

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 бакалавра
на тему: «ПРОЕКТ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ
ОРГАНІЗАЦІЇ НА БАЗІ ПРОТОКОЛІВ GRE ТА IP-SECURITY»

Виконав студент 4-го курсу, групи КІ-3
спеціальності 123 «Комп'ютерна інженерія»

 Охріменко Д.С.

Керівник  Єфіменко. А.А.

Рецензент  Россінський Ю. М.

Житомир – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ФАКУЛЬТЕТ інформаційно-комп'ютерних технологій

(назва прописними)

КАФЕДРА комп'ютерної інженерії та кібербезпеки

(назва прописними)

СПЕЦІАЛЬНІСТЬ 123 «Комп'ютерна інженерія»

(назва прописними)

ЗАТВЕРДЖУЮ

Зав. кафедри комп'ютерної

інженерії та кібербезпеки

(назва кафедри)

Єфіменко А.А.

«12» 04 2021 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента Охріменка Дмитра Сергійовича

Тема роботи: «ПРОЕКТ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ
ОРГАНІЗАЦІЇ НА БАЗІ ПРОТОКОЛІВ GRE TA IP SECURITY»

Затверджена Наказом університету від «12» 04 2021 р. № 133/с

Термін здачі студентом закінченої роботи _____

Вихідні дані роботи (зазначається предмет і об'єкт дослідження) Об'єкт
дослідження: процес побудови та тестування роботи корпоративної мережі
підприємства. Предмет дослідження: набір протоколів для забезпечення захисту
даних IPsec, мережевий протокол рівня застосунків SSH, списки доступу ACL та
протокол тунелювання мережевих пакетів GRE.....

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко. А.А.	2.03.21	2.03.21
2	Єфіменко. А.А.	10.04.21	10.04.21
3	Єфіменко. А.А.	5.05.21	5.05.21

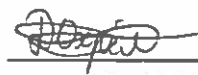
Керівник Єфіменко. А.А.

Єфіменко А.А.

Календарний план

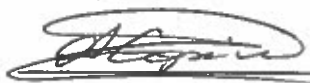
№ з/п	Назва етапів випускної кваліфікаційної роботи	Терміни виконання етапів	Відмітка про виконання
1	Проаналізувати літературні джерела, по темі дипломної роботи	10.12.2020 – 15.12.2020	Виконано
2	Проаналізувати матеріали відповідно методів та засобів віддаленого доступу та протоколів тунелювання	16.01.2021 – 26.01.2021	Виконано
3	Розрахунок параметрів адресації та вибір технології для реалізації	27.01.2021 – 06.02.2021	Виконано
4	Розробити та налаштувати захищену КМ	07.02.2021 - 17.02.2021	Виконано
5	Виконати адміністрування мережі та перевірити працездатність системи	18.02.2021 – 26.02.2021	Виконано
6	Розробити структуру та зміст пояснювальної записки	27.02.2021 – 30.03.2021	Виконано
7	Оформити пояснювальну записку, розробити та оформити презентаційні матеріали до пояснювальної записки	01.04.2021 – 14.05.2021	Виконано
8	Захист дипломної роботи	05.06.2021 – 18.06.2021	Виконано

Студент



Д.С. Охріменко

Керівник проекту



А.А. Єфіменко

РЕФЕРАТ

Структура випускної роботи бакалавра на тему - «Проект корпоративної комп'ютерної мережі організації на базі протоколів GRE та IPSecurity» складається з вступу, трьох розділів, висновків, переліку посилань на 26 найменувань, додатків. Повний обсяг роботи становить 127 сторінок, містить 117 малюнків і 12 таблиць.

В результаті виконання дипломної роботи була спроектована захищена корпоративна мережа організації на базі протоколів GRE та IP-Security, а також була впроваджена система віддаленого доступу для створеної мережі у віртуальному середовищі GNS3. Налаштовано роботу протоколів динамічної маршрутизації OSPF та EIGRP. На створеній інформаційно-комунікаційній мережі було протестовано роботу протоколів GRE та IP-Security, які було застосовано до кінцевих маршрутизаторів рівня розподілу.

При використанні IPSec відбувається подвійна інкапсуляція, що знижує продуктивність - це саме та ціна, яку доведеться заплатити за безпеку переданих даних по тунелям, однак ми отримали велику захищену та відмовостійку мережу з можливістю віддаленого адміністрування маршрутизаторів мережі.

Ключові слова: протоколи віддаленого доступу, протокол тунелювання GRE, протокол маршрутизації OSPF, протокол маршрутизації EIGRP, протокол IPSec, безпека мереж з пакетною передачею даних, інформаційна безпека, захист інформації.

					Житомирська політехніка 21.123.15.000			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Охріменко Д.С.		16.06.21	Проект корпоративної комп'ютерної мережі організації на базі протоколів GRE та IPSec Пояснювальна записка	Літ.	Арк.	Аркушів
Рецензент		Росієнський Ю.М.		16.06.21			4	127
Керівник		Єфіменко А.А.		16.06.21		ФІКТ Гр. КІ-3(2)		
Н. контр.								
Зав. каф		Єфіменко А.А.		16.06.21				

ABSTRACT

The structure of the bachelor's graduate work on the topic - "Project of the corporate computer network of the organization based on the GRE and IPSecurity protocols" consists of an introduction, three sections, conclusions, a list of references to 26 titles, applications. Documentation for bachelor's graduate work contains 149 pages, 117 illustrations, and 12 tables.

As a result of the bachelor's graduate work, a secure corporate network of the organization was designed on the basis of GRE and IP-Security protocols, and a remote access system was introduced for the created network in the GNS3 virtual environment. The OSPF and EIGRP dynamic routing protocols are configured. The work of the GRE and IP-Security protocols, which were applied to the final routers of the distribution layer, was tested on the created information and communication network.

When using IPSec, there is double encapsulation, which reduces performance - this is the price you will have to pay for the security of transmitted data through tunnels, but we have a large secure and fault-tolerant network with the ability to remotely administer network routers.

Keywords: remote access protocols, GRE tunneling protocol, OSPF routing protocol, EIGRP routing protocol, IPSec protocol, packet data network security, information security.

		Охріменко. Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	8
ВСТУП.....	10
РОЗДІЛ 1. Теоретичні аспекти організації захищених з'єднань корпоративних комп'ютерних мереж.	13
1.1. Базові підходи до побудови захищених корпоративних мереж.	13
1.2. Протоколи та технології побудови захищених мережних з'єднань.	16
1.2.1. Забезпечення безпеки корпоративної мережі за OSI моделлю.	16
1.2.2. Безпека на фізичному рівні моделі OSI.	18
1.2.3. Безпека на канальному рівні моделі OSI.	19
1.2.4. Безпека на мережному рівні моделі OSI.	21
1.2.5. Безпека на сеансовому рівні моделі OSI.	24
1.2.6. Протоколи віддаленого доступу.	25
1.2.7. Створення списків управління доступом (ACL).	30
1.2.8. Типи тунельних з'єднань, які застосовуються для побудови VPN-мереж.	31
1.2.9. Технологія Active Directory в Windows Server для зберігання та організації об'єктів в мережі в ієрархічній захищеній логічній структурі.	33
1.3. Принципи організації захищених мережних з'єднань на базі протоколів GRE та IPSec.	35
1.3.2. Internet Protocol Security (IPsec) - стек протоколів для безпечного обміну інформацією по IP.	35
1.3.3. Протокол тунелювання мережових пакетів GRE.	39
1.4. Аналіз існуючих рішень для створення мережі з використанням технологій протоколу тунелювання GRE, протоколу захисту даних IP-Security, протоколів динамічної маршрутизації OSPF та EIGRP, протоколу віддаленого доступу SSH.	42
1.4.1. Аналіз створеного рішення з використанням технологій протоколу тунелювання GRE, протоколу захисту даних IP-Security, протоколів динамічної маршрутизації OSPF та EIGRP.	42
1.4.2. Аналіз створеного рішення з використанням мережевого протоколу SSH.	51
1.5. Технічна постановка завдання.	54
Висновки до першого розділу.	55

РОЗДІЛ 2. ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ.....	56
2.1. Розробка топології комп'ютерної мережі.....	56
2.2. Розробка схеми адресації мережі.	64
2.3. Розробка налаштувань для GRE тунелів з використанням шифрування IPSec.	69
2.4. Розробка параметрів віддаленого підключення для маршрутизаторів мережі за протоколом SSHv2.....	74
2.5. Розробка параметрів для налаштування Active Directory на сервері.	75
Висновки до другого розділу.	76
РОЗДІЛ 3. АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ	77
3.1. Вибір обладнання для організації роботи мережі.	77
3.2. Налаштування маршрутизаторів мережі.....	80
3.4. Налаштування та встановлення Active Directory із роллю первинного контролера домену на першому сервері.....	97
3.5. Перевірка працездатності мережі.	108
3.6. Здійснення перевірки доступу на читання та зміни папки із робочої станції WS2 (Windows 10) під двома створеними раніше користувачами.	124
Висновки до третього розділу.....	127
ВИСНОВКИ	128
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	130

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПК – Персональний комп'ютер

FE – Fast Ethernet

Eth – Ethernet Interface

MAC (MediaAccessControl) – Управління доступом до середовища

IP – Internet Protocol

VPN (Virtual Private Network) - «віртуальна приватна мережа»

TCP (Transmission Control Protocol) - протокол управління передачею

UDP (User Datagram Protocol) - протокол призначених для користувача датаграм

SSH (Secure Shell) – мережевий протокол прикладного рівня

SSL (Secure Sockets Layer) – протокол безпеки на транспортному рівні

PPP (Point-to-Point Protocol) - двоточковий протокол канального рівня (Data Link) мережевий моделі OSI

PPPoE (Point-to-point protocol over Ethernet) - мережевий протокол канального рівня другий рівень мережевої моделі OSI

IPsec скорочення від IP Security - набір протоколів для забезпечення захисту даних, що передаються по межсетевому протоколу IP

OpenVPN - вільна реалізація технології віртуальної приватної мережі (VPN)

PPTP (Point-to-Point Tunneling Protocol) - тунельний протокол типу точка-точка

L2TP (Layer 2 Tunneling Protocol) - протокол тунелювання другого рівня

MPLS (Multiprotocol label switching) - багатопроTOCOLьна комутація по мітках

OpenWrt (OPEN Wireless Router) - проект з відкритим кодом для вбудованої операційної системи на базі Linux

LAN (Local Area Network) - локальні мережі

OSPF – OpenShortestPathFirst – Протокол динамічної маршрутизації

EIGRP - Enhanced Interior Gateway Routing Protocol – Протокол динамічної маршрутизації

GRE - Generic Routing Encapsulation - Протокол тунелювання мережевих пакетів

ISAKMP (Internet Security Association and Key Management Protocol) - Інтернет протокол асоціацій безпеки та керування ключами

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

FTP File Transfer Protocol - Протокол пересилки файлів

ACL (Access list) – список управління доступом

IPSec (IP Security) – набір протоколів для захисту даних

ME - міжмережевий екран

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми роботи: створення локальної корпоративної мережі — це важлива умова функціонування будь-якої сучасної організації, будь-якого бізнесу, у будь-якій галузі. Сьогодні майже кожна організація тісно пов'язана з використанням власної корпоративної мережі, що передбачає оперативний обмін даними як в межах окремого офісу, так і в межах всього світу, завдяки підключенню до глобальної мережі Інтернет. Головне завдання при побудові корпоративної мережі — оптимізація обробки та розподілу інформаційних потоків, а також захист переданих даних. Користувачами корпоративної мережі є тільки співробітники даного підприємства. Високий рівень безпеки і відповідність нормативним вимогам є обов'язковими умовами в проектах по розгортанню корпоративних мереж. Для захисту власних інформаційних ресурсів підприємства впроваджують в інфраструктуру рішення щодо забезпечення безпеки мережі, що гарантують безпеку мережі і комерційних даних на всіх рівнях. Завдяки корпоративній мережі користувачі (співробітники) зможуть отримати доступ до загальних ресурсів, зможуть спільно використовувати принтери та інше мережеве обладнання.

Наше головне завдання при побудові корпоративної мережі — оптимізація обробки та розподілу інформаційних потоків, а також захист переданих даних. Важливість захисту інформаційних ресурсів компанії очевидна — від цього безпосередньо залежить безпека даних, які належать підприємству, його ефективність і рентабельність. Реалізовані засоби захисту не повинні створювати «вузьких» місць у мережі, тобто не повинні суттєво впливати на масштабованість, продуктивність мережі, маршрутизацію, а також повинні забезпечити централізоване адміністрування мережі. Для того щоб забезпечити доступ до послуг локальної мережі при відсутності безпосереднього підключення до неї, служать служби віддаленого доступу до мережі. Служба віддаленого доступу до комп'ютера була першою службою комп'ютерних мереж. Вона надавала користувачу можливість подавати команди на опрацювання даних та переглядати результати їх виконання на одному комп'ютері, а виконувати команди на іншому.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Безумовною перевагою таких систем є зниження витрат на обслуговування обладнання організації. По-перше, зникає необхідність виділення офісного простору виїзним працівникам (наприклад, менеджерам з продажу, програмістам, дизайнерам, журналістам, перекладачам). По-друге, не потрібно купувати додатково меблі, комп'ютер та інше обладнання. По-третє, збільшується ефективність роботи організації її філій, що досягається за рахунок автоматизації багатьох бізнес-процесів. Таким чином, віддалений доступ - це не розкіш, а ще один компонент успішного ведення сучасного адміністрування мережі.

З розвитком мереж з'являються нові типи підключення, зростає трафік, який потребує контролю та захисту. Актуальність, безпеки переданих даних і їх захисту від несанкціонованого доступу в системах віддаленого доступу вимагає особливо пильної уваги і застосування спеціальних методик, які гарантували б достатню конфіденційність і достовірність даних. В іншому випадку, хакер, який підключився в якості віддаленого клієнта або перехоплюючи трафік реально існуючого клієнта, зможе вкрати дані які є комерційною таємницею або фальсифікувати їх. Захистити наш трафік можна за умови використання механізмів його тунелювання та шифрування, що в більшості випадків дозволяє повністю позбавитись від втрати переданої інформації. Тому стає очевидним необхідність створення зв'язки «віддалений доступ + тунелювання + аутентифікація + шифрування», яка дозволяє побудувати захищену корпоративну мережу VPN.

Дана технологія призначена для криптографічного захисту даних, що передаються по комп'ютерних мережах. Віртуальна приватна мережа являє собою сукупність мережевих з'єднань між декількома VPN-шлюзами, на яких виробляється шифрування мережевого трафіку. VPN-шлюзи ще називають криптографічними шлюзами або крипто-шлюзи. Такі властивості технології VPN надають можливість об'єднати територіально віддалені один від одного локальні мережі офісів компанії в єдину корпоративну інформаційну мережу.

Важливість захисту інформаційних ресурсів компанії очевидна – від цього безпосередньо залежить безпека даних, які належать підприємству, його ефективності і рентабельності. Залежно від застосовуваних протоколів і

		Охріменко Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

призначення, VPN може забезпечувати з'єднання трьох видів: вузол-вузол, вузол-мережу та мережу-мережу. Безліч ІТ організацій і мережевих провайдерів успішно використовують цю технологію, в першу чергу, з метою захисту каналів передачі даних і витрат на її утримання, а також для забезпечення високого рівня безпеки, захищеності, надійності мережі, для зменшення часу і складності розгортання нових сервісів.

Отже, корпоративна мережа - це кровоносна система компанії, в якій елементи пов'язані між собою, вони виконують окремі види робіт в рамках єдиного бізнес процесу, застосування технологій віддаленого доступу, тунелювання та шифрування інформації є важливим завданням для кожної організації.

Мета роботи: проектування корпоративної мережі в графічному емуляторі мереж GNS3 з можливістю віддаленого управління обладнанням та забезпечення взаємодії користувачів системи з належною якістю та мінімізацією затримки передачі даних по захищених каналах зв'язку.

Завдання дипломної роботи: дослідити технології, які застосовується для доступу до віддалених мереж, створити безпечну та високошвидкісну корпоративну мережу для передачі даних та захистити трафік за допомогою механізмів тунелювання та шифрування.

Об'єкт дослідження: проектування системи віддаленого доступу для захищеної інформаційно-комунікаційної мережі організації.

Предмет дослідження: набір протоколів для забезпечення захисту даних IPsec, мережевий протокол рівня застосунків SSH та протокол тунелювання мережевих пакетів GRE.

Практична значимість роботи: забезпечення безперебійної роботи мережі, з можливістю віддаленого управління обладнанням та забезпечення взаємодії користувачів системи з належною якістю та мінімізацією затримки передачі даних по захищених каналах зв'язку. Для цього була розроблена схема і обрано мережеве обладнання. Створена мережа дозволяє адміністратору швидко реагувати на несправності та налаштовувати віддалено обладнання мережі.

Методи досліджень: моделювання в графічному емуляторі мереж GNS3 та додаток для підключення до обладнання Putty.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. Теоретичні аспекти організації захищених з'єднань корпоративних комп'ютерних мереж.

1.1. Базові підходи до побудови захищених корпоративних мереж.

Кожна організація представляє собою сукупність взаємодіючих структурних елементів (підрозділів), кожен з яких може мати свою особливість. Корпоративна мережа — це інфраструктура, призначена для передачі великого обсягу різнорідних інформаційних потоків, це мережа що працює по протоколу TCP/IP, використовує різні типи зв'язку, комунікаційні протоколи та дозволяє забезпечити всі потреби організації для інформаційного обміну даними. Головне завдання при побудові корпоративної мережі — оптимізація обробки та розподілу інформаційних потоків, а також захист переданих даних. Важливість захисту інформаційних ресурсів компанії очевидна – від цього безпосередньо залежить безпека даних, які належать підприємству, його ефективність і рентабельність. Реалізовані засоби захисту не повинні створювати «вузьких» місць у мережі, тобто не повинні суттєво впливати на масштабованість, продуктивність мережі, маршрутизацію, а також повинні забезпечити централізоване адміністрування мережі.

Створення локальної корпоративної мережі — це важлива умова функціонування будь-якої сучасної організації, будь-якого бізнесу, у будь-якій галузі. Від правильності і відповідності параметрів мережі усім вимогам підприємства буде залежати робота систем та якість роботи підприємства загалом. Користувачами корпоративної мережі є тільки співробітники даного підприємства. Завдяки корпоративній мережі співробітники (користувачі) зможуть отримати доступ до загальних ресурсів, зможуть спільно використовувати принтери та інше мережеве обладнання. Тому, правильно спроектована та побудована комп'ютерна мережа дає можливість ефективної роботи підприємства, віддаленого адміністрування обладнання. Це кровоносна система компанії, в якій елементи пов'язані між собою, вони виконують окремі види робіт в рамках єдиного бізнес процесу, застосування технологій віддаленого доступу, тунелювання та шифрування інформації є важливим завданням для кожної організації.

Для того щоб об'єднати локальні мережі офісів і віддалених філій, застосовують технологію віртуальних приватних мереж - VPN (Virtual Private

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Network). VPN – найбільш популярна на сьогодні технологія побудови корпоративних мереж – VPN, яка означає об'єднання двох і більше територіально віддалених офісів в єдину захищену мережу для обміну даними, із дотриманням параметрів і правил передачі різномірної інформації. Дана технологія призначена для криптографічного захисту даних, гарантує конфіденційну і цілісну передачу інформації що передається по мережі. Віртуальна приватна мережа являє собою сукупність мережових з'єднань між VPN-шлюзами, на яких виробляється шифрування мережевого трафіку. VPN-шлюзи ще називають криптографічними шлюзами.

У випадку побудови VPN на базі маршрутизаторів необхідно пам'ятати ще і про те, що сам по собі такий підхід не вирішує проблему забезпечення загальної інформаційної безпеки компанії, оскільки усі внутрішні інформаційні ресурси все одно залишаються відкритими для атак ззовні. Для захисту цих ресурсів, як правило, застосовуються міжмережіві екрани (ME), які розташовуються за пограничними маршрутизаторами.

Існують два методи побудови єдиної захищеної корпоративної мережі організації:

1. з використанням обладнання і відповідного комплексу послуг інтернет-провайдера. (Дане рішення може бути застосовано, якщо головний офіс і філії підключені до Інтернет через одного інтернет-провайдера);
2. з використанням власного обладнання, розташованого в головному офісі та філіях. (Метод об'єднання двох мереж із застосуванням технології VPN називається "Peer-to-Peer VPN" або "site-to-site VPN". Між двома мережами встановлюється режим "прозорого шифрування").

Тунелювання це процес встановлення з'єднання між двома точками з використанням інкапсуляції, коли дані одного протоколу поміщаються в "конверти" іншого протоколу з метою забезпечити їх проходження в невідповідному середовищі, забезпечення цілісності та конфіденційності, захисту за допомогою шифрування. Очевидно існує проблема із захистом наших пакетів, які можуть бути перехоплені. Комбінація різних протоколів безпеки дозволяє вибудовувати гнучкі та безпечні канали обміну інформацією і задовольняти конкретні потреби організації. Якщо необхідна максимальна безпека, підійде

		Охріменко. Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

протокол IPSec, а якщо потрібно більш простий канал передачі зашифрованої інформації - PPTP, L2TP або IP2IP.

В такому випадку нам на допомогу приходять набір протоколів шифрування IPsec. Захищена корпоративна мережа генерується шляхом застосування особливого алгоритму шифрування з двох сторін тунелю, що гарантує секретність даних, що пересилаються. Потрібно створити розширений access-list (ACL) та в ньому визначити який трафік потрібно пропускати через VPN-тунель, вказавши IP-адреси відправника та отримувача.

З'єднання точка-точка має на увазі, що воно завжди встановлюється між двома комп'ютерами, які називаються вузлами (peers). Кожен peer відповідає за шифрування даних до того, як вони потраплять в тунель і розшифровку цих даних після того, як вони тунель покинуть.

Хоча VPN-тунель завжди встановлюється між двома точками, кожен peer може встановлювати додаткові тунелі з іншими вузлами. Для прикладу, коли трьома віддаленими станціями необхідно зв'язатися з одним і тим же офісом, буде створено три окремих VPN-тунелю до цього офісу. Для всіх тунелів peer на стороні офісу може бути одним і тим же. Це можливо завдяки тому, що вузол може шифрувати і розшифровувати дані від імені всієї мережі.

Незалежно від застосовуваного обладнання, загальна схема побудови Peer-to-Peer VPN для безпечного об'єднання локальних мереж віддалених офісів в єдину мережу, наступна:

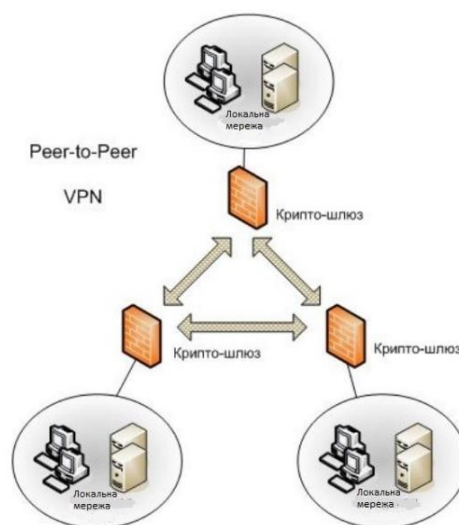


Рис. 1.1. Приклад об'єднання локальних мереж віддалених офісів

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2. Протоколи та технології побудови захищених мережних з'єднань.

1.2.1. Забезпечення безпеки корпоративної мережі за OSI моделлю.

Історично склалося, що базова еталонна модель взаємодії відкритих систем - мережева модель OSI (Open Systems Interconnecton — взаємодія відкритих систем) - є загальноприйнятою мережевою моделлю стека мережевих протоколів, що визначає різні рівні взаємодії систем. На кожен рівень накладаються певні функції, які виконуються залежно від покладених на нього завдань. Всього таких рівнів 7.

Рівні моделі OSI умовно поділяються на 2 глобальні частини: рівні хоста і рівні середовища передачі даних:

I. рівні хоста (хостом тут і далі називається будь-який пристрій, підключений до локальної або глобальної мережі);

7) прикладний рівень. Використовується для доступу до мережних служб;

6) представницький рівень. Інакше званий рівнем уявлення. Необхідний для подання та шифрування даних;

5) сеансовий рівень. Виходячи з назви, використовується для управління сеансом зв'язку;

4) транспортний. Прямий зв'язок між кінцевими пунктами і надійність з'єднання.

II. рівні середовища передачі даних:

3) мережевий рівень визначає маршрут і логічну адресацію;

2) канальний рівень визначає фізичну адресацію;

1) фізичний рівень працює із середовищем передачі даних, сигналами та двійковими даними.

Нижні рівні моделі OSI (з 1 по 3) керують фізичної доставкою даних по мережі і реалізуються у вигляді апаратних засобів і програмного забезпечення.

Верхні рівні моделі OSI (з 4 по 7) забезпечують точну доставку даних між додатками, працюючими на мережевих вузлах, і зазвичай реалізуються тільки на програмному рівні.

Модель OSI не описує служби і протоколи, використовувані на кожному рівні, вона визначає набір дій, які повинен виконати рівень, щоб передати

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

інформацію між вузлами. Модель OSI визначає схему обміну даними між мережевими вузлами, але сама не є способом такого обміну. Обмін даними стає можливим завдяки протоколам.

Таблиця 1.1

Рівні моделі OSI

Рівень		Тип даних	Функції
7	Рівень додатків	Дані користувача	надання сервісів для мережеских додатків
6	Рівень представлення	Дані користувача	Загальний формат представлення даних, стиснення і шифрування
5	Сеансовий рівень	Дані користувача	Встановлення, управління і завершення сесій між додатками
4	Транспортний рівень	Сегменти/дейтаграми	Адресація процесів, сегментація / повторна збірка даних, управління потоком, надійна доставка
3	Мережеский рівень	Пакети/дейтаграми	Передача повідомлень між віддаленими пристроями, вибір найкращого маршруту, логічна адресація
2	Канальний рівень	Кадри	Доступ до середовища передачі, передача повідомлень між локальними пристроями, фізична адресація
1	Фізичний рівень	Біти	Передача електричних і оптичних сигналів між пристроями

Протокол - це формальний набір правил і угод, що регламентує обмін інформацією між вузлами по мережі. він реалізує функції одного або декількох рівнів OSI.

		Охріменко. Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Однак фізичне з'єднання пристроїв виконується тільки на фізичному рівні моделі OSI, отже, щоб дані були передані по мережі іншого пристрою, вони повинні «спуститися» з рівня додатків на фізичний рівень всередині переданого вузла. Коли дані будуть передані по каналу зв'язку, фізичний рівень пристрою-одержувача витягне їх з середовища передачі і передасть вищому рівневі. Таким чином, реальна взаємодія однойменних рівнів відбувається за вертикалі за допомогою взаємодії з сусідніми рівнями (нижчого і вищерозміщеним) свого стека протоколів.

Інкапсуляція - це процес, при якому до даних додається службова інформація певного протоколу (рівня) перед відправкою в мережу.

Стек протоколів - сукупність протоколів різних рівнів. Найбільш відомим є стек протоколів TCP/IP. Правила і процедури, які відповідають за взаємодію між сусідніми рівнями, називаються інтерфейсами.

1.2.2. Безпека на фізичному рівні моделі OSI.

Фізичний рівень (physical layer) має справу з передачею бітів по фізичних каналах зв'язку, таких, наприклад, як коаксіальний кабель, вита пара, оптоволоконний кабель або цифровий територіальний канал. До цього рівня мають відношення характеристики фізичних серед передачі даних, такі як смуга пропускання, прешкодозахищеність, хвильовий опір і інші. На цьому ж рівні визначаються характеристики електричних сигналів, що передають дискретну інформацію, наприклад, крутість фронтів імпульсів, рівні напруження або струму сигналу, що передається, тип кодування, швидкість передачі сигналів. Крім цього, тут стандартизуються типи роз'ємів і призначення кожного контакту.

Функції фізичного рівня реалізуються у всіх пристроях, підключених до мережі. З боку комп'ютера функції фізичного рівня виконуються мережевим адаптером або послідовним портом.

Прикладом протоколу фізичного рівня може служити специфікація 10Base-T технології Ethernet, яка визначає як кабель, що використовується неекрановану пару категорії з хвильовим опором 100 Ом, роз'єм RJ-45, максимальну довжину фізичного сегмента 100 метрів. Фізичний рівень надає засіб транспортування бітів

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

кадра по мережевому се-редовищі. Фізичний рівень одержує кадр від канального рівня та кодує його в середовище за допомогою імпульсів (електричних, світлових, мікрохвильових).

Середовище не передає кадри цілком. Середовище передає сигнали, що представляють біти кадра по одному за раз.

Фізичний рівень відповідає за підтримку зв'язку (link), тобто здійснює інтерфейс між мережевим носієм та мережевим пристроєм. На цьому рівні регламентуються напруги, частоти, довжини хвиль, типи конекторів, число й функціональність контактів, схеми кодування сигналів тощо.

Можна виділити два основні середовища передачі даних:

- проводове (за участю кабелів);
- безпроводове (без участі кабелів).

Забезпечення безпеки на фізичному рівні полягає у забезпеченні структурної цілісності мережі. Структурна цілісність мережі – здатність зберігати неподільність системи. Основними загрозами структурної цілісності мережі є:

- проникнення в систему (отримання несанкціонованого доступу до ресурсів мережі);
- фізичне пошкодження мережі;
- створення завад у безпроводових каналах передачі даних.

Для реалізація цих загроз необхідно володіти апріорними знаннями про будову мережі. Проникнення у систему здійснюється з метою вводу хибної інформації, модифікації інформації, що передається в мережі, несанкціонованого користування ресурсами мережі (частотним, часовим, апаратним).

1.2.3. Безпека на канальному рівні моделі OSI.

Канальний рівень надає доступ до середовища й фреймування для протоколів вищих рівнів та контролює як дані містяться в середовище, а так само відслідковує помилки передачі.

Кадр (frame) – протокольний блок даних канального рівня.

Вузол (node) – пристрій підключений до загального середовища передачі даних.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Середовище (media) – середовище передачі даних (кабель, радіохвилі).

Мережа – вузли з'єднані між собою середовищем передачі даних.

Завдяки каналному рівню, протоколам мережного рівня не потрібно турбується про той яка технологія використовується на конкретному відрізку мережі. Що дозволяє протоколам мережного рівня працювати поверх зовсім різних мереж. Протоколи каналного рівня визначають інкапсуляцію пакетів у кадри й техніки приміщення бітів у середовище.

Методи контролю доступу до середовища (media access control) описані протоколами каналного рівня визначають процеси, за допомогою яких пристрої можуть взаємодіяти із середовищем і передавати кадри в різних мережних середовищах. Фреймуванням і доступом до середовища управляють мережні адаптери пристроїв.

Канальний рівень розділяється на два підрівня:

- LLC – фреймуючий пакет і визначальний протокол мережного рівня. (реалізується в драйверах);
- MAC – додає адреси каналного рівня й маркірує початок і кінець кадру. (реалізується в мережному адаптері).

Одним із завдань каналного рівня є перевірка доступності середовища передачі. Інше завдання каналного рівня – реалізація механізмів виявлення та корекції помилок. Для цього на каналному рівні біти групуються в набори, звані кадрами (frames). Канальний рівень забезпечує коректність передачі кожного кадру.

Структура кадру може відрізнятися залежно від протоколу каналного рівня. Чим складніше умови середовища передачі, тем складніше структура кадру.

Основні поля заголовка кадру для будь-якого протоколу:

- початок кадру;
- адреси;
- довжина кадру або тип протоколу 3 рівня.

З погляду інформаційної безпеки канальний рівень є достатньо дослідженим і відповідає за формування та доставку кадру без помилок. На цьому рівні вико-

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

ристовується апаратна MAC-адресація та здійснюється обчислення контрольної суми. Широко застосовуються зловмисниками атаки на підміну MAC-адреси, атаки на ARP і Spanning-Tree протоколи, кінцевою метою яких є перехоплення трафіку та одержання доступу до більш важливої конфіденційної інформації.

Небезпека уразливості протоколів канального рівня моделі OSI полягає в тому, що, зламавши мережу на канальному рівні, атакуючий може переступити через засоби захисту на вищих рівнях.

1.2.4. Безпека на мережному рівні моделі OSI.

Мережевий рівень – найбільш вразливий рівень з погляду захисту. На ньому формується вся маршрутизована інформація, відправник і одержувач фігурують явно, здійснюється управління потоком. Крім того, протоколами мережевого рівня пакети обробляються на всіх маршрутизаторах, шлюзах та інших проміжних вузлах. Майже всі специфічні мережеві порушення здійснюються з використанням протоколів цього рівня (читання, модифікація, знищення, дублювання, переорієнтація окремих повідомлень або потоку в цілому, маскування під інший вузол тощо). Захист від таких загроз здійснюється протоколами мережевого і транспортного рівнів і за допомогою засобів криптографічного захисту. На цьому рівні може бути реалізована вибіркова маршрутизація.

Протоколи канального рівня локальних мереж забезпечують доставку даних між вузлами тільки в мережі з відповідною топологією. Це обмеження не дозволяє створювати мережі з розвинутою структурою. Тому для того, щоб з одного боку зберегти простоту процедур передачі даних для типових топологій, а з другого – допустити використання довільних топологій, вводиться додатковий мережний рівень. На мережному рівні сам термін «мережа» наділяють специфічним значенням. В даному випадку під мережею розуміється сукупність комп'ютерів, з'єднаних між собою відповідно до одної з типових топологій, які використовують для передачі даних один із протоколів канального рівня, визначений для даної топології. Всередині мережі доставка даних забезпечується канальним рівнем, тоді як передачу даних між мережами забезпечує мережний рівень, який забезпечує можливість правильного вибору маршруту передачі. Для передачі повідомлення

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

від відправника, що знаходиться в одній мережі, отриму-вачу в іншій мережі, потрібно здійснити певну кількість транзитних передач між мережами (хоп – hop – стрибок), щоразу вибираючи найкращий маршрут. Для виконання функцій по передачі даних між вузлами по мережі, мережний рівень використовує:

- адресацію;
- інкапсуляцію/декапсуляцію;
- маршрутизацію.

Протоколи мережного рівня: Ipv4, Ipv6, IPX, Appletalk, CLNS/Decnet.

Характеристики Ipv4:

- без установлення сеансу (connectionless);
- ненадійний (unreliable) – не гарантує доставки (best effort), пакети можуть губитися, функції по забезпеченню надійності покладають на протоколи транспортного рівня;

– не залежить від середовища передачі (media independent), крім MTU, канальний рівень повідомляє розмір максимального блоку передачі (MTU) мережному рівню. При перевищенні розміру MTU пакет може бути фрагментований перед передачею.

Маршрутизація на мережному рівні моделі OSI.

Проблема вибору найкращого шляху, визначення найкращого маршруту передачі інформації від відправника до одержувача, коли відправник і одержувач знаходяться в різних мережах, з'єднаних довільним чином називається маршрутизацією. Також на мережевому рівні вирішуються завдання управління потоком даних і діагностики помилок передачі. Мережевий рівень виконує інкапсуляцію сегментів, отриманих від транспортного рівня в пакети (також звані дейтаграммами). Основним протоколом мережевого рівня є протокол IP (InternetProtocol).

Вирішення проблем з маршрутизацією є однією з головних задач мережного рівня. Ця проблема ускладнюється ще й тим, що найкоротший шлях не завжди є й найкращим. Деякі алгоритми маршрутизації стараються пристосуватися до зміни навантаження, тоді як інші приймають рішення на основі середніх показників за

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

тривалий час. Вибір маршруту може здійснюватися і за іншими критеріями, наприклад, надійності передачі. Мережний рівень розв'язує також задачі узгодження різних технологій, спрощення адресації у великих мережах та створення надійних і гнучких бар'єрів на шляху небажаного трафіку між мережами.

Статична маршрутизація не підходить для великих, складних мереж тому, що зазвичай мережі включають багато протоколів і змішані топології. Маршрутизатори в складних мережах повинні швидко адаптуватися до змін топології і вибирати кращий маршрут з багатьох учасників мережі. З точки зору маршрутизації мережа розглядається як сукупність автономних систем.

Динамічна маршрутизація може бути здійснена з використанням одного і більше протоколів. Ці протоколи часто групуються відповідно до того, де вони використовуються. Протоколи для роботи всередині автономних систем називають внутрішніми протоколами шлюзів (interiorgatewayprotocols (IGP)), а протоколи для роботи між автономними системами називають зовнішніми протоколами шлюзів (exteriorgatewayprotocols (EGP)). До протоколів IGP відносяться RIP, RIP v2, IGRP, EIGRP, OSPF і IS-IS. Протоколи EGP3 і BGP4 відносяться до EGP. Всі ці протоколи можуть бути розділені на два класи: дистанційно-векторні протоколи і протоколи стану зв'язку. Результати роботи маршрутизуючих протоколів заносяться в таблицю маршрутів, яка постійно змінюється при будь-якій зміні в мережі.

Повідомлення мережного рівня прийнято називати пакетами (packets). При організації доставки пакетів на мережному рівні використовують поняття «но-мер мережі». В цьому випадку адреса отримувача складається із старшої частини – номера мережі та молодшої – номера вузла в цій мережі. Усі вузли однієї мережі повинні мати одну й ту ж старшу частину адреси, у зв'язку з чим терміну «мережа» на мережному рівні можна дати й інше, більш формальне визначення: мережа – це сукупність вузлів, мережна адреса яких містить один і той же номер мережі.

На мережному рівні визначаються два види протоколів. Перший вид – мережні протоколи (routedprotocols) – реалізують переміщення пакетів в мережі (саме ці протоколи зазвичай мають на увазі, коли говорять про протоколи мережного

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

рівня). Проте часто до мережного рівня відносять і інший вид протоколів, що називаються протоколами обміну маршрутною інформацією або протоколами маршрутизації (routing protocols). Протоколи мережного рівня реалізуються програмними модулями операційної системи, а також програмними і апаратними засобами маршрутизаторів. На мережному рівні працюють протоколи ще одного типу, які відповідають за відображення адреси вузла, що використовується на мережному рівні, в локальну адресу мережі. Прикладами протоколів мережного рівня є протокол міжмережної взаємодії IP та протокол міжмережного обміну пакетами IPX.

Для передачі інформації між вузлами, що перебувають у різних мережах, необхідні маршрутизатори. Вони є прикордонними пристроями, що з'єднують мережі один з одним. Для маршрутизатора мережі в яких перебувають його порти є підключеними (directly connected). А ті мережі до яких підключені його сусіди – віддаленими (remote). Якщо ПК потрібно відправити інформацію вузлу не з його мережі, то він направляє її своєму шлюзу. Шлюз (він же маршрутизатор) вибирає шлях передачі інформації ґрунтуючись на своїй таблиці маршрутів.

1.2.5. Безпека на сеансовому рівні моделі OSI.

Сеансовий рівень (рівень сесії). На даному рівні встановлюються, обслуговуються і припиняються сесії між представницькими об'єктами додатків (прикладними процесами). В якості прикладу протоколи сеансового рівня можна розглянути протокол RPC (Remote Procedure Call). Як випливає з назви, даний протокол призначений для відображення результатів виконання процедури на віддаленому хості. У процесі виконання цієї процедури між додатками встановлюється сеанс на з'єднання. Призначенням даного з'єднання є обслуговування запитів, які виникають, наприклад, при взаємодії програми-сервера з додатком-клієнтом.

Шлюз сеансового рівня (Session Level Gateway – SLG). Це активний транслятор TCP-з'єднання. Шлюз приймає запит авторизованого клієнта на надання послуг, перевіряє допустимість запитаного сеансу (handshaking), встановлює потрібне з'єднання з адресою призначення зовнішньої мережі і формує статистику з

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

даного сеансу зв'язку. Після встановлення факту, що довірений клієнт і зовнішній хост є «законними» (авторизованими) учасниками сеансу, шлюз транслює пакети в обох напрямках без фільтрації. При цьому часто пункт призначення об-мовляється заздалегідь, а джерел інформації може бути багато (з'єднання «один-до-багатьох») – це, наприклад, типовий випадок використання зовнішнього веб-ресурса. Використовуючи різні порти, можна створювати різні конфігурації спо-лук, обслуговуючи одночасно всіх користувачів, що мають право на доступ до ресурсів мережі. Істотним недоліком SLG є те, що після встановлення зв'язку пакети фільтруються тільки на сеансовому рівні моделі OSI без перевірки їх вмі-сту на рівні прикладних програм. Авторизований зловмисник може спокійно тра-нслювати шкідливі програми через такий шлюз.

На протоколи сеансового рівня і рівня представлення даних лягає основне навантаження по забезпеченню безпеки мережі. На сеансовому рівні безпека за-безпечується за допомогою ідентифікаторів і паролів користувачів. ISO рекоме-ндує при реалізації моделі OSI забезпечувати безпеку мережі за допомогою ши-фрування на рівні представлення даних.

1.2.6. Протоколи віддаленого доступу.

Потреба в віддаленому управлінні виникла з моменту появи мережі і систем, які необхідно було адмініструвати на відстані. Для цього існує декілька дуже поширених протоколів віддаленого адміністрування, що дозволяють управляти системою за допомогою мережі. Основна причина розробки віддаленого протоколу це те, що комп'ютерні системи на початку були ще дуже дорогими і не завжди доступними для всіх. Також їх великий розмір, означало втрату мобільності. Для того щоб зробити комп'ютерні ресурси доступними в університетах і компаніях, Unix була розроблена наприкінці 1960-х років як відповідна операційна система, а Telnet-як відповідна протокольна служба. Це означало, що будь-який користувач, що має право авторизації, може запускати, управляти і використовувати програми на потужних великих комп'ютерах для власного особистого користування.

Telnet – це протокол емуляції терміналу, що часто використовується в мережі Інтернет та в мережах, що працюють по протоколах TCP/IP. Користувач терміналу

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

або персонального комп'ютера, може зареєструватися в системі віддаленого комп'ютера і виконувати програми. Призначення протоколу Telnet належить до організації спільного, двонаправленого, стабільного засобу зв'язку. Це самий перший протокол віддаленого взаємодії, що з'явився на зорі розвитку обчислювальних мереж, коли проблеми безпеки при передачі інформації не приділялося практично ніякої уваги.

Крім протоколу Telnet в UNIX-системах було розроблено ціле сімейство так званих r-програм. До них відносяться rsh, rlogin (початкова буква r трактується як remote) та інші, що дозволяють проводити різні операції, пов'язані з віддаленим адмініструванням. Рівню додатків відповідають всі протоколи Інтернет, з якими працює кінцевий користувач: FTP, Telnet, SMTP, DNS (служба мережеских імен, яка використовується Telnet, FTP і іншими сервісами для трансляції імен віддалених машин в IP-адреси), Gopher (засіб пошуку та перегляду інформації за допомогою системи меню) та інші. Протокол пересилки файлів FTP (File Transfer Protocol) який реалізує віддалений доступ до файлу. Він може використовуватися додатками і користувачами для передачі файлів по мережі. Для того, щоб забезпечити надійну передачу, FTP використовує в якості транспорту протокол з встановленням з'єднань - TCP. Однак, крім пересилання файлів, протокол FTP пропонує й інші послуги. Таким чином, користувачеві надається можливість інтерактивної роботи з віддаленою машиною, наприклад, він може роздрукувати вміст її каталогів. Крім того, FTP дозволяє користувачеві вказувати тип і формат запам'ятовуються даних, а також FTP виконує аутентифікацію користувачів. Існує також спрощений протокол передачі файлів (TFTP) призначений для обміну файлами з зовнішніми хостами. Для передачі файлів TFTP застосовує ненадійний Протокол призначених для користувача дейтаграм, тому зазвичай він працює швидше, ніж FTP. Як і FTP, TFTP підтримує передачу файлів у форматі NETASCII і в 8-розрядному двійковому форматі. На відміну від FTP, TFTP не підтримує перегляд каталогів або перехід в інший каталог зовнішнього хоста. У ньому також не передбачена захист за допомогою пароля. Крім того, TFTP працює тільки з загальними каталогами.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

Однак рівень безпеки при використанні r-програм, як і рівень безпеки при використанні Telnet, також залишає бажати кращого. Існує ще один протокол для управління деякими параметрами системи та отримання інформації про неї. Це протокол SNMP (Simple Network Management Protocol - протокол керування мережами зв'язку на основі архітектури TCP/IP). Протокол SNMP має обмежений спектр можливостей і не позбавлений тих же недоліків в плані безпеки, що і протокол Telnet.

Ці протоколи можуть служити хорошим рішенням для таких локальних мереж, де вимоги, що пред'являються до безпеки, є не дуже високими. Однак, при передачі даних по такій мережі, як Інтернет, де пакет, перш ніж досягти адресата, проходить кілька небезпечних вузлів, їх використання може служити потенційною загрозою безпеці і основною причиною успішного проникнення в систему. На сьогоднішній день одним з найпоширеніших і безпечних протоколів віддаленого адміністрування, що використовують шифрування при передачі даних, є протокол SSH (Secure SHell).

SSH не вирішує всіх проблем мережевої безпеки. Він лише фокусує свою увагу на забезпеченні безпечної роботи таких додатків, як емулятори терміналу (проте цими лише функціями протокол не обмежується, він дозволяє встановлювати безпечні з'єднання і для інших цілей). Використання реалізацій протоколу SSH на серверах і в клієнтських додатках допомагає захистити дані лише в процесі передачі; протокол SSH жодним чином не є заміною брандмауерів, систем виявлення вторгнень, мережевих сканерів, систем аутентифікації та інших інструментів, що дозволяють захистити інформаційні системи і мережі від атак.

Віддалений доступ із SSH зазвичай реалізується для того, щоб працівники могли працювати віддалено або дозволити ІТ-відділу виконувати завдання, не потребуючи фізичного підходу до машини. Його можна використовувати для віддаленого адміністрування, управління мережевою інфраструктурою, для налаштування автоматизації, створення резервних копій тощо.

Протокол SSH розроблявся для надання безпеки переданих даних шляхом реалізації стійкого алгоритму шифрування даних, надійної системи аутентифікації

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

користувача і сервера, наданням системи контролю цілісності переданих даних, а також інкапсуляцією додатків які працюють на основі протоколу TCP для встановлення безпечних тунелів [6].



Рис. 1.2. Принцип роботи протоколу SSH-1

Спочатку клієнт посилає серверу запит на SSH з'єднання і створення нового сеансу. З'єднання буде прийнято сервером, якщо він приймає повідомлення подібного роду і готовий до відкриття нового сеансу зв'язку. Після цього клієнт і сервер обмінюються інформацією, які версії протоколів вони підтримують. З'єднання буде продовжено, якщо буде знайдено відповідність між протоколами і отримано підтвердження про готовність обох сторін продовжити з'єднання по даному протоколу. Відразу після цього сервер посилає клієнтові постійний публічний і тимчасовий серверний ключі. Клієнт використовує ці ключі для шифрування сесійного ключа.

Незважаючи на те, що тимчасовий ключ посилається прямим текстом, сесійний ключ і раніше безпечний. Після цього сесійний ключ шифрується тимчасовим ключем і публічним ключем сервера, таким чином тільки сервер може його розшифрувати. На цьому етапі і клієнт і сервер мають сесійним ключем і, отже, готові до безпечного сеансу передачі зашифрованих пакетів.

Аутентифікація сервера відбувається виходячи з його можливості розшифровки сесійного ключа, який зашифрований публічним ключем сервера. Аутентифікація клієнта може відбуватися різними способами, в тому числі DSA,

RSA, OpenPGP або по пароллю. Сесія триває до тих пір, поки і клієнт і сервер здатні аутентифіцировать один одного.

Встановлене з'єднання по протоколу SSH-1 дозволяє передати дані стійким алгоритмом шифрування, перевіркою цілісності даних і стисненням. Спочатку пакети будуть послані на якийсь відомий на сервері порт, після чого вони будуть переадресовані на 22 порт (який обслуговується сервером SSH) і там будуть перетворені в захищені SSH пакети, інкапсульовані в захищене з'єднання.



Рис. 1.3. Принцип роботи протоколу SSH-2

Обидва протоколи, по суті, виконують одні і ті ж функції, але протокол SSH-2 робить це елегантно, більш гнучко. Основна відмінність між протоколами полягає в тому, що протокол SSH-2 розділяє всі функції протоколу SSH між трьома протоколами, в той час як протокол SSH-1 являє собою один єдиний і неподільний протокол.

Модуляцією функцій протоколу SSH в трьох протоколах - протоколі транспортного рівня, протоколі аутентифікації і протоколі з'єднання, робить протокол SSH-2 найбільш гнучким і потужним механізмом створення безпечних тунелів. Нижче треба короткий опис і призначення кожного з трьох протоколів, що складають протокол SSH-2 [4]:

- Протокол транспортного рівня - надає можливість шифрування і стиснення даних, що передаються, а також реалізує систему контролю цілісності даних.
- Протокол з'єднання - дозволяє клієнтам встановлювати багатопоточний з'єднання через оригінальний SSH тунель, таким чином знижуючи навантаження, яку створюють клієнтські процеси.
- Протокол аутентифікації - протокол аутентифікації відділений від протоколу транспортного рівня, тому що не завжди буває необхідним

використання системи аутентифікації. У разі, якщо потрібна аутентифікація, процес захищається надійним безпечним каналом, встановленим через протокол транспортного рівня.

Протокол з'єднання, що є частиною протоколу SSH-2, дозволить клієнтам зменшити навантаження на центральний процесор шляхом організації многопоточного з'єднання через оригінальне SSH з'єднання.

Все вищесказане говорить на користь того, що протокол Telnet може бути використано тільки в малих мережах при впевненості, що передані дані ніякої важливості не несуть. Можливості ж протоколу SSH майже необмежені.

Недоліком SSH є те, що він не підтримує анонімний доступ до вашого сховища. Якщо ви використовуєте SSH, користувачі зобов'язані мати SSH доступ до вашої, навіть тільки для читання, через що SSH не є продуктивним для проектів з відкритим кодом, у яких люди цілком можуть хотіти просто скопіювати його, щоб ознайомитися з ним. Якщо ви використовуєте його тільки в межах вашої корпоративної мережі, SSH може бути єдиним протоколом, що вам потрібен.

1.2.7. Створення списків управління доступом (ACL).

На сьогодні для будь-якого системного адміністратора однієї з найгостріших проблем залишається забезпечення безпеки комп'ютерної мережі. Здавалося б, такі завдання покликані вирішувати міжмережеві екрани, проте часом перший удар переймають на себе саме комутатори. Хоча це і не основне їх завдання, проте, на даний момент комутатори мають широкий функціонал для успішного вирішення подібного роду завдань. Йдеться не лише про захист мереж від атак ззовні, але і про всілякі атаки усередині мережі, таких як підміна DHCP-сервера, атаки типу DoS, ARP Spoofing, неавторизований доступ і так далі.

Списки управління доступом (Access Control List, ACL) є потужним засобом фільтрації потоків даних без втрати продуктивності, оскільки перевірка вмісту пакетів виконується на апаратному рівні. Фільтруючи потоки даних, адміністратор може обмежити типи додатків, дозволених для використання в мережі, контролювати доступ користувачів до мережі і визначати пристрої, до яких вони

		Охріменко. Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

можуть підключатися. Також ACL можуть використовуватися для визначення політики QoS шляхом класифікації трафіку і перевизначення його пріоритету.

ACL є послідовністю умов перевірки параметрів пакетів даних. Коли повідомлення поступають на вхідний порт, комутатор перевіряє параметри пакетів даних на збіг з критеріями фільтрації, визначеними в ACL, і виконує над пакетами одну з дій: permit («дозволити») або deny («заборонити»).

1.2.8. Типи тунельних з'єднань, які застосовуються для побудови VPN-мереж.

PPTP (Point-to-Point Tunneling Protocol, тунельний протокол точка-точка) - один з найбільш відомих клієнт-серверних протоколів, набув широкого поширення завдяки тому, що починаючи з Windows 95 OSR2 PPTP-клієнт був включений до складу ОС. Технічно PPTP використовує два мережевих з'єднання: канал управління, що працює через TCP і використовує порт 1723 і GRE-тунель для передачі даних. Через це можуть виникати складнощі з використанням в мережах мобільних операторів, проблема з одночасною роботою декількох клієнтів через NAT і проблема проброса PPTP з'єднання через NAT. Ще одним істотним недоліком є низька безпека протоколу PPTP, що не дозволяє будувати на ньому захищені віртуальні мережі.

L2TP (Layer 2 Tunneling Protocol, протокол тунелювання другого рівня) - розробка компаній Cisco і Microsoft, використовує для передачі даних і керуючих повідомлень єдине UDP з'єднання на порту 1701, але не містить ніяких вбудованих засобів захисту інформації. L2TP-клієнт також вмонтований в усі сучасні системи і мережеві пристрої. Без шифрування L2TP широко застосовувався і застосовується провайдерами для забезпечення доступу в інтернет, забезпечуючи таким чином поділ безкоштовного внутрішньомережевого і дорогого інтернет трафіку. Для побудови VPN зазвичай використовують L2TP over IPsec (L2TP / IPsec), де IPsec працює в транспортному режимі і шифрує дані L2TP-пакета. При цьому L2TP-тунель створюється всередині IPsec-каналу і для його встановлення необхідно перш забезпечити IPsec-з'єднання між вузлами. До плюсів L2TP можна віднести високу поширеність і надійність, IPsec не має серйозних вразливостей і вважається

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

дуже безпечним. Мінус - високе навантаження на устаткування і невисока швидкість роботи.

SSTP (Secure Socket Tunneling Protocol, протокол безпечного тунелювання сокетов) - розроблений компанією Microsoft безпечний VPN-протокол, відноситься до так званих SSL VPN, поширений переважно в Windows-середовищі, хоча клієнти доступні в середовищі багатьох сучасних ОС. Технічно SSTP є тунельний PPP-з'єднання всередині HTTPS-сесії на стандартний порт 443. Для стороннього спостерігача доступні тільки HTTPS-заголовки, наявності тунелю в трафіку залишається прихованим. Це дозволяє успішно працювати в будь-яких мережах, так як HTTPS широко використовується для доступу до сайтів і зазвичай дозволений, знімає проблему з прокинувши або роботою через NAT. Безпечний.

IP-IP (IP over IP) - один з найпростіших і має мінімальні накладні витрати протокол тунелювання, але на відміну від GRE інкапсулює тільки IPv4 unicast трафік. Також є протоколом без збереження стану і вбудованих механізмів безпеки, зазвичай використовується в парі з IPsec (IP-IP over IPsec). Підтримується UNIX-like системами і мережевим обладнанням. Як і GRE не використовує порти і не проходить через NAT, номер протоколу 4.

EoIP (Ethernet over IP) - розроблений Mikrotik протокол тунелювання канального рівня (L2), працює на базі протоколу GRE інкапсулюючи Ethernet кадри в GRE пакети. Дозволяє з'єднувати на канальному рівні віддалені мережі і забезпечувати зв'язок без використання маршрутизації. При цьому слід розуміти, що таке з'єднання передбачає проходження широкомовного трафіку, що здатне істотно знизити продуктивність тунелю, особливо на вузьких каналах або каналах з великими затримками. EoIP може бути використаний для підключення торгового і промислового устаткування, яке не вміє працювати на мережевому (L3) рівні з маршрутизацією. Наприклад, для підключення віддалених відеокамер до відеореєстратора.

GRE (Generic Routing Encapsulation, загальна інкапсуляція маршрутів) - протокол тунелювання розроблений компанією Cisco і призначений для інкапсуляції будь-яких протоколів мережевого рівня OSI (тобто не тільки IP), GRE працює

		Охріменко. Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

безпосередньо поверх IP і не використовує порти, не проходить через NAT, номер протоколу 47. Для побудови захищених рішень зазвичай використовується GRE over IPsec, коли тунель GRE розташовується поверх захищеного IPsec каналу, хоча можливо і інше рішення - IPsec over GRE, при переході від захищеного з'єднання встановлюється всередині незашифрованого GRE-тунелю.

1.2.9. Технологія Active Directory в Windows Server для зберігання та організації об'єктів в мережі в ієрархічній захищеній логічній структурі.

Active Directory («Активний каталог», AD) - служби каталогів корпорації Microsoft для операційних систем сімейства Windows Server.

Системні адміністратори використовують технологію Active Directory в Windows Server для зберігання та організації об'єктів в мережі в ієрархічну захищену логічну структуру, наприклад користувачів, комп'ютерів або інших фізичних ресурсів. Розширювана і масштабована служба каталогів Active Directory (Активний каталог) дозволяє ефективно управляти мережевими ресурсами.

Ліс і домен складають основу логічної структури. Домени можуть бути структуровані в лісі, щоб забезпечити незалежність даних і сервісів (але не ізоляцію) і оптимізацію реплікації. Поділ логічних і фізичних структур поліпшує керованість системи і знижує адміністративні витрати, тому що на логічну структуру не впливають зміни в фізичному пристрої. Логічна структура дозволяє контролювати доступ до даних, тобто ви можете використовувати логічну структуру для контролю доступу до різних блоків даних [23].

Дані, що зберігаються в Active Directory, можуть надходити з різних джерел. З великою кількістю різних джерел даних і безліччю різних типів даних Active Directory повинен використовувати деякий стандартизований механізм зберігання, щоб підтримувати цілісність інформації, що зберігається.

У Active Directory об'єкти використовують каталоги для зберігання інформації, всі об'єкти визначені в схемі. Визначення об'єктів містять інформацію, таку як тип даних і синтаксис, яку каталог використовує, щоб гарантувати достовірність зберігання. Ніякі дані не можуть бути збережені в каталозі, поки вони

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

не визначені в схемі. Схема за замовчуванням містить всі визначення і опису об'єктів, які необхідні для коректної роботи Active Directory.

Сховище Active Directory обробляє весь доступ до БД. Сховище даних складається з служб і фізичних файлів, які керують правами доступу, процесами читання і запису даних усередині бази даних на жорсткому диску кожного контролера.

Структура і архітектура сховища Active Directory складається з чотирьох частин:

1) Ліси, домени і організаційні одиниці (OU) складають основні елементи логічної структури Active Directory. Ліс визначає єдиний каталог і представляє кордон безпеки. Ліси містять домени.

2) DNS забезпечує дозвіл імен в ієрархічній архітектурі, котору може використовувати Active Directory.

3) Схема містить визначення об'єктів, які використовуються для со-будівлі об'єктів, що зберігаються в каталозі.

4) Сховище даних (DATA STORE) - це частина каталогу, який управляє зберіганням і витягом даних на кожному контролері домена.

Дані AD зберігаються на одному або декількох рівнозначних контролерах домену. Зміни, внесені на одному, репліцируються на інші, причому передана інформація шифрується і підписується сертифікатом безпеки, що гарантує її справжність. Безпека всієї середовища забезпечується модифікованим протоколом Kerberos v5, аутентифікацією по відкритому ключу, смарт-картками, сертифікатам X.509 v3, а також SSL [23].

Отже, підсумуємо відмінні риси Active Directory:

- використання групових політик і допоміжних інструментів, що значно спрощує загальне адміністрування мережі підприємства;
- відносна легкість розгортання мереж зі складною топологією;
- початкова орієнтація на платформу Windows, що викликає певні проблеми з експлуатацією [23].

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3. Принципи організації захищених мережних з'єднань на базі протоколів GRE та IPSec.

1.3.2. Internet Protocol Security (IPsec) - стек протоколів для безпечного обміну інформацією по IP.

IPsec був розроблений з метою підвищення безпеки IP протоколу. Головну увагу при розробці IPsec приділялося забезпеченню безпеки в IP-мережах на мережевому рівні. Цей протокол добре інтегрується з функціями безпеки Windows NT Server, завдяки чому може служити ідеальною платформою для захисту потоків інформації, що проходять по мережах та Інтернету. IPsec призначений не для клієнт-серверного тунелювання, а для захисту тунелів між серверами і маршрутизаторами. Таким чином, він не замінює протоколи PPTP і L2TP, а доповнює їх.

Поряд із зростаючою проблемою безпеки мережі, технологія VPN (Віртуальна приватна мережа, VPN) забезпечує рішення економічного віддаленого доступу для підприємства. Оскільки протокол IPsec здатний забезпечити найвищий рівень безпеки, використання IPsec VPN для створення безпеки Інтранет стало тенденцією. Відомо що, IPsec (Інтернет-протокол безпеки) не підтримує шифрування багатоадресного та широкомовного пакета, GRE (Generic Routing Encapsulation) тунель необхідний для інкапсуляції багатоадресних та широкомовних пакетів до одноадресного пакету. Шифруючи GRE за допомогою IPsec, гарантується безпека даних і вирішується проблема масштабованості VPN.

Слід зазначити, що IPsec пропонує набір алгоритмів і механізмів, а не готове рішення, завдання налагоджувальника вибрати потрібну і застосувати в залежності від поставлених цілей. Представлені можливості шифрування, аутентифікації і функції для збереження цілісності повідомлення.

Протоколи IPsec забезпечують управління доступом, цілісність даних з'єднання, аутентифікацію джерела даних, захист від відтворення, конфіденційність і частковий захист від аналізу трафіку.

IPsec включає в себе:

- безпечне приховування даних (ESP);

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

- аутентифікаційний заголовок (AH);
- контексти (асоціації) безпеки (SA);
- управління ключами (IKE);
- режими роботи: тунельний і транспортний;

У протоколі IPSec використовуються два режими тунельний і транспортний. Транспортний режим забезпечує безпечне з'єднання двох терміналів шляхом інкапсуляції вмісту IP-даних, в той час як тунельний режим інкапсулює весь IP-пакет на ділянці між шлюзами. Останній варіант використовується для формування традиційної VPN, де тунель створює безпечний шлях через повний небезпек Інтернет.

Протокол IPsec використовується, в більшості випадків для організації VPN-тунелів. Внаслідок чого, протоколи ESP і AH працюють в режимі тунелювання. Крім того, налаштовуючи політики безпеки певним чином, протокол можна використовувати для створення мережевого доступу. Сенс брандмауера полягає в тому, що він контролює і фільтрує проходять через нього пакети відповідно до заданих правил. Встановлюється набір правил, і екран переглядає всі, хто проходить через нього пакети.

Переходимо до принципів роботи кожного з параметрів, а потім до процесу встановлення з'єднання в цілому.

AH (AuthenticationHeader) - протокол заголовка ідентифікації. Забезпечує цілісність переданих даних методом перевірки того, що жоден біт в захищається частини пакета не був змінений під час передачі. Використання AH може викликати проблеми, наприклад, при проходженні пакета через NAT пристрій. Оскільки в пакет при проході через NAT змінюється відправник, то контрольна сума AH стане невірною. Також варто відзначити, що AH розроблявся тільки для забезпечення цілісності. Він не забезпечує шифрування вмісту пакета [25].

ESP (EncapsulatingSecurityProtocol) - інкапсулює протокол безпеки, що забезпечує і цілісність і конфіденційність. У транспортному режимі, ESP заголовок знаходиться між оригінальним IP транспортних протоколів. У режимі тунелю

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

заголовок ESP розміщується між новим IP заголовком і повністю зашифрованим оригінальним IP пакетом.

Оскільки АН і ESP працюють на мережному рівні, вони мають власні ID протоколу, АН зарезервований за ID 51, а ESP за ID 50 [26].

Третій протокол, який використовується IPSec – IKE (InternetKeyExchangeprotocol), призначений для обміну ключами між двома вузлами VPN. Незважаючи на присутню можливість генерувати ключі вручну, найбільш безпечним і масштабується варіантом буде автоматизація цього процесу з допомогою IKE. Для забезпечення безпеки, ключі повинні часто змінюватися, і зручніше довірити цей процес автоматизації. IKE використовує 500 порт UDP.

SA (SecurityAssociation) - це термін IPSec для позначення з'єднання. При налаштованому VPN, для кожного використовуваного протоколу створюється одна SA пара (тобто одна для АН і одна для ESP). SA створюються парами, тому що кожна SA - це односпрямоване з'єднання, а дані необхідно передавати в двох напрямках. Отримані SA пари зберігаються на кожному вузлі. Якщо ваш вузол має SA, значить VPN тунель був встановлений успішно.

Протокол IPSec можна уявити як ще один рівень, що лежить нижче стека TCP / IP. Управління цим рівнем проводиться відповідно до політики безпеки на кожному комп'ютері, враховуються і правила забезпечення безпеки, узгоджені відправником і отримувачем повідомлення. Політика безпеки визначає як використовуваний набір фільтрів, так і асоційовані функції безпеки (associated security behaviors). Якщо IP-адреса, протокол і номер порту, зазначені в пакеті, відповідають критеріям фільтрації, наступним етапом стає перевірка асоційованих функцій безпеки.

Оскільки кожен вузол здатний встановлювати кілька тунелів з іншими вузлами, кожен SA має унікальний номер, що дозволяє визначити до якого вузлу він відноситься. Це номер називається SPI (SecurityParameterIndex) або індекс параметра безпеки.

Кожен вузол IPSec також має другу БД - SPD або SecurityPolicyDatabase (БД політики безпеки). Вона містить налаштовану вами політику вузла.

		Охріменко. Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

Транспортний режим роботи. У цьому варіанті механізми безпеки застосовуються тільки для протоколів, починаючи з транспортного (TCP) рівня і вище, залишаючи дані самого мережевого рівня (заголовок IP) без додаткового захисту. Місця розміщення додаткової інформації, що вставляється протоколами в пакет, представлені відповідно до рисунка.

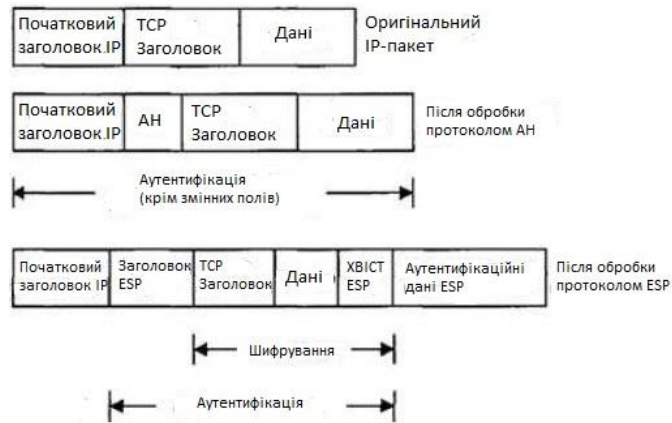


Рис. 1.4. Транспортний режим роботи Ірsec

Тунельний режим роботи. Цей режим цікавий тим, що забезпечує захист також і даних мережевого рівня шляхом додавання нового IP-заголовка. Після визначення асоціацій безпеки (наприклад, між двома шлюзами) істинні адреси хостів відправлення і призначення (і інші службові поля) повністю захищаються від модифікацій для АН або взагалі ховаються для ESP, а в новий заголовок виставляються адреси та інші дані для шлюзів (відправлення / отримання).

У тунельному режимі IPSec підтримується тільки IP-трафік, а всі операції проводяться на нижньому рівні IP-стека. Завдяки цьому всі виконувані тут функції стають доступні для додатків і протоколів вищого рівня.

Відповідно до малюнок видно переваги і недоліки обох протоколів. ESP забезпечує приховування даних, але не повну аутентифікацію за все пакету. АН повністю аутентифікує, але не приховує дані. У цьому причина того, що для забезпечення високого рівня безпеки, застосування протоколів поєднується.



Рис. 1.5. Тунельний режим роботи IPsec

Основна складність управління політиками IPsec в зрізі маршрутизації є той факт, що необхідно налаштовувати політику для кожної мережі. Вирішити цю проблему можна створенням тунелю без функцій захисту, і обробляти IPsec тільки тунель, а визначати можливість доступу до локальних ресурсів за допомогою політик безпеки на мережевому рівні за допомогою мережевого екрану. Таким чином ми досягнемо зменшення кількості точок відмови, спростимо настройку і усунення проблем. Одним з протоколів, забезпечують необхідний нам тунель є GRE.

1.3.3. Протокол тунелювання мережевих пакетів GRE.

GRE (genericroutingencapsulation - загальна інкапсуляція маршрутів) - розроблений Cisco протокол тунелювання мережевих пакетів. Основне призначення - інкапсуляція пакетів мережевого рівня моделі OSI в IP-пакети. Номер протоколу в IP - 47. Протокол не підтримує ніяких режимів аутентифікації або шифрування, його завдання - доставка пакетів. Отже, тунель GRE використовується, коли пакети повинні бути відправлені з однієї мережі в іншу через Інтернет або незахищену мережу. У GRE віртуальний тунель створюється між двома кінцевими точками (маршрутизаторами Cisco), а пакети відправляються через тунель GRE. Протокол GRE вимагає білих IP-адрес для обох сторін тунелю і є протоколом без збереження стану, тобто ніяк не контролює доступність протилежної вузла, хоча більшість сучасних реалізацій містять додаткові механізми, що дозволяють визначити стан каналу.

Важливо відзначити, що пакети, що проходять всередині тунелю GRE, не зашифровано, оскільки GRE не шифрується тунель, а інкапсулює його з заголовком GRE. Отже, GRE є протоколом інкапсуляції і не виконує шифрування. Створення тунелю GRE точка-точка без будь-якого шифрування надзвичайно ризиковано, оскільки конфіденційні дані можуть бути легко вилучені з тунелю і переглянуті іншими.

Якщо потрібен захист даних, IPSec повинен бути налаштований для забезпечення конфіденційності даних - тоді GRE-тунель перетворюється в безпечний VPN-тунель GRE. Тунель GRE використовує інтерфейс «тунель» - логічний інтерфейс, налаштований на маршрутизаторі з IP-адресою, де пакети інкапсулюються і декапсулюються при вході або виході з тунелю GRE.

Таким чином, використовуючи GRE + IPSec, можна домогтися збалансованого по співвідношенню складність налаштувань/безпека рішення без шкоди для конфіденційності особистих переданих даних.

IPsec не може інкапсулювати multicast трафік, broadcast трафік або не-IP-пакети, а GRE не може автентифікувати та шифрувати пакети. За допомогою технології GRE через IPsec багатоадресні (multicast) та широкомовні (broadcast) пакети можуть бути інкапсульовані за допомогою GRE, а потім зашифровані за допомогою IPsec. У той же час інтерфейс, що підтримує GRE, збирає статистику про обсяг зашифрованого та розшифрованого трафіку. Коли шлюзи взаємопов'язані в режимі GRE через IPsec, шлюзи інкапсулюють пакети за допомогою GRE, а потім IPsec.

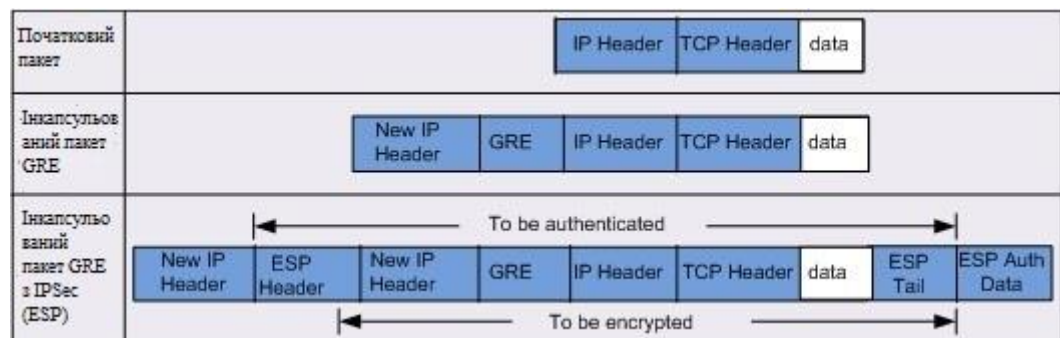


Рис. 1.6. Принцип роботи GRE over IPsec encapsulation mode (тунельний режим)

Потік даних, захищений IPsec, йде від початкової точки GRE до кінцевої точки GRE. У заголовку IP, доданому GRE під час інкапсуляції, адреса джерела - це адреса джерела тунелю GRE, а адреса призначення - адреса призначення тунелю GRE.

Хоча багато хто може подумати, що тунель GRE IPsec між двома маршрутизаторами схожий на VPN-з'єднання IPsec між сайтами, це не так. Основна відмінність полягає в тому, що тунелі GRE дозволяють multicast пакетам проходити через тунель, тоді як IPsec VPN не підтримує multicast пакети.

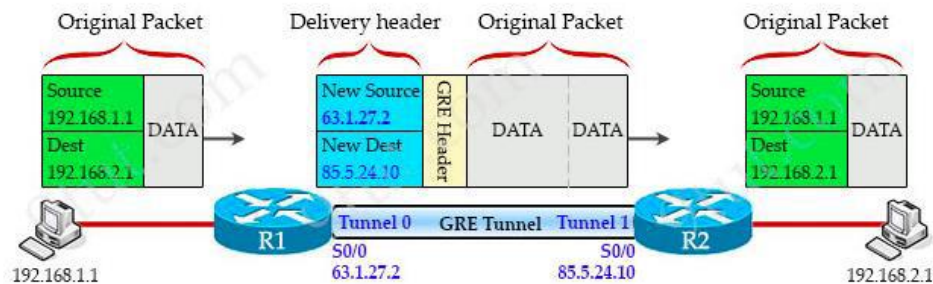


Рисунок 1.7. Реалізація VPN за допомогою GRE

У найбільш загальному випадку система повинна інкапсулювати та доставити пакет до якогось пункту призначення. Назвемо це пакетом корисного навантаження. Склад корисного навантаження спочатку інкапсулюється в пакет GRE. Отриманий пакет GRE потім може бути інкапсульований у якомусь іншому протоколі і потім пересланий. Цей зовнішній протокол називається протоколом доставки.

1.4. Аналіз існуючих рішень для створення мережі з використанням технологій протоколу тунелювання GRE, протоколу захисту даних IP-Security, протоколів динамічної маршрутизації OSPF та EIGRP, протоколу віддаленого доступу SSH.

1.4.1. Аналіз створеного рішення з використанням технологій протоколу тунелювання GRE, протоколу захисту даних IP-Security, протоколів динамічної маршрутизації OSPF та EIGRP.

Проведемо аналіз створеної мережі та конфігурації маршрутизаторів за посиланням: <http://sclabs.blogspot.com/2014/05/ccnp-route-gns3-lab-ospf-over-gre-over.html> та спробуємо створити дане рішення в графічному емуляторі мереж GNS3 для детального аналізу.

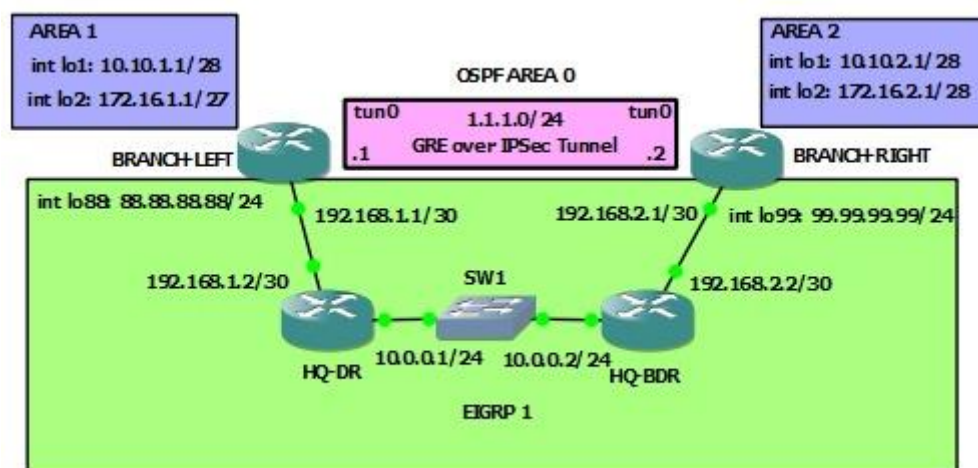


Рис. 1.8. Створена топологія мережі

```
BRANCH-LEFT
BRANCH-LEFT#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BRANCH-LEFT(config)#router eigrp 1
BRANCH-LEFT(config-router)#network 192.168.1.0
BRANCH-LEFT(config-router)#network 88.0.0.0
BRANCH-LEFT(config-router)#no auto-summary
BRANCH-LEFT(config-router)#exit
BRANCH-LEFT(config)#router ospf 1
BRANCH-LEFT(config-router)#network 1.1.1.0 0.0.0.255 area 0
BRANCH-LEFT(config-router)#network 10.10.1.0 0.0.0.15 area 1
BRANCH-LEFT(config-router)#network 172.16.1.0 0.0.0.31 area 1
BRANCH-LEFT(config-router)#exit
BRANCH-LEFT(config)#
*Mar 1 00:00:37.883: %OSPF-4-NORTRID: OSPF process 1 failed to allocate unique
router-id and cannot start
BRANCH-LEFT(config)#exit
```

Рис. 1.9. Налаштування параметрів протоколів динамічної маршрутизації для маршрутизатора BRANCH-LEFT

```

BRANCH-RIGHT
BRANCH-RIGHT#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BRANCH-RIGHT(config)#router eigrp 1
BRANCH-RIGHT(config-router)#network 192.168.1.0
BRANCH-RIGHT(config-router)#network 192.168.2.0
BRANCH-RIGHT(config-router)#network 99.0.0.0
BRANCH-RIGHT(config-router)#no auto-summary
BRANCH-RIGHT(config-router)#exit
BRANCH-RIGHT(config)#router ospf 1
BRANCH-RIGHT(config-router)#network 1.1.1.0 0.0.0.255 area 0
BRANCH-RIGHT(config-router)#network 10.10.2.0 0.0.0.15 area 2
BRANCH-RIGHT(config-router)#network 172.16.2.0 0.0.0.31 area 2
BRANCH-RIGHT(config-router)#exit

```

Рис. 1.10. Налаштування параметрів протоколів динамічної маршрутизації для маршрутизатора BRANCH-RIGHT

```

HQ-DR
HQ-DR#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
HQ-DR(config)#router eigrp 1
HQ-DR(config-router)#network 10.0.0.0
HQ-DR(config-router)#network 192.168.1.0
HQ-DR(config-router)#no auto-summary
HQ-DR(config-router)#exit
HQ-DR(config)#exit
HQ-DR#
*Mar 1 01:35:51.427: %SYS-5-CONFIG_I: Configured from console by console

```

Рис. 1.11. Налаштування параметрів протокола динамічної маршрутизації EIGRP для маршрутизатора HQ-DR

```

HQ-BDR
HQ-BDR#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
HQ-BDR(config)#router eigrp 1
HQ-BDR(config-router)#network 10.0.0.0
HQ-BDR(config-router)#network 192.168.2.0
HQ-BDR(config-router)#no auto-summary
HQ-BDR(config-router)#exit
HQ-BDR(config)#exit
HQ-BDR#
*Mar 1 01:36:45.659: %SYS-5-CONFIG_I: Configured from console by console

```

Рис. 1.12. Налаштування параметрів протокола динамічної маршрутизації EIGRP для маршрутизатора HQ-BDR

У Cisco IOS налаштування IPSec відбувається в CLI в режимі глобальної конфігурації наступним чином:

R1 (config) #crypto isakmp policy [номер] – створюємо політику підключення 1-ї фази,

R1 (config-isakmp) #authentication [параметри] – задаємо метод автентифікації:

- pre-share – метод загального ключа,
- rsa-encr – метод Rivest-Shamir-Adleman Encryption,
- rsa-sig – метод Rivest-Shamir-Adleman Signature.

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

R1 (config-isakmp) #encryption – задаємо метод шифрування (та довжину ключа):

- 3des – алгоритм Three key triple DES (ключ 3х56 біт),
- aes – алгоритм AES – Advanced Encryption Standard (ключ 128, 192, 256 біт),
- des – алгоритм DES – Data Encryption Standard (ключ 56 біт).

R1 (config-isakmp) #group – задаємо групу Diffie-Hellman, яка буде використовуватися для безпечного обміну ключами:

- Diffie-Hellman group 1 (768 bit)

- 14 Diffie-Hellman group 14 (2048 bit)
- 15 Diffie-Hellman group 15 (3072 bit)
- 16 Diffie-Hellman group 16 (4096 bit)
- 19 Diffie-Hellman group 19 (256 bit ecp)

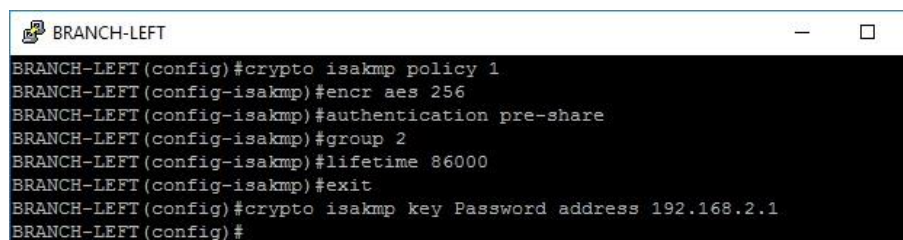
- Diffie-Hellman group 2 (1024 bit)

- 20 Diffie-Hellman group 20 (384 bit ecp)
- 21 Diffie-Hellman group 21 (521 bit ecp)
- 24 Diffie-Hellman group 24 (2048 bit, 256 bit subgroup)

- Diffie-Hellman group 5 (1536 bit).

R1 (config-isakmp) #lifetime [секунди] – задаємо час життя підключення,

R1 (config) #crypto isakmp key [ключ] address [IP-адреса] – задаємо ключ підключення і вказуємо IP-адресу віддаленого маршрутизатора.



```
BRANCH-LEFT
BRANCH-LEFT(config)#crypto isakmp policy 1
BRANCH-LEFT(config-isakmp)#encr aes 256
BRANCH-LEFT(config-isakmp)#authentication pre-share
BRANCH-LEFT(config-isakmp)#group 2
BRANCH-LEFT(config-isakmp)#lifetime 86000
BRANCH-LEFT(config-isakmp)#exit
BRANCH-LEFT(config)#crypto isakmp key Password address 192.168.2.1
BRANCH-LEFT(config)#
```

Рис. 1.13. Налаштування параметрів першої фази IPSec для маршрутизатора
BRANCH-LEFT

```

BRANCH-RIGHT#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BRANCH-RIGHT(config)#crypto isakmp policy 1
BRANCH-RIGHT(config-isakmp)#encr aes 256
BRANCH-RIGHT(config-isakmp)#authentication pre-share
BRANCH-RIGHT(config-isakmp)#group 2
BRANCH-RIGHT(config-isakmp)#lifetime 86000
BRANCH-RIGHT(config-isakmp)#exit
BRANCH-RIGHT(config)#crypto isakmp key Password address 192.168.1.1
BRANCH-RIGHT(config)#exit
BRANCH-RIGHT#
*Mar 1 01:38:32.143: %SYS-5-CONFIG_I: Configured from console by console

```

Рис. 1.14. Налаштування параметрів першої фази IPSec для маршрутизатора
BRANCH-RIGHT

Після чого, переходимо до налаштування другої фази IPSec.

R1 (config) #crypto IPsec transform-set [назва] {параметри} – створюємо transform-set для маршрутизатора R0:

Режим роботи тільки з автентифікаційним заголовком АН:

- ah-md5-hmac – режим АН-НМАС-MD5,
- ah-sha-hmac – режим АН-НМАС-SHA,
- ah-sha256-hmac – режим АН-НМАС-SHA256,
- ah-sha384-hmac – режим АН-НМАС-SHA384,
- ah-sha512-hmac – режим АН-НМАС-SHA512.

Режим роботи тільки з зашифрованими даними ESP:

- esp-3des – режим ESP transform using 3DES(EDE) cipher (168 bits),
- esp-aes – режим ESP transform using AES cipher,
- esp-des – режим ESP transform using DES cipher (56 bits),
- esp-seal – режим ESP transform using SEAL cipher (160 bits).

Режим роботи автентифікаційного заголовка АН для ESP режиму:

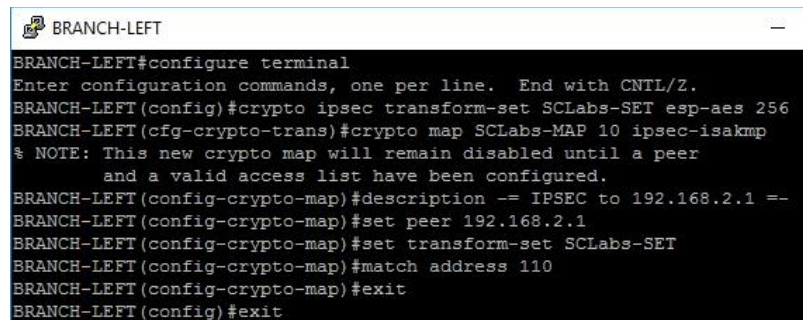
- esp-md5-hmac – режим ESP transform using HMAC-MD5 auth,
- esp-sha-hmac – режим ESP transform using HMAC-SHA auth,
- esp-sha256-hmac – режим ESP transform using HMAC-SHA256 auth,
- esp-sha384-hmac – режим ESP transform using HMAC-SHA384 auth,
- esp-sha512-hmac – режим ESP transform using HMAC-SHA512 auth.

R1 (config) #crypto map [назва] {номер} IPsec-isakmp – створюємо так звану крипто карту з номером. Номер використовується для того, щоб можна було створювати кілька підключень, тобто можна їх створювати одна за одною для всіх наших тунелів. Не треба плутати з політиками, там номер каже про пріоритет підключення, тут це просто номер і не несе якогось смислового навантаження,

R1 (config-crypto-map) #set peer [ip-адреса] – вказуємо ip адресу віддаленого маршрутизатора,

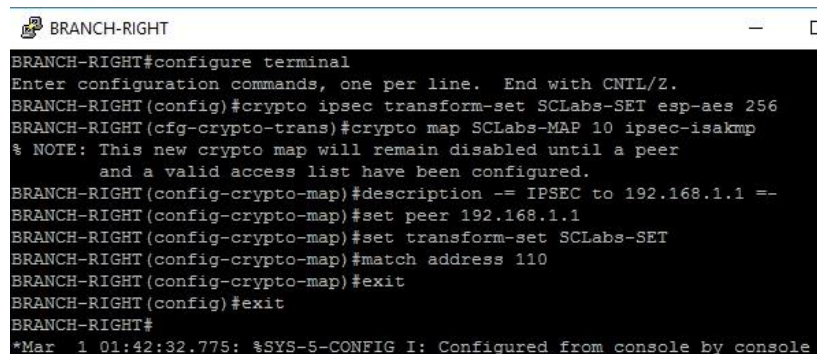
R1 (config-crypto-map) #match address [номер ACL] – застосовуємо створений раніше список доступу,

R1 (config-crypto-map) #set transform-set [назва] – застосовуємо створений раніше transform-set.



```
BRANCH-LEFT#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BRANCH-LEFT(config)#crypto ipsec transform-set SCLabs-SET esp-aes 256
BRANCH-LEFT(cfg-crypto-trans)#crypto map SCLabs-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
BRANCH-LEFT(config-crypto-map)#description -= IPSEC to 192.168.2.1 -=
BRANCH-LEFT(config-crypto-map)#set peer 192.168.2.1
BRANCH-LEFT(config-crypto-map)#set transform-set SCLabs-SET
BRANCH-LEFT(config-crypto-map)#match address 110
BRANCH-LEFT(config-crypto-map)#exit
BRANCH-LEFT(config)#exit
```

Рис. 1.16. Налаштування параметрів другої фази IPsec для маршрутизатора
BRANCH-LEFT



```
BRANCH-RIGHT#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BRANCH-RIGHT(config)#crypto ipsec transform-set SCLabs-SET esp-aes 256
BRANCH-RIGHT(cfg-crypto-trans)#crypto map SCLabs-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
BRANCH-RIGHT(config-crypto-map)#description -= IPSEC to 192.168.1.1 -=
BRANCH-RIGHT(config-crypto-map)#set peer 192.168.1.1
BRANCH-RIGHT(config-crypto-map)#set transform-set SCLabs-SET
BRANCH-RIGHT(config-crypto-map)#match address 110
BRANCH-RIGHT(config-crypto-map)#exit
BRANCH-RIGHT(config)#exit
BRANCH-RIGHT#
*Mar 1 01:42:32.775: %SYS-5-CONFIG I: Configured from console by console
```

Рис. 1.17. Налаштування параметрів другої фази IPsec для маршрутизатора
BRANCH-RIGHT

Переходимо до налаштувань параметрів адресації інтерфейсів маршрутизаторів та застосовуємо створену крипто карту для відповідних інтерфейсів:

R1 (config) #interface [назва] – заходимо в налаштування порту, що виходить у зовнішню мережу,

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

R1 (config-if) #crypto map [назва] – застосовуємо до нього крипто карту.

```
BRANCH-LEFT
BRANCH-LEFT#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BRANCH-LEFT(config)#interface Loopback88
BRANCH-LEFT(config-if)#ip address 88.88.88.88 255.255.255.0
BRANCH-LEFT(config-if)#exit
BRANCH-LEFT(config)#interface Loopback1
BRANCH-LEFT(config-if)#ip address 10.10.1.1 255.255.255.240
BRANCH-LEFT(config-if)#exit
BRANCH-LEFT(config)#interface Loopback2
BRANCH-LEFT(config-if)#ip address 172.16.1.1 255.255.255.224
BRANCH-LEFT(config-if)#exit
BRANCH-LEFT(config)#interface Tunnel0
BRANCH-LEFT(config-if)#ip mtu 1400
BRANCH-LEFT(config-if)#ip tcp adjust-mss 1360
BRANCH-LEFT(config-if)#ip address 1.1.1.1 255.255.255.0
BRANCH-LEFT(config-if)#tunnel source 192.168.1.1
BRANCH-LEFT(config-if)#tunnel destination 192.168.2.1
BRANCH-LEFT(config-if)#exit
BRANCH-LEFT(config)#interface Serial1/0
BRANCH-LEFT(config-if)#ip address 192.168.1.1 255.255.255.252
BRANCH-LEFT(config-if)#no sh
BRANCH-LEFT(config-if)#serial restart-delay 0
BRANCH-LEFT(config-if)#crypto map SCLabs-MAP
BRANCH-LEFT(config-if)#exit
```

Рис. 1.18. Налаштування параметрів адресації для маршрутизатора BRANCH-LEFT

```
BRANCH-RIGHT
BRANCH-RIGHT#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BRANCH-RIGHT(config)#interface Loopback99
BRANCH-RIGHT(config-if)#ip address 99.99.99.99 255.255.255.0
BRANCH-RIGHT(config-if)#exit
BRANCH-RIGHT(config)#interface Loopback1
BRANCH-RIGHT(config-if)#ip address 10.10.2.1 255.255.255.240
BRANCH-RIGHT(config-if)#exit
BRANCH-RIGHT(config)#interface Loopback2
BRANCH-RIGHT(config-if)#ip address 172.16.2.1 255.255.255.224
BRANCH-RIGHT(config-if)#exit
BRANCH-RIGHT(config)#interface Tunnel0
BRANCH-RIGHT(config-if)#ip mtu 1400
BRANCH-RIGHT(config-if)#ip tcp adjust-mss 1360
BRANCH-RIGHT(config-if)#ip address 1.1.1.2 255.255.255.0
BRANCH-RIGHT(config-if)#tunnel source 192.168.2.1
BRANCH-RIGHT(config-if)#tunnel destination 192.168.1.1
BRANCH-RIGHT(config-if)#exit
BRANCH-RIGHT(config)#interface Serial1/0
BRANCH-RIGHT(config-if)#ip address 192.168.2.1 255.255.255.252
BRANCH-RIGHT(config-if)#serial restart-delay 0
BRANCH-RIGHT(config-if)#
*Mar 1 01:45:42.247: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback99
, changed state to up
*Mar 1 01:45:42.743: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up
*Mar 1 01:45:42.879: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2,
changed state to up
*Mar 1 01:45:43.143: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, c
hanged state to down
crypto map SCLabs-MAP
BRANCH-RIGHT(config-if)#no shutdown
BRANCH-RIGHT(config-if)#exit
```

Рис. 1.19. Налаштування параметрів адресації для маршрутизатора BRANCH-RIGHT

```
HQ-DR
HQ-DR#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
HQ-DR(config)#interface FastEthernet0/0
HQ-DR(config-if)#ip address 10.0.0.1 255.255.255.0
HQ-DR(config-if)#no sh
HQ-DR(config-if)#exit
HQ-DR(config)#interface Serial1/0
HQ-DR(config-if)#no sh
HQ-DR(config-if)#ip address 192.168.1.2 255.255.255.252
HQ-DR(config-if)#exit
HQ-DR(config)#
```

Рис. 1.20. Налаштування параметрів адресації для маршрутизатора HQ-DR

```

HQ-BDR
HQ-BDR#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-BDR(config)#interface FastEthernet0/0
HQ-BDR(config-if)#ip address 10.0.0.2 255.255.255.0
HQ-BDR(config-if)#no shutdown
HQ-BDR(config-if)#exit
HQ-BDR(config)#interface Serial1/0
HQ-BDR(config-if)#ip address 192.168.2.2 255.255.255.252
HQ-BDR(config-if)#serial restart-delay 0
HQ-BDR(config-if)#no shutdown
HQ-BDR(config-if)#exit
HQ-BDR(config)#

```

Рис. 1.21. Налаштування параметрів адресації для маршрутизатора HQ-BDR

Переходимо до створення необхідних списків доступу ACL:

R1 (config) #access-list [номер] permit ip {параметри} – створюємо список доступу, який буде визначати в яких ситуаціях пакети будуть потрапляти в IPSec тунель.

```

BRANCH-LEFT
BRANCH-LEFT#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
BRANCH-LEFT(config)#$t gre 192.168.1.0 0.0.0.3 192.168.2.0 0.0.0.3 log
BRANCH-LEFT(config)#$168.1.0 0.0.0.3 eq isakmp 192.168.2.0 0.0.0.3 log
BRANCH-LEFT(config)#access-list 110 deny ip any any log
BRANCH-LEFT(config)#exit
BRANCH-LEFT#
*Mar  1 00:18:57.979: %SYS-5-CONFIG_I: Configured from console by console
BRANCH-LEFT#

```

Рис. 1.22. Створення списку доступу для маршрутизатора BRANCH-LEFT

```

BRANCH-RIGHT
BRANCH-RIGHT#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
BRANCH-RIGHT(config)#$t gre 192.168.2.0 0.0.0.3 192.168.1.0 0.0.0.3 log
BRANCH-RIGHT(config)#$168.2.0 0.0.0.3 eq isakmp 192.168.1.0 0.0.0.3 log
BRANCH-RIGHT(config)#access-list 110 deny ip any any log
BRANCH-RIGHT(config)#exit
BRANCH-RIGHT#
*Mar  1 01:49:38.031: %SYS-5-CONFIG I: Configured from console by console

```

Рис. 1.23. Створення списку доступу для маршрутизатора BRANCH-RIGHT

```

BRANCH-LEFT
BRANCH-LEFT#show crypto session
Crypto session current status

Interface: Serial1/0
Session status: UP-ACTIVE
Peer: 192.168.2.1 port 500
IKE SA: local 192.168.1.1/500 remote 192.168.2.1/500 Active
IPSEC FLOW: deny ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 0, origin: crypto map
IPSEC FLOW: permit 47 192.168.1.0/255.255.255.252 192.168.2.0/255.255.255.252
Active SAs: 2, origin: crypto map
IPSEC FLOW: permit 17 192.168.1.0/255.255.255.252 port 500 192.168.2.0/255.255.255.252
Active SAs: 0, origin: crypto map

BRANCH-LEFT#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: Serial1/0
Session status: UP-ACTIVE
Peer: 192.168.2.1 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 192.168.2.1
Desc: (none)
IKE SA: local 192.168.1.1/500 remote 192.168.2.1/500 Active
Capabilities: (none) connid:1 lifetime:23:48:54
IPSEC FLOW: deny ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 0, origin: crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
IPSEC FLOW: permit 47 192.168.1.0/255.255.255.252 192.168.2.0/255.255.255.252
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 33 drop 0 life (KB/Sec) 4538335/3355
Outbound: #pkts enc'ed 35 drop 0 life (KB/Sec) 4538335/3355
IPSEC FLOW: permit 17 192.168.1.0/255.255.255.252 port 500 192.168.2.0/255.255.255.252
Active SAs: 0, origin: crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

BRANCH-LEFT#

```

Рис. 1.24. Результат виконання діагностичних команд show crypto session та show crypto session detail для маршрутизатора BRANCH-LEFT

```

BRANCH-LEFT
BRANCH-LEFT#show crypto isakmp sa
dst          src          state          conn-id slot status
192.168.1.1  192.168.2.1  QM_IDLE       1         0 ACTIVE

BRANCH-LEFT#show crypto ipsec sa

interface: Serial1/0
Crypto map tag: SCLabs-MAP, local addr 192.168.1.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.252/47/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.252/47/0)
current peer 192.168.2.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 58, #pkts encrypt: 58, #pkts digest: 58
#pkts decaps: 56, #pkts decrypt: 56, #pkts verify: 56
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.2.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x20FF9AAC(553622188)

inbound esp sas:
spi: 0xEDA06CB6(3986713782)
transform: esp-256-aes ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: SW:1, crypto map: SCLabs-MAP
sa timing: remaining key lifetime (k/sec): (4538332/3122)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

```

Рис. 1.25. Результат виконання діагностичних команд show crypto isakmp sa та show crypto ipsec sa для маршрутизатора BRANCH-LEFT

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

```

BRANCH-RIGHT
BRANCH-RIGHT#show crypto session
Crypto session current status

Interface: Serial1/0
Session status: UP-ACTIVE
Peer: 192.168.1.1 port 500
IKE SA: local 192.168.2.1/500 remote 192.168.1.1/500 Active
IPSEC FLOW: deny ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 0, origin: crypto map
IPSEC FLOW: permit 47 192.168.2.0/255.255.255.252 192.168.1.0/255.255.255.252
Active SAs: 2, origin: crypto map
IPSEC FLOW: permit 17 192.168.2.0/255.255.255.252 port 500 192.168.1.0/255.255.255.252
Active SAs: 0, origin: crypto map

BRANCH-RIGHT#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: Serial1/0
Session status: UP-ACTIVE
Peer: 192.168.1.1 port 500 fvrf: (none) ivrf: (none)
Phase1 id: 192.168.1.1
Desc: (none)
IKE SA: local 192.168.2.1/500 remote 192.168.1.1/500 Active
Capabilities: (none) connid:1 lifetime:23:47:41
IPSEC FLOW: deny ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 0, origin: crypto map
Inbound: #pkts dec'd 0 drop 0 life (KB/Sec) 0/0
Outbound: #pkts enc'd 0 drop 0 life (KB/Sec) 0/0
IPSEC FLOW: permit 47 192.168.2.0/255.255.255.252 192.168.1.0/255.255.255.252
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'd 44 drop 0 life (KB/Sec) 4550081/3261
Outbound: #pkts enc'd 42 drop 3 life (KB/Sec) 4550081/3261
IPSEC FLOW: permit 17 192.168.2.0/255.255.255.252 port 500 192.168.1
*Mar 1 02:57:01.447: %SEC-6-IPACCESSLOGRP: list 110 permitted gre 192.168.2.1 -
> 192.168.1.1, 2 packets .0/255.255.255.252
Active SAs: 0, origin: crypto map
Inbound: #pkts dec'd 0 drop 0 life (KB/Sec) 0/0
Outbound: #pkts enc'd 0 drop 0 life (KB/Sec) 0/0

BRANCH-RIGHT#

```

Рис. 1.26. Результат виконання діагностичних команд show crypto session та show crypto session detail для маршрутизатора BRANCH-RIGHT

```

BRANCH-RIGHT
BRANCH-RIGHT#show crypto isakmp sa
dst      src      state      conn-id slot status
192.168.1.1 192.168.2.1 QM_IDLE    1      0 ACTIVE

BRANCH-RIGHT#show crypto ipsec sa

interface: Serial1/0
Crypto map tag: SCLabs-MAP, local addr 192.168.2.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.252/47/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.252/47/0)
current_peer 192.168.1.1 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 63, #pkts encrypt: 63, #pkts digest: 63
#pkts decaps: 64, #pkts decrypt: 64, #pkts verify: 64
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 3, #recv errors 0

local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.1.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0xEDA06CB6(3986713782)

inbound esp sas:
  spi: 0x20FF9AAC(553622188)
    transform: esp-256-aes ,
    in use settings = {Tunnel, }
    conn id: 2001, flow id: SW:1, crypto map: SCLabs-MAP
    sa timing: remaining key lifetime (k/sec): (4550078/3060)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

```

Рис. 1.27. Результат виконання діагностичних команд show crypto isakmp sa та show crypto ipsec sa для маршрутизатора BRANCH-RIGHT

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

```

BRANCH-LEFT
BRANCH-LEFT#traceroute 10.10.2.1

Type escape sequence to abort.
Tracing the route to 10.10.2.1

  1 1.1.1.2 44 msec 64 msec 64 msec
BRANCH-LEFT#traceroute 172.16.2.1

Type escape sequence to abort.
Tracing the route to 172.16.2.1

  1 1.1.1.2 48 msec 60 msec 64 msec
BRANCH-LEFT#traceroute 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.2.1

  1 192.168.1.2 12 msec 16 msec 24 msec
  2 10.0.0.2 36 msec 44 msec 48 msec
  3 192.168.2.1 48 msec 60 msec 64 msec
BRANCH-LEFT#

```

Рис. 1.28. Перевірка наявності зв'язку за допомогою команди traceroute

1.4.2. Аналіз створеного рішення з використанням мережевого протоколу SSH.

Проведемо аналіз створеної мережі та конфігурації маршрутизаторів за посиланням: <https://ipcisco.com/lesson/ssh-configuration-on-packet-tracer/> та спробуємо відворити дане рішення в графічному емуляторі мереж GNS3 для детального аналізу.

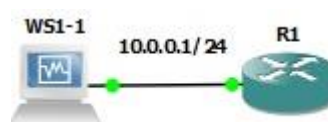


Рис. 1.29. Створена топологія мережі

```

R1
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fa0/0
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#

```

Рис. 1.30. Налаштування параметрів адресації для маршрутизатора R1

У Cisco IOS налаштування роботи протоколу SSH відбувається в CLI в режимі глобальної конфігурації наступним чином:

R1 (config) # service password-encryption – зберігаємо паролі в зашифрованому вигляді в конфігураційному файлі,

R1 (config) # cisco(config)#ip domain name [ім'я] – вказуємо домен для генерації ключа,

R1 (config) # username adminr1 privilege 15 password adminr1 – створюємо користувача adminr1 з паролем для входу adminr1 з максимальними привілеями,

R1 (config) # crypto key generate rsa general-key modulus 1024 – генеруємо RSA ключ з розміром 1024 бітів,

R1 (config) # ip ssh version 2 – включення SSH версії 2 на маршрутизаторі,

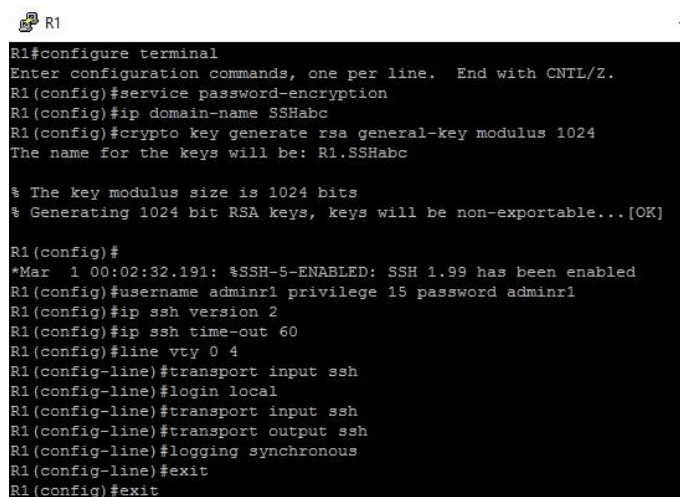
R1 (config) # ip ssh time-out 60 – визначаємо час життя сесії,

R1 (config) # line vty 0 4 – входимо в режим конфігурування термінальних ліній з 0 по 4,

R1 (config) # transport input ssh – вказуємо середовищем доступу через мережу за замовчуванням SSH

R1 (config) # transport output ssh – дозволяємо з маршрутизатора вихідний тільки по ssh,

R1 (config) # logging synchronous – активуємо автоматичне підняття рядка після відповіді системи на пророблені зміни.



```
R1
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#service password-encryption
R1(config)#ip domain-name SSHabc
R1(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: R1.SSHabc

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Mar  1 00:02:32.191: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#username adminr1 privilege 15 password adminr1
R1(config)#ip ssh version 2
R1(config)#ip ssh time-out 60
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#transport output ssh
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#exit
```

Рис. 1.31. Налаштування параметрів протоколу SSH для маршрутизатора R1

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

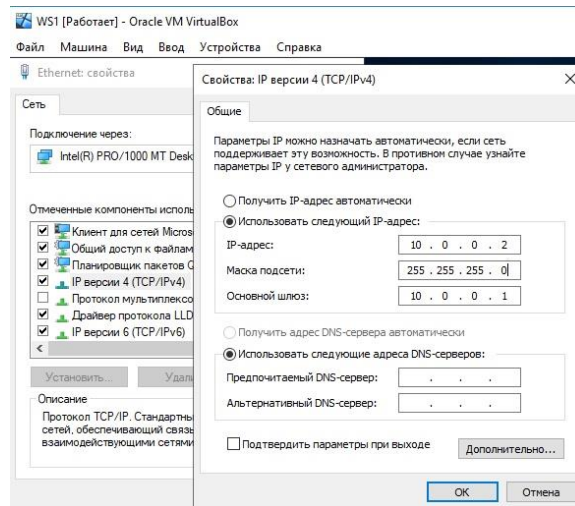


Рис. 1.32. Налаштування параметрів адресації для робочої станції WS1

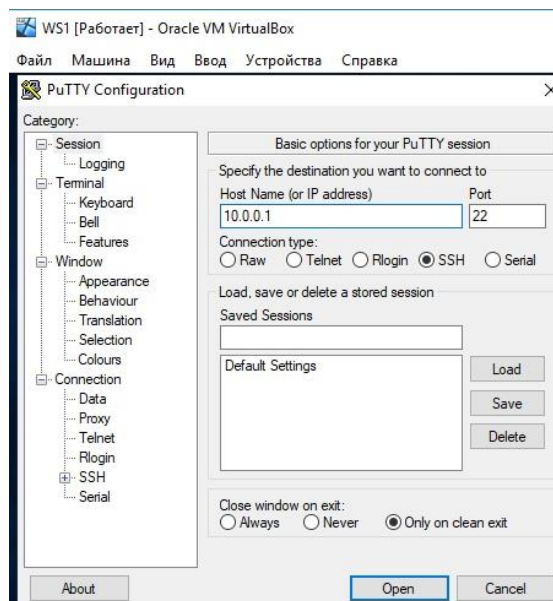


Рис. 1.33. Налаштування додатку putty для підключення до R1

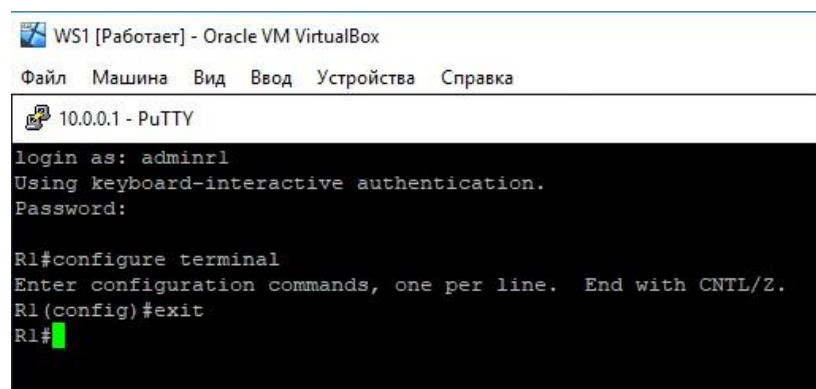


Рис. 1.34. Результат підключення до R1 за допомогою додатку putty

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

1.5. Технічна постановка завдання.

Розробити топологію та створити таблицю адресації корпоративної мережі для організації. Обрати необхідну модель маршрутизатора. Розробити параметри для налаштування роботи протоколів GRE, IP-Security, OSPF, EIGRP, SSHv2. Налаштувати обладнання захищеної корпоративної мережі організації в графічному емуляторі мереж GNS3. За допомогою діагностичних команд перевірити роботу створених IPSec тунелів між внутрішніми мережами, щоб користувачі одної мережі могли безпечно звертатися до ресурсів іншої мережі, налаштувати списки доступу (ACL), щоб переда даних відбувалася тільки по дозволеним IP-адресам. Забезпечити безперебійну роботу мережі. Здійснити підключення до маршрутизаторів мережі через SSH- клієнт PuTTY з робочої станції. Налаштувати та встановити Active Directory із роллю первинного контролера домену на першому сервері. Здійснити перевірку доступу на читання та зміни папки із робочої станції WS2 (Windows 10) під двома створеними користувачами.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до першого розділу.

При виконанні дипломної роботи в першому розділі було з'ясовано, що завдяки корпоративній мережі користувачі (співробітники) зможуть отримати доступ до загальних ресурсів організації, зможуть спільно використовувати принтери та інше мережеве обладнання. Наше головне завдання при побудові корпоративної мережі — оптимізація обробки та розподілу інформаційних потоків, а також захист переданих даних. Важливість захисту інформаційних ресурсів компанії очевидна – від цього безпосередньо залежить безпека даних, які належать підприємству, його ефективність і рентабельність. Реалізовані засоби захисту не повинні створювати «вузьких» місць у мережі, тобто не повинні суттєво впливати на масштабованість, продуктивність мережі, маршрутизацію, а також повинні забезпечити централізоване адміністрування мережі. Актуальність, безпеки переданих даних і їх захисту від несанкціонованого доступу в системах віддаленого доступу вимагає особливо пильної уваги і застосування спеціальних методик, які гарантували б достатню конфіденційність і достовірність даних.

Для вирішення поставленого завдання було проаналізовано два створених рішення з використанням технологій протоколу тунелювання GRE, протоколу захисту даних IP-Security, протоколів динамічної маршрутизації OSPF, EIGRP та мережевого протоколу SSH. Аналіз створених рішень дав розуміння того, які технології використовувати для вирішення поставленого завдання.

Для створення зв'язки «віддалений доступ + тунелювання + аутентифікація + шифрування», яка дозволяє побудувати захищену мережу VPN, було досліджено теоретичні аспекти мережевої моделі OSI як базової еталонної моделі взаємодії відкритих систем. Також було досліджено особливості функціонування стеку протоколів для безпечного обміну інформацією по IP - IPsec та протокол тунелювання мережевих пакетів GRE. Проаналізував особливості функціонування протоколів маршрутизації OSPF та EIGRP та особливості головних протоколів для здійснення віддаленого доступу до обладнання мережі Telnet та SSH.

Це дало розуміння, можливість аналізу та варіанти виконання поставленого завдання.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ

2.1. Розробка топології комп'ютерної мережі.

При проектуванні мережі була використана трирівнева структура, яка включає в себе:

- рівень ядра;
- рівень розподілу;
- рівень доступу.

Дана спроектована мережа представлена на рис 2.1:

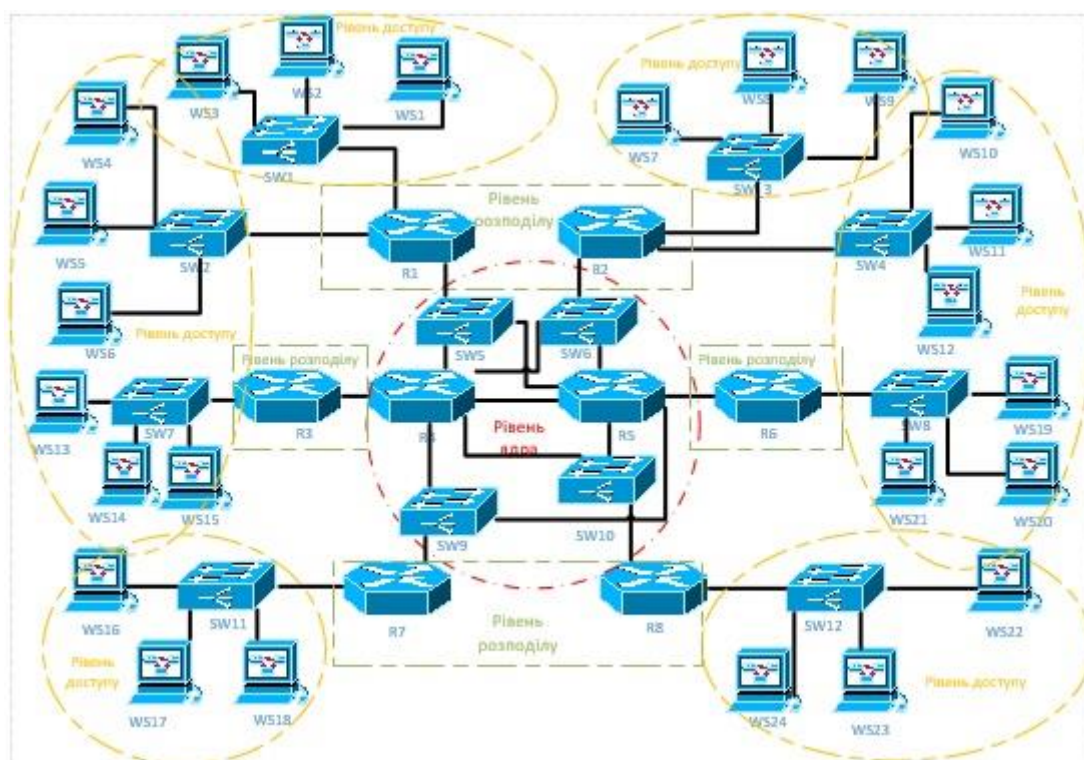


Рис 2.1. Загальна топологія мережі

Рівень ядра складається з 2 маршрутизаторів з'єднаних між собою витою парою Fast Ethernet, 4 комутаторів SW5, SW6, SW9 та SW10 які з'єднані з маршрутизаторами R4 та R5 за допомогою мідного прямогоочного кабелю (copper straight-through cable).

Ядро являє собою комплекс мережевих пристроїв (маршрутизаторів і комутаторів), що забезпечують високошвидкісну передачу даних між різними сегментами рівня розподілу.

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

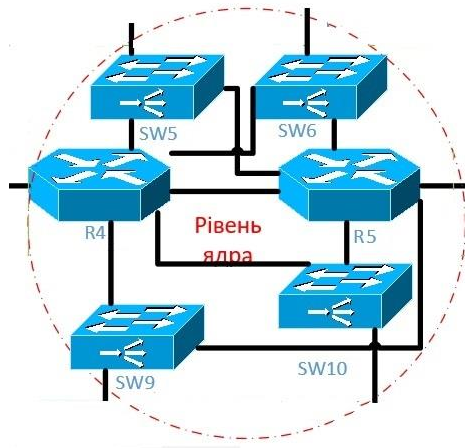


Рис 2.2. Створений рівень ядра мережі

Рівень розподілу представляє собою набір з 5 маршрутизаторів, що під'єднані до ядра мережі. З'єднання з ядром мережі виконано за допомогою мідного прямогооточного кабелю (copper straight-through cable).

На рівні розподілу вирішуються завдання агрегації широкомовних доменів і доменів маршрутизації, фільтрації, забезпечення високого рівня доступності ядра для кінцевих користувачів.

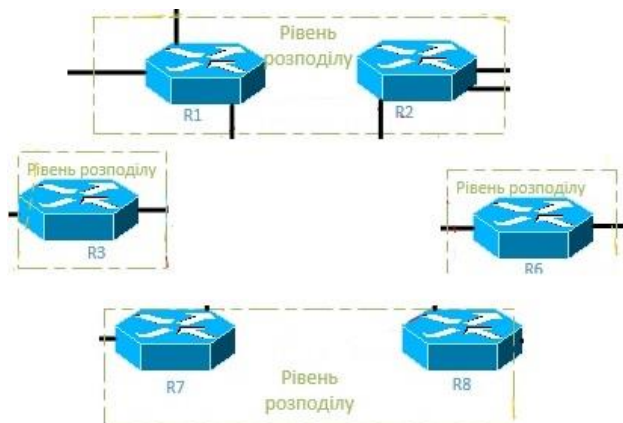


Рис 2.3. Створений рівень розподілу мережі

Рівень доступу представлений кінцевим устаткуванням користувачів та комутаційним обладнанням, що забезпечує функціонування цього рівня.

Особливістю з'єднань комутаційного обладнання є те, що для забезпечення високої продуктивності роботи мережі використовуються високошвидкісні лінії зв'язку Fast Ethernet. Кінцеві вузли під'єднанні до комутаційного обладнання за допомогою ліній Ethernet на витій парі.

Рівень доступу слугує для підключення робочих станцій та серверів компанії. Основна задача комутатора до якого підключені пристрої надання доступу робочих станцій і серверів до наступного рівня (розподілу) ієрархії.

В загальному в мережі використано 8 маршрутизаторів та 12 комутаторів на 24 порта. Створена мережа складається з 15 підмереж. Кожній підмережі належить одна IP-адреса.



Рис 2.4. Під'єднані пристрої до комутатора SW1

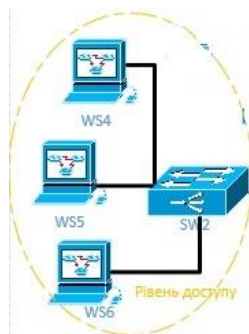


Рис 2.5. Під'єднані пристрої до комутатора SW2



Рис 2.6. Під'єднані пристрої до комутатора SW3

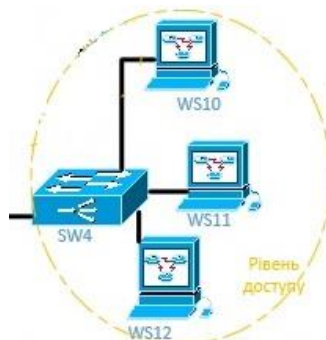


Рис 2.7. Під'єднані пристрої до комутатора SW4



Рис 2.8. Під'єднані пристрої до комутатора SW7

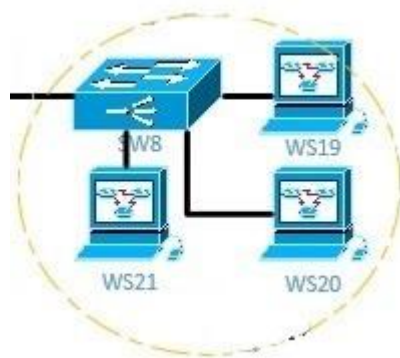


Рис 2.9. Під'єднані пристрої до комутатора SW8



Рис 2.10. Під'єднані пристрої до комутатора SW11

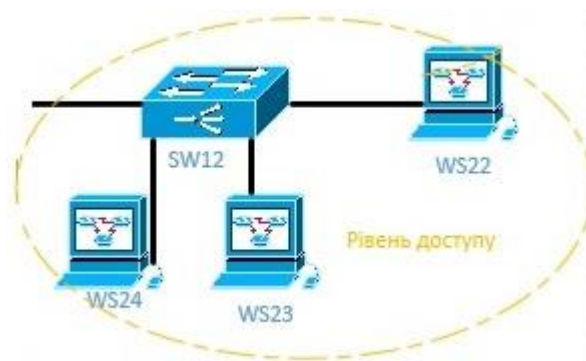


Рис 2.11. Під'єднані пристрої до комутатора SW12

Для спроектованої мережі було заповнено наступну описову таблицю:

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.1

Параметри з'єднань пристроїв та каналів

Пристрій	Канал	Інтерф ейси	Підключення до пристрою	Підключення до інтерфейсів
Маршрутизатор R1	Канал зв'язку між пристроями	Fa0/0	Комутатор SW1	Eth0
	Канал зв'язку між пристроями	Fa0/1	Комутатор SW2	Eth0
	Канал зв'язку між пристроями	Fa1/0	Комутатор SW5	Eth0
Маршрутизатор R2	Канал зв'язку між пристроями	Fa0/0	Комутатор SW3	Eth0
	Канал зв'язку між пристроями	Fa0/1	Комутатор SW4	Eth0
	Канал зв'язку між пристроями	Fa1/0	Комутатор SW5	Eth1
Маршрутизатор R3	Канал зв'язку між пристроями	Fa0/0	Комутатор SW6	Eth0
	Канал зв'язку між пристроями	Fa3/1	Маршрутизатор R4	Fa3/1
Маршрутизатор R4	Канал зв'язку між пристроями	Fa0/0	Комутатор SW5	Eth1
	Канал зв'язку між пристроями	Fa1/0	Комутатор SW9	Eth0
	Канал зв'язку між пристроями	Fa0/1	Маршрутизатор R5	Fa0/1
	Канал зв'язку між пристроями	Fa3/1	Маршрутизатор R3	Fa3/1
	Канал зв'язку між пристроями	Fa3/0	Комутатор SW6	Eth2
	Канал зв'язку між пристроями	Fa3/3	Комутатор SW10	Eth1

Маршрутизатор R5	Канал зв'язку між пристроями	Fa0/0	Комутатор SW5	Eth1
	Канал зв'язку між пристроями	Fa1/0	Комутатор SW10	Eth0
	Канал зв'язку між пристроями	Fa0/1	Маршрутизатор R4	Fa0/1
	Канал зв'язку між пристроями	Fa3/1	Маршрутизатор R6	Fa3/1
	Канал зв'язку між пристроями	Fa3/0	Комутатор SW5	Eth2
	Канал зв'язку між пристроями	Fa3/3	Комутатор SW9	Eth1
Маршрутизатор R6	Канал зв'язку між пристроями	Fa3/1	Маршрутизатор R5	Fa3/1
	Канал зв'язку між пристроями	Fa0/0	Комутатор SW8	Eth0
Маршрутизатор R7	Канал зв'язку між пристроями	Fa0/0	Комутатор SW9	Eth2
	Канал зв'язку між пристроями	Fa0/1	Комутатор SW11	Eth0
Маршрутизатор R8	Канал зв'язку між пристроями	Fa0/0	Комутатор SW10	Eth2
	Канал зв'язку між пристроями	Fa0/1	Комутатор SW12	Eth0
Комутатор SW1	Канал підключення PC	Eth1	WS1	Fa0
	Канал підключення PC	Eth2	WS2	Fa0
	Канал підключення PC	Eth3	WS3	Fa0
	Канал зв'язку між пристроями	Eth0	Маршрутизатор R1	Fa0/0
Комутатор SW2	Канал підключення PC	Eth1	WS4	Fa0
	Канал підключення PC	Eth2	WS5	Fa0
	Канал підключення PC	Eth3	WS6	Fa0
	Канал зв'язку між пристроями	Eth0	Маршрутизатор R1	Fa0/1

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

Комутатор SW3	Канал підключення PC	Eth1	WS7	Fa0
	Канал підключення PC	Eth2	WS8	Fa0
	Канал підключення PC	Eth3	WS9	Fa0
	Канал зв'язку між пристроями	Eth0	Маршрутизатор R2	Fa0/0
Комутатор SW4	Канал підключення PC	Eth1	WS10	Fa0
	Канал підключення PC	Eth2	WS11	Fa0
	Канал підключення PC	Eth3	WS12	Fa0
	Канал зв'язку між пристроями	Eth0	Маршрутизатор R2	Fa0/1
Комутатор SW5	Канал зв'язку між пристроями	Eth0	Маршрутизатор R1	Fa1/0
	Канал зв'язку між пристроями	Eth1	Маршрутизатор R4	Fa0/0
	Канал зв'язку між пристроями	Eth2	Маршрутизатор R5	Fa3/0
Комутатор SW6	Канал зв'язку між пристроями	Eth1	Маршрутизатор R5	Fa0/0
	Канал зв'язку між пристроями	Eth2	Маршрутизатор R4	Fa3/0
	Канал зв'язку між пристроями	Eth0	Маршрутизатор R2	Fa1/0
Комутатор SW7	Канал підключення PC	Eth1	WS13	Fa0
	Канал підключення PC	Eth2	WS14	Fa0
	Канал підключення PC	Eth3	WS15	Fa0
	Канал зв'язку між пристроями	Eth0	Маршрутизатор R3	Fa0/0
Комутатор SW8	Канал підключення PC	Eth1	WS19	Fa0
	Канал підключення PC	Eth2	WS20	Fa0
	Канал підключення PC	Eth3	WS21	Fa0
	Канал зв'язку між пристроями	Eth0	Маршрутизатор R6	Fa0/0
Комутатор SW9	Канал зв'язку між пристроями	Eth2	Маршрутизатор R7	Fa0/0

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

	Канал зв'язку між пристроями	Eth1	Маршрутизатор R5	Fa3/3
	Канал зв'язку між пристроями	Eth0	Маршрутизатор R4	Fa1/0
Комутатор SW10	Канал зв'язку між пристроями	Eth1	Маршрутизатор R4	Fa3/3
	Канал зв'язку між пристроями	Eth2	Маршрутизатор R8	Fa0/0
	Канал зв'язку між пристроями	Eth0	Маршрутизатор R5	Fa1/0
Комутатор SW11	Канал підключення PC	Eth1	WS16	Fa0
	Канал підключення PC	Eth2	WS17	Fa0
	Канал підключення PC	Eth3	WS18	Fa0
	Канал зв'язку між пристроями	Eth0	Маршрутизатор R7	Fa0/1
Комутатор SW12	Канал підключення PC	Eth1	WS22	Fa0
	Канал підключення PC	Eth2	WS23	Fa0
	Канал підключення PC	Eth3	WS24	Fa0
	Канал зв'язку між пристроями	Eth0	Маршрутизатор R8	Fa0/1
Робоча станція WS1	Канал підключення PC	Fa0	Комутатор SW1	Eth1
Робоча станція WS2	Канал підключення PC	Fa0		Eth2
Робоча станція WS3	Канал підключення PC	Fa0		Eth3
Робоча станція WS4	Канал підключення PC	Fa0	Комутатор SW2	Eth1
Робоча станція WS5	Канал підключення PC	Fa0		Eth2
Робоча станція WS6	Канал підключення PC	Fa0		Eth3
Робоча станція WS7	Канал підключення PC	Fa0	Комутатор SW3	Eth1
Робоча станція WS8	Канал підключення PC	Fa0		Eth2
Робоча станція WS9	Канал підключення PC	Fa0		Eth3
Робоча станція WS10	Канал підключення PC	Fa0	Комутатор SW4	Eth1
Робоча станція WS11	Канал підключення PC	Fa0		Eth2
Робоча станція WS12	Канал підключення PC	Fa0		Eth3
Робоча станція WS13	Канал підключення PC	Fa0	Комутатор SW7	Eth1
Робоча станція WS14	Канал підключення PC	Fa0		Eth2

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

Робоча станція WS15	Канал підключення PC	Fa0	Комутатор SW11	Eth3
Робоча станція WS16	Канал підключення PC	Fa0		Eth1
Робоча станція WS17	Канал підключення PC	Fa0		Eth2
Робоча станція WS18	Канал підключення PC	Fa0		Eth3
Робоча станція WS19	Канал підключення PC	Fa0	Комутатор SW8	Eth1
Робоча станція WS20	Канал підключення PC	Fa0		Eth2
Робоча станція WS21	Канал підключення PC	Fa0		Eth3
Робоча станція WS22	Канал підключення PC	Fa0	Комутатор SW12	Eth1
Робоча станція WS23	Канал підключення PC	Fa0		Eth2
Робоча станція WS24	Канал підключення PC	Fa0		Eth3

2.2. Розробка схеми адресації мережі.

Таблиця 2.2

Таблиця адресації пристроїв створеної мережі

Прістрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Мережа А	-	181.3.15.0	255.255.255.240	/28
Мережа В	-	182.3.15.0	255.255.255.240	/28
Мережа С	-	183.3.15.0	255.255.255.248	/29
Мережа D	-	184.3.15.0	255.255.255.248	/29
Мережа Е	-	185.3.15.0	255.255.255.240	/28
Мережа F	-	186.3.15.0	255.255.255.240	/28
Мережа G	-	187.3.15.0	255.255.255.240	/28
Мережа H	-	188.3.15.0	255.255.255.252	/30
Мережа K	-	189.3.15.0	255.255.255.252	/30
Мережа L	-	190.3.15.0	255.255.255.252	/30
Мережа M	-	191.3.15.0	255.255.255.240	/28
Мережа N	-	192.3.15.0	255.255.255.240	/28
Мережа P	-	193.3.15.0	255.255.255.248	/29
Мережа R	-	194.3.15.0	255.255.255.248	/29
Мережа S	-	195.3.15.0	255.255.255.240	/28
R1	Fa0/0	181.3.15.1	255.255.255.240	/28
	Fa0/1	182.3.15.1	255.255.255.240	/28
	Fa1/0	183.3.15.1	255.255.255.248	/29

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

	Інтерфейс Tunnel12	101.3.15.1	255.255.255.0	/24
	Інтерфейс Tunnel13	102.3.15.1	255.255.255.0	/24
	Інтерфейс Tunnel16	103.3.15.1	255.255.255.0	/24
	Інтерфейс Tunnel17	104.3.15.1	255.255.255.0	/24
	Інтерфейс Tunnel18	105.3.15.1	255.255.255.0	/30
	Інтерфейс Loopback 11	11.11.11.11	255.255.255.0	/24
R2	Fa0/0	185.3.15.1	255.255.255.240	/28
	Fa0/1	186.3.15.1	255.255.255.240	/28
	Fa1/0	184.3.15.1	255.255.255.248	/29
	Інтерфейс Tunnel12	101.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel23	106.3.15.1	255.255.255.0	/24
	Інтерфейс Tunnel26	107.3.15.1	255.255.255.0	/24
	Інтерфейс Tunnel27	108.3.15.1	255.255.255.0	/24
	Інтерфейс Tunnel28	109.3.15.1	255.255.255.0	/30
	Інтерфейс Loopback 22	22.22.22.22	255.255.255.0	/24
R3	Fa0/0	187.3.15.1	255.255.255.240	/28
	Fa3/1	188.3.15.1	255.255.255.252	/30
	Інтерфейс Tunnel13	101.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel23	106.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel36	110.3.15.1	255.255.255.0	/24
	Інтерфейс Tunnel37	111.3.15.1	255.255.255.0	/24
	Інтерфейс Tunnel38	112.3.15.1	255.255.255.0	/24
	Інтерфейс Loopback 33	33.33.33.33	255.255.255.0	/24
R4	Fa0/0	183.3.15.2	255.255.255.248	/29
	Fa0/1	189.3.15.1	255.255.255.252	/30
	Fa1/0	193.3.15.2	255.255.255.248	/29
	Fa3/1	188.3.15.2	255.255.255.252	/30
	Fa3/0	184.3.15.3	255.255.255.248	/29
	Fa3/3	194.3.15.3	255.255.255.248	/29
R5	Fa0/0	184.3.15.2	255.255.255.248	/29
	Fa0/1	189.3.15.2	255.255.255.252	/30
	Fa1/0	194.3.15.2	255.255.255.248	/29
	Fa3/1	190.3.15.1	255.255.255.252	/30
	Fa3/0	183.3.15.3	255.255.255.248	/29

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

	Fa3/3	193.3.15.3	255.255.255.248	/29
R6	Fa0/0	191.3.15.1	255.255.255.240	/28
	Fa3/1	190.3.15.2	255.255.255.252	/30
	Інтерфейс Tunnel16	103.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel26	107.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel36	110.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel67	113.3.15.1	255.255.255.0	/24
	Інтерфейс Tunnel68	114.3.15.1	255.255.255.0	/24
	Інтерфейс Loopback 66	66.66.66.66	255.255.255.0	/24
R7	Fa0/0	193.3.15.1	255.255.255.248	/29
	Fa0/1	192.3.15.1	255.255.255.240	/28
	Інтерфейс Tunnel17	104.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel27	108.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel37	111.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel67	113.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel78	115.3.15.1	255.255.255.0	/24
	Інтерфейс Loopback 77	77.77.77.77	255.255.255.0	/24
R8	Fa0/0	191.3.15.4	255.255.255.248	/29
	Fa0/1	193.3.15.1	255.255.255.240	/28
	Інтерфейс Tunnel18	104.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel28	108.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel38	111.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel68	113.3.15.2	255.255.255.0	/24
	Інтерфейс Tunnel78	115.3.15.2	255.255.255.0	/24
	Інтерфейс Loopback 88	88.88.88.88	255.255.255.0	/24
SW1	Інтерфейс Vlan 1	181.3.15.10	255.255.255.240	/28
	Шлюз за замовчуванням	181.3.15.1	-	-
SW2	Інтерфейс Vlan 1	182.3.15.10	255.255.255.240	/28
	Шлюз за замовчуванням	182.3.15.1	-	-
SW3	Інтерфейс Vlan 1	185.3.15.10	255.255.255.240	/28
	Шлюз за замовчуванням	185.3.15.1	-	-
SW4	Інтерфейс Vlan 1	186.3.15.10	255.255.255.240	/28
	Шлюз за замовчуванням	186.3.15.1	-	-
SW5	Інтерфейс Vlan 1	183.3.15.6	255.255.255.248	/29

	Шлюз за замовчуванням	183.3.15.1	-	-
SW6	Інтерфейс Vlan 1	184.3.15.10	255.255.255.248	/29
	Шлюз за замовчуванням	184.3.15.1	-	-
SW7	Інтерфейс Vlan 1	187.3.15.10	255.255.255.240	/29
	Шлюз за замовчуванням	187.3.15.1	-	-
SW8	Інтерфейс Vlan 1	191.3.15.10	255.255.255.240	/28
	Шлюз за замовчуванням	191.3.15.1	-	-
SW9	Інтерфейс Vlan 1	193.3.15.6	255.255.255.248	/29
	Шлюз за замовчуванням	193.3.15.1	-	-
SW10	Інтерфейс Vlan 1	194.3.15.6	255.255.255.248	/29
	Шлюз за замовчуванням	194.3.15.1	-	-
SW11	Інтерфейс Vlan 1	193.3.15.10	255.255.255.240	/28
	Шлюз за замовчуванням	193.3.15.1	-	-
SW12	Інтерфейс Vlan 1	195.3.15.10	255.255.255.240	/28
	Шлюз за замовчуванням	195.3.15.1	-	-
WS1	Мережний адаптер	181.3.15.2	255.255.255.240	/28
	Шлюз за замовчуванням	181.3.15.1	-	-
WS2	Мережний адаптер	181.3.15.3	255.255.255.240	/28
	Шлюз за замовчуванням	181.3.15.1	-	-
WS3	Мережний адаптер	181.3.15.4	255.255.255.240	/28
	Шлюз за замовчуванням	181.3.15.1	-	-
WS4	Мережний адаптер	182.3.15.2	255.255.255.240	/28
	Шлюз за замовчуванням	182.3.15.1	-	-
WS5	Мережний адаптер	182.3.15.3	255.255.255.240	/28
	Шлюз за замовчуванням	182.3.15.1	-	-
WS6	Мережний адаптер	182.3.15.4	255.255.255.240	/28
	Шлюз за замовчуванням	182.3.15.1	-	-
WS7	Мережний адаптер	185.3.15.2	255.255.255.240	/28
	Шлюз за замовчуванням	185.3.15.1	-	-
WS8	Мережний адаптер	185.3.15.3	255.255.255.240	/28
	Шлюз за замовчуванням	185.3.15.1	-	-
WS9	Мережний адаптер	185.3.15.4	255.255.255.240	/28
	Шлюз за замовчуванням	185.3.15.1	-	-

WS10	Мережний адаптер	186.3.15.2	255.255.255.240	/28
	Шлюз за замовчуванням	186.3.15.1	-	-
WS11	Мережний адаптер	186.3.15.3	255.255.255.240	/28
	Шлюз за замовчуванням	186.3.15.1	-	-
WS12	Мережний адаптер	186.3.15.4	255.255.255.240	/28
	Шлюз за замовчуванням	186.3.15.1	-	-
WS13	Мережний адаптер	187.3.15.2	255.255.255.240	/28
	Шлюз за замовчуванням	187.3.15.1	-	-
WS14	Мережний адаптер	187.3.15.3	255.255.255.240	/28
	Шлюз за замовчуванням	187.3.15.1	-	-
WS15	Мережний адаптер	187.3.15.4	255.255.255.240	/28
	Шлюз за замовчуванням	187.3.15.1	-	-
WS16	Мережний адаптер	192.3.15.2	255.255.255.240	/28
	Шлюз за замовчуванням	192.3.15.1	-	-
WS17	Мережний адаптер	192.3.15.3	255.255.255.240	/28
	Шлюз за замовчуванням	192.3.15.1	-	-
WS18	Мережний адаптер	192.3.15.4	255.255.255.240	/28
	Шлюз за замовчуванням	192.3.15.1	-	-
WS19	Мережний адаптер	191.3.15.2	255.255.255.240	/28
	Шлюз за замовчуванням	191.3.15.1	-	-
WS20	Мережний адаптер	191.3.15.3	255.255.255.240	/28
	Шлюз за замовчуванням	191.3.15.1	-	-
WS21	Мережний адаптер	191.3.15.4	255.255.255.240	/28
	Шлюз за замовчуванням	191.3.15.1	-	-
WS22	Мережний адаптер	195.3.15.2	255.255.255.240	/28
	Шлюз за замовчуванням	195.3.15.1	-	-
WS23	Мережний адаптер	195.3.15.3	255.255.255.240	/28
	Шлюз за замовчуванням	195.3.15.1	-	-
WS24	Мережний адаптер	195.3.15.4	255.255.255.240	/28
	Шлюз за замовчуванням	195.3.15.1	-	-

2.3. Розробка налаштувань для GRE тунелів з використанням шифрування IPSec.

Всі тунельні інтерфейси маршрутизаторів завжди повинні бути налаштовані з IP-адресою, який не використовується де-небудь ще в мережі. Кожному тунельному інтерфейсу призначається IP-адреса в тій же мережі, що й іншим тунельним інтерфейсів.

Оскільки GRE є протоколом інкапсуляції, ми встановлюємо максимальну одиницю передачі (MTU - Maximum Transfer Unit) до 1400 байт, а максимальний розмір сегмента (MSS - Maximum Segment Size) - до 1360 байт. Оскільки більшість транспортних MTU мають розмір 1500 байт і у нас є додаткові витрати через GRE, ми повинні зменшити MTU для обліку додаткових службових даних. Встановлення 1400 є звичайною практикою і гарантує, що непотрібна фрагментація пакетів буде зведена до мінімуму. Визначимо основні параметри для налагодження протоколу GRE для пристроїв підмереж. Для визначення параметрів скористаємося даними табл. 2.3, 2.4, 2.5 та 2.6.

Таблиця 2.3

Параметри для налагодження тунелів

Параметр	Маршрутизатор R1	Маршрутизатор R2	Маршрутизатор R1	Маршрутизатор R3	Маршрутизатор R1	Маршрутизатор R6	Маршрутизатор R1	Маршрутизатор R7
Тунельний інтерфейс	Tunnel 12	Tunnel 12	Tunnel 13	Tunnel 13	Tunnel 16	Tunnel 16	Tunnel 17	Tunnel 17
Опис інтерфейсу	TUNNEL_TO_LAN_F	TUNNEL_TO_LAN_AB	TUNNEL_TO_LAN_G	TUNNEL_TO_LAN_AB	TUNNEL_TO_LAN_M	TUNNEL_TO_LAN_AB	TUNNEL_TO_LAN_N	TUNNEL_TO_LAN_AB
IP-адреса інтерфейсу	101.3.15.1	101.3.15.2	102.3.15.1	102.3.15.2	103.3.15.1	103.3.15.2	104.3.15.1	104.3.15.2

Маска	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Tunnel Source	183.3.15.1	184.3.15.1	183.3.15.1	188.3.15.1	183.3.15.1	190.3.15.2	183.3.15.1	193.3.15.1
Tunnel Destination	184.3.15.1	183.3.15.1	188.3.15.1	183.3.15.1	190.3.15.2	183.3.15.1	193.3.15.1	183.3.15.1
Tunnel Mode	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)
IP MTU, байт	1400	1400	1400	1400	1400	1400	1400	1400
TCP MSS, байт	1360	1360	1360	1360	1360	1360	1360	1360

Таблиця 2.4

Параметри для налагодження тунелів

Параметр	Маршрутизатор R1	Маршрутизатор R8	Маршрутизатор R2	Маршрутизатор R3	Маршрутизатор R2	Маршрутизатор R6
Тунельний інтерфейс	Tunnel 18	Tunnel 18	Tunnel 23	Tunnel 23	Tunnel 26	Tunnel 26
Опис інтерфейсу	TUNNEL_TO_LAN_S	TUNNEL_TO_LAN_AB	TUNNEL_TO_LAN_G	TUNNEL_TO_LAN_F	TUNNEL_TO_LAN_M	TUNNEL_TO_LAN_FE
IP-адреса інтерфейсу	105.3.15.1	105.3.15.2	106.3.15.1	106.3.15.2	107.3.15.1	107.3.15.2
Маска	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Tunnel Source	183.3.15.1	194.3.15.1	184.3.15.1	188.3.15.1	184.3.15.1	190.3.15.2

		Охріменко Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Tunnel Destination	194.3.15.1	183.3.15.1	188.3.15.1	184.3.15.1	190.3.15.2	184.3.15.1
Tunnel Mode	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)
IP MTU, байт	1400	1400	1400	1400	1400	1400
TCP MSS, байт	1360	1360	1360	1360	1360	1360

Таблиця 2.5

Параметри для налагодження тунелів

Параметр	Маршрутизатор R2	Маршрутизатор R7	Маршрутизатор R2	Маршрутизатор R8	Маршрутизатор R3	Маршрутизатор R6	Маршрутизатор R3	Маршрутизатор R7
Тунельний інтерфейс	Tunnel 27	Tunnel 27	Tunnel 28	Tunnel 28	Tunnel 36	Tunnel 36	Tunnel 37	Tunnel 37
Опис інтерфейсу	TUNNEL_TO_LAN_N	TUNNEL_TO_LAN_FE	TUNNEL_TO_LAN_S	TUNNEL_TO_LAN_FE	TUNNEL_TO_LAN_M	TUNNEL_TO_LAN_G	TUNNEL_TO_LAN_N	TUNNEL_TO_LAN_G
IP-адреса інтерфейсу	108.3.15.1	108.3.15.2	109.3.15.1	109.3.15.2	110.3.15.1	110.3.15.2	111.3.15.1	111.3.15.2
Маска	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Tunnel Source	184.3.15.1	193.3.15.1	184.3.15.1	194.3.15.1	188.3.15.1	190.3.15.2	188.3.15.1	193.3.15.1
Tunnel Destination	193.3.15.1	184.3.15.1	194.3.15.1	184.3.15.1	190.3.15.2	188.3.15.1	193.3.15.1	188.3.15.1

		Охріменко Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

Tunnel Mode	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)
IP MTU, байт	1400	1400	1400	1400	1400	1400	1400	1400
TCP MSS, байт	1360	1360	1360	1360	1360	1360	1360	1360

Таблиця 2.6

Параметри для налагодження тунелів

Параметр	Маршрутизатор R3	Маршрутизатор R8	Маршрутизатор R6	Маршрутизатор R7	Маршрутизатор R6	Маршрутизатор R8	Маршрутизатор R7	Маршрутизатор R8
Тунельний інтерфейс	Tunnel 38	Tunnel 38	Tunnel 67	Tunnel 67	Tunnel 68	Tunnel 68	Tunnel 78	Tunnel 78
Опис інтерфейсу	TUNNEL_TO_LAN_S	TUNNEL_TO_LAN_G	TUNNEL_TO_LAN_N	TUNNEL_TO_LAN_M	TUNNEL_TO_LAN_S	TUNNEL_TO_LAN_M	TUNNEL_TO_LAN_S	TUNNEL_TO_LAN_N
IP-адреса інтерфейсу	112.3.15.1	112.3.15.2	113.3.15.1	113.3.15.2	114.3.15.1	114.3.15.2	115.3.15.1	115.3.15.2
Маска	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Tunnel Source	188.3.15.1	194.3.15.1	190.3.15.2	193.3.15.1	190.3.15.2	194.3.15.1	193.3.15.1	194.3.15.1
Tunnel Destination	194.3.15.1	188.3.15.1	193.3.15.1	190.3.15.2	194.3.15.1	190.3.15.2	194.3.15.1	193.3.15.1

		Охріменко Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

Tunnel Mode	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)	IP (за замовчуванням)
IP MTU, байт	1400	1400	1400	1400	1400	1400	1400	1400
TCP MSS, байт	1360	1360	1360	1360	1360	1360	1360	1360

Так як, GRE є протоколом інкапсуляції і не виконує шифрування. Створення тунелю GRE точка-точка без будь-якого шифрування надзвичайно ризиковано, оскільки конфіденційні дані можуть бути легко вилучені з тунелю і переглянуті іншими.

Для цього ми використовуємо IPSec для додавання рівня шифрування і захисту тунелю GRE. Це забезпечує нам необхідне шифрування військового рівня. Шифрування IPSec включає в себе два етапи для кожного маршрутизатора. Потрібно виконати наступні кроки:

- Налаштування ISAKMP (ISAKMP Phase 1).
- Налаштування IPSec (ISAKMP Phase 2).

Таблиця 2.7

Налаштування політики ISAKMP Phase 1

Параметри	Встановлені значення для інтерфейсів														
	Tunnel12	Tunnel13	Tunnel16	Tunnel17	Tunnel18	Tunnel23	Tunnel26	Tunnel27	Tunnel28	Tunnel36	Tunnel37	Tunnel38	Tunnel67	Tunnel68	Tunnel78
Політика безпеки	ISAKMP														
Метод шифрування	AES 256														
Метод аутентифікації	pre-share														
Метод обміну	DH 2														

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Маршрутизатор	Розмір ключа, бітів	Інтервал очікування перед розривом сесії, с	Кількість спроб аутентифікації	Максимальна кількість сесій
R1	1024	30	3	5
R2	2048	20	4	9
R3	1024	45	5	6
R4	1280	60	3	4
R5	1024	30	3	5
R6	2048	25	4	9
R7	1024	20	3	5
R8	2048	30	5	4

Таблиця 2.10

Створена база користувачів для маршрутизаторів мережі

Маршрутизатор	Користувач	Пароль	Рівень привілеїв
R1	adminr1	admin	15
	userr1	user	1
R2	adminr2	admin	15
	userr2	user	1
R3	adminr3	admin	15
	userr3	user	1
R4	adminr4	admin	15
	userr4	user	1
R5	adminr5	admin	15
	userr5	user	1
R6	adminr6	admin	15
	userr6	user	1
R7	adminr7	admin	15
	userr7	user	1
R8	adminr8	admin	15
	userr8	user	1

2.5. Розробка параметрів для налаштування Active Directory на сервері.

Таблиця 2.11

Створена база користувачів для Active Directory користувачі і комп'ютери

Пристрій	Користувач	Пароль	Рівень привілеїв	Група ADMINPAPOK
WS1	Okhrimenko2	Qwerty123	admin	Член групи
	Okhrimenko3	Qwerty1234	user	-

Висновки до другого розділу.

Після аналізу теоретичних відомостей та створених рішень в першому розділі, можна зробити висновок, що успішна робота організацій, які використовують ті чи інші інформаційно-комунікаційні системи, залежить від того наскільки добре вони захищені від можливих загроз безпеки. Для реалізації захищеної корпоративної мережі організації було розроблено структуру ядра мережі, наведено обґрунтування вибору маршрутизаторів та зв'язків між ними. Наведено загальну кількість необхідного обладнання.

Для побудованої мережі розроблено схему її адресації, яка дозволяє легке управління адресами пристроїв та призначена до подальшого розширення мережі, обрані типи з'єднання між обладнанням у мережі. Було створено таблицю параметрів для налагодження віддаленого підключення до маршрутизаторів мережі за протоколом SSHv2 та розроблено таблицю параметрів для налагодження тунелів, а також, таблиці для налаштування політики ISAKMP Phase 1 та Phase 2 для маршрутизаторів які належать рівню розподілу. Також були створені налаштування для двох маршрутизаторів які належать рівню ядра, що забезпечують високошвидкісну передачу даних між різними сегментами рівня розподілу. Створено базу користувачів для Active Directory користувачі і комп'ютери.

Отже, в даному розділі були розроблені всі необхідні налаштування обладнання для подальшого проектування захищеної корпоративної мережі організації в графічному емуляторі мереж GNS3.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ

3.1. Вибір обладнання для організації роботи мережі.

При виборі моделі маршрутизатора потрібно враховувати як він маршрутизує пакети в складній мережі з різними видами топологій. Маршрутизатор повинен містити достатню кількість портів, забезпечувати легке розширення мережі, забезпечувати необхідну швидкість передачі даних та швидкість їх обробки.

На рівні ядра та на рівні розподілу нам потрібний маршрутизатор який би підтримував би технологію FastEthernet, протокол OSPF, протокол EIGRP, та містив додаткові функції налаштування. Маршрутизатор CiscoSystems CISCO3660, рис 3.1 та рис 3.2, найбільш оптимальний варіант для великої мережі підприємства чи офісу.

Маршрутизатор Cisco 3660 є результатом подальшого розвитку мультисервісних серій Cisco 2600 і 3600 залучаючи в сферу застосування платформи великі філії, телефонні компанії та великих сервіс-провайдерів. Серія Cisco 3600 - це багатфункціональна та надзвичайно гнучка платформа з широким набором мережевих модулів.



Рис 3.1. Маршрутизатор Cisco Systems CISCO3660

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				77
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис 3.2. Маршрутизатор Cisco Systems CISCO3660

Унікальне модульне шасі Cisco 3660 було розроблене спеціально для побудови високонадійних і легких в обслуговуванні систем, забезпечуючи високопродуктивне і ефективне за ціною рішення для побудови корпоративних мереж. Мережеві модулі, які були використані в серії, сумісні з платформами Cisco 1600, 1700, 2600 і 3600 що забезпечує захист інвестицій та зменшує витрати на підтримку мережі і підготовку необхідних фахівців.

Відмінними рисами Cisco 3660 є наявність резервного джерела живлення і можливості гарячій заміні модулів. Інтегровані порти на материнській платі Cisco 3660 звільняють наявні 6 слотів для досягнення більш високої щільності WAN-портів, або для мультисервисного агрегування. Це дає можливість для застосування Cisco 3660 наприклад в якості мультисервисного концентратора з високою щільністю портів, або маршрутизатора для підключення філії до АТМ-мережі, зі швидкостями від T1 / E1 Inverse Multiplexing for ATM (IMA) до OC-3.

Cisco 3660 може бути замовлена в варіанті з одним і двома Fast Ethernet портами, і забезпечує гарячу заміну мережевих модулів і резервних джерел живлення.

Основні особливості маршрутизатора Cisco 3660:

- Модульна архітектура забезпечує гнучкість в побудові рішення і можливість поступового нарощування потужності.
- Широкий набір підтримуваних інтерфейсів, що варіюються від 300bps асинхронного послідовного каналу до АТМ OC-3, підтримується

		Охріменко Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

підключення до мереж IP, ATM, Frame Relay, TDM, що дозволяє задовольнити потреби будь-якого великого філії. Підтримка інтерфейсів ATM від T1 / E1 IMA до OC-3 дає більшу гнучкість при виборі швидкості з'єднання з центральним офісом.

- Забезпечується ефективно за вартістю рішення, в якому можуть поєднуватися висока щільність голосових портів і набір додаткових інтерфейсів.

Серія Cisco 3600 включає в себе багатокористувацькі платформи Cisco 3660, Cisco 3640 та Cisco 3620. Як модульні рішення, Cisco 3660, Cisco 3640 і Cisco 3620 мають гнучкість для задоволення як поточних, так і майбутніх вимог до підключення. Серія Cisco 3600 повністю підтримується програмним забезпеченням Cisco IOS. Широкі можливості управління досягаються з використанням додатків CiscoWorks, CiscoView, і CiscoView Stack Management Interface.

Одним з найважливіших елементів сучасної мережевої інфраструктури є комутатори доступу. Це те обладнання, яке створює можливість працювати в єдиній мережі. Основним критерієм вибору моделей комутаторів є кількість портів. Також враховується швидкість передачі цих портів. У нашій мережі використовуються всі комутатори на 28 портів. Найбільш оптимальним є комутатор фірми Cisco, а саме Cisco Systems WS-C3650-24PS-L, рис 3.2.



Рис 3.3. Cisco Systems WS-C3650-24PS-L

Cisco Systems WS-C3650-24PS-L – керований комутатор з 24 портами Gigabit Ethernet та 4 слотами Gigabit SFP. Cisco Catalyst 3650 Series (WS-C3650-24PS-L) комутатори рівнів доступу та розподілу, які поєднують в собі основу для конвергенції між провідними та безпроводними мережами.

Дані комутатори обладнані новими Cisco Unified Access Data Plane (UADP) ASIC та побудовані на перевірній Cisco StackWise-160 технології.

		Охріменко. Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

Комутатори Cisco 3650 серії мають повну підтримку стандарту IEEE 802.3at Power Over Ethernet (PoE+), а також пропонують змінні блоки вентиляторів та резервні блоки живлення. Дані комутатори мають фіксовані магістральні порти (uplink) зі швидкістю 1 Гбит\с.

Набір функції IP-Base пропонує розширені інтелектуальні умови, в тому числі управління безпроводним контролером, знаходження найкоротшого шляху до кореневого комутатора (OSPF, BGP та EIGRP), рішення проблем групової маршрутизації (PIM), аналіз трафіка з можливістю детальної інспекції пакетів (Flexible NetFlow), а також базовий набір протоколів для маршрутизації Routing Information Protocol functions.

Особливості комутатору Cisco Systems WS-C3650-24PS-L:

- 1) Вбудовані бездротові можливості, підтримка до 25 точок доступу та до 1000 безпроводних клієнтів (в одиночному режимі або в стеці).
- 2) Підтримка технології energy-efficient Ethernet (EEE) на комутаторах з PoE+.
- 3) Резервний блок живлення та три блока вентиляторів для відмовостійкості.
- 4) Універсальне програмне забезпечення Cisco IOS, яке має можливість апгрейда сервісів за допомогою спеціалізованих ліцензій.
- 5) Підтримка IPv4 та IPv6, багатоадресової маршрутизації, якості обслуговування QoS, протоколу NetFlow v9 та розширених функцій безпеки.

На передній панелі пристрою розташовані Ethernet порти і порти агрегації SFP (Uplinks). На задній панелі розташовані роз'єми живлення, роз'єми стекирования StackWise-160, а також роз'єм для підключення консолі управління і роз'єм Ethernet для управління комутатором через мережу. Детальна характеристика наведена у додатку Б2.

3.2. Налаштування маршрутизаторів мережі.

Перш за все у даній мережі було налаштовано рівень розподілу. Рівень розподілу складається з 6 маршрутизаторів: R1, R2, R3, R6, R7 та R8 з'єднаних між

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

собою за допомогою мідного прямогоочного кабелю (copper straight-through cable). Розглянемо лістинг налаштування першого маршрутизатора R1:

```
enable
configure terminal
hostname R_1
interface fa 0/0
description LINK_TO_LAN_A
ip address 181.3.15.1 255.255.255.240
no shutdown
exit
interface fa 0/1
description LINK_TO_LAN_B
ip address 182.3.15.1 255.255.255.240
no shutdown
exit
interface fa 1/0
description LINK_TO_LAN_C
ip address 183.3.15.1 255.255.255.248
no shutdown
exit
interface loopback 11
ip address 11.11.11.11 255.255.255.0
exit
interface Tunnel12
ip mtu 1400
ip tcp adjust-mss 1360
ip address 101.3.15.1 255.255.255.0
tunnel source 183.3.15.1
tunnel destination 184.3.15.1
exit
interface Tunnel13
ip mtu 1400
ip tcp adjust-mss 1360
ip address 102.3.15.1 255.255.255.0

crypto isakmp key R1R7 address 193.3.15.1
crypto isakmp key R1R8 address 194.3.15.1
crypto ipsec transform-set TRANSF esp-aes 256
crypto map MAP 12 ipsec-isakmp
description IPSEC to 184.3.15.1
set peer 184.3.15.1
set transform-set TRANSF
match address 101
exit
crypto map MAP 13 ipsec-isakmp
description IPSEC to 188.3.15.1
set peer 188.3.15.1
set transform-set TRANSF
match address 102
exit
crypto map MAP 16 ipsec-isakmp
description IPSEC to 190.3.15.2
set peer 190.3.15.2
set transform-set TRANSF
match address 103
exit
crypto map MAP 17 ipsec-isakmp
description IPSEC to 193.3.15.1
set peer 193.3.15.1
set transform-set TRANSF
match address 104
exit
crypto map MAP 18 ipsec-isakmp
description IPSEC to 194.3.15.1
set peer 194.3.15.1
set transform-set TRANSF
match address 105
```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

```

tunnel source 183.3.15.1
tunnel destination 188.3.15.1
exit
interface Tunnel16
ip mtu 1400
ip tcp adjust-mss 1360
ip address 103.3.15.1 255.255.255.0
tunnel source 183.3.15.1
tunnel destination 190.3.15.2
exit
interface Tunnel17
ip mtu 1400
ip tcp adjust-mss 1360
ip address 104.3.15.1 255.255.255.0
tunnel source 183.3.15.1
tunnel destination 193.3.15.1
exit
interface Tunnel18
ip mtu 1400
ip tcp adjust-mss 1360
ip address 105.3.15.1 255.255.255.0
tunnel source 183.3.15.1
tunnel destination 194.3.15.1
exit
router ospf 1
network 101.3.15.0 0.0.0.255 area 0
network 102.3.15.0 0.0.0.255 area 0
network 103.3.15.0 0.0.0.255 area 0
network 104.3.15.0 0.0.0.255 area 0
network 105.3.15.0 0.0.0.255 area 0
network 181.3.15.0 0.0.0.15 area 1
network 182.3.15.0 0.0.0.15 area 1
exit
router eigrp 1

```

```

exit
interface fa 1/0
crypto map MAP
exit
username adminr1 privilege 15 secret admin
username userr1 privilege 1 secret user
enable secret admin
ip domain-name mynet.net
crypto key generate rsa general-keys modulus
1024
ip ssh version 2
ip ssh time-out 30
ip ssh authentication-retries 3
ip ssh maxstartups 5
line vty 0 4
login local
transport input ssh
transport output ssh
logging synchronous
exit
access-list 101 permit gre 183.3.15.1 0.0.0.7
184.3.15.1 0.0.0.7 log
access-list 101 permit udp 183.3.15.1 0.0.0.7 eq
isakmp 184.3.15.1 0.0.0.7 log
access-list 101 deny ip any any log
access-list 102 permit gre 183.3.15.1 0.0.0.7
188.3.15.1 0.0.0.3 log
access-list 102 permit udp 183.3.15.1 0.0.0.7 eq
isakmp 188.3.15.1 0.0.0.3 log
access-list 102 deny ip any any log
access-list 103 permit gre 183.3.15.1 0.0.0.7
190.3.15.2 0.0.0.3 log
access-list 103 permit udp 183.3.15.1 0.0.0.7 eq
isakmp 190.3.15.2 0.0.0.3 log

```

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

```

network 183.3.15.0 0.0.0.7
network 11.11.11.0 0.0.0.255
no auto-summary
exit
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
lifetime 86000
exit
crypto isakmp key R1R2 address 184.3.15.1
crypto isakmp key R1R3 address 188.3.15.1
crypto isakmp key R1R6 address 190.3.15.2

```

```

access-list 103 deny ip any any log
access-list 104 permit gre 183.3.15.1 0.0.0.7
193.3.15.1 0.0.0.7 log
access-list 104 permit udp 183.3.15.1 0.0.0.7 eq
isakmp 193.3.15.1 0.0.0.7 log
access-list 104 deny ip any any log
access-list 105 permit gre 183.3.15.1 0.0.0.7
194.3.15.1 0.0.0.7 log
access-list 105 permit udp 183.3.15.1 0.0.0.7 eq
isakmp 194.3.15.1 0.0.0.7 log
access-list 105 deny ip any any log

```

Лістинг налаштування другого маршрутизатора R2:

```

enable
configure terminal
hostname R_2
interface fa 0/0
description LINK_TO_LAN_E
ip address 185.3.15.1 255.255.255.240
no shutdown
exit
interface fa 0/1
description LINK_TO_LAN_F
ip address 186.3.15.1 255.255.255.240
no shutdown
exit
interface fa 1/0
description LINK_TO_LAN_D
ip address 184.3.15.1 255.255.255.248
no shutdown
exit
interface loopback 22
ip address 22.22.22.22 255.255.255.0

```

```

crypto isakmp key R2R7 address 193.3.15.1
crypto isakmp key R2R8 address 194.3.15.1
crypto ipsec transform-set TRANSF esp-aes 256
crypto map MAP 12 ipsec-isakmp
description IPSEC to 183.3.15.1
set peer 183.3.15.1
set transform-set TRANSF
match address 101
exit
crypto map MAP 23 ipsec-isakmp
description IPSEC to 188.3.15.1
set peer 188.3.15.1
set transform-set TRANSF
match address 106
exit
crypto map MAP 26 ipsec-isakmp
description IPSEC to 190.3.15.2
set peer 190.3.15.2
set transform-set TRANSF
match address 107

```

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

```

exit
interface Tunnel12
ip mtu 1400
ip tcp adjust-mss 1360
ip address 101.3.15.2 255.255.255.0
tunnel source 184.3.15.1
tunnel destination 183.3.15.1
exit
interface Tunnel23
ip mtu 1400
ip tcp adjust-mss 1360
ip address 106.3.15.1 255.255.255.0
tunnel source 184.3.15.1
tunnel destination 188.3.15.1
exit
interface Tunnel26
ip mtu 1400
ip tcp adjust-mss 1360
ip address 107.3.15.1 255.255.255.0
tunnel source 184.3.15.1
tunnel destination 190.3.15.2
exit
interface Tunnel27
ip mtu 1400
ip tcp adjust-mss 1360
ip address 108.3.15.1 255.255.255.0
tunnel source 184.3.15.1
tunnel destination 193.3.15.1
exit
interface Tunnel28
ip mtu 1400
ip tcp adjust-mss 1360
ip address 109.3.15.1 255.255.255.0
tunnel source 184.3.15.1

```

```

exit
crypto map MAP 27 ipsec-isakmp
description IPSEC to 193.3.15.1
set peer 193.3.15.1
set transform-set TRANSF
match address 108
exit
crypto map MAP 28 ipsec-isakmp
description IPSEC to 194.3.15.1
set peer 194.3.15.1
set transform-set TRANSF
match address 109
exit
interface fa 1/0
crypto map MAP
exit
username adminr2 privilege 15 secret admin
username userr2 privilege 1 secret user
enable secret admin
ip domain-name mynet.net
crypto key generate rsa general-keys modulus
2048
ip ssh version 2
ip ssh time-out 20
ip ssh authentication-retries 4
ip ssh maxstartups 9
line vty 0 4
login local
transport input ssh
transport output ssh
logging synchronous
exit
access-list 101 permit gre 184.3.15.1 0.0.0.7
183.3.15.1 0.0.0.7 log

```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

```

tunnel destination 194.3.15.1
exit
router ospf 1
network 101.3.15.0 0.0.0.255 area 0
network 106.3.15.0 0.0.0.255 area 0
network 107.3.15.0 0.0.0.255 area 0
network 108.3.15.0 0.0.0.255 area 0
network 109.3.15.0 0.0.0.255 area 0
network 185.3.15.0 0.0.0.15 area 1
network 186.3.15.0 0.0.0.15 area 1
exit
router eigrp 1
network 184.3.15.0 0.0.0.7
network 22.22.22.0 0.0.0.255
no auto-summary
exit
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
lifetime 86000
exit
crypto isakmp key R1R2 address 183.3.15.1
crypto isakmp key R2R3 address 188.3.15.1
crypto isakmp key R2R6 address 190.3.15.2

```

```

access-list 101 permit udp 184.3.15.1 0.0.0.7 eq
isakmp 183.3.15.1 0.0.0.7 log
access-list 101 deny ip any any log
access-list 106 permit gre 184.3.15.1 0.0.0.7
188.3.15.1 0.0.0.3 log
access-list 106 permit udp 184.3.15.1 0.0.0.7 eq
isakmp 188.3.15.1 0.0.0.3 log
access-list 106 deny ip any any log
access-list 107 permit gre 184.3.15.1 0.0.0.7
190.3.15.2 0.0.0.3 log
access-list 107 permit udp 184.3.15.1 0.0.0.7 eq
isakmp 190.3.15.2 0.0.0.3 log
access-list 107 deny ip any any log
access-list 108 permit gre 184.3.15.1 0.0.0.7
193.3.15.1 0.0.0.7 log
access-list 108 permit udp 184.3.15.1 0.0.0.7 eq
isakmp 193.3.15.1 0.0.0.7 log
access-list 108 deny ip any any log
access-list 109 permit gre 184.3.15.1 0.0.0.7
194.3.15.1 0.0.0.7 log
access-list 109 permit udp 184.3.15.1 0.0.0.7 eq
isakmp 194.3.15.1 0.0.0.7 log
access-list 109 deny ip any any log

```

Лістинг налаштування маршрутизатора R3:

```

enable
configure terminal
hostname R_3
interface fa 0/0
description LINK_TO_LAN_G
ip address 187.3.15.1 255.255.255.240
no shutdown
exit

```

```

crypto ipsec transform-set TRANSF esp-aes 256
crypto map MAP 13 ipsec-isakmp
description IPSEC to 183.3.15.1
set peer 183.3.15.1
set transform-set TRANSF
match address 102
exit
crypto map MAP 23 ipsec-isakmp

```

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface fa 3/1
description LINK_TO_LAN_H
no switchport
ip address 188.3.15.1 255.255.255.252
no shutdown
exit
interface loopback 33
ip address 33.33.33.33 255.255.255.0
exit
interface Tunnel13
ip mtu 1400
ip tcp adjust-mss 1360
ip address 102.3.15.2 255.255.255.0
tunnel source 188.3.15.1
tunnel destination 183.3.15.1
exit
interface Tunnel23
ip mtu 1400
ip tcp adjust-mss 1360
ip address 106.3.15.2 255.255.255.0
tunnel source 188.3.15.1
tunnel destination 184.3.15.1
exit
interface Tunnel36
ip mtu 1400
ip tcp adjust-mss 1360
ip address 110.3.15.1 255.255.255.0
tunnel source 188.3.15.1
tunnel destination 190.3.15.2
exit
interface Tunnel37
ip mtu 1400
ip tcp adjust-mss 1360
ip address 111.3.15.1 255.255.255.0

```

```

description IPSEC to 184.3.15.1
set peer 184.3.15.1
set transform-set TRANSF
match address 105
exit
crypto map MAP 36 ipsec-isakmp
description IPSEC to 190.3.15.2
set peer 190.3.15.2
set transform-set TRANSF
match address 109
exit
crypto map MAP 37 ipsec-isakmp
description IPSEC to 193.3.15.1
set peer 193.3.15.1
set transform-set TRANSF
match address 110
exit
crypto map MAP 38 ipsec-isakmp
description IPSEC to 194.3.15.1
set peer 194.3.15.1
set transform-set TRANSF
match address 111
exit
interface fa 3/1
crypto map MAP
exit
username adminr3 privilege 15 secret admin
username userr3 privilege 1 secret user
enable secret admin
ip domain-name mynet.net
crypto key generate rsa general-keys modulus
1024
ip ssh version 2
ip ssh time-out 45

```

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				86
Змн.	Арк.	№ докум.	Підпис	Дата		

```

tunnel source 188.3.15.1
tunnel destination 193.3.15.1
exit
interface Tunnel38
ip mtu 1400
ip tcp adjust-mss 1360
ip address 112.3.15.1 255.255.255.0
tunnel source 188.3.15.1
tunnel destination 194.3.15.1
exit
router ospf 1
network 102.3.15.0 0.0.0.255 area 0
network 106.3.15.0 0.0.0.255 area 0
network 110.3.15.0 0.0.0.255 area 0
network 111.3.15.0 0.0.0.255 area 0
network 112.3.15.0 0.0.0.255 area 0
network 187.3.15.0 0.0.0.15 area 1
exit
router eigrp 1
network 188.3.15.0 0.0.0.3
network 33.33.33.0 0.0.0.255
no auto-summary
exit
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
lifetime 86000
exit
crypto isakmp key R1R3 address 183.3.15.1
crypto isakmp key R2R3 address 184.3.15.1
crypto isakmp key R3R6 address 190.3.15.2
crypto isakmp key R3R7 address 193.3.15.1
crypto isakmp key R3R8 address 194.3.15.1

```

```

ip ssh authentication-retries 5
ip ssh maxstartups 6
line vty 0 4
login local
transport input ssh
transport output ssh
logging synchronous
exit
access-list 102 permit gre 188.3.15.1 0.0.0.3
183.3.15.1 0.0.0.7 log
access-list 102 permit udp 188.3.15.1 0.0.0.3 eq
isakmp 183.3.15.1 0.0.0.7 log
access-list 102 deny ip any any log
access-list 105 permit gre 188.3.15.1 0.0.0.3
184.3.15.1 0.0.0.7 log
access-list 105 permit udp 188.3.15.1 0.0.0.3 eq
isakmp 184.3.15.1 0.0.0.7 log
access-list 105 deny ip any any log
access-list 109 permit gre 188.3.15.1 0.0.0.3
190.3.15.2 0.0.0.3 log
access-list 109 permit udp 188.3.15.1 0.0.0.3 eq
isakmp 190.3.15.2 0.0.0.3 log
access-list 109 deny ip any any log
access-list 110 permit gre 188.3.15.1 0.0.0.3
193.3.15.1 0.0.0.7 log
access-list 110 permit udp 188.3.15.1 0.0.0.3 eq
isakmp 193.3.15.1 0.0.0.7 log
access-list 110 deny ip any any log
access-list 111 permit gre 188.3.15.1 0.0.0.3
194.3.15.1 0.0.0.7 log
access-list 111 permit udp 188.3.15.1 0.0.0.3 eq
isakmp 194.3.15.1 0.0.0.7 log
access-list 111 deny ip any any log

```

Лістинг налаштування маршрутизатора R6:

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				87
Змн.	Арк.	№ докум.	Підпис	Дата		

```

enable
configure terminal
hostname R_6
interface fa 0/0
description LINK_TO_LAN_M
ip address 191.3.15.1 255.255.255.240
no shutdown
exit
interface fa 3/1
description LINK_TO_LAN_L
no switchport
ip address 190.3.15.2 255.255.255.252
no shutdown
exit
interface loopback 66
ip address 66.66.66.66 255.255.255.0
exit
interface Tunnel16
ip mtu 1400
ip tcp adjust-mss 1360
ip address 103.3.15.2 255.255.255.0
tunnel source 190.3.15.2
tunnel destination 183.3.15.1
exit
interface Tunnel26
ip mtu 1400
ip tcp adjust-mss 1360
ip address 107.3.15.2 255.255.255.0
tunnel source 190.3.15.2
tunnel destination 184.3.15.1
exit
interface Tunnel36
ip mtu 1400
ip tcp adjust-mss 1360

```

```

crypto ipsec transform-set TRANSF esp-aes 256
crypto map MAP 16 ipsec-isakmp
description IPSEC to 183.3.15.1
set peer 183.3.15.1
set transform-set TRANSF
match address 103
exit
crypto map MAP 26 ipsec-isakmp
description IPSEC to 184.3.15.1
set peer 184.3.15.1
set transform-set TRANSF
match address 107
exit
crypto map MAP 36 ipsec-isakmp
description IPSEC to 188.3.15.1
set peer 188.3.15.1
set transform-set TRANSF
match address 110
exit
crypto map MAP 67 ipsec-isakmp
description IPSEC to 193.3.15.1
set peer 193.3.15.1
set transform-set TRANSF
match address 113
exit
crypto map MAP 68 ipsec-isakmp
description IPSEC to 194.3.15.1
set peer 194.3.15.1
set transform-set TRANSF
match address 114
exit
interface fa 3/1
crypto map MAP
exit

```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 110.3.15.2 255.255.255.0
tunnel source 190.3.15.2
tunnel destination 188.3.15.1
exit
interface Tunnel67
ip mtu 1400
ip tcp adjust-mss 1360
ip address 113.3.15.1 255.255.255.0
tunnel source 190.3.15.2
tunnel destination 193.3.15.1
exit
interface Tunnel68
ip mtu 1400
ip tcp adjust-mss 1360
ip address 114.3.15.1 255.255.255.0
tunnel source 190.3.15.2
tunnel destination 194.3.15.1
exit
router ospf 1
network 103.3.15.0 0.0.0.255 area 0
network 107.3.15.0 0.0.0.255 area 0
network 110.3.15.0 0.0.0.255 area 0
network 113.3.15.0 0.0.0.255 area 0
network 114.3.15.0 0.0.0.255 area 0
network 191.3.15.0 0.0.0.15 area 1
exit
router eigrp 1
network 190.3.15.0 0.0.0.3
network 11.11.11.0 0.0.0.255
no auto-summary
exit
crypto isakmp policy 1
encr aes 256
authentication pre-share

```

```

username adminr6 privilege 15 secret admin
username userr6 privilege 1 secret user
enable secret admin
ip domain-name mynet.net
crypto key generate rsa general-keys modulus
2048
ip ssh version 2
ip ssh time-out 25
ip ssh authentication-retries 4
ip ssh maxstartups 9
line vty 0 4
login local
transport input ssh
transport output ssh
logging synchronous
exit
access-list 103 permit gre 190.3.15.2 0.0.0.3
183.3.15.1 0.0.0.7 log
access-list 103 permit udp 190.3.15.2 0.0.0.3 eq
isakmp 183.3.15.1 0.0.0.7 log
access-list 103 deny ip any any log
access-list 107 permit gre 190.3.15.2 0.0.0.3
184.3.15.1 0.0.0.7 log
access-list 107 permit udp 190.3.15.2 0.0.0.3 eq
isakmp 184.3.15.1 0.0.0.7 log
access-list 107 deny ip any any log
access-list 110 permit gre 190.3.15.2 0.0.0.3
188.3.15.1 0.0.0.3 log
access-list 110 permit udp 190.3.15.2 0.0.0.3 eq
isakmp 188.3.15.1 0.0.0.3 log
access-list 110 deny ip any any log
access-list 113 permit gre 190.3.15.2 0.0.0.3
193.3.15.1 0.0.0.7 log

```

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				89
Змн.	Арк.	№ докум.	Підпис	Дата		

```

group 2
lifetime 86000
exit
crypto isakmp key R1R6 address 183.3.15.1
crypto isakmp key R2R6 address 184.3.15.1
crypto isakmp key R3R6 address 188.3.15.1
crypto isakmp key R6R7 address 193.3.15.1
crypto isakmp key R6R8 address 194.3.15.1

```

```

access-list 113 permit udp 190.3.15.2 0.0.0.3 eq
isakmp 193.3.15.1 0.0.0.7 log
access-list 113 deny ip any any log
access-list 114 permit gre 190.3.15.2 0.0.0.3
194.3.15.1 0.0.0.7 log
access-list 114 permit udp 190.3.15.2 0.0.0.3 eq
isakmp 194.3.15.1 0.0.0.7 log
access-list 114 deny ip any any log

```

Лістинг налаштування маршрутизатора R7:

```

enable
configure terminal
hostname R_7
interface fa 0/0
description LINK_TO_LAN_P
ip address 193.3.15.1 255.255.255.248
no shutdown
exit
interface fa 0/1
description LINK_TO_LAN_N
ip address 192.3.15.1 255.255.255.240
no shutdown
exit
interface loopback 77
ip address 77.77.77.77 255.255.255.0
exit
interface Tunnel17
ip mtu 1400
ip tcp adjust-mss 1360
ip address 104.3.15.2 255.255.255.0
tunnel source 193.3.15.1
tunnel destination 183.3.15.1
exit
interface Tunnel27
ip mtu 1400

```

```

crypto ipsec transform-set TRANSF esp-aes 256
crypto map MAP 17 ipsec-isakmp
description IPSEC to 183.3.15.1
set peer 183.3.15.1
set transform-set TRANSF
match address 104
exit
crypto map MAP 27 ipsec-isakmp
description IPSEC to 184.3.15.1
set peer 184.3.15.1
set transform-set TRANSF
match address 108
exit
crypto map MAP 37 ipsec-isakmp
description IPSEC to 188.3.15.1
set peer 188.3.15.1
set transform-set TRANSF
match address 111
exit
crypto map MAP 67 ipsec-isakmp
description IPSEC to 190.3.15.2
set peer 190.3.15.2
set transform-set TRANSF
match address 113
exit

```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip tcp adjust-mss 1360
ip address 108.3.15.2 255.255.255.0
tunnel source 193.3.15.1
tunnel destination 184.3.15.1
exit
interface Tunnel37
ip mtu 1400
ip tcp adjust-mss 1360
ip address 111.3.15.2 255.255.255.0
tunnel source 193.3.15.1
tunnel destination 188.3.15.1
exit
interface Tunnel67
ip mtu 1400
ip tcp adjust-mss 1360
ip address 113.3.15.2 255.255.255.0
tunnel source 193.3.15.1
tunnel destination 190.3.15.2
exit
interface Tunnel78
ip mtu 1400
ip tcp adjust-mss 1360
ip address 115.3.15.1 255.255.255.0
tunnel source 193.3.15.1
tunnel destination 194.3.15.1
exit
router ospf 1
network 104.3.15.0 0.0.0.255 area 0
network 108.3.15.0 0.0.0.255 area 0
network 111.3.15.0 0.0.0.255 area 0
network 113.3.15.0 0.0.0.255 area 0
network 115.3.15.0 0.0.0.255 area 0
network 192.3.15.0 0.0.0.15 area 1
exit

```

```

crypto map MAP 78 ipsec-isakmp
description IPSEC to 194.3.15.1
set peer 194.3.15.1
set transform-set TRANSF
match address 115
exit
interface fa 0/0
crypto map MAP
exit
username adminr7 privilege 15 secret admin
username userr7 privilege 1 secret user
enable secret admin
ip domain-name mynet.net
crypto key generate rsa general-keys modulus
1024
ip ssh version 2
ip ssh time-out 20
ip ssh authentication-retries 3
ip ssh maxstartups 5
line vty 0 4
login local
transport input ssh
transport output ssh
logging synchronous
exit
access-list 104 permit gre 193.3.15.1 0.0.0.7
183.3.15.1 0.0.0.7 log
access-list 104 permit udp 193.3.15.1 0.0.0.7 eq
isakmp 183.3.15.1 0.0.0.7 log
access-list 104 deny ip any any log
access-list 108 permit gre 193.3.15.1 0.0.0.7
184.3.15.1 0.0.0.7 log
access-list 108 permit udp 193.3.15.1 0.0.0.7 eq
isakmp 184.3.15.1 0.0.0.7 log

```

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

```

router eigrp 1
network 193.3.15.0 0.0.0.7
network 77.77.77.0 0.0.0.255
no auto-summary
exit
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
lifetime 86000
exit
crypto isakmp key R1R7 address 183.3.15.1
crypto isakmp key R2R7 address 184.3.15.1
crypto isakmp key R3R7 address 188.3.15.1
crypto isakmp key R6R7 address 190.3.15.2
crypto isakmp key R7R8 address 194.3.15.1

```

```

access-list 108 deny ip any any log
access-list 111 permit gre 193.3.15.1 0.0.0.7
188.3.15.1 0.0.0.3 log
access-list 111 permit udp 193.3.15.1 0.0.0.7 eq
isakmp 188.3.15.1 0.0.0.3 log
access-list 111 deny ip any any log
access-list 113 permit gre 193.3.15.1 0.0.0.7
190.3.15.2 0.0.0.3 log
access-list 113 permit udp 193.3.15.1 0.0.0.7 eq
isakmp 190.3.15.2 0.0.0.3 log
access-list 113 deny ip any any log
access-list 115 permit gre 193.3.15.1 0.0.0.7
194.3.15.1 0.0.0.7 log
access-list 115 permit udp 193.3.15.1 0.0.0.7 eq
isakmp 194.3.15.1 0.0.0.7 log
access-list 115 deny ip any any log

```

Лістинг налаштування маршрутизатора R8:

```

enable
configure terminal
hostname R_8
interface fa 0/0
description LINK_TO_LAN_R
ip address 194.3.15.1 255.255.255.248
no shutdown
exit
interface fa 0/1
description LINK_TO_LAN_S
ip address 195.3.15.1 255.255.255.240
no shutdown
exit
interface loopback 88
ip address 88.88.88.88 255.255.255.0
exit
interface Tunnel18

```

```

crypto map MAP 18 ipsec-isakmp
description IPSEC to 183.3.15.1
set peer 183.3.15.1
set transform-set TRANSF
match address 105
exit
crypto map MAP 28 ipsec-isakmp
description IPSEC to 184.3.15.1
set peer 184.3.15.1
set transform-set TRANSF
match address 109
exit
crypto map MAP 38 ipsec-isakmp
description IPSEC to 188.3.15.1
set peer 188.3.15.1
set transform-set TRANSF
match address 112

```

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip mtu 1400
ip tcp adjust-mss 1360
ip address 105.3.15.2 255.255.255.0
tunnel source 194.3.15.1
tunnel destination 183.3.15.1
exit
interface Tunnel28
ip mtu 1400
ip tcp adjust-mss 1360
ip address 109.3.15.2 255.255.255.0
tunnel source 194.3.15.1
tunnel destination 184.3.15.1
exit
interface Tunnel38
ip mtu 1400
ip tcp adjust-mss 1360
ip address 112.3.15.2 255.255.255.0
tunnel source 194.3.15.1
tunnel destination 188.3.15.1
exit
interface Tunnel68
ip mtu 1400
ip tcp adjust-mss 1360
ip address 114.3.15.2 255.255.255.0
tunnel source 194.3.15.1
tunnel destination 190.3.15.2
exit
interface Tunnel78
ip mtu 1400
ip tcp adjust-mss 1360
ip address 115.3.15.2 255.255.255.0
tunnel source 194.3.15.1
tunnel destination 193.3.15.1
exit

```

```

exit
crypto map MAP 68 ipsec-isakmp
description IPSEC to 190.3.15.2
set peer 190.3.15.2
set transform-set TRANSF
match address 114
exit
crypto map MAP 78 ipsec-isakmp
description IPSEC to 193.3.15.1
set peer 193.3.15.1
set transform-set TRANSF
match address 115
exit
interface fa 0/0
crypto map MAP
exit
username adminr8 privilege 15 secret admin
username userr8 privilege 1 secret user
enable secret admin
ip domain-name mynet.net
crypto key generate rsa general-keys modulus
1024
ip ssh version 2
ip ssh time-out 30
ip ssh authentication-retries 5
ip ssh maxstartups 4
line vty 0 4
login local
transport input ssh
transport output ssh
logging synchronous
exit
access-list 105 permit gre 194.3.15.1 0.0.0.7
183.3.15.1 0.0.0.7 log

```

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				93
Змн.	Арк.	№ докум.	Підпис	Дата		

```

router ospf 1
network 105.3.15.0 0.0.0.255 area 0
network 109.3.15.0 0.0.0.255 area 0
network 112.3.15.0 0.0.0.255 area 0
network 114.3.15.0 0.0.0.255 area 0
network 115.3.15.0 0.0.0.255 area 0
network 195.3.15.0 0.0.0.15 area 1
exit
router eigrp 1
network 194.3.15.0 0.0.0.7
network 88.88.88.0 0.0.0.255
no auto-summary
exit
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
lifetime 86000
exit
crypto isakmp key R1R8 address 183.3.15.1
crypto isakmp key R2R8 address 184.3.15.1
crypto isakmp key R3R8 address 188.3.15.1
crypto isakmp key R6R8 address 190.3.15.2
crypto isakmp key R7R8 address 193.3.15.1
crypto ipsec transform-set TRANSF esp-aes 256

```

```

access-list 105 permit udp 194.3.15.1 0.0.0.7 eq
isakmp 183.3.15.1 0.0.0.7 log
access-list 105 deny ip any any log
access-list 109 permit gre 194.3.15.1 0.0.0.7
184.3.15.1 0.0.0.7 log
access-list 109 permit udp 194.3.15.1 0.0.0.7 eq
isakmp 184.3.15.1 0.0.0.7 log
access-list 109 deny ip any any log
access-list 112 permit gre 194.3.15.1 0.0.0.7
188.3.15.1 0.0.0.3 log
access-list 112 permit udp 194.3.15.1 0.0.0.7 eq
isakmp 188.3.15.1 0.0.0.3 log
access-list 112 deny ip any any log
access-list 114 permit gre 194.3.15.1 0.0.0.7
190.3.15.2 0.0.0.3 log
access-list 114 permit udp 194.3.15.1 0.0.0.7 eq
isakmp 190.3.15.2 0.0.0.3 log
access-list 114 deny ip any any log
access-list 115 permit gre 194.3.15.1 0.0.0.7
193.3.15.1 0.0.0.3 log
access-list 115 permit udp 194.3.15.1 0.0.0.7 eq
isakmp 193.3.15.1 0.0.0.3 log
access-list 115 deny ip any any log

```

Переходимо до налаштування рівня ядра. Рівень ядра складається з 2 маршрутизаторів: R4, R5, з'єднаних між собою за допомогою мідного прямогооточного кабелю (copper straight-through cable). Розглянемо лістинг налаштування маршрутизатора R4:

```

enable
configure terminal
hostname R_4
interface fa 0/0

```

```

interface fa 3/3
description LINK_TO_LAN_R
no switchport
ip address 194.3.15.3 255.255.255.248

```

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				94
Змн.	Арк.	№ докум.	Підпис	Дата		

```

description LINK_TO_LAN_C
ip address 183.3.15.2 255.255.255.248
no shutdown
exit
interface fa 0/1
description LINK_TO_LAN_K
ip address 189.3.15.1 255.255.255.252
no shutdown
exit
interface fa 1/0
description LINK_TO_LAN_P
ip address 193.3.15.2 255.255.255.248
no shutdown
exit
interface fa 3/1
description LINK_TO_LAN_H
no switchport
ip address 188.3.15.2 255.255.255.252
no shutdown
exit
interface fa 3/0
description LINK_TO_LAN_D
no switchport
ip address 184.3.15.3 255.255.255.248
no shutdown
exit

no shutdown
exit
router eigrp 1
network 183.3.15.0 0.0.0.7
network 189.3.15.0 0.0.0.3
network 193.3.15.0 0.0.0.7
network 188.3.15.0 0.0.0.3
network 184.3.15.0 0.0.0.7
network 194.3.15.0 0.0.0.7
no auto-summary
exit
username adminr4 privilege 15 secret admin
username userr4 privilege 1 secret user
enable secret admin
ip domain-name mynet.net
crypto key generate rsa general-keys modulus
1280
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh maxstartups 4
line vty 0 4
login local
transport input ssh
transport output ssh
logging synchronous
exit

```

Лістинг налаштування маршрутизатора R5:

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

```

enable
configure terminal
hostname R_5
interface fa 0/0
description LINK_TO_LAN_D
ip address 184.3.15.2 255.255.255.248
no shutdown
exit
interface fa 0/1
description LINK_TO_LAN_K
ip address 189.3.15.2 255.255.255.252
no shutdown
exit
interface fa 1/0
description LINK_TO_LAN_R
ip address 194.3.15.2 255.255.255.248
no shutdown
exit
interface fa 3/1
description LINK_TO_LAN_L
no switchport
ip address 190.3.15.1 255.255.255.252
no shutdown
exit
interface fa 3/0
description LINK_TO_LAN_C
no switchport
ip address 183.3.15.3 255.255.255.248
no shutdown
exit
interface fa 3/3
description LINK_TO_LAN_P
no switchport
ip address 193.3.15.3 255.255.255.248
no shutdown
exit
router eigrp 1
network 183.3.15.0 0.0.0.7
network 184.3.15.0 0.0.0.7
network 189.3.15.0 0.0.0.3
network 194.3.15.0 0.0.0.7
network 193.3.15.0 0.0.0.7
network 190.3.15.0 0.0.0.3
no auto-summary
exit
username adminr5 privilege 15 secret admin
username userr5 privilege 1 secret user
enable secret admin
ip domain-name mynet.net
crypto key generate rsa general-keys modulus
1024
ip ssh version 2
ip ssh time-out 30
ip ssh authentication-retries 3
ip ssh maxstartups 5
line vty 0 4
login local
transport input ssh
transport output ssh
logging synchronous
exit

```

Рівень доступу представлений кінцевим устаткуванням користувачів та комутаційним обладнанням, що забезпечує функціонування цього рівня. Рівень доступу складається з 8 комутаторів: SW1, SW2, SW3, SW4, SW7, SW8, SW11,

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				96
Змн.	Арк.	№ докум.	Підпис	Дата		

SW12. Налаштування робочих станцій та серверів полягає в ручному присвоєнні IP адреси ipv4. Список використаних адрес наведено в таблиці 2.2.

3.4. Налаштування та встановлення Active Directory із роллю первинного контролера домену на першому сервері.

Для того, щоб відновити роботу мережевого оточення, потрібно включити 4 служби:

- DNS-клієнт (DNS Client);
- Виявлення SSDP (SSDP Discovery);
- Публікація ресурсів виявлення функції (Function Discovery Resource Publication);
- Вузол універсальних PNP-пристроїв (UPnP Device Host).

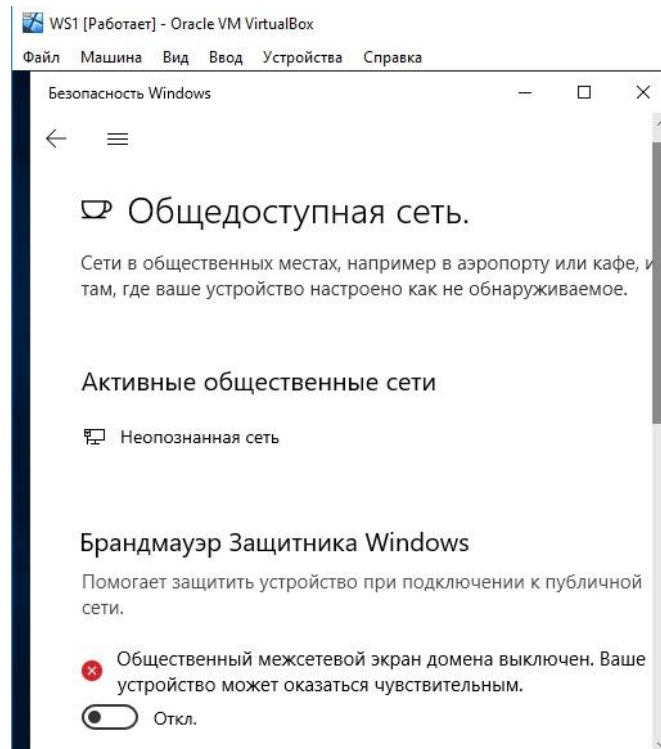


Рис. 3.4. Процес відключення брандмауєра на робочій станції WS1

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				97
Змн.	Арк.	№ докум.	Підпис	Дата		

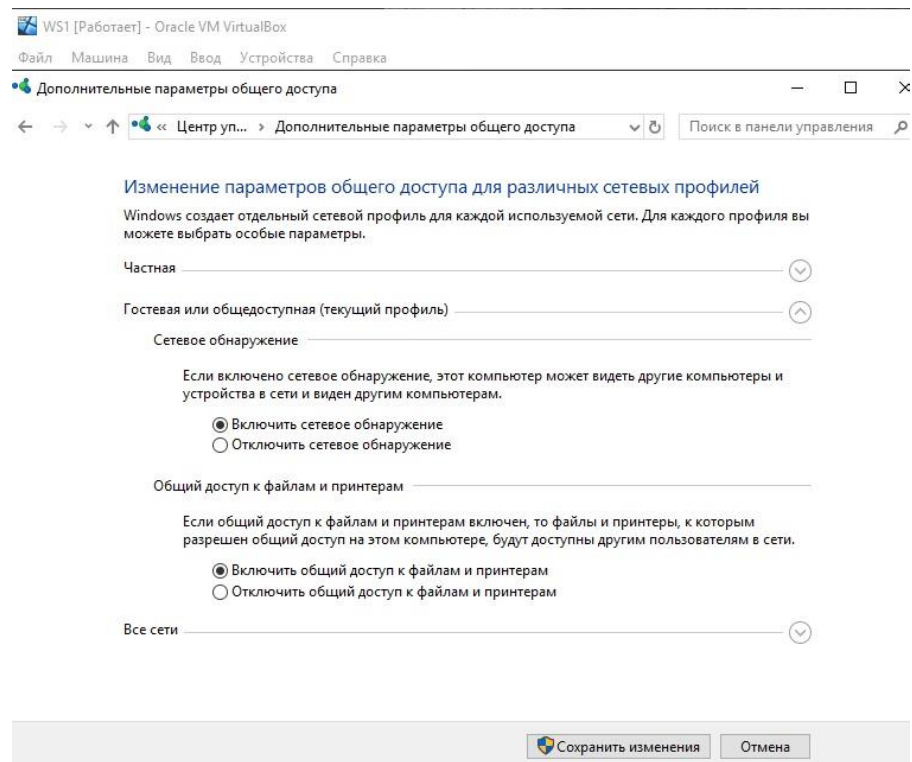


Рис. 3.5. Вмикання видимості машини WS1 в мережевому оточенні

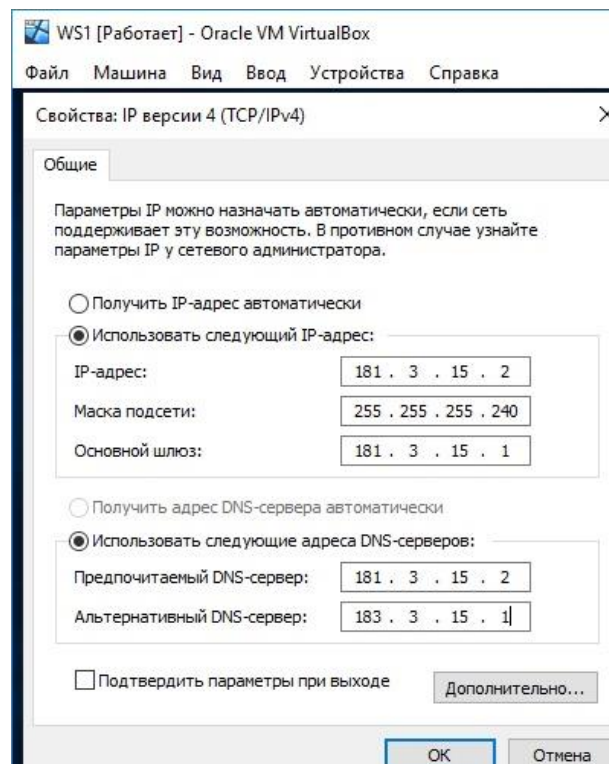


Рис. 3.6. Процес налаштування параметрів адресації сервера WS1

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				98
Змн.	Арк.	№ докум.	Підпис	Дата		

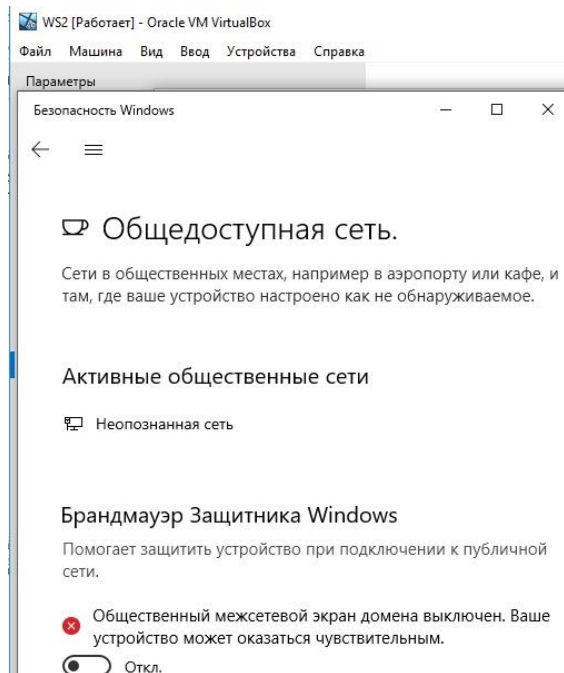


Рис. 3.7. Процес відключення брандмауєра на робочій станції WS2

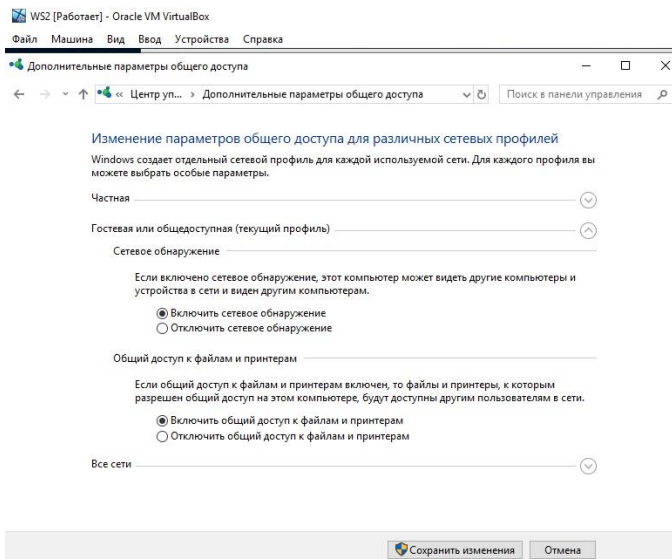


Рис. 3.8. Вмикання видимості машини WS2 в мережевому оточенні

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				99
Змн.	Арк.	№ докум.	Підпис	Дата		

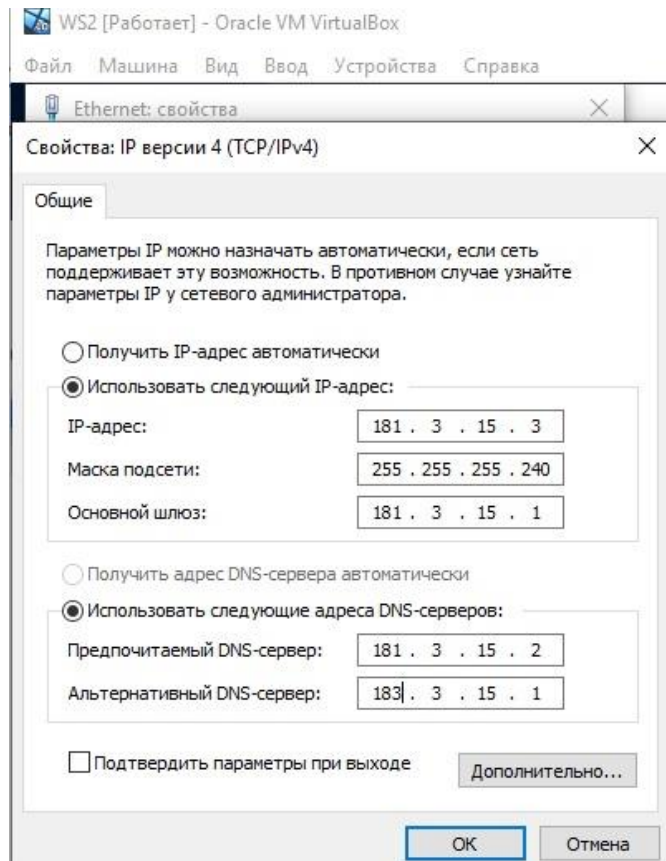


Рис. 3.9. Процес налаштування параметрів адресації машини WS2

Після налаштування параметрів адресації робочих станцій та сервера, переходимо до встановлення Active Directory із роллю первинного контролера домену на першому сервері та проводимо налагодження домену host_Okhrimenko.local на ньому. Для цього на сервері (WS1) переходимо в додатку «Диспетчер серверів» та на панелі в меню «Управління» обираємо пункт «Додати ролі і компоненти».

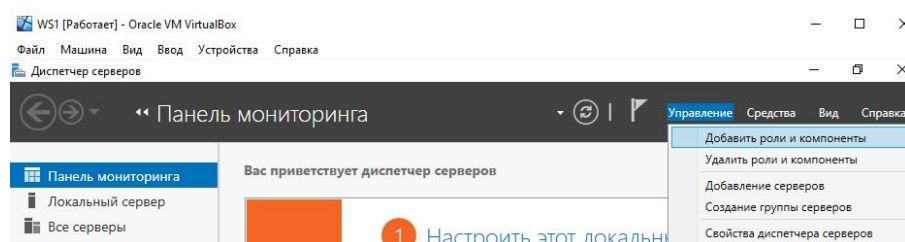


Рис. 3.10. Процес додавання необхідних компонентів

Додамо на даний сервер ролі: Active Directory, файловий сервер та компоненти «Файлових служб та служб iSCSI», NET Framework, менеджер групових політик. Підвищуємо роль даного сервера до рівня контролера домена. Додамо новий ліс (host_Okhrimenko.local). Встановимо пароль.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				100
Змн.	Арк.	№ докум.	Підпис	Дата		

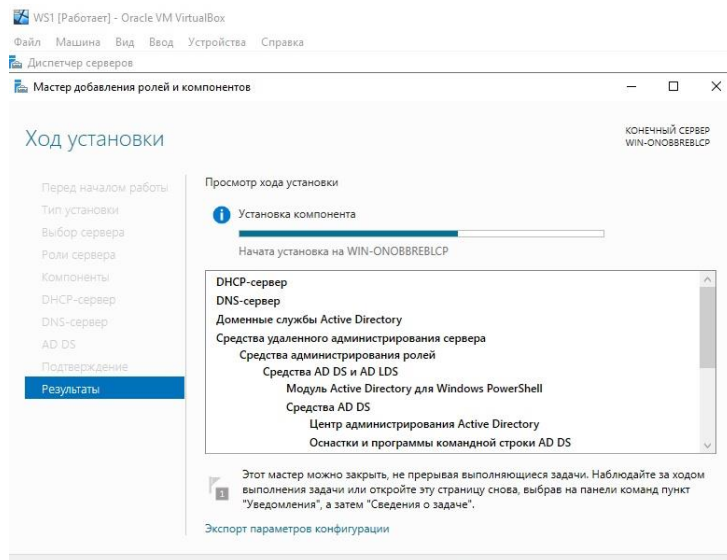


Рис. 3.11. Процес встановлення необхідних компонентів

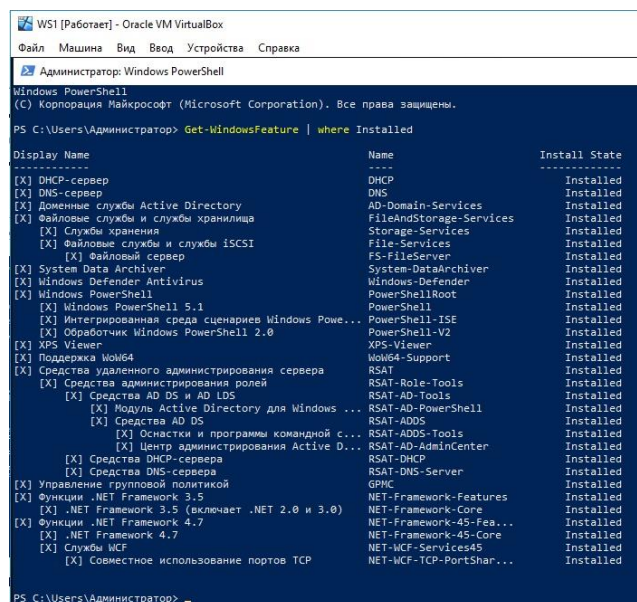


Рис. 3.12. Виведення встановлених компонентів

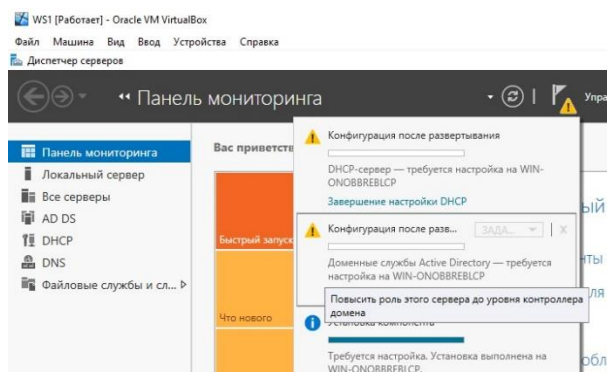


Рис. 3.13. Підвищення ролі даного сервера до рівня контролера домена

		Охріменко. Д.С.			Арк.
		Єфіменко А.А.			101
Змн.	Арк.	№ докум.	Підпис	Дата	Житомирська політехника 21.123.15.000

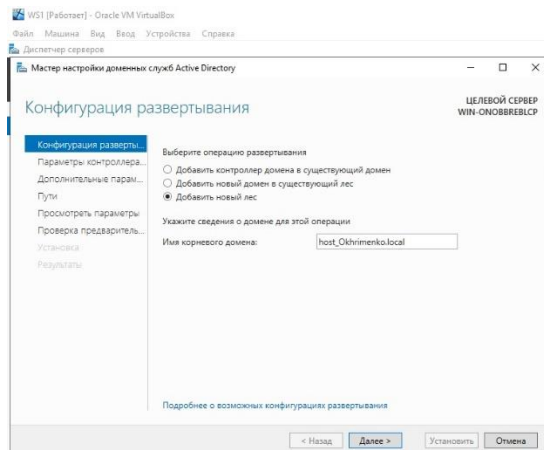


Рис. 3.14. Майстер налаштування доменних служб Active Directory

Додамо 2 користувача з різними правами доступу в службі AD. Для цього використаємо оснащення Active Directory - користувачі і комп'ютери яке призначене для управління користувачами, групами, чергами друку та іншими об'єктами каталогу Active Directory. На сервері в Active Directory створюємо групу, та додамо створеного користувача до цієї групи.

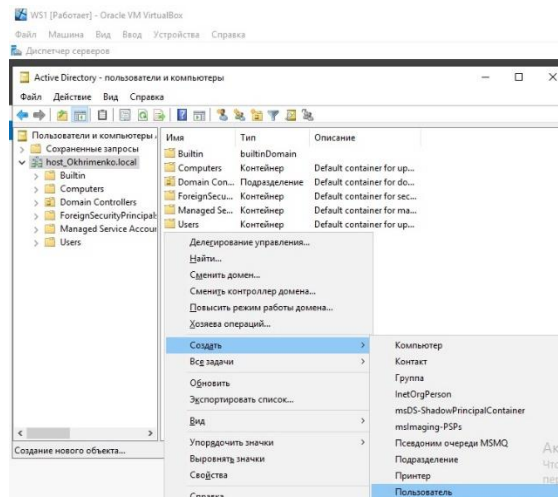


Рис. 3.15. Процес створення нового користувача

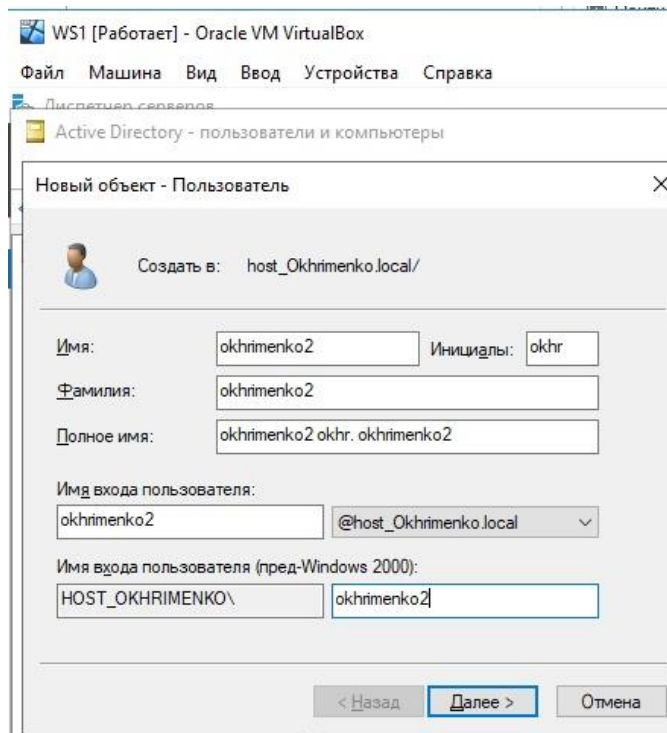


Рис. 3.16. Процес створення першого користувача

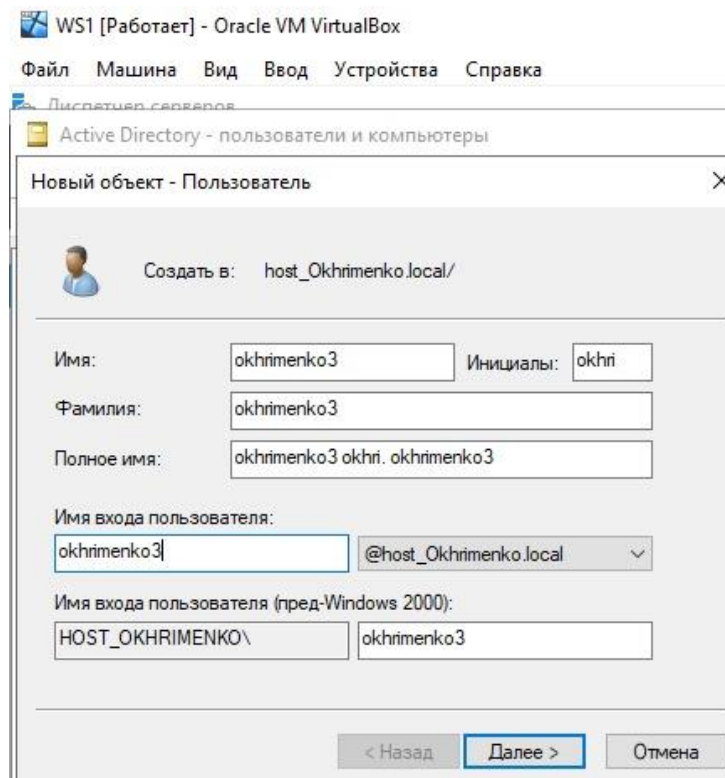


Рис. 3.17. Процес створення другого користувача

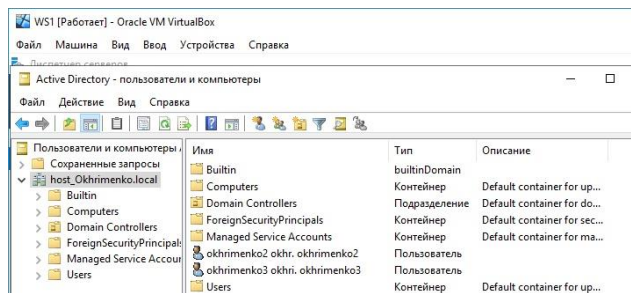


Рис. 3.18. Результат створення двох користувачів

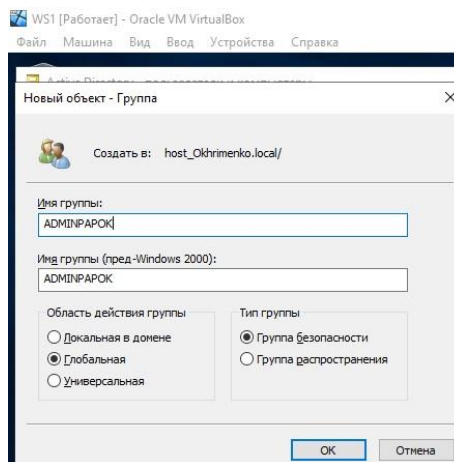


Рис. 3.19. Процесс створення групи для першого користувача

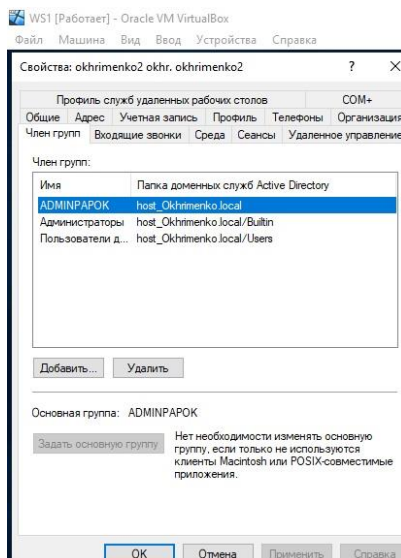


Рис. 3.20. Результат додавання першого користувача до створеної групи

Приєднуємо до доменної інфраструктури клієнтську робочу станцію WS2 (Windows 10). Створюємо на сервері спільний ресурс (Info) та надамо до нього доступ користувачам і відповідні права для доступу до підпапок даного ресурсу.

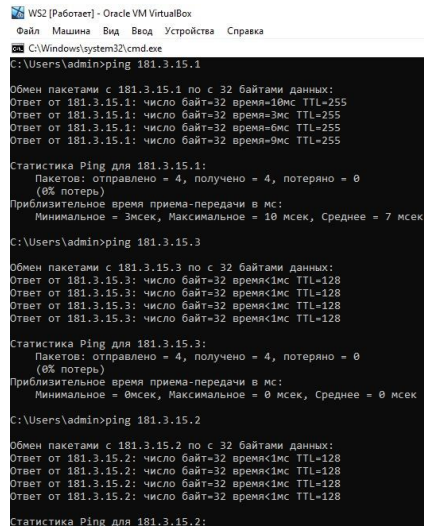


Рис. 3.21. Проверка наявності зв'язку з сервером на робочій станції WS2

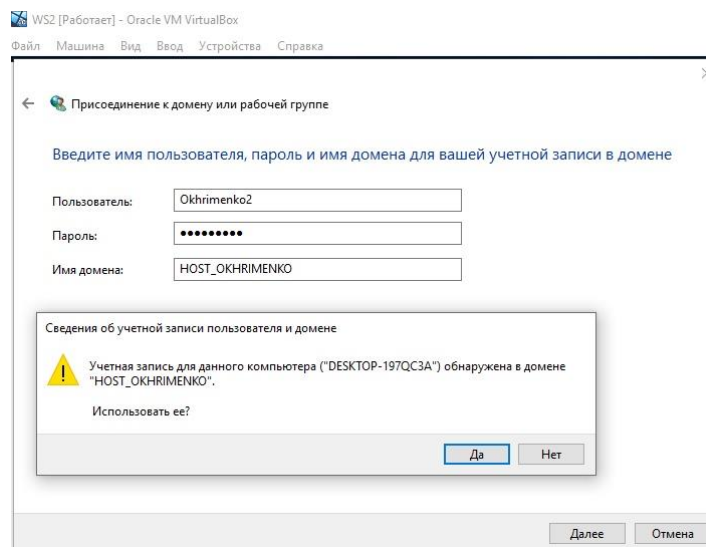


Рис. 3.22. Процес введення необхідних даних для підключення

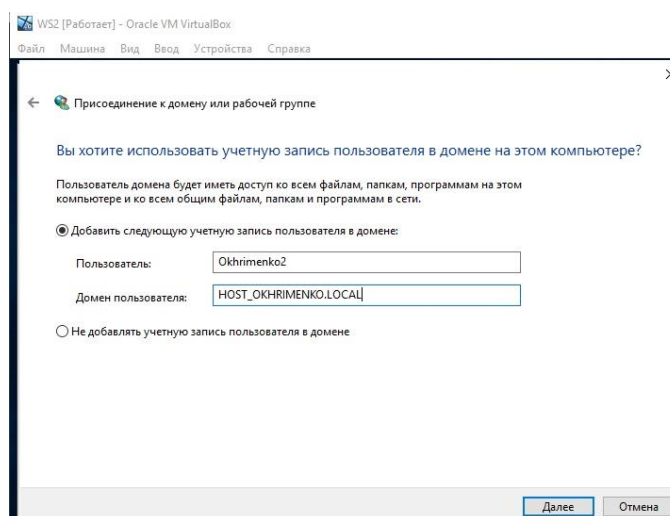


Рис. 3.23. Процес введення необхідних даних для підключення

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		105

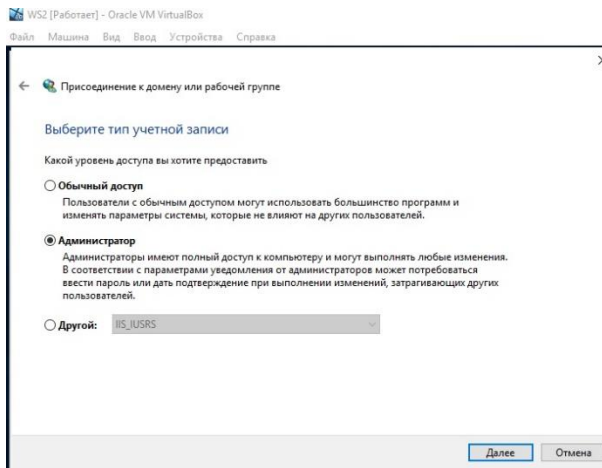


Рис. 3.24. Вікно майстра підключення до домену

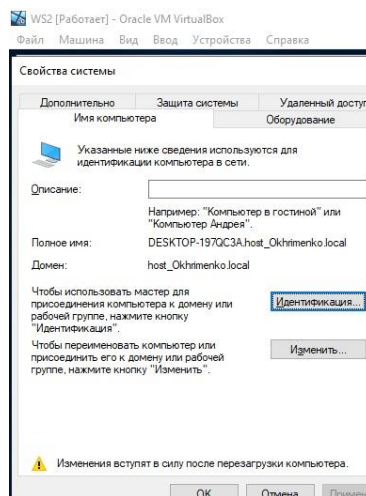


Рис. 3.25. Результат приєднання до доменної інфраструктури робочої станції
WS2

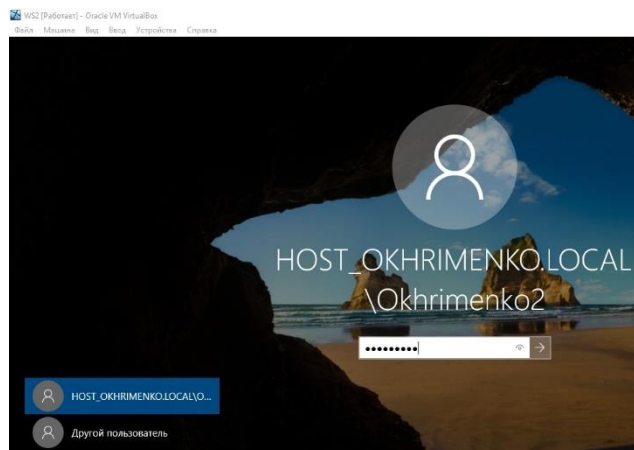


Рис. 3.26. Підключення до серверу за допомогою логіну створеного користувача

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				106
Змн.	Арк.	№ докум.	Підпис	Дата		

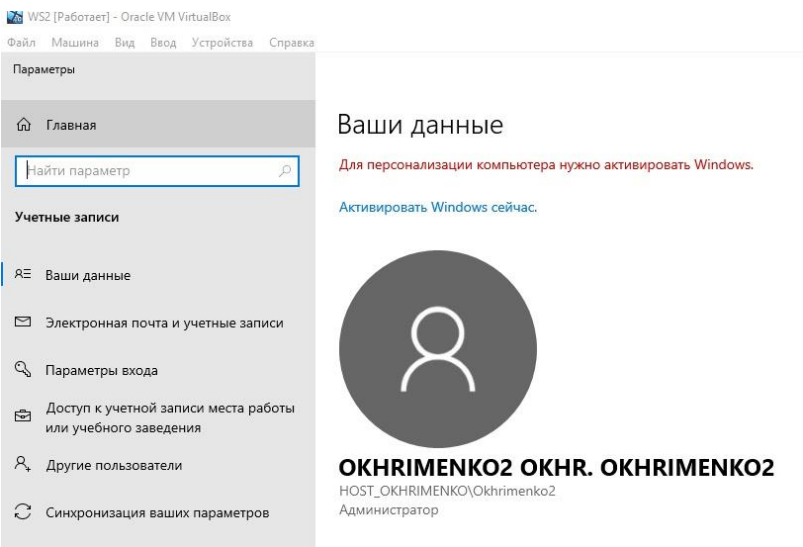


Рис. 3.27. Перевірка облікового запису користувача

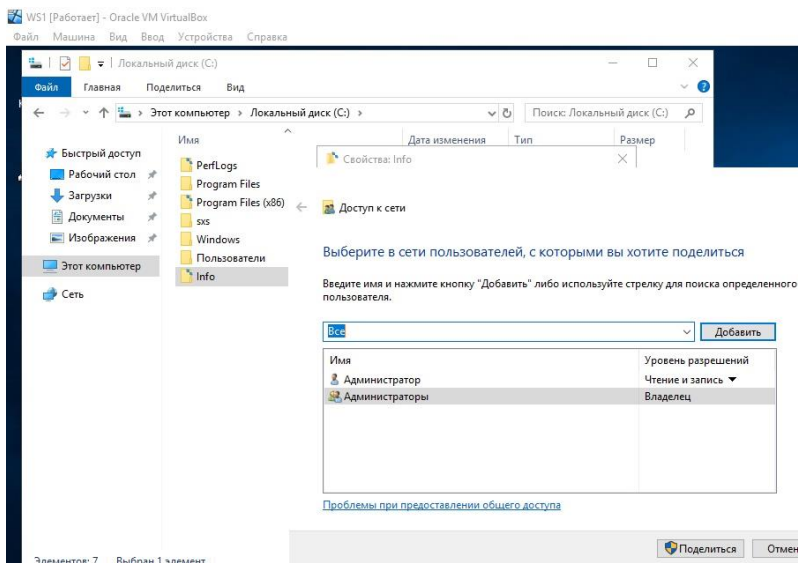


Рис. 3.28. Створення необхідної папки та надання до неї доступу

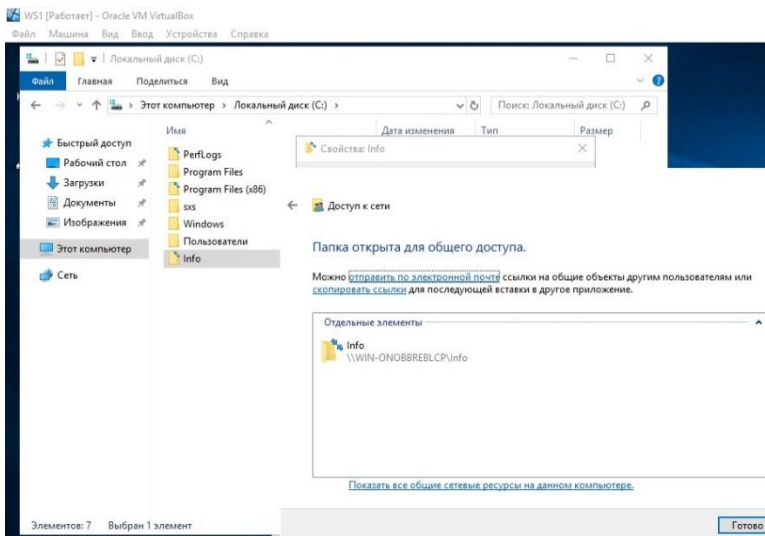


Рис. 3.29. Результат відкриття доступу до створеної папки

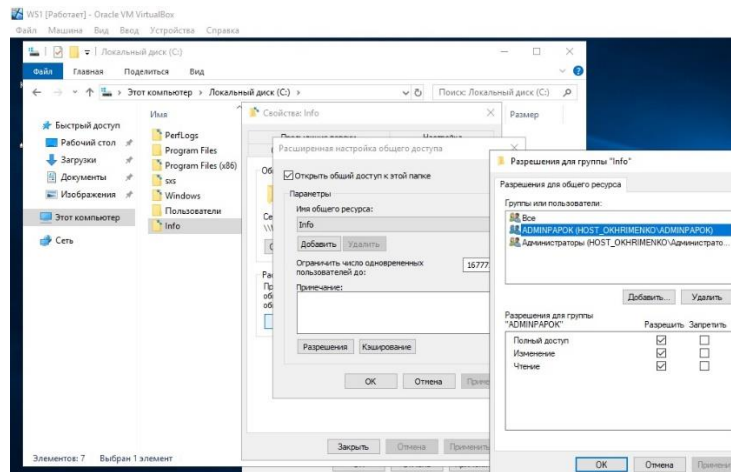


Рис. 3.30. Результат надання прав адміністратору

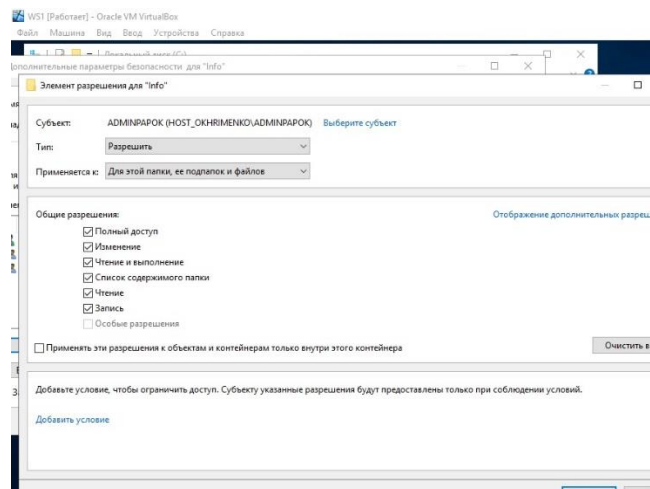


Рис. 3.31. Надання спільного доступу до каталогу

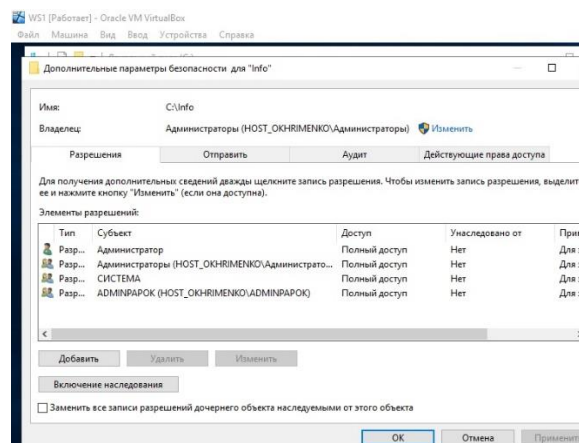


Рис. 3.32. Результат надання спільного доступу до каталогу

3.5. Перевірка працездатності мережі.

Для початку необхідно перевірити наявність зв'язку між кінцевими пристроями які належать до однієї зони OSPF 1. Це можна здійснити за допомогою

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				108
Змн.	Арк.	№ докум.	Підпис	Дата		

команд ping та tracert, рис 3.33, рис 3.34; рис 3.35, рис 3.36, рис 3.37, рис 3.38 та рис 3.39;

```

WS1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Администратор: C:\Windows\system32\cmd.exe
C:\Users\Администратор>ping 181.3.15.3

Обмен пакетами с 181.3.15.3 по 32 байтами данных:
Ответ от 181.3.15.3: число байт=32 время=1мс TTL=128
Ответ от 181.3.15.3: число байт=32 время=1мс TTL=128
Ответ от 181.3.15.3: число байт=32 время=1мс TTL=128
Ответ от 181.3.15.3: число байт=32 время=1мс TTL=128

Статистика Ping для 181.3.15.3:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потеря)
Приблизительное время приема-передачи в мс:
  Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек

C:\Users\Администратор>ping 182.3.15.2

Обмен пакетами с 182.3.15.2 по 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 182.3.15.2: число байт=32 время=21мс TTL=63
Ответ от 182.3.15.2: число байт=32 время=17мс TTL=63
Ответ от 182.3.15.2: число байт=32 время=17мс TTL=63

Статистика Ping для 182.3.15.2:
  Пакетов: отправлено = 4, получено = 3, потеряно = 1
  (25% потеря)
Приблизительное время приема-передачи в мс:
  Минимальное = 17мсек, Максимальное = 21 мсек, Среднее = 18 мсек

C:\Users\Администратор>ping 185.3.15.2

Обмен пакетами с 185.3.15.2 по 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 185.3.15.2: число байт=32 время=58мс TTL=62
Ответ от 185.3.15.2: число байт=32 время=54мс TTL=62
Ответ от 185.3.15.2: число байт=32 время=62мс TTL=62

Статистика Ping для 185.3.15.2:
  Пакетов: отправлено = 4, получено = 3, потеряно = 1
  (25% потеря)
  
```

Рис 3.33. Перевірка наявності зв'язку між кінцевими пристроями інших підмереж за допомогою команди ping

```

WS1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Администратор: C:\Windows\system32\cmd.exe
C:\Users\Администратор>ping 186.3.15.3

Обмен пакетами с 186.3.15.3 по 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 186.3.15.3: число байт=32 время=62мс TTL=62
Ответ от 186.3.15.3: число байт=32 время=55мс TTL=62
Ответ от 186.3.15.3: число байт=32 время=62мс TTL=62

Статистика Ping для 186.3.15.3:
  Пакетов: отправлено = 4, получено = 3, потеряно = 1
  (25% потеря)
Приблизительное время приема-передачи в мс:
  Минимальное = 55мсек, Максимальное = 62 мсек, Среднее = 59 мсек

C:\Users\Администратор>ping 187.3.15.3

Обмен пакетами с 187.3.15.3 по 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 187.3.15.3: число байт=32 время=53мс TTL=62
Ответ от 187.3.15.3: число байт=32 время=50мс TTL=62
Ответ от 187.3.15.3: число байт=32 время=47мс TTL=62

Статистика Ping для 187.3.15.3:
  Пакетов: отправлено = 4, получено = 3, потеряно = 1
  (25% потеря)
Приблизительное время приема-передачи в мс:
  Минимальное = 47мсек, Максимальное = 53 мсек, Среднее = 50 мсек

C:\Users\Администратор>ping 191.3.15.3

Обмен пакетами с 191.3.15.3 по 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 191.3.15.3: число байт=32 время=60мс TTL=62
Ответ от 191.3.15.3: число байт=32 время=55мс TTL=62
Ответ от 191.3.15.3: число байт=32 время=62мс TTL=62

Статистика Ping для 191.3.15.3:
  Пакетов: отправлено = 4, получено = 3, потеряно = 1
  (25% потеря)
  
```

Рис 3.34. Перевірка наявності зв'язку між кінцевими пристроями інших підмереж за допомогою команди ping

```

WS1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Администратор: C:\Windows\system32\cmd.exe

C:\Users\Администратор>ping 192.3.15.3

Обмен пакетами с 192.3.15.3 по с 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 192.3.15.3: число байт=32 время=47мс TTL=62
Ответ от 192.3.15.3: число байт=32 время=44мс TTL=62
Ответ от 192.3.15.3: число байт=32 время=63мс TTL=62

Статистика Ping для 192.3.15.3:
    Пакетов: отправлено = 4, получено = 3, потеряно = 1
    (25% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 44мсек, Максимальное = 63 мсек, Среднее = 51 мсек

C:\Users\Администратор>ping 195.3.15.3

Обмен пакетами с 195.3.15.3 по с 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 195.3.15.3: число байт=32 время=59мс TTL=62
Ответ от 195.3.15.3: число байт=32 время=64мс TTL=62
Ответ от 195.3.15.3: число байт=32 время=61мс TTL=62

Статистика Ping для 195.3.15.3:
    Пакетов: отправлено = 4, получено = 3, потеряно = 1
    (25% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 59мсек, Максимальное = 64 мсек, Среднее = 61 мсек

C:\Users\Администратор>

```

Рис 3.35. Перевірка наявності зв'язку між кінцевими пристроями інших підмереж за допомогою команди ping

```

WS1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Администратор: C:\Windows\system32\cmd.exe

C:\Users\Администратор>tracert 182.3.15.2

Трассировка маршрута к 182.3.15.2 с максимальным числом прыжков 30

  1    5 ms    9 ms    10 ms  181.3.15.1
  2   3005 ms   20 ms   20 ms  182.3.15.2

Трассировка завершена.

C:\Users\Администратор>tracert 185.3.15.3

Трассировка маршрута к 185.3.15.3 с максимальным числом прыжков 30

  1    4 ms    9 ms    9 ms  181.3.15.1
  2   50 ms   52 ms   61 ms  101.3.15.2
  3   51 ms    *    48 ms  101.3.15.2
  4    *    58 ms   62 ms  185.3.15.3

Трассировка завершена.

C:\Users\Администратор>tracert 186.3.15.3

Трассировка маршрута к 186.3.15.3 с максимальным числом прыжков 30

  1    4 ms    8 ms    9 ms  181.3.15.1
  2   53 ms   51 ms   52 ms  101.3.15.2
  3  3064 ms   62 ms   59 ms  186.3.15.3

Трассировка завершена.

C:\Users\Администратор>tracert 187.3.15.3

Трассировка маршрута к 187.3.15.3 с максимальным числом прыжков 30

  1    9 ms    9 ms    8 ms  181.3.15.1
  2   44 ms   51 ms   51 ms  102.3.15.2
  3  3066 ms   62 ms   63 ms  187.3.15.3

Трассировка завершена.

```

Рис 3.36. Перевірка наявності зв'язку між кінцевими пристроями інших підмереж за допомогою команди tracert

```

WS1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Администратор: C:\Windows\system32\cmd.exe

C:\Users\Администратор>tracert 191.3.15.3

Трассировка маршрута к 191.3.15.3 с максимальным числом прыжков 30

  1    10 ms    9 ms    9 ms    181.3.15.1
  2    54 ms   51 ms   52 ms   103.3.15.2
  3   3059 ms   63 ms   62 ms   191.3.15.3

Трассировка завершена.

C:\Users\Администратор>tracert 192.3.15.3

Трассировка маршрута к 192.3.15.3 с максимальным числом прыжков 30

  1     8 ms    9 ms    9 ms    181.3.15.1
  2    54 ms   52 ms   51 ms   104.3.15.2
  3   3053 ms   61 ms   63 ms   192.3.15.3

Трассировка завершена.

C:\Users\Администратор>tracert 195.3.15.3

Трассировка маршрута к 195.3.15.3 с максимальным числом прыжков 30

  1     7 ms    9 ms    8 ms    181.3.15.1
  2    45 ms   52 ms   52 ms   105.3.15.2
  3   3051 ms   51 ms   52 ms   195.3.15.3

Трассировка завершена.

C:\Users\Администратор>

```

Рис 3.37. Перевірка наявності зв'язку між кінцевими пристроями інших підмереж за допомогою команди tracert

```

WS24 - PuTTY

WS24> trace 181.3.15.2 -P 6
trace to 181.3.15.2, 8 hops max (TCP), press Ctrl+C to stop
  1  195.3.15.1  6.890 ms  8.720 ms  10.055 ms
  2  105.3.15.1  52.197 ms  51.509 ms  53.122 ms
  3  181.3.15.2  65.547 ms  59.303 ms  62.995 ms

WS24> trace 182.3.15.2 -P 6
trace to 182.3.15.2, 8 hops max (TCP), press Ctrl+C to stop
  1  195.3.15.1  7.362 ms  9.990 ms  8.503 ms
  2  105.3.15.1  51.876 ms  53.386 ms  53.238 ms
  3  * * *
  4  182.3.15.2  65.060 ms  4294965.659 ms  4294963.753 ms

WS24> trace 185.3.15.2 -P 6
trace to 185.3.15.2, 8 hops max (TCP), press Ctrl+C to stop
  1  195.3.15.1  7.132 ms  9.985 ms  9.042 ms
  2  109.3.15.1  52.671 ms  51.884 ms  51.191 ms
  3  * * *
  4  185.3.15.2  64.043 ms  4294966.602 ms  4294964.745 ms

WS24> trace 186.3.15.3 -P 6
trace to 186.3.15.3, 8 hops max (TCP), press Ctrl+C to stop
  1  195.3.15.1  8.459 ms  8.718 ms  8.780 ms
  2  109.3.15.1  53.158 ms  52.477 ms  53.240 ms
  3  * * *
  4  186.3.15.3  62.240 ms  4294965.650 ms  4294963.739 ms

WS24> trace 187.3.15.3 -P 6
trace to 187.3.15.3, 8 hops max (TCP), press Ctrl+C to stop
  1  195.3.15.1  7.110 ms  9.567 ms  9.840 ms
  2  112.3.15.1  53.583 ms  51.477 ms  53.059 ms
  3  * * *
  4  187.3.15.3  53.326 ms  9.831 ms  9.067 ms

WS24> trace 191.3.15.3 -P 6
trace to 191.3.15.3, 8 hops max (TCP), press Ctrl+C to stop
  1  195.3.15.1  4.092 ms  9.017 ms  10.019 ms
  2  114.3.15.1  51.486 ms  53.105 ms  51.582 ms
  3  * * *
  4  191.3.15.3  63.863 ms  10.004 ms  8.967 ms

```

Рис 3.38. Перевірка наявності зв'язку між кінцевими пристроями інших підмереж за допомогою команди trace

```

WS24> trace 192.3.15.3 -P 6
Trace to 192.3.15.3, 8 hops max (TCP), press Ctrl+C to stop
 1  195.3.15.1    2.176 ms  8.952 ms  10.014 ms
 2  115.3.15.1   51.684 ms  51.939 ms  52.297 ms
 3  * * *
 4  192.3.15.3   63.848 ms  4294966.706 ms  4294964.647 ms
WS24>

```

Рис 3.39. Перевірка наявності зв'язку між кінцевими пристроями інших підмереж за допомогою команди trace

Почнемо виконувати перевірку працездатності протоколу тунелювання GRE. Для цього виконаємо команду show ip interface tunnel на маршрутизаторах R1, R2, R3, R6, R7 та R8.

```

R_1#show ip interface tunnel 12
Tunnel12 is up, line protocol is up
  Internet address is 101.3.15.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1400 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
R_1#

```

Рис. 3.40. Результат виконання діагностичної команди show ip interface tunnel 12 на маршрутизаторі R1

```

R1
R_1#show ip interface tunnel 13
Tunnel13 is up, line protocol is up
Internet address is 102.3.15.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1400 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.5
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF Feature Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
R_1#

```

Рис. 3.41. Результат виконання діагностичної команди show ip interface tunnel 13 на маршрутизаторі R1

```

R1
R_1#show ip interface tunnel 16
Tunnel16 is up, line protocol is up
Internet address is 103.3.15.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1400 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.5
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF Feature Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
R_1#

```

Рис. 3.42. Результат виконання діагностичної команди show ip interface tunnel 16 на маршрутизаторі R1

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				113
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R1
R_1#show ip interface tunnel 17
Tunnel17 is up, line protocol is up
  Internet address is 104.3.15.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1400 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
R_1#

```

Рис. 3.43. Результат виконання діагностичної команди show ip interface tunnel 17 на маршрутизаторі R1

```

R1
R_1#show ip interface tunnel 18
Tunnel18 is up, line protocol is up
  Internet address is 105.3.15.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1400 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
R_1#

```

Рис. 3.44. Результат виконання діагностичної команди show ip interface tunnel 18 на маршрутизаторі R1

		Охріменко. Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				114
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R2
R_2#show ip interface tunnel 23
Tunnel23 is up, line protocol is up
  Internet address is 106.3.15.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1400 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
R_2#

```

Рис. 3.45. Результат виконання діагностичної команди show ip interface tunnel 23 на маршрутизаторі R2

```

R2
R_2#show ip interface tunnel 26
Tunnel26 is up, line protocol is up
  Internet address is 107.3.15.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1400 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
R_2#

```

Рис. 3.46. Результат виконання діагностичної команди show ip interface tunnel 26 на маршрутизаторі R2

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				115
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R2
R_2#show ip interface tunnel 27
Tunnel27 is up, line protocol is up
  Internet address is 108.3.15.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1400 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
R_2#

```

Рис. 3.47. Результат виконання діагностичної команди show ip interface tunnel 27 на маршрутизаторі R2

```

R2
R_2#show ip interface tunnel 28
Tunnel28 is up, line protocol is up
  Internet address is 109.3.15.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1400 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
R_2#

```

Рис. 3.48. Результат виконання діагностичної команди show ip interface tunnel 28 на маршрутизаторі R2

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				116
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R3
R_3#show ip interface tunnel 36
Tunnel36 is up, line protocol is up
Internet address is 110.3.15.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1400 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.5
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF Feature Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
R_3#

```

Рис. 3.49. Результат виконання діагностичної команди show ip interface tunnel 36 на маршрутизаторі R3

```

R3
R_3#show ip interface tunnel 37
Tunnel37 is up, line protocol is up
Internet address is 111.3.15.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1400 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.5
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF Feature Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
R_3#

```

Рис. 3.50. Результат виконання діагностичної команди show ip interface tunnel 37 на маршрутизаторі R3

 R3

```

R_3#show ip interface tunnel 38
Tunnel38 is up, line protocol is up
  Internet address is 112.3.15.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1400 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
R_3#

```

Рис. 3.51. Результат виконання діагностичної команди show ip interface tunnel 38 на маршрутизаторі R3

 R6

```

R_6#show ip interface tunnel 67
Tunnel67 is up, line protocol is up
  Internet address is 113.3.15.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1400 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Feature Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
R_6#

```

Рис. 3.52. Результат виконання діагностичної команди show ip interface tunnel 67 на маршрутизаторі R6

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				118
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R8
R 8#show ip interface tunnel 68
Tunnel68 is up, line protocol is up
Internet address is 114.3.15.2/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1400 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.5
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF Feature Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
R 8#

```

Рис. 3.53. Результат виконання діагностичної команди show ip interface tunnel 68 на маршрутизаторі R8

```

R7
R 7#show ip interface tunnel 78
Tunnel78 is up, line protocol is up
Internet address is 115.3.15.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1400 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.5
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF Feature Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
R 7#

```

Рис. 3.54. Результат виконання діагностичної команди show ip interface tunnel 78 на маршрутизаторі R7

Після успішної відправки ехо-запитів на кінцеві вузли інших підмереж, здійснимо також перевірку працездатності протоколу ipsec. Для цього виконаємо

команди show crypto isakmp sa та show crypto ipsec sa на маршрутизаторах R1 R2, R3, R6; R7 та R8.

```

R1
R_1#show crypto isakmp sa
dst          src          state          conn-id slot status
194.3.15.1   183.3.15.1   QM_IDLE        2      0 ACTIVE
184.3.15.1   183.3.15.1   QM_IDLE        1      0 ACTIVE
183.3.15.1   193.3.15.1   QM_IDLE        3      0 ACTIVE
190.3.15.2   183.3.15.1   QM_IDLE        5      0 ACTIVE
183.3.15.1   188.3.15.1   QM_IDLE        4      0 ACTIVE
R_1#

```

Рис. 3.55. Результат виконання діагностичної команди show crypto isakmp sa на маршрутизаторі R1

```

R2
R_2#show crypto isakmp sa
dst          src          state          conn-id slot status
184.3.15.1   193.3.15.1   QM_IDLE        3      0 ACTIVE
194.3.15.1   184.3.15.1   QM_IDLE        4      0 ACTIVE
184.3.15.1   183.3.15.1   QM_IDLE        2      0 ACTIVE
188.3.15.1   184.3.15.1   QM_IDLE        5      0 ACTIVE
190.3.15.2   184.3.15.1   QM_IDLE        1      0 ACTIVE
R_2#

```

Рис. 3.56. Результат виконання діагностичної команди show crypto isakmp sa на маршрутизаторі R2

```

R3
R_3#show crypto isakmp sa
dst          src          state          conn-id slot status
188.3.15.1   184.3.15.1   QM_IDLE        4      0 ACTIVE
188.3.15.1   193.3.15.1   QM_IDLE        5      0 ACTIVE
190.3.15.2   188.3.15.1   QM_IDLE        3      0 ACTIVE
183.3.15.1   188.3.15.1   QM_IDLE        2      0 ACTIVE
188.3.15.1   194.3.15.1   QM_IDLE        1      0 ACTIVE
R_3#

```

Рис. 3.57. Результат виконання діагностичної команди show crypto isakmp sa на маршрутизаторі R3

```

R6
R_6#show crypto isakmp sa
dst          src          state          conn-id slot status
194.3.15.1   190.3.15.2   QM_IDLE        2      0 ACTIVE
190.3.15.2   183.3.15.1   QM_IDLE        4      0 ACTIVE
190.3.15.2   184.3.15.1   QM_IDLE        1      0 ACTIVE
190.3.15.2   188.3.15.1   QM_IDLE        5      0 ACTIVE
190.3.15.2   193.3.15.1   QM_IDLE        3      0 ACTIVE
R_6#

```

Рис. 3.58. Результат виконання діагностичної команди show crypto isakmp sa на маршрутизаторі R6

```

R7
R_7#show crypto isakmp sa
dst          src          state          conn-id slot status
188.3.15.1   193.3.15.1   QM_IDLE        10     0 ACTIVE
184.3.15.1   193.3.15.1   QM_IDLE        9      0 ACTIVE
183.3.15.1   193.3.15.1   QM_IDLE        7      0 ACTIVE
194.3.15.1   193.3.15.1   QM_IDLE        11     0 ACTIVE
190.3.15.2   193.3.15.1   QM_IDLE        8      0 ACTIVE
R_7#

```

Рис. 3.59. Результат виконання діагностичної команди show crypto isakmp sa на маршрутизаторі R7

```

R8
R_8#show crypto isakmp sa
dst          src          state          conn-id slot status
194.3.15.1   190.3.15.2   QM_IDLE       9            0 ACTIVE
194.3.15.1   193.3.15.1   QM_IDLE       11           0 ACTIVE
194.3.15.1   183.3.15.1   QM_IDLE       7            0 ACTIVE
194.3.15.1   184.3.15.1   QM_IDLE       10           0 ACTIVE
188.3.15.1   194.3.15.1   QM_IDLE       8            0 ACTIVE
R_8#

```

Рис. 3.60. Результат виконання діагностичної команди show crypto isakmp sa на маршрутизаторі R8

```

R1
outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (183.3.15.0/255.255.255.248/47/0)
remote ident (addr/mask/prot/port): (188.3.15.0/255.255.255.252/47/0)
current_peer 188.3.15.1 port 500
  PERMIT, flags=(origin_is_acl,)
#pkts encaps: 14174, #pkts encrypt: 14174, #pkts digest: 14174
#pkts decaps: 14111, #pkts decrypt: 14111, #pkts verify: 14111
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 183.3.15.1, remote crypto endpt.: 188.3.15.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
current outbound spi: 0xC683892C(3464726828)

inbound esp sas:
  spi: 0x481B324(1209381668)
    transform: esp-256-aes ,
    in use settings = (Tunnel, )
    conn id: 2007, flow id: SW:7, crypto map: MAP
    sa timing: remaining key lifetime (k/sec): (4491088/2932)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xC683892C(3464726828)
    transform: esp-256-aes ,
    in use settings = (Tunnel, )
    conn id: 2008, flow id: SW:8, crypto map: MAP
    sa timing: remaining key lifetime (k/sec): (4491088/2926)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

outbound ah sas:

```

Рис. 3.61. Результат виконання діагностичної команди show crypto ipsec sa на маршрутизаторі R1

```

R2
protected vrf: (none)
local ident (addr/mask/prot/port): (184.3.15.0/255.255.255.248/47/0)
remote ident (addr/mask/prot/port): (188.3.15.0/255.255.255.252/47/0)
current_peer 188.3.15.1 port 500
  PERMIT, flags=(origin_is_acl,)
#pkts encaps: 14144, #pkts encrypt: 14144, #pkts digest: 14144
#pkts decaps: 14157, #pkts decrypt: 14157, #pkts verify: 14157
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 184.3.15.1, remote crypto endpt.: 188.3.15.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
current outbound spi: 0x8F21084E(3206613070)

inbound esp sas:
  spi: 0xC683892C(3464726828)
    transform: esp-256-aes ,
    in use settings = (Tunnel, )
    conn id: 2011, flow id: SW:11, crypto map: MAP
    sa timing: remaining key lifetime (k/sec): (4528747/2087)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x8F21084E(3206613070)
    transform: esp-256-aes ,
    in use settings = (Tunnel, )
    conn id: 2012, flow id: SW:12, crypto map: MAP
    sa timing: remaining key lifetime (k/sec): (4528747/2087)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

outbound ah sas:

```

Рис. 3.62. Результат виконання діагностичної команди show crypto ipsec sa на маршрутизаторі R2

```

R3

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (188.3.15.0/255.255.255.252/47/0)
remote ident (addr/mask/prot/port): (193.3.15.0/255.255.255.248/47/0)
current_peer 193.3.15.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 13954, #pkts encrypt: 13954, #pkts digest: 13954
  #pkts decaps: 14142, #pkts decrypt: 14142, #pkts verify: 14142
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 34, #recv errors 0

local crypto endpt.: 188.3.15.1, remote crypto endpt.: 193.3.15.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet3/1
current outbound spi: 0x88CCCFB6(2295123894)

inbound esp sas:
  spi: 0xECAFA4E8(3970933992)
  transform: esp-256-aes ,
  in use settings = {Tunnel, }
  conn id: 2001, flow id: SW:1, crypto map: MAP
  sa timing: remaining key lifetime (k/sec): (4510984/2058)
  IV size: 16 bytes
  replay detection support: N
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x88CCCFB6(2295123894)
  transform: esp-256-aes ,

```

Рис. 3.63. Результат виконання діагностичної команди show crypto ipsec sa на маршрутизаторі R3

```

R6

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (190.3.15.0/255.255.255.252/47/0)
remote ident (addr/mask/prot/port): (184.3.15.0/255.255.255.248/47/0)
current_peer 184.3.15.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 14095, #pkts encrypt: 14095, #pkts digest: 14095
  #pkts decaps: 14163, #pkts decrypt: 14163, #pkts verify: 14163
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

local crypto endpt.: 190.3.15.2, remote crypto endpt.: 184.3.15.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet3/1
current outbound spi: 0x5013B0EE(1343467758)

inbound esp sas:
  spi: 0xD98519B0(3649378736)
  transform: esp-256-aes ,
  in use settings = {Tunnel, }
  conn id: 2013, flow id: SW:13, crypto map: MAP
  sa timing: remaining key lifetime (k/sec): (4493355/2403)
  IV size: 16 bytes
  replay detection support: N
  Status: ACTIVE

```

Рис. 3.64. Результат виконання діагностичної команди show crypto ipsec sa на маршрутизаторі R6

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				122
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R7
protected vrf: (none)
local ident (addr/mask/prot/port): (193.3.15.0/255.255.255.248/47/0)
remote ident (addr/mask/prot/port): (183.3.15.0/255.255.255.248/47/0)
current peer 183.3.15.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 14105, #pkts encrypt: 14105, #pkts digest: 14105
  #pkts decaps: 14161, #pkts decrypt: 14161, #pkts verify: 14161
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

local crypto endpt.: 193.3.15.1, remote crypto endpt.: 183.3.15.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x2C19DFDC(739893212)

inbound esp sas:
  spi: 0xA93A7A9C(2839181980)
    transform: esp-256-aes ,
    in use settings ={Tunnel, }
    conn id: 2004, flow_id: SW:4, crypto map: MAP
    sa timing: remaining key lifetime (k/sec): (4607285/2175)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x2C19DFDC(739893212)
    transform: esp-256-aes ,
    in use settings ={Tunnel, }
    conn id: 2003, flow_id: SW:3, crypto map: MAP
    sa timing: remaining key lifetime (k/sec): (4607285/2173)
    IV size: 16 bytes

```

Рис. 3.65. Результат виконання діагностичної команди show crypto ipsec sa на маршрутизаторі R7

```

R8
local ident (addr/mask/prot/port): (194.3.15.0/255.255.255.248/47/0)
remote ident (addr/mask/prot/port): (184.3.15.0/255.255.255.248/47/0)
current peer 184.3.15.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 14077, #pkts encrypt: 14077, #pkts digest: 14077
  #pkts decaps: 14030, #pkts decrypt: 14030, #pkts verify: 14030
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

local crypto endpt.: 194.3.15.1, remote crypto endpt.: 184.3.15.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x7A68C572(2053686642)

inbound esp sas:
  spi: 0x6E535C65(1850956901)
    transform: esp-256-aes ,
    in use settings ={Tunnel, }
    conn id: 2008, flow_id: SW:8, crypto map: MAP
    sa timing: remaining key lifetime (k/sec): (4500294/2890)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x7A68C572(2053686642)
    transform: esp-256-aes ,
    in use settings ={Tunnel, }

```

Рис. 3.66. Результат виконання діагностичної команди show crypto ipsec sa на маршрутизаторі R8

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				123
Змн.	Арк.	№ докум.	Підпис	Дата		

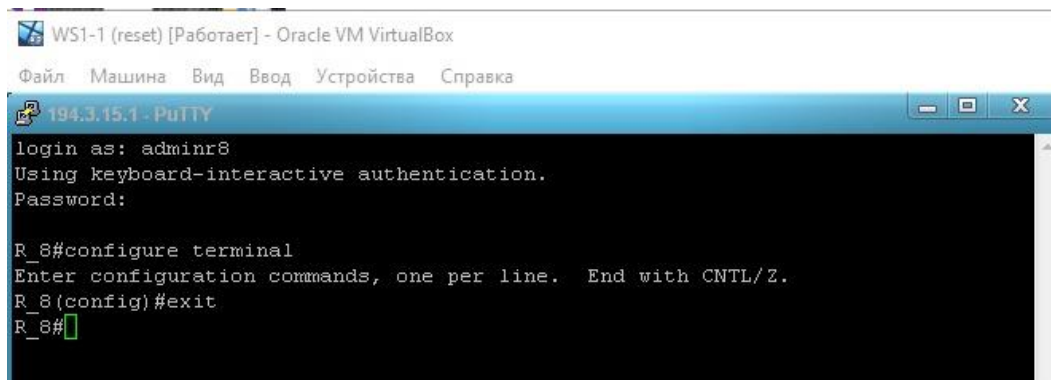


Рис. 3.67. Здійснене підключення до маршрутизатора мережі R8 через SSH- клієнт PuTTY

3.6. Здійснення перевірки доступу на читання та зміни папки із робочої станції WS2 (Windows 10) під двома створеними раніше користувачами.

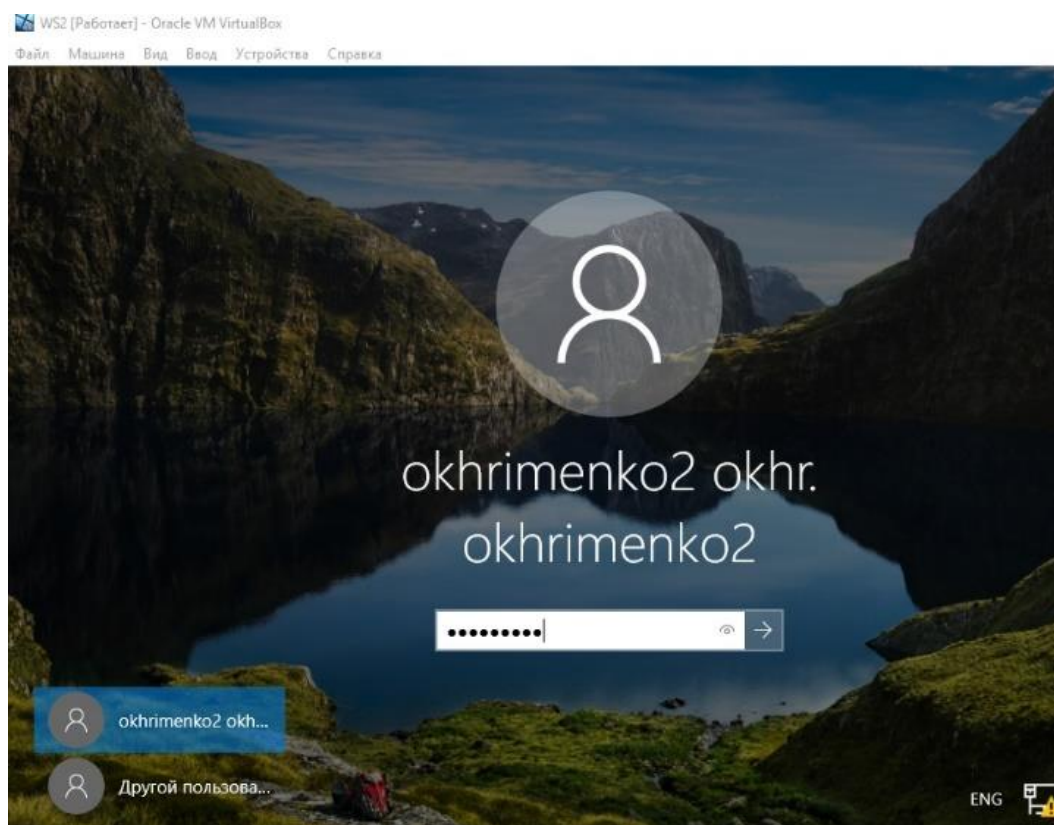


Рис. 3.68. Підключення до серверу за допомогою логіну створеного користувача

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				124
Змн.	Арк.	№ докум.	Підпис	Дата		

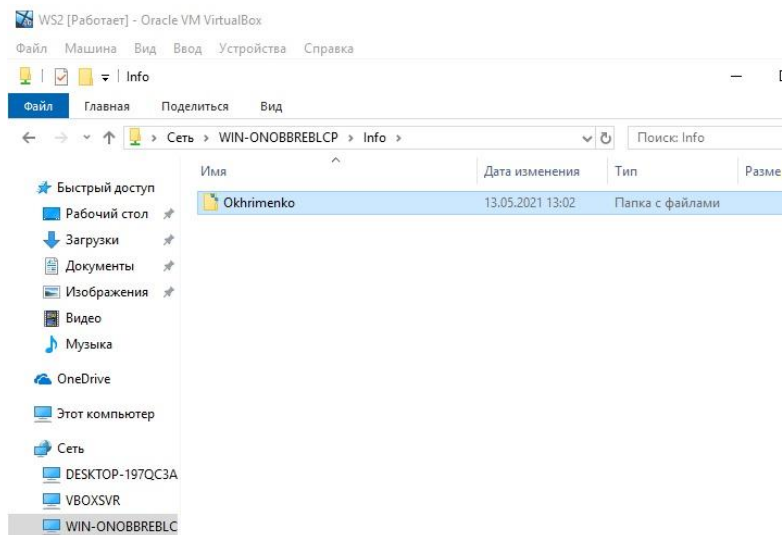


Рис. 3.69. Перегляд файлів в створеній папці

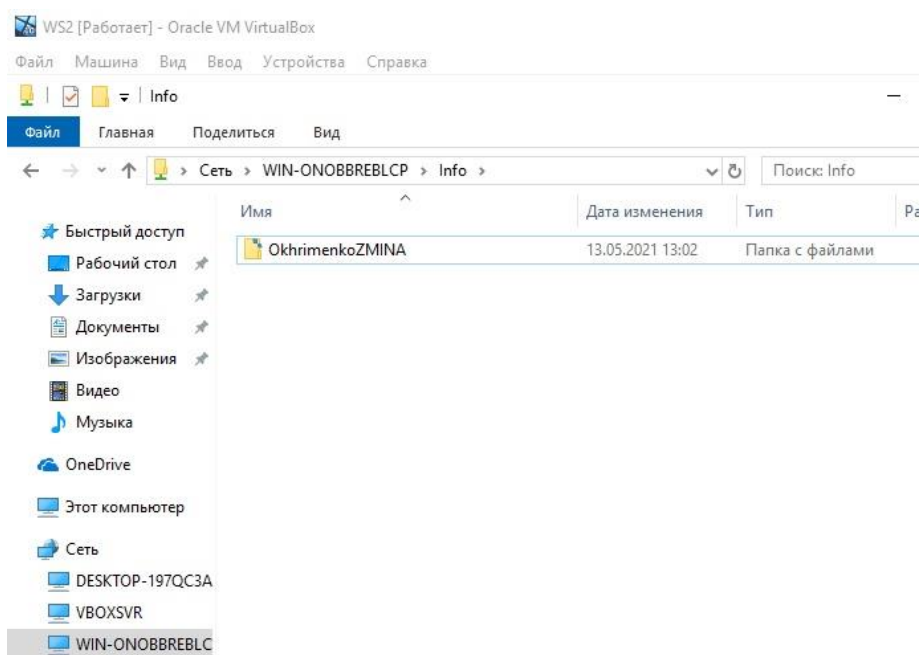


Рис. 3.70. Зміна назви папки на сервері WS1

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				125
Змн.	Арк.	№ докум.	Підпис	Дата		

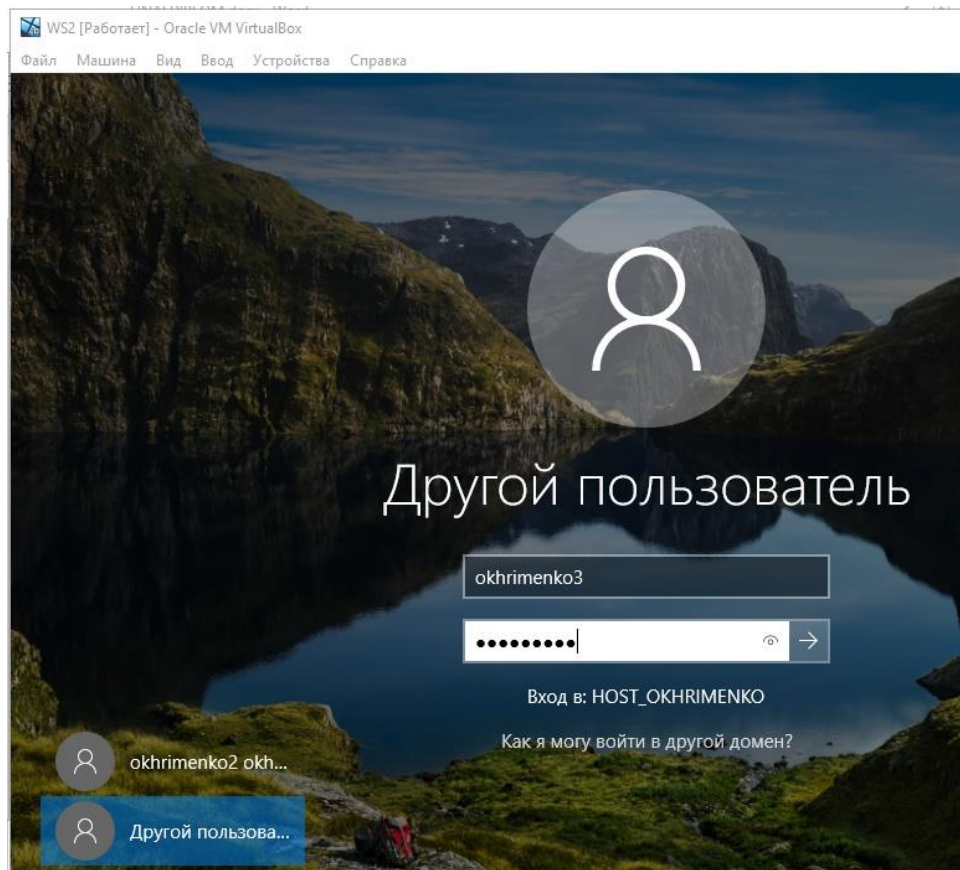


Рис. 3.71. Підключення до серверу за допомогою логіну створеного користувача

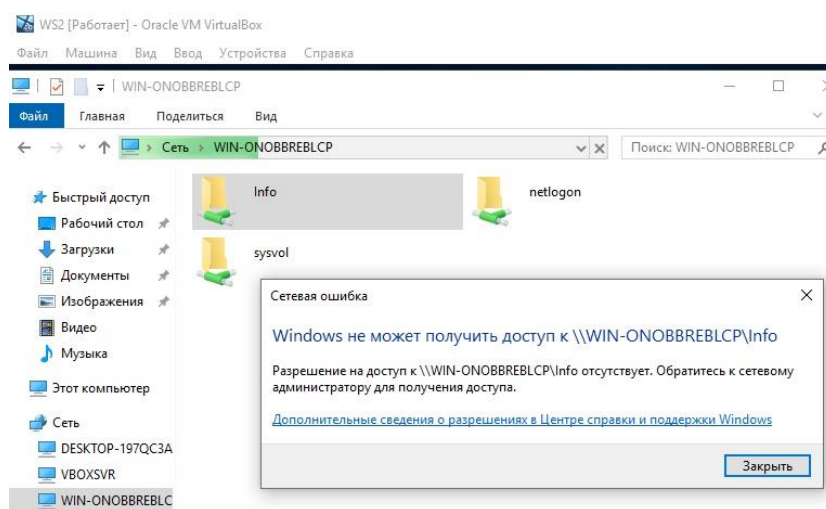


Рис. 3.72. Неможливість переглянути вміст створеної папки без необхідних прав доступу

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				126
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до третього розділу.

В третьому розділі проаналізувавши основні вимоги технічного завдання та особливості побудови захищеної мережі, було обране необхідне обладнання для організації роботи мережі, спираючись на наявне в продажі обладнання. Було наведено технічні характеристики вибраного обладнання. Було побудовано та налагоджено спроектовану топологію в симуляторі GNS3.

Протестовано мережу на коректність налаштування, роботу протокола тунелювання GRE та особливості роботи протоколів маршрутизації OSPF та EIGRP. Так як, GRE є протоколом інкапсуляції і не виконує шифрування. Створення тунелю GRE точка-точка без будь-якого шифрування надзвичайно ризиковано, оскільки конфіденційні дані можуть бути легко вилучені з тунелю і переглянуті іншими. В такому випадку нам на допомогу приходять набір протоколів шифрування IPsec для додавання рівня шифрування і захисту тунелю GRE. В результаті весь трафік, який надходить в тунель GRE, буде шифруватися протоколом IPsec. Протестовано роботу створених IPSec тунелів між внутрішніми мережами, щоб користувачі одної мережі могли безпечно звертатися до ресурсів іншої мережі, при цьому трафік буде шифруватися та за допомогою списків доступу (ACL) переда даних буде відбуватися тільки по дозволеним IP-адресам. Після чого, було створено крипто-карти (Crypto map) IPSec до вихідних інтерфесів кінцевих маршрутизаторів. Звісно, відбулося невелике зростання «пінгу» та зменшення каналу передачі даних, однак ми отримали велику захищену та відмовостійку мережу.

Для віддаленого адміністрування, що дозволяють управляти системою за допомогою мережі було налаштовано протокол SSHv2 та встановлено Active Directory із роллю первинного контролера домену на першому сервері. Для створення домена використовувався Windows Server 2019. Здійснено підключення до маршрутизаторів мережі через SSH- клієнт PuTTY. Здійснено перевірку доступу на читання та зміни створеної папки «Info» із робочої станції WS2 (Windows 10) під двома створеними раніше користувачами.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				127
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У випускній дипломній кваліфікаційній роботі представлені етапи проектування захищеної корпоративної комп'ютерної мережі організації на базі протоколів GRE та IP-Security та впровадження протоколу віддаленого доступу для створеної мережі.

Для вирішення поставленого завдання було проаналізовано два створених рішення з використанням технологій протоколу тунелювання GRE, протоколу захисту даних IP-Security, протоколів динамічної маршрутизації OSPF, EIGRP та мережевого протоколу SSH. Аналіз створених рішень дав розуміння того, які технології використовувати для вирішення поставленого завдання.

Після аналізу теоретичних відомостей та створених рішень в першому розділі, можна зробити висновок, що успішна робота організацій, які використовують ті чи інші інформаційні системи, залежить від того наскільки добре вони захищені від можливих загроз безпеки. Дослідивши апаратно-програмні засоби побудови, управління мережею та організації безпечної та високошвидкісної передачі даних було розроблено структуру ядра мережі, наведено обґрунтування вибору маршрутизаторів та зв'язків між ними. Наведено загальну кількість необхідного обладнання. Для побудованої мережі розроблено схему її адресації, яка дозволяє легке управління адресами пристроїв та призначена до подальшого розширення мережі, обрані типи з'єднання між обладнанням.

Для того щоб об'єднати локальні мережі офісів і віддалених філій, було застосовано технологію віртуальних приватних мереж - VPN (Virtual Private Network), яка забезпечила об'єднання віддалених офісів в єдину захищену мережу для обміну даними, із захистом інформації. На маршрутизаторах мережі було налаштовано безпечні тунелі VPN типу «site-to-site» через створену мережу з використанням протоколу IP Security (IPSec). Було створено таблицю параметрів для налагодження віддаленого підключення до маршрутизаторів мережі за протоколом SSHv2 та розроблено таблицю параметрів для налагодження тунелів, а також, таблиці для налаштування політики ISAKMP Phase 1 та Phase 2 для маршрутизаторів які належать рівню розподілу. Також були створені налаштування для двох маршрутизаторів які належать рівню ядра, що забезпечують високошвидкісну передачу даних між сегментами рівня розподілу.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				128
Змн.	Арк.	№ докум.	Підпис	Дата		

Це дало змогу побудувати та налагодити спроектовану мережу в симуляторі GNS3. Протестовано мережу на коректність налаштування та особливості роботи налаштованих протоколів маршрутизації OSPF та EIGRP. Весь трафік, який надходить в тунель GRE, шифрується протоколом IPsec. Розкрито принципи роботи протокола GRE за допомогою діагностичних команд при передачі даних по мережі з використанням механізмів захисту IP-Security. Здійснено підключення до маршрутизаторів мережі через SSH- клієнт PuTTY. Після цього, було створено ліс і кореневий домен, створено базу користувачів для Active Directory користувачі і комп'ютери. Для створення домена використовувався Windows Server 2019.

Здійснено перевірку доступу на читання та зміни створеної папки «Info» із робочої станції WS2 (Windows 10) під двома створеними раніше користувачами. В результаті, адміністратор зможе швидко відреагувати та усунути відповідну проблему на будь-якому маршрутизаторі мережі, відновити його працездатний стан за допомогою протоколу SSHv2, та переглянути необхідну інформацію в папці на сервері WS1.

Отже, в результаті виконання дипломної роботи була спроектована захищена корпоративна комп'ютерна мережа організації на базі протоколів GRE та IP-Security, а також було налаштовано протокол віддаленого доступу для створеної мережі у віртуальному середовищі GNS3.

На побудованій мережі було протестовано роботу створених IPSec тунелів між внутрішніми мережами на маршрутизаторах рівня розподілу, щоб користувачі одної мережі могли безпечно звертатися до ресурсів іншої мережі, при цьому трафік буде шифруватися та за допомогою списків доступу (ACL) переда даних буде відбуватися тільки по дозволеним IP-адресам. В результаті весь трафік, який надходить в тунель GRE, шифрується протоколом IPsec. При використанні IPSec відбувається подвійна інкапсуляція, що знижує продуктивність - це саме та ціна, яку доведеться заплатити за безпеку переданих даних по тунелям, однак ми отримали велику захищену та відмовостійку мережу з можливістю віддаленого адміністрування маршрутизаторів мережі використовуючи мережевий протокол рівня застосунків SSH. Здобуто теоретичні та практичні навички пов'язані з проектуванням та побудовою корпоративних мереж для організацій.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				129
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Баумана М. из Н. библиотеки им. Н.Э. IPsec (IP Security) [Електронний ресурс] 2017. URL: [https://ru.bmstu.wiki/IPsec \(IP Security\)](https://ru.bmstu.wiki/IPsec_(IP_Security))
2. Васин Н.Н. Основы сетевых технологий на базе коммутаторов и маршрутизаторов: Учебное пособие. – М.: ИНТУИТ: БИНОМ, 2011. – 270 с.
3. Віртуальна приватна мережа VPN – (Virtual Private Network) [Електронний ресурс]. URL: <https://sites.google.com/site/zahistlokalnoiemerezi/zahist/virtualna-privatna-mereza>
4. Віддалений робочий стіл Linux. Віддалений доступ. Віддалений графічний доступ до Ubuntu через VNC Linux доступ до робочого столу користувача [Електронний ресурс] 2020. URL: <https://flypods.ru/uk/udalennyyi-rabochii-stol-linux-udalennyyi-dostup-udalennyyi-graficheskii/>
5. Ермаков А.Е. - Основы конфигурирования корпоративных сетей Cisco Издательство: ФГБОУ, 2013. – 400 с.
6. История протокола SSH [Електронний ресурс]. 2016. URL: <https://poznayka.org/s25580t1.html>
7. Концепція інформаційної безпеки Загальні положення концепції інформаційної безпеки [Електронний ресурс] 2016. URL: <https://uchika.in.ua/konceptsiya-informacijnoyi-bezpeki-zagaleni-polojennya-konceptsi.html?page=5>
8. Корневская О. С. Электронное учебное пособие «Динамическая маршрутизация в корпоративных компьютерных сетях». Выпускная квалификационная работа бакалавра — Екатеринбург: РГППУ, 2016. - 48 с.
9. Куроуз Д. Компьютерные сети. Настольная книга системного администратора. / Д. Куроуз, Т. Росс — М: Эксмо, 2016. - 912 с.
10. Лэммл Т. CCNA Cisco Certified Network Associate. Учебное руководство: учебное пособие. - 2-е изд., перераб. и доп. – М.: ЛОРИ, 2014. – 576 с.
11. Лэммл Т. Настройка коммутаторов. Учебное руководство / Т. Лэммл, К. Хейлзю – М.: Лори, 2015. – 464 с.
12. 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.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				130
Змн.	Арк.	№ докум.	Підпис	Дата		

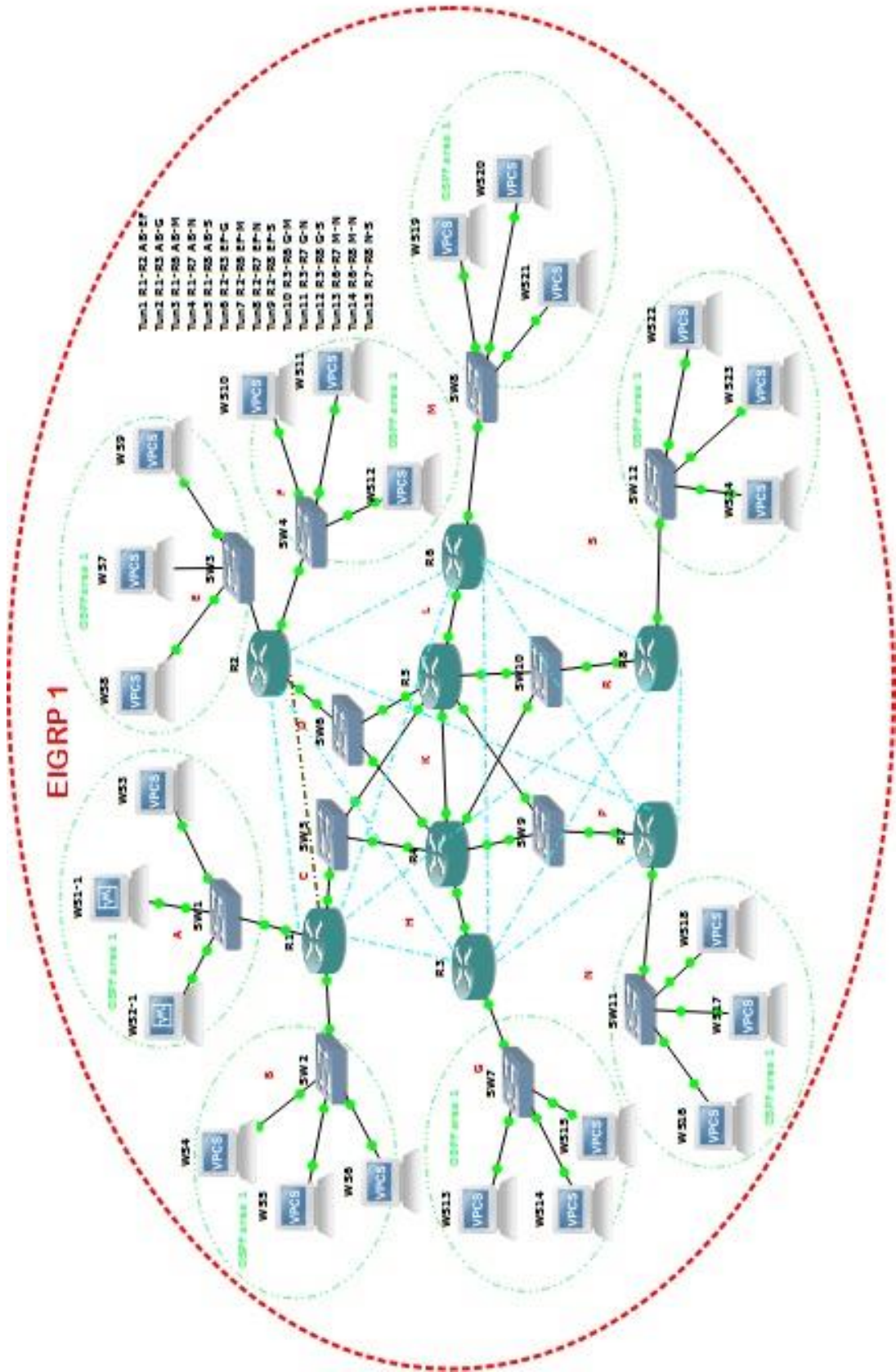
13. Максимов Н.В. Компьютерные сети: учебник для вузов /Н.В. Максимов, И.И. Попов — под общ. ред. Н.В. Максимова. — 3-е изд. — Москва, 2013. - 448 с.
14. Олифер В., Олифер Н. Компьютерные сети принципы, технологии, протоколы. 5th-е издани ed. / ed. Питер, 2016. 920 с.
15. Сергеев А. Основы локальных компьютерных сетей — СПб, 2016. – 184 с.
16. Таненбаум Э. Компьютерные сети./Э. Таненбаум, Д. Уэзеролл — СПб.: Питер, 2016. - 960 с.
17. Тониевич А. Компьютерные сети — М.: Асерфан, 2012. – 235 с.
18. Шаньгин. В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. Пособие. – М:ИД ФОРУМ: Инфра-М, 2010. – 416 с.
19. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях — М.: «ДМК Пресс», 2012. – 593 с.
20. Що таке VPN - опис технології, переваги використання. [Електронний ресурс]. 2019. URL: <https://alternativa.dp.ua/shho-take-vpn-opis-tehnologiyi-perevagi-vikoristannya/>
21. Як працює ipsec. Технології використовувати в IPSEC. Вхідно у внутрішню мережу [Електронний ресурс]. 2019. URL: <https://beasthackerz.ru/uk/audio/kak-rabotaet-ipsec-tehnologii-ispolzuemye-v-ipsec-vhodim-vo-vnutrennyuyu.html>
22. CCNP Route GNS3 Lab: OSPF over GRE over IPSec over EIGRP [Електронний ресурс]. URL: <http://sclabs.blogspot.com/2014/05/ccnp-route-gns3-lab-ospf-over-gre-over.html>
23. Desmond B., Richards J. Active Directory: Designing, Deploying, and Running Active Directory O'Reilly Media, Fifth edition – May 31, 2013. – 738 с.
24. SSH Configuration on Packet Tracer [Електронний ресурс]. URL: <https://ip-cisco.com/lesson/ssh-configuration-on-packet-tracer/>
25. Vpn віртуальна приватна мережа. Побудова безпечних мереж на основі VPN. Що таке vpn в iphone [Електронний ресурс] 2020. URL: <https://shyza.ru/uk/vpn-virtualnaya-chastnaya-set-postroenie-bezopasnyh-setei-na-osnove-vpn-chto-takoe-vpn.html>
26. VPN и IPSec на пальцах [Електронний ресурс] 2002. URL: https://www.opennet.ru/docs/RUS/vpn_ipsec/

		Охріменко. Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				131
Змн.	Арк.	№ докум.	Підпис	Дата		

Додатки

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				132
Змн.	Арк.	№ докум.	Підпис	Дата		

Детальна схема побудованої мережі



Б.1 Технічні характеристики маршрутизатора Cisco Systems CISCO3660

Інтерфейси: 1х/2х LAN, 1х serial, 6х NM (Слоти мережевих модулів), 2х AIM (Слоти розширеного інтеграційного модуля). Максимум 24 Ethernet порти, 32 FastEthernet порти або 24 serial порти. Cisco 3660 містить на шасі вбудований порт Ethernet і завдяки цьому має можливість встановити шість модулів NM-HDV-2E1-60E, що в залежності від обраного типу кодеків, дозволяє отримати від 180 до 360 голосових портів.

Безпека: Ідентифікація користувачів, списки доступу, контроль подій, шифрування, побудова приватних мереж та тунелювання. Підтримується широкий спектр протоколів безпеки, включаючи TACACS +, Radius, Kerberos.

Функції безпеки: повний набір мережевих протоколів (Enterprise Feature Set), віддалений моніторинг (RMON), протокол резервування ресурсів (RSVP), шифрування на мережевому рівні з використанням стандартної технології IPSec (Plus Encryption Feature Set).

Протоколи: IPv4, IPv6, static routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Novell IPX, AppleTalk, IGMP, RSVP, PIM, WFQ, ISL (InterSwitch Link).

Інкапсуляція: Ethernet, 802.1q VLAN, MPP (Multichassis Multilink Point-to-Point Protocol), Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Serial (RS-232, RS-449, X.21, V.35, and EIA-530);

Апаратна підтримка шифрування: DES, 3DES, AES 128, AES 192, AES 256;

Пам'ять DRAM: 32 МБ DRAM, можна збільшити до 256 МБ;

Пам'ять Flash: 8 МБ, можна збільшити до 64 МБ;

Зовнішнє джерело живлення: на вході: 110 ~ 220 В змінного струму, 50 ~ 60 Гц; максимальна вихідна потужність: 250 Вт; на виході: 12 В постійного струму.

Робоча температура: 0 ~ 50 ° C;

Розміри: 22,1 x 44,5 x 30,0 см;

Вага: 19.6 кг.

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				134
Змн.	Арк.	№ докум.	Підпис	Дата		

Б.2 Технічні характеристики комутатора Cisco Systems WS-C3650-24PS-L

Опис:

24 порти Gigabit Ethernet;

4 Комбінованих порти Gigabit SFP;

Максимальна кількість мереж VLAN 4000;

Пропускна здатність: 88 Гбит\с.

Набір функції LAN Base;

Пам'ять DRAM: 4 Gb;

Пам'ять Flash: 2 Gb;

Порти стекування: Так;

Стекування StackWise: 160/9;

Кількість точок доступу на комутатор/стек: 25;

Кількість бездротових клієнтів на комутатор/стек: 1000;

Пропускна здатність в стеці: 160 Гбит/с;

Максимальний розмір пакета (MTU): До 9000 байт;

Таблиця MAC – адрес: 32000;

Стандарти:

IEEE 802.1d (Spanning Tree)

IEEE 802.1p (Priority tags)

IEEE 802.1q (VLAN)

IEEE 802.1s (Multiple Spanning Tree)

IEEE 802.3x (Flow control)

IEEE 802.3at (PoE+)

IEEE 802.3bz (2.5GBASE-T та 5GBASE-T)

IEEE 802.1ba (AVB)

Безпека: Secure Shell (SSH) Protocol; Kerberos; (SNMPv3);

Гарантія: обмежена довічна гарантія;

Середній час безвідмовної роботи 528280 г;

Потужність PoE: 390 Вт;

Живлення: 640 Вт AC

Розміри: 4,4 x 44,5 x 44,8 см;

Вага: 7,26 кг;

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				135
Змн.	Арк.	№ докум.	Підпис	Дата		

Лістинги конфігурацій:

```
R_1#show run
Building configuration...
Current configuration : 5667 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$r/sI$VDg/XEQQp-PhLiqsUzz8h61
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
ip domain name mynet.net
!
username adminr1 privilege 15 secret 5
$1$Jsbd$eHv9Y0facnCqv/1eD/Ac91
username userr1 secret 5
$1$u/Ym$ERC9B4/M8sL.8XWSMIK5U/
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 30
ip ssh version 2
!
crypto isakmp policy 1
  encr aes 256
  authentication pre-share
  group 2
  lifetime 86000
crypto isakmp key R1R2 address 184.3.15.1
crypto isakmp key R1R3 address 188.3.15.1
crypto isakmp key R1R6 address 190.3.15.2
crypto isakmp key R1R7 address 193.3.15.1
crypto isakmp key R1R8 address 194.3.15.1
!
crypto ipsec transform-set TRANSF esp-aes 256
!
crypto map MAP 12 ipsec-isakmp
  description IPSEC to 184.3.15.1
  set peer 184.3.15.1
```

```
R_2#show run
Building configuration...
Current configuration : 5699 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_2
!
boot-start-marker
boot-end-marker
!
enable secret 5
$1$LU7/$aqkfCym/nMLq2zO/QbjOS0
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
ip domain name mynet.net
!
username adminr2 privilege 15 secret 5
$1$G1yP$vsv4rf2qUTM0qBydoE8WK.
username userr2 secret 5 $1$OLaH$jUx-
arB6sovr0.X4VkF.x10
!
ip tcp synwait-time 5
ip ssh maxstartups 9
ip ssh time-out 20
ip ssh authentication-retries 4
ip ssh version 2
!
crypto isakmp policy 1
  encr aes 256
  authentication pre-share
  group 2
  lifetime 86000
crypto isakmp key R1R2 address 183.3.15.1
crypto isakmp key R2R3 address 188.3.15.1
crypto isakmp key R2R6 address 190.3.15.2
crypto isakmp key R2R7 address 193.3.15.1
crypto isakmp key R2R8 address 194.3.15.1
!
crypto ipsec transform-set TRANSF esp-aes 256
!
crypto map MAP 12 ipsec-isakmp
  description IPSEC to 183.3.15.1
```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				136
Змн.	Арк.	№ докум.	Підпис	Дата		

```

set transform-set TRANSF
match address 101
crypto map MAP 13 ipsec-isakmp
description IPSEC to 188.3.15.1
set peer 188.3.15.1
set transform-set TRANSF
match address 102
crypto map MAP 16 ipsec-isakmp
description IPSEC to 190.3.15.2
set peer 190.3.15.2
set transform-set TRANSF
match address 103
crypto map MAP 17 ipsec-isakmp
description IPSEC to 193.3.15.1
set peer 193.3.15.1
set transform-set TRANSF
match address 104
crypto map MAP 18 ipsec-isakmp
description IPSEC to 194.3.15.1
set peer 194.3.15.1
set transform-set TRANSF
match address 105
!
interface Loopback11
ip address 11.11.11.11 255.255.255.0
!
interface Tunnel12
ip address 101.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 183.3.15.1
tunnel destination 184.3.15.1
!
interface Tunnel13
ip address 102.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 183.3.15.1
tunnel destination 188.3.15.1
!
interface Tunnel16
ip address 103.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 183.3.15.1
tunnel destination 190.3.15.2
!
interface Tunnel17
ip address 104.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 183.3.15.1

```

```

set peer 183.3.15.1
set transform-set TRANSF
match address 101
crypto map MAP 23 ipsec-isakmp
description IPSEC to 188.3.15.1
set peer 188.3.15.1
set transform-set TRANSF
match address 106
crypto map MAP 26 ipsec-isakmp
description IPSEC to 190.3.15.2
set peer 190.3.15.2
set transform-set TRANSF
match address 107
crypto map MAP 27 ipsec-isakmp
description IPSEC to 193.3.15.1
set peer 193.3.15.1
set transform-set TRANSF
match address 108
crypto map MAP 28 ipsec-isakmp
description IPSEC to 194.3.15.1
set peer 194.3.15.1
set transform-set TRANSF
match address 109
!
interface Loopback22
ip address 22.22.22.22 255.255.255.0
!
interface Tunnel12
ip address 101.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 184.3.15.1
tunnel destination 183.3.15.1
!
interface Tunnel23
ip address 106.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 184.3.15.1
tunnel destination 188.3.15.1
!
interface Tunnel26
ip address 107.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 184.3.15.1
tunnel destination 190.3.15.2
!
interface Tunnel27
ip address 108.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360

```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				137
Змн.	Арк.	№ докум.	Підпис	Дата		

```

tunnel destination 193.3.15.1
!
interface Tunnel18
ip address 105.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 183.3.15.1
tunnel destination 194.3.15.1
!
interface FastEthernet0/0
description LINK_TO_LAN_A
ip address 181.3.15.1 255.255.255.240
duplex auto
speed auto
!
interface FastEthernet0/1
description LINK_TO_LAN_B
ip address 182.3.15.1 255.255.255.240
duplex auto
speed auto
!
interface FastEthernet1/0
description LINK_TO_LAN_C
ip address 183.3.15.1 255.255.255.248
duplex auto
speed auto
crypto map MAP
!
interface Vlan1
no ip address
!
router eigrp 1
network 11.11.11.0 0.0.0.255
network 183.3.15.0 0.0.0.7
no auto-summary
!
router ospf 1
log-adjacency-changes
network 101.3.15.0 0.0.0.255 area 0
network 102.3.15.0 0.0.0.255 area 0
network 103.3.15.0 0.0.0.255 area 0
network 104.3.15.0 0.0.0.255 area 0
network 105.3.15.0 0.0.0.255 area 0
network 181.3.15.0 0.0.0.15 area 1
network 182.3.15.0 0.0.0.15 area 1
!
no ip http server
no ip http secure-server
ip forward-protocol nd
!
access-list 101 permit gre 183.3.15.0 0.0.0.7
184.3.15.0 0.0.0.7 log

```

```

tunnel source 184.3.15.1
tunnel destination 193.3.15.1
!
interface Tunnel28
ip address 109.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 184.3.15.1
tunnel destination 194.3.15.1
!
interface FastEthernet0/0
description LINK_TO_LAN_E
ip address 185.3.15.1 255.255.255.240
duplex auto
speed auto
!
interface FastEthernet0/1
description LINK_TO_LAN_F
ip address 186.3.15.1 255.255.255.240
duplex auto
speed auto
!
interface FastEthernet1/0
description LINK_TO_LAN_D
ip address 184.3.15.1 255.255.255.248
duplex auto
speed auto
crypto map MAP
!
interface Vlan1
no ip address
!
router eigrp 1
network 22.22.22.0 0.0.0.255
network 184.3.15.0 0.0.0.7
no auto-summary
!
router ospf 1
log-adjacency-changes
network 101.3.15.0 0.0.0.255 area 0
network 106.3.15.0 0.0.0.255 area 0
network 107.3.15.0 0.0.0.255 area 0
network 108.3.15.0 0.0.0.255 area 0
network 109.3.15.0 0.0.0.255 area 0
network 185.3.15.0 0.0.0.15 area 1
network 186.3.15.0 0.0.0.15 area 1
!
no ip http server
no ip http secure-server
ip forward-protocol nd
!
!

```

		Охріменко Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				138
Змн.	Арк.	№ докум.	Підпис	Дата		

```

access-list 101 permit udp 183.3.15.0 0.0.0.7 eq
isakmp 184.3.15.0 0.0.0.7 log
access-list 101 deny ip any any log
access-list 102 permit gre 183.3.15.0 0.0.0.7
188.3.15.0 0.0.0.3 log
access-list 102 permit udp 183.3.15.0 0.0.0.7 eq
isakmp 188.3.15.0 0.0.0.3 log
access-list 102 deny ip any any log
access-list 103 permit gre 183.3.15.0 0.0.0.7
190.3.15.0 0.0.0.3 log
access-list 103 permit udp 183.3.15.0 0.0.0.7 eq
isakmp 190.3.15.0 0.0.0.3 log
access-list 103 deny ip any any log
access-list 104 permit gre 183.3.15.0 0.0.0.7
193.3.15.0 0.0.0.7 log
access-list 104 permit udp 183.3.15.0 0.0.0.7 eq
isakmp 193.3.15.0 0.0.0.7 log
access-list 104 deny ip any any log
access-list 105 permit gre 183.3.15.0 0.0.0.7
194.3.15.0 0.0.0.7 log
access-list 105 permit udp 183.3.15.0 0.0.0.7 eq
isakmp 194.3.15.0 0.0.0.7 log
access-list 105 deny ip any any log
no cdp log mismatch duplex
!
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
logging synchronous
login local
transport input ssh
transport output ssh
!
end

```

```

R_3#show run
Building configuration...
Current configuration : 5662 bytes
!
version 12.4
service timestamps debug datetime msec

```

```

!
access-list 101 permit gre 184.3.15.0 0.0.0.7
183.3.15.0 0.0.0.7 log
access-list 101 permit udp 184.3.15.0 0.0.0.7 eq
isakmp 183.3.15.0 0.0.0.7 log
access-list 101 deny ip any any log
access-list 106 permit gre 184.3.15.0 0.0.0.7
188.3.15.0 0.0.0.3 log
access-list 106 permit udp 184.3.15.0 0.0.0.7 eq
isakmp 188.3.15.0 0.0.0.3 log
access-list 106 deny ip any any log
access-list 107 permit gre 184.3.15.0 0.0.0.7
190.3.15.0 0.0.0.3 log
access-list 107 permit udp 184.3.15.0 0.0.0.7 eq
isakmp 190.3.15.0 0.0.0.3 log
access-list 107 deny ip any any log
access-list 108 permit gre 184.3.15.0 0.0.0.7
193.3.15.0 0.0.0.7 log
access-list 108 permit udp 184.3.15.0 0.0.0.7 eq
isakmp 193.3.15.0 0.0.0.7 log
access-list 108 deny ip any any log
access-list 109 permit gre 184.3.15.0 0.0.0.7
194.3.15.0 0.0.0.7 log
access-list 109 permit udp 184.3.15.0 0.0.0.7 eq
isakmp 194.3.15.0 0.0.0.7 log
access-list 109 deny ip any any log
no cdp log mismatch duplex
!
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
logging synchronous
login local
transport input ssh
transport output ssh
!
end

```

```

R_4#show run
Building configuration...
Current configuration : 2944 bytes
!
version 12.4
service timestamps debug datetime msec

```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				139
Змн.	Арк.	№ докум.	Підпис	Дата		

```

service timestamps log datetime msec
no service password-encryption
!
hostname R_3
!
boot-start-marker
boot-end-marker
!
enable secret 5
$1$Rv5J$bQ6MWlq4H4fAD1JfsBOs.1
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
ip domain name mynet.net
!
username adminr3 privilege 15 secret 5
$1$4KUi$U126w4ekzJdnM7xpK5YY50
username userr3 secret 5 $1$9ZAI$mppm-
Bel7uU/L4M2T/LPkSr/
!
ip tcp synwait-time 5
ip ssh maxstartups 6
ip ssh time-out 45
ip ssh authentication-retries 5
ip ssh version 2
!
crypto isakmp policy 1
  encr aes 256
  authentication pre-share
  group 2
  lifetime 86000
crypto isakmp key R1R3 address 183.3.15.1
crypto isakmp key R2R3 address 184.3.15.1
crypto isakmp key R3R6 address 190.3.15.2
crypto isakmp key R3R7 address 193.3.15.1
crypto isakmp key R3R8 address 194.3.15.1
!
crypto ipsec transform-set TRANSF esp-aes 256
!
crypto map MAP 13 ipsec-isakmp
  description IPSEC to 183.3.15.1
  set peer 183.3.15.1
  set transform-set TRANSF
  match address 102
crypto map MAP 23 ipsec-isakmp
  description IPSEC to 184.3.15.1
  set peer 184.3.15.1
  set transform-set TRANSF

```

```

service timestamps log datetime msec
no service password-encryption
!
hostname R_4
!
boot-start-marker
boot-end-marker
!
enable secret 5
$1$DS4.$B4hJ/oOLR1pWabUBG6Tml/
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
ip domain name mynet.net
!
username adminr4 privilege 15 secret 5
$1$upSN$.6BvwC17nX.1v5maHGE9e1
username userr4 secret 5
$1$AKE.$Qa4o3KpgnqJaIjW9YB.fc1
!
ip tcp synwait-time 5
ip ssh maxstartups 4
ip ssh time-out 60
ip ssh version 2
!
interface FastEthernet0/0
  description LINK_TO_LAN_C
  ip address 183.3.15.2 255.255.255.248
  duplex auto
  speed auto
!
interface FastEthernet0/1
  description LINK_TO_LAN_K
  ip address 189.3.15.1 255.255.255.252
  duplex auto
  speed auto
!
interface FastEthernet1/0
  description LINK_TO_LAN_P
  ip address 193.3.15.2 255.255.255.248
  duplex auto
  speed auto
!
interface FastEthernet3/0
  description LINK_TO_LAN_D
  no switchport
  ip address 184.3.15.3 255.255.255.248
!

```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				140
Змн.	Арк.	№ докум.	Підпис	Дата		

```

match address 105
crypto map MAP 36 ipsec-isakmp
description IPSEC to 190.3.15.2
set peer 190.3.15.2
set transform-set TRANSF
match address 109
crypto map MAP 37 ipsec-isakmp
description IPSEC to 193.3.15.1
set peer 193.3.15.1
set transform-set TRANSF
match address 110
crypto map MAP 38 ipsec-isakmp
description IPSEC to 194.3.15.1
set peer 194.3.15.1
set transform-set TRANSF
match address 111
!
interface Loopback33
ip address 33.33.33.33 255.255.255.0
!
interface Tunnel13
ip address 102.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 188.3.15.1
tunnel destination 183.3.15.1
!
interface Tunnel23
ip address 106.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 188.3.15.1
tunnel destination 184.3.15.1
!
interface Tunnel36
ip address 110.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 188.3.15.1
tunnel destination 190.3.15.2
!
interface Tunnel37
ip address 111.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 188.3.15.1
tunnel destination 193.3.15.1
!
interface Tunnel38
ip address 112.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360

```

```

interface FastEthernet3/1
description LINK_TO_LAN_H
no switchport
ip address 188.3.15.2 255.255.255.252
!
interface FastEthernet3/3
description LINK_TO_LAN_R
no switchport
ip address 194.3.15.3 255.255.255.248
!
interface Vlan1
no ip address
!
router eigrp 1
network 183.3.15.0 0.0.0.7
network 184.3.15.0 0.0.0.7
network 188.3.15.0 0.0.0.3
network 189.3.15.0 0.0.0.3
network 193.3.15.0 0.0.0.7
network 194.3.15.0 0.0.0.7
no auto-summary
!
no ip http server
no ip http secure-server
ip forward-protocol nd
!
no cdp log mismatch duplex
!
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
logging synchronous
login local
transport input ssh
transport output ssh
!
end

```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				141
Змн.	Арк.	№ докум.	Підпис	Дата		

```

tunnel source 188.3.15.1
tunnel destination 194.3.15.1
!
interface FastEthernet0/0
description LINK_TO_LAN_G
ip address 187.3.15.1 255.255.255.240
duplex auto
speed auto
!
interface FastEthernet3/1
description LINK_TO_LAN_H
no switchport
ip address 188.3.15.1 255.255.255.252
crypto map MAP
!
interface Vlan1
no ip address
!
router eigrp 1
network 33.33.33.0 0.0.0.255
network 188.3.15.0 0.0.0.3
no auto-summary
!
router ospf 1
log-adjacency-changes
network 102.3.15.0 0.0.0.255 area 0
network 106.3.15.0 0.0.0.255 area 0
network 110.3.15.0 0.0.0.255 area 0
network 111.3.15.0 0.0.0.255 area 0
network 112.3.15.0 0.0.0.255 area 0
network 187.3.15.0 0.0.0.15 area 1
!
no ip http server
no ip http secure-server
ip forward-protocol nd
!
access-list 102 permit gre 188.3.15.0 0.0.0.3
183.3.15.0 0.0.0.7 log
access-list 102 permit udp 188.3.15.0 0.0.0.3 eq
isakmp 183.3.15.0 0.0.0.7 log
access-list 102 deny ip any any log
access-list 105 permit gre 188.3.15.0 0.0.0.3
184.3.15.0 0.0.0.7 log
access-list 105 permit udp 188.3.15.0 0.0.0.3 eq
isakmp 184.3.15.0 0.0.0.7 log
access-list 105 deny ip any any log
access-list 109 permit gre 188.3.15.0 0.0.0.3
190.3.15.0 0.0.0.3 log
access-list 109 permit udp 188.3.15.0 0.0.0.3 eq
isakmp 190.3.15.0 0.0.0.3 log
access-list 109 deny ip any any log

```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				142
Змн.	Арк.	№ докум.	Підпис	Дата		

```

access-list 110 permit gre 188.3.15.0 0.0.0.3
193.3.15.0 0.0.0.7 log
access-list 110 permit udp 188.3.15.0 0.0.0.3 eq
isakmp 193.3.15.0 0.0.0.7 log
access-list 110 deny ip any any log
access-list 111 permit gre 188.3.15.0 0.0.0.3
194.3.15.0 0.0.0.7 log
access-list 111 permit udp 188.3.15.0 0.0.0.3 eq
isakmp 194.3.15.0 0.0.0.7 log
access-list 111 deny ip any any log
no cdp log mismatch duplex
!
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
logging synchronous
login local
transport input ssh
transport output ssh
!
end

```

```

R_5#show run
Building configuration...
Current configuration : 2944 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_5
!
boot-start-marker
boot-end-marker
!
enable secret 5
$1$pydf$q.1bfg2KonaNrouPYmsO.0
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
ip cef

```

```

R_6#show run
Building configuration...
Current configuration : 5662 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_6
!
boot-start-marker
boot-end-marker
!
enable secret 5
$1$shjo$ibKx666.oqaMvQ0cZFBuZ1
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
ip cef

```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				143
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip domain lookup
ip domain name mynet.net
!
username adminr5 privilege 15 secret 5
$1$1QwL$1WJDANjP..wXOxUatxKwX.
username userr5 secret 5
$1$M8IZ$J43vDruuxgDO.STJy/VFG1
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 30
ip ssh version 2
!
interface FastEthernet0/0
description LINK_TO_LAN_D
ip address 184.3.15.2 255.255.255.248
duplex auto
speed auto
!
interface FastEthernet0/1
description LINK_TO_LAN_K
ip address 189.3.15.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
description LINK_TO_LAN_R
ip address 194.3.15.2 255.255.255.248
duplex auto
speed auto
!
interface FastEthernet3/0
description LINK_TO_LAN_C
no switchport
ip address 183.3.15.3 255.255.255.248
!
interface FastEthernet3/1
description LINK_TO_LAN_L
no switchport
ip address 190.3.15.1 255.255.255.252
!
interface FastEthernet3/3
description LINK_TO_LAN_P
no switchport
ip address 193.3.15.3 255.255.255.248
!
interface Vlan1
no ip address
!
router eigrp 1
network 183.3.15.0 0.0.0.7
network 184.3.15.0 0.0.0.7

```

```

no ip domain lookup
ip domain name mynet.net
!
username adminr6 privilege 15 secret 5
$1$dbK6$se3WLE8LynMmIqisN6DfZ0
username userr6 secret 5
$1$jf.y$k4Nbkf2PZMLM71qS1RErM0
!
ip tcp synwait-time 5
ip ssh maxstartups 9
ip ssh time-out 25
ip ssh authentication-retries 4
ip ssh version 2
!
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
lifetime 86000
crypto isakmp key R1R6 address 183.3.15.1
crypto isakmp key R2R6 address 184.3.15.1
crypto isakmp key R3R6 address 188.3.15.1
crypto isakmp key R6R7 address 193.3.15.1
crypto isakmp key R6R8 address 194.3.15.1
!
crypto ipsec transform-set TRANSF esp-aes 256
!
crypto map MAP 16 ipsec-isakmp
description IPSEC to 183.3.15.1
set peer 183.3.15.1
set transform-set TRANSF
match address 103
crypto map MAP 26 ipsec-isakmp
description IPSEC to 184.3.15.1
set peer 184.3.15.1
set transform-set TRANSF
match address 107
crypto map MAP 36 ipsec-isakmp
description IPSEC to 188.3.15.1
set peer 188.3.15.1
set transform-set TRANSF
match address 110
crypto map MAP 67 ipsec-isakmp
description IPSEC to 193.3.15.1
set peer 193.3.15.1
set transform-set TRANSF
match address 113
crypto map MAP 68 ipsec-isakmp
description IPSEC to 194.3.15.1
set peer 194.3.15.1
set transform-set TRANSF
match address 114

```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				144
Змн.	Арк.	№ докум.	Підпис	Дата		

```

network 189.3.15.0 0.0.0.3
network 190.3.15.0 0.0.0.3
network 193.3.15.0 0.0.0.7
network 194.3.15.0 0.0.0.7
no auto-summary
!
no ip http server
no ip http secure-server
ip forward-protocol nd
!
no cdp log mismatch duplex
!
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
logging synchronous
login local
transport input ssh
transport output ssh
!
end

```

```

!
interface Loopback66
ip address 66.66.66.66 255.255.255.0
!
interface Tunnel16
ip address 103.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 190.3.15.2
tunnel destination 183.3.15.1
!
interface Tunnel26
ip address 107.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 190.3.15.2
tunnel destination 184.3.15.1
!
interface Tunnel36
ip address 110.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 190.3.15.2
tunnel destination 188.3.15.1
!
interface Tunnel67
ip address 113.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 190.3.15.2
tunnel destination 193.3.15.1
!
interface Tunnel68
ip address 114.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 190.3.15.2
tunnel destination 194.3.15.1
!
interface FastEthernet0/0
description LINK_TO_LAN_M
ip address 191.3.15.1 255.255.255.240
duplex auto
speed auto
!
interface FastEthernet3/1
description LINK_TO_LAN_L
no switchport
ip address 190.3.15.2 255.255.255.252
crypto map MAP
!
interface Vlan1

```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				145
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip address
!
router eigrp 1
network 11.11.11.0 0.0.0.255
network 190.3.15.0 0.0.0.3
no auto-summary
!
router ospf 1
log-adjacency-changes
network 103.3.15.0 0.0.0.255 area 0
network 107.3.15.0 0.0.0.255 area 0
network 110.3.15.0 0.0.0.255 area 0
network 113.3.15.0 0.0.0.255 area 0
network 114.3.15.0 0.0.0.255 area 0
network 191.3.15.0 0.0.0.15 area 1
!
no ip http server
no ip http secure-server
ip forward-protocol nd
!
access-list 103 permit gre 190.3.15.0 0.0.0.3
183.3.15.0 0.0.0.7 log
access-list 103 permit udp 190.3.15.0 0.0.0.3 eq
isakmp 183.3.15.0 0.0.0.7 log
access-list 103 deny ip any any log
access-list 107 permit gre 190.3.15.0 0.0.0.3
184.3.15.0 0.0.0.7 log
access-list 107 permit udp 190.3.15.0 0.0.0.3 eq
isakmp 184.3.15.0 0.0.0.7 log
access-list 107 deny ip any any log
access-list 110 permit gre 190.3.15.0 0.0.0.3
188.3.15.0 0.0.0.3 log
access-list 110 permit udp 190.3.15.0 0.0.0.3 eq
isakmp 188.3.15.0 0.0.0.3 log
access-list 110 deny ip any any log
access-list 113 permit gre 190.3.15.0 0.0.0.3
193.3.15.0 0.0.0.7 log
access-list 113 permit udp 190.3.15.0 0.0.0.3 eq
isakmp 193.3.15.0 0.0.0.7 log
access-list 113 deny ip any any log
access-list 114 permit gre 190.3.15.0 0.0.0.3
194.3.15.0 0.0.0.7 log
access-list 114 permit udp 190.3.15.0 0.0.0.3 eq
isakmp 194.3.15.0 0.0.0.7 log
access-list 114 deny ip any any log
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15

```

		Охріменко. Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				146
Змн.	Арк.	№ докум.	Підпис	Дата		

```

logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
!
end

```

```

R_7#show run
Building configuration...
Current configuration : 5590 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_7
!
boot-start-marker
boot-end-marker
!
enable secret 5
$1$qI/e$jSEHp0Y.VnAEyFWnKYMoo/
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
ip domain name mynet.net
!
username adminr7 privilege 15 secret 5
$1$vyUJ$23lY5le6o0dHM0EiH8BjZ1
username userr7 secret 5
$1$hVIC$G7vmwYj6mQUnRPVzx6Pag/
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 20
ip ssh version 2
!
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2

```

```

R_8#show run
Building configuration...
Current configuration : 5622 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_8
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$9nF2$pcQn-
NUgO9NtBpVwZoa9Qx.
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
ip cef
no ip domain lookup
ip domain name mynet.net
!
username adminr8 privilege 15 secret 5
$1$qlq6$P/5zjX/eW0EIVYEIXBEnv1
username userr8 secret 5
$1$8HB9$LLYp8sJoXtd6VtkF.0JFY0
!
ip tcp synwait-time 5
ip ssh maxstartups 4
ip ssh time-out 30
ip ssh authentication-retries 5
ip ssh version 2
!
crypto isakmp policy 1
encr aes 256
authentication pre-share

```

		Охріменко. Д.С.			Житомирська політехніка 21.123.15.000	Арк.
		Єфіменко А.А.				147
Змн.	Арк.	№ докум.	Підпис	Дата		

```

lifetime 86000
crypto isakmp key R1R7 address 183.3.15.1
crypto isakmp key R2R7 address 184.3.15.1
crypto isakmp key R3R7 address 188.3.15.1
crypto isakmp key R6R7 address 190.3.15.2
crypto isakmp key R7R8 address 194.3.15.1
!
crypto ipsec transform-set TRANSF esp-aes 256
!
crypto map MAP 17 ipsec-isakmp
description IPSEC to 183.3.15.1
set peer 183.3.15.1
set transform-set TRANSF
match address 104
crypto map MAP 27 ipsec-isakmp
description IPSEC to 184.3.15.1
set peer 184.3.15.1
set transform-set TRANSF
match address 108
crypto map MAP 37 ipsec-isakmp
description IPSEC to 188.3.15.1
set peer 188.3.15.1
set transform-set TRANSF
match address 111
crypto map MAP 67 ipsec-isakmp
description IPSEC to 190.3.15.2
set peer 190.3.15.2
set transform-set TRANSF
match address 113
crypto map MAP 78 ipsec-isakmp
description IPSEC to 194.3.15.1
set peer 194.3.15.1
set transform-set TRANSF
match address 115
!
interface Loopback77
ip address 77.77.77.77 255.255.255.0
!
interface Tunnel17
ip address 104.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 193.3.15.1
tunnel destination 183.3.15.1
!
interface Tunnel27
ip address 108.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 193.3.15.1
tunnel destination 184.3.15.1
!

```

```

group 2
lifetime 86000
crypto isakmp key R1R8 address 183.3.15.1
crypto isakmp key R2R8 address 184.3.15.1
crypto isakmp key R3R8 address 188.3.15.1
crypto isakmp key R6R8 address 190.3.15.2
crypto isakmp key R7R8 address 193.3.15.1
!
crypto ipsec transform-set TRANSF esp-aes 256
!
crypto map MAP 18 ipsec-isakmp
description IPSEC to 183.3.15.1
set peer 183.3.15.1
set transform-set TRANSF
match address 105
crypto map MAP 28 ipsec-isakmp
description IPSEC to 184.3.15.1
set peer 184.3.15.1
set transform-set TRANSF
match address 109
crypto map MAP 38 ipsec-isakmp
description IPSEC to 188.3.15.1
set peer 188.3.15.1
set transform-set TRANSF
match address 112
crypto map MAP 68 ipsec-isakmp
description IPSEC to 190.3.15.2
set peer 190.3.15.2
set transform-set TRANSF
match address 114
crypto map MAP 78 ipsec-isakmp
description IPSEC to 193.3.15.1
set peer 193.3.15.1
set transform-set TRANSF
match address 115
!
interface Loopback88
ip address 88.88.88.88 255.255.255.0
!
interface Tunnel18
ip address 105.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 194.3.15.1
tunnel destination 183.3.15.1
!
interface Tunnel28
ip address 109.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 194.3.15.1
tunnel destination 184.3.15.1

```

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				148
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Tunnel37
ip address 111.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 193.3.15.1
tunnel destination 188.3.15.1
!
interface Tunnel67
ip address 113.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 193.3.15.1
tunnel destination 190.3.15.2
!
interface Tunnel78
ip address 115.3.15.1 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 193.3.15.1
tunnel destination 194.3.15.1
!
interface FastEthernet0/0
description LINK_TO_LAN_P
ip address 193.3.15.1 255.255.255.248
duplex auto
speed auto
crypto map MAP
!
interface FastEthernet0/1
description LINK_TO_LAN_N
ip address 192.3.15.1 255.255.255.240
duplex auto
speed auto
!
interface Vlan1
no ip address
!
!
router eigrp 1
network 77.77.77.0 0.0.0.255
network 193.3.15.0 0.0.0.7
no auto-summary
!
router ospf 1
log-adjacency-changes
network 104.3.15.0 0.0.0.255 area 0
network 108.3.15.0 0.0.0.255 area 0
network 111.3.15.0 0.0.0.255 area 0
network 113.3.15.0 0.0.0.255 area 0
network 115.3.15.0 0.0.0.255 area 0
network 192.3.15.0 0.0.0.15 area 1
!

```

```

!
interface Tunnel38
ip address 112.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 194.3.15.1
tunnel destination 188.3.15.1
!
interface Tunnel68
ip address 114.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 194.3.15.1
tunnel destination 190.3.15.2
!
interface Tunnel78
ip address 115.3.15.2 255.255.255.0
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 194.3.15.1
tunnel destination 193.3.15.1
!
interface FastEthernet0/0
description LINK_TO_LAN_R
ip address 194.3.15.1 255.255.255.248
duplex auto
speed auto
crypto map MAP
!
interface FastEthernet0/1
description LINK_TO_LAN_S
ip address 195.3.15.1 255.255.255.240
duplex auto
speed auto
!
interface Vlan1
no ip address
!
!
router eigrp 1
network 88.88.88.0 0.0.0.255
network 194.3.15.0 0.0.0.7
no auto-summary
!
router ospf 1
log-adjacency-changes
network 105.3.15.0 0.0.0.255 area 0
network 109.3.15.0 0.0.0.255 area 0
network 112.3.15.0 0.0.0.255 area 0
network 114.3.15.0 0.0.0.255 area 0
network 115.3.15.0 0.0.0.255 area 0
network 195.3.15.0 0.0.0.15 area 1
!

```

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				149
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip http server
no ip http secure-server
ip forward-protocol nd
!
access-list 104 permit gre 193.3.15.0 0.0.0.7
183.3.15.0 0.0.0.7 log
access-list 104 permit udp 193.3.15.0 0.0.0.7 eq
isakmp 183.3.15.0 0.0.0.7 log
access-list 104 deny ip any any log
access-list 108 permit gre 193.3.15.0 0.0.0.7
184.3.15.0 0.0.0.7 log
access-list 108 permit udp 193.3.15.0 0.0.0.7 eq
isakmp 184.3.15.0 0.0.0.7 log
access-list 108 deny ip any any log
access-list 111 permit gre 193.3.15.0 0.0.0.7
188.3.15.0 0.0.0.3 log
access-list 111 permit udp 193.3.15.0 0.0.0.7 eq
isakmp 188.3.15.0 0.0.0.3 log
access-list 111 deny ip any any log
access-list 113 permit gre 193.3.15.0 0.0.0.7
190.3.15.0 0.0.0.3 log
access-list 113 permit udp 193.3.15.0 0.0.0.7 eq
isakmp 190.3.15.0 0.0.0.3 log
access-list 113 deny ip any any log
access-list 115 permit gre 193.3.15.0 0.0.0.7
194.3.15.0 0.0.0.7 log
access-list 115 permit udp 193.3.15.0 0.0.0.7 eq
isakmp 194.3.15.0 0.0.0.7 log
access-list 115 deny ip any any log
no cdp log mismatch duplex
!
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
logging synchronous
login local
transport input ssh
transport output ssh
!
end

```

```

no ip http server
no ip http secure-server
ip forward-protocol nd
!
access-list 105 permit gre 194.3.15.0 0.0.0.7
183.3.15.0 0.0.0.7 log
access-list 105 permit udp 194.3.15.0 0.0.0.7 eq
isakmp 183.3.15.0 0.0.0.7 log
access-list 105 deny ip any any log
access-list 109 permit gre 194.3.15.0 0.0.0.7
184.3.15.0 0.0.0.7 log
access-list 109 permit udp 194.3.15.0 0.0.0.7 eq
isakmp 184.3.15.0 0.0.0.7 log
access-list 109 deny ip any any log
access-list 112 permit gre 194.3.15.0 0.0.0.7
188.3.15.0 0.0.0.3 log
access-list 112 permit udp 194.3.15.0 0.0.0.7 eq
isakmp 188.3.15.0 0.0.0.3 log
access-list 112 deny ip any any log
access-list 114 permit gre 194.3.15.0 0.0.0.7
190.3.15.0 0.0.0.3 log
access-list 114 permit udp 194.3.15.0 0.0.0.7 eq
isakmp 190.3.15.0 0.0.0.3 log
access-list 114 deny ip any any log
access-list 115 permit gre 194.3.15.0 0.0.0.7
193.3.15.0 0.0.0.3 log
access-list 115 permit udp 194.3.15.0 0.0.0.7 eq
isakmp 193.3.15.0 0.0.0.3 log
access-list 115 deny ip any any log
no cdp log mismatch duplex
!
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
logging synchronous
login local
transport input ssh
transport output ssh
!
end

```

		Охріменко Д.С.			Житомирська політехника 21.123.15.000	Арк.
		Єфіменко А.А.				150
Змн.	Арк.	№ докум.	Підпис	Дата		