

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни

"Комп'ютерні мережі"

для студентів спеціальності 123 Комп'ютерна інженерія,
усіх форм навчання.

Симуляція мережевих з'єднань. Частина 3

Методичні вказівки до виконання лабораторних робіт з дисципліни "Комп'ютерні мережі" для студентів спеціальності 123 Комп'ютерна інженерія, усіх форм навчання. Симуляція мережевих з'єднань. Частина 3 / Укл. Г.Г. Киричек. – Запоріжжя: Національний університет «Запорізька політехніка», 2024. – 30 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.

Рецензент:

М.Ю. Тягунова, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 5 від 18.12.2023

Затверджено
на засіданні НМК КНТ
Протокол № 5 від 25.12.2023

ЗМІСТ

1 Загальні відомості.....	4
1.1 Вітуальні локальні мережі.....	4
1.2 Прості методи захисту.....	7
2 Лабораторна робота. Комутація та налаштування віртуальних локальних мереж	12
2.1 Побудова моделі мережі.....	12
2.2 Основні налаштування комутаторів.....	15
2.3 Налаштування VLAN.....	16
2.4 Індивідуальне завдання	17
2.5 Зміст звіту	19
2.6 Контрольні питання.....	19
3 Лабораторна робота. Стандартні списки контролю доступу	19
3.1 Рір маршрутизація та ACL.....	19
3.2 OSPF та стандартний ACL	22
3.3 Міжмережні налаштування ACL.....	25
3.4 Самостійне завдання.....	28
3.5 Зміст звіту	29
3.6 Контрольні питання.....	29
Рекомендована література.....	30

1 ЗАГАЛЬНІ ВІДОМОСТІ

1.1 Вітуальні локальні мережі

VLAN (*Virtual Local Area Network* — віртуальна локальна комп'ютерна мережа) — група хостів з загальним набором вимог, які взаємодіють так, ніби вони прикріплені до одного домену, незалежно від їх фізичного розташування. VLAN має ті самі атрибути, як і фізична локальна мережа, але дозволяє кінцевим станціям бути згрупованими разом, навіть якщо вони не перебувають на одному мережевому комутаторі. Реконфігурація мережі може бути зроблена за допомогою програмного забезпечення замість фізичного переміщення пристроїв.

Це означає, що передача кадрів між різними віртуальними мережами на підставі адреси каналного рівня неможлива, незалежно від типу адреси - унікальної, групової або широкомовної. У той же час усередині віртуальної мережі кадри передаються за технологією комутації, тобто тільки на той порт, що зв'язаний з адресою призначення кадру. Віртуальні мережі можуть перетинатися, якщо один або кілька комп'ютерів входять до складу більш ніж однієї віртуальної мережі.

Віртуальна мережа утворює *домен широкомовного трафіка* (**broadcast domain**), за аналогією з доменом колізій, який утворюється повторювачами мереж Ethernet.

Призначення технології віртуальних мереж складається в полегшенні процесу створення ізольованих мереж, які потім повинні зв'язуватися за допомогою маршрутизаторів, що реалізують який-небудь протокол мережевого рівня, наприклад IP. Така побудова мережі створює набагато могутніші бар'єри на шляху помилкового трафіка з однієї мережі в іншу. Сьогодні вважається, що будь-яка велика мережа повинна включати маршрутизатори, інакше потоки помилкових кадрів, наприклад широкомовних, будуть періодично затоплювати всю мережу через прозорі для них комутатори, приводячи її в непрацездатний стан.

Технологія віртуальних мереж створює гнучку основу для побудови великої мережі, з'єднаної маршрутизаторами, тому що комутатори дозволяють створювати повністю ізольовані сегменти програмним шляхом, не прибігаючи до фізичної комутації.

Для того, щоб фізично копіювати функції VLAN, необхідно встановити окремий, паралельний збір мережевих кабелів і перемикачів, які зберігаються окремо від первинної мережі. Однак на відміну від фізичної відділеної мережі, VLAN ділить пропускну здатність, тому дві окремих одно-гігабітних віртуальних мережі які використовують одно-гігабітний зв'язок мають знижену пропускну здатність. Це віртуалізує поведінку VLAN (настроювання портів комутатора, позначки кадрів при вході в мережу VLAN, пошук MAC таблиці, щоб перейти до магістральних зв'язків і видалення тегів при виході з VLAN).

Віртуальні локальні мережі 2-го рівня конструкції є важливими, порівняно з IP-підмережами, які є конструкціями 3-го рівня. При використанні VLAN, можна управляти пакетами трафіку і швидко реагувати на переміщення. Мережі VLAN забезпечують гнучкість, щоб адаптуватися до змін у мережі вимогам і дозволяють спрощене адміністрування.

Оскільки комутатори 2 рівня не пересилають кадри між VLAN, мережа повинна використовувати маршрутизатори для маршрутизації IP-пакетів між підмережами, щоб дозволити цим пристроям у різних VLAN/підмережах спілкуватися між собою. Маємо три методи маршрутизації між мережами VLAN:

- маршрутизація VLAN із магістральними лініями маршрутизатора 802.1Q: спочатку обговоримо, як налаштувати маршрутизатор для використання транкінгової мережі VLAN під час підключення до комутатора рівня 2. Маршрутизатор виконує маршрутизацію, а комутатор створює VLAN. З'єднання між маршрутизатором і комутатором використовує транкінг, щоб маршрутизатор мав інтерфейс, підключений до кожної VLAN/підмережі. Ця функція відома як маршрутизація по транку VLAN;

- маршрутизація VLAN за допомогою комутаторів 3 рівня SVI (switched virtual interfaces): далі розглянемо використання комутатора локальної мережі, який підтримує як комутацію рівня 2, так і маршрутизацію рівня 3 (є комутатором рівня 3 або багаторівневим комутатором). Для маршрутизації конфігурація комутатора рівня 3 використовує інтерфейси, які називаються комутованими віртуальними інтерфейсами (SVI), або інтерфейсами VLAN;

- маршрутизація VLAN із маршрутизованими портами комутатора рівня 3: потім розглянемо альтернативу SVI, яка називається маршрутизованими портами, у яких фізичні порти комутатора діють як інтерфейси на маршрутизаторі та концепцію EtherChannel, який використовується як маршрутизований порт у функції під назвою Layer 3 EtherChannel.

На рисунку 1.1 показані випадки, в яких можна використовувати наведені параметри.

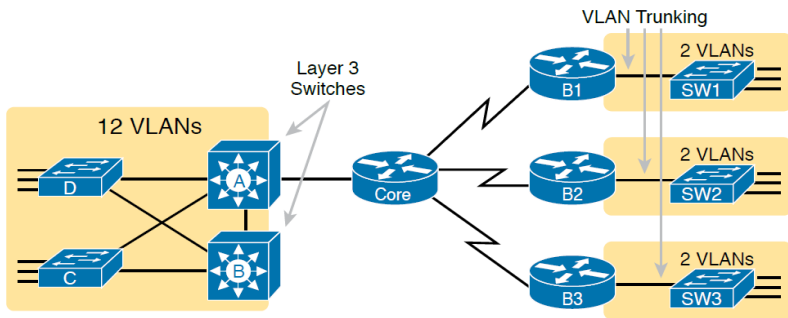


Рисунок 1.1 – Маршрутизація VLAN

Можемо бачити два комутатори, позначені A і B, які можуть працювати як комутатори рівня 3 - обидва з SVI (комутаційними віртуальними інтерфейсами) і маршрутизованими інтерфейсами. На рисунку ліворуч наведено центральну локальну мережу кампусу з 12 VLAN.

Комутатори A і B діють як комутатори рівня 3, поєднуючи функції маршрутизатора та комутатора, маршрутизуючи дані між усіма 12 підмережами/VLAN, а також маршрутизуючи дані до/та від основного маршрутизатора. Ці комутатори рівня 3 можуть використовувати SVI (комутаційні віртуальні інтерфейси) та маршрутизованими інтерфейси.

На рисунку також показаний класичний випадок використання маршрутизатора з VLAN транкінгом. Віддалені мережі на правій стороні рисунка, можуть мати підключений до WAN маршрутизатор і LAN комутатор. Ці сайти (мережі) можуть використовувати керований ROAS (Router-on-a-Stick), щоб скористатися можливістю

маршрутизатора маршрутизувати дані через магістраль, з підтримкою стандарту 802.1Q.

Комутатор рівня 3 (або багаторівневий комутатор) - це один пристрій, але він виконує логіку на двох рівнях: це комутація локальної мережі 2 рівня і IP-маршрутизація 3 рівня (згідно моделі OSI). Функція комутатора 2 рівня пересилає кадри всередині кожної VLAN, але не пересилає кадри між VLAN. Логіка пересилання (маршрутизації) 3 рівня пересилає IP-пакети між VLAN.

Для підтримки функції комутації 3 рівня потрібен віртуальний інтерфейс, підключений до кожної внутрішньої VLAN налаштованої на комутаторі. Ці інтерфейси VLAN діють як інтерфейси маршрутизаторів з IP-адресою та маскою. Комутатор рівня 3 має таблицю IP-маршрутизації з підключеними маршрутами від кожного з цих інтерфейсів VLAN

1.2 Прості методи захисту

Списки контролю доступу IPv4 (ACL) надають мережевим інженерам можливість запрограмувати фільтри доступу на маршрутизаторі. Кожен маршрутизатор на кожному інтерфейсі як для вхідного, так і для вихідного трафіку може ввімкнути різні ACL за різними правилами. Кожне правило ACL повідомляє маршрутизатору, які пакети блокувати, а які пропускати. ACL складається з ролей і ресурсів. Ресурсами є об'єкти, на які накладаються певні дозволи за допомогою ACL. Ролями є об'єкти, які запитують доступ до ресурсів і отримують відповідь від ACL: дозволено / заборонено.

Списки контролю доступу IPv4 (IP ACL) надають можливість ідентифікувати різні типи пакетів. Для цього в конфігурації ACL перераховуються значення, які маршрутизатор може бачити в заголовках IP, TCP, UDP та інших.

Наприклад, ACL може відповідати пакетам, IP-адреса відправника яких дорівнює 1.1.1.1, або пакетам, IP-адреса призначення яких є адресою в підмережі 10.1.1.0/24, або пакетам із портом призначення TCP-порт 23 (Telnet). ACL (access control list) - механізм для вибору частини з усього потоку трафіку, за заданими критеріями.

Наприклад, через маршрутизатор проходить безліч пакетів, і ACL вибирає тільки ті пакети, які йдуть з мережі 172.16.1.0/24: `access-list 1 permit 172.16.1.0`. Є два способи використання ACL: основний - фільтрація трафіку та другий - використання ACL при налаштуванні NAT. Але не має значення для яких цілей ми використовуємо ACL, правила написання ACL не змінюються.

Маршрутизатори Cisco можуть застосовувати логіку ACL до пакетів у точці, в якій IP-пакети входять в інтерфейс, або в точці, в якій вони виходять з інтерфейсу. Іншими словами, ACL стає пов'язаним з інтерфейсом і напрямком потоку пакетів (вхідний або вихідний). Тобто ACL може бути вхідним та застосованим до маршрутизатора, перш ніж маршрутизатор прийме рішення про пересилання (чи маршрутизацію), або вже вихідним, після того, як маршрутизатор прийме рішення про пересилання та визначить вихідний інтерфейс.

Стрілки на рисунку 1.2 показують місця, в яких можна фільтрувати пакети, які переміщуються зліва направо в наведеній топології. Наприклад, уявіть, що ви хочете дозволити пакети, надіслані хостом А на сервер S1, але відхилити пакети, надіслані хостом В на сервер S1. Кожна лінія зі стрілками позначає розташування та напрямок, у якому маршрутизатор може застосувати ACL, фільтруючи пакети, надіслані хостом В.

Чотири лінії зі стрілками на рисунку вказують на розташування та напрямки інтерфейсів маршрутизатора, які використовуються для пересилання пакета з хоста В на сервер S1.

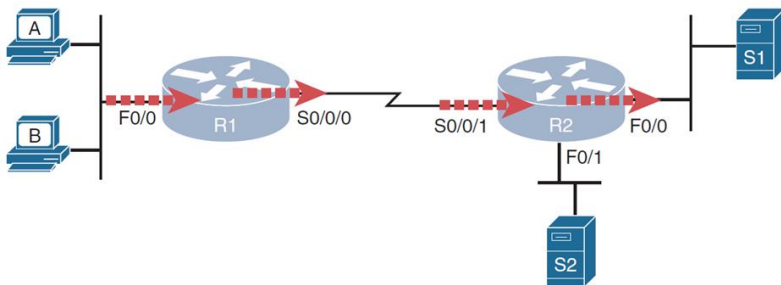


Рисунок 1.2 – Фільтрація пакетів

У цьому конкретному прикладі ці інтерфейси та напрямки є вхідними на інтерфейсі F0/0 маршрутизатора R1, вихідними на інтерфейсі S0/0/0 маршрутизатора R1, вхідними на інтерфейсі S0/0/1 маршрутизатора R2 та вихідними на інтерфейсі F0/0 маршрутизатора R2.

Якщо, наприклад, ви ввімкнули ACL на інтерфейсі F0/1 маршрутизатора R2 в будь-якому напрямку, цей ACL не зможе відфільтрувати пакет, надісланий з хоста В на сервер S1, оскільки інтерфейс F0/1 маршрутизатора R2 не є частиною маршруту від В до сервера S1.

Коротше кажучи, щоб відфільтрувати пакет, ви повинні ввімкнути ACL на інтерфейсі, який обробляє пакет, у тому ж напрямку, в якому пакет проходить через цей інтерфейс.

Якщо ACL ввімкнено, маршрутизатор обробляє кожен вхідний або вихідний IP-пакет за допомогою цього ACL. Наприклад, якщо ввімкнути ACL на маршрутизаторі R1 для пакетів, які надходять на інтерфейс F0/0, то маршрутизатор R1 порівнюватиме кожен вхідний IP-пакет на F0/0 з ACL, щоб вирішити подальшу долю цього пакета: продовжувати з ним працювати чи його потрібно відкинути.

Заборона або доступ мережевого трафіку забезпечуються на підставі аналізу співпадінь зі списком умов і правил, які адміністратор мав задати при налаштуванні ACL. Для цього списки доступу представляються у вигляді послідовних записів, в яких аналізуються один або декілька з наступних параметрів:

- адреса джерела;
- адреса призначення;
- протокол, який використовується;
- номер порту верхнього рівня.

Кожний інтерфейс маршрутизатора може містити окремий список доступу для вхідного та вихідного трафіків і для кожного встановленого мережевого протоколу. Наприклад, на трьох інтерфейсах маршрутизатора з двома мережевими протоколами, IPv4 та IPv6, може бути створено 12 окремих списків доступу: шість для IPv4 і шість для IPv6 - на кожному інтерфейсі по 4 списки: 2 для вхідного і 2 для вихідного трафіку.

Cisco додала багато функцій ACL, зараз вони використовують:

- стандартні нумеровані ACL (1–99);
- розширені нумеровані ACL (100–199);

- додаткові номери для ACL (1300–1999 стандартні, 2000–2699 розширені);

- іменовані ACL;

- покращене редагування за допомогою порядкових номерів.

Крім того, якщо ми тільки створили ACL, то він поки ні на що не впливає. ACL - це просто декілька непрацюючих рядків у конфігурації, до тих пір поки ми його не застосуємо, наприклад, до інтерфейсу або для фільтрації трафіку.

ACL є двох видів: стандартні і розширені. Стандартні дозволяють фільтрувати трафік тільки за одним критерієм: адреса відправника, що є не завжди достатнім.

Для конфігурування стандартних списків управління доступом IP використовуються номери 1-99 або 1300-1999. Але на пріоритет номер списку не має ніякого впливу. Можна, наприклад, поставити на виході з мережі такий ACL:

```
access-list 1 permit host 172.16.10.50
```

```
access-list 1 permit host 172.16.10.53
```

```
access-list 1 permit host 172.16.10.60
```

Цей ACL дозволяє вихід в інтернет тільки з перерахованих трьох ір адрес.

ACL - набір правил. Кожне правило складається з дії (permit, deny) і критерію (для стандартних ACL - ір адреса відправника, для розширених - безліч критеріїв). Розглянемо приклад стандартного нумерованого ACL:

```
access-list 1 permit host 172.16.1.1
```

```
access-list 1 deny 172.16.1.0
```

```
access-list 1 permit any
```

Цей ACL забороняє доступ для мережі 172.16.1.0/24 крім хоста 172.16.1.1 і надає доступ для всіх інших мереж.

Трафік на відповідність ACL перевіряється за рядком. Приходить, наприклад, пакет з адреси 172.16.2.2 на роутер, а на інтерфейсі через який він прийшов стоїть на вхід вказаний вище ACL. IP адреса відправника звіряється з даними ACL - до першого збігу.

Як тільки пакет співпадає з одним із рядків, спрацює дія (permit - пропустити пакет або deny - знищити пакет) і далі ніяких перевірок проводитися не буде. Якщо все рядки пройдено, а пакет так і не потрапив ні під одне з правил, то він за замовчуванням знищується. У нашому випадку будь-який пакет підходить під третій запис (замість адреси вжито слово «any»), будь-яка адреса може бути використана для налаштування мережі.

Наведений ACL можна читати так:

- якщо пакет прийшов з адреси 172.16.1.1 - його треба відразу ж пропустити і не робити більше ніяких перевірок в цьому ACL;
- якщо пакет прийшов з мережі 172.16.1.0 (крім адреси 172.16.1.1), пакет треба знищити і закінчити перегляд ACL;
- якщо пакет не потрапив під перші два правила, він завжди потрапляє під правило permit any, тобто, пакет треба пропустити далі.

Дуже важливо розуміти наведений вище порядок перегляду рядків в ACL, він єдиний для всіх типів ACL (не тільки для стандартного).

Крім того, з цього порядку слідує правило: «У ACL спочатку повинні йти найбільш специфічні, вузькі, точні рядки, а найбільш абстрактні, загальні - в кінці». Якби попередній приклад був би відсортований у зворотному порядку:

```
access-list 1 permit any  
access-list 1 deny 172.16.1.0  
access-list 1 permit host 172.16.1.1
```

То згідно попереднього алгоритму, працює він таким чином. Перевіряємо перший рядок, якщо пакет з будь-якої мережі (any) то його треба пропустити і перегляд далі припинити. Крапка.

На цьому перегляд списку завершено і зовсім неважливо, що написано у другому, третьому і далі рядках, бо весь трафік потрапляє під дію першої команди і на цьому процес роботи ACL завершується.

ACL застосовується для різних цілей, але основна мета - фільтрація трафіку на інтерфейсі.

2 ЛАБОРАТОРНА РОБОТА.

Комутація та налаштування віртуальних локальних мереж

Мета роботи: вивчення основ комутації та налаштування віртуальних локальних мереж. Створення топології на основі комутаторів.

2.1 Побудова моделі мережі

Відкрийте інтегроване середовище моделювання Packet Tracer.

Побудуйте мережу за схемою, представленою на рисунку 2.1, з основними параметрами комутаційного обладнання та інтерфейсів (рис.2.2, 2.3). Для цього виконайте наступні дії.

З панелі приладів в робочу область перенесіть 3 комутатора 2950-24 (для цього на панелі приладів необхідно вибрати перший елемент - Switches (рис.2.4).

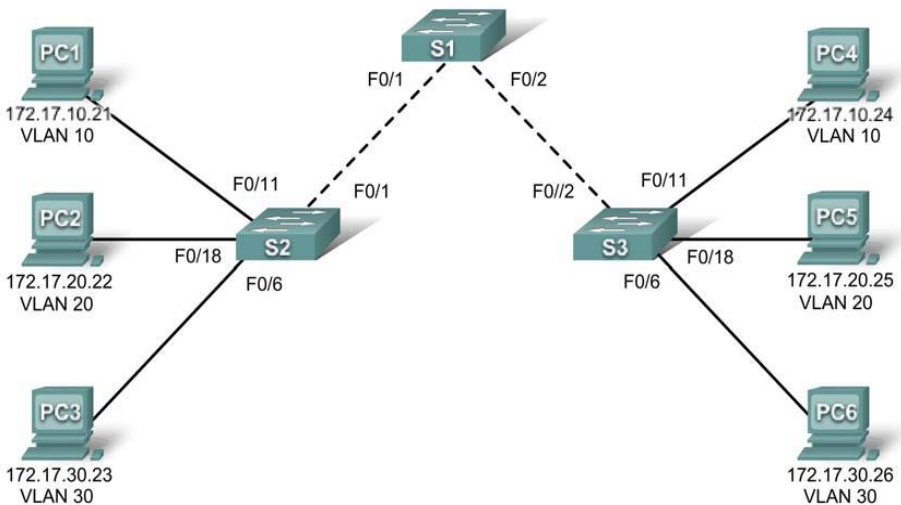


Рисунок 2.1 – Модель мережі

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1

Рисунок 2.2 – Параметри інтерфейсів

Initial Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Рисунок 2.3 – Таблиця віртуальних локальних мереж

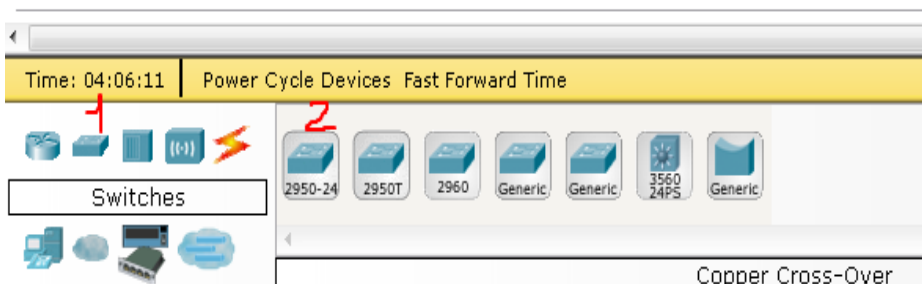


Рисунок 2.4 – Панель обладнання

Додайте 3 комп'ютера (до кожного комутатора) і з'єднайте їх з комутаторами консольним кабелем (комп'ютери знаходяться в розділі End Devices).

Тепер необхідно організувати зв'язок між комп'ютерами і комутаторами, зробимо це за допомогою консольного кабелю. Вибираємо консольний кабель (рис.2.5, елемент 5). На комутаторі вибираємо порт «Console», а на комп'ютері - «RS 232». Але можна це зробити відразу підключивши комп'ютер до комутатора, використовуючи кабель виту пару.

Примітка. Для вибору перехресної або прямої витвої пари необхідно натиснути на елементи 3 або 4 (рис.2.5) відповідно.

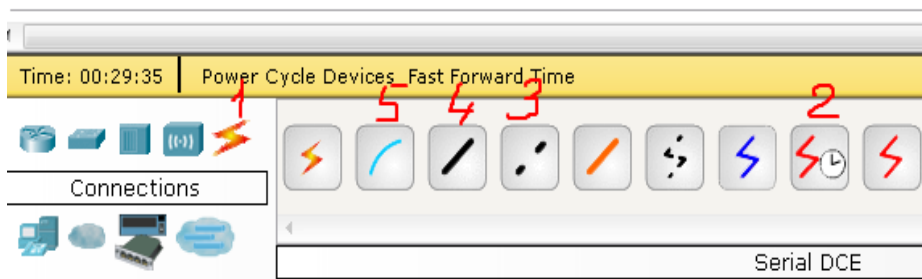


Рисунок 2.5 – Вибір типу кабелю

Для того, щоб з'єднати 2 інтерфейси різних пристроїв виконайте наступне:

- виберіть відповідний кабель, після чого покажчик миші зміниться;
- далі клікнути лівою кнопкою по першому пристрою, який ви хочете підключити;
- у спливаючому вікні клікніть по порту, до якого буде підключено кабель;
- тепер потрібно задати кінцеву точку підключення кабелю: вибираємо наступний пристрій і аналогічно підключаємо порт (рис.2.6).

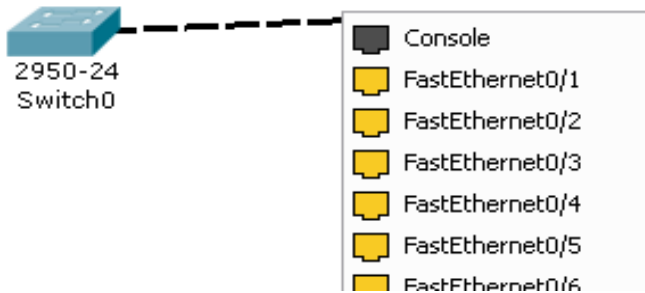


Рисунок 2.6 –Підключення кабелю

Зайдіть в налаштування комутатора у вікно CLI.

Примітка. Всі подальші команди потрібно вводити в цьому вікні – CLI.

Відключіть порти комутаторів, ввівши в кожному терміналі команди:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#exit
```

2.2 Основні налаштування комутаторів

Для того, щоб задати ім'я комутатора S1 вводимо:

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

Аналогічно налаштовуємо імена S2 і S3.

Для того, щоб налаштувати паролі, потрібно ввести наступну частину коду:

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
```

```

S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#enable secret class

```

Таким же чином налаштовуються паролі на комутаторах S2, S3. Включаємо інтерфейси на комутаторах S2 і S3 і переводимо їх в режим доступу.

У режим доступу переводяться інтерфейси, до яких безпосередньо підключені комп'ютери. Для цього в терміналі вводимо:

```

S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode access
S2(config-if-range)#no shutdown

```

2.3 Настроювання VLAN

Створити на комутаторі S1 VLAN-и і задати їм імена відповідно рисунку 2.3.

```

S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#end

```

Примітка. Перевірити настройку можна командою S1 **#show vlan brief**

Аналогічно налаштовуємо віртуальні локальні мережі.

Призначити VLAN-ам порти комутаторів S2 і S3.

```

S2(config)#interface range fa0/6-10
S2(config-if-range)#switchport access vlan 30
S2(config-if-range)#interface range fa0/11-17
S2(config-if-range)#switchport access vlan 10

```

```
S2(config-if-range)#interface range fa0/18-24
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#end
```

Аналогічно налаштовуємо S3.

Призначити management VLAN.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown.
```

Примітка. Таким же чином проводиться налаштування комутаторів S2 і S3 (згідно з таблицею IP-адрес, рис. 2.2).

Налаштування магістральних VLAN-ов на всіх комутаторах.

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end
```

Таке ж налаштування робимо і на інших комутаторах.

Примітка. Перевірка виконується командою **S1#show interface trunk**.

2.4 Індивідуальне завдання

Побудуйте мережу. Для цього необхідно:

- додати до кожного комутатора ще один комп'ютер (порт згідно з таблицею 2.1). Перевести підключений порт в режим доступу на всіх комутаторах;
- створити додаткову віртуальну локальну мережу (VLAN). В якості імені VLAN-а використовувати своє прізвище;
- додати ще один комутатор (**ім'я комутатора**);
- з'єднати інтерфейс fa0/1 доданого комутатора з інтерфейсом fa0/5 комутатора S1;
- налаштувати VLAN-и і інтерфейси доданого комутатора так само, як виконано налаштування на інших комутаторах вашої топології;
- додати IP-адресу на VLAN 99 нового комутатора (**IP-адреси**);

– додати ще один комп'ютер і підключити його до інтерфейсу доданого вами VLAN-а комутатора;

– коротко законспектувати хід роботи і записати таблицю VLAN-ов доданого комутатора.

–

Таблиця 2.1 – Варіанти завдань

№ вар.	Порт	VLAN	Ім'я комутатора	IP-адреса
1	2	3	4	5
1.	19	101	S11	172.17.99.21/24
2.	20	102	S12	172.17.99.22/24
3.	21	103	S13	172.17.99.23/24
4.	22	104	S14	172.17.99.24/24
5.	23	105	S15	172.17.99.25/24
6.	24	106	S16	172.17.99.26/24
7.	19	107	S17	172.17.99.27/24
8.	20	108	S18	172.17.99.28/24
9.	21	109	S19	172.17.99.29/24
10.	22	110	S20	172.17.99.30/24
11.	23	111	S21	172.17.99.31/24
12.	24	112	S22	172.17.99.32/24
13.	19	113	S23	172.17.99.33/24
14.	20	114	S24	172.17.99.34/24
15.	21	115	S25	172.17.99.35/24
16.	22	116	S26	172.17.99.36/24
17.	23	117	S27	172.17.99.37/24
18.	24	118	S28	172.17.99.38/24
19.	19	119	S29	172.17.99.39/24
20.	20	120	S30	172.17.99.40/24
21.	21	121	S31	172.17.99.41/24
22.	22	122	S32	172.17.99.42/24
23.	23	123	S33	172.17.99.43/24
24.	24	124	S34	172.17.99.44/24
25.	19	125	S35	172.17.99.45/24

2.5 Зміст звіту

1. Хід роботи.
2. Індивідуальна схема з зазначенням конфігурації інтерфейсів.
3. Відповіді на контрольні питання.

2.6 Контрольні питання

1. Чим відрізняється комутатор від маршрутизатора?
2. Що таке маршрутизовані комутатори?
3. На якому рівні OSI працює комутатор?
4. Що таке VLAN?
5. Для чого використовується VLAN?
6. Пропінгуйте з PC1 комп'ютери PC4, PC5 і PC6. Результат запишіть у звіт і поясніть.

3 ЛАБОРАТОРНА РОБОТА. Стандартні списки контролю доступу

Мета роботи: навчитися безпечної маршрутизації трафіку при налаштуванні списків контролю доступу в комп'ютерних мережах.

3.1 Rip маршрутизація та ACL

Для початку в середовищі моделювання Packet Tracer треба зібрати схему з трьох маршрутизаторів (рис.2.1). При моделюванні можна використовувати маршрутизатор моделі 1841 (вказано на схемі).

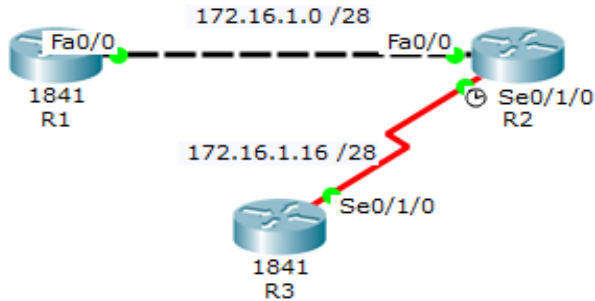


Рисунок 3.1 – Модель мережі

До R2 та R3 маршрутизатора додаємо додаткові плати з Serial портами (WIC-2T).

Примітка. Обов'язково виключаємо маршрутизатори при встановленні нових плат.

Далі призначимо адреси інтерфейсів згідно таблиці 3.1. При налаштуванні Serial портів не забувайте задати значення синхронізації (наприклад 64000).

Таблиця 3.1 – Налаштування

	R1	R2	R3
Ethernet порти	172.16.1.2 /28	172.16.1.1 /28	
Serial порти		172.16.1.17 /28	172.16.1.18 /28

Здійснимо конфігурацію RIP маршрутизації на всіх маршрутизаторах, за допомогою налаштування у вкладці CLI або Config RIP.

Для Router1

```
Router1(config)#router rip
Router1(config- router)#version 2
Router1(config- router)#network 172.16.0.0
```

Для Router2

```
Router2(config)#router rip
Router2(config- router)#version 2
```

```
Router2(config-router)#network 172.16.0.0
```

Для Router3

```
Router3(config)#router rip
```

```
Router3(config-router)#version 2
```

```
Router3(config-router)#network 172.16.0.0
```

Перевіримо дієздатність мережі за допомогою команди ping (можливість пінгувати інтерфейс Ethernet0/0 (172.16.1.2) Router1 з Router3).

```
Router3#ping 172.16.1.2
```

Успішна відповідь є такою:

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms.

Створимо стандартний список доступу, який не дозволить пінгувати маршрутизатор 1 з маршрутизатора 3.

Для цього блокуємо єдину адресу 172.16.1.18 маршрутизатора 3 і дозволимо інший трафік. Список створимо на маршрутизаторі 1 наступними командами:

```
Router1(config)#access-list 1 deny 172.16.1.18 0.0.0.0
```

```
Router1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
```

Застосуємо список до інтерфейсу Ethernet маршрутизатора 1

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

```
Router1(config-if)#ip access-group 1 in
```

Перевіримо, що список доступу запущено. Для цього переглянемо працюючу конфігурацію

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

```
Router1#show ip interface
```

Можемо бачити, що список застосовано до інтерфейсу, використовуючи команду "show ip interface".

Знайдіть в виведеній інформації рядок з "Innbound access list is 1". Команда "show access-lists" покаже нам вміст створеного списку доступу.

Router1#show access-lists

Standard IP access list 1

10 deny host 172.16.1.18

20 permit any (4 match (es))

host 172.16.1.18 теж саме 172.16.1.18 0.0.0.0.

Тепер при спробі пінгувати інтерфейс Ethernet (172.16.1.2) маршрутизатора 1 з маршрутизатора 3:

Router3#ping 172.16.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:

UUUUU

Success rate is 0 percent (0/5)

Отримали рядок "UUUUU", який означає, що список доступу є коректним.

3.2 OSPF та стандартний ACL

Створимо і завантажимо в симулятор топологію з рисунку 3.2, Призначимо адреси інтерфейсів згідно з таблицею 3.2.

Примітка. Уважно перевіряйте реальні порти, в реальних мережах.

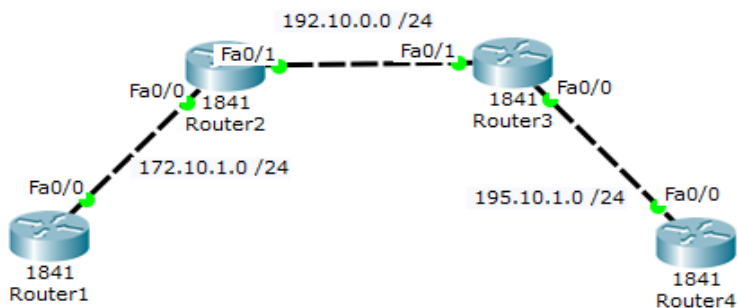


Рисунок 3.2 – Модель мережі

Таблиця 3.2 – Налаштування

	Router1	Router2	Router3	Router4
Ea0/0	172.10.1.2	172.10.1.1	195.10.1.2	195.10.1.1
Ea0/1		192.10.0.1	192.10.0.2	

Виконуємо налаштування конфігурації OSPF маршрутизації.

Для Router1

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

Router1(config- router)#**network 172.10.1.0 0.0.0.255 area 0**

Вийти з режиму налаштування командою: > **end** та зберегти зміни командою: > **write**.

Для Router2

Router2(config)#**router ospf 1**

Router2(config- router)#**network 172.10.1.0 0.0.0.255 area 0**

Router2(config- router)#**network 192.10.0.0 0.0.0.255 area 0**

Вийти з режиму налаштування командою: > **end** та зберегти зміни командою: > **write**.

Для Router3

Router3(config) #**router ospf 1**

Router3(config- router)#**network 192.10.0.0 0.0.0.255 area 0**

Router3(config- router)#**network 195.10.1.0 0.0.0.255 area 0**

Вийти з режиму налаштування командою: > **end** та зберегти зміни командою: > **write**.

Для Router4

Router4(config) #**router ospf 1**

Router4(config- router)#**network 195.10.1.0 0.0.0.255 area 0**

Вийти з режиму налаштування командою: > **end** та зберегти зміни командою: > **write**.

Для перевірки пропінгуйте крайні точки.

Router1 #**ping 195.10.1.1**

Router4 #**ping 172.10.1.2**

Створимо стандартний список доступу для фільтрації трафіку, що приходить на інтерфейс 172.10.1.1 router2 і дозволяє трафік від мережі 192.10.0.0 (router3) і блокує трафік від інших пристроїв.

```
Router2 (config) #access-list 1 permit 192.10.0.0 0.0.0.255
```

Перевірте, що він створився

```
Router2#show access-list
```

```
Standard IP access list 1
```

```
permit 192.10.0.0 0.0.0.255
```

Приєднайте список як вхідний до інтерфейсу Ethernet 1.

```
Router2 (config) #interface FastEthernet0/1
```

```
Router2 (config-if) #ip access-group 1 in
```

Перевірте приєднання командою

```
Router2 #show running-config
```

Перевірте зв'язок між 3 і 1 маршрутизаторами та між 4 і 1.

```
Router3 #ping 172.10.1.2
```

```
Router4 #ping 172.10.1.2
```

Зв'язок між 3 і 1-м роутерами повинен бути, а між 4 і 1 - ні.

Змінимо список доступу - дозволимо трафік від мережі 195.10.1.0 (R4) і заблокуємо трафік від інших пристроїв.

```
Router2 (config) #no access-list 1 permit 192.10.0.0 0.0.0.255
```

```
Router2 (config) #access-list 1 permit 195.10.1.0 0.0.0.255
```

Перевірте, що він змінився

```
Router2 #show access-list
```

```
Standard IP access list 1
```

```
permit 195.10.1.0 0.0.0.255
```

Від'єднайте список як вхідний до інтерфейсу Ethernet 1

```
Router2(config)#interface FastEthernet0/0
```

```
Router2(config-if)#no ip access-group 1 in
```

Приєднайте список як вихідний до інтерфейсу Ethernet 0

```
Router2(config)#interface FastEthernet0/0
```

Router2(config-if)#**ip access-group 1 out**

Перевірте приєднання командою

Router2#**show running-config**

Перевірте зв'язок між 3 і 1 маршрутизаторами та між 4 і 1.

Router3#**ping 172.10.1.2**

Router4#**ping 172.10.1.2**

Зв'язок між 4 і 1-м роутерами повинен бути, а між 3 і 1 - ні.

3.3 Міжмережні налаштування ACL

Здійснить і перевірте конфігурацію IP для мережі на рисунку 3.3 (табл. 3.3) і застосуєте OSPF для організації динамічної маршрутизації.

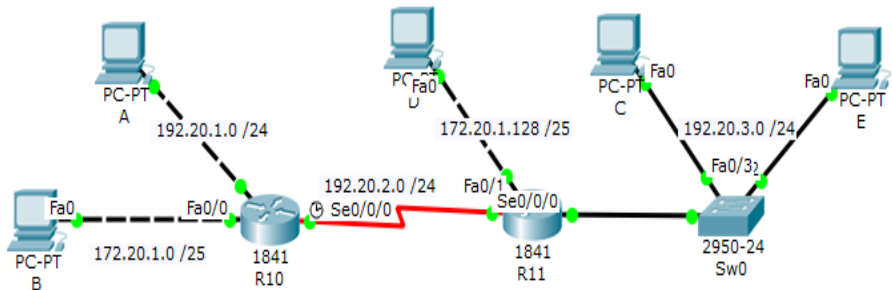


Рисунок 3.3 – Модель мережі

Таблиця 3.3 – Налаштування

	Ea0/0	Ea0/1	S0/0/0	Ea0
R10	172.20.1.1/25	192.20.1.1/24	192.20.2.1/24	
R11	192.20.3.1/24	172.20.1.129/25	192.20.2.2/24	
PC A				192.20.1.2 /24
PC B				172.20.1.2 /25
PC C				192.20.3.2 /24
PC D				172.20.1.130 /25
PC E				192.20.3.3 /24

Для маршрутизатора R10

```
Router10 (config)#router ospf 1
Router10 (config-router)#network 192.20.1.0 0.0.0.255 area 0
Router10 (config-router)#network 192.20.2.0 0.0.0.255 area 0
Router10 (config-router)#network 172.20.1.0 0.0.0.127 area 0
```

Вийти з режиму налаштування командою: > **end** та зберегти зміни командою: > **write**.

Для маршрутизатора R11

```
Router11(config)#router ospf 1
Router11(config-router)#network 172.20.1.128 0.0.0.127 area 0
Router11(config-router)#network 192.20.3.0 0.0.0.255 area 0
Router11(config-router)#network 192.20.2.0 0.0.0.255 area 0
```

Вийти з режиму налаштування командою: > **end** та зберегти зміни командою: > **write**.

Перевірте працездатність мережі: ви повинні з будь-якого пристрою пінгувати будь-який інтерфейс. Або простіше: всі комп'ютери А, В, С, D, Е повинні взаємно попарно пінгуватись.

Далі налаштуємо списки контролю доступу.

Спочатку виконаємо налаштування на маршрутизаторі R10.

```
Router10 (config)#access-list 2 deny 172.20.1.128 0.0.0.127
Router10 (config)#access-list 2 permit host 192.20.3.2
Router10 (config)#access-list 2 deny 192.20.3.0 0.0.0.255
Router10 (config)#access-list 2 permit 0.0.0.0 255.255.255.255
```

і застосуємо його до інтерфейсу Еа0/0 як вихідний

```
Router10 (config)#interface FastEthernet0/0
Router10 (config-if)#ip access-group 2 out
```

Створити скріншот результату виконання команди

Router10#**show access-list**

Після успішного виконання команди отримали наступні рядки.

Standard IP access list 2

10 deny 172.20.1.128 0.0.0.127

20 permit host 192.20.3.2

30 deny 192.20.3.0 0.0.0.255

40 permit any

Попарно пропінгуємо А, В, С, Е, D. У результаті отримали наступну схему доступу 1 (табл. 3.4).

Таблиця 3.4 – Схема доступу 1

	A	B	C	E	D
A	+	+	+	+	+
B	+	+	+	-	-
C	+	+	+	+	+
E	+	-	+	+	+
D	+	-	+	+	+

Бачимо, що політика безпеки повністю реалізована для РС з ідентифікатором В.

Тепер трафік між мережами 172.20.1.0/25 і 172.20.1.128/25 заборонено. Неможливий також трафік між мережею 172.20.1.0/25 і мережею 192.20.3.0/24 за винятком комп'ютера С з адресою 192.20.3.2/24.

Вилучимо ACL с інтерфейсу ea0/0 і застосуємо як вхідний до інтерфейсу s0/0/0.

Router10(config)#**interface fa0/0**

Router10(config-if)#**no ip access-group 2 out**

Router10(config-if)#**int s0/0/0**

Router10(config-if)#**ip access-group 2 in**

Попарно пропінгуєм А, В, С, Е, D.

У результаті отримали наступну схему доступу 2 (табл. 3.5).

Таблиця 3.5 – Схема доступу 2

	A	B	C	E	D
A	+	+	+	-	-
B	+	+	+	-	-
C	+	+	+	+	+
E	-	-	+	+	+
D	-	-	+	+	+

Політика безпеки тепер повністю реалізована і для РС з ідентифікатором А.

Тепер трафік також заборонено між мережами 192.20.1.0/24 і 172.20.1.128/25. Неможливий також трафік між мережею 192.20.1.0/25 і мережею 192.20.3.0/24 за винятком комп'ютера С з адресою 192.20.3.2/24.

3.4 Самостійне завдання

Виконання даного завдання є обов'язковим при зарахуванні цієї лабораторної роботи.

Використовуючи модель мережі міжмережного налаштування ACL (рис.2.3), додайте та підключить до маршрутизатора R11 додатковий маршрутизатор R12. Якщо треба додайте плату до R12 та ще одну плату до R11.

До маршрутизатора R12 підключить ноутбук або РС (назва – перша літера прізвища студента англійською і номер у списку групи (Приклад. Василенко (№ за списком 12) **V12**)).

Адреса мережі між R11 та R12 – 10.(номер студента у списку групи).1.0 маска /28 – (приклад:10.12.1.0/28).

Адреса локальної мережі R12 - ноутбук – 10.(номер студента у списку групи).1.16 маска /28 – (приклад:10.12.1.16/28).

Створити список ACL, який дозволить доступ пакетів к ноутбуку тільки з комп'ютерів А та Е.

З усіх інших пристроїв доступ закрити.

3.5 Зміст звіту

- хід роботи;
- налаштування;
- схеми мереж;
- відповіді на контрольні питання.

3.6 Контрольні питання

1. Наведіть визначення ACL?
2. Види та типи ACL. Їх характеристики.
3. Загальні команди налаштування стандартних ACL?
4. Які номери використовуються для налаштування стандартних списків контролю доступу?
5. Сформулюйте загальне правило порядку перегляду списків контролю лоступу. Його особливості.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Odom, W. CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. 2019.
2. Odom, W. CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press. 2019.
3. Киричек Г.Г. Конспект лекцій з дисципліни «Комп'ютерні мережі» для студентів спеціальності 123 Комп'ютерна інженерія, усіх форм навчання. Запоріжжя: Національний університет «Запорізька політехніка», 2024. 58 с.
4. Киричек Г.Г. Методичні вказівки до проходження тестування з дисципліни "Комп'ютерні мережі" для студентів спеціальності 123 Комп'ютерна інженерія, усіх форм навчання. Частина 1. Запоріжжя: Національний університет «Запорізька політехніка», 2024. – 30 с
5. Киричек Г.Г. Методичні вказівки до проходження тестування з дисципліни "Комп'ютерні мережі" для студентів спеціальності 123 Комп'ютерна інженерія, усіх форм навчання. Частина 2. Запоріжжя: Національний університет «Запорізька політехніка», 2024. – 30 с.
6. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 1. Навчальний посібник. 2020.
7. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 2. Навчальний посібник. 2020.
8. Блозва А.І. Комп'ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька. К.: Компрінт, 2017.
9. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. 2nd Edition. USA: Cisco Press, 2015. 578 p.
10. Tulloch M., Team WS Introducing Windows Server 2012 R2. - Microsoft press, 2013.
11. Krause J. Mastering Windows Server 2016. - Packt Publishing Ltd, 2016.
12. IT Блог Тараса Кучинського. Знайомство з програмою "Cisco packet tracer". URL: <https://kychinskiy.blogspot.com/2017/12/cisco-packet-tracer.html>