

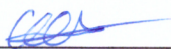
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

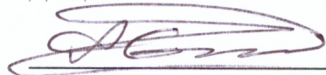
до випускної кваліфікаційної роботи магістра на тему:

«Методи та технології побудови підсистем безпеки
корпоративних мереж побудованих на базі рішень компанії
Cisco»

Виконав студент 2-го курсу групи КІм-23-1
спеціальності 123 «Комп'ютерна інженерія»

 Могильний Є.Л.

Керівник, завідувач кафедри КІ та КБ, к.т.н,
доцент

 Єфіменко А.А.

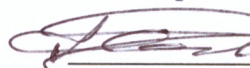
Рецензент, доцент кафедри КІ та КБ, к.т.н.

 Шелуха О.О.

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

17 вересня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента **Могильного Євгенія Леонідовича**

Тема роботи: **Методи та технології побудови підсистем безпеки корпоративних мереж побудованих на базі рішень компанії Cisco**

затверджена Наказом по університету від **17 вересня 2024 р. № 478/С**

Термін здачі студентом закінченої роботи – 16.12.2024р.

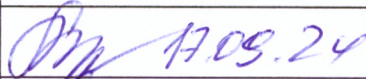
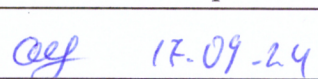
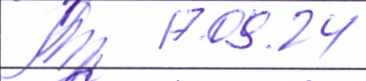
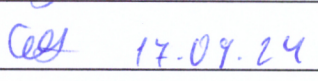
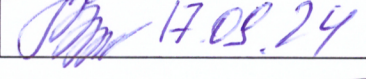
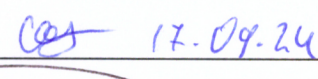
Вихідні дані для роботи:

1. Фізична топологія мережі
2. Логічна топологія мережі

Обладнання та програмне забезпечення:

1. Маршрутизатори Cisco
2. Комутатори Cisco
3. Операційні системи Cisco IOS, Windows 7, Ubuntu, Linux.
4. Графічний симулятор мереж GNS3

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

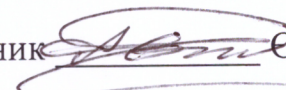
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Воротніков В.В.	 17.09.24	 17.09.24
2	Воротніков В.В.	 17.09.24	 17.09.24
3	Воротніков В.В.	 17.09.24	 17.09.24

Керівник  Єфіменко А.А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	12 квітня 2024 – 13 квітня 2024	Виконано
2	Дослідження літератури для побудови організаційних мереж.	14 квітня 2024 – 15 квітня 2024	Виконано
3	Аналіз протоколів безпеки маршрутизаторів CISCO.	16 квітня 2024 – 17 квітня 2024	Виконано
4	Аналіз потенціалу побудови корпоративних мереж на базі обладнання Cisco.	18 квітня 2024 – 20 квітня 2024	Виконано
5	Розвиток інституційних мереж/проектів	20 квітня 2024 – 24 квітня 2024	Виконано
6	Вибір обладнання та початок реалізації проекту	25 квітня 2024 – 30 квітня 2024	Виконано
7	Проектування таблиці маршрутизації	1 листопада 2024 – 4 листопада 2024	Виконано
8	Координація мережевих тестів	5 листопада 2024 – 12 листопада 2024	Виконано
9	Базова конфігурація мережевого обладнання	13 листопада 2024 – 17 листопада 2024	Виконано
10	Створення організаційної мережі	18 листопада 2024 – 25 листопада 2024	Виконано
11	Тестування продуктивності корпоративної мережі	26 листопада 2024 – 29 листопад 2024	Виконано
12	Аналіз результатів тестування	30 листопада 2024 – 03 грудня 2024	Виконано
13	Написання пояснювальної записки	04 грудня 2024 – 08 грудня 2024	Виконано
14	Підготовка презентації та виступу	09 грудня 2024 – 15 грудня 2024	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	20 грудня 2024 – 22 грудня 2024	Виконано
16	Захист		Виконано

Студент  Могильний Є.Л.

Керівник  Єфіменко А.А.

АНОТАЦІЯ

Кваліфікаційна робота включає проєкти для корпоративних мереж на базі обладнання Cisco. Пояснювальна записка складається з 66 сторінок, 33 ілюстрацій та п'яти таблиць.

Дана кваліфікаційна робота присвячений розробці корпоративної мережі на базі обладнання Cisco. Цілями проєкту є надійність та безпека. Мережа повинна забезпечувати стабільний обмін даними та безпеку пристроїв, тому створюються користувачі для віддаленого доступу.

Кваліфікаційна робота складається з трьох частин і включає розробку логічної та фізичної структури мережі, вибір мережевого обладнання та програмного забезпечення, сценарії конфігурації мережі та тестування проєкту. У додатках наведено конфігурацію мережевих маршрутизаторів та комутаторів.

КЛЮЧОВІ СЛОВА: ЗАХИСТ, КОМП'ЮТЕРНА МЕРЕЖА, КОРПОРАТИВНІ МЕРЕЖІ, RADIUS, CISCO.

ANNOTATION

The qualification work includes projects for corporate networks based on Cisco equipment. The manual consists of 58 pages, 33 illustrations and five tables.

This qualification work is dedicated to the development of a corporate network based on Cisco equipment. The project goals are reliability and security. The network must provide stable data exchange and device security, so users are created for remote access.

The qualification work consists of three parts and includes the development of the logical and physical structure of the network, the selection of network equipment and software, network configuration scenarios and project testing. The appendices provide the configuration of network routers and switches.

KEY WORDS: SECURITY, COMPUTER NETWORK, ENTERPRISE NETWORK, RADIUS, CISCO.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА КОРПОРАТИВНИХ МЕРЕЖ НА БАЗІ ОБЛАДНАННЯ CISCO.....	10
1.1. Характеристика структури корпоративної мережі	10
1.2. Протокол маршрутизації OSPF	13
1.3. Існуючі аналоги підсистем у обраній інформаційній системі	16
1.4. Протокол DHCP	19
1.5. Протокол RADIUS	20
РОЗДІЛ 2 ПРОЄКТУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ З ВИКОРИСТАННЯМ ОБРАНИХ ПРОТОКОЛІВ НА БАЗІ ОБЛАДНАННЯ CISCO	24
2.1 Працездатність мережі.....	24
2.2 Створення логічних мережевих структур.	28
2.3 Вибір обладнання та програмного забезпечення.....	32
РОЗДІЛ 3 ВИВЧЕННЯ КОНФІГУРАЦІЇ ТА ПРОЄКТУВАННЯ ПІДСИСТЕМ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	37
3.1 Конфігурація мережі	37
3.2 Тестували підсистему безпеки корпоративної мережі на базі обладнання Cisco.	44
3.3 Аналіз результатів тестування	48
ВИСНОВКИ	50
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	51
ДОДАТКИ	53

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

КМ – комп'ютерна мережі

ОС – операційна система

GNS3 – Graphical Network Simulator-3

ВСТУП

Актуальність теми. Корпоративні мережі часто використовуються в усьому світі, і їхня актуальність безмежна. Різні типи комп'ютерів містять тисячі різних компонентів, таких як мережеві адаптери, комутатори, маршрутизатори та кабельні системи. Основна роль цих систем - оптимальне опрацювання потоку інформації, що циркулює між співробітниками компанії, що дає змогу ухвалювати своєчасні та раціональні рішення.

Корпоративні мережі зазвичай географічно розподілені та об'єднують офіси, відділи та інші організації, які розташовані на значній відстані один від одного. Крім того, під час проєктування корпоративної мережі необхідно вжити всіх заходів для мінімізації обсягу переданих даних.

Для практичної реалізації підсистем використовується графічний симулятор GNS3. Для забезпечення гетерогенності мережі будуть використовуватися різні версії операційних систем Windows і Linux [13].

Метою кваліфікаційної роботи є розробка проєкту корпоративної мережі на базі обладнання Cisco.

Для досягнення цієї мети будуть вирішені наступні завдання:

- Аналіз сучасного обладнання
- Вибір структури мережі
- Вибір програмного забезпечення для реалізації мережі
- Реалізація підсистем безпеки

Об'єктом дослідження є процес побудови підсистем безпеки корпоративних мереж на базі рішень компанії Cisco, який включає розробку архітектури мережі, налаштування обладнання, впровадження протоколів безпеки (OSPF, DHCP, RADIUS) і перевірку функціональності системи для забезпечення захисту даних та стабільності роботи.

Предметом дослідження є способи та засоби захисту корпоративної мережі з використанням протоколів безпеки. Під час виконання кваліфікаційної роботи було розроблено проєкт із підсистем безпеки для корпоративних мереж на базі обладнання Cisco.

Визначена мета обумовлює наступні завдання:

- Аналіз потенціалу побудови корпоративних мереж на базі обладнання Cisco;
- Вибір обладнання та початок реалізації проекту;
- Проектування таблиці маршрутизації;
- Базова конфігурація мережевого обладнання;
- Створення організаційної мережі;
- Тестування продуктивності корпоративної мережі;
- Аналіз результатів тестування.

У процесі виконання кваліфікаційної роботи було розроблено проєкт побудови підсистем безпеки корпоративних мереж побудованих на базі рішень компанії Cisco. Дослідження методів захисту даних, аналізі актуальних загроз і вразливостей, а також впровадженні інноваційних рішень для підвищення рівня безпеки інформаційної інфраструктури підприємств.

РОЗДІЛ 1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА КОРПОРАТИВНИХ МЕРЕЖ НА БАЗІ ОБЛАДНАННЯ CISCO

1.1. Характеристика структури корпоративної мережі

Оскільки корпоративні мережі містять велику кількість пристроїв різного призначення, такі великі підсистеми необхідно сегментувати. Для цього використовується технологія VLAN: За допомогою VLAN локальну мережу можна розділити на підмережі за функціональною ознакою, незалежно від місця розташування пристроїв.

Це означає, що пристрої, які належать до однієї VLAN, можуть бути підключені до різних комутаторів, віддалених один від одного. І навпаки, пристрої, що належать до різних VLAN, можуть бути підключені до одного комутатора.

Пристрої в різних VLAN не можуть взаємодіяти один з одним, що зменшує можливість несанкціонованого доступу до пристроїв системи. Зв'язок між різними підмережами можливий тільки через маршрутизатори. Крім того, маршрутизатори можна використовувати для встановлення політик безпеки, які можна застосовувати до всіх груп пристроїв, що належать до однієї підмережі.

Головні фактори які мають бути в корпоративній мережі:

- Продуктивність мережі - варіації часу відгуку, пропускної здатності, затримок передачі і затримок передачі даних
- Надійність - здатність мережі нормально функціонувати протягом тривалого часу
- Безпека - здатність системи захищати дані від несанкціонованого доступу
- Розширюваність - позначає ймовірність щодо легкого додавання окремих елементів мережі(користувачів, комп'ютерів, тощо)

- Масштабованість - означає, що мережа може нарощувати кількість вузлів і протяжність зв'язку у межах, у своїй ефективності мережі не погіршується.

- Прозорість - якість мережі приховувати від користувачів деталі свого внутрішнього пристрою, спрощуючи цим його роботу в мережі.

Структура корпоративної мережі є складною і багаторівневою системою, що забезпечує ефективну комунікацію та обмін даними між усіма підрозділами організації, а також із зовнішнім середовищем. Основою мережі є ядро мережі (Core Layer), яке відповідає за забезпечення високошвидкісної передачі даних і оптимізацію трафіку між різними частинами мережі. Це рівень, де використовуються потужні маршрутизатори та комутатори з високою пропускну здатністю, що дозволяють здійснювати швидку маршрутизацію і з'єднувати різні сегменти корпоративної мережі. У цьому рівні мінімізуються затримки, забезпечується висока швидкість і надійність з'єднання.

Далі йде рівень агрегації (Distribution Layer), де зосереджуються функції маршрутизації між локальними мережами (LAN), безпекового контролю, управління трафіком і з'єднання з іншими мережами, такими як VPN або інтернет. На цьому рівні можуть бути розташовані міжмережеві екрани, системи виявлення та запобігання вторгнень (IDS/IPS), а також балансувальники навантаження, які оптимізують розподіл трафіку між різними серверами та користувачами, забезпечуючи ефективність роботи всієї мережі. Тут також реалізуються політики безпеки, що дозволяють контролювати доступ до ресурсів на основі рівнів доступу та прав користувачів.

Рівень доступу (Access Layer) забезпечує підключення кінцевих пристроїв до мережі. Це можуть бути робочі станції, сервери, IP-телефони, камери відеоспостереження, датчики IoT та інші пристрої. На цьому рівні використовуються комутатори, точки бездротового доступу (Wi-Fi), що дозволяє співробітникам підключатися до корпоративної мережі через

проводові або бездротові з'єднання. Важливим аспектом на рівні доступу є забезпечення управління доступом, що часто здійснюється за допомогою VLAN (Virtual Local Area Network), протоколів 802.1X або технологій Zero Trust. Ці технології гарантують, що лише авторизовані пристрої та користувачі мають доступ до внутрішніх ресурсів мережі.

Сучасні корпоративні мережі не можуть обійтися без рішення для віддаленого доступу (Remote Access), оскільки все більше працівників працює з дому або з інших локацій. Для цього використовуються VPN-сервіси, що дозволяють створювати захищені канали для передачі даних через публічні мережі, або інші хмарні платформи, які забезпечують доступ до мережевих ресурсів із будь-якої точки світу. У зв'язку з переходом на гібридну модель роботи, також активно впроваджуються рішення SASE (Secure Access Service Edge), які поєднують функції безпеки і доступу в єдину хмарну платформу, що дозволяє забезпечити високий рівень захисту для віддалених співробітників та пристроїв.

Інтеграція з хмарними платформами (Cloud Integration) стає важливим елементом структури корпоративних мереж. Хмари використовуються для зберігання даних, хостингу додатків, резервного копіювання та надання різних сервісів. Основні гравці на ринку хмарних послуг, такі як Microsoft Azure, AWS та Google Cloud, пропонують гнучкі рішення для зберігання та обробки даних, що дозволяють масштабувати ресурси в залежності від потреб організації. Хмара також стає основою для розвитку додатків з високою доступністю, що дозволяє забезпечити безперервну роботу бізнесу навіть у разі непередбачених подій.

Що стосується систем захисту та безпеки, то сучасні корпоративні мережі вимагають постійного моніторингу та захисту від численних кіберзагроз. Це включає в себе використання міжмережевих екранів (firewalls), систем виявлення вторгнень (IDS) та запобігання вторгненням (IPS), а також технології для захисту кінцевих точок (endpoint protection). Інструменти, що базуються на AI та машинному навчанні, активно застосовуються для

автоматизації виявлення загроз і забезпечення оперативної реакції на них. Окрім цього, реалізація архітектури Zero Trust, яка передбачає безперервну перевірку доступу до ресурсів незалежно від місцезнаходження користувача чи пристрою, стає все більш популярною серед великих корпорацій.

Корпоративні мережі також включають в себе інфраструктуру для забезпечення високої доступності (High Availability), що включає в себе дублювання мережових з'єднань, серверів, а також зберігання даних. Це дозволяє мінімізувати час простою мережі та швидко відновлювати її роботу у разі аварій.

Таким чином, структура корпоративної мережі включає в себе декілька важливих рівнів: ядро, агрегація, доступ і захист, кожен з яких виконує свою роль у забезпеченні надійної та безпечної роботи всіх корпоративних ресурсів. За допомогою сучасних технологій і рішень для інтеграції, віддаленого доступу, хмарних обчислень та безпеки, корпоративні мережі здатні ефективно підтримувати бізнес-процеси та захищати дані від сучасних кіберзагроз.

1.2 Протокол маршрутизації OSPF

Open Shortest Path First (OSPF) – це протокол динамічної маршрутизації. Він заснований на технології стану з'єднання і використовується для пошуку найкоротшого шляху. Обмін інформацією, який виконує маршрутизатор для визначення шляхів передачі в межах області, показано зеленими стрілками на схемі (рис. 1.1). У цьому випадку маршрутизація та обмін інформацією між областями відбувається через спеціальну центральну область (AREA 0). Використовуючи таку логічну схему побудови мережі, можна значно зменшити частку неінформаційного трафіку, що передається по шляхах передачі даних між областями. Зокрема, в цьому випадку канали (червоні), що використовуються для передачі даних між областями, несуть не тільки інформацію про локальну мережу. При використанні протоколу

маршрутизації OSPF можлива наявність декількох маршрутів в напрямку конкретного вузла мережі.

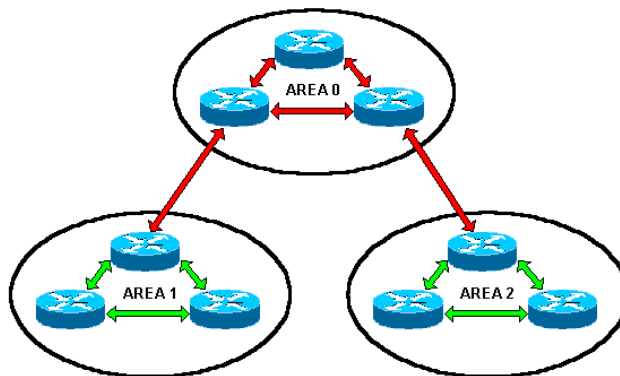


Рис.1.1 - Модель маршрутизації

Якщо ці маршрути забезпечують передачу даних однакової якості, то інформаційні потоки на адресу цього вузла можуть передаватися одночасно по всіх цих каналах, що призводить до значного збільшення швидкості передачі даних. Динамічний перерозподіл трафіку між паралельними каналами виконується пропорційно ступеню завантаженості цих каналів і називається балансуванням навантаження.

Розглянемо переваги OSPF:

- OSPF легко масштабується. Тобто його можна без особливих зусиль розширити для використання в дуже великих мережах;
- Перший відкритий протокол найкоротшого шляху повністю підтримує підмережі: OSPF надсилає невеликі пакети привітання для тестування поведінки зв'язку та ігнорує передачу великих таблиць;
- OSPF підтримує тегування маршрутів: OSPF дозволяє легко взаємодіяти з довільними значеннями;
- Маршрути можуть бути позначені, щоб полегшити взаємодію з довільними значеннями;
- Маршрутизація: OSPF може маршрутизувати пакети на основі поля типу сервісу.

Недоліки OSPF:

- OSPF - це інтенсивний протокол, що використовує багато процесорних ресурсів;

- Він споживає більше пам'яті, оскільки зберігає декілька копій інформації про маршрутизацію;
- OSPF складніший для розуміння і вивчення, ніж інші інтернет-протоколи;
- OSPF вимагає, щоб всі області були підключені до магістральної області.

Якщо безперервність магістралі порушена або магістраль навмисно розділена, можна встановити віртуальне з'єднання. Дві кінцеві точки віртуального каналу є ABR. Віртуальне з'єднання має бути налаштоване на обох маршрутизаторах. Інформація про конфігурацію кожного маршрутизатора складається з окремої віртуальної кінцевої точки (інший ABR) інтегрованої області (яка називається транзитною областю), спільної для двох маршрутизаторів. Зауважте, що віртуальні канали не можуть бути налаштовані через заглушки областей.

OSPF використовує найбільшу IP-адресу, налаштовану на інтерфейсі, як ідентифікатор маршрутизатора. Якщо інтерфейс, пов'язаний з цією IP-адресою, виходить з ладу або адреса видаляється, процес OSPF повинен перерахувати новий ідентифікатор маршрутизатора і повторно надіслати всю інформацію про маршрутизацію на цей інтерфейс. Якщо для інтерфейсу зі зворотним зв'язком налаштовано IP-адресу, програмне забезпечення Cisco IOS використовує цю IP-адресу як ідентифікатор маршрутизатора, навіть якщо інші інтерфейси мають більші IP-адреси. Інтерфейс зі зворотним зв'язком ніколи не вимикається, тому таблиця маршрутизації є більш стабільною.

OSPF автоматично надає пріоритет інтерфейсу зі зворотним зв'язком над іншими типами і вибирає найбільшу IP-адресу серед усіх інтерфейсів зі зворотним зв'язком. Якщо інтерфейсу зворотного зв'язку немає, вибирається найбільша IP-адреса на маршрутизаторі неможливо вказати OSPF використовувати певний інтерфейс. По-перше, як протокол маршрутизації, він займає важливе місце в інфраструктурі Інтернету.

Можливість швидко і легко знайти найкоротший шлях може зменшити непотрібне навантаження на мережу, а можливість знайти альтернативний шлях у разі збою на оптимальному рівні може підвищити стабільність мережі.

1.3. Існуючі аналоги підсистем у обраній інформаційній системі

Існують численні аналоги підсистем безпеки корпоративних мереж, побудованих на рішеннях Cisco, які мають свої переваги, підходи до безпеки та функціональні можливості. Серед таких рішень виділяються Palo Alto Networks, яка впроваджує інноваційні підходи до аналізу загроз через штучний інтелект та автоматизацію. Їхні міжмережеві екрани нового покоління (NGFW) швидко виявляють і блокують загрози в реальному часі, а платформа WildFire забезпечує захист від складних атак шляхом виявлення невідомих загроз. Fortinet, зі своєю інтегрованою екосистемою рішень FortiGate, FortiAnalyzer та FortiClient, пропонує централізоване управління мережею та забезпечує високу продуктивність, навіть у великих корпоративних середовищах. Check Point Software Technologies зосереджується на багаторівневій безпеці за допомогою Quantum Security Gateway, SandBlast (для захисту від складних загроз) та CloudGuard, який інтегрується із хмарними середовищами.

Інші важливі гравці ринку, такі як Juniper Networks, пропонують SRX Series для забезпечення безпеки через апаратні брандмауери, а також Sky ATP для аналізу загроз у хмарному середовищі. Їхній інструмент Junos Space забезпечує ефективне управління мережею та аналіз безпеки, що дозволяє зменшити час реагування на інциденти. Huawei зі своїм рішенням CloudFabric Security націлений на великі корпоративні мережі та центри обробки даних. Їхня екосистема включає iNGFW і SecoManager, які підтримують централізоване управління великими мережами. SonicWall фокусується на простоті впровадження та доступності, що робить його ідеальним для малого та середнього бізнесу. Їхня система Capture ATP використовує штучний інтелект для боротьби зі складними кіберзагрозами. Microsoft Azure Security

пропонує інтеграцію хмарних рішень із корпоративними мережами через продукти Azure Firewall та Microsoft Defender for Cloud, забезпечуючи захист даних та інфраструктури в умовах віддаленої роботи.

Додатково, варто зазначити Sophos, яка спеціалізується на захисті від загроз типу ransomware за допомогою Intercept X і пропонує централізоване управління мережею через Sophos Central. Такі аналоги, як Palo Alto Networks та Fortinet, активно впроваджують прогнозувальні технології для аналізу мережевого трафіку та попередження атак, у той час як Cisco вирізняється інтеграцією своїх продуктів у межах єдиної екосистеми. Cisco пропонує широкий спектр рішень, таких як Cisco Firepower, Cisco SecureX та Cisco Umbrella, які забезпечують багаторівневий захист, включно з аналітикою трафіку, захистом кінцевих точок та сегментацією мережі. Інструменти на кшталт Cisco Stealthwatch дозволяють виявляти аномалії навіть у зашифрованому трафіку, що додає важливого рівня безпеки для корпоративних мереж.

Cisco також підтримує сучасні підходи до побудови архітектури Zero Trust, що передбачає максимальну перевірку всіх користувачів і пристроїв, а також архітектуру SASE (Secure Access Service Edge), яка об'єднує мережеві та безпекові функції в єдиній хмарній платформі. Це особливо актуально для великих корпорацій, які працюють у гібридному форматі. Конкуренти, такі як Palo Alto Networks і Fortinet, також активно розвивають ці технології, але Cisco виграє за рахунок інтеграції своїх продуктів і підтримки IoT-пристроїв.

Сучасні корпоративні мережі стикаються з новими викликами, що зумовлені зростанням кількості кіберзагроз, переходом на віддалену роботу та інтеграцією хмарних технологій. Основними тенденціями є активне впровадження архітектури Zero Trust, яка забезпечує мінімізацію ризиків доступу до мережі, та перехід до використання хмарних рішень для безпеки (SASE). Корпоративні мережі також змінюються під впливом зростання кількості IoT-пристроїв, які додають новий рівень складності до забезпечення безпеки через їхню високу вразливість.

Інтеграція AI та машинного навчання в системи безпеки дозволяє прогнозувати потенційні атаки та швидко адаптувати мережі до нових типів загроз. Проте значною проблемою залишається зростання кількості складних атак, таких як ransomware та атак на ланцюжки поставок (supply chain attacks), які важко виявити традиційними методами.

Більшість сучасних рішень, таких як Cisco, Fortinet, Palo Alto Networks та інші, спрямовані на створення багаторівневих систем захисту з інтеграцією аналітики, автоматизації та безперервного моніторингу мережі. Глобальні компанії все більше орієнтуються на хмарні інструменти, які дозволяють гнучко масштабувати ресурси, забезпечуючи при цьому високий рівень безпеки. Основною задачею для корпоративних мереж залишається баланс між зручністю користування, продуктивністю та рівнем захисту, що робить впровадження комплексних рішень, таких як Cisco SecureX, все більш актуальним у сучасних умовах.

Окремо варто відзначити Sophos, яка має потужний захист від ransomware завдяки системі Intercept X та централізоване управління через Sophos Central. Аналоги Cisco, такі як Palo Alto Networks та Fortinet, часто орієнтуються на новітні AI-технології, прогнозування загроз і глибоку сегментацію мережі. Тим часом, Cisco вирізняється широкою інтеграцією своїх продуктів, що забезпечує ефективну взаємодію між різними компонентами мережі, такими як Cisco Firepower, Cisco SecureX, і підтримка сучасних стандартів безпеки (Zero Trust Architecture, SASE). Ці рішення дозволяють захистити інфраструктуру від складних багаторівневих атак, забезпечуючи одночасно високу продуктивність і зручність в управлінні.

Вибір між аналогами залежить від специфіки інфраструктури організації, бюджету, необхідного рівня безпеки, а також вимог до інтеграції з існуючими рішеннями.

1.4. Протокол DHCP

DHCP - це протокол для автоматизації розподілу IP-адрес серед клієнтів. Він широко використовується в сучасних мережах: IP-адреси можна призначати користувачам вручну, але це забирає багато часу. Тому в 1993 році було розроблено протокол DHCP. Він автоматизував налаштування IP-адрес, спростив діагностику мережових з'єднань і забезпечив доступ з однієї підмережі в іншу.

Коли клієнт підключається до мережі, починається процес ініціалізації. Оскільки комп'ютер користувача не має IP-адреси, усім пристроям у мережі надсилається повідомлення DHCPDISCOVER. У тій же мережі має бути DHCP-сервер. Це може бути комутатор або маршрутизатор. Клієнт перебуває в стані ініціалізації (INIT) і не має власної IP-адреси. З цієї причини клієнт надсилає широкомовні повідомлення DHCPDISCOVER усім пристроям у локальній мережі.

У тій же локальній мережі є DHCP-сервер, наприклад, маршрутизатор або комутатор, але існують і виділені DHCP-сервери: в одній мережі не завжди один DHCP-сервер, а часто кілька одночасно. Сервер завжди прослуховує порт 67, очікує широкомовних повідомлень від клієнтів і відправляє DHCPOFFER, коли отримує їх. Клієнт отримує повідомлення на порт 68. Сервер DHCP відповідає пропозицією і повідомляє клієнту IP-адресу, відповідну для нього IP-адресу, яка виділяється з діапазону доступних адрес (SCOPE), встановленого адміністратором адреси виділяється сервером DHCP.

Якщо є адреси, які не повинні виділятися, діапазон можна обмежити тільки тими адресами, які дозволені. Наприклад, адміністратор може встановити діапазон використовуваних IP-адрес 192.168.1.10 - 192.168.1.255.

Однак, можливо, немає необхідності призначати клієнтам усі доступні адреси. Наприклад, адміністратор може виключити діапазон 192.0.0.100 - 192.0.0.200 зі сфери використання. Таке обмеження називається виключенням: оскільки DHCP лише тимчасово призначає доступні IP-адреси з цього

діапазону, немає жодної гарантії, що під час наступного підключення клієнт отримає той самий IP.

Однак можна постійно призначати певну IP-адресу будь-якому клієнту. Наприклад, можна зарезервувати 192.0.0.10 для комп'ютера системного адміністратора. Таке збереження IP-адрес для окремих клієнтів називається резервуванням, у DHCP є вразливості. Головна з них полягає в чотирьох кроках, необхідних для отримання IP: процес DORA надсилає широкомовне повідомлення, і перший DHCP-сервер, який відповів, може надати IP із цієї області.

Якщо зловмисник зможе використовувати сервер, який відповідає клієнту раніше за всіх, він зможе контролювати поведінку користувачів у мережі та завдати значної шкоди. Ще один пролом у безпеці полягає в тому, що DHCP використовує протокол UDP, який є протоколом обміну даними без з'єднань і не потребує шифрування; інформація, передана по UDP, не захищена і може бути «перехоплена» і використана зловмисниками.

Третій недолік - знову ж таки ненадійність UDP, але це недолік в іншому сенсі UDP не дає гарантії доставки інформації. Протокол терпимий до втрат і помилок, які можуть вплинути на DHCP, особливо під час завантаження PXE.

1.5. Протокол RADIUS

RADIUS (Remote Authentication Dial-In Service) - це стандарт IETF для AAA. Спочатку він використовувався для розширення 2-го рівня протоколу Point-to-Point (PPP) між кінцевими користувачами і серверами мережевого доступу (NAS), а також для передачі трафіку автентифікації від NAS до сервера AAA.

Дайджести автентифікації та авторизації включені в один тип пакетів, а білінг обробляється в окремому процесі [10] Cisco підтримує RADIUS на

основі парадигми безпеки автентифікації, авторизації та обліку (AAA). RADIUS, TACACS+, Kerberos та інші протоколи безпеки AAA, а також локальний пошук імен користувачів. Всі платформи Cisco підтримують RADIUS, але деякі функції з підтримкою RADIUS доступні лише на певних платформах.

Використовуйте RADIUS у наступних мережових середовищах, де потрібна безпека доступу. Наприклад, сервери доступу від різних виробників використовують єдину базу даних безпеки на основі сервера RADIUS. В IP-мережах з декількома серверами доступу користувачі, що підключаються до телефонів, авторизуються через сервер RADIUS, налаштований на роботу з безпекою Kerberos.

Програма підтримує готові середовища мережової безпеки з підтримкою RADIUS, такі як системи контролю доступу на основі смарт-карт. Мережі, які вже використовують RADIUS, можуть додавати пристрої Cisco RADIUS до мережі. Це перший крок до переходу на сервер TACACS+. RADIUS можна використовувати для контролю доступу користувачів до одного хоста, однієї утиліти (наприклад, Telnet) або одного протоколу (наприклад, PPP).

Наприклад, коли користувач входить в систему, RADIUS ідентифікує його як користувача, уповноваженого ініціювати PPP за IP-адресою 10.2.3.4 і ініціювати певний список доступу. На додаток до автентифікації або авторизації RADIUS можна також використовувати облік RADIUS. Функція обліку радіуса дозволяє надсилати дані на початку і в кінці послуги, показуючи кількість ресурсів (наприклад, час, пакети, байти), використаних під час сеансу зв'язку. Провайдери можуть використовувати безкоштовні версії програмного забезпечення для контролю доступу та обліку RADIUS для конкретних потреб безпеки та обліку.

Коли в мережі використовується сервер RADIUS, можна налаштувати попередню автентифікацію AAA і профілі попередньої автентифікації. Попередня автентифікація дозволяє постачальникам послуг використовувати існуючі рішення RADIUS для поліпшення управління портами, ефективного управління використанням спільних ресурсів і надання різних угод про рівень обслуговування. Визначення сервера RADIUS і автентифікації RADIUS.

Після того, як ви визначили комутатори, необхідно визначити список методів автентифікації RADIUS. `aaa` полегшує автентифікацію RADIUS, тому ви повинні ввести команду `aaa authentication` і вказати RADIUS як метод автентифікації. `aaa accounting` дозволяє визначити службу AAA полегшує облік RADIUS, тому ви повинні вказати RADIUS як метод обліку і ввести команду `aaa accounting`.

Автентифікація AAA дозволяє встановити параметри для обмеження доступу користувачів до мережі, включаючи одноразову або для кожного сервісу автентифікацію, список облікових записів і профілів для кожного користувача, підтримку груп користувачів, підтримку віддаленого доступу по IP, IPX і AppleTalk. Доступ (ARA), підтримка віддаленого входу і т.д. Автентифікація RADIUS забезпечується AAA, тому необхідно ввести команду `aaa authentication` і вказати RADIUS в якості методу автентифікації. Сервери безпеки RADIUS ідентифікуються ім'ям хоста або IP-адресою, ім'ям хоста і певним номером порту UDP або IP-адресою і певним номером порту UDP; комбінація IP-адреси і номера порту UDP створює унікальний ідентифікатор, який дозволяє ідентифікувати різні порти індивідуально як хост RADIUS, що надає послуги AAA. Цей унікальний ідентифікатор дозволяє надсилати RADIUS-запити на декілька UDP-портів на сервері з однією IP-адресою.

Якщо два різні записи хостів на одному сервері RADIUS налаштовані на одну і ту ж послугу (наприклад, облік), другий налаштований запис хоста діє як резервна копія для першого хоста. Якщо перший запис хоста не може

надавати послуги обліку, сервер мережевого доступу намагається запустити другий запис хоста, налаштований на тому ж пристрої для надання послуг обліку. Сервер RADIUS і пристрій Cisco мають спільний секретний текстовий рядок. Рядок використовується для шифрування пароля і зміни відповідей. Щоб налаштувати RADIUS на використання команд безпеки AAA, необхідно вказати хост, на якому запущено демон сервера RADIUS, і секретний текстовий рядок (ключ), який він використовує спільно з пристроєм.

Висновки до розділу 1

Аналіз характеристик корпоративних мереж дозволив виявити основні принципи побудови планів та способи їх захисту. Необхідно розробити підсистеми корпоративної мережі з більш високим рівнем безпеки.

Для автоматичного призначення IP-адрес пристроям було обрано протокол маршрутизації OSPF та протокол DHCP. Оскільки пристрої CISCO можуть бути сконфігуровані з усіма обраними протоколами і технологіями, для контролю доступу до хостів також був використаний протокол RADIUS провідного виробника CISCO.

Для побудови корпоративної мережі використовувався симулятор GNS3. Цей симулятор дозволяє побачити, як комунікаційні пристрої та віртуальні машини взаємодіють один з одним в обраній операційній системі.

РОЗДІЛ 2 ПРОЄКТУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ З ВИКОРИСТАННЯМ ОБРАНИХ ПРОТОКОЛІВ НА БАЗІ ОБЛАДНАННЯ CISCO

2.1 Працездатність мережі

Оскільки корпоративна мережа складається з великої кількості пристроїв, вона повинна бути розділена на локальні мережі: Віртуальні локальні мережі поділяють підсистему на окремі широкомовні домени. Це означає, що широкомовні повідомлення будуть прийматися тільки пристроями, що належать до тієї ж VLAN. Продуктивність системи в цілому. В мережі буде використовуватися велика кількість пристроїв яким потрібно швидко надати IP-адреси, тому для цього використаємо протокол DHCP. Керувати буде маршрутизатор DHCP Router.

Оскільки схема має велику кількість підмереж, необхідно створити IP-топологію. Для цього використовується протокол OSPF; OSPF використовує найбільшу IP-адресу, налаштовану на інтерфейсі, як ідентифікатор маршрутизатора. Якщо інтерфейс, пов'язаний з цією IP-адресою, виходить з ладу або адреса видаляється, процес OSPF повинен перерахувати новий ідентифікатор маршрутизатора і повторно надіслати всю інформацію про маршрутизацію на цей інтерфейс.

Протокол RADIUS також використовується для швидкого доступу та налаштування пристроїв. Для того, щоб він працював, необхідно налаштувати автентифікацію AAA. Якщо коротко, AAA-клієнт надсилає автентифікаційну інформацію на сервер автентифікації, який вирішує, відхилити чи дозволити запит на основі відповіді (або відсутності відповіді). Відповідно до налаштованої політики AAA, пристрій запитує логін і пароль та надсилає їх на сервер RADIUS.

Таблиця 2.1

Розподілення на підмережі пристроїв мережі

Назва мережі	Кількість робочих станцій	DHCP-сервер
LAN10	1 робоча станція (3 додаванням)	Сервер під керуванням Windows 10 Server
LAN20	1 робоча станція(3 додаванням)	Маршрутизатор
LAN40	1 робоча станція (3 додаванням)	Маршрутизатор
LAN50	1 робоча станція (3 додаванням)	Маршрутизатор
LAN70	1 робоча станція (3 додаванням)	Маршрутизатор
LAN80	1 робоча станція (Без додавання)	Маршрутизатор

Таблиця 2.2

Адресація мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Підмережа А	-	192.168.1.0	255.255.255.0	/24
Підмережа В	-	192.168.2.0	255.255.255.*	/24
Підмережа С	-	192.168.3.0	255.255.255.*	/24
Підмережа D	-	192.168.4.0	255.255.255.*	/24
Підмережа Е	-	192.168.5.0	255.255.255.*	/24
Підмережа 10	-	192.168.10.0	255.255.255.*	/24
Підмережа 20	-	192.168.20.0	255.255.255.*	/24
Підмережа 30	-	192.168.30.0	255.255.255.*	/24

Адресація мережі

Продовження таблиці 2.2

Підмережа 40	-	192.168.40.0	255.255.255.0	/24
Підмережа 50	-	192.168.50.0	255.255.255.*	/24
Підмережа 60	-	192.168.60.0	255.255.255.*	/24
Підмережа 70	-	192.168.70.0	255.255.255.*	/24
Підмережа 80	-	192.168.80.0	255.255.255.*	/24
Підмережа 90	-	192.168.90.0	255.255.255.*	/24
Інтернет підключення				
Маршрутизатор EDGERouter_1	e2/0	192.168.50.1	255.255.255.0	/24
	g1/0	192.168.2.1	255.255.255.*	/24
Маршрутизатор EDGERouter_2	g1/0	192.168.2.2	255.255.255.*	/24
	e2/1	192.168.3.8	255.255.255.*	/24
	e2/2	192.168.5.2	255.255.255.*	/24
Комутатор ServerSW	Vlan 3	192.168.3.5	255.255.255.*	/24
	Vlan 4	192.168.4.6	255.255.255.*	/24
Комутатор DMZSwitch	Vlan 5	192.168.5.1	255.255.255.*	/24
Server-Ubuntu	e0	192.168.5.3	255.255.255.*	/24
RADIUS	e0	192.168.3.6	255.255.255.*	/24
Комутатор Core1	Vlan 4	192.168.4.5	255.255.255.*	/24
Комутатор Core2	Vlan 4	192.168.4.3	255.255.255.*	/24
Комутатор Core 3	Vlan 3	192.168.3.2	255.255.255.*	/24
Комутатор Core 4	Vlan 4	192.168.4.2	255.255.255.*	/24

Адресація мережі

Продовження таблиці 2.2

DHCPRouter	e1/0	192.168.3.1	255.255.255.0	/24
	e1/1	192.168.4.1	255.255.255.*	/24
	e2/0	192.168.30.1	255.255.255.*	/24
	e2/1	192.168.60.1	255.255.255.*	/24
	e2/2	192.168.90.1	255.255.255.*	/24
Рівень доступу і розподілу				
Комутатор Dis1	Vlan 30	192.168.30.2	255.255.255.0	/24
	Vlan 10	192.168.10.1	255.255.255.*	/24
	Vlan 20	192.168.20.1	255.255.255.*	/24
Комутатор Dis2	Vlan 60	192.168.60.2	255.255.255.*	/24
	Vlan 40	192.168.40.1	255.255.255.*	/24
	Vlan 50	192.168.50.1	255.255.255.*	/24
Комутатор Dis3	Vlan 90	192.168.90.2	255.255.255.*	/24
	Vlan 70	192.168.70.1	255.255.255.*	/24
	Vlan 80	192.168.80.1	255.255.255.*	/24
Комутатор Асс1	Vlan 10	192.168.10.2	255.255.255.*	/24
Робоча станція PC1	e0	DHCP		
Комутатор Асс2	Vlan 20	192.168.20.2	255.255.255.0	/24
Робоча станція PC2	e0	DHCP		
Комутатор Асс3	Vlan 40	192.168.40.2	255.255.255.0	/24
Робоча станція PC3	e0	DHCP		

Адресація мережі

Продовження таблиці 2.2

Комутатор Асс4	Vlan 50	192.168.50.2	255.255.255.*	/24
Робоча станція PC4	e0	DHCP		
Комутатор Асс5	Vlan 70	192.168.70.2	255.255.255.*	/24
Робоча станція PC5	e0	DHCP		
Комутатор Асс6	Vlan 80	192.168.80.2	255.255.255.*	/24
Робоча станція ADMIN	e0	DHCP		

2.2 Створення логічних мережевих структур.

План використовує модель корпоративної мережі, яка гарантує продуктивність і надійність мережі та складається з п'яти рівнів: Ядро з DHCP-серверами, центр обробки даних, демілітаризована зона (DMZ), розподіл і доступ та підключення до Інтернету.

Ядро гарантує швидку передачу даних між комутаторами; DHCP-сервер також налаштований для автоматичного розподілу IP-адрес та інших параметрів між пристроями.

Центр обробки даних використовує протокол RADIUS для зберігання користувачів і паролів. Для підтримки зв'язку з мережею також встановлено комутатор L3.

Рівень розподілу забезпечує мережеву маршрутизацію, а DHCP-ретранслятори налаштовані на отримання IP-адрес між VLAN.

Загальний вигляд моделі наведено на рисунку 2.1.

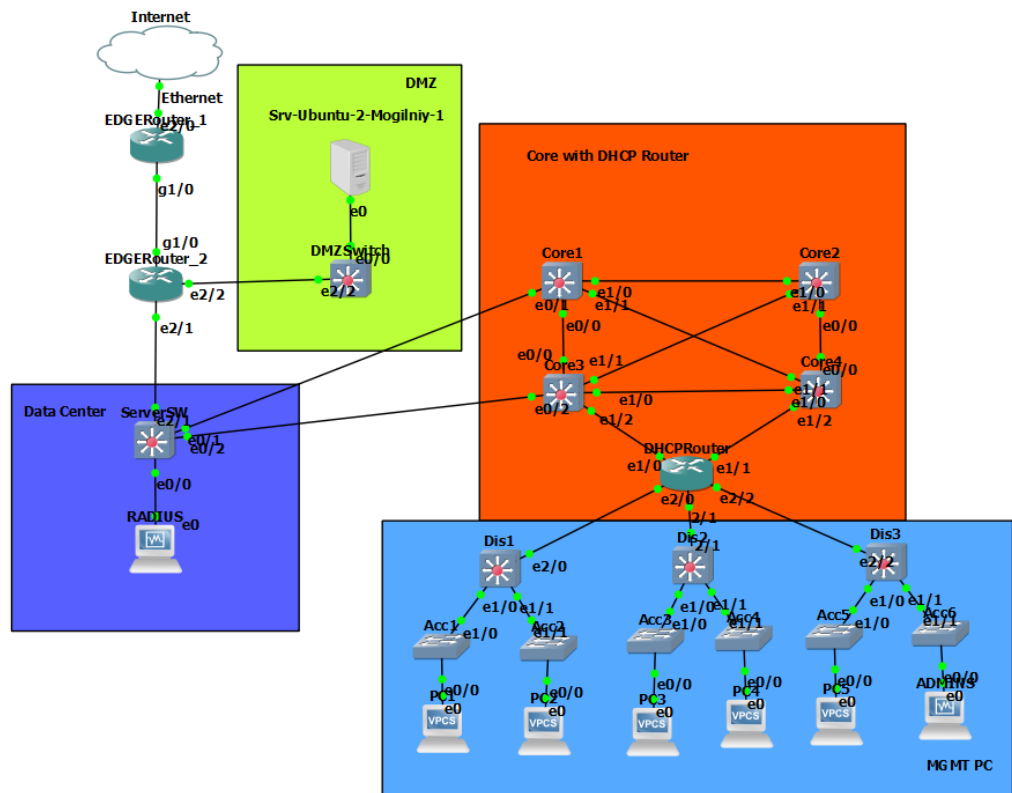


Рис.2.1 - Корпоративна модель

Для кращого розуміння моделі розглянемо всі рівні мережі окремо. Всі наведенні рівні знаходяться на рисунках (Рис.2.2 – Рис.2.8).

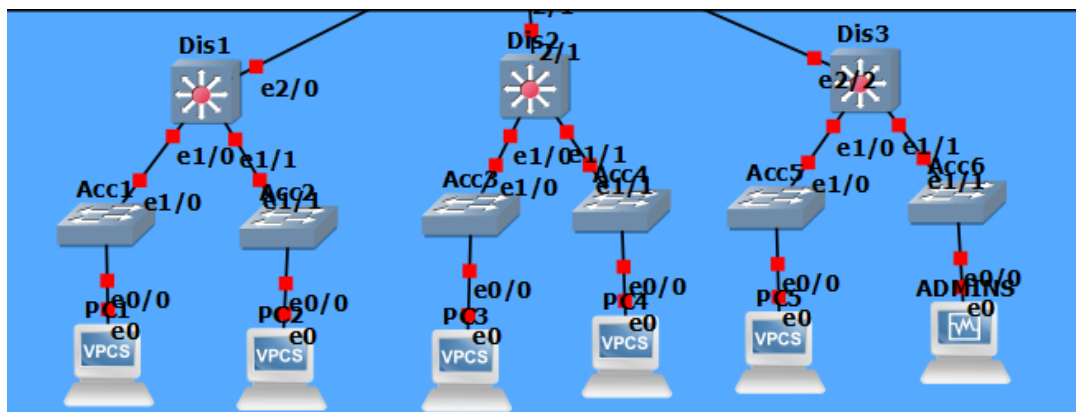


Рис.2.2 - Рівні доступу та розподілу

Таблиця 2.3

Рівні доступу та розподілу

Комутатори	Switch L3 (i86bi-linux-l3-tpgen- ipbase-12.4.bin) Switch L2 (i86bi-linux-l2- adventerprisek9-15.1a.bin)
Робочі станції	Windows 7

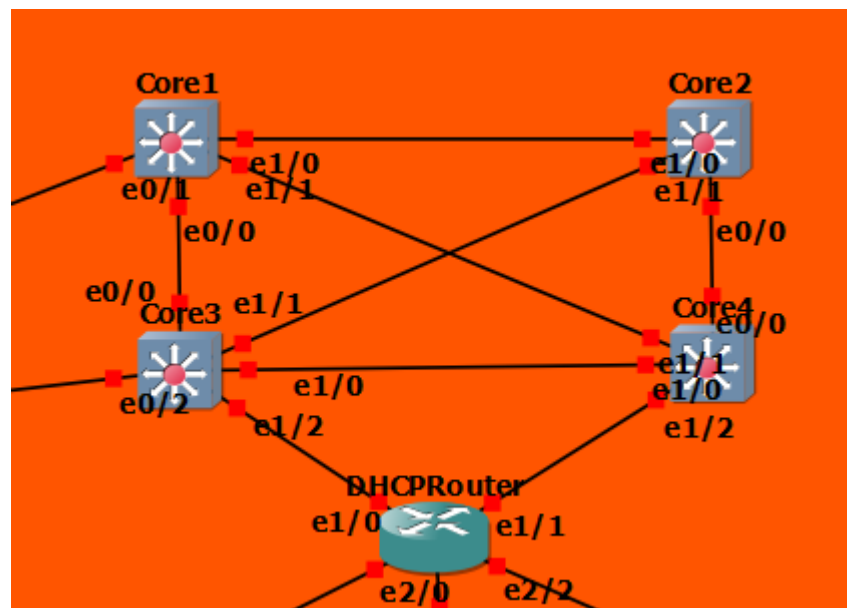


Рис.2.3 - Ядро та DHCP-сервер

Таблиця 2.4

Ядро та DHCP-сервер

Комутатори	Switch L3 (i86bi-linux-l3-tpgen- ipbase-12.4.bin)
Маршрутизатори	c7200(c7200-adventerprisek9_sna- mz.150-1.M3.image)

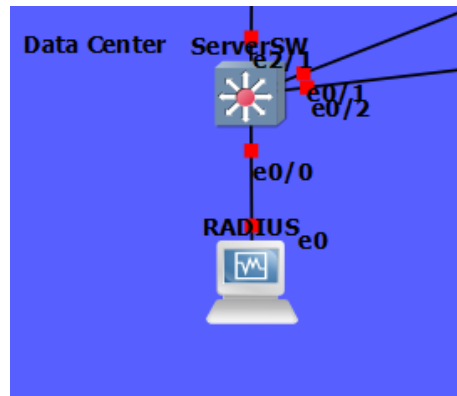


Рис.2.4 - Data Center

Таблиця 2.5

Пристрої, що входять до Data Center

Комутатори	Switch L3 (i86bi-linux-l3-tpgen-ipbase-12.4.bin)
Робочі станції	RADIUS

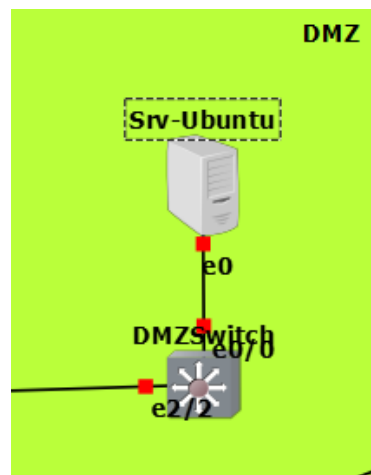


Рис.2.5 - Модель DMZ

Таблиця 2.6

Пристрої DMZ

Комутатори	Switch L3 (i86bi-linux-l3-tpgen-ipbase-12.4.bin)
Робочі станції	Ubuntu

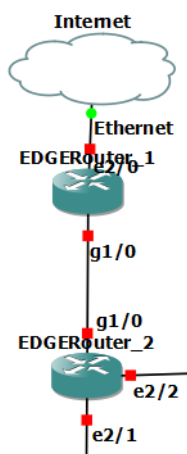


Рис.2.6 - Інтернет з'єднання

Таблиця 2.7

Пристрої інтернет з'єднання

Маршрутизатори	c7200(c7200-adventerprisek9_sna-mz.150-1.M3.image)
----------------	--

2.3 Вибір обладнання та програмного забезпечення.

До потреб, що зазначені вище, було сформовані вимоги до програмного забезпечення:

- Налаштування DHCP сервера.
- Наявність захищеного доступу до робочих станцій.
- Сервер RADIUS.
- Списки доступу

Безпека мережі забезпечується паролем доступу та створенням користувачів за допомогою RADIUS, який шифрує паролі.

Для реалізації цього плану ми будемо використовувати обладнання CISCO; основні рекомендації CISCO полягають у наступному:

- Багатофункціональні маршрутизатори
- Потужні, розумні комутатори
- Пристрої активного захисту – ASA, ACE

- Системи запобігання вторгненням – IPS
- Системи централізованого бездротового доступу
- Уніфіковані комунікації (VoIP, відеоконференції, telepresence, системи керування дзвінками)
- Системи централізованого захисту хостів (CSA)
- Система контролю доступу (NAC)

Головне - cisco не зупиняється на досягнутому і «тримає ніс за вітром», вкладаючи гроші в перспективні напрямки та вигадуючи нові, наприклад, купуючи перспективні розробки та вбудовуючи їх у свої рішення.

Особливості обладнання CISCO є:

- Надійність - ламається все, питання лише коли. Надійність Cisco перевірена роками успішної експлуатації.
- Гнучкість - одне і те ж залізо, залежно від операційної системи та набивання модулів, може виконувати абсолютно різні функції: захисні, шлюза уніфікованих комунікацій, сервісні... Це означає, що коли вони хочуть чогось нового, вони можуть найняти кілька команд, не купуючи нічого.
- Взаємозалежність - різне залізо, що виконують різні функції, можуть залежати один від одного та керувати один одним. Це дозволяє зробити мережу живим організмом, а чи не набором розрізнених пристроїв.
- Налагодження - дуже важливо для налаштування та налаштувачів: найширші можливості пошуку несправностей, вбудовані практично у всі пристрої Cisco.
- Інтелектуальність - всі пристрої Cisco містять широкий спектр технологій, протоколів, ідеологій як стандартних, так і своїх власних, що дозволяють розширити можливості мережі.

Іншими словами, можна зробити висновок, що обладнання CISCO є дуже гнучким з точки зору конфігурації та надійності як для великого, так і для малого бізнесу. Тому ми використовуємо зображення маршрутизатора

серії 7200 (рис. 2.7) та комутатора 9300 (рис. 2.8). Для створення моделі корпоративної мережі будемо використовувати програму GNS3.

Додатково використовується програма VirtualBox, а також Wireshark для перевірки трафіку в нашій мережі.



Рис.2.7 - Маршрутизатор (Cisco 7200)



Рис. 2.8 - Комутатор (Cisco Catalyst 9300)

Графічний симулятор мережі. Це справжній перекладний графічний симулятор мережі. Він дозволяє створювати різні мережеві топології на комп'ютері. Часто GNS використовують як тестові стенди, на яких можна тестувати певні технології та схеми [18].

Емулятори дозволяють користувачам створювати моделі комп'ютерів та інших пристроїв і запускати на них оригінальне програмне забезпечення. Емулюються всі основні компоненти пристрою, включаючи процесор, пам'ять і пристрої введення/виведення. У прикладі з Cisco емулятор створює модель маршрутизатора і запускає всередині нього справжню операційну систему Cisco IOS. Таким чином, ви отримуєте повністю функціональний маршрутизатор.

Першою і головною причиною вибору GNS3 є повна функціональність емульованого пристрою. Це означає, що завантаживши той самий

маршрутизатор Cisco, ви отримаєте доступ майже до всіх функцій, які працюють на справжньому маршрутизаторі; згадайте Cisco Packet Tracer, який є лише симулятором, тому значна частина його функціональності недоступна.

Можливість створювати гетерогенні мережі. Це означає, що схеми можуть включати як пристрої Cisco, так і Juniper, Mikrotik, CheckPoint тощо.

Додайте до мережі повноцінні робочі станції та сервери. Знову ж таки, якщо ви пам'ятаєте Cisco Packet Tracer, клієнтські комп'ютери і сервери з дуже обмеженою функціональністю могли використовуватися як кінцеві точки; з GNS3 ви можете додати повноцінні комп'ютери з Windows 7 і Ubuntu; в схемі можна використовувати Windows Server і RedHat. Це робиться або за допомогою технології віртуалізації (VirtualBox або VMWare), або шляхом підключення GNS3 до реальної мережі. Таким чином, в лабораторії можна протестувати встановлення VPN-клієнтів на робочих станціях, аутентифікацію користувачів через AAA-сервер і використання браузерів при підключенні до реального інтернету. Загалом, все можна робити так само, як і в реальному житті.

VirtualBox - це програмне забезпечення, яке імітує справжній комп'ютер, дозволяючи користувачам встановлювати, запускати і використовувати інші операційні системи як звичайні програми. Це як комп'ютер у комп'ютері [19].

Віртуальні машини створюють на комп'ютері своєрідне ізольоване середовище, що складається з віртуальних компонентів реального комп'ютера, таких як жорсткі диски, відеокарти, оперативна пам'ять і контролери різних пристроїв. Таким чином, повністю перевірено, що операційна система, встановлена у VirtualBox, працює на реальному обладнанні.

Способів застосування віртуальних машин є безліч. Розглянемо найпопулярніші серед звичайних користувачів:

- Про інші операційні системи Незалежно від операційної системи, встановленої на вашому комп'ютері, підтримувані операційні системи включають багато дистрибутивів Linux, FreeBSD, MacOS, всі версії Windows, Android тощо. Незалежно від операційної системи, встановленої на вашому

комп'ютері, у VirtualBox можна встановити будь-яку підтримувану операційну систему, включаючи багато дистрибутивів Linux, FreeBSD, MacOS, всі версії Windows, Android тощо. Віртуальна машина працює незалежно, і ви можете експериментувати, як вам подобається. Якщо вона вам більше не потрібна, просто видаліть її, і вона не залишить жодних слідів; Ще один спосіб застосування VirtualBox – необхідність запуску програми, яка не працює у вашій основній ОС або її версії. Наприклад ви працюєте у Windows і вам знадобилася програма, яка доступна лише під Linux. Іноді єдиним виходом буде встановлення Linux у VirtualBox та використання потрібного ПЗ звідти. Детальна ситуація може бути, коли вам потрібна програма, що працює лише під старими версіями Windows;

– Тестування різного програмного забезпечення Вам може знадобитися часто використовувати певні програми або тестувати різні програми, і ви не хочете захищати свою робочу машину. У цьому випадку VirtualBox також може допомогти. Крім того, використовуючи віртуальну машину, ви можете не турбуватися про зараження комп'ютера вірусами під час запуску операційної системи у VirtualBox.

Висновки до розділу 2

Була розроблена модель підмережі, що складається з ядра, розподілу, доступу, DHCP-сервера, підключення до Інтернету та RADIUS-сервера. Також було створено розподіл мережі та таблиці адресації.

Пристрій, що використовується, обирається як найпотужніший на рівні ядра. Описано можливості пристроїв, які можуть бути використані для вирішення поставленої задачі. Також обґрунтовується вибір програмного забезпечення, включаючи симулятор, на якому будується мережа, та операційну систему, яка використовується для забезпечення гетерогенності мережі.

РОЗДІЛ 3 ВИВЧЕННЯ КОНФІГУРАЦІЇ ТА ПРОЄКТУВАННЯ ПІДСИСТЕМ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO

3.1 Конфігурація мережі

В даному пункті розглянуто основні налаштування пристроїв мережі. Спочатку повністю складемо схему, яку спроектували в попередньому розділі (рис.3.1).

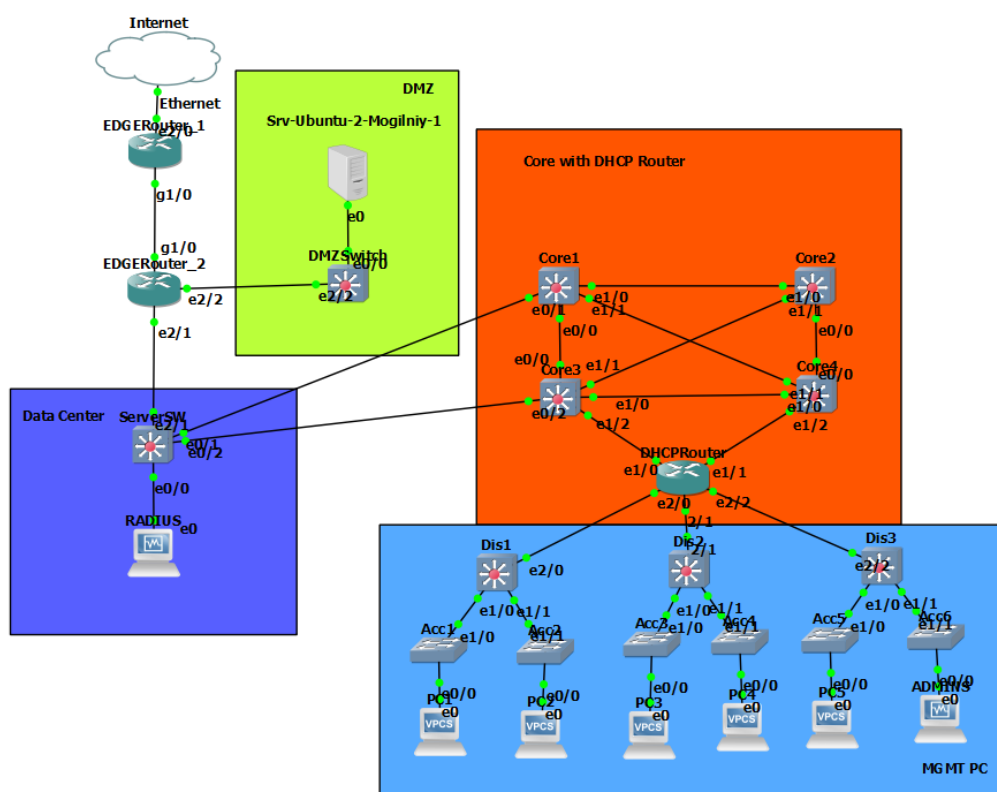


Рис. 3.1 - Схема мережі

Спочатку налаштуємо рівні розподілу та доступу. Для цього використовується протокол VLAN. Пристрої, що належать до різних VLAN, будуть належати до різних підмереж. Але в той же час, VLAN не залежать від місця розташування пристрою, тому пристрої у віддалених місцях можуть перебувати в одній VLAN незалежно від їхнього місцезнаходження.

```

Acc1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Acc1(config)#vlan 10
Acc1(config-vlan)#name OFFICE_1
Acc1(config-vlan)#exit
Acc1(config)#int vlan 10
Acc1(config-if)#ip address 192.168.10.2 255.255.255.0
Acc1(config-if)#no shut
Acc1(config-if)#exit
Acc1(config)#int e1/0
Acc1(config-if)#switchport mode access
Acc1(config-if)#switchport access vlan 10
Acc1(config-if)#exit
Acc1(config)#int e0/0
Acc1(config-if)#switchport mode access
Acc1(config-if)#switchport access vlan 10
Acc1(config-if)#exit

```

Рис. 3.2 - Налаштування VLAN на комутаторі

Всі інші комутатори доступу налаштовуються аналогічно.

Далі необхідно налаштувати розподільчий комутатор і підключити його до комутатора доступу і DHCP-сервера.

```

Dis1(config)#vlan 10
Dis1(config-vlan)#name OFFICE_1
Dis1(config-vlan)#exit
Dis1(config)#vlan 20
Dis1(config-vlan)#name OFFICE_2
Dis1(config-vlan)#exit
Dis1(config)#vlan 30
Dis1(config-vlan)#name DHCP_Router
Dis1(config-vlan)#exit
Dis1(config)#int vlan 30
Dis1(config-if)#ip address 192.168.30.2 255.255.255.0
Dis1(config-if)#no shut
Dis1(config-if)#int vlan 10
Dis1(config-if)#ip address 192.168.10.1 255.255.255.0
Dis1(config-if)#ip helper-address 192.168.30.1
Dis1(config-if)#no shut
Dis1(config-if)#exit
Dis1(config)#int vlan 20
Dis1(config-if)#ip address 192.168.20.1 255.255.255.0
Dis1(config-if)#ip helper-address 192.168.30.1
Dis1(config-if)#no shut
Dis1(config-if)#exit
Dis1(config)#int e1/0
Dis1(config-if)#description LINK TO ACC1
Dis1(config-if)#switchport mode access
Dis1(config-if)#switchport access vlan 10
Dis1(config-if)#no shut
Dis1(config-if)#exit
Dis1(config)#int e1/1
Dis1(config-if)#description LINK_TO_ACC2
Dis1(config-if)#switchport mode access
Dis1(config-if)#switchport access vlan 20
Dis1(config-if)#no shut
Dis1(config-if)#int e2/0
Dis1(config-if)#description LINK_TO_DHCPROUTER
Dis1(config-if)#switchport mode access
Dis1(config-if)#switchport access vlan 30
Dis1(config-if)#no shut
Dis1(config-if)#exit

```

Рис. 3.3 - Налаштування VLAN на комутаторі

Наступним кроком буде налаштування динамічної маршрутизації за допомогою протоколу OSPF.

Розглянемо це трохи детальніше: Команда `network` не налаштовує мережу, на яку маршрутизатор здійснює трансляцію, а визначає інтерфейси, задіяні в цьому процесі.

Всі інтерфейси маршрутизатора з IP-адресами в діапазоні 192.168.10.0/24 (192.168.10.0-192.168.10.255) включені в цей процес. Це означає, що з цих інтерфейсів надсилаються повідомлення Hello, через них встановлюються відносини сусідства і надсилаються оновлення топології мережі.

```
Dis1(config)#router ospf 1
Dis1(config-router)#network 192.168.10.0 0.0.0.255 area 0
Dis1(config-router)#network 192.168.20.0 0.0.0.255 area 0
Dis1(config-router)#network 192.168.30.0 0.0.0.255 area 0
Dis1(config-router)#exit
Dis1(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.2
Dis1(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.2
Dis1(config)#ip route 0.0.0.0 0.0.0.0 192.168.30.1
```

Рис. 3.4 - OSPF на комутаторі Dis1

Також виконаємо аналогічне налаштування маршрутизації на сервері DHCP.

```
DHCPRouter(config)#int e2/0
DHCPRouter(config-if)#ip address 192.168.30.1 255.255.255.0
DHCPRouter(config-if)#no shut
DHCPRouter(config-if)#exit
DHCPRouter(config)#int e2/1
DHCPRouter(config-if)#ip address 192.168.60.1 255.255.255.0
DHCPRouter(config-if)#no shut
DHCPRouter(config-if)#exit
DHCPRouter(config)#int e2/2
DHCPRouter(config-if)#ip address 192.168.90.1 255.255.255.0
DHCPRouter(config-if)#no shut
DHCPRouter(config-if)#exit
DHCPRouter(config)#int e1/0
DHCPRouter(config-if)#ip address 192.168.3.1 255.255.255.0
DHCPRouter(config-if)#no shut
DHCPRouter(config-if)#exit
DHCPRouter(config)#int e1/1
DHCPRouter(config-if)#ip address 192.168.4.1 255.255.255.0
DHCPRouter(config-if)#no shut
DHCPRouter(config-if)#exit
DHCPRouter(config)#router ospf 1
DHCPRouter(config-router)#network 192.168.10.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.20.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.30.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.40.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.50.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.60.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.70.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.80.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.90.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.3.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.4.0 0.0.0.255 area 0
DHCPRouter(config-router)#exit
DHCPRouter(config)#ip route 0.0.0.0 0.0.0.0 192.168.30.2
DHCPRouter(config)#ip route 0.0.0.0 0.0.0.0 192.168.60.2
DHCPRouter(config)#ip route 0.0.0.0 0.0.0.0 192.168.90.2
DHCPRouter(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.2
DHCPRouter(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.2
```

Рис.3.5 - Налаштування DHCP-сервера

Перейдемо до налаштування DHCP протоколу. Який забезпечить автоматичне призначення IP-адреси до робочих станцій.

```
DHCPRouter(config)#ip dhcp pool OFFICE_1
DHCPRouter(dhcp-config)#network 192.168.10.0 255.255.255.0
DHCPRouter(dhcp-config)#default-router 192.168.10.1
DHCPRouter(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCPRouter(dhcp-config)#exit
DHCPRouter(config)#ip dhcp pool OFFICE_2
DHCPRouter(dhcp-config)#network 192.168.20.0 255.255.255.0
DHCPRouter(dhcp-config)#default-router 192.168.20.1
DHCPRouter(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCPRouter(dhcp-config)#exit
DHCPRouter(config)#ip dhcp pool OFFICE_3
DHCPRouter(dhcp-config)#network 192.168.40.0 255.255.255.0
DHCPRouter(dhcp-config)#default-router 192.168.40.1
DHCPRouter(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCPRouter(dhcp-config)#exit
DHCPRouter(config)#ip dhcp pool OFFICE_4
DHCPRouter(dhcp-config)#network 192.168.50.0 255.255.255.0
DHCPRouter(dhcp-config)#default-router 192.168.50.1
DHCPRouter(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCPRouter(dhcp-config)#exit
DHCPRouter(config)#ip dhcp pool OFFICE_5
DHCPRouter(dhcp-config)#network 192.168.70.0 255.255.255.0
DHCPRouter(dhcp-config)#default-router 192.168.70.1
DHCPRouter(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCPRouter(dhcp-config)#exit
DHCPRouter(config)#ip dhcp pool ADMINS
DHCPRouter(dhcp-config)#network 192.168.80.0 255.255.255.0
DHCPRouter(dhcp-config)#default-router 192.168.80.1
DHCPRouter(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCPRouter(dhcp-config)#exit
DHCPRouter(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
DHCPRouter(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.10
DHCPRouter(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.10
DHCPRouter(config)#ip dhcp excluded-address 192.168.50.1 192.168.50.10
DHCPRouter(config)#ip dhcp excluded-address 192.168.70.1 192.168.70.10
DHCPRouter(config)#ip dhcp excluded-address 192.168.80.1 192.168.80.10
DHCPRouter(config)#
```

Рис.3.6 - Налаштування DHCP-сервера

Ви наблизилися до ядра мережі. Ядро необхідне для пересилання пакетів через мережу на високій швидкості, тому налаштуйте його за допомогою маршрутизації: створіть дві VLAN, одну для основної VLAN і резервну на випадок, якщо основна VLAN вийде з ладу і її потрібно буде відремонтувати.

```
Core1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Core1(config)#vlan 4
Core1(config-vlan)#exit
Core1(config)#int vlan 4
Core1(config-if)#ip address 192.168.4.5 255.255.255.0
Core1(config-if)#no shut
Core1(config-if)#exit
Core1(config)#int e1/1
Core1(config-if)#switchport mode access
Core1(config-if)#switchport access vlan 4
Core1(config-if)#exit
Core1(config)#int e1/0
Core1(config-if)#switchport mode access
Core1(config-if)#switchport access vlan 4
Core1(config-if)#exit
Core1(config)#int e0/1
Core1(config-if)#switchport mode access
Core1(config-if)#switchport access vlan 4
Core1(config-if)#exit
Core1(config)#router ospf 1
Core1(config-router)#network 192.168.4.0 0.0.0.255 area 0
Core1(config-router)#exit
Core1(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.2
Core1(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.6
Core1(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.3
```

Рис.3.7 - Налаштування Core1

Перейдемо до інтернет-з'єднання, яке дозволяє мережам отримати доступ до інтернету. NAT може допомогти в цьому; NAT перетворює приватні адреси на публічні. Це дозволяє пристроям з приватними IPv4-адресами отримувати доступ до ресурсів за межами приватної мережі. NAT виявився корисним способом захисту публічних IPv4-адрес у поєднанні з приватними IPv4-адресами. Одна публічна IPv4-адреса може використовуватися сотнями або тисячами пристроїв, кожен з яких має приватну IPv4-адресу; перевага NAT полягає в тому, що вона приховує внутрішні IPv4-адреси від зовнішньої мережі, тим самим підвищуючи конфіденційність і безпеку мережі.

Маршрутизатори з підтримкою NAT можна налаштувати з однією або декількома дійсними публічними IPv4-адресами. Ці публічні адреси називаються пулами NAT. Коли пристрій у внутрішній мережі надсилає трафік за межі мережі, маршрутизатор з підтримкою NAT транлює внутрішню IPv4-адресу пристрою на публічну адресу в пулі NAT. Для зовнішніх пристроїв весь трафік, що входить і виходить з мережі, має публічну IPv4-адресу.

```
EDGERouter_1(config)#int e2/0
EDGERouter_1(config-if)#ip add
EDGERouter_1(config-if)#ip address 192.168.1.50 255.255.255.0
EDGERouter_1(config-if)#no shut
EDGERouter_1(config-if)#exit
EDGERouter_1(config)#
*Jun  5 16:48:47.471: %LINK-3-UPDOWN: Interface Ethernet2/0, changed state to up
*Jun  5 16:48:48.471: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/0, changed state to up
EDGERouter_1(config)#int g1/0
EDGERouter_1(config-if)#ip add
EDGERouter_1(config-if)#ip address 192.168.2.1 255.255.255.0
EDGERouter_1(config-if)#no shut
EDGERouter_1(config-if)#ip
*Jun  5 16:49:25.671: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*Jun  5 16:49:26.671: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
EDGERouter_1(config-if)#ip nat inside

*Jun  5 16:49:34.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface NV10, changed state to up
EDGERouter_1(config-if)#exit
EDGERouter_1(config)#int e2/0
EDGERouter_1(config-if)#ip nat outside
EDGERouter_1(config)#exit
EDGERouter_1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
EDGERouter_1(config)#acce
EDGERouter_1(config)#access-list 1 per
EDGERouter_1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.20.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.40.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.50.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.70.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.80.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.3.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.4.0 0.0.0.255
EDGERouter_1(config)#s 192.168.1.51 192.168.1.100 netmask 255.255.255.0
EDGERouter_1(config)#ip nat inside source list 1 pool global-ips
EDGERouter_1(config)#router ospf 1
EDGERouter_1(config-router)#network 192.168.1.0 0.0.0.255 area 0
EDGERouter_1(config-router)#network 192.168.2.0 0.0.0.255 area 0
EDGERouter_1(config-router)#network 192.168.3.0 0.0.0.255 area 0
EDGERouter_1(config-router)#exit
```

Рис.3.8 - Конфігурація NAT та списків доступу

Списки доступу створюються для кращої безпеки мережі. Списки доступу - це універсальний і потужний механізм фільтрації. За допомогою ACL можна вирішити, кому призначити певні політики, а кому ні, кому брати участь у певних процесах, а кому ні, кому обмежити до 56к, а кому до 56 метрів.

Також необхідно налаштувати віддалений доступ до пристрою. Для цього є два способи: ssh або telnet. Для цієї мережі використовується SSHv2. Це пов'язано з тим, що SSHv2 створює захищений канал між пристроями. Тому, навіть якщо пакети будуть перехоплені, паролі та логіни будуть надійно зашифровані і не будуть відомі злоумиснику.

```
Acc2(config)#enable secret office2
Acc2(config)#username office2 privilege 15 secret rootnet
Acc2(config)#service password-encryption
Acc2(config)#banner exec c
Enter TEXT message. End with the character 'c'.
Acc2
Acc2(config)#ip domain-name marvelcs
Acc2(config)#crypto key generate rsa modulus 1024
The name for the keys will be: Acc2.marvelcs

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

Acc2(config)#ip ssh version 2
Acc2(config)#ip ssh time-out 15
Acc2(config)#ip ssh logging events
Acc2(config)#line vty 0 4
Acc2(config-line)#transport input ssh
Acc2(config-line)#transport output ssh
Acc2(config-line)#logging synchronous
Acc2(config-line)#login local
Acc2(config-line)#exec-timeout 5 0
Acc2(config-line)#exit
Acc2(config)#
*Jun  4 13:43:03.831: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Рис.3.9 - Налаштування SSHv2

Наступним кроком буде налаштування сервера RADIUS. Для початку налаштуйте автентифікацію AAA, щоб дозволити використання RADIUS: Відповідно до налаштувань політики AAA, пристрій запитує логін і пароль і надсилає їх на сервер RADIUS.

```

ServerSW(config)#aaa ne
ServerSW(config)#aaa new-model
ServerSW(config)#aaa au
ServerSW(config)#aaa authen
ServerSW(config)#aaa authentication lo
ServerSW(config)#aaa authentication login def
ServerSW(config)#aaa authentication login default gr
ServerSW(config)#aaa authentication login default group ra
ServerSW(config)#aaa authentication login default group radius n
ServerSW(config)#aaa authentication login default group radius none
ServerSW(config)#rad
ServerSW(config)#radius se
ServerSW(config)#radius server TEST
ServerSW(config-radius-server)#address ipv4 192.168.3.11
ServerSW(config-radius-server)#key WinRadius
ServerSW(config-radius-server)#end

```

Рис.3.10 - Налаштування аутентифікації AAA.

На вкладці «Властивості» змініть режим сумісності на Windows 7 і поставте галочку біля пункту «Відкрити програму від імені адміністратора».

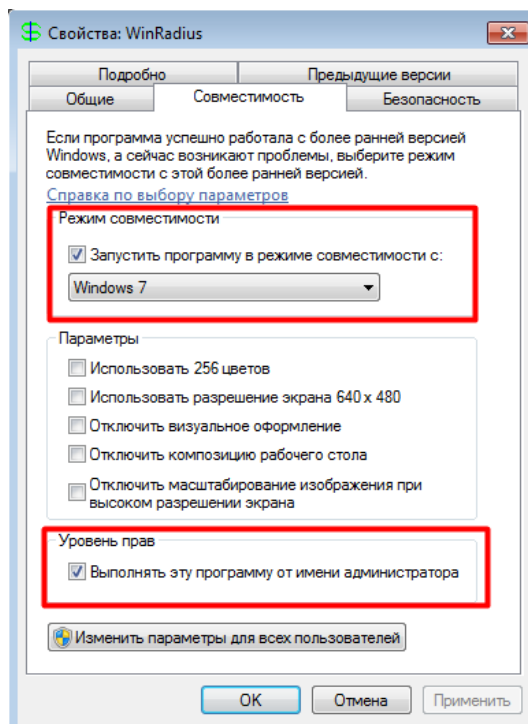


Рис.3.11 - Зміна властивостей

Після запуску програми потрібно створити користувачів для підключення до пристроїв у мережі.

Рис.3.12 - Створення користувача

Далі підключимося до комутатора ServerSW за допомогою користувача, створеного на попередньому кроці.

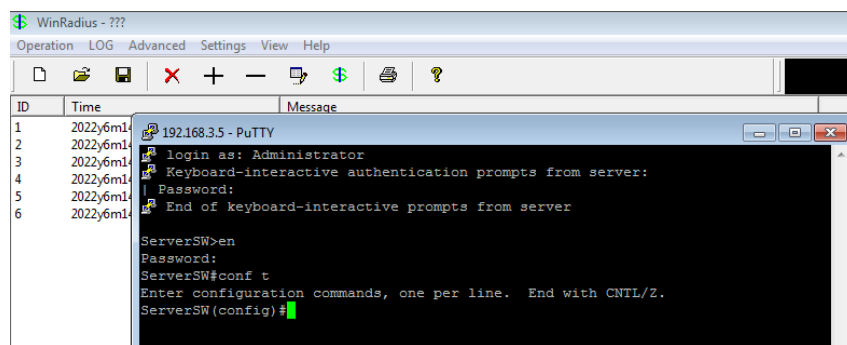


Рис.3.13 - Вхід до обладнання

Як ви можете бачити (Рисунок 3.13), вхід в систему пройшов успішно, і основні команди для перевірки функціональності також були введені.

3.2 Тестували підсистему безпеки корпоративної мережі на базі обладнання Cisco.

Тестування підсистем безпеки корпоративної мережі проводиться на предмет відповідності поставленим завданням.

Для початку перевіримо правильність налаштування маршрутизації протоколу OSPF (Рис 3.14).

```
DHCPRouter#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.90.2	1	FULL/DR	00:00:37	192.168.90.2	Ethernet2/2
192.168.60.2	1	FULL/BDR	00:00:35	192.168.60.2	Ethernet2/1
192.168.30.2	1	FULL/BDR	00:00:33	192.168.30.2	Ethernet2/0
192.168.4.2	1	FULL/BDR	00:00:37	192.168.4.2	Ethernet1/1
192.168.3.2	1	FULL/BDR	00:00:30	192.168.3.2	Ethernet1/0

Рис. 3.14 - Перевірка конфігурації OSPF

За допомогою Wireshark перевіримо розсилання Hello-повідомлення.

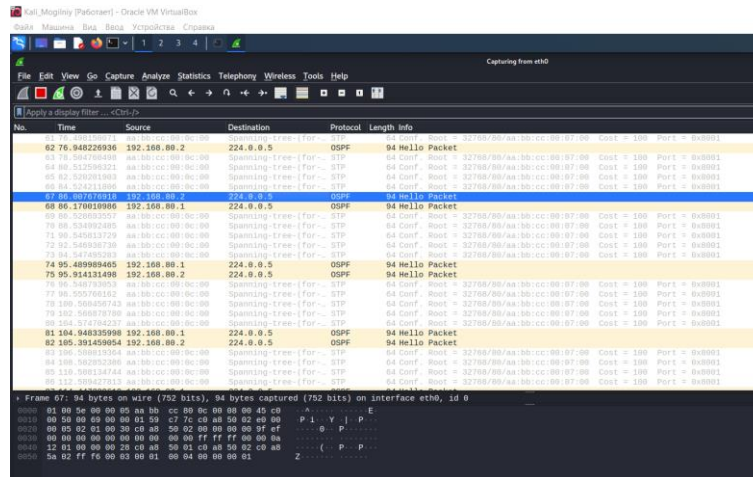


Рис. 3.15 - Розсилання пакетів

Проведемо перевірку на працездатність мережі автоматично призначати IP-адреси робочим станція через DHCP (Рис.3.16 - Рис.3.19).

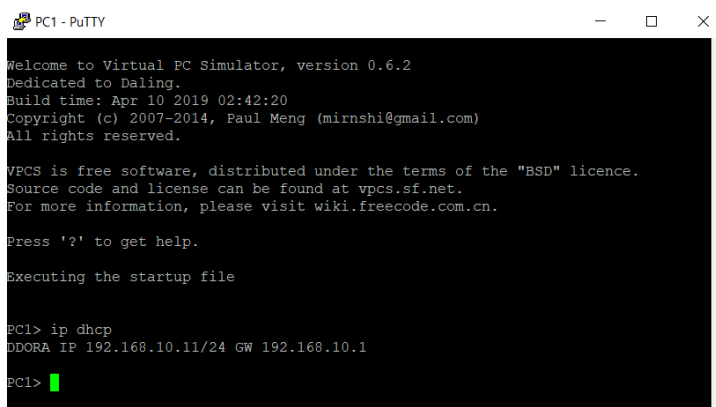


Рис. 3.16 - Отримання DHCP-адреси

```

Kali_Mogilniy [Роботаєт] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# dhclient -r eth0
# dhclient -v eth0
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:95:bd:54
Sending on   LPF/eth0/08:00:27:95:bd:54
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 6
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 12
DHCPOFFER of 192.168.80.11 from 192.168.80.1
DHCPREQUEST for 192.168.80.11 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.80.11 from 192.168.80.1
bound to 192.168.80.11 -- renewal in 37161 seconds.

```

Рис. 3.17 - Отримання DHCP-адреси

```

DHCPRouter#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration    Type
                Hardware address/
                User name
192.168.10.11    0100.5079.6668.04 Jun 06 2022 06:01 PM Automatic
192.168.20.11    0100.5079.6668.00 Jun 06 2022 06:03 PM Automatic
192.168.40.11    0100.5079.6668.01 Jun 06 2022 06:03 PM Automatic
192.168.50.11    0100.5079.6668.02 Jun 06 2022 06:04 PM Automatic
192.168.70.11    0100.5079.6668.03 Jun 06 2022 06:04 PM Automatic
192.168.80.11    0108.0027.95d2.ee Jun 06 2022 06:03 PM Automatic

```

Рис. 3.18 - Підключення робочих станцій

```

DHCPRouter#show ip dhcp pool

Pool OFFICE_1 :
Utilization mark (high/low)    : 100 / 0
Subnet size (first/next)        : 0 / 0
Total addresses                  : 254
Leased addresses                 : 1
Pending event                    : none
1 subnet is currently in the pool :
Current index  IP address range      Leased addresses
192.168.10.12  192.168.10.1 - 192.168.10.254  1

Pool OFFICE_2 :
Utilization mark (high/low)    : 100 / 0
Subnet size (first/next)        : 0 / 0
Total addresses                  : 254
Leased addresses                 : 1
Pending event                    : none
1 subnet is currently in the pool :
Current index  IP address range      Leased addresses
192.168.20.12  192.168.20.1 - 192.168.20.254  1

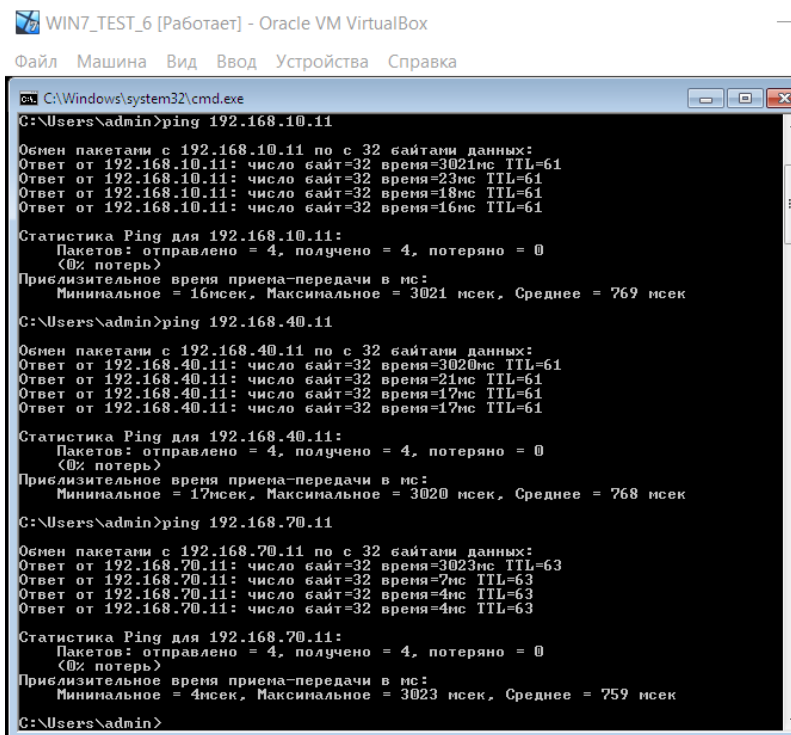
Pool OFFICE_3 :
Utilization mark (high/low)    : 100 / 0
Subnet size (first/next)        : 0 / 0
Total addresses                  : 254
Leased addresses                 : 1
Pending event                    : none
1 subnet is currently in the pool :
Current index  IP address range      Leased addresses
192.168.40.12  192.168.40.1 - 192.168.40.254  1

Pool OFFICE_4 :
Utilization mark (high/low)    : 100 / 0
Subnet size (first/next)        : 0 / 0
Total addresses                  : 254
Leased addresses                 : 1
Pending event                    : none
1 subnet is currently in the pool :
Current index  IP address range      Leased addresses
192.168.50.12  192.168.50.1 - 192.168.50.254  1

```

Рис. 3.19 - Перевірка пулів

Як ми бачимо всі робочі станції отримали свої IP-адреси, тому варто перевірити зв'язок між ними (Рис.3.20).



```
C:\Windows\system32\cmd.exe
C:\Users\admin>ping 192.168.10.11

Обмен пакетами с 192.168.10.11 по 32 байтам данных:
Ответ от 192.168.10.11: число байт=32 время=3021мс TTL=61
Ответ от 192.168.10.11: число байт=32 время=23мс TTL=61
Ответ от 192.168.10.11: число байт=32 время=18мс TTL=61
Ответ от 192.168.10.11: число байт=32 время=16мс TTL=61

Статистика Ping для 192.168.10.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 16мсек, Максимальное = 3021 мсек, Среднее = 769 мсек

C:\Users\admin>ping 192.168.40.11

Обмен пакетами с 192.168.40.11 по 32 байтам данных:
Ответ от 192.168.40.11: число байт=32 время=3020мс TTL=61
Ответ от 192.168.40.11: число байт=32 время=21мс TTL=61
Ответ от 192.168.40.11: число байт=32 время=17мс TTL=61
Ответ от 192.168.40.11: число байт=32 время=17мс TTL=61

Статистика Ping для 192.168.40.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 17мсек, Максимальное = 3020 мсек, Среднее = 768 мсек

C:\Users\admin>ping 192.168.70.11

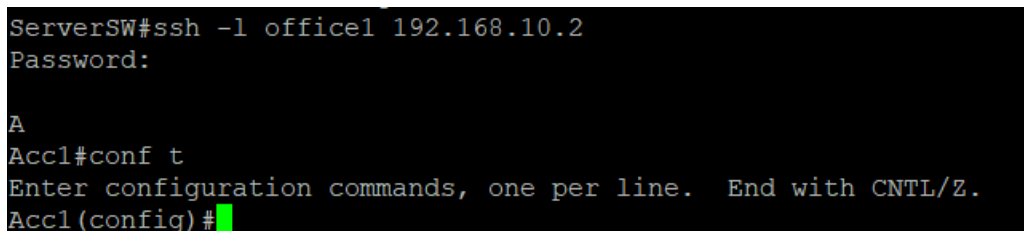
Обмен пакетами с 192.168.70.11 по 32 байтам данных:
Ответ от 192.168.70.11: число байт=32 время=3023мс TTL=63
Ответ от 192.168.70.11: число байт=32 время=7мс TTL=63
Ответ от 192.168.70.11: число байт=32 время=4мс TTL=63
Ответ от 192.168.70.11: число байт=32 время=4мс TTL=63

Статистика Ping для 192.168.70.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 4мсек, Максимальное = 3023 мсек, Среднее = 759 мсек

C:\Users\admin>
```

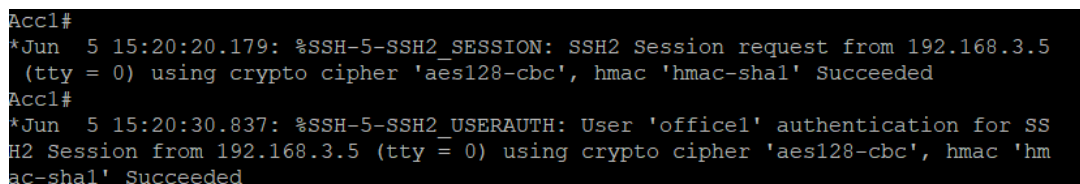
Рис. 3.20 - Перевірка зв'язку між робочими станціями

Зробимо перевірку віддаленого доступу в мережі. Для цього спробуємо підключитися з ServerSW до Acc1 (Рис.3.21 – Рис.3.23).



```
ServerSW#ssh -l office1 192.168.10.2
Password:
A
Acc1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Acc1(config)#
```

Рис. 3.21 - Перевірка зв'язку між робочими станціями



```
Acc1#
*Jun  5 15:20:20.179: %SSH-5-SSH2_SESSION: SSH2 Session request from 192.168.3.5
(tty = 0) using crypto cipher 'aes128-cbc', hmac 'hmac-shal' Succeeded
Acc1#
*Jun  5 15:20:30.837: %SSH-5-SSH2_USERAUTH: User 'office1' authentication for SS
H2 Session from 192.168.3.5 (tty = 0) using crypto cipher 'aes128-cbc', hmac 'hm
ac-shal' Succeeded
```

Рис. 3.22 - Успішність підключення

```
(root@kali)-[/home/kali]
# ssh -l marvelcs 192.168.80.2
(marvelcs@192.168.80.2) Password:
(marvelcs@192.168.80.2) Password:

A
Acc6#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Acc6(config)#
```

Рис. 3.22 - Підключення через Kali

Спробуємо перехватити SSH-пакети та отримати логіни та паролі(Рис.3.23).

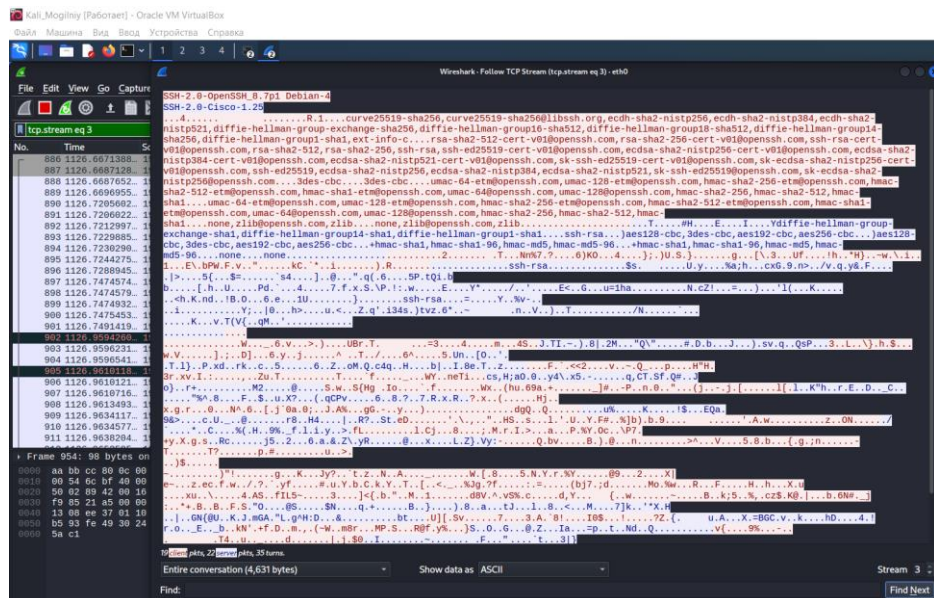


Рис. 3.23 - Пакет SSH

Так як SSH має високий рівень шифрування, то паролі та логіни дізнатися не зможемо.

3.3 Аналіз результатів тестування

Як і планувалося, всі раніше згадані вимоги були виконані. У майбутньому ця мережа може бути розширена і вдосконалена під конкретні завдання. Для цього є всілякі можливості: DHCP допомагає встановлювати нові робочі станції та пристрої, сервер допомагає конфігурувати та

контролювати нові пристрої, базовий рівень використовує маршрутизатори CISCO і тому є гнучким для майбутніх налаштувань.

Ще однією перевагою цієї мережі є наявність двох VLAN на рівні ядра. Якщо одна з них виходить з ладу, інша перебирає на себе відповідальність і продовжує роботу першої VLAN.

Висновки до розділу 3

В даному розділі було описано базові налаштування всіх пристроїв даної мережі. Була налаштована статична та динамічна (DHCP) маршрутизація. Для зручності використання та налаштування пристроїв було надано кожному особисту назву.

На маршрутизаторах було налаштовано протокол SSH для віддаленого доступу до них. Провели маршрутизацію за допомогою протоколу OSPF. Також завдяки RADIUS ми вдосконалили безпеку мережі захистивши її від несанкціонованого доступу, зашифрувавши паролі користувачів.

Було проведено аналіз тестування та описано можливості масштабування та покращення мережі.

ВИСНОВКИ

У дипломному проєкті спроектовано корпоративну модель комп'ютерної мережі на базі обладнання Cisco. Були враховані всі вимоги до проєкту.

Для початку було обрано доступні технології для побудови мережі. Зокрема, було обрано графічний емулятор GNS3, операційні системи Windows 7 та 10, протоколи RADIUS, OSPF, DHCP, NAT, SSHv2 та VLAN.

Оскільки корпоративна мережа складається з великої кількості пристроїв, вона розбивається на локальні мережі; VLAN ділять підсистему на окремі широкомовні домени. Це означає, що широкомовні повідомлення будуть прийматися тільки пристроями, що належать до тієї ж VLAN. Побудова системи з використанням технології VLAN дозволила зменшити обсяг широкомовного трафіку в мережі, тим самим знизити навантаження на мережеве обладнання і підвищити загальну продуктивність системи.

Схема використовує модель корпоративної мережі, яка гарантує продуктивність і надійність мережі та складається з п'яти рівнів: Ядро з DHCP-сервером, центр обробки даних, демілітаризована зона (DMZ), розподіл і доступ та підключення до Інтернету.

Ядро забезпечувало швидку передачу даних між комутаторами; також було встановлено DHCP-сервер для автоматичного призначення IP-адрес та інших параметрів пристроям.

Data Center зберіг користувачів та паролі завдяки протоколу RADIUS. Також було додано комутатор L3 який підтримував зв'язок з мережею.

Рівень розподілу забезпечив маршрутизацію мережі, також було налаштовано DHCP-relay для отримання IP-адреси між VLAN.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Корпоративна мережа [Електронний ресурс] –
https://uk.wikipedia.org/wiki/Корпоративна_мережа
2. NAT [Електронний ресурс] – <https://uk.wikipedia.org/wiki/NAT>
3. Протокол OSFP [Електронний ресурс] – Режим доступу до ресурсу:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xen-16/iro-xe-16-book/iro-cfg.html
4. CISCO DHCP [Електронний ресурс] – Режим доступу до ресурсу:
<https://blog.sedicomm.com/2018/03/19/konfiguratsiya-dhcp-cisco/>
5. DNS Server [Електронний ресурс] - https://freehost.com.ua/ukr/faq/faq/chtotakoe-dns-i-zachem-on-nuzhen/?gad_source=1&gclid=Cj0KCQiA1Km7BhC9ARIsAFZfEluGafr2iEYwNo-ib8EdCY7arjopd_G_IoM0PnpKulEwKsCLlYXzicAaAg2UEALw_wcB
6. SSHv2 [Електронний ресурс] - <https://community.cisco.com/t5/security-knowledge-base/sshv2/ta-p/3114418>
7. Ієрархічна модель мережі від Cisco [Електронний ресурс] -
<http://www.telesphera.net/blog/model-mereghi-vid-cisco.html>
8. SSH [Електронний ресурс] – <https://freehost.com.ua/ukr/faq/wiki/chtotakoe-ssh/>
9. Windows XP [Електронний ресурс] -
https://en.wikipedia.org/wiki/Windows_XP#:~:text=Windows%20XP%20is%20an%20operating,NT%20family%20of%20operating%20systems.&text=It%20was%20Microsoft%27s%20operating%20system,Windows%20Vista%20in%20February%202007.
10. RADIUS [Електронний ресурс] -
<https://www.fortinet.com/resources/cyberglossary/radius-protocol>
11. Windows 7 [Електронний ресурс] -https://ru.wikipedia.org/wiki/Windows_7
12. Linux [Електронний ресурс] - <https://dou.ua/forums/topic/41333/>
13. Ubuntu [Електронний ресурс] - <https://ubuntu.com>
14. Хешування MD5 [Електронний ресурс] – <https://habr.com/ru/sandbox/26876/>

15. Налаштування CISCO port-security [Електронний ресурс] – Режим доступу до ресурсу: <https://linkmeup.gitbook.io/sdsm/4.-stp/06-port-security>
16. Cisco IOS - Privilege Levels [Електронний ресурс] - https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/sec/b_166_sec_9400_cg/controlling_switch_access_with_passwords_and_privilege_levels.pdf
17. GNS3 [Електронний ресурс] - <https://gns3.com/initiatives/gns3-2-2-17-released>
18. VirtualBox [Електронний ресурс] - https://www.virtualbox.org/wiki/Download_Old_Builds_6_1
19. Wireshark [Електронний ресурс] - <https://en.wikipedia.org/wiki/Wireshark>

ДОДАТКИ

Комутатор Dis1

Dis1

Dis1#show running-config	!
Building configuration...	no ip domain-lookup
	no ipv6 cef
	ipv6 multicast rpf use-bgp
	!
	!
Current configuration : 2194 bytes	!
!	!
version 15.1	!
service timestamps debug datetime msec	!
service timestamps log datetime msec	!
no service password-encryption	spanning-tree mode pvst
service compress-config	spanning-tree extend system-id
!	!
hostname Dis1	!
!	!
boot-start-marker	!
boot-end-marker	vlan internal allocation policy ascending
!	!
!	ip tcp synwait-time 5
logging discriminator EXCESS severity drops 6	!
msg-body drops EXCESSCOLL	!
logging buffered 50000	!
logging console discriminator EXCESS	!
!	!
no aaa new-model	!
no ip icmp rate-limit unreachable	interface Ethernet0/0
!	duplex auto
ip cef	!
!	interface Ethernet0/1

duplex auto	!
!	interface Ethernet2/1
interface Ethernet0/2	duplex auto
duplex auto	!
!	interface Ethernet2/2
interface Ethernet0/3	duplex auto
duplex auto	!
!	interface Ethernet2/3
interface Ethernet1/0	duplex auto
description LINK_TO_ACC1	!
switchport access vlan 10	interface Ethernet3/0
switchport mode access	duplex auto
duplex auto	!
!	interface Ethernet3/1
interface Ethernet1/1	duplex auto
description LINK_TO_ACC2	!
switchport access vlan 20	interface Ethernet3/2
switchport mode access	duplex auto
duplex auto	!
!	interface Ethernet3/3
interface Ethernet1/2	duplex auto
duplex auto	!
!	interface Vlan1
interface Ethernet1/3	no ip address
duplex auto	shutdown
!	!
interface Ethernet2/0	interface Vlan10
description LINK_TO_DHCPROUTER	ip address 192.168.10.1 255.255.255.0
switchport access vlan 30	ip helper-address 192.168.30.1
switchport mode access	!
duplex auto	interface Vlan20

```
ip address 192.168.20.1 255.255.255.0
```

```
ip helper-address 192.168.30.1
```

```
!
```

```
interface Vlan30
```

```
ip address 192.168.30.2 255.255.255.0
```

```
!
```

```
router ospf 1
```

```
network 192.168.10.0 0.0.0.255 area 0
```

```
network 192.168.20.0 0.0.0.255 area 0
```

```
network 192.168.30.0 0.0.0.255 area 0
```

```
!
```

```
no ip http server
```

```
!
```

```
ip route 0.0.0.0 0.0.0.0 192.168.10.2
```

```
ip route 0.0.0.0 0.0.0.0 192.168.20.2
```

```
ip route 0.0.0.0 0.0.0.0 192.168.30.1
```

```
control-plane
```

```
!
```

```
!
```

```
line con 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
logging synchronous
```

```
line aux 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
logging synchronous
```

```
line vty 0 4
```

```
login
```

```
!
```

```
endprivilege exec level 1 show running-config
```

```
privilege exec level 1 show interfaces
```

```
privilege exec level 1 show
```

```
banner
```

```
login
```

```
^C=====
```

```
Device hostname -$(R_1)
```

```
Your connection is -$(line)
```

```
Enter Admin's LOGIN and Password
```

```
=====^C
```

```
!
```

```
line con 0
```

```
privilege level 15
```

```
logging synchronous
```

```
login local
```

```
line aux 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
logging synchronous
```

```
line vty 0 4
```

```
login local
```

```
transport input ssh
```

```
!
```

```
End
```

Маршрутизатор DHCPRouter	!
DHCPRouter	!
DHCPRouter#show running-config	aaa session-id common
Building configuration...	!
	!
Current configuration : 3899 bytes	!
!	ip source-route
! Last configuration change at 17:34:12 UTC Tue	no ip icmp rate-limit unreachable
Jun 14 2022 by Administrator	ip cef
!	!
upgrade fpd auto	!
version 15.0	ip dhcp excluded-address 192.168.10.1
service timestamps debug datetime msec	192.168.10.10
service timestamps log datetime msec	ip dhcp excluded-address 192.168.20.1
service password-encryption	192.168.20.10
!	ip dhcp excluded-address 192.168.40.1
hostname DHCPRouter	192.168.40.10
!	ip dhcp excluded-address 192.168.50.1
boot-start-marker	192.168.50.10
boot-end-marker	ip dhcp excluded-address 192.168.70.1
!	192.168.70.10
enable secret 5	ip dhcp excluded-address 192.168.80.1
\$1\$..BA\$Qi.HzKJm/CAV7JAdcFtNK1	192.168.80.10
!	ip dhcp excluded-address 192.168.3.1
aaa new-model	192.168.3.10
!	!
!	ip dhcp pool OFFICE_1
!	network 192.168.10.0 255.255.255.0
aaa authentication login default group radius none	default-router 192.168.10.1
	dns-server 8.8.8.8 8.8.4.4

!	!
ip dhcp pool OFFICE_2	no ip domain lookup
network 192.168.20.0 255.255.255.0	ip domain name marvelcs
default-router 192.168.20.1	no ipv6 cef
dns-server 8.8.8.8 8.8.4.4	!
!	multilink bundle-name authenticated
ip dhcp pool OFFICE_3	!
network 192.168.40.0 255.255.255.0	!
default-router 192.168.40.1	!
dns-server 8.8.8.8 8.8.4.4	!
!	!
ip dhcp pool OFFICE_4	!
network 192.168.50.0 255.255.255.0	!
default-router 192.168.50.1	!
dns-server 8.8.8.8 8.8.4.4	username dhcproute privilege 15 secret 5
!	\$1\$tyyR\$p6ZA1p3RyB2/JH16nmcsG/
ip dhcp pool OFFICE_5	!
network 192.168.70.0 255.255.255.0	redundancy
default-router 192.168.70.1	!
dns-server 8.8.8.8 8.8.4.4	!
!	ip tcp synwait-time 5
ip dhcp pool ADMINS	ip ssh time-out 15
network 192.168.80.0 255.255.255.0	ip ssh logging events
default-router 192.168.80.1	ip ssh version 2
dns-server 8.8.8.8 8.8.4.4	!
!	!
ip dhcp pool RADIUS	!
network 192.168.3.0 255.255.255.0	!
default-router 192.168.3.1	!
dns-server 8.8.8.8 8.8.4.4	!
!	!

!	duplex half
interface FastEthernet0/0	!
no ip address	!
shutdown	interface Ethernet2/1
duplex half	ip address 192.168.60.1 255.255.255.0
!	duplex half
!	!
interface Ethernet1/0	!
ip address 192.168.3.1 255.255.255.0	interface Ethernet2/2
duplex half	ip address 192.168.90.1 255.255.255.0
!	duplex half
!	!
interface Ethernet1/1	!
ip address 192.168.4.1 255.255.255.0	interface Ethernet2/3
duplex half	no ip address
!	shutdown
!	duplex half
interface Ethernet1/2	!
no ip address	!
shutdown	!
duplex half	router ospf 1
!	log-adjacency-changes
!	network 192.168.3.0 0.0.0.255 area 0
interface Ethernet1/3	network 192.168.4.0 0.0.0.255 area 0
no ip address	network 192.168.10.0 0.0.0.255 area 0
shutdown	network 192.168.20.0 0.0.0.255 area 0
duplex half	network 192.168.30.0 0.0.0.255 area 0
!	network 192.168.40.0 0.0.0.255 area 0
!	network 192.168.50.0 0.0.0.255 area 0
interface Ethernet2/0	network 192.168.60.0 0.0.0.255 area 0
ip address 192.168.30.1 255.255.255.0	network 192.168.70.0 0.0.0.255 area 0

network 192.168.80.0 0.0.0.255 area 0	shutdown
network 192.168.90.0 0.0.0.255 area 0	!
!	banner exec ^C
ip forward-protocol nd	DHCPRoute
no ip http server	!
no ip http secure-server	line con 0
!	exec-timeout 0 0
!	privilege level 15
ip route 0.0.0.0 0.0.0.0 192.168.30.2	logging synchronous
ip route 0.0.0.0 0.0.0.0 192.168.60.2	stopbits 1
ip route 0.0.0.0 0.0.0.0 192.168.90.2	line aux 0
ip route 0.0.0.0 0.0.0.0 192.168.3.2	exec-timeout 0 0
ip route 0.0.0.0 0.0.0.0 192.168.4.2	privilege level 15
!	logging synchronous
no cdp log mismatch duplex	stopbits 1
!	line vty 0 4
!	exec-timeout 5 0
!	logging synchronous
!	transport input ssh
!	transport output ssh
radius-server host 192.168.3.11 auth-port 1645	!
acct-port 1646 key 7 01240F0A690A0206345F	end
!	
control-plane	
!	
!	
!	
!	
!	
!	
gatekeeper	

Маршрутизатор EDGERouter_1

EDGERouter_1

EDGERouter_1#show running-config

Building configuration...

Current configuration : 1955 bytes

!

upgrade fpd auto

version 15.0

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname EDGERouter_1

!

boot-start-marker

boot-end-marker

!

!

no aaa new-model

!

!

!

ip source-route

no ip icmp rate-limit unreachable

ip cef

!

!

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

!

redundancy

!

!

ip tcp synwait-time 5

!

!

!

!

!

!

!

!

interface FastEthernet0/0

no ip address

shutdown

duplex half

!	duplex half
!	!
interface GigabitEthernet1/0	!
ip address 192.168.2.1 255.255.255.0	!
ip nat inside	router ospf 1
ip virtual-reassembly	log-adjacency-changes
negotiation auto	network 192.168.1.0 0.0.0.255 area 0
!	network 192.168.2.0 0.0.0.255 area 0
!	network 192.168.3.0 0.0.0.255 area 0
interface Ethernet2/0	!
ip address 192.168.1.50 255.255.255.0	ip forward-protocol nd
ip nat outside	no ip http server
ip virtual-reassembly	no ip http secure-server
duplex half	!
!	!
!	ip nat pool global-ips 192.168.1.51 192.168.1.100 netmask 255.255.255.0
interface Ethernet2/1	ip nat inside source list 1 pool global-ips
no ip address	ip route 0.0.0.0 0.0.0.0 192.168.1.1
shutdown	!
duplex half	access-list 1 permit 192.168.10.0 0.0.0.255
!	access-list 1 permit 192.168.20.0 0.0.0.255
!	access-list 1 permit 192.168.40.0 0.0.0.255
interface Ethernet2/2	access-list 1 permit 192.168.50.0 0.0.0.255
no ip address	access-list 1 permit 192.168.70.0 0.0.0.255
shutdown	access-list 1 permit 192.168.80.0 0.0.0.255
duplex half	access-list 1 permit 192.168.3.0 0.0.0.255
!	access-list 1 permit 192.168.4.0 0.0.0.255
!	no cdp log mismatch duplex
interface Ethernet2/3	!
no ip address	!
shutdown	

```

!
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login

```

