Хмельницький національний університет
Факультет програмування
та комп'ютерних і телекомунікаційних систем
Кафедра комп'ютерної інженерії та системного програмування

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Локальна комп'ютерна мережа для підприємства «Паспортний сервіс»
Назва теми

КвРКІ 170342.17.03.30 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 123 «Комп'ютерна інженерія»
Шифр, назва

Освітня програма «Комп'ютерна інженерія»
Назва

Виконав: студент IV курсу, група КІ–17–3 _____ І. Л. Кротевич
Підпис Ініціали, прізвище

Керівник _____ С.М. Лисенко
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ С.М. Лисенко
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної інженерії та системного програмування _____ Т.О. Говорущенко
Підпис Ініціали, прізвище

«_10___» _червня_ 2021 р.

Хмельницький 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Програмування та комп'ютерних і телекомунікаційних систем

Кафедра Комп'ютерної інженерії та системного програмування

Освітній рівень бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

" 11 " 01 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Кротевичу Івану Леонідовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Локальна комп'ютерна мережа для підприємства «Паспортний сервіс»

Керівник проекту (роботи) Лисенко С.М., д.т.н., доц.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 05.02.2021 р. № 11

2. Строк подання студентом проекту (роботи) на кафедру 07.06.2021 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Дослідження предметної області та постановка задачі

Проєктування комп'ютерної мережі

Програмно-апаратна реалізація комп'ютерної мережі для підприємства «Паспортний сервіс»

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Схеми мережі

Схеми мережі на поверхах будівлі

Конфігурація брандмауера

на основі зонування

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КІСП		
Антиплагіат	Нічепорук А.О., доцент кафедри КІСП		

7. Дата видачі завдання «_11_»_____01_____2021 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	11.01.2021	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об’єкта та предмета дослідження	01.02.2021	виконано
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.03.2021	виконано
4	Робота над розділом 2 – проєктування мережі	01.04.2021	виконано
5	Робота над розділом 3 – програмно-апаратна реалізація комп’ютерної мережі	30.04.2021	виконано
6	Оформлення пояснювальної записки згідно вимог	31.05.2021	виконано
7	Попередній захист ВКР	02.06.2021	виконано
8	Захист ВКР на засіданні ЕК	Червень 2021 року	

Студент  Підпис І.Л. Кротевич Ініціали, прізвище

Керівник проекту (роботи)  Підпис С. М. Лисенко Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 170375.17.03.30 ПЗ	Пояснювальна записка	55		
			Графічні матеріали			
2		КвРКІ 170375.17.03.30 Е8	Логічні схеми алгоритмів	1		
3		КвРКІ 170375.17.03.30 Е8	Мікрокомандна схема	1		
			та граф-схема переходів			
			автомату Мура			
4		КвРКІ 170375.17.03.30 Е8	Конфігурація	1		
			брандмауера на основі			
			зонування			

					КвРКІ 170375.17.03.30 ВП			
Зм	Арк	№ докум	Підпис	Дата				
Розробив		Кротевич			Відомість проекту	Літера	Аркуш	Аркушів
Перевір.		Лисенко				У	1	1
						ХНУ, КІ-17-3		
Н. контр.		Лисенко						
Затв.		Говорущенко						

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Локальна комп’ютерна мережа для підприємства «Паспортний сервіс»».

Автор роботи: Кротевич Іван Леонідович

Керівник роботи: Лисенко Сергій Миколайович.

Пояснювальна записка: 60 с., 27 рис., 4 табл., 3 дод., 43 джерела.

Графічна частина: 7 презентаційних слайдів.

КОМП’ЮТЕРНА МЕРЕЖА, CISCO, МАРШРУТИЗАТОР, VLAN, LINUX, СЕРВЕР, ОПЕРАЦІЙНА СИСТЕМА.

Метою роботи є проєктування та реалізація комп’ютерної мережі для підприємства «Паспортний сервіс».

Об’єктом дослідження є програмно-технічний (апаратний) засіб – комп’ютерна мережі для підприємства «Паспортний сервіс».

Предметом дослідження є опис та схеми локальної комп’ютерної мережі для для підприємства «Паспортний сервіс».

_____ _____

Підпис студента Дата

ЗМІСТ

Зм.	Арк.	№докум.	Підпис	Дата	КвРКІ 170342.17.03.30 ПЗ		
Виконав		Кротевич І.Л.			Синтез та моделювання операційного автомату на основі автомату Мура. Пояснювальна записка	Літера: у	Аркуш: 67
Перевір.		Лисенко С.М.					Аркушів:
Н.контр.		Лисенко С.М.				ХНУ КІ-17-3	
Затвер.		Говорущенко Т.О.					

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

КМ – комп’ютерна мережа

БД - база даних

ОС - операційна система

ПЗ - програмне забезпечення

IDS - система виявлення вторгнень

ВСТУП

У сучасному світі, орієнтованому на технології, спільне використання стало невід'ємною частиною бізнесу та інших видів діяльності. Цього обміну можна досягти за допомогою мереж. Комп'ютерна мережа пов'язує два чи більше комп'ютери для спільного використання файлів або ресурсів.

Потреби в комп'ютерних мережах зумовлені:

1. Для спільного використання комп'ютерних файлів. Мережі дозволяють користувачам ділитися файлами з іншими. Наприклад, у компанії один файл повинен спільно використовувати декілька відділень. Коли ми знаходимо цей файл у мережевій системі, усі гілки можуть використовувати цей файл.

2. Спільно використовувати комп'ютерну техніку. Лазерні принтери та великі жорсткі диски можуть коштувати дорого. Мережі дозволяють користувачам спільно використовувати таке обладнання за допомогою мережевих мікрокомп'ютерів або робочих станцій.

3. Щоб забезпечити можливість спілкування на відміну від комп'ютерного обладнання.

4. Для підвищення швидкості та точності зв'язку.

5. Надсилання повідомлень через мережі відбувається практично миттєво, а також менше шансів втратити повідомлення.

6. Знизити вартість передачі даних. Вартість передачі файлів за допомогою комп'ютерів, пов'язаних з мережами, є менш дорогою, ніж інші традиційні засоби, такі як телеграми.

7. Перевірте передачу даних. Коливання витрат в іноземній валюті та акціях можна оперативно транслювати за допомогою каналу комп'ютерного зв'язку. Коробка передач може бути збільшена та перевірена у будь-який час.

8. Висока надійність. Усі файли можна відтворити на декількох машинах, і тому, якщо один із них недоступний (через несправність обладнання), можна використовувати різні копії.

Таким чином, впровадження комп’ютерних мереж для підприємства «Паспортний сервіс» є актуальною та практично значимою задачею.

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Цілі застосування комп’ютерних мереж

Комп’ютерна мережа означає взаємозв’язок автономних (автономних) комп’ютерів для обміну інформацією.

Сполучним носієм може бути мідний дріт, оптичне волокно, мікрохвильова піч або супутник.

Мережеві елементи - Комп’ютерна мережа включає такі мережеві елементи:

1. Принаймні два комп'ютери.
2. Середовище передачі - дротове або бездротове.
3. Протоколи або правила, що регулюють спілкування.
4. Мережеве програмне забезпечення, таке як Network Operating System.

Критерії мережі. Критеріями, яким повинна відповідати комп’ютерна мережа, є:

1. Ефективність - вона вимірюється як час проїзду та час відгуку.
2. Час транзиту - час, протягом якого повідомлення переходить з одного пристрою на інший.
3. Час відповіді - це час, що минув між запитом та відповіддю.
4. Ефективність роботи залежить від наступних факторів.
5. Кількість користувачів.
6. Тип середовища передачі
7. Можливість підключеної мережі
8. Ефективність програмного забезпечення
9. Надійність - вона вимірюється в термінах
10. Частота відмов
11. Відновлення після невдач
12. Надійність під час катастрофи.
13. Безпека - означає захист даних від несанкціонованого доступу.

Цілі комп’ютерних мереж: Нижче наведено кілька важливих цілей комп’ютерних мереж:

Спільне використання ресурсів – багато організацій мають значну кількість комп’ютерів, які працюють окремо.

Наприклад, група офісних працівників може спільно використовувати спільний принтер, факс, модем, сканер тощо.

Висока надійність - якщо є альтернативні джерела постачання, усі файли можуть бути відтворені на двох або більше машинах.

Якщо одна з них недоступна, через несправність обладнання можуть бути використані інші копії.

Міжпроцесовий зв’язок - користувачі мережі, розташовані географічно один від одного, можуть спілкуватися в інтерактивному сеансі через мережу.

Для того, щоб це дозволити, мережа повинна забезпечувати майже без помилок зв'язок.

Гнучкий доступ – файли можна отримати з будь-якого комп’ютера в мережі. Проект можна розпочати на одному комп’ютері, а закінчити на іншому.

Інші цілі включають розподіл функцій обробки, централізоване управління та розподіл мережевих ресурсів, сумісність різнорідного обладнання та програмного забезпечення, хорошу продуктивність мережі, масштабованість, економія грошей, доступ до віддаленої інформації, спілкування від особи до людини тощо.

Протокол - набір певних правил, який повинен слідувати кожний підключених пристроїв по всій мережі , щоб спілкуватися і обмінюватися інформацією між ними.

Для того, щоб полегшити наскрізне спілкування, ряд протоколів працювали разом, щоб сформувати набори протоколів або стеки .

Деякі основні протоколи:

1. IP : Інтернет-протокол.
2. FTP : Протокол передачі файлів.

3. SMTP : Простий протокол передачі пошти.

4. HTTP : Протокол передачі гіпертексту.

В еталонних моделях мережі були розроблені, щоб продукти від різних виробників мали змогу взаємодіяти через мережу.

Мережева еталонна модель служить проектом, детально описуючи стандарти того, як має відбуватися зв’язок за протоколом.

Найбільш загальновизнаними еталонними моделями є модель Open System Interconnect (OSI) та модель Міністерства оборони (DoD, також відома як TCP / IP) [5].

Типи мережі часто класифікуються за їх розміром та функціональністю. Залежно від розміру, мережу можна класифікувати за трьома категоріями

1. Локальні мережі (локальні мережі).

2. MAH (столичні мережі).

3. WAN (широкосмугові мережі).

Міжмережевий являє собою загальний термін , який описує кілька мереж, з'єднаних разом. Інтернет - це найбільша та найбільш відома мережа.

Деякі мережі класифікуються за їх функціями, на відміну від їх розміру. Наприклад:

1. SAN (Мережа зберігання даних). SAN пропонує системам швидкісний доступ без втрат до пристроїв зберігання великої ємності.

2. VPN (віртуальна приватна мережа). VPN дозволяє надійно надсилати інформацію через загальнодоступну або незахищену мережу, таку як Інтернет. Типовим використанням VPN є підключення філій або віддалених користувачів до головного офісу.

У мережі будь-який підключений пристрій називається як хост.

Хост може служити наступними способами:

1. Хост може виступати в ролі Клієнта , коли він запитує інформацію.

2. Хост може діяти як Сервер, коли він надає інформацію.

3. Хост також може запитувати та надавати інформацію, називається Peer

1.2 Типи топології мережі

Розташування мережі, що містить вузли та сполучні лінії через відправника та приймача, називається топологією мережі (рис.1.1).

Відомі топології мережі: сітка, зірка, кільце

1. Топологія сітки.

У сітчастій топології кожен пристрій підключений до іншого пристрою через певний канал.

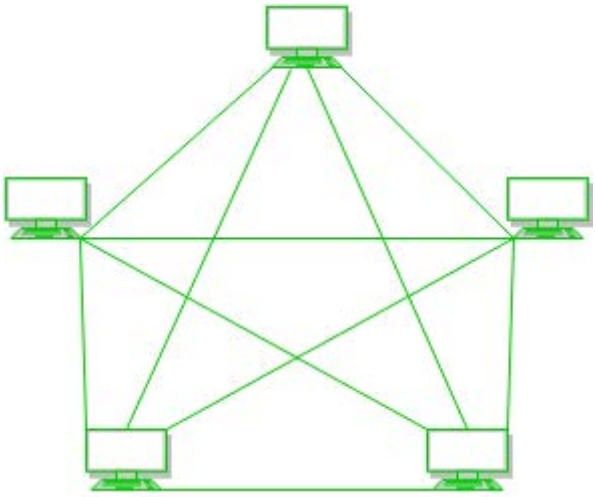


Рисунок 1.1 - Кожен пристрій підключено до іншого через виділені канали. Ці канали відомі як посилання

Якщо припустимо, N кількість пристроїв з'єднано між собою в топології сітки, загальна кількість портів, необхідних кожному пристрою, становить N-1.

На рисунку 1.1. є 5 пристроїв, підключених один до одного, отже, загальна кількість портів, необхідних кожному пристрою, дорівнює 4. Загальна кількість необхідних портів = N * (N-1).

Якщо припустимо, N кількість пристроїв пов'язано між собою в топології сітки, то загальна кількість виділених посилань, необхідних для їх з'єднання, становить N C 2, тобто N (N-1) / 2.

На рисунку 1.1 є 5 пристроїв, підключених один до одного, отже загальна кількість необхідних посилань становить 5 * 4/2 = 10.

Переваги цієї топології:

1. Несправність діагностується легко. Дані надійні, оскільки дані передаються між пристроями через виділені канали або посилання.

2. Забезпечує безпеку та конфіденційність.

Проблеми з цією топологією:

1. Встановлення та налаштування складні.

2. Вартість кабелів висока, оскільки потрібна об’ємна проводка, отже, придатна для меншої кількості пристроїв.

3. Витрати на обслуговування високі.

2. Топологія зірок (рис. 1.2).

У топології зірок всі пристрої підключені до одного концентратора за допомогою кабелю.

Цей концентратор є центральним вузлом, а всі інші вузли підключені до центрального вузла.

Хаб може мати пасивний характер, тобто не інтелектуальний хаб, такий як пристрої мовлення, в той же час хаб може бути інтелектуальним, відомим як активні хаби.

У активних концентраторах є ретранслятори.

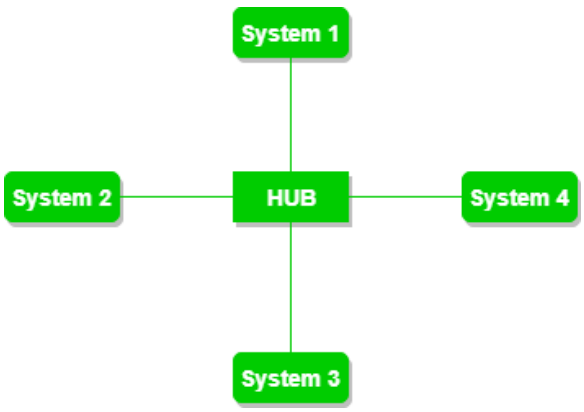


Рисунок 1.2 - Топологія зірки, що має чотири системи, підключені до однієї точки з'єднання, тобто до концентратора

Переваги цієї топології.

Якщо N пристроїв підключено один до одного в топології зірки, тоді кількість кабелів, необхідних для їх підключення, дорівнює N. Отже, налаштувати це легко.

Для кожного пристрою потрібен лише 1 порт, тобто для підключення до концентратора, тому загальна кількість необхідних портів - N.

Проблеми з цією топологією:

Якщо концентратор (концентратор), на який покладається вся топологія, виходить з ладу, вся система вийде з ладу.

Вартість монтажу висока.

Ефективність базується на одному концентраторі, тобто на концентраторі.

в) Топологія шини (рис.1.3).

Топологія шини - це тип мережі, в якому кожен комп'ютер і мережевий пристрій підключені до одного кабелю.

Він передає дані з одного кінця на інший в одному напрямку.

У топології шини немає жодної двонаправленої функції.

Це багатоточкове з’єднання та ненадійна топологія, тому що, якщо магістраль виходить з ладу, топологія виходить з ладу.

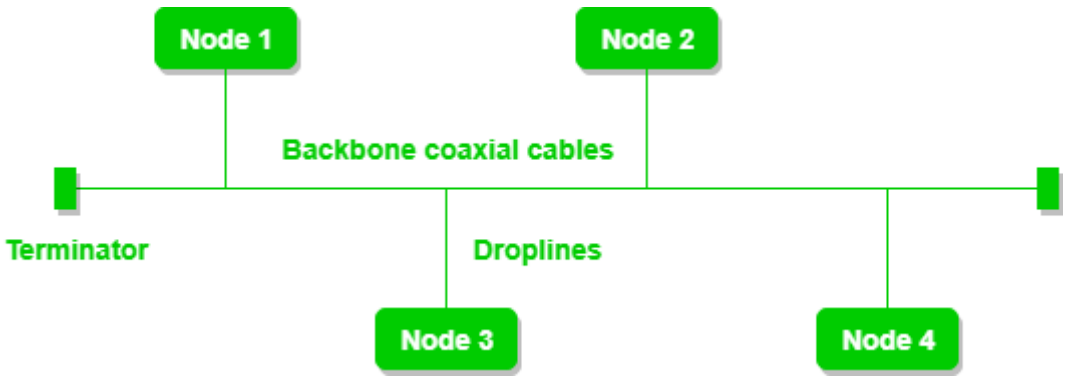


Рисунок 1.3 - Топологія шини із загальним магістральним кабелем. Вузли з'єднані з каналом за допомогою прямих ліній.

Переваги цієї топології.

Якщо N пристроїв підключено один до одного за топологією шини, тоді кількість кабелів, необхідних для їх підключення, дорівнює 1, що відоме як магістральний кабель, і потрібно N дробових ліній.

Вартість кабелю менша порівняно з іншими топологіями, але він використовується для побудови невеликих мереж.

Проблеми з цією топологією:

Якщо загальний кабель вийде з ладу, то вся система вийде з ладу.

Якщо мережевий трафік інтенсивний, це збільшує зіткнення в мережі. Щоб уникнути цього, у рівні MAC використовуються різні протоколи, відомі як Pure Aloha, Slotted Aloha, CSMA / CD тощо.

Захист дуже низький.

3. Топологія кільця (рис .1.4).

У цій топології він утворює кільце, що з'єднує пристрої, з рівно двома сусідніми пристроями.

Ряд ретрансляторів використовується для кільцевої топології з великою кількістю вузлів, тому що якщо хтось хоче надіслати деякі дані до останнього вузла в кільцевій топології зі 100 вузлами, то дані повинні пройти через 99 вузлів, щоб досягти 100-го вузол.

Таким чином, для запобігання втраті даних в мережі використовуються повторювачі.

Передача є односпрямованою, але її можна зробити двонаправленою, маючи 2 з'єднання між кожним вузолом мережі, вона називається подвійна топологія кільця.

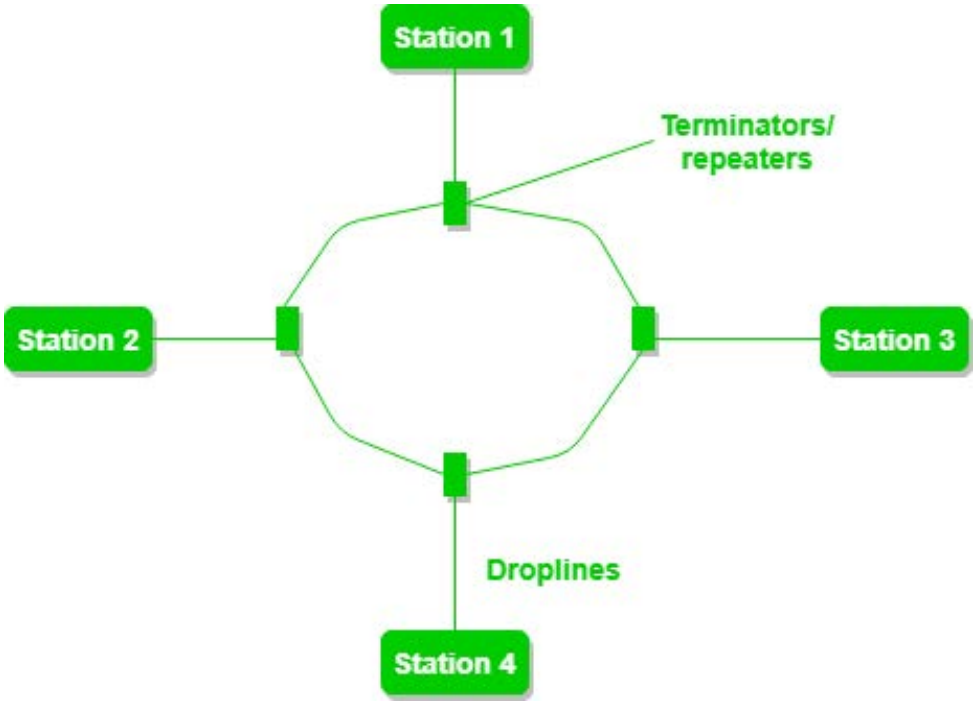


Рисунок 1.4 - Топологія кільця складається з 4 станцій, з'єднаних з кожною, що утворює кільце

У кільцевій топології виконуються такі операції.

Одна станція відома як станція моніторингу, яка бере на себе всю відповідальність за виконання операцій.

Для передачі даних станція повинна утримувати маркер.

Після завершення передачі маркер повинен бути випущений для використання іншими станціями.

Коли жодна станція не передає дані, то маркер буде циркулювати по кільцю.

Існує два типи техніки випуску токена: дострокове вивільнення токена звільняє маркер відразу після передачі даних, а вивільнення маркера затримки звільняє маркер після отримання підтвердження від одержувача.

Переваги цієї топології:

Можливість зіткнення мінімальна для цього типу топології.

Дешево встановити та розширити.

Проблеми з цією топологією:

1. Усунення несправностей у цій топології складно.

2. Додавання станцій між або видалення станцій може порушити всю топологію.

3. Менш захищений.

3. Топологія дерево.

Ця топологія є варіацією топології зірки (рис. 1.5).

Ця топологія має ієрархічний потік даних.

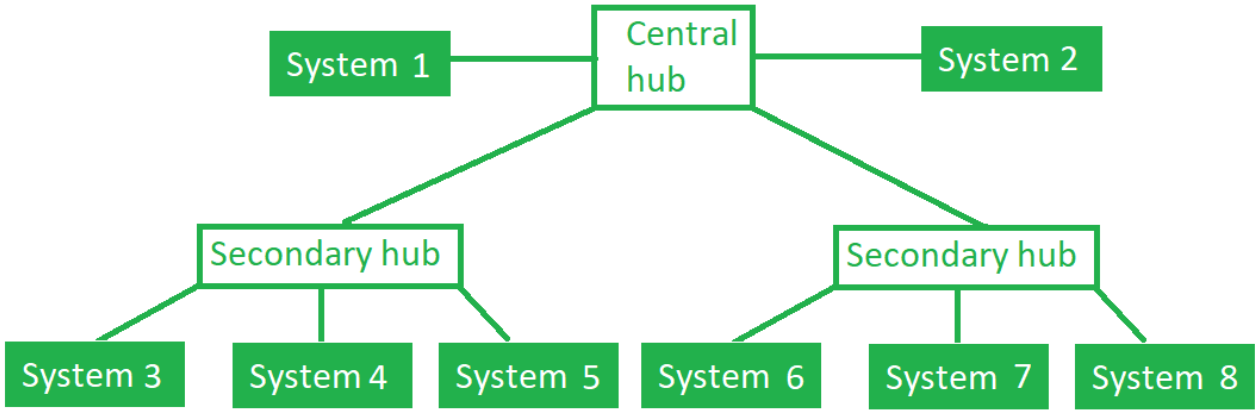


Рисунок 1.5 – Топологія зірки

При топології зірки різні вторинні концентратори з'єднані з центральним концентратором, який містить ретранслятор.

При цьому потік даних зверху вниз, тобто від центрального концентратора до вторинного, а потім до пристроїв або знизу до верху, тобто пристроїв до вторинного концентратора, а потім до центрального концентратора.

Це багатоточкове з’єднання та ненадійна топологія, тому що, якщо магістраль виходить з ладу, топологія виходить з ладу.

Переваги цієї топології.

Це дозволяє приєднати більше пристроїв до єдиного центрального концентратора, таким чином, це збільшує відстань, яку проходить сигнал, що надходить до пристроїв.

Це дозволяє мережі отримувати ізоляцію, а також визначати пріоритети з різних комп'ютерів.

Проблеми з цією топологією.

1. Якщо центральний концентратор отримує збій, виходить з ладу вся система.

Вартість висока через кабель.

Мережі MANET.

MANET розшифровується як Mobile adhoc Network, яку також називають бездротовою adhoc мережею або adhoc бездротовою мережею, яка зазвичай має мережеве середовище, що маршрутизується, поверх спеціальної мережі Link Layer (рис.1.6).

Вони складаються з безлічі мобільних вузлів, підключених бездротовим способом до самоконфігурованого, мережа самовідновлення без встановленої інфраструктури.

Вузли MANET можуть вільно переміщатися безладно, оскільки топологія мережі часто змінюється.

Кожен вузол поводиться як маршрутизатор, коли вони перенаправляють трафік на інші вказані вузли в мережі.

MANET може працювати самостійно, або вони можуть бути частиною великого Інтернету.

Вони утворюють високодинамічну автономну топологію з наявністю одного або декількох різних приймачів між вузлами.

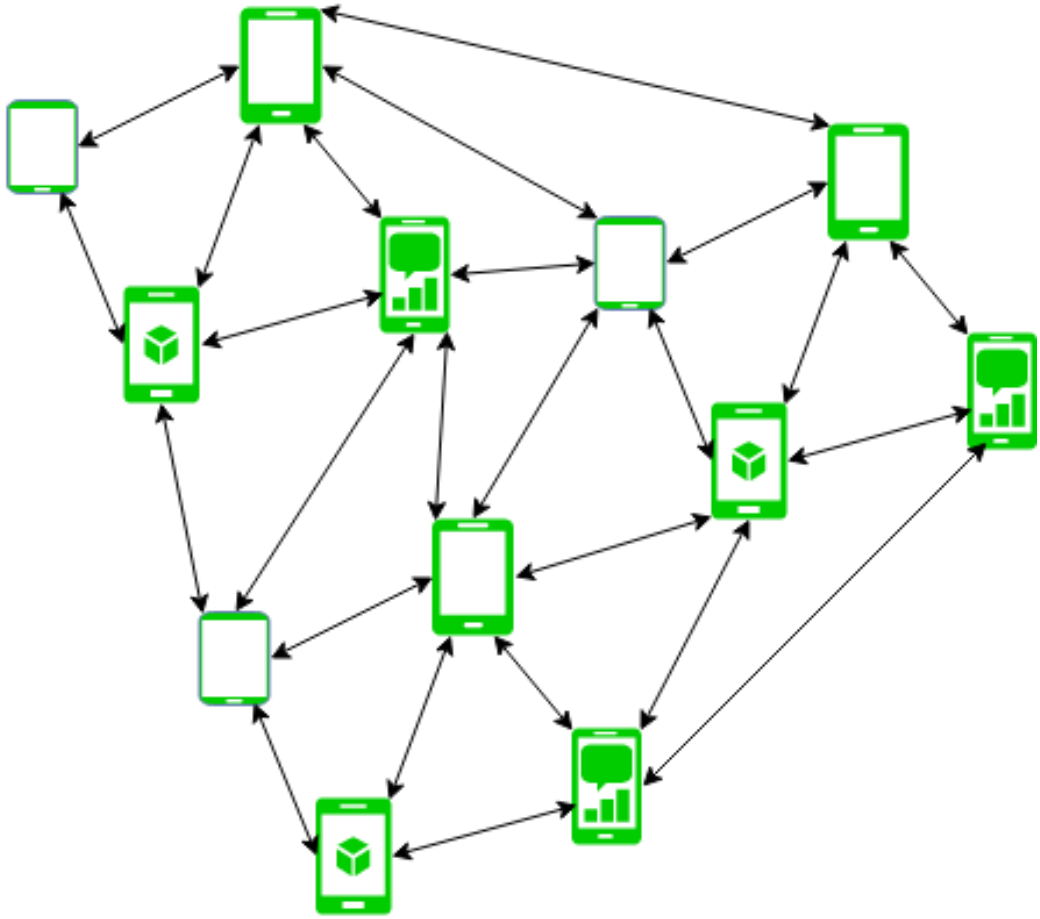


Рисунок 1.6 – Схема MANET

Основною проблемою для MANET є оснащення кожного пристрою для постійного підтримання інформації, необхідної для належного маршрутування трафіку.

MANET складаються з однорангової, самоформуючої, самовідновлювальної мережі MANET приблизно 2000-2021 рр.

Зазвичай спілкуються на радіочастотах (30 МГц-5 ГГц). Це може бути використано в безпеці дорожнього руху, починаючи від датчиків навколишнього середовища, дому, здоров'я, операцій з порятунку внаслідок катастроф, протиповітряної / сухопутної / військово-морської оборони, зброї, роботів тощо

Характеристики MANET .

Динамічні топології: топологія мережі, яка, як правило, багатократна, може змінюватися випадково і швидко з часом, вона може утворювати односпрямовані або двонаправлені посилання.

Обмежена пропускна здатність, змінна пропускна здатність каналів: бездротові зв'язки зазвичай мають нижчу надійність, ефективність, стабільність і пропускну здатність порівняно з дротовою мережею.

Автономна поведінка

Кожен вузол може виступати в ролі хоста та маршрутизатора, що демонструє свою автономну поведінку.

Енергообмежена робота.

Оскільки деякі або всі вузли покладаються на батареї або інші вичерпні засоби для отримання енергії. Мобільні вузли характеризуються меншою пам'яттю, потужністю та легкими функціями.

Обмежена безпека.

Бездротові мережі більш схильні до загроз безпеці. Централізований брандмауер відсутній через його розподілений характер операцій з безпеки, маршрутизації та конфігурації хоста.

Менше втручання людини.

Для налаштування мережі їм потрібно мінімальне втручання людини, тому вони динамічно автономні за своїм характером.

Переваги та недоліки MANET.

Переваги:

1. Відокремлення від центральної адміністрації мережі.
2. Кожен вузол може виконувати обидві ролі, тобто. маршрутизатора та хоста, що демонструє автономний характер.
3. Самоконфігурування та самовідновлення вузлів не вимагають втручання людини.

Недоліки:

1. Ресурси обмежені через різні обмеження, такі як шум, умови перешкод тощо.
2. Відсутність дозволів.
3. Більш схильний до атак через обмежену фізичну безпеку.

1.3 Висновки

В першому розділі було досліджено предметнуобласть, зокрема було окреслено цілі застосування комп’ютерних мереж, проаналізовано типи топології мережі, поставлено задачу проектування мережі.

2 ПРОЄКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Мережеві пристрої

До основних мережевих пристроїв відносять концентратори, ретранслятори, мости, комутатори, маршрутизатори, шлюзи та роутери.

1. Повторювач. Повторювач працює на фізичному рівні. Його завдання полягає в регенерації сигналу в одній і тій же мережі до того, як сигнал стане занадто слабким або пошкодженим, щоб збільшити довжину, на яку сигнал може передаватися по тій же мережі. Важливим моментом, який слід зазначити щодо ретрансляторів, є те, що вони не підсилюють сигнал. Коли сигнал стає слабким, вони потроху копіюють сигнал і відновлюють його з початковою силою. Це 2-портовий пристрій.

2. Концентратор - хаб - це, в основному, багатопортовий ретранслятор. Концентратор з'єднує кілька проводів, що надходять від різних гілок, наприклад, з'єднувач у топології зірок, який з'єднує різні станції. Концентратори не можуть фільтрувати дані, тому пакети даних надсилаються на всі підключені пристрої. Іншими словами, область зіткнень усіх хостів, підключених через концентратор, залишається однією. Крім того, вони не мають розуму, щоб знайти найкращий шлях до пакетів даних, що призводить до неефективності та втрат.

Типи концентраторів.

Активний концентратор - це концентратори, які мають власний блок живлення і можуть очищати, посилювати та передавати сигнал разом з мережею. Він служить як ретранслятором, так і як центр проводки.

Вони використовуються для збільшення максимальної відстані між вузлами.

Пасивний концентратор: - це концентратори, які збирають проводку від вузлів та джерело живлення від активного концентратора.

Ці концентратори передають сигнали в мережу без їх очищення та посилення і не можуть використовуватися для збільшення відстані між вузлами.

Інтелектуальний концентратор працює як активні концентратори та включає можливості віддаленого управління.

Вони також забезпечують гнучкі швидкості передачі даних для мережевих пристроїв.

Це також дозволяє адміністратору контролювати трафік, що проходить через хаб, і налаштовувати кожен порт у хабі.

3. Міст - міст працює на рівні каналу передачі даних.

Міст - це ретранслятор, який додає функціональність фільтрації вмісту, зчитуючи MAC-адреси джерела та пункту призначення.

Він також використовується для взаємозв'язку двох локальних мереж, що працюють за одним протоколом. Він має один вхідний та вихідний порти, що робить його 2-портовим пристроєм.

Типи мостів:

1. Прозорі мости: - це міст, на якому станції абсолютно не знають про існування мосту, тобто додається чи видаляється міст з мережі, переконфігурація станцій непотрібна. Ці мости використовують два процеси, тобто переадресацію мостів та навчання мостів.

2. Мости маршрутизації джерела: - У цих мостах операція маршрутизації виконується вихідною станцією, і кадр визначає, який маршрут слід слідувати. Хост може виявити кадр, надіславши спеціальний кадр, який називається кадром виявлення, який поширюється по всій мережі, використовуючи всі можливі шляхи до місця призначення.

4. Комутатор - комутатор - це багатопортовий міст з буфером та конструкцією, який може підвищити свою ефективність (велика кількість портів означає менший трафік) та продуктивність. Комутатор - це пристрій рівня передачі даних. Комутатор може виконувати перевірку помилок перед переадресацією даних, що робить його дуже ефективним, оскільки він не переадресовує пакети, що мають помилки, і пересилає хороші пакети вибірково для корекції лише порту.

Іншими словами, комутатор розділяє домен зіткнення хостів, але домен трансляції залишається незмінним.

5. Маршрутизатори- Маршрутизатор - це пристрій на зразок комутатора, який направляє пакети даних на основі їх IP-адрес. Маршрутизатор - це в основному пристрій мережевого рівня. Маршрутизатори зазвичай з'єднують локальні мережі та глобальні мережі та мають динамічно оновлюється таблицю маршрутизації, на основі якої вони приймають рішення щодо маршрутизації пакетів даних. Маршрутизатор розділяє домени мовлення підключених через нього хостів (рис .2.1).

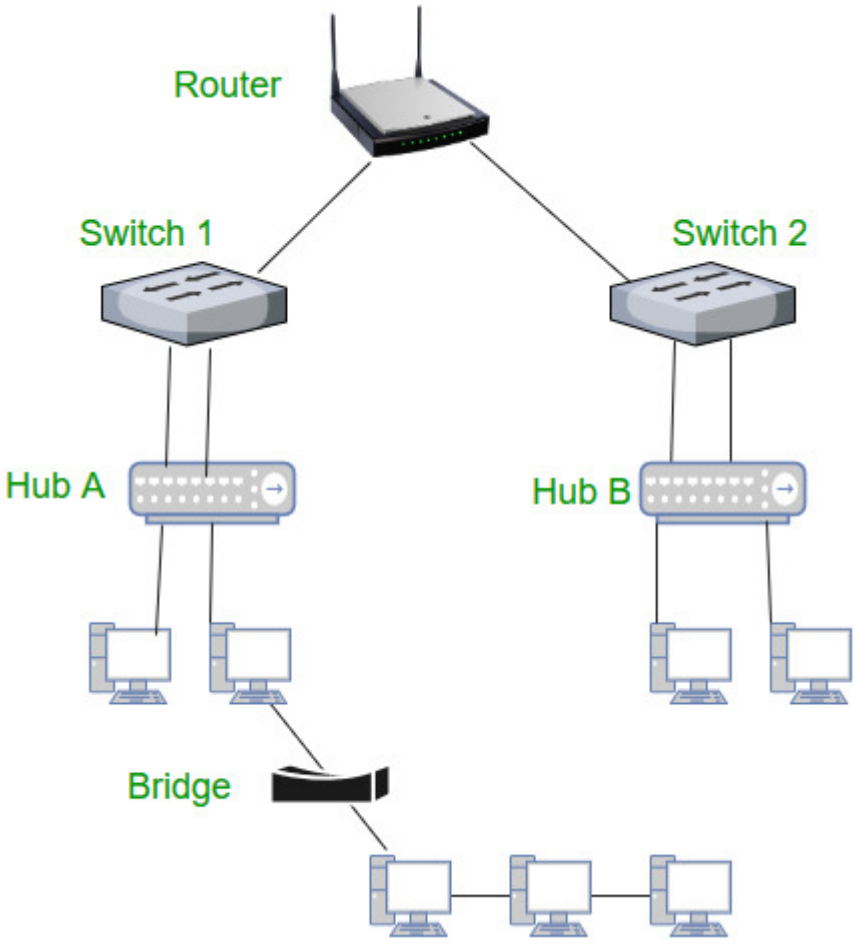


Рисунок 2.1 – Схема застосування маршрутизатора

6. Шлюз - шлюз, як випливає з назви, являє собою прохід для з'єднання двох мереж разом, які можуть працювати на різних мережевих моделях. Вони в

основному працюють як агенти обміну повідомленнями, які беруть дані з однієї системи, інтерпретують їх і передають в іншу систему. Шлюзи також називаються перетворювачами протоколів і можуть працювати на будь-якому мережевому рівні. Шлюзи, як правило, складніші, ніж комутатори або маршрутизатори.

7. Роутер також відомий як мостовий маршрутизатор - це пристрій, що поєднує в собі функції і моста, і маршрутизатора. Він може працювати як на рівні каналу передачі даних, так і на рівні мережі. Працюючи як маршрутизатор, він здатний маршрутизувати пакети по мережах і працювати як міст, він здатний фільтрувати трафік локальної мережі.

2.2 Типи носіїв передачі даних

У термінології передачі даних носій передачі - це фізичний шлях між передавачем і приймачем, тобто це канал, по якому дані передаються з одного місця в інше. Передавальний носій класифікується на такі типи:

Керований носій - дротовим або обмеженим носій передачі даних. Сигнали, що передаються, спрямовуються і обмежуються вузьким шляхом за допомогою фізичних посилань.

Особливості:

1. Висока швидкість.
2. Захищений.
3. Використовується для порівняно менших відстаней.

Існує три основних типи керованих засобів масової інформації:

Кабель витої пари – складається з 2 окремо ізольованих провідних проводів, намотаних один на одного. Як правило, кілька таких пар об'єднані в захисну оболонку. Вони є найбільш широко використовуваними носіями передачі.

Вита пара буває двох типів:

Неекранована вита пара (UTP):

Цей тип кабелю має здатність блокувати перешкоди і для цього не залежить від фізичного екрану. Він використовується для телефонних додатків.

Переваги:

1. Найменш дорогий.
2. Простота установки.
3. Високошвидкісна ємність.
4. Сприйнятливий до зовнішніх втручань.
5. Менша потужність та продуктивність у порівнянні зі STP.

Екранована вита пара (STP).

Цей тип кабелю складається із спеціальної оболонки для блокування зовнішніх перешкод.

Він використовується в Ethernet із швидкою швидкістю передачі даних, а також у голосових та каналах передачі даних телефонних ліній.

Переваги:

1. Краща продуктивність при вищій швидкості передачі даних у порівнянні з UTP.
2. Усуває перехресні перешкоди.
3. Порівняно швидше.
4. Порівняно важко встановити та виготовити.
5. Дорожчий.
6. Громіздкий.

Коаксіальний кабель - має зовнішнє пластикове покриття, що містить 2 паралельних провідника, кожен з яких має окрему ізольовану захисну кришку. Коаксіальний кабель передає інформацію у двох режимах: режимі базової смуги (виділена пропускна здатність кабелю) та широкосмуговому режимі (смуга пропускання кабелю розділена на окремі діапазони).

Кабельне телебачення та аналогові телевізійні мережі широко використовують коаксіальні кабелі.

Переваги:

1. Висока пропускна здатність.
2. Кращий стійкість до шуму.
3. Простота установки та розширення.
4. Недорогий.

Недоліки: у випадку несправності одного кабелю може порушити роботу всієї мережі

Оптичний волоконний кабель використовує концепцію відбиття світла через серцевину, складену зі скла або пластику.

Ядро оточене менш щільним скляним або пластиковим покриттям, яке називається облицюванням.

Він використовується для передачі великих обсягів даних.

Кабель може бути односпрямованим або двонаправленим. WDM (мультиплексор з діленням довжини хвилі) підтримує два режими, а саме односпрямований і двонаправлений режим.

Переваги:

1. Збільшена ємність і пропускна здатність.
2. Фізично легкий.
3. Менше ослаблення сигналу.
4. Імунітет до електромагнітних перешкод.
5. Стійкість до корозійних матеріалів.

Недоліки:

1. Важко встановлювати та обслуговувати.
2. Висока вартість.
3. Крихкий.

2.3 Впровадження брандмауера в комп'ютерну мережу

Брандмауер - це мережевий пристрій захисту, апаратний чи програмний, який контролює весь вхідний та вихідний трафік і на основі визначеного набору правил безпеки, який він приймає, відхиляє або скидає цей конкретний трафік.

Прийняти: дозволити трафік. Відхилити: заблокувати трафік, але відповісти “недосяжною помилкою” Падіння: блокувати трафік без відповіді.

Брандмауер встановлює бар’єр між захищеними внутрішніми мережами та зовнішніми ненадійними мережами, такими як Інтернет (рис. 2.2).

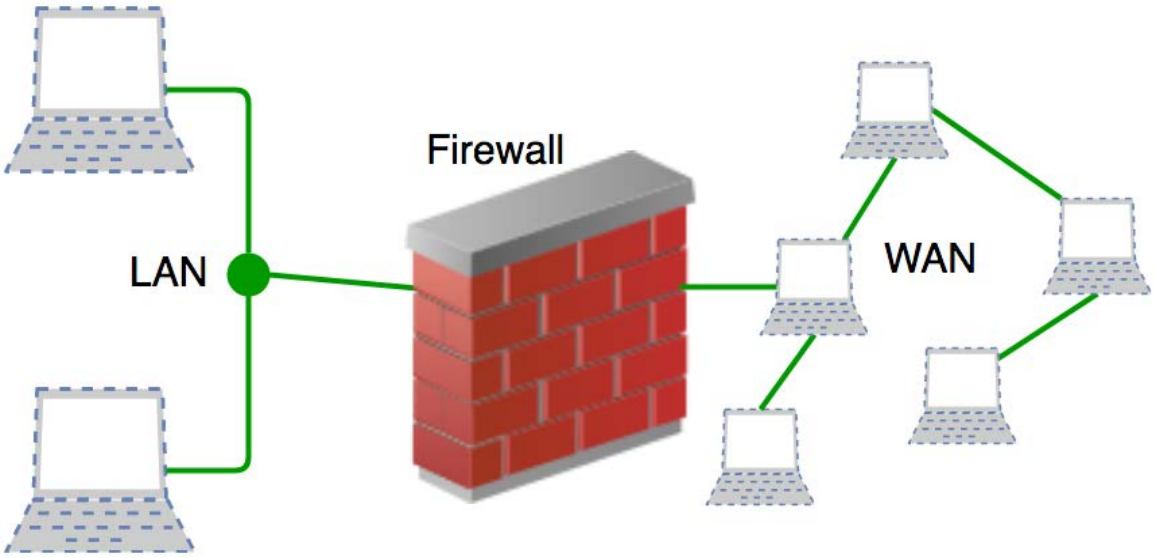


Рисунок 2.2 – Схема провадження фаєрволу в структуру мережі

Необхідність брандмауера. До брандмауерів захист мережі здійснювався за допомогою списків контролю доступу (ACL), що розміщуються на маршрутизаторах. ACL - це правила, які визначають, надавати чи забороняти доступ до мережі за певною IP-адресою.

Але ACL не можуть визначити природу пакета, який він блокує.

Крім того, лише ACL не має можливості утримувати загрози поза мережею. Таким чином, був введений брандмауер.

Підключення до Інтернету більше не є необов'язковим для організацій. Однак доступ до Інтернету надає переваги організації; це також дозволяє зовнішньому світу взаємодіяти з внутрішньою мережею організації.

Це створює загрозу для організації. Для того, щоб захистити внутрішню мережу від несанкціонованого трафіку, нам потрібен брандмауер.

Брандмауер відповідає мережевому трафіку набору правил, визначеному в його таблиці.

Як тільки правило збігається, асоційована дія застосовується до мережевого трафіку. Наприклад, в правилі визначено, що будь-який співробітник відділу кадрів не може отримати доступ до даних із кодового сервера, і одночасно визначається

інше правило, як системний адміністратор може отримати доступ до даних як з управління персоналом, так і з технічного відділу.

Правила можна визначити на брандмауері, виходячи з необхідності та політики безпеки організації.

З точки зору сервера, мережевий трафік може бути як вихідним, так і вхідним.

Брандмауер підтримує чіткий набір правил для обох випадків. Передавати переважно вихідний трафік, що походить від самого сервера.

Тим не менше, встановлення правила щодо вихідного трафіку завжди краще, щоб досягти більшої безпеки та запобігти небажаному спілкуванню.

Вхідний трафік трактується по-різному.

Більшість трафіку, який потрапляє на брандмауер, є одним із цих трьох основних протоколів транспортного рівня - TCP, UDP або ICMP. Усі ці типи мають адресу джерела та адресу призначення.

Крім того, TCP і UDP мають номери портів. ICMP використовує код типу замість номера порту, який визначає призначення цього пакета.

Політика за замовчуванням: Дуже складно явно охопити всі можливі правила брандмауера. З цієї причини брандмауер завжди повинен мати політику за замовчуванням.

Політика за замовчуванням складається лише з дії (прийняти, відхилити або відмовитись).

Припустимо, не визначено правила щодо підключення SSH до сервера на брандмауері. Отже, він буде дотримуватися політики за замовчуванням. Якщо політика по замовчуванням на брандмауері встановлена в приймати , то будь-який комп'ютер , поза вашого офісу може встановити з'єднання з SSH до сервера. Тому встановлення політики за замовчуванням як випадання (або відхилення) - це завжди хороша практика.

Брандмауери класифікують на основі їх генерації.

Брандмауер фільтрації пакетів першого покоління. Брандмауер фільтрації пакетів використовується для управління доступом до мережі шляхом моніторингу

вихідних та вхідних пакетів та дозволяючи їм проходити або зупинятись на основі IP-адреси джерела та призначення, протоколів та портів.

Він аналізує трафік на рівні транспортного протоколу (але в основному використовує перші 3 шари).

Брандмауери пакетів обробляють кожен пакет ізольовано. Вони не можуть визначити, чи є пакет частиною існуючого потоку трафіку.

Тільки брандмауер може дозволити або заборонити пакети на основі унікальних заголовків пакетів.

Брандмауер фільтрації пакетів підтримує таблицю фільтрації, яка визначає, буде пакет переадресований або відхилений.

З таблиці фільтрації пакети будуть відфільтровані відповідно до таких правил (рис. 2.3).

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Рисунок 2.3 - Таблиця фільтрації пакети відфільтровані відповідно до правил

Вхідні пакети з мережі 192.168.21.0 блокуються.

Вхідні пакети, призначені для внутрішнього сервера TELNET (порт 23), блокуються.

Вхідні пакети, призначені для хосту 192.168.21.3, блокуються.

Усі відомі послуги мережі 192.168.21.0 дозволені.

Брандмауер другого покоління - Stateful Inspection: брандмауери Stateful (виконують Stateful Packet Inspection) можуть визначати стан з'єднання пакета, на відміну від брандмауера фільтрації пакетів, що робить його більш ефективним. Він

відстежує стан мережевого з'єднання, що проходить через нього, наприклад, потоки TCP.

Отже, рішення про фільтрацію базуватиметься не тільки на визначених правилах, але й на історії пакетів у таблиці стану.

Брандмауер третього покоління - брандмауер прикладного рівня: брандмауер прикладного рівня може перевіряти та фільтрувати пакети на будь-якому рівні OSI, аж до прикладного рівня.

Він має можливість блокувати певний вміст, а також розпізнавати випадки зловживання певними програмами та протоколами (наприклад, HTTP, FTP). Іншими словами, брандмауери рівня додатків - це хости, на яких працюють проксі-сервери.

Брандмауер проксі запобігає прямому з'єднанню між будь-якою стороною брандмауера, кожен пакет повинен проходити через проксі. Він може дозволити або заблокувати трафік на основі заздалегідь визначених правил.

Примітка. Брандмауери прикладного рівня також можна використовувати як перетворювач мережевих адрес (NAT).

Брандмауери наступного покоління (NGFW). Брандмауери наступного покоління в даний час розгортаються, щоб зупинити сучасні порушення безпеки, такі як попередні атаки шкідливого програмного забезпечення та атаки на рівні додатків.

NGFW складається з глибокої перевірки пакетів, перевірки додатків, перевірки SSL / SSH та багатьох функцій для захисту мережі від цих сучасних загроз.

Брандмауери, як правило, бувають двох типів: на основі хоста та мережі.

Брандмауери на основі хостів. Брандмауер на основі хосту встановлюється на кожному вузлі мережі, який контролює кожен вхідний та вихідний пакет.

Це програмний додаток або набір програм, що входить до складу операційної системи.

Брандмауери на основі хоста необхідні, оскільки мережеві брандмауери не можуть забезпечити захист всередині надійної мережі.

Брандмауер хосту захищає кожного хоста від атак та несанкціонованого доступу.

Мережеві брандмауери: функція мережевого брандмауера на рівні мережі. Іншими словами, ці брандмауери фільтрують весь вхідний та вихідний трафік по мережі. Він захищає внутрішню мережу, фільтруючи трафік, використовуючи правила, визначені на брандмауері.

Мережевий брандмауер може мати дві або більше мережевих карт (NIC). Мережевий брандмауер, як правило, є виділеною системою з встановленим фірмовим програмним забезпеченням.

Обидва типи брандмауера мають свої переваги.

Брандмауер - це мережева система безпеки, яка фільтрує та контролює трафік за попередньо визначеним набором правил. Це посередницька система між пристроєм та Інтернетом.

Принцип роботи брандмауера Linux. Більшість дистрибутивів Linux мають інструменти брандмауера за замовчуванням, які можна використовувати для їх налаштування.

Для встановлення брандмауера ми будемо використовувати “IPTables”, інструмент за замовчуванням, який надається в Linux.

Iptables використовується для налаштування, обслуговування та перевірки таблиць правил фільтрування пакетів IPv4 та IPv6 у ядрі Linux.

Усі команди потребують привілеїв sudo.

Ланцюги - це набір правил, визначених для конкретного завдання.

У нас є три ланцюжки (набір правил), які використовуються для обробки трафіку:

1. INPUT Chains.
2. OUTPUT Chains.
3. FORWARD Chains.

INPUT Chains. Будь-який трафік, що надходить з Інтернету (мережі) до локальної машини, повинен проходити через ланцюги введення.

Це означає, що вони повинні пройти всі правила, встановлені в ланцюжку введення.

OUTPUT Chains. Будь-який трафік, що надходить з вашої локальної машини в Інтернет, повинен проходити через вихідні ланцюги.

FORWARD Chains. Будь-який трафік, який надходить із зовнішньої мережі та надходить до іншої мережі, повинен проходити по прямому ланцюжку. Він використовується, коли підключено два або більше комп'ютерів, і ми хочемо надсилати дані між ними.

Є три дії, які iptables можуть виконувати на трафіку:

1. ACCEPT.
2. DROP.
3. REJECT.

ACCEPT - коли трафік передає правила у вказаному ланцюжку, тоді iptable приймає трафік.

Це означає, що брандмауер відкритий.

DROP - коли трафік не може передати правила у вказаному ланцюжку, iptable блокує цей трафік.

Це означає, що брандмауер закритий.

REJECT. Цей тип дій схожий на дію скидання, але він відправляє повідомлення відправнику трафіку про те, що передача даних не вдалася.

Як загальне правило, використовуйте REJECT, коли необхідно, щоб інший кінець знав, що порт недоступний, і необхідно використовувати DROP для з'єднань із хостами, яких бачили не потрібно.

Примітка**.** Правила, встановлені в iptables, перевіряються від верхніх правил до низу.

Щоразу, коли пакет проходить будь-яке з основних правил, йому дозволяється пройти брандмауер.

Нижні правила не перевіряються.

Основні команди iptables:

1. Перерахувати поточні правила iptable:

Щоб перерахувати правила поточних iptables:

```
sudo iptables -L
```

Результат подано на рисунку 2.4.

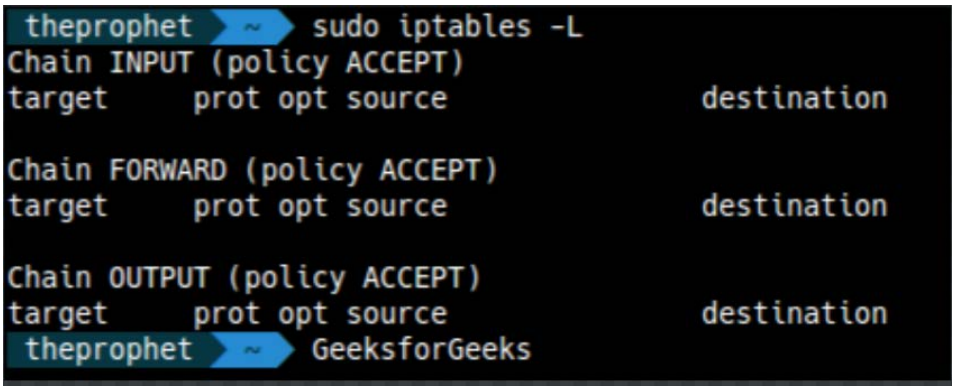


Рисунок 2.4 – Результати роботи команд iptables

Як видно, маємо три ланцюжки (ACCEPT, DROP, REJECT, FORWARD, EXIT). Також можна бачити заголовки стовпців, але вони не є фактичними правилами. Це пояснюється тим, що більшість Linux поставляються без попередньо визначених правил.

Ціль визначає, які дії потрібно зробити з пакетом (ACCEPT, DROP тощо).

Prot визначає протокол (TCP, IP) пакета.

Джерело повідомляє адресу джерела пакета.

Пункт призначення визначає адресу призначення пакета.

Якщо необхідно очистити / змити всі існуючі правила, необхідно виконати команду:

```
sudo iptables -F
```

Це скине iptables.

Зміна політики ланцюжків за замовчуванням:

```
sudo iptables -P Chain_name Action_to_be_taken
```

Як можна бачити, політикою за замовчуванням для кожного ланцюжка є ACCEPT.

Для того, щоб змінити політику переадресації:

sudo iptables -P FORWARD DROP

Наведена команда зупинить будь-який трафік, який буде переадресований через вашу систему. Це означає, що жодна інша система не може ваша система як посередник передавати дані.

Можна також скласи своє правило, тобто будувати власні політики брандмауера.

Спочатку необхідно працювати над ланцюжком введення, оскільки саме туди буде надсилатися вхідний трафік.

Синтаксис:

sudo iptables -A / -I chain_name -s source_ip -j action_to_take

Припустимо, необхідно заблокувати трафік, що надходить з IP-адреси 192.168.1.3.

Тоді можна використати команду:

sudo iptables -A INPUT -s 192.168.1.3 -j DROP

Перегляд компоненти:

-A INPUT

Прапор -A використовується для додавання правила до кінця ланцюжка. Ця частина команди повідомляє iptable, що неохідно додати правило в кінець ланцюжка INPUT.

-I INPUT

У цьому прапорі правила додаються у верхній частині ланцюжка.

-s 192.168.1.3:-

Прапор -s використовується для вказівки джерела пакета. Це вказує iptable шукати пакети, що надходять з джерела 192.168.1.3

-j DROP

Це визначає, що iptable повинен робити з пакетом.

Коротше кажучи, вищевказана команда додає правило до ланцюжка INPUT, яке говорить, що якщо приходить будь-який пакет, вихідна адреса якого 192.168.1.3, тоді скиньте цей пакет, це означає, що не дозволяють пакету дістатися до комп'ютера.

Після виконання вищевказаної команди ви можете побачити зміни за допомогою команди: -

sudo iptables -L

Результат подано на рисунку 2.5.

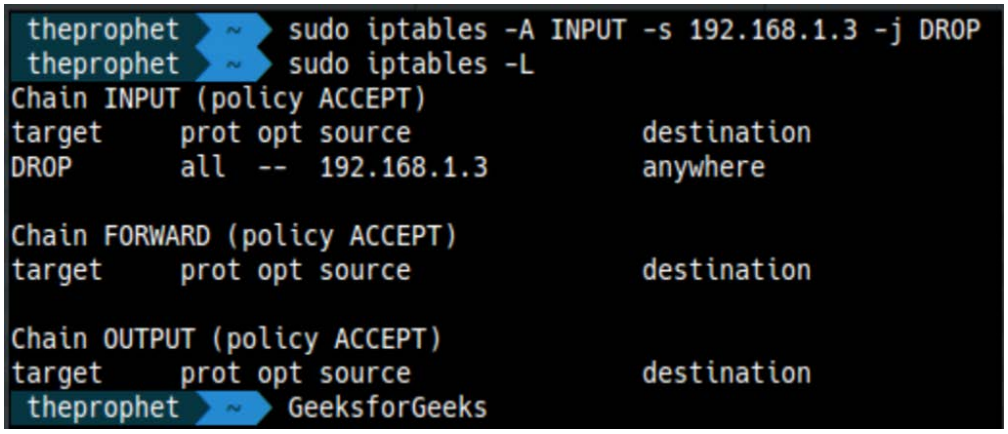


Рисунок 2.5 – Результат роботи команди в iptables

Впровадження правила ACCEPT. Якщо необхідно додати правила до певних портів вашої мережі, тоді можна використовувати такі команди.

Синтаксис:

sudo iptables -A/-I chain_name -s source_ip -p protocol_name --dport port_number -j Action_to_take

-p имя_протокола: -

Цей параметр використовується для узгодження пакетів, що слідують за протоколом_назви_назви.

-dport номер_порту:

ця опція доступна, лише якщо ви вказали опцію -p protocol_name. Він визначає пошук пакетів, які йдуть до порту "номер_порту".

Приклад, нехай необхідно тримати наш порт SSH відкритим (у цьому посібнику ми припустимо, що стандартним портом SSH є 22) із мережі 192.168.1.3, яку було заблоковано у наведеному вище випадку.

Тобто потрібно дозволити лише ті пакети, що надходять з 192.168.1.3 і які хочуть перейти до порту 22.

```
sudo iptables -A INPUT -s 192.168.1.3 -p tcp --dport 22 -j ACCEPT
```

У наведеній вище команді йдеться про пошук пакетів, що походять з IP-адреси 192.168.1.3, мають протокол TCP і хочуть доставити щось у порт 22 визначеного комп'ютера.

Результат подано на рисунку 2.6.

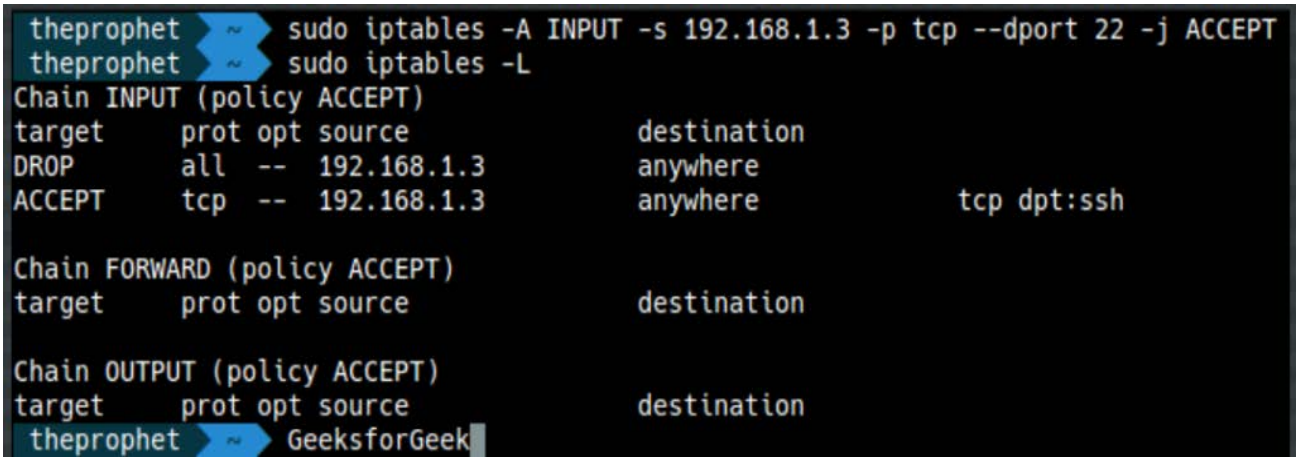


Рисунок 2.6 – Результат роботи команди в iptables

Правила, встановлені iptables, перевіряються зверху вниз.

Щоразу, коли пакет обробляється за одним із верхніх правил, він не перевіряється за нижчими правилами.

У такому випадку пакет перевірявся за допомогою верхнього правила, яке говорить, що iptable повинен скинути будь-який пакет, що надходить з 192.168.1.3.

Отже, як тільки пакет отримав доступ через це правило, він не перейшов до наступного правила, яке дозволяло пакети потрапляти до порту 22.

Тому воно не вдалося.

Для вирішення проблеми необхідно додати правило у верхню частину ланцюжка. Все, що потрібно зробити, це змінити параметр -A на -I.

Команда для цього є: -

```
sudo iptables -I INPUT -s 192.168.1.3 -p tcp --dport 22 -j ACCEPT
```

Тепер перевірте конфігурацію iptable за допомогою команди -L.

Результат подано на рисунку 2.7.

```
theprophet ~ sudo iptables -I INPUT -s 192.168.1.3 -p tcp --dport 22 -j ACCEPT
theprophet ~ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.1.3          anywhere             tcp dpt:ssh
DROP       all  --  192.168.1.3          anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
theprophet ~ GeeksforGeek
```

Рисунок 2.7 – Результат роботи команди в iptables

Отже, будь-який пакет, що надходить з 192.168.1.3, спочатку перевіряється, чи надходить він до порту 22, якщо ні, то він запускається через наступне правило в ланцюжку. В іншому випадку дозволяється пройти брандмауер.

Видалення правила з iptable.

Синтаксис:

sudo iptables -D chain_name rule_number

Приклад: -

Якщо ми хочемо видалити правило, яке приймає трафік до порту 22 і яке ми додали в попередньому розділі, тоді: -

sudo iptables -D ВХІД 1

Пам'ятайте починається номер правила від 1

Результат подано на рисунку 2.8.

```
theprophet ~ sudo iptables -D INPUT 1
theprophet ~ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.1.3          anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
theprophet ~ GeeksforGeeks
```

Рисунок 2.8 - Результат роботи команди в iptables

Збереження конфігурації. Ця оперція непотрібна, якщо здійснюється впровадження її на персональному комп'ютері, який не є сервером, але якщо це виконується впровадження брандмауера на сервері, то є велика ймовірність того, що сервер може бути пошкоджений, і є ризик втрати даних.

Тому, завжди необхідно зберігати свої конфігурації.

Існує багато способів зробити це, але найпростіший спосіб - це пакет iptables-persistent.

Його отримаи можна завантаживши пакет із стандартних сховищ Ubuntu:

```
sudo apt-get update
sudo apt-get install iptables-persistent
```

Після завершення встановлення можна зберегти конфігурацію за допомогою команди:

```
sudo invoke-rc.d iptables-persistent save
```

2.6 Висновки

В другому розділі було подано особливості проєктування комп’ютерної мережі, зокрема розглянуто мережеві пристрої, представлено типи носіїв передачі даних.

Також в розділі було подано особливості впровадження брандмауера в комп'ютерну мережу.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ ПІДПРИЄМСТВА «ПАСПОРТНИЙ СЕРВІС»

3.1 Апаратне забезпечення спроєктованої комп'ютерної мережі

Для вирішення поставленої задачі основним питанням став вибір монтажного обладнання, такого як комутаційна шафа, необхідні патч-кодри, кабелі, відповідні розетки, кабельні лотки (табл. 3.1).

Таблиця 3.1 – Необхідне апаратне забезпечення для монтування комутаційної шафи

Назва	Опис	Необхідна кількість
Вита пара (кабель UTP)	(24-AWG), катег. 5E, чотири пари, одно-проволочний, сірий колір, PVC (бухта 305.0 м)	22 бухти
Патч-корд UTP/0,5	Катег. 5e, з захистом, , довжина 0,50 м	300 шт.
Патч-корд UTP/1	Катег. 5e, із захистом, довжина 1.0 м	180 шт.
Розетка ст. RJ-11	Legrand 1M RJ-11	38 шт.
Кабель оптоволокно	Corning SMF-24 оптоволокно, 62.50/125.0, ст. багатомод.	80 метрів
Кабель ст. UTP	Катег. 3, сірого кольору, PVC	40 метрів
Розетка	DLP-2M, RJ-45, тип FTP катег.5e з рамкою та суппортом для кришки 65.0 мм	310 шт.
Розетка із заземл. Legrand	DLP, 2X-2K+3 б/зажим. із супортом для кабельних каналів, кришка, 65.0 мм	500 шт.

Кінець таблиці 3.1 - Необхідне апаратне забезпечення для монтування комутаційної шафи

Форм-фактори: Лоток	DKC, 100 x 50 L3000, 35022, глибина:50.0mm, довж.: 3.0 м, шир.: 100.0 mm	50 шт.
Форм-фактори: Труба	ПВХ, діаметр 63.0 мм	18 метрів
Шкаф комутаційний (для апаратної кімнати)	Шкаф напольний, ст. 19" 24U, заземл., з ніжками	1 шт.
Шкаф комутаційний (для кросової кімнати)	Шкаф ст. 19" напольний, 24U	3 шт.

В роботі використано блок безперебійного живлення для забезпечення сожливості автономного функціонування апаратного забезпечення (рис. 3.1).

Рисунок 3.1 – Блок безперебійного живлення

В роботі було обрано ДБЖ Volter™UPS-500.

Також було вибрано серверне апаратне забезпечення Сервер Dell EMC T140 (210-T140-2134) (рис. 3.2, таблиця 3.2).

Вказане апаратне забезпечення має:

1) високу обчислювальну продуктивність;
2) доступність;
3) високу масштабованість;
4) доступне керування в корпоративних мережах.

Рисунок 3.2 – Серверна станція в розробленій мережі

Таблиця 3.2 – Специфікація серверного апаратного забезпеченняї

Процесор	Intel Xeon, E-2134 частота 3.5GHz, 8M кеш, 4C/8T, (71Ват)
Оперативна пам'ять	Один 1x16GB 2666MT/s, пам’ять DDR4 ECC UDIMM (до чотирьох 4x DDR4 DIMM слотів, підтримка UDIMMs, швидкість доо 2666MT/s, 64GB max. Supports registered підтримка ECC)
Накопичувач пам’яті	3.5" Chassis до 4 Cabled Hard Drives пристроїв
Наявний HDD	Два 2x2TB швидкість 7.2K RPM NLSAS, швидкість 12Gbps 512n 3.5in
Дисковий контролер	Один PERC H330 RAID Controller, Adapter, Full Height
Мережний контролер	Два порти 2 x 1GbE
Привід	DVD +/- RW SATA
Слоти розширення плати	Один 1x8 Gen3 (x16 connector); один 1x8 Gen3 (вісім x8 connector); 1x4 Gen3 (вісім x8 connector); 1x1 Gen3 (один x1 connector) FH / HL
Зовнішні порти введення-виведення	Передній Front Ports: один 1x USB 3.0, один 1x, а також micro USB 2.0, port Rear Ports: два 2x USB 3.0, чотири 4x USB 2.0, порт VGA, порт serial connector Internal USB: один 1x internal USB 3.0
Джерело живлення	Типу Single cabled 370W, PSU
Управління	Типу iDrac9, Basic
Форм-фактор	Типу Tower server

В роботі було використано такі керовані комутатор DGS-1210-20 [18].

DGS-1210-20 - керований комутатор вважається пристроєм 2 рівня. Він оснащений 16 портами 10/100/1000Base-T, а також має 4 комбо-порти 100/1000Base-T/SFP (рис. 3.3).

Пристрій підтримує технологію D-Link Green та має множину розширених функцій керування, забезпечує високу обчислювальну продуктивність, а також масштабованість комп'ютерної мережі.

Функції керування мають можливості SNMP, керування на основі наявного Web-інтерфейсу, а також інтерфейс Telnet і SSH.

Даний комутатор має пасивну систему охолодження, яка забезпечує безшумність роботи, а також надає можливість продовження терміну експлуатації апаратного пристрою.

Комутатор DGS-1210-20 підтримує функції рівня 2, такі як:

1) функція IGMP Snooping;
2) функція Port Mirroring;
3) функція Spanning Tree Protocol (STP).

Функція управління потоком IEEE 802.3x надає можливість оптимізувати навантаження на апаратуру для підвищення надійності передачі даних.

Підтримуючи швидкість на кожному з портів до 2000 Мбіт/с в режимі повного дуплексу, комутатор забезпечує високу продуктивність, необхідну для підключення робочих місць.

Комутатор має здатність підтримки функції діагностування кабелів а такожі функції Loopback Detection.

Функція Loopback Detection може використовуватися для визначення наявності петель, а також автоматичного відключення порту, на якому вже було виявлено петлю.

Функція діагностування кабелю призначена для виявлення крученості витої пари, а також інших типів несправності кабелю в мережі.

Всі наявні Ethernet-порти комутатора підтримують вбудований захист від статичної електрики в межах 6 кВ.

Вона забезпечує підтримку мідних портів, а також захист від напруги, та дозволяє запобігати пошкодження апаратури та інших підключених до нього пристроїв.

Функція D-Link Safeguard Engine, наявна в комутаторі, забезпечує механізм захисту комутатора від шкідливого програмного забезпечення та шкідливого трафіку.

Аутентифікація на основі 802.1X забезпечує можливість використання зовнішнього сервера RADIUS для авторизації користувачів мережі.

Наявна функція списків управління доступом (ACL) забезпечує збільшення безпеки комп'ютерної мережі для фільтрування трафіку, який надходить від несанкціонованих IP-адрес чи MAC-адрес.

Комутатор DGS-1210-20 підтримує програмне забезпечення D-View 7.0, а також інтерфейс Telnet та SSH.

D-View 7.0 - системне мережеве керування, що дозволяє керувати найбільш усіма параметрами (працездатності, надійності, гнучкості, а також безпеки).

Комутатор DGS-1210-20 дозволяє здійснювати економію електроенергії.

Комутатор має здатність визначення статусу з'єднання для кожного наявного порту і забезпечувати автоматичний перехід певних неактивних портів в сплячий режим.

Чіпсет обраного комутатора DGS-1210-20 має можливість скоротити енерговитрати.

Рисунок 3.3 – Комутатор DGS-1210-20

В роботі було обрано точка доступу Cisco AIR-CAP3502I-E-K9.

Точка доступу Wi-Fi CISCO AIR-CAP3502I-E було обрано через оптимальний набір можливостей для установки в офісних приміщень з метою забезпечення високопродуктивних бездротових мереж.

Бездротова точка доступу CISCO AIR-CAP3502I-E відноситься до стандарту 802.11n. Вона має автоматичне налаштування з вбудованими антенами двох діапазонів 2,4 і 5 ГГц і функціонує з круговою спрямованістю

Точка має порт Ethernet зі швидкістями 10/100/1000 Мбіт / с, має 128 MB DRAM пам’яті та і 32 MB flash-пам'яті.

Для забезпечення живлення точки доступу можливим є використання технології PoE.

Точка доступу є сумісною з стандартом 802.11n і дозволяє досягти високих швидкостей передачі даних.

Також точка доступу має підтримку технології CleanAir, яка забезпечує оптимальне покриття приміщень, а також відсутність взаємного впливу кількох пристроїв в мережі один на одного (рис. 3.4).

Рисунок 3.4 – Cisco AIR-CAP3502I-E-K9

3.3 Програмне забезпечення комп’ютерної мережі для підприємства «Паспортний сервіс»

В якості серверної ОС була обрана Linux на основі SUSE SUSE Linux Enterprise Server 15 SP2 - серверного варіанту дистрибутиву Linux [42].

SUSE®Сервер Linux Enterprise 15 - це модульна операційна система, яка дозволяє спростити IT-середовище, модернізувати IT-інфраструктуру та пришвидшити інновації завдяки залучувальній платформі для розробників. Як результат, можна легко розгорнути та передати критично важливі для бізнесу робочі навантаження в локальних та загальнодоступних хмарних середовищах.

Багато організацій використовують традиційну інфраструктуру, програмно визначену інфраструктуру або поєднання традиційного та програмного забезпечення.

Основні переваги SUSE Linux Enterprise 15:

1. Платформа «спільного коду» SUSE Linux Enterprise допомагає здійснювати міграцію робочих навантажень додатків, покращити управління системами та полегшує прийняття контейнерів.

2. Здатність модернізації IT-інфраструктури шляхом впровадження інновацій та покращення ефективності IT-інфраструктури, не порушуючи стабільність, безпеку та перевірені стандарти. Архітектура Modular + допомагає IT-адміністратору зменшити ризик, спрощуючи планування та прийняття рішень. Починаючи з одного інсталяційного образу, можна додавати продукти SUSE Linux Enterprise Server або легко додавати модулі у міру зростання потреб бізнесу.

Крім того, SUSE Linux Enterprise Server підтримує контейнери Linux та механізм контейнерів Docker з відкритим кодом. Можна керувати контейнерами Linux, використовуючи загальну структуру віртуалізації (libvirt). Для підтримки механізму контейнерів Docker з відкритим кодом включений приватний реєстр з інструментами для безпечної співпраці, застосування виправлень безпеки та автоматизації розгортання додатків у контейнерах Linux.

Модулі. В SUSE Linux Enterprise 15 з архітектурою Modular +, все є модулем. Отже, можна впроваджувати інновації, не виходячи з традиційної моделі постачання програмного забезпечення для підприємств. Модулі, доступні в SUSE Linux Enterprise Server, забезпечують швидшу інтеграцію з оновленими версіями. Цей підхід до проектування дозволяє збалансувати гнучкість модульної архітектури та стабільність інфраструктури. За допомогою Unified Installer клієнти можуть шукати пакет, який їм подобається, і вибрати набір пакетів, який вони хочуть у системі.

Повний відкат системи. Системні адміністратори можуть завантажуватися зі образу для підвищення безпеки даних.

В якості клієнтської операційної системи було обрано систему Windows 10 [43].

Для налаштування мережевих інтерфейсів в Linux SLES було використано команду ifconfig (рис. 3.5).

```
infer@infer-VB:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::e101:3f6e:be38:3a80  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:96:e9:70  txqueuelen 1000  (Ethernet)
        RX packets 42845  bytes 45536052 (45.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6608  bytes 522024 (522.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Локальная петля (Loopback))
        RX packets 225  bytes 18617 (18.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 225  bytes 18617 (18.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

infer@infer-VB:~$
```

Рисунок 3.5 – Конфігурування мережі в ОС SLED

Наявний в мережі сервер було використано для протоколу динамічної конфігурації хосту (DHCP) - призначений для мережевих налаштувань централізовано (із сервера), а не налаштування їх локально на кожній робочій станції.

Хост, налаштований на використання DHCP не має контролю над власною статичною адресою. Це дозволено налаштувати повністю та автоматично відповідно до вказівок від сервера.

В роботі було використано NetworkManager на стороні клієнта.

В роботі було налаштуовано сервера DHCP за допомогою YaST в експертному режимі конфігурації, що дозволяє змінити налаштування сервера DHCP в кожній деталі.

Для цього було запущено конфігурацію експерта, натиснувши DHCP Конфігурація експерта сервера під час запуску діалогове вікно (див. рисунок 3.6).

У діалоговому вікні було зроблено наявну конфігурацію доступною для редагування вибравши запустити DHCP-сервер.

Важливою особливістю поведінки сервера DHCP - це його здатність працювати в chroot середовищі, щоб захистити хост сервера.

Якщо DHCP сервер повинен коли-небудь бути скомпрометований зовнішньою атакою зловмисником, то це буде неможливо.

У нижній частині діалогового вікна відображаються параметри з уже визначеними деклараціями.

Змінити це можна за допомогою Add , Delete та Редагувати.

Якщо вибрати Додатково, можна потрапити до додаткових експертних діалогів.

Рисунок 3.6 демонструє налаштування керуванням ключами TSIG та налаштування конфігурації брандмауера відповідно до налаштування сервера DHCP.

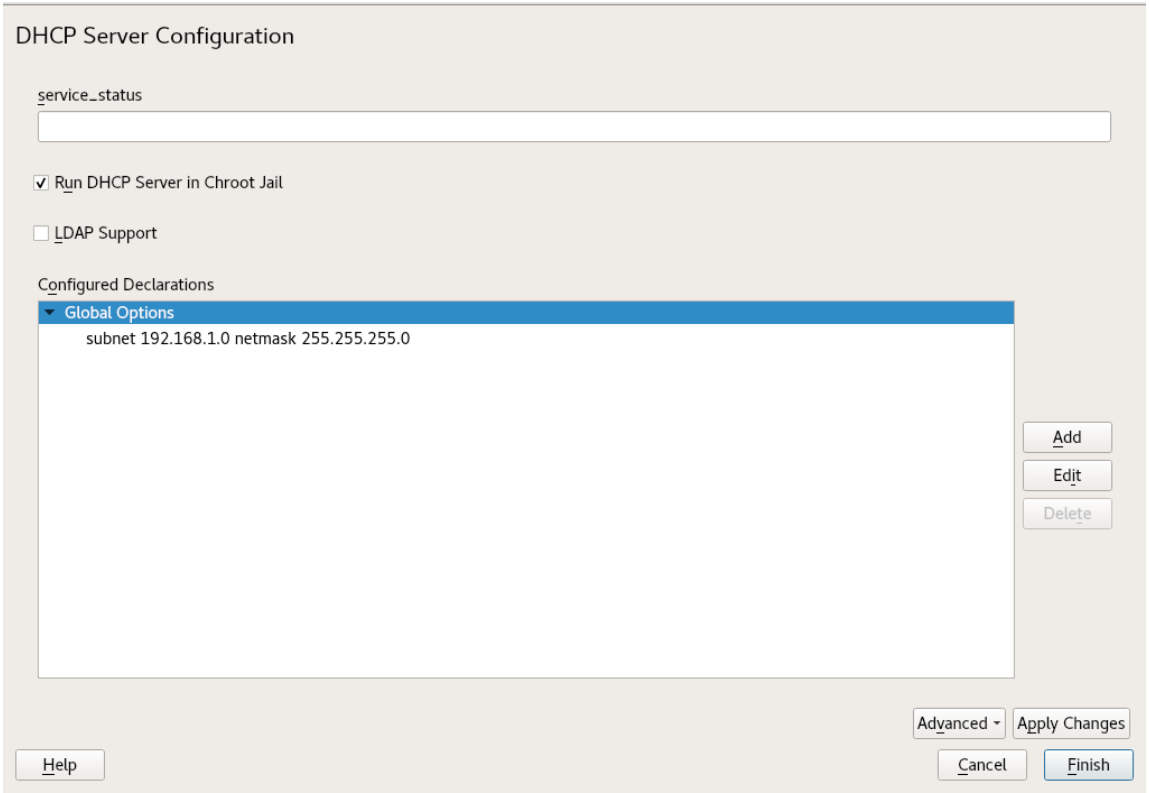


Рисунок 3.6 -Сервер DHCP

В глобальні параметри від сервера DHCP було вписано кілька декларацій. Це діалогове вікно дозволило встановити типи декларації Підмережа, хост, спільний доступ до мережі, група, пул адреси та клас (див. рис.3.7).

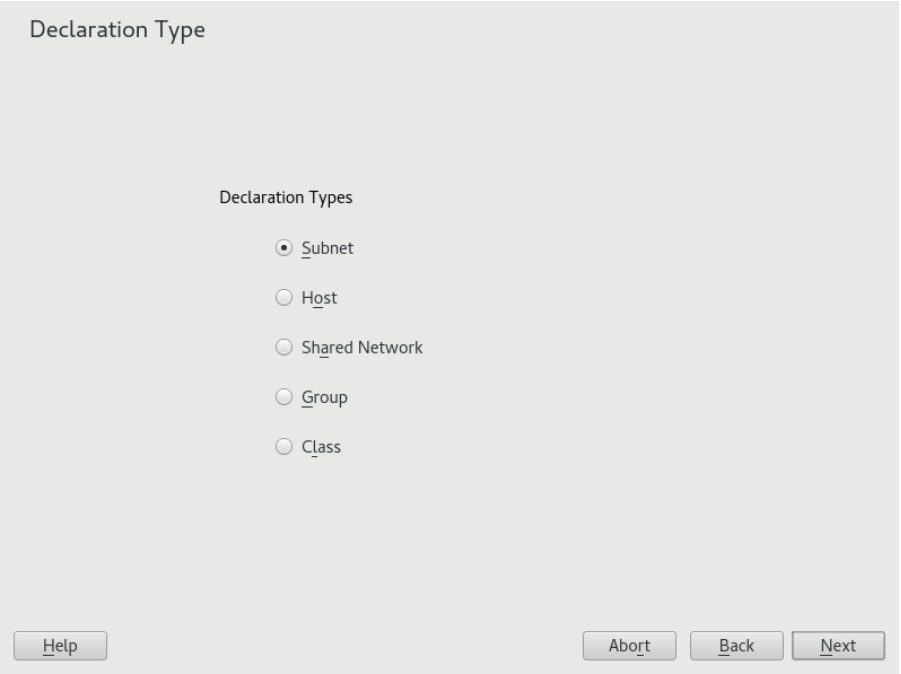


Рисунок 3.7 - Сервер DHCP: Вибір типу декларації

В роботі було сконфігурловано підмережі. За допомогою діалогового вікна було вказано нову підмережу з її IP-адресою та маску мережі. У середній частині діалогового вікна було запущено сервер DHCP параметри для вибраної підмережі.

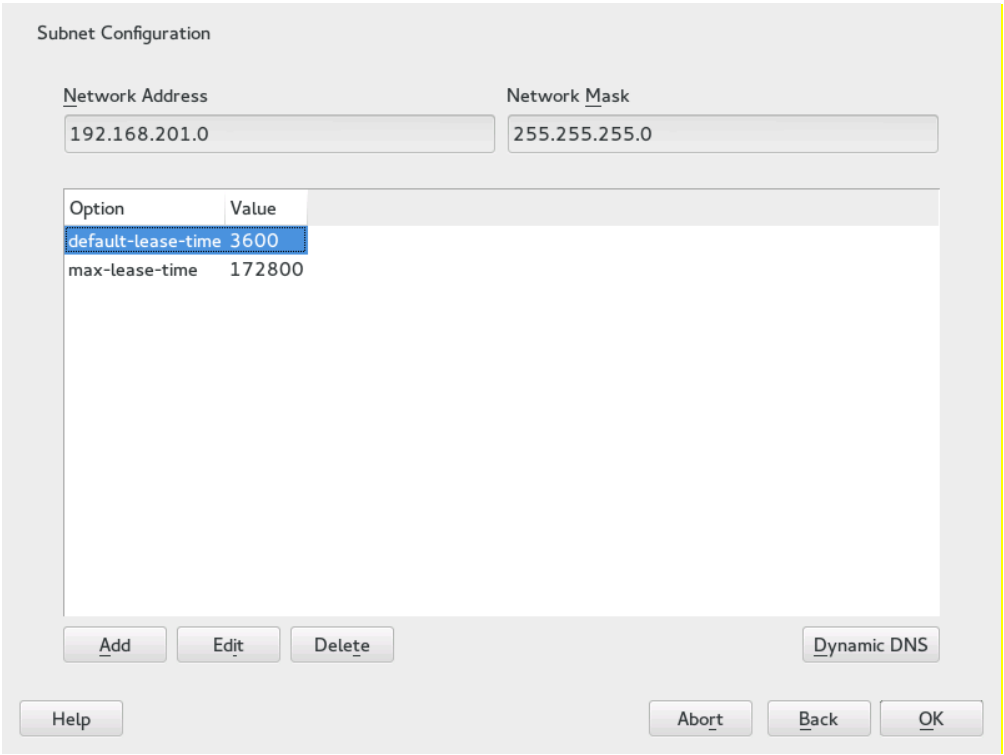


Рисунок 3.8 - DHCP сервер. Налаштування підмережі

Також було здійснено керування ключами TSIG (див. рис 3.9).

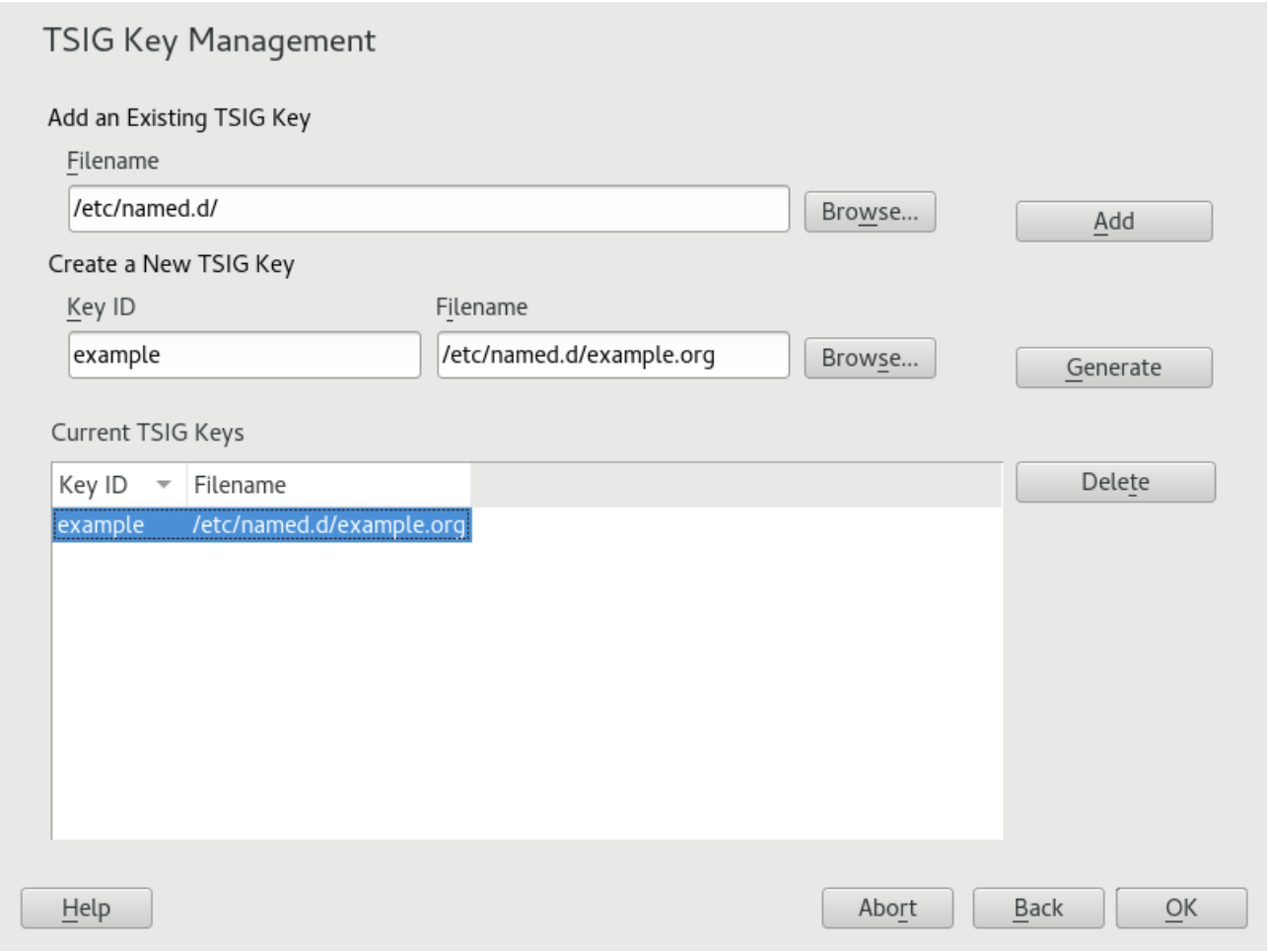


Рисунок 3.9 - Сервер DHCP. Конфігурація TSIG

Далі було активовано динамічний DNS для підмережі (див. рис 3.10).

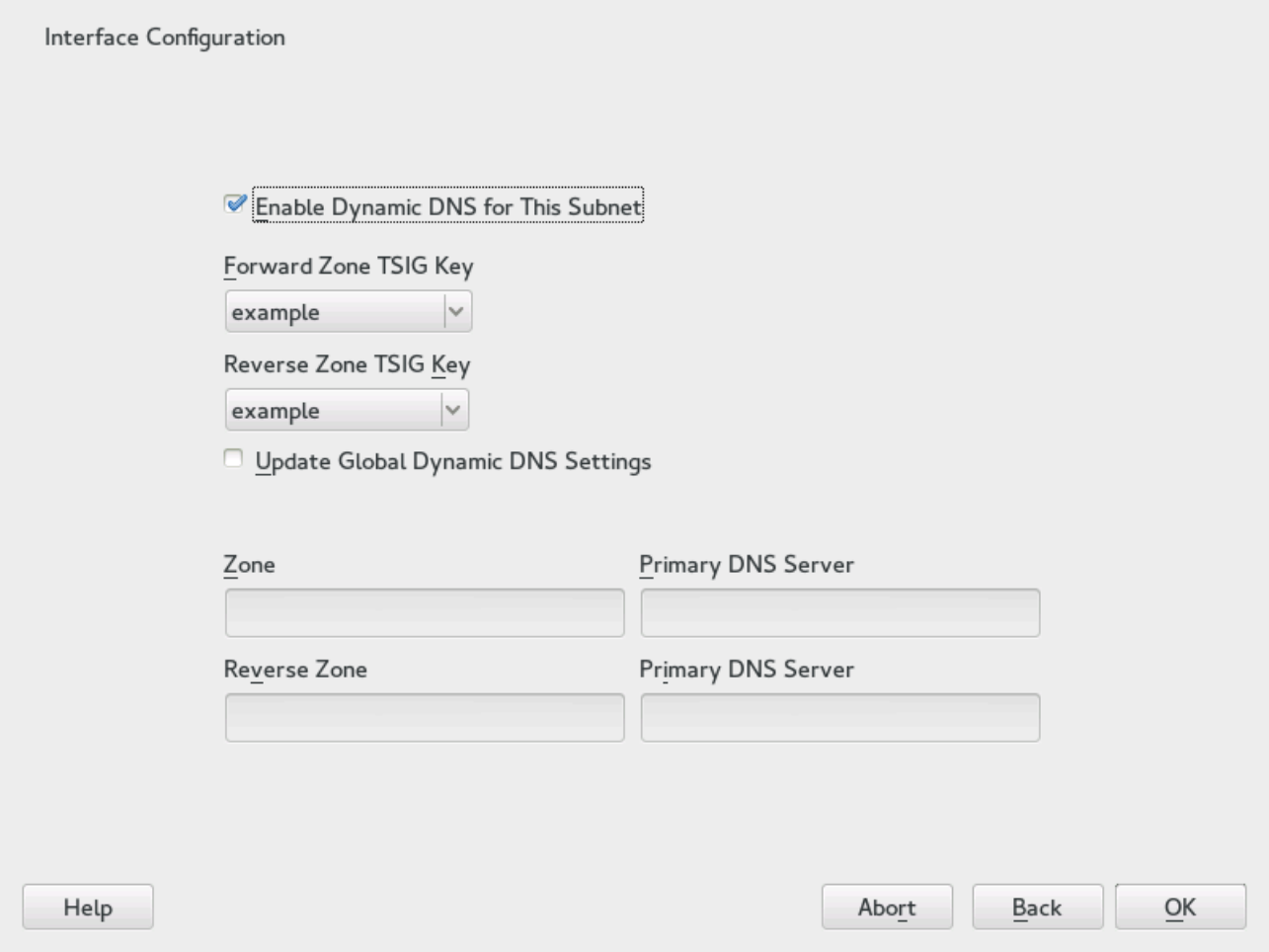


Рисунок 3.10 - Сервер DHCP. Конфігурація інтерфейсу

3.3 Конфігурація брандмауера на основі зонування

Обов'язкова умова - брандмауер на основі зони - це вдосконалений метод брандмауера, що має статус. У брандмауері, що містить державний статус, запис, що містить IP-адресу джерела, IP-адресу призначення, номер порту джерела та номер порту призначення, підтримується для трафіку, що генерується довіреною (приватною) мережею в базі даних, що містить дані про стан. Це буде лише трафік, включаючи відповіді для приватної (довіреної) мережі, що використовує базу даних, що містить дані про стан.

Процедура брандмауера на основі зони. Створення зон і призначення інтерфейсу до них - у брандмауері на основі зони створюються логічні зони. Інтерфейсу присвоюється зона.

За замовчуванням трафік з однієї зони в іншу заборонений.

Створити карту класів - після створення зони створюється політика мапи класів, яка визначає тип трафіку, наприклад ICMP, до якого застосовуватимуться політики.

Було створено карту політики та призначте карту класів політиці - Визначивши тип трафіку в мапі класів, ми повинні визначити, які дії потрібно вжити щодо трафіку.

Дія може здійснювати:

1. Перевірку - це те саме, що й перевірка, тобто лише те, що буде дозволений трафік із зовнішньої мережі, яка буде перевірятися (повернути трафік всередині (довіреної) мережі.

2. Падіння - це дія за замовчуванням для всього трафіку. Карта класів, налаштована на карті політики, може бути налаштована на скидання небажаного трафіку.

3. Пропуск: це дозволить перевезення з однієї зони в іншу. На відміну від дії перевірки, вона не створить стан сеансу для трафіку. Якщо ми хочемо дозволити рух з протилежного напрямку, слід створити відповідну політику.

Також було налаштовано пару зон і призначено політику - пара зон налаштована лише для одного напрямку.

Визначається політика, в якій ідентифікується трафік (який тип трафіку), а потім які дії слід вжити (перевірка відмовлена, дозвіл).

Тоді стало можливим застосування вищевказаної політику до пари зон.

Конфігурація подана рисунком 3.11:

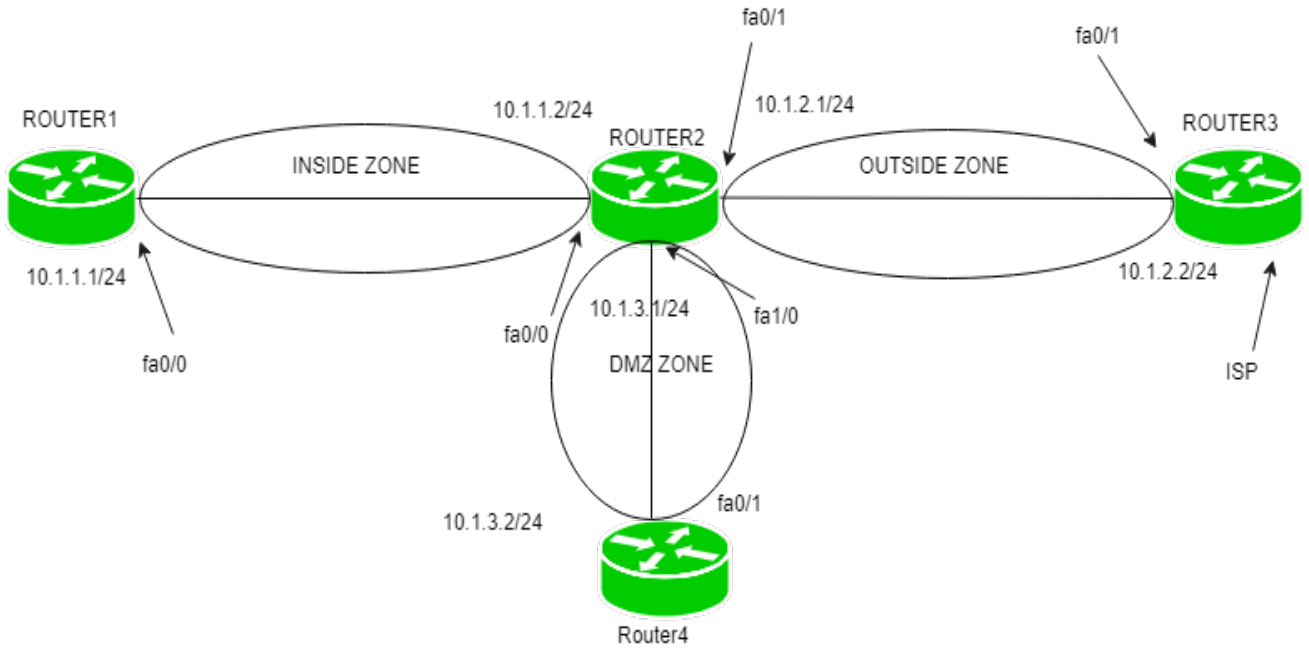


Рисунок 3.11 – Конфігурація брандмауера на основі зонування

Як показано на рисунку, 4 маршрутизатори з'єднані між собою, а саме:

1) Router1, що має ip-адресу 10.1.1.1/24 на своєму інтерфейсі fa0 / 0;

2) _#network_ з IP-адресою 10.1.1.2/24 на своєму fa0 / 0 10.1.2.1/24 на його інтерфейс fa0 / 1 та 10.1.3.1/24 на його інтерфейс fa1 / 0;

3) Router3 має IP-адресу 10.1.2.2/24 на своєму інтерфейсі fa0 / 1, а Router4 має 10.1.3.2/24 на своєму інтерфейсі fa0 / 1.

Спочатку ми повинні виконати маршрутизацію, щоб маршрутизатори були доступні один одному.

Налаштування RIP на _#network_:

_#network__(config)_#router rip

#network(_config-router)#network 10.1.1.0

#network(_config-router)#network 10.1.2.0

#network(_config-router)#network 10.1.3.0

#network(_config-router)#no auto-summary

Тепер, вказавши маршрут за замовчуванням на Router1:

Router1 (_config) #ip route 0.0.0.0 0.0.0.0 10.1.1.2

Надання маршруту за замовчуванням на _#network_

Router3 (_config) #ip route 0.0.0.0 0.0.0.0 10.1.2.1

Даючи маршрут за замовчуванням на Router4

Router4 (_config) #ip route 0.0.0.0 0.0.0.0 10.1.3.1

Тепер ми повинні перерозподілити маршрути за замовчуванням у RIP:

#network(_config) # router rip

#network (_config-router) #default-information originate

Ці маршрутизатори зможуть пінгувати один одного.

Тепер налаштуйте брандмауер на основі зони.

У цьому сценарії було дозволено лише ICMP-трафік і трафік telnet із внутрішньої зони на зовнішню.

Для досягнення цього завдання будуть виконані наступні кроки:

Створення зон і призначення інтерфейсів для зон - спочатку було налаштовано ім'я для зони, а потім застосовано його до інтерфейсу (тут, _#network_). Налаштування зон і назвіть їх як всередині, зовні, так і dmz.

#network(_config)#zone security inside

#network(_config-sec-zone)#exit

#network(_config)#zone_ security outside

#network(_config-sec-zone)#exit

#network(_config)#zone_ security dmz

#network(_config-sec-zone)#exit

Тепер, застосовуючи зони до інтерфейсів.

#network(_config)#interface fa0/0

#network(_config-if)#zone-member security inside

#network(_config)_#interface fa0/1

#network(_config-if)_#zone-member_ security outside

#network(_config)_#interface fa1/0

#network(_config-if)_#zone-member security dmz

Після застосування зон до інтерфейсу маршрутизатори не зможуть пінгувати один одного, оскільки за замовчуванням трафік з однієї зони в іншу буде зменшений (відповідно до політики за замовчуванням).

Також було створено карту класів для визначення типу трафіку, в якому ми хочемо виконати операцію.

Налаштування карти класу із зазначенням типу трафіку, за яким буде проводитися перевірка.

#network(config)_#class-map type inspect match-any in-out

#network(config-cmap)_#match protocol icmp

#network(config-cmap)_#match protocol telnet

match-any означає будь-який з операторів, що збігається на карті класів, тобто для telnet або ICMP.

Було надано назву входу-виходу на карту класу.

В роботі було створено карту політики та застосовано карту класу до карти політики.

Карта політики була налаштована так, щоб зазначити, яку операцію (перевірку, скидання або проходження) буде виконано.

У роботі було використано інспекцію, тобто лише те, що трафік буде надходити ззовні всередину зони, якщо він має запис у базі даних з підтримкою стану (відповіді трафіку, ініційовані всередині зони).

#network(config)_#policy-map type inspect in-out

#network(config-pmap)_#class in-out

#network(config-pmap-c)_#inspect

Тут було налаштовано карту політики з назвою ввести їй присвоєння карти класу (з іменем in-out), і буде здійснено перевірку.

Тут було взято однакову назву map-class та map-policy.

В роботі було створено пару зон і застосовано карту політики до пари зон.

Маршрутизатор2 (конфігурація) # джерело безпеки, виведене з ладу пара зон, всередині пункту призначення зовні

#network(config)_#zone-pair security _in-outpair _source inside destination outside

#network(config-sec-zone-pair)_#service-policy_ type inspect in-out

Тут, у першій команді, зауважте, що in-outpair - це назва пари зон, в якій внутрішня зона буде джерелом, а зовнішня зона буде пунктом призначення.

Це означає, що пара зон була визначена в напрямку від внутрішньої зони до зовнішньої зони. У другій команді in-out - це назва політики-карти.

Тепер внутрішньою зоною буде пінг та телнет зовнішніми пристроями зони, але необхідним було визначити окрему пару зон.

Крім того, пристрої всередині зони тепер зможуть дістатися до пристроїв поза зоною, але не до зони DMZ, оскільки для них не визначена пара зон.

3.7 Висновки

В третьому розділі представлено програмно-апаратну реалізацію локальної комп'ютерної мережі для підприємства «паспортний сервіс, зокреа подано апаратне та програмне забезпечення спроєктованої комп'ютерної мережі.

Також в розділі подано особливості конфігурації брандмауера на основі зонування.

ВИСНОВКИ

В результаті виконаної роботи було спроєктовано та реалізовано локальну комп’ютерну мережу для підприємства «Паспортний сервіс».

В першому розділі було досліджено предметнуобласть, зокрема було окреслено цілі застосування комп’ютерних мереж, проаналізовано типи топології мережі, поставлено задачу проектування мережі.

В другому розділі було подано особливості проєктування комп’ютерної мережі, зокрема розглянуто мережеві пристрої, представлено типи носіїв передачі даних.

Також в розділі було подано особливості впровадження брандмауера в комп'ютерну мережу.

В третьому розділі представлено програмно-апаратну реалізацію локальної комп’ютерної мережі для підприємства «паспортний сервіс, зокреа подано апаратне та програмне забезпечення спроєктованої комп’ютерної мережі.

Також в розділі подано особливості конфігурації брандмауера на основі зонування.

В додатках представлено копії креслень спроєктованої мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Комп’ютерні мережі : навчальний посібник / Азаров О. Д., Захарченко С. М., Кадук О. В. та ін. Вінниця : ВНТУ, 2013. 371с.

2. Буров Є. В. Комп'ютерні мережі: підручник / Євген Вікторович Буров. Львів: «Магнолія 2006», 2010. 262 с.

3. Кулаков Ю.О., Жуков І.А. Комп’ютерні мережі. Навчальний посібник/ за ред. Кулакова Ю.О. К: НАУ, 2009. -392 с.

4. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. Львів: «Магнолія 2006», 2013. 256 с.

5. Лосев Ю. І. Комп'ютерні мережі: навчальний посібник / Ю. І. Лосев, К. М. Руккас,. С. І. Шматков / За редакцією Ю. І. Лосева. – Х. : ХНУ імені В. Н. Каразіна, 2013. 248 с.

6. Олифер В. Г. Компьютерные сети. Принципы, технологии, прото-колы : учебник для ВУЗов / В. Г. Олифер, Н. А. Олифер. — С-Пт. : Пи-тер, 2013. 944 с

7. Ситник В.Ф., Козак І.А. Телекомунікації в бізнесі: Навч.-посібник. К.: КНЕУ, 2003. 204с.

8. Валецька Т.М. Комп’ютерні мережі: Апаратні засоби.Навч. посібник.-К.:Центр навч. Літератури, 2002.

9. Лозікова Г.М. Комп’ютерні мережі.Навч.-методичний посібник.-К.:Центр навч. Літератури, 2004.

10. Спартак Марк, Паппас Френк и др. Компьютерные сети и сетевие технологии: Пер. с англ. К.:000 “ТНД ДС”, 2002. 736 с.

11. Александров А. В. и ф. Электронная почта для каждого. М.: Приор, 2006.— 160с.

12. Андрианов В. И., Бородин В. А., Соколов А. В. «Шпионские штучки» и уст ройства для защиты объектов и информации: Справоч. пособие. Спб.: Лань, 2006. 272 с.

13. Андрианов В. И., Соколов А. В. Охранные устройства для дома и офиса. Спб.: Лань, 2007.304 с.

14. Камер Д. Компьютерные сети и Internet.Пер. с англ.-М.-К.:”Вильямс”, 2002.

15. Коварт Р., Уотерс Б. Windows NT Server. Учебный курс. С.-Пт.-М.-Харьков-Минск, “Питер”, 1999.

16. Архитектура, протоколы и тестирование открытых информационных сетей: Толковый словарь. М: Финансы и статистика, 2000.

17. Блек Ю. Сети ЭВМ: протоколы, стандарты, интерфейсы. М.: Мир, 2000.

18. Боккер Я. ISDN -і- цифровая сеть с интеграцией служб. Понятия, методы, системы. М.: Радио и связь, 2001.

19. Бэрри Нанс. Компьютерные сети. М.: Бином, 2005.

20. Веттіі Дітер. Novell NetWare. К.: Торгово-видавниче бюро BHV, 2003.

21. Вильховченко С. Д. Модем-97: выбор, установка, настройка. Бесплатные приложения: терминалы, скрипты, факсы, BBS, Fido.М.: АВҐ, 2007. 541 С.

22. Гольц Г. Робочі станції і інформаційні мережі. М.: Машинобудування, 2000.

23. Джамса К. Изучи сам Java сегодня / Пер. с англ. Минск: Шпури, 2006. 416 с.

24. Джейсон М. JavaScript: основы программирования / Пер. с англ. К.: Из-дат. группа BHV, 2007. —512 с.

25. Дунаев С. lNTRANET-технологии. —М.: Диалог-МИФИ, 2007. 288 с.

26. Жуков Ігор Анатолійович. Комп`ютерні мережі та технології: навчальний посібник /Жуков І.А., Гуменюк В.О., Альтман І.Є./ К.: НАУ, 2004.-276с.

27. Мельников В. Криптография от папируса до компьютера. М.: ABF, 2006.

28. Крэйнек Д. Windows 10 / Пер. с англ. М: Компьютер: ЮНИТИ, 2016. 312 с.

29. Кулаков Ю. А., Луцкий Г. М. Компьютерные сети. К.: Юниор, 2006. - 384 с.

30. Мельников В. В. Защита информации в компьютерных системах. М.: Финансы и статистика: Электроинформ, 2007. 364 с.

31. Нессер Д. Дж. Оптимизация и поиск неисправностей в сетях. К.: Диалектика, 2006.384 с.

32. Технологии электронных коммуникаций. М: ЭКОТРЕНДЗ, 2003. т. 1-31.

33. Фафенберг Б., Уолл Д. Толковый словарь по компьютерным технологиям, Internet. 6-е изд. К.: Диалектика, 2006.480 с.

34. Фролов А. В., Фролов Г. В. Сети компьютеров в вашем офисе. М.: Диализ МИФИ, 2006. 272 с.

35. Хант К. Персональные компьютеры в сетях TCP/IP: руководство администратора сети / Пер. с англ. К.: Издат. группа BHV, 2007. 384 с.

36. Шатт С. Мир компьютерных сетей / Пер. с англ. К.: BHV, 2006. 288 с.

37. Швиденко М.З., Матус Ю.В.. Комп'ютерні мережні технології. / Навч.-метод. посібник. Київ. ТОВ "Авета", 2008.

38. Швиденко М.З., Матус Ю.В.. Технології комп'ютерних мереж. Навч.-метод. посібник., Київ. Видавництво ООО "Береста", 2007.

39. Хеслоп Б., Бадник Л. HTML с самого начала. СПб.: Питер, 2007.

40. Anylogic. URL: https://www.anylogic.ru/

41. Cisco. URL: www.cisco.com.

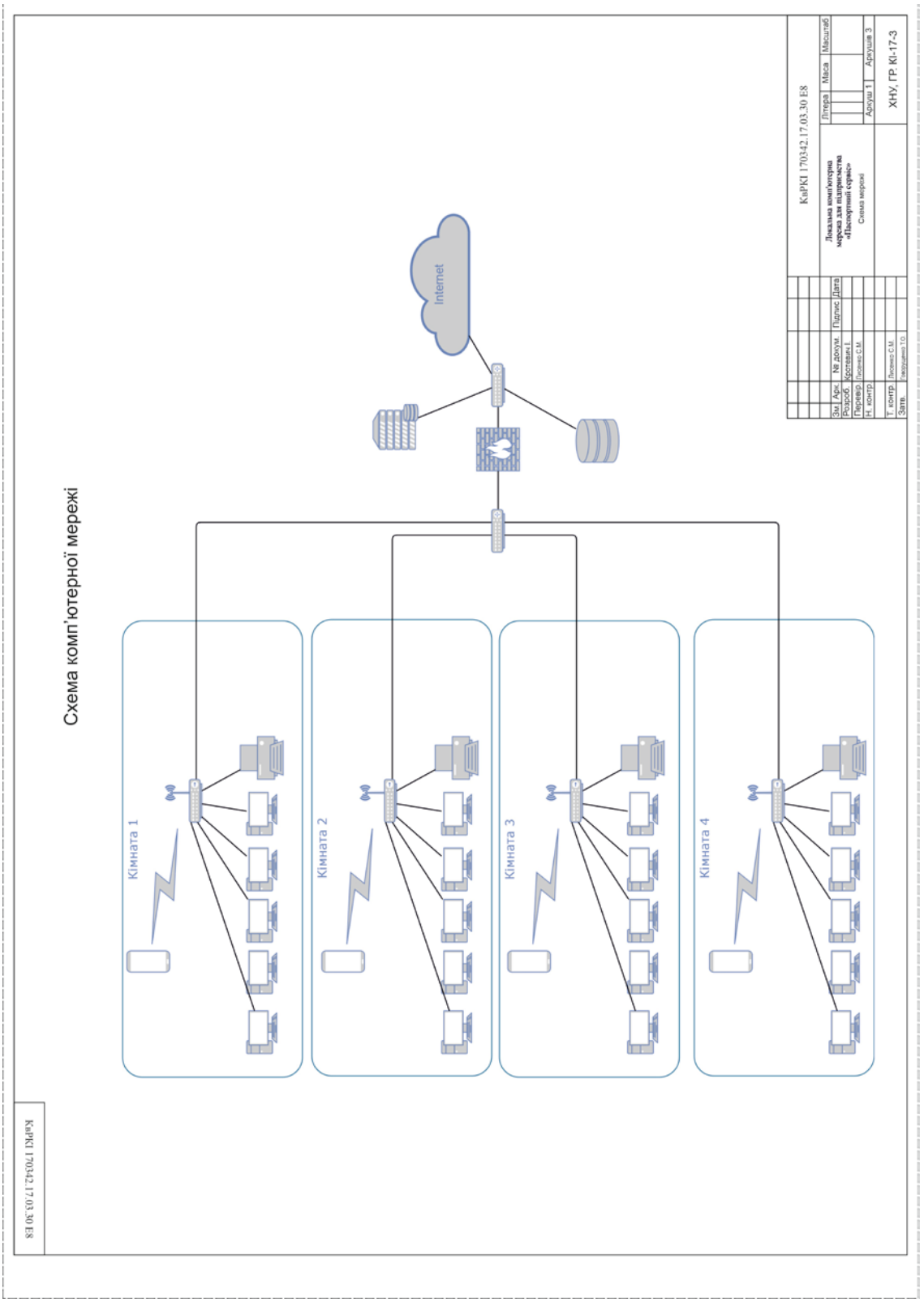
42. SUSE Linux Server 15. URL: https: https://www.suse.com/download/sled.

43. Windows 10. URL: www.microsoft.com.

Додаток А

(обов’язковий)

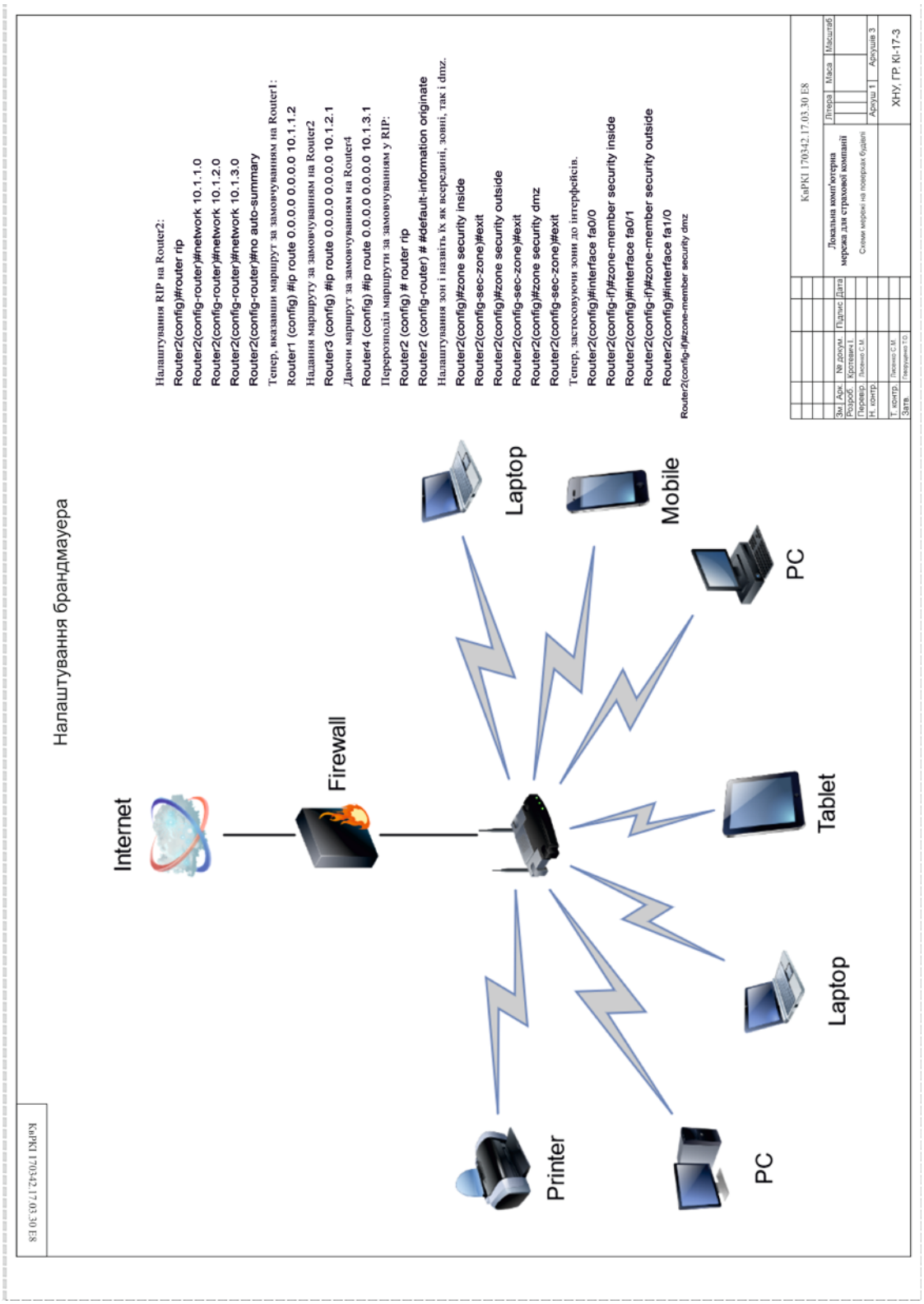
Копія креслення «Схеми мережі»



Додаток Б

(обов’язковий)

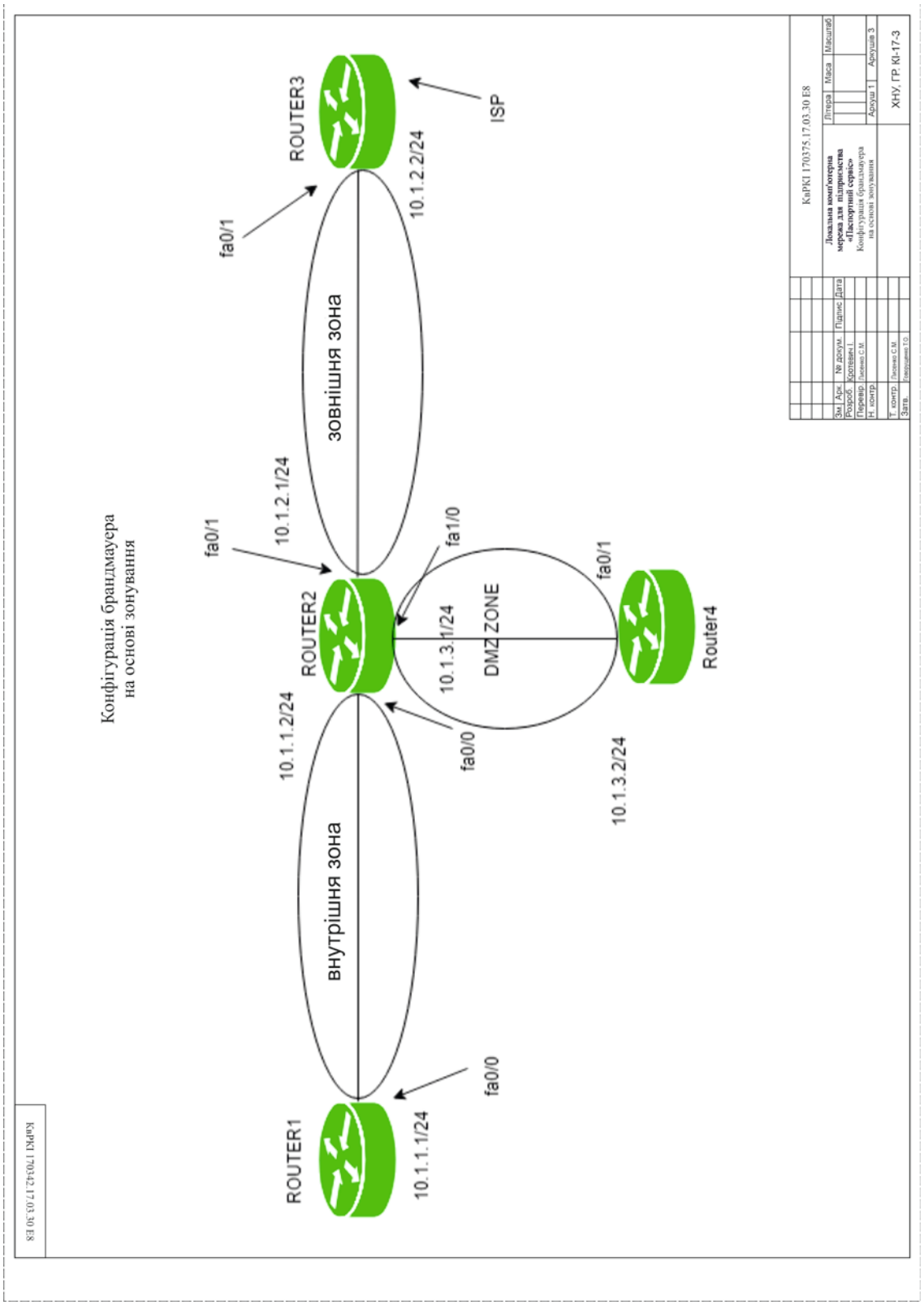
Копія креслення «Схеми мережі на поверхах будівлі мережі»



Додаток В

(обов’язковий)

Копія креслення «Конфігурація брандмауера на основі зонування»



Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 11%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 93024 Название: Локальна комп'ютерна мережа для підприємства «Паспортний сервіс» Добавлено в БД: 2021-06-10 Авторы: Кротевич І. Руководители: С.М. Лисенко Консультанты: Оппоненты:	Символы	Лексемы	Символы	Лексемы
	51472	527	586 (1%)	8 (2%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Ім'я користувача:
Кафедра КІ

ID перевірки:
1008255397

Дата перевірки:
10.06.2021 11:43:41 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
10.06.2021 11:44:14 EEST

ID користувача:
100005591

Назва документа: Кротевич_Локальна комп'ютерна мережа для підприємства «Паспортний сервіс»

Кількість сторінок: 64 Кількість слів: 8329 Кількість символів: 63258 Розмір файлу: 2.02 MB ID файлу: 1008326972

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

4.17%
Схожість

Найбільша схожість: 1.79% з джерелом з Бібліотеки (ID файлу: 1008275345)

2.43% Джерела з Інтернету	67	Сторінка 66
2.04% Джерела з Бібліотеки	66	Сторінка 66

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	7
Підозріле форматування	13 сторінок

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Кротевич Іван Леонідович

Тема: Локальна комп'ютерна мережа для підприємства «Паспортний сервіс»

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3____ Кількість сторінок записки _____

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є проєктування локальної комп'ютерної мережі для підприємства «Паспортний сервіс».

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: В першому розділі кваліфікаційної роботи проведено дослідження предметної області (проаналізовано теорію проєктування комп'ютерних мереж) та виконано постановку задачі дослідження. В другому розділі кваліфікаційної роботи проведено аналіз засобів проєктування комп'ютерних мереж. В третьому розділі кваліфікаційної роботи виконано реалізацію локальної комп'ютерної мережі для підприємства «Паспортний сервіс», зокрема спроєктовано карту локальної мережі для підприємства «Паспортний сервіс», топологічну схему корпоративної локальної мережі.

4. Позитивні сторони роботи: висока практична цінність проведеної роботи.

5. Негативні сторони роботи: не достатньо описане програмне забезпечення, яке необхідне для функціонування інфраструктури для підприємства «Паспортний сервіс».

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: -

9. Оцінка дипломної роботи: добре

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) доцент кафедри інженерії програмного забезпечення Хмельницького національного університету, к.т.н., доцент, Гурман І.В.

"10" червня 2021 р. (підпис)

Завідувачу кафедри КІСП
д-ру техн.наук, проф. Говорущенко Т. О.

Кротевича І.Л..
ПІБ здобувача вищої освіти
ФПКТС, 4 курсу, групи КІ-17-3

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений(а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність плагіату ознайомлений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

10.07.2021

_____ _____

дата підпис

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА СИСТЕМНОГО ПРОГРАМУВАННЯ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Локальна комп'ютерна мережа для підприємства «Паспортний сервіс»

Автор: Кротевич Іван Леонідович

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Лисенко Сергій Миколайович, д.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
2) в якості запозичень в роботі виступає графічна рамка, а також титульний лист та бланк задання, які загальними для усіх студентів;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 4.17%, що з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ С. М. Лисенко

Гарант ОП _____ С. М. Лисенко

Завідувач кафедри КІСП _____ Т. О. Говорущенко