Міністерство освіти і науки України
Національний університет «Львівська політехніка»

Пояснювальна записка до курсової роботи
«Розробка корпоративної мережі»
з дисципліни «Технології та протоколи інформаційних систем»

Виконав:
ст. гр. ІК-21
Бухарінов М.С

Прийняв:
доцент каф ТК
Красько О. В.

Львів 2024

ЗАВДАННЯ НА КУРСОВУ РОБОТУ

Створити кампусну мережу з використанням Wi-Fi. Радіус покриття Wi-Fi 600m. Передбачити стаціонарну мережу на 100 клієнтів та дві Wi-Fi мережі. Для мобільних користувачів 90 підключень та для гостьової 25 підключень. Керування точками доступу використати WLC-контролер. Для виходу в Інтернет передбачити резервний канал. Для виходу в Інтернет передбачити трансляцію адрес (PAT). Заборонити з гостьової мережі доступ до ресурсів кампусної мережі.

ЗМІСТ

ВСТУП

У даній курсовій роботі поставлено завдання розробити кампусну мережу з використанням технологій бездротового підключення WI-FI. Мета роботи полягає у створенні надійної і безпечної мережі, яка забезпечить стабільне підключення до Інтернету та доступ до внутрішніх ресурсів для різних категорій користувачів.

Завдання передбачає створення мережевої інфраструктури, яка складається зі стаціонарної мережі на 100 клієнтів та двох Wi-Fi мереж. Перша Wi-Fi мережа призначена для мобільних користувачів і має забезпечувати підключення для 90 пристроїв, друга – для гостьових користувачів з обмеженням у 25 підключень. Для управління точками доступу використовуватиметься WLC-контролер (Wireless LAN Controller), який забезпечує централізоване керування всіма точками доступу, підвищуючи ефективність та безпеку мережі.

Вибір технології Wi-Fi для реалізації даної мережі обумовлений її численними перевагами. По-перше, бездротові мережі дозволяють забезпечити мобільність користувачів, що є одним з найважливіших факторів у розробці сучасних мереж. По-друге, Wi-Fi мережі дозволяють знизити витрати на прокладання кабельної інфраструктури, що є особливо актуальним при розширенні або модернізації вже існуючих кампусів з точки зору доцільного використання ресурсів та економії коштів

Для реалізації поставленого завдання будуть використані наступні технології та обладнання:

Wi-Fi (802.11ax): Це новітній стандарт Wi-Fi, який забезпечує високу швидкість передачі даних, велику пропускну здатність і низьку затримку. Він ідеально підходить для середовищ з великою щільністю користувачів, де одночасно підключена велика кількість пристроїв.

WLC-контролер (Wireless LAN Controller): Використання WLC дозволить централізовано керувати всіма точками доступу, спрощуючи адміністрування мережі, забезпечуючи високий рівень безпеки та оптимізацію

радіочастотного спектру. Це знижує навантаження на IT-персонал і підвищує стабільність мережі.

Резервний канал виходу в Інтернет: Для забезпечення надійності мережі буде використано два канали виходу в Інтернет від різних провайдерів. Це дозволить автоматично перемикатися на резервний канал у разі збоїв основного, забезпечуючи безперервний доступ до мережі.

PAT (Port Address Translation): Ця технологія дозволяє використовувати один публічний IP-адрес для виходу в Інтернет всіх внутрішніх клієнтів, приховуючи при цьому внутрішню IP-структуру мережі. Це підвищує рівень безпеки, запобігаючи зовнішнім атакам на внутрішні ресурси мережі.

Віртуальні локальні мережі (VLAN): Для сегментації мережі будуть використовуватися VLAN, що дозволить розділити трафік гостьових користувачів від основних користувачів. Це забезпечить додатковий рівень безпеки та підвищить продуктивність мережі за рахунок зменшення широкомовних доменів.

Щоб забезпечити безпеку та розділення доступу до ресурсів, гостьова мережа буде ізольована від основної кампусної мережі. Це дозволить захистити важливі дані та ресурси університету від потенційно небезпечних пристроїв, підключених до гостьової мережі. Гостьова мережа матиме обмежений доступ до Інтернету, без можливості взаємодії з внутрішніми сервісами кампусу.

Таким чином, проект передбачає створення комплексної мережевої інфраструктури, яка відповідає сучасним вимогам безпеки, надійності та ефективності. Використання передових технологій Wi-Fi, централізоване управління точками доступу через WLC, резервний вихід в Інтернет та сегментація мережі сприятимуть створенню стабільної, безпечної та зручної у використанні мережі.

1. ТЕОРЕТИЧНА ЧАСТИНА

1.1 Топологія мережі

На рис. 1 представлена топологія кампусної мережі з використанням Wi-Fi. Мережа складається з декількох сегментів, включаючи стаціонарну мережу для внутрішніх користувачів, дві окремі Wi-Fi мережі для мобільних і гостьових користувачів, а також інтернет-з'єднання з резервним каналом. Основні компоненти мережі включають маршрутизатор, комутатори, контролер бездротових мереж (WLC), точки доступу (LAP) і кінцеві пристрої (смартфони та ПК).

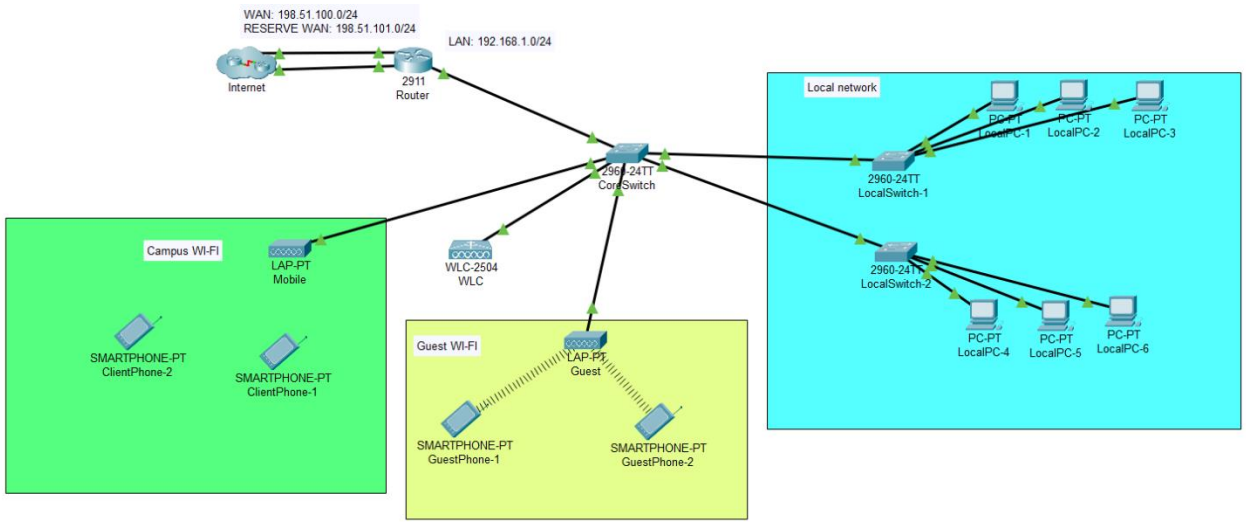


Рис. 1.1. Топологія мережі

1.2 Компоненти мережі та їх функції

1. Маршрутизатор 2911 (Router):

Забезпечує підключення до Інтернету через WAN-порт (198.51.100.0/24).

Виконує трансляцію мережевих адрес (PAT) для забезпечення виходу в Інтернет для всіх пристроїв локальної мережі.

Маршрутизація трафіку між різними сегментами мережі (LAN, Campus Wi-Fi, Guest Wi-Fi).

Забезпечення резервного каналу для підвищення надійності підключення до Інтернету.

2. Комутатор 2960-24TT (Core Switch):

Об'єднує маршрутизатор, контролер WLC та комутатор локальної мережі.

Забезпечує високу швидкість передачі даних між основними компонентами мережі.

3. Комутатор 2960-24T (Local Switch 1):

Підключає стаціонарні комп'ютери (PC-PT) до мережі.

Забезпечує комунікацію між стаціонарними комп'ютерами.

4. Контролер WLC-2504 (WLC):

Централізоване керування точками доступу Wi-Fi (LAP-PT).

Налаштування параметрів безпеки Wi-Fi мереж (Campus Wi-Fi та Guest Wi-Fi).

Моніторинг стану точок доступу та клієнтів Wi-Fi.

Забезпечення роумінгу між точками доступу для безперервного підключення.

5. Точки доступу LAP-PT (LAP-PT):

Створення двох бездротових мереж:

Campus Wi-Fi (радіус покриття 600м, 90 підключень).

Guest Wi-Fi (радіус покриття 600м, 25 підключень).

Забезпечення бездротового підключення для мобільних пристроїв.

6. Стаціонарні комп'ютери (PC-PT):

Клієнти локальної мережі, що підключаються до комутатора Local Switch 1.

7. Мобільні пристрої (SMARTPHONE-PT, ClientPhone):

Клієнти мережі Campus Wi-Fi.

8. Гостьові пристрої (SMARTPHONE-PT GuestPhone):

Клієнти мережі Guest Wi-Fi.

1.3 Огляд основних протоколів та технологій

1.3.1 PAT(Port Address Translation)

Опис протоколу:

PAT (Port Address Translation), також відомий як Network Address Port Translation (NAPT), є різновидом технології NAT (Network Address Translation). PAT дозволяє багатьом пристроям у локальній мережі використовувати одну загальну IP-адресу для виходу в Інтернет, при цьому зберігаючи унікальність кожного з'єднання через використання різних номерів портів.

Принцип роботи:

Вихідний трафік: Коли внутрішній пристрій (з приватною IP-адресою) надсилає запит в Інтернет, маршрутизатор змінює вихідну IP-адресу на свою загальну (публічну) IP-адресу, змінюючи при цьому номер порту.

Таблиця трансляції: Маршрутизатор створює запис у таблиці трансляції, який пов'язує приватну IP-адресу і порт пристрою з публічною IP-адресою і новим портом.

Вхідний трафік: Коли відповідь надходить з Інтернету, маршрутизатор використовує таблицю трансляції, щоб змінити публічну IP-адресу та порт назад на приватну IP-адресу і порт внутрішнього пристрою.

Причини для використання у проекті:

Економія IP-адрес: Оскільки кількість публічних IP-адрес обмежена, PAT дозволяє великій кількості пристроїв використовувати одну публічну IP-адресу, що знижує потребу у великій кількості публічних IP-адрес.

Безпека: Внутрішні IP-адреси залишаються прихованими від зовнішнього світу, що забезпечує додатковий рівень захисту від зовнішніх атак.

Масштабованість: PAT дозволяє легко масштабувати мережу без необхідності купувати нові публічні IP-адреси.

1.3.2 DHCP (Dynamic Host Configuration Protocol)

Опис протоколу:

DHCP (Dynamic Host Configuration Protocol) є мережевим протоколом, який використовується для автоматичного присвоєння IP-адрес та інших мережевих параметрів пристроям у мережі. DHCP знижує потребу у ручній конфігурації мережевих параметрів для кожного пристрою.

Принцип роботи:

DHCP Discover: Коли новий пристрій підключається до мережі, він надсилає широкомовний запит (DHCP Discover), шукаючи DHCP-сервер.

DHCP Offer: DHCP-сервер відповідає на запит, пропонуючи IP-адресу та інші мережеві параметри (маска підмережі, шлюз за замовчуванням, DNS-сервери).

DHCP Request: Пристрій відповідає, приймаючи запропоновані параметри (DHCP Request).

DHCP Acknowledgment: DHCP-сервер підтверджує, що параметри були присвоєні (DHCP Acknowledgment), і пристрій починає використовувати отримані параметри.

Причини для використання у проекті:

Автоматизація конфігурації: DHCP автоматично присвоює IP-адреси та мережеві параметри новим пристроям, що знижує потребу у ручній конфігурації та можливі помилки.

Легкість адміністрування: Адміністратори можуть легко керувати і змінювати мережеві параметри через центральний DHCP-сервер, спрощуючи управління великою кількістю пристроїв.

Гнучкість: Пристрої можуть легко переміщуватися між підмережами без необхідності ручного переналаштування мережевих параметрів.

1.3.3 ACL (Access Control List)

ACL – це набір правил, які визначають, який мережевий трафік дозволено або заборонено пропускати через інтерфейс маршрутизатора. ACL діють як фільтр, дозволяючи вам контролювати, які пакети даних можуть входити або виходити з вашої мережі.

Типи ACL:

Стандартні ACL: Фільтрують трафік на основі IP-адреси джерела.

Розширені ACL: Фільтрують трафік на основі IP-адреси джерела, IP-адреси призначення, типу протоколу (TCP, UDP, ICMP тощо) та номерів портів.

Як працюють ACL?

Створення ACL: Ви створюєте ACL, визначаючи правила, які вказують, який трафік дозволено або заборонено.

Застосування ACL: Ви застосовуєте ACL до інтерфейсу маршрутизатора (вхідного або вихідного).

Фільтрація трафіку: Маршрутизатор перевіряє кожен пакет даних, що проходить через інтерфейс, на відповідність правилам ACL. Якщо пакет відповідає правилу "дозволити", він пропускається. Якщо пакет відповідає правилу "заборонити" або не відповідає жодному правилу, він відкидається.

2. РЕАЛІЗАЦІЯ ЗАВДАННЯ

2.1 Таблиці адресації

Таблиця 2.1

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
Router	G0/1	192.168.1.1	255.255.255.0	N/A
	G0/2	198.51.101.2	255.255.255.0	
	G0/0	198.51.100.2	255.255.255.0	
WLC	Management	192.168.1.10	255.255.255.0	192.168.1.1
LocalPC	F0/0	DHCP	255.255.255.0	192.168.1.1
ClientPhone	WI-FI	DHCP	255.255.255.0	192.168.1.1
GuestPhone	WI-FI	DHCP	255.255.255.0	192.168.1.1
CoreSwitch	VLAN	N/A	255.255.255.0	192.168.1.1
LocalSwitch	VLAN	N/A	255.255.255.0	192.168.1.1
Internet	G0/0	198.51.100.1	255.255.255.0	N/A

Таблиця 2.2

Таблиця VLAN

VLAN	Назва	Інтерфейс
10	Local	CoreSwitch: F0/1 - 7
20	Mobile	CoreSwitch: F0/24
30	Guest	CoreSwitch: F0/22
999	ParkingLot	CoreSwitch: F0/8 - 21
1000	Native	N/A

2.2 Налаштування пристроїв

2.2.1 Конфігурація маршрутизатора

Враховуючи поставлене завдання, необхідно налаштувати маршрутизатор таким чином, щоб він відповідав всім вказаним критеріям, а саме:

1. Виконував маршрутизацію в локальній мережі через LAN-порт (G0/1)

2. Мав доступ до Інтернету через WAN-порт (G0/0) та резервний порт G0/2

3. Підтримував протокол трансляції адрес PAT для надання послуг підключення до інтернету кінцевим пристроям в локальній мережі

4. Блокував доступ з гостьової мережі до кампусної мережі за допомогою технології ACL (Access Contol List)

5. Підтримував протокол DHCP (Dynamic Host Configuration Protocol) для автоматичної конфігурації кінцевих пристроїв

Враховуючи зазначені критерії, виконавши команду для показу конфігурації show running-config маємо такі налаштування маршрутизатора:

```
Current configuration : 1224 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp pool LAN-POOL
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX15246E6P-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 198.51.100.2 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
```

```
 ip helper-address 192.168.1.1
 ip nat inside
 duplex auto
 speed auto
 standby 0 ip 192.168.1.1
 standby preempt
interface GigabitEthernet0/2
 ip address 198.51.101.2 255.255.255.0
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip nat inside source list NAT-ACL interface GigabitEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.10.1
ip route 0.0.0.0 0.0.0.0 10.10.10.5 10
ip flow-export version 9
ip access-list extended NAT-ACL
 permit ip 192.168.1.0 0.0.0.255 any
line con 0
line aux 0
line vty 0 4
 login
end
```

2.2.2 Конфігурація комутатора

Згідно з поставленою задачою необхідно налаштувати на комутаторі VLAN та присвоїти їх інтерфейсам з метою використання їх для розподілу трафіку в мережі та блокування доступу з гостьової мережі до кампусної. Деталі

налаштування VLAN зображені у таблиці 2.2. Команди, які необхідно виконати у середовищі Cisco CLI на комутаторі CoreSwitch:

1. Створення VLAN:

```
vlan 10
name Local
vlan 20
name Mobile
vlan 30
name Guest
vlan 999
name ParkingLot
vlan 1000
name Native
```

2. Призначення інтерфейсів до VLAN (режим access):

```
interface range FastEthernet0/1 - 7
switchport mode access
switchport access vlan 10
interface FastEthernet0/24
switchport mode access
switchport access vlan 20
interface FastEthernet0/22
switchport mode access
switchport access vlan 30
interface range FastEthernet0/8 - 21
switchport mode access
switchport access vlan 999
```

2.2.3 Конфігурація WLC-контролера та точок доступу

Для налаштування WLC-контролера необхідно скористатись графічним інтерфейсом, попередньо підключившись до його management порту через браузер на одному з кінцевих пристроїв у мережі.

1. Необхідно налаштувати дві WLAN мережі: Mobile та Guest (рис 2.1)

Рис. 2.1. Налаштування WLAN на WLC-контролері

2. Необхідно переконатися що обидві точки доступу мають підключення CAPWAP до WLC-контролера (рис 2.2)

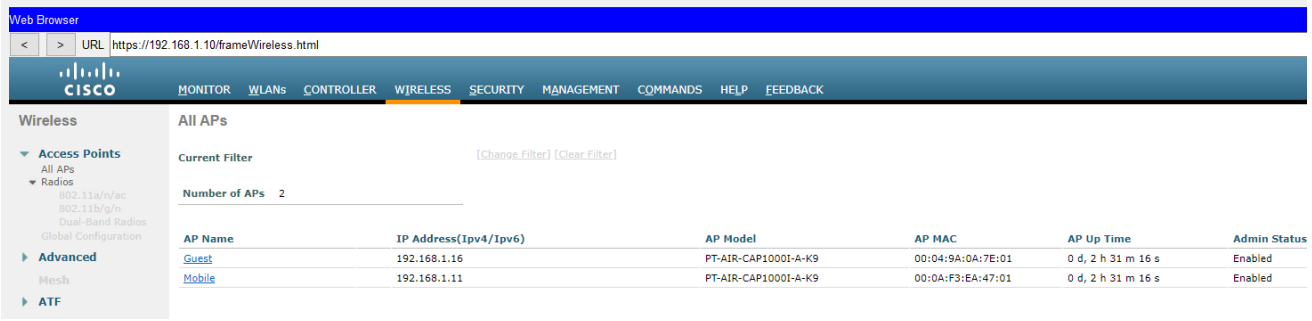


Рис. 2.2. Підключення точок доступу до WLC-контролера

3. Необхідно налаштувати дві AP-групи для присвоєння точкам доступу певних WLAN (рис 2.3)

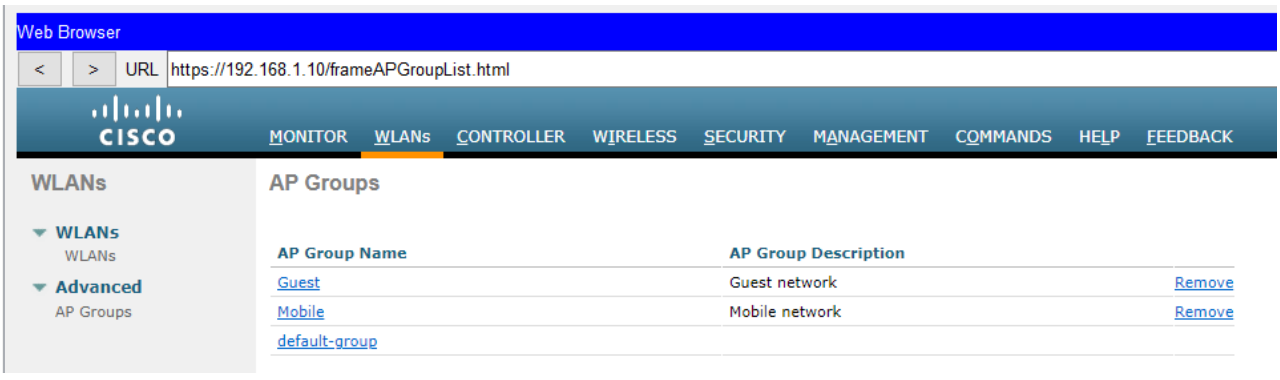


Рис. 2.3. Налаштування AP Groups на WLC-контролері

ВИСНОВКИ

У курсовому проєкті було успішно розроблено, охарактеризовано, запропоновано та реалізовано кампусну мережу з використанням технології Wi-Fi.

Розроблено:

1. Архітектуру кампусної мережі: Створено детальний план мережі, що включає стаціонарну мережу на 100 клієнтів, дві Wi-Fi мережі (90 підключень для мобільних користувачів та 25 підключень для гостей), WLC-контролер для управління точками доступу, резервний канал для виходу в Інтернет та механізм трансляції адрес (PAT).

2. План розміщення точок доступу: Визначено оптимальне розташування точок доступу Wi-Fi для забезпечення радіусу покриття 600 метрів та якісного сигналу по всій території кампусу.

3. Конфігурацію WLC-контролера: Налаштувано WLC-контролер для централізованого управління точками доступу, забезпечення безпеки та моніторингу роботи Wi-Fi мережі.

4. Конфігурацію мережевого обладнання: Налаштовано маршрутизатори, комутатори та точки доступу Wi-Fi для забезпечення роботи стаціонарної та бездротових мереж.

5. Механізм трансляції адрес (PAT): Впроваджено технології PAT для ефективного використання публічних IP-адрес та забезпечення виходу в Інтернет для всіх користувачів кампусної мережі.

6. Політики безпеки: Розроблено та впроваджено політики безпеки, включаючи заборону доступу з гостьової мережі до ресурсів кампусної мережі, налаштування шифрування трафіку та інші заходи для захисту мережі від несанкціонованого доступу.

Охарактеризовано:

1. Технології Wi-Fi: Проаналізовано переваги та недоліки різних технологій Wi-Fi, включаючи Wi-Fi 5 та Wi-Fi 6, та обґрунтовано вибір Wi-Fi для побудови кампусної мережі.

2. WLC-контролери: Досліджено функціональність та можливості WLC-контролерів різних виробників та обрано оптимальний варіант для даного проекту.

3. Мережеве обладнання: Проведено порівняльний аналіз мережевого обладнання різних виробників та вибрано оптимальні моделі маршрутизаторів, комутаторів та точок доступу Wi-Fi.

Запропоновано:

1. Оптимізацію розміщення точок доступу: Запропоновано варіанти покращення покриття Wi-Fi в окремих зонах кампусу шляхом встановлення додаткових точок доступу або зміни їх розташування.

2. Впровадження нових сервісів: Розглянуто можливість впровадження додаткових сервісів, таких як гостьовий портал, система моніторингу стану мережі та інші, для підвищення якості обслуговування користувачів та ефективності управління мережею.

Реалізовано:

1. Функціонуючу кампусну мережу: Успішно створено та налаштовано кампусну мережу, що відповідає всім вимогам завдання та забезпечує надійний та безпечний доступ до мережевих ресурсів для всіх користувачів.

2. Можливість масштабування: Забезпечено можливість розширення мережі в майбутньому шляхом додавання нових точок доступу, підключення додаткових користувачів та впровадження нових сервісів.

Загальний висновок:

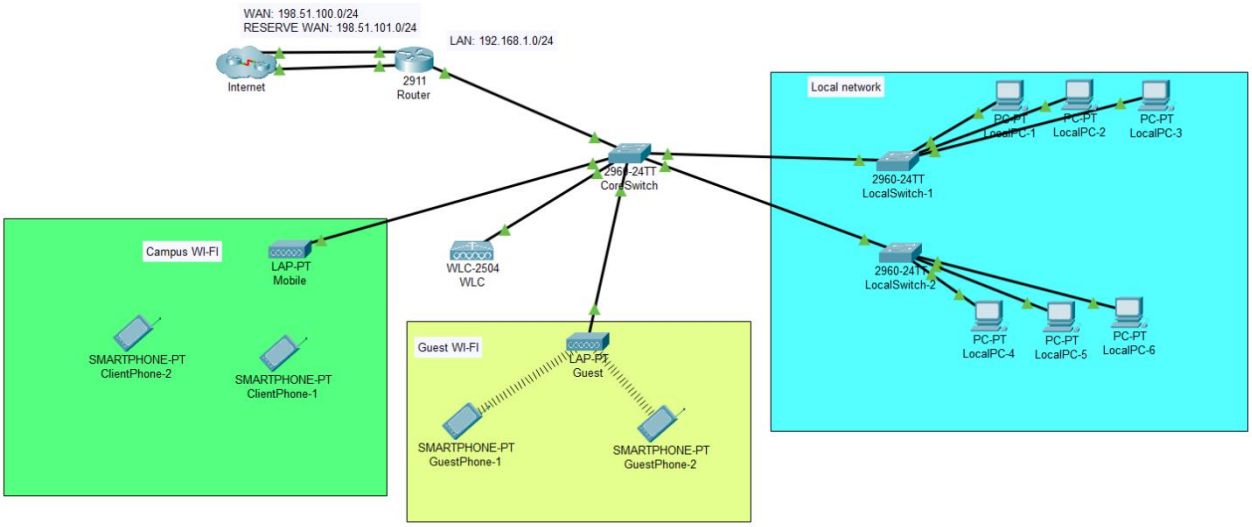
У результаті виконання курсового проекту було створено сучасну, масштабовану та безпечну кампусну мережу з використанням технології Wi-Fi. Розроблена мережа забезпечує високу якість обслуговування користувачів, ефективне управління мережевими ресурсами та можливість подальшого розвитку.

Посилання на GitHub:

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Приклади реалізації деяких проектів: https://itexamanswers.net
2. Теоретична інформація щодо деяких протоколів: https://habr.com
3. Детальна інформація про протокол NAT: https://www.geeksforgeeks.org/network-address-translation-nat/
4. Загальна інформація про реалізацію технології трансляції адрес NAT: https://en.wikipedia.org/wiki/Network_address_translation
5. Приклад налаштування WLC-контролера: https://www.packettracernetwork.com/tutorials/pt71-wlc-configuration
6. Теоретична інформація щодо протоколу DHCP: https://www.fortinet.com/resources/cyberglossary/dynamic-host-configuration-protocol-dhcp
7. Детальніша інформація про протокол DHCP: https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
8. Інформація про налаштування WLC-контролера: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-7/config-guide/b_cg87/initial_setup
9. Приклад налаштування DHCP на маршрутизаторі Cisco: https://ipcisco.com/lesson/router-dhcp-configuration-with-packet-tracer-ccna
10. Теоретична інформація щодо технології VLAN: https://en.wikipedia.org/wiki/VLAN
11. Приклад налаштування комутатора Cisco: https://networklessons.com/switching/how-to-configure-vlans-on-cisco-catalyst-switch
12. Теоретична інформація щодо застосування технології ACL (Access Control List): https://www.cbtnuggets.com/blog/certifications/cisco/networking-basics-how-to-configure-standard-acls-on-cisco-routers

ДОДАТОК 1. СХЕМА МЕРЕЖІ



Router:

```
Current configuration : 1224 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp pool LAN-POOL
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX15246E6P-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 198.51.100.2 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 192.168.1.1
 ip nat inside
 duplex auto
 speed auto
 standby 0 ip 192.168.1.1
 standby preempt
interface GigabitEthernet0/2
 ip address 198.51.101.2 255.255.255.0
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip nat inside source list NAT-ACL interface GigabitEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.10.1
ip route 0.0.0.0 0.0.0.0 10.10.10.5 10
ip flow-export version 9
ip access-list extended NAT-ACL
 permit ip 192.168.1.0 0.0.0.255 any
```

line con 0
line aux 0
line vty 0 4
 login
end

Switch:

Current configuration : 1168 bytes
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname CoreSwitch
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
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
switchport mode access
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
switchport trunk allowed vlan 10,20
switchport mode trunk
interface Vlan1
no ip address
shutdown
line con 0
line vty 0 4
login
line vty 5 15
login
end