**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА**

ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра радіотехніки та радіоелектронних систем

«На правах рукопису»

Робота допущена до захисту в ЕК
рішенням кафедри радіотехніки та радіоелектронних систем
від _____, протокол №___.
Завідувач кафедри доктор фіз.-мат. наук, професор
_____ Ігор АНІСІМОВ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

# «ПРОЄКТ КОРПОРАТИВНОЇ ІНТЕРНЕТ МЕРЕЖІ В CISCO PACKET TRACER»

**Виконав:**
студент 4 -го курсу
денної форми навчання
спеціальності 172 - Телекомунікації та радіотехніка
ОПП «Інформаційна безпека телекомунікаційних систем і мереж»
Гуржин Віталій Віталійович _____

**Науковий керівник**:
кандидат фіз.-мат. наук, асистент
Богданов Роман Вікторович _____

Рецензент:
кандидат технічних наук, асистент
кафедри комп'ютерної інженерії
Слюсар Євген Андрійович _____

Засвідчую, що у цій бакалаврській роботі
немає запозичень з праць інших авторів
без відповідних посилань
Студент _____ Віталій ГУРЖИН

Київ – 2025

# РЕФЕРАТ

Дипломний проєкт, 30 с., 21 рис., 5 табл., 10 джерел.

ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ, CISCO PACKET TRACER, ЖИТТЄВИЙ ЦИКЛ УПРАВЛІННЯ МЕРЕЖЕЮ.

Об'єкт дослідження – корпоративна телекомунікаційна мережа, створена за допомогою Cisco Packet Tracer.

Мета проєкту – комплексне проектування, налаштування та тестування моделі захищеної корпоративної мережі з використанням сучасних протоколів сегментації та моніторингу в середовищі симуляції Cisco Packet Tracer.

Оригінальність роботи полягає в комплексному підході до проєктування, що об'єднує не лише базові налаштування сегментації (VLAN) та безпеки (ACL), але й інтеграцію одразу трьох ключових інструментів моніторингу (Syslog, SNMP, NetFlow) в єдиній моделі. Це дозволяє продемонструвати повний життєвий цикл управління невеликою корпоративною мережею: від створення до моніторингу та аналізу її стану.

Основні цілі:

– Спроєктувати логічну топологію корпоративної мережі, що включає три окремі функціональні підрозділи.

– Реалізувати сегментацію мережі за допомогою технології віртуальних локальних мереж (VLAN) та налаштувати маршрутизацію між ними.

– Впровадити політики безпеки для розмежування доступу до мережевих ресурсів за допомогою списків контролю доступу (ACL).

– Налаштувати та перевірити роботу ключових протоколів моніторингу та управління мережею: Syslog, SNMP та NetFlow.

# ПЕРЕЛІК СКОРОЧЕНЬ

IP – Internet Protocol (інтернет протокол)

ACL – Access Control List (access-list, список контролю доступу, список доступу)

SysLog – System Logging (системне логування)

MAC – Media Access Control (керування доступом до посередників)

VLAN – Virtual Local Area Network (віртуальна локальна мережа)

WAN – Wide Area Network (глобальна мережа)

WPA – Wireless Protected Access (захищений доступ до бездротової мережі)

ICMP – Internet Control Message Protocol (міжмережевий протокол контрольного повідомлення)

SNMP – Simple Network Management Protocol (простий протокол керування мережею)

NetFlow – Network Flow (Мережевий Потік)

# ЗМІСТ

# ВСТУП

В епоху цифрової трансформації функціонування сучасних підприємств є нерозривно пов'язаним з надійністю, безпекою та ефективністю їхніх інформаційних інфраструктур. Корпоративні телекомунікаційні мережі перестали бути лише допоміжним інструментом і перетворилися на критично важливий актив, що забезпечує обмін даними, доступ до хмарних сервісів, внутрішню комунікацію та взаємодію з клієнтами.

Однак зі зростанням масштабів та складності корпоративні мережі стикаються з низкою суттєвих викликів. По-перше, це проблема безпеки. Несегментовані мережі є вкрай вразливими: один скомпрометований пристрій може стати точкою входу для атаки на всю інфраструктуру. Несанкціонований доступ співробітників до критичних ресурсів також становить значний ризик. По-друге, це питання керованості та масштабованості. Збільшення кількості пристроїв та обсягів трафіку ускладнює адміністрування, призводить до перевантажень та зниження продуктивності. По-третє, це відсутність прозорості та засобів проактивного реагування. Без інструментів моніторингу адміністратори змушені реагувати на проблеми вже після їх виникнення, замість того, щоб запобігати їм, аналізуючи стан мережі в реальному часі.

Сучасний підхід до побудови корпоративних мереж пропонує комплексне вирішення цих проблем. Технологія віртуальних локальних мереж (VLAN) дозволяє логічно сегментувати мережу, ізолюючи трафік різних підрозділів та підвищуючи рівень безпеки. Списки контролю доступу (ACL) надають гранулярний інструмент для фільтрації трафіку та розмежування прав доступу до ресурсів. Водночас інтеграція протоколів моніторингу, таких як Syslog, SNMP та NetFlow, забезпечує всебічну видимість стану мережі, дозволяючи відстежувати події, аналізувати потоки даних та своєчасно виявляти підозрілу активність або збій у її роботі.

# РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ МОДЕЛЮВАННЯ

## 1.1. Порівняльний аналіз програмних засобів для моделювання телекомунікаційних мереж

Телекомунікаційною мережею називають сукупністю термінальних і проміжних вузлів, з’єднаних каналами зв’язку таким чином, щоб між будь-якими двома терміналами можна було обмінюватися інформацією. [1]

Усередині мережевого обладнання традиційно виділяють три “площини” або логічні рівні. Площина керування відповідає за прийняття рішень, зокрема за побудову й оновлення таблиць маршрутизації, визначення оптимального шляху для пакетів і політик безпеки. Площина передачі даних фактично пересилає пакети згідно з вказівками керування. Площина керування забезпечує адміністрування, моніторинг і конфігурування мережевих елементів. [1]

Канали зв’язку можуть бути дротовими (виті пари, коаксіальні кабелі, оптоволокно) або бездротовими (радіохвилі, супутниковий зв’язок), що визначає швидкість, довжину та стійкість з’єднання. Протоколи рівня каналу (наприклад, Ethernet) регулюють доступ до середовища, а мережеві протоколи (IP, BGP, OSPF) відповідають за маршрутизацію й доставку пакетів. [2]

Передача інформації відбувається завдяки взаємодії трьох взаємопов’язаних сфер: сукупності обладнання й каналів, набору правил (протоколів) та алгоритмів маршрутизації й комутації. Телекомунікаційна мережа являє собою організовану систему, де пристрої (вузли) й канали зв’язку об’єднуються в єдине ціле, щоб на будь-які відстані передавати голос, дані чи відео. Кожен її елемент відіграє свою роль: обладнання генерує й приймає інформацію, канали доставляють сигнали (пакети даних), а протоколи й алгоритми гарантують упорядкованість і надійність обміну. [2]

Моделювання телекомунікаційних мереж є невід'ємним етапом їх проєктування, тестування та вивчення. Воно дозволяє перевіряти складні конфігурації, аналізувати потоки трафіку та відпрацьовувати навички

адміністрування без ризику для реальної інфраструктури та без потреби у дорогому фізичному обладнанні. На сучасному ринку існує два фундаментально різних підходи до моделювання: симуляція та емуляція. Розуміння різниці між ними є ключовим для вибору оптимального інструменту для конкретних завдань. [3]

Симулятори, яскравим представником яких є Cisco Packet Tracer, створюють програмну модель мережевих пристроїв та протоколів [3]. Вони не виконують реальний код операційної системи, а лише імітують його поведінку на основі заздалегідь запрограмованих алгоритмів [4]. Емулятори, такі як GNS3, йдуть іншим шляхом: вони створюють віртуальне середовище (віртуальну машину), в якому запускається справжній, немодифікований образ операційної системи мережевого пристрою (наприклад, Cisco IOS). Це забезпечує максимальний реалізм, але висуває значно вищі вимоги до елементів комп'ютерного заліза. [4]

Cisco Packet Tracer — це віртуальне середовище для моделювання та симуляції комп’ютерних мереж, створене компанією Cisco Systems. Основне його призначення — надати студентам, викладачам та початківцям-мережевикам можливість практикуватися в проєктуванні, налаштуванні й дослідженні мереж без необхідності використання справжнього обладнання. Завдяки цьому можна швидко перевіряти різні конфігурації, експериментувати з протоколами та інструментами без ризику порушити роботу реальної інфраструктури. [3]

У Packet Tracer користувачі будують віртуальні топології, перетягуючи на робоче поле маршрутизатори, комутатори, точки доступу, сервери й кінцеві пристрої. Підключення між ними імітуються різними типами кабелів, тому можна відтворити сценарії від простої локальної мережі до складних багаторівневих архітектур із VLAN, WAN-зв’язками та бездротовими сегментами. Особливість програми в тому, що вона підтримує два режими роботи: реальну передачу пакетів і покрокову симуляцію, коли видно, як дані

проходять через кожен пристрій і як спрацьовують налаштовані правила чи протоколи. [3]

Програма дозволяє відпрацьовувати налаштування різноманітних протоколів — від базових IP-адресації і статичної маршрутизації до динамічних протоколів (OSPF, EIGRP), комутаційних механізмів (VLAN), сервіси безпеки (ACL, шифрування Wi-Fi, VPN), протоколи відстежування мережевого трафіку та надання інформації щодо компонентів мережі (NetFlow, SysLog, SNMP) а також створювати віртуальні сервери для DNS, DHCP, HTTP тощо. [3]

GNS3 (Graphical Network Simulator-3) є емулятором з відкритим вихідним кодом, що дозволяє створювати віртуальні мережі з використанням реальних образів операційних систем. Забезпечується найвищий рівень реалізму, оскільки віртуальні пристрої поводяться ідентично до своїх фізичних аналогів. Це досягається завдяки інтеграції з технологіями віртуалізації, такими як Dynamips (для емуляції старих апаратних платформ Cisco), KVM (Kernel-based Virtual Machine) та VirtualBox/VMware. Такий підхід забезпечує найвищий рівень реалізму, оскільки віртуальний пристрій у GNS3 поводиться абсолютно ідентично до свого фізичного аналога, з повним набором команд та функцій. [4]

GNS3 є мультивендорною платформою, що підтримує обладнання не тільки Cisco, але й Juniper, Arista та інших виробників. Недоліками є високі вимоги до апаратних ресурсів комп'ютера (CPU та RAM), а також складніший процес початкового налаштування, що вимагає від користувача самостійного імпорту образів ОС. [4]

Для вирішення поставлених завдань, а саме проєктування мережі з використанням VLAN, ACL та протоколів моніторингу, було обрано симулятор Cisco Packet Tracer. Цей вибір обґрунтований тим, що програма повністю підтримує необхідний функціонал, не вимагаючи значних апаратних ресурсів. На відміну від емуляторів GNS3, Packet Tracer надає зручний інтерфейс та цілком візуально зрозумілу логічну топологію, що є критично важливим для навчальних цілей та перевірки логіки роботи ACL. Не останню роль тут відіграє й різниця у

системних вимогах при використанні віртуальних машин та сторонніх програм – лише достатньо потужна система зможе в повній мірі реалізувати функціонал проєктів на GNS3. Крім того, наявність вбудованих серверів для Syslog та колектора NetFlow дозволило реалізувати всі завдання моніторингу в рамках єдиного середовища.

# РОЗДІЛ 2. ПРОЄКТ КОРПОРАТИВНОЇ МЕРЕЖІ

## 2.1. Призначення та функціонал основних компонентів мережі

На рисунку 2.1 зображено логічну топологію мережі, сама мережа ділиться на три підрозділи (відділи), доступ до інтернету у кожному з підрозділів реалізується бездротовим підключенням за допомогою точки доступу (Access Point).

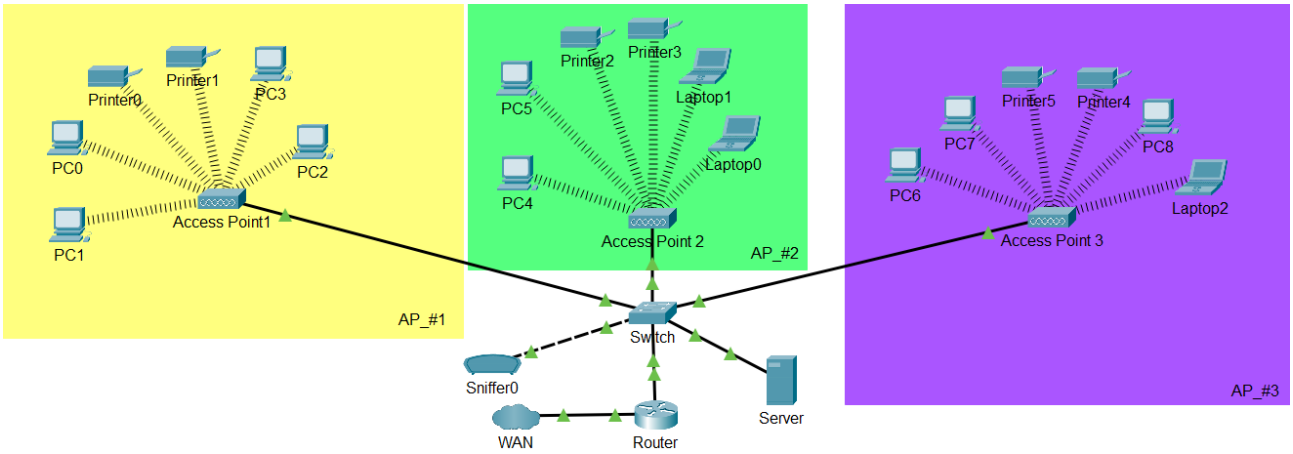



Рис.2.1. Логічна топологія корпоративної мережі

Точка доступу тут виконує роль бездротового роутера і була обрана для побудови мережі здебільшого для простоти налаштування в подальшому, так як додатково до змін конфігурації комутатора і роутера потрібно було б змінювати конфігурації бездротового, у якого інтерфейс налаштування відрізняється від попередньо зазначених пристроїв, а саме відсутність командної строки, тому, у ролі «репітеру» сигналу було обрано точку доступу. У сучасних мережах роль усіх передавальних пристроїв може виконувати бездротовий маршрутизатор (роутер) до якого підключене оптоволокно через WAN інтерфейс. Передача інтернет-сигналу та маршрутизація повідомлень реалізується за допомогою роутера, який підключений до умовного «ядра», позначеного у топології як WAN. Комутатор виконує розподіл підрозділів мережі на три віртуальні локальні мережі (VLAN), які можна позначити як підмережі.

## 2.2. Конфігурація віртуальних мереж

Віртуальна локальна мережа (Virtual Local Area Network, VLAN) — це технологія, що дозволяє логічно розділити єдиний фізичний комутатор на декілька незалежних внутрішніх доменів. Пристрої, що належать до різних VLAN, не можуть взаємодіяти між собою на канальному (Data Link) рівні OSI моделі (Layer 2), навіть якщо вони підключені до одного й того ж фізичного комутатора. [5]

Налаштування віртуальних мереж у командному рядку комутатора відбувається таким чином (на прикладі першого відділу) [6] (рис.2.2):

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#ex
Switch(config)#interface fa2/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#do wr
Building configuration...
[OK]
```

Рис.2.2. Конфігурація віртуальних мереж на комутаторі

Switch>en (enable) – перехід з режиму користувача у режим адміністратора

#conf t (config terminal) – перехід до режиму глобальної конфігурації комутатора, зміни налаштувань віртуальних мереж

#vlan 10 – створює віртуальну локальну мережу і додає її до переліку мереж на комутаторі

#name VLAN10 – створення назви мережі

#interface fa2/1 – перехід до налаштування безпосередньо обраного інтерфейсу (порту)

#switchport mode access – встановлює порт у режим доступу, це означає, що порт працює лише з однією підмережею і він надає доступ кінцевим пристроям на користування портом

#switchport access vlan 10 – призначає створену підмережу до обраного інтерфейсу, тепер пристрої, підключені через точку доступу будуть відноситись до віртуальної мережі VLAN10

При налаштуваннях на роутері вказується вже віртуальний інтерфейс, який є частиною підключеного до комутатору фізичного інтерфейсу (рис.2.3)

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface g0/1.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#do wr
Building configuration...
[OK]
```

Рис.2.3. Конфігурація віртуальних мереж на роутері

#interface g0/1.10 – створює віртуальний інтерфейс у роутері, який відповадє за VLAN10. Завдяки створенню даних інтерфейсів, з'являється можливість створити декілька віртуальних мереж які будуть закріплені за одним портом

#encapsulation dot1Q 10 – вмикає маркування мережевого трафіку, який надсилається або надходить з/до VLAN10. Дана команда дає розуміти комутатору що повідомлення надходитиме саме з позначеної підмережі

#ip address 192.168.10.1 255.255.255.0 – встановлює внутрішню IP-адресу для підмережі та його маску. Для маршрутизації повідомлень, усі пристрої підмережі повинні мати ідентичну внутрішню адресу.

#no shutdown – мануально активує інтерфейс, активує усі вище введені налаштування

#do wr – зберігає конфігурацію у пам'ять пристрою

При налаштуванні, були вказані подібні IP-адреси та маски підмереж для простішої подачі інформації та полегшення мануальної конфігурації мережевих пристроїв (табл.№1)

Таблиця 1. Характеристика підмереж

| Порт комутатора | Назва підмережі | Внутрішня IP-адреса | Маска підмережі | Префікс |
|---|---|---|---|---|
| Fa2/1 | VLAN10 | 192.168.10.1 | 255.255.255.0 | /24 |
| Fa3/1 | VLAN20 | 192.168.20.1 | 255.255.255.0 | /24 |
| Fa0/1 | VLAN30 | 192.168.30.1 | 255.255.255.0 | /24 |

Усі підмережі подібні між собою, VLAN10 складаються з чотирьох ПК та двох принтерів (рис.8, табл.2) , у випадку з VLAN20 (рис.2.5, табл.3) та VLAN30 (рис.2.6, табл.4), ПК замінені ноутбуками (лептопами). Усі кінцеві пристрої у кожному з відділів об’єднані однією внутрішньою IP-адресою та унікальним паролем за стандартом захисту WPA2-PSK.

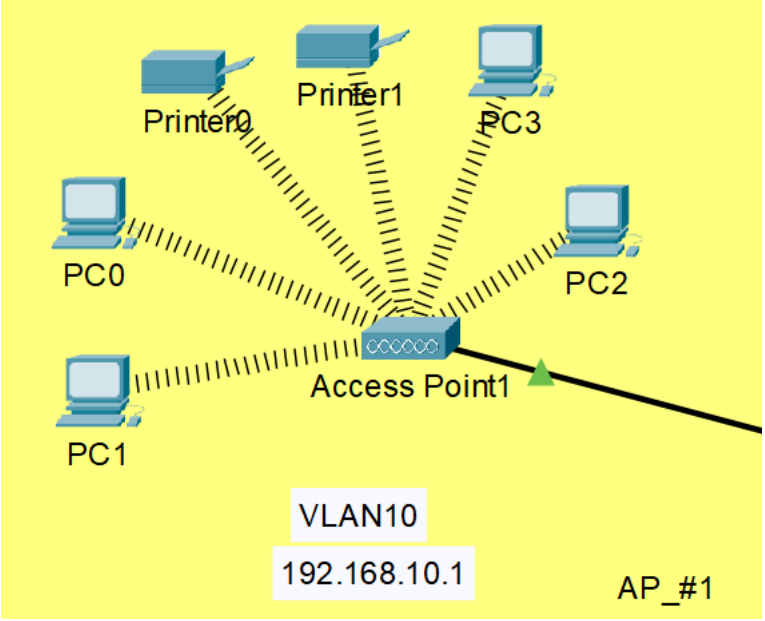



Рис.2.4. Вигляд VLAN10

Таблиця 2. Характеристика пристроїв VLAN10

| Назва пристрою | IP-адреса | MAC-адреса |
|---|---|---|
| PC0 | 192.168.10.10 | 0030.F247.D412 |
| PC1 | 192.168.10.11 | 00D0.D367.39BE |
| PC2 | 192.168.10.17 | 0001.6383.8352 |
| PC3 | 192.168.10.19 | 0001.63C4.AB68 |
| Printer0 | 192.168.10.20 | 0060.474E.6689 |
| Printer1 | 192.168.10.23 | 00D0.BC1C.E18C |

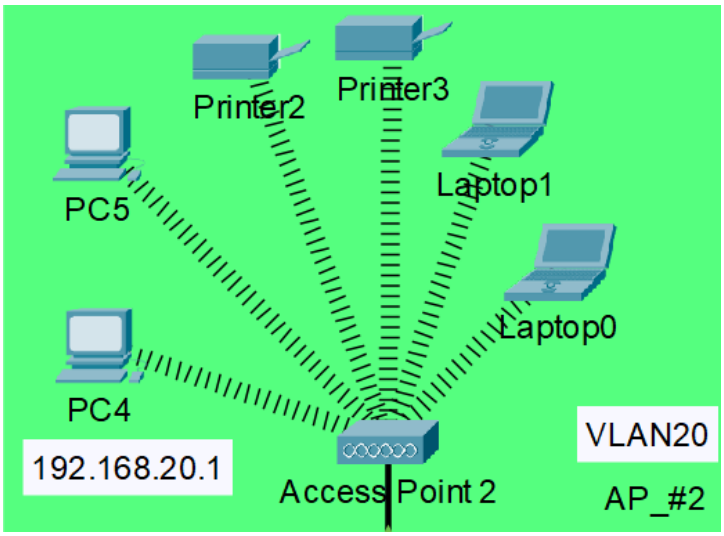



Рис.2.5. Вигляд VLAN20

Таблиця 3. Характеристика пристроїв VLAN20

| Назва пристрою | IP-адреса | MAC-адреса |
|---|---|---|
| PC4 | 192.168.20.14 | 0060.3E71.9921 |
| PC5 | 192.168.20.15 | 0001.97DA.EB62 |
| Laptop0 | 192.168.20.20 | 0060.4707.5DB1 |
| Laptop1 | 192.168.20.21 | 0001.4321.635C |
| Printer2 | 192.168.20.26 | 0001.6427.C764 |
| Printer3 | 192.168.20.25 | 0004.9A7A.4A7A |

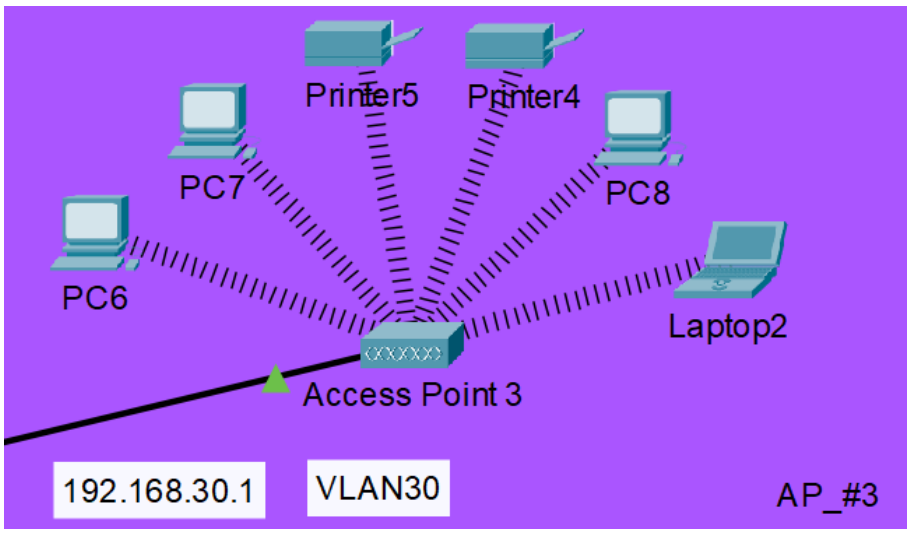



Рис.2.6. Вигляд VLAN30

Таблиця 4. Характеристика пристроїв VLAN30

| Назва пристрою | IP-адреса | MAC-адреса |
|---|---|---|
| PC6 | 192.168.30.18 | 0001.C9E8.9E64 |
| PC7 | 192.168.30.19 | 0007.EC1A.4E26 |
| PC8 | 192.168.30.22 | 000A.F347.1243 |
| Laptop2 | 192.168.30.12 | 000C.8530.7BB2 |
| Printer4 | 192.168.30.24 | 0030.F21D.3D60 |
| Printer5 | 192.168.30.27 | 00E0.F961.2540 |

Комунікація між підмережами налаштована встановленням режиму trunk на підключений до комутатора порт роутера Gig0/1, який оперує вже на мережевому (Network) рівні. Різниця між режимом trunk та вище згаданим режимом access полягає в тому, що trunk передаватиме трафік з багатьох VLAN по одному порту (кабелю), що необхідно для маршрутизації повідомлень, так як при відсутності trunk порту передача повідомлень між пристроями з різних підмереж буде або блокуватися або не буде оброблятися мережевими пристроями. [6]

На рисунку.2.7 зазначено, що комунікація між пристроями з різних підмереж присутня, при спробі відправлення PING запиту з пристрою з адресою 192.168.10.12 на адресу 192.168.30.18 усі згенеровані запити прийшли без втрат.

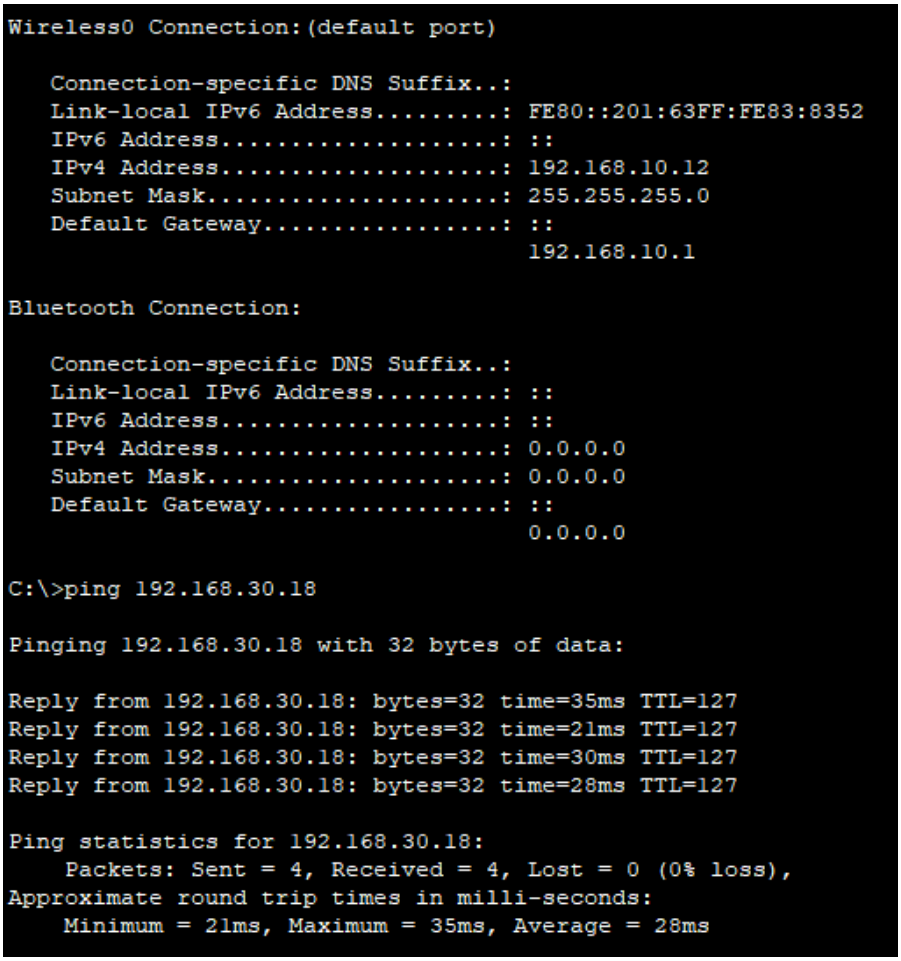



Рис.2.7. Перевірка комунікації між різними підмережами

## 2.3. Налаштування Access-lists в мережевих пристроях

При налаштуванні мережі, принтери, як і усі кінцеві пристрої, можуть отримувати запити також й з інших підмереж, що може викликати певні незручності у роботі відділів такі як втручання у процес друку або «заспамлювання» принтеру. Найдієвішим способом вирішити потенційну загрозу в роботі мережі - імплементування «списків доступу» (access-list) у конфігурацію мережі, завдяки яким можна заблокувати доступ до певної IP-адреси. Особливо це дієво коли у пристрої не вбудований фаєрвол та доступ до нього потрібно обмежити. [3]

Списки контролю доступу (ACL) — це набір послідовних правил, що застосовуються до інтерфейсів мережевих пристроїв (маршрутизаторів, комутаторів L3) для фільтрації трафіку. Кожне правило в ACL визначає, чи слід

"дозволити" (permit) чи "заборонити" (deny) пакет на основі заданих критеріїв, таких як IP-адреса джерела та призначення, протокол (TCP, UDP, ICMP тощо) та номери портів. ACL є фундаментальним інструментом для реалізації політик безпеки в мережі. «Список» створюється у роутері за допомогою таких команд (на прикладі надання доступу PC2, рис.2.8) [7]:

```
Router(config)#access-list 111 deny ip any host 192.168.10.20
Router(config)#access-list 111 permit ip host 192.168.10.17 host 192.168.10.20
Router(config)#do wr
```

Рис.2.8. Команди до налаштування «списку доступу»

При створенні access-list'у в першу чергу потрібно обрати нумерацію, списки під номерами «1-99» відносяться до стандартних налаштувань доступу, які, наприклад, можуть налаштовувати доступ до мережі лише одного IP. Розширені «списки» нумеруються зі «100-999» і можуть налаштовувати комунікацію між двома адресами. [7] [3]

#access-list 111 deny ip any host 192.168.10.20 – блокує весь мережевий трафік, який надходить на вказану адресу

#access-list 111 permit ip host 192.168.10.17 host 192.168.10.20 – дає дозвіл на отримання повідомлень з вказаного IP

Щоб застосувати список доступу, потрібно вказати порт до якого встановлено підключення з комутатором та додати «список» до його конфігурації:

#interface g0/1

#ip access-group 111 in – встановлення «списку доступу на мережевий інтерфейс

На рисунку 2.9 було проведено перевірку доступу до принтера з однакової підмережі, при надсиланні PING-запиту на його IP-адресу було отримано відповідь без жодних втрат у пакетах повідомлення, на рисунку 2.10 показано як реалізується подібний запит, якщо він надходить вже з іншої підмережі – його запит блокується, так як мережевий доступ до даного принтера мають лише ПК з підмережі VLAN10, що підтверджує коректність роботи «списків доступу».

```
Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::230:F2FF:FE47:D412
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.10.17
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.10.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.10.20

Pinging 192.168.10.20 with 32 bytes of data:

Reply from 192.168.10.20: bytes=32 time=37ms TTL=128
Reply from 192.168.10.20: bytes=32 time=22ms TTL=128
Reply from 192.168.10.20: bytes=32 time=27ms TTL=128
Reply from 192.168.10.20: bytes=32 time=27ms TTL=128

Ping statistics for 192.168.10.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 37ms, Average = 28ms
```

```
Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::207:ECFF:FE1A:4E26
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.30.19
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.30.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.10.20

Pinging 192.168.10.20 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рис.2.9-2.10. Перевірка дії «списку доступу»

# РОЗДІЛ 3. ПІДКЛЮЧЕННЯ СЕРВЕРУ ТА КОНФІГУРУВАННЯ ПРОТОКОЛІВ ВІДСТЕЖЕННЯ ТРАФІКУ МЕРЕЖІ

## 3.1. Системне логування SysLog

SysLog це протокол, який обробляє повідомлення про стан системи мережевих пристроїв. Завдяки ньому можна провести моніторинг роботи пристроїв, виявляти які помилки виникли у їх роботі в точний час, перевірити зміну підключення портів, вимкнення/увімкнення мережевих пристроїв, тощо. Усі перелічені повідомлення надсилаються та зберігаються на сервері. Повідомлення поділяються на 7 рівнів (табл.№5) [1]:

Таблиця 5. Опис повідомлень SysLog

| Рівень | Тип повідомлення | Опис |
|---|---|---|
| 1 | Невідкладне (emergency) | Вихід з ладу мережевого пристрою |
| 2 | Важливе попередження (alert) | Вихід з ладу інтерфейсу на який підключена точка доступу |
| 3 | Критичне (critical) | Помилки в роботі мережі, блокуванні передачі повідомлень |
| 4 | Помилка (error) | Помилки при конфігуруванні пристроїв |
| 5 | Сповіщення конфігурації (config) | Повідомлення про зміну стану портів або конфінурації |
| 6 | Інформаційний (informational) | Надання загальної інформації щодо конфігурації пристроїв |
| 7 | Відладка (debugging) | Діагностика |

Реалізація системного логування проходить таким чином:

До комутатора мережі під'єднується сервер (рис.3.1), порт по якому його було підключено додається до однієї з VLAN, записується її внутрішня IP-адреса та маска, і встановлюється IP вже самого пристрою.

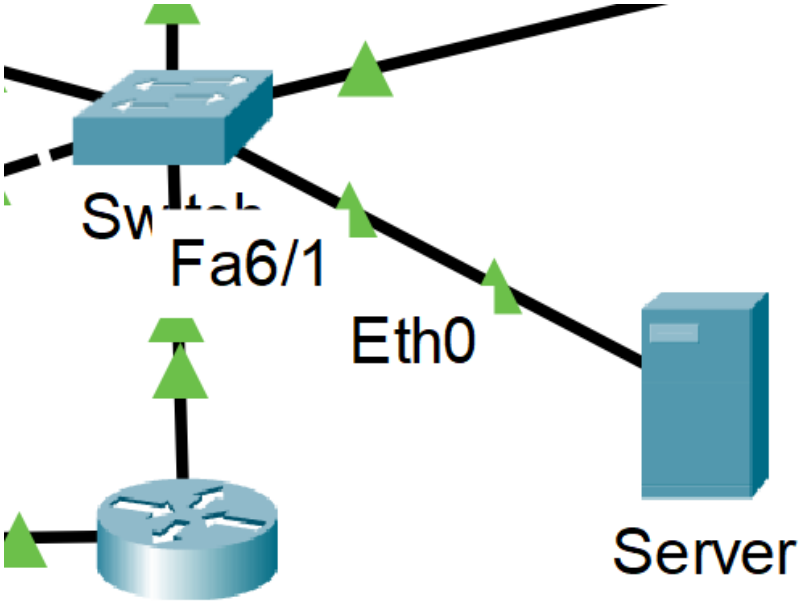



Рис.3.1. Топологія підключення серверу

Щоб мережеві пристрої мали змогу передавати «логи», комутатору потрібно надати віртуальну адресу, створивши окремий віртуальний інтерфейс і додати конфігурацію logging (рис.3.2):

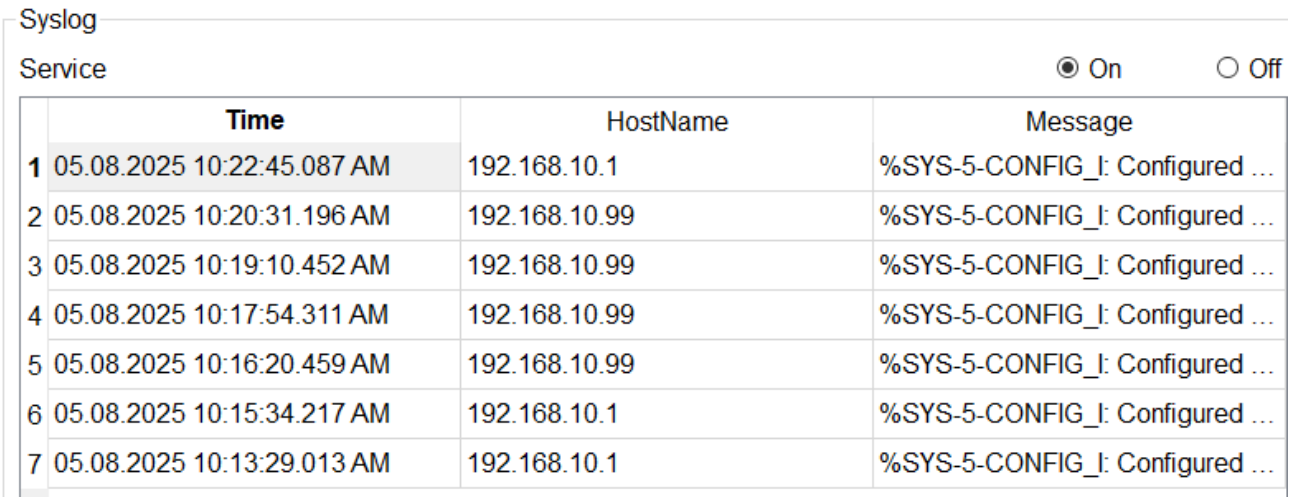
```
logging trap debugging
logging 192.168.10.100
```

Рис.3.2. Команди до конфігурації SysLog

#logging trap debugging – встановлення передачі SysLog повідомлень усіх рівнів (повідомлення типу debugging мають найвищий пріоритет у передачі, встановивши даний рівень, на сервер будуть передаватися усі можливі типи повідомлень разом з діагностикою)

#logging 192.168.10.100 – встановлення IP-адреси серверу, який збирає «логи»

На рисунку 3.3 показано кількість повідомлень системного логування, усі вони є сповіщеннями, які повідомляли про вихід з меню конфігурації


Syslog

Service ◉ On ○ Off

| | Time | HostName | Message |
|---|---|---|---|
| 1 | 05.08.2025 10:22:45.087 AM | 192.168.10.1 | %SYS-5-CONFIG_I: Configured ... |
| 2 | 05.08.2025 10:20:31.196 AM | 192.168.10.99 | %SYS-5-CONFIG_I: Configured ... |
| 3 | 05.08.2025 10:19:10.452 AM | 192.168.10.99 | %SYS-5-CONFIG_I: Configured ... |
| 4 | 05.08.2025 10:17:54.311 AM | 192.168.10.99 | %SYS-5-CONFIG_I: Configured ... |
| 5 | 05.08.2025 10:16:20.459 AM | 192.168.10.99 | %SYS-5-CONFIG_I: Configured ... |
| 6 | 05.08.2025 10:15:34.217 AM | 192.168.10.1 | %SYS-5-CONFIG_I: Configured ... |
| 7 | 05.08.2025 10:13:29.013 AM | 192.168.10.1 | %SYS-5-CONFIG_I: Configured ... |

Рис.3.3. Вигляд вікна SysLog

## 3.2. Імплементація протоколу керування мережею SNMP

SNMP – протокол, який використовується для проведення моніторингу та керування мережею через вбудовану базу даних мережі (MIB). Ці MIB містять ідентифікатори об'єктів (OID), які позначають кожен керований параметр (тип мережі, IP-адреси пристроїв, швидкість передачі даних, тощо) в мережевій інфраструктурі. [3]

Протокол підтримує три основні операції: GET-запити дозволяють менеджерам отримувати певну інформацію від агентів, SET-запити дозволяють змінювати конфігурацію на віддалених пристроях, а TRAP-повідомлення надають асинхронні сповіщення при перевищенні попередньо визначених подій або порогових значень. [8]

Для встановлення протоколу у конфігурацію роутеру та комутаора потрібно додати команди

snmp-server host 192.168.10.100 version 2 public – встановлення адреси серверу, на який буде приходити інформація про пристрої або віртуальні мережі (за допомогою GET-запитів)

У проєкті впроваджується 2-га версія протоколу, так як функціонал третьою версії є обмеженим та не може забезпечити повноцінну реалізацію передачі інформації.

snmp-server community corporateRO RO – встановлення паролю (corporateRO) для доступу до читання GET-запитів.

snmp-server community privateRW RW – встановлення паролю (privateRW) для можливості зміни налаштувань мережі через MIB браузер.

При введені обирається адреса однієї з віртуальних підмереж, зареєстрованих у роутері для збору інформації. За замовчуванням портом SNMP у програмі виступає 161 та 162 віртуальні порти (рис.3.4).

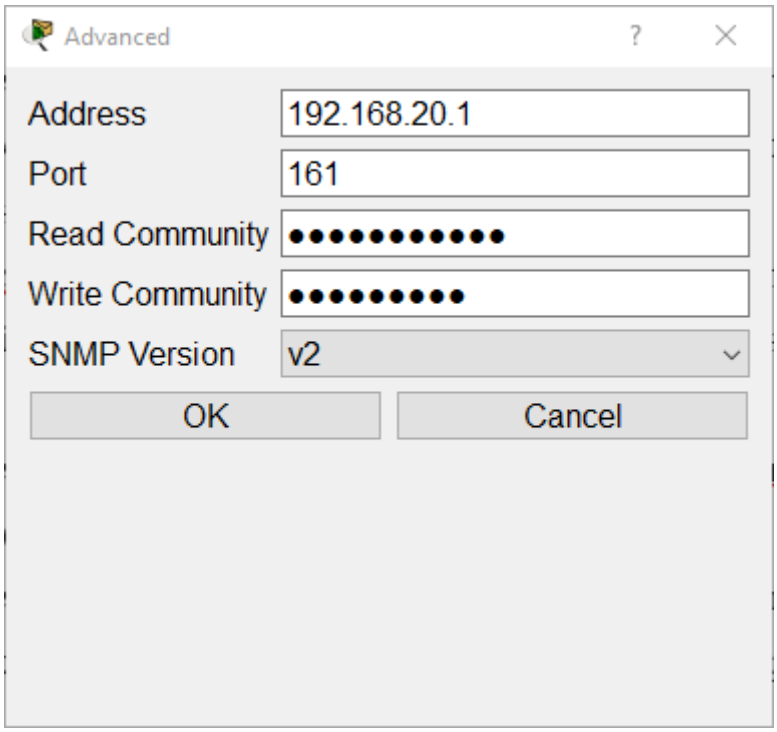



Рис.3.4. Вікно вводу адреси та порту для моніторингу SNMP

На рисунку 3.5 було отримано список усіх унікальних ідентифікаторів IP-адрес підмереж та їх цільовими адресами з таблиці маршрутів роутера.

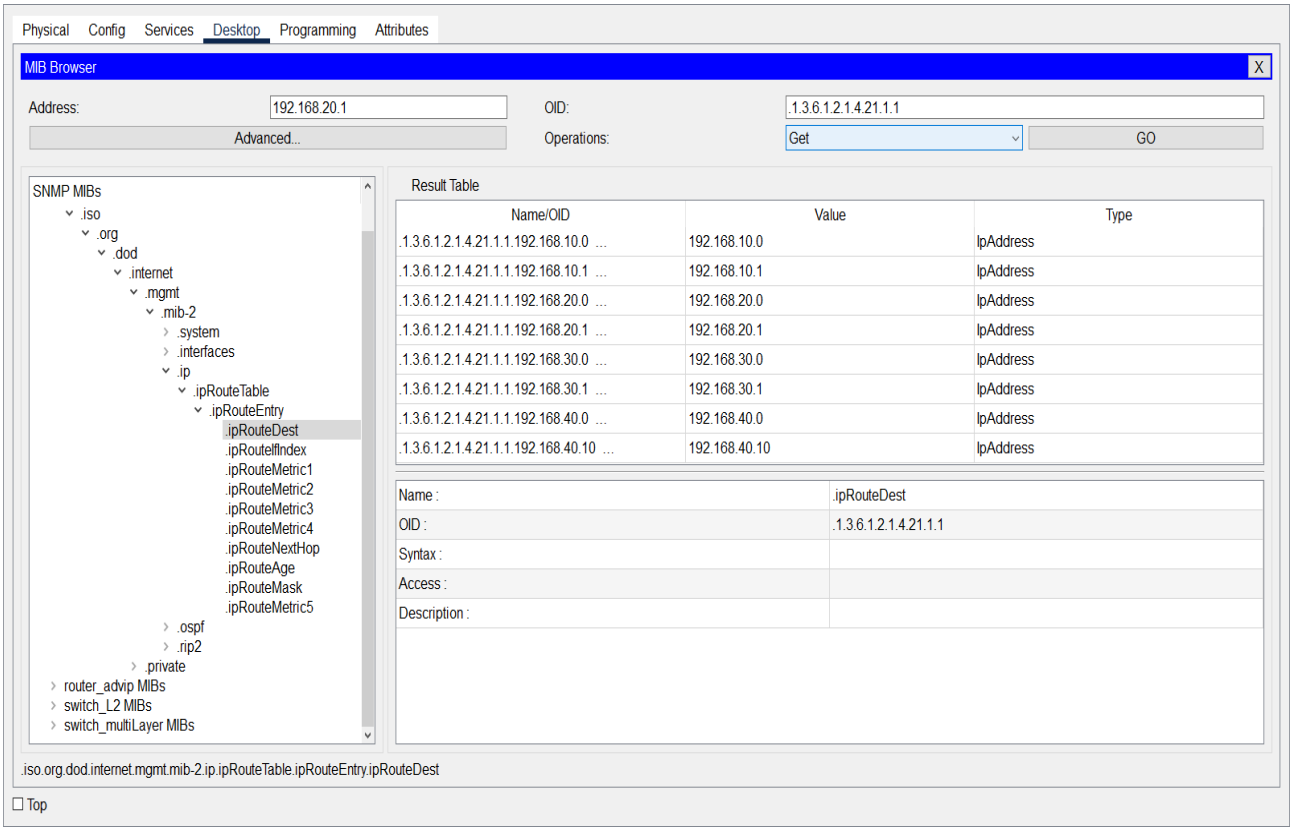



Рис.3.5. Список IP-адрес підмереж

## 3.3. Мережевий протокол NetFlow

NetFlow представляє собою мережевий протокол, розроблений компанією Cisco для збору та аналізу інформації про IP-трафік, що проходить через мережеві інтерфейси.

Даний протокол функціонує шляхом створення записів потоків на основі семи ключових параметрів: IP-адреси джерела та призначення, порти джерела та призначення, протокол IP, тип сервісу та вхідний логічний інтерфейс. Коли повідомлення з однаковими характеристиками проходять через пристрій, вони групуються в потоки, а статистична інформація про ці потоки збирається та передається до колектора NetFlow для подальшого аналізу. [9]

Для роботи NetFlow у конфігурацію роутеру додаються такі команди:

ip flow-export destination 192.168.10.100 9996 – задає на яку IP-адресу потрібно відправляти записи пакетів повідомлення та стандартний UDP порт для передачі інформації NetFlow

ip flow-export version 9 – вибір версії NetFlow (9та версія єдина яка підтримується в Packet Tracer)

ip flow-export source GigabitEthernet0/1 – позначення інтерфейсу джерела з якого будуть обробляти повідомлення під формат NetFlow та відправляти їх на сервер (як джерело вказується саме інтрефейс, через який роутер підключається до комутатора та на якому встановлені віртуальні інтерфейси)

Щоб збирати інформацію про мережевий трафік з підмереж, на кожному віртуальному інтерфейсі додаються команди

ip flow egress – збір даних про повідомлення які надходять на інтерфейс

ip flow ingress – збір даних про повідомлення які відправляються з інтерфейсу

На рисунку 3.6, до огляду надається діаграма кількості повідомлень, надісланих з різних джерел

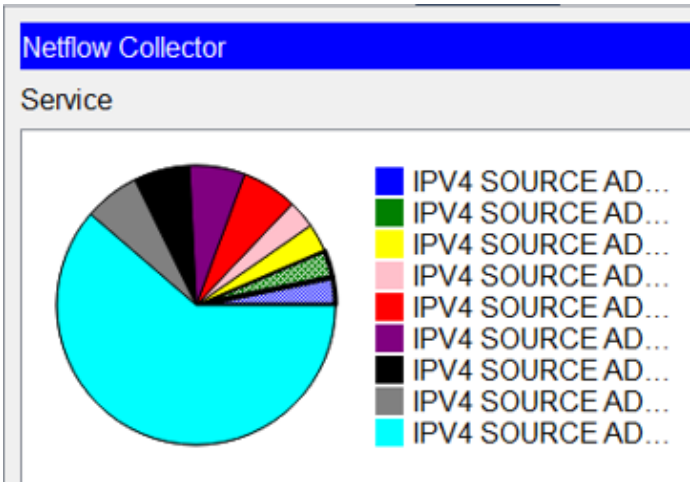



Рис.3.6. Діаграма потоків повідомлень NetFlow

На рисунку 3.7 описано інформацію про обраний на діаграмі мережевий трафік. У розділі Traffic Contribution вказано яку частину мережевого трафіку займає дане повідомлення. Розділ Flow information складається з інформації про атрибути самого повідомлення:

IPv4 SOURCE ADDRESS: IP-адреса відправника (у прикладі: 192.168.20.14)

IPv4 DESTINATION ADDRESS: IP-адреса отримувача (192.168.10.12)

INTERFACE INPUT – інтерфейс маршрутизатора, на якому цей потік було зафіксовано входом

TRNS SOURCE PORT – порт джерела транспортного протоколу (0 — значить не TCP/UDP)

TRNS DESTINATION PORT – порт призначення (0)

IP PROTOCOL – номер мережевого протоколу (1 = ICMP, 6 = TCP, 17 = UDP тощо)

FLOW DIRECTION – у даному випадку, вказується, що потік повідомлення прямує на вхід інтерфейсу роутера

ipv4 source mask – маска підмережі джерела

ipv4 destination mask – маска підмережі призначення

counter bytes – кількість байтів переданих в рамках цього потоку

counter packets – кількість мережевих пакетів переданих в цьому повідомленні

timestamp first/last – час початку і завершення реєстрації потоку

ip next hop address – наступна IP-адреса, з якої пересилатиметься повідомлення

```
Traffic Contribution: 3.22581% (1/31)

Flow information:
IPV4 SOURCE ADDRESS:          192.168.20.14
IPV4 DESTINATION ADDRESS:     192.168.10.12
INTERFACE INPUT:    Gig
TRNS SOURCE PORT:             0
TRNS DESTINATION PORT:        0
IP TOS:             0x00
IP PROTOCOL:                  1
FLOW SAMPLER ID:    0
FLOW DIRECTION:     Input
ipv4 source mask:   /24
ipv4 destination mask: /24
counter bytes:                512
ipv4 next hop address: 192.168.10.12
tcp flags:          0x00
interface output:   Gig
counter packets:    4
timestamp first:              10:02:12.772
timestamp last:               10:02:15.857
ip source as:                 0
ip destination as:  0
```

Рис.3.7. Інформація про вибраний потік мережевого трафіку

# ВИСНОВКИ

У ході виконання кваліфікаційної роботи було проведено комплексне моделювання корпоративної мережі, що дозволило зробити наступні висновки:

1. Сегментація мережі за допомогою Віртуальної Локальної Мережі є не просто технічним, а фундаментальним рішенням для безпеки. Було доведено, що такий підхід ефективно ізолює трафік, створюючи бар'єри для поширення мережевих загроз шляхом блокування доменів ззовні усіх підмереж.
2. Списки контролю доступу підтвердили свою дієвість як гнучкий інструмент політики безпеки. Практичне застосування для захисту мережевого принтера показало, що навіть прості правила здатні надійно заблокувати несанкціонований доступ, що доводить важливість контролю не лише на рівні мережі, але й на рівні доступу до окремих пристроїв.
3. Найбільш значущим результатом є доведена взаємодія елементів комплексного моніторингу. Аналіз показав, що інтеграція Системного логування, Простого Протоколу Керування Мережею та Мережевого Потоку перетворює моніторинг з пасивного спостереження на проактивний інструмент управління. Поєднання аналізу подій, стану обладнання та потоків трафіку забезпечує повну видимість мережі, що є критично важливим для своєчасного виявлення проблем та інцидентів.

Таким чином, робота доводить, що комплексний підхід, який поєднує сегментацію, контроль доступу та багаторівневий моніторинг, дозволяє створити захищену, керовану та прозору мережеву інфраструктуру, що відповідає сучасним вимогам. Поставлена мета була повністю досягнута.

.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ


1. Kurose, J. F., Ross, K. W. Computer Networking: A Top-Down Approach. 7th Edition. Pearson, 2017. 864 p.
2. О.В. Полоневич, В.Р.Косенко, К.П.Сторчак, О.М.Ткаленко. «Інформаційні мережі» Навчальний посібник, ДУТ, Київ, 2018, -96 с. – URL: http://www.dut.edu.ua/uploads/l_1175_82154550.pdf 2.
3. CCNA 200-301 Hands-on Mastery with Packet Tracer (Networking Technology) – Cisco Press, - 496 p.
4. The Book of GNS3: Build Virtual Network Labs Using Cisco, Juniper, and More 1st Edition, Jason C. Neumann, 2015. 272 p.
5. GeeksforGeeks. URL: https://www.geeksforgeeks.org/virtual-lan-vlan/
6. GeeksforGeeks. URL: https://www.geeksforgeeks.org/configuring-and-verifying-vlans-in-cisco/
7. GeeksforGeeks. URL: https://www.geeksforgeeks.org/access-lists-acl/
8. GeeksforGeeks. URL: https://www.geeksforgeeks.org/simple-network-management-protocol-snmp/
9. GeeksforGeeks. URL: https://www.geeksforgeeks.org/network-monitoring-and-packet-capture-techniques/
10. Jena S. R. Cisco Packet Tracer Implementation: Building and Configuring Networks. Kindle Edition, 2023. 199 p.

# ДОДАТОК. Опис функціоналу Cisco Packet Tracer

Графічний інтерфейс Packet Tracer схожий на інші програми по типу CAD або SPICE: у верхній частині є меню з пунктами File, Edit, Options, View, Tools, Extensions, Window, Help для команд відкриття/збереження файлів, налаштувань, тощо.

Під меню розташовані панель швидких інструментів та Common Tools, де є іконки вибору, видалення, малювання приміток, генерації тестових пакетів (Add Simple/Complex PDU) тощо. [10]

Основна область інтерфейсу – робочий простір для побудови мережі: він може бути у двох виглядах – Logical (рисунок 4.1) і Physical (рисунок 4.2). Переключення між ними відбувається кнопками у верхній частині робочого вікна.

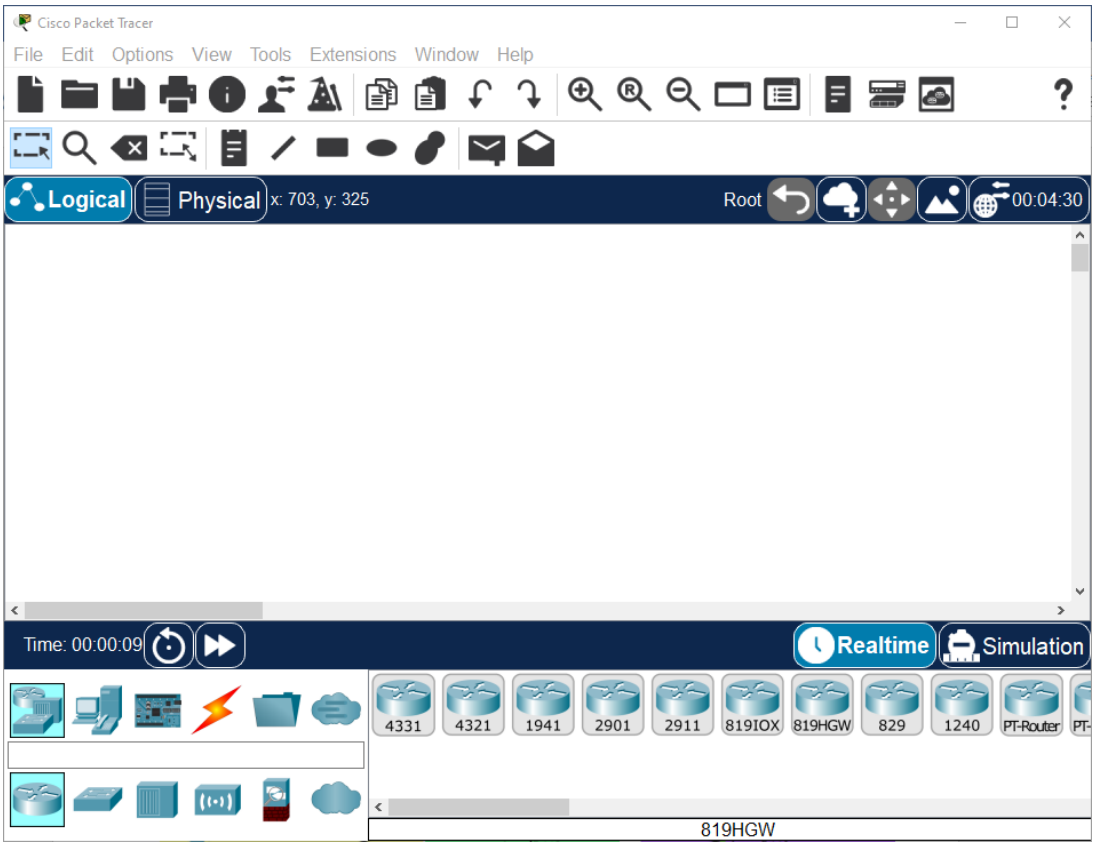



Рис.4.1. Вікно логічного виду

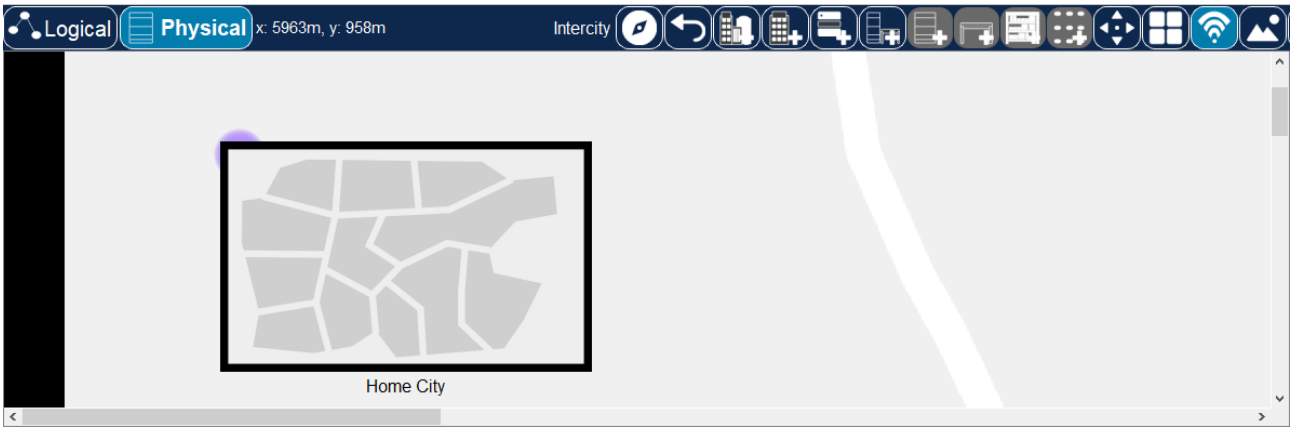



Рис.4.2. Вікно фізичної виду

Логічний простір призначено для проєктування топологій та їхнього налаштування, а фізичний показує розташування об’єктів (наприклад, розподіл по місту, будівлі, комірці). Нижче робочого простору розташована панель режимів – там можна перемикатися між Realtime і Simulation.

У режимі симуляції з’являються кнопки керування відтворенням (play/pause, fast forward) і журнал подій. Зліва від панелі режимів – панель вибору компонентів: Device-Type Selection Box (список категорій пристроїв) та Device-Specific Selection Box (конкретні моделі/кабелі). [3]

Категорії вибору компонентів діляться End Devices (кінцеві пристрої), Network Devices (мережеві пристрої), Компоненти IoT (Components), Кабелі під’єднання. Деякі з них мають такі підкатегорії [3] [10] (Рис.4.3):

Network Devices:

- Роутери
- Комутатори
- Хаби
- Бездротові пристрої
- Фаєрволи (брандмауери)
- Пристрої для симуляції WAN
- Кінцеві пристрої (ПК, Ноутбуки, Смартфони, Принтери та ін.)
- Пристрої інтер’єру (Датчики руху, диму, Сонячна панель, Термометр)
- Пристрої «розумного міста» (RFID-мітки, розумна LED-підсвітка)

Components:

- MCU-плата, SBC-плата

- «Актуатори» (Нагріваючі та охолоджуючі елементи, Система сповіщення тривоги)

- Сенсори (Датчики вологості, звуку, температури, вітру)

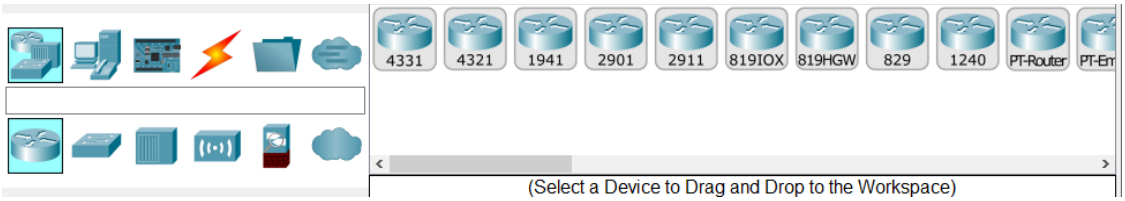



Рис.4.3. Меню вибору компонентів

Меню конфігурації мережевого підключення у більшості кінцевих пристроїв складається з показнику швидкості підключення (bandwidth), MAC-адреси, назви пристрою (SSID), методу автентифікації до мережі, конфігурації IPv4 та IPv6 (Рис.4.4):

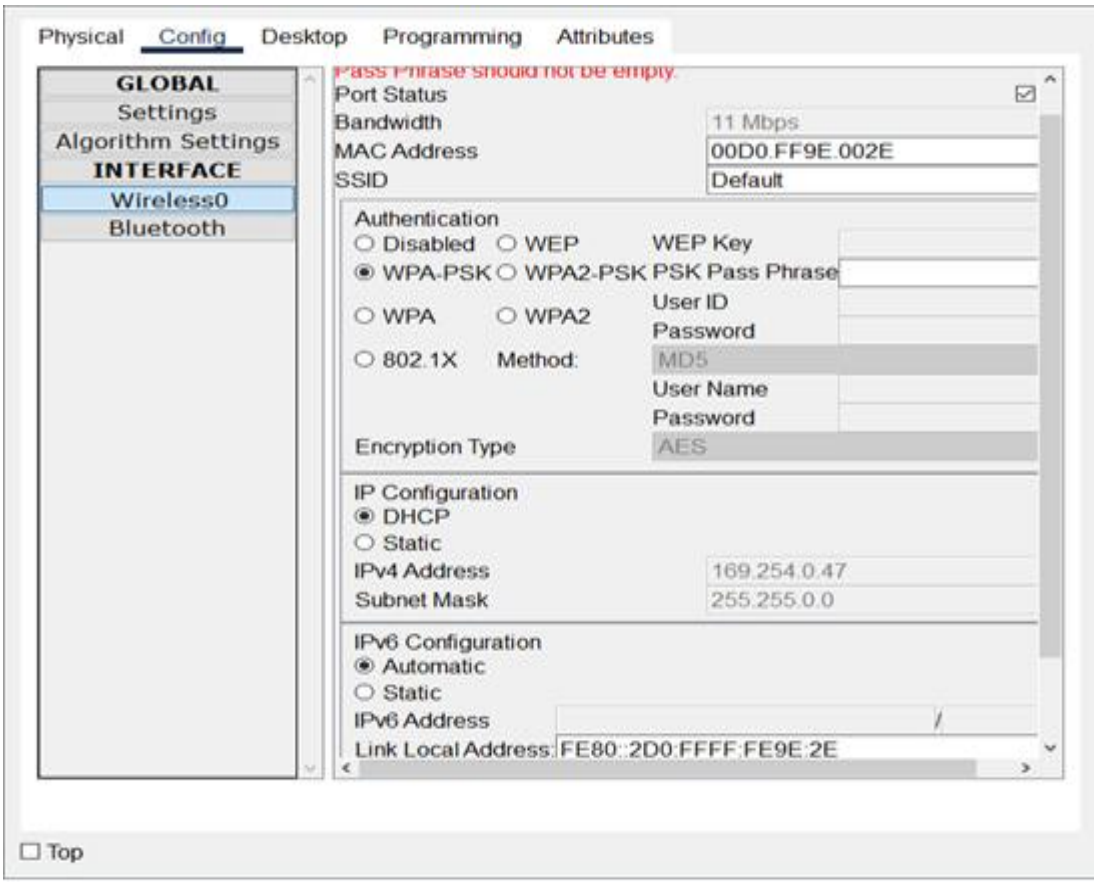



Рис.4.4. Вікно налаштування кінцевого пристрою