Міністерство освіти і науки України
Чернівецький національний університет
імені Юрія Федьковича

Л. І. Д’яченко

ОРГАНІЗАЦІЯ КОМП’ЮТЕРНИХ МЕРЕЖ

Навчально-методичний посібник з лабораторних робіт

(видання електронне)

Чернівці
Чернівецький національний університет

2022

УДК 004.42(078)
Д675

Друкується за ухвалою
Вченої ради навчально-наукового інституту фізико-технічних та комп’ютерних наук
Чернівецького національного університету
імені Юрія Федьковича
Протокол № 8 від 22.09.2022 р.

Д’яченко Л.І.
Д675 Організація комп’ютерних мереж: навч.-метод. посіб. лаб. роб. / Л. І. Д’яченко. – Чернівці: Чернівецький нац. ун-т, 2022. – 49 с.

Навчально-методичний посібник з лабораторних робіт містить теоретичні матеріали та покрокові завдання, що мають за мету навчити студентів розпізнавати базові структурні елементи мережі, проводити базове налаштування підключення робочих станцій до мережі, розуміти базові принципи IP адресації та створення підмереж.

Для студентів вищих навчальних закладів, які навчаються за спеціальностями 121 - Інженерія програмного забезпечення, 122 – Комп’ютерні науки та суміжними.

УДК 004.42(078)

ЗМІСТ

ВСТУП

Розвиток локальних комп'ютерних мереж для об'єднання комп'ютерів починався з використанням найрізноманітніших не стандартизованих пристроїв і програмного забезпечення. Створення мережі в цей час вимагало від розробників великих зусиль і винахідливості. В середині 80-х років ситуація почала кардинально змінюватися в сторону створення стандартних технологій об'єднання комп'ютерів в єдину мережу. Були розроблені спеціальні методи і правила обміну інформацією між комп'ютерами, серед яких найбільш відомими стали стандарти Ethernet, Token Ring, FDDI, Arcnet. У зазначених стандартах були строго регламентовані довжина, вид і порядок проходження кодів, що посилаються комп'ютерами в мережу, правила доступу до мережі окремими комп'ютерами і т.д. Крім цього в цей час інтенсивно почали використовуватися певні протоколи, які дозволяли проводити налаштування додаткових функцій мережі, наприклад протокол STP. Розроблені стандартні мережеві технології, а так само використання персональних комп'ютерів значно спростили процес створення комп'ютерних мереж. З'явилася можливість швидкого доступу до поділюваних обчислювальних ресурсів, до бази даних відразу декількома користувачами, причому користувач використовував на своєму мережевому комп'ютері ті ж знайомі команди, як і при роботі з окремим комп'ютером. Завдання обробки цих команд і розподілу завдань між окремими комп'ютерами взяла на себе мережева операційна система.

Лабораторних практикум складається з восьми лабораторних робіт, які охоплюють налаштування базового підключення комп’ютера до локальної мережі, протоколу STP, визначення кількості доменів колізій та широкомовних доменів, розрахунок адрес мережі та підмережі, знайомство з особливостями IP адресації та розробку топології та адресної схеми локальної мережі.

ЛАБОРАТОРНА РОБОТА №1

ПОБУДОВА МЕРЕЖІ ЕОМ ЛОКАЛЬНОЇ НА ОСНОВІ ТЕХНОЛОГІЇ 100BASE-TX ТА ПРОТОКОЛЬНОГО СТЕКУ TCP/IP

Мета:

- вивчити призначення, склад, основні технічні характеристики апаратних засобів та особливості побудови мережі ЕОМ локальної з двох абонентських станцій за технологією 100Base-TX;
- навчитися користуватися обжимним інструментом і тестером Fluke;

Обладнання:

- дві робочі станції з встановленими мережевими адаптерами Fast Ethernet;
- кабель UTP 5-ї категорії;
- два конектори RJ-45;
- обжимний інструмент і тестер Fluke.

Завдання:

1. Отримати допуск до виконання лабораторної роботи, давши відповідь на питання для підготовки.
2. За допомогою обжимного інструменту виготовити cross-over кабель та перевірити працездатність кабеля за допомогою тестера Fluke;
3. Підключити cross-over-ний кабель до мережевих адаптерів;
4. Настроїти протокол TCP/IP за допомогою методичних вказівок;
5. За допомогою утиліти PING перевірити мережеве з'єднання;
6. Відповісти на контрольні запитання у письмовому иигляді;
7. Оформити звіт за результатами виконання лабораторної роботи.

Література:

1. В.Г.Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологии, протоколы. - Спб, изд. Питер, 2000 г.
2. Оглтри, Терри. Модернизация и ремонт сетей, 2-е изд.-.М: Изд. дом. „Вильямс",2000 г.
3. А.В. Фролов, Г.В. Фролов. Локальные сети персональных компьютеров. М.:ДиалогМИФИ, 1993.

Питання для підготовки.

1. Чим відрізняються кабелі 5-ї, 5е, 6-ї та 7-ї категорії між собою?
2. Чим відрізняються між собою кабеля UTP, STP, S-STP?
3. Які перешкоди можуть впливати на середовища передачі даних на мідній основі у процесі їх роботи? Які ви знаєте способи уникнення або зменшення впливу цих перешкод?
4. Опишіть принцип роботи оптоволоконного кабеля. Що таке мода та числова апертура?

5. Чому для забезпечення повнодуплексного режиму роботи оптоволоконного кабеля необхідна наявність двох окремих волокон?

МЕТОДИЧНІ ВКАЗІВКИ

1. Неекранована вита пара (Unshielded Twisted Pair) UTP.

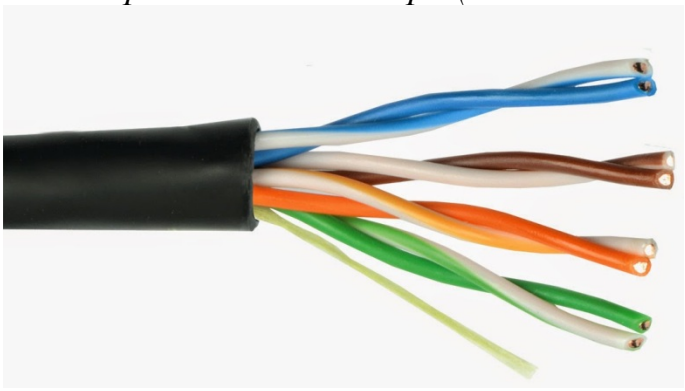


Рис. 1.1. Неекранована вита пара UTP

Кабель "Twisted Pair" - "Вита пара", складається з пар проводів, закручених один навколо одного й одночасно закручених навколо інших пар, у межах однієї оболонки. Кожна пара складається з проводу, який називається "Ring" і проводу "Tip" (назви прийшли з телефонії).

Зовнішній вигляд витої пари показаний на рис. 1.1

Кожна пара в оболонці має свій номер, таким чином, кожен провід можна ідентифікувати як Ringl, Tipl, Ring2, Tip2, …

Додатково до нумерації проводів кожна пара має свою унікальну кольорову схему:

- Синій і білий із синіми смужками для 1-ої пари (Ring1, Tip1);
- Оранжевий і білий з оранжевими смужками - для 2-ої пари;
- Зелений і білий із зеленими смужкамп - для 3-ої пари;
- Коричневий і білий з коричневими смужками - для 4-ої пари.

Для кожної пари проводів Ring-провід зафарбований в основний колір, а Tip-провід - білий із смужками основного кольору. Наприклад, для пари 1: Ring1-провід буде синій, а Tip 1-провід - білий із синіми смужками.

Для позначення діаметра проводу часто застосовується американська міра - AWG (American Wire Gauge) (gauge-калібр, діаметр). Нормальний провід для використання в 10Base-T відповідає 22 або 24 AWG. Причому чим менше діаметр проводу, тим більша ця величина.

Відповідно до стандартів, кабель поділяється на кілька категорій :

ANSI/EIA/TIA-568, ISO/IEC 1 1801

Тип кабелю	Область застосування
Category 1 (Cat.l)	Використовується для телефонних комунікацій і не підходить для передачі даних
Cat. 2	Використовується для передачі даних зі швидкістю до 4 М біт/с (Mbps) включно
Cat.3	Використовується для передачі даних зі швидкістю до 10Мбіт/с

	включно. Використовується в мережах 10base-T
Cat. 4	Використовується для передачі даних зі швидкістю до 16Мбіт/с включно. Використовується в мережах Token Ring
Cat. 5	Використовується для передачі даних зі швидкістю до 100Мбіт/с включно. Використовується в мережах 100base-TX і інших в яких вимагається подібна швидкість.

Також існують кабелі категорій 5e, 6 та 7, які докладно описані у відповідній літературі. Використання кабелів 5 категорії і категорії 5e регламентовано на діапазон частот від 1 до 100 МГц, але при цьому кожен виробник тестує своє устаткування на більш широкому діапазоні частот(до 350 Мгц). Таку можливість дає сучасне вимірювальне устаткування. Характеристики і, як наслідок, надійність кабеля категорії 5e значно більші в порівнянні з кабелем категорії 5 (сама назва 5e - від слова розширена Expanded).

5 червня 2002 року Комітет електропровідних кабельних систем TIA TR-42.7 Асоціації телекомунікаційної промисловості (TIA) одноголосне затвердив стандарт категорії 6. Доповнення до стандарту ANSI/TIA/EJA-568-B.2-1, що .визначає параметри симетричних кабелів із хвильовим опором 100 Ом у діапазоні частот 250 Мгц, було опубліковано 20 червня 2002 року. Документ включає специфікацію ліній, каналів, роз'єднань, вимоги і процедури вимірів. Визначено допустимі погрішності і заходи для досягнення стабільності результатів. Це повинно забезпечити надійність установлених систем. Стандарт категорії 6 включає:

- специфікацію системи, включаючи параметри комплектуючих, каналів, стаціонарних ліній і гнучких кабелів;
- розширення смуги до 200 Мгц (у два рази в порівнянні з категорією 5e);
- специфікацію комплектуючих до частоти 250 Мгц.

UTP кабель 7-ої категорії має параметри кабелів, роз’ємів, лінії і каналу, визначені до частоти 600 Мгц.

2. Роз'єми для витої пари (восьмиконтактпий з'єднувач RJ-45)

Вилка RJ-45 схожа на вилку від сучасних телефонів, тільки вона трохи більшого розміру і має вісім контактів.

1- контакти 8шт.
2- фіксатор роз’єма
3- фіксатор кабеля

В процесі обжиму контакти будуть утоплені всередину корпусу, проріжуть ізоляцію (2) провода і втиснуться в жилу (1).

Вилки поділяються на екрановані і неекрановані, із вставкою і без, для круглого і для плоского кабелю, для одножильного і для багатожильного кабелю, із двома і з трьома зубцями.

Корисно разом з вилкою на кабель установлювати захисний ковпачок.

3. Монтаж вилки RJ-45 на кабель.

Для монтажу найкраще всього користуватися спеціальним обжимним інструментом, який дозволяє обрізати кабель, знімати зовнішню ізоляцію і обжимати вилку RJ-45.

Рис. 1.2. Обжимний інструмент

Зовнішній вигляд обжимного інструменту показаний на рис. 1.2.

Для створення прямого (straight) кабеля, виту пару обжимають однаково з обох кінців за стандартом EIA/TIA-568A або EIA/TIA-568B. Вибір варіанта обжиму 568A чи 568B залежить винятково від прийнятого у мережі стандарту. Прямий кабель використовується для з’єднання різнотипних пристроїв – наприклад, комп’ютера з комутатором або концентратором.

Для з'єднання двох комп'ютерів без додаткового активного обладнання, з використанням тільки адаптерів мережного інтерфейсу (NIC), а також для з'єднання концентраторів використовується кабель, який має назву cross-over. Для його створення слід обжати кінці кабеля за різними стандартами.

Для виготовлення Cross-over-ного кабеля необхідно виконати наступні дії:

1. Зніміть зовнішню ізоляцію кабеля на довжину 12.5 мм (1/2 дюйма). В обжимному інструменті є спеціальний ніж і обмежувач для цієї операції. Проводи зачищати не потрібно.

2. Розплетіть кабель з однієї сторони і розташуйте проводи у відповідності зі схемою 568A, при чому довжина розплетення не повинна перевищувати 12,5 мм.

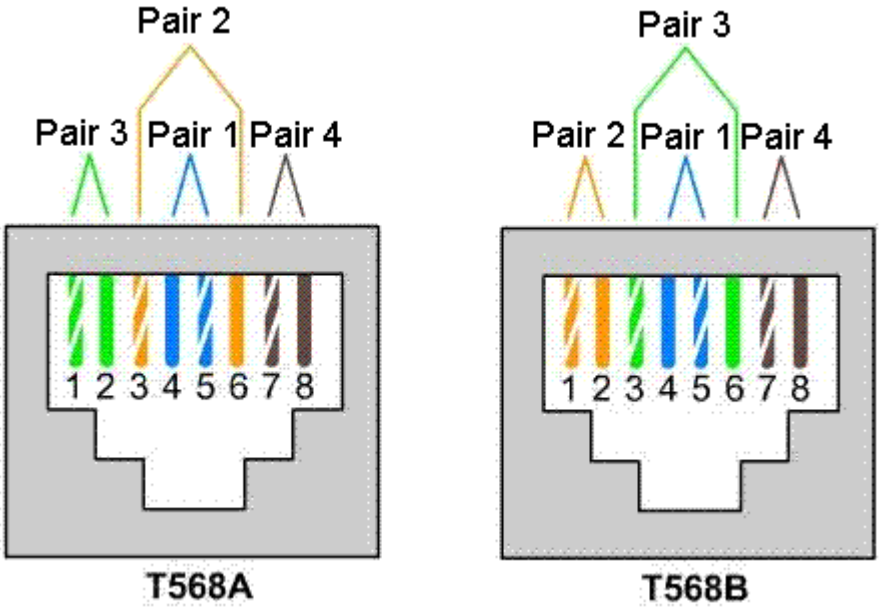


Рис. 1.3. Кольорові схеми 568 А та 568 В

3. Розплетіть кабель з іншої сторони і розташуйте провода у відповідності зі схемою 568В.

4. Поверніть вилку контактами до себе, як на першому малюнку, і акуратно насуньте на кабель до упора, щоб проводи пройшли під контактами. Результат цієї операції зображений на другому малюнку.

5. Обіжміть вилку. На обжимному інструменті є спеціальне гніздо, в яке вставляється вилка з проводами і натискуванням на ручки інструмента обжимається.

6. При цьому контакти будуть утоплені всередину і проріжуть ізоляцію проводів. Фіксатор проводу також повинен бути утопленим в корпус.

7. Результатом пророблених дій буде cross-over-ний кабель.

8. Перевірка кабелю тестером Fluke полягає в наступному. Необхідно вставити обидва кінця обжатого кабелю в два гнізда, які присутні на тестері. Натиснути кнопку ON, і на екрані тестера подивитись результат. Якщо все зроблено правильно, то на екрані можна буде побачити 2 лінії, що перетинаються (кабель cross-over-ний) та довжину кабелю.

Контрольні питання

1. Яке основне призначення мережного адаптера? Яким чином від взаємодіє із материнською платою і середовищем передачі даних?
2. В чому основна відмінність між концентратором та повторювачем? Де необхідне використання одних та інших?
3. Які пари проводів з 4-х використовуються у кабелі UTP cat.5 в технології 100Base-Tx? Які з проводів приймають інформацію, а які передають?
4. Чому в cross-over-ному кабелі необхідно використовувати різні стандарти на кінцях при обжимці? Де необхідне використання цього кабелю?

ЛАБОРАТОРНА РОБОТА № 2

ЗНАЙОМСТВО З СЕРЕДОВИЩЕМ МОДЕЛЮВАННЯ

CISCO PACKET TRACER

Мета:

- вивчити призначення, основні компоненти, інтерфейс та можливості середовища моделювання Cisco Packet Tracer

Теоретична частина

Cisco Packet Tracer це потужна програма для емуляції роботи мережі, яка дозволяє студентам експериментувати з поведінкою мережі та відповідати на питання «А що як?» Packet Tracer дозволяє проводити емуляцію, візуалізацію, демонстрацію та вивчення складних мережних комплексів. Ця програма дозволяє замінити фізичне обладнання та дозволяє студентам створювати мережі з практично необмеженою кількістю пристроїв. Студенти можуть будувати, конфігурувати та проводити діагностику мережних проблем, використовуючи віртуальне обладнання та середовища передачі даних, самостійно або в кооперації з колегами.

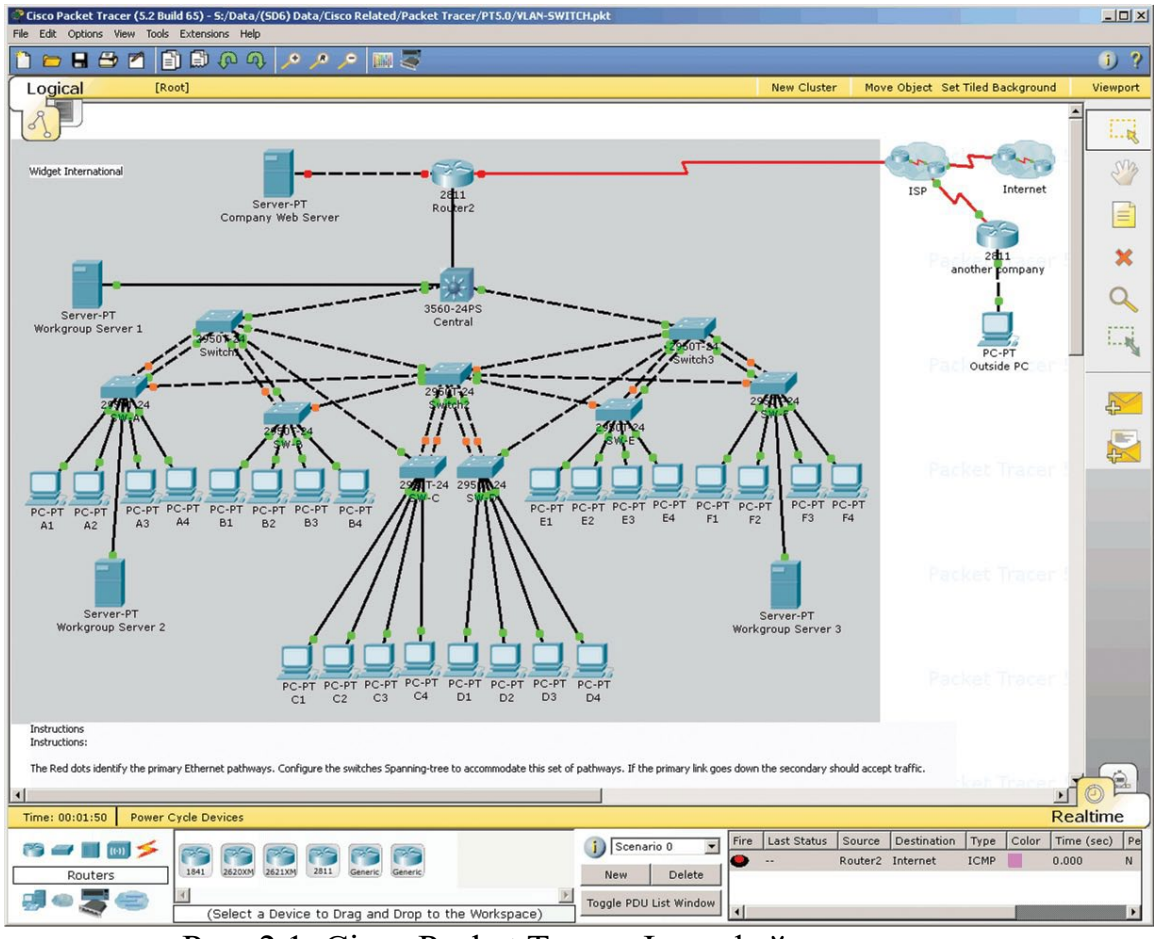


Рис. 2.1. Cisco Packet Tracer. Інтерфейс програми.

Ключові характеристики Cisco Packet Tracer:

1. Дана програма має два основних режими відображення мережі: фізичний та логічний. Логічний дозволяє користувачам будувати логічну мережеву топологію розміщуючи та з'єднуючи віртуальні мережеві пристрої. Фізичний дозволяє показати реальне фізичне розміщення віртуальної мережі, показуючи реальні масштаби розміщення мережевих пристроїв. Також можна показати мережеві зв'язки через декілька міст, країн і т.п.

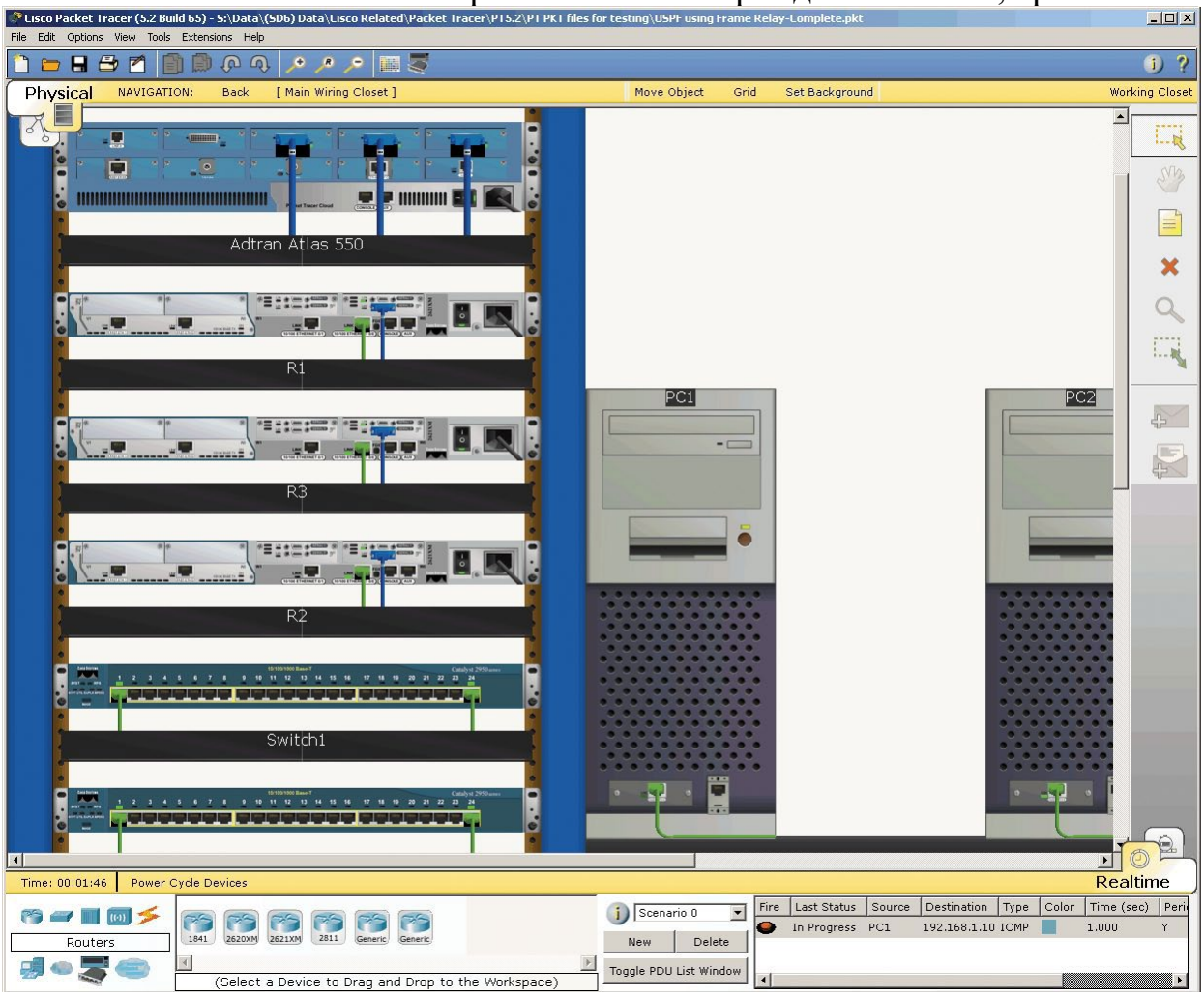


Рис. 2.2. Фізичний режим відображає реальний вигляд віртуальних пристроїв

2. Cisco Packet Tracer підтримує два операційних режими для відображення поведінки мережі: режим реального часу та режим симуляції. В режимі реального часу поведінка мережі виглядає так як відповідають реальні пристрої на події в мережі. Цей режим дозволяє студентам отримати практичні навички в конфігурації мережевих пристроїв перед тим як налаштовувати реальні пристрої. В режимі симуляції користувач може контролювати часові інтервали, передачу даних та розповсюдження інформації по мережі.
3. Cisco Packet Tracer підтримує наступні протоколи:

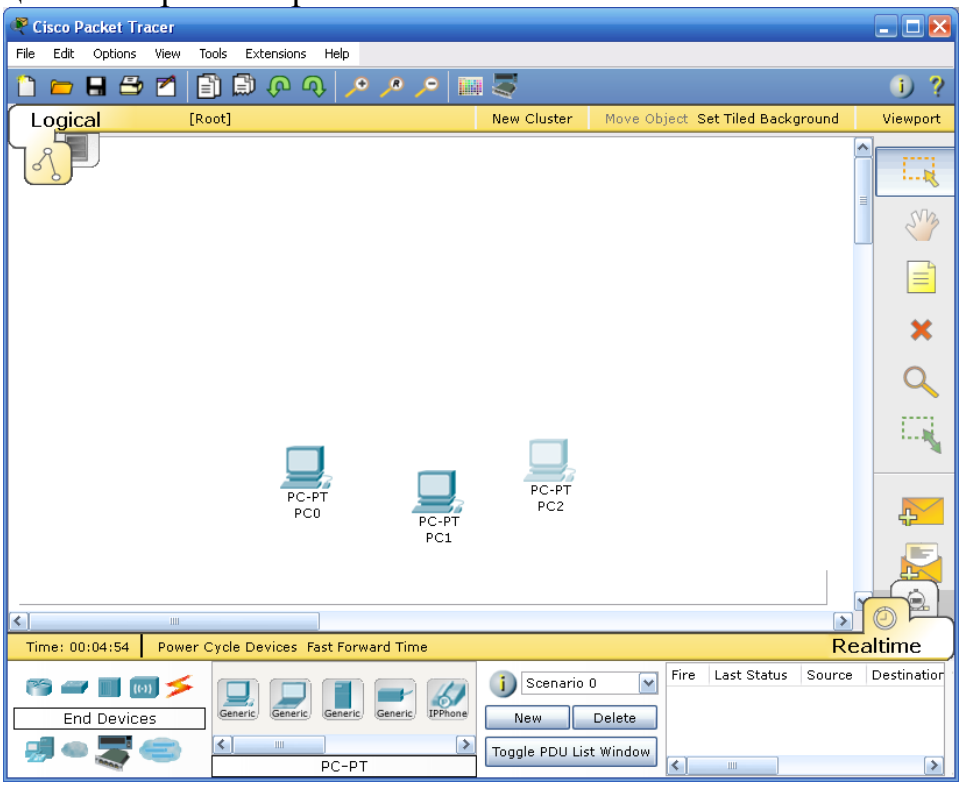
Layer	Cisco Packet Tracer Supported Protocols
Application	• FTP , SMTP, POP3, HTTP, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, ISR VOIP, SCCP config and calls ISR command support, Call Manager Express
Transport	• TCP and UDP, TCP Nagle Algorithm & IP Fragmentation, RTP
Network	• BGP, IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, RIPv1/ v2/ng, Multi-Area OSPF, EIGRP, Static Routing, Route Redistribution, Multilayer Switching, L3 QoS, NAT, CBAL , Zone-based policy firewall and Intrusion Protection System on the ISR, GRE VPN, IPSec VPN
Network Access/ Interface	• Ethernet (802.3), 802.11, HDLC, Frame Relay, PPP, PPPoE, STP, RSTP, VTP, DTP, CDP, 802.1q, PAgP, L2 QoS, SLARP, Simple WEP, WPA, EAP

Практична частина

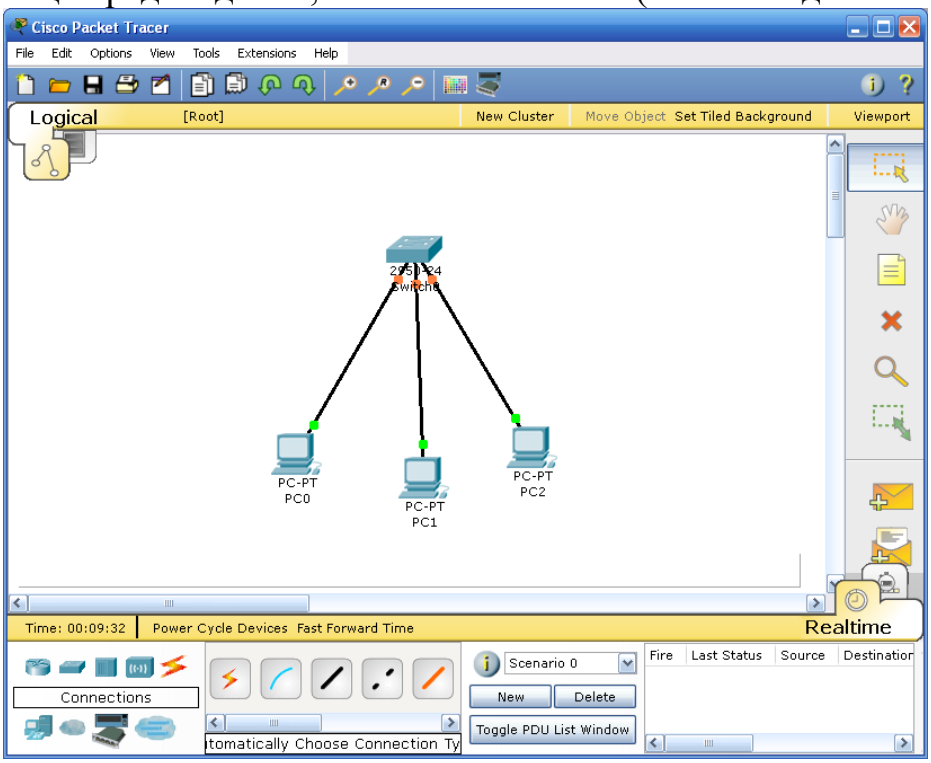
Для знайомства з середовищем моделювання Cisco Packet Tracer студентам пропонується побудувати схему найпростішої мережі яка буде складатися з трьох комп‘ютерів та свіча.

Хід роботи

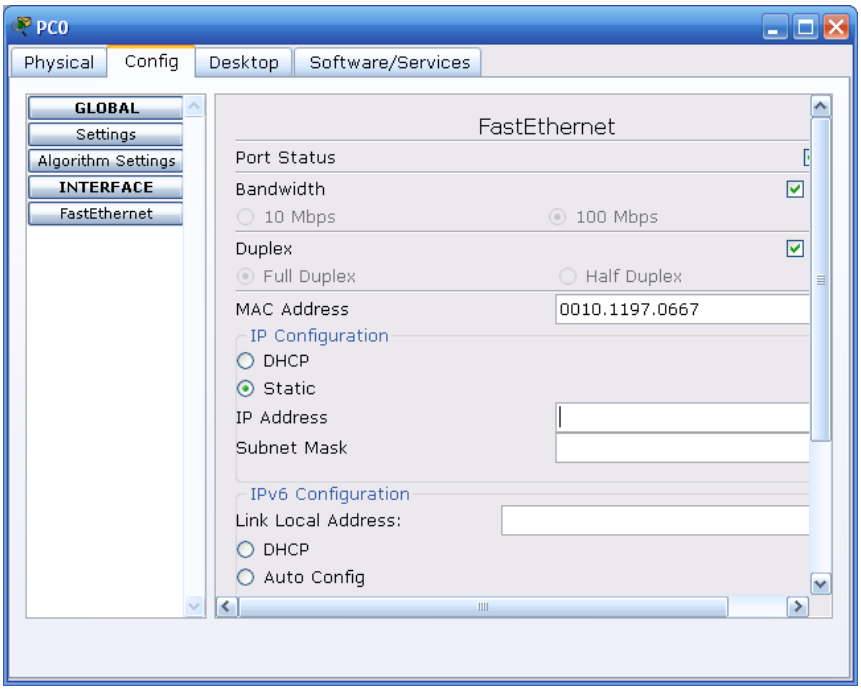
1. Запускаємо Cisco Packet Tracer та вибираємо логічний режим відображення мережі:
2. В нижньому лівому куті головного вікна програми вибираємо іконку End Devices, натискаємо на неї та вибираємо персональний комп‘ютер. Операцію повторюємо тричі.



3. Після цього натискаємо іконку Switches та вибираємо будь-який свіч.
4. Потім починаємо процедуру з‘єднання мережевих пристроїв за допомогою середовищ передачі даних, іконка Connections (має вигляд блискавки).



5. Після цього починаємо прописувати параметри налаштування для персональних комп‘ютерів. Це робиться за допомогою натиску лівою кнопкою миші на іконці персонального комп‘ютера, після цього відкривається вікно налаштування його параметрів. Вибираємо закладку Config/Interface/FastEthernet.



6. В полі IP Address та Subnet Mask прописуємо відповідно ip адресу та маску підмережі для даного комп‘ютера. Повторюємо операцію тричі.
7. Свіч налаштовувати не потрібно.
8. Після здійснення необхідних налаштувань потрібно перевірити працездатність створеної мережі. Для цього вибираємо закладку Desktop/Command Prompt та набираємо команду ping, вказуючи в якості параметру ip адресу сусіднього комп‘ютера.
9. У випадку успішного виконання команди ви здійснили налаштування правильно. Якщо результат виконання команди інший то необхідно виявити та усунути помилки в налаштуваннях.

Контрольні питання

1. Для чого призначена програма Cisco Packet Tracer та які її можливості?
2. Які режими відображення мережі існують в даній програмі та в чому їх відмінності?
3. Які операційні режими є в програмі?
4. Протоколи яких рівнів підтримує Cisco Packet Tracer? Наведіть приклади протоколів кожного рівня.
5. Для чого призначена команда ping?

ЛАБОРАТОРНА РОБОТА № 3

МЕРЕЖЕВІ НАЛАШТУВАННЯ ПЕРСОНАЛЬНОГО КОМП‘ЮТЕРА ТА ДІАГНОСТИКА ПРОТОКОЛУ IP

Мета: навчитися проводити діагностику та збір мережевих налаштувань та комп’ютері під керуванням операційної системи Windows.

Теоретична частина

Налаштування параметрів персонального комп‘ютера для підключення його до локальної мережі значним чином залежить від того яку операційну систему Ви використовуєте. В даній лабораторній роботі ми розглянемо налаштування підключення по локальній мережі для операційних систем Windows XP та Windows 7.

У Windows XP вирішення всіх проблем візьме на себе Майстер налаштування мережі (Network Setup Wizard), який можна знайти в папці Пуск / Всі програми / Стандартні / Зв'язок. Однак настройка мережевих параметрів вручну має перевагу, оскільки дозволяє контролювати всі налаштування. Спочатку необхідно визначити параметри комп‘ютера, для чого командою Пуск-Настройки-Панель керування відкрийте вікно Панель керування, потім клацніть на ярлику Мережеві підключення. У вікні Мережні підключення виберіть мережеве підключення і, клацнувши правою кнопкою миші, виберіть у контекстному меню команду Властивості.

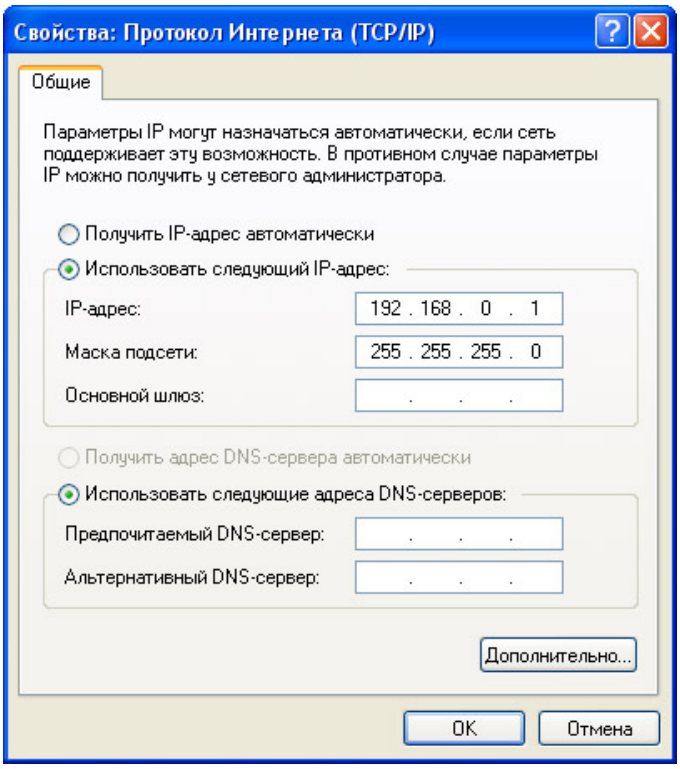


Рис. 3.1. Визначення властивостей протоколу інтернету (TCP/IP)

В даному вікні можна ввести необхідні параметри локальної мережі такі як: IP адреса робочої станції, маска підмережі, адреса шлюзу, тощо. Внесені зміни вступають в силу після перезавантаження персонального комп‘ютера.
Як перейти до конфігурації мережі в Windows 7? Просто переходимо в меню Пуск, потім в Панель управління і вибираємо Мережа та інтернет (Network and Internet).

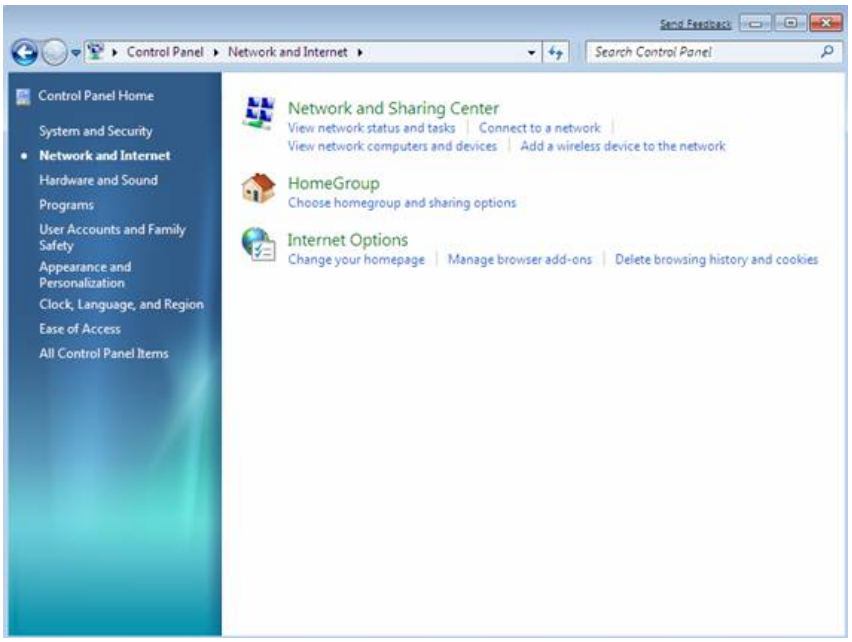
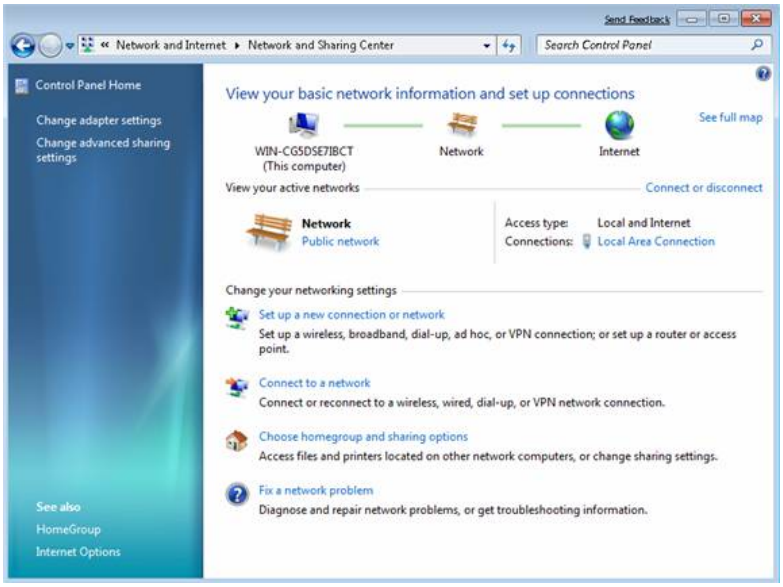


Рис 3.2. Конфігурація мережі та Інтернет параметрів в Windows 7

Далі вибираємо центр управління мережами та загальним доступом

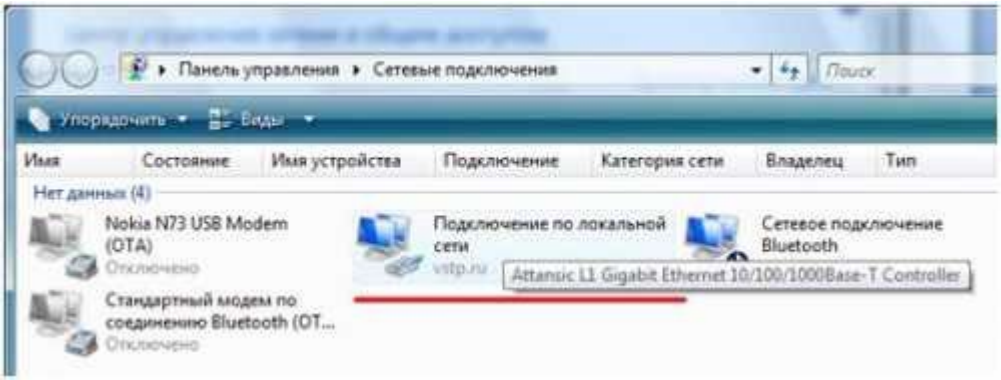


Вибираємо посиланням Створення підключення або мережі. Тут нам на вибір будуть запропоновані чотири варіанти:

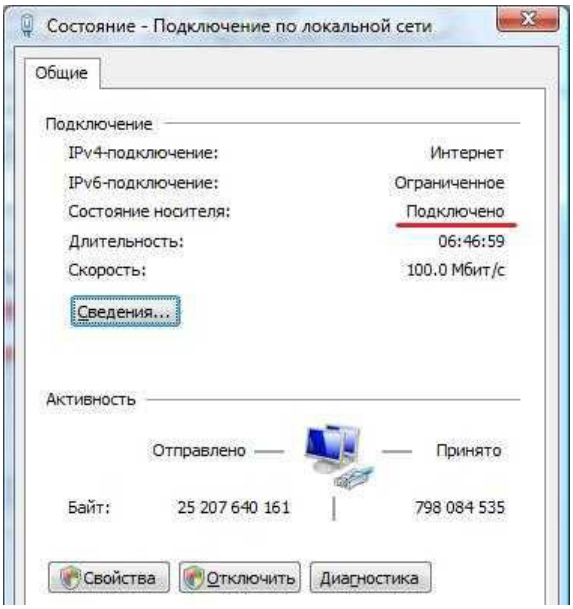
- Підключення до Інтернету (швидкісне, бездротове або телефонне) - цей варіант потрібен для підключення через локальну мережу.
- Налаштування маршрутизаторів і точок доступу.
- Телефонне підключення - вибираємо в тому випадку, якщо ми виходимо в Мережу через звичайний модем. Тут нам знадобиться номер телефону, логін і пароль. Після цього у вікні Керування мережними підключеннями (посилання на нього ви знайдете на лівій панелі Центру) з'явиться значок підключення.

Натиснувши на нього, ви встановите з'єднання з Інтернетом. До речі, керувати підключенням можна і за допомогою значка на панелі повідомлень (нижній правий кут екрану)

- Підключення до робочого місця в «віртуальній мережі» VPN - цей вид підключення практикується не тільки в корпоративному середовищі, а й у деяких інтернет-провайдерів: у цьому випадку з їх місцевою локальною мережею ми працюємо за звичайним каналу, а для інтернету створюється нове «віртуальне» підключення.



У вікні, що в лівій колонці перейдіть за посиланням Управління мережевими підключеннями, після чого виберіть підключення, присвоєне вашому мережному адаптеру і двічі клацніть по ньому мишкою:



Переконайтеся, що у вікні стану статус пристрою знаходиться в режимі «Підключено», якщо ж ситуація інша, то перейдіть в диспетчер пристроїв і примусово запустіть Ваш мережевий адаптер.
Отже, тепер необхідно перевірити конфігурацію IP-адресації (кнопка Властивості у вікні Стан мережевого підключення) і переконатися в наступному:
• Вашому з'єднанню присвоєно статичний реальний IP-адресу;
• Ця IP-адреса коректна і відповідає адресам вашої мережі і адресі основного шлюзу, якщо такий в мережі присутній;
• Вказані параметри хоча б основного DNS-сервера.

Після здійснення налаштувань підключення по локальній мережі необхідно перевірити правильність роботи. Це можна здійснити використовуючи стандартні утиліти Windows: ipconfig, ping, tracert, hostname.

Ipconfig

В операційних системах Microsoft Windows ipconfig - це утиліта командного рядка для виводу деталей поточного з'єднання і управління клієнтськими сервісами DHCP і DNS. Утиліта ipconfig дозволяє визначати, які значення конфігурації були отримані за допомогою DHCP, APIPA або іншої служби IP-конфігурування або задані адміністратором вручну.
Доступні ключі командного рядка в Windows

Ключ	Опис
/all	Відображення повної інформації по всіх адаптерах.
/renew [адаптер]	Оновлення IP-адреси для певного адаптера або якщо адаптер не заданий, то для всіх. Доступно тільки при настроєному автоматичному отриманні IP-адрес.
/flushdns	Очищення DNS кеша.
/displaydns	Відображення вмісту кеша DNS.
/?	Справка.

Ping

ping - утиліта для перевірки з'єднань в мережах на основі TCP / IP. Вона відправляє запити (ICMP Echo-Request) протоколу ICMP зазначеному вузлу мережі й фіксує відповіді, що надходять (ICMP Echo-Reply). Час між відправленням запиту й одержанням відповіді (RTT, від англ. Round Trip Time) дозволяє визначати двосторонні затримки (RTT) за маршрутом і частоту втрати пакетів, тобто визначати завантаженість на каналах передачі даних і проміжних пристроях.
Також пінгом іноді називають час, витрачений на передачу пакету інформації в комп'ютерних мережах від клієнта до сервера і назад від сервера до клієнта. Цей час також називається лагом (англ. відставання, затримка, запізнювання) чи власне затримкою і вимірюється в мілісекундах. Лаг пов'язаний зі швидкістю з'єднання і завантаженістю каналів на всьому протязі від клієнта до сервера.

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

Tracert

traceroute - це службова комп'ютерна програма, призначена для визначення маршрутів прямування даних в мережах TCP / IP. Traceroute заснована на протоколі ICMP. Програма traceroute виконує відправку даних вказаному вузлу мережі, при цьому відображаючи відомості про всі проміжні маршрутизатори, через які пройшли дані на шляху до цільового вузла. В разі проблем при доставці даних до якогось вузла програма дозволяє визначити, на якій саме ділянці мережі виникли неполадки. Програма працює тільки в напрямку від джерела пакетів і є досить грубим інструментом для виявлення неполадок в мережі. У силу особливостей роботи протоколів маршрутизації в мережі Інтернет, зворотні маршрути часто не збігаються з прямими, тому ICMP відповідь від кожного проміжного вузла може йти своїм власним маршрутом, загубитися або прийти з великою затримкою, хоча в реальності з пакетами які адресовані кінцевому вузлу цього не відбувається . Крім того, на проміжних маршрутизаторах часто стоїть обмеження числа відповідей ICMP в одиницю часу, що призводить до появи помилкових втрат.
Для визначення проміжних маршрутизаторів traceroute відправляє серію (зазвичай три) пакетів даних цільовим вузлу, при цьому щоразу збільшуючи на 1 значення поля TTL («час життя»). Це поле зазвичай вказує максимальну кількість маршрутизаторів, які можуть бути пройдені пакетом. Перша серія пакетів відправляється з TTL, рівним 1, і тому перший же маршрутизатор повертає назад повідомлення ICMP, що вказує на неможливість доставки даних. Traceroute фіксує адресу маршрутизатора, а також час між відправленням пакета й одержанням відповіді (ці відомості виводяться на монітор комп'ютера). Потім traceroute повторює відправку серії пакетів, але вже з TTL, рівним 2, що дозволяє першому маршрутизатору пропустити їх далі.
Процес повторюється до тих пір, поки при певному значенні TTL пакет не досягне цільового вузла. При отриманні відповіді від цього вузла процес трасування вважається завершеним.

Hostname

Команда hostname надає швидкий спосіб отримати ім'я вузла локальної системи. Ця команда не підтримує віддалене визначення імені.
Команда має простий синтаксис: hostname. Відразу ж після виконання команди, ім'я комп'ютера буде відображено на екрані.

Практична частина

Перевірте налаштування підключення Вашого комп‘ютера до локальної мережі використовуючи вказівки з теоретичної частини в залежності від встановленої операційної системи на Вашому комп‘ютері.
Зберіть інформацію про параметри Вашого підключення до Інтернету використовуючи команди наведені в теоретичній частині лабораторної роботи. Для відображення параметрів IP-протоколу натисніть кнопку Пуск, виберіть рядок меню Виконати, наберіть символи cmd і натисніть клавішу Enter на клавіатурі. Після цього введіть команди описані в теоретичній частині лабораторної роботи. По результатах виконання команд заповніть наступні таблиці:

Таблиця №1.

Ім‘я NetBIOS	
Ім‘я в домені NT (Win 2000)	
Тип мережевого клієнта	
Ім‘я встановленого драйвера NIC.	
Встановлений мережевий протокол	
Інші мережеві компоненти	

Таблиця №2.

Параметр	Вид інформації	Значення
IP адрес.	Яким чином комп‘ютер отримує свій IP адрес	
IP адрес.	IP адрес комп‘ютера	
IP адрес.	Маска підмережі	
Шлюз	Шлюз по замовчуванню	
Конф. DNS	DNS дозволений?	
Конф. DNS	IP адрес сервера DNS	
Конф. WINS	WINS дозволений?	
Конф. WINS	IP адрес сервера WINS	

Таблиця №3.

Виробник NIC	
NIC працює без помилок?	
Дата драйвера NIC	
Список файлів драйвера	

Контрольні запитання

1. Опишіть процес налаштування під‘єднання комп‘ютера до локальної мережі в операційних системах Windows XP і Windows 7. Назвіть основні відмінності налаштувань у вказаних операційних системах.
2. Які утиліти використовуються для перевірки налаштувань протоколу IP ?
3. Назвіть основні відмінності в роботі утиліт ping та tracert.
4. Назвіть основні параметри команди ping.
5. Назвіть основні параметри команди tracert.
6. Для чого призначена команда hostname?

ЛАБОРАТОРНА РОБОТА № 4

ДОСЛІДЖЕННЯ РОБОТИ ПРИСТРОЇВ КАНАЛЬНОГО РІВНЯ. ДОМЕНІ КОЛІЗІЙ ТА ШИРОКОМОВНІ ДОМЕНИ

Мета: навчитися проводити розпізнавання на мережевих топологіях доменів колізій та широкомовних доменів.

Теоретична частина

Канальний рівень (Data Link layer)

Цей рівень призначений для забезпечення взаємодії мереж на фізичному рівні й контролю за помилками, які можуть виникнути. Отримані з фізичного рівня дані він упаковує в кадри даних, перевіряє на цілісність, якщо потрібно виправляє помилки й відправляє на мережний рівень. Канальний рівень може взаємодіяти з одним або декількома фізичними рівнями, контролюючи й управляючи цією взаємодією. Специфікація IEEE 802 розділяє цей рівень на 2 підрівня - MAC (Media Access Control) регулює доступ до поділюваного фізичного середовища, LLC (Logical Link Control) забезпечує обслуговування мережного рівня. На цьому рівні працюють комутатори, мости й мережні адаптери.

MAC-підрівень забезпечує коректне спільне використання загального середовища, надаючи його в розпорядження тієї або іншої станції мережі. Також додає адресну інформацію до фрейму, позначає початок і кінець фрейму.

Рівень LLC відповідає за достовірну передачу кадрів даних між вузлами, а також реалізовує функції інтерфейсу з мережевим рівнем за допомогою фреймування кадрів. Також здійснює ідентифікування протоколу мережевого рівня.

У програмуванні цей рівень представляє драйвер мережної карти, в операційних системах є програмний інтерфейс взаємодії канального й мережного рівня між собою, це не новий рівень, а просто реалізація моделі для конкретної ОС. Приклади таких інтерфейсів: NDIS, ODI.

Ethernet — базова технологія локальних обчислювальних (комп'ютерних) мереж з комутацією пакетів, що використовує протокол CSMA/CD (множинний доступ з контролем несучої та виявленням колізій). Цей протокол дозволяє в кожний момент часу лише один сеанс передачі в логічному сегменті мережі. При появі двох і більше сеансів передачі одночасно виникає колізія, яка фіксується станцією, що ініціює передачу. Станція аварійно зупиняє процес і очікує закінчення поточного сеансу передачі, а потім знову намагається повторити передачу.

Ethernet-мережі функціонують на швидкостях 10Мбіт/с, Fast Ethernet — на швидкостях 100Мбіт/с, Gigabit Ethernet — на швидкостях 1000Мбіт/с, 10 Gigabit

Ethernet — на швидкостях 10Гбіт/с. В кінці листопада 2006 року було прийняте рішення про початок розробок наступної версії стандарту з досягненням швидкості 100Гбіт/с (100 Gigabit Ethernet).

Технологія

З самого початку Ethernet базувався на ідеї зв'язку комп'ютерів через єдиний коаксіальний кабель, який виконував роль транзитного середовища. Використовуваний метод був дещо схожим на методи радіопередач (хоча й з суттєвими відмінностями, наприклад, те, що в кабелі значно легше виявити колізію, ніж в радіоефірі). Загальний мережний кабель, через який велася передача, був дещо подібним на ефір, і з цієї аналогії походить назва Ethernet (англ. *net* — «мережа»).

З плином часу з відносно простої початкової специфікації Ethernet розвинувся у складну мережну технологію, яка зараз використовується у більшості комп'ютерних систем. Щоб зменшити ціну та полегшити управління та виявлення помилок в мережі, коаксіальний кабель згодом був замінений зв'язками типу «точка-точка», що з'єднувалися між собою концентраторами/комутаторами (хабами/світчами). Своїм комерційним успіхом технологія Ethernet завдячує появі стандарту з використанням кабелю типу «вита пара» в якості транзитного середовища.

На фізичному рівні станції Ethernet спілкуються між собою за допомогою передачі одна одній пакетів — невеликих блоків даних, які відправляються та доставляються індивідуально. Кожна Ethernet-станція має свою власну 48-бітну MAC-адресу, яка використовується як кінцевий пункт або джерело для кожного пакету. Мережні картки, як правило, не сприймають пакетів, що адресовані іншим Ethernet-станціям. Унікальна MAC-адреса є записаною в контролер кожної мережної карти.

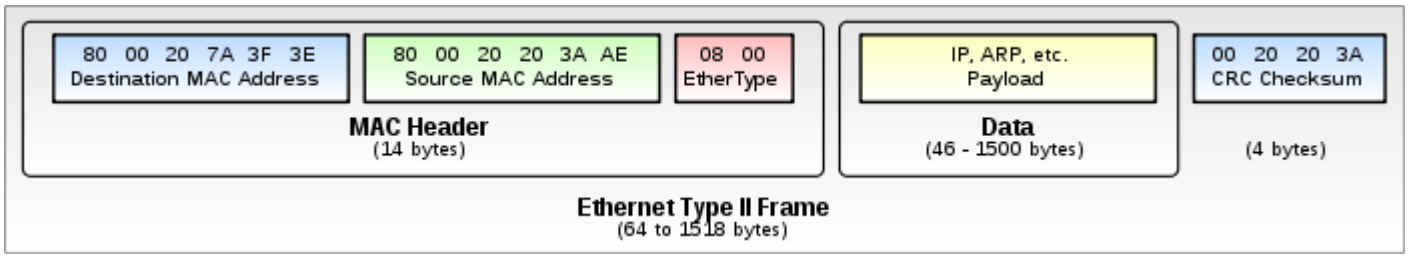
Незважаючи на серйозні зміни від 10-Мбітного товстого коаксіалу до 1-Гбітного оптоволоконного зв'язку типу «точка-точка», різні варіанти Ethernet на найнижчому рівні є майже однаковими з точки зору програміста і можуть бути легко з'єднані між собою за допомогою дешевого обладнання. Це є можливим, оскільки формат кадру лишається незмінним, незважаючи на різні процедури доступу до мережі.

Формат кадру

Існує декілька форматів Ethernet-кадру.

- Первинний Version I (більше не застосовується).
- Ethernet Version 2 або Ethernet-кадр II, ще званий DIX (абревіатура перших букв фірм-розробників DEC, Intel, Xerox) - найпоширена і

використовується до сьогодні. Часто використовується безпосередньо протоколом інтернет.



Найпоширеніший формат кадру Ethernet II

Мережевий комутатор

Atlantis A02-F5P

Мере́жний комута́тор (*network switch*) або світч (від англ. *switch* — перемикач) — пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента. На відміну від концентратора, що поширює трафік від одного підімкненого пристрою до всіх інших, комутатор передає дані тільки безпосередньо отримувачу. Це підвищує продуктивність і безпеку мережі, рятуючи інші сегменти мережі від необхідності (і можливості) обробляти дані, які їм не призначалися.

Комутатор працює на канальному рівні моделі OSI, і тому в загальному випадку може тільки поєднувати вузли однієї мережі по їхніх MAC-адресах. Для з'єднання декількох мереж на основі мережного рівня служать маршрутизатори.

Комутатор зберігає в пам'яті таблицю, у якій вказуються відповідні MAC-адреси вузла порту комутатора. При включенні комутатора ця таблиця порожня, і він працює в режимі навчання. У цьому режимі дані, що поступають на який-небудь порт передаються на всі інші порти комутатора. При цьому комутатор аналізує кадри й, визначивши MAC-адресу хоста-відправника, заносить його в таблицю. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, MAC-адреса якого вже є в таблиці, то цей кадр буде переданий тільки через порт, зазначений у таблиці. Якщо MAC-адреса хоста-отримувача ще не відома, то кадр буде продубльований на всі інтерфейси. Згодом комутатор будує повну таблицю для всіх своїх портів, і в результаті трафік локалізується.

Режими комутації

Існує три способи комутації. Кожний з них — це комбінація таких параметрів, як час очікування й надійність передачі.

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

Можливості й різновиди комутаторів

Комутатори позділяються на керовані й некеровані (найбільш прості). Більш складні комутатори дозволяють керувати комутацією на канальному (другому) і мережному (третьому) рівні моделі OSI. Звичайно їх іменують відповідно, наприклад *Layer 2 Switch* або просто, скорочено *L2*. Керування комутатором може здійснюватися за допомогою Web-інтерфейсу

Домен колізій

В технології Ethernet, незалежно від вживаного стандарту фізичного рівня, існує поняття домена колізій.

Домен колізій (collision domain) – це частина мережі Ethernet, всі вузли якої розпізнають колізію незалежно від того, в якій частині цієї мережі колізія виникла. Мережа Ethernet, побудована на повторювачах, завжди утворює один домен колізій. Домен колізій відповідає одному середовищу, що розділяється. Мости, комутатори і маршрутизатори ділять мережу Ethernet на декілька доменів колізій.

Широкомовним доменом або логічним сегментом мережі називається така її частина у якій розповсюджуються без змін широкомовні повідомлення.

Практична частина

Хід роботи

1. Виконати завдання на визначення кількості широкомовних доменів та доменів колізій. Пояснити викладачу Ваші відповіді (як мінімум 5 прикладів).
2. Виконати завдання на принцип роботи свічів. Показати та пояснити викладачу результати як мінімум 5 прикладів роботи комутатора.
3. Дати відповіді на контрольні запитання.

Контрольні запитання

1. Що таке логічна та фізична сегментація мережі?
2. Для чого призначений комутатор?
3. Які режими роботи комутатора Ви знаєте?
4. Яке призначення та функції канального рівня?
5. Який формат фрейму? Які основні поля фрейму Ви знаєте?

ЛАБОРАТОРНА РОБОТА № 5

SPANNING TREE PROTOCOL (IEEE 802.1D)

Мета: навчитися проводити розрахунок топології STP.

Теоретичні відомості

Один з методів, що використовується для підвищення відмовостійкості комп'ютерної мережі, - протокол покриваючого дерева Spanning Tree Protocol (STP). Розроблений досить давно, він до цих пір залишається актуальним. У мережах Ethernet комутатори підтримують тільки деревоподібні зв'язку, які не містять петель. Це означає, що для організації альтернативних каналів потрібні особливі протоколи та технології, що виходять за рамки базових, яких стосується Ethernet.

Поняття петель

Якщо для забезпечення надлишковості між комутаторами створюється кілька зв‘язків, то можуть виникнути петлі. Петля припускає існування декількох маршрутів по проміжних мережах, а мережа з декількома маршрутами між джерелом і приймачем відрізняється підвищеною стійкістю до збоїв. Хоча наявність надлишкових каналів зв'язку дуже корисно, неконтрольовані петлі, тим не менш, створюють проблеми, найактуальніші з яких:

- Широкомовні шторми;
- Множинні копії кадрів;
- Множинні петлі.

Широкомовний шторм

Поширення широкомовних повідомлень в мережах з петлями представляє серйозну проблему. Припустимо, що перший кадр, що надійшов від вузла 1, є широкомовним. Тоді всі комутатори пересилатимуть кадри нескінченно (Рис. 1), використовуючи всю доступну смугу пропускання мережі і блокуючи передачу інших кадрів у всіх сегментах.

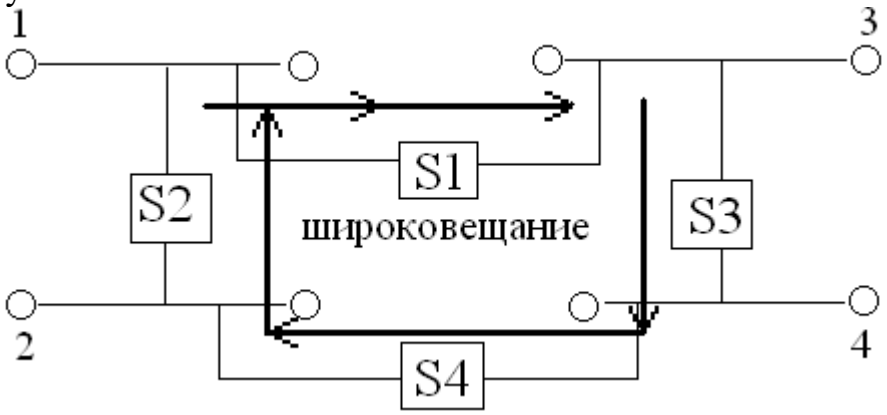


Рис. 5.1. Мостові петлі в середовищі прозорих мостових з'єднань

Множинні копії кадрів

Ще одна проблема полягає в тому, що комутатор отримує кілька копій одного кадру, що одночасно приходять з декількох ділянок мережі. У цьому випадку таблиця комутації не зможе визначити розташування пристрою, тому що комутатор буде отримувати кадр з декількох каналів. Може трапитися так, що комутатор взагалі не зможе переслати кадр, так як буде постійно оновлювати таблицю комутації.

Множинні петлі

Одна з найскладніших проблем - це множинні петлі, що утворюються в об'єднаній мережі. Можлива поява петлі всередині інших петель. Якщо за цим послідує широкомовний шторм, то мережа не зможе виконувати комутацію кадрів. Для вирішення цих проблем і був розроблений протокол покриваючого дерева STP, що використовує алгоритм STA (Spanning Tree Algorithm). STA дозволяє комутаторам автоматично визначати деревоподібну конфігурацію зв'язків у мережі при довільному поєднанні портів між собою. Комутатори, що підтримують протокол STP, автоматично створюють деревоподібну конфігурацію зв'язків без петель в комп'ютерній мережі. Така конфігурація називається покриваючим деревом - Spanning Tree.

Конфігурація покриваючого дерева будується комутаторами автоматично з використанням обміну службовими пакетами. Алгоритм STA вимагає, щоб кожному мосту був присвоєний ідентифікатор. Ідентифікатор моста-8-байтне поле, яке складається з двох частин: 2-байтного пріоритету, призначеного адміністратором і 6-байтної MAC-адреси його блоку управління. Кожному порту також призначається унікальний ідентифікатор в межах мосту, як правило, це його MAC-адрес. Кожному порту моста ставиться у відповідність вартість маршруту, що відповідає витратам на передачу кадру по локальній мережі через цей порт. Процес обчислення покриваючого дерева починається з вибору кореневого моста (root switch), від якого буде будуватися дерево. Як кореневий міст вибирається комутатор з найменшим значенням ідентифікатора. За замовчуванням всі комутатори мають однакове значення пріоритету, рівне 32768 (8000h). У цьому випадку кореневий комутатор визначається за найменшою MAC-адресою. Іноді такий вибір може виявитися далеко не раціональним. Для того щоб в якості кореневого моста був обраний певний пристрій (виходячи з необхідної структури мережі), адміністратор може вплинути на процес виборів, привласнивши відповідному комутатору найменший ідентифікатор вручну.

Другий етап роботи STP - вибір кореневого порту (root port) для кожного з інших комутаторів мережі. Кореневий порт комутатора - це порт, який має по мережі найкоротшу відстань до кореневого комутатора. Третій крок роботи STP - визначення призначених портів. Кожен сегмент в комутованій мережі має один призначений порт (designated port). Цей порт функціонує як єдиний порт моста, який приймає пакети від сегмента і передає їх в напрямку кореневого моста через кореневий порт даного комутатора. Комутатор, що містить призначений

порт для даного сегмента, називається призначеним мостом (designated bridge) цього сегмента. Призначений порт сегмента має найменшу відстань до кореневого мосту серед усіх портів, підключених до даного сегменту. Призначений порт у сегмента може бути тільки один. У кореневого моста всі порти є призначеними, а їх відстань до кореня вважається рівною нулю. Кореневого порту у кореневого моста немає.

При побудові покриваючого дерева важливу роль грає поняття відстані. За цим критерієм вибирається єдиний порт, що з'єднує кожен комутатор з кореневим комутатором, і єдиний порт, що з'єднує кожен сегмент мережі з кореневим комутатором. Всі інші порти переводяться в резервний стан, тобто такий, при якому вони не передають звичайні кадри даних. При такому виборі активних портів в мережі виключаються петлі і залишилися зв'язки, що утворюють покриваюче дерево.

Як відстань в STA використовується метрика вартість шляху (Path Cost) - вона визначається як сумарний умовний час на передачу пакета від порту даного комутатора до порту кореневого комутатора. Умовний час сегмента розраховується, як час передачі одного біта інформації через канал з певною смугою пропускання. Табл. 5.1 показує типові вартості шляху відповідно до стандарту IEEE 802.1d.

Таблиця 5.1

Вартість шляху в протоколі IEEE 802.1d

Швидкість каналу	**Рекомендоване значення**	**Рекомендований діапазон**	**діапазон**
4 Мбіт/с	**250**	**100-1000**	**1-65535**
10 Мбіт/с	**100**	**50-600**	**1-65535**
16 Мбіт/с	**62**	**40-400**	**1-65535**
100 Мбіт/с	**19**	**10-60**	**1-65535**
1 Гбіт/с	**4**	**3-10**	**1-65535**
10 Гбіт/с	**2**	**1-5**	**1-65535**

Обчислення покриваючого дерева відбувається при включенні комутатора і при зміні топології. Ці обчислення вимагають періодичного обміну інформацією між комутаторами покриваючого дерева, що досягається за допомогою спеціальних пакетів, які називаються блоками даних протоколу моста - BPDU (Bridge Protocol Data Unit). Пакети BPDU містять основну інформацію, необхідну для побудови топології мережі без петель:

- ідентифікатор комутатора, на підставі якого вибирається кореневий комутатор;
- відстань від комутатора-джерела до кореневого комутатора (вартість кореневого маршруту);
- ідентифікатор порту;
- пакети BPDU поміщаються в поле даних кадрів канального рівня, наприклад кадрів Ethernet.

Комутатори обмінюються BPDU через рівні проміжки часу (зазвичай 1-4 с). У разі відмови кореневого мосту (що сигналізує про зміну топології) сусідні комутатори, не отримавши пакет BPDU протягом заданого часу (Max Age), починають перерахунок покриваючого дерева.

Приклад роботи STP

Для прикладу розглянуто 3 комутатори, підключені з утворенням петлі (рис. 2). Таким чином, у мережі можуть виникнути проблеми з зацикленням пакетів. Наприклад, нехай будь-який комп'ютер в мережі LAN1 посилає широкомовний пакет. Відповідно до логіки роботи комутаторів комутатор А передасть цей пакет в усі підключені до нього сегменти, за винятком того, з якого він прийшов. Комутатор В отримає цей пакет і передасть його комутатору С. Комутатор С також отримає широкомовний пакет від комутатора А і

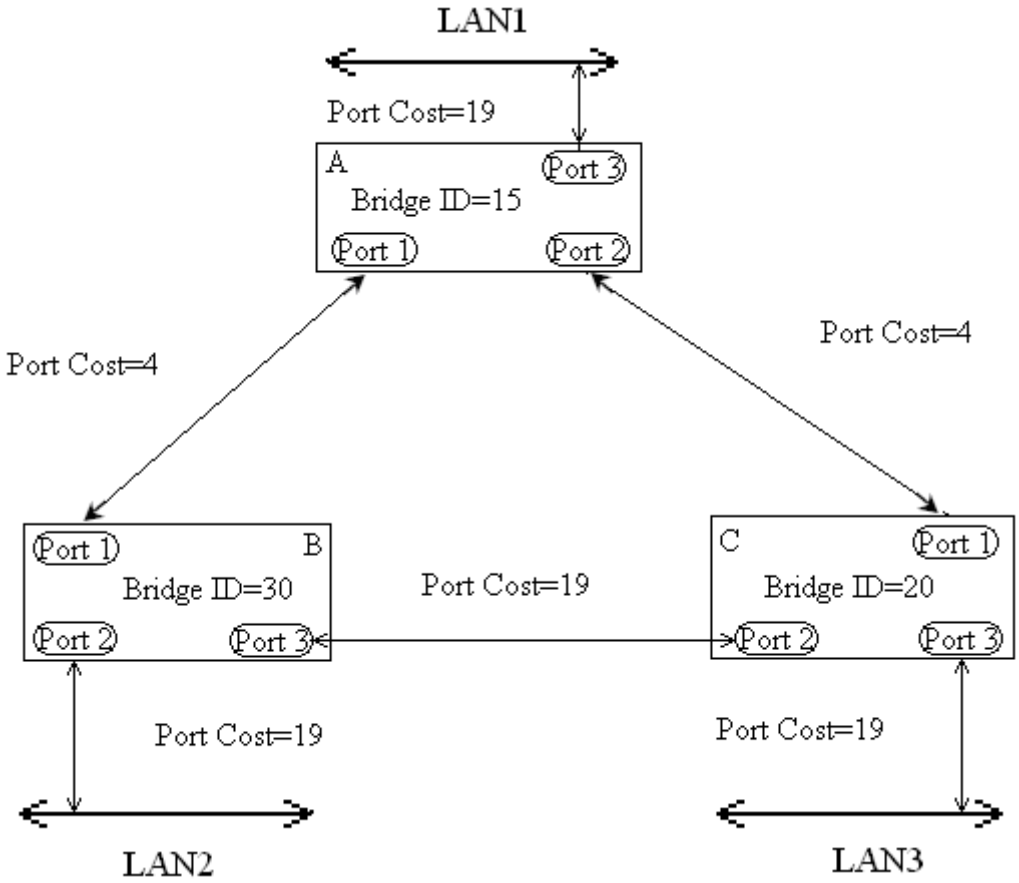


Рис. 5.2. Схема мережі перед застосуванням Spanning Tree

передасть його комутатору В. Той, у свою чергу, поверне його комутатору А і т. д. Пакети можуть ходити по мережі нескінченно довго, що може привести до порушення працездатності мережі. У цьому прикладі з допомогою STP блокується з'єднання між комутаторами С і В.

Отже, після включення живлення і завантаження кожен комутатор починає вважати себе кореневим. Коли він генерує BPDU (через інтервал hello), він поміщає свій ідентифікатор у полі «ідентифікатор кореневого комутатора»,

відстань до кореня встановлюється в 0, а в якості ідентифікатора порту вказується ідентифікатор того порту, через який буде передаватися BPDU. Як тільки комутатор отримує BPDU, в якому є ідентифікатор кореневого комутатора менший ніж його власний, він перестає генерувати свої власні кадри BPDU і починає ретранслювати тільки кадри нового претендента на звання кореневого комутатора. При ретрансляції кадрів він нарощує відстань до кореня, вказану у отриманому BPDU, на умовний час сегмента, через який прийнятий цей кадр.

При ретрансляції кадрів кожен комутатор для кожного свого порту запам'ятовує мінімальну відстань до кореня. При завершенні процедури встановлення конфігурації покриваючого дерева, кожен комутатор знаходить свій кореневої порт - це порт, який ближче інших портів знаходиться по відношенню до кореня дерева.

Розглянемо вибори кореневих портів комутаторів на прикладі (рис. 5.2). Коли комутатор A (кореневий міст) посилає BPDU, вони містять вартість шляху до кореневого мосту рівну 0. Коли комутатор B отримує ці BPDU, він додає вартість шляху Port 1 (4) до вартості, зазначеної в отриманому BPDU (0). Комутатор B потім використовує значення 4 і посилає BPDU з вартістю шляху до кореня, що дорівнює 4, через Port 3 та Port 2. Коли комутатор C отримує BPDU від комутатора B, він збільшує вартість шляху до кореня до 23 (4 + 19). Однак комутатор C також отримує BPDU від кореневого комутатора A через Port 1. Вартість шляху до кореня в цьому BPDU дорівнює 0 і комутатор C збільшує її вартість до 4 (вартість його Port 1 дорівнює 4). Тепер комутатор C повинен вибрати єдиний кореневий порт. Комутатор C вибирає Port 1 як кореневий, оскільки його вартість шляху до кореня менша. Після цього комутатор C починає оголошувати вартість шляху до кореня, рівну 4, комутаторам нижчого рівня. Вибори кореневого порту комутатора B відбуваються аналогічно і кореневим портом для нього стає Port 1 з вартістю 4.

Крім цього, комутатори вибирають для кожного сегмента мережі призначений порт. Для цього вони виключають з розгляду свій кореневий порт, а для всіх портів, що залишилися порівнюють прийняті по них мінімальні відстані до кореня з відстанню до кореня свого кореневого порту. Якщо у свого порту ця відстань менше прийнятих, то це означає, що він є призначеним портом. Коли є кілька портів з однаковим найкоротшим відстанню до кореневого комутатора, то для вибору призначеного порту сегмента STP приймає рішення на основі послідовного порівняння ідентифікаторів мостів і ідентифікаторів портів.

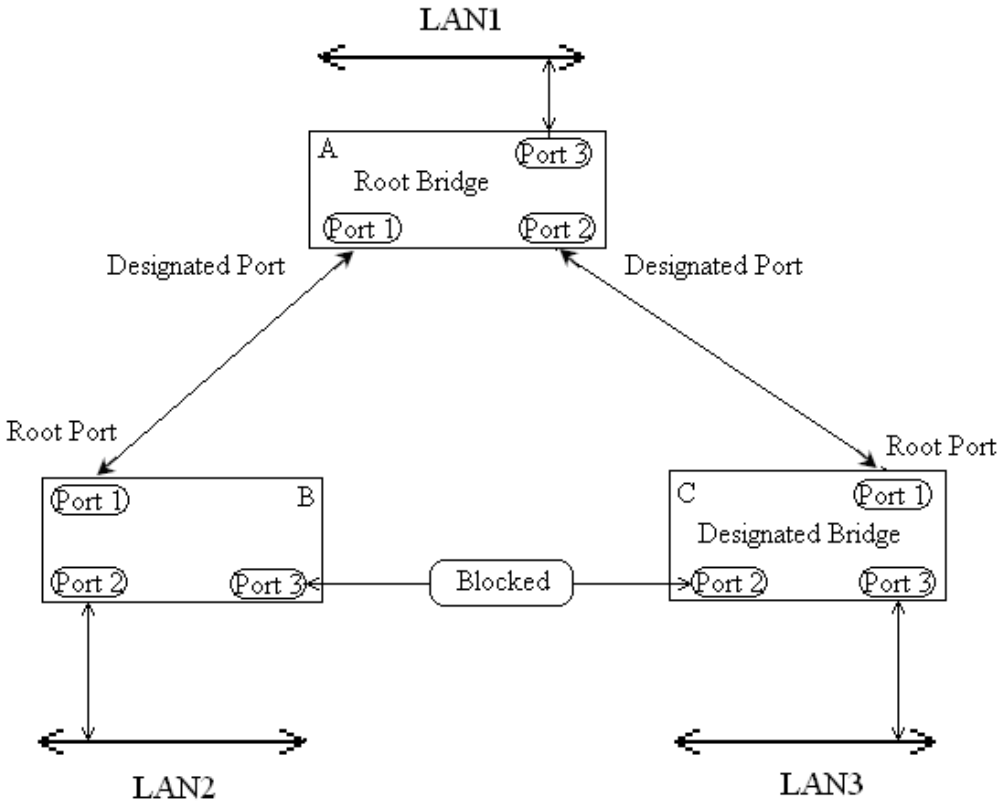


Рис. 5.3. Схема мережі після застосування Spanning Tree

Всі порти, крім призначених, переводяться в заблокований стан і на цьому побудова покриваючого дерева закінчується. На комутаторі B кореневим портом є Port 1 (вартість 4). Тому для сегмента комутатор A - комутатор B призначеним портом буде Port 1 комутатора A. На комутаторі C кореневим портом є Port 1 (вартість 4). Тому для сегмента комутатор A - комутатор C призначеним портом буде Port 2 комутатора A. У сегменті комутатор B - комутатор C обидва порти Port 3 та Port 2 мають однакову вартість шляху, що дорівнює 23. У цьому випадку STP вибере призначений порт сегмента на основі порівняння ідентифікаторів мостів. Оскільки ідентифікатор комутатора C (20) менше ідентифікатора комутатора B (30), то призначеним портом для цього сегменту стане Port 2 комутатори C. Port 3 на комутаторі C заблокується (рис. 5.3). Таким чином, в процесі побудови топології мережі кожен порт комутатора проходить кілька стадій (рис. 4).

1) порт активний або відбулася ініціалізація порту;
2) порт відключений адміністратором або відбувся збій порту;
3) порт обраний як кореневий або призначений порт;
4) порт заблокований;
5) закінчився таймер зміни станів.

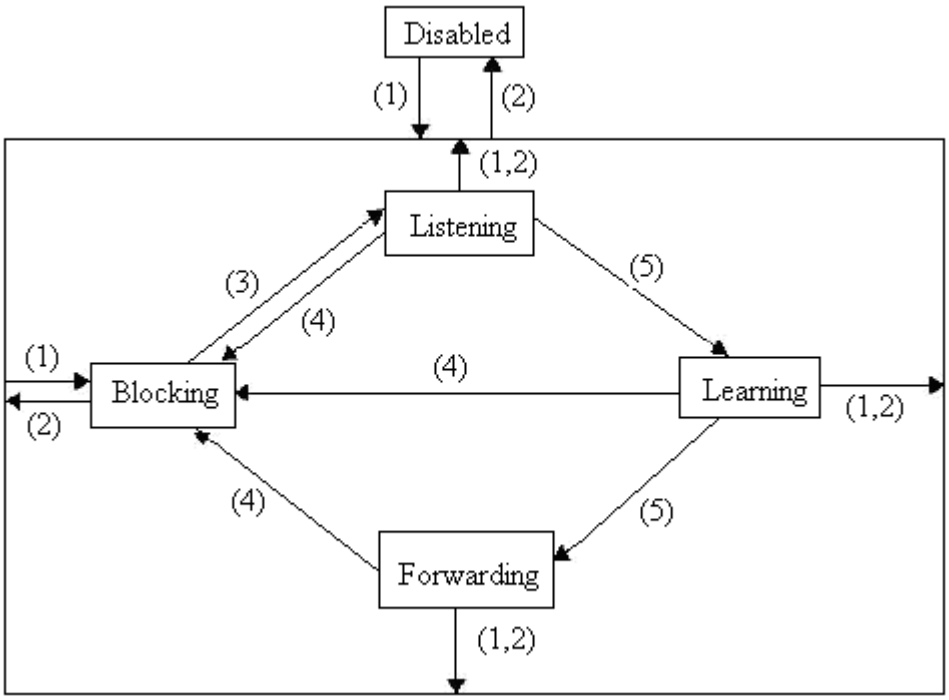


Рис. 5.4. Стани портів в STP

Blocking – при ініціалізації комутатора всі порти (за винятком відключених) автоматично переводяться в стан «Заблоковано». У цьому випадку порт приймає і обробляє тільки пакети BPDU. Всі інші пакети відкидаються.

Listening (прослуховування) - в цьому стані порт продовжує приймати, обробляти і ретранслювати тільки пакети BPDU. З цього стану порт може перейти у стан «Заблоковано», якщо отримає BPDU з кращими параметрами, ніж його власні (відстань, ідентифікатор комутатора або порту). В іншому випадку при закінченні таймера зміни станів порт перейде в наступний стан «Навчання».

Learning (навчання) - порт починає приймати всі пакети і на основі адрес джерела будувати таблицю комутації. Порт в цьому стані все ще не просуває пакети. Порт продовжує брати участь в роботі алгоритму STA і при надходженні BPDU з кращими параметрами переходить у стан «Заблоковано». В іншому випадку при закінченні таймера зміни станів порт перейде в наступний стан «Просування».

Forwarding (просування) - в цьому стані порт може обробляти пакети даних відповідно до побудованої таблиці комутації. Також продовжують прийматися, передаватися і оброблятися пакети BPDU.

Disable (відключений) - в цей стан порт переводить адміністратор. Відключений порт не бере участь ні в роботі протоколу STP, ні в просуванні пакетів даних. Порт можна також вручну включити і він спочатку перейде в стан Blocking. У процесі нормальної роботи кореневий комутатор продовжує генерувати службові пакети BPDU, а решта комутаторів продовжують їх приймати своїми кореневими портами і ретранслювати призначеними. Якщо після закінчення максимального часу життя повідомлення (за замовчуванням -

20 с) кореневий порт будь-якого комутатора мережі не отримає службовий пакет BPDU, то він ініціалізує нову процедуру побудови покриваючого дерева.

Хід роботи

1. Розрахувати вартості шляхів схеми (рис. 5.5) за табл. 5.1.
2. Знайти кореневий комутатор. Кореневим вважається комутатор, який має найменший пріоритет (пріоритети визначаються по перших 6 байтах MAC-адреси комутатора).
3. Визначити кореневі (root) і призначені (designated) порти.

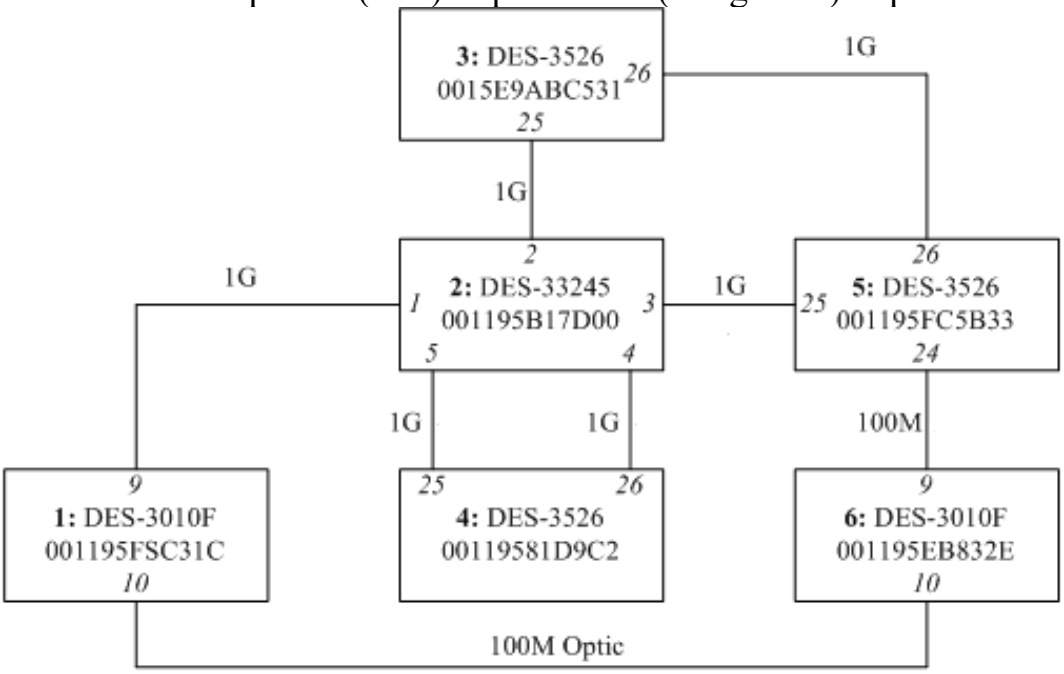


Рис. 5.5. Початкова схема мережі

Приклад розрахунку схеми

Розглянемо наступну схему (рис. 5.6), що складається з 4 комутаторів. Порти комутаторів і вартості шляхів вказані.

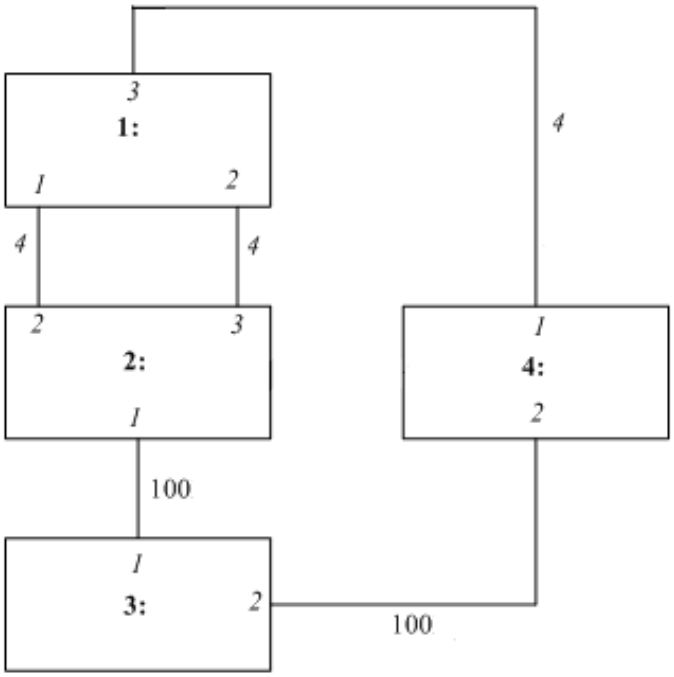


Рис. 5.6. Початкова схема

1. Вибираємо кореневий комутатор. Вартості шляхів від будь-якого комутатора до кореневий повинні бути мінімальні. Отже, проходження пакетів через 10-мегабітні порти (вартості шляхів 100) нам не вигідно.

Таким чином, в даній схемі вигідно, щоб трафік проходив через гігабітні порти (вартості шляхів 4), тоді будемо отримувати найменшу сумарну вартість всього шляху. Отже, як кореневий (ROOT) комутатор вигідно вибрати 1-й комутатор. Йому і присвоюємо найвищий пріоритет (наприклад, 10). Всі його порти стають призначеними d (designated). Решті комутаторів присвоюємо пріоритети, наприклад, 110, 500, 90 (відповідно 2, 3, 4). Схема прийме вигляд, як на рис. 5.7.

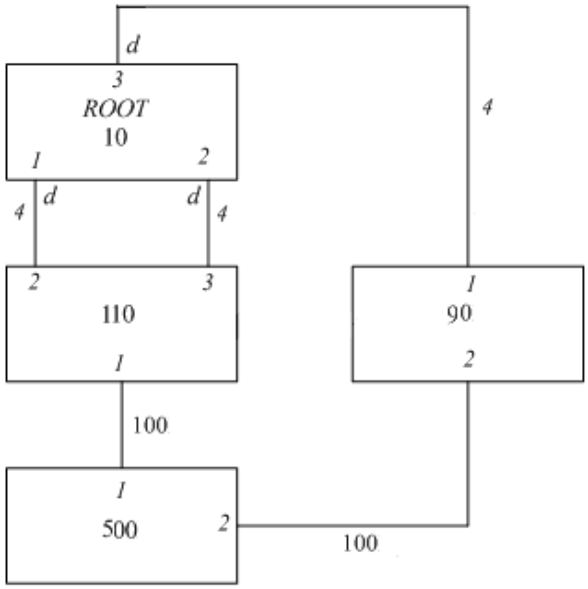


Рис. 5.7. Схема мережі після присвоєння пріоритетів

2. Розрахуємо вартості шляхів для кожного порту на комутаторах, що залишились:

- комутатор 110:
  Port 2 має вартість 4, Port 3 має вартість 4, port 1 має вартість 204 (4+100+100);
- комутатор 500:
  Port 1 має вартість 104 (4+100), port 2 має вартість 104 (4+100);
- комутатор 90:
  Port 1 має вартість 4, port 2 має вартість 204 (4+100+100).

3. Оскільки у 10-го комутатора порти призначені, отже, порти 2, 3 комутатора 110 і порт 1 комутатора 90 повинні бути кореневими R (ROOT). Але у комутатора не може бути двох кореневих портів, отже, в комутаторі 110 один з портів (2 або 3) повинен бути альтернативним. Кореневим залишається порт, вартість шляху до якого менша. У нашому випадку вартості рівні, отже, кореневим залишається порт з найменшим номером, тобто другий, а третій стає альтернативним.

4. Порт 1 комутатора 110 і порт 2 комутатори 90 стають призначеними (d), так як пріоритет цих комутаторів вищі, ніж пріоритет комутатора 500 (його пріоритет 500). Обидва порти комутатора 500 повинні стати кореневими (R), але такого бути не може. Вартості шляхів до обох портів однакові, отже, чинимо, як і раніше: кореневим залишається порт, номер якого менший (тобто 1), третій стає альтернативним. У підсумку схема набуває вигляду, як на рис. 5.8.

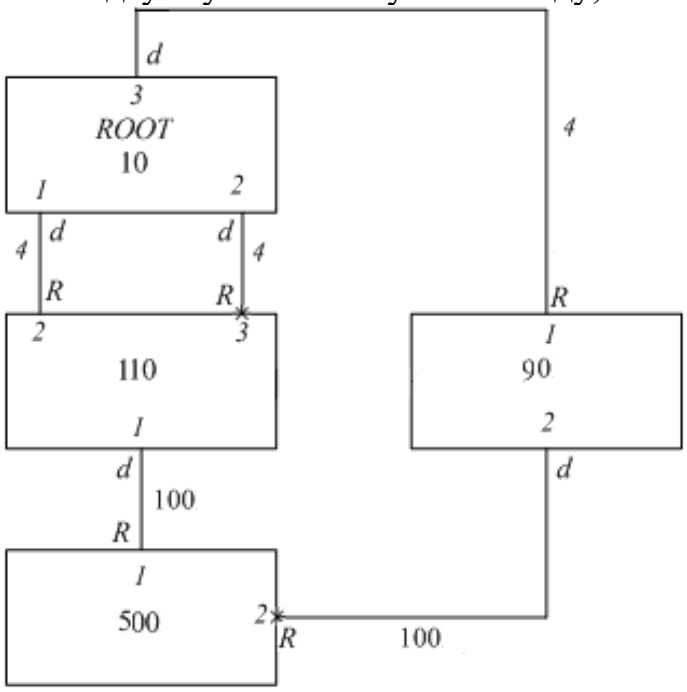


Рис. 5.8. Результуючий вигляд схеми

ЛАБОРАТОРНА РОБОТА № 6

ПІДМЕРЕЖЕВЕ МАСКУВАННЯ

***Мета*:** навчитися виділяти підмережі на основі даної IP-адреси та додаткової інформації; навчитися розраховувати адреси хостів у підмережах та широкомовні адреси.

Обладнання: ПК із встановленим текстовим та графічним редактором.

***Завдання*:**

1. Отримати допуск до виконання лабораторної роботи, давши відповідь на питання для підготовки.
2. Розрахувати маску підмережі відповідно до висунутих вимог. Вказати точну кількість:

А) підмереж, які можливо створити із даною маскою;

Б) хостів у кожній підмережі.

3. Вирахувати IP-адреси вказаних підмереж.
4. Вирахувати широкомовні адреси для вказаних мереж.
5. Вказати межі використовуваних адрес хостів у кожній з вказаних підмереж.
6. Вирахувати адреси вказаних хостів у вказаній підмережі.
7. Дати відповіді на контрольні запитання.

Література:

1. В.Олифер, Н. Олифер. Новые технологии и оборудование IP-сетей.-СПб.: БХВ-Петербург, 2001.
2. В.Олифер. Н.Олифер. Компьютерные сети: принципы, технологии, протоколы.
3. Цифрові ресурси мережі Інтернет.

Питання для підготовки.

1. Які із класів IP адрес не можуть бути використані для адресації кінцевих вузлів? Для чого вони використовуються?
2. Наведіть формат заголовку IP-пакету та поясніть значення вмісту його полів.

Примітка. Варіант завдання вибирається відповідно до порядкового номера студента у журналі із циклічним переходом. Звіт про виконання завдання кожен студент здає окремо.

Варіанти завдань.

1. Дано IP-адресу 141.32.0.0. Передбачити створення на її основі мінімум 50 підмереж із мінімум 500 комп´ютерів у кожній. Вказати IP-адреси 12, 41 та 49 підмереж. Вказати IP-адресу 447 комп´ютера у 38 підмережі.

2. Дано IP-адресу 149.24.0.0. Передбачити створення на її основі мінімум 70 підмереж із мінімум 500 комп´ютерів у кожній. Вказати IP-адреси 10, 2 та 61 підмереж. Вказати IP-адресу 321 комп´ютера у 21 підмережі.

3. Дано IP-адресу 130.221.0.0. Передбачити створення на її основі мінімум 30 підмереж із мінімум 1000 комп´ютерів у кожній. Вказати IP-адреси 8, 15 та 25 підмереж. Вказати IP-адресу 995 комп´ютера у 19 підмережі.

4. Дано IP-адресу 165.121.0.0. Передбачити створення на її основі мінімум 55 підмереж із мінімум 600 комп´ютерів у кожній. Вказати IP-адреси 11, 45 та 54 підмереж. Вказати IP-адресу 500 комп´ютера у 17 підмережі.

5. Дано IP-адресу 190.1.0.0. Передбачити створення на її основі мінімум 8 підмереж із мінімум 20 комп´ютерів у кожній. Вказати IP-адреси 1, 5 та 7 підмереж. Вказати IP-адресу 19 комп´ютера у 3 підмережі.

6. Дано IP-адресу 139.15.0.0. Передбачити створення на її основі мінімум 60 підмереж із мінімум 30 комп´ютерами у кожній. Вказати IP-адреси 13, 25 та 56 підмереж. Вказати IP-адресу 27 комп´ютера у 29 підмережі.

7. Дано IP-адресу 187.254.0.0. Передбачити створення на її основі мінімум 100 підмереж із мінімум 80 комп´ютерів у кожній. Вказати IP-адреси 25, 51 та 78 підмереж. Вказати IP-адресу 59 комп´ютера у 99 підмережі.

8. Дано IP-адресу 150.150.0.0. Передбачити створення на її основі мінімум 25 підмереж із мінімум 400 комп´ютерів у кожній. Вказати IP-адреси 9, 12 та 20 підмереж. Вказати IP-адресу 332 комп´ютера у 15 підмережі.

9. Дано IP-адресу 191.45.0.0. Передбачити створення на її основі мінімум 40 підмереж із мінімум 200 комп´ютерів у кожній. Вказати IP-адреси 15, 21 та 35 підмереж. Вказати IP-адресу 192 комп´ютера у 30 підмережі.

10. Дано IP-адресу 135.56.0.0. Передбачити створення на її основі мінімум 45 підмереж із мінімум 1000 комп´ютерів у кожній. Вказати IP-адреси 9, 28 та 37 підмереж. Вказати IP-адресу 826 комп´ютера у 43 підмережі.

11. Дано IP-адресу 10.0.0.0. Передбачити створення на її основі мінімум 500 підмереж із мінімум 1000 комп´ютерів у кожній. Вказати IP-адреси 100, 243 та 429 підмереж. Вказати IP-адресу 735 комп´ютера у 29 підмережі.

Контрольні запитання

1. Яку долю всієї множини IP-адрес складають адреси класу A? Класу B? Класу C?

2. Які із наведених нижче IP-адрес можуть бути використані в якості IP-адреси кінцевого вузла мережі, під′єднаної до Інтернет? Для синтаксично правильних адрес визначте клас.

a) 127.0.0.1 e) 10.234.17.25 i) 193.256.1.16
b) 201.13.123.245 f) 154.12.255.255 j) 194.87.45.0
c) 226.4.37.105 j) 13.13.13.13 k) 195.34.116.255
d) 103.24.254.0 h) 204.0.3.1 l) 161.23.45.305

3. Чому навіть при використанні підмережевого маскування в IP-пакеті маска не передається?

ЛАБОРАТОРНА РОБОТА № 7

ПРОЕКТУВАННЯ СТРУКТУРОВАНОЇ МЕРЕЖІ ЕОМ ЛОКАЛЬНОЇ

***Мета*:** засвоїти основні принципи розробки адресної схеми структурованої мережі ЕОМ локальної; освоїти 3-рівневу схему проектування мереж.

***Обладнання*:** ПК із встановленим текстовим та графічним редактором, емулятор Packet Tracer.

***Рекомендована література*:**

4. В.Олифер, Н. Олифер. Новые технологии и оборудование IP-сетей.-СПб.: БХВ-Петербург, 2001.
5. В.Олифер. Н.Олифер. Компьютерные сети: принципы, технологии, протоколы.
6. Цифрові ресурси мережі Інтернет.

Питання для підготовки.

1. Чим відрізняється комутація 2 рівня від комутації 3 рівня? Які пристрої здійснюють ту і іншу?
2. Для чого перед початком проектування мережі проводити аналіз трафіку, який нею передається?
3. Які компоненти включає в себе поняття працездатності мережі?
4. Чим відрізняється логічна структуризація мережі від фізичної?

***Завдання*.**

1. Отримати допуск до виконання лабораторної роботи, давши відповідь на питання для підготовки.
2. Вказати адресу комп’ютера А підмережі Б.
3. Розробити адресну схему мережі згідно із варіантом завдання.
4. Розробити структурну схему мережі.
5. Скласти список необхідного комутуючого та маршрутизуючого обладнання.
6. Обгрунтувати вибір проміжних пристроїв.
7. Обгрунтувати вибір середовища передачі даних.
8. Вказати, на якому рівні 3-рівневої моделі проектування працюють пристрої.
9. Дати відповідь на контрольні запитання.
10. Підготувати звіт за результатами виконання лабораторної роботи.

Примітка. До звіту додається електронний варіант схеми мережі, розроблений з допомогою емулятора Packet Tracer.

МЕТОДИЧНІ ВКАЗІВКИ

Першопочатковим завданням при проектуванні будь-якої мережі є аналіз завдань цієї мережі, і як наслідок – аналіз видів трафіку, що передаватимуться нею.

Типи трафіку включають:

- голосові/факсимільні повідомлення
- транзакції
- клієнт-серверна інформація
- текстові повідомлення (e-mail)
- передача файлів
- групові повідомлення
- управляючі повідомлення
- відеоконференції

Аналіз та категоризація трафіку є базовою для ключових рішень проектування.

Характеристики трафіку включають:

- граничні та усереднені значення об’ємів потоків інформації
- необхідність встановлення попереднього з’єднання
- стійкість до затримок, включаючи їх довжину та непостійність
- стійкість до помилок
- приорітет
- типи протоколів
- середню довжину пакету

Користувачів мережі цікавить у першу чергу працездатність мережевих служб та додатків. Поняття працездатності включає наступні компоненти:

- **Час реакції** – час між вводом команди або запиту і виконанням команди або приходом відповіді на запит. Додатки, у яких час реакції є критичним, включають інтерактивні он-лайн сервіси або програмне забезпечення касових терміналів.
- **Пропускна здатність** – деякі додатки вимагають передачі великого об’єму інформації. Але, як правило, вони мають низькі вимоги до часу реакції системи, або працюють у час, коли трафік, чутливий до часу реакції, зменшено (наприклад, у вечірні години)
- **Надійність** – деякі додатки мають підвищені вимоги. Наприклад, бізнесові організації, що ведуть свою діяльність у он-лайн режимі , вимагають 100% надійності каналів зв’язку. Також прикладами можуть бути фінансові системи, системи безпеки, міліцейські та військові системи. Такі ситуації вимагають високого рівня надійності апаратного забезпечення та наявності надлишкових зв’язків.

Необхідно також проаналізувати вимоги до мережі , включаючи ділові та технічні цілі замовника. Для цього слід відповісти на наступні питання: які нові програмні додатки буде встановлено? Чи є вони Інтернет-орієнтованими ? Які завдання виконуватимуть користувачі у мережі? Якими технічними

характеристиками повинна володіти мережа для забезпечення виконання цих завдань?

Мета проведення такого аналізу – визначити або змоделювати усереднений та граничний об'єм інформації для кожного джерела за одиницю часу. Необхідно змоделювати діяльність мережі протягом нормального робочого дня та визначити тип трафіку, його величину, час відповіді хостів, час передачі файлів.

Такий аналіз можна проводити на вже існуючій мережі. Якщо отримані характеристики близькі до необхідних характеристик проектованої мережі, можна взяти тестовану за прототип і на її основі спроектувати нову, внісши необхідні корективи.

Проблема, яка виникає у цьому випадку, полягає в тому, що досить важко точно визначити завантаженість мережі та продуктивність мережевих пристроїв як функцію кількості користувачів, типу програмних додатків та віддаленості від сервера.

Фактори, які впливають на динамічну поведінку мережі:

- характер доступу до мережі залежить від часу – пікові періоди можуть змінюватися; тому вимірювання повинні проводитися у досить широкому часовому проміжку;
- відмінності, пов'язані з типом трафіку - комутований та маршрутизований трафік висуває різні вимоги до мережевих пристроїв та протоколів; деякі протоколи чутливі до втрачених пакетів; деякі додатки вимагають більше пропускної здатності каналу;
- випадкова природа мережевого трафіку – певна поведінка мережі при несподіваних впливах є непередбачуваною.

Після того, як розглянуто всі вимоги до мережі, необхідно визначити та спроектувати обчислювальне середовище, яке зможе забезпечити виконання цих вимог.

Ієрархічна модель проектування мереж дозволяє проектувати мережі по рівнях. Як і використання моделі OSI, це спрощує завдання в цілому, розбиваючи його на кілька простіших і легше виконуваних задач. Кожен рівень може бути сфокусовано на забезпеченні специфічних функцій, дозволивши таким чином проектувальнику вибрати відповідні характеристики системи.

Використання ієрархічного проектування сприяє подальшим змінам мережі. Модульність у проектуванні мережі дозволяє створювати елементи, які можуть бути замінені із зростанням мережі. Також такий підхід спрощує визначення ділянки, на якій відбувся збій у роботі мережі.

Переваги використання ієрархічної моделі:

- Масштабованість
- Легкість реалізації
- Легкість пошуку несправностей
- Передбачуваність
- Підтримка багатопротокольності
- Керованість.

Ієрархічна модель проектування мереж включає наступні 3 рівні:

- **Базовий рівень** – забезпечує оптимальне транспортування між підрозділами
- **Рівень розповсюдження** – забезпечує взаємодію користувачів відповідно до певної політики доступу
- **Рівень доступу** – забезпечує доступ до мережі на рівні користувачів та робочих груп

Під рівнем розуміється точка у мережі, де відбувається розмежування між функціями пристроїв 3-го (мережевого) рівня моделі OSI. (рис. 7.1)

Трирівнева модель проектування мереж може забезпечити вимоги більшості корпоративних мереж. Однак не всі мережі вимагають повної трирівневої ієрархії. У деяких випадках може підходити дворівневе проектування, або навіть плоска однорівнева мережа. У будь-якому випадку структура мережі повинна бути ієрархічною, щоб надати можливість розширення мережі у майбутньому при потребі.

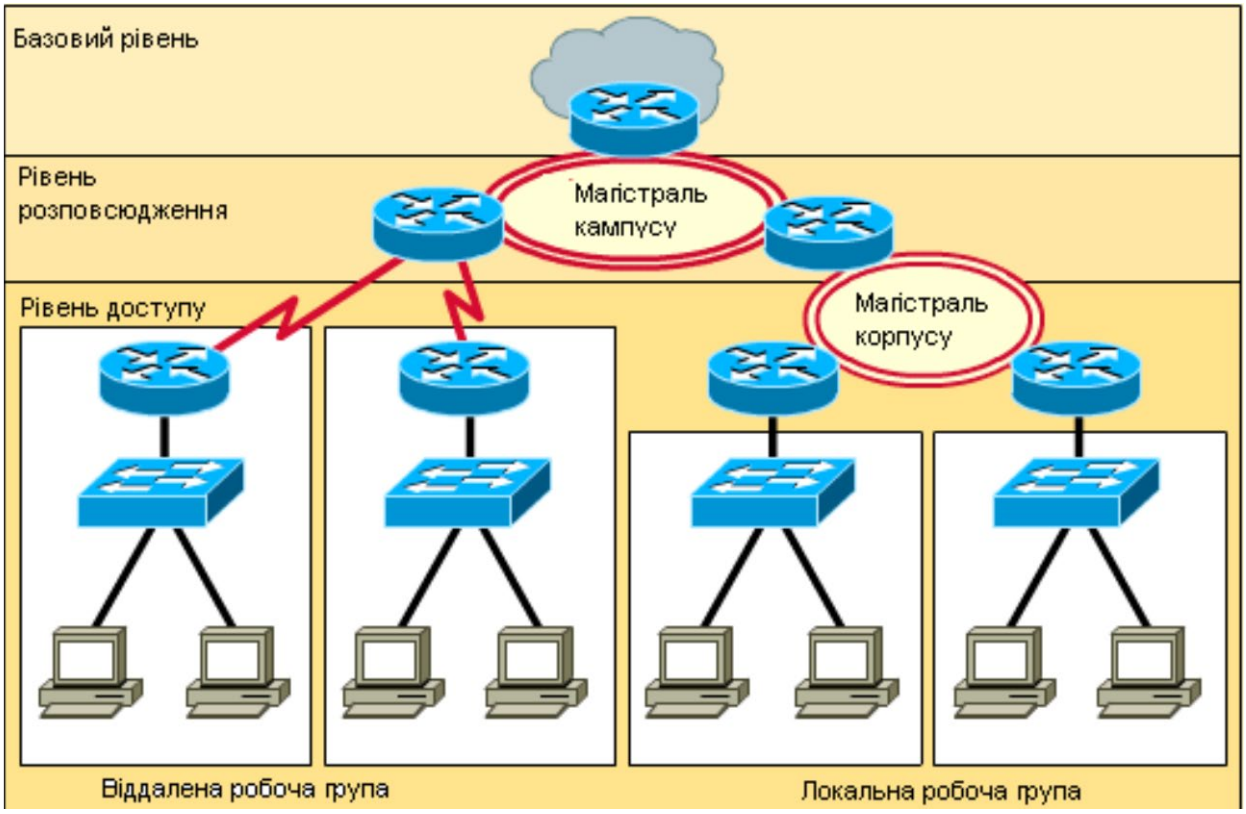


Рис. 7.1. Приклад трирівневої ієрархії мережі.

До завдання базового рівня входить забезпечення швидкого обміну інформацією між віддаленими робочими групами. Цей рівень мережі не повинен забезпечувати контролю доступу або фільтрації, оскільки це уповільнює комутацію пакетів. Базовий рівень, як правило, втілюється технологіями глобальних мереж. Він повинен забезпечувати певні надлишкові зв’язки (для підвищення відмовостійкості). Протоколи маршрутизації, які використовуються на цьому рівні, повинні володіти швидким часом збіжності, та підтримувати розподіл навантаження кількома шляхами. Також одним із основних завдань базового рівня є ефективне використання пропускної здатності каналу. Тут в

основному використовуються зв’язки типу “point-to-point” та немає окремих хостів.

Рівень розповсюдження – це точка поділу між базовим рівнем та рівнем доступу, його наявність допомагає описати та відділити ядро мережі. До його функцій входять:

- забезпечення адресації
- доступ робочої групи або відділу до базового рівня
- визначення широкомовних доменів
- маршрутизація віртуальних мереж (VLAN)
- забезпечення належного рівня безпеки інформації

Рівень розповсюдження включає магістраль корпусу із всіма під’єднаними маршрутизаторами.

Рівень доступу – це точка, у якій кінцеві користувачі отримують доступ до мережі. Цей рівень також може включати списки доступу або певні фільтри для оптимізації забезпечення потреб певних користувачів. Функції рівня доступу можуть включати наступні:

- розділення каналів
- комутація каналів
- фільтрація на MAC-рівні
- мікросегментація

Наявність рівня доступу дозволяє логічно сегментувати мережу і групувати користувачів за функціями, які вони виконують, а не за їх фізичним розміщенням.

Контрольні запитання

1. Які з проміжних мережевих пристроїв здійснюють сегментацію, а які – мікросегментацію мережі?
2. Поясніть різницю між термінами “розширюваність” та “масштабованість”.
3. Які характеристики мережі включає у себе поняття “якість обслуговування” (Quality of Service, QoS)?

Варіанти завдань

№ варіанту	IP адреса\маска	А	Б
1	151.9.0.0\21	87, 48	13, 22
2	146.78.0.0\22	45, 34	3, 30
3	31.0.0.0\21	116, 1	5, 64
4	55.0.0.0\23	33, 24	115, 68
5	123.0.0.0\17	307, 13	42, 9
6	187.119.0.0\23	181, 24	11, 56
7	164.254.0.0\27	4, 9	45, 10
8	98.0.0.0\19	256, 67	17, 22

1. Будинок корпорації “Альфа” має 3 поверхи. На кожному поверсі 5 відділів по 8 комп’ютерів у кожному, та 1 операційний зал на 50 машин. На кожному поверсі стоять основний та резервний сервери баз даних. Зв’язок із Інтернет необхідний рідко, 2 рази на день відправити і прийняти пошту. Відеоконференції не проводяться, основний вид трафіку – транзакції із сереверами БД.

2. Банк “Бета” відкриває регіональне відділення. Необхідно забезпечити можливість обладнання обчислювальною технікою 6 відділів, у кожному 10 секторів мінімум по 2 комп’ютери. У подальшому можливий переїзд головної контори у дану будівлю, тому забезпечити можливість розширення мережі у 10-15 разів. Сервери баз даних банку розташовані у головній конторі, доступ здійснюється через провайдера Інтернет. Трафік інтенсивний, працюють файлові сервери.

3. Навчальний корпус “Гамма” обладнано 20 лабораторіями по 30 комп’ютерів у кожній; планується введення в дію ще 10. Крім того, працюють дослідницькі кімнати (5 по 15 комп’ютерів), яким необхідно мати доступ до Інтернету окремо від лабораторій. Значну частину трафіку складають мультимедійні додатки.

4. Компанія “Дельта” вводить у дію новий корпус. Там обладнано 3 операційні зали (30 машин, трафік в основному локальний) та 5 відділів по 7 машин у кожному . Між відділами – інтенсивний обмін файлами, бухгалтерською інформацією. Відділ зовнішніх зв’язків активно працює із веб-сторінкою компанії, розміщеною на сервері провайдера. Адмініструванням мережі займається людина, яка має окрему кімнату, доступ посторонніх туди обмежено, знаходиться точка присутності (Point of Presence, PoP).

5. Фірма “Ікс” займає двоповерховий корпус. На першому поверсі – 2 операційні зали по 30 машин та 2 сервери баз даних у кожному. У кінці дня проводиться резервне копіювання інформації на сервери, що знаходяться на другому поверсі. Крім того, на другому поверсі ще 4 відділи по 7 комп’ютерів, які інтенсивно обмінюються інформацією між собою та інколи вимагають доступу до серверів баз даних. Доступ до Інтернет через комутований канал.

6. Компанія “Ігрек” розширила площі, за рахунок чого необхідно розширити та реорганізувати мережу. Раніше вони володіли 5 кімнатами, у кожній з яких стояло по 8 комп’ютерів. Тепер вводяться в дію ще 3 такі кімнати і операційний зал на 50 машин. Працівники операційного залу вимагають постійного доступу до Інтернет, всі інші – лише до поштового серверу компанії.

7. Інститут “Зет” отримав фінансування на нові лабораторії. Їх буде 5, по 20 комп’ютерів у кожній . Крім того, мережа повинна обслуговувати 40 індивідуальних комп’ютерів працівників та веб-сервер, який знаходиться у цьому ж приміщенні. Працівники періодично дивляться фільми, що містяться на файловому сервері.

8. Компанія “Тау” реорганізовує мережу у зв’язку із переїздом до нового приміщення. Там будуть знаходитися 5 відділів компанії по 10 комп’ютерів, 2 операційні зали по 40 машин та 7 принт-серверів (по 1 на кожну кімнату). Трафік у операційних залах в основному локальний, але проходить інтенсивний обмін інформацією між відділами. Зв’язок з Інтернет нерегулярний.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Wendell Odom, Sean Wilkins. CCNA 200-301 Official Cert Guide and Network Simulator Library. – Cisco Press, 2022, 560p.
2. Scott Empson. CCNA 200-301 Portable Command Guide, 5th Edition. – Cisco Press, 2019, 320p.
3. Billy Calvert. CCNA: CCNA 200-301: Cisco Certified Network Associate. – Cisco Press, 2020, 206p.
4. Johnson Allan. 31 Days Before your CCNA Exam: A Day-By-Day Review Guide for the CCNA 200-301 Certification Exam. – Cisco Press, 2020, 464p.
5. Todd Lammle, Jon Buhagiar. CCNA Certification Study Guide and Practice Tests Kit: Exam 200-301. – SYBEX, 2020, 1360p.
6. Wendell Odom. CCNA 200-301 Official Cert Guide, Volume 1. – Cisco Press, 2020, 848p.
7. Wendell Odom. CCNA 200-301 Official Cert Guide, Volume 2. – Cisco Press, 2020, 624p.

Навчально-методичне видання

Д’яченко Лілія Іванівна

Організація комп’ютерних мереж:
Навчально-методичний посібник з лабораторних робіт
(видання електронне)

для студентів спеціальностей
121 - Інженерія програмного забезпечення, 122 – Комп’ютерні науки
усіх форм навчання

Відповідальний за випуск – Л.І. Д’яченко
Літературний редактор – О.В. Лупул
Технічний редактор та дизайнер обкладинки – А.В. Цвіра

Підписано до друку 1.10.2022. Формат 60х84/16.
Папір офсетний. Друк різографічний. Умов.-друк. арк. 18,59.
Обл.-вид. Арк. 16,73. Тираж 150. Зам. Н-008п.
Видавництво та друкарня Чернівецького національного університету.
58012, Чернівці, вул. Коцюбинського, 2.
e-mail: ruta@chnu.edu.ua

Свідоцтво суб’єкта видавничої справи ДК № 891 від 08.04.2002.