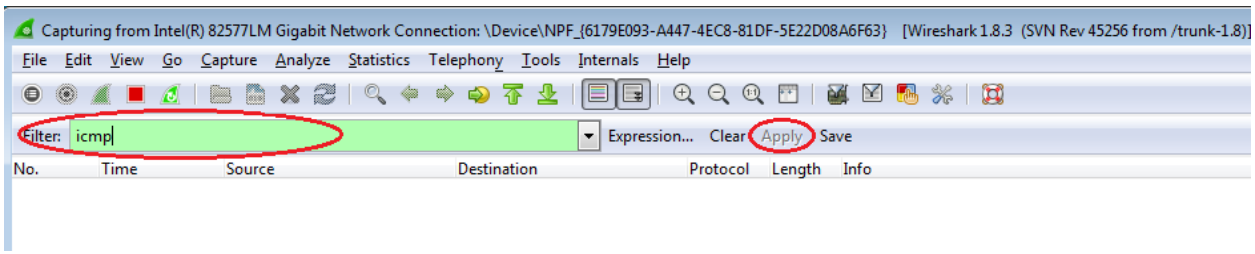
Після цього натисніть кнопку **Start** (Почати), щоб почати перехоплення даних.



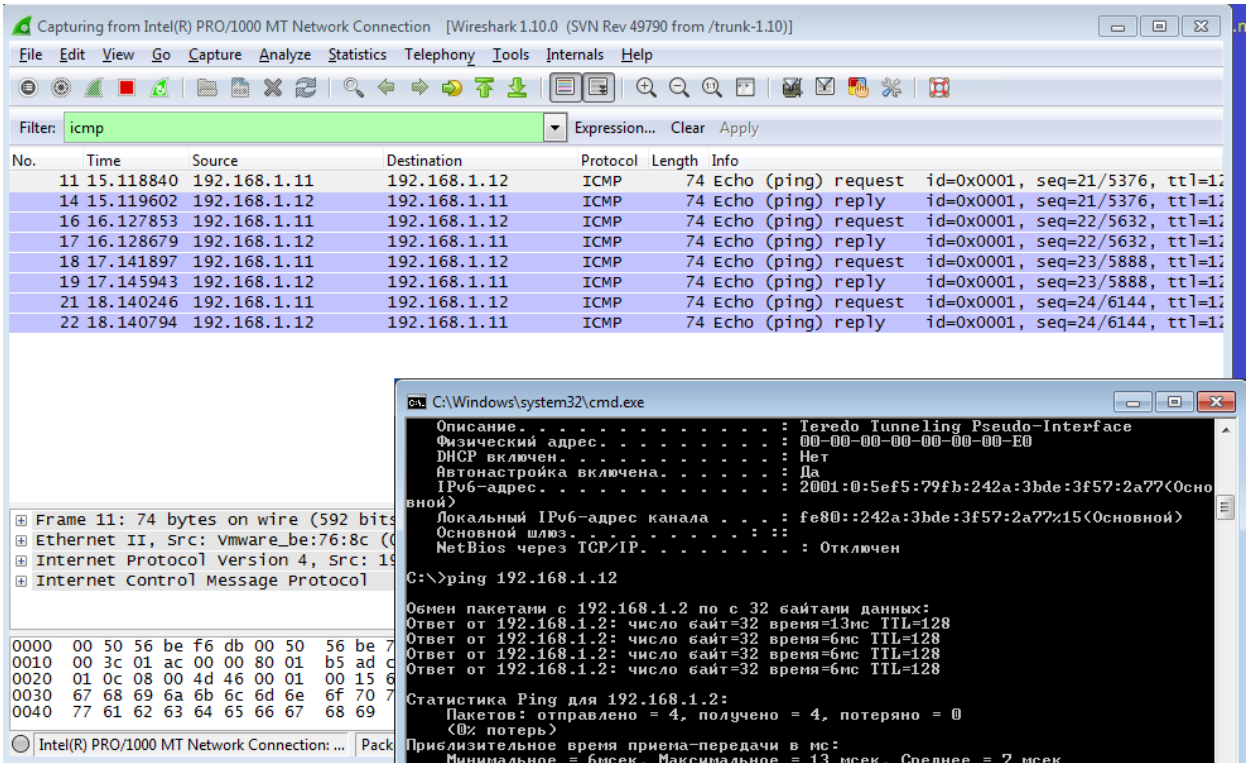
У верхній частині вікна програми Wireshark почне прокручуватися інформація. Рядки даних виділяються різними кольорами залежно від протоколу.



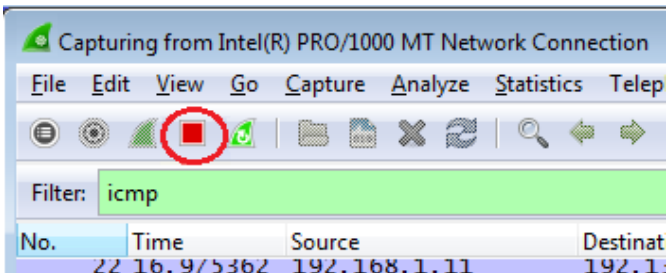
Інформація може прокручуватися дуже швидко залежно від типу зв'язку між ПК і локальною мережею. Щоб полегшити перегляд і роботу з даними, зібраними програмою Wireshark, можна застосувати фільтр. У цій лабораторній роботі нам потрібні тільки протокольні блоки даних (PDU) ICMP (exo-запит за допомогою команди **ping**). Щоб вивести на екран тільки протокольні блоки даних ICMP (exo-запит за допомогою команди **ping**), в полі фільтру у верхній частині вікна програми Wireshark введіть **icmp** і натисніть клавішу ВВЕДЕННЯ або кнопку **Apply** (Застосувати).



Після цього усі дані у верхньому вікні зникнуть, проте перехоплення трафіку в інтерфейсі продовжиться. Відкрийте вікно командного рядка, яке ви відкривали раніше, і відправте exo- запит за допомогою команди **ping** на IP -адресу, отриману від іншого студента. Зверніть увагу на те, що у верхній частині вікна програми Wireshark знову з'являться дані.



Зупиніть перехоплення даних, натиснувши на значок **Stop Capture** (Зупинити перехоплення).



Проаналізуйте отримані дані. Якщо комп'ютер іншого студента не відповідає на ваші ехо-запити, це може бути викликано тим, що брандмауер його комп'ютера блокує ці запити.

Пропуск трафіку ICMP через брандмауер для ОС Windows

Якщо ехо-запити за допомогою команди **ping** з інших комп'ютерів не проходять на ваш ПК, можливо, їх блокує брандмауер. **Брандмауер або міжмережевий екран** (англ. *Firewall*, буквально «вогняна стіна») – пристрій, що дозволяє допускати, відмовляти, шифрувати, пропускати через проксі весь комп'ютерний трафік між областями різної безпеки згідно з набором правил та інших критеріїв.

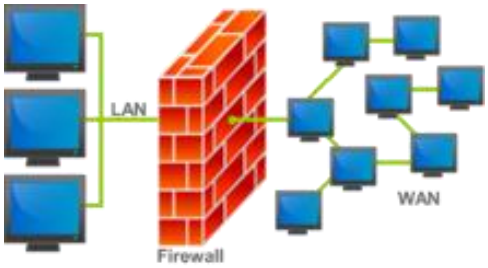


Рис. 4.1. Схематичне зображення міжмережевого екрану (Firewall)

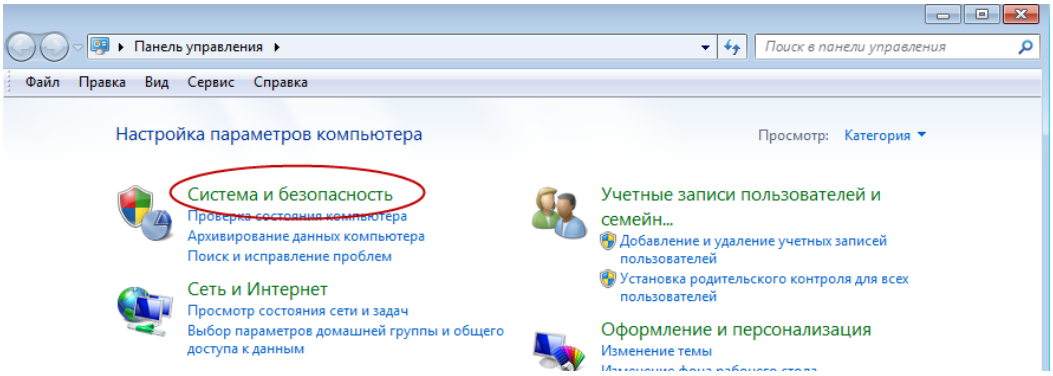
Міжмережевий екран може бути у вигляді окремого пристрою (маршрутизатора), або програмного забезпечення, що встановлюється на персональний комп'ютер чи проксі-сервер. В залежності від активних з'єднань, що відслідковуються, бранмауери розділяють на: **stateless** (проста фільтрація), які не відслідковують поточні з'єднання (наприклад TCP), а фільтрують потік даних виключно на основі статичних правил; **stateful** (фільтрація з урахуванням контексту), з відслідковуванням поточних з'єднань та пропуском тільки тих пакетів, що задовольняють логіці й алгоритмам роботи відповідних протоколів та програм. Такі типи фаєрволів дозволяють ефективніше боротися з різноманітними DDoS-атаками та вразливістю деяких протоколів мереж.

Існує три типи фаєрволів: мережевого рівня, прикладного рівня і рівня з'єднання. Кожен з цих типів використовує свій, відмінний від інших підхід до захисту мережі.

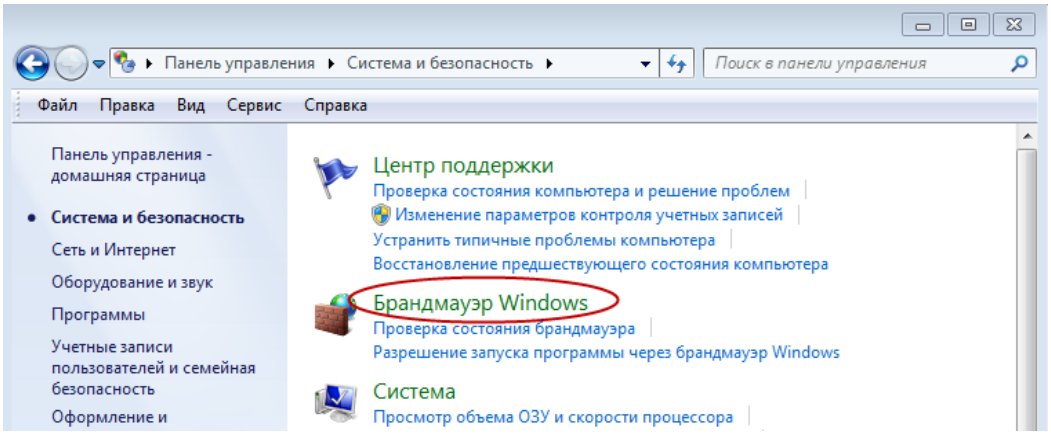
Бранмауери мережевого рівня представлені екрануючими маршрутизаторами. Вони контролюють лише дані мережевого і транспортного рівнів службової інформації пакетів. Мінусом таких маршрутизаторів є те, що ще п'ять рівнів залишаються неконтрольованими. Адміністратори, які працюють з екрануючими маршрутизаторами, повинні пам'ятати, що у більшості пристроїв, що здійснюють фільтрацію пакетів, відсутні механізми аудиту та подачі сигналу тривоги. Іншими словами, маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не будуть про це проінформовані.

Бранмауери прикладного рівня або проксі-сервери (сервери-посередники) встановлюють певний фізичний поділ між локальною мережею та Internet, тому вони відповідають найвищим вимогам безпеки, сервер-посередник використовує швидші комп'ютери.

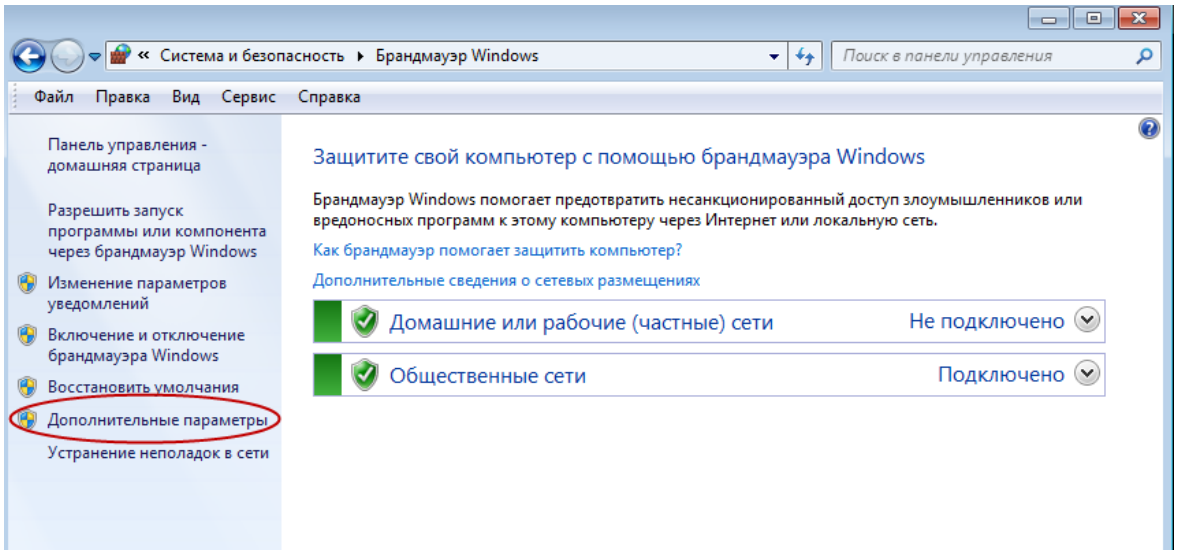
Для виконання лабораторної роботи необхідно пропустити ехо-запити за допомогою команди **ping** через брандмауер і **відмінити нове правило брандмауера після закінчення лабораторної роботи.** Необхідно створити нове правило, що дозволяє проходження ICMP -трафіку через брандмауер. Для цього у панелі управління виберіть пункт **Система і безпека**.



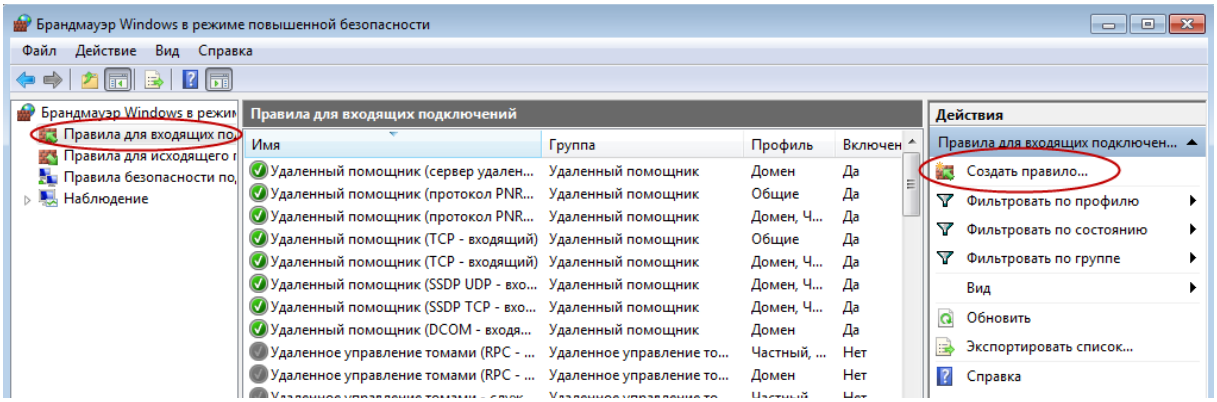
У вікні "Система і безпека" виберіть **Брандмауер Windows**.



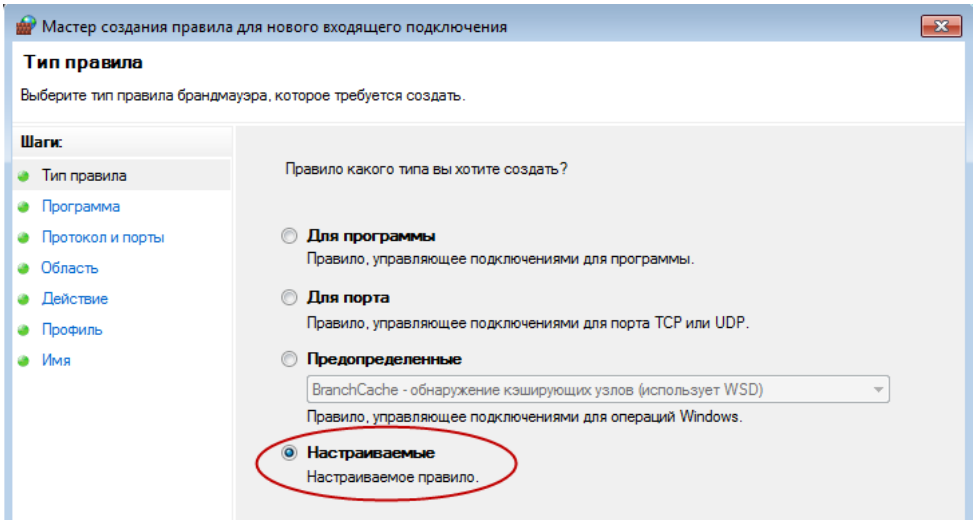
У лівій частині вікна "Брандмауер Windows" виберіть **Додаткові параметри**.



У вікні "Додаткові параметри" виберіть в лівій бічній панелі **Правила для вхідних підключень**, а потім **Створити правило**..в правій бічній панелі.

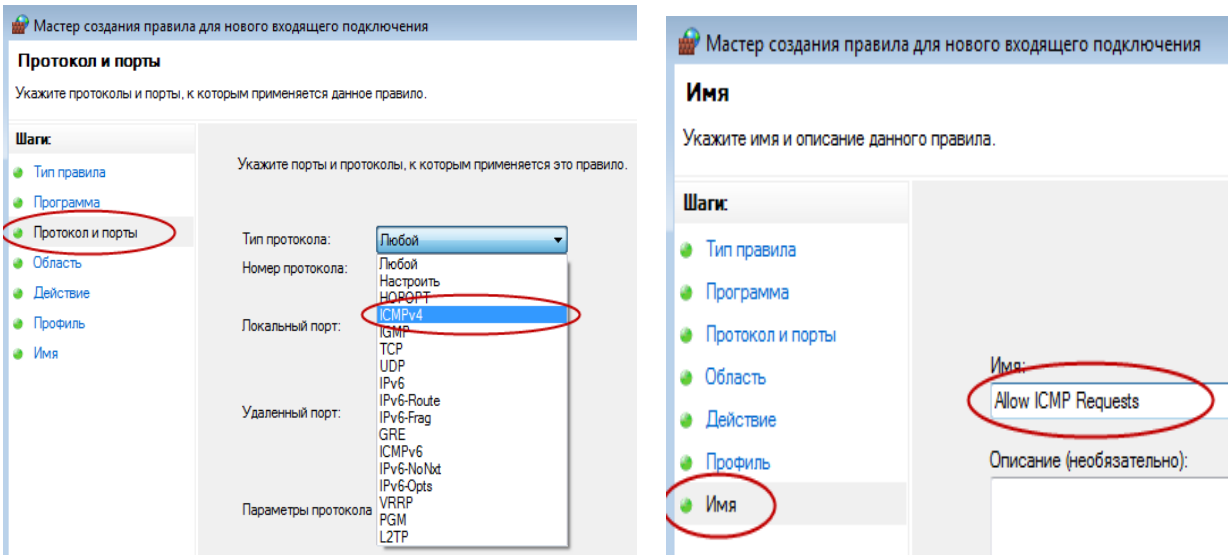


Відкриється майстер створення нових правил для вхідних підключень. У вікні "**Тип правила**" встановіть перемикач **Настроювані**, і натисніть кнопку **Далі**.



У лівій панелі виберіть **Протоколи і порти** і виберіть пункт **ICMPv4** в меню типів протоколу, що розкривається.

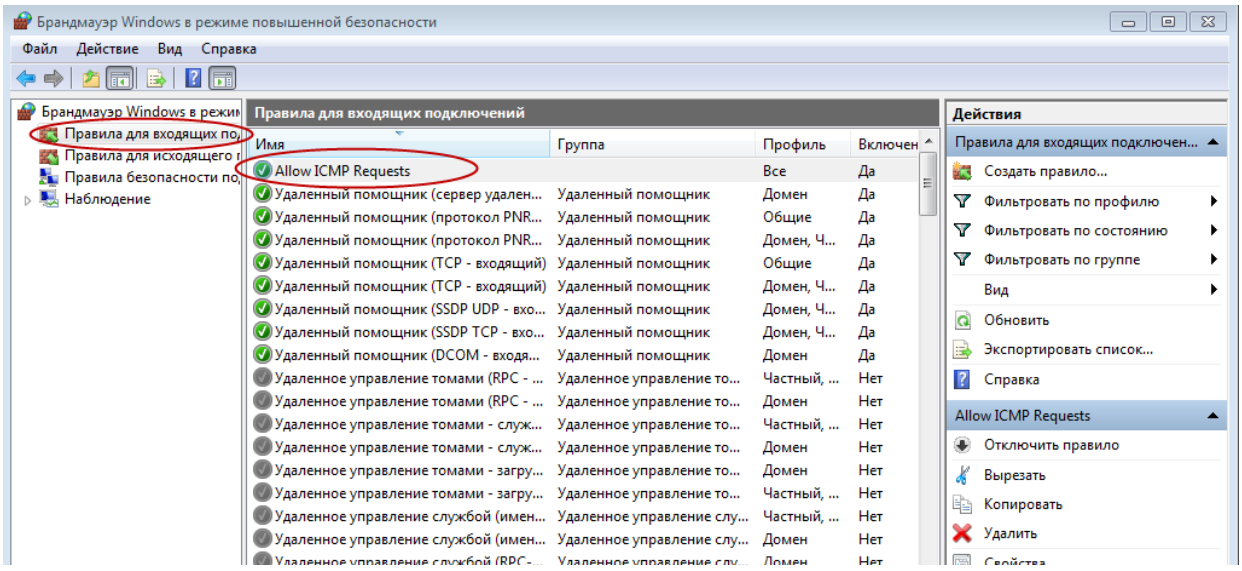
Після цього натисніть кнопку **Далі**. У лівій панелі виберіть Ім'я і введіть у відповідне поле **Allow ICMP Requests**. Натисніть кнопку **Finish** (Готово).



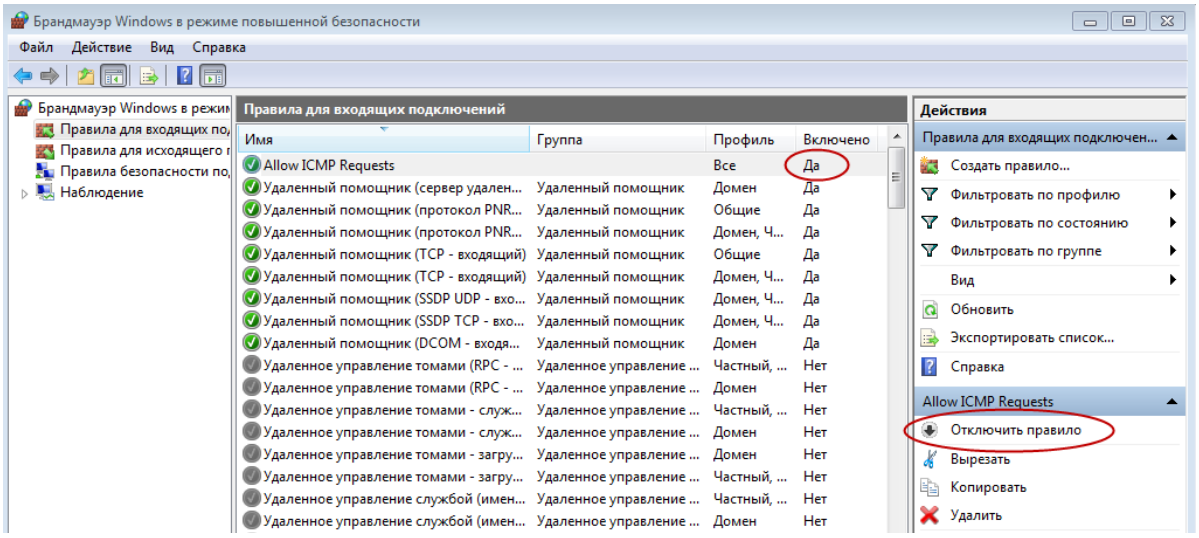
Створене правило дозволить іншому студенту отримувати ехо-відгуки з вашого ПК.

Відключіть і видаліть нове правило ICMP. Після закінчення лабораторної роботи **необхідно відключити або видалити нове створене правило**. Варіант **Відключити правило** дозволить знову включити його при необхідності. Повне видалення правила назавжди видалить його із списку правил для вхідних підключень.

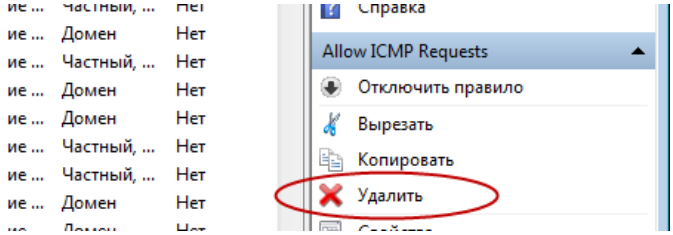
У лівій частині вікна "**Додаткові налаштування безпеки**" виберіть **Правила для вхідних підключень**, і знайдіть правило, створене в кроці 1.



Щоб відключити правило, виберіть варіант **Відключити правило**. Після цього він зміниться на варіант **Включити правило**. Правило можна включати і відключати. Стан правила відображується в стовпці "**Включено**" списку правил для вхідних підключень.



Щоб видалити правило ICMP назавжди, виберіть варіант **Видалити**. Після цього для дозволу запитів ICMP це правило необхідно буде створити знову.



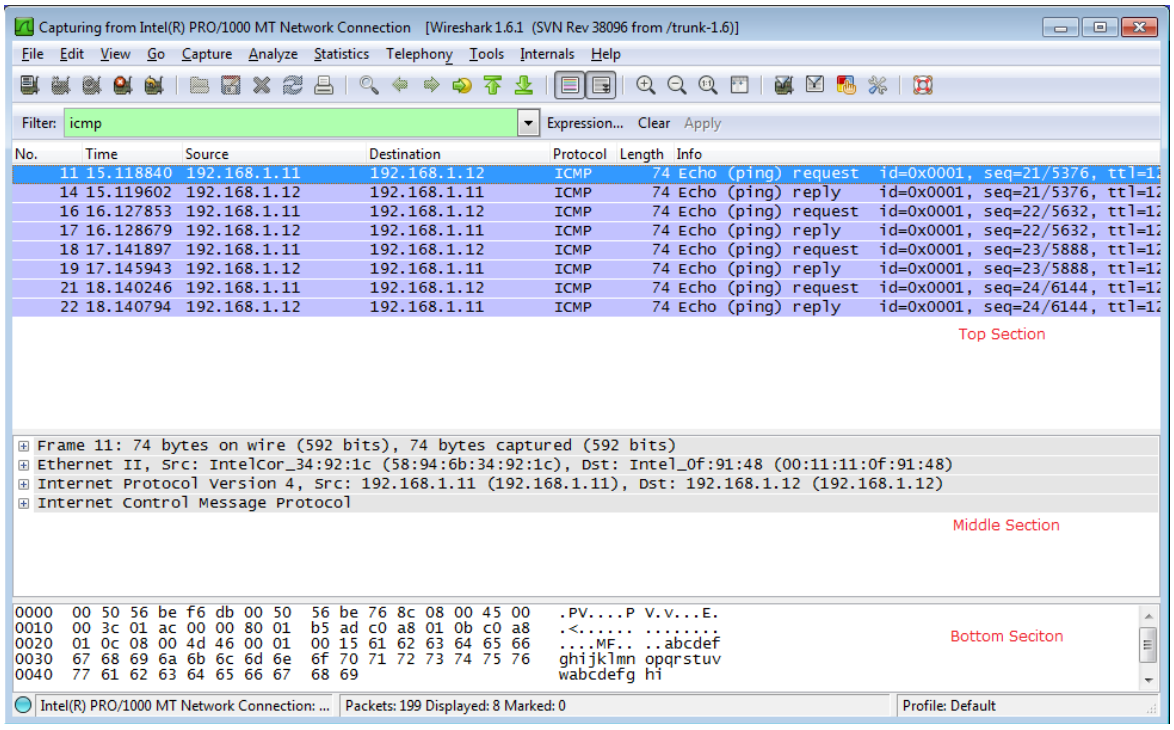
Далі потрібно перевірити дані, сформовані ехо-запитами за допомогою команди **ping** ПК іншого студента. Програма Wireshark відображує дані в трьох розділах:

1) у верхньому розділі відображується список отриманих кадрів PDU із звідною інформацією про IP -пакети;

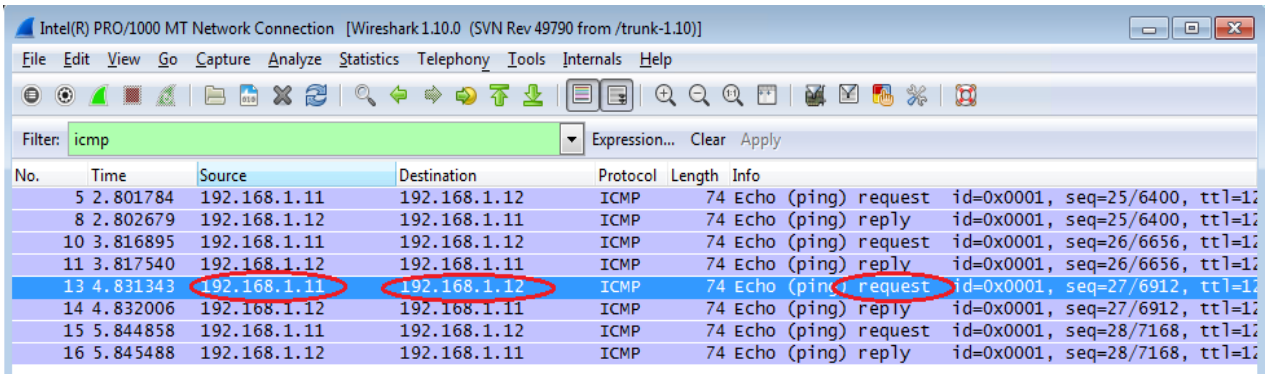
2) в середньому розділі приводиться інформація про PDU для кадру, вибраного у верхньому розділі екрану, і ділення кадру PDU на шари протоколів;

3) в нижньому розділі показуються необроблені дані кожного рівня.

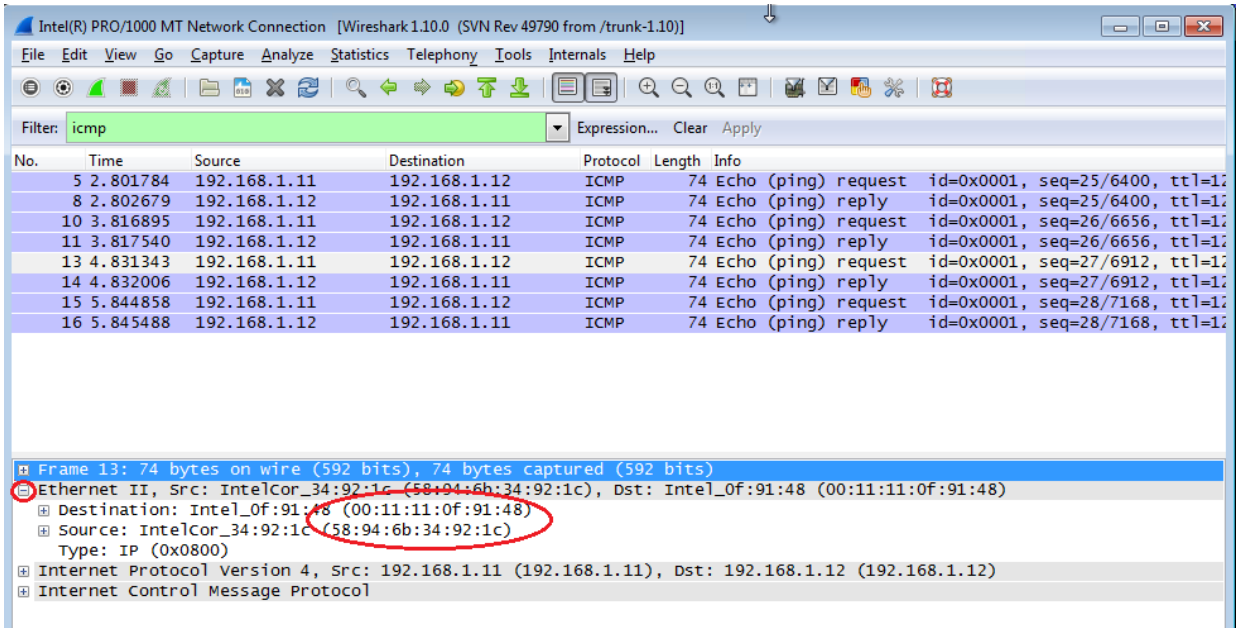
Необроблені дані відображуються як в шістнадцятковому, так і десятковому форматах.



Виберіть PDU-кадри першого запиту ICMP у верхньому розділі вікна програми Wireshark. Зверніть увагу на те, що в стовпці **Source** (Джерело) вказується IP-адреса вашого комп'ютера, а в стовпці **Destination** (Призначення) – IP-адреса ПК, якій ви відправили ехо-запит за допомогою команди **ping**.



Не міняючи вибір PDU -кадра у верхньому розділі програми, перейдіть в середній розділ. Натисніть на символ + зліва від рядка "Ethernet II", щоб побачити MAC-адреси джерела і призначення.



Чи співпадає MAC -адреса джерела з інтерфейсом вашого комп'ютера?

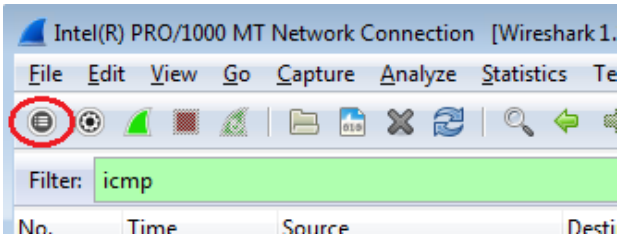
Чи співпадає MAC -адреса призначення в програмі Wireshark з MAC -адресою іншого студента? Як ваш ПК визначив MAC -адресу ПК, на який був відправлений ехо-запит за допомогою команди **ping**?

У прикладі перехопленого ICMP-запиту дані протоколу ICMP інкапсулюються усередині PDU-пакету IPv4 (заголовка IPv4), який потім інкапсулюється в пакеті кадру Ethernet II (заголовок Ethernet II) для передачі по локальній мережі.

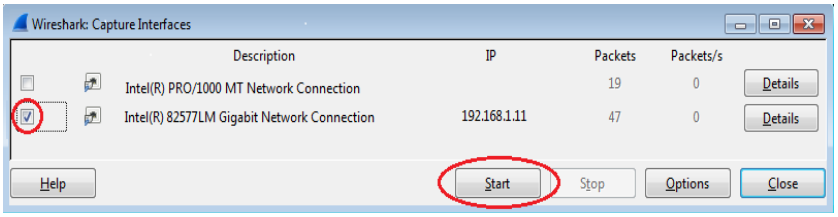
Збір і аналіз даних протоколу ICMP по віддалених вузлах в програмі Wireshark

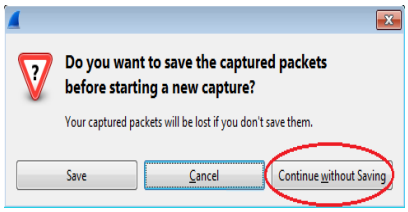
Далі вам потрібно відправити ехо-запити за допомогою команди **ping** на віддалені вузли (вузли за межами локальної мережі) і вивчити дані, сформовані цими запитами. Потім ви визначите відмінності між цими даними і даними, вивченими для локальної мережі. Запустіть перехоплення даних в інтерфейсі.

Натисніть на значок **Interface List** (Список інтерфейсів), щоб знову відкрити список інтерфейсів ПК.



Переконаєтеся в тому, що навпроти інтерфейсу локальної мережі встановлений прапорець, і натисніть кнопку **Start** (Почати).



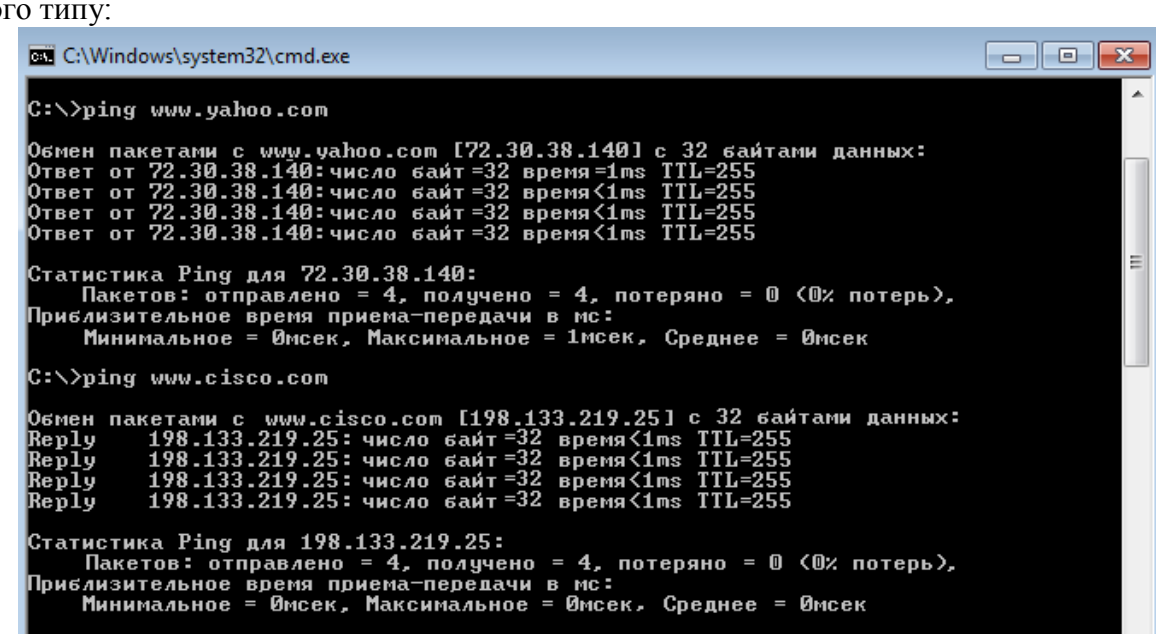


З'явиться вікно з пропозицією зберегти отримані раніше дані перед початком нового перехоплення. Зберігати ці дані необов'язково. Натисніть кнопку **Continue withoutSaving** (Продовжити без збереження).

Завдання для лабораторної роботи:

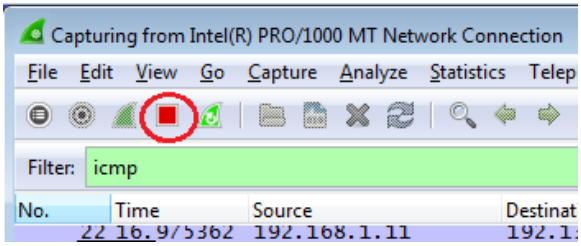
1. Налаштуйте локальну мережу з іншим студентом та виконайте збір даних протоколу ICMP засобами Wireshark згідно вказівок до лабораторної роботи. Перевірте, чи правильно ви визначили власну MAC-адресу та MAC-адресу іншого студента (в скріншоті виконання даного завдання необхідно зафарбувати перші/останні три символи отриманих MAC-адрес виходячи з конфіденційності інформації).

2. Необхідно перехопити дані протоколу ICMP для двох віддалених серверів. Активувавши перехоплення даних, відправте ехо-запит за допомогою команди **ping** на URL-адреси Серверу 1 та Серверу 2 (згідно варіанту) для перевірки можливості з'єднання. Наприклад, для серверів www.yahoo.com та www.cisco.com буде отримано ехо-відповіді такого типу:



При відправці ехо-запитів за допомогою команди **ping** на вказані URL -адреси зверніть увагу на те, що служба доменних імен (DNS) перетворить URL в IP -адресу. Запишіть IP -адреси, отримані для кожної URL –адреси (адреси можуть відрізнятися).

Зупиніть перехоплення даних, натиснувши на значок **Stop Capture** (Зупинити перехоплення).



Проаналізуйте дані, отримані від віддалених вузлів.

Прогляньте зібрані дані і вивчите IP - і MAC-адреси запрошених веб-сайтів. Вкажіть IP і MAC -адреси призначення для веб-сайтів:

Сервер 1: IP: _____._____._____._____ MAC: ____:____:____:____:____:____
Сервер 2: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

Яка особливість цих даних?

Чому програма Wireshark показує фактичну MAC -адресу локальних вузлів, але не відображає фактичну MAC -адресу віддалених вузлів?

Варіант	Сервер 1	Сервер 2
1	**32.** www.java.com	www.yahoo.com
2	**33.** www.google.com	www.cisco.com
3	www.gmail.com	**34.** www.facebook.com
4	www.ford.com	www.gokcecan.com
5	www.travelandleisure.com	www.phyton.com
6	www.apple.com	www.telegram.org
7	www.oracle.com	www.bbc.com
8	www.scopus.com	www.ibm.com
9	www.linkedin.com	**35.** www.java.com
10	www.att.com	www.chevron.com
11	www.yahoo.com	www.scopus.com
12	www.aig.com	www.verizon.com
13	www.chevron.com	www.linkedin.com
14	www.ibm.com	www.google.com
15	www.linkedin.com	www.apple.com
16	www.microsoft.com	www.verizon.com
17	www.cisco.com	www.scopus.com
18	www.pepsico.com	www.aig.com/
19	www.scopus.com	www.gmail.com
20	www.apple.com	www.cisco.com
21	www.verizon.com	www.att.com
22	www.facebook.com	www.ford.com
23	www.ibm.com	www.java.com
24	www.chevron.com	www.microsoft.com
25	www.ge.com	www.att.com

Вимоги до оформлення звіту

Звіт має включати:

1.Титульний аркуш.

2.Індивідуальне завдання на лабораторну роботу (скріншот завдання згідно варіанту).

3.Хід роботи (послідовний опис виконуваних кроків (з вказівкою їх суті) з скріншотами).

4.Висновки.

Питання для самоперевірки

1. Яке призначення програми Wireshark та які особливості її використання?
2. Яка структура вікна програми Wireshark?
3. Яка послідовність дій для збору та аналізу даних протоколу ICMP засобами Wireshark?
4. Яке призначення бранмауера?
5. Які є типи бранмауерів?
6. Чому програма Wireshark показує фактичну MAC -адресу локальних вузлів, але не показує фактичну MAC -адресу віддалених вузлів?

Рекомендована література

1.CNA R&S ITN // Електронний ресурс. режим доступу: http://static-course-assets.s3.amazonaws.com
2.Wireshark // Електронний ресурс. Режим доступу: www.wireshark.org
3. Міжмережевий екран. Захист локальної мережі // Електронний ресурс. Режим доступу: https://sites.google.com/site/zahistlokalnoiemerezi/zahist/mizmerezevij-ekran

ЛАБОРАТОРНА РОБОТА №5. IP-АДРЕСАЦІЯ. РОЗБИТТЯ МЕРЕЖІ НА ПІДМЕРЕЖІ

Мета: навчитися розраховувати число підмереж та вузлів за префіксом підмережі, розраховувати мережеву адресу, а також користуватися он-лайн калькуляторами для розрахунку основних кількісних та якісних показників заданих мереж.

Теоретичні відомості та вказівки щодо виконання завдання

При роботі з комп'ютерами і мережевими пристроями мережеві фахівці використовують двійкові, десяткові і шістнадцяткові числа. У операційну систему компанії Microsoft входить вбудований калькулятор. Версія калькулятора в ОС Windows 7 включає звичайний режим, який можна використовувати для виконання простих арифметичних задач, а також розширені можливості для програмних, наукових і статистичних розрахунків. Натисніть кнопку Пуск в ОС Windows і виберіть пункт "Усі програми". Відкрийте теку "Стандартні" і натисніть на "Калькулятор". Коли калькулятор відкриється, виберіть меню "Вид". Доступні чотири режими: Звичайний, Інженерний, Програміст і Статистика.

Переведення чисел з однієї системи числення в іншу

У режимі "Програміст" калькулятора Windows доступні декілька систем числення : **Hex** (шістнадцяткова з основою 16), **Dec** (десяткова з основою 10), **Oct** (вісімкова з основою 8) і **Bin** (двійкова з основою 2). Комп'ютери та інші електронні пристрої для зберігання і передачі даних, а також числових обчислень, використовують двійкову систему, що складається тільки з нулів і одиниць. Усі комп'ютерні розрахунки виконуються в двійковій (цифровий) формі, незалежно від того, в якому виді вони відображуються.

Шістнадцятковіі числа мають основу 16, а для представлення двійкових або десяткових еквівалентів використовується комбінація цифр від 0 до 9 і букв від A до F. Шістнадцяткові символи використовуються для відображення IPv6 - і MAC-адрес.

У цій лабораторній роботі калькулятор Windows 7 використовується для перетворення чисел між різними системами числення в режимі "Програміст". Відкрийте меню Вид і виберіть режим **Програміст**. Переведіть в двійкову, десяткову і шістнадцятиричну системи числення наступні числа:

Десятковий формат	Двійковий формат	Шістнадцятковий формат
175		
204		
19		
77		
56		
147		
228		

Перетворення IPv4 -адрес вузлів і масок підмережі в двійкову систему числення

IPv4 -адреси і маски підмережі виражаються в десятковому форматі з крапкою-роздільником (чотири октети), наприклад 192.168.1.10 і 255.255.255.0 відповідно. Кожен десятковий октет в адресі або масці можна перетворити в 8 двійкових розрядів. Октет завжди є 8 двійковими бітами. Тому **IPv4-адреса міститиме 32 біта нулів та одиниць.**

За допомогою калькулятора Windows переведіть IP -адресу 192.168.1.10 в двійковий формат і запишіть його в наступну таблицю:

Десятковий формат	Двійковий формат
192	
168	
1	
10	

Маски підмереж, такі як 255.255.255.0, також відображуються в десятковому форматі з точкою-роздільником. Маска підмережі завжди складається з чотирьох 8-розрядних октетів, кожен з яких виражається десятковим числом. За допомогою калькулятора Windows перетворіть вісім можливих десяткових значень октетів маски підмережі в двійкові числа і запишіть їх в наступну таблицю:

Десятковий формат	Двійковий формат
0	
128	
192	
224	
240	
248	
252	
254	
255	

Використовуючи комбінацію IPv4 -адреси і маски підмережі, можна визначити мережеву частину і розрахувати кількість вузлів, доступних в цій IPv4 -підмережі.

Визначення кількості вузлів в мережі за допомогою двох цифр

За адресою IPv4 -мережі і маскою підмережі можна визначити мережеву частину, а також кількість доступних в мережі вузлів.

Щоб розрахувати кількість вузлів в мережі, необхідно визначити мережеву і вузлову частини адреси.

Адреса і маска підмережі переводяться в двійкові числа на прикладі адреси 192.168.1.10 з підмережею 255.255.248.0. Записуючи результати перекладу даних в двійкові числа, виставте біти.

IP -адреса і маска підмережі в десятковому форматі	IP -адреса і маска підмережі в двійковому форматі
192.168.1.10	
255.255.248.0	

(Оскільки перші 21 біти **в масці підмережі йдуть підряд одиницями, це мережева частина адреси**, інші **11 біти - це вузлова частина адреси**).

Оскільки номер мережі і широкомовна адреса використовують дві адреси з підмережі, для визначення кількості доступних вузлів в IPv4 -підмережі потрібно цифру 2 піднести в степінь кількості вузлових бітів і відняти 2.

Кількість доступних вузлів = 2^(число бітів вузла) - 2

У цій мережі доступні приблизно 2046 вузлів (2^11-2). Знаючи кількість вузлових бітів, визначите кількість доступних вузлів і запишіть це значення в приведену нижче таблицю.

Кількість доступних вузлових бітів	Кількість доступних вузлів
5	
14	
24	
10	

Для цієї маски підмережі визначите кількість доступних вузлів і запишіть відповідь в приведену нижче таблицю.

Маска підмережі	Двійкова маска підмережі	Кількість доступних вузлових бітів	Кількість доступних вузлів
255.255.255.0	11111111.11111111.11111111.00000000		
255.255.240.0	11111111.11111111.11110000.00000000		
255.255.255.128	11111111.11111111.11111111.10000000		
255.255.255.252	11111111.11111111.11111111.11111100		
255.255.0.0	11111111.11111111.00000000.00000000		

Перетворення MAC - і IPv6 -адрес в двійкову форму

Для зручності адреси управління доступом до середовища передачі даних і адреси інтернет-протоколу версії 6 (IPv6) виражаються шістнадцятковими цифрами. Проте комп'ютери здатні розпізнавати і використовують для обчислень тільки двійкові цифри.

MAC-адреса (фізична адреса) зазвичай виражається 12 шістнадцятковими цифрами, згрупованими в пари і розділеними дефісами (-). У комп'ютерах на базі ОС Windows фізичні адреси зазвичай мають формат xx - xx - xx - xx - xx - xx, де x - це цифра від 0 до 9 або латинська буква від A до F. Кожну шістнадцяткову цифру в адресі можна конвертувати в чотири двійкові розряди, зрозумілих комп'ютеру.

Переведення IPv6 -адреси в двійкове число

Для зручності IPv6 -адреси також записують шістнадцятковими символами. Для комп'ютерів ці IPv6 -адреси можна переводити в двійкові цифри. IPv6-адреса – це двійкові числа, представлені у вигляді зрозумілого для людини запису: 2001:0 DB8: ACAD:0001:0000:0000:0000:0001 або в короткій формі: 2001: DB8: ACAD:1::1.

Довжина IPv6 -адреси складає 128 біт. За допомогою калькулятора Windows переведіть IPv6 -адресу в двійкове число і запишіть результат в приведену нижче таблицю.

Шістнадцятковий формат	Двійковий формат
2001	
00DB8	
ACAD	
0001	
0000	
0000	
0000	
0001	

Конвертація IPv4 -адрес в двійкову систему числення

Кожна IPv4 -адреса складається з двох частин – мережевої і вузлової. Мережева частина адреси однакова для усіх пристроїв, які знаходяться в одній і тій же мережі. Вузлова частина визначає конкретний вузол в межах відповідної мережі. **Маска підмережі використовується для визначення мережевої частини IP -адреси.** Пристрої в одній мережі можуть обмінюватися даними безпосередньо; для взаємодії між пристроями з різних мереж потрібно проміжний пристрій рівня 3, наприклад, маршрутизатор.

Щоб зрозуміти принцип роботи пристроїв в мережі, необхідно побачити адреси в тому виді, в якому з ними працюють пристрої, – в двійковому представленні. Для цього необхідно перевести IP -адресу та її маску підмережі з десяткового представлення з крапками в двійкове значення. Після цього можна визначити мережеву адресу за допомогою побітової операції **I (AND).**

Розглянемо порядок визначення мережевої і вузлової частин IP -адрес. Для цього треба перевести адреси і маски підмережі з десяткового представлення з крапками в двійковий формат, а потім застосувати побітову операцію **I.** Після цього скористатися отриманою інформацією для визначення адрес в мережі.

Спочатку вам необхідно перевести десяткові числа в двійковий еквівалент. Виконавши це завдання, конвертуйте IPv4 -адреси і маски підмережі з десяткового представлення з точками в двійкову систему.

Заповніть таблицю, перетворивши десяткове число в 8-бітове двійкове значення. Перше число вже перетворене для прикладу. Пам'ятайте, що вісім двійкових бітових значень в октеті мають основу 2 і зліва направо виглядають як 128, 64, 32, 16, 8, 4, 2 і 1.

Десяткове представлення	Двійкове представлення
192	11000000
168	
10	
255	
2	

IPv4 -адреси перетворяться так само, як і було описано вище. Заповніть приведену нижче таблицю двійковими еквівалентами вказаних адрес. Щоб ваші відповіді було простіше сприймати, розділяйте двійкові октети крапками.

Десяткове представлення	Двійкове представлення
192.168.10.10	11000000.10101000.00001010.00001010
209.165.200.229	
172.16.18.183	
10.86.252.17	
255.255.255.128	
255.255.192.0	

Використання побітової операції I для визначення мережевих адрес

Розрахуємо мережеву адресу для наявних адрес вузлів за допомогою побітової операції **I**. Спочатку вам необхідно перевести десяткову IPv4 -адресу і маску підмережі в їх двійковий еквівалент. Отримавши мережеву адресу в двійковому форматі, переведемо її в десятковий. При використанні операції **I** десяткове значення в кожній бітовій позиції 32-бітової IP -адреси вузла порівнюється з відповідною позицією в 32-бітовій масці підмережі. За наявності двох нулів або 0 і 1 результатом операції **I** буде 0. За наявності двох одиниць результатом буде 1, як показано в наведеному прикладі.

Приклад. Визначити, скільки біт треба використовувати для розрахунку мережевої адреси.

Опис	Десяткове представлення	Двійкове представлення
IP -адреса	192.168.10.131	11000000.10101000.00001010.10000011
Маска підмережі	255.255.255.192	11111111.11111111.11111111.11000000
Мережева адреса	192.168.10.128	11000000.10101000.00001010.10000000

Для розрахунку мережевої адреси використовуються біти, які в двійковій масці підмережі мають значення 1. У наведеному вище прикладі використовується 26 біт для розрахунку мережевої адреси.

Виконайте операцію I, щоб визначити мережеву адресу.

Введіть відсутню інформацію в таблицю нижче **(для непарного варіанту):**

Опис	Десяткове представлення	Двійкове представлення
IP -адреса	172.16.145.29	
Маска підмережі	255.255.0.0	
Мережева адреса		

Опис	Десяткове представлення	Двійкове представлення
IP -адреса	192.168.10.10	
Маска підмережі	255.255.255.0	
Мережева адреса		

Введіть відсутню інформацію в таблицю нижче **(для парного варіанту):**

Опис	Десяткове представлення	Двійкове представлення
IP -адреса	192.168.68.210	
Маска підмережі	255.255.255.128	
Мережева адреса		

Опис	Десяткове представлення	Двійкове представлення
IP -адреса	172.16.188.15	
Маска підмережі	255.255.240.0	
Мережева адреса		

Застосування розрахунків мережевих адрес

Вам необхідно розрахувати мережеву адресу для вказаних IP -адрес і масок підмережі. Отримавши мережеву адресу, записати відповіді, необхідні для виконання цієї лабораторної роботи.

Визначіть, чи знаходяться IP -адреси в одній і тій же мережі.

(для непарного варіанту)

Налаштування двох ПК для мережі. Комп'ютеру ПК-А присвоєна IP -адреса 192.168.1.18, а комп'ютеру ПК-Б - IP -адреса 192.168.1.33. Маска підмережі обох комп'ютерів - 255.255.255.240.

Яка мережева адреса у ПК-А? _____

Яка мережева адреса у ПК-Б? _____

Чи зможуть ці ПК взаємодіяти один з одним безпосередньо? _____

Яка найбільша адреса, присвоєна комп'ютеру ПК-Б, дозволить йому знаходитися в одній мережі з ПК-А? _____

Визначіть, чи знаходяться IP -адреси в одній і тій же мережі.

(для парного варіанту)

Налаштування двох ПК для мережі. Комп'ютеру ПК-А присвоєна IP -адреса 10.0.0.16, а комп'ютеру ПК-Б - IP -адреса 10.1.14.68. Маска підмережі обох комп'ютерів - 255.254.0.0.

Яка мережева адреса у ПК-А? _____

Яка мережева адреса у ПК-Б? _____

Чи зможуть ці ПК взаємодіяти один з одним безпосередньо? _____

Яка найменша адреса, присвоєна комп'ютеру ПК-Б, дозволить йому знаходитися в одній мережі з ПК-А? _____

Встановіть адресу шлюзу за замовчуванням (для непарного варіанту)

У вашій компанії діє політика використання першої IP -адреси в мережі в якості адреси шлюзу за замовчуванням. Вузол в локальній мережі має IP -адресу 172.16.140.24 і маску підмережі 255.255.192.0.

Яка у цієї мережі мережева адреса? _____

Яка адреса має шлюз за замовчуванням для цього вузла? _____

Встановіть адресу шлюзу за замовчуванням (для парного варіанту)

У вашій компанії діє політика використання першої IP -адреси в мережі в якості адреси шлюзу за замовчуванням. Ви отримали вказівку налаштувати новий сервер з IP -адресою 192.168.184.227 і маскою підмережі 255.255.255.248.

Яка у цієї мережі мережева адреса? _____

Яким буде шлюз за замовчуванням для цього сервера? _____

Визначення IPv4 -адрес

Заповніть таблиці відповідними даними.

Проаналізуйте приведену нижче таблицю і визначите мережеву і вузлову частини вказаних IPv4 -адрес.

Перші два рядки містять приклади заповнення таблиці.

Скорочення, що використовуються в таблиці:

М = усі 8 біт для октету містяться в мережевій частині адреси

м = біт в мережевій частині адреси

В = усі 8 біт для октету містяться у вузловій частині адреси

в = біт у вузловій частині адреси

IP - адреса/префікс	**Мережа/вузол** **М, м = мережа** **В, в = вузол**	**Маска підмережі**	**Мережева адреса**
192.168.10.10/24	М. М. М. В	255.255.255.0	192.168.10.0
10.101.99.17/23	М. М. ммммммв.В	255.255.254.0	10.101.98.0
172.31.45.252/24			
10.1.8.200/26			
172.16.117.77/20			
10.1.1.101/25			
209.165.202.140/27			
192.168.28.45/28			

Проаналізуйте приведену нижче таблицю і вкажіть діапазон адрес вузлів і широкомовних адрес у вигляді пари маски підмережі і префікса.

IP -адреса/префікс	**Адреса першого вузла**	**Адреса останнього вузла**	**Широкомовна адреса**
192.168.10.10/24	192.168.10.1	192.168.10.254	192.168.10.255
10.101.99.17/23			
209.165.200.227/27			
172.31.45.252/24			
10.1.8.200/26			
172.16.117.77/20			
10.1.1.101/25			
209.165.202.140/27			
192.168.28.45/28			

Класифікація IPv4 -адрес

Вам необхідно визначити і класифікувати декілька прикладів IPv4 -адрес.

Проаналізуйте приведену нижче таблицю і визначите тип адреси (адреса мережі, вузла, багатоадресної або широкомовної розсилки).

У першому рядку наведений приклад завершення таблиці.

IP -адреса	Маска підмережі	Тип адреси
10.1.1.1	255.255.255.252	вузол
192.168.33.63	255.255.255.192	широкомовна розсилка
239.192.1.100	255.252.0.0	багатоадресна розсилка
172.25.12.52	255.255.255.0	
10.255.0.0	255.0.0.0	
172.16.128.48	255.255.255.240	
209.165.202.159	255.255.255.224	
172.16.0.255	255.255.0.0	
224.10.1.11	255.255.255.0	

Проаналізуйте приведену нижче таблицю і визначите тип адреси - загальний або приватний.

IP -адреса/префікс	Загальний або приватний
209.165.201.30/27	Загальний
192.168.255.253/24	Приватний
10.100.11.103/16	
172.30.1.100/28	
192.31.7.11/24	
172.20.18.150/22	
128.107.10.1/16	
192.135.250.10/24	
64.104.0.11/16	

Проаналізуйте приведену нижче таблицю і визначите, чи являється пара адреси і префікса допустимою адресою вузла.

IP -адреса/префікс	Допустима адреса вузла?	Причина
127.1.0.10/24		
172.16.255.0/16	Так	Адреса вузла
241.19.10.100/24	Ні	Зарезервовано
192.168.0.254/24		
192.31.7.255/24	Ні	Широкомовна розсилка
64.102.255.255/14		
224.0.0.5/16	Ні	Багатоадресна розсилка
10.0.255.255/8		
198.133.219.8/24		

Розрахунок підмереж IPv4

Уміння працювати з підмережами IPv4 і визначати інформацію про мережі і вузли на основі відомої IP -адреси і маски підмережі потрібні для розуміння принципів роботи IPv4 -мереж. Необхідно розраховувати IP -адресу мережі на основі відомої IP -адреси і маски підмережі.

Знаючи IP -адресу і маску підмережі, можна встановити наступні дані підмережі:

- мережеву адресу;
- широкомовну адресу;
- загальну кількість бітів вузлів;
- кількість вузлів в підмережі;

Визначати для вказаної IP -адреси і маски підмережі :

- мережеву адресу цієї підмережі;
- широкомовну адресу цієї підмережі;
- діапазон адрес вузлів для цієї підмережі;
- кількість створених підмереж;
- кількість вузлів для кожної підмережі.

Щоб визначити мережеву адресу, необхідно виконати бінарну операцію **I** для IPv4 -адреси, використовуючи вказану маску підмережі. В результаті отримаємо мережеву адресу. Якщо маска підмережі має в октеті десяткове значення 255, результатом ЗАВЖДИ буде початкове значення цього октету. Якщо маска підмережі має в октеті десяткове значення 0, результатом для цього октету ЗАВЖДИ буде 0.

Приклад.

IP -адреса **192.168.10.10**

Маска підмережі **255.255.255.0**

==========

Результат (мережа) **192.168.10.0**

Знаючи це, можна виконати бінарну операцію **I** тільки для того октету, значення якого в масці підмережі відрізняється від 255 або 0.

Приклад.

IP -адреса **172.30.239.145**

Маска підмережі **255.255.192.0**

Проаналізувавши цей приклад, ми бачимо, що бінарна операція **I** вимагається тільки для третього октету. У цій масці підмережі перші два октети дадуть результат 172.30, а четвертий - 0.

IP -адреса **172.30.239.145**

Маска підмережі **255.255.192.0**

==========

Результат (мережа) **172.30.?.0**

Виконайте бінарну операцію **I** для третього октету.

	Десяткове	**Двійкове**
	239	11101111
	192	11000000
	=======	
Результат	**192**	**11000000**

Аналіз цього прикладу знову дасть наступний результат:

IP –адреса **172.30.239.145**

Маска підмережі **255.255.192.0**

==========

Результат (мережа) **172.30.192.0**

Розрахувати кількість вузлів для кожної мережі в цьому прикладі можна шляхом аналізу маски підмережі. Маска підмережі буде представлена в десятковому форматі з точкою-роздільником, наприклад 255.255.192.0, або у форматі мережевого префікса, наприклад /18. IPv4 -адреса завжди містить 32 біта. Віднявши кількість бітів, що використовуються мережевою частиною (як показано в масці підмережі), ви отримаєте кількість бітів, використовуваних для вузлів.

У нашому прикладі маска підмережі 255.255.192.0 рівна **/18** в префіксному записі. Віднімання **18 біт** мережі з 32 біт дасть нам **14 біт, що залишилися для вузлової частини.**

Виходячи з цього, можна виконати простий розрахунок:

2 ^(кількість бітів вузла) - 2 = кількість вузлів

2^14 - 2 = 16 382 вузли

Визначте мережеві і широкомовні адреси і кількість бітів вузлів для IPv4 -адрес і префіксів, вказаних в приведеній нижче таблиці.

Адреса IPv4/префікс	Мережева адреса	Широкомовна адреса	Загальна кількість бітів вузлів	Загальна кількість вузлів
192.168.100.25/28	192.168.100.16	192.168.100.31	4	14
172.30.10.130/30				
10.1.113.75/19				
198.133.219.250/24				
128.107.14.191/22				
172.16.104.99/27				

Розрахунок даних мережі за IPv4 -адресою

Приклад.

Дано:	
IP -адреса вузла	172.16.77.120
Початкова маска підмережі	255.255.0.0
Нова маска підмережі	255.255.240.0
Знайти:	
Кількість бітів підмережі	4
Кількість створених підмереж	16
Кількість бітів вузлів в підмережі	12
Кількість вузлів в підмережі	4094
Мережева адреса цієї підмережі	172.16.64.0
Адреса IPv4 першого вузла в цій підмережі	172.16.64.1
Адреса IPv4 останнього вузла в цій підмережі	172.16.79.254
Широкомовна адреса IPv4 в цій підмережі	172.16.79.255

Розглянемо, як була отримана така таблиця.

Початкова маска підмережі мала вигляд **255.255.0.0 або /16**. Нова маска підмережі – **255.255.240.0 або /20**. Отримана різниця складає 4 біта. Оскільки 4 біта були запозичені, ми можемо визначити, що було створено 16 підмереж, оскільки 2^4= 16.

У новій масці, рівній 255.255.240.0 або /20, залишається 12 біт для вузлів. Якщо для вузлів залишилося 12 біт, скористаємося наступною формулою: 2^12-2= 4096-2=4094 вузли для кожної підмережі.

Бінарна операція **І** допоможе визначити підмережу для цього завдання, внаслідок чого ми отримаємо мережу 172.16.64.0.

Один із способів визначення діапазону вузлів – використовувати двійкові значення для вузлової частини адреси. У нашому прикладі вузлова частина – це останні 12 біт адреси. У першому вузлі для усіх старших бітів буде встановлено значення 0, а для молодшого біта – значення 1. У останньому вузлі для усіх старших бітів буде встановлено значення 1, а для молодшого біта – значення 0. В даному прикладі вузлова частина адреси знаходиться в третьому та четвертому октетах.

Опис	**1-й октет**	**2-й октет**	**3-й октет**	**4-й октет**	**Опис**
Мережа/вузол	**мммммммм**	**мммммммм**	**ммммвввв**	вввввввв	Маска підмережі
Двійкове	**10101100**	**00010000**	**0100**0000	00000001	Перший вузол
Десяткове	172	16	64	1	Перший вузол
Двійкове	**10101100**	**00010000**	**0100**1111	11111110	Останній вузол
Десяткове	172	16	79	254	Останній вузол
Двійкове	**10101100**	**00010000**	**0100**1111	11111111	Широкомовна
Десяткове	172	16	79	255	Широкомовна

Заповніть приведені нижче таблиці, вказавши необхідні значення для вказаної IPv4 -адреси, а також початкової і нової масок підмережі.

(непарний варіант)

Завдання 1.

Дано:	
IP -адреса вузла	192.168.200.139
Початкова маска підмережі	255.255.255.0
Нова маска підмережі	255.255.255.224
Знайти:	
Кількість бітів підмережі	
Кількість створених підмереж	
Кількість бітів вузлів в підмережі	
Кількість вузлів в підмережі	
Мережева адреса цієї підмережі	
Адреса IPv4 першого вузла в цій підмережі	
Адреса IPv4 останнього вузла в цій підмережі	
Широкомовна адреса IPv4 в цій підмережі	

Завдання 2.

Дано:	
IP -адреса вузла	10.101.99.228
Початкова маска підмережі	255.0.0.0
Нова маска підмережі	255.255.128.0
Знайти:	
Кількість бітів підмережі	
Кількість створених підмереж	
Кількість бітів вузлів в підмережі	
Кількість вузлів в підмережі	
Мережева адреса цієї підмережі	
Адреса IPv4 першого вузла в цій підмережі	
Адреса IPv4 останнього вузла в цій підмережі	
Широкомовна адреса IPv4 в цій підмережі	

(парний варіант)

Завдання 1.

Дано:	
IP -адреса вузла	172.22.32.12
Початкова маска підмережі	255.255.0.0
Нова маска підмережі	255.255.224.0
Знайти:	
Кількість бітів підмережі	
Кількість створених підмереж	
Кількість бітів вузлів в підмережі	
Кількість вузлів в підмережі	
Мережева адреса цієї підмережі	
Адреса IPv4 першого вузла в цій підмережі	
Адреса IPv4 останнього вузла в цій підмережі	
Широкомовна адреса IPv4 в цій підмережі	

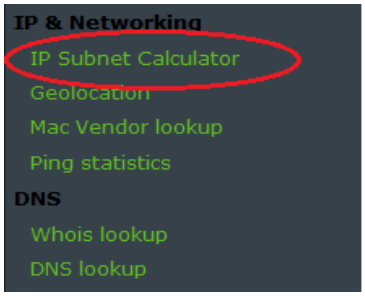
Завдання 2.

Дано:	
IP -адреса вузла	192.168.1.245
Початкова маска підмережі	255.255.255.0
Нова маска підмережі	255.255.255.252
Знайти:	
Кількість бітів підмережі	
Кількість створених підмереж	
Кількість бітів вузлів в підмережі	
Кількість вузлів в підмережі	
Мережева адреса цієї підмережі	
Адреса IPv4 першого вузла в цій підмережі	
Адреса IPv4 останнього вузла в цій підмережі	
Широкомовна адреса IPv4 в цій підмережі	

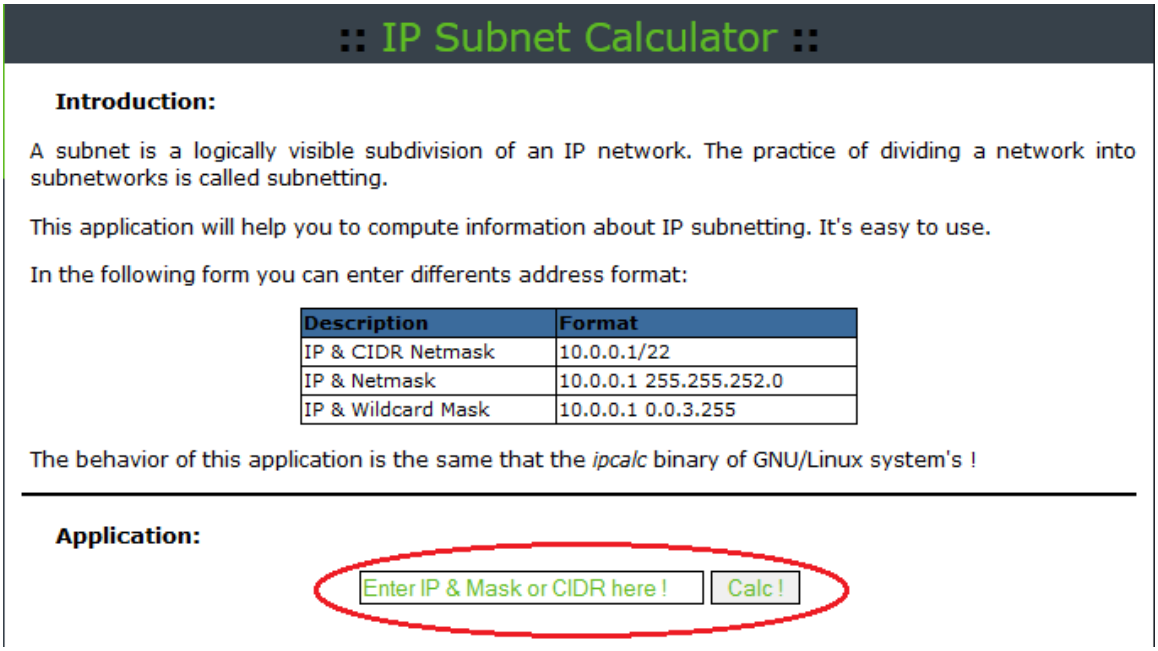
Вивчення калькуляторів підмереж

Розуміння принципів перетворення десяткової IP-адреси в двійковий формат і застосування побітової операції **I** для визначення мережевої адреси є важливим, але сама процедура є трудомістким процесом з великою ймовірністю помилок. Для спрощення розрахунків багато мережевих адміністраторів використовують **програми-калькулятори для IP -підмереж**. Існує цілий ряд подібних програм, які можна завантажити і встановити або запускати безпосередньо з Інтернету.

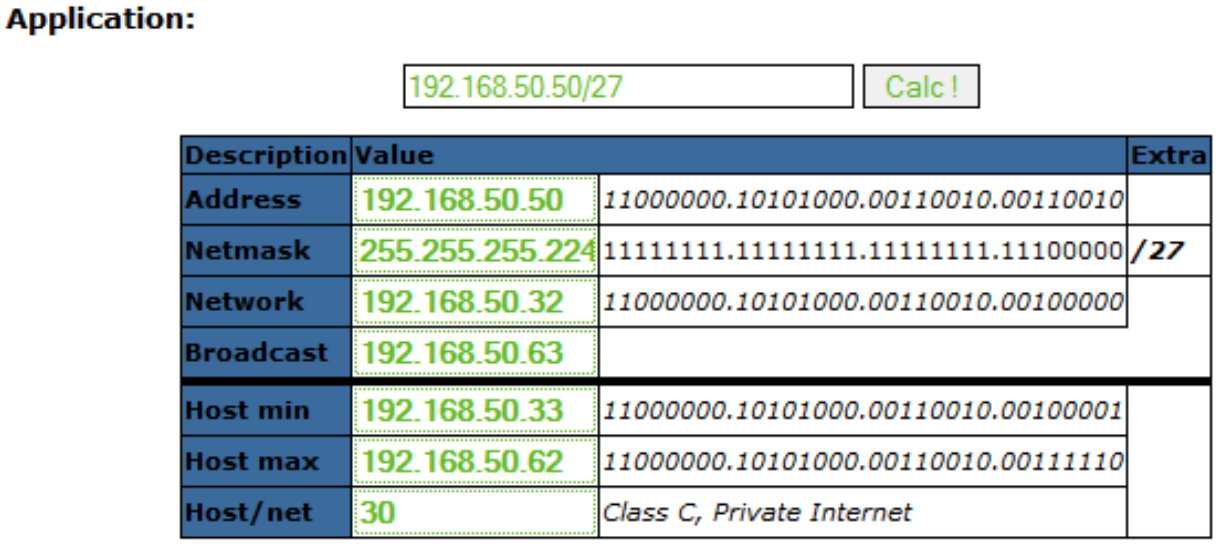
Для розрахунку мережевих даних будемо використовувати веб-калькулятор для IP -підмереж. Наприклад, компанія **Solarwinds** пропонує безкоштовний калькулятор підмереж, який можна завантажити і встановити на комп'ютер під управлінням ОС Windows. Завантажити і встановити калькулятор підмереж **Solarwinds** можна з веб-сайту компанії **www.solarwinds.com**. Якщо ви використовуєте комп'ютер під управлінням **ОС Linux**, можна використовувати утиліту **ipcalc**, яку можна знайти в більшості версій системи Linux. Для установки утиліти **ipcalc** на комп'ютер під управлінням **Linux** скористайтеся командою **apt - get install ipcalc**. Відкрийте браузер, перейдіть на сайт **www.ipcalc.org** і виберіть посилання **IP Subnet Calculator** (Калькулятор IP -підмереж).У цьому меню доступні і інші корисні утиліти, такі як засіб для пошуку виробників по MAC -адресам (Mac Vendor lookup) або сервіси WHOIS (Whois lookup) і DNS (DNS lookup) для отримання інформації про домени.



Натисніть посилання **IP Subnet Calculator** (Калькулятор IP - підмереж), і введіть у вікні IP, що відкрилося, -адресу і маску підмережі або IP -адресу і префіксний запис CIDR.



У полі **Application** (Застосування) введіть 192.168.50.50/27 і натисніть кнопку **Calc!** (Розрахувати). Нижче з'явиться таблиця з інформацією про мережу в десятковому і двійковому форматах.



У даному випадку: мережева адреса 192.168.50.32; маска підмережі 255.255.255.224; мережа підтримує 30 вузлів; найменша адреса вузла 192.168.50.33; найбільша адреса вузла 192.168.50.62; широкомовна адреса 192.168.50.63.

Розрахунок мережевих даних за допомогою калькулятора підмереж

Заповніть таблиці, користуючись веб-калькулятором підмереж на сайті **www.ipcalc.org.**

(непарний варіант)

1. Заповніть приведену нижче таблицю для адреси 10.223.23.136/10.

Опис	Десяткове представлення	Двійкове представлення
Адреса	10.223.23.136	
Маска підмережі		
Мережева адреса		
Широкомовна адреса		
Адреса першого вузла		
Адреса останнього вузла		
Число доступних вузлів		Недоступно

Загальний або приватний тип адреси? _____

2. Заповніть приведену нижче таблицю, використовуючи адресу 192.168.184.78 з маскою підмережі 255.255.255.252.

Опис	Десяткове представлення	Двійкове представлення
Адреса	192.168.184.78	
Маска підмережі		
Мережева адреса		
Широкомовна адреса		
Адреса першого вузла		
Адреса останнього вузла		
Число доступних вузлів		Недоступно

Який в цій мережі префіксний запис CIDR? ___Загальний або приватний тип адреси?

(парний варіант)

1. **Заповніть приведену нижче таблицю для адреси 172.18.255.92 з маскою підмережі 255.255.224.0.**

Опис	Десяткове представлення	Двійкове представлення
Адреса	172.18.255.92	
Маска підмережі	255.255.224.0	
Мережева адреса		
Широкомовна адреса		
Адреса першого вузла		
Адреса останнього вузла		
Число доступних вузлів		Недоступно

Загальний або приватний тип адреси? _____

2.Заповнітьприведену нижче таблицю для адреси 209.165.200.225/27.

Опис	Десяткове представлення	Двійкове представлення
Адреса	209.165.200.225	
Маска підмережі		
Мережева адреса		
Широкомовна адреса		
Адреса першого вузла		
Адреса останнього вузла		
Число доступних вузлів		Недоступно

Загальний або приватний тип адреси? __ Який в цій мережі префіксний запис CIDR? __

Завдання для лабораторної роботи:

Необхідно заповнити усі незаповнені поля таблиць та відповісти на питання, поставлені у вказівках до виконання лабораторної роботи.

Вимоги до оформлення звіту

Звіт має включати: титульний аркуш, хід роботи з скріншотами завдань та виконаними розрахунками (цей розділ складається з послідовного опису виконуваних обчислень (з вказівкою їх суті) та висновки.

Питання для самоперевірки

1. У чому перевага програм та веб-калькуляторів для розрахунку підмереж?
2. Яка роль при визначенні мережевої адреси маски підмережі?
3. Чому необхідно продовжувати вивчення IPv4 -адресації, якщо доступний простір IPv4 - адрес вичерпаний?
4. Яке значення має маска підмережі при аналізі IPv4 -адреси?
5. Які ви знаєте правила для визначення мережевої адреси вузла, визначення кількості підмереж та вузлів за маскою?
6. Як можна визначити адресу першого та останнього вузла, широкомовну адресу?

Рекомендована література

1.CNA R&S // Електронний ресурс. режим доступу: http://static-course-assets.s3.amazonaws.com
2. Ділення IP-мережі на підмережі // Електронний ресурс. Режим доступу: http://zaycev.me/index.php/myblog/entry/2015/08/04/razbienie-ipv4-seti-na-podseti
3. VLSM (CIDR) Subnet Calculator // Електронний ресурс. Режим доступу: http://www.vlsm-calc.net
4. IP-адресація і створення підмереж для нових користувачів // Електронний ресурс. Режим доступу: http://www.cisco.com
5. Розрахунок кількості хостів та підмереж на основі IP-адреси і маски // Електронний ресурс. Режим доступу: https://help.keenetic.net
6. Solarwinds // Електронний ресурс. Режим доступу: www.solarwinds.com.

ЛАБОРАТОРНА РОБОТА №6. СТВОРЕННЯ І НАЛАШТУВАННЯ VLAN

Мета: навчитися створювати та налаштовувати VLAN в локальній мережі, змінювати приналежніть вузлів до різних VLAN в мережі, видаляти та змінювати VLAN.

Теоретичні відомості

В цілях підвищення продуктивності мережі великі широкомовні домени 2-го рівня ділять на домени меншого розміру. Для цього сучасні комутатори використовують **віртуальні локальні мережі (VLAN)**. Також мережі VLAN можна використовувати для визначення вузлів, між якими можливий обмін даними, що дозволяє підвищити рівень безпеки.

Транкові канали мережі VLAN використовуються для поширення мереж VLAN по різних пристроях та дозволяють передачу трафіку з множини мереж VLAN через один канал, не завдаючи шкоди ідентифікації і сегментації мережі VLAN.

Створення транкового каналу мережі VLAN між двома комутаторами необхідне для того, щоб вузли в межах однієї мережі VLAN могли обмінюватися даними по транку незалежно від того, до якого комутатора підключений вузол.

Вказівки щодо виконання завдання

Розглянемо приклад створення мережі VLAN на двох комутаторах в локальній мережі для логічного розмежування трафіку студентів та викладачів, налаштування параметрів VLAN на комутаторах, перевірки коректності роботи мереж VLAN (рис.6.1).

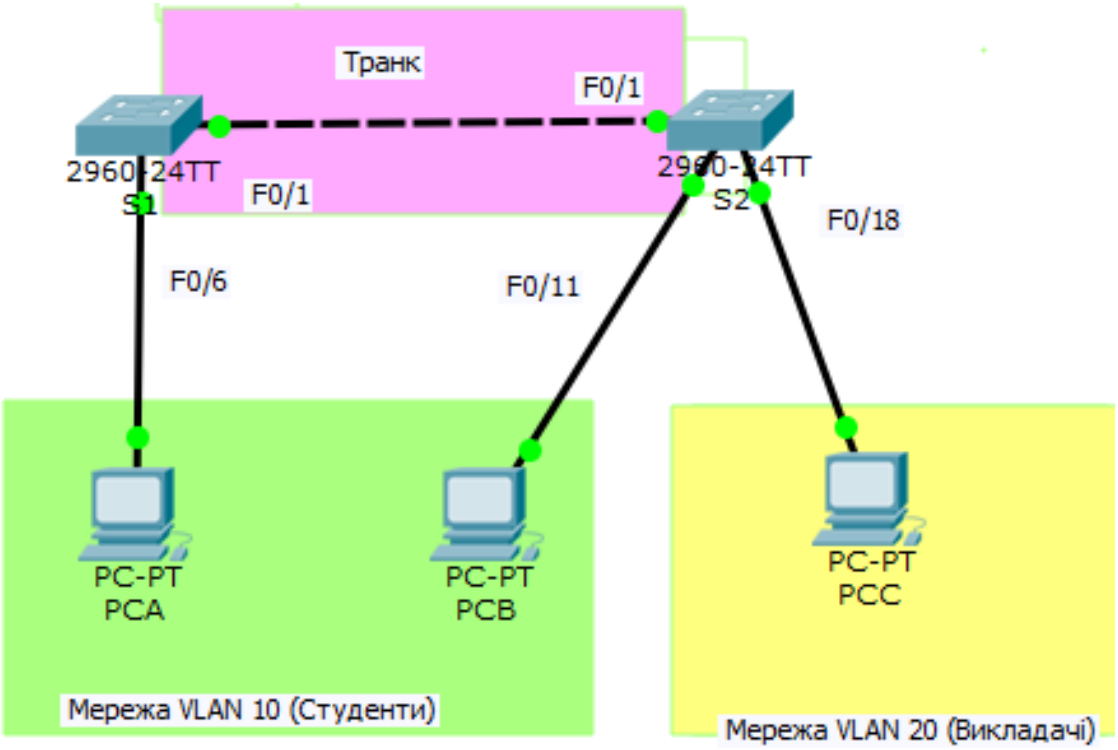


Рис. 6.1. Мережа з VLAN 10 для студентів та VLAN 20 для викладачів

Таблиця адресації

Пристрій	Інтерфейс	IP -адреса	Маска підмережі	Шлюз за замовчуванням
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC - A	Мережевий адаптер	192.168.10.3	255.255.255.0	192.168.10.1
PC - B	Мережевий адаптер	192.168.10.4	255.255.255.0	192.168.10.1
PC - C	Мережевий адаптер	192.168.20.3	255.255.255.0	192.168.20.1

Створення мереж VLAN і призначення портів комутатора

Створимо мережі VLAN для студентів та викладачів на двох комутаторах у локальній мережі. Потім призначимо мережі VLAN відповідному інтерфейсу. Для перевірки параметрів конфігурації використовується команда **show vlan.**

Створення мережі VLAN на комутаторах

Створимо мережі VLAN на комутаторі S1.

```
S1(config)# vlan 10
S1(config - vlan)# name Student
S1(config - vlan)# vlan 20
S1(config - vlan)# name Faculty
S1(config - vlan)# vlan 99
S1(config - vlan)# name Management
S1(config - vlan)# end
```

Створимо таку ж мережу VLAN на комутаторі S2.

Виконаємо команду **show vlan**, щоб проглянути список мереж VLAN на комутаторі S1.

```
S1# show vlan
VLAN Name                       Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                    active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                          Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                          Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                          Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                          Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                          Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                          Gi0/1, Gi0/2
10   Student                    active
20   Faculty                    active
99   Management                 active
1002 fddi - default             act/unsup
1003 token - ring - default     act/unsup
1004 fddinet - default          act/unsup
1005 trnet - default            act/unsup
```

```
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

Призначення мережі VLAN відповідним інтерфейсам комутатора

Призначимо мережі VLAN інтерфейсам на комутаторі S1.
Призначимо вузол PC - A мережі VLAN для студентів.

```
S1(config)# interface f0/6
S1(config - if)# switchport mode access
S1(config - if)# switchport access vlan 10
```

Перемістимо IP -адресу комутатора мережі VLAN 99.

```
S1(config)# interface vlan 1
S1(config - if)# no ip address
S1(config - if)# interface vlan 99
S1(config - if)# ip address 192.168.1.11 255.255.255.0
S1(config - if)# end
```

Виконаємо команду **show vlan brief** і переконаємося, що мережі VLAN призначені правильним інтерфейсам.

```
S1# show vlan brief
VLAN Name                         Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                            Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                            Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                            Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                            Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                            Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                            Gi0/2
10   Student                      active    Fa0/6
20   Faculty                      active
99   Management                   active
1002 fddi - default               act/unsup
1003 token - ring - default       act/unsup
1004 fddinet - default            act/unsup
1005 trnet - default              act/unsup
```

Виконаємо команду **show ip interfaces brief.**

```
S1# show ip interface brief
Interface          IP - Address     OK? Method Status                Protocol
Vlan1              unassigned       YES unset  up                    up
Vlan99             192.168.1.11     YES manual up                    down
FastEthernet0/1    unassigned       YES unset  up                    up
FastEthernet0/2    unassigned       YES unset  administratively down down
FastEthernet0/3    unassigned       YES unset  administratively down down
FastEthernet0/4    unassigned       YES unset  administratively down down
FastEthernet0/5    unassigned       YES unset  administratively down down
FastEthernet0/6    unassigned       YES unset  up                    up
FastEthernet0/7    unassigned       YES unset  administratively down down
```

Мережа VLAN 99 знаходиться в стані up/down (вкл/викл), оскільки вона ще не була призначена активному порту.

Використовуємо топологію, щоб призначити мережі VLAN відповідним портам комутатора S2.

Видаляємо IP -адресу для мережі VLAN 1 на комутаторі S2.

Настроюємо IP -адресу для мережі VLAN 99 на комутаторі S2 відповідно до таблиці адресації.

Виконуємо команду **show vlan brief,** щоб переконатися, що мережі VLAN призначені правильним інтерфейсам.

```
S2# show vlan brief
VLAN Name                        Status    Ports
---- ------------------------------- --------- -------------------------------
1    default                     active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   Student                     active    Fa0/11
20   Faculty                     active    Fa0/18
99   Management                  active
1002 fddi - default              act/unsup
1003 token - ring - default      act/unsup
1004 fddinet - default           act/unsup
1005 trnet - default             act/unsup
```

Ехо-запит від вузла PC-A на вузол PC-B не успішний, оскільки інтерфейс F0/1 не призначений мережі VLAN 10, тому трафік мережі VLAN 10 не вирушатиме через цей інтерфейс.

Призначення мережі VLAN декільком інтерфейсам

На комутаторі S1 призначимо інтерфейси F0/11 - 24 мережі VLAN 10.

```
S1(config)# interface range f0/11-24
S1(config - if - range)# switchport mode access
S1(config - if - range)# switchport access vlan 10
```

S1(config - if - range)# end

Виконаємо команду **show vlan brief**, щоб перевірити призначення VLAN.

S1# show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Gi0/1, Gi0/2
10	**Student**	**active**	**Fa0/6, Fa0/11, Fa0/12, Fa0/13** **Fa0/14, Fa0/15, Fa0/16, Fa0/17** **Fa0/18, Fa0/19, Fa0/20, Fa0/21** **Fa0/22, Fa0/23, Fa0/24**
20	Faculty	active	
99	Management	active	
1002	fddi - default	act/unsup	
1003	token - ring - default	act/unsup	
1004	fddinet - default	act/unsup	
1005	trnet - default	act/unsup	

Заново призначимо порти F0/11 і F0/21 мережі VLAN 20.

S1(config)# interface range f0/11, f0/21
S1(config - if - range)# switchport access vlan 20
S1(config - if - range)# end

Переконаємося, що призначення мережі VLAN налагоджені вірно.

S1# show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Gi0/1, Gi0/2
10	Student	active	Fa0/6, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/22, Fa0/23 Fa0/24
20	Faculty	active	Fa0/11, Fa0/21
99	Management	active	
1002	fddi - default	act/unsup	
1003	token - ring - default	act/unsup	
1004	fddinet - default	act/unsup	
1005	trnet - default	act/unsup	

Видалення призначення VLAN з інтерфейсу

Використаємо команду **no switchport access vlan**, щоб видалити призначення мережі VLAN 10 для F0/24.

S1(config)# interface f0/24
S1(config - if)# no switchport access vlan

S1(config - if)# end

Переконаємося, що це зміна мережі VLAN набула чинності.

S1# show vlan brief

```
VLAN Name                       Status    Ports
      -------------------------------- --------- -------------------------------
1    default                    active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                  Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                  Fa0/10, Fa0/24, Gi0/1, Gi0/2
10   Student                    active    Fa0/6, Fa0/12, Fa0/13, Fa0/14
                                                  Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                  Fa0/19, Fa0/20, Fa0/22, Fa0/23
20   Faculty                    active    Fa0/11, Fa0/21
99   Management                 active
1002 fddi - default             act/unsup
1003 token - ring - default          act/unsup
1004 fddinet - default           act/unsup
1005 trnet - default            act/unsup
```

Видалення ідентифікатора VLAN з бази даних VLAN

Додамо мережу VLAN 30 в інтерфейс F0/24, не вводячи команду мережі VLAN.

S1(config)# interface f0/24

S1(config - if)# switchport access vlan 30

% % Access VLAN does not exist. Creating vlan 30

Переконаємося, що нова мережа VLAN відображується в таблиці VLAN.

S1# show vlan brief

```
VLAN Name                       Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                    active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                  Fa0/9, Fa0/10, Gi0/1, Gi0/2
10   Student                    active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                  Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                  Fa0/20, Fa0/22, Fa0/23
20   Faculty                    active    Fa0/11, Fa0/21
30   VLAN0030                   active    Fa0/24
99   Management                 active
1002 fddi - default             act/unsup
1003 token - ring - default          act/unsup
1004 fddinet - default           act/unsup
1005 trnet - default            act/unsup
```

Видалимо мережу VLAN 30 з бази даних VLAN.

S1(config)# no vlan 30

S1(config)# end

Виконаємо команду **show vlan brief**. Порт F0/24 було призначений мережі VLAN 30.

```
S1# show vlan brief
VLAN Name                    Status    Ports
---- ------------------------------- --------- -------------------------------
1    default                 active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                       Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                       Fa0/9, Fa0/10, Gi0/1, Gi0/2
10   Student                 active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                       Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                       Fa0/20, Fa0/22, Fa0/23
20   Faculty                 active    Fa0/11, Fa0/21
99   Management              active
1002 fddi - default          act/unsup
1003 token - ring - default      act/unsup
1004 fddinet - default        act/unsup
1005 trnet - default         act/unsup
```

Виконаємо команду **no switchport access vlan** на інтерфейсі F0/24.

```
S1(config)# interface f0/24
S1(config - if)# no switchport access vlan
S1(config - if)# end
```

Виконаємо команду **show vlan brief**, щоб визначити призначення мережі VLAN для F0/24. Якій мережі VLAN призначений порт F0/24?

```
S1# show vlan brief
VLAN Name                    Status    Ports
---- ------------------------------- --------- -------------------------------
1    default                 active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                       Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                       Fa0/10, Fa0/24, Gi0/1, Gi0/2
10   Student                 active    Fa0/6, Fa0/12, Fa0/13, Fa0/14
                                       Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                       Fa0/19, Fa0/20, Fa0/22, Fa0/23
20   Faculty                 active    Fa0/11, Fa0/21
99   Management              active
1002 fddi - default          act/unsup
1003 token - ring - default      act/unsup
1004 fddinet - default        act/unsup
1005 trnet - default         act/unsup
```

Примітка. Перш ніж видаляти мережу VLAN з бази даних, рекомендується перепризначувати усі порти, призначені для цієї мережі VLAN.

Чому перед видаленням мережі VLAN з бази даних рекомендується призначити порт іншої мережі VLAN?

Конфігурація транкового каналу стандарту 802.1Q між комутаторами

Налаштуємо інтерфейс F0/1 для використання **протоколу динамічного створення транкового каналу (DTP)**, щоб він міг узгоджуватися з транковим режимом. Після виконання і перевірки налаштування треба буде відключити DTP на інтерфейсі F0/1 і вручну настроїти його в якості транкового каналу.

За замовчуванням протокол DTP на порту комутатора налаштований на динамічний автоматичний режим. Завдяки цьому інтерфейс може перетворити канал в транковий канал, якщо сусідній інтерфейс налагоджений на транковий або динамічний рекомендований режим.

Налаштуємо порт F0/1 на комутаторі S1 для узгодження транкового режиму.

```
S1(config)# interface f0/1
S1(config - if)# switchport mode dynamic desirable
```

На комутаторах S1 і S2 виконаємо команду **show vlan brief**. Інтерфейс F0/1 більше не призначений мережі VLAN 1. Транкові інтерфейси не вказані в таблиці VLAN.

```
S1# show vlan brief
VLAN Name                       Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/24, Gi0/1, Gi0/2
10   Student                        active    Fa0/6, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/22, Fa0/23
20   Faculty                        active    Fa0/11, Fa0/21
99   Management                     active
1002 fddi - default                 act/unsup
1003 token - ring - default         act/unsup
1004 fddinet - default              act/unsup
1005 trnet - default                act/unsup
```

Для перегляду транкових інтерфейсів виконаємо команду **show interfaces trunk**.

```
S1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/1       1-4094
Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
S2# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/1       1-4094
Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

Налаштування транкового інтерфейсу F0/1

Команда **switchport mode trunk** дозволяє вручну настроїти порт в якості транкового каналу. Цю команду слід виконувати на обох кінцях каналу.

Змінимо режим порту комутатора на інтерфейсі F0/1, щоб примусово створити транковий зв'язок на обох комутаторах.

```
S1(config)# interface f0/1
S1(config - if)# switchport mode trunk
S2(config)# interface f0/1
S2(config - if)# switchport mode trunk
```

Для перегляду транкового режиму виконаємо команду **show interfaces trunk**. Зверніть увагу, що режим змінений з рекомендованого (**desirable**) на вкл (**on**).

```
S2# show interfaces trunk
Port      Mode         Encapsulation  Status        Native vlan
Fa0/1     on           802.1q         trunking      99
Port      Vlans allowed on trunk
Fa0/1     1-4094
Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,99
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,99
```

Чому замість використання протоколу DTP рекомендується вручну налаштовувати інтерфейс на транковий режим?

Виконаємо команду **show flash**, щоб перевірити, чи міститься файл **vlan.dat** у флеш-пам’яті.

```
S1# show flash
```

Видалення бази даних VLAN

Виконаємо команду **delete vlan.dat**, щоб видалити файл **vlan.dat** з флеш-пам’яті і повернути налаштування бази даних VLAN до параметрів за замовчуванням.

```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
S1#
```

Виконаємо команду **show flash**, щоб переконатися, що файл **vlan.dat** був видалений.

Завдання до лабораторної роботи

1. Згідно варіанту для всіх комутаторів задати ім’я (S1, S2, S3 тощо), а також аутентифікацію на вхід в консоль та привілейований режим (при перегляді конфігурації пристрою мають бути зашифровані паролі). Для спроб несанкціонованого доступу на комутаторі налаштувати банерне повідомлення.

2. Згідно варіанту, засобами середовища моделювання **Cisco Packet Tracer** змоделювати локальну мережу з заданою кількістю комутаторів та відповідним їм вузлами. Налаштувати IP-адресацію з указаного діапазону адрес для кожного із заданої кількості вузлів, віртуальні локальні мережі для вузлів згідно варіанту, виділити їх

різними кольорами, додати надписи VLAN, як показано на рис.6.2. Вручну встановити транкові з'єднання між комутаторами. Перевірити створені VLAN, використовуючи відповідні команди, перевірити з'єднання між вузлами за допомогою команди **ping**.

Вузол	IP-адреса	Вузол	IP-адреса
		PC 8	192.168.3.4
PC 0	192.168.2.1	PC 9	192.168.4.3
PC 1	192.168.4.1	PC 10	192.168.2.4
PC 2	192.168.4.2	PC 11	192.168.2.5
PC 3	192.168.2.2	PC 12	192.168.4.4
PC 4	192.168.2.3	PC 13	192.168.4.5
PC 5	192.168.3.1	PC 14	192.168.3.5
PC 6	192.168.3.2	PC 15	192.168.3.6
PC 7	192.168.3.3	PC 16	192.168.3.7

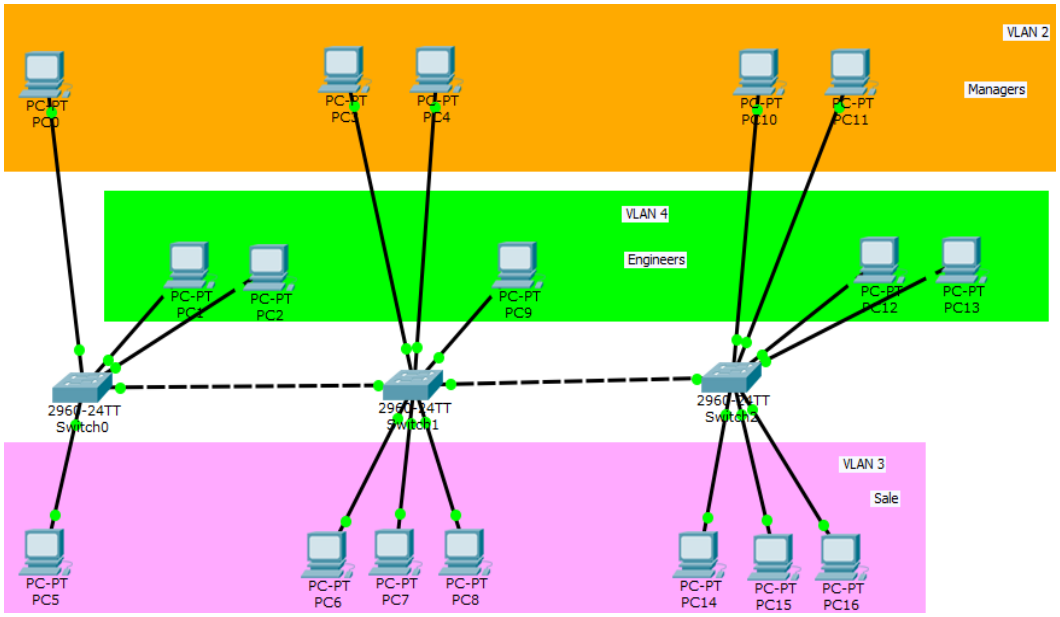


Рис.6.2. Мережа з трьома VLAN (2,3,4) для відділів менеджерів, продаж та інженерів

Варіант	Комутатори	Вузол, VLAN №	№ VLAN - Name	Мережа
1	S1 (3 вузли) S2 (4 вузли) S3 (4 вузли)	1- VLAN 2, 2,3 - VLAN 3 1-3- VLAN 2, 4- VLAN 4 1- VLAN 3, 2-4- VLAN 4	2- Accounting 3- Sale 4- Advertising	172.16.0.0/12
2	S1 (6 вузлів) S2 (5 вузлів)	1-VLAN 20, 2,3- VLAN 30, 4-6- VLAN 40 1- VLAN 20, 2,3- VLAN 30, 4,5- VLAN 40	20- Managers 30- Projects 40- Engineers	192.168.0.0/16
3	S1 (4 вузли) S2 (3 вузли) S3 (4 вузли)	1- VLAN 10, 2-4 - VLAN 20 1- VLAN 10, 2,3- VLAN 30 1- VLAN 10, 2- VLAN 20, 3,4- VLAN 30	10-Directors 20-Financiers 30- Programmers	172.16.0.0/12
4	S1 (5 вузлів) S2 (5 вузлів) S3 (6 вузлів)	1- VLAN 4, 2-5 - VLAN 5 1- VLAN 4, 2-5- VLAN 5 1- VLAN 4, 2-6- VLAN 5	4- Teachers 5- Students	192.168.0.0/16
5	S1 (6 вузлів) S2 (5 вузлів)	1,2- VLAN 10, 3,4- VLAN 30, 5,6-VLAN 40 1-4- VLAN 10, 5- VLAN 30, 6- VLAN 40	10- Managers 30- Programmers 40- Financiers	172.16.0.0/12
6	S1 (5 вузлів) S2 (7 вузлів)	1- VLAN 4, 2-4 - VLAN 5, 5- VLAN 6 1-3- VLAN 4, 4- VLAN 5, 5-7- VLAN 6	4- Surgeons 5- Therapists 6- Neurosurgery	192.168.0.0/16
7	S1 (5 вузлів)	1- VLAN 10, 2-4 - VLAN 20, 5- VLAN 30	10-Deaneries	172.16.0.0/12

	S2 (4 вузли) S3 (4 вузли)	1,2- VLAN 10, 3,4- VLAN 30 1- VLAN 10, 2- VLAN 20, 3,4- VLAN 30	20-Departments 30-Teachers	
8	S1 (4 вузли) S2 (3 вузли) S3 (2 вузли)	1- VLAN 10, 2,3 - VLAN 20, 4 - VLAN 30 1- VLAN 10, 2,3- VLAN 30 1- VLAN 10, 2- VLAN 20	10-Marketers 20-Analysts 30- Sale	192.168.0.0/16
9	S1 (8 вузлів) S2 (4 вузли)	1-VLAN 20, 2,3- VLAN 30, 4-8- VLAN 40 1- VLAN 20, 2,3- VLAN 30, 4- VLAN 40	20-Promotion 30-Marketing 40-Commerce	172.16.0.0/12
10	S1 (4 вузли) S2 (3 вузли) S3 (5 вузлів)	1- VLAN 2, 2,3 - VLAN 3, 4- VLAN 4 1- VLAN 2, 2- VLAN 3 , 3- VLAN 4 1- VLAN 2 , 2-5- VLAN 4	2- Stock 3- Sale 4- Accounting	192.168.0.0/16
11	S1 (6 вузлів) S2 (4 вузли) S3 (5 вузлів)	1,2- VLAN 4, 3-6 - VLAN 5 1,2- VLAN 4, 3,4- VLAN 5 1- VLAN 4, 2-5- VLAN 5	4- Managers 5- Programmers	172.16.0.0/12
12	S1 (4 вузли) S2 (5 вузлів)	1-VLAN 40, 2,3- VLAN 50, 4- VLAN 60 1- VLAN 40, 2,3- VLAN 50, 4,5- VLAN 60	40-Promotion 50- Analysts 60- Financiers	192.168.0.0/16
13	S1 (4 вузли) S2 (8 вузлів) S3 (3 вузли)	1- VLAN 2, 2,3 - VLAN 3, 4- VLAN 5 1,2- VLAN 2, 3- VLAN 4, 4-8- VLAN 5 1- VLAN 3, 2- VLAN 4, 3- VLAN 5	2- Managers 3- Advertising 4- Promotion 5- Projects	172.16.0.0/12
14	S1 (6 вузлів) S2 (4 вузли) S3 (6 вузлів)	1,2- VLAN 3, 3-6 - VLAN 4 1,2- VLAN 3, 3,4- VLAN 4 1- VLAN 3, 2-6- VLAN 4	3- Managers 4- Workers	192.168.0.0/16
15	S1 (5 вузлів) S2 (4 вузли) S3 (2 вузли)	1- VLAN 10, 2-4 - VLAN 20, 5- VLAN 30 1,2- VLAN 10, 3,4- VLAN 30 1- VLAN 10, 2- VLAN 20	10-Webmasters 20-Library 30- Workers	172.16.0.0/12
16	S1 (7 вузлів) S2 (7 вузлів)	1,2-VLAN 40, 3- VLAN 50, 4-7- VLAN 60 1- VLAN 40, 2,3- VLAN 50, 4-7- VLAN 60	40-Lawyers 50-Branches 60-Judges	192.168.0.0/16
17	S1 (8 вузлів) S2 (3 вузли) S3 (5 вузлів)	1- VLAN 2, 2,3 - VLAN 3, 4- VLAN 4, 5-8- VLAN 5 1- VLAN 2, 2- VLAN 3 , 3- VLAN 4 1- VLAN 2 , 2,3- VLAN 3, 4- VLAN 4, 5- VLAN 5	2- Personnel 3- Tax 4- Insurance 5- Consulting	172.16.0.0/12
18	S1 (4 вузли) S2 (7 вузлів) S3 (4 вузли)	1- VLAN 10, 2,3 - VLAN 20, 4 - VLAN 30 1- VLAN 10, 2,3- VLAN 20, 4-7- VLAN 30 1- VLAN 10, 2-4- VLAN 20	10- Managers 20- Marketing 30- Promotion	192.168.0.0/16
19	S1 (9 вузлів) S2 (6 вузлів)	1,2-VLAN 12, 3- VLAN 13, 4-7- VLAN 14, 8,9- VLAN 15 1,2- VLAN 12, 3- VLAN 13, 4- VLAN 14, 5,6- VLAN 15	12-Webmasters 13-Programmers 14- Workers 15- Analysts	172.16.0.0/12
20	S1 (5 вузлів) S2 (9 вузлів) S3 (4 вузли)	1- VLAN 10, 2-4 - VLAN 20, 5- VLAN 30 1,2- VLAN 10, 3- VLAN 20, 4-9- VLAN 30 1- VLAN 10, 2- VLAN 20, 3,4- VLAN 30	10- Managers 20- Branches 30- Office	192.168.0.0/16
21	S1 (8 вузлів) S2 (3 вузли) S3 (5 вузлів)	1- VLAN 2, 2,3 - VLAN 3, 4- VLAN 4, 5-8- VLAN 5 1- VLAN 2, 2- VLAN 3 , 3- VLAN 4 1- VLAN 2 , 2,3- VLAN 3, 4- VLAN 4, 5- VLAN 5	2-Deaneries 3-Departments 4-Teachers 5-Students	172.16.0.0/12
22	S1 (4 вузли) S2 (3 вузли) S3 (5 вузлів)	1- VLAN 2, 2,3 - VLAN 3, 4- VLAN 4 1- VLAN 2, 2- VLAN 3 , 3- VLAN 4 1- VLAN 2 , 2-5- VLAN 4	2- Managers 3- Programmers 4- Financiers	192.168.0.0/16
23	S1 (6 вузлів) S2 (4 вузли) S3 (5 вузлів)	1,2- VLAN 4, 3-6 - VLAN 5 1,2- VLAN 4, 3,4- VLAN 5 1- VLAN 4, 2-5- VLAN 5	4- Accounting 5- Sale	172.16.0.0/12

24	S1 (6 вузлів) S2 (5 вузлів)	1,2- VLAN 10, 3,4- VLAN 30, 5,6-VLAN 40 1-4- VLAN 10, 5- VLAN 30, 6- VLAN 40	10-Marketers 30-Analysts 40- Sale	192.168.0.0/16
25	S1 (3 вузли) S2 (4 вузли) S3 (4 вузли)	1- VLAN 2, 2,3 - VLAN 3 1-3- VLAN 2, 4- VLAN 4 1- VLAN 3, 2-4- VLAN 4	2- Managers 3- Marketing 4- Promotion	172.16.0.0/12

Вимоги до оформлення звіту

Звіт має включати: титульний аркуш, індивідуальне завдання на лабораторну роботу, хід роботи та висновки. Необхідно зробити скріншот створеної топології мережі, навести опис всіх введених команд для налаштування конфігурації комутаторів і VLAN. Створити таблицю адресації для вузлів, як наведено у прикладі, або зробити надписи IP-адрес у логічній топології мережі.

Питання до лабораторної роботи

1. Яке призначення VLAN?
2. Які вимоги до створення VLAN?
3. Яка команда використовується для перевірки стану підключених інтерфейсів комутатора?
4. Як перевірити чи були створені віртуальні локальні мережі на комутаторі?
5. Яким чином можна видалити VLAN?
6. Які переваги віртуальних локальних мереж?
7. Які є типи віртуальних локальних мереж?
8. Що таке транк? Для чого використовуються транкові канали?
9. Яка максимальна кількість та які діапазони VLAN на сучасних комутаторах?
10. Які команди використовуються для створення віртуальної локальної мережі?
11. Які команди використовуються для призначення порту та одночасно декільком портам мережі VLAN?
12. Як змінити приналежність портів віртуальної локальної мережі?
13. Як перевірити інформацію про мережу VLAN?
14. Опишіть загальні рекомендації по проектуванню віртуальної локальної мережі.

Рекомендована література

1.CNA R&S // Електронний ресурс. режим доступу: http://static-course-assets.s3.amazonaws.com

2. VLAN // Електронний ресурс. Режим доступу: http://linkmeup.ru/blog/13.html

3.Налаштування VLAN // Електронний ресурс. Режим доступу: https://it.oneweb.pro

4. Налаштування VLAN на Mikrotik // Електронний ресурс. Режим доступу: http://www.technotrade.com.ua/Articles/mikrotik_vlan.php

5. Налаштування VLAN на комутаторах Cisco Catalyst // Електронний ресурс. Режим доступу: https://supportforums.cisco.com/ru/document/124406

6. Команди VLAN на основі портів і стандарту IEEE 802.1Q // Електронний ресурс. Режим доступу: http://www.intuit.ru/studies/courses/3591/833/lecture/14260

Лабораторна робота №7. Статична та динамічна маршрутизація

Мета: ознайомитися з будовою та операційною системою маршрутизатора. Розглянути типи та протоколи маршрутизації. Навчитися налаштовувати динамічну маршрутизацію в мережі за допомогою протоколу OSPF.

Теоретичні відомості

Маршрутизатор – спеціальний тип комп'ютера, він має всі ті ж основні компоненти, що і звичайний комп'ютер: процесор, пам'ять, системну шину та різні пристрої введення/виведення.

Маршрутизатор дозволяє взаємодіяти різним пристроям та визначає найоптимальніший маршрут для передачі даних у мережі.

Як і звичайний комп'ютер, маршрутизатор має операційну систему. У даній лабораторній роботі розглядається операціна система Cisco IOS (Internetwork Operating System).

Основними компонентами маршрутизатора є оперативна пам'ять (RAM), незмінна оперативна пам’ять (NVRAM), флеш-пам'ять (Flash), ROM та інтерфейси.

Функції оперативної пам'яті маршрутизатора:

- збереження таблиць маршрутизації;
- збереження ARP-кеша;
- збереження кеша швидкого перемикання;
- збереження робочої конфігурації маршрутизатора.

Функції NVRAM:

- збереження конфігурації маршрутизатора.

Функції флеш-пам'яті:

- збереження образів операційної системи;
- дозволяє оновлювати забезпечення системи без купівлі нових мікросхем.

Функції ROM:

- підтримує інструкції по POST;
- зберігає BIOS.

Функції інтерфейсів:

- приєднання маршрутизатора до мережі.
- виконані у вигляді плати до материнської плати, або вбудовані в материнську плату.

Режими доступу до маршрутизатора. Команда show

Існує кілька основних режимів доступу до маршрутизатора.

Користувацький режим. У цьому режимі доступний лише обмежений набір команд, який дозволяє лише переглянути деякі параметри маршрутизатора. Запит у командному рядку даного режиму виглядає в такий спосіб: **router>**. Значок „>” саме й показує, що режим користувацький.

Привілейований режим. У даному режимі доступні команди для перегляду всіх параметрів маршрутизатора (перегляд конфігурацій, інтерфейсів тощо). Перехід у цей режим здійснюється командою **enable**. Запит у командному рядку даного режиму виглядає так: **router#**. Значок „#” вказує на те, що маршрутизатор перебуває у привілейованому режимі.

Режим глобальної конфігурації. У даному режимі здійснюється налаштування основних параметрів і ресурсів маршрутизатора. Перехід у даний режим здійснюється за допомогою команди **configure terminal.**

Розглянемо основні команди для перегляду інформації про маршрутизатор (табл.7.1)

Табл.7.1. Команди для перегляду інформації про маршрутизатор

Команда	Опис команди
Router> ?	Переглянути список доступних команд у користувацькому режимі
Router> enable	Перейти в привілейований режим
Router#?	Переглянути список доступних команд у привілейованому режимі
Router# show ?	Переглянути список доступних команд для команди show
Router# show running-config	Переглянути поточну конфігурацію маршрутизатора
Router# disable	Перехід з привілейованого режиму в користувацький
Router# show flash	Переглянути вміст флеш-пам’яті
Router# show history	Переглянути список раніше введених 10 команд
Router# show protocols	Переглянути список протоколів, які використовуються на маршрутизаторі
Router# show version	Переглянути тип платформи, версію операційної системи, кількість інтерфейсів та пам'ять
Router# show clock	Переглянути встановлений час на маршрутизаторі
Router# show hosts	Переглянути локальний список DNS-імен
Router# show interfaces	Переглянути інформацію про кожен інтерфейс маршрутизатора

Базове налаштування маршрутизатора

Базове налаштування маршутизатора містить:
- налаштування імені маршутизатора;
- налаштування пароля на доступ у привілейований режим;
- налаштування паролів на віддалений доступ та доступ по консолі;
- налаштування параметрів інтерфейсів.

Табл.7.2. Команди для налаштування маршрутизатора

Команда	Опис команди
Router> enable	Перейти в привілейований режим
Router#configure terminal	Перейти в режим глобальної конфігурації
Router(config)#hostname R1	Задати ім’я маршрутизатора R1
Router (config)#enable secret cisco	Встановити пароль cisco на доступ у привілейований режим
Router(config)#banner motd !Message!	Встановити банерне повідомлення
Router#copy running-config startup-config	Зберегти поточну конфігурацію в NVRAM
Router#erase startup-config	Видалити конфігураційний файл з NVRAM
Router#reload	Перезавантажити маршрутизатор
Router(config)#interface fa0/1	Перехід в режим конфігурування інтерфейсу fa0/1
Router(config-if)#ip address 192.168.10.100 255.255.0.0	Встановлення IP-адреси на інтерфейсі
Router(config-if)#no shutdown	Активізувати інтерфес (за замовчуванням усі інтерфейси не активні)
Router#show ip int brief	Переглянути коротку інформацію про стан інтерфейсів

Протокол CDP

Даний протокол дозволяє маршрутизаторам обмінюватися деякою інформацією без попереднього налаштування. Даний протокол дозволяє визначити сусідів по мережі (тип платформи, операційну систему, інтерфейси тощо).

Табл.7.3. Команди для перевірки роботи протоколу CDP

Команда	Опис команди
Router> enable	Перейти в привілейований режим
Router#show cdp neighbors	Переглянути інформацію про своїх сусідів
Router# show cdp	Переглянути загальну інформацію про протокол
Router (config)#cdp run	Ввімкнути протокол cdp
Router(config-if)#cdp enable	Ввімкнути протокол cdp на конкретному інтерфейсі

Статична маршрутизація

Мережа Internet (WAN – Wide Area Network) є сегментованою. Сегментом є прозора ділянка широкомовної (Ethernet) мережі. IP-адреса привласнюється не комп'ютеру, а інтерфейсу (мережевому виходу або послідовному порту). Декільком інтерфейсам можна задати одну адресу. Можна також привласнити кілька адрес одному інтерфейсу. У сегменті мережі всі вузли мають IP-адреси з однаковим номером мережі та однаковою маскою. В одній локальній мережі можна сполучити дві та більше різних IP-мереж, але це все-таки будуть дві різні мережі. Прийнято наступний розподіл залежно від значення старшого байта IP-адреси:

- 0..127 – мережі класу A по 224 адрес із маскою 0xFF000000;
- 128..191 – мережі класу B по 216 адрес із маскою 0xFFFF0000;
- 192..223 – мережі класу C по 28 адрес із маскою 0xfFFFFF00;
- 224..239 – мережі класу D для multicast (групової) розсилки;
- інші.

Багато програм за адресою автоматично визначають клас мережі. Можна розбити мережу на дві або більше підмереж із будь-якими масками, але організаціям як правило виділяють адреси блоками, відповідними до класів A, B і C – це пов'язано із системою DNS, що дозволяє довідатися доменне ім'я вузла за його IP-адресою.

Мережа класу A з номером 127 – **loopback**, призначена для спілкування комп'ютера із собою. У будь-якій мережі номер (IP-номер *AND* маска) є номером усієї мережі й не може бути привласнений нікому конкретно. Номер (IP-номер *OR NOT* маска), що є останнім номером у мережі, призначений для **broadcasting** (широкомовних) повідомлень, які доставляються всім вузлам сегмента мережі. Відповідно, при виділенні групи адрес у мережу дві адреси стають недоступними.

Статична маршрутизація полягає у прописуванні маршрутів передачі даних по мережі, виконується адміністратором вручну за допомогою команди **ip route**.

Синтаксис команди: **ip route *ip_address netmask gateway,*** де

- IP_address – IP - адреса мережі, яку потрібно маршрутизувати;
- Netmask – мережева маска мережі;
- Gateway – шлюз мережі.

Приклад: Для маршрутизатора запишемо команду для доступу до мережі:

172.16.10.0 ip route 172.16.10.0 255.255.255.0 10.1.1.2 – маршрутизація через свій інтерфейс, або **ip route 172.16.10.0 255.255.255.0 10.1.1.1** – маршрутизація через інтерфейс сусіда. Для перегляду таблиці маршрутизації використовується команда **show ip route**.

Динамічні протоколи маршрутизації

Алгоритм маршрутизації повинен мати такі властивості як надійність, коректність, стабільність, простоту й оптимальність. Серед параметрів оптимізації можуть бути мінімальна затримка доставки, максимальна пропускна здатність, мінімальна ціна, максимальна надійність або мінімальна ймовірність помилки. Алгоритми маршрутизації є адаптивними та неадаптивними.

Неадаптивні алгоритми маршрутизації при виборі маршруту не беруть до уваги існуючу в цей момент топологію або завантаження каналів. Такі алгоритми називаються **статичними.**

Адаптивні алгоритми маршрутизації передбачають періодичний вимір характеристик каналів і постійне дослідження топології маршрутів. Вибір того або іншого маршруту тут проводиться на підставі цих вимірів. Практично всі методи маршрутизації базуються на наступному твердженні (*принцип оптимальності*): якщо маршрутизатор **M** перебуває на оптимальному шляху від маршрутизатора **I** до маршрутизатора **J**, тоді оптимальний шлях від **M** до **J** проходить цим шляхом. Наслідком принципу оптимальності є твердження, що оптимальні маршрути від усіх відправників до загального місця призначення утворюють дерево, позбавлене циклів. Таке дерево (*sink tree*) може бути не єдиним, можуть існувати інші дерева з тими ж довжинами шляху. А це, у свою чергу означає, що будь-який пакет буде доставлений за строго обмежений час, пройшовши однократно певне число маршрутизаторів.

Головним параметром при маршрутизації пакета в Інтернеті є IP-адреса його місця призначення. Повна таблиця маршрутів може містити 10^7! записів. Звичайний користувач не замислюється над проблемами маршрутизації. IP ділить усі пристрої на маршрутизатори та звичайні ЕОМ (host), останні, як правило, не розсилають свої маршрутні таблиці. Передбачається, що маршрутизатор володіє вичерпною інформацією про правильні маршрути. Звичайна ЕОМ має мінімальну маршрутну інформацію (наприклад, адреса маршрутизатора локальної мережі й сервера імен).

Автономна система (АС) може містити багато маршрутизаторів, але взаємодію з іншими АС вона здійснює лише через один, **прикордонний маршрутизатор** (**border gateway**, він дав назву протоколу **BGP**). Прикордонний маршрутизатор потрібний тоді, коли АС має більше одного зовнішнього каналу, а якщо ні, то його функції виконує порт зовнішнього підключення (**gateway**). Якщо адресат досяжний більш ніж одним шляхом, маршрутизатор повинен зробити вибір, цей вибір здійснюється на підставі оцінки маршрутів-кандидатів. Кожному сегменту, що входить до маршруту, привласнюється оцінка цього сегмента. Кожний протокол маршрутизації використовує свою систему оцінки маршрутів. Оцінка сегмента маршруту називається **метрикою.** При виборі маршруту всім сегментам шляху повинні бути дані порівнянні значення метрик. Не можна, щоб одні сегменти оцінювалися числом кроків, а інші – величиною затримки в мілісекундах. У межах автономної системи це звичайно не створює проблем, адже це зона відповідальності одного адміністратора. Але в регіональних мережах, де працює багато адміністраторів, проблема вибору метрики може стати реальною проблемою. Саме із цієї причини в таких мережах використовується **вектор відстані**, що виключає суб'єктивність оцінок метрики. Крім класичної схеми маршрутизації за адресою місця призначення, часто використовується варіант вибору маршруту відправником (даний варіант одержав подальший розвиток при введенні стандарту IPv6). У цьому випадку IP-пакет містить відповідний код опції й список проміжних адрес вузлів, які він повинен відвідати на шляху до місця призначення.

Алгоритм вибору маршруту універсальний і не залежить від протоколу маршрутизації, який використовується лише для формування маршрутної таблиці.

Алгоритму вибору маршруту:

1) витягти IP-адресу (ID) місця призначення з дейтаграми;

2) обчислити IP-адресу мережі призначення (IN) **if IN** відповідає якій-небудь адресі локальної мережі, відправити дейтаграму за цією адресою; **else if IN** є присутнім у маршрутній таблиці, то послати дейтаграму до сервера, зазначеного в таблиці; **else if** описаний маршрут за замовчуванням, то послати дейтаграму до цього сервера; **else** видати повідомлення про помилку маршрутизації.

Якщо мережа містить у собі підмережі, то для кожного запису в маршрутній таблиці проводиться побітова операція <I> для ID і маски підмережі. Якщо результат цієї операції співпаде із вмістом адресного поля мережі, дейтаграма посилається серверу підмережі. На практиці при наявності підмереж у маршрутну таблицю додаються відповідні записи з масками й адресами мереж. Одна з базових ідей маршрутизації полягає в тому, щоб сконцентрувати маршрутну інформацію в обмеженому числі вузлових маршрутизаторів. Оптимізувати розв'язок дозволяє **backbone** (опорна мережа), до якої підключаються вузлові маршрутизатори. Будь-яка АС підключається до backbone через вузловий маршрутизатор. "Прозорі" мости важко діагностувати, тому що вони не дотримуються протоколу ICMP (команда **ping** не працює, останнім часом такі об'єкти забезпечуються SNMP-підтримкою), зате вони дозволяють перерозподіляти навантаження через кілька маршрутизаторів, що неможливо для більшості протоколів. Маршрутизація через опорні мережі (backbone) вимагає індивідуального підходу для кожного вузла. Адміністратори опорних мереж повинні узгоджувати свої принципи маршрутизації. Ситуація, коли вузол не володіє вичерпною маршрутною інформацією, у комбінації з використанням маршрутів за замовчуванням може привести до зациклення пакетів. Протоколи маршрутизації відрізняються один від одного тим, де зберігається і як формується маршрутна інформація. Оптимальність маршруту досяжна лише при повній інформації про всі можливі маршрути, але такі дані потребують занадто великого обсягу пам'яті.

У маршрутизаторі з динамічним протоколом резидентно завантажена програма-драйвер змінює таблиці маршрутизації на основі інформації, отриманої від сусідніх маршрутизаторів. В ЕОМ, що працює під UNIX і виконує функції маршрутизатора, це завдання часто вирішує резидентна програма **gated** або **routed**. Остання підтримує тільки внутрішні протоколи маршрутизації. Застосування динамічної маршрутизації не змінює алгоритм маршрутизації, здійснюваної на IP-рівні. Програма-драйвер при пошуку маршрутизатора-адресата як і раніше переглядає таблиці. Будь-який маршрутизатор може використовувати два протоколи маршрутизації одночасно, один для зовнішніх зв'язків, інший – для внутрішніх.

При передачі мультимедіа інформації використовуються принципово інші протоколи маршрутизації. Тут шлях прокладається від одержувача до відправника, а не навпаки. Це пов'язане з тим, що там при доставці застосовується мультикастинговий метод. Тут, як правило, один відправник посилає пакети багатьом користувачам. При цьому важливо, щоб розмноження пакета відбувалося якнайближче до кластера адресатів. Така стратегія інколи подовжує маршрут, але завжди знижує результуюче завантаження мережі. Останнім часом конфігурування мережевого устаткування (маршрутизаторів, DNS і поштових серверів) ускладнилося настільки, що це стало становити помітну частину витрат при формуванні комунікаційного вузла.

EIGRP (**Enhanced Interior Gateway Routing Protocol**) – дистанційно-векторний протокол маршрутизації, розроблений фірмою Cisco на основі протоколу IGRP. Протокол IGRP був створений як альтернатива протоколу RIP (до того, як був розроблений OSPF). Хоча протоколи стану зв'язків (OSPF) відпрацьовують зміни в топології мережі швидше, ніж EIGRP, OSPF має ряд додаткових можливостей, а EIGRP має свої переваги: він більш простий в реалізації і менш вимогливий до обчислювальних ресурсів маршрутизатора. EIGRP-маршрутизатор виявляє своїх сусідів шляхом періодичної розсилки повідомлень "Hello". Ці ж повідомлення використовуються для моніторингу стану зв'язку з сусідом (розсилаються кожні 5 секунд в мережах з великою пропускною здатністю – наприклад,

Ethernet кожні 60 секунд у "повільних" мережах). Такий моніторинг дозволяє розсилати в мережі вектори відстані не періодично, а тільки при зміні топології мережі. EIGRP використовує комплексне значення метрики, що обчислюється на підставі показників пропускної здатності та затримки при передачі даних в мережі. Також у розрахунок метрики можуть бути включені показники завантаження і надійності мережі.

При отриманні від сусідів векторів відстаней, маршрутизатор для кожної мережі призначення не тільки обирає сусіда, через якого лежить найкоротший шлях в цю мережу, але також запам'ятовує і ймовірних заступників (feasible successors). Ймовірним заступником стає маршрутизатор, який оголосив метрику маршруту від себе до даної мережі меншу, ніж повна метрика встановленого маршруту.

Розглянемо приклад EIGRP-системи на рис. 7.1 (для простоти метрики всіх зв'язків, крім (4) - (5), вважаємо рівними одиниці; метрика зв'язку (4) - (5) дорівнює 0,5).

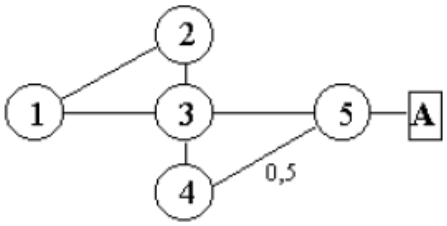


Рис. 7.1 Приклад EIGRP-системи
(колами позначені маршрутизатори, прямокутником – мережа призначення А)

Маршрутизатор (3) отримує від (5) елемент вектора відстаней (А=1), а від (4) – (А = 1,5). У таблиці маршрутизатора (3) вузол (5) стає наступним маршрутизатором на шляху в мережу А, а вузол (4) – вірогідним заступником, так як заявлена ним відстань до А (1,5) менше повної метрики встановленого маршруту (3) - (5) – А, яка дорівнює 2. Розглянемо маршрутизатори (1) і (2). Вони надсилають вузлу (3) елемент (А = 3) і, отже, не є ймовірними заступниками маршруту з (3) в А. Якщо зв'язок між вузлами (3) і (5) обривається, то (3) шукає у своїй EIGRP-таблиці ймовірного заступника (4) і негайно встановлює маршрут в мережу А через нього. Таким чином час, протягом якого маршрут в мережу А був відсутній, істотно скорочується порівняно з протоколом RIP, де потрібно чекати, коли сусіди надішлють чергові вектори відстаней.

Якщо жодного ймовірного заступника не знайдено (припустимо, зв'язок (3) - (4) теж обривається), то маршрутизатор переходить в активний стан і починає опитування всіх своїх сусідів на предмет наявності маршруту в мережу А, повідомляючи при цьому, що його власна відстань до А дорівнює нескінченності. EIGRP використовує **алгоритм DUAL (Diffusing Update Algorithm):** сусід відповідає на запит тільки тоді, коли у нього є або готовий маршрут в А, або ймовірний заступник – у будь-якому з цих випадків сусід надсилає у вузол (3) свою відстань до А. Інакше сусід сам переходить в активний стан і процес повторюється (з тією різницею, що до маршрутизатора (3) запит не надсилається; крім того, маршрутизатор, що знаходиться у активному стані, сам може відповідати на запити, посилаючи у відповідь своє поточне значення відстані до А). Таким чином, область "активізованих" маршрутизаторів розширюється до тих пір, поки не буде виявлено маршрут в мережу А або доведено його відсутність, після чого хвиля сходиться в зворотному напрямку до вузла, який ініціював процес, при цьому всі маршрутизатори вносять у свої таблиці належні зміни.

У нашому прикладі, після того як (3) переходить в активний стан, вузли (1) і (2) отримують від нього запит про маршрут в мережу А з позначкою, що відстань від (3) до А тепер дорівнює нескінченності. Кожен з них, оскільки раніше він добирався в А через (3), позначає цей маршрут як недосяжний, і, не знайшовши ймовірного заступника, активізується і опитує свого сусіда. Отримавши ці запити, (1) і (2) відповідають один одному, що мережа А недосяжна, переходять у пасивний стан і повертають вузлу (3) інформацію про недосяжність мережі А. Подібна процедура (пошук ймовірного

заступника, а за відсутності такого – запуск алгоритму DUAL) відбувається не тільки при обриві зв'язку, а також і в загальному випадку: якщо наступний маршрутизатор на шляху в А прислав вектор, в якому відстань до мережі А збільшилося в порівнянні з попереднім повідомленням від того ж маршрутизатора.

EIGRP-маршрутизатор не просто приймає від сусідів вектори відстаней, а будує на їх основі деяке уявлення про топологію мережі ("ймовірні заступники"), контролює стан зв'язку з сусідами і використовує алгоритм DUAL.

Табл.7.4. Конфігурування EIGRP на маршрутизаторі

Команда	Опис команди
Router> enable	Перейти в привілейований режим
Router#configure terminal	Перейти в режим глобальної конфігурації
Router(config)#router eigrp 100	Перейти в режим конфігурації протоколу маршрутизації EIGRP 100
Router (config-router)#network 172.16.0.0	Додавання мережі, яка буде розсилатися в таблицях маршрутизації
Router#show ip protocols	Переглянути, які протоколи маршрутизації використовуються на маршрутизаторі
Router# show ip route	Переглянути таблицю маршрутизації
Router# show ip eigrp neighbors	Переглянути таблицю сусідів EIGRP
Router#debug eigrp packet	Переглянути трафік EIGRP

Протокол динамічної маршрутизації OSFP (**Open Shortest Path First**) являє собою протокол, заснований на технології відстеження стану каналу (link-state technology), він використовує **алгоритм Дейкстри (SPF)** – алгоритм пошуку найкоротшого шляху в графі. Протокол OSPF використовується для внутрішньої маршрутизації в системах мереж будь-якої складності.

Розглянемо роботу алгоритму SPF і побудову маршрутів на прикладі системи, зображеної на рис.7.2. Для спрощення будемо розглядати OSPF-систему, що складається тільки з маршрутизаторів, з'єднаних лініями зв'язку типу "точка-точка".

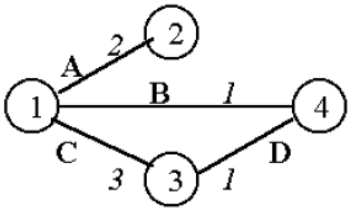


Рис.7.2. Приклад OSPF-системи

Позначення на рисунку: ① ,② ,③ ,④ – маршрутизатори; A,B,C,D – лінії зв’язку (або просто зв’язки), цифри позначають метрику кожного зв’язку.

Метрика являє собою оцінку якості зв'язку в даній мережі (в даному фізичному каналі); чим менше метрика, тим краще якість з'єднання. Метрика маршруту дорівнює сумі метрик всіх зв'язків (мереж), що входять у маршрут.

У простому випадку метрика кожної мережі дорівнює одиниці, а метрика маршруту тоді просто є його довжиною в хопах. Оскільки при роботі алгоритму SPF ситуації, що призводять до нескінченної лічби, неможливі, значення метрик можуть змінюватись в широкому діапазоні. Крім того, протокол OSPF дозволяє визначити для будь-якої мережі різні значення метрик залежно від типу сервісу. Для кожного типу сервісу буде обчислюватися свій маршрут, і дейтаграми, що запитують найбільш швидкісний канал, можуть бути відправлені по одному маршруту, а ті, що запитують найменш дорогий канал

– по іншому. Метрика мережі, яка оцінює пропускну здатність, визначається як кількість секунд, необхідних для передачі 100 Мбіт через фізичне середовище даної мережі.

Для роботи алгоритму SPF на кожному маршрутизаторі будується **база даних стану зв'язків**. Ця база являє собою повний опис графа OSPF-системи. При цьому вершинами графа є маршрутизатори, а ребрами – зв'язки, що їх з'єднують. Бази даних на всіх маршрутизаторах ідентичні. За створення баз даних і підтримку їх взаємної синхронізації при змінах у структурі системи мереж відповідають інші алгоритми, що містяться у протоколі OSPF. База даних стану зв'язків являє собою таблицю, де для кожної пари суміжних вершин графа (маршрутизаторів) зазначено ребро (зв'язок), що їх з'єднує, і метрика цього ребра.

Для досягнення мереж, що не входять в OSPF-систему (в автономну систему), використовуються прикордонні маршрутизатори автономної системи (**autonomous system border router, ASBR**), які мають зв'язки, що йдуть за межі системи. ASBR вносять до бази даних стану зв'язків дані про мережі за межами системи, досяжних через той чи інший ASBR. Такі мережі, а також маршрути, що ведуть до них називаються **зовнішніми** (external). У простому випадку, якщо в системі є тільки один ASBR, він оголошує через себе маршрут за замовчуванням (default route) і всі дейтаграми, адресовані в мережі, що не входять в базу даних системи, відправляються через цей маршрутизатор.

Якщо в системі є декілька ASBR, то, можливо, внутрішнім маршрутизаторам системи доведеться обирати, через який саме прикордонний маршрутизатор потрібно відправляти дейтаграми в ту чи іншу зовнішню мережу. Це робиться на основі спеціальних записів, внесених ASBR в базу даних системи. Ці записи містять адресу і маску зовнішньої мережі, а також метрику відстані до неї, яка може бути, а може і не бути порівнянною з метриками, що використовуються в межах OSPF-системи. Якщо можливо, адреси декількох зовнішніх мереж агрегуються в загальну адресу з коротшою маскою. ASBR може отримувати інформацію про зовнішні маршрути від протоколів зовнішньої маршрутизації, всі або деякі зовнішні маршрути також можуть бути налаштовані адміністратором (у тому числі єдиний маршрут за замовчуванням).

Після ініціалізації модуля OSPF (наприклад, після подачі живлення на маршрутизатор) через всі інтерфейси, включені в OSPF-систему, починають розсилатися Hello-повідомлення для виявлення сусідів і встановлення з ними відносин суміжності.

Сусідами називаються OSPF-маршрутизатори, що підключені до однієї мережі (до однієї лінії зв'язку) і обмінюються Hello-повідомленнями.

Суміжними називаються сусідні OSPF маршрутизатори, які прийняли рішення обмінюватися один з одним інформацією, необхідною для синхронізації бази даних стану зв'язків і побудови маршрутів. Не всі сусіди стають суміжними. Hello-пакети продовжують періодично розсилатися і після того, як сусіди були виявлені. Таким чином, маршрутизатор контролює стан своїх зв'язків з сусідами і може своєчасно виявити зміну цього стану (наприклад, обрив зв'язку або відключення одного з сусідів). Обрив зв'язку може бути також виявлений і за допомогою протоколу канального рівня, який просигналізує про недоступність каналу.

Після встановлення відносин суміжності для кожної пари суміжних маршрутизаторів відбувається синхронізація їх баз даних. Ця ж операція відбувається при відновленні раніше розірваного з'єднання, оскільки в двох ізольованих підсистемах, що утворилися після аварії, бази даних розвивалися незалежно одна від одної.

Синхронізація баз даних відбувається за допомогою **протоколу обміну** (Exchange protocol). Спочатку маршрутизатори обмінюються тільки описами своїх баз даних (Database Description), що містять ідентифікатори записів і номери їх версій, це дозволяє уникнути пересилання всього вмісту бази даних, якщо потрібно синхронізувати тільки кілька записів. Під час цього обміну кожен маршрутизатор формує список записів, вміст яких він повинен запросити (тобто ці записи в його базі даних застаріли або відсутні), і відповідно відправляє пакети запитів про стан зв'язків (Link State Request). У відповідь він

отримує зміст останніх версій потрібних йому записів у пакетах типу "Оновлення стану зв'язків (Link State Update)". Після синхронізації баз даних проводиться побудова маршрутів.

Табл.7.5. Конфігурування OSPF Single Area

Команда	Опис команди
Router> enable	Перейти в привілейований режим
Router#configure terminal	Перейти в режим глобальної конфігурації
Router(config)#router ospf 100	Перейти в режим конфігурації протоколу маршрутизації OSPF 100
Router (config-router)#network 172.16.0.0 0.0.255.255 area 0	Додавання мережі, яка буде розсилатися в таблицях маршрутизації
Router (config-if)#ip ospf cost 10	Встановлення метрики на інтерфейсі
Router (config-if)#ip ospf dead-interval 20	Встановлення часового інтервалу, після якого сусід маршрутизатора вважатиметься недоступним
Router (config-if)#ip ospf hello-interval 20	Встановлення часового інтервалу, після якого буде надсилатись hello-пакет
Router#show ip protocols	Переглянути, які протоколи маршрутизації використовуються на маршрутизаторі
Router# show ip route	Переглянути таблицю маршрутизації
Router# show ip ospf interface	Переглянути таблицю інтерфейсів OSPF
Router# show ip ospf database	Переглянути таблицю топології
Router# show ip ospf	Переглянути загальну інформацію про OSPF
Router# show ip ospf neighbor detail	Переглянути інформацію про конкретного сусіда по OSPF

Приклад. Є двоповерхова будівля, на кожному поверсі є дві частини приміщень, кожна частина використовує свою мережу (рис.7.3):

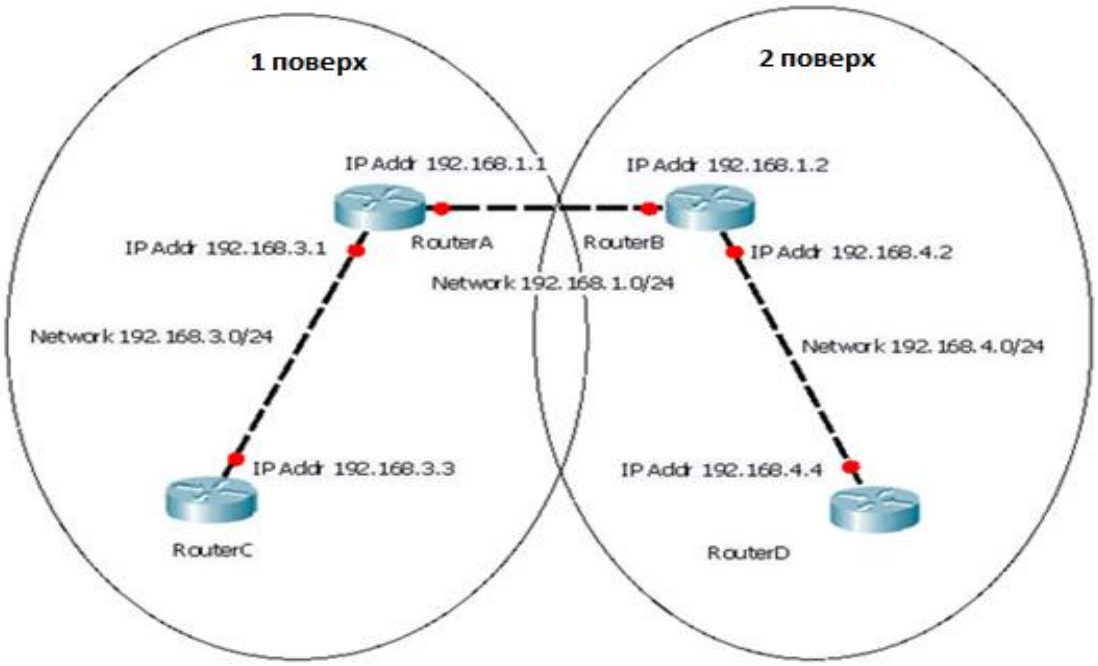


Рис.7.3. IP- маршрутизація у двоповерховій будівлі

RouterA і RouterC обслуговують співробітників першого поверху, RouterB і RouterD – другого поверху. Зв'язок між першим і другим поверхом здійснюється через маршрутизатори RouterA і RouterB. Необхідно налаштувати динамічну маршрутизацію на кожному маршрутизаторі, щоб не вносити маршрути підмереж на всіх пристроях. Це здійснюється шляхом наступних налаштувань маршрутизаторів:

RouterA

Переходимо в режим глобальної конфігурації:

Router# **conf t**

Задаємо ім’я маршрутизатору:

Router(config)#**hostname RouterA**

Переглядаємо доступні интерфейси:

RouterA(config)#**do sh ip int bri**

```
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

Налаштовуємо інтерфейс, який «дивиться» на RoutrB:

RouterA(config)#**int fa 0/0**

Задаємо опис інтерфейсу:

RouterA(config-if)#**description RouterA to RouterB**

Задаємо ip адресу:

RouterA(config-if)#ip addr 192.168.1.1 255.255.255.0

Якщо інтерфейс був виключений (administratively down), включаємо його:

RouterA(config-if)#**no shut**

Налаштовуємо інтерфейс, сусід у якого RouterC:

```
RouterA(config-if)#int fa 0/1
RouterA(config-if)#descr RouterA to RouterC
RouterA(config-if)#ip addr 192.168.3.1 255.255.255.0
RouterA(config-if)#no shut
```

Налаштування OSPF

Включаємо процес на маршрутизаторі, команда router ospf – включення процесу OSPF на маршрутизаторі, а 1111 – довільне id даного процесу:

RouterA(config)#**router ospf 1111**

Задаємо підмережі, які будуть брати участь в процесі OSPFкомандою network, після підмережі необхідно вказати її wildcard маску, в кінці командою area - зону дії OSPF:

RouterA(config-router)#**network 192.168.1.0 0.0.0.255 area 0**

RouterA(config-router)#**network 192.168.3.0 0.0.0.255 area 0**

Для маршрутизатора RouterA в процесі OSPF ми задали дві підмережі:

• **192.168.1.0** - підмережа, за яку відповідає маршрутизатор RouterA;

• **192.168.3.0** - підмережа сусіда (neighbour) за яку відповідає маршрутизатор RouterC.

Дані підмережі маршрутизатор RouterA надалі транслюватиме своїм наступним сусідам, у нашому випадку це RouterB. Налаштовуємо так само інші маршрутизатори.

RouterB

```
Router#conf t
Router(config)#hostname RouterB
RouterB(config)#int fa 0/0
RouterB(config-if)#ip addr 192.168.1.2  255.255.255.0
RouterB(config-if)#no shut
RouterB(config-if)#int fa 0/1
RouterB(config-if)#ip addr 192.168.4.2  255.255.255.0
RouterB(config-if)#no shut
RouterB(config)#router ospf 2222
RouterB(config-router)#network 192.168.1.0  0.0.0.255 area 0
RouterB(config-router)#network 192.168.4.0  0.0.0.255 area 0
```

RouterC

```
Router#conf t
Router(config)#hostname RouterC
RouterC(config)#int fa 0/0
RouterC(config-if)#ip addr 192.168.3.3  255.255.255.0
RouterC(config-if)#no shut
RouterC(config)#router ospf 3333
RouterC(config-router)#network 192.168.3.0  0.0.0.255 area 0
```

RouterD

```
Router#conf t
Router(config)#hostname RouterD
RouterD(config)#int fa 0/0
RouterD(config-if)#ip addr 192.168.3.3  255.255.255.0
RouterD(config-if)#no shut
RouterD(config)#router ospf 4444
RouterD(config-router)#network 192.168.4.0  0.0.0.255 area 0
```

Після налаштування маршрутизатора RouterD має з'явитися повідомлення про те, що процес OSPF завантажив таблицю маршрутизації. Приклад:

```
00:38:13: %OSPF-5-ADJCHG: Process 4444,
Nbr 192.168.4.2 on FastEthernet0/0 from LOADING to FULL, Loading Done
```

Перевірка. Для перевірки необхідно подивитися таблицю маршрутизації на кінцевих пристроях. У нашому випадку RouterD повинен знати маршрут до RouterC і навпаки.

```
RouterD#sh ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
O    192.168.1.0/24 [110/2] via 192.168.4.2, 00:12:14, FastEthernet0/0
O    192.168.3.0/24 [110/3] via 192.168.4.2, 00:00:02, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet0/0
```

```
RouterC#sh ip route
```

```
O    192.168.1.0/24 [110/2] via 192.168.3.1, 00:00:50, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
O    192.168.4.0/24 [110/3] via 192.168.3.1, 00:00:39, FastEthernet0/0
```

Також вони повинні зв’язуватись один з одним.

```
RouterD#ping 192.168.3.3
```

```
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/60/60 ms
RouterC#ping 192.168.4.4
Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 50/60/70 ms
```

Команда, яка відображає інтерфейси сусідніх маршрутизаторів:

```
RouterB#sh cdp neighbors
Capability Codes: R - Router, T - Trans
Bridge, B - Source Route Bridge
                S - Switch, H - Host, I
```

```
- IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce    Holdtme    Capability
Platform    Port ID
RouterA      Fas 0/0
174          R       C1841       Fas 0/0
RouterD      Fa 0/1

166          R       C1841       Fas 0/0
```

Команда, яка показує сусідів по OSPF:

```
RouterB#sh ip ospf neighbor
Neighbor ID     Pri   State           Dead
Time   Address         Interface
192.168.4.4       1   FULL/DR         00:00:33
192.168.4.4     FastEthernet0/1
```

Завдання до лабораторної роботи

У середовищі моделювання Cisco Packet Tracer створити мережу згідно заданої топології (рис.7.4), налаштувати всі пристрої згідно заданої мережевої адресації. Налаштувати і перевірити маршрутизацію OSPF на роутерах R1, R2, R3, яким привласнити імена RN, RN+1, RN+2, де N – номер варіанту (наприклад, якщо варіант 10, то будуть маршрутизатори з іменами R10, R11 та R12).

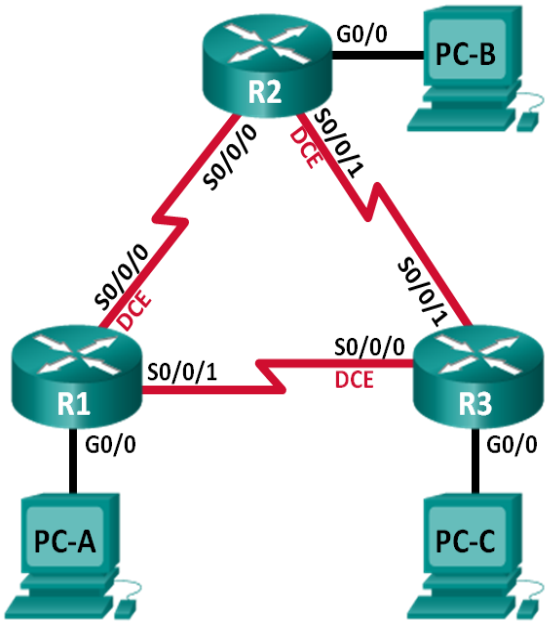


Рис. 7.4. Мережа з трьома маршрутизаторами

Таблиця адресації

Пристрій	Інтерфейс	IP -адреса	Маска підмережі	Шлюз за замовчуванням
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A
PC - A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC - B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC - C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Необхідно налаштувати мережу з маршрутизацією OSPFv2 і перевірити дані маршрутизації OSPF згідно подальших інструкцій.

2. Перевірка з'єднання

Маршрутизатори повинні мати можливість відправляти успішні ехо-запити один одному, і усі ПК повинні мати можливість відправляти успішні ехо-запити на свої шлюзи за замовчуванням. Комп'ютери не можуть відправляти успішні ехо- запити на інші ПК, поки не налагоджена маршрутизація OSPF. При невдалому виконанні ехо- запитів необхідно виконати пошук і усунення неполадок. Потрібно налаштувати маршрутизацію OSPFv2 на усіх маршрутизаторах в мережі, а потім переконатися, що таблиці маршрутизації оновлюються правильно.

3. Налаштування OSPF на маршрутизаторі R1

Використовуйте команду **router ospf** в режимі глобальної конфігурації, щоб активувати OSPF на маршрутизаторі R1.

```
R1(config)# router ospf 1
```

Примітка. Ідентифікатор процесу OSPF зберігається локально і не має відношення до інших маршрутизаторів в мережі.

Використовуйте команду **network** для мереж маршрутизатора R1. Використовуйте ідентифікатор області, рівний 0.

```
R1(config - router)# network 192.168.1.0 0.0.0.255 area 0
R1(config - router)# network 192.168.12.0 0.0.0.3 area 0
R1(config - router)# network 192.168.13.0 0.0.0.3 area 0
```

4. Налаштування OSPF на маршрутизаторах R2 і R3

Використовуйте команду **router ospf** і додайте команду **network** для мереж маршрутизаторів R2 і R3. Коли маршрутизація OSPF буде налагоджена на R2 і R3, на маршрутизаторі R1 з'являться повідомлення про встановлені стосунки суміжності.

```
R1#
0000:22:29: %OSPF - 5 - ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from
LOADING to FULL, Loading Done
R1#
0000:23:14: %OSPF - 5 - ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from
LOADING to FULL, Loading Done
R1#
```

5. Перевірка інформації про сусідів і маршрутизацію OSPF

Використовуйте команду **show ip ospf neighbor** для перевірки списку суміжних маршрутизаторів на кожному маршрутизаторі відповідно до заданої топології.

```
R1# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.23.2      0   FULL/  -        00:00:33    192.168.13.2    Serial0/0/1
192.168.23.1      0   FULL/  -        00:00:30    192.168.12.2    Serial0/0/0
```

Виконайте команду **show ip route**, щоб переконатися, що в таблицях маршрутизації усіх маршрутизаторів відображуються усі мережі.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
               D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
               N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
               E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
               i - IS - IS, L1 - IS - IS level - 1, L2 - IS - IS level - 2, ia - IS
- IS inter area
        * -        * - candidate default, U - per - user static route, o - ODR
               P - periodic downloaded static route
Gateway of last resort is not set
          192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
          192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
          192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
          192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
           [110/128] via 192.168.13.2, 00:31:38, Serial0/0/1
```

Для перегляду маршрутів OSPF в таблиці маршрутизації використовується команда **show ip route ospf.**

6. Перевірка налаштування протоколу OSPF

Команда **show ip protocols** забезпечує швидку перевірку критично важливих даних конфігурації OSPF. До таких даних відносяться ідентифікатор процесу OSPF, ідентифікатор маршрутизатора, мережі, що оголошуються маршрутизатором, сусідні пристрої, від яких маршрутизатор приймає оновлення, і значення адміністративної дистанції за замовчуванням, що рівне 110 для OSPF.

```
R1# show ip protocols
*** *** IP Routing is NSF aware ***
Routing Protocol is "ospf 1"
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
    Router ID 192.168.13.1
    Number of areas in this router is 1. 1 normal 0 stub 0 nssa
    Maximum path: 4
    Routing for Networks :
        192.168.1.0 0.0.0.255 area 0
        192.168.12.0 0.0.0.3 area 0
        192.168.13.0 0.0.0.3 area 0
    Routing Information Sources :
        Gateway         Distance      Last Update
    192.168.23.2         110      00:19:16
    192.168.23.1         110      00:20:03
    Distance: (default is 110)
```

7. Перевірка даних процесу OSPF

Використовуйте команду **show ip ospf**, щоб проглянути ідентифікатори процесу OSPF і маршрутизатора. Ця команда відображує дані про зону OSPF і показує час, коли останній раз виконувався алгоритм пошуку найкоротшого шляху SPF.

```
R1# show ip ospf
  Routing Process "ospf 1" with ID 192.168.13.1
  Start time: 00:20:23.260, Time elapsed: 00:25:08.296
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Link - local Signaling (LLS)
  Supports area transit capability
  Supports NSSA (compatible with RFC 3101)
  Event - log enabled, Maximum number of events: 1000, Mode: cyclic
  Router is not originating router - LSAs with maximum metric
  Initial SPF schedule delay 5000 msecs
  Minimum hold time between two consecutive SPFs 10000 msecs
  Maximum wait time between two consecutive SPFs 10000 msecs
  Incremental - SPF disabled
  Minimum LSA interval 5 secs
  Minimum LSA arrival 1000 msecs
  LSA group pacing timer 240 secs
  Interface flood pacing timer 33 msecs
  Retransmission pacing timer 66 msecs
  Number of external LSA 0. Checksum Sum 0x000000
  Number of opaque AS LSA 0. Checksum Sum 0x000000
  Number of DCbitless external and opaque AS LSA 0
  Number of DoNotAge external and opaque AS LSA 0
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Number of areas transit capable is 0
  External flood list length 0
  IETF NSF helper support enabled
  Cisco NSF helper support enabled
  Reference bandwidth unit is 100 mbps
        Area BACKBONE(0)
                Number of interfaces in this area is 3
                Area has no authentication
                SPF algorithm last executed 00:22:53.756 ago
                SPF algorithm executed 7 times
                Area ranges are
                Number of LSA 3. Checksum Sum 0x019A61
                Number of opaque link LSA 0. Checksum Sum 0x000000
                Number of DCbitless LSA 0
                Number of indication LSA 0
                Number of DoNotAge LSA 0
                Flood list length 0
```

8. Перевірка налаштування інтерфейсу OSPF

Виконаєте команду **show ip ospf interface brief**, щоб відобразити дані про інтерфейси, на яких активований алгоритм OSPF.

```
R1# show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Se0/0/1      1     0               192.168.13.1/30    64    P2P   1/1
Se0/0/0      1     0               192.168.12.1/30    64    P2P   1/1
Gi0/0        1     0               192.168.1.1/24     1     DR    0/0
```

Для того, щоб побачити детальніші дані про інтерфейси, на яких активований OSPF, виконайте команду **show ip ospf interface**.

```
R1# show ip ospf interface
Serial0/0/1 is up, line protocol is up
    Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
    Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost : 64
    Topology - MTID    Cost    Disabled    Shutdown      Topology Name
        0                  0           64        no          no            Base
    Transmit Delay is 1 sec, State POINT_TO_POINT
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
        oob - resync timeout 40
        Hello due in 00:00:01
    Supports Link - local Signaling (LLS)
    Cisco NSF helper support enabled
    IETF NSF helper support enabled
    Index 3/3, flood queue length 0
    Next 0x0(0)/0x0(0)
    Last flood scan length is 1, maximum is 1
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 1, Adjacent neighbor count is 1
        Adjacent with neighbor 192.168.23.2
    Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
    Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement
    Process ID 1, Router ID 192.168.13.1, Network Type POINT_TO_POINT, Cost : 64
    Topology - MTID    Cost    Disabled    Shutdown      Topology Name
        0                  0           64        no          no            Base
    Transmit Delay is 1 sec, State POINT_TO_POINT
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
        oob - resync timeout 40
        Hello due in 00:00:03
    Supports Link - local Signaling (LLS)
    Cisco NSF helper support enabled
    IETF NSF helper support enabled
    Index 2/2, flood queue length 0
    Next 0x0(0)/0x0(0)
    Last flood scan length is 1, maximum is 1
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 1, Adjacent neighbor count is 1
        Adjacent with neighbor 192.168.23.1
    Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
    Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
    Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost : 1
    Topology - MTID    Cost    Disabled    Shutdown      Topology Name
        0                  0           1         no          no            Base
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
        oob - resync timeout 40
        Hello due in 00:00:01
    Supports Link - local Signaling (LLS)
    Cisco NSF helper support enabled
    IETF NSF helper support enabled
    Index 1/1, flood queue length 0
    Next 0x0(0)/0x0(0)
    Last flood scan length is 0, maximum is 0
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 0, Adjacent neighbor count is 0
    Suppress hello for 0 neighbor(s)
```

9. Перевірка наявності наскрізного з'єднання

Усі комп'ютери повинні успішно виконувати ехо-запити до усіх інших комп'ютерів, вказаних в топології. При невдалому виконанні ехо-запитів виконати пошук і усунення неполадок.

Вимоги до оформлення звіту

Звіт має включати: титульний аркуш, індивідуальне завдання на лабораторну роботу, хід роботи та висновки. Необхідно зробити скріншот створеної топології мережі, навести опис всіх введених команд для налаштування динамічної маршрутизації.

Питання до лабораторної роботи

1. Яка будова і призначення маршрутизатора?
2. Які користувацькі режими існують в Packet Tracer? Чим вони відрізняються один від одного? Які команди використовуються для переходу в кожний з режимів?
3. Коротка характеристика та призначення протоколу CDP.
4. Для чого використовується статична маршрутизація?
5. Який синтаксис команд статичної маршрутизації?
6. Для чого використовується динамічна маршрутизація?
7. Які типи та протоколи динамічної маршрутизації ви знаєте?
8. Які особливості EIGRP та OSPF – маршрутизації?
9. Які особливості налаштування OSPF?
10. Які алгоритми пошуку найкоротших маршрутів використовують протоколи EIGRP та OSPF?

Рекомендована література

1. CNA R&S // Електронний ресурс. Режим доступу: http://static-course-assets.s3.amazonaws.com
2. MCITCM – 2. Методи та засоби автоматизованого моделювання та проектування комп'ютерних мереж. Методичні вказівки до виконання лабораторних робіт. [Електронне видання] / Уклад.: Я.Ю. Дорогий, М.М. Букасов. – К.: НТУУ «КПІ», 2012. – 76 с.
3. Порівняння статичної та динамічної маршрутизації // Електронний ресурс. Режим доступу: http://posibnyky.vntu.edu.ua/kom_m/4.4.html
4. Статична маршрутизація // Електронний ресурс. Режим доступу: https://habrahabr.ru/post/140552/
5. Маршрутизація // Електронний ресурс. Режим доступу: http://www.cs.vsu.ru/~kas/doc/exe/cisco/CCNA05.pdf
6. Review the OSPF basics// Електронний ресурс. Режим доступу: http://www.setup32.com/network-administration/networking/know-ospf.php
7. Введення в EIGRP // Електронний ресурс. Режим доступу: http://novacom.ru/tech_support/Cisco/eigrp.html

ЛАБОРАТОРНА РОБОТА № 8. СПИСКИ КОНТРОЛЮ ДОСТУПУ

Мета роботи: навчитися виконувати налаштування IP ACLs для доступу або заборони певного трафіку та зменшення кількості мережевих атак.

Теоретичні відомості

ACL (англ. **Access Control List** – список контролю доступу) визначає, хто або що може отримувати доступ до конкретного об'єкта, і які саме операції дозволено або заборонено виконувати над об'єктом. У мережах ACL подають список правил, що визначають порти служб або імена доменів, доступних на вузлі або іншому пристрою третього рівня OSI, кожен зі списком вузлів та/або мереж, яким дозволений доступ до сервісу. Мережеві ACL

можуть бути налаштовані як на звичайному сервері, так і на маршрутизаторі і можуть керувати як вхідним, так і вихідним трафіком, в якості брандмауера.

Списки ACL визначають дозволений і небажаний мережевий трафік. Перед тим, як почати дозволяти або забороняти певний тип мережевого трафіку, необхідно визначитися з відповідними критеріями. При розробці критеріїв дозволу або відхилення трафіку мережі слід встановити порядок важливості для цих критеріїв. Залежно від встановлених критеріїв, у кінці процесу відбору відмова або дозвіл на доступ до мережі можуть отримати один або декілька вузлів.

ACL застосовується:

• на інтерфейсі: пакетна фільтрація;
• на лінії Telnet: обмеження доступу до маршрутизатора;
• VPN: який трафік потрібно шифрувати;
• QoS: який трафік обробляти приоритетніше;
• NAT: які адреси необхідно транслювати.

ACL розміщуються на інтерфейсах, самі вони створюються незалежно, а вже потім вони налаштовуються до інтерфейсу. Як тільки ви його налаштували до інтерфейсу, маршрутизатор починає переглядати трафік. Маршрутизатор розглядає трафік як вхідний і вихідний. Трафік, який входить в маршрутизатор називається **вхідним**, той який з нього виходить – **вихідним**. Відповідно ACL розміщуються на вхідному або на вихідному напрямі.

Наприклад, з приватної мережі приходить пакет на інтерфейс маршрутизатора fa0/1, маршрутизатор перевіряє, чи є ACL на інтерфейсі чи ні, якщо він є, то далі обробка ведеться за правилами списку доступу строго в тому порядку, в якому записані вирази, якщо список доступу дозволяє проходити пакету, то в даному випадку маршрутизатор відправляє пакет провайдеру через інтерфейс fa0/0, якщо список доступу не дозволяє проходити пакету, пакет знищується. Якщо списку доступу немає – пакет пролітає без всяких обмежень. Перед тим, як відправити пакет провайдеру, маршрутизатор ще перевіряє інтерфейс fa0/0 на наявність вихідного ACL. Наприклад у нас є ACL з правилом заборонити всім вузлам в Інтернеті посилати в нашу мережу пакети. На який інтерфейс прикріпити даний ACL? Якщо ми прикріпимо ACL на інтерфейс fa0/1 як вихідний, це буде не зовсім вірно, хоча і ACL працювати буде. На маршрутизатор приходить ехо-запит для якогось вузла в приватній мережі, він перевіряє на інтерфейсі fa0/0 чи є ACL, його немає, далі перевіряє інтерфейс fa0/1, на даному інтерфейсі є ACL, він налаштований як вихідний, тоді пакет не проникає в мережу, а знищується маршрутизатором. Але якщо ми прикріпимо ACL за інтерфейсом fa0/0 як вхідний, то пакет знищиться відразу, як прийде на маршрутизатор. Останнє рішення є правильним, так як маршрутизатор менше навантажує свої обчислювальні ресурси. Розширені ACL потрібно розміщувати як можна ближче до джерела, стандартні ж якомога ближче до одержувача. Це потрібно для того, щоб не ганяти пакети по всій мережі даремно.

ACL являє собою набір текстових виразів, в яких написано **permit** (дозволити) або **deny** (заборонити), і обробка ведеться строго в тому порядку в якому задані вирази. Відповідно, коли пакет потрапляє на інтерфейс, він перевіряється на першу умову, якщо перша умова збігається з пакетом, подальша його обробка припиняється. Пакет або перейде далі, або знищиться. Якщо пакет збігся з умовою, далі він не обробляється. Якщо перша умова не співпала, йде обробка другої умови, якщо вона співпала, обробка припиняється, якщо немає, йде обробка третьої умови і так далі поки не перевірятися всі умови, якщо жодна з умов не збігається, пакет знищується. У кожному кінці списку стоїть неявний **deny any** (заборонити весь трафік).

ACL поділяються на два типи:

- **стандартні (Standard)**: можуть перевіряти тільки адреси джерел;

• **розширені (Extended)**: можуть перевіряти адреси джерел, а також адреси отримувачів, в разі IP ще тип протоколу і TCP / UDP порти.

Стандартні ACL нумеруються в діапазоні (1-99) та (1300-1999), **розширені** (100-199) та (2000-2699). Позначаються списки доступу або номерами, або символьними іменами. ACL також використовуються для різних мережевих протоколів. Символьні ACL поділяються теж на стандартні і розширені. Розширені ACL можуть перевіряти набагато більше, ніж стандартні, а й працюють вони повільніше, так як доведеться заглядати всередину пакета, на відміну від стандартних, де ми дивимося тільки поле **Source Address** (Адреса відправника).

При створенні ACL кожен запис списку доступу позначається порядковим номером, за замовчуванням в рамках десяти (10, 20, 30 і т.д). Не можна розмістити понад 1 списку доступу на інтерфейс, на протокол, на напрям.

Якщо у нас є маршрутизатор і у нього є інтерфейс, ми можемо на вхідний напрямок для IP-протоколу розмістити тільки один список доступу, наприклад під номером 10. Ще одне правило, яке стосується самих маршрутизаторів, ACL не діє на трафік, згенерований самим маршрутизатором .

Для фільтрації адрес в ACL використовується **WildCard-маска**. Це зворотна маска. Беремо шаблонний вираз: 255.255.255.255 і віднімаємо від шаблону звичайну маску:

255.255.255.255-255.255.255.0, у нас виходить WildCard маска 0.0.0.255.

Налаштування ACL

Самі ACL створюються окремо, тобто це просто список, який створюється в режимі глобальної конфігурації, потім він присвоюється до інтерфейсу і тільки тоді він і починає працювати. Необхідно пам'ятати деякі моменти, для того, щоб правильно налаштувати списки доступу:

• обробка ведеться строго в тому порядку, в якому записані умови;
• якщо пакет збігся з умовою, далі він не обробляється;
• у кінці кожного списку доступу варто неявний **deny any** (заборонити все);
• розширені ACL потрібно розміщувати як можна ближче до джерела, стандартні ж якомога ближче до одержувача;
• не можна розмістити понад 1 списку доступу на інтерфейс, на протокол, на напрям;
• ACL не діє на трафік, згенерований самим маршрутизатором;
• для фільтрації адрес використовується WildCard маска.

Стандартний список доступу

Router (config) # access-list <номер списку> {permit | deny | remark} {address | any | host} [source-wildcard] [log],

permit: дозволити;
deny: заборонити;
remark: коментар про список доступу;
address: забороняємо або дозволяємо мережу;
any: дозволяємо або забороняємо все;
host: дозволяємо або забороняємо хосту;
source-wildcard: WildCard маска мережі;
log: включаємо логовані пакети проходять через даний запис ACL.

Правило **deny ip any any** часто дописують в кінці правил, щоб явно бачити по спрацьовуванню лічильників, що трафік заблокував ACL.

Розширений список доступу

Router (config) # access-list <номер списку> {permit | deny | remark} protocol source [source-wildcard] [operator operand] [port <порт або назва протоколу> [established],

protocol source: який протокол будемо дозволяти або ні (ICMP, TCP, UDP, OSPF тощо);

deny: заборонити;

operator:

A.B.C.D – адреса одержувача;

any – будь-який кінцевий хост;

eq – тільки пакети на цьому порті;

gt – тільки пакети з великим номером порту;

host – єдиний кінцевий хост;

lt – тільки пакети з нижчим номером порту;

neq – тільки пакети не на даному номері порту;

range – діапазон портів;

port: номер порту (TCP або UDP), можна вказати ім'я;

established: дозволяємо проходження TCP-сегментів, які є частиною створеної TCP-сесії.

Прикріплення ACL до інтерфейсу

Router (config-if) #ip access-group <номер списку або ім'я ACL> {in | out}

in: вхідний напрямок;

out: вихідний напрямок.

Іменовані списки доступу

Router (config) #ip access-list {standard | extended} {<номер ACL> | <Ім'я ACL>}
Router (config-ext-nacl) # {default | deny | exit | no | permit | remark}

standard: стандартний ACL;

extended: розширений ACL;

default: встановити команду в значення за замовчуванням.

Отже, ACL можна конфігурувати **для протоколу, напрямку та інтерфейсу.**

SSH (англ. **Secure SHell** – «безпечна оболонка») – мережевий протокол сеансового рівня, що дозволяє проводити віддалене управління операційною системою і тунелювання TCP-з'єднань (наприклад, для передачі файлів). Схожий за функціональністю з протоколами **Telnet** і **rlogin**, але, на відміну від них, шифрує весь трафік, включаючи і передані паролі. SSH допускає вибір різних алгоритмів шифрування. SSH-клієнти і SSH-сервери наявні для більшості мережевих операційних систем. Існує кілька версій протоколу SSH, що розрізняються використанням алгоритмів шифрування і загальними схемами роботи. SSH надає 3 способи аутентифікації клієнта: за ip адресою клієнта (небезпечно), за публічним ключем клієнта і стандартний метод з використанням пароля. Ssh версії 2 працює наступним чином: при запиті клієнта сервер повідомляє йому, які методи аутентифікації він підтримує і клієнт по черзі намагається перевірити їх. За замовченням клієнт спочатку намагається аутентифікуватися за своєю адресою, потім за публічним ключем і, якщо нічого не спрацювало, передає пароль, введений з клавіатури (при цьому пароль шифрується асиметричним шифруванням). Після проходження аутентифікації одним з методів з наявних у клієнта і сервера пар ключів генерується ключ симетричного шифрування на підставі свого секретного та віддаленого публічного ключа. Після чого всі наступні дані, передані через ssh, шифруються даним ключем (зазвичай використовується алгоритм aes з довжиною ключа 128 біт). Протокол ssh версії 1 мав деякі баги в шифруванні переданого трафіку і був по суті методом безпечної аутентифікації, тому даний протокол вважається небезпечним. Протокол версії 2 підтримує більш сучасні методи шифрування тарфіку, також разом з даними надсилаються контрольні суми формату sha або md5, що виключає підміну чи іншу модифікацію переданого трафіку (чого не було у ssh версії 1).

Способи аутентифікації користувачів через ssh:

• **За адресою клієнта.** При використанні даного способу аутентифікації відбувається наступне: кожен клієнт і сервер мають свої пари ключів RSA, які називаються ключі хоста. При цьому існує кілька методів перевірки адреси клієнта.

• **Аутентифікація користувача за його публічним ключем**. Аутентифікація віддаленого користувача за ключем, ідентична перевірці ключа хоста (з посилкою випадкового рядка) з тим винятком, що перевіряється не адреса клієнтської машини, а ключ клієнта та ім'я користувача. Даному користувачеві на сервері може відповідати його публічний ключ, тоді клієнт, маючи секретний ключ, зможе заходити на сервер без пароля.

• **Звичайна аутентифікація з використанням пароля**. Тут можна відзначити тільки одне: у будь-якому випадку спочатку йде обмін асиметричними ключами, і хеш пароля передається в зашифрованому вигляді.

Розглянемо приклад. Нехай маємо мережу заданої топології (рис.8.1).

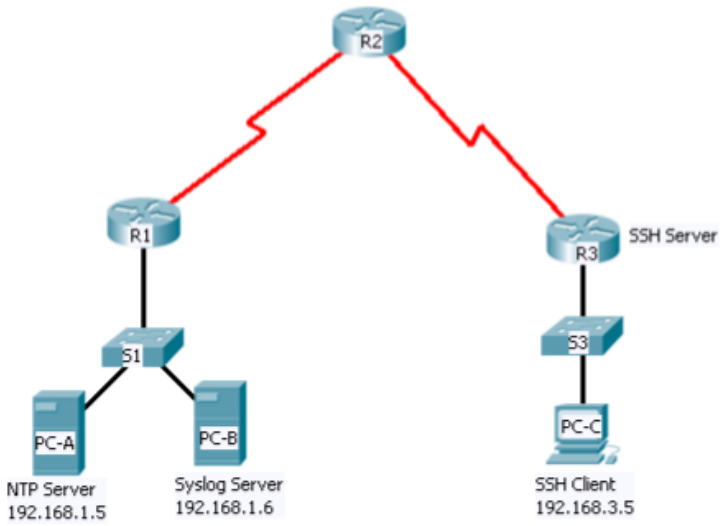


Рис.8.1. Модель мережі з трьома маршрутизаторами

Таблиця адресації

Пристрій	Інтерфейс	IP - адреса	Маска підмережі	Шлюз за замовчуванням
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC A	NIC	192.168.1.5	255.255.255.0	192.168.1.1
PC B	NIC	192.168.1.6	255.255.255.0	192.168.1.1
PC C	NIC	192.168.3.5	255.255.255.0	192.168.3.1

Маршрутизатор R2 (ISP) з'єднаний з двома віддаленими мережами: R1 і R3. Локальний адміністратор з R3 може виконати більшість налаштувань маршрутизатора або усунути несправність, однак, так як R3 – керований маршрутизатор, ISP потребує доступу до R3 для пошуку та усунення несправностей або оновлення. Щоб забезпечити цей доступ

безпечним способом, адміністратори погодилися використовувати Secure Shell (SSH). Для налаштування можна використовувати CLI замість Telnet, він буде захищений за допомогою SSH – мережевого протоколу, який встановлює безпечне термінальне з'єднання з маршрутизатором або іншим мережним пристроєм. SSH шифрує всю інформацію, яка проходить через мережу і забезпечує аутентифікацію віддаленого комп'ютера. Для підключення за допомогою безпечного протоколу SSH потрібно скористатися командою **transport input ssh**. Щоб дозволити весь трафік, потрібно ввести команду **transport input all**.

Маршрутизатори були попередньо сконфігуровані з наступними параметрами:

• Enable password: ciscoenpa55

• Password for vty lines: ciscovtypa55

• Static routing

Необхідно налаштувати R3 для підтримки SSH-з'єднання. Налаштувати доменне ім'я **ccnasecurity.com** на R3.

R3(config)# ip domain-name ccnasecurity.com

Налаштувати користувачів для входу в систему за допомогою SSH на R3 Створити код користувача **SSHadmin** з максимально можливим рівнем повноважень і секретним паролем **ciscosshpa55**.

R3(config)# username SSHadmin privilege 15 secret ciscosshpa55

Налаштувати вхідну лінію VTY на R3. Використовувати локальний обліковий запис для обов'язкового логіна і пароля. Дозволити тільки SSH з'єднання.

R3(config)# line vty 0 4

R3(config-line)# login local

R3(config-line)# transport input ssh

Стерти існуючі пари ключа на R3. Будь-які існуючі пари ключів RSA повинні бути стерті на маршрутизаторі:

R3(config)#crypto key zeroize rsa

Примітка. Якщо ключі відсутні, ви отримаєте це повідомлення:% No Signature RSA Keys found in configuration.

Згенерувати пару ключів шифрування RSA для R3. Маршрутизатор використовує пару ключів RSA для аутентифікації і шифрування переданих даних SSH. Налаштувати ключі RSA з модулем 1024. Значення за замовчуванням 512, і діапазон від 360 до 2048.

R3(config)# crypto key generate rsa

[Enter] The name for the keys will be: R3.ccnasecurity.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]:1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Перевірити SSH конфігурацію. Використання **show ip ssh** команди дозволяє побачити поточні налаштування SSH. Перевірити, щоб тайм-аути аутентифікації і повторення мали значення за замовчуванням 120 і 3.

Налаштувати SSH тайм-аут і параметрів аутентифікації. Тайм-аути SSH за замовчуванням і параметри аутентифікації можуть бути змінені. Встановіть тайм-аут 90 секунд, число повторень аутентифікації 2, і версію 2.

R3(config)# ip ssh time-out 90

R3(config)# ip ssh authentication-retries 2

R3(config)# ip ssh version 2

Виконати **show ip ssh** команду знову, щоб упевниться, що значення були змінені.

Спробувати з'єднатися з R3 через Telnet від PC-C. Відкрити робочий стіл PC-C. Обрати значок Command Prompt. З PC-C, ввести команду, щоб з'єднатися з R3 через Telnet.

PC> telnet 192.168.3.1

Це з'єднання буде перервано, оскільки R3 був налаштований на прийом тільки SSH з'єднань на віртуальній лінії терміналу.

З'єднатися з R3, використовуючи SSH на PC-C Відкрити робочий стіл PC-C. Обрати значок Command Prompt. Від PC-C, ввести команду, щоб з'єднатися з R3 через SSH. Коли буде запитаний пароль, ввести пароль, сконфігурований для адміністратора: **ciscosshpa55.**

PC> ssh –l SSHadmin 192.168.3.1

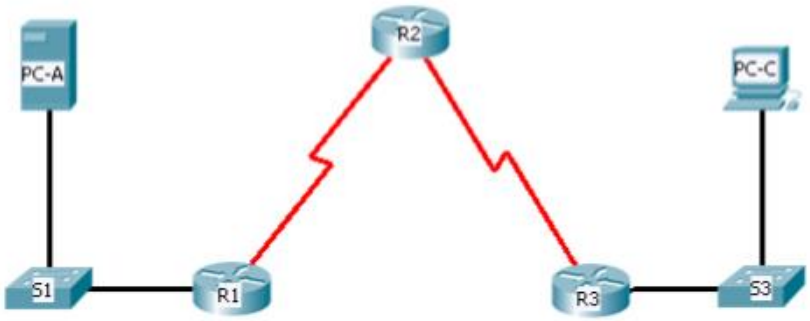
З'єднатися з R3, використовуючи SSH на R2. Для того, щоб діагностувати і підтримувати R3 маршрутизатор, адміністратор ISP повинен використовувати SSH для доступу до CLI маршрутизатора. З CLI R2, ввести команду, щоб з'єднатися з R3 через SSH версії 2, використовуючи обліковий запис користувача **SSHadmin**. Коли буде запитано пароль, ввести пароль, сконфігурований для адміністратора: **ciscosshpa55.**

R2# ssh –v 2 –l SSHadmin 10.2.2.1

Перевірити результати.

Розглянемо інший приклад. Нехай у нас є мережа заданої топології та таблиця адресації пристроїв даної мережі.

Топологія мережі



Таблиця адресації

Пристрій	Інтерфейс	IP - адреса	Маска підмережі	Шлюз за замовчуванням
R N (R1)	Fa0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R N+1 (R2)	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	LoO	192.168.2.1	255.255.255.0	N/A
R N+2 (R3)	Fa0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Необхідно, щоб виконувались наступні умови.

Доступ до маршрутизаторів R1, R2 і R3 повинен бути дозволений лише від вузла PC-C.

PC-C також використовується для перевірки підключень до PC-A, сервер надає DNS, SMTP, FTP, і HTTPS послуги. Стандартний режим роботи повинен використовувати ACL на граничних маршрутизаторах, для зменшення спільної загрози до атак, заснованих на

IP-адресі джерела та/або адресі призначення. Необхідно створити ACL на граничних маршрутизаторах R1 і R3 та перевірити роботу ACL від внутрішніх і зовнішніх вузлів.

Виконання роботи

1) Перевірити зв'язки мережі

Перевірити підключення до мережі перед налаштуванням IP ACL:

Від PC-C в командному рядку, зробити **ping** до PC-A сервера.

Від PC-C в командному рядку, підключитися через **SSH** до маршрутизатора R2 на Lo0 інтерфейс.

Вийти з сеансу SSH.

Від PC-C, відкрити web браузер і підключитися на PC-A сервер, щоб відобразити web сторінку. Закрити браузер на PC-C.

Від PC-A сервера в командному рядку, зробити **ping** PC-C.

2) Безпечний доступ до маршрутизатора

Налаштувати ACL 10, щоб заблокувати весь віддалений доступ до маршрутизаторів окрім як від PC-C. Використати команду **access-list** щоб створити нумерований IP ACL на R1, R2, і R3.

R1(config)# access-list 10 permit 192.168.3.3 0.0.0.0
R2(config)# access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)# access-list 10 permit 192.168.3.3 0.0.0.0

Застосувати ACL 10 до вхідного трафіку на VTY лінії. Використати команду **access-class** щоб застосувати нумерований список доступу (access-list) до вхідного трафіку на VTY лінії.

R1(config-line)# access-class 10 in
R2(config-line)# access-class 10 in
R3(config-line)# access-class 10 in

Перевірити монопольний доступ від станції управління PC-C.

SSH до 192.168.2.1 від PC-C (повинен бути вдалим).

SSH до 192.168.2.1 від PC-A (повинен бути невдалим).

3) Створити нумерований IP ACL 100. На R3, блокувати всі пакети, що містять IP-адресу джерела з наступних адрес: 127.0.0.0 / 8, будь-яких RFC 1918 приватних адрес, а також будь-які широкомовні IP адреси.

Налаштувати ACL 100 для блокування певного трафіку із зовнішньої мережі. Також блокувати трафік, отриманий від внутрішнього адресного простору, якщо це не адреса RFC 1918 (у цьому випадку, внутрішнє адресний простір - частина приватного адресного простору, визначеного в RFC 1918).

Використти команду **access-list** щоб створити нумерований IP ACL.

R3(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)# access-list 100 permit ip any any

Застосувати ACL до інтерфейсу Serial 0/0/1. Використати команду **ip access-group**, щоб застосувати список доступу до вхідного трафіку на інтерфейсі Serial 0/0/1.

R3(config)# interface s0/0/1
R3(config-if)# ip access-group 100 in

Переконатися, що вказаний трафік приходить на інтерфейс Serial 0/0/1 заблокованим. З командного рядка PC-C пропінгувати сервер PC-A. ICMP exo-відповіді блокуються ACL, оскільки вони отримані від адресного простору 192.168.0.0.

Прибрати ACL з Serial 0/0/1.

Видалити ACL. В іншому випадку, весь трафік від зовнішньої мережі (розглядаючи щодо приватних IP адрес джерела) буде закритий для інших. Команда **no ip access-group** видаляє список доступу з інтерфейсу Serial 0/0/1.

R3(config)# interface s0/0/1

R3(config-if)# no ip access-group 100 in

4) Створити нумерований IP ACL 110

Заборонити всі вихідні пакети з адреси джерела за межами діапазону внутрішніх IP адрес.

Налаштувати ACL 110 на дозвіл доступу трафіку тільки з внутрішньої мережі Скористатися коммандою **access-list** для створення нумерованого списку IP ACL.

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 any

Застосувати ACL для інтерфейсу F0/1. Використати команду **ip access-group** щоб застосувати список доступу до вхідного трафіку на інтерфейсі F0/1.

R3(config)# interface fa0/1 R3(config-if)# ip access-group 110 in

5) Створити нумерований IP ACL 120 Дозволити будь-який зовнішній вузол для DNS, SMTP, і FTP сервісів на сервері PC-A, заборонити будь-який зовнішній доступ до служби HTTPS на PC-A, і дозволити PC-C доступ до R1 через SSH.

Перевірити, що PC-C може отримати доступ до PC-A через HTTPS, використовуючи веб-браузер Переконатися, що відключили HTTP і включили HTTPS на PC-A сервері

Налаштувати ACL 120, на дозвіл і заборону зазначеного трафіку. Використати команду **access-list**, щоб створити пронумерований IP ACL.

R1(config)# access-list 120 permit udp any host 192.168.1.3 eq domain

R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq smtp

R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq ftp

R1(config)# access-list 120 deny tcp any host 192.168.1.3 eq 443

R1(config)# access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22

Застосувати ACL до інтерфейсу S0/0/0. Використати команду **ip access-group**, щоб застосувати список доступу до вхідного трафіку на інтерфейсі S0/0/0.

R1(config)# interface s0/0/0

R1(config-if)# ip access-group 120 in

Перевірити, що PC-C не зможе отримати доступ до PC-A через HTTP, використовуючи веб-браузер.

6) Зміна існуючого ACL/ Дозволити ICMP exo-відповіді та недосяжні адресату повідомлення із зовнішньої мережі (порівняно з R1); заборонити всі інші вхідні ICMP пакети.

Перевірити, що PC-A не може успішно виконати ping-запит loopback інтерфейс на R2.

Змінити ACL 120, щоб дозволяти і забороняти вказаний трафік. Використати команду **access-list** щоб створити пронумерований IP ACL.

R1(config)# access-list 120 permit icmp any any echo-reply

R1(config)# access-list 120 permit icmp any any unreachable

R1(config)# access-list 120 deny icmp any any

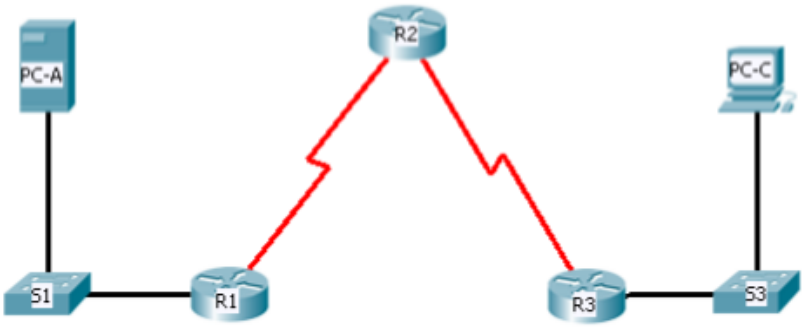
R1(config)# access-list 120 permit ip any any

Перевірити, що PC-A може успішно виконати **ping**-запит на петлевий (**loopback**) інтерфейс R2.

Завдання до лабораторної роботи

Задано мережу заданої топології та таблиця адресації пристроїв, необхідно задати імена маршрутизаторам, RN, RN+1, RN+2, де N – номер варіанту (наприклад, якщо варіант 10, то будуть маршрутизатори з іменами R10, R11 та R12).

Топологія мережі



Таблиця адресації

Пристрій	Інтерфейс	IP - адреса	Маска підмережі	Шлюз за замовчуванням
R N	Fa0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R N+1	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	LoO	192.168.2.1	255.255.255.0	N/A
R N+2	Fa0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Необхідно:

Налаштувати маршрутизатори для підтримки SSH з'єднання. Налаштувати користувачів для вхід в систему за допомогою SSH. Створити код користувача з максимально можливим рівнем повноважень і секретним паролем. Налаштувати вхідну лінію VTY на R3. Використовувати локальний обліковий запис для обов'язкового логіна і пароля. Дозволити тільки SSH з'єднання. Стерти існуючі пари ключа на R3. Будь-які існуючі пари ключів RSA повинні бути стерті на маршрутизаторі. Згенерувати пару ключів шифрування RSA для маршрутизаторів. Налаштувати ключі RSA з модулем 1024. Значення за замовчуванням 512, і діапазон від 360 до 2048.

Налаштувати SSH тайм-аут і параметрів аутентифікації.

Встановити тайм-аут 90 секунд, число повторень аутентифікації 2, і версію 2.

Виконати **show ip ssh** команду знову, щоб упевниться, що значення були змінені.

Перевірити, чи є з'єднання з R3 через Telnet від PC-C.

З'єднатися з R3, використовуючи SSH на PC-C.

З'єднатися з R3, використовуючи SSH на R2.

Доступ до маршрутизаторів R1, R2 і R3 повинен бути дозволений лише від вузла PC-C.

PC-C також використовується для перевірки підключень до PC-A. Створити ACL на граничних маршрутизаторах R1 і R3 та перевірити роботу ACL від внутрішніх і зовнішніх вузлів.

Налаштувати ACL 10, щоб заблокувати весь віддалений доступ до маршрутизаторів окрім як від PC-C. Створити нумерований IP ACL на R1, R2, і R3.

Перевірити монопольний доступ від станції управління PC-C.

Створити нумерований IP ACL 100. На R3, блокувати всі пакети, що містять IP-адресу джерела з наступних адрес: 127.0.0.0/8, будь-яких RFC 1918 приватних адрес, а також будь-які широкомовні IP адреси.

Налаштувати ACL 100 для блокування певного трафіку із зовнішньої мережі. Блокувати трафік, отриманий від внутрішнього адресного простору.

Створити нумерований IP ACL 110.

Заборонити всі вихідні пакети з адреси джерела за межами діапазону внутрішніх IP адрес.

Налаштувати ACL 110 на дозвіл доступу трафіку тільки з внутрішньої мережі.

Застосувати ACL для інтерфейсу F0/1 для вхідного трафіку.

Створити нумерований IP ACL 120.

Дозволити будь-який зовнішній вузол для **DNS, SMTP, TFTP (для парного варіанту)**, та **FTP, IMAP, SNMP** (**для непарного варіанту**) сервісів на сервері PC-A, заборонити будь-який зовнішній доступ до служби HTTPS на PC-A, і дозволити PC-C доступ до R1 через SSH.

Перевірити, що PC-C може отримати доступ до PC-A через HTTPS, використовуючи веб-браузер. Переконатися, що відключили HTTP і включили HTTPS на PC-A сервері.

Налаштувати ACL 120, на дозвіл і заборону зазначеного трафіку.

Застосувати ACL до інтерфейсу S0/0/0 для вхідного трафіку.

Перевірити, що PC-C не зможе отримати доступ до PC-A через HTTP, використовуючи веб-браузер.

Вимоги до оформлення звіту

Звіт має включати: титульний аркуш, індивідуальне завдання на лабораторну роботу, хід роботи та висновки. Необхідно зробити скріншот створеної топології мережі, навести опис всіх введених команд для налаштування списків контролю доступу на маршрутизаторах.

Питання до лабораторної роботи

1. Яке призначення ACL? Які є типи ACL?
2. Які є правила налаштування ACL?
3. Яке призначення простих і розширених ACL?
4. Які ви знаєте команди ACL?
5. Яке призначення SSH?
6. Які правила налаштування SSH? Як налаштувати маршрутизатор лише на SSH з'єднання?
7. Як заборонити/дозволити вхідний/вихідний трафік на/з маршрутизатора?
8. Як заборонити первний тип трафіку на деякий вузол мережі?

Рекомендована література

1. CNA R&S // Електронний ресурс. Режим доступу: http://static-course-assets.s3.amazonaws.com
2. МСІТСМ – 2. Методи та засоби автоматизованого моделювання та проектування комп'ютерних мереж. Методичні вказівки до виконання лабораторних робіт. [Електронне видання] / Уклад.: Я.Ю. Дорогий, М.М. Букасов. – К.: НТУУ «КПІ», 2012. – 76 с.
2. Access Control List // Електронний ресурс. Режим доступу: https://habrahabr.ru/post/147996/
3. Стандартні та розширені ACL // Електронний ресурс. Режим доступу: http://xgu.ru/wiki/Cisco_ACL
4. Configuring IP Access Lists // Електронний ресурс. Режим доступу: http://www.cisco.com/c/ru_ru/support/docs/security/ios-firewall/23602-confaccesslists.html

ЛАБОРАТОРНА РОБОТА № 9. НАЛАШТУВАННЯ NAT

Мета роботи: навчитися виконувати налаштування NAT, а також NAT-пула з перевантаженням на маршрутизаторі з метою скорочення кількості публічних IP -адрес, які використовує організація або компанія.

Теоретичні відомості

Перетворення мережевих адрес NAT (Network Address Translation) – це процес, при якому мережевий пристрій (маршрутизатор) призначає публічну адресу вузловим пристроям в межах приватної мережі.

NAT використовують для того, щоб скоротити кількість публічних IP -адрес, що використовує організація, оскільки кількість доступних публічних IPv4 -адрес обмежене. NAT використовують в мережі: при нестачі публічних IP -адрес, для економії на купівлі публічних адрес від інтернет-провайдера. Крім того, в цілях безпеки NAT може закрити внутрішні адреси від зовнішніх мереж.

NAT має обмеження: для процесу NAT потрібна інформація про IP -адресу і номер порту в заголовках пакетів IP і TCP, призначених для перетворення. Також є протоколи, які не можна використовувати з NAT: SNMP, LDAP, Kerberos версії 5.

Метод динамічного перетворення мережевих адрес (динамічний NAT) використовує пул публічних адрес, які привласнюються в порядку живої черги. Коли внутрішній устрій просить доступ до зовнішньої мережі, динамічний NAT привласнює доступний публічний IPv4 -адрес з пулу. Динамічний NAT є зіставленням адрес за схемою "багато до багатьох" між локальними і глобальними адресами.

Вказівки щодо виконання завдання

Розгянемо сценарій 1, згідно якого інтернет-провайдер (Internet Service Provider, ISP) виділив для компанії простір публічних IP -адрес 209.165.200.224/27. В результаті компанія отримала 30 публічних IP -адрес. Адреси від 209.165.200.225 до 209.165.200.241 підлягають статичному розподілу, а адреси від 209.165.200.242 до 209.165.200.254 - динамічному розподілу. Статичним маршрутом є шлях від інтернет-провайдера до шлюзового маршрутизатора, тоді як маршрут за замовчуванням представлений в якості шляху від шлюзу до маршрутизатора інтернет-провайдера. Підключення інтернет-провайдера до Інтернету змодельоване loopback -адресою на маршрутизаторі інтернет-провайдера (рис.9.1).

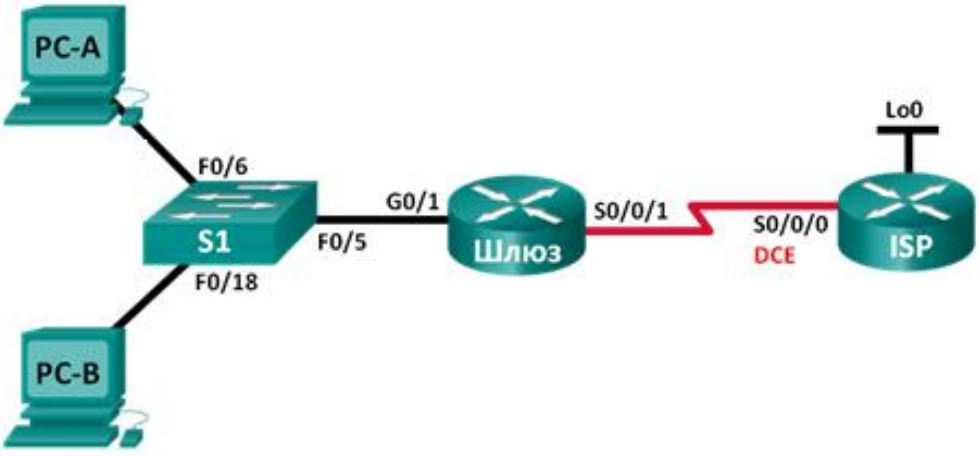


Рис.9.1. Топологія мережі з двома вузлами PC-A та PC-B, які використовують послуги інтернет-провайдера

Таблиця адресації

Пристрій	Інтерфейс	IP -адреса	Маска підмережі	Шлюз за замовчуванням
Шлюз	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
Інтернет-провайдер	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A (змодельований сервер)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC - B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Нехай у компанії використовуються наступні ресурси:

- 2 маршрутизатори (Cisco 1941 під управлінням ОС Cisco IOS 15.2(4) M3 (образ universal) або аналогічна модель);
- 1 комутатор (Cisco 2960 під управлінням ОС Cisco IOS 15.0(2), образ lanbasek9 або аналогічна модель);
- 2 ПК (під управлінням ОС Windows 7, Vista або XP з програмою емуляції терміналу, наприклад Tera Term);
- консольні кабелі для налаштування пристроїв Cisco IOS через консольні порти;
- кабелі Ethernet і послідовні кабелі відповідно до топології.

Побудова мережі та перевірка підключення

Спочатку необхідно виконати базові налаштування пристроїв, IP -адрес інтерфейсів, статичної маршрутизації, доступу до пристроїв. Необхідно підключити пристрої відповідно до топології і провести необхідні кабелі, налаштувати вузли ПК та мережеві пристрої, виконати ініціалізацію і перезавантаження маршрутизатора і комутаторів.

Створення моделі веб-сервера для інтернет-провайдера

Створимо локального користувача під ім'ям **webuser** із зашифрованим паролем **webpass**:

ISP(config)# username webuser privilege 15 secret webpass

Включимо службу HTTP -сервера на маршрутизаторі інтернет-провайдера:

ISP(config)# ip http server

Налаштуємо сервіс HTTP так, щоб він використовував локальну базу даних:

ISP(config)# ip http authentication local

Налаштування статичної маршрутизації

Створимо статичний маршрут від маршрутизатора інтернет-провайдера до маршрутизатора шлюзу, використовуючи діапазон призначених публічних мережевих адрес 209.165.200.224/27:

ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18

Створимо маршрут за замовчуванням від маршрутизатора Gateway до маршрутизатора ISP:

Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17

Перевірка мережевого з'єднання

З вузлів ПК необхідно відправити ехо-запити на інтерфейс G0/1 на шлюзовому маршрутизаторі. Необхідно відобразити таблиці маршрутизації на обох маршрутизаторах, щоб переконатися, що статичні маршрути містяться в таблиці маршрутизації і правильно налагоджені на обох маршрутизаторах.

Налаштування і перевірка статичного перетворення NAT

Статичний NAT використовує зіставлення локальних і глобальних адрес за схемою "один до одного". Метод статичного перетворення мережевих адрес особливо корисний для веб-серверів або пристроїв, які повинні мати постійну адресу, доступну з Інтернету, - наприклад, для веб-сервера компанії.

Налаштування статичного зіставлення

Налагоджена статична прив'язка дозволяє маршрутизатору здійснювати трансляцію адрес між приватною внутрішньою адресою сервера 192.168.1.20 і публічною адресою 209.165.200.225. Завдяки цьому користувач може дістати доступ до комп'ютера PC-A через Інтернет. Комп'ютер PC-A моделює сервер або пристрій з постійною адресою, до якої можна дістати доступ через Інтернет:

Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225

Задання інтерфейсів

Виконаємо команди **ip nat inside** та **ip nat outside** на інтерфейсах:

Gateway(config)# interface g0/1
Gateway(config - if)# ip nat inside
Gateway(config - if)# interface s0/0/1
Gateway(config - if)# ip nat outside

Перевірка конфігурації

Відобразимо таблицю статичних перетворень NAT за допомогою команди show ip nat translations.

Gateway# show ip nat translations

Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---

Отже, внутрішня адреса локального вузла 192.168.1.20 була перетворена в адресу 209.165.200.225 маршрутизатором з пулу NAT.

На шлюзовому маршрутизаторі (Gateway) відобразимо таблицю NAT.

Gateway# show ip nat translations

Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1
--- 209.165.200.225 192.168.1.20 --- ---

Коли комп'ютер PC-A відправив ICMP-запит на адресу інтернет-провайдера 192.31.7.1, в таблицю був доданий запис NAT, де ICMP вказаний у вигляді протоколу.

Оскільки статичний NAT налагоджений для комп'ютера PC-A, необхідно переконатися в успішній відправці ехо-запиту від інтернет-провайдера на комп'ютер PC-A з публічною NAT -адресою (209.165.200.225).

На шлюзовому маршрутизаторі (Gateway) відобразимо таблицю NAT, щоб перевірити перетворення:

Gateway# show ip nat translations

Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:12 192.168.1.20:12 209.165.201.17:12 209.165.201.17:12
--- 209.165.200.225 192.168.1.20 --- ---

Зверніть увагу, що зовнішня локальна і зовнішня глобальна адреси співпадають. Ця адреса - адреса джерела віддаленої мережі інтернет-провайдера. Для успішної відправки

ехо-запиту від інтернет-провайдера, внутрішня глобальна статична NAT -адреса 209.165.200.225 була перетворена у внутрішню локальну адресу комп'ютера PC-A. (192.168.1.20).

Перевіримо статистику NAT, виконавши команду **show ip nat statistics** на шлюзовому маршрутизаторі (Gateway).

Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39 Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets : 0

Налаштування і перевірка динамічного перетворення NAT

Очищення даних NAT

Перед додаванням динамічних перетворень очистимо усі NAT і видалимо статистику:
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics

Створення ACL -списку, який відповідає діапазону приватних IP -адрес

локальної мережі

Для трансляції адрес з мережі 192.168.1.0/24 використовується ACL1:
Gateway(config)# access - list 1 permit 192.168.1.0 0.0.0.255

Переконаємося, що конфігурації інтерфейсу NAT все ще дійсні:

Щоб перевірити конфігурації NAT, на маршрутизаторі Gateway виконаємо команду **show ip nat statistics**:

Gateway# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
Serial0/0/1
Inside interfaces:
FastEthernet0/1
Hits: 0 Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets : 0

Визначимо пул придатних до використання публічних IP –адрес:

Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224

Визначимо відповідність в NAT внутрішнього списку адрес джерела і пулу зовнішніх адрес:

Gateway(config)# ip nat inside source list 1 pool public_access

Примітка. Імена пулу NAT чутливі до регістра, а ім'я пулу, що вводиться тут, повинне співпадати з ім'ям, використаним на попередньому кроці.

Перевірка конфігурації

З комп'ютера PC-B відправимо ехо-запит на інтерфейс Lo0 (192.31.7.1) інтернет-провайдера. Якщо ехо-запит пройшов невдало, необхідно знайти і усунути проблеми. На шлюзовому маршрутизаторі (Gateway) відобразимо таблицю NAT:

Gateway# show ip nat translations

```
Pro Inside global     Inside local       Outside local      Outside global
--- 209.165.200.225   192.168.1.20       ---                ---
icmp 209.165.200.242:1 192.168.1.21:1    192.31.7.1:1       192.31.7.1:1
--- 209.165.200.242   192.168.1.21       ---                ---
```

Тобто внутрішня адреса локального вузла для комп'ютера PC-B 192.168.1.21 перетворена в адресу 209.165.200.242.

У комп'ютері PC-B відкриємо веб-браузер і введемо IP -адресу змодельованого веб-сервера інтернет-провайдера (інтерфейс Lo0). При запиті увійдемо до системи під ім'ям **webuser** і з паролем **webpass**.

Відобразимо таблицю NAT:

```
Pro     Inside global       Inside local        Outside local      Outside global
--- 209.165.200.225     192.168.1.20       ---                ---
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80      192.31.7.1:80
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80      192.31.7.1:80
--- 209.165.200.242     192.168.1.22       ---                ---
```

У нашому випадку для цього перетворення використовується протокол TCP, номери використовуваних портів: внутрішній: від 1038 до 1052, зовнішній: 80 (сервіс http).

Перевіримо статистику NAT, виконавши команду **show ip nat statistics** на шлюзовому маршрутизаторі (Gateway):

Gateway# show ip nat statistics

```
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345  Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
```

-- -- Inside Source
[Id: 1] access - list 1 pool public_access refcount 2
pool public_access: netmask 255.255.255.224
start 209.165.200.242 end 209.165.200.254
type generic, total addresses 13, allocated 1 (7%), misses 0
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets : 0

Видалимо статичний NAT. При запиті про видалення дочірніх записів введемо **yes**.

Gateway(config)# no ip nat inside source static 192.168.1.20 209.165.200.225
Static entry in use, do you want to delete child entries? [no]: **yes**

Відобразимо таблицю і статистику NAT.

Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
Serial0/0/1
Inside interfaces:
GigabitEthernet0/1
Hits: 16 Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- -- Inside Source
[Id: 1] access - list 1 pool public_access refcount 4
pool public_access: netmask 255.255.255.224
start 209.165.200.242 end 209.165.200.254
type generic, total addresses 13, allocated 2 (15%), misses 0
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets : 0

Gateway# show ip nat translation

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.243:512	192.168.1.20:512	192.31.7.1:512	192.31.7.1:512
---	209.165.200.243	192.168.1.20	---	---
icmp	209.165.200.242:512	192.168.1.21:512	192.31.7.1:512	192.31.7.1:512
---	209.165.200.242	192.168.1.21	---	---

Налаштування NAT -пула з перевантаженням

За сценарієм 2 інтернет-провайдер виділив компанії діапазон публічних IP -адрес 209.165.200.224/29. Завдяки цьому компанія отримала шість публічних IP -адрес. Перевантаження пулу динамічного NAT використовує пул IP -адрес згідно моделі "багато до багатьох". Маршрутизатор використовує першу IP -адресу в пулі і призначає підключення за допомогою IP -адреси і унікального номера порту. Після досягнення на маршрутизаторі максимальної кількості перетворень для однієї IP -адреси (для платформи і устаткування), використовується наступна IP -адреса в пулі.

Нехай інтернет-провайдер виділив вашій компанії одну IP -адресу, 209.165.201.18, для підключення до Інтернету від маршрутизатора Gateway до мережі інтернет-провайдера (рис.9.2). Для перетворення декількох внутрішніх адрес в одну придатну для використання публічну адресу необхідно використати перетворення адрес портів (PAT).

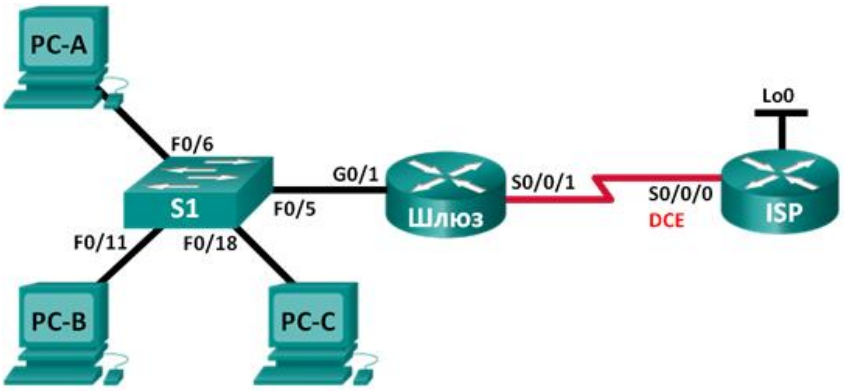


Рис.9.2. Топологія мережі з трьома вузлами

Таблиця адресації

Пристрій	Інтерфейс	IP -адреса	Маска підмережі	Шлюз за замовчуванням
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC - A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC - B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC - C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

Нехай використовуються наступні ресурси:

- 2 маршрутизатори (Cisco 1941 під управлінням ОС Cisco IOS 15.2(4) M3 (образ universal) або аналогічна модель);
- 1 комутатор (Cisco 2960 під управлінням ОС Cisco IOS 15.0(2), образ lanbasek9 або аналогічна модель);
- 3 комп'ютери (під управлінням Windows 7, Vista або XP з програмою емуляції терміналу, наприклад Tera Term);
- консольні кабелі для налаштування пристроїв Cisco IOS через консольні порти;
- кабелі Ethernet і послідовні кабелі відповідно до топології.

Налаштування статичної маршрутизації

Створимо статичний маршрут від інтернет-провайдера до маршрутизатора Gateway:

ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18

Створимо маршрут за замовчуванням від маршрутизатора Gateway до маршрутизатора ISP:

Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17

Перевірка мережевого з'єднання

З вузлів ПК необхідно відправити ехо-запити на інтерфейс G0/1 на шлюзовому маршрутизаторі та виявити і усунути неполадки, якщо ехо-запит не проходить.

Налаштування і перевірка NAT -пула с перевантаженням

Необхідно налаштувати маршрутизатор Gateway для перетворення IP -адреси з мережі 192.168.1.0/24 в одну з шести придатних до використання адрес в діапазоні 209.165.200.224/29.

Створення ACL -списку, який відповідає діапазону приватних IP -адрес локальної мережі

Для трансляції адрес з мережі 192.168.1.0/24 використаємо ACL1:

Gateway(config)# access - list 1 permit 192.168.1.0 0.0.0.255

Визначення пулу придатних до використання публічних IP -адрес

Gateway(config)# ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248

Визначимо відповідність в NAT внутрішнього списку адрес джерела і пулу зовнішніх адрес:

Gateway(config)# ip nat inside source list 1 pool public_access overload

Виконаємо команди **ip nat inside** та **ip nat outside** на інтерфейсах:

Gateway(config)# interface g0/1
Gateway(config - if)# ip nat inside
Gateway(config - if)# interface s0/0/1
Gateway(config - if)# ip nat outside

Перевірка конфігурації NAT -пула з перевантаженням

З кожного ПК відправимо ехо-запит на адресу маршрутизатора інтернет-провайдера 192.31.7.1.

Відобразимо статистику NAT по маршрутизатору Gateway:

Gateway# show ip nat statistics

```
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:25 ago
Outside interfaces:
   Serial0/0/1
Inside interfaces:
   GigabitEthernet0/1
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- -- Inside Source
[Id: 1] access - list 1 pool public_access refcount 3
  pool public_access: netmask 255.255.255.248
  start 209.165.200.225 end 209.165.200.230
  type generic, total addresses 6, allocated 1 (16%), misses 0
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets : 0
```

Відобразимо перетворення NAT на маршрутизаторі Gateway:

Gateway# show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:0	192.168.1.20:1	192.31.7.1:1	192.31.7.1:0
icmp	209.165.200.225:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp	209.165.200.225:2	192.168.1.22:1	192.31.7.1:1	192.31.7.1:2

У даному випадку вказано 3 внутрішні локальні IP –адреси у вихідних даних, вказано 1 внутрішню глобальну IP –адресу, використовується 3 номери портів в парі з внутрішніми глобальними адресами. У результаті відправки ехо-запиту на внутрішню локальну адресу комп'ютера PC-A від маршрутизатора інтернет-провайдера ехо-запит буде невдалим,

оскільки маршрутизатор знає розташування внутрішньої глобальної адреси у своїй таблиці маршрутизації, але внутрішня локальна адреса не оголошена.

Налаштування та перевірка перетворення PAT

Налаштуємо PAT, використовуючи інтерфейс для визначення зовнішніх адрес замість пулу адрес.

Видалимо пул придатних до використання публічних IP-адрес:

Gateway(config)# no ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248

Видалимо NAT трансляцію між ACL -списком і пулом зовнішніх адрес:

Gateway(config)# no ip nat inside source list 1 pool public_access overload

Зіставимо список джерела із зовнішнім інтерфейсом:

Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload

Перевірка конфігурації PAT

З кожного ПК відправимо ехо-запит на адресу маршрутизатора інтернет-провайдера - 192.31.7.1. Відобразимо статистику NAT по маршрутизатору Gateway:

Gateway# show ip nat statistics

```
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:19 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- -- Inside Source
[Id: 2] access - list 1 interface Serial0/0/1 refcount 3
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets : 0
```

Відобразимо перетворення NAT на Gateway:

Gateway# show ip nat translations

```
Pro Inside global     Inside local       Outside local      Outside global
icmp 209.165.201.18:3 192.168.1.20:1     192.31.7.1:1       192.31.7.1:3
icmp 209.165.201.18:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
icmp 209.165.201.18:4 192.168.1.22:1     192.31.7.1:1       192.31.7.1:4
```

Завдання до лабораторної роботи

1. У середовищі моделювання Packet Tracer створити модель мережі (рис.9.1) згідно сценарію 1 лабораторної роботи. Побудувати мережу та виконати підключення. Створити модель веб-сервера для інтернет-провайдера. Налаштувати статичний маршрут від маршрутизатора інтернет-провайдера до маршрутизатора шлюзу, використовуючи діапазон призначених публічних мережевих адрес 209.165.200.224/27. Перевірити мережеве з'єднання, налаштувати статичне перетворення NAT для трансляції адрес між приватною внутрішньою адресою сервера 192.168.1.20 і публічною адресою 209.165.200.225.

2. Згідно сценарію 1 лабораторної роботи налаштувати і перевірити динамічне перетворення NAT. Створити ACL -список, який відповідає діапазону приватних IP -адрес локальної мережі для трансляції адрес з мережі 192.168.1.0/24. У комп'ютері PC-B відкрити веб-браузер і ввести IP -адресу змодельованого веб-сервера інтернет-провайдера (інтерфейс Lo0). При запиті увійти до системи під ім'ям **webuser** і з паролем **webpass.** Відобразити таблицю NAT. Перевірити статистику NAT на шлюзовому маршрутизаторі (Gateway). Видалити статичний NAT.

3. У середовищі моделювання Packet Tracer створити модель мережі (рис.9.2) згідно сценарію 2 лабораторної роботи. Побудувати мережу та виконати підключення. Створити статичний маршрут від інтернет-провайдера до маршрутизатора Gateway. Перевірити мережеве з'єднання. Налаштувати маршрутизатор Gateway для перетворення IP -адреси з мережі 192.168.1.0/24 в одну з шести придатних до використання адрес в діапазоні 209.165.200.224/29. Створити ACL -список, який відповідає діапазону приватних IP -адрес локальної мережі для трансляції адрес з мережі 192.168.1.0/24. Визначити відповідність в NAT внутрішнього списку адрес джерела і пулу зовнішніх адрес. Перевірити конфігурацію NAT-пула з перевантаженням. Відобразити статистику NAT по маршрутизатору Gateway. Налаштувати та перевірити конфігурацію PAT.

Вимоги до оформлення звіту

Звіт має включати: титульний аркуш, індивідуальне завдання на лабораторну роботу, хід роботи та висновки. Необхідно зробити скріншот створеної топології мережі, навести опис всіх введених команд для налаштування NAT на маршрутизаторах.

Питання до лабораторної роботи

1. У чому полягає технологія NAT?
2. Чому існує потреба використовувати технологію NAT в мережі?
3. У чому полягають переваги статичного NAT?
4. У чому полягають переваги PAT?
5. Які особливості налаштування NAT на маршрутизаторі?
6. Як перевірити поточну конфігурацію NAT?
7. Які обмеження NAT?

Рекомендована література

1. CNA R&S // Електронний ресурс. Режим доступу: http://static-course-assets.s3.amazonaws.com

2. МСІТСМ – 2. Методи та засоби автоматизованого моделювання та проектування комп’ютерних мереж. Методичні вказівки до виконання лабораторних робіт. [Електронне видання] / Уклад.: Я.Ю. Дорогий, М.М. Букасов. – К.: НТУУ «КПІ», 2012. – 76 с.

3. What is Network Address Translation? // Електронний ресурс. Режим доступу: http://whatismyipaddress.com/nat

4. NAT // Електронний ресурс. Режим доступу: https://neerc.ifmo.ru/wiki/index.php?title=NAT

5. Peer-to-Peer Communication Across Network Address Translators // Електронний ресурс. Режим доступу: http://www.brynosaurus.com/pub/net/p2pnat/

6. NAT // Електронний ресурс. Режим доступу: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat.html

7. PAT // Електронний ресурс. Режим доступу: https://uk.wikipedia.org/wiki/PAT

NAT and PAT - What's the Difference? // Електронний ресурс. Режим доступу: http://blog.boson.com/bid/53313/NAT-and-PAT-What-s-the-Difference