ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ

Л.В. Бубенцова

ТЕХНОЛОГІЇ IP-МЕРЕЖ

Методичний посібник

Одеса
«ДУІТЗ»
2025

УДК 004.7

Автори:
Бубенцова Л.В., к.т.н., старший викладач кафедри комп'ютерної інженерії та інформаційних систем Державного університету інтелектуальних технологій і зв'язку

Рецензенти:
Корчинський В.В., д.т.н., професор кафедри кібербезпеки та технічного захисту інормації Державного університету інтелектуальних технологій і зв'язку;
Генсерук Г.Р., к.т.н., доц., декан фізико-математичного факультету Тернопільського національного педагогічного університету ім. В. Гнатюка.

Рекомендовано до друку Навчально-методичною Радою
Державного університету інтелектуальних технологій і зв'язку
(протокол № 3 від 13.12 2024 р.)

Технології IP-мереж: методичний посібник. [для здобувачів першого (бакалаврський) рівня вищої освіти галузі знань F «Інформаційні технології»] / Уклад. Л.В. Бубенцова. Одеса: ДУІТЗ, (Електр. вид. https://metod.suitt.edu.ua), 2025. 57 с.

Матеріал присвячений практичним аспектам побудови стабільних, прогнозованих, захищених сегментів IP-мережі. Висвітлюються короткі теоретичн відомості; приклади команд конфігурування протоколів для реалізації відповідної функції обладнання; питання для самоконтролю та варіанти індивідуальних завдань для виконання робіт. Буде корисним для всіх, хто прагне розібратися в розв'язанні спеціалізованих задач та практичних проблем під час створення, модернізації, забезпечення стабільних сегментів IP-мереж з затребуваними показниками якості обслуговування.

ЗМІСТ

ЛАБОРАТОРНА РОБОТА №1 ……..4

ЛАБОРАТОРНА РОБОТА №2 ……..14

ЛАБОРАТОРНА РОБОТА №3 ……..26

ЛАБОРАТОРНА РОБОТА №4 ……..36

ЛАБОРАТОРНА РОБОТА №5 ……..42

ЛАБОРАТОРНА РОБОТА №6 ……..49

ЛАБОРАТОРНА РОБОТА №1

Вивчення і налаштування базових параметрів комутатора

Мета роботи

1.Вивчення базових параметрів комутатора локальної мережі.
2.Набуття практичних навичок конфігурування базових параметрів комутатора.

Ключові положення

Комутатор та його складові

Комутатори – це пристрої, які використовуються для підключення кількох пристроїв до однієї мережі. У правильно спроектованій мережі комутатори локальної мережі відповідають за напрямок потоку даних та керування ним на рівні доступу до мережевих ресурсів.

Комутатор дуже схожий з комп'ютером, він також є електронно-обчислювальною машиною, яка має ті ж основні складові для роботи, а саме:

– Центральний процесор (ЦП) – який виконує обробку даних машинного коду.

– Блок живлення (БП) – для забезпечення живлення складових комутатора.

– Материнська плата – використовується для підключення всіх складових через порти, а також від блока живлення.

– Постійна пам'ять, ROM (Read Only Memory) – використовується для зберігання завантажувального програмного забезпечення.

– Енергонезалежна пам'ять, NVRAM (Non Volatile Random Access Memory) – зберігає стартову конфігурацію.

– Флеш-пам'ять (flash memory) – містить операційну систему (ОС) комутатора IOS. IOS копіюється з флеш-пам'яті під час процесу завантаження. Flash-пам'ять є незалежною і не втрачає свій вміст, коли живлення вимикається . На рис. 2.1 подано приклад вигляду флеш пам'яті комутаторів cisco розміром 4 GB.

Рисунок 2.1 – Флэш-пам'ять cisco 4 GB

– Пам'ять, що оперативно запам'ятовує, RAM (Random Access Memory), – містить у собі запущені процеси, такі як: підвантажений з NVRAM файл стартової конфігурації (startup configuration), який буде поточною конфігурацією (running configuration); підвантажену із флеш-пам'яті ОС IOS; таблицю комутації, таблицю ARP та ін. таблиці.

– Інтерфейси для підключення консольного дроту, якими можуть виступати RJ45, RS-232, mini-USB, зазвичай виділені блакитним кольором .

Примітка: Консольний порт – це порт керування, який дає змогу скористатися бездротовим доступом до пристрою Cisco. Бездротовий доступ – це доступ через виділений адміністративний канал, який використовується виключно для технічного обслуговування пристрою.

– Інтерфейси для підключення комутатора до мережі, якими можуть виступати serial, Fast/Gigabit Ethernet та оптичні порти.

– Роз'єми для підключення модулів із додатковими інтерфейсами підключення до мережі. На рис.2.2 наведено приклад модуля з додатковими інтерфейсами комутатора Cisco Catalyst WS 2960-24 TC-L.

Рисунок 2.2 – VIC модуль

На передній панелі комутатора розташовані світлодіодні індикатори його стану. Комутатори Cisco Catalyst оснащені кількома індикаторами стану. Індикатори стану комутатора дозволяють швидко та легко відстежувати активність та продуктивність комутатора. Комутатори різних моделей та з різними функціями оснащені різними індикаторами, їхнє розташування на передній панелі також може відрізнятися.

На рис. 2.3 показаний зовнішній вигляд комутатора Cisco C1000-24P-4X-L.

Рисунок 2.3 – Комутатор Cisco C1000-24P-4X-L

Кнопка режиму (Mode) використовується для перемикання стану порту, дуплексного режиму порту, швидкості порту та стану PoE (якщо ця функція підтримується) на індикаторах портів. Нижче описується призначення світлодіодних індикаторів та значення їх кольорів.

Світлодіодний індикатор (SYST) вказує, чи отримує система живлення та чи працює вона нормально. Якщо індикатор не світиться, система вимкнена. Якщо індикатор горить зеленим

світлом, система працює нормально. Якщо індикатор світиться жовтим, система отримує живлення, але працює з перебоями.

Індикатор системи резервного живлення (RPS) відображає стан RPS. Якщо цей індикатор не світиться, RPS вимкнено або підключено неправильно. Якщо індикатор горить зеленим, то RPS підключена та готова до забезпечення резервного живлення. Якщо індикатор блимає зеленим, то RPS підключено, але недоступне, оскільки забезпечує живлення іншого пристрою. Якщо індикатор світиться жовтим, RPS знаходиться в режимі очікування або несправно. Якщо індикатор блимає жовтим, то внутрішнє джерело живлення комутатора не працює і задіяне джерело резервного живлення.

Індикатор стану порта (STAT) вказує на вибраний режим стану порту. Цей режим є стандартним режимом. При виборі відповідної функції світлодіодні індикатори порту відображатимуть кольори з різними значеннями. Якщо індикатор вимкнено, зв'язок відсутній або порт вимкнено адміністратором. Якщо індикатор горить зеленим, зв'язок є. Якщо індикатор блимає зеленим, це свідчить про активність порту, і він надсилає або отримує дані. Якщо колір індикатора чергується між зеленим та жовтим, то зв'язок порушений. Якщо індикатор горить жовтим, порт заблокований для перевірки домену пересилання на наявність петлі, що пересилає дані (зазвичай порти знаходяться в цьому стані протягом перших 30 секунд після активації). Якщо індикатор блимає жовтим, порт заблоковано, щоб запобігти можливій петлі в домені пересилання.

Індикатор дуплексного режима порта (DUPLX) вказує на вибраний дуплексний режим порту. Індикатор дуплексного режиму порту вимкнено, якщо порт працює у напівдуплексному режимі. Якщо індикатор порту світиться зеленим, порт знаходиться в повнодуплексному режимі.

Індикатор швидкості портів (SPEED) вказує на вибраний режим швидкості портів. При виборі відповідної функції світлодіодні індикатори порту відображатимуть кольори з різними значеннями. Якщо індикатор вимкнено, порт працює на швидкості 10 Мбіт/с. Якщо індикатор горить зеленим, порт працює на швидкості 100 Мбіт/с. Якщо індикатор блимає зеленим, порт працює на швидкості 1000 Мбіт/с.

Індикатор режима живлення через Ethernet (PoE) – цей індикатор є, якщо підтримується PoE. Якщо індикатор вимкнено, режим PoE не вибраний, живлення або функціональність портів не порушено. Якщо індикатор блимає жовтим, то режим PoE не вибраний, але принаймні живлення одного з портів порушено або виник збій у роботі PoE. Якщо індикатор горить зеленим, то вибрано режим PoE, і індикатори порту відображатимуть кольори з різними значеннями. Якщо цей індикатор не світиться, то PoE також вимкнено. Якщо індикатор світиться зеленим, PoE функціонує. Якщо колір індикатора чергується між зеленим та жовтим, то PoE був вимкнений, оскільки подача живлення пристрою зі справним живленням може перевищити допустиму потужність комутатора. Якщо індикатор блимає жовтим, то PoE вимкнено через неполадки. Якщо індикатор горить жовтим, PoE для порту було вимкнено.

Функціональна структура пам'яті, інтерфейсів комутатора та розташування файлів у структурі представлені на рис 2.4.

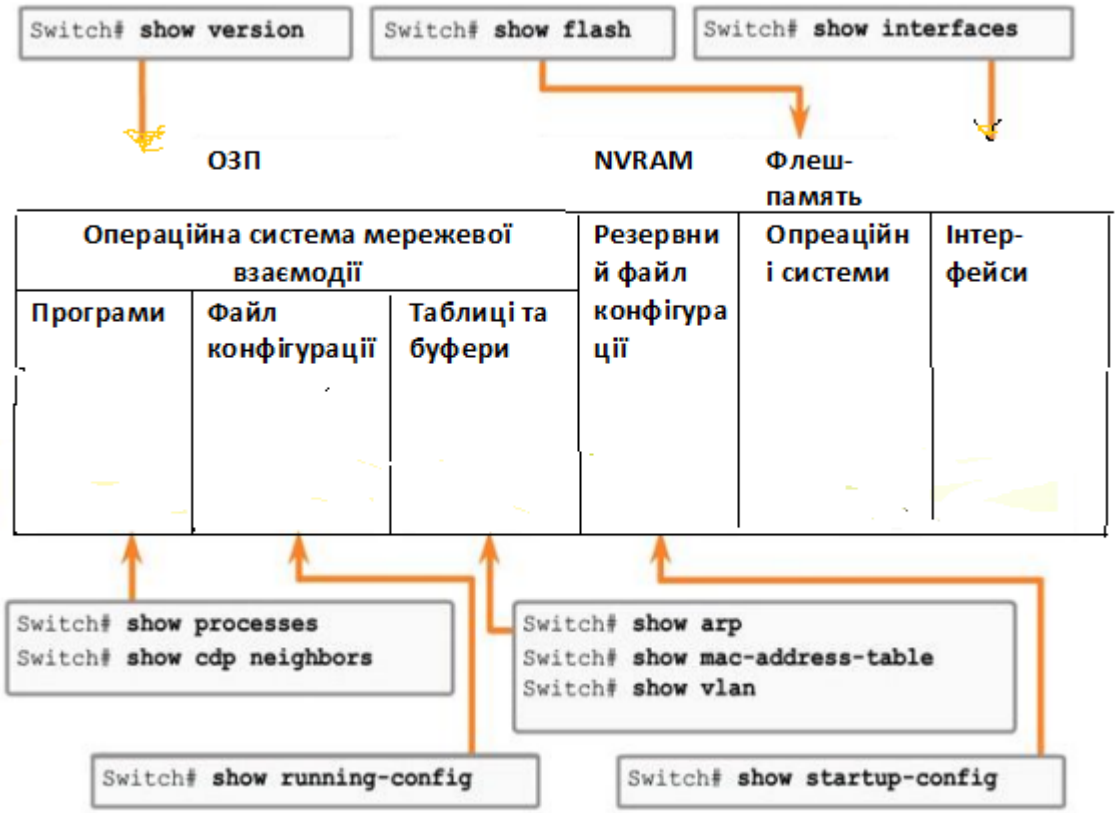

Рисунок 2.4 – Функціональна структура пам'яті, інтерфейсів комутатора та розташування файлів у структурі

Домашнє завдання

1. Вивчіть, використовуючи цей методичний посібник, принцип роботи комутатора, алгоритм базової настройки конфігурації комутатора Cisco, алгоритм налаштування функцій безпеки

2.Складіть план виконання лабораторної роботи, керуючись п.5.

Завдання до лабораторної роботи:

У робочій області Cisco Packet Tracer створити мережу, згідно з топологією, представленою на рис.5.1.

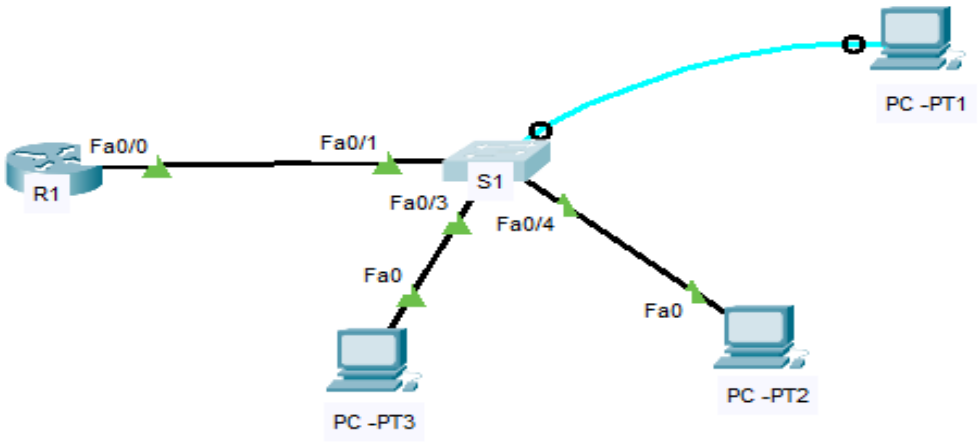

Рисунок 5.1–Топологія мережі

Необхідне обладнання:

1 маршрутизатор Cisco XXXX з Cisco IOS.

1 комутатор Cisco XXXX з Cisco IOS.

1 компютер (PC-PT на базі Windows 10 з програмою емуляції терминалу, такий наприклад, як Tera Term).

Консольні кабелі для конфігурування пристроїв Cisco IOS через консольний порт.

Кабелі Ethernet для підєднання пристроїв згідно топології.

Примітка: Параметр X в схемі мережі оберіть згідно варіанту, наданого викладачем. Перевірте, чи маршрутизатор і комутатор не мають початкової конфігурації, записаної у файлі startup. Якщо не знаєте, як це зробити, зверніться до викладача.

Таблиця 5.1 – Адресна схема мережі

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.10.1	255.255.255.0	N/A
S1	VLAN 99	192.168.10.10	255.255.255.0	192.168.10.1
PC-PT	NIC	192.168.10.2	255.255.255.0	192.168.10.1

Частина 1 Аналіз встановленої (default)-конфигурації комутатора

Крок 1: Вхід в привілейований режим

Ви можете отримати доступ до всіх команд конфігурування комутатора, увійшовши до привілейованого режиму. Привілейований режим має бути захищений паролем для запобігання несанкціонованому доступу.

a. Клікніть на S1, далі на вкладці CLI і нажміть клавішу .
b. Увійдіть привілейований режим EXEC шляхом введення команди enable:
Switch> enable
Switch#

Крок 2: Аналіз поточної конфигурації комутатора

a. Уведіть команду

Switch# show running-config

b. Проаналізуйте Default-конфігурацію комутатора:
Скільки інтерфейсів FastEthernet та Gigabit Ethernet має комутатор?
Скільки віртуальних інтерфейсів має комутатор?
Яка IP-адреса у інтерфейсу Vlan1? Чи активний цей інтерфейс?

Щоб переглянути версію Cisco IOS, введіть команду

Switch# show version

Номер версії Cisco IOS, встановленої в комутаторі, обсяг флеш-пам'яті, MAC-адресу комутатора та кількість інтерфейсів FastEthernet та Gigabit Ethernet відобразіть у протоколі.

Частина 2 Налаштування базових параметрів комутатора

У 2-й частині необхідно налаштувати базові параметри комп'ютера, маршрутизатора та комутатора для роботи в IP-мережі.

Крок 1: Налаштування IP-протокола в комп'ютері PC-PT

Крок 2: Налаштування базових параметрів маршрутизатора
Надайте маршрутизатору ім'я R1, налаштуйте IP-адресу інтерфейсу F0/0, відповідно до таблиці адрес.

Крок 3: Конфігурування базових параметрів комутатора

3.1 Увійдіть в режим глобального конфігурування комутатора:

Switch# configure terminal

3.2 Привласніь комутатору им'я:

Switch(config)# hostname S1

3.3 Створіть віртуальну локальну мережу для трафіку керування з ім'ям Management

S1(config)#vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit

Конфігуруйте IP-адресу інтерфейсу vlan 99 та активуйте її:

S1(config)#interface vlan 99
S1(config-if)#ip address 192.168.10.10 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end

3.7 Виконайте команди **show vlan, show ip interface brief**, проаналізуйте статус vlan 99 та інтерфейсу vlan 99. Чому протокол не активний, незважаючи на те, що було введено команду no shutdown для інтерфейсу vlan 99? Результати аналізу занесіть у протокол.

3.8 Призначте порти f0/1, f0/2 комутатора для vlan 99.

S1# configure terminal
S1(config)#interface f0/1
S1(config-if)#switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# interface f0/2
S1(config-if)#switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)#end

Виконайте команду **show ip interface brief**.
Яким є статус протоколу на інтерфейсі vlan 99? Результати аналізу занесіть у протокол.

Крок 4: Конфігурування банера

Cisco IOS включає команду налаштування банера – повідомлення, яке інформує про правові наслідки несанкціонованого доступу. Для створення банера використовуйте команди

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

Крок 5: Перевірка зв'язку між пристроям

5.1 Виконайте команду ping від PC-A за адресою стандартного шлюзу.
5.2 Виконайте команду ping від PC-A на адресу мережі управління комутатора S1.
5.3 Виконайте команду ping від комутатора за адресою стандартного шлюзу.
5.4 Результати занесіть у протокол.
5.5 Відкрийте Web-браузер у комп'ютері PC-A та введіть адресу: http://192.168.10.10 .

Частина 3 Конфігурування і перевірка протокола SSH на S1

Крок 1: Для конфігурування протоколу SSH необхідно вказати ім'я домену

S1(config)#**ip domain name Lab.com**

Крок 2: Сформувати базу даних користувачів, які мають право на віддалений доступ

S1(config)#**username admin privilege 15 secret sshprotocol**
S1(config)# **username student password lab4**

Крок 3: Конфігурувати віртуальні лінії vty для дозволу тільки ssh-з'єднання та використовувати локальну базу даних пристрою для аутентифікації

S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit

Крок 4: Згенерувати пари ключів для шифрування

S1(config)#crypto key generate rsa Modulus 1024
S1(config)#end

Крок 5: Корегування конфигурації ssh

Відкоригуйте кількість дозволених спроб аутентифікації та тайм-аут між ними

S1#config t
S1(config)#ip ssh time-out 75
S1(config)#ip ssh authentication-retries 2

Крок 6 Перевірка звязків

У PC-PT використовуйте програму ssh-client, таку як Putty (Tera Term), щоб відкрити ssh-сесію до S1.

Частина 4 Перевірка та збереження конфігурації S1

Крок 1: Перевірка правильності конфігурації

Перевірте правильність конфігурації S1

S1#show running-config

Крок 2: Збереження конфігураційного файлу

Збережіть конфігураційний файл у пам'яті NVRAM
S1# **copy running-config startup-config**
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]

Вміст протокола

У протоколі має бути відображено назву даної роботи, її мету, результати виконання домашнього завдання, результати виконання лабораторного завдання, висновки за результатами виконаної роботи.

Література

1. Астраханцев А.А., Безрук В.М. Маршрутизація в мережах зв'язку: навч. посіб. Х.: ТОВ «Компанія СМІТ», 2011. 368 с.

2. Тарнавський Ю. А., Кузьменко І. М.. Організація комп'ютерних мереж: підручник: для студ. Київ : КПІ ім. Ігоря Сікорського, 2018. 259 с.

3. Tanenbaum A., Feamster N., Wetherall D. Computer Networks. 6th Edition: Pearson Education, 2020. 960 p. URL: https://www.amazon.com/

4. The Cisco Learning Network. URL:https://learningnetwork.cisco.com/s

5. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі: Підручник для вищих навчальних закладів. К.:САММІТ-КНИГА, 2010. 640 с.

6 Павлиш В., Гліненко Л., Шаховська Н. Основи інформаційних технологій і систем: Львівська політехніка, 2018 620 с. URL: https://www.yakaboo.ua/ua/komp-juterna-tehnika-ta-informacijnitehnologii-1230362.html#tab-attributes.

7. Козловський А.В., Погріщук Б.В, Паночишин Ю.М. Комп'ютерна техніка та інформаційні технології Знання, 2012, 463 с. URL: https://www.yakaboo.ua/ua/komp-juternatehnika-ta-informacijni-tehnologii-1230362.html#tab-attributes

8. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. Комп'ютерні мережі. Книга 1: навч. посіб. (рекомендовано МОН України). Львів: «Магнолія 2006», 2021. 256 с.

ЛАБОРАТОРНА РОБОТА №2

Конфігурування VLAN в мережі Ethernet

Мета роботи

1.Придбання практичних навичок конфігурування VLAN в IP-мережі.

2.Аналіз функціонування IP-мережі, структурованої з використанням технології VLAN.

Ключові положення

У сучасних комутаторах технологія віртуальних локальних мереж (Virtual Local Area Network, VLAN) використовується для підвищення продуктивності мережі, поділяючи лише на рівні 2 моделі OSI великі широкомовні домени на більш дрібні.

Застосування VLAN дозволяє також посилити безпеку мережі, полегшити процес її проектування, націлений на максимальне задоволення потреб користувачів мережі.

Транкові з'єднання VLAN дозволяють трафіку від декількох VLAN передаватися по одному каналу, зберігаючи при цьому ідентифікацію та сегментацію VLAN незайманими.

Ключові питання

1 Вкажіть переваги структурування мережі за допомогою VLAN.

2 Зобразіть структуру кадру Ethernet IEEE 802.1Q.

3 Який номер має мережа VLAN Default?

4 Які порти комутатора призначаються VLAN Default?

5 З якою метою комутатору призначається IP-адреса?

6 Які команди Cisco IOS потрібно використовувати, щоб перевірити правильність налаштувань VLAN?

7 Де зберігається інформація про VLAN?

8 Які команди Cisco IOS необхідно використовувати для налаштування VLAN на порті комутатора, підключеного до хоста?

9 Що станеться, якщо VLAN налаштована на інтерфейсі комутатора, але не створена за допомогою команди S(config)#vlan № vlan?

10 Які команди Cisco IOS необхідно використовувати для налаштування транкового каналу?

11 Як змінити номер VLAN, призначений портам?

12 Як видалити VLAN із vlan database?

13 Що станеться з інтерфейсом VLAN, якщо його видалити з vlan database?

Домашнє завдання

1 Вивчіть, використовуючи рекомендовану літературу, а також даним методичним посібником, ключові особливості технології VLAN.

2 Підготуйтеся до співбесіди щодо ключових питань п.3.

3 Проаналізуйте план виконання лабораторної роботи, керуючись п.5.

Завдання до лабораторної роботи

План роботи:

1. Побудова мережі та налаштування базових параметрів пристроїв.
2. Створення мереж VLAN та налаштування портів комутатора.
3. Підтримка призначених портів та бази даних VLAN.
4. Налаштування режиму 802.1Q Trunk між комутаторами.
5. Видалення бази даних VLAN.

Частина 1 Побудова мережі та конфігурування базових параметрів пристроїв

Крок 1: У робочій області Cisco Packet Tracer створити мережу згідно з топологією, представленою на рис.5.1.

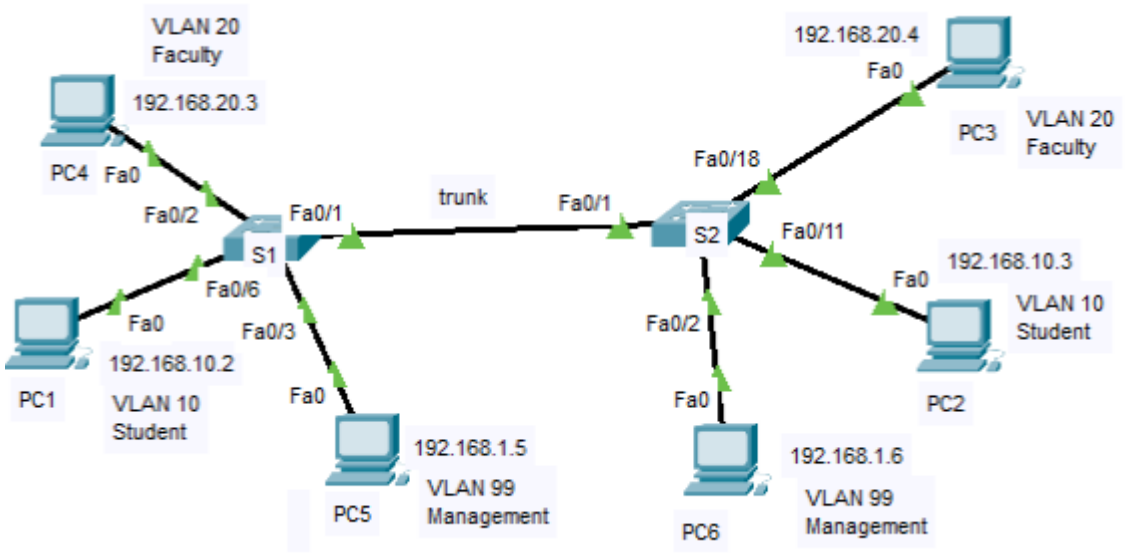

Рисунок 5.1–Топологія мережі

Необхідне обладнання:

Комутатори (Cisco XXXX з Cisco IOS (lanbasek9 образом).

6 PC (Windows10 з програмою емуляції терміналу, такий як Tera Term, Putty) Консольні кабелі конфігурують Cisco IOS пристроїв через консольний порт.

Кабелі Ethernet для створення мережі.

Таблиця 5.1 – Адресна схема мережі

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC–1	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC–2	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC–3	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC–4	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC–5	NIC	192.168.1.5	255.255.255.0	192.168.1.1
PC–6	NIC	192.168.1.6	255.255.255.0	192.168.1.1

Крок 2: Ініціалізуйте та перезавантажте пристрої, якщо це необхідно. Виконайте команду: S1#show startup-config. Якщо файл startup-config є, виконайте:

S1#**erase startup-config**
S1#**reload**

Крок 3:
a. Конфігуруйте імена пристроїв відповідно до топології.
b. Конфігуруйте IP-адреси VLAN 1 на обох комутаторах
c. Скопіюйте поточну конфігурацію у файл startup.

Крок 4: Конфігуруйте параметри IP-протоколу на хостах PC.

Крок 5: Перевірте, чи є зв'язки між PC, а також між PC і комутаторами, посилаючи команду ping. Результати відобразіть у протоколі.

Примітка: Можливо, потрібно вимкнути PC-firewall, щоб виконати команду ping

Частина 2: **Створення мереж VLAN та налаштування портів комутатора**

У частині 2 необхідно створити віртуальні мережі для студентів (Student), викладачів (Faculty) та управління (Management) на обох комутаторах. Далі необхідно призначити VLAN на відповідних інтерфейсах комутатора.

Використовуйте **Show VLAN** для перевірки параметрів конфігурації.

Крок 1: Створення VLAN на комутаторах.

Створення VLAN на S1.

S1(config)# **vlan 10**
S1(config-vlan)# **name Student**
S1(config-vlan)# **vlan 20**
S1(config-vlan)# **name Faculty**
S1(config-vlan)# **vlan 99 5**
S1(config-vlan)# **name Management**
S1(config-vlan)# **end**

b. Створення VLAN на S2.
Створіть такі ж VLAN на комутаторі S2.
c. Використовуйте команду show vlan, щоб перевірити правильність налаштувань.

S1# show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8
			Fa0/1, Fa0/2, Fa0/3, Fa0/4
			Fa0/5, Fa0/6, Fa0/7, Fa0/8
			Fa0/9, Fa0/10, Fa0/11, Fa0/12
			Fa0/13, Fa0/14, Fa0/15, Fa0/16
			Fa0/17, Fa0/18, Fa0/19, Fa0/20
10			Fa0/21, Fa0/22, Fa0/23, Fa0/24
20	Student	active	Gi0/1, Gi0/2
99	Faculty	active	
	Management	active	

```
1002 fddi-default                       act/unsup
1003 token-ring-default                 act/unsup
1004 fddinet-default                    act/unsup
1005 trnet-default                      act/unsup

VLAN  Type   SAID        MTU   Parent  RingNo  BridgeNo  Stp   BrdgMode  Trans1  Trans2
----  -----  ----------  -----  ------  ------  --------  ----  --------  ------  ------
1     enet   100001      1500  -       -       -         -     -         0       0
10    enet   100010      1500  -       -       -         -     -         0       0
20    enet   100020      1500  -       -       -         -     -         0       0
99    enet   100099      1500  -       -       -         -     -         0       0

VLAN  Type   SAID        MTU   Parent  RingNo  BridgeNo  Stp   BrdgMode  Trans1  Trans2
----  -----  ----------  -----  ------  ------  --------  ----  --------  ------  ------
1002  fddi   101002      1500  -       -       -         -     -         0       0
1003  tr     101003      1500  -       -       -         -     -         0       0
1004  fdnet  101004      1500  -       -       -         ieee  -         0       0
1005  trnet  101005      1500  -       -       -         ibm   -         0       0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type                  Ports
```

Який номер у мережі VLAN default?
Які порти призначені мережі VLAN default?

Крок 2: Налаштування VLAN на відповідних інтерфейсах комутатора
а. Налаштування VLANs на інтерфейсах S1.

1) Призначте інтерфейсу, підключеному до компютера PC-1, VLAN Student
S1(config)# **interface f0/6**
S1(config-if)# **switchport mode access**
S1(config-if)# **switchport access vlan 10**
2) Присвойте IP адресу комутатора S1 мережі VLAN 99.
S1(config)# **interface vlan 1**
S1(config-if)# **no ip address**
S1(config-if)# **interface vlan 99**
S1(config-if)# **ip address 192.168.1.11 255.255.255.0**
S1(config-if)# **end**

b.Використайте команду show vlan brief для перевірки правильності налаштувань.

S1# show vlan brief

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

Використовуйте команду show ip interfaces brief.
Яким є статус мережі VLAN 99 (up або down)? Чому?
Результат занесіть у потокол.

d. Відповідно до топології, призначте VLAN відповідним портам комутатора S2.
e. Видаліть IP-адресу комутатора S2 із VLAN 1.
f. Налаштуйте IP-адресу комутатора S2 на VLAN 99 відповідно до таблиці адрес.
h. Використовуйте show vlan brief для перевірки коректності налаштування інтерфейсів.

S2# **show vlan brief**

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

Чи успішний результат виконання команди ping від S1 комутатора за адресою S2? Результат занесіть у потокол.

```
VLAN Name                              Status    Ports

1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
     default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/1, Fa0/2, Fa0/3, Fa0/4
10                                               Fa0/5, Fa0/6, Fa0/7, Fa0/8
     Student                           active    Fa0/9, Fa0/10, Gi0/1, Gi0/2
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
20                                               Fa0/16, Fa0/17, Fa0/18, Fa0/19
30   Faculty                           active    Fa0/20, Fa0/22, Fa0/23
99   VLAN0030                          active    Fa0/11, Fa0/21
     Management                        active    Fa0/24
```

c. Використовуйте команду no vlan 30, щоб видалити VLAN 30 з VLAN database

S1(config)# **no vlan 30**
S1(config)# **end**

d. Використовуйте команду show vlan brief..

Після видалення VLAN 30, який VLAN призначений порт F0/24? Що станеться з трафіком від хоста, підключеного до порту F0/24?

S1# **show vlan brief**

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

e. Використовуйте команду no switchport access vlan на F0/24.

f. Використовуйте команду show vlan brief, щоб переглянути, яка VLAN призначена F0/24. Результати відобразіть у протоколі.

Примітка: Перед видаленням VLAN з database необхідно переналаштувати всі порти, які їй належали.

Чому потрібно переналаштувати всі порти, що належать VLAN, що видаляється?

Частина 4: Конфігурування транкового канала 802.1Q між комутаторами

У частині 4 необхідно налаштувати інтерфейс F0/1 комутатора використання протоколу Dynamic Trunking Protocol (DTP) з метою автоматичного створення транкового з'єднання. Після автоматичного створення та перевірки транкового з'єднання необхідно вимкнути протокол DTP на інтерфейсі F0/1 та налаштувати транкове з'єднання вручну

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
*Mar 1 05:07:28.746:   %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar 1 05:07:29.744:   %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S1(config-if)#
*Mar 1 05:07:32.772:   %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S1(config-if)#
*Mar 1 05:08:01.789:   %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
*Mar 1 05:08:01.797:   %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

S1# **show vlan brief**

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

```
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       desirable        802.1q         trunking      1

Port
Fa0/1       Vlans allowed on trunk
            1-4094
Port
Fa0/1       Vlans allowed and active in management domain
            1,10,20,99
Port
Fa0/1       Vlans in spanning tree forwarding state and not pruned
            1,10,20,99

S2# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       auto             802.1q         trunking      1

Port
Fa0/1       Vlans allowed on trunk
            1-4094
Port
Fa0/1       Vlans allowed and active in management domain
            1,10,20,99
Port
Fa0/1       Vlans in spanning tree forwarding state and not pruned
            1,10,20,99
```

За замовчувнням у транковому каналі дозволені всі VLAN**.** Команда **switchport trunk дозволяє** задати конкретні VLAN які будут проходити через транковый канал. В даній лабораторній будемо використовувати налаштування «за ».замовчуванням.

d. Перевірте можливість прохождення трафіка по транку.

Чи успішний результат виконання команди ping від

S1 - S2?

PC-A - PC-B?

PC-A PC-C?

PC-B - PC-C?

Can PC-A ping S1?

PC-B - S2?

PC-C- S2?

Результати занесіть в протокол.

Крок 2: Ручне налаштування транкового каналу на интерфейсі F0/1

Для ручного конфігурування транкового зєднання команда **switchport mode trunк**

S1(config)# **interface f0/1**

```
S2# show interfaces trunk

Port        Mode             Encapsulation    Status        Native vlan
Fa0/1       on               802.1q           trunking      99

Port
Fa0/1       Vlans allowed on trunk
            1-4094
Port
Fa0/1       Vlans allowed and active in management domain
            1,10,20,99
Port
Fa0/1       Vlans in spanning tree forwarding state and not pruned
            1,10,20,99
```

Частина 5: Видаліть VLAN Database

У цій частині необхідно видалити файл VLAN Database. Це необхідно, якщо здійснюється ініціалізація пристрою та повернення до параметрів «за замовчуванням».

Крок 1: Просмотр наявності бази даних VLAN
Виконайте команду show flash і перевірте присутність файла **vlan.dat**

S1# **show flash**

```
Directory of flash:/

    2  -rwx        1285     Mar  1 1993  00:01:24  +00:00   config.text
    3  -rwx        43032    Mar  1 1993  00:01:24  +00:00   multiple-fs
    4  -rwx            5    Mar  1 1993  00:01:24  +00:00   private-config.text
    5  -rwx     11607161    Mar  1 1993  02:37:06  +00:00   c2960-lanbasek9-mz.150-2.SE.bin
    6  -rwx          736    Mar  1 1993  00:19:41  +00:00   vlan.dat

32514048 bytes total (20858880 bytes free)
```

Зверніть увагу, якщо у flash-пам'яті комутатора є база даних VLAN (vlan.dat), то не використовуються налаштування «за замовчуванням».

Крок 2: Видаліть базу даних VLAN

a. Виконайте команду **delete vlan.dat** , щоб використати настройки VLAN database default.
b. Використовуйте команду **show flash** для перевірки

S1# **show flash**

```
Directory of flash:/

    2  -rwx        1285     Mar  1 1993  00:01:24  +00:00   config.text
    3  -rwx        43032    Mar  1 1993  00:01:24  +00:00   multiple-fs
    4  -rwx            5    Mar  1 1993  00:01:24  +00:00   private-config.text
    5  -rwx     11607161    Mar  1 1993  02:37:06  +00:00   c2960-lanbasek9-mz.150-2.SE.bin

32514048 bytes total (20859904 bytes free)
```

Вміст протокола

У протоколі необхідно подати назву даної роботи, її мету, результати виконання домашнього завдання, результати виконання лабораторного завдання, висновки.

Література

1. Астраханцев А.А., Безрук В.М. Маршрутизація в мережах зв'язку: навч. посіб. Х.: ТОВ «Компанія СМІТ», 2011. 368 с.

3. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. Комп'ютерні мережі. Книга 1: навч. посіб. (рекомендовано МОН України). Львів: «Магнолія 2006», 2021. 256 с.

4. Тарнавський Ю. А., Кузьменко І. М.. Організація комп'ютерних мереж: підручник: для студ. Київ : КПІ ім. Ігоря Сікорського, 2018. 259 с.

5. Tanenbaum A., Feamster N., Wetherall D. Computer Networks. 6th Edition: Pearson Education, 2020. 960 p. URL: https://www.amazon.com/

6. The Cisco Learning Network. URL:https://learningnetwork.cisco.com/s/

ЛАБОРАТОРНА РОБОТА №3

Конфігурування функцій безпеки на портах комутатора

Мета роботи

1 Аналіз функціонування мережі із функцією безпеки на портах комутатора.

2 Набуття практичних навичок конфігурування віддаленого доступу до комутатора за протоколом SSH.

3 Набуття практичних навичок конфігурування функцій безпеки на портах комутатора.

Ключові положення

"Port security" – функція комутатора, що дозволяє вказати MAC-адреси хостів, яким дозволено передавати дані через порт. Після цього порт не передає пакети, якщо MAC-адреса відправника не вказана як дозволена. Крім того, при конфігуруванні цієї функції можна вказувати не конкретні MAC-адреси, дозволені на порті комутатора, а обмежити кількість MAC-адрес, яким дозволено передавати трафік через порт. Використовується для запобігання:

– несанкціонованої зміни MAC-адреси мережного пристрою або підключення до мережі,

– атак спрямованих на переповнення таблиці комутації комутатора.

Комутатор cisco підтримує такі типи безпечних MAC-адрес:

Статичні MAC-адреси:
статично стають командою switchport port-security mac-address mac-address в режимі налаштування інтерфейсу,
зберігаються у таблиці адрес,
додаються до поточної конфігурації комутатора;

Динамічні MAC-адреси:
динамічно вивчаються,
зберігаються лише у таблиці адрес,
видаляються при перезавантаженні комутатора;

Sticky MAC-адреси:
можуть бути статично налаштовані або динамічно вивчені,
зберігаються у таблиці адрес,
додаються до поточної конфігурації комутатора. Якщо ці адреси збережені в конфігураційному файлі, після перезавантаження комутатора, їх не потрібно заново переналаштовувати.

Порушенням безпеки при включеній port security вважаються ситуації:

– максимальну кількість безпечних MAC-адрес було додано до таблиці адрес і хост, чия MAC-адреса не записана в таблиці адрес, намагається отримати доступ через інтерфейс,

– адреса, вивчена або налаштована як безпечна на одному інтерфейсі, з'явилася на іншому безпечному інтерфейсі в тій же VLAN.

На інтерфейсі можуть бути налаштовані такі режими реагування на порушення безпеки:

– **protect** – коли кількість безпечних MAC-адрес досягає максимального значення обмеження, налаштованого на порту, пакети з невідомою MAC-адресою відправника відкидаються до тих пір, поки не буде видалено достатню кількість безпечних MAC-адрес, таку, щоб їх кількість була меншою за максимальне значення, або збільшено максимальну кількість дозволених адрес. Повідомлень про порушення безпеки немає.

– **restrict** – коли кількість безпечних MAC-адрес досягає максимального значення обмеження, налаштованого на порту, пакети з невідомою MAC-адресою відправника відкидаються до тих пір, поки не буде видалено достатню кількість безпечних MAC-адрес, таку, щоб їх кількість була меншою за максимальне значення, або збільшено максимальну кількість дозволених адрес. У цьому режимі при порушенні безпеки відправляється сповіщення SNMP trap, повідомлення Syslog і збільшується лічильник порушень (violation counter).

– **shutdown** – порушення безпеки призводить до того, що інтерфейс переводиться в стан негайного вимкнення (error-disabled) і вимикається LED порту. Надсилається SNMP trap, повідомлення syslog і збільшується лічильник порушень (violation counter). Коли порт переведений в стан error-disabled, вивести з цього стану його можна ввівши команду errdisable recovery cause psecure-violation або вручну включити інтерфейс ввівши в режимі налаштування інтерфейсу команди shutdown і no shutdown. Це стандартний режим.

Режим protect не рекомендується налаштовувати для транка. Цей режим вимикає процес запам'ятовування адрес, коли будь-яка VLAN досягає максимуму безпечних адрес, навіть якщо на порту не досягнуто максимальне значення обмеження.

На комутаторах Cisco такі параметри за замовчуванням для функції port security: Функція Port security – вимкнена.

Запам'ятовування sticky-адрес – вимкнено.

Максимальна кількість безпечних MAC-адрес на порту – 1.

Режим реагування на порушення – shutdown.

Час зберігання адрес:

вимкнено. Значення aging time – 0,

для статичних адрес – відключено,

тип часу - абсолютне.

Ключові питання

1.Для яких цілей використовуються лінії vty у комутаторі?

2 Вкажіть переваги організації віддаленого доступу до мережі з використанням протоколу SSH в порівнянні з використанням протоколу telnet.

3 Як настроїти віддалений доступ до пристрою мережі за допомогою протоколу SSH?

4 Як перевірити коректність налаштувань віддаленого доступу до пристрою мережі за допомогою протоколу SSH? 3.4 Вкажіть типи безпечних адрес, які підтримують комутатори cisco.

5 Де зберігаються безпечні MAC-адреси статичні, динамічні, Sticky?

6 Вкажіть режими реагування на порушення безпеки, які застосовуються в комутаторах cisco.

7 Охарактеризуйте функцію Port security комутатора cisco.

8 Охарактеризуйте режими реагування на порушення безпеки, які застосовуються в комутаторах cisco.

9 Як настроїти функцію безпеки на порті комутатора cisco?

10 Як настроїти режим реагування на порушення безпеки на порті комутатора cisco?

11 Як переглянути інформацію про налаштування функції безпеки на порті комутатора cisco?

12 Як переглянути інформацію про налаштування протоколу SSH?

13 Що таке «банер» та як його налаштувати?

Домашнє завдання

1.Вивчіть, використовуючи рекомендовану літературу, а також даний методичний посібник, ключові особливості технологій Port-security, віддаленого доступу до пристрою по SSH.

2 Підготуйтеся до співбесіди щодо ключових питань п.3.

3 Проаналізуйте план виконання лабораторної роботи, керуючись п.5

Завдання до лабораторної роботи

План роботи:

1 Побудова мережі та налаштування базових установок пристроїв.

2 Налаштування та перевірка доступу протоколу SSH до комутатора S1.

3 Налаштування та перевірка функції безпеки на портах комутатора S1

Частина 1 Побудова мережі та конфігурація базових параметрів пристроїв

Крок 1: У робочій області Cisco Packet Tracer створити мережу згідно з топологією, представленою на рис.5.1.

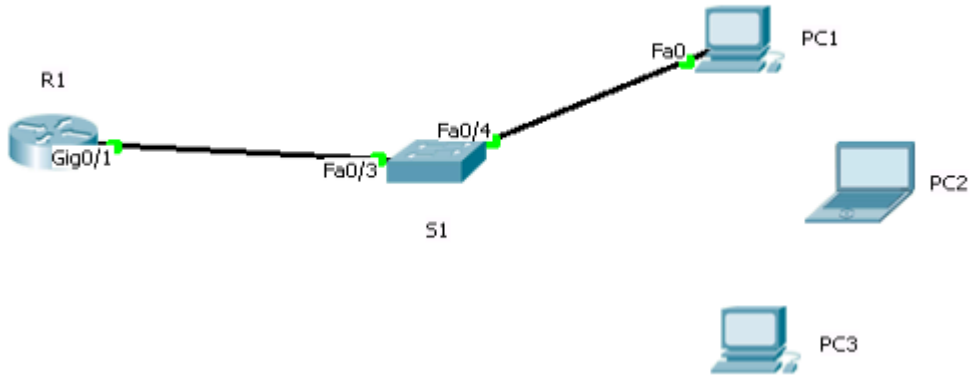

Рисунок 5.1–Топологія мережі

Необхідне обладнання:

Маршрутизатор Cisco XXXX з Cisco IOS Release (образ universalk9).
Комутатор Cisco XXXX з Cisco IOS (lanbasek9 образом).
3 ПК (Windows 10, 11 з програмами емуляції термінала, такими як Tera Term, Putty).
Консольні кабелі для конфігурації Cisco IOS пристроїв через консольний порт.
Кабелі Ethernet для створення мережі

Таблиця 5.1 – Адресна схема мережі.

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.5	255.255.255.0	172.16.99.1
PC-1	NIC	172.16.99.10	255.255.255.0	172.16.99.1

Примітка: Параметр X в схемі мережі оберіть згідно варіанту, наданого викладачем.

Перевірте, що маршрутизатор і комутатор не мають початкової конфігурації. В іншому випадку видаліть її та перезавантажте пристрій. Якщо ви не знаєте, як це зробити, зверніться до викладача.

Крок 2: Конфігуруйте параметри IP-протоколу на PC1.

Крок 3: Конфігурування базових параметрів на R1.

a. Конфігуруйте ім'я пристрою згідно з топологією.
b. Вимкніть функцію DNS lookup.
c. Конфігуруйте IP-адресу на інтерфейсі G0/1 маршрутизатора, згідно з таблицею адресів.
d. Задайте пароль **onat** для входу в привілейований режим роботи маршрутизатора.
e. Задайте пароль **onatmz** для доступу до консольного порту та віртуальних інтерфейсів vty. Увімкніть **login**.
f. Увімкніть функцію шифрування паролів.
g. Збережіть поточну конфігурацію пристрою у файлі **startup**.

Крок 4: Конфігурування базових параметрів на S1.

Хорошим правилом підвищення безпеки є призначення IP-адреси VLAN для управлінської мережі комутатора, відмінної від VLAN 1, а також від VLAN-мереж користувачів. У цій роботі використовуйте для цієї мети VLAN 99.
a. Конфігуруйте ім'я пристрою згідно з топологією.
b. Створіть VLAN 99 на комутаторі з ім'ям Management.

S1(config)# **vlan 99**
S1(config-vlan)# **name Management**
S1(config-vlan)# **exit**
S1(config)#

c. Конфігуруйте IP-адресу VLAN 99 на комутаторі.

S1(config)# **interface vlan 99**
S1(config-if)# **ip address 172.16.99.5 255.255.255.0**
S1(config-if)# **no shutdown**
S1(config-if)# **end**
S1#

d. Використовуйте команду show vlan для перегляду статусу VLAN 99.
e. Використовуйте команду show ip interface brief для перегляду статусу та протоколу інтерфейсу управління. Результати виконаної роботи на кроках d та e відобразіть у протоколі.
f. Вимкніть функцію DNS lookup.
g. Задайте пароль onat для входу в привілейований режим роботи маршрутизатора.
h. Задайте пароль onatmz для доступу до консольного порту та віртуальних інтерфейсів vty. Увімкніть login.
k. Увімкніть функцію шифрування паролів.
l. Конфігуруйте default gateway для S1, згідно з таблицею адресів.
m. Збережіть поточну конфігурацію пристрою у файлі startup.

Крок 5: Перевірка коректності налаштувань

a. Перевірте з'єднання між PC1 і default gateway, PC1 і мережею управління S1, S1 і default gateway. Результати відобразіть у протоколі.

Частина 2: Конфігурування та перевірка віддаленого доступу до комутатора через протокол SSH

Крок 1: Конфігурування віддаленого доступу до комутатора через протокол SSH

. Увімкніть протокол SSH на S1. Використовуйте ім'я домену SUITT-Lab.com.

S1(config)# ip domain-name SUITT-Lab.com

b. Створіть БД користувачів для віддаленого доступу.

c. Конфігуруйте протокол SSH на віртуальних інтерфейсах та використовуйте локальну БД для автентифікації

S1(config)# **line vty 0 15**
S1(config-line)# **transport input ssh**
S1(config-line)# **login local**
S1(config-line)# **exit**

d. Створіть ключ розміром 1024 біти..

S1(config)# **crypto key generate rsa modulus 1024**

Им'я ключа S1 SUITT -Lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

S1(config)#
S1(config)# **end**

e. Перевірте SSH-з'єднання.

S1# show ip ssh

Яку версію SSH використовує комутатор? Скільки спроб автентифікації можливо? Який тайм-аут між спробами?

Результати відобразіть у протоколі.

Крок 2: Модифікація конфігурації SSH на S1

Змініть інтервал часу тайм-ауту та кількість спроб, задане за замовчуванням.

S1# **config t**
S1(config)# **ip ssh time-out 75**
S1(config)# **ip ssh authentication-retries 2**

Крок 3: Перевірка коректності налаштувань

a. Використовуйте програму SSH-клієнт на PC для відкриття сеансу зв'язку з комутатором через SSH. Увійдіть, використовуючи логін та пароль, які були налаштовані.

Частина 3: Налаштування та перевірка функції безпеки на портах комутатора

Крок 1: Налаштування банера

a. Налаштуйте банер MOTD (повідомлення дня при вході).

S1(config)# banner motd # Unauthorized access is strictly prohibited #

Крок 2: Вимкнення не використовуваних портів

a. Використовуючи команду show ip interface brief, визначте, які фізичні порти комутатора активні.

b. Вимкніть не використовувані порти.

S1(config)# **interface range f0/1 - 2**
S1(config-if-range)# **shutdown**
S1(config-if-range)# **interface range f0/5 - 24**
S1(config-if-range)# **shutdown**
S1(config-if-range)# **interface range g0/1 - 2**
S1(config-if-range)# **shutdown**
S1(config-if-range)#**end**

Крок 3: Налаштування та перевірка функції «Port security» на S1

a. Визначте MAC-адресу порту G0/1 маршрутизатора R1 за допомогою команди:

show interface g0/1

R1# **show interface g0/1**
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 00f7.0ca3.d821 (bia 00f7.0ca3.d821)

b. Використовуючи команду **show mac address-table**, проаналізуйте вміст таблиці MAC-адрес комутатора S1. Результат занесіть у протокол.

c. Вимкніть порт f0/3.
S1(config)# **interface f0/3**
S1(config-if)# **shutdown**

d. Увімкніть функцію port security на порту f0/3.

g. Увімкніть порт f0/3.

h. Перевірте коректність налаштувань, використовуючи команду.

S1# **show port-security interface f0/3**

```
Port Security              :Enabled
Port Status                :Secure-shutdown
Violation Mode             :Shutdown
Aging Time                 0 mins
Aging Type                 :Absolute
SecureStatic Address Aging :Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses
                           : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Каков статус порта f0/3?

l. За допомогою команди ping перевірте зв'язок між R1 і PC1. Результат відобразіть у протоколі.

R1#**ping 172.16.99.10**

Моделюйте ситуацію порушення безпеки, змінивши MAC-адресу інтерфейсу g0/1 маршрутизатора R1.

R1# **config t**
R1(config)# **interface g0/1**
R1(config-if)# **shutdown**
R1(config-if)# **mac-address aaaa.bbbb.cccc**

p. Увімкніть інтерфейс g0/1 маршрутизатора R1 і за допомогою команди ping перевірте зв'язок R1-PC. Результат відобразіть у протоколі.

r. Перевірте стан безпечного порту комутатора.

S1# **show port-security**

```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)         (Count)                (Count)
---------------------------------------------------------------------
      Fa0/3             1            1                   1          Shutdown
---------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)       :0
Max Addresses limit in System (excluding one mac per port) :8192

S1# show port-security interface f0/3

Port Security                :Enabled
Port Status                  : Secure-shutdown
Violation Mode               :Shutdown
Aging Time                   :0 mins
Aging Type                   :Absolute
SecureStatic Address Aging   :Disabled
Maximum MAC Addresses        : 1
Total MAC Addresses          : 1
Configured MAC Addresses     : 1
Sticky MAC Addresses         : 0
Last Source Address:Vlan     : aaaa.bbbb.cccc:99
Security Violation Count     : 1

S1# show interface f0/3

FastEthernet0/3 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 00f7.0ca3.d821 (bia 00f7.0ca3.d821)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>

S1# show port-security address
                Secure Mac Address Table
------------------------------------------------------------------------
Vlan      Mac Address         Type                  Ports       Remaining Age
                                                                  (mins)
----      -----------         ----                  -----    -------------
  99      00f7.0ca3.d821    SecureConfigured        Fa0/3          -
------------------------------------------------------------------------
---
Total Addresses in System (excluding one mac per port)       :0
Max Addresses limit in System (excluding one mac per port) :8192
```

Результати роботи, виконаної на цьому кроці, відобразіть у протоколі.

s. Вимкніть інтерфейс g0/1 маршрутизатора R1, видаліть налаштований MAC-адрес інтерфейсу і знову увімкніть інтерфейс.

R1(config-if)# **shutdown**
R1(config-if)# **no mac-address aaaa.bbbb.cccc**
R1(config-if)# **no shutdown**
R1(config-if)# **end**

t. Надішліть команду ping від R1 до PC1. Результат відобразіть у протоколі.

u. Використовуйте команду show interface f0/3, щоб зрозуміти причину неуспішного виконання команди ping.

n. Змініть статус error disabled порту f0/3.

S1# **config t**
S1(config)# **interface f0/5**
S1(config-if)# **shutdown**
S1(config-if)# **no shutdown**

z. Використовуйте команду **show interface f0/3** для перевірки, зміни статусу порту f0/3.

S1# show interface f0/3

```
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 00f7.0ca3.d821 (bia00f7.0ca3.d821)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

y. Надішліть команду ping від R1 до PC1. Результат успішний?

Зміст протокола

У протоколі має бути відображено назву даної роботи, її мету, результати виконання домашнього завдання, результати виконання лабораторного завдання, висновки за результатами виконаної роботи.

Література

1. Астраханцев А.А., Безрук В.М. Маршрутизація в мережах зв'язку: навч. посіб. Х.: ТОВ «Компанія СМІТ», 2011. 368 с.

3. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. Комп'ютерні мережі. Книга 1: навч. посіб. (рекомендовано МОН України). Львів: «Магнолія 2006», 2021. 256 с.

4. Тарнавський Ю. А., Кузьменко І. М.. Організація комп'ютерних мереж: підручник: для студ. Київ : КПІ ім. Ігоря Сікорського, 2018. 259 с.

5. Tanenbaum A., Feamster N., Wetherall D. Computer Networks. 6th Edition: Pearson Education, 2020. 960 p. URL: https://www.amazon.com/

6. The Cisco Learning Network. URL:https://learningnetwork.cisco.com/s/

ЛАБОРАТОРНА РОБОТА №4

Налаштування маршрутизації між VLAN в мережі Ethernet

Мета роботи

1 Набуття практичних навичок конфігурування VLAN з маршрутизацією трафіку.
2 Аналіз функціонування IP-мережі, структурованої з урахуванням VLAN.

Ключові положення

Структуризація мережі з використанням технології VLAN (Virtual Local Area Network) дозволяє отримати такі переваги:

– Гнучкий поділ пристроїв на групи

Як правило, одній VLAN відповідає одна підмережа. Пристрої, що знаходяться у різних VLAN, будуть знаходитися у різних підмережах. Але в той же час VLAN не прив'язана до розташування пристроїв і тому пристрої, що знаходяться на відстані один від одного, все одно можуть бути в одній VLAN незалежно від розташування.

–Зменшення кількості широкомовного трафіку у мережі

Кожна VLAN – це окремий широкомовний домен. Наприклад, комутатор - це пристрій 2 рівня моделі OSI. Всі порти на комутаторі з одним VLAN знаходяться в одному широкомовному домені. Створення додаткових VLAN на комутаторі означає розбиття комутатора на кілька широкомовних доменів. Якщо один і той же VLAN налаштований на різних комутаторах, то порти різних комутаторів утворюватимуть один широкомовний домен.

– Збільшення безпеки та керованості мережі

Коли мережа розбита на VLAN, спрощується завдання застосування політик та правил безпеки. З VLAN політики можна застосовувати до цілих підмереж, а не до окремого пристрою. Крім того, перехід з одного VLAN в інший передбачає проходження через пристрій 3 рівня, на якому зазвичай застосовуються політики, що дозволяють або забороняють доступ з VLAN в VLAN.

Ключові питання

1 Вкажіть переваги структурування мережі за допомогою VLAN.

2 Зобразіть структуру кадру Ethernet IEEE 802.1Q.

3 Який номер має мережа VLAN Default?

4 Які порти комутатора призначаються VLAN Default?

5 З якою метою комутатору призначається IP-адреса?

6 Які команди Cisco IOS потрібно використовувати, щоб перевірити правильність налаштувань VLAN?

7 Де зберігається інформація про VLAN?

8 Які команди Cisco IOS необхідно використовувати для налаштування VLAN на порті комутатора, підключеного до хоста?

9 Що станеться, якщо VLAN налаштована на інтерфейсі комутатора, але не створена за допомогою команди S(config)#vlan № vlan?

10 Які команди Cisco IOS потрібно використовувати для налаштування маршрутизатора?

11 Як змінити номер VLAN, призначений портам?

12 Як видалити VLAN із vlan database?

13 Що станеться з інтерфейсом VLAN, якщо його видалити з vlan database?

Домашнє завдання

1.Вивчіть, використовуючи рекомендовану літературу, а також даний методичний посібник, ключові особливості технологій Port-security, віддаленого доступу до пристрою по SSH.

2 Підготуйтеся до співбесіди щодо ключових питань п.3.

3 Проаналізуйте план виконання лабораторної роботи, керуючись п.5

Завдання до лабораторної роботи

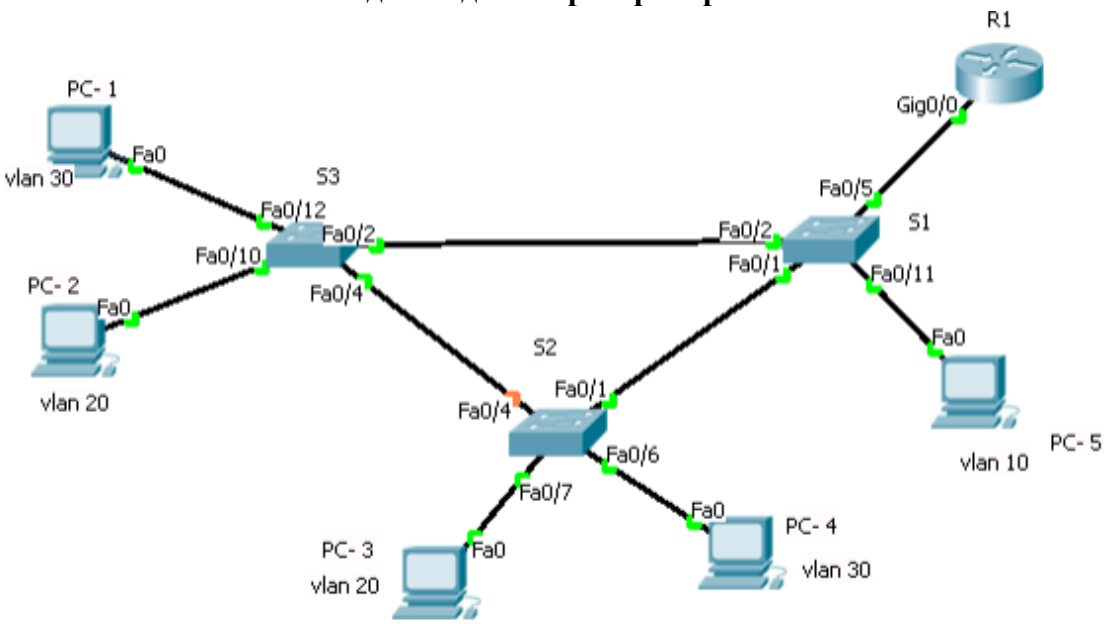

Рисунок 5.1–Топологія мережі

Необхідне обладнання:
– комутатори Cisco XXXX;
– 5 PC (Windows 10 із програмою емуляції терміналу, такий як Tera Term, Putty);
– консольні кабелі конфігурують Cisco IOS пристроїв через консольний порт;
– маршрутизатор Cisco XXXX з Cisco IOS (universalk9 чином);
– кабелі Ethernet для створення мережі

Таблиця 5.1 – Адресна схема мережі

Device :	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1 X	G0/0.10	172.16+X.10.1	255.255.255.0	N/A
	G0/0.20	172.16+X.20.1	255.255.255.0	N/A
	G0/0.30	172.16+X.30.1	255.255.255.0	N/A
PC–1	NIC	172.16+X.30.10	255.255.255.0	172.16+X.30.1
S1	VLAN 1	172.16+X.1.2	255.255.255.0	172.16+X.1.1
S2	VLAN 1	172.16+X.1.3	255.255.255.0	172.16+X.1.1
S3	VLAN 1	172.16+X.1.4	255.255.255.0	172.16+X.1.1
PC–2	NIC	172.16+X.5	255.255.255.0	172.16+X.20.1
PC–3	NIC	172.16+X.20.6	255.255.255.0	172.16+X.20.1
PC–4	NIC	172.16+X.30.11	255.255.255.0	172.16+X.30.1
PC–5	NIC	172.16+X.10.10	255.255.255.0	172.16+X.10.1

X - номер варіанта

Крок 2: Ініціалізуйте та перезавантажте пристрої, якщо це необхідно.
Виконайте команду: *S1#show startup-config*. Якщо файл startup-config є, виконайте:

S1#**erase startup-config**
S1#**reload**

Крок 3:
а. Конфігуруйте імена пристроїв відповідно до топології.
в. Скопіюйте поточну конфігурацію у startup.

Крок 4: Конфігуруйте параметри IP-протоколу на хостах PC.

Крок 5: Перевірте, чи зв'язки між PC, а також між PC і комутаторами, посилаючи команду ping. Результати відобразіть у протоколі.

Частина 2 Створення мереж VLAN та налаштування портів комутаторів

Крок 1:

a. Створіть VLAN на комутаторах та надайте їм імена: VLAN 10 – Faculty, VLAN 20 – Departement, VLAN 30 – Student.
b. Конфігуруйте режим access на портах комутаторів, приєднаних до хостів.
c. Призначте access-портам номера VLAN, згідно з топологією.

d. Конфігуруйте порти Fa0/1, Fa0/2. Fa0/5 комутатора S1, Fa0/1 комутатора S2, Fa0/2 комутатора S3 як транкові.

Крок 2: Перевірка коректності роботи мережі

a. Виконайте команду **show vlan brief** на S1, S2, S3 для перевірки коректності сконфігурованих VLAN.

S3#**show vlan brief**

30 Student active Fa0/12

Результати роботи, виконаної на кроці 2.a, занесіть у протокол.

b. Виконайте ping, щоб перевірити зв'язок мережі. Чи є зв'язок між PC-1 та PC-5? Чи є зв'язок між PC-1 та PC-4? Чи є зв'язок між PC-1 та PC-2? Результати роботи, виконаної на кроці 2.b, занесіть у протокол.

Частина 3 Конфигурування маршрутизації між VLAN

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/11, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig1/1, Gig1/2
10	Faculty	active	
20	Departement	active	Fa0/10

Крок 1: Конфігуруйте підінтерфейси на маршрутизаторі R1 для стандарту 802.1Q.
a. Створіть підінтерфейс G0/0.10 командою

R1(config)#**interface g0/0.10**

a. Задайте піддтримку стандарта 802.1Q

R1(config-subif)#**encapsulation dot1Q 10**

b. Задайте IP-адресу підінтерфейса для VLAN 10

R1(config-subif)#**ip address 172.17.10.1 255.255.255.0**

c. Аналогічно налаштуйте підінтерфейси G0/0.20 та G0/0.30 для підтримки VLAN 20 та VLAN 30.

Крок 2: Перевірка коректності конфігурування маршрутизатора

а. За допомогою команди show ip interface brief перевірте конфігурацію підінтерфейсів. Вони активні? Оскільки інтерфейси віртуальні, необхідно підняти фізичний інтерфейс, з яким вони асоційовані.

а. Виконайте команду ping, щоб перевірити зв'язок мережі.

Чи є зв'язок між PC-1 та PC-5?

Чи є зв'язок між PC-1 та PC-4?

Чи є зв'язок між PC-1 та PC-2? Крок 3: Перевірка коректності роботи мережі

Результати роботи, виконаної в частині 3а, занесіть у протокол.

Зміст протокола

У протоколі має бути відображено назву даної роботи, її мету, результати виконання домашнього завдання, результати виконання лабораторного завдання, висновки за результатами виконаної роботи.

Литература

1. Астраханцев А.А., Безрук В.М. Маршрутизація в мережах зв’язку: навч. посіб. Х.: ТОВ «Компанія СМІТ», 2011. 368 с.

3. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. Комп’ютерні мережі. Книга 1: навч. посіб. (рекомендовано МОН України). Львів: «Магнолія 2006», 2021. 256 с.

4. Тарнавський Ю. А., Кузьменко І. М.. Організація комп’ютерних мереж: підручник: для студ. Київ : КПІ ім. Ігоря Сікорського, 2018. 259 с.

5. Tanenbaum A., Feamster N., Wetherall D. Computer Networks. 6th Edition: Pearson Education, 2020. 960 p. URL: https://www.amazon.com/

6. The Cisco Learning Network. URL:https://learningnetwork.cisco.com/s/

ЛАБОРАТОРНА РОБОТА №5

Об'єднання каналів у мережі Ethernet за допомогою технології EtherChannel

Мета роботи

1 Набуття практичних навичок конфігурування агрегованих каналів у мережі Ethernet.

2 Аналіз функціонування Ethernet-мережі з агрегованими каналами.

Ключові положення

Агрегування каналів – це метод, який дозволяє створювати логічні зв'язки, які складаються із двох або більше фізичних зв'язків. Це забезпечує підвищену пропускну здатність каналу. Об'єднання каналів також забезпечує надмірність, якщо один або кілька фізичних зв'язків виходить з ладу.

Одним з ефективних способів агрегування каналів є використання технології EtherChannel. Канали EtherChannel можуть бути налаштовані вручну адміністратором мережі або за допомогою одного з двох проколів – PAgP або LACP. PAgP є протоколом, розробленим компанією Cisco. Його можна конфігурувати лише на комутаторах Cisco та комутаторах, які мають ліцензію постачальників для підтримки PAgP. LACP є відкритим протоколом. LACP є протоколом агрегації каналів, який визначений стандартом IEEE 802.3ad, і він не пов'язаний з будь-яким конкретним постачальником обладнання

Ключові питання

1 Охарактеризуйте технологію EtherChannel.

2 Порівняйте можливості технології EtherChannel і підхід з використанням більш швидких каналів. 3 Вкажіть переваги технології EtherChannel порівняно з використанням більш швидких каналів. .

4 Опишить варіанти реалізації EtherChannel.

5 Охарактеризуйте режими інтерфейсів у PagP.

6 Охарактеризуйте режими інтерфейсів у LACP.

7 Як налаштувати канал EtherChannel на комутаторі Cisco?

8 Як здійснити перевірку налаштувань EtherChannel Cisco?

Домашнє завдання

1 Вивчіть, використовуючи рекомендовану літературу, а також дане методичне керівництво, ключові особливості технології EtherChannel.

2 Підготуйтеся до співбесіди щодо ключових питань п.3.

3 Проаналізуйте план виконання лабораторної роботи, керуючись п.5.

Завдання до лабораторної роботи

1. Побудова мережі та налаштування базових параметрів пристроїв.
2. Налаштування протоколу PAgP на комутаторах.
3. Налаштування протоколу LACP на комутаторах.

4. Перевірка коректності налаштувань.

У робочій області Cisco Packet Tracer створити мережу згідно з топологією, представленою на рис.5.1.

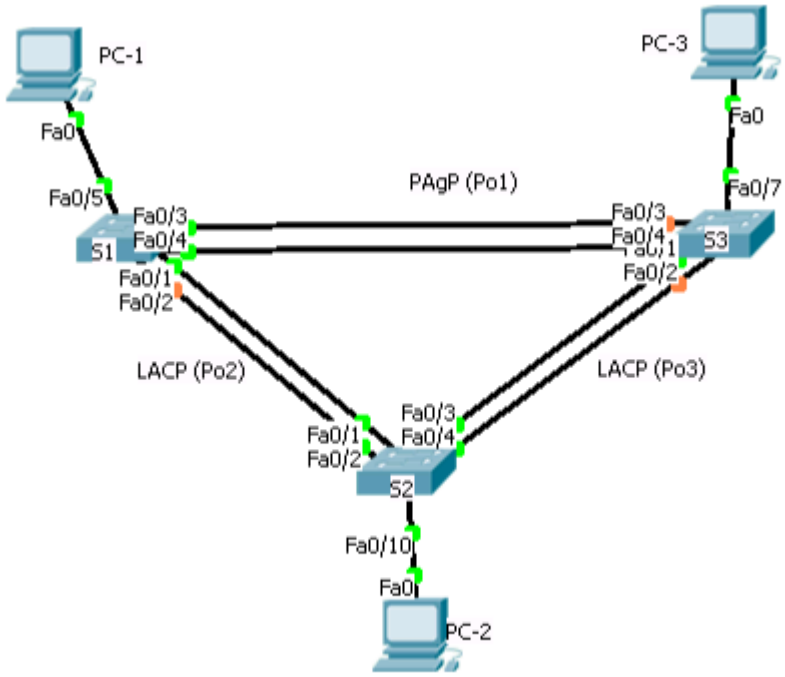

Рисунок 5.1–Топологія мережі

Необхідне обладнання:
– 3 Комутатори Cisco XXXX;
– 3 PC (Windows 10,11 із програмою емуляції терміналу, такою, як Tera Term, Putty;
– консольні кабелі для конфігурування Cisco IOS пристроїв через консольний порт;
– кабелі Ethernet для створення мережі.

Пристрій	Інтерфейс	IPv4 адреса	Маска підмережі
S1	VLAN 99	192.168.99.5	255.255.255.0
S2	VLAN 99	192.168.99.6	255.255.255.0
S3	VLAN 99	192.168.99.7	255.255.255.0
PC–1	NIC	192.168.10.10	255.255.255.0
PC–2	NIC	192.168.10.11	255.255.255.0
PC–3	NIC	192.168.10.12	255.255.255.0

Таблиця 5.1 – Адресна схема мережі

Крок 2: Ініціалізуйте та перезавантажте пристрої, якщо це необхідно.

Виконайте команду: Switch#**show startup-config**. Якщо файл startup-config присутній, виконайте:

Switch #**erase startup-config**

Switch #**reload**

Крок 3:

a. Конфігуруйте імена пристроїв, згідно топології.

b. Вимкніть усі порти комутаторів, за винятком тих, до яких підключено комп'ютери.

c. Створіть VLAN 99 з іменем Management.

d. Створіть VLAN 10 під назвою Staff.

e. Надайте портам комутаторів, підключеним до комп'ютерів, належність до мережі VLAN 10.

f. Налаштуйте параметри IP-протоколу на пристроях.

g. Збережіть поточну конфігурацію комутаторів.

Частина 2. Налаштування протоколу PAgP

Крок 1: Конфігурування лінка між комутаторами S1 та S3 з використанням протоколу PagP.

a. Налаштуйте віртуальний порт з номером 1 (Po1) на інтерфейсах f0/3 та f0/4 комутатора S1 та встановіть режим desirable. Увімкніть порт. Налаштуйте віртуальний порт із номером 1 на інтерфейсах f0/3 та f0/4 комутатора S2 та встановіть режим auto. Увімкніть його.

S1(config)# **interface range f0/3-4**
S1(config-if-range)# **channel-group 1 mode desirable**
Creating a port-channel interface Port-channel 1

S1(config-if-range)# **no shutdown**
S3(config)# **interface range f0/3-4**
S3(config-if-range)# **channel-group 1 mode auto**
Creating a port-channel interface Port-channel 1
S3(config-if-range)# **no shutdown**

```
*Mar  1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
*Mar  1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to up
S3(config-if-range)#
*Mar  1 00:09:15.384: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
*Mar  1 00:09:16.265: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,
changed state to up

S3(config-if-range)#

Mar  1 00:09:16.357: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
*Mar  1 00:09:17.364: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1,
changed state to up

*Mar  1 00:09:44.383: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

Крок 2: Перевірка коректності налаштувань

Інтерфейси F0/3, F0/4 і логічний інтерфейс Po1 (Port-channel 1) на комутаторах S1 і S3 повинні перебувати в режимі access operational і в стані desirable і dynamic відповідно.

Для перевірки використовуйте команду:

show interfaces interface-id **switchport**

Нижче наведено приклад результату виконання команди:

```
S1# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access (member of bundle Po1)
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: noneAdministrative private-vlan
trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none

Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Для перевірки об'єднання портів у логічний канал використовуйте команду

show etherchannel summary

```
S3# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3      S - Layer2
U - in use      f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
1      Po1(SU)         PAgP      Fa0/3(P)    Fa0/4(P)
```

```
S3# show etherchannel summary

Flags:  D - down
P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use      f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
1      Po1(SU)         PAgP      Fa0/3(P)    Fa0/4(P)
```

S3# show etherchannel summary

```
Flags:  D - down
P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use      f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
1      Po1(SU)         PAgP      Fa0/3(P)    Fa0/4(P)
```

Чому встановлено прапори SU та P?
Результати перевірки відобразіть у протоколі.

Крок 4: Конфігурування транкових портів

Для спільної роботи портів, об'єднаних у канал Ether Channel, створіть trunk-з'єднання. Для цього, використовуючи команду interface port-channel № інтерфейсу, конфігуруйте логічний інтерфейс Po1 на S1 та S3 для роботи в режимі trunk та призначте йому native VLAN 99.

Крок 5: Перевірка коректности налаштувань

Використовуйте команди show interfaces trunk та show spanning-tree на S1 та S3 для перевірки коректності налаштувань. Який порт і native VLAN відображаються? Яка оцінка (port cost) та пріоритет (port priority) логічного інтерфейсу? Результати відобразіть у протоколі.

Частина 3. Налаштування протоколу LACP

Крок 1: Конфігурування лінка між комутаторами S1 та S2 з використанням протоколу LACP.

a. Конфігуруйте лінк між комутаторами S1 та S2 як логічний канал Po2 та використовуйте протокол LACP для його створення. Для створення логічного каналу використовуйте команду **channel-group № каналу mode active (passive).** Для спільної роботи портів, об'єднаних у канал Ether Channel, створіть trunk-з'єднання та конфігуруйте логічний інтерфейс Po2 на S1 та S2 для роботи в режимі trunk. Транковому з'єднанню призначте native VLAN 99.

Крок 2: Перевірка коректності налаштувань
Використовуйте відповідні команди для перевірки коректності налаштувань.

Крок 3: Конфігурування лінка між комутаторами S2 та S3 з використанням протоколу LACP.

a. Конфігуруйте лінк між комутаторами S2 та S3 як логічний канал Po3 та використовуйте протокол LACP для його створення. Для створення логічного каналу використовуйте команду **channel-group № каналу mode active (passive)**. Для спільної роботи портів, об'єднаних у канал Ether Channel, створіть trunk-з'єднання та конфігуруйте логічний інтерфейс Po2 на S1 та S2 для роботи в режимі trunk. Транковому з'єднанню призначте native VLAN 99.

b. Перевірте наявність сформованого каналу.

Крок 4: Перевірка зв'язності мережі

За допомогою команди ping перевірте, чи є зв'язок між комп'ютерами. Результати відобразіть у протоколі.

Вміст протоколу

У протоколі має бути відображено назву даної роботи, її мету, результати виконання домашнього завдання, результати виконання лабораторного завдання, висновки за результатами виконаної роботи.

Література

1. Астраханцев А.А., Безрук В.М. Маршрутизація в мережах зв'язку: навч. посіб. Х.: ТОВ «Компанія СМІТ», 2011. 368 с.

3. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. Комп'ютерні мережі. Книга 1: навч. посіб. (рекомендовано МОН України). Львів: «Магнолія 2006», 2021. 256 с.

4. Тарнавський Ю. А., Кузьменко І. М.. Організація комп'ютерних мереж: підручник: для студ. Київ : КПІ ім. Ігоря Сікорського, 2018. 259 с.

5. Tanenbaum A., Feamster N., Wetherall D. Computer Networks. 6th Edition: Pearson Education, 2020. 960 p. URL: https://www.amazon.com/

6. The Cisco Learning Network. URL:https://learningnetwork.cisco.com/s/

ЛАБОРАТОРНА РОБОТА №6

Налаштування фільтрації трафіка в IP-мережі. Конфігурування стандартного ACL

Мета роботи

1 Набуття практичних навичок конфігурування стандартного списку доступу до IP-мережі.

2 Аналіз функціонування IP-мережі з функціями фільтрації трафіку.

Ключові положення

У мережах списки доступу (Access Control List, ACL) представляють список правил, що визначають порти служб або імена доменів, доступних на вузлі або іншому пристрої третього рівня OSI, кожен зі списком вузлів та/або мереж, яким дозволено доступ до сервісу. Мережеві ACL можуть бути налаштовані як на звичайному сервері, так і на маршрутизаторі і можуть керувати як вхідним, так і вихідним трафіком як міжмережевий екран.

Списки доступу використовуються в ряді випадків і є загальним механізмом завдання умов, які маршрутизатор перевіряє перед виконанням будь-яких дій. Деякі приклади використання списків доступу:

Керування передачі пакетів на інтерфейсах.

Управління доступом до віртуальних терміналів маршрутизатора та управління через SNMP.

Обмеження інформації, що передається динамічними протоколами марщрутизації.

Списки доступу або нумеруються, або називаються. Використання нумерованих або іменованих списків доступу визначається їх застосуванням (деякі протоколи вимагають використання тільки нумерованих списків, деякі - допускають як іменовані, так і нумеровані списки).

Якщо використовуються нумеровані списки, то номери їх мають лежати у певних діапазонах, залежно від сфери застосування списку.

Деякі діапазони, що найчастіше застосовуються, наведені нижче:

Протокол Діапазон нумерів
Стандартный список IP 1 to 99
Расширенный список IP 100 to 199
MAC Ethernet address 700 to 799
IPX 800 to 899
Extended IPX 900 to 999
IPX SAP 1000 to 1099

Завдання та правила побудови списків доступу для різних протоколів різні, але в загальному можна виділити два етапи роботи з будь-якими списками доступу. Спочатку необхідно створити список доступу, потім застосувати його до відповідного інтерфейсу, лінії або логічної операції, що виконується маршрутизатором.

Списки доступу визначають критерії, на відповідність яким перевіряється кожен пакет, оброблюваний маршрутизатором на точці списку доступу.

Типовими критеріями є адреси відправника та отримувача пакету, тип протоколу. Однак для кожного конкретного протоколу існує свій власний набір критеріїв, які можна задавати в списках доступу.

Список доступу в цілому представляє собою набір рядків з критеріями, які мають один і той самий номер (або ім'я). Кожен критерій у списку доступу записується окремим рядком.

Доповнення списку новими критеріями здійснюється в кінець списку. Неможливо виключити який-небудь критерій зі списку. Є тільки можливість стерти весь список цілком.

Порядок задавання критеріїв у списку суттєвий. Перевірка пакету на відповідність списку здійснюється послідовним застосуванням критеріїв з цього списку (у тому порядку, в якому вони були введені). Якщо пакет задовольняє хоча б одному з критеріїв, то подальші перевірки його на відповідність наступним критеріям у списку не проводяться.

В кінці кожного списку системою додається неявне правило «Запретити все» (Deny any). Таким чином, пакет, який не відповідає жодному з введених критеріїв, буде відхилений.

Оскільки порядок рядків у списку доступу дуже важливий, а також оскільки неможливо змінити цей порядок або виключити які-небудь рядки з існуючого списку доступу, рекомендується створювати списки доступу на *tftp-сервері* та завантажувати їх цілком у маршрутизатор, а не намагатися редагувати їх на маршрутизаторі.

Крім того, якщо список доступу з даним номером (ім'ям) існує, то рядки з тим самим номером (ім'ям) будуть додаватися до існуючого списку в кінець його. Тому першою строкою в файлі, що містить опис списку доступу для завантаження з *tftp-сервера,* має стояти команда скасування цього списку "no access-list "..

Для кожного протоколу на інтерфейс може бути призначений тільки один список доступу. Для більшості протоколів можна задати окремі списки для різних напрямків трафіку.

Якщо список доступу призначений на вхідний трафік через інтерфейс, то при отриманні пакету маршрутизатор перевіряє критерії, задані в списку. Якщо пакет дозволено цим списком, то він передається для подальшої обробки. Якщо пакет заборонено, то він відкидається.

Якщо список доступу призначений на вихідний трафік через інтерфейс, то після прийняття рішення про передачу пакету через цей інтерфейс маршрутизатор перевіряє критерії, задані в списку. Якщо пакет дозволено цим списком, то він передається в інтерфейс. Якщо пакет заборонено, то він відкидається.

Підтримуються наступні види списків доступу для IP:

Стандартні списки доступу (перевіряють адресу відправника пакету)

Розширені списки доступу (перевіряють адресу відправника, адресу отримувача і ще ряд параметрів пакету)

Динамічні розширені списки доступу

При створенні стандартного списку доступу критерії записуються послідовно в такому форматі:

access-list access-list-number {deny | permit} source [source-wildcard]

Приклад:

access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.0.0 0.0.255.255

Дозволяється проходження пакетів з адресами в блоці **192.168.0.0/16** за винятком адрес **192.168.1.0/24**.

Зверніть увагу на порядок запису критеріїв. Запис їх в іншому порядку призведе до того, що друге умова не буде працювати ніколи. Зверніть увагу на запис маски: на відміну від методу запису маски на мережевих інтерфейсах, маска в списках доступу записана інверсно, одиницями позначені біти, які НЕ будуть перевірятися.

Часто використовуване опис фільтра, якому задовольняє будь-яка адреса **0.0.0.0 255.255.255.255**, має спеціальне позначення "**any**"

access-list access-list-number {deny | permit} any

Якщо на інтерфейс призначений список доступу, який не визначений у конфігурації, вважається, що жоден список не призначено і фільтрація пакетів не буде проводитися. Нагадуємо, що як тільки буде введено хоча б один критерій з цим номером/іменем списку доступу, після нього з'явиться критерій **Deny any**, який додається в кінець всього існуючого списку доступу. Тому, щоб уникнути повної блокування системи при створенні списків доступу, слід:

– або скасувати призначення списку доступу на інтерфейс перед редагуванням списку і призначати на інтерфейс тільки повністю сформовані та перевірені списки,
– або створювати і редагувати списки доступу на **tftp-сервері** та завантажувати в маршрутизатор повністю сформовані та перевірені списки доступу.

Ключові питання

1 Вкажіть основне призначення списків доступу.
2 Вкажіть типи списків доступу.
3 Що являє собою wildcard-маска?
4 Наведіть синтаксис стандартного списку доступу.
5 Яка процедура конфігурування списку доступу?
6 Як здійснюється фільтрація трафіку за допомогою шаблону та wildcard-маски?
7 Вкажіть діапазони номерів списків доступу для протоколу IP.
8 Як опрацьовуються правила списку доступу?
9 Вкажіть команду фільтрації трафіку списком доступу від одного хоста.
10 Вкажіть команду, яка стоїть наприкінці списку доступу.

Домашнє завдання

1 Вивчіть, користуючись рекомендованою літературою, а також цим методичним посібником, ключові особливості технології ACL.

2 Підготуйтеся до співбесіди за ключовими питаннями п.3.

3 Проаналізуйте план виконання лабораторної роботи, керуючись п.5.

Завдання до лабораторної роботи

1. Побудова мережі.

2 Налаштування базових установок пристроїв та перевірка зв'язків.

3 Реалізація політики фільтрації трафіку за допомогою стандартних списків доступу.

4 Перевірка коректності налаштувань

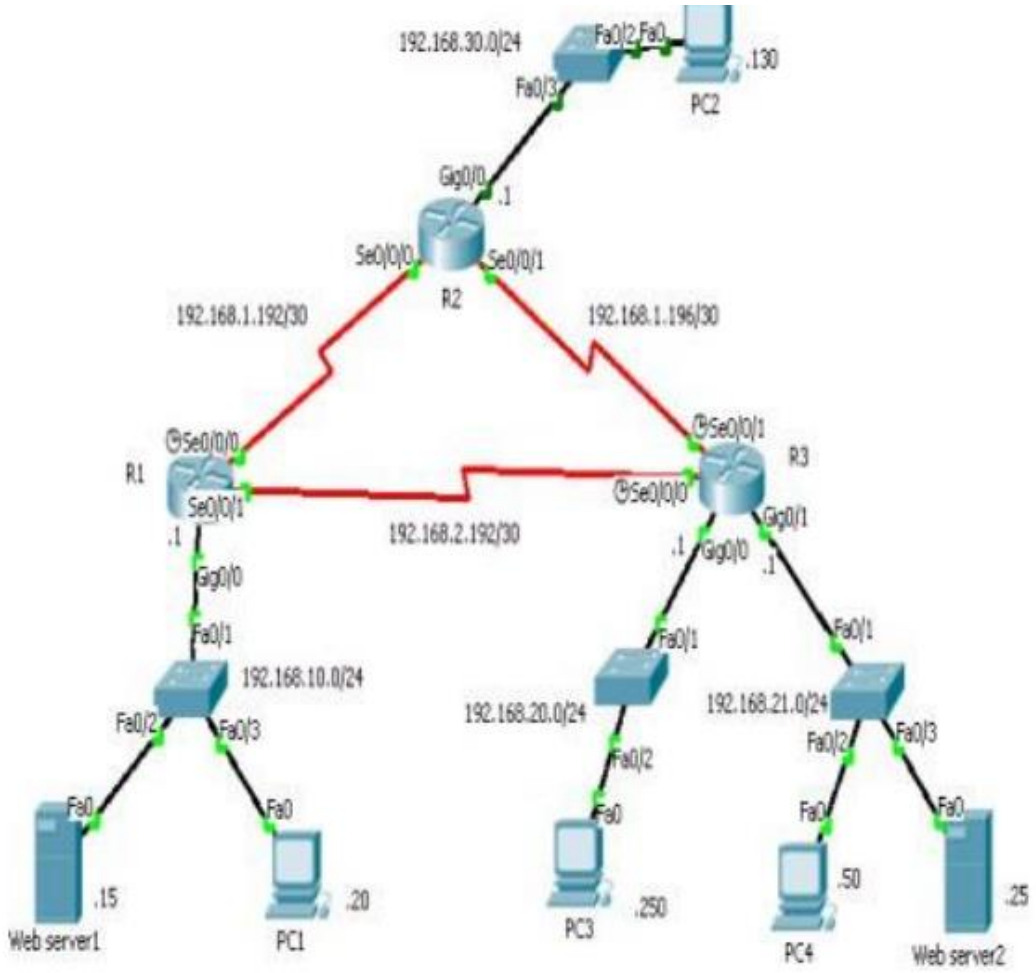

Рисунок 5.1 – Топологія мережі

Необхідне обладнання:

– 4 комутатори Cisco XXXX із образом Cisco IOS (lanbasek9).

– 3 маршрутизатори Cisco XXXX з інтегрованими сервісами (ISR) із образом Cisco IOS (universalk9).

– 2 Web-сервери.

– 4 ПК (Windows 10, 11 із програмою емуляції терміналу, такою як Tera Term, Putty).

– Консольні кабелі для конфігурування пристроїв Cisco IOS через консольний порт.

– Кабелі Ethernet для створення мережі.

Таблиця 5.1 – Адресна схема мережі

Device	Interface	IPv4 Address	Default Gateway
R1	G0/0	192.168.10.1/24	N/A
	S0/0/0	192.168.1.193/30	N/A
	S0/0/1	192.168.2.193/30	N/A
R2	G0/0	192.168.30.1/24	N/A
	S0/0/0	192.168.1.194/30	N/A
	S0/0/1	192.168.2.197/30	N/A
R3	G0/0	192.168.20.1/24	N/A
	G0/1	192.168.21.1/24	N/A
	S0/0/0	192.168.2.194/30	N/A
	S0/0/1	192.168.2.198/30	N/A
PC-1	NIC	192.168.10.20	192.168.10.1
PC-2	NIC	192.168.30.130	192.168.30.1
PC-3	NIC	192.168.20.250	192.168.20.1
PC-4	NIC	192.168.21.50	192.168.21.1
Web server1	NIC	192.168.10.15	192.168.10.1
Web server2	NIC	192.168.21.25	192.168.21.1

Крок 2: Ініціалізуйте та перезавантажте пристрої, якщо це необхідно.

Виконайте команду: **R1#show startup-config**. *Я*кщо файл *startup-config* присутній, виконайте:

R1#**erase startup-config**

R1#**reload**

Частина 2: Налаштування базових параметрів пристроїв і перевірка зв'язку

У частині 2 необхідно налаштувати базові параметри пристроїв, такі як ім'я пристрою, паролі для обмеження доступу до режимів роботи пристрою, IP-адреси інтерфейсів.

Крок 1: Налаштуйте параметри протоколу IP на комп'ютерах (IP-адресу, маску підмережі, IP-адресу шлюзу за замовчуванням). Присвойте комп'ютерам імена.

Крок 2: Налаштування базових параметрів маршрутизаторів.
а. Налаштуйте імена пристроїв відповідно до топології.
б. Вимкніть функцію DNS lookup.
с. Вкажіть onat як пароль доступу до привілейованого режиму пристрою.
г. Збережіть поточну конфігурацію пристрою у файлі startup.

Крок 3: Налаштування параметрів IP на маршрутизаторах.
а. Налаштуйте IP-адреси на інтерфейсах маршрутизаторів R1 - R3 відповідно до таблиці адрес.
б. Налаштуйте протокол маршрутизації на маршрутизаторах R1 - R3 або сконфігуруйте статичні маршрути.

Крок 4: Перевірка зв'язку.
а. Перевірте за допомогою команди **ping** зв'язок кожного ПК із шлюзом за замовчуванням, який був налаштований для цього хоста.
б. Перевірте за допомогою команди **ping** з'єднання між безпосередньо підключеними маршрутизаторами.
с. Перевірте зв'язок між пристроями, які безпосередньо не з'єднані між собою.

Результати роботи, виконаної на кроці 4, зафіксуйте в протоколі.

Частина 3: Реалізація політики фільтрації трафіку за допомогою стандартних списків доступу

Крок 1: Необхідно реалізувати таку політику:

a. Мережа *192.168.21.0/24* не повинна мати доступу до *Web-сервера1*.
b. Мережа *192.168.30.0/24* не повинна мати доступу до мережі *192.168.20.0/24*.
c. Всі інші взаємодії дозволені.

Частина 4: Перевірка коректності налаштувань

a. Виконайте команду **show access-list** для перевірки правильності налаштування списків доступу.
b. Для перевірки коректності налаштування інтерфейсу виконайте команди **show run** і **show ip interface interface**.
c. Перевірте правильність фільтрації трафіку за допомогою команди **ping**.
Результати перевірки коректності налаштувань внесіть у протокол.

Зміст протоколу

У протоколі має бути відображено назву даної роботи, її мету, результати виконання домашнього завдання, результати виконання лабораторного завдання, висновки за результатами виконаної роботи.

Література

1. Астраханцев А.А., Безрук В.М. Маршрутизація в мережах зв'язку: навч. посіб. Х.: ТОВ «Компанія СМІТ», 2011. 368 с.
3. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. Комп'ютерні мережі. Книга 1: навч. посіб. (рекомендовано МОН України). Львів: «Магнолія 2006», 2021. 256 с.
4. Тарнавський Ю. А., Кузьменко І. М.. Організація комп'ютерних мереж: підручник: для студ. Київ : КПІ ім. Ігоря Сікорського, 2018. 259 с.
5. Tanenbaum A., Feamster N., Wetherall D. Computer Networks. 6th Edition: Pearson Education, 2020. 960 p. URL: https://www.amazon.com/
6. The Cisco Learning Network. URL:https://learningnetwork.cisco.com/s/