

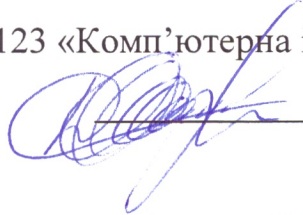
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему:

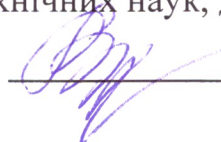
«Методи та технології захисту кампусних мереж, побудованих на базі технології Ethernet та Wi-Fi»

Виконала студентка 2-го курсу групи КІм-22-1
спеціальності 123 «Комп'ютерна інженерія»

 Ольга Дячук

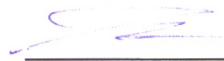
Керівник

професор кафедри комп'ютерної інженерії та кібербезпеки, доктор технічних наук, доцент

 Володимир Воротніков

Рецензент

доцент кафедри комп'ютерної інженерії та кібербезпеки, кандидат технічних наук, доцент

 Юрій Россінський

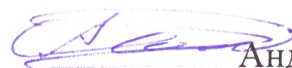
Житомир – 2023

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки



Андрій Єфіменко
«13» жовтня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Дячук Ольга Юріївна

Тема роботи: «Методи та технології захисту кампусних мереж, побудованих на базі технології Ethernet та Wi-Fi»

затверджена Наказом університету від «13» жовтня 2023 р. № 572/с

Термін здачі студентом закінченої роботи «21» грудня 2023 р.

1. Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Об'єктом дослідження є процес проектування та налаштування підсистеми захисту мережевої інфраструктури кампусної мережі, побудованої на базі обладнання Cisco.

2. Предметом дослідження є методи та заходи безпеки для захисту кампусних комп'ютерних мереж від кіберзагроз.

2. Обладнання та програмне забезпечення:

1. Cisco Packet Tracer

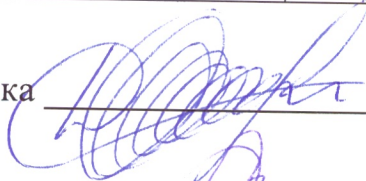
3. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посади консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Андрій Єфіменко, завідувач кафедри кафедри КІ та КБ, к.т.н., доцент	05.10.2023	05.10.2023
2	Андрій Єфіменко, завідувач кафедри кафедри КІ та КБ, к.т.н., доцент	09.11.2023	09.10.2023
3	Андрій Єфіменко, завідувач кафедри кафедри КІ та КБ, к.т.н., доцент	06.12.2023	06.12.2023

Дата видачі завдання «13» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів роботи	Примітка
1	Отримання та конкретизація завдання для виконання кваліфікаційної роботи	13 жовтня 2023 – 14 жовтня 2023	Виконано
2	Проведення пошуку та аналізу літературних джерел, а також вивчення існуючих аналогів систем захисту.	15 жовтня 2023 – 24 жовтня 2023	Виконано
3	Оформлення технічного завдання проекту захисту кампусних мереж згідно державних стандартів НД ТЗІ та ДСТУ	25 жовтня 2023 – 31 жовтня 2023	Виконано
4	Розробка та тестування системи захисту кампусних мереж, побудованих на базі технології Ethernet та Wi-Fi	1 листопада 2023 – 5 листопада 2023	Виконано
5	Побудова та налагодження мережі та системи	6 листопада 2023 – 14 листопада 2023	Виконано
6	Перевірка працездатності створеного проекту системи	15 листопада 2023 – 19 листопада 2023	Виконано
7	Захист	29 грудня 2023	Виконано

Студентка  Ольга Дячук

Керівник  Володимир Воротніков

РЕФЕРАТ

Кваліфікаційна робота складається з проєкту підсистеми захищеної кампусної мережі побудованої на базі технологій Ethernet та Wi-Fi та пояснювальної записки до нього. Пояснювальна записка до кваліфікаційної роботи складається з анотації, вступу, трьох розділів, висновків, списку використаної літератури та додатків.

Текст пояснювальної записки викладено на 78 сторінках та містить 34 ілюстрації та 9 таблиць. Список використаної літератури налічує 21 найменування.

Метою кваліфікаційної роботи є формування систематичного підходу та розробка пропозицій щодо захисту кампусних комп'ютерних мереж та забезпечення їх надійного та ефективного функціонування в умовах сучасного освітнього середовища.

Досліджено теоретичні аспекти побудови кампусних мереж. Визначено основні фактори та загрози що впливають на безпеку мереж. Здійснено огляд та аналіз сучасних технологій та методів захисту.

Виконано проєктування кампусної мережі. Структуровані та запропоновані ефективні рішення та механізми захисту.

Здійснено налаштування та тестування проєкту мережі.

Проведені діагностичні та тестові результати які підтверджують працездатність та ефективність запропонованих рішень.

КЛЮЧОВІ СЛОВА: КАМПУСНА МЕРЕЖА, ІНФОРМАЦІЙНА БЕЗПЕКА, МЕТОДИ, ТЕХНОЛОГІЇ, ПРОТОКОЛ, ЗАГРОЗА, HSRP, VLAN.

ABSTRACT

The qualification work consists of a project of a subsystem of a secure campus network built on the basis of Ethernet and Wi-Fi technologies and an explanatory note to it. The explanatory note to the qualification work consists of an abstract, an introduction, three chapters, conclusions, a list of references, and appendices.

The text of the explanatory note is set out on 78 pages and contains 34 illustrations and 9 tables. The list of references includes 21 titles.

The purpose of the qualification work is to form a systematic approach to protecting campus computer networks and ensuring their reliable and effective functioning in a modern educational environment.

The theoretical aspects of building campus networks are investigated. The main factors and threats affecting network security are identified. A review and analysis of modern technologies and methods of protection is carried out.

The design of the campus network is completed. Effective solutions and protection mechanisms are structured and proposed.

The network design was configured and tested.

The diagnostic and test results confirm the operability and effectiveness of the proposed solutions.

KEYWORDS: CAMPUS NETWORK, INFORMATION SECURITY, METHODS, TECHNOLOGIES, PROTOCOL, THREAT, HSRP, VLAN.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КАМПУСНИХ МЕРЕЖ НА БАЗІ ТЕХНОЛОГІЙ ETHERNET ТА WI-FI.....	11
1.1. Принципи побудови захищеної кампусної мережі	11
1.2. Загальна характеристика технологій Ethernet та Wi-Fi.....	14
1.3. Особливості побудови кампусних мереж на базі технологій Ethernet та Wi-Fi	17
1.4. Методи та протоколи маршрутизації в кампусних мережах.....	21
1.5. Вразливості та атаки на інфраструктуру кампусних мереж.....	26
1.6. Методи захисту кампусних мереж.....	32
РОЗДІЛ 2. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ КАМПУСНОЇ МЕРЕЖІ	42
2.1. Розробка загального проекту кампусної мережі	42
2.2. Розробка логічної структури мережі	46
2.3. Розробка проекту підсистеми захисту	48
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ ЗАХИСТУ КАМПУСНОЇ МЕРЕЖІ.....	53
3.1. Вибір мережевого обладнання та програмного забезпечення	53
3.2. Базове налаштування пристроїв кампусної мережі.....	57
3.3. Налаштування підсистеми захисту мережі	63
3.4. Тестування системи захисту та аналіз результатів.....	67
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	77
ДОДАТКИ	79

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

CAN (Campus Area Network) – кампусна мережа

IEEE (Institute of Electrical and Electronics Engineers) – Інститут інженерів електрики і електроніки (

DHCP (Dynamic Host Configuration Protocol) – протокол динамічної конфігурації вузлів

VLAN (Virtual Local Area Network) – віртуальна локальна мережа

LAN (Local Area Network) – локальна мережа

MAC (Media Access Control) – управління доступом до середовища

PC – персональний комп'ютер

SW (switch) – коммутатор

IP (Internet Protocol) – протокол мережевої взаємодії

VTP (VLAN Trunking Protocol) – протокол віртуальних мереж

STP (Spanning Tree Protocol) – канальний протокол

RSTP (Rapid Spanning Tree Protocol) – розширення протоколу STP

CLI (Command Line Interface) – інтерфейс командного рядку

OSI (Open Systems Interconnection Basic Reference Model) – базова еталона модель взаємодії відкритих систем

HSRP (Hot Standby Router Protocol, Hot Standby Redundancy Protocol) — протокол маршрутизації сімейства FHRP

ВСТУП

Актуальність. З розвитком інформаційних технологій та швидкою інтеграцією усі сфери суспільства, навчання та освіта також зазнають суттєвих змін. Кампусні комп'ютерні мережі, що об'єднують велику кількість пристроїв, стають невід'ємною частиною як сучасного освітнього закладу так і будь якої державної та комерційної організації. Вони надають користувачам можливість обмінюватися інформацією, проводити дослідження та будь які як організаційні так і розважальні заходи, а також виконувати різні адміністративні функції. Однак, така мережева інфраструктура також схильна до різних загроз, яким необхідно ефективно протистояти.

Зростаюча кількість кіберзагроз та технологічних викликів ставлять під загрозу конфіденційність, цілісність та доступність даних. Зловмисники, постійно вдосконалюючи свої методи, можуть шкодити не тільки роботі мережі, але й використовувати здобуту інформацію для крадіжок конфіденційних даних або здійснення кібератак.

Таким чином, проблема кібербезпеки кампусних мереж набуває надзвичайної актуальності, адже недостатні заходи безпеки можуть призвести до серйозних наслідків інформаційної безпеки. Вирішення цієї проблеми передбачає ретельне дослідження стану захисту кампусних комп'ютерних мереж, ідентифікацію потенційних загроз і розробку ефективних заходів для підвищення рівня їхньої безпеки.

Метою кваліфікаційної роботи є розробка комплексного технологічного рішення для захисту кампусних мереж, побудованих на базі технології Ethernet та Wi-Fi

Поставлена мета зумовлює наступні завдання роботи:

- проведення глибокого та комплексного дослідження сфери захисту кампусних комп'ютерних мереж з метою визначення актуальності проблеми та розробки ефективних стратегій для підвищення рівня їх безпеки;
- проаналізувати сучасний стан інформаційних технологій та визначити основні тенденції розвитку;

- виявити та проаналізувати актуальні загрози та ризики, пов'язані з використанням кампусних комп'ютерних мереж;
- ідентифікувати потенційні загрози конфіденційності, цілісності та доступності даних в кампусних мережах;
- вивчити вже існуючі приклади кібератак та визначити їхні наслідки.
- ретельно проаналізувати технічні та організаційні аспекти сучасних кампусних комп'ютерних мереж;
- визначити проблеми та вразливості, які можуть призвести до небезпеки для інформаційної безпеки в кампусній мережі.
- провести огляд сучасних технологій та методів кіберзахисту.
- розробити конкретні рекомендації для вдосконалення існуючих заходів безпеки та впровадження нових технологій.

Це дослідження спрямоване на формування систематичного підходу до захисту кампусних комп'ютерних мереж, забезпечуючи надійність та ефективність їх функціонування в умовах сучасного освітнього середовища.

Об'єктом дослідження є процес проектування та налаштування підсистеми захисту мережної інфраструктури кампусної мережі, побудованої на базі обладнання Cisco.

Предметом дослідження є заходи безпеки, спрямовані на захист кампусних мереж від кіберзагроз. Дослідження охоплює аналіз потенційних загроз, визначення найбільш критичних вразливостей та розробку пропозицій щодо вдосконалення існуючих заходів безпеки.

В процесі виконання кваліфікаційної роботи був розроблений проект підсистеми захисту мережної інфраструктури кампусної мережі, побудованої на базі обладнання Cisco з використанням емулятора Cisco Packet Tracer.

Це дослідження є актуальним і важливим, оскільки результати його можуть стати основою для розробки та впровадження ефективних стратегій безпеки, сприяючи надійному та безпечному функціонуванню кампусних комп'ютерних мереж.

Апробація результатів:

1. Дячук О.Ю., Єфіменко А.А. АНАЛІЗ ОСНОВНИХ МЕТОДІВ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ // Тези VI Всеукраїнська науково-технічна конференція «Комп'ютерні технології: інновації, проблеми, рішення» «Комп'ютерна інженерія та кібербезпека», м. Житомир, 29-30 листопада 2023 року. – Житомир: Житомирська політехніка, 2023

2. Колощук М.С., Дячук О.Ю. Дослідження впливу різних технологій передачі даних на швидкість та стабільність роботи мережі. Тези XIII Міжнародної науково-технічної конференції "Інформаційні комп'ютерні технології". м. Житомир, 30-31 березня 2023 р. – Житомир: Житомирська політехніка, 2023. С. 22 -23.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КАМПУСНИХ МЕРЕЖ НА БАЗІ ТЕХНОЛОГІЙ ETHERNET ТА WI-FI

1.1. Принципи побудови захищеної кампусної мережі

Забезпечення безпеки кампусних мереж є складним завданням, оскільки вони, як правило, є великими та складними системами. Однак існує ряд принципів, які можна дотримуватися для створення більш захищеної мережі [2], до цих принципів відносяться:

1. Аудит безпеки
2. Захист периметра
3. Безпека кінцевих точок
4. Безпека даних
5. Обізнаність про безпеку

Аудит безпеки – процес виявлення та оцінки уразливостей у системі безпеки. Він є важливим кроком у побудові захищеної кампусної мережі.

Аудит безпеки повинен включати в себе оцінку таких факторів, як:

- Архітектура мережі, яка визначає будову, принцип роботи та оцінку відповідності архітектури мережі найкращим практикам безпеки.
- Фізична безпека, яка відноситься до захисту фізичних активів мережі, таких як сервери, комутатори та маршрутизатори. Аудит безпеки повинен оцінити, чи вживаються відповідні заходи фізичної безпеки для захисту цих активів.
- Безпека програмного забезпечення, яка відноситься до захисту програмного забезпечення, яке використовується в мережі. Аудит безпеки повинен оцінити, чи оновлюється програмне забезпечення вчасно, чи використовуються всі доступні засоби безпеки.
- Безпека даних, яка відноситься до захисту даних, які зберігаються в мережі. Аудит безпеки повинен оцінити, чи використовуються відповідні заходи безпеки для захисту даних.

За результатами аудиту безпеки розробляються рекомендації щодо вдосконалення безпеки кампусної мережі. Ці рекомендації можуть включати в себе такі заходи, як:

- Розділ мережі на зони безпеки;
- Запровадження заходів фізичної безпеки;
- Оновлення програмного забезпечення;
- Шифрування даних;

Аудит безпеки слід проводити регулярно, щоб забезпечити постійний захист кампусної мережі.

Периметр мережі – це точка, де вона з'єднується з зовнішнім світом. Захист периметра є важливим для запобігання несанкціонованому доступу до мережі. До заходів захисту периметра відносять:

- Використання брандмауерів – пристроїв, які контролюють вхідний та вихідний трафік з мережі. Вони можуть блокувати несанкціонований доступ, наприклад, доступ з невідомих IP-адрес.
- Використання систем виявлення вторгнень (IDS) – програмне забезпечення, яке відстежує мережевий трафік на наявність ознак зловмисної діяльності. Вони можуть виявляти атаки, такі як спроби зламу облікових записів або поширення шкідливого програмного забезпечення.
- Використання межових контролерів доступу (ACL) – правила, які визначають, який трафік дозволено або заборонено передавати через межу мережі. ACL можуть використовуватися для блокування несанкціонованого доступу до мережі.

Кінцеві точки – це комп'ютери, пристрої та інші системи, які підключені до мережі. Безпека кінцевих точок є важливою для запобігання поширенню шкідливого програмного забезпечення та інших загроз.

Заходи безпеки кінцевих точок включають:

- Використання антивірусного програмного забезпечення, яке виявляє та видаляє шкідливе програмне забезпечення, яке слід регулярно оновлювати, щоб забезпечити захист від останніх загроз.

- Використання програмного забезпечення для захисту від шкідливого програмного забезпечення, яке виявляє та блокує шкідливе програмне забезпечення, яке намагається поширитися по мережі.

- Використання програмного забезпечення для захисту від фішингу, яке допомагає користувачам розпізнавати та уникати фішингових атак.

Крім вище зазначених заходів забезпечення безпеки кінцевих точок можна застосовувати наступні рекомендації:

- Встановлення складних паролей та регулярно їх змінювати.
- Ігнорування електронних листів або файлів від невідомих відправників.
- Регулярне оновлення програмного забезпечення на своїх кінцевих точках.

- Створення резервних копій даних на своїх кінцевих точках.

Дані, які зберігаються в кампусній мережі, можуть бути цінними для кіберзлочинців. Безпека даних є важливою для запобігання крадіжці або втраті даних.

Заходи безпеки даних включають:

- Шифрування даних – процес перетворення даних в нечитабельний формат. Шифровані дані можуть бути прочитані лише тими, хто має ключ для дешифрування.

- Використання політик безпеки доступу до даних – визначення осіб, які матимуть доступ до даних, часу коли вони отримають доступ до даних і як ці дані можуть бути використані.

- Регулярне резервне копіювання даних яке допоможе відновити дані у разі втрати або крадіжки.

Обізнаність про безпеку – це важливий аспект безпеки кампусної мережі. Користувачі повинні бути навчені розпізнавати та запобігати кібератакам.

Заходи підвищення обізнаності про безпеку включають:

- Проведення тренінгів з основ мережної безпеки;
- Розміщення інформаційних матеріалів про безпеку які повинні бути доступними користувачам у різних форматах (електронні листи, брошури та

веб-сайти). Ці матеріали повинні інформувати користувачів про ризики та заходи безпеки, які вони можуть вжити для захисту себе.

- Заохочення користувачів до звітування про підозрілі події, невідомі пристрої, підключені до мережі, електронні листи або файли від невідомих відправників та зміни в роботі мережі.

Всі вище зазначені підходи є важливою частиною загальної системи безпеки кампусної мережі.

Застосування всіх цих заходів допоможе захистити мережу від несанкціонованих доступів, поширення шкідливого програмного забезпечення та запобігти кібератакам.

1.2. Загальна характеристика технологій Ethernet та Wi-Fi

Найчастіше в локальних мережах використовуються два основних типи передавання даних між вузлами – по дротах, такі мережі називаються кабельними і використовують технологію Ethernet, а також за допомогою радіосигналу по бездротових мережах, побудованих на базі стандарту IEEE 802.11, який більш відомий користувачам під назвою Wi-Fi.

1. Ethernet – технологія локальних обчислювальних мереж з комутацією пакетів. Вона використовує протокол CSMA/CD, який контролює доступ до мережі та виявляє колізії. Цей протокол дозволяє лише одному сеансу передачі в логічному сегменті мережі, і при конфлікті станція призупиняє передачу.

Ethernet-мережі діють на різних швидкостях: 10 Мбіт/с, 100 Мбіт/с, 1000 Мбіт/с, та 10 Гбіт/с залежно від використовуваного обладнання (Ethernet, Fast Ethernet, Gigabit Ethernet та Ten Gigabit Ethernet).

З початку свого існування Ethernet використовував коаксіальний кабель для забезпечення зв'язку між комп'ютерами. Метод був подібний до радіопередачі, але із суттєвими відмінностями.

З часом Ethernet еволюціонував у складну технологію, замінивши коаксіальний кабель на зв'язки "точка-точка" через концентратори/комутатори. Успіх технології Ethernet був визначений використанням кабелю типу "вита пара" для зниження вартості та полегшення управління мережею.

На фізичному рівні станції Ethernet обмінюються пакетами даних, кожна має унікальну 48-бітну MAC-адресу. Незважаючи на зміни в технології з 10-Мбітного коаксіалу до 1-Гбітного оптоволокна, різні варіанти Ethernet залишаються схожими та можуть легко взаємодіяти між собою. Це досягається завдяки стабільному формату кадру, який залишається незмінним, незалежно від методів доступу до мережі.

2. Wi-Fi – бездротова локальна мережа, часто позначена як WLAN або wireless LAN, дозволяє комп'ютерам та іншим пристроям обмінюватися даними за допомогою технології радіочастот (RF). Ця передова технологія надає користувачам можливість вільного руху без втрати зв'язку з мережею, уникнувши при цьому потреби у використанні кабелів, що характерне для традиційних мереж Ethernet [8].

Інститут інженерів електрики і електроніки (IEEE) відіграє ключову роль у розробці та впровадженні стандартів для бездротового обміну даними. Їхній набір стандартів, відомий як IEEE 802.11, включає в себе різні протоколи, стандарти та описує різні аспекти, які визначають методи обміну даними в бездротових мережах.

Основні характеристики стандартів IEEE 802.11 включають [15]:

Шар доступу до середовища:

- *IEEE 802.11b*. Введений у 1999 році, працює на частоті 2,4 ГГц і забезпечує максимальну швидкість передачі даних 11 Мбіт/с.
- *IEEE 802.11a*. Також введений у 1999 році, але працює на вищій частоті 5 ГГц, і надає швидкість до 54 Мбіт/с.

Шар мережі:

- *IEEE 802.11g*. Введений у 2003 році, комбінує характеристики 802.11b і 802.11a, працює на частоті 2,4 ГГц і досягає швидкості до 54 Мбіт/с.
- *IEEE 802.11n*. Прийнятий у 2009 році, працює як на частоті 2,4 ГГц, так і на 5 ГГц, може досягати швидкості до 600 Мбіт/с завдяки використанню технології MIMO (Multiple Input Multiple Output).

Шар керування:

- *IEEE 802.11i*. Введений для підвищення безпеки бездротових мереж, надає протоколи шифрування і аутентифікації для захисту від несанкціонованого доступу.

- *IEEE 802.11e*. Визначає механізми для підтримки якісного обслуговування (QoS) у бездротових мережах.

Шар управління:

- *IEEE 802.11k*. Надає механізми для оптимізації мережевих ресурсів та підвищення ефективності бездротового зв'язку.

- *IEEE 802.11r*. Розроблений для поліпшення швидкості переключення між точками доступу у розширених мережах.

Ці стандарти регулюють аспекти фізичного, канального і керівництва бездротових мереж, забезпечуючи стандартизовані протоколи для їхньої ефективної реалізації та взаємодії. Нові версії та розширення стандартів розробляються для вдосконалення ефективності, безпеки та мобільності в бездротових мережах.

І хоча сучасні бездротові технології чисто теоретично теж можуть забезпечити передачу даних до 1,3 Гбіт/с (стандарт Wi-Fi 802.11ac), на практиці ця цифра виглядає набагато скромнішою і здебільшого не перевищує величину 150 – 300 Мбіт/с. Виною тому служить дорожнеча високошвидкісного Wi-Fi обладнання і низький рівень його використання в нинішніх пристроях.

До переваг використання технологій Ethernet відносяться те, що дротові мережі, як правило, мають стабільніший зв'язок і менше схильні до втрат сигналу в порівнянні з бездротовими аналогами. Вони можуть забезпечити високі швидкості передачі даних, особливо у високопропускних мережах. В деяких випадках дротові мережі можуть бути менш вразливими до атак інтродукції або перехоплення даних.

Як недоліки можна зазначити те що використання фізичних кабелів обмежує мобільність пристроїв, що може бути неефективним у великих просторах або для мобільних працівників та розгортання дротових мереж може бути трудомістким завданням через необхідність прокладання фізичних кабелів.

Перевагами технології Wi-Fi є те, що бездротові мережі дозволяють велику свободу руху, що особливо важливо для мобільних пристроїв та робочих місць, та те що не потрібно прокладати фізичні кабелі, що полегшує інсталяцію та дозволяє ефективно використовувати мережу у великих просторах.

До недоліків відносять вразливість до перешкод, таких як стіни чи інші бездротові пристрої, що може призвести до втрати сигналу та погіршення зв'язку. Менша пропускна спроможність ніж у дротових мереж. Вразливість до несанкціонованого доступу, атак інтродукції та перехоплення даних.

У короткостроковій перспективі дротові мережі можуть залишатися популярними в областях, де стабільність та висока пропускна спроможність є ключовими факторами, а бездротові технології будуть активно використовуватися там, де важливою є мобільність та легкість установки.

У довгостроковій перспективі очікується подальший розвиток технологій, як дротових, так і бездротових мереж.

Швидше за все, бездротові технології будуть отримувати більшу популярність завдяки постійному покращенню їхньої стабільності та пропускної спроможності.

1.3. Особливості побудови кампусних мереж на базі технологій Ethernet та Wi-Fi

Кампусна мережа (Campus Area Network) CAN – це локальна мережа, що об'єднує комп'ютери та інші пристрої в межах одного або декількох офісних будівель, навчальних закладів тощо.

Кампусна мережа може бути реалізована дво- або трирівневою ієрархічною архітектурою, де кожен рівень виконує певні функції. Такий поділ спрощує проектування, розгортання та адміністрування мережі.

Першим кроком до поділу мережі на функціональні рівні стала дворівнева ієрархічна архітектура (рисунки 1.1), що складається з рівня доступу (access layer) та рівня ядра (core/distribution layer).

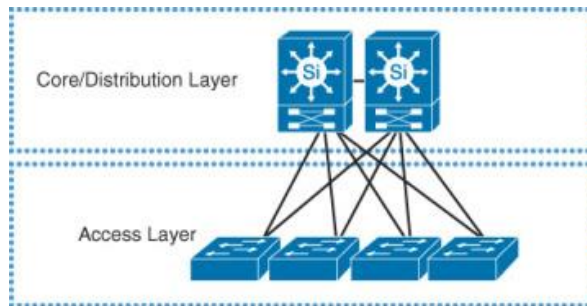


Рисунок 1.1. Схема дворівневої CAN

Рівень доступу надає кінцевим пристроям і користувачам підключення до комп'ютерної мережі та виконує функції: L2-комутації, VLAN, ARP, STP, безпеки інтерфейсів, QoS-маркування кадрів і визначення меж довіри, VACL, PoE та ін. Рівень ядра вирішує завдання, пов'язані з надійністю функціонування комп'ютерної мережі. Зазвичай цей рівень містить основні та резервні L3-пристрої, а також надмірну кількість каналів між ними, які виключають єдину точку відмови і дають змогу в разі виходу з ладу будь-якого проміжного вузла забезпечити зв'язок між кінцевими користувачами.

Класично ж CAN реалізовано трирівневою ієрархічною архітектурою (рисунок 1.2), що складається з рівня доступу, рівня розподілу та рівня ядра.

Рівень розподілу вирішує завдання агрегування каналів і даних, внутрішньої фільтрації трафіку, маршрутизації між підмережами і VLAN, балансування навантаження, управління широкомовними доменами тощо [8].

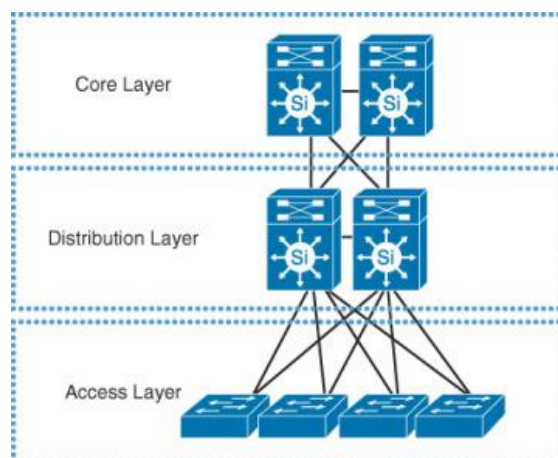


Рисунок 1.2. Схема трирівневої CAN

Рівень ядра називають також мережевою магістраллю. Рівень ядра складається з високошвидкісних мережевих пристроїв, призначених для більш швидкої комутації пакетів (часто в різнорідних мережах) і зв'язку декількох

компонентів усередині комплексу будівель, наприклад модулів розподілу, сервісних модулів, центрів обробки даних і кордону WAN.

Слід також враховувати такі міркування щодо рівня ядра:

- забезпечення високошвидкісної комутації (тобто швидкої передачі даних);
- забезпечення надійності та стійкості до збоїв;
- масштабування за рахунок використання більш швидкодіючого обладнання, а не за рахунок збільшення кількості пристроїв;
- усунення операцій із пакетами, що вимагають великого завантаження ЦП (центрального процесора), які породжуються процесами забезпечення безпеки, класифікації QoS або іншими процесами.

Останнім часом у зв'язку із збільшенням обсягу трафіку, активним використанням ресурсів мережі для передавання медіа-трафіку (аудіо та відео) виникла необхідність відокремлювати сервери від звичайних комп'ютерів, підключати їх через виділені комутатори з метою більш гнучкого управління пропускнуою спроможністю каналів.

Серверна ферма являє собою групу комутаторів, що є ключовим компонентом LAN, що забезпечує підключення до неї серверів. Важлива вимога, що пред'являється до серверної ферми, полягає у високій продуктивності та надійності. Таким чином, багаторівнева архітектура мережі дає змогу індивідуально вирішувати завдання організації, скорочувати час простою мережі та інформаційних систем і мінімізувати втрати робочого часу, а також створює можливість впровадження додаткових додатків і сервісів.

За допомогою трирівневого підходу ми можемо легко розширювати кампусну мережу, додаючи нові блоки, та забезпечувати високий рівень визначеності у поведінці мережі. Крім того, цей підхід дозволяє легко виявляти та усувати проблеми, не витрачаючи зайвих зусиль та ресурсів. Інтелектуальні сервіси на L3 (такі як протоколи OSPF, EIGRP, HSRP) допомагають скорочувати зону впливу проблем при виникненні несправностей або неправильному налаштуванні обладнання.

Теоретично можна комбінувати різні логічні рівні (наприклад, доступ/розподіл або розподіл/магістраль) в одному фізичному пристрої, особливо для невеликої мережі. Але, якщо мережа росте, перехід до багаторівневого дизайну є необхідним, оскільки це дозволяє оптимально використовувати обладнання у різних частинах мережі та мінімізувати вартість утримання системи.

Основними мережевими пристроями на рівні ядра є маршрутизатори та комутатори. Маршрутизатори забезпечують маршрутизацію трафіку між різними сегментами мережі, а комутатори – з'єднання між вузлами в одному сегменті.

Пристрої рівня ядра мають наступні можливості:

- Запобігання та управління перевантаженнями (Congestion Avoidance & Management) – здатність керувати поведінкою мережі під час перевантаження, відкидаючи певні пакети на основі класифікації або політики в моменти перевантаження мережі за допомогою технології Weighted Random Early Detection (WRED) і безлічі черг на інтерфейсах. Використовуючи можливості транспортного протоколу TCP, ці механізми дають змогу ефективно керувати швидкістю передавання даних і знизити швидкість передавання між кінцевими системами, до того як перевантаження торкнеться пріоритетних додатків. Адміністратор встановлює порогові значення для різних рівнів пріоритету.
- Планування (Scheduling) – здатність здійснювати пріоритетну передачу пакетів, засновану на класифікації або політиці якості обслуговування, за допомогою декількох черг і технології Weighted Round Robin (WRR).

Для з'єднання пристроїв рівня ядра використовується технологія Ethernet з різними швидкостями від 10 Мбіт/с до 100 Гбіт/с (Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, 40 Gigabit Ethernet, 100 Gigabit Ethernet) та ін.

Основними мережевими пристроями на рівнях розподілу та доступу є комутатори. Комутатори на рівні розподілу забезпечують з'єднання між вузлами в різних сегментах мережі, а на рівні доступу в одному сегменті мережі. Бездротові точки доступу забезпечують бездротовий доступ до мережі.

Пристрої рівнів доступу та/або розподілу мають наступні можливості:

- Класифікація трафіку (Traffic Classification) – здатність класифікувати трафік за типами застосунків, фізичними та мережевими адресами джерел і одержувачів, портами комутаторів. Класифікований трафік отримує мітку, що позначає призначений пакетам рівень пріоритету, тим самим даючи можливість пристроям мережі відповідним чином обслуговувати цей трафік. Також забезпечується рекласифікація пакетів на основі заданої адміністратором політики якості обслуговування. Наприклад, користувач призначає високий пріоритет своєму трафіку і передає його в мережу. Цей пріоритет може потім бути знижений відповідно до мережевої політики, а не на основі вимог користувача. Цей механізм є ключовим у забезпеченні якості обслуговування у межах усієї мережі.

Для з'єднання комутаторів на рівні розподілу використовується технологія Ethernet, а для рівня доступу Ethernet та Wi-Fi.

Незахищена мережа являє собою серйозний ризик. Можливості забезпечення безпеки мають бути сфокусовані не на окремих продуктах, а на системному рішенні.

Важливо зазначити, що вибір конкретних пристроїв і технологій залежить від вимог і потреб. Під час проектування кампусної мережі необхідно враховувати розміри мережі, кількість під'єднаних пристроїв, необхідну пропускну здатність і рівень безпеки.

1.4. Методи та протоколи маршрутизації в кампусних мережах

Маршрутизація представляє собою процес вибору оптимального маршруту для передачі даних в комп'ютерних мережах. У цьому контексті протоколи та таблиці маршрутизації виконують ключову роль, реалізуючи алгоритми маршрутизації для визначення найефективніших та найбільш прийнятних шляхів для пересилання пакетів даних [9].

Маршрутизатор, як пристрій, визначає оптимальний шлях для передачі даних між мережами. Таблиця маршрутизації, розміщена в маршрутизаторі або мережевому комп'ютері, містить інформацію про топологію мережі та розрахо-

вана на перерахування маршрутів та, в окремих випадках, пов'язаних метрик (відстаней).

Також, таблиця маршрутизації може містити два види записів:

- Статичні, де інформація про маршрут вводиться вручну, але цей метод може викликати проблеми при змінах у топології мережі чи відмовах на ділянці.
- Динамічні, де маршрутизація оновлюється за допомогою обміну даними між пристроями за допомогою протоколів маршрутизації. Цей процес може бути періодичним або тригернутим залежно від протоколу.

У випадку наявності кількох шляхів для передачі інформації від джерела до призначення, використовується адміністративна відстань. Це число від 0 до 255, що використовується для визначення надійності протоколу маршрутизації при виборі оптимального шляху. Кожен протокол маршрутизації має свої метрики для визначення найкращого шляху, і якщо використовуються різні протоколи, то прийнятний шлях визначається на основі адміністративної відстані.

Чим менше числове значення адміністративної відстані, тим вище ступінь надійності вибраного маршруту. Обрання протоколу з найменшим значенням адміністративної відстані вказує на його визнану вищою надійністю в контексті маршрутизації.

Протокол маршрутизації можна розглядати як набір правил, які використовуються маршрутизатором для обміну інформацією про стан мережі та доступність різних шляхів. Два ключові поняття, які слід відрізняти, це маршрутизований протокол (наприклад, IP) та протокол маршрутизації, який включає в себе обмін і аналіз інформації для визначення оптимальних маршрутів між мережевими вузлами.

У сфері кампусних мереж використовуються різноманітні протоколи маршрутизації, такі як RIP, OSPF, EIGRP та інші. Ці протоколи можна класифікувати за використанням конкретного алгоритму маршрутизації, який визначає оптимальний шлях для передачі пакетів від джерела до призначення.

Вимоги до алгоритмів маршрутизації включають оптимальність, простоту, живучість, швидку збіжність та гнучкість. Швидка збіжність є особливо важли-

вою, оскільки повідомлення про зміни топології мережі повинні досягати інших маршрутизаторів з мінімальною затримкою. Слабка збіжність може викликати негативні наслідки, такі як вихід з ладу всієї мережі.

Однією з найбільш поширених реалізацій протоколів маршрутизації на основі вектора відстаней є протокол RIP (Routing Information Protocol). Основні параметри протоколу RIP включають в себе:

- використання дистанційно-векторного протоколу маршрутизації з використанням метрики у вигляді числа переходів;
- максимальна кількість переходів обмежена 15;
- регулярне широкомовне відсилання оновлень маршрутизації за замовчуванням кожні 30 секунд.

Еволюція протоколу RIP виявилася у переході від класового протоколу маршрутизації (RIPv1) до безкласового протоколу (RIPv2). Основні вдосконалення RIPv2 включають:

- підтримку масок змінної довжини;
- включення маски підмережі в інформацію оновлення маршрутизації;
- заміна широкомовного відсилання на групове (RIPv1 використовує широкомовне відсилання);
- можливість ручного сумування маршрутів;
- введення механізму аутентифікації для перевірки автентичності даних.

Основний принцип функціонування протоколу RIP полягає в тому, що маршрутизатори взаємодіють лише із своїми прямими сусідами, обмінюючи періодичні повідомлення про стан маршрутизації. Ці оновлення, незалежно від змін у топології мережі, включають в себе повну таблицю маршрутизації. Після отримання такої таблиці маршрутизації, маршрутизатор вносить відповідні зміни до власної таблиці.

У сучасних комп'ютерних мережах протокол RIP визнається не найоптимальнішим рішенням для обрання протоколу маршрутизації, оскільки його можливості відстають від більш сучасних альтернатив, таких як EIGRP і OSPF. Обмеження в 15 переходів (хопів) робить його неефективним для застосування

в розгалужених мережах. Тим не менше, протокол RIP відзначається простотою конфігурації, що є його перевагою.

Протокол OSPF (Open Shortest Path First) представляє собою поширений протокол на основі стану каналу для маршрутизації в кампусних комп'ютерних мережах. Цей безкласовий протокол працює на основі технології відстеження стану каналів та визначення найкоротших шляхів (SPF) за допомогою алгоритму Дейкстри. OSPF підтримує складну топологічну базу даних.

На відміну від протоколів на базі вектора відстані, які не містять інформації про віддалені мережі, протоколи на основі стану каналу зберігають усю інформацію про віддалені маршрутизатори та їх з'єднання. Стан каналу включає в себе опис інтерфейсу (IP-адреса, маска, тип мережі) та його взаємозв'язок з сусідніми маршрутизаторами, утворюючи базу даних стану каналів.

База даних заповнюється завдяки отриманню повідомлень про стан каналу (Link-State Advertisement – LSA), які розповсюджуються після змін у топології мережі або при змінах на маршрутизаторах.

На основі отриманих повідомлень LSA, маршрутизатор використовує алгоритм SPF, який будує дерево найкоротших маршрутів. Цей алгоритм виконує розрахунки на основі бази даних топології мережі, видаляючи непотрібні гілки (усі можливі шляхи). Отримані маршрути записуються в таблицю маршрутизації.

Протокол OSPF є внутрішнім протоколом маршрутизації і функціонує всередині однієї автономної системи, яку можна розділити на зони або області для логічного поділу. Маючи ряд переваг, таких як відсутність циклічних маршрутів, масштабованість для великих мереж та швидка реакція на зміни топології мережі, протокол OSPF також має недоліки, такі як ієрархічна топологія, відсутність розподілу навантаження для нерівноцінних шляхів та використання метрики лише для оцінки вартості маршруту.

Протокол EIGRP (Enhanced Interior Gateway Routing Protocol) представляє собою вдосконалену реалізацію протоколу маршрутизації на основі вектора відстані, розроблену компанією Cisco Systems та широко застосовується на їх-

ньому обладнанні. Основні характеристики цього протоколу можуть бути визначені наступним чином:

EIGRP володіє вищою швидкістю збіжності порівняно з іншими протоколами на основі вектора відстані, завдяки використанню алгоритму DUAL (Diffusing Update Algorithm). Цей алгоритм дозволяє протоколу ефективно визначати та підтримувати два оптимальних шляхи до призначених мереж.

Механізм DUAL спрямований на мінімізацію використання полоси пропускання, надсилаючи лише необхідні оновлення при зміні стану мережі, замість повного пересилання таблиці маршрутизації.

Протокол EIGRP дозволяє ефективно підтримувати кілька протоколів мережевого рівня, включаючи IP, IPX та AppleTalk.

EIGRP використовує безкласову архітектуру маршрутизації, що спрощує управління мережевими ресурсами та забезпечує більш гнучку конфігурацію.

Протокол використовує мультиадресну та одноадресну розсилку, замість широкомовної, що дозволяє ефективно відправляти оновлення маршрутизації, обмежуючи їх вплив на непов'язані маршрутизатори.

Таким чином, принцип роботи протоколу EIGRP базується на вдосконалених механізмах збіжності, економії ресурсів мережі та підтримці мультипротоковості, роблячи його важливим інструментом для керування маршрутизацією у сучасних мережових середовищах.

Таблиця 1.1.

Порівняльна характеристика внутрішніх протоколів маршрутизації

	RIPv2	OSPF	EIGRP
Тип протоколу	Вектор відстаней	Стан каналу	Удосконалений дистанційно-векторний
Алгоритм	Беллмана-Форда	Дейкстри	Алгоритм дифузного оновлення (Diffused Update)
Розрахунок метрик	Кількість переходів	Смуга пропускання	Смуга пропускання, затримка, надійність і навантаження
Оновлення маршрутною інформації	Уся таблиця	Тільки зміни	Тільки зміни
Адміністративна відстань	120	110	90
Безкласовий	Так	Так	Так

Продовження таблиці 1.1.

Максимальна кількість маршрутизаторів в мережі	15	Безлімітний	255
Відкритий стандарт	Так	Так	Ні
Метрика	Одна основна	Одна основна	Комбінована
Планування мережі	Ні	Так (вибір зон)	Ні
Складність конфігурації	*	****	***

За даними (таблиця 1.1) можна зробити висновок, що найкращими внутрішніми протоколами маршрутизації є OSPF та EIGRP. Особливо в застосуванні до великих і складних мереж. Але так само ці протоколи, не дивлячись на широкий спектр позитивних якостей, мають і свої недоліки. Протокол OSPF має високі вимоги до ресурсів маршрутизації через занадто складний обчислювальний розрахунок найкоротших шляхів. Хоча протокол EIGRP виграє у цьому плані, він все ж є закритим. Його реалізація можлива тільки на обладнанні Cisco Systems. Але в наш час у мережах застосовується обладнання різноманітних фірм. Тому у великих мережах вигідніше застосовувати протокол OSPF.

1.5. Вразливості та атаки на інфраструктуру кампусних мереж

Вкрай важливо зрозуміти, що безпека – це не продукт, який можна купити в магазині і бути впевненим у власній захищеності. Безпека – це поєднання як технічних, так і адміністративних заходів. Адміністративні заходи також включають в себе не тільки папери, рекомендації, інструкції, а й людей. Неможливо вважати свою мережу безпечною, якщо не довіряти людям, які працюють із цією мережею. Ідеальна безпека – недосяжний міф, який можуть реалізувати, у кращому разі, тільки кілька професіоналів. Є один фактор, який неможливо подолати на шляху до ідеальної безпеки – це людина.

Цілі мережевої безпеки можуть змінюватися залежно від ситуації, але основних цілей зазвичай три (рисунок 1.3):

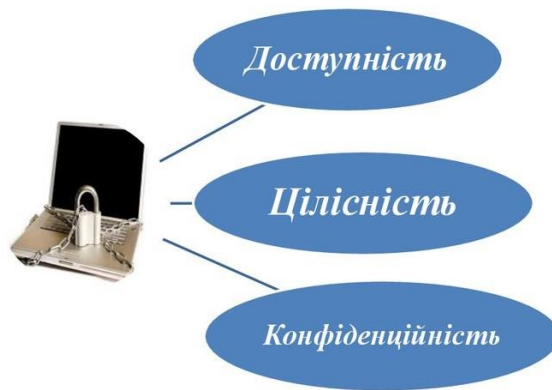


Рисунок 1.3. Цілі мережевої безпеки

Одна з основних цілей мережевої безпеки – гарантованість того, щоб дані не були змінені, підмінені або знищені. Цілісність даних повинна гарантувати їх збереження як у разі зловмисних дій, так і випадковостей. Забезпечення цілісності даних є зазвичай одним із найскладніших завдань мережевої безпеки.

Другою головною метою мережевої безпеки є забезпечення конфіденційності даних. Не всі дані можна відносити до конфіденційної інформації. Існує досить велика кількість інформації, яка має бути доступна всім. Але навіть у цьому випадку забезпечення цілісності даних, особливо відкритих, є основним завданням. До конфіденційної інформації можна віднести такі дані:

- особиста інформація користувачів;
- облікові записи (імена та паролі);
- дані про кредитні картки;
- дані про розробки та різні внутрішні документи;
- бухгалтерська інформація.

Третьою метою безпеки даних є їхня доступність. Марно говорити про безпеку даних, якщо користувач не може працювати з ними через їхню недоступність. Ось приблизний список ресурсів, які зазвичай мають бути "доступні" в локальній мережі: принтери; сервери; робочі станції; дані користувачів; будь-які критичні дані, необхідні для роботи.

Класифікація загроз мережної безпеки можлива за різними критеріями, один з яких ми вже розглянули (доступність, цілісність і конфіденційність). В залежності від розташування джерела, загрози можуть бути внутрішніми (комп'ютерні віруси) або зовнішніми (DDoS-атаки, сніфери для перехоплення тра-

фіку). Зазвичай проблеми безпеки часто мають комбінований характер: спершу зломисники здійснюють зовнішню атаку на сервер, а після успішного проникнення, впроваджують шкідливе програмне забезпечення [2].

Основні компоненти, на які найчастіше націлюються загрози:

- Інфраструктура віддаленого ресурсу. Це включає в себе різні аспекти, від фізичної доступності сервера до контролю над його ресурсами, такими як потужність процесора та обсяг оперативної пам'яті. Зниження продуктивності може суттєво впливати на рентабельність ресурсу.
- Програмне забезпечення. Зломисники можуть модифікувати або вивести з ладу програмне забезпечення з метою крадіжки цінної інформації, такої як паролі або банківські дані. Головна мета полягає в завданні матеріальної шкоди шляхом відсутності прибутку або прямої крадіжки коштів.
- Файли (дані). Зломисники активно використовують доступ до інформації, шифруючи, видаляючи або порушуючи схеми підключення до баз даних. Важливо враховувати, що загрози можуть виникати як у результаті цілеспрямованих хакерських атак, так і випадкових вразливостей, коли сервер не має належного захисту.

Визначення вразливостей мережі насамперед обумовлене присутністю конкретних слабкостей на віддалених серверах. Без їх наявності будь-які атаки не досягали б успіху. Заходи забезпечення полягають у виявленні та усуненні "уразливих точок" інформаційних систем. Наприклад, сервіс Telnet передбачає передачу інформації, такої як ім'я користувача і пароль, у відкритому вигляді, без шифрування, представляючи собою відомий недолік, який надає можливість перехоплення даних під час "прослуховування" мережевого трафіку.

Звичайно, вразливості класифікуються наступним чином:

- Відома проблема, для якої існує рішення (за допомогою пакетів оновлень тощо).
- Відома проблема, але рішення наразі не розроблено (закриття вразливості можливе через сторонні програми).

- Проблема, яка залишається невідомою, поки не виникає факт "вторгнення". Цей випадок часто визначається терміном "вразливість нульового дня". Вне залежності від категорії, вони виникають через недоліки програмного забезпечення, такого як операційні системи, користувацькі програми, драйвери. Навіть міжмережеві екрани та антивіруси не позбавлені помилок, а типовий перелік можна взяти з баз даних CVE (Common Vulnerabilities and Exposures) або NVD (National Vulnerabilities Database), де фахівці систематизують інформацію про відомі проблеми.

Вразливості в мережевих протоколах є актуальним аспектом, особливо в контексті 14 широко використовуваних протоколів обміну даними в мережі, кожен з яких має власні особливості та призначення. Наприклад, мережеві протоколи, використовувані для організації дротових та бездротових мереж, а також ті, які використовуються для потокового мовлення та передачі даних через Інтернет [11].

ARP – дозволяє ідентифікувати MAC-адресу, але в одноранговій мережі відсутній механізм перевірки джерела пакета, що використовують зломисники для отримання трафіку.

DNS – призначений для перетворення цифрової IP-адреси на зрозумілий людині домен. Стає уразливим через "отруєння" кешу, коли зломисники підмінюють відомості про віддалений хост.

FTP – протокол передачі файлів, не використовує шифрування і контролю з'єднання, що робить його вразливим для перехоплення даних.

HTTP/S – використовується для безпечної передачі даних між користувачем і сайтом. Має уразливості, які можуть бути використані для атаки Drown, що дозволяє зламати шифрування і здійснити крадіжку конфіденційної інформації.

POP3, як інструмент для отримання електронної пошти, має вразливості, які дозволяють атакам з використанням методу FireWire для отримання прямого доступу до пам'яті. Інші відомі проблеми існують і в протоколах IMAP, RDP, SIP, SMB, SMTP, SNMP, SSH, VNC, Telnet.

Хоча брандмауер та антивірус можуть ефективно "закривати" багато з цих вразливостей, їх ефективність залежить від належного налаштування заходів безпеки при розгортанні віддаленого сервера. Важливо зауважити, що пізніше вжиті заходи безпеки не завжди гарантують інформаційну безпеку, оскільки існують віруси, що можуть перешкоджати встановленню антивірусного захисту, як, наприклад, Trojan Multi Gen Autorun.

Уразливості в апаратній частині мережі виникають переважно через непередбачені помилки в програмному забезпеченні, або так званих прошивках, якими керує більшість мережевого обладнання. Ці помилки призводять до вразливостей, і нам пропонується типовий приклад: у маршрутизаторах Mikrotik, обладнаних системою RouterOS, існує проблема, яка надає можливість будь-якій особі з обліковим записом адміністратора підвищити свої привілеї до рівня Super Admin. Схожі проблеми також виявляються в мережевих комутаторах, мікрокодів процесорів та іншому обладнанні.

У разі вразливостей у програмному забезпеченні, низка небезпеки пов'язана з операційними системами та користувацьким софтом. Відповідно патчі (оновлення) використовуються для усунення цих вразливостей. Критичним є використання піратських програм, які часто залишаються непоновленими та потенційно небезпечними. Наприклад, з моменту випуску Microsoft закрила понад 100 вразливостей у Windows 2019/2022, де враховано високий рівень безпеки, що є характерним для серверних операційних систем.

Людський фактор, як уразливість, також відзначається непередбачуваністю. Часті проблеми виникають через банальну недбалість користувачів, які ігнорують або недостатньо серйозно ставляться до рекомендацій експертів. Споживачі встановлюють занадто прості паролі для своїх облікових записів, забувають налаштовувати захисне програмне забезпечення, таке як брандмауер або антивірус, і легко потрапляють в пастки, клікнувши по сумнівним посиланням, де обіцяють "секретну інформацію" чи інші атракції.

Атаки в мережі орієнтовані на отримання несанкціонованого доступу до віддалених або локальних систем і можуть викликати різні сценарії під час їх реалізації. Загальна характеристика для всіх видів атак полягає в експлуатації

уразливостей в апаратній або програмній частині комп'ютера. Атаки поділяються на пасивні та активні, з додатковою категорією, яка включає соціальну інженерію, спрямовану на користувачів.

Пасивні атаки розглядаються як більш небезпечні, оскільки вони не призводять до прямого впливу на мережу чи її компоненти. Зловмисники залишаються "невидимими" від моменту підключення до виявлення витоку або порушення інформації. Наприклад, така атака може бути порівняна з прослуховуванням телефону.

- Підслуховування (Sniffing). Сніфери, що призначені для перехоплення пакетів без порушення сеансу зв'язку, націлені на пошук незашифрованих даних, які передаються відкрито, такі як логіни, паролі та інші особисті або комерційно важливі відомості.

- Аналіз трафіку (Traffic Analysis). Цей спосіб перехоплення є більш досконалим, оскільки він передбачає можливість вилучення інформації навіть із зашифрованих пакетів. Хоча ефективність його відносно низька, при наявності відкритого тексту є можливість підібрати ключ і отримати доступ до всіх переданих відомостей через мережу.

Активні атаки передбачають прямий вплив на ІТ-інфраструктуру і часто спрямовані на обмеження працездатності або перенаправлення користувачів на шкідливі ресурси. Ці атаки залишають сліди, які можна виявити за допомогою лог-файлів.

- ARP-отруєння (ARP Poisoning). Метод ARP-отруєння або ARP-спуфінгу передбачає прив'язку до MAC-адреси мережевої карти замість істинної IP-адреси, що надає зловмиснику контроль над передачею повідомлень. Ця атака ефективна всередині конкретної мережі через відсутність аутентифікації в ARP-протоколі.

- Міжмережеве проникнення (Intrusion). Метод міжмережевого проникнення використовується для атак "ззовні" і спрямований на отримання доступу до хоста. Відмінні методи використовуються для вразливостей, таких як слабкі

паролі, неправильна конфігурація операційних систем чи додатків, або використання незахищених протоколів.

Соціальна інженерія використовує різноманітний інструментарій для обману користувачів і включає такі методи, як фішинг, цільовий фішинг, голосовий фішинг, змішинг, "китобійний" фішинг, клон-фішинг та інші. Ці атаки спрямовані на залучення користувача до шкідливих дій, таких як відвідування шкідливих веб-сайтів чи завантаження шкідливих файлів. Результатом завжди є інфікування та компрометація системи.

Необхідність забезпечення мережевої безпеки виходить далеко за рамки простого етапу розгортання віддаленого сервера та встановлення спеціалізованого програмного забезпечення для користувачів. Відсутність ефективного захисту робить будь-який комп'ютер, раніше чи пізніше, схильним до атак хакерів, які часто автоматизовано скористовуються програмами для виявлення та використання вразливостей. Ці програми значно полегшують процес злому шляхом ефективного "перебору" можливих слабкостей системи. На практиці виявлення потенційних загроз у мережі включає різні ризики, починаючи від уразливих протоколів до непередбачених помилок у програмах та маршрутизаторах.

Одним із ключових підходів до забезпечення мережевої стійкості є систематична перевірка та усунення виявлених недоліків. Це може включати встановлення рекомендованих патчів, ефективне використання брандмауерів, антивірусних програм та інших інструментів безпеки. Підкреслюється, що регулярні заходи безпеки стають необхідністю в умовах постійно зростаючого обсягу мережевих загроз. В цьому контексті, комплексний підхід до управління безпекою, що об'єднує технічні та організаційні заходи, є важливим елементом збереження стабільності інформаційних систем.

1.6. Методи захисту кампусних мереж

Існує багато підходів до класифікації загроз та потенційних атак, спрямованих на кампусні мережі. Враховуючи те, що апаратні та програмні складові мереж функціонують на конкретних рівнях моделі взаємодії відкритих систем

(такої як модель OSI), для проведення аналізу методів та технологій захисту використовується класифікація, орієнтована на відповідні рівні моделі OSI. Найбільша кількість атак найчастіше здійснюється на п'яти рівнях (фізичний, канальний, мережевий, транспортний, прикладний) [4].

Узагальнені вразливості та заходи захисту на різних рівнях моделі взаємодії відкритих систем наведено в таблиці 1.2.

Таблиця 1.2.

Класифікація вразливостей та заходів захисту за рівнями моделі OSI

Рівень моделі OSI	Вразливості	Заходи убезпечення
Фізичний рівень	Втрата потужності Фізичні крадіжки даних і устаткування Фізичне пошкодження або знищення даних і устаткування Несанкціоновані зміни у функціональному середовищі (передачі даних, змінних носіїв, додавання / видалення ресурсів) Вимкнення фізичних каналів передачі даних Приховане перехоплення даних з клавіатури та інших засобів введення інформації	Закриття периметру і корпусів мережі Електронний механізм блокування для реєстрації та авторизації Відео та аудіо спостереження Застосування PIN-кодів і паролів Біометричні системи аутентифікації Електромагнітне екранування
Канальний рівень	Підміна MAC-адреси Обхід технологій VLAN Використання помилок алгоритму Spanning Tree для передачі пакетів у нескінченний цикл У бездротових мережах безкоштовне несанкціоноване підключення до мережі Затоплення комутаторами всіх портів VLAN	Фільтрація MAC-адрес Не використовувати мережі VLAN для захисту інформації Фізична ізоляція різних зон мережі за допомогою брандмауерів Бездротові мережі необхідно захищати з використанням вбудованого шифрування, автентифікації та фільтрації MAC-адрес
Мережевий рівень	Підміна маршруту – поширення неправдивої топології мережі Підміна IP-адреси — джерело помилкового рішення після дії шкідливих пакетів Проблеми одноразової ідентифікації	Застосування політики управління маршрутами – жорсткі фільтри маршрутів і антиспуфінг Використання міжмережевих екранів із потужною політикою фільтрації Моніторинг програмного забезпечення, для мінімізації можливих зловживань

Транспортний рівень	Неправильна передача пакетів Відмінності в реалізації транспортного протоколу дозволяють здійснити несанкціонований доступ Перевантаження транспортного рівня за рахунок великої кількості звернень до номерів портів обмежує можливості для ефективної фільтрації трафіку Механізми передачі пакетів можуть бути предметом підміни і атаки на основі сформованих пакетів і призводити до руйнування або захоплення контролю над мережею	Жорсткі правила брандмауера обмежують доступ до певних протоколів передачі інформації, таких як номер портів TCP/UDP або тип ICMP Перевірка брандмауером пакетів з урахуванням аналізу вмісту та з'єднання дозволяє закрити доступ до мережі шкідливим пакетам Посилення механізмів ідентифікації з'єднання, щоб уникнути нападу і захоплення контролю над мережею
Сеансовий рівень	Слабкі або відсутні механізми автентифікації Передача під час сеансу інформації, такої як ім'я користувача і пароль у відкритому вигляді, дозволяє її перехоплення та несанкціоноване використання Ідентифікація сеансу може бути предметом підміни і викрадення Витік інформації на основі невдалих спроб автентифікації Здійснення атаки на облікові дані для доступу в разі необмеженої кількості спроб на встановлення сеансу	Зашифрований обмін і зберігання паролів Обмежений термін дії для паролів та повноважень користувачів Захист інформації про ідентифікацію сеансу за допомогою криптографічних засобів Обмеження невдалих спроб встановлення сеансу за допомогою механізму синхронізації, а не блокування.
Представницький рівень	Погана обробка даних може призвести до збою програми Ненавмисне або необачне використання зовнішніх даних, що вводяться в контексті управління може призвести до віддаленої маніпуляції або витоку інформації Криптографічні недоліки можуть бути використані для обходу захисту конфіденційності	Ретельна перевірка даних, що вводяться до програми Контроль дій користувачів та функцій управління Ретельний і безперервний огляд рішень криптографії для забезпечення поточних завдань безпеки до загрози, що постійно оновлюються

Прикладний рівень	Використання безкоштовних ресурсів та програм невідомого походження Недоліки програмного забезпечення, наявність backdoors і можливостей обійти стандартні засоби управління безпекою Недостатній контроль засобів захисту за принципом «все або нічого», в результаті чого або надмірний або недостатній доступ до мережі Надмірно ускладнений механізм контролю безпеки, можна обійти або важко застосувати Збої програмного забезпечення при великих навантаженнях	Контроль на рівні програм визначає і забезпечує доступ до ресурсів. Простий та прозорий механізм забезпечення безпеки, з метою уникнення складностей у конфігуруванні. Реалізація криптографічного та антивірусного захисту даних
-------------------	---	---

Загрози, що виникають на сеансовому та представницькому рівнях, переважно пов'язані з процедурами ідентифікації, автентифікації та шифрування. Алгоритми і протоколи цих процедур втілені в операційних системах, і їх вплив на роботу мереж адміністраторами є мінімальним.

Найпоширенішими атаками на фізичний рівень, спрямованими на об'єкти, такі як канали передачі даних, є:

- фізичне пошкодження;
- несанкціоновані зміни у функціональному середовищі;
- вимкнення фізичних каналів передачі даних;
- створення шумів по всій полосі пропускання каналу.

У сучасних кампусних мережах для реалізації каналів передачі використовуються обмежені середовища (з оптичними та мідними кабелями) та необмежені середовища передачі (відкритий ефір). Вибір середовища передачі здійснюється враховуючи призначення каналу, його довжину, безпеку передачі інформації, швидкість передачі даних, електромагнітну сумісність, вартість створення і експлуатації.

З точки зору захисту від наведених атак оптичний кабель виявляється найефективнішим рішенням, оскільки його фізична природа унеможливорює

прослуховування, зняття інформації та постановку шумів. Використання сучасних технологій мультиплексування за довжинами хвиль дозволяє досягати високої пропускної здатності оптичних каналів.

Для коротких відстаней можна використовувати екрановану звиту пару, яка забезпечує захист від електромагнітного впливу. Однак такі лінії зв'язку мають обмежену довжину та пропускну здатність.

Незахищена звита пара та безпроводові технології (Wi-Fi) є популярними для мереж доступу, але менш захищеними від наведених атак. Для їх захисту рекомендується використовувати шифрування даних.

Для запобігання атакам, спрямованим на несанкціоновані зміни у функціональному середовищі, важливо обмежити фізичний доступ, реалізувати політику віддаленого доступу, використовувати системи відеоспостереження та контролю доступу. Резервування критичних каналів, пристроїв та серверів також сприяє надійності інформаційно-комунікаційних систем [6].

Атаки на каналний рівень мережевої інфраструктури часто включають генерацію ширококомовних кадрів з метою перевантаження каналів передачі даних і комутаційного обладнання, відомих як "широкомовні шторми" у великих комутуваних мережах. Іншими типовими атаками є підміна MAC-адрес вузлів, атаки на протоколи ARP і Spanning-Tree.

Захист на каналному рівні передбачає реалізацію технологій, спрямованих, передусім, на роботу з MAC-адресами вузлів. Хоча деякі захисні функції комутаторів можуть аналізувати і використовувати IP-адреси вузлів, що розширює їхні можливості на мережевий рівень.

Основні підходи до захисту на каналному рівні включають:

- MAC-фільтрація та прив'язка MAC-адрес до портів комутаторів. Ця функція (наприклад, Portsecurity комутатора) дозволяє обмежувати доступ до мережі лише певним MAC-адресам, що зменшує ризик недозволеного доступу.
- Застосування додаткових захисних функцій комутаторів. Такі функції, як DHCP Snooping, Dynamic ARP Inspection, IP SourceGuard, допомагають у виявленні та блокуванні аномальних активностей, таких як зміна адрес чи ARP-атаки.

- Сегментація мережі на окремі зони (домени широкомовлення). Застосування технології віртуальних локальних мереж (VLAN) дозволяє обмежити комунікацію між різними частинами мережі, що робить складніше розповсюдження атак.

- автентифікація та авторизація. Використання методів автентифікації (наприклад, 802.1X) дозволяє забезпечити, що тільки вповноважені користувачі отримують доступ до мережі, а авторизація контролює їхні права доступу.

Ці підходи взаємодіють для створення комплексної системи захисту, яка зменшує вразливість канального рівня перед мережевими загрозами [12].

Port Security – це важлива функція комутатора, спрямована на захист мережі від різних атак. Вона дозволяє адміністратору адміністративно визначати MAC-адреси вузлів, що підключені до конкретного порту, або обмежувати кількість MAC-адрес на порту. Ця функція використовується для запобігання несанкціонованій зміні MAC-адреси мережного пристрою, несанкціонованому підключенню вузла до мережі та атакам, спрямованим на переповнення таблиць комутації.

Функція відстеження DHCP (DHCP Snooping) – DHCP Snooping захищає мережу від атак, пов'язаних із протоколом DHCP, такими як підміна або додавання несанкціонованого DHCP-сервера в мережу чи атака DHCP starvation. Вона визначає DHCP-повідомлення від ненадійних джерел, відсіює їх, розмежовує повідомлення від надійних та ненадійних джерел, будує та підтримує базу даних прив'язок для надійних та ненадійних вузлів [19].

При налаштуванні цієї функції комутатор відстежує процес отримання IP-адрес вузлами з DHCP-серверів, аналізує DHCP-повідомлення та створює запис IP-MAC з прив'язкою до порту підключення вузла. Трафік від вузлів, що отримали IP-адреси з ненадійних DHCP-серверів або вузлів зі статичними IP-адресами, не пропускається через комутатор.

База даних прив'язок, що отримана в процесі роботи функції DHCP Snooping, використовується і для інших захисних функцій комутатора, таких як Dynamic ARP Inspection (Protection), спрямована на боротьбу з атаками ARP-spoofing, та IP SourceGuard, спрямована на боротьбу з атаками IP-spoofing.

Dynamic ARP Inspection (Protection) (DAI) – це захисна функція, спрямована на боротьбу з атаками, використовуючи протокол ARP. Ця функція виявляє та відкидає ARP-повідомлення, які не відповідають раніше створеним адресним прив'язкам IP-MAC. DAI допомагає запобігти атакам ARP-spoofing, які можуть порушити зв'язок між вузлами та викликати розголос.

Функція захисту від підміни IP-адрес (IP SourceGuard або Dynamic IP Lockdown) – це захисна функція, що фільтрує трафік на рівні канального рівня відповідно до бази даних прив'язок DHCP Snooping або статичних прив'язок IP-MAC. Вона застосовується для запобігання атакам типу IP-spoofing. IP SourceGuard блокує трафік через захищений порт, поки вузол не отримає дійсну IP-адресу та не буде зазначено в базі даних прив'язок.

Ці функції сприяють комплексному захисту мережі від різноманітних загроз, а їхні взаємодії дозволяють створити надійний механізм захисту на рівні комутаторів.

Сегментація мережі на ізольовані зони, відомі як домени ширококомовлення, за допомогою технології віртуальних локальних мереж (VLAN), відкриває широкі можливості для реалізації важливих функцій. Ці функції включають контроль за ширококомовним трафіком, можливість створення функціональних робочих груп і підвищення рівня інформаційної безпеки.

VLAN представляє собою ізольовану групу вузлів мережі, де трафік, включаючи ширококомовний, на канальному рівні повністю ізольований від інших вузлів. Це означає, що передача кадрів між різними віртуальними мережами на підставі MAC-адреси неможлива, незалежно від типу адреси.

Важливою особливістю VLAN є можливість переносити вузли між різними віртуальними мережами без фізичного переключення ліній зв'язку на інші порти або комутатори. Це дає більшу гнучкість в управлінні мережею [18].

Однією з ключових переваг технології VLAN є можливість контролювати ширококомовний трафік та обмежувати його в рамках окремих сегментів. Віртуальні мережі дозволяють створювати логічно налаштовані границі для ширококомовного домену, що підвищує продуктивність мережі та обмежує поширення ширококомовного трафіку.

Технологія VLAN також вносить значний внесок у підвищення рівня інформаційної безпеки. Всі вузли в межах однієї VLAN утворюють закриту групу, де кожна група ізольована від інших. Це перешкоджає користувачам однієї групи отримувати доступ до даних іншої групи, забезпечуючи ефективний контроль доступу.

Для обміну даними між вузлами різних VLAN може використовуватися маршрутизація, що забезпечує виконання політики взаємодії користувачів з різних віртуальних мереж. Передача даних між вузлами відбувається за допомогою мережного рівня, що підсилює контроль доступу та політики безпеки.

Отже, технологія VLAN виступає як ключовий елемент загальної стратегії мережевої безпеки, надаючи засоби для контролю трафіку та ефективного управління доступом до ресурсів мережі.

Для вирішення завдань автентифікації та авторизації кінцевих пристроїв та користувачів в точках їх підключення, наприклад, на портах комутаторів локальних мереж або точках доступу Wi-Fi, і для реалізації централізованого контролю доступу до мережі, використовується протокол IEEE 802.1x [12]. Цей протокол операційно діє на каналному рівні, є сумісним з протоколом PPP (Point-to-Point Protocol) та протоколами каналного рівня 802 набору стандартів та реалізує порторієнтовану (port-based) авторизацію.

У випадку відсутності програмного клієнту 802.1x на пристроях користувача, таких як мережні принтери чи IP-відеокамери, авторизацію можна провести за MAC-адресою (режим MAC Authentication Bypass – MAB) або після проходження веб-автентифікації (режим Web-Auth) [12].

За допомогою такої системи контролю доступу можна надавати користувачам права доступу до корпоративної мережі незалежно від фізичного підключення та технології (проводової чи безпроводової). Після успішної авторизації пристрій користувача автоматично підключається до відповідної VLAN, визначеної політикою безпеки, та отримує IP-адресу з блоку адрес, призначеного даній VLAN, до якої застосовуються відповідні списки доступу (детальніше розглянуті у наступній статті циклу). Протокол 802.1x може використовуватися для управління доступом до мережі не лише на основі ідентифікаційних даних при-

строїв та користувачів, але і спільно з протоколами верхніх рівнів, реалізуючи відповідні політики мережевої безпеки.

Основний недолік протоколу 802.1x – це те, що він не забезпечує шифрування даних. Це означає, що зловмисник може перехопити дані, що передаються по мережі, і використовувати їх для атак. Наприклад, зловмисник може перехопити паролі або інші конфіденційні дані. Крім того, зловмисник може використовувати перехоплені дані для реалізації DoS-атак [3].

Більш захищеним рішенням є використання комбінації протоколів IPSec та 802.1x. Протокол IPSec забезпечує шифрування даних на рівні IP, а протокол 802.1x забезпечує аутентифікацію пристроїв. Таким чином, комбінація цих двох протоколів забезпечує більш високий рівень безпеки.

Іншим варіантом є використання нових протоколів IEEE 802.1AE та IEEE 802.1AR. Протокол 802.1AE забезпечує шифрування даних на рівні каналу, а протокол 802.1AR визначає унікальний захищений ідентифікатор пристроїв (SecureDeviceIdentity / DevID) для їх авторизації. Таким чином, ці протоколи забезпечують більш високий рівень безпеки, ніж протокол 802.1x.

Для ефективного захисту комп'ютерних мереж від різноманітних загроз фізичного та каналного рівнів OSI моделі використовуються різні методи та технології. Системи захисту, засновані на сучасному телекомунікаційному обладнанні, є ключовою технічною складовою цього завдання.

Аналізуючи загрози, такі як фізичне пошкодження та каналні атаки, виявлено, що використання методів, таких як MAC-фільтрація, прив'язки MAC-адрес до портів комутаторів, а також застосування додаткових захисних функцій, дозволяє ефективно протистояти внутрішнім загрозам інформаційної безпеки.

Проведений аналіз методів та технологій допомагає обґрунтовано вибрати заходи захисту, враховуючи конкретні потреби та призначення мережі.

Висновки до першого розділу

В даному розділі розглянуті основні принципи побудови захищеної кампусної мережі, включаючи різноманітні компоненти, такі як комутатори, маршрутизатори, точки доступу, сервери та робочі станції. Для забезпечення безпеки враховано технологію передачі даних, архітектуру мережі, методи маршрутизації, вразливості та атаки. Крім цього були розглянуті основні методи захисту кампусних мереж включають механізми аутентифікації та авторизації, шифрування, виявлення та запобігання вторгненням. Забезпечення безпеки кампусних мереж вимагає комплексного підходу, враховуючи всі фактори, що можуть впливати на безпеку, та впровадження комплексу заходів безпеки.

Також були сформовані рекомендації для забезпечення безпеки кампусних мереж, які включають використання сучасних технологій передачі даних, архітектури мережі, яка відповідає вимогам безпеки, сучасних методів та протоколів маршрутизації, а також впровадження комплексу заходів безпеки для захисту від різних типів атак.

РОЗДІЛ 2. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ КАМПУСНОЇ МЕРЕЖІ

2.1. Розробка загального проекту кампусної мережі

За основу проектування захищеної кампусної мережі було обрано факультет вищого навчального закладу. Головною вимогою до проектування мережі є те що вона має бути легко маштабована та змінена за вимогою керівництва.

Для моделювання кампусної мережі було використано програму Cisco Packet Tracer 8.2.1.

Cisco Packet Tracer 8.2.1 – це програмний комплекс для вдосконалення навичок у побудові та налаштуванні комп’ютерних мереж, розроблений компанією Cisco Systems в межах мережевої академії NetAcad. Cisco дозволяє безкоштовно завантажувати і використовувати Packet Tracer студентам мережевої академії Cisco.

Packet Tracer є емулятором мережі передачі даних. У ньому моделюються працездатні проекти мереж із комутаторів, маршрутизаторів та кінцевих пристроїв. Всі проміжні пристрої емулюють операційну систему Cisco IOS. Для налаштування використовується інтерфейс командного рядка.

Програмне забезпечення включає мережне обладнання різних серій, різні сервери (DHCP, HTTP, TFTP, FTP, DNS та ін.), робочі станції, модулі для кінцевих вузлів та мережевого обладнання, пристрої Wi-Fi, різноманітні з’єднувальні пристрої та різні технології з’єднання.

Крім того, комутатори та маршрутизатори Cisco є модульними, їхній функціонал можна розширити додатковими платами та SFP-модулями.

Packet Tracer ефективно дозволяє створювати навіть складні макети мереж, перевіряти топології на працездатність.

На рисунку 2.1. приведена логічна схема мережі яка показує приблизне розташування мережевого обладнання факультету по кабінетах.

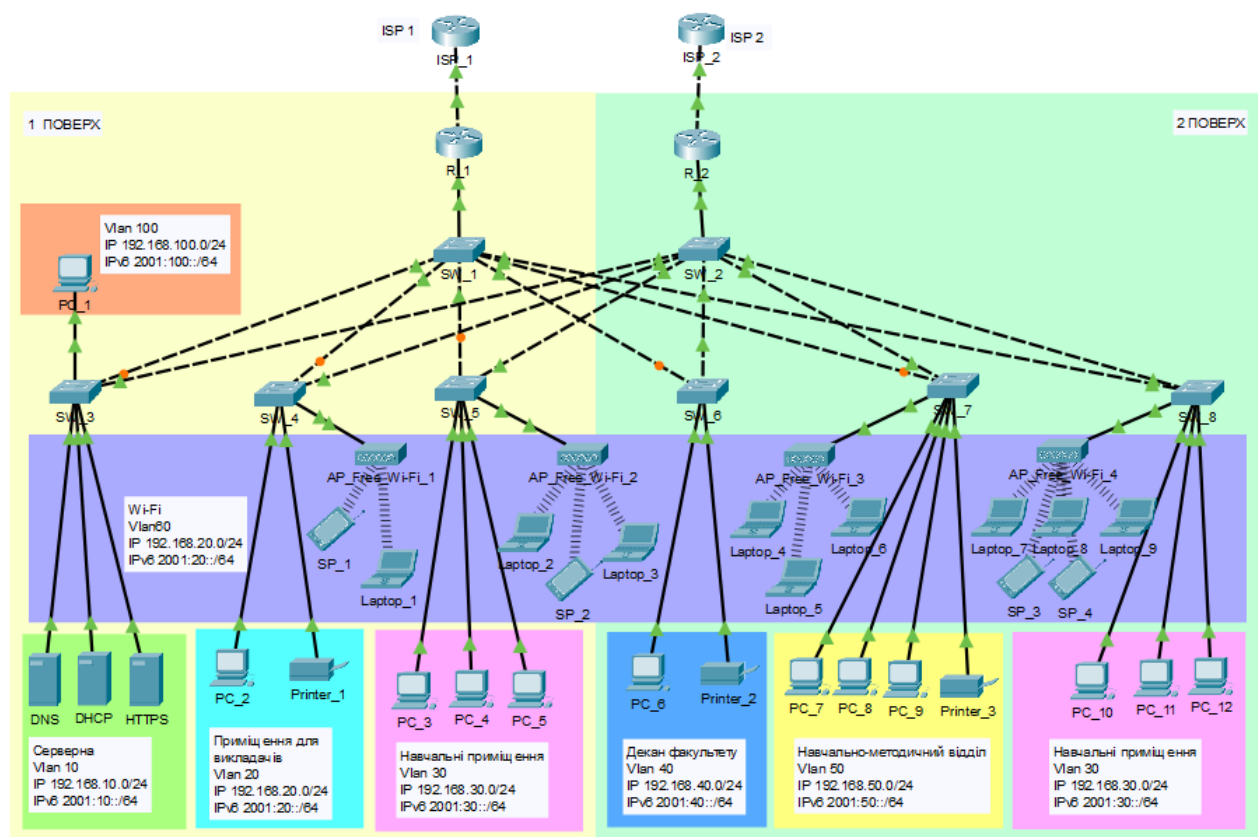


Рисунок 2.1. Логічна схема мережі

Головна будівля вищого навчального закладу має п'ять поверхів, два з яких займає обраний факультет. Як на першому так і на другому поверхах факультет займає певну кількість приміщень, в кожному з яких є мережне обладнання та комп'ютерна техніка.

Кількість обладнання та користувачів по приміщенням факультету занесені у таблицю 2.1.

Таблиця 2.1.

Кількість обладнання та користувачів

Приміщення	Обладнання	Користувачі
І поверх – комутатор (SW_1) та маршрутизатор (R_1) рівня ядра		
Серверна	1 SW – Комутатор рівня розподілу 1 PC – робоча станція управління 1 AP – безпроводна точка доступу 3 Сервери – DNS, DHCP, HTTPS	Від 1 до 3 користувачів
Викладацька 1	1 SW – Комутатор рівня розподілу 1 PC – комп'ютер загального використання 1 AP – безпроводна точка доступу 1 Printer – принтер Кінцеві вузли – ноутбуки, смартфони, планшети	Від 1 до 6 користувачів

Продовження таблиці 2.1.

Викладацька 2	1 PC – комп'ютер загального використання 1 AP – безпроводна точка доступу 1 Printer – принтер Кінцеві вузли – ноутбуки, смартфони, планшети	Від 1 до 6 користувачів
Навчальний клас 1	1 SW – Комутатор рівня розподілу 15 PC – робочі комп'ютери 1 AP – безпроводна точка доступу Кінцеві вузли – ноутбуки, смартфони, планшети	Від 1 до 30 користувачів
Навчальний клас 2	15 PC – робочі комп'ютери 1 AP – безпроводна точка доступу Кінцеві вузли – ноутбуки, смартфони, планшети	Від 1 до 30 користувачів
Навчальний клас 3	15 PC – робочі комп'ютери; 1 AP – безпроводна точка доступу Кінцеві вузли – ноутбуки, смартфони, планшети	Від 1 до 30 користувачів
II поверх – комутатор (SW_2) та маршрутизатор (R_2) рівня ядра.		
Кабінет декана	1 SW – Комутатор рівня розподілу 1 PC – комп'ютер 1 Printer – принтер 1 AP – безпроводна точка доступу Кінцеві вузли – ноутбуки, смартфони, планшети	1 користувач
Навчально-методичний відділ	1 SW – Комутатор рівня розподілу 2 PC – комп'ютери 1 Printer – принтер 1 AP – безпроводна точка доступу Кінцеві вузли – ноутбуки, смартфони, планшети	Від 2 до 4 користувачів
Деканат	3 PC – комп'ютери 2 Printer – принтери 1 AP – безпроводна точка доступу Кінцеві вузли – ноутбуки, смартфони, планшети	Від 3 до 6 користувачів
Навчальний клас 1	1 SW – Комутатор рівня розподілу 15 PC – робочі комп'ютери 1 AP – безпроводна точка доступу Кінцеві вузли – ноутбуки, смартфони, планшети	Від 1 до 30 користувачів
Навчальний клас 2	15 PC – робочі комп'ютери 1 AP – безпроводна точка доступу Кінцеві вузли – ноутбуки, смартфони, планшети	Від 1 до 30 користувачів
Навчальний клас 3	15 PC – робочі комп'ютери 1 AP – безпроводна точка доступу Кінцеві вузли – ноутбуки, смартфони, планшети	Від 1 до 30 користувачів

Для проектування мережі обрано змішану (зірка-кільце-зірка) топологію, бо така топологія вважається найбільш надійною та економічно доцільною відносно вартості та стійкості до відмов у мережі.

Також всі компоненти мережі структуровані за рівнями ієрархії відповідно до функцій. Для систематизації всіх компонентів в зручну для аналізу модель використовується ієрархічна модель Cisco, яка сприяє створенню, експлуатації і

обслуговуванню великих, ефективних і надійних мереж. Крім того, ієрархія визначає характеристики кожного рівня.

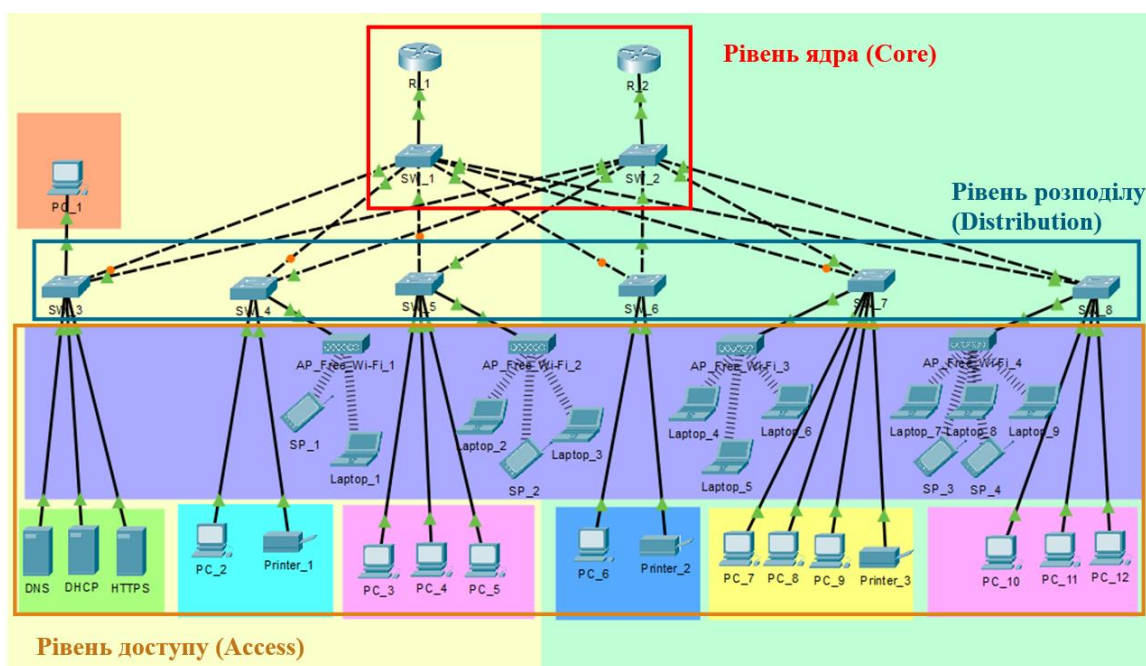


Рисунок 2.2. Розподіл мережі за тривірневою ієрархічною моделлю

Розглядаючи представлену на рисунку 2.2 схему, розподіл об'єктів мережі за рівнями відбувається згідно з функціоналом, який виконує кожен об'єкт, це допомагає аналізувати кожен рівень незалежно від інших, тобто розподіл відбувається в основному не за фізичними поняттями, а за логічними.

На рівні ядра необхідна швидка та відмовостійка пересилка великого обсягу трафіку без появи затримок. Тут слід враховувати що при виникненні проблем з продуктивністю рівня ядра рекомендується не розширювати, а модернізувати обладнання, і іноді цілком замінювати його на більш продуктивне. Тому краще відразу використовувати максимально краще обладнання, не забуваючи про наявність високошвидкісних інтерфейсів з запасом на майбутнє. Якщо використовуються кілька вузлів, рекомендується їх об'єднати в кільце для забезпечення резерву. На цьому рівні використовують маршрутизатори з принципом налаштування – VLAN. В наведеній схемі мережі (рис. 2.2) рівень ядра представлений 2 маршрутизаторами та 2 комутаторами фірми Cisco серії Catalyst.

Рівень розподілу представлений 6 комутаторами Cisco Catalyst. На цьому рівні описується політика мережі для кінцевих користувачів, формуються broadcast та multicast домени розсилок. Цей рівень вимагає використання обла-

днання з великою кількістю портів для забезпечення можливості підключення потрібної кількості вузлів рівня доступу. Часто використовуються комутатори з функціями маршрутизації (L2/3) і з принципом налаштування VLAN.

На рівня доступу фізично приєднані кінцеві пристрої (PC, принтери, точки доступу) та самі користувачі.

Зазвичай, аналізуючи один із рівнів ієрархії мережі, можна знехтувати функціями інших рівнів. Сучасні мережі визначаються великою складністю через різноманітні конфігурації, протоколи і технології. Кожен рівень відзначається виконанням конкретних функцій, хоча ці рівні є логічними і не завжди збалансовані з фізичними пристроями.

Концепція рівнів у моделі ієрархії є не лише логічним каркасом для організації мережі, але й стратегічним підходом до забезпечення ефективності, масштабованості та надійності в її функціонуванні.

За стандарти передачі даних кампусної мережі було обрано технології Fast Ethernet 100BASE-TX, Gigabit Ethernet 1000BASE-T та Wi-Fi.

2.2. Розробка логічної структури мережі

При створенні моделі мережі використовується обладнання компанії Cisco для всіх трьох рівнів ієрархії, хоча на практиці такий вибір обладнання лише одного бренду не часто зустрічається, через велику різницю в ціні. Зважаючи на те що на рівень доступу здебільшого необхідно ставити велику кількість комутаторів, нарощуючи ємність портів, не всі можуть собі дозволити, щоб ці комутатори були Cisco.

Схему спрощено для розуміння практики, тому кожен рівень, особливо розподілу і доступу, можуть містити іншу (більшу) кількість пристроїв.

Для побудови мережі для з'єднання пристроїв використано дані таблиці параметрів з'єднань наведеної у додатку 1. Для налагодження параметрів адресації пристроїв використано дані табл. 2.2. Більш детальний розподіл ір адресації наведений у додатку 2.

Таблиця 2.2.

Розподіл VLAN відповідно до відділів і приміщень

Мережа/Пристрій	IP-адреса	Маска	Префікс	IPv6-адреса
MGMT VLAN	192.168.100.0	255.255.255.0	/24	2001:100::/64
SERVER VLAN	192.168.10.0	255.255.255.0	/24	2001:10::/64
TEACHER VLAN	192.168.20.0	255.255.255.0	/24	2001:20::/64
VLAN CLASS 1 AND 2	192.168.30.0	255.255.255.0	/24	2001:30::/64
DEAN OF THE FACULTY VLAN	192.168.40.0	255.255.255.0	/24	2001:40::/64
DEAN'S OFFICE VLAN	192.168.50.0	255.255.255.0	/24	2001:50::/64
VLAN FREE Wi-Fi	192.168.60.0	255.255.255.0	/24	2001:60::/64

IP адреси VLAN обрані довільно, кількість вузлів обрана з урахуванням подальшого зростання. У побудованій мережі всім VLAN обрано стандартну маску мережі класу C – 255.255.255.0, яка відповідає префіксу /24. Крім IP версії 4, було передбачене налаштування адрес IPv6.

Схему побудована за клієнт-серверною архітектурою, спочатку налаштовуються сервери (DNS, DHCP та HTTPS), а кінцеві вузли як клієнти цих протоколів.

У кожному відділі є інформація, доступ до якої повинен бути регламентований виключно для працівників відповідного відділу, і користувачі зовнішнього середовища чи представники інших відділів не мають права на такий доступ. Відокремлення і захист інформації буде здійснений за допомогою віртуальних локальних мереж (VLAN).

VLAN (Virtual Local Area Network) – це «віртуальна» локальна комп'ютерна мережа, яка представляє собою групу робочих станцій із загальним набором вимог, які взаємодіють так, ніби вони підключені до одного маршрутизатора, незалежно від їх фізичного розташування. У спроектованій мережі буде використано 7 віртуальних локальних мереж (VLAN), кожна з яких представлена окремою IP адресою мережі. Номери віртуальних локальних мереж, їх назви та розподіл по приміщеннях згідно до схеми мережі наведені у таблиці 2.3.

Таблиця 2.3.

Розподіл VLAN відповідно до відділів і приміщень

№ з/п	Номер VLAN	Назва VLAN	Відділ або приміщення
1	100	MGMT_VLAN	
2	10	SERVER_VAN	Серверна
3	20	TEACHER_VLAN	Приміщення для викладачів
4	30	VLAN_CLASS_1	Навчальні приміщення 1 та 2 поверхів
5	40	DEAN_OF_THE_FACULTY_VLAN	Кабінет декана
6	50	DEAN'S_OFFICE_VLAN	Навчально-методичний відділ та деканат
7	60	VLAN_FREE_Wi-Fi	Навчальні приміщення 1 та 2 поверхів

2.3. Розробка проекту підсистеми захисту

Побудова підсистеми захисту мережі передбачає наявність складових, які забезпечуватимуть різні аспекти мережного захисту, тобто, передбачає наявність модулів, що виконуватимуть функції безпеки.

Найважливішим при цьому є запровадження модулів, що забезпечуватимуть:

- Налаштування аутентифікації IOS
- Відображення попереджувального повідомлення
- Налаштування віддаленого підключення SSH (Secure SHell)
- Налаштування протоколу VTP (VLAN Trunking Protocol)
- Налаштування протоколу RSTP (Rapid spanning tree protocol)
- Налаштування функції Port Fast
- Налаштування функції BPDU Guard
- Налаштування Port-Security
- Створення Access lists на обмеження віддаленого підключення
- Налаштування протоколу HSRP (Hot Standby Router Protocol)
- Налаштування DHCP snooping

Використання локальної аутентифікації IOS, де логіни та паролі будуть зберігатись на самому пристрої значною мірою підвищать рівень безпеки проєктованої мережі. На кожному мережному пристрої буде створено користувачів з

унікальними логінами та паролями та різними рівнями привілеїв. Для забезпечення безпеки паролі будуть шифруватись. Крім того, ми налаштуємо пристрої на вимогу аутентифікації при доступі до привілейованого режиму.

Пристрої налаштовуватимуться таким чином, щоб при підключенні користувача відображалось повідомлення про правила використання мережі та наслідки порушення безпеки. Це може бути інформація про заборонені дії, необхідність дотримання політик безпеки або нагадування про відповідальність за несанкціоновану діяльність. Повідомлення може бути виведеним перед входом у привілейований режим або під час підключення до пристрою.

Протокол SSH – мережевий протокол прикладного рівня, призначений для безпечного віддаленого доступу до різних систем (IOS, Linux, Windows, Mac).

Цей протокол шифрує всю передану мережею інформацію, використовуючи криптографічні техніки. Переважно він потрібен для віддаленого керування даними користувача на сервері, запуску службових команд, роботи в консольному режимі з базами даних.

Протокол VTP відповідає за поширення відомостей про VLAN, що існують на одних комутаторах, між рештою комутаторів певної групи (таку групу комутаторів зазвичай називають VTP доменом) і сильно спрощує процес реконфігурації віртуальних локальних мереж на комутаторах фірми Cisco.

Усі комутатори, на яких функціонує протокол VTP, можуть працювати в одному з трьох режимів: сервер, клієнт, прозорий режим. Комутатори, що працюють у режимі сервера, дають змогу вносити зміни в конфігурацію VLAN на поточному комутаторі, а також здатні поширювати цю конфігурацію між іншими комутаторами VTP домену, передаючи дані про внесені зміни через магістральні порти. Комутатори, що працюють у режимі клієнта, здатні приймати дані про зміни у складі віртуальних локальних мереж, які надіслали комутатори, що працюють у режимі VTP серверів, і здатні на підставі цих даних перебудовувати свої списки наявних VLAN [18]. Комутатори, що працюють у прозорому режимі, пропускають через свої магістральні порти дані про зміну в конфігурації VLAN, але не застосовують їх щодо своєї конфігурації VLAN.

Протокол RSTP має істотно менший час збіжності. Він набагато швидше перебудовує топологію мережі в разі відмови обладнання або каналів зв'язку. Час збіжності для низки відмов цього протоколу менше ніж 1 секунда проти 30+ секунд протоколу STP. RSTP будує на всі VLANи одну загальну топологію. Це не дуже зручно, оскільки не дає змоги навіть у ручному режимі балансувати трафік різними каналами. А отже, ми втрачаємо щонайменше половину пропускну здатності в разі наявності надлишкових шляхів.

Portfast – функція, яка дає змогу порту пропустити стани listening і learning та одразу ж перейти у стан forwarding. Налаштовується на портах рівня доступу, до яких підключені користувачі або сервери.

Фактично, PortFast змінює дві речі в стандартній роботі STP:

- порт пропускає стани listening і learning
- при зміні статусу порту, не відправляється повідомлення про зміну стану порту TCN BPDU (topology change notification BPDU).

Коли на інтерфейсі ввімкнено PortFast, він все одно відправляє BPDU.

Але якщо увімкнути PortFast на портах, які з'єднані з іншими комутаторами, то є ризик створення петлі. Оскільки після отримання BPDU порт залишається в стані Forwarding. За цей час уже може утворитися петля.

Тому, у зв'язці з PortFast, як правило, використовується BPDUGuard (хоча і це, звичайно ж, не дасть 100% гарантії, що не буде петлі).

BPDU Guard – функція, яка дає змогу вимикати порт під час отримання BPDU.

Може бути ввімкнена глобально на комутаторі або на інтерфейсі, у цих режимів є деякі відмінності:

Якщо BPDU Guard увімкнено глобально на комутаторі, то для портів з увімкненою функцією Port Fast:

При коректному налаштуванні, порти з увімкненим Port Fast не повинні отримувати BPDU, отримання BPDU на портах із Port Fast свідчить про неправильні налаштування або про те, що під'єднано неавторизований пристрій, у разі отримання BPDU на інтерфейсі, функція BPDU Guard переведе його в стан error-disabled.

Якщо BPDU Guard увімкнено на інтерфейсі (без увімкнення функції Port Fast):

При отриманні BPDU на інтерфейсі, функція BPDU Guard переведе його в стан error-disabled.

Port-Security – механізм забезпечення безпеки та контролю доступу заснований на контролі досліджуваних MAC-адрес. Може використовуватися як доповнення до наявної аутентифікації 802.1x і аутентифікації MAC. Port-security контролює доступ неавторизованих пристроїв до мережі, перевіряючи MAC-адресу джерела прийнятого кадру і доступ до неавторизованих пристроїв, перевіряючи MAC-адресу призначення відправленого кадру.

Якщо функціонал port-security налаштований на портах комутатора, при отриманні кадру з невірною MAC-адресою, комутатор запускає задану користувачем функцію захисту порту і автоматично виконує задану дію.

Списки доступу самі по собі не є якимись правилами, що обмежують доступ. Ці рядки лише вказують певний трафік. Ефект від них з'являється тоді, коли в налаштуваннях певної функції маршрутизатора вказується посилення на відповідний список доступу.

Логіка пристрою така, що спочатку ми показуємо маршрутизатору трафік, який нам цікавий, а потім вказуємо, що маршрутизатор має з ним зробити. Наприклад, в одному випадку список доступу вказуватиме адресу, з якої можливий віддалений доступ до маршрутизатора за протоколом SSH, а в іншому вказуватиме маршрут, який буде розповсюджено за допомогою протоколу динамічної маршрутизації.

HSRP – це протокол, який дає змогу налаштувати резервування маршрутизаторів у мережі. Він забезпечує відмовостійкість і безперервність роботи мережі шляхом автоматичного перемикання на резервний маршрутизатор у разі відмови основного. Для забезпечення безпеки мережі ми використовуватимемо автентифікацію маршрутизаторів із використанням протоколу MD5. Це дасть змогу запобігти можливості підміни або несанкціонованого доступу.

DHCP snooping використовується для запобігання атакам з використанням протоколу DHCP. Використання DHCP snooping має інформативний характер.

Наприклад, дуже зручно можна побачити, на якому порту, в якому VLAN, на якому маку яку IP-адресу видано. Ця функція захищає вашу мережу від підміни DHCP сервера. На комутаторах вручну налаштовуються довірені порти, які, як правило, під'єднані до маршрутизатора або DHCP-сервера.

Висновки до другого розділу

У даному розділі було розроблено проект захищеної кампусної мережі для факультету вищого навчального закладу. Для спроектованої мережі було обрано змішану топологію типу "зірка-кільце-зірка" як найбільш надійну та економічно доцільну. Також мережа структурована за трирівневою ієрархічною моделлю Cisco з рівнями ядра, розподілу та доступу. Крім цього розроблено логічну структуру мережі з використанням обладнання Cisco та клієнт-серверної архітектури. Передбачено 7 віртуальних локальних мереж VLAN для відокремлення та захисту трафіку різних відділів. Також детально опрацьовано методи захисту мережі, такі як: аутентифікація користувачів, протоколи SSH та VTP, механізми RSTP, Port Fast, BPDU Guard, Port Security, списки доступу, протокол HSRP, функція DHCP Snooping тощо. Отже, у другому розділі комплексно підійшли до проектування безпечної та надійної кампусної мережі з урахуванням сучасних вимог та можливостей для подальшого розвитку та масштабування.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ ЗАХИСТУ КАМПУСНОЇ МЕРЕЖІ

3.1. Вибір мережевого обладнання та програмного забезпечення

Для впровадження запропонованої мережі кампусу використовується різноманітне апаратне та програмне забезпечення. До активного мережевого обладнання входять комутатори, маршрутизатори та різноманітні кінцеві пристрої. Давайте розглянемо перелік необхідного активного мережевого обладнання для створення цієї системи.

Cisco Catalyst 2960 – це серія стекових комутаторів фіксованої конфігурації, призначених для групового об'єднання пристроїв та подальшої передачі інформації. Цей пристрій є ефективним та відносно доступним засобом для розв'язання різноманітних завдань [10]. Технічні характеристики пристрою наведені в таблиці 3.1.

Таблиця 3.1

Технічні характеристики комутатора Cisco Catalyst 2960

Характеристика	Опис характеристики
Загальні характеристики	
Тип	комутатор
Маршрутизація/тип комутації	L2 (другий рівень моделі OSI)
Кількість і тип портів Ethernet	24 x RJ45 10/100 Fast Ethernet 2 x SFP/1000BASE-T комбінований 1 x Консольний порт RJ45 Ethernet
Набір функцій програмного забезпечення Cisco IOS	LAN Base
Протокол віддаленого адміністрування	SNMP 3
Комутаційна здатність	16 Гбіт/сек
Максимальна кількість активних VLAN	255
Комутаційна смуга пропускання	повнодуплексна ємність
Робоча напруга, струм	від 100 до 240 В змінного струму, 0.4 - 0.2 А
Пам'ять пристрою	
Flash-пам'ять	64 МБ
Динамічний ОЗП	128 МБ
Стандарти, що підтримуються	IEEE 802.1Q VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab (LLDP), IEEE 802.3ad, IEEE 802.3af; Повний дуплекс IEEE 802.3x на портах 10BASE-T, 100BASE-TX і 1000BASE-T, IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, IEEE 802.3ab 1000BASE-T, IEEE 802.3z 1000BASE-X
Фізичні габарити	
Габарити	4.4 x 45 x 24.2 см
Вага	3.6 кг



Рис. 3.1. Комутатор Cisco Catalyst 2960

Cisco Catalyst 3650-24 – це ряд комутаторів третього рівня від компанії Cisco, які є передовими високотехнологічними пристроями, призначеними для використання в офісах та на підприємствах [10]. Технічні характеристики цього пристрою наведені у таблиці 3.2.

Таблиця 3.2

Технічні характеристики комутатора Cisco Catalyst 3650-24

Характеристика	Опис характеристики
Загальні характеристики	
Тип	комутатор
Маршрутизація/тип комутації	L3 (третій рівень моделі OSI)
Кількість і тип портів Ethernet	24 x 10/100/1000 (POE+); 4 x 1G SFP1
Набір функцій програмного забезпечення Cisco IOS	LAN Base
Протокол віддаленого адміністрування	SNMP 3
Комутаційна здатність	160 Гбіт/сек
Максимальна кількість активних VLAN	4,094
Комутаційна смуга пропускання	повнодуплексна ємність
Робоча напруга, струм	від 100 до 240 В змінного струму, 0.4 - 0.2 А
Пам'ять пристрою	
Flash-пам'ять	2 ГБ
Динамічний ОЗП	4 ГБ
Стандарти, що підтримуються	IEEE 802.1D STP, IEEE 802.1p CoS Prioritization, IEEE 802.1Q VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1X-Rev, IEEE 802.11, IEEE 802.1ab (LLDP), IEEE 802.3ad, IEEE 802.3x повний дуплекс 10BASE-T, 100BASE-TX та 1000BASE-T, IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, IEEE 802.3ab 1000BASE-T, IEEE 802.3z 1000BASE-X
Фізичні габарити	
Габарити	44,5 x 44,5 x 4.4 см
Вага	17.49 кг



Рис. 3.2. – Комутатор Cisco Catalyst 3650-24

Cisco 2811 – це серія маршрутизаторів, розроблених для використання в підприємствах та офісах. Цей маршрутизатор є одним з найбільш поширених пристроїв в асортименті компанії Cisco і повністю відповідає висунутим вимогам [10]. У таблиці 3.3 представлені специфікації та технічні характеристики цього пристрою.

Таблиця 3.3

Технічні характеристики маршрутизатора Cisco 2811

Характеристика	Опис характеристики
Загальні характеристики	
Тип	маршрутизатор
Призначення роутера	серверний
Інтерфейси	WAN: 2 x 10/100/1000 RJ-45 1 x USB 2.0
Протокол віддаленого адміністрування	SNMP 3
Сукупна пропускна здатність	від 100 Мбіт/с до 300 Мбіт/с
Робоча напруга, струм	від 100 до 240 В змінного струму, 0.4 - 0.2 А
Пам'ять пристрою	
Flash-пам'ять	64 МБ
Динамічний ОЗП	256 МБ / 760 МБ максимум
Фізичні габарити	
Габарити (висота x ширина x довжина)	4.5 x 43.8 x 41.7 см
Вага	6.4 кг



Рис. 3.5. Зовнішній вигляд Cisco 2811

Cisco Aironet серії 700 – це компактна точка доступу з дводіапазонним радіозв'язком 802.11n і технологією MIMO за схемою 2x2, що забезпечує про-

пускну здатність, яка щонайменше вшестеро перевершує пропускну здатність наявних мереж 802.11a/g, надають усі переваги стандарту 802.11n за привабливою ціною. Точки доступу Cisco серії 700 Aironet входять до складу уніфікованої бездротової мережі Cisco і завдяки чудовій інтеграції в наявну мережу вирізняються низькою вартістю володіння і забезпечують надійний захист інвестицій [10].

Точки доступу Cisco Aironet 700 серії підтримують одночасну роботу в двох діапазонах 2,4 ГГц і 5 ГГц і поліпшену конструкцію антени та радіо. Узгодженість передавання та приймання даних у мережі для оптимізації співвідношення швидкості та відстані, управління радіоресурсами (RRM), можливість автоматичного самовідновлення в разі виникнення проблем, пов'язаних із непередбачуваністю радіочастот, сприяє усуненню "мертвих зон" і гарантує високу доступність клієнтських під'єднань. Технологія Cisco BandSelect покращує клієнтські підключення 5 ГГц у різномірних клієнтських середовищах. Також, в пристроях Cisco Aironet 700 серії присутні передові засоби захисту, в тому числі для виявлення сторонніх пристроїв, WIPS і обробки контекстних даних.

Cisco Aironet серії 700 випускаються в наступних комплектаціях:

- AIR-CAP702W-x-K9 – дводіапазонна, з контролером, 802.11a/g/n
- AIR-CAP702W-xK910 – Есо-pack з 10 точок доступу (дводіапазонних, з контролером, 802.11a/g/n)

У таблиці 3.4 представлені специфікації та технічні характеристики цього пристрою.

Таблиця 3.4

Технічні характеристики точки доступу Cisco Aironet 700

Характеристика	Опис характеристики
Загальні характеристики	
Тип	Безпроводна точка доступу
Інтерфейси	6 x 10/100/1000, (POE+)
Стандарт бездротової локальної мережі	IEEE 802.11n
Мінімальна та максимальна частоти ISM	2,41 ГГц – 2,47 ГГц
Мінімальна та максимальна частоти UNI	5,18 ГГц – 5,70 ГГц
Посилення антени	2 дБі – 4дБі
Швидкість бездротової передачі	300 Мбіт/с

Бездротова безпека	IEEE 802.11i WPA2 WPA IEEE 802.1X AES TKIP EAP-TLS EAP-TTLS MSCHAPv2 PEAP EAP-MSCHAPv2 EAP-FAST PEAP v1 EAP-GTC
особливість	Технологія MIMO
Фізичні габарити	
Габарити (висота x ширина x довжина)	15.2 x 10.2 x 4.1 см
Вага	0.38 кг



Рис. 3.6. Зовнішній вигляд Cisco Aironet 700

3.2. Базове налаштування пристроїв кампусної мережі

Даний розділ буде містити основні команди та сценарії налаштування обладнання Cisco для програмного середовища моделювання мереж Cisco Packet Tracer.

До основних команд та сценаріїв налаштування обладнання Cisco відносяться:

1. Базові команди IOS
2. Налаштування IPv4
3. Налаштування IPv6
4. Налаштування VLAN
5. Налаштування DHCP
6. Налаштування DNS та HTTPS серверів

Сценарій використання базових команд приведений нижче:

```
Device>enable - вхід до привілейованого режиму EXEC;  
Device>ping {address or domain name} - відправка ехо-пакету хосту;  
Device>traceroute {address or domain name} - трасування маршруту до хосту;  
Device#disable - вихід з привілейованого режиму EXEC;  
Device#show running-config - перегляд налаштувань поточної конфігурації;  
Device#show startup-config - перегляд налаштувань стартової конфігурації;  
Device#copy running-config startup-config - збереження налаштувань поточної конфігурації у стартову;  
Device#configure terminal - вхід до режиму глобальної конфігурації пристрою;  
Device(config)#end - вихід з режиму конфігурації пристрою;  
Device(config)#exit - вихід з поточного режиму;  
Device(config)#do {privileged mode command} - запуск команди привілейованого режиму у режимі конфігурації пристрою.
```

Для налаштування статичних IPv4-адрес на інтерфейсах пристроїв було використано наступні сценарії:

```
R_1(config-if)#interface GigabitEthernet 0/1.100  
R_1(config-subif)#encapsulation dot1q 100  
R_1(config-subif)#ip address 192.168.100.1 255.255.255.0  
R_1(config-subif)#exit
```

```
SW_1(config)#interface vlan 100  
SW_1(config-if)#ip address 192.168.100.3 255.255.255.0  
SW_1(config-if)#no shutdown  
SW_1(config-if)#exit
```

Налаштування параметрів IPv4 адресації на пристроях рівня доступу (PC, принтери, точки доступу, сервери) відбувається за допомогою графічного інтерфейсу CLI. Статичне налаштування параметрів IPv4 адресації приведені на рисунку 3.7.

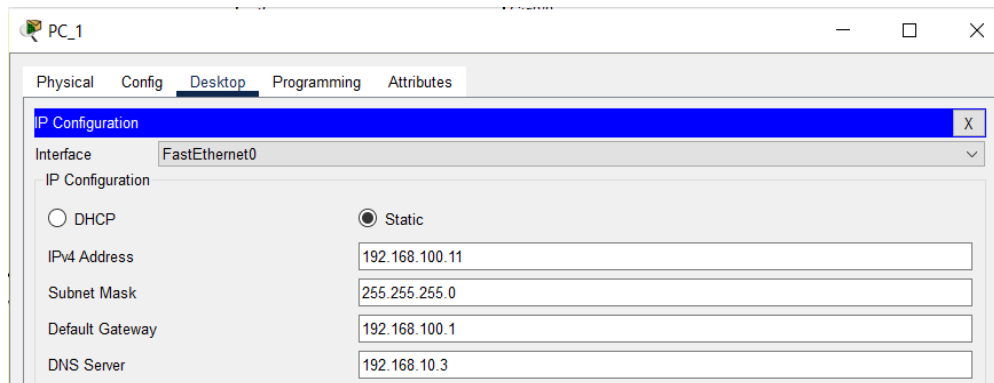


Рисунок 3.7. Налаштування параметрів IPv4 адресації PC_1

Всі інші вузли мережі, зі статичним призначенням IPv4 адресації, налаштовуються аналогічно.

Налаштування параметрів статичної IPv6-адресації на інтерфейсах проводилось за наступним сценарієм:

```
R_1(config)#ipv6 unicast-routing
R_1(config)#interface gigabitEthernet 0/1.100
R_1(config-subif)#ipv6 address 2001:100::1/64
R_1(config-subif)#ipv6 address fe80::210:11ff:fe95:1402 link-local
```

Налаштування параметрів IPv6-адресації на реальних комутаторах L2 здійснюються аналогічно до вищенаведеного сценарію, на логічному інтерфейсі VLAN, Packet Tracer не підтримує данної функції.

Налаштування параметрів IPv6 інтерфейсів кінцевих пристроїв приведено на рисунку 3.8.

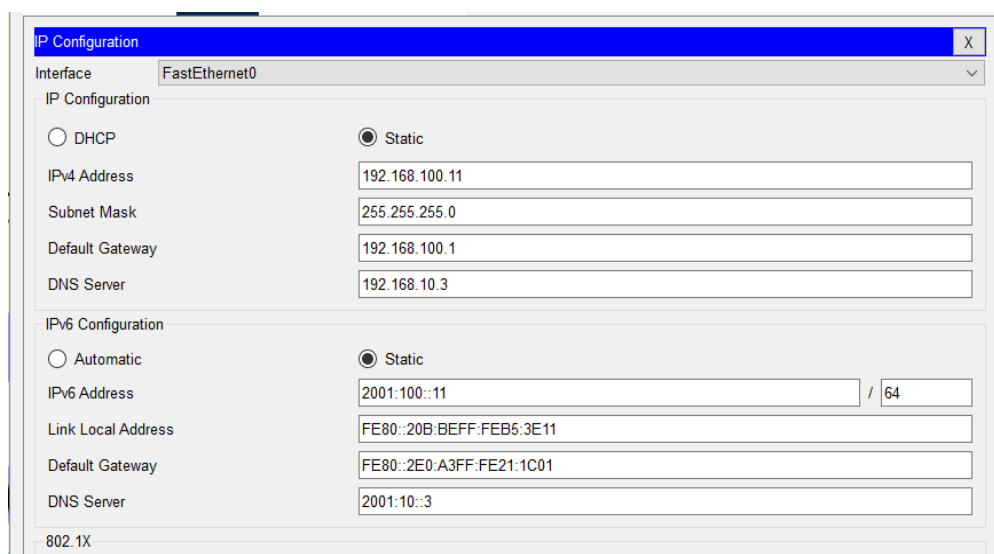


Рисунок 3.8. Налаштування параметрів IPv6 адресації PC_1

Маршрутизація трафіку між VLAN здійснюється через маршрутизатор R_1. Для того, щоб маршрутизатор міг направляти трафік від однієї VLAN до іншої (з однієї мережі до іншої), необхідно мати інтерфейс у кожній мережі. Налаштування маршрутизації між VLAN здійснюється на маршрутизаторі через інтерфейс GigabitEthernet 0/1 з використанням технології інкапсуляції 802.1Q.

Нижче представлені часткові сценарії створення VLAN, налагодження належності портів до певних VLAN та транкових каналів маршрутизатора R_1 та комутатора SW_1 (рівень ядра). Маршрутизатор R_2 та комутатор SW_2 налаштовуються аналогічно за наведеними нижче сценаріями.

```
R_1(config)#interface GigabitEthernet 0/1
R_1(config-if)#no shutdown
R_1(config-if)#interface GigabitEthernet 0/1.100
R_1(config-subif)#encapsulation dot1q 100
R_1(config-subif)#ip address 192.168.100.1 255.255.255.0
R_1(config-subif)#ipv6 address 2001:100::1/64
R_1(config-subif)#ipv6 address fe80::210:11ff:fe95:1402 link-local
R_1(config-subif)#exit
```

Всі логічні підінтерфейси маршрутизатора будуть отримувати тегований трафік з вказаним номером VLAN саме для цього інтерфейсу.

```
SW_1>enable
SW_1#configure terminal
SW_1(config)#vlan 100
SW_1(config-vlan)#name MGMT_VLAN_100
SW_1(config-vlan)#exit
SW_1(config)#vlan 10
SW_1(config-vlan)#name SERVER_VLAN_10
SW_1(config-vlan)#exit
SW_1(config)#interface range GigabitEthernet 0/1-2
SW_1(config-if-range)# switchport mode trunk
SW_1(config-if-range)# switchport nonegotiate
SW_1(config-if)#switchport trunk allowed vlan add 100
SW_1(config-if)#switchport trunk allowed vlan add 10
SW_1(config-if)#switchport trunk allowed vlan add 20
SW_1(config-if)#switchport trunk allowed vlan add 30
SW_1(config-if)#switchport trunk allowed vlan add 40
SW_1(config-if)#switchport trunk allowed vlan add 50
SW_1(config-if)#switchport trunk allowed vlan add 60
```

На комутаторі SW_1 інтерфейси G0/1 та G0/2 налаштовані як теговані порт (транкові канали).

Налаштування створення VLAN, налагодження належності портів до певних VLAN та транкових каналів комутаторів SW_3 – SW_8 (рівень розподілу) відбувається аналогічно.

Крім параметрів з вищезазначених сценаріїв на SW_3 – SW_8 були налаштовані режими доступу інтерфейсів до певних VLAN. Сценарій налаштування зазначений нижче:

```
SW_3(config)#interface range FastEthernet 0/2-4
SW_3(config-if-range)#switchport mode access
SW_3(config-if-range)#switchport access vlan 10
SW_3(config-if-range)#exit
SW_3(config)#interface FastEthernet 0/1
SW_3(config-if-range)#switchport mode access
SW_3(config-if-range)#switchport access vlan 100
SW_3(config-if-range)#exit
```

Для проектованої мережі сервер DHCP реалізовано на маршрутизаторі R_1. Нижче приведені часткові сценарії налаштування DHCP серверу для IPv4 та IPv6:

```
R_1(config)# service dhcp
R_1(config)#ip dhcp excluded-address 192.168.100.1 192.168.100.11
R_1(config)#ip dhcp pool MGMT_VLAN_100
R_1(dhcp-config)#network 192.168.100.0 255.255.255.0
R_1(dhcp-config)#default-router 192.168.100.1
R_1(dhcp-config)#dns-server 192.168.10.3
```

```
R_1(config)#ipv6 dhcp pool MGMT_VLAN_100_v6
R_1(config-dhcpv6)#address prefix 2001:100::/64
R_1(config-dhcpv6)#dns-server 2001:10::3
R_1(config-dhcpv6)#int GigabitEthernet 0/1.100
R_1(config-if)#ipv6 dhcp server MGMT_VLAN_100_v6
R_1(config-if)#ipv6 nd other-config-flag
```

Налаштування DHCP серверу для інших VLAN виконується аналогічно вищеприведеним сценаріям.

Динамічне призначення параметрів IPv4 адресації за протоколом DHCP на PC_2 наведено на рисунку 3.9.

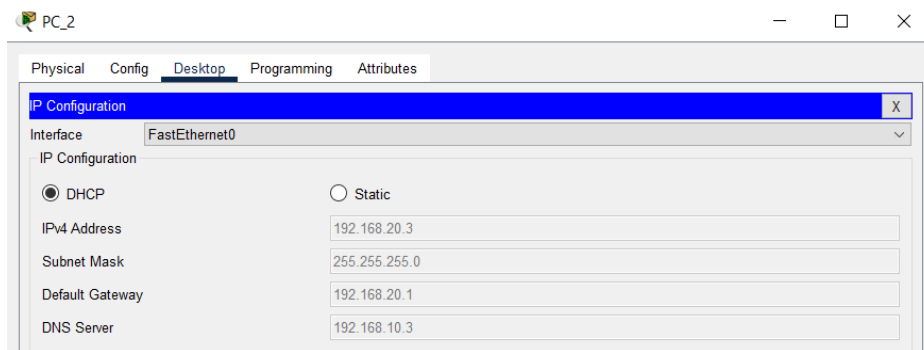


Рисунок 3.9. Динамічне призначення параметрів IPv4 адресації PC_2

Динамічне призначення параметрів IPv6 адресації за протоколом DHCP на PC_2 наведено на рисунку 3.10.

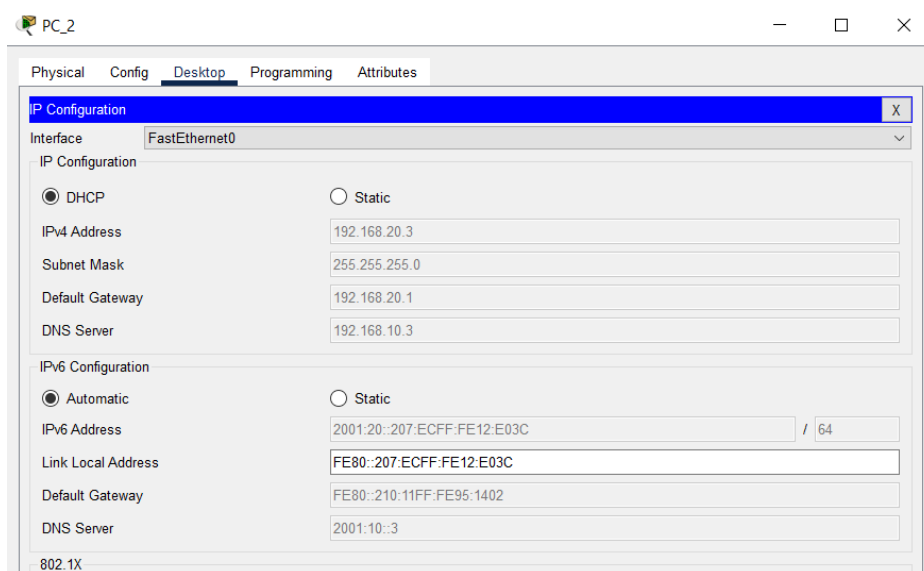


Рисунок 3.10. Динамічне призначення параметрів IPv6 адресації PC_2

Для проектованої мережі DNS та HTTPS сервери знаходяться в приміщенні серверної і належить до VLAN 10, тому IPv4-адреса DNS-сервера 192.168.10.3 а HTTPS-сервера 192.168.10.5 із шлюзом за замовчуванням 192.168.10.1, а для IPv6 – DNS-сервер 2001:10::3 а HTTPS-сервер 2001:10::5. Налаштування параметрів адресації IPv4 та IPv6 DNS та HTTPS серверів відбувається аналогічно до рисунків 3.7 – 3.8.

Налаштування DNS-серверу, здійснюється у вкладці «Services» у DNS-службі. Для створення запису DNS-сервісу в полі Name вводиться ім'я сайту, до якого звертатимуться клієнти а в полі Address вводиться IP-адреса HTTPS-сервера, на якому зберігається сайт.

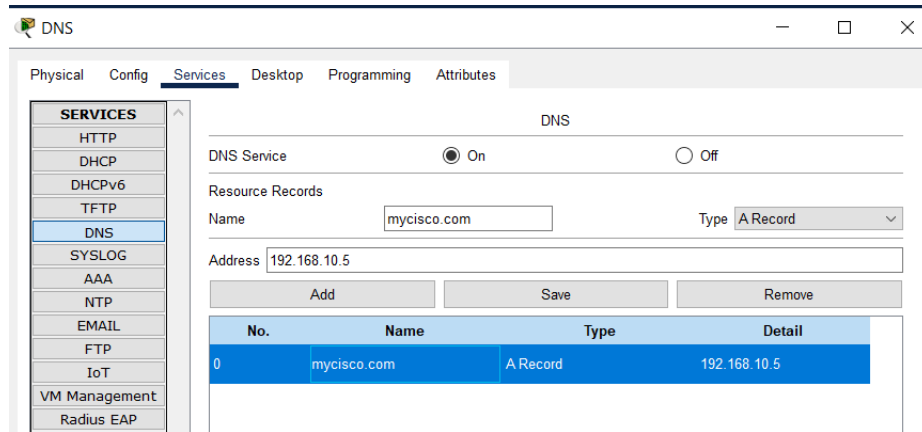


Рисунок 3.11. Налаштування DNS-серверу

Після виконання вище наведених налаштувань, ми отримаємо працездатну мережу, в якій користувачі кожної VLAN можуть отримувати доступ до інтернету та обмінюватись даними з іншими користувачами мережі різних VLAN.

3.3. Налаштування підсистеми захисту мережі

Налаштування підсистеми захисту передбачає активацію та налаштування відповідних модулів згідно даних розділу 2.3

1. Налаштування аутентифікації IOS і відображення повідомлення. Для забезпечення безпечного доступу до привілейованого режиму перед введенням команди `enable` встановлено пароль. Для цього в режимі конфігурації пристрою виконано наступну команду:

```
Device(config)# enable password {password}
```

Для збереження паролю в зашифрованому вигляді використано команду:

```
Device(config)# enable secret {password}
```

Для забезпечення безпечного доступу до консольного підключення також встановлено пароліне підключення наступними командами

```
Device(config)# line console 0
Device(config-line)# password {password}
Device(config-line)# login
```

Шифрування пароля доступу до консольного підключення виконано командою:

```
Device(config)# service password-encryption
```

На кожному мережевому пристрої було налаштоване повідомлення, яке попереджає неавторизованих користувачів про те, що доступ заборонено.

Його також можна використовувати для того, щоб залишити повідомлення мережевим інженерам (наприклад, про заплановане відключення системи або до кого звертатися за отриманням доступу). Це повідомлення називається банер MOTD (message of the day) і налаштовується такою командою:

```
Device(config)# banner motd "Authorized Access Only!"
```

2. Налаштування SSH-доступу. Для безпечного керування віддаленими підключеннями рекомендується замінити стандартний активний протокол Telnet на протокол SSH, який забезпечує захист віддалених під'єднань, надаючи надійне шифрування даних аутентифікації пристрою (ім'я користувача та пароль). Для налаштування протоколу віддаленого доступу SSH використано наступну послідовність команд:

```
Router(config)#hostname R_1  
R_1(config)#ip domain name FACULTY.COM  
R_1(config)# crypto key generate rsa general-keys modulus 1024  
R_1(config)#username admin privilege 15 secret  
R_1(config)#ip ssh version 2  
R_1(config)#line vty 0 4  
R_1(config-line)#transport input SSH  
R_1(config-line)#transport output SSH
```

3. Налаштування протоколу VTP. Перед налаштуванням протоколу VTP було визначено ролі комутатори мережі (клієнт, сервер). Комутатором сервером було обрано SW_1, так як він приблизно рівновіддалений від усіх інших пристроїв VTP домену, для того щоб скоротити навантаження, яке виникає в мережі під час поширення оновлень протоколу VTP між комутаторами.

Для того щоб сконфігурувати SW_1 як VTP-сервер, виконано наступні команди:

```
SW_1(config)#vtp domain FACULTY  
SW_1(config)#vtp password 111  
SW_1(config)#vtp version 2
```

Обов'язкова з цих команд лише перша. Рештою за бажанням всіма наступними можна знехтувати.

Далі конфігуруємо комутатори SW_2 – SW_8 як клієнтів VTP, виконавши на них команди:

```
SW_2(config)#vtp domain FACULTY
SW_2(config)#vtp password 111
SW_2(config)#vtp version 2
SW_2(config)#vtp mode client
```

4. Налаштування STP. Налаштування комутаторів в межах однієї VLAN необхідно робити таким чином, щоб уникнути утворення петель. Для цього необхідно задати пріоритет комутатора. Цей параметр визначає вибір root bridge. Пріоритет може набувати значення від 0 до 61 440 з кроком 4096. Значення за замовчуванням 32 768. Налаштування пріоритету виконується наступними командами

```
SW_1(config)#spanning-tree vlan 1 priority 24586
```

Для призначення комутатору ролі основного або вторинного root bridge необхідно виконати наступні команди:

Налаштування основного root bridge:

```
SW_1(config)# spanning-tree vlan 1 root primary
```

При цьому значення priority буде виставлено меншим, ніж у нинішнього root bridge.

Налаштування вторинного root bridge:

```
SW_3(config)#spanning-tree vlan 1 root secondary
```

Для того щоб налаштувати пріоритет інтерфейсу необхідний для визначення найкоротшого шляху до root bridge змінити пріоритет використання ліній зв'язку. Пріоритет інтерфейсу може набувати значення від 0 до 240 із кроком 16. Значення за замовчуванням 128. Налаштування має вигляд:

```
SW_1(config-if)#spanning-tree vlan 1 port-priority 240
```

5. Налаштування RSTP. Після налаштування протоколу STP на комутаторах мережі вмикаємо RSTP:

```
SW_1(config)#spanning-tree mode rapid-pvst
```

Цей протокол потрібен для того, щоб у разі виходу з одного з каналів передачі трафіку, збіжність мережі відбувалася майже миттєво і з мінімальною втратою пакетів під час передачі.

6. Налаштування функцій прискорення PortFast. Спочатку Port Fast налаштовано глобально на всіх інтерфейсах у режимі access, а потім на інтерфейсах які приймають участь у побудові активної топології відключаємо Port Fast. Ці налаштування мають наступний вигляд:

```
SW_3(config)#spanning-tree portfast default
SW_3(config)#interface range gig 0/1-2
SW_3(config-if-range)#spanning-tree portfast disable
```

7. Налаштування функцій захисту BPDU Guard. Увімкнення BPDU Guard глобально на комутаторі, на портах з увімкненою функцією Port Fast здійснюється наступною командою:

```
SW_3(config)# spanning-tree portfast bpduguard default
```

8. Налаштування Port-security. На порті Fa 0/1 комутатора SW_3, підключеного до PC_1 (станція управління), налаштована функція безпеки таким чином, щоб тільки одному вузлу був дозволений доступ до порту. MAC-адреса пристрою додається статично в поточну конфігурацію. При порушенні системи безпеки порт виключається. Команди використані на комутаторі наведені нижче:

```
SW_3(config)#interface fa 0/1
SW_3(config-if)#switchport mode access
SW_3(config-if)#switchport port-security
SW_3(config-if)#switchport port-security maximum 1
SW_3(config-if)#switchport port-security mac-address sticky
SW_3(config-if)#switchport port-security violation shutdown
```

9. Налаштування access list, який використовується для обмеження віддаленого доступу до консолі R_1 тільки з певних ір адрес. У нашому випадку – адреса PC_1 (станція управління), наведене нижче:

```
R_1(config)#ip access-list standard REMOTE_ACCESS
R_1(config-std-nacl)#permit host 192.168.100.11
R_1(config)#line vty 0 4
R_1(config-line)#access-class REMOTE_ACCESS in
```

При невірному налаштуванні access list помилку можна буде виправити тільки підключившись консольним кабелем або скинувши налаштування маршрутизатора до заводських.

10. Налаштування DHCP snooping відбувається за наступним сценарієм:

Насамперед вмикаємо глобально DHCP snooping на комутаторі:

```
SW_5(config)#ip dhcp snooping
```

Вмикаємо DHCP snooping у потрібному VLAN:

```
SW_5(config)#ip dhcp snooping vlan 30
```

Вказуємо довірені порти, для цього переходимо до конфігурації потрібних нам портів і оголошуємо їх довіреними:

```
SW_5(config)#interface range fa 0/1-2
SW_5(config-if-range)#ip dhcp snooping trust
```

На даному етапі DHCP snooping працює в 30 VLAN і довіреним портом є порти fa 0/1 та fa 0/2, подальші налаштування не є обов'язковими в базовому випадку.

Далі налаштовуємо DHCP snooping на обмеження кількості DHCP звернень на не довірених інтерфейсах.

```
SW_5(config)#interface range fastEthernet 0/3-7  
SW_5(config-if-range)#ip dhcp snooping limit rate 15
```

11. Налаштування протоколу HSRP. Навіть якщо топологію кампусної мережі спроектовано з урахуванням надмірності (два маршрутизатори і два комутатори в одній мережі LAN), всі інші пристрої мережі необхідно налаштовувати з адресою шлюзу, враховуючи сегментацію на VLAN, і що у кожній VLAN своя адреса шлюзу. У разі збою на одному з цих маршрутизаторів або інтерфейсів маршрутизаторів комп'ютер може втратити підключення до мережі Інтернет. Для того щоб цього не відбулося на SVI маршрутизатора було налаштовано протокол резервування шлюзу HSRP за наступними сценаріями:

```
R_1#conf  
R_1(config)#interface g0/1.100  
R_1(config-subif)#standby 100 priority 80  
R_1(config-subif)#standby 100 ip 192.168.100.254
```

```
R_2(config)#interface g0/1.100  
R_2(config-subif)#no standby 100 ip 192.168.100.254  
R_2(config-subif)#standby 100 preempt
```

Налаштування всіх інших пристроїв кампусної мережі відбувались за приведеними вище сценаріями, результати налаштувань приведені в додатках у вигляді конфігураційних файлів.

3.4. Тестування системи захисту та аналіз результатів

Тестування працездатності мережі представлені на рисунках 3.12. – 3.13. На рисунку 3.12. представлені результати обміну даними з PC_1 до R_1 по IPv4 та IPv6, а на рисунку 3.13. обмін даних між PC управління з PC які відносяться до різних Vlan.

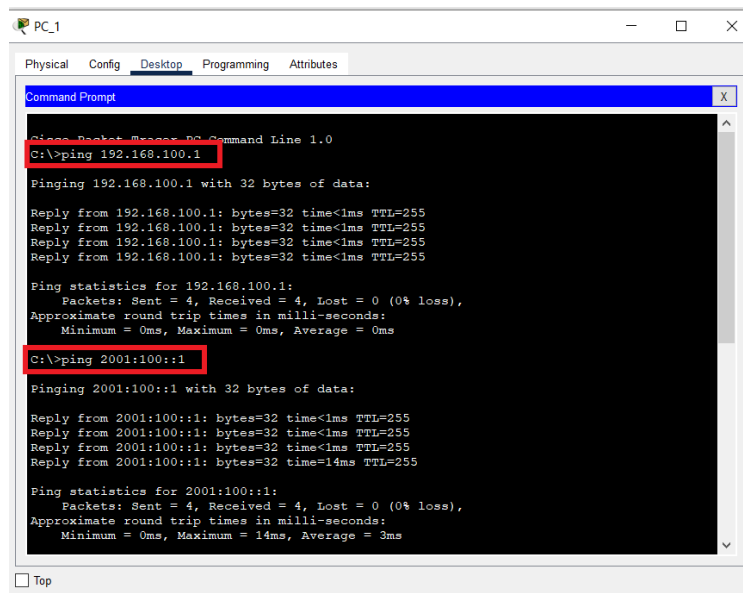


Рисунок 3.12. Ping від PC_1 до маршрутизатора R_1

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC_1	PC_2	ICMP		0.000	N	0	(edit)	
	Successful	PC_1	PC_3	ICMP		0.000	N	1	(edit)	
	Successful	PC_1	PC_3	ICMP		0.000	N	2	(edit)	
	Successful	PC_1	PC_6	ICMP		0.000	N	3	(edit)	
	Successful	PC_1	PC_7	ICMP		0.000	N	4	(edit)	
	Successful	PC_1	PC_10	ICMP		0.000	N	5	(edit)	
	Successful	PC_1	Laptop_1	ICMP		0.000	N	6	(edit)	

Рисунок 3.13. Ping від PC_1 до PC всіх VLAN

На рисунку 3.14. представлено результати тестування SSH-доступу. Приведено вдалу спробу віддаленого підключення за протоколом SSH до маршрутизатора R_1 з PC_1 (станції управління).

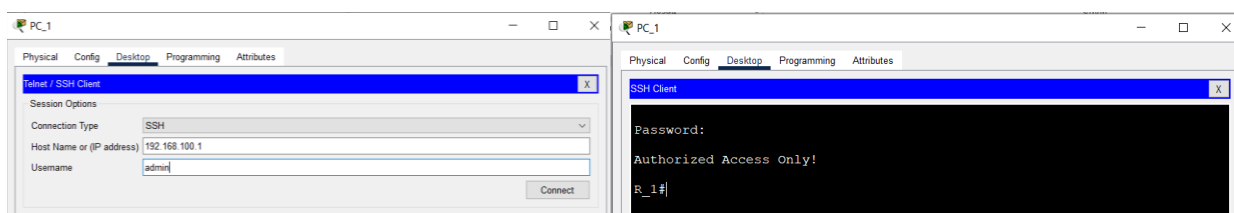


Рисунок 3.14. Результат виконання віддаленого підключення

Для перевірки роботи протоколу VTP виконаємо на комутаторі SW_1 наступні команди:

```

SW_1(config)#Vlan 99
SW_1(config-vlan)#name TEST_VLAN_99
  
```

А потім проаналізуємо виведення команд `show vtp status` та `show vlan brief` на комутаторах SW_1 та SW_2, якщо протокол VTP працює, то ми повинні побачити таку картину:

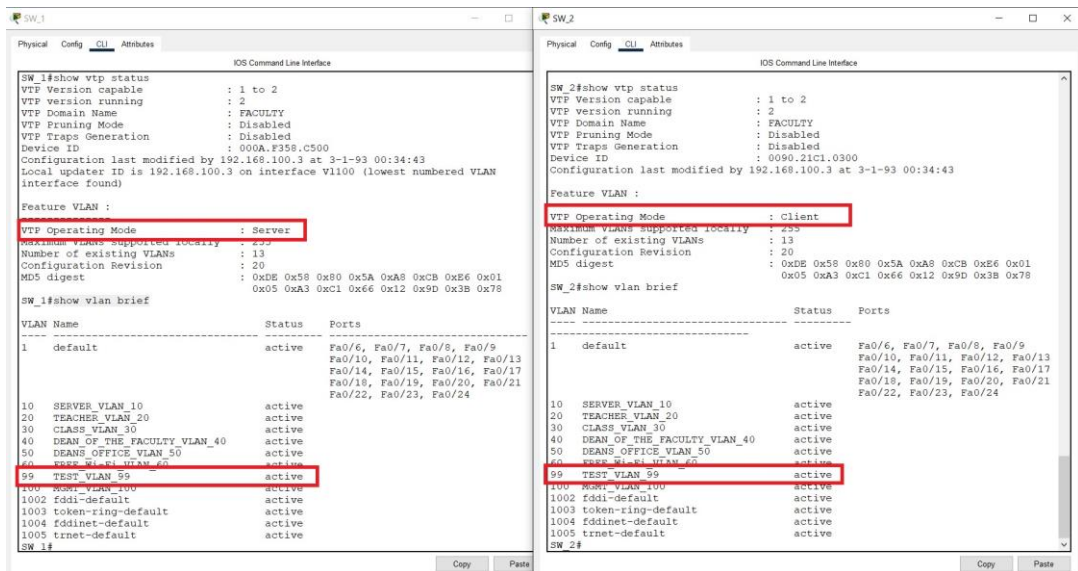


Рисунок 3.15. Результат виконання команд show vtp status та show vlan brief

З вищеприведених діагностичних команд можна побачити роль сервера чи клієнта протоколу VTP, а також наявність VLAN з номером 99 на комутаторі SW_2, без його створення на цьому пристрої, завдяки роботі протоколу VTP.

Тепер спробуємо додати новий VLAN з номером 101 на комутаторі SW_2, виконавши команду:

SW_1(config)#Vlan 101

Після введення цієї команди ми отримаємо повідомлення вигляду:

VTP VLAN configuration not allowed when device is in CLIENT mode.

Створення VLAN на комутаторах, які функціонують як клієнти у VTP домені не можливо.

Результати налаштування протоколу RSTP на первинному і вторинному root bridge комутаторах приведені на рисунку 3.16:

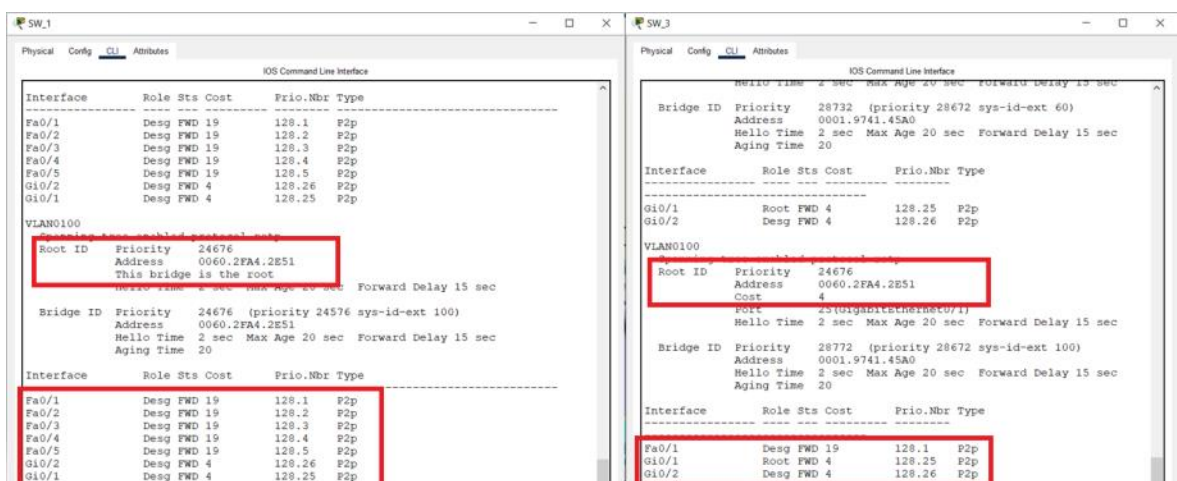


Рисунок 3.16 Результати налаштування протоколу RSTP

Нижче приведена інформація про статус функції Port Fast та налаштування spanning-tree на інтерфейсі Gig 0/1:

```

SW_3>en
SW_3#show spanning-tree interface gig 0/1 portfast
VLAN0001          disabled
VLAN0010          enabled
VLAN0020          enabled
VLAN0030          enabled
VLAN0040          enabled
VLAN0050          enabled
VLAN0060          enabled
VLAN0100          enabled
SW_3#show spanning-tree interface gig 0/1 detail

Port 25 (GigabitEthernet0/1) of VLAN0001 is root forwarding
Port path cost 4, Port priority 128, Port Identifier 128.25
Designated root has priority 24577, address 0060.2FA4.2E51
Designated bridge has priority 24577, address 0060.2FA4.2E51
Timers: message age 16, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default

Port 25 (GigabitEthernet0/1) of VLAN0010 is root forwarding
Port path cost 4, Port priority 128, Port Identifier 128.25
Designated root has priority 24586, address 0060.2FA4.2E51
Designated bridge has priority 24586, address 0060.2FA4.2E51
Timers: message age 16, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default

```

Рисунок 3.17. Результати налаштування функції Port Fast

Якщо Port Fast було ввімкнено глобально на всіх access-портах, то це можна подивитися в сумарній інформації про налаштування STP на комутаторі:

```

SW_3#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for:
Portfast Default is enabled
Portfast BPDU Guard Default is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
EtherChannel misconfig guard is disabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short

```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	4	0	0	2	6
VLAN0010	1	0	0	5	6
VLAN0020	4	0	0	2	6
VLAN0030	4	0	0	2	6
VLAN0040	4	0	0	2	6
VLAN0050	4	0	0	2	6
VLAN0060	4	0	0	2	6
VLAN0100	3	0	0	3	6
8 vlans	28	0	0	20	48

Рисунок 3.18. Результати налаштування функції Port Fast глобально

Діагностика та тестування функції BPDU Guard приведені нижче:

Так як функцію BPDU Guard було ввімкнено глобально на комутаторі, то результати налаштувань можна подивитися в сумарній інформації про налаштування STP на комутаторі

```

SW_3>en
SW_3#sh
SW_3#show sp
SW_3#show spanning-tree su
SW_3#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for:
Extended system ID      is enabled
PortFast Default        is enabled
PortFast BPDUGuard Default is enabled
PortFast BPDUGuard Filter Default is disabled
Loopguard Default       is disabled
EtherChannel misconfig guard is disabled
UplinkFast              is disabled
BackboneFast            is disabled
Configured Pathcost method used is short

```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	4	0	0	2	6
VLAN0010	1	0	0	5	6
VLAN0020	4	0	0	2	6
VLAN0030	4	0	0	2	6
VLAN0040	4	0	0	2	6
VLAN0050	4	0	0	2	6
VLAN0060	4	0	0	2	6
VLAN0100	3	0	0	3	6
8 vlans	28	0	0	20	48

Рисунок 3.19. Результати налаштування функції BPDU Guard

Після налаштування функції захисту при спробі під'єднати новий комутатор «ЗЛОВМИСНИК» до комутаторі SW_3 до порта, де була підключена PC_1, інтерфейс переходить у вимкнений стан.

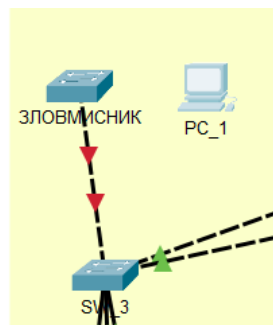


Рисунок 3.20. Підключення комутатора «ЗЛОВМИСНИК» до комутатор SW_3

```

SW_3#show interfaces fast Ethernet 0/1
FastEthernet0/1 is down, line protocol is down (err-disabled)
Hardware is Ethernet, address is 00e0.a321.1c01 (bia 00e0.a321.1c01)
BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue 10/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    956 packets input, 193351 bytes, 0 no buffer
    Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    2357 packets output, 263570 bytes, 0 underruns
    0 output errors, 0 collisions, 10 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out

```

Рисунок 3.21. Стан інтерфейсу при підключенні комутатора «ЗЛОВМИСНИК»

Після налаштування функції Port-security при спробі під'єднати нову робочу станцію «ЗЛОВМИСНИК» до комутаторі SW_3 до порта, де була підключена PC_1, інтерфейс переходить у вимкнений стан.

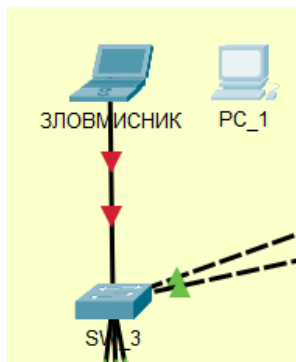


Рисунок 3.22. Підключення ноутбука «ЗЛОВМИСНИК» до комутатора SW_3
Результати налаштувань і стану інтерфейсу приведені на рисунку 3.23.

```
SW_3
Physical Config CLI Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (100), with Switch FastEthernet0/1 (1).
%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/1 with
BPDU Guard enabled. Disabling port.
%PM-4-ERR_DISABLE: bpduguard error detected on 0/1, putting 0/1 in err-
disable state
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down
show port-security interface fa0/1
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 : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 00D0.BCD4.BA01:100
Security violation count : 0
```

Рисунок 3.23. Стан інтерфейсу при підключенні ноутбука «ЗЛОВМИСНИК»

Далі приведені результати тестування обмеження віддаленого доступу налаштованого Access list.

Спроби віддаленого підключення за протоколом SSH з PC_1 та PC_2 приведені на рисунку 3.24. Як ми можемо побачити спроба підключення з PC_2 є невдалою за рахунок обмеження віддаленого доступу.

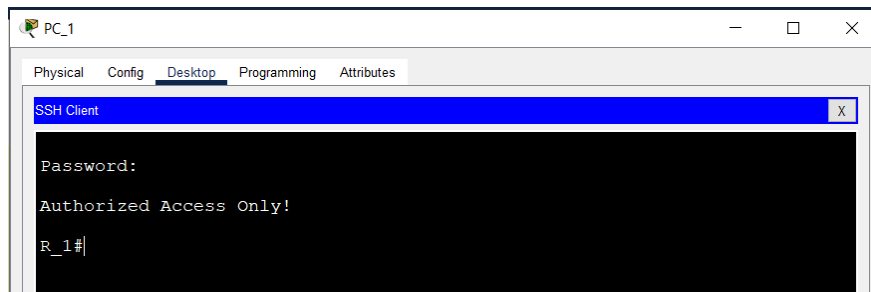


Рисунок 3.24. Спроби вдалого віддаленого підключення з PC_1

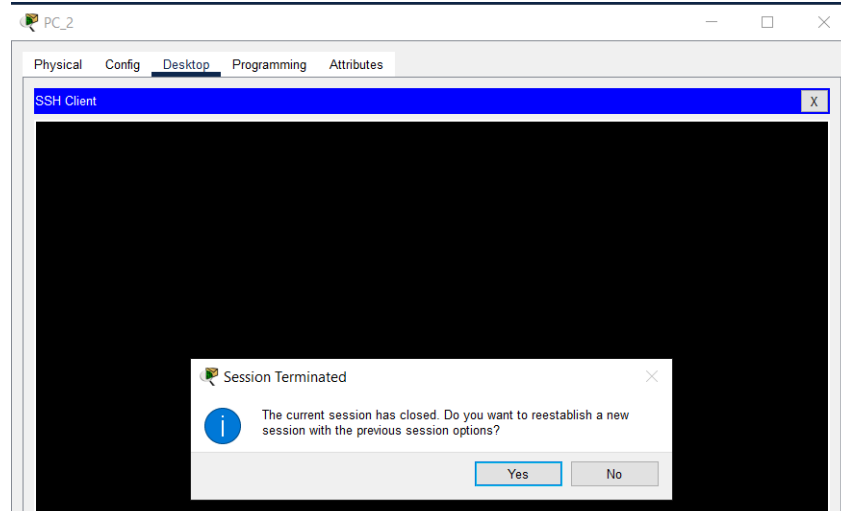


Рисунок 3.25. Спроби невдалого віддаленого підключення з PC_2

На рисунку 3.26. представлені результати налаштування DHCP snooping.

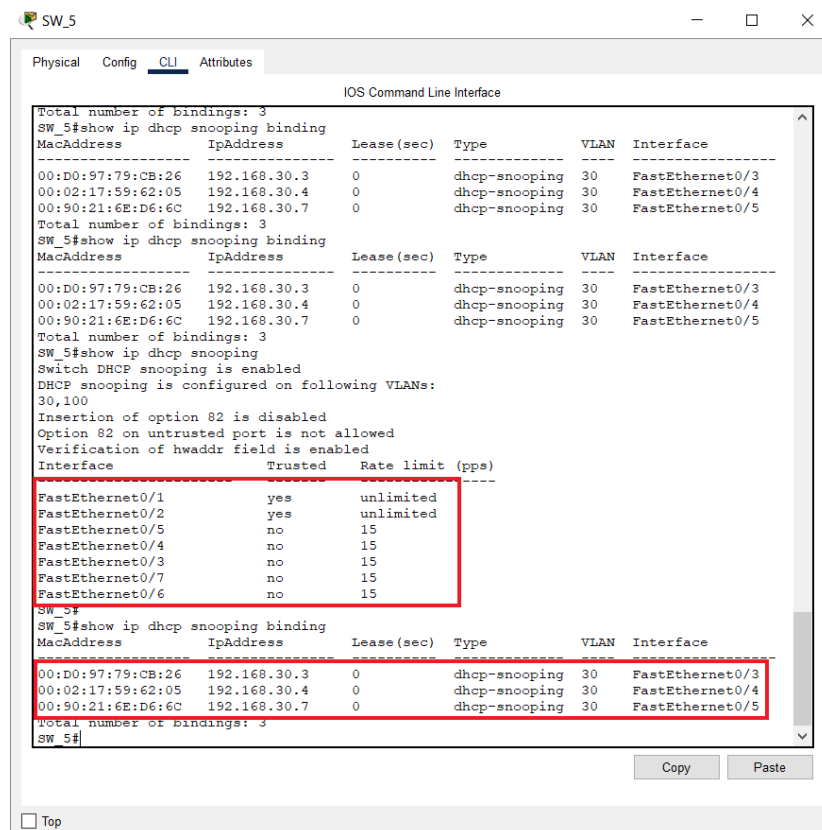


Рисунок 3.26. Результати налаштування DHCP snooping

На рисунку 3.27. представлені налаштування резервування шлюзу за замовчуванням для Vlan 100 (Vlan керування).

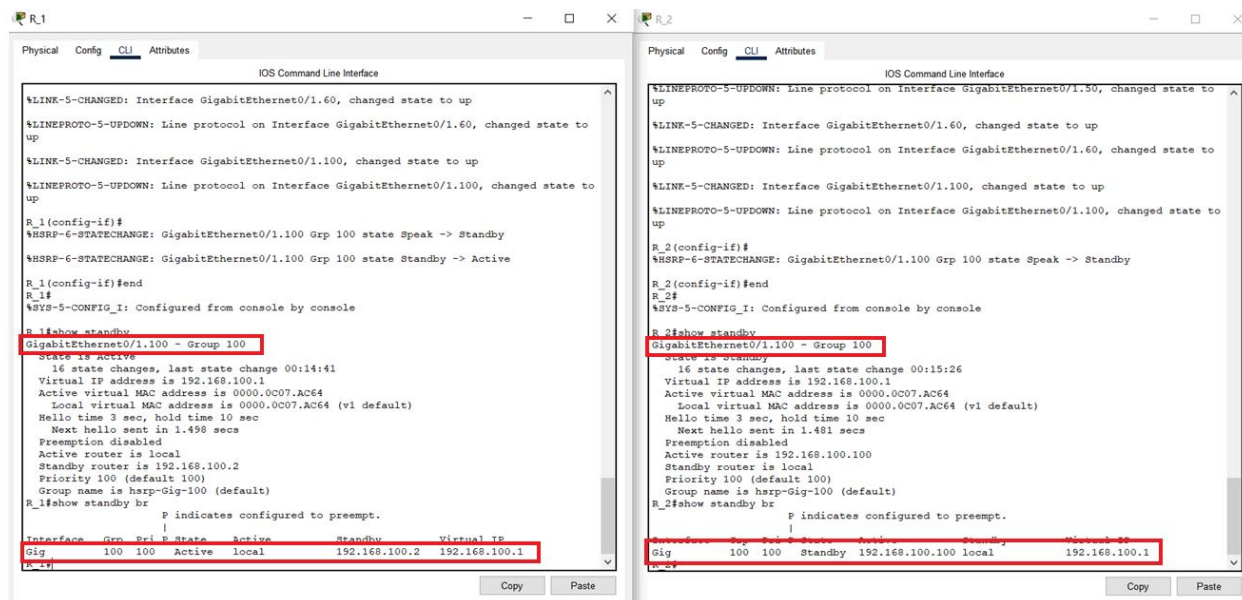


Рисунок 3.27. Налаштування HSRP

На рисунках 3.28 та 3.29 приведені успішні результати доступності віртуального шлюзу за замовчуванням при доступному і недоступному маршрутизатору R_1.

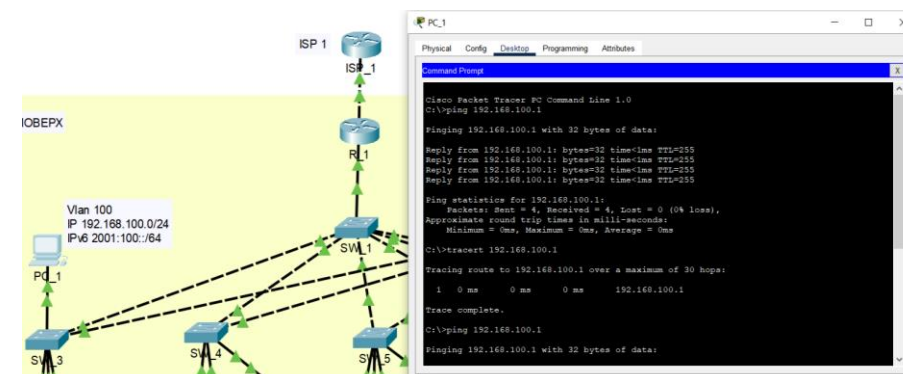
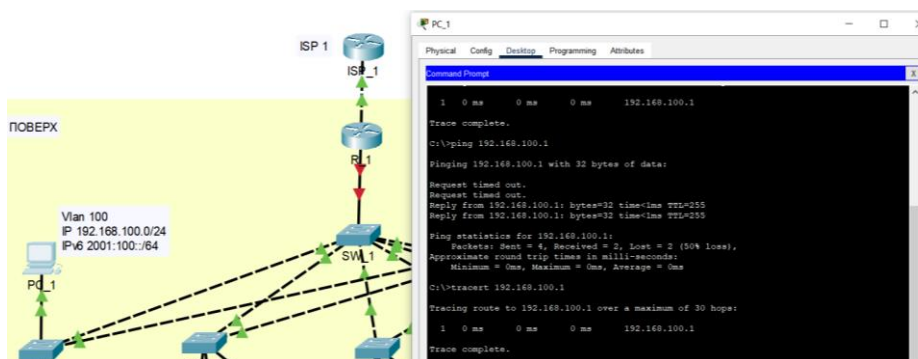


Рисунок 3.28. Ping з доступним R_1



3.29. Ping з доступним R_1

Висновки з третього розділу

В даному розділі описано практичну реалізацію та тестування системи захисту кампусної мережі. Крім цього вибрано необхідне мережеве обладнання та програмне забезпечення для реалізації системи захисту кампусної мережі. Детально розглянуті технічні характеристики обраного обладнання: комутаторів Cisco Catalyst 2960, 3650-24, маршрутизатора Cisco 2811, точок доступу Cisco Aironet 700. Виконано базове налаштування пристроїв кампусної мережі: налаштування IP адресації IPv4 та IPv6, VLAN, DHCP, DNS та HTTPS серверів. Виконано налаштування підсистеми захисту мережі: аутентифікації IOS, SSH доступу, протоколів VTP, STP, RSTP, функцій PortFast, BPDU Guard, Port Security, access list, DHCP snooping, HSRP. Проведено тестування роботи системи захисту та проаналізовано отримані результати. В ході тестування перевірено працездатність мережі, SSH доступу, протоколів VTP, STP, RSTP, функцій PortFast, BPDU Guard, Port Security, access list, DHCP snooping, HSRP.

Всі тести демонструють успішну практичну реалізацію, підтверджують працездатність та ефективність запропонованих в проекті рішень. Таким чином детально описаний процес реалізації та тестування системи захисту кампусної мережі досягли поставленої задачі та виконані в повному обсязі.

ВИСНОВКИ

В кваліфікаційній роботі представлено ефективний план захисту мережі, який вимагає глибокого розуміння проблем безпеки, ідентифікації потенційних загроз, встановлення відповідного рівня безпеки та врахування факторів, які роблять мережу вразливою для атак.

У першому розділі наведено ґрунтовний теоретичний огляд основних понять, принципів та технологій побудови захищеної кампусної мережі. Розглянуто фактори та основні загрози, що впливають на безпеку, та основні методи та технології захисту.

У другому розділі виконано проектування захищеної кампусної мережі для конкретного об'єкта, за надійною та економічно доцільною топологією. Мережа структурована за трирівневою ієрархічною моделлю та передбачено сегментація на VLAN для відокремлення та захисту трафіку. Структуровані та запропоновані ефективні рішення та механізми захисту мережі.

Третій розділ присвячено практичній реалізації та тестуванню спроектованої системи захисту. Обрано необхідне мережеве обладнання, виконано його базове налаштування, та впроваджені механізми. Проведені діагностичні та тестові результати які підтверджують працездатність та ефективність запропонованих рішень.

У результаті дослідження було розроблено ефективні рішення щодо побудови та захисту кампусних комп'ютерних мереж. Запропоновані рішення дозволяють підвищити надійність та ефективність захисту мережі від атак на доступ, конфіденційність та цілісність.

Отримані результати можуть бути використані для впровадження алгоритмів захисту як для державних так і комерційних кампусних мереж. Перспективним напрямком подальших досліджень є вивчення нових сучасніших методів та технологій захисту кампусних мереж, а також розробка ефективних методів виявлення та запобігання новим загрозам які зростають і вдосконалюються щодня.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Вертузаєв М. Захист інформації в комп'ютерних системах від несанкціонованого доступу : навч. посіб. / М. Вертузаєв, О. Юрченко ; ред. С. Глаптев. – Київ : Європ. ун-ту, 2001. – 321 с.
2. Грайворонський М. В. Безпека інформаційно-комунікаційних систем : підручник / Микола Владленович Грайворонський, Олексій Миколайович Новіков. – Київ : Вид. група BHV, 2009. – 698 с.
3. Дослідження мережевих DOS-атак, що ґрунтуються на використанні протоколу ICMP / С. Л. Михайлюта [та ін.] // Вісник Інженерної академії України. – 2009. – № 2. – С. 146–149.
4. Корнієнко Б. Я. Дослідження моделі взаємодії відкритих систем з погляду інформаційної безпеки / Б. Я. Корнієнко // Мікросистеми, Електроніка та Акустика. – 2017. – Т. 22, № 6. – С. 64–70.
5. Коробейнікова Т. І. Технології захисту локальних мереж на основі обладнання CISCO : навч. посіб. / Т. І. Коробейнікова, С. М. Захарченко. – Львів : Львів. політехніки, 2021. – 188 с.
6. Кучернюк П. В. Методи і технології захисту комп'ютерних мереж (мережний, транспортний та прикладний рівні) / П. В. Кучернюк // Мікросистеми, Електроніка та Акустика. – 2018. – Т. 23, № 1. – С. 52–58.
7. Кучернюк П. В. Модель загроз безпеки в інформаційно-комунікаційних системах на основі регресійного аналізу / П. В. Кучернюк, А. О. Довгаль // Електроніка та зв'язок. – 2017. – Т. 22, № 2. – С. 79–84.
8. Кучернюк П. В. Основи побудови інформаційних мереж : навч. посіб. для студентів спец. «Радіоелектронні апарати та засоби» / П. В. Кучернюк. – Київ : НТУУ «КПІ», 2014. – 269 с.
9. Методичні рекомендації для виконання лабораторних робіт з навчальної дисципліни «Комп'ютерні мережі». Частина 3 для здобувачів вищої освіти освітнього ступеня «бакалавр» спеціальності 125 «Кібербезпека» (ОПП «Кібербезпека») : Метод. рек. / О. Дячук [та ін.]. – Житомир : [б. в.], 2021. – 138 с.
10. Офіційний сайт виробника обладнання Cisco Systems [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/uk_ua/index.html.
11. Побудова швидкісних мультисервісних мереж / Т. І. Трояновська [та ін.] // Smart and Young. – 2016. – № 8. – С. 72–78.

12. Технології забезпечення безпеки мережевої інфраструктури : підручник / В. Л. Бурячок [та ін.]. – Київ : КУБГ, 2019. – 218 с.
13. 802.1AE: MAC Security (MACsec) | [Electronic resource]. – Mode of access: <https://1.ieee802.org/security/802-1ae/> (date of access: 26.12.2023). – Title from screen.
14. Bhaiji F. H. Y. Network security technologies and solutions / Fahim Hussain Yusuf Bhaiji. – Indianapolis, IN : Cisco Press, 2008. – 792 p.
15. Ferguson N. Cryptography Engineering: Design Principles and Practical Applications / Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. – [S. l.] : Wiley & Sons, Limited, John, 2015. – 384 p.
16. IEEE 802.1: 802.1X-2001 - Port Based Network Access Control [Electronic resource] // IEEE802. – Mode of access: <http://www.ieee802.org/1/pages/802.1x-2001.html> (date of access: 26.12.2023). – Title from screen.
17. Llovente O. W. IPv6 deployment, not only a network problem / Omar Walid Llovente, Tomás P. de Miguel Moro, David Fernández Cambronero // IFIP International Federation for Information Processing. – 2006. – Vol. 196. – P. 105–118.
18. Seifert R. The all-new switch book: The complete guide to LAN switching technology / Rich Seifert. – 2nd ed. – Indianapolis, IN : Wiley Pub., 2008. – 784 p.
19. Slattery T. What is a VLAN (Virtual LAN)? [Electronic resource] / Terry Slattery, John Burke // Networking. – Mode of access: <https://www.techtarget.com/searchnetworking/definition/virtual-LAN> (date of access: 26.12.2023). – Title from screen.
20. S. Roy D. Issues with Dual Stack IPv6 on by Default / Durand S. Roy, J. Paugh // IETF Internet Draft. – 2004. – P. 1–13.
21. Yaibuates M. Implementing of IP address Recovery for DHCP Service / M. Yaibuates, R. Chaisricharoen // International Journal of Applied Engineering Research. – 2018. – Vol. 13, no. 5. – P. 2659–2662.

ДОДАТКИ

Додаток 1

Таблиця з'єднань кампусної мережі

Комутатор / Ідентифікатор комутатора	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
R_1	Gig 0/1	SW_1	Gig 0/1
R_2	Gig 0/1	SW_2	Gig 0/1
SW_1	Gig 0/1	R_1	Gig 0/1
	Gig 0/2	SW_3	Gig 0/1
	Fa 0/1	SW_4	Fa 0/1
	Fa 0/2	SW_5	Fa 0/1
	Fa 0/3	SW_6	Fa 0/1
	Fa 0/4	SW_7	Fa 0/1
	Fa 0/5	SW_8	Fa 0/1
SW_2	Gig 0/1	R_2	Gig 0/1
	Gig 0/2	SW_3	Gig 0/2
	Fa 0/1	SW_4	Fa 0/2
	Fa 0/2	SW_5	Fa 0/2
	Fa 0/3	SW_6	Fa 0/2
	Fa 0/4	SW_7	Fa 0/2
	Fa 0/5	SW_8	Fa 0/2
SW_3	Gig 0/1	SW_1	Gig 0/2
	Gig 0/2	SW_2	Gig 0/2
	Fa 0/1	PC_1	Fa 0
	Fa 0/2	DNS	Fa 0
	Fa 0/3	DHCP	Fa 0
	Fa 0/4	HTTPS	Fa 0
SW_4	Fa 0/1	SW_1	Fa 0/1
	Fa 0/2	SW_2	Fa 0/1
	Fa 0/3	PC_2	Fa 0
	Fa 0/4	AP_Free_Wi-Fi_1	Port 0
	Fa 0/5	Printer_1	Fa 0
SW_5	Fa 0/1	SW_1	Fa 0/2
	Fa 0/2	SW_2	Fa 0/2
	Fa 0/3	PC_3	Fa 0
	Fa 0/4	PC_4	Fa 0
	Fa 0/5	PC_5	Fa 0
	Fa 0/7	AP_Free_Wi-Fi_2	Port 0
SW_6	Fa 0/1	SW_1	Fa 0/3
	Fa 0/2	SW_2	Fa 0/3
	Fa 0/3	PC_6	Fa 0
	Fa 0/4	Printer_2	Fa 0
SW_7	Fa 0/1	SW_1	Fa 0/4
	Fa 0/2	SW_2	Fa 0/4
	Fa 0/3	PC_7	Fa 0
	Fa 0/4	PC_8	Fa 0
	Fa 0/5	PC_9	Fa 0
	Fa 0/6	Printer_3	Fa 0
	Fa 0/7	AP_Free_Wi-Fi_3	Port 0
SW_8	Fa 0/1	SW_1	Fa 0/5
	Fa 0/2	SW_2	Fa 0/5
	Fa 0/3	PC_10	Fa 0
	Fa 0/4	PC_11	Fa 0
	Fa 0/5	PC_12	Fa 0
	Fa 0/7	AP_Free_Wi-Fi_4	Port 0

Продовження таблиці

AP_Free_Wi-Fi_1	Port 0	SW_4	Fa 0/4
	Port 1	SP_1	Wireless0
	Port 1	Laptop_1	Wireless0
AP_Free_Wi-Fi_2	Port 0	SW_5	Fa 0/7
	Port 1	Laptop_2	Wireless0
	Port 1	Laptop_3	Wireless0
	Port 1	SP_2	Wireless0
AP_Free_Wi-Fi_3	Port 0	SW_7	Fa 0/7
	Port 1	Laptop_4	Wireless0
	Port 1	Laptop_5	Wireless0
	Port 1	Laptop_6	Wireless0
AP_Free_Wi-Fi_4	Port 0	SW_8	Fa 0/7
	Port 1	Laptop_7	Wireless0
	Port 1	Laptop_8	Wireless0
	Port 1	Laptop_9	Wireless0
	Port 1	SP_3	Wireless0
	Port 1	SP_4	Wireless0
SP_1	Wireless0	AP_Free_Wi-Fi_1	Port 1
SP_2	Wireless0	AP_Free_Wi-Fi_2	Port 1
SP_3	Wireless0	AP_Free_Wi-Fi_4	Port 1
SP_4	Wireless0		Port 1
Laptop_1	Wireless0	AP_Free_Wi-Fi_1	Port 1
Laptop_2	Wireless0	AP_Free_Wi-Fi_2	Port 1
Laptop_3	Wireless0		Port 1
Laptop_4	Wireless0		Port 1
Laptop_5	Wireless0	AP_Free_Wi-Fi_3	Port 1
Laptop_6	Wireless0		Port 1
Laptop_7	Wireless0		Port 1
Laptop_8	Wireless0	AP_Free_Wi-Fi_4	Port 1
Laptop_9	Wireless0		Port 1
DNS	Fa 0	SW_3	Fa 0/2
DHCP	Fa 0		Fa 0/3
HTTPS	Fa 0		Fa 0/4
Printer_1	Fa 0	SW_4	Fa 0/5
Printer_2	Fa 0	SW_6	Fa 0/4
Printer_3	Fa 0	SW_7	Fa 0/6
PC_1	Fa 0	SW_3	Fa 0/1
PC_2	Fa 0	SW_4	Fa 0/3
PC_3	Fa 0	SW_5	Fa 0/3
PC_4	Fa 0		Fa 0/4
PC_5	Fa 0		Fa 0/5
PC_6	Fa 0	SW_6	Fa 0/3
PC_7	Fa 0	SW_7	Fa 0/3
PC_8	Fa 0		Fa 0/4
PC_9	Fa 0		Fa 0/5
PC_10	Fa 0	SW_8	Fa 0/3
PC_11	Fa 0		Fa 0/4
PC_12	Fa 0		Fa 0/5

Таблиця розподілу IP адрес кампусної мережі

Мережа / Пристрій	Інтерфейс/ Мережний адаптер/Шлюз	IP-адреса	Маска	Префікс	IPv6-адреса
MGMT VLAN	-	192.168.100.0	255.255.255.0	/24	2001:100::/64
SERVER VLAN	-	192.168.10.0	255.255.255.0	/24	2001:10::/64
TEACHER VLAN	-	192.168.20.0	255.255.255.0	/24	2001:20::/64
VLAN CLASS 1 AND 2	-	192.168.30.0	255.255.255.0	/24	2001:30::/64
DEAN OF THE FAC- ULTY VLAN	-	192.168.40.0	255.255.255.0	/24	2001:40::/64
DEAN'S OFFICE VLAN	-	192.168.50.0	255.255.255.0	/24	2001:50::/64
VLAN FREE Wi-Fi	-	192.168.60.0	255.255.255.0	/24	2001:60::/64
Маршрутизатор R_1	Інтерфейс Gig0/0	-	-	-	-
	Підінтерфейс Gig0/1.100	192.168.100.1	255.255.255.0	/24	2001:100::1/64
	Підінтерфейс Gig0/1.10	192.168.10.1	255.255.255.0	/24	2001:10::1/64
	Підінтерфейс Gig0/1.20	192.168.20.1	255.255.255.0	/24	2001:20::1/64
	Підінтерфейс Gig0/1.30	192.168.30.1	255.255.255.0	/24	2001:30::1/64
	Підінтерфейс Gig0/1.40	192.168.40.1	255.255.255.0	/24	2001:40::1/64
	Підінтерфейс Gig0/1.50	192.168.50.1	255.255.255.0	/24	2001:50::1/64
	Підінтерфейс Gig0/1.60	192.168.60.1	255.255.255.0	/24	2001:60::1/64
Маршрутизатор R_2	Інтерфейс Gig0/0	-	-	-	-
	Підінтерфейс Gig0/1.100	192.168.100.2	255.255.255.0	/24	2001:100::2/64
	Підінтерфейс Gig0/1.10	192.168.10.2	255.255.255.0	/24	2001:10::2/64
	Підінтерфейс Gig0/1.20	192.168.20.2	255.255.255.0	/24	2001:20::2/64
	Підінтерфейс Gig0/1.30	192.168.30.2	255.255.255.0	/24	2001:30::2/64
	Підінтерфейс Gig0/1.40	192.168.40.2	255.255.255.0	/24	2001:40::2/64
	Підінтерфейс Gig0/1.50	192.168.50.2	255.255.255.0	/24	2001:50::2/64
	Підінтерфейс Gig0/1.60	192.168.60.2	255.255.255.0	/24	2001:60::2/64
MGMT VLAN – VLAN 100					
Комутатор SW_1	Мережний адаптер	192.168.100.3	255.255.255.0	/24	2001:100::3/64
	Шлюз за замовчуванням	192.168.100.1	-	-	2001:100::1
Комутатор SW_2	Мережний адаптер	192.168.100.4	255.255.255.0	/24	2001:100::4/64
	Шлюз за замовчуванням	192.168.100.1	-	-	2001:100::1
Комутатор SW_3	Мережний адаптер	192.168.100.5	255.255.255.0	/24	2001:100::5/64
	Шлюз за замовчуванням	192.168.100.1	-	-	2001:100::1
Комутатор SW_4	Мережний адаптер	192.168.100.6	255.255.255.0	/24	2001:100::6/64
	Шлюз за замовчуванням	192.168.100.1	-	-	2001:100::1
Комутатор SW_5	Мережний адаптер	192.168.100.7	255.255.255.0	/24	2001:100::7/64
	Шлюз за замовчуванням	192.168.100.1	-	-	2001:100::1
Комутатор SW_6	Мережний адаптер	192.168.100.8	255.255.255.0	/24	2001:100::8/64
	Шлюз за замовчуванням	192.168.100.1	-	-	2001:100::1
Комутатор SW_7	Мережний адаптер	192.168.100.9	255.255.255.0	/24	2001:100::9/64
	Шлюз за замовчуванням	192.168.100.1	-	-	2001:100::1
Комутатор SW_8	Мережний адаптер	192.168.100.10	255.255.255.0	/24	2001:100::10/64
	Шлюз за замовчуванням	192.168.100.1	-	-	2001:100::1
PC – 1	Мережний адаптер	192.168.100.11	255.255.255.0	/24	2001:100::11/64
	Шлюз за замовчуванням	192.168.100.1	-	-	2001:100::1
MGMT VLAN – VLAN 10					
Server DNS	Мережний адаптер	192.168.10.3	255.255.255.0	/24	2001:10::3/64
	Шлюз за замовчуванням	192.168.10.1	-	-	2001:10::1
Server DHCP	Мережний адаптер	192.168.10.4	255.255.255.0	/24	2001:10::4/64
	Шлюз за замовчуванням	192.168.10.1	-	-	2001:10::1

Продовження таблиці

Server HTTPS	Мережний адаптер	192.168.10.5	255.255.255.0	/24	2001:10::5/64
	Шлюз за замовчуванням	192.168.10.1	-	-	2001:10::1
TEACHER VLAN – VLAN 20					
Printer 1	Мережний адаптер	192.168.20.3	255.255.255.0	/24	2001:20::2/64
	Шлюз за замовчуванням	192.168.10.1	-	-	2001:10::1
PC_1 та інші вузли данного приміщення	DHCP				DHCPv6
VLAN CLASS 1 AND 2 – VLAN 30					
PC_3 – PC_5	DHCP				DHCPv6
PC_10 – PC_12					
Всі інші вузли даних приміщень					
DEAN OF THE FACULTY VLAN – VLAN 40					
Printer 2	Мережний адаптер	192.168.40.3	255.255.255.0	/24	2001:40::4/64
	Шлюз за замовчуванням	192.168.40.1	-	-	2001:40::1
PC_6 та інші вузли данного приміщення	DHCP				DHCPv6
DEAN’S OFFICE VLAN – VLAN 50					
Printer 3	Мережний адаптер	192.168.50.3	255.255.255.0	/24	2001:40::5/64
	Шлюз за замовчуванням	192.168.50.1	-	-	2001:50::1
Всі інші вузли данного приміщення	DHCP				DHCPv6
VLAN_FREE_Wi-Fi – VLAN 60					
AP Free 1	Мережний адаптер	192.168.60.3	255.255.255.0	/24	2001:60::2/64
	Шлюз за замовчуванням	192.168.60.1	-	-	2001:60::1
AP Free 2	Мережний адаптер	192.168.60.4	255.255.255.0	/24	2001:60::3/64
	Шлюз за замовчуванням	192.168.60.1	-	-	2001:60::1
AP Free 3	Мережний адаптер	192.168.60.5	255.255.255.0	/24	2001:60::4/64
	Шлюз за замовчуванням	192.168.60.1	-	-	2001:60::1
AP Free 4	Мережний адаптер	192.168.60.6	255.255.255.0	/24	2001:60::4/64
	Шлюз за замовчуванням	192.168.60.1	-	-	2001:60::1
Всі інші абоненти Wi-Fi	DHCP				DHCPv6

Конфігураційний файл R_1

```

R_1#show running-config
Building configuration...
Current configuration : 3682
bytes
version 15.1
no service timestamps log
datetime msec
no service timestamps debug
datetime msec
no service password-encryption
hostname R_1
ip dhcp excluded-address
192.168.20.1 192.168.20.2
ip dhcp excluded-address
192.168.60.1 192.168.60.2
ip dhcp excluded-address
192.168.40.1 192.168.40.2
ip dhcp excluded-address
192.168.30.1 192.168.30.2
ip dhcp excluded-address
192.168.50.1 192.168.50.2
ip dhcp pool
TEACHER_VLAN_20
network 192.168.20.0
255.255.255.0
default-router 192.168.20.1
dns-server 192.168.10.3
ip dhcp pool FREE_Wi-
Fi_VLAN_60
network 192.168.60.0
255.255.255.0
default-router 192.168.60.1
dns-server 192.168.10.3
ip dhcp pool
DEAN_OF_THE_FACULTY_V
LAN_40
network 192.168.40.0
255.255.255.0
default-router 192.168.40.1
dns-server 192.168.10.3
ip dhcp pool CLASS_VLAN_30
network 192.168.30.0
255.255.255.0
default-router 192.168.30.1
dns-server 192.168.10.3
ip dhcp pool
DEANS_OFFICE_VLAN_50
network 192.168.50.0
255.255.255.0
default-router 192.168.50.1
dns-server 192.168.10.3
ip cef
ipv6 unicast-routing
no ipv6 cef
ipv6 dhcp pool
DEAN_OF_THE_FACULTY_V
LAN_40_v6
address prefix 2001:40::/64
lifetime 172800 86400
dns-server 2001:10::3
ipv6 dhcp pool
FREE_Wi-
Fi_VLAN_60_v6
address prefix 2001:60::/64
lifetime 172800 86400
dns-server 2001:10::3
ipv6 dhcp pool
TEACHER_VLAN_20_v6
address prefix 2001:20::/64
lifetime 172800 86400
dns-server 2001:10::3
ipv6 dhcp pool
CLASS_VLAN_30_v6
address prefix 2001:30::/64
lifetime 172800 86400
dns-server 2001:10::3
username admin privilege 15
secret 5
$1$mERr$vTbHul1N28cEp8lkLq
r0f/
!license udi pid CISCO2911/K9
sn FTX1524V049-
ip ssh version 2
ip domain-name
FACULTY.COM
spanning-tree mode pvst
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
ipv6 dhcp server
TEACHER_VLAN_20_v6
interface GigabitEthernet0/1.2
no ip address
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 192.168.10.1
255.255.255.0
ipv6 address 2001:10::1/64
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 192.168.20.1
255.255.255.0
ipv6 address 2001:20::1/64
ipv6 dhcp server
TEACHER_VLAN_20_v6
interface GigabitEthernet0/1.30
encapsulation dot1Q 30
ip address 192.168.30.1
255.255.255.0
ipv6 address 2001:30::1/64
ipv6 dhcp server
CLASS_VLAN_30_v6
interface GigabitEthernet0/1.40
encapsulation dot1Q 40
ip address 192.168.40.1
255.255.255.0
ipv6 address 2001:40::1/64
ipv6 dhcp server
DEAN_OF_THE_FACULTY_V
LAN_40_v6
interface GigabitEthernet0/1.50
encapsulation dot1Q 50
ip address 192.168.50.1
255.255.255.0
ipv6 address 2001:50::1/64
ipv6 dhcp server
DEANS_OFFICE_VLAN_50_v6
interface GigabitEthernet0/1.60
encapsulation dot1Q 60
ip address 192.168.60.1
255.255.255.0
ipv6 address 2001:60::1/64
ipv6 dhcp server FREE_Wi-
Fi_VLAN_60_v6
interface GigabitEthernet0/1.100
encapsulation dot1Q 100
ip address 192.168.100.100
255.255.255.0
ipv6 address 2001:100::1/64
standby 100 ip 192.168.100.1
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
interface Vlan1
no ip address
shutdown
interface Vlan30
mac-address 0001.976d.0001
no ip address
ip access-group 130 in
ip classless
ip flow-export version 9
access-list 130 deny ip
192.168.30.0 0.0.0.255
192.168.100.0 0.0.0.255
banner motd ^CAuthorized
Access Only!^C
line con 0
line aux 0
line vty 0 4
login local
transport input ssh
transport output ssh
end

```

Конфігураційний файл SW_1 рівня ядра

```

SW_1#show running-config
Building configuration...

Current configuration :
2135 bytes
!
version 15.0
no service timestamps log
datetime msec
no service timestamps
debug datetime msec
no service password-
encryption
!
hostname SW_1
ip ssh version 2
ip domain-name
FACULTY.COM
!
username admin secret 5
$1$mERr$VtBHul1N28cEp
8lkLqr0f/
spanning-tree mode rapid-
pvst
spanning-tree portfast
default
spanning-tree portfast
bpduguard default
spanning-tree extend
system-id
spanning-tree vlan
1,10,20,30,40,50,60,100
priority 24576
spanning-tree vlan 400
priority 28672
!
interface FastEthernet0/1
switchport mode trunk
switchport nonegotiate
spanning-tree portfast
disable
!
interface FastEthernet0/2
switchport mode trunk
switchport nonegotiate
spanning-tree portfast
disable
!
interface FastEthernet0/3
switchport mode trunk
switchport nonegotiate
spanning-tree portfast
disable
!
interface FastEthernet0/4
switchport mode trunk
switchport nonegotiate
spanning-tree portfast
disable
!
interface FastEthernet0/5
switchport mode trunk
switchport nonegotiate
spanning-tree portfast
disable
!
interface FastEthernet0/6
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
switchport mode trunk
switchport nonegotiate
spanning-tree portfast
disable
interface GigabitEthernet0/2
switchport mode trunk
switchport nonegotiate
spanning-tree portfast
disable
!
interface Vlan1
no ip address
shutdown
!
interface Vlan100
ip address 192.168.100.3
255.255.255.0
!
ip default-gateway
192.168.100.1
!
banner motd ^CAuthorized
Access Only!^C
!
!
!
line con 0
!
line vty 0 4
login local
transport input ssh
transport output ssh
line vty 5 15
login
end

```

Конфігураційний файл SW_3 рівня розподілу

```

SW_3#show running-config
Building configuration...

Current configuration :
1876 bytes
!
version 15.0
no service timestamps log
datetime msec
no service timestamps
debug datetime msec
no service password-
encryption
!
hostname SW_3
!
!
!
ip ssh version 2
ip domain-name
FACULTY.COM
!
username admin secret 5
$1$mERr$VtBHul1N28cEp
8lkLqr0f/
!
!
!
spanning-tree mode rapid-
pvst
spanning-tree portfast
default
spanning-tree portfast
bpduguard default
spanning-tree extend
system-id
spanning-tree vlan 1-100
priority 28672
!
interface FastEthernet0/1
switchport access vlan 100
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
!
interface GigabitEthernet0/1
switchport mode trunk
switchport nonegotiate
spanning-tree portfast
disable
!
interface GigabitEthernet0/2
switchport mode trunk
switchport nonegotiate
spanning-tree portfast
disable
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
no ip address
!
interface Vlan100
ip address 192.168.100.5
255.255.255.0
!
ip default-gateway
192.168.100.1
!
banner motd ^CAuthorized
Access Only!^C
!
!
line con 0
!
line vty 0 4
login local
transport input ssh
transport output ssh
line vty 5 15
login
!
!
!
!
end

```