**ВІДЗИВ НАУКОВОГО КЕРІВНИКА НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ**

**Студента Куліша Вадима Віталійовича**
**представлену на здобуття освітнього ступеня бакалавр**
**зі спеціальності 123 «Комп'ютерна інженерія»**

1. Робота виконана на тему „Проект мережі організації на базі технологій DMVPN та BGP".

2. Актуальність роботи зумовлена потребою у розробці та впровадженні у практику діяльності організації захищених засобів комунікацій між віддаленими підрозділами.

3. Основний зміст пояснювальної записки роботи викладено на 72 сторінках тексту. Записка містить 2 таблиці, 31 ілюстрацію, 3 додатки. Список використаних літературних джерел налічує 30 найменувань. Невід'ємною складовою роботи є реалізований у віртуальному середовищі моделювання EVE-ng проект мережі на базі обладнання фірми Cisco.

4. Пояснювальна записка складається з реферату, вступу, трьох розділів основного тексту, висновків, списку використаної літератури, додатків.

Розділ 1 присвячений аналізу загальних принципів побудови приватних віртуальних мереж, аналізу технологій та протоколів, які використовуються при побудові мереж DMVPN зокрема, у розділі розглянуто: питання тунелювання у віртуальних приватних мережах, засоби підтримки безпеки VPN, рівневу організацію захищених каналів, класифікацію віртуальних приватних мереж, теоретичні аспекти протоколів і технологій GRE, BGP, IPsec, NHRP. На основі цих технологій визначені особливості побудови, переваги та недоліки мереж DMVPN.

Розділ 2 присвячений питанням проектування комп'ютерної мережі організації, зокрема, у ньому здійснено проектування фізичної топології мережі, визначені ролі для всіх вузлів, розроблено схему адресації пристроїв мережі, проведено вибір обладнання, розроблено політику інформаційної безпеки.

Розділ 3 присвячений питанням базового налагодження пристроїв мережі та питанням налагодження технології пристроїв DMVPN. Також у цьому розділі здійснено перевірку функціоналу мережі DMVPN, проведено діагностування та тестування мережі на відмовостійкість.

5. Висновки містять сумарні результати проведеної роботи.

6. Список використаних літературних джерел має достатній для даного виду робіт обсяг, є правильно оформленим та повністю опрацьованим у ході виконання роботи.

7. Додатки містять змодельовану схему мережі, технічні характеристики мережевого обладнання, лістинги конфігураційних файлів налагоджених пристроїв.

8. Таблиці та ілюстрації оформлені якісно, є інформативними та наведені у відповідних місцях роботи.

9. Якість оформлення роботи є високою.

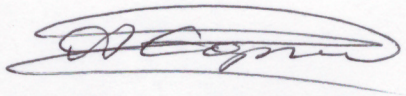
10. Виявлені на етапі попереднього захисту недоліки оформлення пояснювальної записки та презентації усунені. Рекомендації стосовно покращення проекту враховані та впроваджені.

11. Ставлення студента до виконання випускної кваліфікаційної роботи – дуже відповідальне. Глибина аналізу, дослідження проблем, проведення налагоджень пристроїв, формування висновків є надзвичайно ґрунтовними. Студентом сформовано перспективний план подальших досліджень.

12. У цілому при написанні випускної кваліфікаційної роботи студент Куліш В. В. виявив здібності до оволодіння знаннями, уміннями і навичками з таких дисциплін, як «Теорія систем і системний аналіз», «Операційні системи», «Комп'ютерні мережі», «Захист інформації в інформаційно-комунікаційних системах», «Адміністрування комп'ютерних систем та мереж». Також студент Куліш В.В. показав вміння підібрати необхідну літературу та інші інформаційні джерела, проаналізувати їх, виконати постановку задачі на розробку, розробити проект захищеної мережі, обрати відповідний інструментарій, створити закінчений цілісний продукт (у вигляді змодельованого проекту) і оформити свої розробки та напрацювання як випускну кваліфікаційну роботу.

Випускна кваліфікаційна робота студента Куліша В.В. написана на високому рівні та може бути допущена до захисту в Екзаменаційній комісії.

Пропонована оцінка – «відмінно».

Науковий керівник
к.т.н., завідувач кафедри КІ та КБ  А.А. Єфіменко
10 червня 2020 року

**РЕЦЕНЗІЯ**
**на кваліфікаційну роботу**
**студента 4 курсу групи КІ-2 спеціальності 123 «Комп'ютерна інженерія»**
**факультету інформаційно-комп'ютерних технологій**
**Державного університету «Житомирська політехніка»**
**Куліша Вадима Віталійовича**
**на тему: „Проект мережі організації на базі технологій DMVPN та BGP"**

Кваліфікаційна робота студента Куліша В. В. „Проект мережі організації на базі технологій DMVPN та BGP" присвячена актуальній тематиці – проблемі організації безпечного обміну інформацією між територіально рознесеними підрозділами великої організації на базі технології DMVPN та протоколу маршрутизації BGP.

Робота містить реалізований у середовищі моделювання EVE-ng проект мережі на базі обладнання фірми Cisco та пояснювальну записку наступного складу: вступ, три розділи основного тексту, висновки, список використаної літератури, три додатки.

У першому розділі проаналізовано питання принципів побудови VPN, а також технологій, протоколів, які використовуються при побудові мереж DMVPN. Зокрема, у розділі проаналізовано та визначено переваги та недоліки наступних технологій та протоколів: тунелювання у VPN, засоби підтримки безпеки VPN, GRE, BGP, IPsec, NHRP. На основі проведеного аналізу окремих складових визначено особливості побудови, переваги та недоліки мереж DMVPN.

У другому розділі пояснювальної записки розглянуті питання проектування комп'ютерної мережі, зокрема, у ньому здійснено проектування фізичної топології мережі, визначені ролі для всіх хостів та можливі топології VPN, розроблено схему IP-адресації мережі, проведено вибір обладнання, розроблено політику інформаційної безпеки.

У третьому розділі пояснювальної записки розглянуто особливості базового налагодження пристроїв мережі та питання налагодження пристроїв технології DMVPN. Також у цьому розділі здійснено перевірку функціоналу побудованої мережі DMVPN, проведено діагностування та тестування мережі на відмовостійкість.

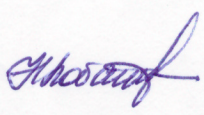
Зміст роботи відповідає поставленому завданню. У цілому кваліфікаційна робота виконана на високому рівні. Тема роботи розкрита повністю. Студентом продемонстровані ґрунтовні фахові компетентності, що отримані як під час навчання, так і у процесі виконання роботи. Матеріал пояснювальної записки викладено логічно, науково і технічно грамотно. Ілюстративний матеріал (рисунки, таблиці), що наведений у роботі, оформлений якісно і наведений у відповідних місцях. Оформлення роботи відповідає вимогам стандартів. Функціонал реалізованого у середовищі моделювання Eve-ng проекту мережі відповідає заявленому.

Позитивною стороною є те, що отримані результати мають практичну цінність – відпрацьована політика та сценарії налагодження мережі організації на базі технологій DMVPN та BGP з незначними модифікаціями можуть застосовуватися при налагодженні реальних пристроїв та у освітньому процесі при вивченні відповідних тем студентами спеціальностей 123 «Комп'ютерна інженерія» та 125 «Кібербезпека». Робота має перспективи подальшого розвитку в контексті взаємодії з обладнанням інших виробників та впровадженням нових елементів функціоналу технологій. Недоліками роботи є наступні: наявність деяких відхилень від вимог щодо оформлення пояснювальної записки. Зазначені недоліки у цілому не впливають на високу якість і актуальність роботи.

У цілому кваліфікаційна робота студента Куліша В. В. „Проект підсистеми захисту периметру мережі на базі обладнання Cisco" відповідає вимогам рівня вищої освіти «бакалавр» спеціальності 123 «Комп'ютерна інженерія» і рекомендується до захисту в ЕК.

Пропонована оцінка роботи – «відмінно».

Рецензент,
декан факультету
інформаційно-комп'ютерних технологій,
к.т.н., доцент
15 червня 2020 р.



Н.М. Лобанчикова

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 мережі організації на базі технологій DMVPN та BGP»

Виконав студент 4-го курсу, групи КІ-2
спеціальності 123 «Комп’ютерна інженерія»
_____ Куліш В.В.
Керівник, завідувач кафедри КІ та КБ, к.т.н.
_____ Єфіменко А. А.
Рецензент, декан ФІКТ, к.т.н., доцент
_____ Лобанчикова Н. М.

Житомир 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки
Єфіменко А. А.
«06» квітня 2020 р.

**ЗАВДАННЯ**
на випускну кваліфікаційну роботу

Студента **Куліша Вадима Віталійович**

Тема роботи: **Проект мережі організації на базі технологій DMVPN та BGP**
затверджена Наказом по університету від **«06» квітня 2020 р. № 98с**
Термін здачі студентом закінченої роботи – **1 червня 2020 р.**
Вихідні дані для роботи:

1. Фізична топологія мережі
2. Маршрутизатори Cisco 7200
3. Комутатори Cisco 2960
4. Операційна система Cisco IOS
5. Емулятор віртуального мережевого середовища EVE-ng

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

| Розділ | Консультант | Підпис, дата | |
|---|---|---|---|
| | | Завдання видав | Завдання прийняв |
| 1 | Єфіменко А. А. | 06.04.20 | 06.04.20 |
| 2 | Єфіменко А. А. | 20.04.20 | 20.04.20 |
| 3 | Єфіменко А. А. | 11.05.20 | 11.05.20 |

Керівник _____ Єфіменко А. А.

**Календарний план**

| № з/п | Назва етапів випускної кваліфікаційної роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Постановка завдання | 6 квітня 2020 – 7 квітня 2020 | Виконано |
| 2 | Пошук, огляд та аналіз літературних джерел щодо базових понять VPN | 8 квітня 2020 – 11 квітня 2020 | Виконано |
| 3 | Аналіз технологій NHRP, mGRE, IPsec, BGP | 12 квітня 2020 – 16 квітня 2020 | Виконано |
| 4 | Аналіз можливостей технології DMVPN, її переваг та недоліків | 17 квітня 2020 – 19 квітня 2020 | Виконано |
| 5 | Розробка проекту мережі та його фізичної топології | 20 квітня 2020 – 24 квітня 2020 | Виконано |
| 6 | Розробка параметрів адресації мережі | 25 квітня 2020 – 30 квітня 2020 | Виконано |
| 7 | Розробка політик безпеки | 1 травня 2020 – 4 травня 2020 | Виконано |
| 8 | Базове налагодження пристроїв мережі | 5 травня 2020 – 9 травня 2020 | Виконано |
| 9 | Налагодження аспектів технології DMVPN | 10 травня 2020 – 13 травня 2020 | Виконано |
| 10 | Діагностування та тестування налаштувань | 14 травня 2020 – 18 травня 2020 | Виконано |
| 11 | Аналіз результатів тестування | 19 травня 2020 – 22 травня 2020 | Виконано |
| 12 | Визначення переваг та недоліків мережі | 23 травня 2020 – 24 травня 2020 | Виконано |
| 13 | Написання пояснювальної записки | 25 травня 2020 – 29 травня 2020 | Виконано |
| 14 | Підготовка презентації та виступу | 30 травня 2020 – 31 травня 2020 | Виконано |
| 15 | Отримання відгуку керівника та рецензії на кваліфікаційну роботу | 4 червня 2020 – 8 червня 2020 | Виконано |
| 16 | Захист | 20 червня 2020 | Виконано |

Студент _____ Куліш В. В.

Керівник _____ Єфіменко А. А.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ ..... 7
ВСТУП ..... 8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО VPN, ПРОТОКОЛІВ DMVPN, GRE, NHRP, BGP, IPSEC ..... 9
1.1 Теоретичні відомості про технологію VPN ..... 9
1.2 Теоретичні аспекти протоколів та технологій GRE, NHRP, BGP, IPsec ..... 22
1.3 Загальна характеристика технології DMVPN ..... 33
РОЗДІЛ 2. ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА ПОЛІТИК БЕЗПЕКИ ..... 36
2.1 Проект мережі та його фізична топологія ..... 36
2.2 Розробка параметрів адресації ..... 45
2.3 Розробка політик безпеки ..... 51
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ОБЛАДНАННЯ МЕРЕЖІ, ЇЇ ДІАГНОСТИКА ТА ТЕСТУВАННЯ ..... 55
3.1 Базове налагодження мережі ..... 55
3.2 Налагодження аспектів технології DMVPN ..... 59
3.3 Діагностування та тестування налаштувань ..... 64
ВИСНОВКИ ..... 74
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ..... 75
ДОДАТКИ ..... 78

# РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи на тему «Організація корпоративної мережі, побудованої з використанням технології DMVPN та BGP» складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаної літератури.

Текстова частина викладена на 77 сторінках друкованого тексту.

Пояснювальна записка має 31 сторінок додатків. Список використаних джерел містить 30 найменувань і займає три сторінки. В роботі наведено 31 рисунок. Загальний обсяг складає - 109 сторінок.

У першому розділі було обґрунтовано загальні поняття пов’язані з роботою VPN, їх використання, реалізації та загальні поняття про протоколи і технології DMVPN, BGP, IPsec, GRE, NHRP.

У другому розділі було спроектвано проект мережі, визначено відповідне обладнання, розроблена фізична топологія та обраховані параметри адресації. Визначені основні концепції політик безпеки та сформовані свої власні.

У третьому розділі було проведено налаштування мережі, також було продемонстровано базові налаштування на прикладі маршрутизатора з мережі, був перевірений зв’язок між локальними зонами. При діагностиці та тестуванні визначені переваги та недоліки мережі.

Висновок містить в собі результат виконання кожного розділу, результат налаштування комп’ютерної мережі та кваліфікаційної роботи.

У додатку представлений лістинг налаштування кожного приладу.

КЛЮЧОВІ СЛОВА: ЗАХИЩЕНА КОМП’ЮТЕРНА МЕРЕЖА ОРГАНІЗАЦІЇ, ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА, DMVPN, BGP

# ABSTRACT

Explanatory note to the qualification work on "Organization of a corporate network built on the use of DMVPN and BGP technology" consists of a list of conditional ABBREVIATIONS, introduction, three sections, conclusions, list of references.

Text part of the presentation on 77 pages of printed text.

The explanatory note has 31 pages of Appendices. The list of used sources contains 30 items and takes up three pages. The paper shows 31 figures. TOTAL VOLUME is - 109 pages.

In the First section the GENERAL Concepts connected with VPN work, their use, implementations and GENERAL Concepts about protocols and technologies DMVPN, BGP, IPsec, GRE, NHRP were substantiated.

In another section, a network design was designed, appropriate equipment was identified, a physical topology was developed, and addressing parameters were calculated. You have defined the basic Concepts of security policies and formed your own.

In the third section, the network settings were performed, as well as the basic settings were demonstrated on the example of a router from the network, the connection between the local zones was tested. The advantages and disadvantages of the network are identified during diagnostics and testing.

The conclusion contains the result of each section, the result of setting up a computer network and qualifying work.

In the Appendices submissions listing the skin fitting settings.

KEYWORDS: PROTECTED COMPUTER NETWORK OF ORGANIZATION, VIRTUAL PRIVATE NETWORK, DMVPN, BGP

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ ..... 7
ВСТУП ..... 8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО VPN, ПРОТОКОЛІВ DMVPN, GRE, NHRP, BGP, IPSEC ..... 9
1.1 Теоретичні відомості про технологію VPN ..... 9
1.2 Теоретичні аспекти протоколів та технологій GRE, NHRP, BGP, IPsec ..... 22
1.3 Загальна характеристика технології DMVPN ..... 33
РОЗДІЛ 2. ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА ПОЛІТИК БЕЗПЕКИ ..... 36
2.1 Проект мережі та його фізична топологія ..... 36
2.2 Розробка параметрів адресації ..... 45
2.3 Розробка політик безпеки ..... 51
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ОБЛАДНАННЯ МЕРЕЖІ, ЇЇ ДІАГНОСТИКА ТА ТЕСТУВАННЯ ..... 55
3.1 Базове налагодження мережі ..... 55
3.2 Налагодження аспектів технології DMVPN ..... 59
3.3 Діагностування та тестування налаштувань ..... 64
ВИСНОВКИ ..... 74
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ..... 75
ДОДАТКИ ..... 78

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЛКМ – Локальна комп’ютерна мережа

VPN – Virtual Private Network

OSI - Open Systems Interconnection model

IPX - Internetwork Packet Exchange

ПК – Персональний комп’ютер

ISO - International Standards Organization

IP – Internet Protocol

GRE - Generic Routing Encapsulation

NHRP – Next Hop Resolution Protocol

IPsec – IP security

IKE - Internet Key Exchange

L2F - Layer 2 forwarding

PPTP - Point-to-Point Tunneling Protocol

L2TP - Layer 2 Tunneling Protocol

DMVPN – Dynamic Multipoint Virtual Private Network

TCP – Transmission Control Protocol

UDP - User Datagram Protocol

ISP - Internet Service Provider

EGP – Exterior Gateway Protocol

IGP - Interior Gateway Protocol

mGRE – Multipoint Generic Routing Encapsulation

ATMARP - Asynchronous Transfer Mode Address Resolution Protocol

NBMA - Non-Broadcast Multiple Access Network

NHS – Next-Hop server

BGP - Border Gateway Protocol

ASN - Autonomous System Number

DHCP - Dynamic Host Configuration Protocol

SSH - Secure Shell

# ВСТУП

Складно сьогодні знайти сферу діяльності людини, яка б не потребувала використання комп'ютерних мереж. Науково-дослідні, проектно-конструкторські, виробничі, торговельні, фінансові, консультаційні, освітні та адміністративні установи; міжнародні корпорації та малий бізнес, – усі ці та багато інших підприємств для своєї діяльності потребують надійної та ефективної роботи комп'ютерних мереж. Своєю чергою, комп'ютерна мережа, навіть локальна, є надзвичайно складною системою. Розробники мережевого обладнання та програмного забезпечення, а також мережеві адміністратори докладають багато зусиль, щоб зробити роботу в мережі легкою, налаштування прозорим та дати змогу комфортно працювати з мережевими технологіями користувачеві з мінімальним рівнем підготовки. Проте, розглянувши за допомогою спеціального інструментарію роботу мережі зсередини, можна пересвідчитись у складності та багатогранності процесів, що забезпечують її працездатність. Відповідно проектування, впровадження та підтримка комп'ютерних мереж потребує спеціальних знань та практичної підготовки.

Ситуація ускладнюється тим, що існує велике розмаїття мережевого обладнання та протоколів, а самі мережеві технології змінюються та вдосконалюються надзвичайно швидко. Буквально щодня можна знайти повідомлення чи то про появу мережевих пристроїв з покращеними характеристиками, чи то про розширення можливостей певних протоколів чи появу нових версій інструментарію для моніторингу мереж та їх дослідження. Щоб вірно скористатись цими несистематизованими фактами, необхідно мати знання, що уможливлюють сприймати мережу не як сукупність розрізнених об'єктів, процесів та даних, а як систему з певним набором підсистем і елементів, структурою зв'язків та правил їх взаємодії.

Дослідженням побудови ефективних комп'ютерних мереж людство займається досить довго. Принципи налаштування, та використання вірних протоколів є ключовим розумінням на сьогодні. Тому, метою цієї кваліфікаційної роботи є побудова мережі організації з використанням технологій BGP та DMVPN.

# РОЗДІЛ 1. ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО VPN, ПРОТОКОЛІВ DMVPN, GRE, NHRP, BGP, IPSEC

## 1.1 Теоретичні відомості про технологію VPN

### 1.1.1 Визначення терміну, цілі та задачі

Завдяки розвитку криптографічних технологій з'явився спосіб вирішити завдання захисту інформації в сучасній мережевий середовищі за рахунок використання технології захищених віртуальних приватних мереж (Virtual Private Network - VPN), які можуть надійно шифрувати інформацію, передану по відкритим мереж, включаючи Internet.

VPN (англ. Virtual Private Network - віртуальна приватна мережа) - логічна мережа, створена поверх іншої мережі, наприклад Internet [18]. Відкрита мережа може служити основою для одночасного співіснування безлічі віртуальних мереж, кількість яких визначається пропускною здатністю відкритих каналів зв'язку. Незважаючи на те, що комунікації здійснюються по публічним мережам з використанням небезпечних протоколів, за рахунок шифрування створюються закриті від сторонніх канали обміну інформацією. VPN дозволяє об'єднати, наприклад, кілька офісів організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

В своїй суті VPN володіє багатьма властивостями виділеної лінії, проте розгортається вона в межах загальнодоступної мережі, наприклад Інтернету.
Реалізація віртуальної приватної мережі на практиці виглядає наступним чином. У локальної обчислювальної мережі офісу фірми встановлюється сервер VPN. Віддалений користувач (або маршрутизатор, якщо здійснюється з'єднання двох офісів) з використанням клієнтського програмного забезпечення VPN ініціює процедуру з'єднання з сервером. Відбувається аутентифікація користувача - перша фаза встановлення VPN-з'єднання. У разі підтвердження повноважень настає друга фаза - між клієнтом і сервером виконується узгодження деталей забезпечення безпеки

з'єднання. Після цього організовується VPN-з'єднання, що забезпечує обмін інформацією між клієнтом і сервером у формі, коли кожен пакет з даними проходить через процедури шифрування / дешифрування і перевірки цілісності - аутентифікації даних.

Мета VPN-технологій полягає в максимальному ступені відособлення потоків даних одного підприємства від потоків даних всіх інших користувачів публічної мережі. Відособленість повинна бути забезпечена відносно параметрів пропускної здатності потоків і в конфіденційності переданих даних. Таким чином, основними завданнями технологій VPN є забезпечення в публічній мережі гарантованої якості обслуговування для потоків користувацьких даних, а також захист їх від можливого розкриття корпоративних даних або їх руйнування.

VPN-технології забезпечують:

- захист (конфіденційність, автентичність і цілісність) переданої через мережі інформації;
- захист внутрішніх сегментів мережі від несанкціонованого доступу з боку загальнодоступних мереж;
- контроль доступу в захищений периметр мережі;
- приховування внутрішньої структури сегментів мережі;
- ідентифікацію та аутентифікацію користувачів мережевих об'єктів
- централізоване управління політикою корпоративної мережевої безпеки і VPN-мережі;
- криптографічний захист даних, що передаються по каналах;
- зв'язку мереж загального користування між захищеними сегментами мережі;
- безпечний доступ користувачів VPN до ресурсів мереж загального користування.

### 1.1.2 Тунелювання у віртуальних приватних мережах

Кожна віртуальна захищена мережа VPN формується шляхом побудови віртуальних захищених каналів зв'язку, що створюються на базі відкритих каналів зв'язку загальнодоступної мережі. Ці віртуальні захищені канали зв'язку називаються тунелями VPN.

При тунелюванні пакет протоколу нижчого рівня поміщується в поле даних пакета протоколу більш високого або такого ж рівня. Наприклад, при тунелюванні кадр Ethernet може бути розміщений в пакеті IP, а пакет IPX - в пакеті IP. Можливий і такий варіант: пакет IP розміщується в пакеті IP.

Тунель створюється двома граничними пристроями, які розміщуються в точках входу в публічну мережу. Ініціатор тунелю інкапсулює пакети локальної мережі (в тому числі пакети немаршрутизованих протоколів) в IP-пакети, що містять в заголовку адреси ініціатора і термінатора тунелю. Термінатор тунелю витягує вихідний пакет. Природно, при подібній передачі потрібно вирішувати проблему конфіденційності і цілісності даних, що не забезпечується простим туннелюванням. Конфіденційність інформації, переданої корпоративної інформації досягається шифруванням (алгоритм однаковий на обох кінцях тунелю).

Особливістю тунелювання є те, що ця технологія дозволяє зашифрувати вихідний пакет цілком, разом із заголовком, а не тільки його поле даних. Вихідний пакет зашифровують повністю, разом із заголовком, і цей зашифрований пакет поміщають в інший, зовнішній пакет з відкритим заголовком. Для транспортування даних по "небезпечній" мережі використовуються відкриті поля заголовка зовнішнього пакета, а при прибутті зовнішнього пакета в кінцеву точку захищеного каналу з нього витягують внутрішній пакет, розшифровують і використовують його заголовок для подальшої передачі вже у відкритому вигляді по мережі, яка потребує захисту. При цьому для зовнішніх пакетів використовуються адреси граничних маршрутизаторів, встановлених в цих двох точках, а внутрішні адреси кінцевих вузлів містяться у внутрішніх пакетах в захищеному вигляді[18](рис. 1.1)

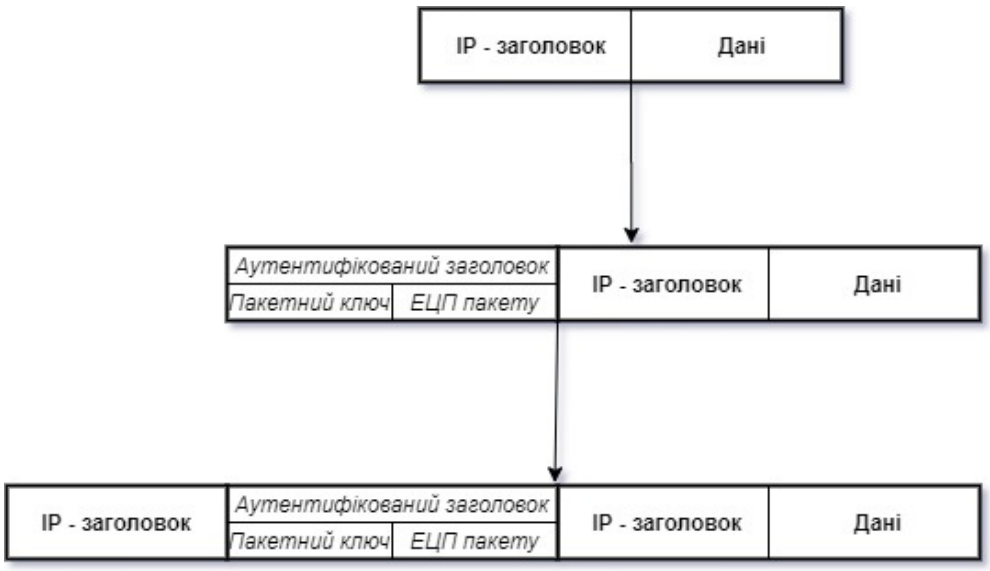



Рисунок 1.1 – Процедура тунелювання пакетів

Тунелювання може бути використано для захисту не тільки конфіденційності вмісту пакета, але і його цілісності та автентичності, при цьому електронний цифровий підпис можна поширити на все поля пакета. Разом з приховуванням мережевої структури між двома точками, тунелювання може також запобігти можливому конфлікту адрес між двома локальними мережами. При створенні локальної мережі, не пов'язаної з Internet, компанія може використовувати будь-які IP-адреси для своїх мережевих пристроїв і комп'ютерів. При об'єднанні раніше ізольованих мереж ці адреси можуть почати конфліктувати один з одним і з адресами, які вже використовуються в Internet. Інкапсуляція пакетів вирішує цю проблему, оскільки дозволяє приховати початкові адреси і додати нові, унікальні в просторі IP-адрес Internet, які потім використовуються для пересилання даних по розділяються мереж. Сюди ж входить завдання налаштування IP-адреси та інших параметрів для мобільних користувачів, що підключаються до локальної мережі.

Механізм тунелювання широко застосовується в різних протоколах формування захищеного каналу. Зазвичай тунель створюється тільки на ділянці відкритої мережі, де існує загроза порушення конфіденційності та цілісності даних, наприклад між точкою входу у відкритий Інтернет і точкою входу в корпоративну мережу.

При цьому для зовнішніх пакетів використовуються адреси граничних маршрутизаторів, встановлених в цих двох точках, а внутрішні адреси кінцевих вузлів містяться у внутрішніх вихідних пакетах в захищеному вигляді.

Таким чином мережа тунелі можуть VPN з'єднати центральний офіс, офіси філій, офіси бізнес-партнерів і віддалених користувачів і безпечно передавати інформацію через Інтернет.

### 1.1.3 Засоби підтримки безпеки VPN

При побудові захищеної віртуальної мережі VPN першочергове значення має завдання забезпечення інформаційної безпеки. Згідно загальноприйнятим визначенням, під безпекою даних розуміють їх конфіденційність, цілісність і доступність. Що стосується завдання VPN критерії безпеки даних можуть бути визначені наступним чином:

- конфіденційність - гарантія того, що в процесі передачі даних по захищених каналах VPN ці дані можуть бути відомі тільки легальним відправнику і одержувачу;

- цілісність - гарантія збереження переданих даних під час проходження по захищеному каналу VPN. Будь-які спроби зміни, модіфіцікації, руйнування або створення нових даних будуть виявлені і стануть відомі легальним користувачам;

- доступність - гарантія того, що засоби, які виконують функції VPN, постійно доступні легальним користувачам. Доступність засобів VPN є комплексним показником, який залежить від надійності реалізації, якості обслуговування і ступеня захищеності самого засобу від зовнішніх атак.

Конфіденційність забезпечується за допомогою різних методів і алгоритмів симетричного і асиметричного шифрування. Цілісність переданих даних зазвичай досягається за допомогою різних варіантів технології електронного підпису, заснованих на асиметричних методах шифрування і односторонніх функціях [19].

Аутентифікація здійснюється на основі багаторазових і одноразових паролів, цифрових сертифікатів, смарт-карт, різних протоколів аутентифікації, забезпечує

встановлення VPN-з'єднання тільки між легальними користувачами і запобігає доступ до засобів VPN небажаних осіб.

Авторизація передбачає надання абонентам, які довели свою легальність (автентичність), різних видів обслуговування, зокрема різних способів шифрування їх трафіку. Авторизація та управління доступом часто реалізуються одними і тими ж засобами. Для забезпечення безпеки даних, що передаються в віртуальних захищених мережах повинні бути вирішені такі основні завдання мережевої безпеки:

- взаємна аутентифікація абонентів при встановленні з'єднання;
- забезпечення конфіденційності, цілісності та автентичності інформації, що передається;
- авторизація та управління доступом;
- безпеку периметра мережі і виявлення вторгнень;
- управління безпекою мережі.

### 1.1.4 Рівні захищених каналів

При побудові VPN однією з найбільш гострих є проблема сумісності. Кінцеві точки тунелю VPN повинні вивикористовувати одні і ті ж методи взаємної аутентифікації, шифрування даних і генерації секретних ключів. Природне рішення цієї проблеми - підтримка кожним VPN-пристроєм деякого набору стандартних технологій і протоколів захисту даних, щоб при встановленні захищеного з'єднання два вузла мережі в результаті переговорного процесу змогли знайти загальну технологію і загальний протокол. Особливо це важливо при організації екстрамережі, коли недостатньо прийняти якийсь стандарт захисту даних в рамках одного підприємства.

Важливою характеристикою стандартів захищеного каналу є рівень моделі взаємодії відкритих систем OSI, на якому працюють протоколи даного стандарту (рис. ). Модель OSI розроблена Міжнародною організацією зі стандартизації (International Standards Organization - ISO), визначає сім рівнів, на яких комп'ютерні

системи взаємодіють один з одним, починаючи з рівня фізичної середовища передачі даних і закінчуючи рівнем прикладних програм, що використовуються для комунікацій.




Рисунок 1.2 – Модель OSI та стека протоколів TCP/IP

Захищений канал можна побудувати на основі системних коштів, реалізованих на різних рівнях стека комунікаційних протоколів . Для порівняння (рисунок 1.2) наведено відповідність цих же протоколів стеку протоколів TCP / IP. Звичайно, можливий і такий варіант, коли додаток самостійно, без звернення до системних засобів, забезпечує конфіденційність і цілісність переданих їм даних. Але оскільки в цьому випадку від прикладного програміста потрібні додаткові витрати зусиль, такий варіант рідко зустрічається на практиці, хіба що для вирішення вельми специфічних завдань.

### 1.1.5 Класифікація VPN

Завдяки технології VPN багато компаній починають будувати свою стратегію з урахуванням використання Інтернету в якості головного засобу передачі інформації, причому навіть тієї, яка є вразливою або життєво важливою. Існують різні ознаки класифікації VPN. Найбільш часто використовуються:

- «робочий» рівень моделі OSI;
- архітектура технічного рішення VPN;
- спосіб технічної реалізації VPN

Класифікація VPN за «робочому» рівню моделі OSI представляє значний інтерес, оскільки від обраного рівня OSI багато в чому залежить функціональність реалізується VPN і її сумісність з додатками, а також з іншими засобами захисту. За ознакою «робочого» рівня моделі OSI розрізняють наступні групи VPN:

- VPN канального рівня;
- VPN мережевого рівня;
- VPN сеансового рівня.

Засоби VPN, які використовуються на канальному рівні моделі OSI, дозволяють забезпечити інкапсуляцію різних видів трафіку третього рівня (і вище) і побудова віртуальних тунелів типу «точка-точка» (від маршрутизатора до маршрутизатора або від персонального комп'ютера до шлюзу ЛВС)[27]. До цієї групи належать VPN-продукти, які використовують протоколи:

- L2F (Layer 2 forwarding)
- PPTP (Point-to-Point Tunneling Protocol),
- стандарт L2TP (Layer 2 Tunneling Protocol), розроблений спільно фірмами Cisco Systems і Microsoft.

VPN-продукти мережевого рівня виконують інкапсуляцію IP в IP. Одним з широко відомих протоколів на цьому рівні є протокол IPSec (IP Security), призначеним для аутентифікації, тунелювання і шифрування IP-пакетів. Стандартизований консорціумом Internet Engineering Task Force (IETF) протокол IPSec увібрав в себе всі кращі рішення щодо шифрування пакетів і повинен увійти в якості обов'язкового компонента в протокол IPv6. З протоколом IPSec пов'язаний протокол IKE (Internet Key Exchange), вирішальний завдання безпечного управління та обміну криптографічними ключами між віддаленими пристроями. Протокол IKE автоматизує обмін ключами і встановлює захищене з'єднання, тоді як IPSec шифрує і «підписує» пакети. Крім того, IKE дозволяє змінювати ключ для вже встановленого з'єднання, що підвищує конфіденційність переданої інформації.

VPN сеансового рівня використовують інший підхід під назвою «посередники каналів» (circuit proxy). Цей метод функціонує над транспортним рівнем і ре-

транслює трафік з захищеної мережі в загальнодоступну мережу Internet для кожного сокета окремо. (Сокет IP ідентифікується комбінацією TCP-з'єднання і конкретного порту або заданим портом UDP. Стек TCP / IP не має п'ятого - сеансового - рівня, однак орієнтовані на сокети операції часто називають операціями сеансового рівня.) Шифрування інформації, що передається між ініціатором і термінатором тунелю, часто здійснюється за допомогою захисту транспортного рівня TLS (Transport Layer Security). Для стандартизації аутентифицированного проходу через МЕ консорціум IETF визначив протокол під назвою SOCKS, і в даний час протокол SOCKS v.5 застосовується для стандартизованої реалізації посередників каналів.

За архітектуру технічного рішення прийнято виділяти три основних види віртуальних приватних мереж:

- внутрішньокорпоративні VPN (Intranet VPN);

- VPN з віддаленим доступом (Remote Access VPN);

- міжкорпоративні VPN (Extranet VPN).

Intranet VPN - призначені для забезпечення захищеного взаємодії між підрозділами всередині підприємства або між групою підприємств, об'єднаних корпоративними мережами зв'язку, включаючи виділені лінії. Вони будуються з використанням Internet або розділюваних мережевих інфраструктур, що надаються сервіс-провайдерами. Компанії досить відмовитися від використання дорогих виділених ліній, замінивши їх більш дешевим зв'язком через Internet. Це істотно скорочує витрати на використання смуги пропускання, оскільки в Internet відстань ніяк не впливає на вартість з'єднання [21].

Переваги Intranet VPN:

- застосування потужних криптографічних протоколів шифрування даних для захисту конфіденційної інформації;

- надійність функціонування при виконанні таких критичних додатків, як системи автоматизованого продажу і системи управління базами даних;

- гнучкість управління ефективним розміщенням швидко зростаючого числа нових користувачів, нових офісів і нових програмних додатків.

Побудова Intranet VPN, що використовує Internet, є самим рентабельним способом реалізації VPN-технології. Однак в Internet рівні сервісу взагалі не гарантуються. Компанії, яким потрібні гарантовані рівні сервісу, повинні розглянути можливість розгортання своїх VPN з використанням поділюваних мережевих інфраструктур, що надаються сервіс-провайдерами.

Remote Access VPN - призначені для забезпечення захищеного віддаленого доступу до корпоративних інформаційних ресурсів мобільним і / або віддаленим (home-office) співробітникам компанії. Такі мережі VPN дозволяють значно скоротити щомісячні витрати на використання комутованих і виділених ліній. Принцип їх роботи простий: користувачі встановлюють з'єднання з місцевої точкою доступу до глобальної мережі, після чого їх виклики тунелюють через Інтернет, що позбавляє від плати за міжміський і міжнародний зв'язок або виставлення рахунків власникам безкоштовних міжміських номерів; потім всі виклики концентруються на відповідних вузлах і передаються в корпоративні мережі. Переваги переходу від приватно керованих dial networks до Remote Access VPN:

- можливість використання місцевих dial-in numbers замість міжміських дозволяє значно знизити витрати на міжміські телекомунікації;

- ефективна система встановлення автентичності віддалених і мобільних користувачів забезпечує надійне проведення процедури аутентифікації;

- висока масштабованість і простота розгортання для нових користувачів, що додаються до неї;

- зосередження уваги компанії на основних корпоративних бізнес цілях замість відволікання на проблеми забезпечення роботи мережі.

Велика економія при використанні Remote Access VPN є чудовим способом для використання цієї технлогії, однак застосування відкритого Internet в якості об'єднуючої магістралі для транспорту чутливого корпоративного трафіку стає все більш масштабним, що робить механізми захисту інформації життєво важливими елементами даної технології.

Extranet VPN - призначені для забезпечення захищеного обміну інформацією зі стратегічними партнерами по бізнесу, постачальниками, великими замовниками,

користувачами, клієнтами і т.д. Extranet VPN забезпечує прямий доступ з мережі однієї компанії до мережі іншої компанії і тим самим сприяє підвищенню надійності зв'язку, підтримуваної в ході ділового співробітництва. Мережі Extranet VPN в цілому схожі на Intranet віртуальні приватні мережі з тією лише різницею, що проблема захисту інформації є для них більш гострою. Для Extranet VPN характерно використання стандартизованих VPN-продуктів, які гарантують здатність до взаємодії з різними VPN-рішеннями, які ділові партнери могли б застосовувати в своїх мережах. Коли кілька компаній приймають рішення працювати разом і відкривають один для одного свої мережі, вони повинні подбати про те, щоб їх нові партнери мали доступ тільки до певної інформації. При цьому конфіденційна інформація повинна бути надійно захищена від несанкціонованого використання. Саме тому в міжкорпоративних мережах велике значення надається контролю доступу з відкритої мережі за допомогою маршрутизатора за міжмережевого екрану. Важлива і аутентифікація користувачів, покликана гарантувати, що доступ до інформації отримують тільки ті, кому він дійсно дозволений. Разом з тим, розгорнута система захисту від несанкціонованого доступу не повинна привертати до себе уваги. З'єднання Extranet VPN розгортаються, використовуючи ті ж архітектуру і протоколи, які застосовуються при реалізації Intranet VPN і Remote Access VPN. Основна відмінність полягає в тому, що дозвіл доступу, яке дається користувачам Extranet VPN, пов'язане з мережею їх партнера. Іноді в окрему групу виділяють локальний варіант мережі VPN (Localnet VPN). Локальна мережа Localnet VPN забезпечує захист інформаційних потоків, що циркулюють всередині локальних мереж компанії (як правило, Центрального офісу), від несанкціонованого доступу з боку «надмірно цікавих» співробітників самої компанії. В даний час спостерігається тенденція до конвергенції різних способів реалізацій VPN.

Також розрізняють VPN за способом технічної реалізації.Конфігурація і характеристики віртуальної приватної мережі багато в чому визначаються типом застосовуваних VPN-пристроїв. За способом технічної реалізації розрізняють VPN на базі:

- маршрутизаторів;

- міжмережевих екранів;

- програмних рішень;

- спеціалізованих апаратних засобів

VPN на основі маршрутизаторів передбачає застосування маршрутизаторів для створення захищених каналів. Оскільки вся інформація, яка виходить із локальної мережі, проходить через маршрутизатор, то цілком природно покласти на нього і завдання шифрування. Приклад обладнання для VPN на маршрутизаторах - пристрої компанії Cisco Systems.

VPN на основі міжмережевих екранів дуже часто використовуються в загальнійпрактиці. Міжмережеві екрани в більшості виробників підтримують функції тунелювання і шифрування даних, наприклад продукт FireWall-1 компанії Check Point Software Technologies. При використанні МЕ на базі ПК потрібно пам'ятати, що подібне рішення підходить тільки для невеликих мереж з невеликим обсягом переданої інформації. Недоліками цього методу є висока вартість рішення в перерахунку на одне робоче місце і залежність продуктивності від апаратного забезпечення, на якому працює МЕ.

VPN-продукти, реалізовані програмним способом, з точки зору продуктивності поступаються спеціалізованим пристроям, однак володіють достатньою потужністю для реалізації VPN-мереж. Слід зазначити, що в разі віддаленого доступу вимоги до необхідної смузі пропускання невеликі. Тому чисто програмні продукти легко забезпечують продуктивність, достатню для віддаленого доступу. Безсумнівним достоїнством програмних продуктів є гнучкість і зручність в застосуванні, а також відносно невисока вартість.

Головна перевага VPN на основі спеціалізованих апаратних засобів - висока продуктивність, оскільки швидкодія обумовлено тим, що шифрування в них здійснюється спеціалізованими мікросхемами. Спеціалізовані VPN-пристрої забезпечують високий рівень безпеки, однак вони дуже дорого коштують.

Отже, технології VPN відіграють велике значення в побудові корпоративних мереж, тому можна виділити такі їх переваги:

- можливість захисту всієї корпоративної мережі від великих локальних мереж офісів до окремих робочих місць. Захист може бути поширений на всі ланки мережі від сегментів локальних мереж до комунікаційних каналів глобальних мереж, в тому числі виділених і комутованих ліній;

- масштабованість системи захисту, тобто для захисту об'єктів різної складності і продуктивності можна використовувати адекватні за рівнем складності, продуктивності і вартості програмні або програмно-апаратні засоби захисту;

- використання ресурсів відкритих мереж в якості окремих комунікаційних ланок корпоративної мережі; всі загрози, що виникають при використанні мереж загального користування, будуть компенсуватися засобами захисту інформації;

- забезпечення підконтрольності роботи мережі і достовірна ідентифікація всіх джерел інформації. При необхідності може бути забезпечена аутентифікація трафіку на рівні окремих користувачів;

- сегментація ІС і організація безпечної експлуатації системи, що обробляє інформацію різних рівнів конфіденційності, програмними і програмно-апаратними засобами захисту інформації.

Технологія VPN входить в число найважливіших технологій, які планують використовувати підприємства в найближчому майбутньому. Необхідність використання VPN очевидна. Інтернет не є безпечним місцем, це багато в чому «дикий захід» мереж, пристроїв, хороших і поганих користувачів. З'єднання піддаються ризику злому, веб-сайти можуть завантажити шкідливі програми, на персональні дані оголошено полювання і потік інформації все більше ускладнюється. Навіть в тих місцях, де Інтернет є відносно безпечним, Ви будете стикатися з обмеженнями, які блокують вільний потік інформації, починаючи від глобальних новин до найпопулярніших американських і британських телевізійних шоу.

Це означає, що віртуальні приватні мережі більш, ніж будь-коли, важливі для Інтернет-безпеки, а також вільного доступу до Інтернету. Технології VPN будуть розвиватися разом з Інтернетом, і чим швидше переваги VPN стануть відомі користувачам, тим більша кількість людей стане їх використовувати. Якщо Ви все ще не використовуєте VPN, немає ніяких підстав і жодної причини зволікати з цим.

## 1.2 Теоретичні аспекти протоколів та технологій GRE, NHRP, BGP, IPsec

### 1.2.1 Загальна характеристика протоколу GRE

GRE (англ. Generic Routing Encapsulation — загальна інкапсуляція маршрутів) — протокол тунелювання мережевих пакетів, розроблений компанією Cisco Systems [9]. Його основне призначення — інкапсуляція пакетів мережевого рівня мережевої моделі OSI в IP пакети. Номер протокола в IP — 47. Сам по собі протокол широко як сам по собі, так і разом з IPsec для створення тунелів.

Сам по собі GRE не забезпечує ніякої безпеки переданих даних - це site-to-site VPN тунель в чистому вигляді. Використовується зазвичай такий тунель, коли є специфічні завдання, пов'язані з маршрутизацією і немає вимог до безпеки. Не варто забувати, що чистий GRE тунель - не навантажує обладнання, а навантаження при шифруванні великого обсягу даних досить велике.

Протокол GRE інкапсулюється безпосередньо в IP, минаючи TCP або UDP, в IP пакеті є спеціальне поле «Protocol type», в якому міститься число, що позначає протокол, інкапсульований в даний IP пакет, для GRE protocol type дорівнює 47. У зв'язку з цим, якщо в мережі є GRE тунелі, то варто уважно ставитися до написання розширених списків контролю доступу (ACL), так як permit tcp any any і permit udp any any приведуть до заборони на GRE через те, що він и інкапсулюється безпосередньо в пакет, треба писати або permit ip any any або permit gre any any.




Рисунок 1.3 – Схема інкапсуляції GRE

Як видно, IP інкапсулюється в GRE, який інкапсулюється в IP. При цьому заголовок GRE і заголовок зовнішнього IP пакета додають 24 байта, відповідно, зменшуючи розмір пакета на цю величину.

У зв'язку зі службовим заголовком розмір переданих даних усередині IP пакета через GRE-тунель зменшується при збереженні загального розміру пакета. У IP-пакеті передбачено наявність біта DF (do not fragment), що забороняє поділ пакета на кілька при передачі через середовище з меншим розміром MTU. У цьому випадку пакет з розміром корисної області даних (англ. payload), що перевищує MTU IP пакету в GRE-тунелі, відкидається, що призводить до втрат пакетів при істотному навантаженні (проходять пакети малого розміру, такі як SYN пакети TCP, ICMP повідомлення (ping), але губляться пакети з даними в TCP потоці (тобто з'єднання рветься)). Для вирішення цієї проблеми рекомендується використовувати path-mtu-discovery (визначення TCP MSS, тобто максимального розміру IP-пакетів на всьому шляху) при передачі даних через GRE-тунель, щоб уникнути надмірної фрагментації або втрати великих пакетів

Так як GRE є протоколом мережевого рівня і не використовує порти (як протоколи TCP або UDP), а однією з необхідних умов роботи механізму PAT є наявність «відкритого» порту, то робота протоколу GRE через міжмережевий екран може бути ускладнена.

Зазвичай GRE використовується в поєднанні з PPTP для створення віртуальних приватних мереж. Застосовується в технології WDS для координації дій точок доступу і контролера WDS. Використовується в технологіях мобільного IP. В нашому випадку буде використаано версію протоколу mGRE для створення приватної мережі DMVPN.

mGRE - протокол тунелювання, що відрізняється від традиційного GRE можливістю встановлення тунелів з декількома сусідами на одному інтерфейсі. В основі лежить використання Next-Hop Resolution Protocol (NHRP), який дозволяє динамічно встановлювати такі сполуки. IPSec, взаємодіючи з NHRP, в разі потреби встановлює SA і забезпечує шифрування кожного окремо сполуки.

### 1.2.2 Загальна характеристика протоколу NHRP

NHRP (Next Hop Resolution Protocol) - протокол визначення наступного переходу), основною метою якого є дозвіл IP- і ATM-адрес пристроїв в мережі, що складається з декількох логічних підмереж. Протокол NHRP можна розглядати як розширену версію протоколу ATMARP, основна функція якого полягає в визначення відповідності між IP- я ATM-адресами пристроїв в одній логічної підмережі. На відміну від ATMARP, протокол NHRP підтримує дозвіл адрес в мережі з безліччю логічних підмереж[29].

Спочатку протокол NHRP розроблявся як доповнення до класичного IP та, отже, повинен застосовуватися тільки в мережах на базі цього протоколу. Однак теоретично він може підтримувати роботу будь-якого протоколу третього рівня (IP, IPX, AppleTalk) в будь-якій мережі, яка належить до класу NBMA (ATM, Frame Relay, X.25, SMDS і т. Д.).

Слід зазначити, що NHRP - це більше, ніж просто протокол.Он включає в себе, крім службових повідомлень, два важливих компоненти: сервер наступного переходу (Next Hop Server, NHS) і клієнт наступного переходу (Next Hop Client, NHC).

Основне завдання сервера NHS полягає в наданні сервісу протоколу NHRP клієнтам в мережі класу NBMA (подальші міркування будуть ставитися до мереж ATM). Для цього він зберігає в пам'яті спеціальну таблицю IP- і ATM-адрес пристроїв, підключених до мережі. Цей сервер може встановлюватися як на комп'ютері, підключеному до мережі ATM, так і на маршрутизаторі.

Клієнти протоколу NHRP підключаються до мережі із зазначенням ATM-адреси сервера NHS, який їх обслуговує. Існують два основні методи, які можуть використовуватися для реєстрації клієнтів на сервері NHS: ручний і автоматичний. У другому випадку використовується спеціальне реєстраційне повідомлення протоколу NHRP.

За допомогою спеціальних повідомлень, що посилаються від клієнтів до сервера, останній формує в своїй пам'яті таблицю IP- і ATM-адрес пристроїв. Незаперечною перевагою автоматичної реєстрації адрес є те, що не потрібно вручну заносити пари адрес в таблицю. Процес дозволу адреси в мережі ATM, що містить безліч логічних підмереж, здійснюється за кілька кроків.

В нашій мережі DMVPN NHRP буде відігравати дуже велику роль. Якщо зовсім коротко, ідея NHRP полягає в завданні хаба або NHS (Next-Hop Server), зазначеного для всіх spoke статично. Кожен spoke реєструється динамічно (тобто спочатку NHS не знає адрес spoke), встановлює сталі тунельні з NHS і NHS вносить відповідність його тунельного і реально адреси (mapping) в базу сусідів, а також в разі потреби повідомляє про це іншим spoke, щоб вони могли встановити з'єднання один з одним безпосередньо, а не через хаб. З'єднання spoke-to-spoke, на відміну від hub-to-spoke, що не постійні, а тимчасові. Як тільки трафік між філіями відсутня деякий час, тунель між ними видаляється. Це дозволяє використовувати в якості spoke-маршрутизаторів слабші моделі, оскільки на них немає необхідності тримати стільки сполук, скільки є spoke. В якості хаба ж, навпаки, доводиться вибирати маршрутизатор досить сильний, щоб витримати сполучення з усіма spoke.

Отже, ми дізнались для чого потрібен протокол NHRP так як він буде взаємодіяти з mGRE. Надалі буде розглянута характеристика протоколу BGP, який буде виконувати маршрутизацію між тунелями та локальними мережами

### 1.2.3 Загальна характеристика протоколу BGP

Так, як в цій кваліфікаційній роботі протокол динамічної маршрутизації BGP займає основну роль, то розглянемо його детальніше, ніж вище згадані та сформуємо основні висновки з розділу.

BGP (англ. Border Gateway Protocol, укр. Протокол Граничного Шлюзу) — з 1994 року єдиний протокол маршрутизації між автономними системами в глобальній мережі Інтернет, а його розширена версія MBGP (Multiprotocol BGP) використовується в MPLS-мережах IT-провайдерів [14].

BGP є протоколом міждоменної маршрутизації та належить до класу дистанційно-векторних протоколів. Як протокол міждоменної маршрутизації використовується усіма інтернет-провайдерами, а також великими компаніями та організаціями, які мають власні публічні номери автономних систем (ASN) та користуються послугами більш ніж одного інтернет-провайдера (мултіхомінг) або мають прямі IP-з'єднання з багатьма іншими великими компаніям, що також мають власні публічні номери автономних систем, без використання послуг інтернет-провайдерів.

Разом з тим немає ніяких обмежень на використання BGP в локальних мережах крім рекомендацій про приватні ASN (64512-65534), але використання BGP як протоколу внутрішньодоменної маршрутизації є недоцільним через значний час конвергенції (збіжності) у порівнянні з іншими протоколами маршрутизації, що закладено в його дизайні.

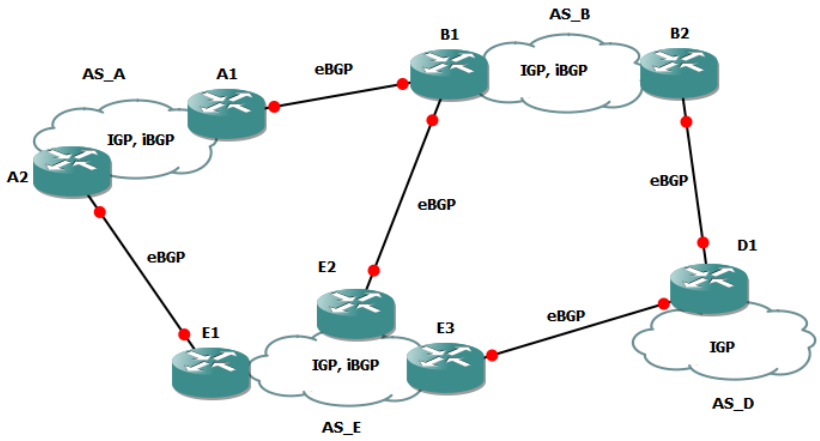



Рисунок 1.4 – Типовий приклад використання протоколу BGP

На відміну від класичного дистанційно-векторного протоколу RIP, метрикою якого є кількість хопів (відрізків шляху) між маршрутизаторами, найкращий маршрут BGP обирається по точно визначеному пріоритету атрибутів, одним із яких, але не найпріоритетнішим, є кількість хопів між автономними системами — найкоротший шлях між автономними системами (англ. shortest AS path). Тому іноді цей протокол зараховують до окремого класу шляхо-векторних протоколів.

Маршрутизатор, на якому працює BGP. передає своїм BGP-сусідам (англ. peer) IP-префікси та набір атрибутів до них на основі вибору своїх найкращих маршрутів до конкретних IP-мереж. В свою чергу ці атрибути використовуються BGP-сусідами для калькуляції своїх власних маршрутів.

Маршрутизатор взаємодіє з іншими маршрутизаторами по протоколу BGP тільки в тому випадку, якщо адміністратор явно вказує при конфігуруванні, що ці маршрутизатори є його сусідами.

Такий спосіб взаємодії зручний в ситуації, коли маршрутизатори, що обмінюються маршрутною інформацією, належать різним постачальникам послуг (ISP). Адміністратор ISP може вирішувати, з якими автономними системами він буде обмінюватися трафіком, а з якими ні, задаючи список сусідів для своїх зовнішніх шлюзів. Протоколи RIP і QSPF, розроблені для застосування всередині автономної системи, обмінюються маршрутною інформацією з усіма маршрутизаторами, що знаходяться в межах їх безпосередньої досяжності (по локальній мережі або через двоточковий канал). Це означає, що інформація про всі мережах з'являється в таблиці маршрутизації кожного маршрутизатора, так що кожна мережа виявляється досяжною для кожної. У корпоративної мережі це нормальна ситуація, а в мережах ISP немає, тому протокол BGP і виконує тут особливу роль.

Для встановлення сеансу з зазначеними сусідами BGP-маршрутизатори використовують протокол TCP (порт 179). При встановленні BGP-сеансу можуть застосовуватися різноманітні способи аутентифікації маршрутизаторів, що підвищують безпеку роботи автономних систем.

Основним повідомленням протоколу BGP є повідомлення UPDATE (оновити), за допомогою якого маршрутизатор повідомляє маршрутизатора сусідній автономної системи про досяжності мереж, що належать до його власної автономної системи. Сама назва цього повідомлення говорить про те, що це - тригерні оголошення, яке посилається сусідові тільки тоді, коли в автономній системі що-небудь різко змінюється: з'являються нові мережі або нові шляхи до мереж або ж, навпаки, зникають існуючі мережі або шляху.

В одному повідомленні UPDATE можна оголосити про одне новий маршрут або анулювати кілька маршрутів, які перестали існувати. Під маршрутом в BGP розуміється послідовність автономних систем, яку потрібно пройти на шляху до зазначеної в адресі сіті. Більш формально інформація про маршрут (BGP Route) до мережі (Network / Maskjength) виглядає так:

BGP Route = AS_Path; NextHop; Network / Maskjength

Тут AS_Palh - набір номерів автономних систем, NextHop - IP-адреса маршрутизатора, через який потрібно передавати пакети в мережу Network / Maskjength.

Атрибути в BGP поділяються на категорії:

1. Добре знані (Well-known) — усі BGP-реалізації мусять підтримувати ці атрибути
   - Обов'язкові (Mandatory) — усі BGP-маршрутизатори мусять надсилати ці атрибути своїм сусідам
   - Дискреційні (Discretionary) — надсилання цих атрибутів відбувається на власний розсуд або за обопільною згодою
2. Додаткові (Optional) — необов'язкові
   - Транзитні (Transitive) — мають передаватися по ланцюжку від одного маршрутизатора до іншого
   - Нетранзитні (Non-transitive) — маршрутизатор передає лише своїм BGP-сусідам, які не зобов'язані передавати ці атрибути далі по мережі

Маршрутизатор взаємодіє з іншими маршрутизаторами по протоколу BGP тільки в тому випадку, якщо адміністратор явно вказує при конфігуруванні, що ці маршрутизатори є його сусідами.

BGP-маршрутизатор призначає перший отриманий маршрут найкращим поточним маршрутом для конкретної IP-мережі. Якщо BGP-маршрутизатор отримує новий маршрут то порівнює його з найкращим поточним маршрутом згідно зі спи-

ском пріоритетності BGP-атрибутів. Якщо поточний крок вирішив неоднозначність, до наступного кроку не переходять, а вважається, що найкращий маршрут знайдено:

1. Перевага надається маршруту з найбільшим значенням параметра (атрибута) WEIGHT (Вага). Застосовується лише на маршрутизаторах Cisco.
2. Маршрут, що має найбільше значення атрибуту LOCAL_PREF (Локальна Перевага), за замовченням цей атрибут має значення 100.
3. Маршрутизатори Cisco надають перевагу своїм власним маршрутам над маршрутами отриманими від BGP-сусідів[7]. Маршрутизатори інших виробників можуть ігнорувати цей крок, або мати свої власні правила.
4. Надання переваги найкоротшому шляху до конкретної IP-мережі на основі атрибуту AS_PATH (Шлях по автономних системах). Тобто найкращим маршрутом є той до якого веде шлях через мінімальну кількість автономних систем
5. Вибір на основі атрибуту ORIGIN (Джерело). Якщо IP-префікс якоїсь мережі спочатку був отриманий BGP із протоколу внутрішньодоменної маршрутизації[en] тоді маршрут, що веде до цієї мережі, є пріоритетнішим, ніж маршрути, які отримали IP-префікс цієї мережі з EGP (протокол наразі не використовується) або джерело отримання невідоме.
6. Надання переваги маршруту з найменшим значенням атрибута MED (multi-exit discriminator, дискримінатор мульти-виходу)
7. Перевага маршруту, отриманому через eBGP (Exterior, Зовнішній BGP) над iBGP (Interior, Внутрішній BGP) тобто маршрут отриманий від BGP-сусіда з іншої автономної системи має перевагу над маршрутом отриманим від BGP-сусіда тієї ж самої AS.
8. Обирається маршрут, який отриманий від ближчого BGP-сусіда. Ближчим сусідом є той до якого є найменшою відстань в таблиці маршрутизації сформованій на основі прямих з'єднань, статичних маршрутів[en] та протоколів внутрішньодоменної маршрутизації (IGP).

9. Цей пункт виконується, коли ми використовуємо Багатошляховий[en] (Multipath) BGP, тобто коли для цілей балансування навантаження[en] використовується окрім найкращого один чи більше додаткових маршрутів до конкретної IP-мережі. Якщо претендент на найкращий маршрут має такі ж самі характеристик згідно з попередніми пунктами, як і раніше обраний, то він не стає новим найкращим, але може бути обраним, як додатковий. Маршрутизатори CISCO можуть мати до 6 BGP-маршрутів до конкретної IP-мережі.
10. Маршрут отриманий першим має пріоритет.
11. Перевага маршруту, що отриманий від BGP сусіда з найменшим значенням його ідентифікатора (Router ID)
12. Цей пункт виконується лише при використанні багатошляхової маршрутизації. Надається перевага маршруту, що проходить через мінімальну довжину кластерного списку.

База даних BGP включає в себе:

1. Таблицю сусідів.
2. BGP-таблицю, яку також часто називають база даних надсилання (forwarding database) або база даних топології (topology database). Таблиця включає у себе усі IP-маршрути з їх BGP-атрибутами, отриманими від сусідів.
3. Таблиця IP-маршрутизації (IP routing table). Тільки найкращі маршрути до конкретних IP-мереж, обраних згідно з алгоритмом вибору маршруту.

### 1.2.4 Загальна характеристика технології IPsec

IPsec (скорочення від IP Security) — набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP, дозволяє здійснювати підтвердження справжності та/або шифрування IP-пакетів. IPsec також містить в собі протоколи для захищеного обміну ключами в мережі Інтернет.

Протоколи IPsec, на відміну від інших добре відомих протоколів SSL та TLS, працюють на мережевому рівні (рівень 3 моделі OSI). Це робить IPsec гнучкішим, так що він може використовуватися для захисту будь-яких протоколів, що базуються на TCP та UDP. IPsec може використовуватися для забезпечення безпеки між двома IP-вузлами, між двома шлюзами безпеки або між IP-вузлом і шлюзом безпеки. Протокол є «надбудовою» над IP-протоколом, і обробляє сформовані IP-пакети описаним нижче способом. IPsec може забезпечувати цілісність та / або конфіденційність даних переданих по мережі.

IPsec використовує наступні протоколи для виконання різних функцій:

- Authentication Header (AH) забезпечує цілісність віртуального з'єднання (переданих даних), аутентифікацію джерела інформації та додаткову функцію із запобігання повторної передачі пакетів
- Encapsulating Security Payload (ESP) може забезпечити конфіденційність (шифрування) переданої інформації, обмеження потоку конфіденційного трафіку. Крім цього, він може забезпечити цілісність віртуального з'єднання (переданих даних), аутентифікацію джерела інформації та додаткову функцію із запобігання повторної передачі пакетів (Всякий раз, коли застосовується ESP, в обов'язковому порядку повинен використовуватися той чи інший набір даних послуг із забезпечення безпеки)
- Security Association (SA) забезпечують зв'язку алгоритмів і даних, які надають параметри, необхідні для роботи AH і / або ESP. Internet security association and key management protocol (ISAKMP) забезпечує основу для аутентифікації і обміну ключами, перевірки автентичності ключів.

В роботі протоколів IPsec можна виділити п'ять етапів:

- Перший етап починається зі створення на кожному вузлі, що підтримує стандарт IPsec, політики безпеки. На цьому етапі визначається, який трафік підлягає шифрування, які функції і алгоритми можуть бути використані.
- Другий етап є по суті першою фазою IKE. Її мета - організувати безпечний канал між сторонами для другої фази IKE. На другому етапі виконуються:

Аутентифікація і захист ідентифікаційної інформації вузлів, перевірка відповідностей політик IKE SA вузлів для безпечного обміну ключами, обмін Діффі-Хеллмана, в результаті якого у кожного вузла буде загальний секретний ключ, створення безпечного каналу для другої фази IKE

- Третій етап є другою фазою IKE. Його завданням є створення IPsec-тунелю. На третьому етапі виконуються наступні функції: узгоджуються параметри IPsec SA по захищається IKE SA каналу, створеному в першій фазі IKE, встановлюється IPsec SA, періодично здійснюється перегляд IPsec SA, щоб переконатися в її безпеці, (За бажанням) виконується додатковий обмін Діффі-Хеллмана.
- Робочий етап. Після створення IPsec SA починається обмін інформацією між вузлами через IPsec-тунель, використовуються протоколи і параметри, встановлені в SA. Припиняють діяти поточні IPsec SA. Це відбувається при їх видаленні або при закінченні часу життя (певне в SA в байтах інформації, переданої через канал, або в секундах), значення якого міститься в SAD на кожному вузлі. Якщо потрібно продовжити передачу, запускається фаза два IKE (якщо потрібно, то і перша фаза) і далі створюються нові IPsec SA. Процес створення нових SA може відбуватися і до завершення дії поточних, якщо потрібна безперервна передача даних. IPSec зобов'язує підтримувати ручне і автоматичне керування контекстами безпеки і криптографічними ключами. У першому випадку все системи заздалегідь забезпечуються ключовим матеріалом і іншими даними, необхідними для захищеного взаємодії з іншими системами. У другому - матеріал і дані виробляються динамічно, на основі певного протоколу - IKE, підтримка якого обов'язкова.

Отже, була розглянута технологія IPsec, її логіка роботи та призначення. Завершальним кроком буде характеристика DMVPN, який являє собою набором всіх протоколів вище, окрім BGP.

## 1.3 Загальна характеристика технології DMVPN

DMVPN (англ. Dynamic Multipoint Virtual Private Network - динамічна багатоточкова віртуальна приватна мережа) - технологія для створення віртуальних приватних мереж, розроблена Cisco Systems [1]. Є подальшим розвитком VPN, і грунтується на спільній роботі протоколів дозволу шлюзу NHRP, протоколу тунелювання mGRE, шифрування IPSec і протоколів динамічної маршрутизації: OSPF, ODR, RIP, EIGRP, BGP.

Cisco DMVPN може бути розгорнута як спільно з системами безпеки Cisco IOS Firewall і Cisco IOS IPS, так і разом з такими необхідними в сучасних мережах механізмами як QoS, IP Multicast, Split Tunneling і механізмами резервних маршрутів (routing-based failover). Використовуючи можливості Cisco DMVPN можна створювати великі VPN мережі з десятками і сотнями вузлів, з можливістю балансування завантаження каналів і резервування. При цьому немає необхідності вручну конфігурувати кожне з'єднання між вузлами мережі - з'єднання буде встановлено автоматично відповідно с політиками доступу і безпеки.

Як зазначалося вище, зараз в об'єднаній мережі всі двоточкові тунелі IPsec (або IPsec + GRE) повинні бути налаштовані на всі маршрутизатори, навіть якщо деякі або більшість з них діють не весь час. Використовуючи рішення DMVPN, один маршрутизатор стає концентратором, а інші маршрутизатори (промені) налаштовуються на концентратор за допомогою тунелів. Тунелі з топологією "зірка" постійно включені, і налашутування прямого тунелю між будь-якими променями не потрібно. Маршрутизатор концентратора діє в якості сервера NHRP і обробляє цей запит для вихідного променя. Потім два промені динамічно створюють між собою тунель IPsec (через єдиний інтерфейс mGRE), що забезпечує пряму передачу даних. Даний динамічний тунель між двома променями буде автоматично розірвано після закінчення (налаштованого) періоду бездіяльності.

При використанні Інтернету в якості посередника між концентратором і променями, промені також мають прямий доступ один до одного без додаткових ма-

теріальних витрат, але до теперішнього часу було практично неможливо встановити і / або керувати повної (часткової) об'єднаної мережею. Мережі з повністю або частково комірчастою структурою часто є кращими, так як вони дозволяють заощадити кошти, якщо трафік між двома променями можна передати безпосередньо, а не через концентратор. Трафік між двома променями, що проходить через концентратор, використовує ресурси концентратора і може викликати додаткову затримку, особливо при використанні шифрування IPsec, тому що концентратора доведеться розшифровувати приходять пакети від посилають променів, а потім знову шифрувати трафік для передачі його на який одержує промінь. Ще один приклад, коли прямий трафік між променями більш кращий, - ситуація, коли два кінця променя перебувають в одному місті, а концентратор - на іншому кінці країни.

Технологія DMVPN дозволяє вирішити цю задачу більш масштабованим методом, ніж створення зв'язків точка-точка між усіма офісами і об'єднання їх в повнозв'язну топологію.

При додаванні нових маршрутизаторів в існуючу мережу DMVPN, необхідно налаштувати тільки новий маршрутизатор, змін на вже існуючих маршрутизаторах не потрібно.

Переваги технології DMVPN:

- Динамічна маршрутизація між вузлами мережі VPN
- Протоколи динамічної маршрутизації можуть пересилати інформацію про IP-мережах по зашифрованим тунелях між підрозділами компанії. Підтримуються протоколи маршрутизації: Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), і Border Gateway Protocol (BGP).
- Невеликий обсяг конфігураційних даних
- Немає необхідності налаштовувати кожне з'єднання окремо. Додавання нового вузла в мережу VPN не вимагає змін в конфігурації як сусідніх вузлів мережі VPN, так і центрального вузла такої мережі. Наприклад, типовий

конфігураційний файл для мережі з 1000 вузлів в разі традиційних мереж IP-sec буде містити 3900 рядків на кожному пристрої VPN, в той час як для технології DMVPN необхідно тільки 13 рядків на один пристрій.

- Динамічні тунелі без участі центрального вузла
- Відповідно до політиками безпеки компанії окремі вузли зможу встановлювати з'єднання VPN між собою без участі центрального вузла. Це витрати на транзитний трафік для центрального вузла, так і підвищує швидкість обробки таких даних як трафік систем IP-телефонії.
- Механізми відмовостійкості
- Мережа VPN може бути побудована як з використанням одного центрального вузла, так і декількох центральних вузлів для забезпечення резервування пристроїв і каналів зв'язку.
- Підтримка якості обслуговування QoS
- Як на центральному вузлі мережі VPN, так і на віддалених вузлах можлива реалізація політик QoS з класифікацією трафіку, настройка шейпірованія трафіку, обслуговування трафіку з різним пріоритетом для різних вузлів мережі.
- Масштабованість мережі
- Мережа DMVPN може складатися як з декількох вузлів, так і вирости до мережі з тисяч вузлів з використанням технології server load balancing (SLB). Продуктивність центральних вузлів може бути збільшена простим додаванням додаткових пристроїв.

Отже, в першому розділі було розглянуто теоретичні відомості про технологію VPN, розглянуто її основні визначення та терміни, тунелювання, рівні захищених каналів, а також її класифікацію. За допомгогою загальних знань VPN сформовані принципи, уявлення про процеси, які будуть відбуватися в нашому кваліфікційному проекті. Розглянувши різні протоколи та технології було вивчено їх прицнипи для налаштування приватної мережі DMVPN. Зокрема, було досліджено, що мережа DMVPN неможлива без їх використання. Ці знання знадобляться у подальшому налаштуванні.

# РОЗДІЛ 2. ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА ПОЛІТИК БЕЗПЕКИ

## 2.1 Проект мережі та його фізична топологія

Головна ідея кваліфікаційної роботи така: існує два головних офіси, вони являють собою основу організації. Будь-яка велика організація завжди має в своїх панах розширювати склад співробітників і офісів. Тому потрібно створити захищену приватну віртуальну мережу між цими офісами. Також одна з головних умов, щоб налаштування в цій мережі були мінімальними і зручними. Щоб реалізувати вищесказану ідею можна використати один із видів Site-to-Site віртуальних приватних мереж. Так, як вся мережа буде будуватись на Cisco обладнанні, то чудовим вибором стане DMVPN. Так, як реального обладнання немає можливості використати, проект буде створюватись в графічному мережевому емуляторі EVE-ng(Emulated Virtual Environment Next Generation). На відміну від популярного додатку GNS3(Graphical Network Simulator-3) він має більш продвинуті можливості налаштування, сучасний графічний веб-дизайн та вирізняється кращою стабільністю роботи.

Проект можна умовно поділити на такі зони: private zone, server zone, internet zone. Private zone являє собою зону користувачів, в ній буде зосереджена велика кількість робочих станцій та два комутатори.

Користувачі повинні отримувати ip-адреси динамічно, для цього використаємо протокол динамічної роздачі IP-адрес.

Кожна мережа потребує певних змін час від часу і не завжди є можливість мати прямий доступ до мережевого обладнання. Тому потрібно організувати віддалений доступ до цих пристроїв. Чудовим рішенням стане віддалене підключення за допомогою SSH.

Server zone має більш спрощену топологію. Вона складається з серверу і граничного маршутизатора. Головна призначення цієї зони: збереження даних на сер-

вері від користувачів private zone, доступ в інтернет та зв'язок між іншими серверами філій. Він буде мати статичну IP-адресу, так як нема потреби в надані динамічної. Ця зона виділена по ряду причин. Одна із них краща захищеність.

Прокладання окремих ліній між офісами є доволі поганим рішенням, одні з головних причин – це достатньо дорого і потребує постійного обслуговування. Тому зв'язок між офісами буде реалізовано через глобальну мережу Internet. В зоні Internet буде присутня певна кількість маршрутизаторів, які будуть імітувати цю глобальну мережу. По суті вони є певним мостом між офісами та способом зв'язку. Варто зауважити, що маршрутизатори в цій зоні не належать офісам, тому налаштування в них будуть мінімальні та спрямовані лиш на підтримку маршуртизації.

Для мережі DMVPN вибрано 5 маршрутизаторів, два з них будуть головні(HUBs), а інші другорядні(Spokes). Всі ці маршрутизатори будуть граничними, вони будуть з'єднувати офіси через глобальну мережу Інтернет.

Умовно схему можна поділити на три рівні представлені на рисунку 2.1.




Рисунок 2.1 – Рівні взаємодії маршрутизаторів

За допомогою статичної маршрутизації маршрутизатори матимуть змогу можливість зв'язку на фізичному рівні. Рівень DMVPN використовує тунельні інтерфейси і базується на статичній маршрутизації. Другорядні маршрутизатори(Spokes) матимуть змогу знаходити головний маршрутизатор(Hub) і співвідносити адресу фізичного і віртуального тунельного інтрфейсу. Після цього потрібно налаштувати BGP маршрутизацію, яка буде працювати поверх DMVPN, також використувати тунельні інтерфейси, і буде давати змогу спілкуватись офісам один з одним.

Варто зауважити, що якщо маршрутизатори являються граничними, тобто знаходяться на перетині всіх зон, то і навантаження на них буде найбільшим, бо

вони одночасно повинні виконувати роль DHCP серверу, бути клієнтом, або сервером мережі DMVPN, та здійснювати маршрутизацію. Тому варто зупинити свій вибір на найбільш потужніших моделях обладнання компанії Cisco.

Для забезпечення функціонування мережі організації було обрано оптимальні багаторівневі комутатори корпорації CISCO. Також потрібно приділити особливу увагу технологіям, котрі необхідні для мережі, зокрема це підтримка GigabitEthernet.

Комутатор Cisco Catalyst WS-C2960-24TT-L дуже добре підходить для внутрішніх мереж, оскільки має велику кількість FE портів та кілька GE.



Рисунок 2.2 - Комутатор Cisco Catalyst WS-C2960-24TT-L

Cisco Catalyst 2960 - нове сімейство комутаторів другого рівня з фіксованою конфігурацією, яке дозволяє підключати робочі станції до мереж Fast Ethernet і Gigabit Ethernet на швидкості середовища передачі, задовольняючи зростаючі потреби в пропускної здатності на периферії мережі. Для агрегації застосовуються комбіновані гігабітні uplink-порти, які можуть об'єднуватися в єдиний канал за технологією GigabitEtherChannel.

Дана серія комутаторів орієнтована в першу чергу на підприємства малого і середнього бізнесу, а також філії великих компаній для вирішення завдання реалізації рівня доступу до мережі. У порівнянні з популярною серією комутаторів Catalyst 2950 моделі сімейства 2960 забезпечують більш широкий набір функцій забезпечення безпеки і якості обслуговування, а також управління смугою пропускання. Для спрощення завдання конфігурації в комутаторах серії Catalyst 2960 передбачена функція Smartports, що дозволяє виконати основні настройки порту ко-

мутаторів, грунтуючись на його призначення. Cisco Catalyst 2960 забезпечують потребу в передачі даних зі швидкістю 100 Мбіт / сек і 1 Гбіт / сек, дозволяють використовувати LAN сервіси, наприклад, для мереж передачі даних, побудованих у філіях корпорацій. Сімейство Catalyst 2960 дозволяє забезпечити високу безпеку даних за рахунок вбудованого NAC, підтримки QoS і високого рівня стійкості системи.

Основні особливості:

- високий рівень безпеки, вдосконалені списки контролю доступу (ACL);
- організація контролю мережі і оптимізація ширини каналу з використанням QoS, диференційованого обмеження швидкості і ACL.
- для забезпечення безпеки мережі комутатори використовують широкий спектр методів аутентифікації користувача, технології шифрування даних і організації розмежування доступу до ресурсів на підставі ідентифікатора користувача, порту і MAC адрес.
- комутатори прості в управлінні і конфігурації
- доступна функція авто конфігурації за допомогою Smart портів для деяких спеціалізованих додатків.

Наступний маршрутизатор буде використовуватись як в проміжних машрутах, так і в граничних зонах

Cisco 7201- це компактний високопродуктивний маршрутизатор з широким набором інтерфейсів і функцій і низьким енергоспоживанням. Він є ідеальним рішенням для постачальників послуг і корпоративних додатків. Cisco 7201 створений для задоволення потреби замовників в високопродуктивному, компактному і гнучкому маршрутизаторі, допускає подальше збільшення продуктивності і застосування новітніх функцій Cisco IOS Software.



Рисунок 2.3 - Комутатор Cisco 7201

Маршрутизатор призначений для вирішення широкого кола завдань як постачальників послуг, так і корпоративних клієнтів:

- Широкосмугове агрегування (Broadband aggregation) - Термінування PPP і концентрація доступу L2TP, маршрутизатор здатний обробляти до 8000 одночасних сесій і дозволяє розширюватися в міру потреби.
- Service Provider Edge Applications
- IPv6 шлюз-з'єднання між IPv4 і IPv6 мережами, включаючи архітектуру IPv6 VPN.
- Managed services-Високопродуктивне (customer premises equipment (CPE)) або Multiprotocol Label Switching-customer edge (MPLS-CE) пристрій.
- Високо надійні рішення-Резервування за використанням двох CPE налаштованих для Hot Standby Router Protocol (HSRP) або Layer 3 load balancing.
- Enterprise Applications
- Високопродуктивні CPE у великих філіях - чотири вбудованих GE інтерфейсів в компактному форм фактор 1RU з потужною підтримкою всіх необхідних сервісів для великого філії.
- Високошвидкісний шлюз Internet підприємства - Cisco 7201 високошвидкісний шлюз Internet з можливістю підключення до провайдерів з використанням FE або GE портів і традиційним WAN через модуль port adapter (PA).

- Tunnel-less VPN-Рішення використовує Cisco 7201 як сервер ключів, а Cisco 7206 як hub site, і ISR- маршрутизатори в філіях, підтримуючи Cisco Group Encrypted Transport (GET) VPN
- Підтримка самого широкого спектру функцій IP / MPLS в програмному забезпеченні Cisco IOS (управління якістю обслуговування, агрегування широкосмугових підключень, безпеку, мультисервісний доступ, мультипротокольна комутація на основі міток і інші)
- Широкий асортимент гнучких, модульних інтерфейсів (від DS0 до OC12)
- Підтримка інтерфейсів Fast Ethernet, Gigabit Ethernet, Packet Over Sonet та інших
- Повністю модульна конструкція в форматі 3RU
- Повна підтримка термінації L2TP і PPP
- Підтримка до 16000 широкосмугових абонентських сесій
- Акселератор послуг на базі технології Cisco PXF
- Підтримка різних протоколів
- Низькі початкові капіталовкладення
- Масштабованість і гнучкість; ідеально підходять для модернізації мереж

Загалом при побудові топології використано 11 маршрутизаторів, 10 комутаторів, 5 серверів, та 37 робочих станцій. Повну інформацію про фізичні з'єднання буде представлено у вигляді таблиці 2.1.

Таблиця 2.1

Параметри інтерфейсів пристроїв

| Пристрій | Інтерфейс | Підключення до пристрою | Підключення до інтерфейсу |
|---|---|---|---|
| Маршрутизатор R_2_14_1 | Fa0/0 | Маршрутизатор R_2_14_6 | Fa0/0 |
| | Fa1/0 | Комутатор SW_2_14_2 | E0/0 |
| | Fa2/0 | Сервер Serv_2_14_1 | Eth0 |
| Маршрутизатор R_2_14_2 | Fa0/0 | Маршрутизатор R_2_14_7 | Fa0/0 |
| | Fa1/0 | Комутатор SW_2_14_3 | E0/0 |
| | Fa2/0 | Сервер Serv_2_14_2 | Eth0 |
| Маршрутизатор R_2_14_3 | Fa0/0 | Маршрутизатор R_2_14_8 | Fa0/0 |
| | Fa1/0 | Комутатор SW_2_14_5 | E0/0 |
| | Fa2/0 | Сервер Serv_2_14_3 | Eth0 |

Продовження табл. 2.1

| | | | |
|---|---|---|---|
| Маршрутизатор R_2_14_4 | Fa0/0 | Маршрутизатор R_2_14_9 | Fa0/0 |
| | Fa1/0 | Комутатор SW_2_14_7 | E0/0 |
| | Fa2/0 | Сервер Serv_2_14_4 | Eth0 |
| Маршрутизатор R_2_14_5 | Fa0/0 | Маршрутизатор R_2_14_11 | Fa0/0 |
| | Fa1/0 | Комутатор SW_2_14_9 | E0/0 |
| | Fa3/0 | Сервер Serv_2_14_5 | Eth0 |
| Маршрутизатор R_2_14_6 | Fa0/0 | Маршрутизатор R_2_14_1 | Fa0/0 |
| | Fa1/0 | Маршрутизатор R_2_14_7 | Fa1/0 |
| | Fa2/0 | Маршрутизатор R_2_14_8 | Fa1/0 |
| Маршрутизатор R_2_14_7 | Fa0/0 | Маршрутизатор R_2_14_2 | Fa0/0 |
| | Fa1/0 | Маршрутизатор R_2_14_6 | Fa1/0 |
| | Fa2/0 | Маршрутизатор R_2_14_9 | Fa1/0 |
| Маршрутизатор R_2_14_8 | Fa0/0 | Маршрутизатор R_2_14_3 | Fa0/0 |
| | Fa1/0 | Маршрутизатор R_2_14_6 | Fa2/0 |
| | Fa2/0 | Маршрутизатор R_2_14_10 | Fa0/0 |
| | Fa3/0 | Маршрутизатор R_2_14_9 | Fa3/0 |
| Маршрутизатор R_2_14_9 | Fa0/0 | Маршрутизатор R_2_14_4 | Fa0/0 |
| | Fa1/0 | Маршрутизатор R_2_14_7 | Fa2/0 |
| | Fa2/0 | Маршрутизатор R_2_14_11 | Fa1/0 |
| | Fa3/0 | Маршрутизатор R_2_14_8 | Fa3/0 |
| Маршрутизатор R_2_14_10 | Fa0/0 | Маршрутизатор R_2_14_8 | Fa2/0 |
| | Fa1/0 | Маршрутизатор R_2_14_11 | Fa2/0 |
| Маршрутизатор R_2_14_11 | Fa0/0 | Маршрутизатор R_2_14_5 | Fa0/0 |
| | Fa1/0 | Маршрутизатор R_2_14_9 | Fa2/0 |
| | Fa2/0 | Маршрутизатор R_2_14_10 | Fa1/0 |
| Комутатор SW_2_14_1 | E0/0 | Комутатор SW_2_14_2 | E0/1 |
| | E0/1 | WS_2_14_1 | Eth0 |
| | E0/2 | WS_2_14_2 | Eth0 |
| | E0/3 | WS_2_14_3 | Eth0 |
| Комутатор SW_2_14_2 | E0/0 | Маршрутизатор R_2_14_1 | Fa1/0 |
| | E0/1 | Комутатор SW_2_14_1 | E0/0 |
| | E0/2 | Робоча станція WS_2_14_4 | Eth0 |
| | E0/3 | Робоча станція WS_2_14_5 | Eth0 |
| | E1/0 | Робоча станція WS_2_14_6 | Eth0 |
| Комутатор SW_2_14_3 | E0/0 | Маршрутизатор R_2_14_2 | Fa1/0 |
| | E0/1 | Комутатор SW_2_14_4 | E0/0 |
| | E0/2 | Робоча станція WS_2_14_7 | Eth0 |
| | E0/3 | Робоча станція WS_2_14_8 | Eth0 |
| | E1/0 | Робоча станція WS_2_14_9 | Eth0 |
| Комутатор SW_2_14_4 | E0/0 | Комутатор SW_2_14_3 | E0/1 |
| | E0/1 | Робоча станція WS_2_14_10 | Eth0 |
| | E0/2 | Робоча станція WS_2_14_11 | Eth0 |
| | E0/3 | Робоча станція WS_2_14_12 | Eth0 |
| | E1/0 | Робоча станція WS_2_14_13 | Eth0 |
| Комутатор SW_2_14_5 | E0/0 | Маршрутизатор R_2_14_3 | Fa1/0 |
| | E0/1 | Комутатор SW_2_14_6 | E0/0 |
| | E0/2 | Робоча станція WS_2_14_14 | Eth0 |

Продовження табл. 2.1

| | | | |
|---|---|---|---|
| | E0/3 | Робоча станція WS_2_14_15 | Eth0 |
| | E1/2 | Робоча станція WS_2_14_16 | Eth0 |
| | E1/0 | Робоча станція WS_2_14_17 | Eth0 |
| | E1/1 | Робоча станція WS_2_14_18 | Eth0 |
| Комутатор SW_2_14_6 | E0/0 | Комутатор SW_2_14_5 | E0/1 |
| | E0/1 | Робоча станція WS_2_14_19 | Eth0 |
| | E0/2 | Робоча станція WS_2_14_20 | Eth0 |
| | E0/3 | Робоча станція WS_2_14_21 | Eth0 |
| | E1/0 | Робоча станція WS_2_14_22 | Eth0 |
| Комутатор SW_2_14_7 | E0/0 | Маршрутизатор R_2_14_4 | Fa1/0 |
| | E0/1 | Комутатор SW_2_14_8 | E0/0 |
| | E0/2 | Робоча станція WS_2_14_23 | Eth0 |
| | E0/3 | Робоча станція WS_2_14_24 | Eth0 |
| | E1/0 | Робоча станція WS_2_14_25 | Eth0 |
| | E1/1 | Робоча станція WS_2_14_26 | Eth0 |
| Комутатор SW_2_14_8 | E0/0 | Комутатор SW_2_14_7 | E0/1 |
| | E0/1 | Робоча станція WS_2_14_27 | Eth0 |
| | E0/2 | Робоча станція WS_2_14_28 | Eth0 |
| | E0/3 | Робоча станція WS_2_14_29 | Eth0 |
| | E1/0 | Робоча станція WS_2_14_30 | Eth0 |
| Комутатор SW_2_14_9 | E0/0 | Маршрутизатор R_2_14_5 | Fa1/0 |
| | E0/1 | Комутатор SW_2_14_10 | E0/0 |
| | E0/2 | Робоча станція WS_2_14_31 | Eth0 |
| | E0/3 | Робоча станція WS_2_14_32 | Eth0 |
| | E1/0 | Робоча станція WS_2_14_33 | Eth0 |
| Комутатор SW_2_14_10 | E0/0 | Комутатор SW_2_14_9 | E0/1 |
| | E0/1 | Робоча станція WS_2_14_34 | Eth0 |
| | E0/2 | Робоча станція WS_2_14_35 | Eth0 |
| | E0/3 | Робоча станція WS_2_14_36 | Eth0 |
| | E1/0 | Робоча станція WS_2_14_37 | Eth0 |
| Сервер Serv_2_14_1 | Eth0 | Маршрутизатор R_2_14_1 | Fa2/0 |
| Сервер Serv_2_14_2 | Eth0 | Маршрутизатор R_2_14_2 | Fa2/0 |
| Сервер Serv_2_14_3 | Eth0 | Маршрутизатор R_2_14_3 | Fa2/0 |
| Сервер Serv_2_14_4 | Eth0 | Маршрутизатор R_2_14_4 | Fa2/0 |
| Сервер Serv_2_14_5 | Eth0 | Маршрутизатор R_2_14_5 | Fa3/0 |
| Робоча станція WS_2_14_1 | Eth0 | Комутатор SW_2_14_1 | E0/1 |
| Робоча станція WS_2_14_2 | Eth0 | Комутатор SW_2_14_1 | E0/2 |
| Робоча станція WS_2_14_3 | Eth0 | Комутатор SW_2_14_1 | E0/3 |
| Робоча станція WS_2_14_4 | Eth0 | Комутатор SW_2_14_2 | E0/2 |

Продовження табл. 2.1

| | | | |
|---|---|---|---|
| Робоча станція WS_2_14_5 | Eth0 | Комутатор SW_2_14_2 | E0/3 |
| Робоча станція WS_2_14_6 | Eth0 | Комутатор SW_2_14_2 | E1/0 |
| Робоча станція WS_2_14_7 | Eth0 | Комутатор SW_2_14_3 | E0/2 |
| Робоча станція WS_2_14_8 | Eth0 | Комутатор SW_2_14_3 | E0/3 |
| Робоча станція WS_2_14_9 | Eth0 | Комутатор SW_2_14_3 | E1/0 |
| Робоча станція WS_2_14_10 | Eth0 | Комутатор SW_2_14_4 | E0/1 |
| Робоча станція WS_2_14_11 | Eth0 | Комутатор SW_2_14_4 | E0/2 |
| Робоча станція WS_2_14_12 | Eth0 | Комутатор SW_2_14_4 | E0/3 |
| Робоча станція WS_2_14_13 | Eth0 | Комутатор SW_2_14_4 | E1/0 |
| Робоча станція WS_2_14_14 | Eth0 | Комутатор SW_2_14_5 | E0/2 |
| Робоча станція WS_2_14_15 | Eth0 | Комутатор SW_2_14_5 | E0/3 |
| Робоча станція WS_2_14_16 | Eth0 | Комутатор SW_2_14_5 | E1/2 |
| Робоча станція WS_2_14_17 | Eth0 | Комутатор SW_2_14_5 | E1/0 |
| Робоча станція WS_2_14_18 | Eth0 | Комутатор SW_2_14_5 | E1/1 |
| Робоча станція WS_2_14_19 | Eth0 | Комутатор SW_2_14_6 | E0/1 |
| Робоча станція WS_2_14_20 | Eth0 | Комутатор SW_2_14_6 | E0/2 |
| Робоча станція WS_2_14_21 | Eth0 | Комутатор SW_2_14_6 | E0/3 |
| Робоча станція WS_2_14_22 | Eth0 | Комутатор SW_2_14_6 | E1/0 |
| Робоча станція WS_2_14_23 | Eth0 | Комутатор SW_2_14_7 | E0/2 |
| Робоча станція WS_2_14_24 | Eth0 | Комутатор SW_2_14_7 | E0/3 |
| Робоча станція WS_2_14_25 | Eth0 | Комутатор SW_2_14_7 | E1/0 |
| Робоча станція WS_2_14_26 | Eth0 | Комутатор SW_2_14_7 | E1/1 |
| Робоча станція WS_2_14_27 | Eth0 | Комутатор SW_2_14_8 | E0/1 |
| Робоча станція WS_2_14_28 | Eth0 | Комутатор SW_2_14_8 | E0/2 |

Продовження табл. 2.1

| | | | |
|---|---|---|---|
| Робоча станція WS_2_14_29 | Eth0 | Комутатор SW_2_14_8 | E0/3 |
| Робоча станція WS_2_14_30 | Eth0 | Комутатор SW_2_14_8 | E1/0 |
| Робоча станція WS_2_14_31 | Eth0 | Комутатор SW_2_14_9 | E0/2 |
| Робоча станція WS_2_14_32 | Eth0 | Комутатор SW_2_14_9 | E0/3 |
| Робоча станція WS_2_14_33 | Eth0 | Комутатор SW_2_14_9 | E1/0 |
| Робоча станція WS_2_14_34 | Eth0 | Комутатор SW_2_14_10 | E0/1 |
| Робоча станція WS_2_14_35 | Eth0 | Комутатор SW_2_14_10 | E0/2 |
| Робоча станція WS_2_14_36 | Eth0 | Комутатор SW_2_14_10 | E0/3 |
| Робоча станція WS_2_14_37 | Eth0 | Комутатор SW_2_14_10 | E1/0 |

## 2.2 Розробка параметрів адресації

Для забезпечення функціонування мережі, перш за все були виконано розрахунок адрес мережі. Під час розрахунку параметрів врахована економія адрес та використання масок змінної довжини. Таким чином адресація не забрала багато адрес та їх вдалося використати доволі економно. Для private зони використані діапазони приватних адрес або так звані “сірі” IP-адреси. Internet та Server зони використовують публічні “білі” IP-адреси. Мережа DMVPN використовує також “сірі” IP-адреси, але з іншого діапазону приватних адрес. Для кращого розуміння значення приведемо пояснення щодо термінів IP-адрес.

В мережі Інтернет використовуються саме публічні глобальні адреси. Публічним IP-адресою називається IP-адреса, що використовується для виходу в Інтернет. Публічні (глобальні) IP-адреси маршрутизируются в Інтернеті, на відміну від приватних адрес. Такі адреси ще називають “білими”/

Наявність публічного IP-адреси на вашому маршрутизаторі або комп'ютері дозволить організувати власний сервер (VPN, FTP, WEB та ін.), Віддалений доступ

до комп'ютера, камерам відеоспостереження, і отримати до них доступ з будь-якої точки глобальної мережі.

З "білою" IP-адресою можна організувати будь-який власний домашній сервер для публікації його в мережі Інтернет: веб (HTTP), VPN (PPTP / IPSec / OpenVPN), медіа (аудіо / відео), FTP, мережевий накопичувач NAS, ігровий сервер і т.д. У зв'язку з тим що "білих" IP-адрес існує обмежена кількість, а зростання числа користувачів Інтернету збільшується, інтернет-провайдери все частіше використовують приватні ("сірі") IP-адреси, які призначаються абонентам.

Приватні внутрішні адреси не маршрутизируются в Інтернеті і на них не можна відправити трафік з Інтернету, вони працюють тільки в межах локальної мережі.

До приватних "сірим" адресами відносяться IP-адреси з наступних підмереж:

- Від 10.0.0.0 до 10.255.255.255 з маскою 255.0.0.0 або / 8
- Від 172.16.0.0 до 172.31.255.255 з маскою 255.240.0.0 або / 12
- Від 192.168.0.0 до 192.168.255.255 з маскою 255.255.0.0 або / 16
- Від 100.64.0.0 до 100.127.255.255 з маскою підмережі 255.192.0.0 або / 10; дана підмережа рекомендована згідно rfc6598 для використання в якості адрес для CGN (Carrier-Grade NAT)

Це зарезервовані IP-адреси. Такі адреси призначені для застосування в закритих локальних мережах, розподіл таких адрес ніким не контролюється.

Безпосередньо доступ до мережі Інтернет, використовуючи приватну IP-адресу, неможливий. У цьому випадку зв'язок з Інтернетом здійснюється через NAT (трансляція мережевих адрес замінює приватний IP-адреса на публічний). Приватні IP-адреси в межах однієї локальної мережі повинні бути унікальні і не можуть повторюватися.

Що стосується безпеки в Інтернеті, то використання "сірого" IP-адреси більш безпечно, ніж використання "білого" IP-адреси, тому що "Сірі" IP-адреси не видно безпосередньо в Інтернеті і знаходяться за NAT, який також забезпечує безпеку до-

машньої мережі. При використанні "білого" IP-адреси необхідні заходи для забезпечення додаткової безпеки комп'ютера або сервера (наприклад, використання брандмауера для блокування портів і протоколів, які не використовуються сервером; застосування сегмента мережі DMZ для відділення загальнодоступних сервісів від локальної мережі і т.п. ).

Надалі для кожної зони буде продемонстровані параметри адресації.

Таблиця 2.2

Параметри адресації мережі

| Пристрій | Інтерфейс/Мережний адаптер/Шлюз | IP-адреса | Маска підмережі | Префікс |
|---|---|---|---|---|
| Підмережа A | - | 100.2.14.0 | 255.255.255.252 | /30 |
| Підмережа B | - | 101.2.14.0 | 255.255.255.252 | /30 |
| Підмережа C | - | 102.2.14.0 | 255.255.255.252 | /30 |
| Підмережа D | - | 103.2.14.0 | 255.255.255.252 | /30 |
| Підмережа E | - | 104.2.14.0 | 255.255.255.252 | /30 |
| Підмережа F | - | 105.2.14.0 | 255.255.255.252 | /30 |
| Підмережа G | - | 106.2.14.0 | 255.255.255.252 | /30 |
| Підмережа H | - | 107.2.14.0 | 255.255.255.252 | /30 |
| Підмережа I | - | 108.2.14.0 | 255.255.255.252 | /30 |
| Підмережа J | - | 109.2.14.0 | 255.255.255.252 | /30 |
| Підмережа K | - | 110.2.14.0 | 255.255.255.252 | /30 |
| Підмережа L | - | 111.2.14.0 | 255.255.255.252 | /30 |
| Підмережа M | - | 10.10.10.0(DMVPN) | 255.255.255.0 | /24 |
| Підмережа N | - | 190.2.14.0 | 255.255.255.252 | /24 |
| Підмережа O | - | 191.2.14.0 | 255.255.255.252 | /32 |
| Підмережа P | - | 192.2.14.0 | 255.255.255.252 | /32 |
| Підмережа Q | - | 193.2.14.0 | 255.255.255.252 | /32 |
| Підмережа R | - | 194.2.14.0 | 255.255.255.252 | /32 |
| Підмережа S | - | 192.168.1.0 | 255.255.255.0 | /24 |
| Підмережа T | - | 192.168.2.0 | 255.255.255.0 | /24 |
| Підмережа U | - | 192.168.3.0 | 255.255.255.0 | /24 |
| Підмережа V | - | 192.168.4.0 | 255.255.255.0 | /24 |
| Підмережа W | - | 192.168.5.0 | 255.255.255.0 | /24 |
| Маршрутизатор R_2_14_1 | FastEthernet0/0 | 100.2.14.1 | 255.255.255.252 | /30 |
| | FastEthernet1/0 | 192.168.1.1 | 255.255.255.0 | /24 |
| | FastEthernet2/0 | 190.2.14.1 | 255.255.255.252 | /30 |
| | Tunnel 0 | 10.10.10.1 | 255.255.255.0 | /24 |
| Маршрутизатор R_2_14_2 | FastEthernet0/0 | 101.2.14.1 | 255.255.255.252 | /30 |
| | FastEthernet1/0 | 192.168.2.1 | 255.255.255.0 | /24 |

Продовження табл. 2.2

| | | | | |
|---|---|---|---|---|
| | FastEthernet2/0 | 191.2.14.1 | 255.255.255.252 | /30 |
| | Tunnel 0 | 10.10.10.2 | 255.255.255.0 | /24 |
| Маршрутизатор R_2_14_3 | FastEthernet0/0 | 105.2.14.1 | 255.255.255.252 | /30 |
| | FastEthernet1/0 | 192.168.3.1 | 255.255.255.0 | /24 |
| | FastEthernet2/0 | 192.2.14.1 | 255.255.255.252 | /30 |
| | Tunnel 0 | 10.10.10.3 | 255.255.255.0 | /24 |
| Маршрутизатор R_2_14_4 | FastEthernet0/0 | 107.2.14.1 | 255.255.255.252 | /30 |
| | FastEthernet1/0 | 192.168.4.1 | 255.255.255.0 | /24 |
| | FastEthernet2/0 | 193.2.14.1 | 255.255.255.252 | /30 |
| | Tunnel 0 | 10.10.10.4 | 255.255.255.0 | /24 |
| Маршрутизатор R_2_14_5 | FastEthernet0/0 | 110.2.14.1 | 255.255.255.252 | /30 |
| | FastEthernet1/0 | 192.168.5.1 | 255.255.255.0 | /24 |
| | FastEthernet3/0 | 194.2.14.1 | 255.255.255.252 | /30 |
| | Tunnel 0 | 10.10.10.5 | 255.255.255.0 | /24 |
| Маршрутизатор R_2_14_6 | FastEthernet0/0 | 100.2.14.2 | 255.255.255.252 | /30 |
| | FastEthernet1/0 | 102.2.14.1 | 255.255.255.252 | /30 |
| | FastEthernet2/0 | 103.2.14.2 | 255.255.255.252 | /30 |
| Маршрутизатор R_2_14_7 | FastEthernet0/0 | 101.2.14.2 | 255.255.255.252 | /30 |
| | FastEthernet1/0 | 102.2.14.2 | 255.255.255.252 | /30 |
| | FastEthernet2/0 | 104.2.14.1 | 255.255.255.252 | /30 |
| Маршрутизатор R_2_14_8 | FastEthernet0/0 | 105.2.14.2 | 255.255.255.252 | /30 |
| | FastEthernet1/0 | 103.2.14.2 | 255.255.255.252 | /30 |
| | FastEthernet2/0 | 108.2.14.1 | 255.255.255.252 | /30 |
| | FastEthernet3/0 | 106.2.14.1 | 255.255.255.252 | /30 |
| Маршрутизатор R_2_14_9 | FastEthernet0/0 | 107.2.14.2 | 255.255.255.252 | /30 |
| | FastEthernet1/0 | 104.2.14.2 | 255.255.255.252 | /30 |
| | FastEthernet2/0 | 111.2.14.1 | 255.255.255.252 | /30 |
| | FastEthernet3/0 | 106.2.14.2 | 255.255.255.252 | /30 |
| Маршрутизатор R_2_14_10 | FastEthernet0/0 | 108.2.14.2 | 255.255.255.252 | /30 |
| | FastEthernet1/0 | 109.2.14.1 | 255.255.255.252 | /30 |
| Маршрутизатор R_2_14_11 | FastEthernet0/0 | 110.2.14.2 | 255.255.255.252 | /30 |
| | FastEthernet1/0 | 111.2.14.2 | 255.255.255.252 | /30 |
| | FastEthernet2/0 | 109.2.14.2 | 255.255.255.252 | /30 |
| Комутатор SW_2_14_1 | Інтерфейс Vlan 1 | 192.168.1.250 | 255.255.255.0 | /24 |
| Комутатор SW_2_14_2 | Інтерфейс Vlan 1 | 192.168.1.251 | 255.255.255.0 | /24 |
| Комутатор SW_2_14_3 | Інтерфейс Vlan 1 | 192.168.2.250 | 255.255.255.0 | /24 |
| Комутатор SW_2_14_4 | Інтерфейс Vlan 1 | 192.168.2.251 | 255.255.255.0 | /24 |
| Комутатор SW_2_14_5 | Інтерфейс Vlan 1 | 192.168.3.250 | 255.255.255.0 | /24 |

Продовження табл. 2.2

| | | | | |
|---|---|---|---|---|
| Комутатор SW_2_14_6 | Інтерфейс Vlan 1 | 192.168.3.251 | 255.255.255.0 | /24 |
| Комутатор SW_2_14_7 | Інтерфейс Vlan 1 | 192.168.4.250 | 255.255.255.0 | /24 |
| Комутатор SW_2_14_8 | Інтерфейс Vlan 1 | 192.168.4.251 | 255.255.255.0 | /24 |
| Комутатор SW_2_14_9 | Інтерфейс Vlan 1 | 192.168.5.250 | 255.255.255.0 | /24 |
| Комутатор SW_2_14_10 | Інтерфейс Vlan 1 | 192.168.5.251 | 255.255.255.0 | /24 |
| Сервер Serv_2_14_1 | Ethernet0 | 190.2.14.2 | 255.255.255.0 | /30 |
| | Шлюз за замов-чуванням | 190.2.14.1 | - | - |
| Сервер Serv_2_14_2 | Ethernet0 | 191.2.14.2 | 255.255.255.252 | /30 |
| | Шлюз за замов-чуванням | 191.2.14.1 | - | - |
| Сервер Serv_2_14_3 | Ethernet0 | 192.2.14.2 | 255.255.255.252 | /30 |
| | Шлюз за замов-чуванням | 192.2.14.1 | - | - |
| Сервер Serv_2_14_4 | Ethernet0 | 193.2.14.2 | 255.255.255.252 | /30 |
| | Шлюз за замов-чуванням | 193.2.14.1 | - | - |
| Сервер Serv_2_14_4 | Ethernet0 | 194.2.14.2 | 255.255.255.252 | /30 |
| | Шлюз за замов-чуванням | 194.2.14.1 | - | - |
| Робоча станція WS_2_14_1 | Ethernet0 | DHCP | | |
| Робоча станція WS_2_14_2 | | | | |
| Робоча станція WS_2_14_3 | | | | |
| Робоча станція WS_2_14_4 | | | | |
| Робоча станція WS_2_14_5 | | | | |
| Робоча станція WS_2_14_6 | | | | |
| Робоча станція WS_2_14_7 | | | | |
| Робоча станція WS_2_14_8 | | | | |
| Робоча станція WS_2_14_9 | | | | |
| Робоча станція WS_2_14_10 | | | | |
| Робоча станція WS_2_14_11 | | | | |

Продовження табл. 2.2

| | | |
|---|---|---|
| Робоча станція WS_2_14_12 | Ethernet0 | DHCP |
| Робоча станція WS_2_14_13 | | |
| Робоча станція WS_2_14_13 | | |
| Робоча станція WS_2_14_14 | | |
| Робоча станція WS_2_14_15 | | |
| Робоча станція WS_2_14_16 | | |
| Робоча станція WS_2_14_17 | | |
| Робоча станція WS_2_14_18 | | |
| Робоча станція WS_2_14_19 | | |
| Робоча станція WS_2_14_20 | | |
| Робоча станція WS_2_14_21 | | |
| Робоча станція WS_2_14_22 | | |
| Робоча станція WS_2_14_23 | | |
| Робоча станція WS_2_14_24 | | |
| Робоча станція WS_2_14_25 | | |
| Робоча станція WS_2_14_26 | | |
| Робоча станція WS_2_14_27 | | |
| Робоча станція WS_2_14_28 | | |
| Робоча станція WS_2_14_29 | | |
| Робоча станція WS_2_14_30 | | |
| Робоча станція WS_2_14_31 | | |
| Робоча станція WS_2_14_32 | | |
| Робоча станція WS_2_14_33 | | |
| Робоча станція WS_2_14_34 | | |

Продовження табл. 2.2

| | | |
|---|---|---|
| Робоча станція WS_2_14_35 | Ethernet0 | DHCP |
| Робоча станція WS_2_14_36 | | |
| Робоча станція WS_2_14_37 | | |

Отже, після визначення з топологією мережі, та розрахунком параметрів адресації, перейдемо до визначення політик безпеки, які є основоположними в будь-якій мережі VPN.

## 2.3 Розробка політик безпеки

Важливим питанням при створенні VPN є те, що в кожній локальній мережі повинні використовуватися еквівалентні політики безпеки. VPN по суті створює одну велику мережу з групи незалежних раніше мереж. Тому безпека VPN буде дорівнювати безпеці найменш захищеної локальної мережі - якщо хоча б одна локальна мережа дозволяє здійснити незахищений доступ по комутованих лініях, то під загрозою опиняться всі ресурси VPN.

Відповідно до загальноприйнятого визначення, безпеку даних означає їх конфіденційність, цілісність і доступність. Що стосується завданням VPN критерії безпеки можуть бути визначені наступним чином:

- Конфіденційність - гарантія того, що в процесі передачі по захищених каналах VPN дані не можуть бути переглянуті ніким, крім легальних відправника і одержувача.
- Цілісність - гарантія збереження незмінності передаваних даних під час проходження по захищеному каналу VPN.
- Доступність - гарантія того, що кошти, які виконують функції VPN, постійно доступні легальним користувачам.
- Доступність засобів VPN - це комплексний показник, що залежить від кількох факторів: надійності реалізації, якості обслуговування, а також ступеня захищеності самого кошти від зовнішніх атак. Якщо засіб VPN підтримується

провайдером, то доступність є однією з характеристик, зазвичай включаються в угоду про рівень сервісу.

VPN не можуть робити онлайн-з'єднання повністю анонімними, але зазвичай вони можуть підвищити конфіденційність і безпеку. Щоб запобігти розкриттю приватної інформації, VPN зазвичай дозволяють лише аутентіфіцированний віддалений доступ з використанням протоколів тунелювання і методів шифрування.

Також потрібно звертати увагу на можливість неправильного налаштування, що дає базову безпеку, може стати причиною витоку даних. Це безпосередньо суперечить меті використання VPN як засобу конфіденційності. Щоб не потрапити в халепу, варто уважно ознайомитися з політикою конфіденційності вашого провайдера.

Нікому не хочеться потрапити в незручне становище зіткнувшись з тим, що VPN не виконує функцій, на нього покладених. Для цього будь-яку обіцянку гарантії надійності і безпеки варто перевіряти самостійно. Багато VPN-сервісів зберігають ваші метадані, історію вашого трафіку і т.д. Переконайтеся, що політика конфіденційності задовольняє вас і ваші очікування від використання інструменту від того чи іншого розробника. І це стосується не тільки такого інструменту, як VPN.

Існує три основні варіанти створення VPN:

1. Захищені канали. Міжмережевий екран або маршрутизатор шифрує весь трафік, що передається по віддаленого хосту (хост - це комп'ютер, який має унікальну IP-адресу) або мережі, і розшифровує весь трафік, прийнятий від них. Трафік між хостами в VPN, пов'язаними захищеними каналами, передається вільно. Насправді трафік маршрутизируется маршрутизатором або міжмережевим екраном VPN. Його обробка проксі-серверами (proxy-сервер, або сервер повноважень, або сервер-посередник чекає директив з мережі, пересилає запит до віддаленого сервера, розташованого за межами захисної системи, отримує від нього відповідне повідомлення і передає його за призначенням) і аутентифікація не потрібна. Будь-які два хоста всередині VPN, пов'язані захищеними каналами, можуть вільно обмінюватися даними між собою, і надавати всі сервіси TCP / IP, які у них є. Захищені

канали часто використовуються для з'єднання географічно розділених мереж, що належать одній організації, кожна з яких має своє власне підключення до Internet через провайдера, в одну віртуальну мережу безпечним способом.

2. Приватні канали. Трафік між маршрутизатором і віддаленим хостом шифрується так само, як і для захищеного каналу. Але трафік між віддаленими хостами, пов'язаними приватними каналами, не передається вільно, а повинен бути оброблений проксі сервером МЕ і з'єднання аутентифицироваться, як того вимагає звичайна політика доступу для проксі-сервера. Цей вид каналу забезпечує аутентифікацію відправника трафіку і конфіденційність даних, але в даному випадку дві мережі забезпечують наявність двох різних периметрів безпеки, і можуть використовуватися тільки ті сервіси, для яких налаштована передача проксі-сервера в МЕ. Приватні канали часто використовуються для організації зв'язку між мережами різних організацій, які не хочуть надавати повного доступу до їхніх мереж, і вимагають конфіденційності трафіку між ними

3. Проміжні канали. Ці канали використовуються для проміжної передачі зашифрованого трафіку між хостами, розташованими за маршрутизатором чи міжмережевого екрану і входять до складу іншого VPN. Це дозволяє маршрутизатору, що знаходиться між двох інших VPN, бути сконфігурованим так, щоб передавати тільки зашифровані дані. Він не розшифровує трафік і навіть не знає ключа шифрування.

Використовуючи тільки що введені поняття каналів VPN, наведемо приклади деяких політик безпеки (ПБ) при використанні каналів Internet для побудови VPN.

1. Для високих ПБ VPN , що використовують Internet, маршуртизатори організації повинні працювати в режимі приватного каналу, шифрувати трафік VPN і вимагати використання проксі-серверів для обмеження доступу до сервісів з боку віддалених хостів VPN. Також повинні бути кошти, що забезпечують швидке створення резервного каналу для передачі в разі тимчасової неможливості передачі через Internet.

2. Для Низько-середньої ПБ VPN, що використовують Internet, маршрутизатори організації повинні працювати в режимі захищеного каналу, шифрувати трафік VPN і не вимагати використання проксі серверів для його обробки.
3. Для Середньо-високих ПБ, VPN між локальними не повинні використовувати Internet для передачі критичного до оперативності передачі трафіку. Якщо рівень надійності, що надається Internet, недостатній для забезпечення необхідного рівня сервісу, для передачі даних повинні використовуватися інші способи.

Дізнавшись загальні поняття про політики безпеки VPN, сформулюємо свої власні правила та вимоги мережі DMVPN. Перш за все наша мережа будуватиметься на захищених каналах, весь трафік потрібно шифрувати за допомогою відповідних протоколів. Користувачі повинні мати прямий доступ зв'язку один до одного. Для кращого захисту мережі потрібно використати аутентифікацію на рівні тунельних каналів, на рівні протоколу NHRP, а також на рівні протоколу BGP. Для шифрування трафіку використати найбільш сучасні методи, зокрема IKEv2 (Internet Key Exchange). Доступ для конфігурування пристроїв повинен бути лише в межах локальної зони з відповідними користувачами, які будуть мати різні рівні привілеїв. Потребується висока доступність та відмовостійкість мережі. Для цього буде використано 2 хаби, які зможуть брати роль головного один в одного під час екстренних ситуацій, таких припинення зв'язку, або пошкодження каналу.

Певні співробітники компанії й авторизовані партнери (клієнти, постачальники і т. Д.) Можуть використовувати VPN, що є службою, контрольованої користувачем. Це означає, що користувач відповідальний за вибір провайдера послуг інтернет, координацію установки устаткування і ПО і оплату відповідних тарифів. Подальша інформація доступна в політиці віддаленого доступу.

Отже, в другому розділі був обгрунтований проект мережі, вибрано оптимальне обладнання для нього, визначені параметри адресації пристроїв та фізична топологія. Фінальним етапом стало обгрунтування політик безпеки організації.

# РОЗДІЛ 3. НАЛАГОДЖЕННЯ ОБЛАДНАННЯ МЕРЕЖІ, ЇЇ ДІАГНОСТИКА ТА ТЕСТУВАННЯ

## 3.1 Базове налагодження мережі

Перш за все потрібно почати налаштування мережі зі зміни назв хостів. Це допоможе структирозувати схему та додасть зручності в налаштуванні. Надати назву пристрою можна в конфігураційному режимі за допомогою команди host-name. Команда do copy running-config startup-config дозволяє зберегти налаштування пристрою з конфігураційного режиму.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R_2_14_1
R_2_14_1(config)#do copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R_2_14_1(config)#
```

Наступним кроком стане налаштування інтерфейсів маршуртизаторів. Для цього потрібно спочатку увійти в конфігураційний режим, потім в режим конфігурвання інтерфейсу і за допомогою команди ip address задати налуштування на кожен інтерфейс, який маршрутизатор чи комутатор буде використовувати. Команда no shutdown використовується для увімкнення інтерфейсу. Наведено налаштування на одному з інтерфейсів. Для всіх інших пристроїв налаштування буде виглядати аналогічним чином. Відмінність буде в налаштуванні комутаторів. Там потрібно налаштовувати не фізичний, а віртуальний інетрфейс vlan 1.

R_2_14_1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R_2_14_1(config)#interface fa0/0

R_2_14_1(config-if)#ip address 100.2.14.1 255.255.255.252

R_2_14_1(config-if)#no shutdown

R_2_14_1(config-if)#

*Jun  9 17:37:08.079: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed stateo up

*Jun  9 17:37:09.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtheet0/0, changed

Як було зазначено в розділі 2  для зручності і спрощення налаштування кінцевих пристроїв потрібно використати протокол динамічної роздачі IP-адрес. Було вирішено використати DHCP. DHCP(Dynamic Host Configuration Protocol) - являє собою мережевий протокол, що дозволяє мережевим пристроям автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі TCP / IP [22]. Даний протокол працює по моделі «клієнт-сервер». Тобто клієнт звертається до так званого сервера DHCP і отримує від нього потрібні параметри. Мінімальними параметрами для успішного зв'язку між клієнтом і сервером є IP-адреса виділена з набору адрес для private зони, маска підмережі та адреса шлюзу, або іншими словами серверу. В якості DHCP серверу буде виступати граничний маршрутизатор, який буде роздавати IP-адреси клієнтам. Таким чином користувачам не потрібно буде статично прописувати свої адреси, а вони зможуть їх отримувати безпосередньо від DHCP серверу. Налаштування приведено нижче. Виключити певні адреси з пулу IP-адрес можна за допомогою команди ip dhcp excluded-address. В нашому випадку нам потрібно виключити адресу маршрутизатору та комутаторів, які розташовані в локальній зоні. Команда ip dhcp pool по суті створює DHCP pool, в якому потрібно прописати команду network для роздачі IP-адрес. Команда default-router зазначає шлюз по замовчуванню. В нашому випадку цю роль бере на себе DHCP-сервер.

R_2_16_1(config)#ip dhcp excluded-address 192.168.1.1

R_2_16_1(config)#ip dhcp excluded-address 192.168.1.250

R_2_16_1(config)#ip dhcp excluded-address 192.168.1.251

R_2_16_1 (config)#ip dhcp pool LAN_A1

R_2_16_1 (dhcp-config)# network 192.168.2.0 255.255.255.0

R_2_16_1 (dhcp-config)# default-router 192.168.2.1

Після налаштування потрібно налаштувати віддалене підключення. Чудовим рішенням стане SSH. SSH(Secure Shell) - мережевий протокол прикладного рівня, що дозволяє здійснювати віддалене управління операційною системою. На відміну від Telnet він здійснює захищене піключення шифруючи весь трафік, включаючи і паролі. Надалі приведемо пояснення щодо основних команд. Спочатку потрібно задати домен та згенерувати RSA ключ за допомогою команди crypto key generate rsa. Команда service password-encryption буде шифрувати локальні паролі і вони не будуть доступні у відкритому вигляді переглядаючи конфіги. Командою username створимо користувачів з різними рівнями доступу. Додамо список доступу за допомогою команди access-list, щоб тільки користувачі з локальної мережі мали змогу авторизуватись в консолі. Далі в режимі конфігурування vty ліній додамо підтримку SSH командою transport input ssh та використання локальних користувачів для авторизації командами logging synchronous, login local. В цьому ж інтерфейсі потрібно

R_2_14_1>enable

R_2_14_1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R_2_14_1(config)#ip domain name cisco.com

R_2_14_1(config)#crypto key generate rsa

The name for the keys will be: R_2_14_1.cisco.com

Choose the size of the key modulus in the range of 360 to 4096 for your

```
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R_2_14_1(config)#service password-encryption
R_2_14_1(config)#username Admin_2_14_1 privilege 15 secret twibro123
R_2_14_1(config)#username User_2_14_1 privilege 10 secret twibro123
R_2_14_1(config)#username User_2_14_2 privilege 5 secret twibro123
R_2_14_1(config)#enable secret twibro123
R_2_14_1(config)#access-list 23 permit 192.168.5.0 0.0.0.255
R_2_14_1(config)#line vty 0 4
R_2_14_1(config-line)#transport input ssh
R_2_14_1(config-line)#logging synchronous
R_2_14_1(config-line)#login local
R_2_14_1(config-line)#exec-timeout 60 0
R_2_14_1(config-line)#access-class 23 in
R_2_14_1(config-line)#exit
R_2_14_1(config)#line console 0
R_2_14_1(config-line)#login local
*Jun  9 18:34:49.727: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Фінальним етапом базового налашутвання стане налаштування статичної маршрутизації. Для цього в режимі конфігурування терміналу пропишемо маршрути, про які маршрутизатор не знає. Після того, як ми виконаємо цю операцію на всіх маршрутизаторах ми будемо мати зв'язок між всіма пристроями всередині зони Internet. Також для кращої відмовостійкості мережі потрібно зазначити резервні ма-

ршрути, які будуть активні у разі технічних проблем всередині мережі. Для прикладу візьмемо маршрутизатор під номером 8. Як можна побачити в прикладах нижче використовується команда ip route. В граничних маршрутизаторах будуть маршрути по замовчуванню.

```
R_2_14_6(config)#ip route 101.2.14.0 255.255.255.252 FastEthernet1/0
R_2_14_6(config)#ip route 101.2.14.0 255.255.255.252 FastEthernet2/0 5
R_2_14_6(config)#ip route 104.2.14.0 255.255.255.252 FastEthernet1/0
R_2_14_6(config)#ip route 104.2.14.0 255.255.255.252 FastEthernet2/0 5
R_2_14_6(config)#ip route 105.2.14.0 255.255.255.252 FastEthernet2/0
R_2_14_6(config)#ip route 105.2.14.0 255.255.255.252 FastEthernet1/0 5
R_2_14_6(config)#ip route 106.2.14.0 255.255.255.252 FastEthernet2/0
R_2_14_6(config)#ip route 106.2.14.0 255.255.255.252 FastEthernet1/0 5
R_2_14_6(config)#ip route 107.2.14.0 255.255.255.252 FastEthernet1/0
R_2_14_6(config)#ip route 107.2.14.0 255.255.255.252 FastEthernet2/0 5
R_2_14_6(config)#ip route 108.2.14.0 255.255.255.252 FastEthernet2/0
R_2_14_6(config)#ip route 108.2.14.0 255.255.255.252 FastEthernet1/0 5
R_2_14_6(config)#ip route 109.2.14.0 255.255.255.252 FastEthernet2/0
R_2_14_6(config)#ip route 109.2.14.0 255.255.255.252 FastEthernet1/0 5
R_2_14_6(config)#ip route 110.2.14.0 255.255.255.252 FastEthernet2/0
R_2_14_6(config)#ip route 110.2.14.0 255.255.255.252 FastEthernet1/0 5
R_2_14_6(config)#ip route 111.2.14.0 255.255.255.252 FastEthernet1/0
R_2_14_6(config)#ip route 111.2.14.0 255.255.255.252 FastEthernet2/0 5
```

### 3.2 Налагодження аспектів технології DMVPN

Будь-яке налашутвання DMVPN краще почати з налаштування віртуальних т mGRE тунелів. Для адресації виділена мережа 10.10.10.0/24, всі тунелі знаходяться в одній мережі. Для цього розглянемо налаштування на маршрутизаторі R_2_16_1,

всі інші spokes налаштовуються аналогічно. Про те, яка специфіка робота тунелів було приведено в розділі 1. В цьому підрозділі буде висвітлено лиш роз'яснення щодо конфігураційних команд. Перш за все потрібно почати зі створення тунелю та задання відповідної IP-адреси. Так як GRE додає додаткові заголовки до IP-пакету, необхідно змінити значення MTU на інтерфейсі за допомогою команди ip mtu. Команда tunnel source налаштовує співвідношення відповідності між тунельним інтерфейсом і фізичним. Для захисту також додамо ідентифікаційний ключ на тунель. Він буде слугувати певним ідентифікатором.

R_2_14_1(config)#interface Tunnel 0

R_2_14_1(config-if)#

*Dec 27 00:06:27.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel16, changed state to down

R_2_14_1(config-if)#ip address 10.10.10.1 255.255.255.0

R_2_14_1(config-if)#ip mtu 1416

R_2_14_1(config-if)#tunnel source FastEthernet0/0

R_2_14_1(config-if)#tunnel mode gre multipoint

R_2_14_1(config-if)#tunnel key 999

Далі перейдемо до налаштування протоколу NHRP. Слід зауважити, що налаштування для hub та spoke буде відрізнятись. Так як в схемі у нас присутні два хаби, то другий hub буде мати дві ролі: як NHRP сервер так і spoke клієнт. Протокол NHRP буде автоматично визначати адресами spoke-маршрутизаторів. Це буде можливо за допомогою команди ip nhrp map multicast dynamic. Команда ip nhrp redirect потрібна для увімкнення 3 фази DMVPN і її конфігурація потрібна лише на Hub маршрутизаторах. Для увімкнення 3 фази на Spokes використаємо команду ip nhrp shortcut. Також для захисту увімкнено авторизацію по паролю.

Налаштування на Hub-маршрутизаторі(R_2_14_1):

R_2_14_1#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R_2_14_1(config)#int Tunnel 0

R_2_14_1(config-if)#ip nhrp network-id 333

R_2_14_1(config-if)#ip nhrp map multicast dynamic

R_2_14_1(config-if)#ip nhrp authentication nhrppass

R_2_14_1(config-if)#ip nhrp redirect

Налаштування на Hub-маршрутизаторі(R_2_14_2):

R_2_14_2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

R_2_14_2(config)#int Tunnel 0

R_2_14_2(config-if)#ip nhrp network-id 333

R_2_14_2(config-if)#ip nhrp map multicast dynamic

R_2_14_2(config-if)#ip nhrp map multicast 100.2.14.1

R_2_14_2(config-if)#ip nhrp map 10.10.10.1 100.2.14.1

R_2_14_2(config-if)#ip nhrp nhs 10.10.10.1

R_2_14_2(config-if)#ip nhrp authentication nhrppass

R_2_14_2(config-if)#ip nhrp redirect

Налаштування на Spoke-маршрутизаторі:

R_2_14_4(config)#int Tunnel0

R_2_14_4(config-if)#ip nhrp network-id 333

R_2_14_4(config-if)#ip nhrp nhs 10.10.10.1

R_2_14_4(config-if)#ip nhrp nhs 10.10.10.2

R_2_14_4(config-if)#ip nhrp map 10.10.10.1 100.2.14.1

R_2_14_4(config-if)#ip nhrp map 10.10.10.2 101.2.14.1

R_2_14_4(config-if)#ip nhrp map multicast 100.2.14.1

R_2_14_4(config-if)#ip nhrp map multicast 101.2.14.1

R_2_14_4(config-if)#ip nhrp authentication nhrppass

R_2_14_4(config-if)#ip nhrp shortcut

Наступним кроком стане налаштування BGP, щоб з локальної зони можна було користувачам мати доступ саме через тунелі. Важливим моментом стане використання Hub маршрутизаторів в ролі route-reflectors. Є у нас доволі велика кількість маршрутизаторів, нам потрібно вибрати один роутер, і зробити його сервером (дзеркалом), кожен роутер матиме тільки один лінк до цього сервера, такі роутери називаються клієнтами. Такий сервер (reflector) і клієнти в сукупності називаються кластерами. Тепер, отримуючи маршрут Route Reflector відправляє своїм клієнтам цей маршрут, клієнт отримує і не відправляє нікому, адже у нього немає лінків більше ні з ким. Таким чином суттєво скорочується кількість налаштувань і звичайно ж TCP сесій.

Налаштування на Hub-маршрутизаторі(R_2_14_2):

R_2_14_2(config)#router bgp 333

R_2_14_2(config-router)# bgp cluster-id 333

R_2_14_2(config-router)# bgp log-neighbor-changes

R_2_14_2(config-router)# network 191.2.14.0 mask 255.255.255.252

R_2_14_2(config-router)# network 192.168.2.0

R_2_14_2(config-router)# neighbor 10.10.10.1 remote-as 333

R_2_14_2(config-router)# neighbor 10.10.10.1 password 7 15061C05063824757A60

R_2_14_2(config-router)# neighbor 10.10.10.1 update-source Tunnel0

R_2_14_2(config-router)# neighbor 10.10.10.1 next-hop-self

R_2_14_2(config-router)# neighbor 10.10.10.3 remote-as 333

R_2_14_2(config-router)# neighbor 10.10.10.3 password 7 120D121E101903557878

R_2_14_2(config-router)# neighbor 10.10.10.3 update-source Tunnel0

R_2_14_2(config-router)# neighbor 10.10.10.3 route-reflector-client

R_2_14_2(config-router)# neighbor 10.10.10.3 next-hop-self

R_2_14_2(config-router)# neighbor 10.10.10.4 remote-as 333

R_2_14_2(config-router)# neighbor 10.10.10.4 password 7 105A1E1007051D5A5E57

R_2_14_2(config-router)# neighbor 10.10.10.4 update-source Tunnel0

R_2_14_2(config-router)# neighbor 10.10.10.4 route-reflector-client

R_2_14_2(config-router)# neighbor 10.10.10.4 next-hop-self

R_2_14_2(config-router)# neighbor 10.10.10.5 remote-as 333

R_2_14_2(config-router)# neighbor 10.10.10.5 password 7 120D121E101903557878

R_2_14_2(config-router)# neighbor 10.10.10.5 update-source Tunnel0

R_2_14_2(config-router)# neighbor 10.10.10.5 route-reflector-client

R_2_14_2(config-router)# neighbor 10.10.10.5 next-hop-self

Налаштування на Spoke-маршрутизаторі:

R_2_14_5(config)#router bgp 333

R_2_14_5(config-router)# bgp log-neighbor-changes

R_2_14_5(config-router)# network 192.168.5.0

R_2_14_5(config-router)# network 194.2.14.0 mask 255.255.255.252

R_2_14_5(config-router)# neighbor 10.10.10.1 remote-as 333

R_2_14_5(config-router)# neighbor 10.10.10.1 password 7 051F1106235E41584B56

R_2_14_5(config-router)# neighbor 10.10.10.1 update-source Tunnel0

R_2_14_5(config-router)# neighbor 10.10.10.1 next-hop-self

R_2_14_5(config-router)# neighbor 10.10.10.2 remote-as 333

R_2_14_5(config-router)# neighbor 10.10.10.2 password 7 03104C02041D2E1D1C5A

R_2_14_5(config-router)# neighbor 10.10.10.2 update-source Tunnel0

R_2_14_5(config-router)# neighbor 10.10.10.2 next-hop-self

Для захисту тунельних з'єднань налаштуємо IPsec шифрування з IKEv2.

R_2_14_5(config)#crypto ikev2 keyring DMVPN

R_2_14_5(config-ikev2-keyring)#peer DMVPN

R_2_14_5(config-ikev2-keyring-peer)#address 0.0.0.0 0.0.0.0

R_2_14_5(config-ikev2-keyring-peer)#pre-shared-key twibro123

R_2_14_5(config-ikev2-keyring-peer)#exit

R_2_14_5(config-ikev2-keyring)#crypto ikev2 profile DMVPN_IKEv2

IKEv2 profile MUST have:

1. A local and a remote authentication method.
2. A match identity or a match certificate statement.

R_2_14_5(config-ikev2-profile)#match identity remote address 0.0.0.0

R_2_14_5(config-ikev2-profile)#authentication remote pre-share

R_2_14_5(config-ikev2-profile)#authentication local pre-share

R_2_14_5(config-ikev2-profile)#keyring local DMVPN

R_2_14_5(config-ikev2-profile)#exit

R_2_14_5(config)#crypto ipsec transform-set DMVPN esp-aes esp-sha256-hmac

R_2_14_5(cfg-crypto-trans)#mode transport

R_2_14_5(cfg-crypto-trans)#exit

R_2_14_5(config)#crypto ipsec profile DMVPN_Profile

R_2_14_5(ipsec-profile)#set transform-set DMVPN

R_2_14_5(ipsec-profile)#set ikev2-profile DMVPN_IKEv2

R_2_14_5(ipsec-profile)#exit

R_2_14_5(config)#int Tunnel0

R_2_14_5(config-if)#tunnel protection ipsec profile DMVPN_Profile

*Jun 12 09:33:37.279: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

## 3.3 Діагностування та тестування налаштувань

Перш за все перевіримо роботу DHCP. Клієнти повинні отримувати IP-адресу, відповідну маску та шлюз по замовчуванню. Як бачимо з рисунку 3.1 – DHCP успішно функціонує.




Рисунок 3.1 – Перевірка роботи DHCP

Наступним кроком стане перевірка віддаленого підключення через SSH. Є можливість успішно під'єднуватись з маршрутизатора до комутаторів і навпаки в межах своїх локальних зон.

```
R_2_14_2#ssh -l Admin_2_14_1 192.168.2.250
Password:

SW_2_14_3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_2_14_3(config)#
```

Рисунок 3.2 – Перевірка роботи віддаленого підключення через SSH

Для перевірки роботи статичної маршрутизації виконаємо службову команду show ip route на кількох маршрутизаторах.

```
R_2_14_8#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      100.0.0.0/30 is subnetted, 1 subnets
S        100.2.14.0 is directly connected, FastEthernet1/0
      101.0.0.0/30 is subnetted, 1 subnets
S        101.2.14.0 is directly connected, FastEthernet1/0
      102.0.0.0/30 is subnetted, 1 subnets
S        102.2.14.0 is directly connected, FastEthernet1/0
      103.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        103.2.14.0/30 is directly connected, FastEthernet1/0
L        103.2.14.2/32 is directly connected, FastEthernet1/0
      104.0.0.0/30 is subnetted, 1 subnets
S        104.2.14.0 is directly connected, FastEthernet1/0
      105.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        105.2.14.0/30 is directly connected, FastEthernet0/0
L        105.2.14.2/32 is directly connected, FastEthernet0/0
      106.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        106.2.14.0/30 is directly connected, FastEthernet3/0
L        106.2.14.1/32 is directly connected, FastEthernet3/0
      107.0.0.0/30 is subnetted, 1 subnets
S        107.2.14.0 is directly connected, FastEthernet1/0
      108.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        108.2.14.0/30 is directly connected, FastEthernet2/0
L        108.2.14.1/32 is directly connected, FastEthernet2/0
      109.0.0.0/30 is subnetted, 1 subnets
S        109.2.14.0 is directly connected, FastEthernet2/0
      110.0.0.0/30 is subnetted, 1 subnets
S        110.2.14.0 is directly connected, FastEthernet2/0
      111.0.0.0/30 is subnetted, 1 subnets
S        111.2.14.0 is directly connected, FastEthernet2/0
```

Рисунок 3.3 – Виконання службової команди на R_2_14_8 для перевірки роботи статичної маршрутизації

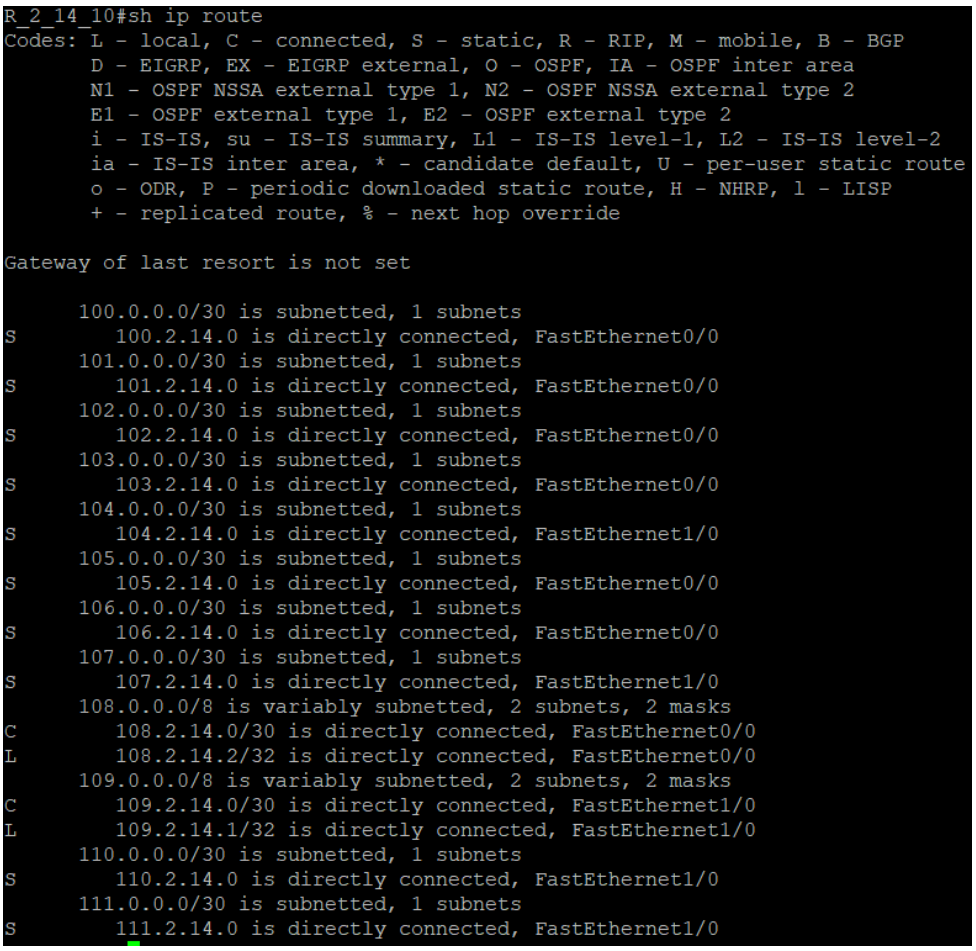



Рисунок 3.4 – Виконання службової команди на R_2_14_10 для перевірки роботи статичної маршрутизації

Переконавшись що статична маршрутизація успішно функціонує і маршрути вивчаються коректно перейдомо до перевірки роботи mGRE тунелів.

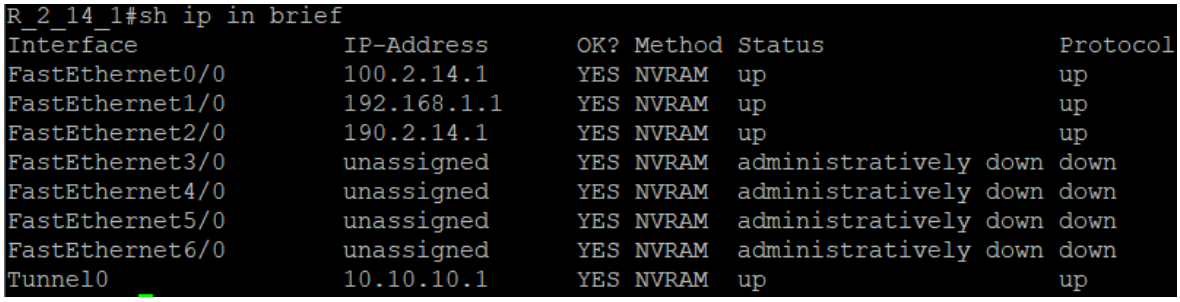



Рисунок 3.5 – Виконання команди show ip int brief на R_2_14_1

```
R_2_14_1#show int Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.10.10.1/24
  MTU 17870 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 100.2.14.1 (FastEthernet0/0)
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with FastEthernet0/0
          Set of tunnels with source FastEthernet0/0, 1 member (includes iterato
rs), on interface <OK>
  Tunnel protocol/transport multi-GRE/IP
    Key 0x14D, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1430 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
```

Рисунок 3.6 – Виконання команди show int tunnel 0 на R_2_14_1

```
R_2_14_1#ping 10.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/63/84 ms
R_2_14_1#ping 10.10.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/73/84 ms
R_2_14_1#ping 10.10.10.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/72/84 ms
R_2_14_1#ping 10.10.10.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/88/108 ms
```

Рисунок 3.7 – Виконання команди ping між всіма граничними маршрутизаторами

Далі проведемо перевірку NHRP. Як бачимо з команди show ip nhrp brief тунелі між spokes створюються динамічно і потім з'єднання закривається коли час асоціації закінчується.

```
R_2_14_5#sh ip nhrp nhs
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
10.10.10.1  RE priority = 0 cluster = 0
10.10.10.2  RE priority = 0 cluster = 0
```

Рисунок 3.8 – Виконання команди show ip nhrp nhs на R_2_14_5

```
R_2_14_5#sh ip nhrp brief
   Target             Via             NBMA           Mode   Intfc   Claimed
10.10.10.1/32        10.10.10.1      100.2.14.1      static   Tu0     <   >
10.10.10.2/32        10.10.10.2      101.2.14.1      static   Tu0     <   >
```

```
R_2_14_5#sh ip nhrp brief
   Target             Via             NBMA           Mode   Intfc   Claimed
10.10.10.1/32        10.10.10.1      100.2.14.1      static   Tu0     <   >
10.10.10.2/32        10.10.10.2      101.2.14.1      static   Tu0     <   >
10.10.10.3/32        10.10.10.3      105.2.14.1      dynamic  Tu0     <   >
10.10.10.5/32        10.10.10.5      110.2.14.1      dynamic  Tu0     <   >
```

Рисунок 3.9-3.10 – Перевірка створених тунелів до команди ping між R_5 і R_3, та після неї

```
R_2_14_1#sh ip nhrp
10.10.10.2/32 via 10.10.10.2
   Tunnel0 created 00:25:47, expire 01:47:35
   Type: dynamic, Flags: unique registered used
   NBMA address: 101.2.14.1
10.10.10.3/32 via 10.10.10.3
   Tunnel0 created 00:25:47, expire 01:34:26
   Type: dynamic, Flags: unique registered used
   NBMA address: 105.2.14.1
10.10.10.4/32 via 10.10.10.4
   Tunnel0 created 00:25:50, expire 01:34:36
   Type: dynamic, Flags: unique registered used
   NBMA address: 107.2.14.1
10.10.10.5/32 via 10.10.10.5
   Tunnel0 created 00:25:47, expire 01:34:56
   Type: dynamic, Flags: registered used
   NBMA address: 110.2.14.1
```

```
R_2_14_1#sh ip nhrp traffic
Tunnel0: Max-send limit:100Pkts/10Sec, Usage:0%
    Sent: Total 8
          3 Resolution Request  0 Resolution Reply  0 Registration Request
          5 Registration Reply  0 Purge Request  0 Purge Reply
          0 Error Indication  0 Traffic Indication  0 Redirect Suppress
    Rcvd: Total 8
          3 Resolution Request  0 Resolution Reply  5 Registration Request
          0 Registration Reply  0 Purge Request  0 Purge Reply
          0 Error Indication  0 Traffic Indication  0 Redirect Suppress
```

Рисунок 3.11-3.12 – Виконання різних службових команд для перевірки роботи nhrp на R_2_16_1

Роботу BGP можна перевірити за допомогою службових команд представлених нижче.

```
R_2_14_1#show ip bgp summary
BGP router identifier 192.168.1.1, local AS number 333
BGP table version is 10, main routing table version 10
9 network entries using 1296 bytes of memory
14 path entries using 1120 bytes of memory
2/2 BGP path/bestpath attribute entries using 272 bytes of memory
3 BGP rrinfo entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2760 total bytes of memory
BGP activity 9/0 prefixes, 14/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State
/PfxRcd
10.10.10.2      4          333      41      44       10    0    0 00:33:31
  7
10.10.10.3      4          333      35      46       10    0    0 00:34:34
  2
10.10.10.4      4          333      35      45       10    0    0 00:34:26
  2
10.10.10.5      4          333      40      45       10    0    0 00:34:03
  1
```

```
R_2_14_2#show ip bgp
BGP table version is 10, local router ID is 192.168.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 190.2.14.0/30    10.10.10.1               0    100      0 i
 *>  191.2.14.0/30    0.0.0.0                  0         32768 i
 * i 192.2.14.0/30    10.10.10.3               0    100      0 i
 *>i                  10.10.10.3               0    100      0 i
 *>i 192.168.1.0      10.10.10.1               0    100      0 i
 *>  192.168.2.0      0.0.0.0                  0         32768 i
 * i 192.168.3.0      10.10.10.3               0    100      0 i
 *>i                  10.10.10.3               0    100      0 i
 * i 192.168.4.0      10.10.10.4               0    100      0 i
 *>i                  10.10.10.4               0    100      0 i
 * i 192.168.5.0      10.10.10.5               0    100      0 i
 *>i                  10.10.10.5               0    100      0 i
 * i 193.2.14.0/30    10.10.10.4               0    100      0 i
 *>i                  10.10.10.4               0    100      0 i
```

```
R_2_14_5#sh ip bgp neighbors
BGP neighbor is 10.10.10.1,  remote AS 333, internal link
  BGP version 4, remote router ID 192.168.1.1
  BGP state = Established, up for 00:32:17
  Last read 00:00:15, last write 00:00:08, hold time is 180, keepalive interval
is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                2          6
    Keepalives:            37         40
    Route Refresh:          0          0
    Total:                 42         47
  Default minimum time between advertisement runs is 0 seconds
```

Рисунок 3.13-3.15 – Виконання різних службових команд для перевірки роботи BGP

Останнім кроком діагностування мережі стане діагностування IPsec за допомогою відповідних службових команд.

```
R_2_14_1#show crypto isakmp policy

Default IKE policy
Protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys
).
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65510
```

```
R_2_14_1#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 100.2.14.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (100.2.14.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (101.2.14.1/255.255.255.255/47/0)
   current_peer 101.2.14.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 123, #pkts encrypt: 123, #pkts digest: 123
    #pkts decaps: 119, #pkts decrypt: 119, #pkts verify: 119
    #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.: 100.2.14.1, remote crypto endpt.: 101.2.14.1
     path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0x41E1EA21(1105324577)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x37DC0F29(937168681)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Transport, }
        conn id: 7, flow_id: 7, sibling_flags 80000000, crypto map: Tunnel0-hea
-0
        sa timing: remaining key lifetime (k/sec): (4188216/664)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

Рисунок 3.16-3.17 – Виконання різних службових команд для перевірки роботи IPSec на маршрутизаторі R_2_14_1

```
R_2_14_1#show crypto engine connection active
Crypto Engine Connections

   ID  Type    Algorithm           Encrypt  Decrypt LastSeqN IP-Address
    1  IPsec   AES+SHA256                0      114      114 100.2.14.1
    2  IPsec   AES+SHA256              115        0        0 100.2.14.1
    3  IPsec   AES+SHA256                0      107      107 100.2.14.1
    4  IPsec   AES+SHA256              106        0        0 100.2.14.1
    5  IPsec   AES+SHA256                0      123      123 100.2.14.1
    6  IPsec   AES+SHA256              124        0        0 100.2.14.1
    7  IPsec   AES+SHA256                0      117      117 100.2.14.1
    8  IPsec   AES+SHA256              121        0        0 100.2.14.1
 1001  IKEv2   SHA512+AES256             0        0        0 100.2.14.1
 1002  IKEv2   SHA512+AES256             0        0        0 100.2.14.1
 1003  IKEv2   SHA512+AES256             0        0        0 100.2.14.1
 1004  IKEv2   SHA512+AES256             0        0        0 100.2.14.1
```

Рисунок 3.18-3.19 – Виконання команди show crypto engine connection active

Потрібним етапом стане перевірка відмовостійкості мережі для цього потрібно вимкнути маршрутизатор R_2_14_1 і перевірити чи мережа буде доступна.

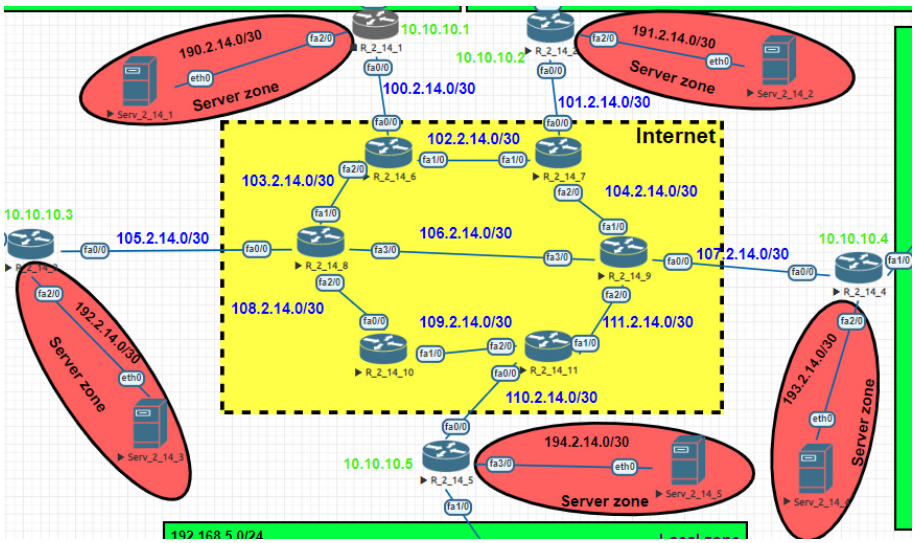



Рисунок 3.20 – Демонстрація вимкненення голвоного маршрутизатора

```
R_2_14_5#ping 10.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/77/84 ms
R_2_14_5#ping 10.10.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/89/112 ms
```

Рисунок 3.21 – Демонстрація наявності зв’язку

Як було продемонстровано на скріншотах мережа залишається активною навіть коли головний Hub стає недоступний. Це стало можливим завдяки тому, що роль головного хаба перейняв на себе R_2_14_2. Також під час тестування виявився один недолік. Після включення маршуртизатора R_2_14_1 він достатньо довгий час не може встановити сесію між своїми сусідами. Тільки після 30-40 хв очікування він успішно встановлює сесію. Вирішення цієї проблеми потребує більш глибшого детального дослідження специфікироботи BGP. Наостанок продемонструємо службову команду DMVPN.

```
R_2_14_1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Hub, NHRP Peers:4,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 101.2.14.1           10.10.10.2    UP 00:01:05     D
     1 105.2.14.1           10.10.10.3    UP 00:02:05     D
     1 107.2.14.1           10.10.10.4    UP 00:00:57     D
     1 110.2.14.1           10.10.10.5    UP 00:00:45     D
```

```
R_2_14_2#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Hub/Spoke, NHRP Peers:4,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 100.2.14.1           10.10.10.1    UP 00:01:29     S
     1 105.2.14.1           10.10.10.3    UP 00:02:26     D
     1 107.2.14.1           10.10.10.4    UP 00:01:21     D
     1 110.2.14.1           10.10.10.5    UP 00:01:10     D
```

Рисунок 3.22-3.23 – Виконання команди show dmvpn на хабах

```
R_2_14_4#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 100.2.14.1          10.10.10.1    UP 00:02:16     S
     1 101.2.14.1          10.10.10.2    UP 00:02:16     S
     1 110.2.14.1          10.10.10.5    UP 00:01:59     D
```

Рисунок 3.24 – Виконання команди show dmvpn на spoke

Отже в третьому розділі було проведено налаштування обладнання згідно його ролі, проведено діагностику за допомогою різноманітних діагностичних команд, проведення тестування мережі на наявність зв'язку та відмовостікості. Була врахована можливість маштабованості мережі до 253 пристроїв, а також визначена поведінка мережі в разі певних технічних проблем.

# ВИСНОВКИ

При виконанні курсового проекту в першому розділі було проаналізовано особливості компанії Cisco та її операційну систему. Проаналізовано особливості функціонування протоколів та технологій GRE, DMVPN, BGP, NHRP, IPsec їх структуру та функції, переваги та недоліки, порівняли протокол ці протоколи між собою, що дало розуміння, можливість аналізу та варіанти виконання поставленого завдання.

В другому розділі розробили проект глобальної мережі організації. Було розроблено структуру ядра глобальної 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. Обгрунтовані загальні політики безпеки

В третьому розділі було проведено налаштування обладнання згідно його ролі, проведено діагностику за допомогою різноманітних діагностичних команд, проведення тестування мережі на наявність зв’язку та відмовостікості в мережевому симуляторі Eve-ng. Була врахована можливість маштабованості мережі до 253 пристроїв, а також визначена поведінка мережі в разі певних технічних проблем.

В результаті виконання кваліфікаційної роботи було створену глобальну мережу організації з використанням технологій DMVPN та BGP. Проведені різноманітні методи для її захисту так покращення відмовостійкості. Визначені переваги та недоліки цієї мережі, а також спроектовано можливість її розширення у майбутньому.

# СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Налаштування DMVPN на маршрутизаторах Cisco [Електронний ресурс] - Режим доступу до ресурсу: http://xgu.ru/wiki/dmvpn
2. Таненбаум Э. Компьютерные сети. 5-е изд. / Э. Таненбаум, Д. Уэзеролл. – СПб.: Питер, 2012. – 960 с.
3. Олифер В.Г Компьютерные сети. Принципы, технологии, протоколы / Олифер В.Г., Олифер Н.А. – СПб.: Питер, 2001. – 672 с.
4. Маршрутизація в Cisco [Електронний ресурс] - Режим доступу до ресурсу: http://xgu.ru/wiki/Маршрутизация_в_Cisco
5. Cisco corporation, Cisco Dynamic Multipoint VPN Configuration Guide / Cisco Community. - 228 ст.
6. Аутентифікація в BGP [Електронний ресурс] – Режим доступу до ресурсу: http://xgu.ru/wiki/Аутентификация_BGP
7. Cisco Networking Academy [Електронний ресурс] – Режим доступу до ресурсу: https://www.netacad.com
8. CCNA BGP configuration and troubleshooting: Cisco CCNA prep [Електронний ресурс] - Режим доступу до ресурсу: https://www.udemy.com/course/ccna-bgp-configuration-and-troubleshooting-exam-preparation/
9. GRE протокол [Електронний ресурс] - Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/GRE_(протокол)
10. Налаштування SSH в Cisco[Електронний ресурс] - Режим доступу до ресурсу: https://www.dmosk.ru/instruktions.php?object=cisco-ssh
11. Cisco Systems [Електронний ресурс] - Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Cisco_Systems
12. Захист інформації [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Захист_інформації
13. Cisco IOS [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/w/index.php?title=Cisco_IOS&stable=1
14. BGP (Border Gateway Protocol) [Електронний ресурс] – Режим доступу до ресурсу: http://xgu.ru/wiki/BGP

15.Dynamic Multipoint IPsec VPNs [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.comipsec/negotiation-ike-protocols/

16. Носов В.В. Безпека інформаційних та комунікаційних систем / Носов В.В. - 2007 р. – 251 с.

17. Використання технології VPN для забезпечення інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-vpn-dlya-obespecheniya-informatsionnoy-bezopasnosti

18. Запечников С. В Основы построения виртуальных частных сетей. Учебное пособие для вузов/ Запечников С. В, Милославская Н. Г., Толстой А. И.– 2-е изд., стереотип. – М.: Горячая линия–Телеком, 2011. – 248 с

19. Стивен Браун Виртуальные частные сети / Стивен Браун - 2-е изд. 2001. – 502 с.

20. Брайан Хетч, Создание VPN с использованием протоколов PPP и SSH/ Олег Колесников, Брайан Хетч – 302 с.

21. Александр Росляков Виртуальные частные сети VPN. Модели и методы анализа/ Александр Росляков. – Изд. 2001. – 412 с.

22. DHCP (Dynamic Host Configuration Protocol) [Електронний ресурс] - Режим доступу до ресурсу: http://xgu.ru/wiki/DHCP

23. BGP Case Studies [Електронний ресурс] - Режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

24. BGP: ROUTE REFLECTOR, CLUSTER_ID [Електронний ресурс] - Режим доступу до ресурсу: http://admindoc.ru/1394/bgp-route-reflector-cluster_id/

25. Cisco DMVPN Dual Hub Single Cloud [Електронний ресурс] - Режим доступу до ресурсу: https://knowtoshare.wordpress.com/2017/01/06/cisco-dmvpn-dual-hub-single-topology/

26. Технологія Cisco Dynamic Multipoint VPN [Електронний ресурс] - Режим доступу до ресурсу: http://www.technorium.ru/vpn/cisco-dmvpn.shtml

27. Типы VPN соединений. Масштабирование VPN [Електронний ресурс] - Режим доступу до ресурсу: https://habr.com/ru/post/246281/
28. Dynamic Multipoint IPsec VPNs (Using Multipoint GRE/NHRP to Scale IPsec VPNs) [Електронний ресурс] - Режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/41940-dmvpn.html
29. Динамические многоточечные виртуальные частные сети IPSec (с применением протокола GRE/NHRP для масштабирования сети VPN IPSec) Електронний ресурс] - Режим доступу до ресурсу: https://www.cisco.com/c/ru_ru/support/docs/security-vpn/ipsec-negotiation-ike-protocols/41940-dmvpn.html
30. Cisco - базовая настройка DMVPN [Електронний ресурс] - Режим доступу до ресурсу: https://kinzersky.ru/page/dmvpn

# ДОДАТКИ

Додаток А

Проект мережі в графічному мережевому емуляторі Eve-ng:

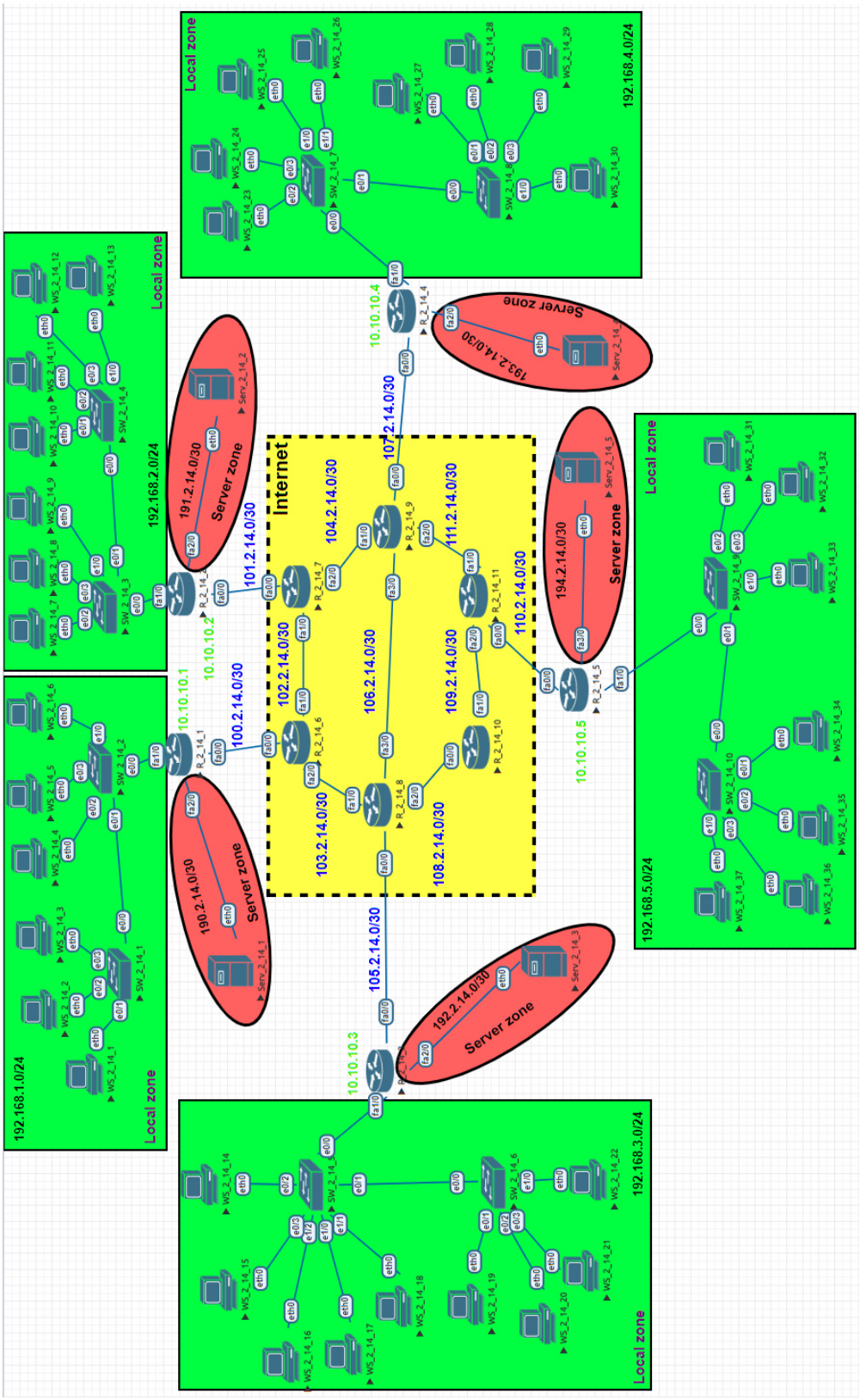



Рисунок 1 – Організація захисту корпоративної мережі, побудованої з використанням технологій DMVPN та BGP

Додаток Б

Технічні характеристики обладнання мережі:

Таблиця Б.1

Технічні характеристики комутатора Cisco 2960

| | |
|---|---|
| Виробник | Cisco |
| ID продукту | WS-C2960-24TC-L |
| Опис продукту | Cisco Catalyst 2960 24 10/100 + 2T/SFP LAN Base Image |
| Тип продукту | Ethernet Switch |
| Кількість портів | 24 |
| Uplink Port: | Так |
| Деталі слота для порту / розширення: | 24 x Fast Ethernet Network<br>2 x Gigabit Ethernet Uplink<br>2 x Fast Ethernet Expansion Slot |
| Підтримуваний тип носія: | Вита пара |
| Стандартний кабель із витою парою: | 5 категорія |
| Ethernet Технологія: | Fast Ethernet |
| Типи інтрнет технологій | 10Base-T<br>100/1000Base-T |
| Кількість загальних слотів розширення: | 2 |
| Тип слота розширення: | SFP |
| Спільний слот SFP: | Так |
| Кількість слотів SFP: | 2 |
| Підтримуваний layer | 2 |

Продовження таблиці Б.1

| | |
|---|---|
| Управління: | Telnet<br>Syslog<br>Web browser<br>CiscoWorks<br>Remote SPAN<br>SNMP v1, v2c, and v3<br>Command-line interface<br>Switching Database Manager<br>Cisco Service Assurance Agent<br>IEEE 802.1p CoS<br>IEEE 802.1Q VLAN<br>RMON groups (history, statistics, alarms, and events) |
| Стандартна пам'-ять: | 64 Мб |
| Технологія пам'яті: | DRAM |
| Флеш-пам’ять: | 32 Мб |
| Вхідна напруга: | 110 В змінного струму<br>220 В змінного струму |
| Джерело живлення: | Блок живлення |
| Підтримується джерело живлення: | Так |

Таблиця Б.2

Технічні характеристики маршрутизатора 7201:

| | |
|---|---|
| Виробник | Cisco |
| ID продукту | CISCO7201 |
| Опис продукту | Cisco 7201 Chassis, 1GB Memory, Dual P/S, 64MB Flash |
| Тип продукту | Router Chassis |
| Кількість портів | 2 |
| Uplink Port: | Так |
| Призначення | Для бізнесу |

Продовження таблиці Б.2

| | |
|---|---|
| Деталі слота для порту / розширення: | SFP (mini-GBIC)<br>Port Adapter |
| Ethernet Технологія: | Fast/Gigabit Ethernet |
| Типи інтрнет технологій | 100/1000Base-T |
| Кількість загальних слотів розширення: | 4 |
| Тип слота розширення: | SFP |
| Спільний слот SFP: | Так |
| Кількість слотів SFP: | 2 |
| Підтримуваний layer | 3 |
| Можливості захисту | Network Address Translation (NAT)<br>Access control lists (ACLs) |
| Стандартна пам'ять: | 1 GB |
| Максимум пам’яті | 2 GB |
| Технологія пам'яті: | SDRAM |
| Флеш-пам’ять: | 64 MB |
| Підтримка карт пам’яті | 64 MB |
| Вхідна напруга: | 110 В змінного струму |
| Джерело живлення: | Блок живлення |
| Підтримується джерело живлення: | Так |
| Додаткова інформація | Забезпечує один USB-порт для загального зберігання та збереження маркерів безпеки<br>Підтримується повний набір функцій програмного забезпечення Cisco IOS |

Додаток В

Лістинг конфігураційних файлів пристроїв мережі:

```
R_2_14_1(HUB)#sh run
Current configuration : 3296 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
!
!
!
hostname R_2_14_1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$dC1O$g1O6JaTUzTbIVz8WxP3pT.
!
no aaa new-model
!
!
!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.250
ip dhcp excluded-address 192.168.1.251
!
ip dhcp pool LAN_A
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
!
!
ip domain name cisco.com
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
username Admin_2_14_1 privilege 15 secret 5
$1$lfw.$cnVlTxfhIzYbfhhW8rwWU0
username User_2_14_1 privilege 10 secret 5
$1$SSHB$4Pc7mJlmtzb8GGad2zN5F0
username User_2_14_2 privilege 5 secret 5
$1$hCZ3$7NPIhCY1Ee3Zl8aa6eeXl0
!
!
!
crypto ikev2 keyring DMVPN
 peer DMVPN
  address 0.0.0.0 0.0.0.0
  pre-shared-key twibro123
 !
!
!
crypto ikev2 profile DMVPN_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
```

```
 authentication local pre-share
 keyring local DMVPN
!
!
!
!
!
!
crypto ipsec transform-set DMVPN esp-aes
esp-sha256-hmac
 mode transport
!
!
!
!
crypto ipsec profile DMVPN_Profile
 set transform-set DMVPN
 set ikev2-profile DMVPN_IKEv2
!
!
!
!
!
!
!
interface Tunnel0
 ip address 10.10.10.1 255.255.255.0
 no ip redirects
 ip mtu 1416
 ip nhrp authentication nhrppass
 ip nhrp map multicast dynamic
 ip nhrp network-id 333
 ip nhrp redirect
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 333
 tunnel protection ipsec profile DMVPN_Pro-
file
!
interface FastEthernet0/0
 ip address 100.2.14.1 255.255.255.252
 duplex full
!
!
interface FastEthernet1/0
 ip address 192.168.1.1 255.255.255.0
 duplex half
!
!
interface FastEthernet2/0
 ip address 190.2.14.1 255.255.255.252
 duplex full
!
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex full
!
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
```

```
!
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router bgp 333
 bgp cluster-id 332
 bgp log-neighbor-changes
 network 190.2.14.0 mask 255.255.255.252
 network 192.168.1.0
 neighbor 10.10.10.2 remote-as 333
 neighbor 10.10.10.2 password 7
0107110D5919095E731F
 neighbor 10.10.10.2 update-source Tunnel0
 neighbor 10.10.10.3 remote-as 333
 neighbor 10.10.10.3 password 7
095859001B171843595F
 neighbor 10.10.10.3 update-source Tunnel0
 neighbor 10.10.10.3 route-reflector-client
 neighbor 10.10.10.3 next-hop-self
 neighbor 10.10.10.4 remote-as 333
 neighbor 10.10.10.4 password 7
071B36454C1B16544541
!
!
!
line con 0
 login local
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 23 in
 neighbor 10.10.10.4 update-source Tunnel0
 neighbor 10.10.10.4 route-reflector-client
 neighbor 10.10.10.4 next-hop-self
 neighbor 10.10.10.5 remote-as 333
 neighbor 10.10.10.5 password 7
140305020E16257A767B
 neighbor 10.10.10.5 update-source Tunnel0
 neighbor 10.10.10.5 route-reflector-client
 neighbor 10.10.10.5 next-hop-self
!
ip forward-protocol nd
!
!
!
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
access-list 23 permit 192.168.1.0 0.0.0.255
!
!
!
control-plane
 exec-timeout 60 0
 logging synchronous
 login loca
 transport input ssh
!
!
!
End
```

**R_2_14_2(Second hub)**#sh run
Current configuration : 3424 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
!
!
!
hostname R_2_14_2
!
boot-start-marker
boot-end-marker
!
!
!
enable secret 5 $1$BgOc$9dlMEPtVfN.TLi-OyKODtz.
!
no aaa new-model
!
!
!
ip dhcp excluded-address 192.168.2.1
ip dhcp excluded-address 192.168.2.250
ip dhcp excluded-address 192.168.2.251
!
ip dhcp pool LAN_A
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
!
!
!
ip domain name cisco.com
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
username Admin_2_14_1 privilege 15 secret 5 $1$/AEE$QyzcODY5FXRqBMqfi6.kB.
username User_2_14_1 privilege 10 secret 5 $1$ey4S$A.Ie5DU/zwxVAgDfcOKZZ1
username User_2_14_2 privilege 5 secret 5 $1$x2FW$F9zoh.bAC82tO/wMyCPy7.
!
!
!
crypto ikev2 keyring DMVPN
 peer DMVPN
  address 0.0.0.0 0.0.0.0
  pre-shared-key twibro123
 !
!
!
crypto ikev2 profile DMVPN_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local DMVPN
!

```
!
!
!
!
!
crypto ipsec transform-set DMVPN esp-aes
esp-sha256-hmac
 mode transport
!
!
!
crypto ipsec profile DMVPN_Profile
 set transform-set DMVPN
 set ikev2-profile DMVPN_IKEv2
!
!
!
!
!
!
interface Tunnel0
 ip address 10.10.10.2 255.255.255.0
 no ip redirects
 ip mtu 1416
 ip nhrp authentication nhrppass
 ip nhrp map multicast dynamic
 ip nhrp map multicast 100.2.14.1
 ip nhrp map 10.10.10.1 100.2.14.1
 ip nhrp network-id 333
 ip nhrp nhs 10.10.10.1
 ip nhrp redirect
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 333
 tunnel protection ipsec profile DMVPN_Pro-
file
!
interface FastEthernet0/0
 ip address 101.2.14.1 255.255.255.252
 duplex full
!
!
!
interface FastEthernet1/0
 ip address 192.168.2.1 255.255.255.0
 duplex half
!
!
interface FastEthernet2/0
 ip address 191.2.14.1 255.255.255.252
 duplex full
!
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex full
!
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
```

```
!
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router bgp 333
 bgp cluster-id 333
 bgp log-neighbor-changes
 network 191.2.14.0 mask 255.255.255.252
 network 192.168.2.0
 neighbor 10.10.10.1 remote-as 333
 neighbor 10.10.10.1 password 7
15061C05063824757A60
 neighbor 10.10.10.1 update-source Tunnel0
 neighbor 10.10.10.1 next-hop-self
 neighbor 10.10.10.3 remote-as 333
 neighbor 10.10.10.3 password 7
120D121E101903557878
 neighbor 10.10.10.3 update-source Tunnel0
 neighbor 10.10.10.3 route-reflector-client
 neighbor 10.10.10.3 next-hop-self
 neighbor 10.10.10.4 remote-as 333
 neighbor 10.10.10.4 password 7
105A1E1007051D5A5E57
 neighbor 10.10.10.4 update-source Tunnel0
 neighbor 10.10.10.4 route-reflector-client
 neighbor 10.10.10.4 next-hop-self
 neighbor 10.10.10.5 remote-as 333
 neighbor 10.10.10.5 password 7
120D121E101903557878
 neighbor 10.10.10.5 update-source Tunnel0
 neighbor 10.10.10.5 route-reflector-client
 neighbor 10.10.10.5 next-hop-self
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
access-list 23 permit 192.168.2.0 0.0.0.255
!
!
!
control-plane
!
!
line con 0
 login local
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 23 in
 exec-timeout 60 0
 logging synchronous
 login local
 transport input ssh
!
!
!
!
!
End
```

```
R_2_14_3(Spoke)#sh run
Building configuration...

Current configuration : 3002 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R_2_14_3
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$kwSD$ltAOrKmAz0goG-
VDNe7kYQ.
!
no aaa new-model
!
!
!
ip dhcp excluded-address 192.168.3.1
ip dhcp excluded-address 192.168.3.250
ip dhcp excluded-address 192.168.3.251
!
ip dhcp pool LAN_A
 network 192.168.3.0 255.255.255.0
 default-router 192.168.3.1
!
!
!
ip domain name cisco.com
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
username Admin_2_14_1 privilege 15 secret 5
$1$pP57$2K8c83t4zPlm6EgxI77vI.
username User_2_14_1 privilege 10 secret 5
$1$Wz2H$c9.TTobLY4xrXMsmhdsWI0
username User_2_14_2 privilege 5 secret 5
$1$azOr$exrENTcLFK/9UjR3K/Wje.
!
!
!
crypto ikev2 keyring DMVPN
 peer DMVPN
  address 0.0.0.0 0.0.0.0
  pre-shared-key twibro123
 !
!
!
crypto ikev2 profile DMVPN_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local DMVPN
!
!
!
```

```
!
!
!
crypto ipsec transform-set DMVPN esp-aes
esp-sha256-hmac
 mode transport
!
crypto ipsec profile DMVPN_Profile
 set transform-set DMVPN
 set ikev2-profile DMVPN_IKEv2
!
!
!
!
!
!
!
interface Tunnel0
 ip address 10.10.10.3 255.255.255.0
 no ip redirects
 ip mtu 1416
 ip nhrp authentication nhrppass
 ip nhrp map multicast 100.2.14.1
 ip nhrp map multicast 101.2.14.1
 ip nhrp map 10.10.10.2 101.2.14.1
 ip nhrp map 10.10.10.1 100.2.14.1
 ip nhrp network-id 333
 ip nhrp nhs 10.10.10.1
 ip nhrp nhs 10.10.10.2
 ip nhrp shortcut
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 333
 tunnel protection ipsec profile DMVPN_Pro-
file
!
interface FastEthernet0/0
 ip address 105.2.14.1 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 ip address 192.168.3.1 255.255.255.0
 duplex half
!
interface FastEthernet2/0
 ip address 192.2.14.1 255.255.255.252
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router bgp 333
 bgp log-neighbor-changes
```

```
 network 192.2.14.0 mask 255.255.255.252
 network 192.168.3.0
 neighbor 10.10.10.1 remote-as 333
 neighbor 10.10.10.1 password 7
03104C02041D2E1D1C5A
 neighbor 10.10.10.1 update-source Tunnel0
 neighbor 10.10.10.1 next-hop-self
 neighbor 10.10.10.2 remote-as 333
 neighbor 10.10.10.2 password 7
120D121E101903557878
 neighbor 10.10.10.2 update-source Tunnel0
 neighbor 10.10.10.2 next-hop-self
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
access-list 23 permit 192.168.3.0 0.0.0.255
!
!
!
control-plane
!
!
line con 0
 login local
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 23 in
 exec-timeout 60 0
 logging synchronous
 login local
 transport input ssh
!
!
End
```

```
R_2_14_4(Spoke)#sh run
Building configuration...

Current configuration : 3020 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R_2_14_4
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$pG4S$leKVB4PS.7IaO0TUxZhXw/
!
no aaa new-model
!
!
!
ip dhcp excluded-address 192.168.4.1
ip dhcp excluded-address 192.168.4.250
ip dhcp excluded-address 192.168.4.251
!
ip dhcp pool LAN_A
 network 192.168.4.0 255.255.255.0
 default-router 192.168.4.1
!
!
!
ip domain name cisco.com
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
username Admin_2_14_1 privilege 15 secret 5
$1$Ah4J$HTJY5/ssRQy.eBg0YZYxW0
username User_2_14_1 privilege 10 secret 5
$1$47sO$TI6s3rByrQYA8X1b5h7zo0
username User_2_14_2 privilege 5 secret 5
$1$v8cr$QpIs42mx/IOv2qlIz6lDm/
!
!
!
crypto ikev2 keyring DMVPN
 peer DMVPN
  address 0.0.0.0 0.0.0.0
  pre-shared-key twibro123
 !
!
!
crypto ikev2 profile DMVPN_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local DMVPN
!
!
!
```

```
!
!
!
crypto ipsec transform-set DMVPN esp-aes
esp-sha256-hmac
 mode transport
!
crypto ipsec profile DMVPN_Profile
 set transform-set DMVPN
 set ikev2-profile DMVPN_IKEv2
!
!
!
!
!
!
!
interface Tunnel0
 ip address 10.10.10.4 255.255.255.0
 no ip redirects
 ip mtu 1416
 ip nhrp authentication nhrppass
 ip nhrp map multicast 100.2.14.1
 ip nhrp map multicast 101.2.14.1
 ip nhrp map 10.10.10.2 101.2.14.1
 ip nhrp map 10.10.10.1 100.2.14.1
 ip nhrp network-id 333
 ip nhrp nhs 10.10.10.1
 ip nhrp nhs 10.10.10.2
 ip nhrp shortcut
 ip nhrp redirect
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 333
 tunnel protection ipsec profile DMVPN_Pro-
file
!
interface FastEthernet0/0
 ip address 107.2.14.1 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 ip address 192.168.4.1 255.255.255.0
 duplex half
!
interface FastEthernet2/0
 ip address 193.2.14.1 255.255.255.252
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
```

```
router bgp 333
 bgp log-neighbor-changes
 network 192.168.4.0
 network 193.2.14.0 mask 255.255.255.252
 neighbor 10.10.10.1 remote-as 333
 neighbor 10.10.10.1 password 7
08355B470B0B0A464058
 neighbor 10.10.10.1 update-source Tunnel0
 neighbor 10.10.10.1 next-hop-self
 neighbor 10.10.10.2 remote-as 333
 neighbor 10.10.10.2 password 7
0010040F064904575D72
 neighbor 10.10.10.2 update-source Tunnel0
 neighbor 10.10.10.2 next-hop-self
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
access-list 23 permit 192.168.4.0 0.0.0.255
!
!
!
control-plane
!
!
line con 0
 login local
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 23 in
 exec-timeout 60 0
 logging synchronous
 login local
 transport input ssh
!
!
End
```

```
R_2_14_5(Spoke)#sh run
Current configuration : 3021 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R_2_14_5
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$Udhh$wy3qMJy7ewUnOl1SYBRGm0
!
no aaa new-model
!
!
!
ip dhcp excluded-address 192.168.5.1
ip dhcp excluded-address 192.168.5.250
ip dhcp excluded-address 192.168.5.251
!
!
!
!
ip dhcp pool LAN_A
 network 192.168.5.0 255.255.255.0
 default-router 192.168.5.1
!
!
!
ip domain name cisco.com
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
username Admin_2_14_1 privilege 15 secret 5
$1$9jA9$eNchXINSxyfRBsFfBmDss.
username User_2_14_1 privilege 10 secret 5
$1$792r$LyzF2bhJI/JBrQD4wHHgX1
username User_2_14_2 privilege 5 secret 5
$1$0aml$jR1yaohElnJFtRKIWSBpI0
!
!
!
crypto ikev2 keyring DMVPN
 peer DMVPN
  address 0.0.0.0 0.0.0.0
  pre-shared-key twibro123
 !
!
!
crypto ikev2 profile DMVPN_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
```

```
 keyring local DMVPN
!
!
!
!
!
!
crypto ipsec transform-set DMVPN esp-aes
esp-sha256-hmac
 mode transport
!
!
!
!
!
crypto ipsec profile DMVPN_Profile
 set transform-set DMVPN
 set ikev2-profile DMVPN_IKEv2
!
!
!
!
!
!
!
!
!
interface Tunnel0
 ip address 10.10.10.5 255.255.255.0
 no ip redirects
 ip nhrp authentication nhrppass
 ip nhrp map multicast 100.2.14.1
 ip nhrp map multicast 101.2.14.1
 ip nhrp map 10.10.10.1 100.2.14.1
 ip nhrp map 10.10.10.2 101.2.14.1
 ip nhrp network-id 333
 ip nhrp nhs 10.10.10.1
 ip nhrp nhs 10.10.10.2
 ip nhrp registration no-unique
 ip nhrp shortcut
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 333
 tunnel protection ipsec profile DMVPN_Pro-
file
!
!
!
interface FastEthernet0/0
 ip address 110.2.14.1 255.255.255.252
 duplex full
!
!
!
interface FastEthernet1/0
 ip address 192.168.5.1 255.255.255.0
 duplex half
!
!
!
interface FastEthernet2/0
 no ip address
 duplex full
!
!
!
interface FastEthernet3/0
 ip address 194.2.14.1 255.255.255.252
 shutdown
```

```
 duplex full
!
!
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex full
!
!
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
!
router bgp 333
 bgp log-neighbor-changes
 network 192.168.5.0
 network 194.2.14.0 mask 255.255.255.252
 neighbor 10.10.10.1 remote-as 333
 neighbor 10.10.10.1 password 7
051F1106235E41584B56
 neighbor 10.10.10.1 update-source Tunnel0
 neighbor 10.10.10.1 next-hop-self
 neighbor 10.10.10.2 remote-as 333
 neighbor 10.10.10.2 password 7
03104C02041D2E1D1C5A
 neighbor 10.10.10.2 update-source Tunnel0
 neighbor 10.10.10.2 next-hop-self
!
!
!
!
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
access-list 23 permit 192.168.5.0 0.0.0.255
!
!
!
control-plane
!
!
line con 0
 login local
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 23 in
 exec-timeout 60 0
 logging synchronous
 login local
 transport input ssh
!
!
End
```

```
R_2_14_6#sh run
Building configuration...

Current configuration : 1913 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R_2_14_6
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 100.2.14.2 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 ip address 102.2.14.1 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 ip address 103.2.14.1 255.255.255.252
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex full
```

```
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 101.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 101.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 104.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 104.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 105.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 105.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 106.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 106.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 107.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 107.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 108.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 108.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 109.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 109.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 110.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 110.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 111.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 111.2.14.0 255.255.255.252 FastEther-
net2/0 5
!
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
End
```

```
R_2_14_7#sh run
Current configuration : 1913 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R_2_14_7
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 101.2.14.2 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 ip address 102.2.14.2 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 ip address 104.2.14.1 255.255.255.252
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet5/0
```

```
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 100.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 100.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 103.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 103.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 105.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 105.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 106.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 106.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 107.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 107.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 108.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 108.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 109.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 109.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 110.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 110.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 111.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 111.2.14.0 255.255.255.252 FastEther-
net1/0 5
!
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
End
```

```
R_2_14_8#sh run
Current configuration : 2261 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R_2_14_8
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 105.2.14.2 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 ip address 103.2.14.2 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 ip address 108.2.14.1 255.255.255.252
 duplex full
!
interface FastEthernet3/0
 ip address 106.2.14.1 255.255.255.252
 duplex full
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
```

```
 shutdown
 duplex full
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 100.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 100.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 100.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 101.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 101.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 101.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 102.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 102.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 102.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 104.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 104.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 104.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 107.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 107.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 107.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 109.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 109.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 109.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 110.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 110.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 110.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 111.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 111.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 111.2.14.0 255.255.255.252 FastEther-
net3/0 10
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
End
```

```
R_2_14_9#sh run
Current configuration : 2207 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R_2_14_9
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 107.2.14.2 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 ip address 104.2.14.2 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 ip address 111.2.14.1 255.255.255.252
 duplex full
!
interface FastEthernet3/0
 ip address 106.2.14.2 255.255.255.252
 duplex full
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
```

```
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 100.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 100.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 100.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 101.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 101.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 101.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 102.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 102.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 102.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 103.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 103.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 103.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 105.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 105.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 105.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 108.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 108.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 108.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 109.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 109.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 109.2.14.0 255.255.255.252 FastEther-
net3/0 10
ip route 110.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 110.2.14.0 255.255.255.252 FastEther-
net1/0 10
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
End
```

```
R_2_14_10#sh run
Building configuration...

Current configuration : 2006 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R_2_14_10
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 108.2.14.2 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 ip address 109.2.14.1 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet5/0
 no ip address
```

```
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 100.2.14.0 255.255.255.252 FastEther-
net0/0
ip route 100.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 101.2.14.0 255.255.255.252 FastEther-
net0/0
ip route 101.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 102.2.14.0 255.255.255.252 FastEther-
net0/0
ip route 102.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 103.2.14.0 255.255.255.252 FastEther-
net0/0
ip route 103.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 104.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 104.2.14.0 255.255.255.252 FastEther-
net0/0 5
ip route 105.2.14.0 255.255.255.252 FastEther-
net0/0
ip route 105.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 106.2.14.0 255.255.255.252 FastEther-
net0/0
ip route 106.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 107.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 107.2.14.0 255.255.255.252 FastEther-
net0/0 5
ip route 110.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 110.2.14.0 255.255.255.252 FastEther-
net0/0 5
ip route 111.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 111.2.14.0 255.255.255.252 FastEther-
net0/0 5
!
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
End
```

```
R_2_14_11#sh run
Current configuration : 1914 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R_2_14_11
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 110.2.14.2 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 ip address 111.2.14.2 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 ip address 109.2.14.2 255.255.255.252
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet5/0
```

```
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 100.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 100.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 101.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 101.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 102.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 102.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 103.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 103.2.14.0 255.255.255.252 FastEther-
net1/0 5
ip route 104.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 104.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 105.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 105.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 106.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 106.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 107.2.14.0 255.255.255.252 FastEther-
net1/0
ip route 107.2.14.0 255.255.255.252 FastEther-
net2/0 5
ip route 108.2.14.0 255.255.255.252 FastEther-
net2/0
ip route 108.2.14.0 255.255.255.252 FastEther-
net1/0 5
!
!
!
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end
```