ВІДЗИВ НАУКОВОГО КЕРІВНИКА НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ

Студента Колесника Владислава Вікторовича
представлену на здобуття освітнього ступеня бакалавр
зі спеціальності 123 «Комп'ютерна інженерія»

1. Робота виконана на тему «Проект базової мережі Інтернет-провайдера».

2. Актуальність роботи зумовлена потребою у розробці та впровадженні у практику діяльності сучасних мереж провайдерів такого типу.

3. Основний зміст пояснювальної записки роботи викладено на 72 сторінках тексту, записка містить 1 таблицю, 65 ілюстрацій, 2 додатки. Список використаних літературних джерел налічує 30 найменувань. Невід'ємною складовою роботи є реалізований у середовищі моделювання GNS3 проект мережі на базі обладнання фірми Cisco та Juniper.

4. Пояснювальна записка складається з реферату, вступу, трьох розділів основного тексту, висновків, списку використаної літератури, 2 додатків.

Розділ 1 присвячений аналізу принципів, моделей, протоколів та технологій побудови базових мереж Інтернет-провайдерів, зокрема, у розділі розглянуто: загальні підходи та моделі до побудови таких мереж, стандартні сервіси, що надаються провайдерами, особливості рівнівевої організації мереж Інтернет-провайдера. У цьому ж розділі проведено аналіз протоколів та технології побудови мереж провайдерів.

Розділ 2 містить опис етапів проектування мережі, зокрема розробці загального проекту мережі, схеми адресації пристроїв мережі, здійсненню вибору інструментарію віртуалізації, вибору обладнання Cisco та Juniper.

Розділ 3 містить опис базового налагодження пристроїв мережі та процесів налагодження налагодження MPLS L3VPN Inter-AS Option B, GETVPN. Також у цьому розділі виконано перевірку функціоналу побудованого проекту мережі провайдера та наведено результати тестування та їх аналіз.

5. Висновки містять сумарні результати проведеної роботи.

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

7. Додатки А та Б містять файли конфігурацій налагоджених пристроїв Cisco (Cisco IOS) та Juniper (JunOS) відповідно.

8. Таблиця та ілюстрації пояснювальної записки 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.

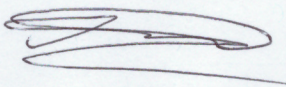
11. Ставлення студента до виконання випускної кваліфікаційної роботи – дуже відповідальне. Студентом самостійно відпрацьовано та проаналізовано великий масив інформаційних джерел та здійснені коректні технічні рішення.

12. У цілому при написанні випускної кваліфікаційної роботи студент Колесник В.В. виявив здібності до оволодіння знаннями, уміннями і навичками з таких дисциплін, як «Архітектура комп'ютера», «Адміністрування та захист баз та сховищ даних», «Хмарні технології», «Операційні системи», «Комп'ютерні мережі», «Захист інформації в інформаційно-комунікаційних системах», «Адміністрування комп'ютерних систем та мереж», «Теорія системі і системний аналіз». Також студент Колесник В. В. показав вміння підібрати необхідну літературу та інші інформаційні джерела, проаналізувати їх, виконати постановку задачі на розробку, розробити проект мережі базового Інтернет-провайдера, коректно 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 Колесника 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
15 червня 2020 року



А.А. Єфіменко

РЕЦЕНЗІЯ
на кваліфікаційну роботу
студента 4 курсу групи КІ-2 спеціальності 123 «Комп'ютерна інженерія»
факультету інформаційно-комп'ютерних технологій
Державного університету «Житомирська політехніка»
Колесника Владислава Вікторовича
на тему: „Проект базової мережі інтернет-провайдера"

Кваліфікаційна робота студента Колесника В.В. „Проект базової мережі Інтернет-провайдера" присвячена актуальній тематиці – розробці та впровадженню у практику сучасної схеми інтернет-провайдера.

Робота містить реалізований у середовищі моделювання GNS3 проект мережі на базі обладнання фірми Cisco,Juniper та пояснювальну записку наступного складу: вступ, три розділи основного тексту, висновки, список використаної літератури, 2 додатки.

У першому розділі пояснювальної записки проведено аналіз принципів, моделей, протоколів та технологій побудови базових мереж Інтернет-провайдерів, зокрема, у розділі розглянуто: загальні підходи та моделі до побудови таких мереж, стандартні сервіси, характеристики та особливості рівнів моделі побудови мережі інтернет-провайдера. У цьому ж розділі наведено описі та аналіз протоколів та технологій побудови мереж провайдерів. У другому розділі пояснювальної записки здійснено вибір програмного засобу для розробки та віртуалізації проекту мережі, розроблено схему адресації, проведено вибір обладнання та операційних систем.

У третьому розділі пояснювальної записки наведено опис процесу базового налагодження пристроїв мережі та процесу налагодження обраних технологічних рішень MPLS L3VPN та GETVPN. Також у цьому розділі проведено перевірку функціонування пристроїв мережі та мережі в цілому, наведено результати тестування.

Зміст роботи відповідає поставленому завданню. У цілому кваліфікаційна робота виконана на високому рівні. Тема роботи розкрита повністю. Студентом продемонстровані гарні 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 в цілому відповідає вимогам стандартів. Проект мережі реалізовано за допомогою програмного комплексу моделювання та віртуалізації GNS3. Функціонал виконаного проекту відповідає заявленому.

Позитивною стороною є те, що отримані результати мають практичну цінність – розроблені сценарії налагодження пристроїв можуть застосовуватися при налагодженні реальних мереж. Недоліками роботи є наступні: деякий теоретичний матеріал варто було б винести до розділу 1 (опис ОС JunOS), наявність деяких відхилень від вимог щодо оформлення пояснювальної записки (наприклад, підрозділ 2.4 не містить описової частини, а лише результати розрахунків). Зазначені недоліки у цілому не впливають на високу якість і актуальність роботи.

У цілому кваліфікаційна робота студента Колесника В. В. „Проект базової мережі Інтернет-провайдера" 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 базової мережі Інтернет-провайдера»

Виконав студент 4-го курсу, групи КІ-2
спеціальності 123 «Комп’ютерна інженерія»
_____ Колесник 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 **Колесника Владислава Вікторовича**
Тема роботи: **Проект базової мережі інтернет-провайдера**
затверджена Наказом по університету від **«06» квітня 2020 р. № 98с**
Термін здачі студентом закінченої роботи – **1 червня 2020 р.**
Вихідні дані для роботи:

1. Програмний продукт засобів віртуалізації Virtual Box
2. Графічний емулятор мереж GNS3
3. Маршрутизатори Cisco 7200
4. Операційна система JunOS Olive12.1R1.9
5. Mpls l3vpn inter-as option b
6. Cisco Group Encrypted Transport Virtual Private Network

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А. А.	07.04.20	07.04.20
2	Єфіменко А. А.	24.04.20	24.04.20
3	Єфіменко А. А.	06.05.20	06.05.20

Керівник _____ Єфіменко А. А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2020 – 9 квітня 2020	Виконано
2	Пошук та аналіз джерел інформації з реалізації MPLS	10 квітня 2020 – 13 квітня 2020	Виконано
3	Аналіз інформації про технологію GETVPN	14 квітня 2020 – 19 квітня 2020	Виконано
4	Пошук та аналіз джерел інформації з реалізації MPLS L3VPN Inter-AS Option B	20 квітня 2020 – 30 квітня 2020	Виконано
5	Пошук та вибір програмного забезпечення для виконання проекту	1 травня 2020 – 3 травня 2020	Виконано
6	Встановлення операційної ситстеми JUNOS	3 травня 2020 – 5 травня 2020	Виконано
7	Розробка схеми адресації пристроїв мережі	5 травня 2020 – 10 травня 2020	Виконано
8	Налагодження базової маршрутизації за допомогою протоколу OSPF	11 травня 2020 – 21 травня 2020	Виконано
9	Налагодження MPLS та VRF	22 травня 2020 – 24 травня 2020	Виконано
10	Налагодження GETVPN	25 травня 2020 – 25 травня 2020	Виконано
11	Перевірка працездатності мережі	26 травня 2020 – 29 травня 2020	Виконано
12	Аналіз результатів тестування	30 травня 2020 – 31 травня 2020	Виконано
13	Написання пояснювальної записки	4 червня 2020 – 8 червня 2020	Виконано
14	Підготовка презентації та виступу	9 червня 2020 – 10 червня 2020	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	11 червня 2020 – 12 червня 2020	Виконано
16	Захист	20 червня 2020	Виконано

Студент _____ Колесник В.В.

Керівник _____ Єфіменко А. А

РЕФЕРАТ

Кваліфікаційна робота складається з проекту базової мережі інтернет-провайдера та пояснювальної записки до нього. Пояснювальна записка до роботи містить 72 сторінки, 65 ілюстрацій та 1 таблицю.

Метою роботи є розробка проекту базової мережі інтернет-провайдера з використанням обладнання Cisco та Juniper.

У роботі визначено основні завдання на розробку мережі інтернет-провайдера, розглянуто загальні підходи та моделі до побудови мереж провайдерів, описані стандартні сервіси інтернет-провайдера, обґрунтований вибір виробників обладнання – Cisco та Juniper. Розроблений, сформований та налагоджений загальний проект мережі. Наведені сценарії налаштування пристроїв мережі, зокрема, технологій MPLS та GETVPN, проведено тестування функціоналу проекту.

КЛЮЧОВІ СЛОВА: ЗАХИСТ, МЕРЕЖА, JUNIPER, CISCO, GETVPN, MPLS.

ABSTRACT

The qualification work consists of the project of the basic network of the Internet provider and the explanatory note to it. The explanatory note to the work contains 72 pages, 65 illustrations and 1 table.

The purpose of the work is to develop a project of the basic network of the Internet provider using Cisco and Juniper equipment.

The main tasks for the development of the ISP network are defined, the general approaches and models to the construction of ISP networks are considered, the standard services of the ISP are described, the choice of equipment manufacturers - Cisco and Juniper is substantiated. The general network project is developed, formed and adjusted. Scenarios for configuring network devices, in particular, MPLS and GETVPN technologies, and testing the functionality of the project.

KEY WORDS: SECURITY, NETWORK, JUNIPER, CISCO, GETVPN, MPLS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 7
ВСТУП 8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ВІДОМОСТІ ЩОДО ПОБУДОВИ СУЧАСНОГО ІНТЕРНЕТ-ПРОВАЙДЕРА 9
1.1 Організація мережі інтернет-провайдера (ядро, розподіл, доступ) 9
1.2 Протоколи та технології побудови мереж інтернерт-провайдерів 22
1.3 Безпека мереж провайдерів 26
Висновки з першого розділу 31
РОЗДІЛ 2. ВИБІР ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВСТАНОВЛЕННЯ ВІРТУАЛЬНИХ МАШИН ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ 32
2.1 Вибір програми для налаштування схеми та її встановлення 32
2.2. Завантаження та налаштування Virtual Box 36
2.3 Опис та встановлення обладнання Juniper Networks в схему інтернет-провайдера 39
2.4. Розробка схеми адресації пристроїв 43
Висновки з другого розділу 46
РОЗДІЛ 3. АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ 47
3.1. Налагодження MPLS L3VPN Inter-AS Option B 47
3.2. Налагодження Cisco Group Encrypted Transport Virtual Private Network (GET VPN) 53
3.3. Тестування роботи схеми мережі 58
Висновки з третього розділу 66
ВИСНОВКИ 67
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 69
ДОДАТКИ 72

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

VPN - Virtual Private Network

GET VPN - Group Encrypted Transport VPN

MPLS - Multiprotocol label switching

ISAKMP - Internet Security Association and Key Management Protocol

IPsec - IP Security

BGP - Border Gateway Protocol

GDOI - Group Domain of Interpretation

EIGRP - Enhanced Interior Gateway Routing Protocol

OSPF - Open Shortest Path First

IBGP - Internal BGP

AS - Autonomous system

WAN - Wide Area Network

ВСТУП

Актуальність теми. Сучасний розвиток інформаційних технологій і, зокрема, мережі Internet, призводить до необхідності захисту інформації, переданої в рамках розподіленої корпоративної мережі, що використовує мережі відкритого доступу. При використанні своїх власних фізичних каналів доступу ця проблема так гостро не стоїть, тому що в цю мережу не має доступу ніхто зі сторонніх. Однак вартість таких каналів висока, тому не кожна компанія дозволить собі використовувати їх. VPN - це технологія, яка об'єднує довірені мережі, вузли і користувачів через відкриті мережі. На мій погляд, це найбільш яскравий образ технології, яка набуває все більшого поширення серед не тільки технічних фахівців, а й серед пересічних користувачів, яким також потрібно захищати свою інформацію.

Метою кваліфікаційної роботи є створення, налаштування та перевірка базової мережі інтернет-провайдера на обладнанні різних виробників.

Зі встановленої мети випливають наступні завдання:

1. пошук підходів та моделей по створенню та налаштуванню мережі;
2. вибір оптимальної моделі для побудови мережі провайдера;
3. розробка мережі;
4. налаштування серверів та користувачів;
5. дослідження відмінностей між обладнанням Juniper та Cisco.

Об’єктом дослідження є процес налаштування базової мережі інтернет-провайдера на обладненні Cisco та Juniper.

Предметом дослідження є використання всіх доступних ресурсів та можливостей на маршрутизаторах Cisco та Juniper для побудови сучасної базової мережі інтернет-провайдера.

В процесі виконання випускної роботи було налаштовано MPLS L3VPN Inter-AS Option B, Cisco Group Encrypted Transport VPN, перевірено взаємодію двох серверів та користувачів мережі.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ВІДОМОСТІ ЩОДО ПОБУДОВИ СУЧАСНОГО ІНТЕРНЕТ-ПРОВАЙДЕРА

1.1 Організація мережі інтернет-провайдера (ядро, розподіл, доступ)

1.1.1 Загальні підходи та моделі до побудови мереж провайдерів

ISP (Інтернет-провайдер) - це компанія, яка надає особам та іншим компаніям доступ до Інтернету та інших супутніх послуг, таких як побудова веб-сайтів та віртуальний хостинг. Інтернет-провайдер оснащений обладнанням та телекомунікаційним доступом, необхідним для доступу до Інтернету для географічного району, що обслуговується. Більш великі Інтернет-провайдери мають власні високошвидкісні орендовані лінії, щоб вони менше залежали від телекомунікаційних провайдерів і могли надавати кращі послуги своїм клієнтам[13].

Сучасний Інтернет - вельми складна і високотехнологічна система, що дозволяє користувачеві спілкуватися з людьми, що знаходяться в будь-якій точці земної кулі, швидко і комфортно відшукувати будь-яку необхідну інформацію, публікувати для загального відома дані, які він хотів би повідомити всьому світу.

Кожне підключення до інтернету, що знаходиться в залежності від свого типу (мобільне, телефонне, за виделенною лінією) - це в першу чергу підключення обладнання, що вимагає необхідного потенціалу від потужного провайдера. Ваш комп'ютер отримує доступ до серверів провайдера, який має постійний канал зв'язку з інтернетом. Принципові характеристики серверів в Інтернеті визначають, скільки користувачів можуть одночасно обслуговуватися, а також пропонувати якість послуг та швидкість інтернету. Як правило, компанії-провайдери пропонують своїм клієнтам декілька тарифів з різними умовами і відповідно до них визначають кількість ресурсів на користувача, тобто певну частину від загальнодоступної можливості свого власного каналу виходу в Інтернет. Ідентифікація користувачів проводиться за

логіном та паролем підключення. Взаємодія з всемирною паутиною проходить за наступним сценарієм:

– запит користувача до сервера провайдера;

– обробка запиту та перенаправлення його на потрібний сервер в інтернеті;

– відповідь інтернет-сервера на обладнання провайдера;

– передача інформації на обладнання користувача.

Діяльність постачальників послуг орієнтована на організацію так званих сервісних вузлів (Service Nodes), використовуючи які реалізує доступ користувача до різних мереж послуг та інформаційних ресурсів як даного вузла, так і віддалених вузлів Інтернету. При цьому постачальник також є споживачем телекомунікаційних послуг (послуги з транспортування інформації), що надаються мережевими операторами. Доступ користувачів до сервісного вузла, як правило, здійснюється через місцеві мережі операторів, однак окремі провайдери можуть мати власні мережі абонентського доступу.

Прийнято розрізняти сервіс-провайдерів різних рівнів: місцевого рівня, регіонального рівня та національного рівня.

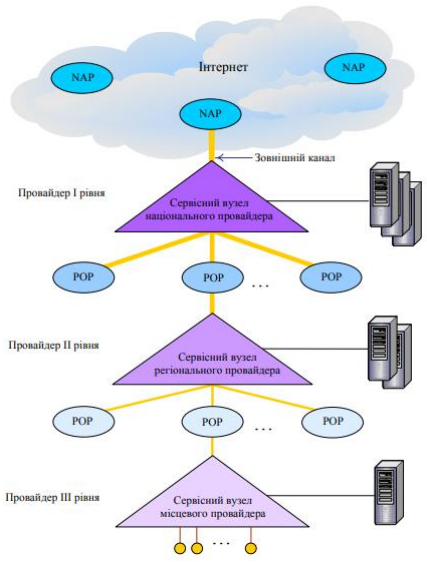


Рис. 1.1. Інтернет-сервіс-провайдинг

Постачальники провайдерів доступу надають доступ до Інтернету, використовуючи низку технологій для підключення користувачів до їх мережі. Наявні технології варіюються від комп'ютерних модемів із акустичними

з’єднувачами до телефонних ліній, до телевізійного кабелю (CATV), Wi-Fi та оптоволоконної оптики. Для користувачів та малого бізнесу традиційні варіанти включають мідні дроти для забезпечення комутованого зв'язку , DSL, як правило, асиметричної цифрової абонентської лінії (ADSL), кабельного модема або цифрової мережі інтегрованих служб (ISDN) (зазвичай інтерфейс базової швидкості). Використання волоконної оптики для кінцевих користувачів називається «Fiber To The Home» або подібними назвами. Для клієнтів з більш вищими вимогами(наприклад, для середнього та великого бізнесу або інших провайдерів) можна використовувати високошвидкісні DSL (такі як однопарна швидкісна цифрова абонентська лінія), Ethernet , столичний Ethernet , гігабітний Ethernet , Frame Relay , Інтерфейс первинної швидкості ISDN , синхронні оптичні мережі (SONET).

Той, хто володіє великими мережами і високошвидкісними каналами, що з'єднують міста, країни і континенти - той є магістральним провайдером .

Той, хто надає доступ до мережі мереж в більш локальному масштабі (мікрорайону, міста, села, району та ін.) є провайдером послуг доступу.

Магістральні провайдери зазвичай продають трафік у великих обсягах і надають послуги зв'язку провайдерам доступу, а провайдери доступу забезпечують доступ до всієї інфраструктури Інтернет індивідуальним користувачам. Основні пристрої, що становлять типову мережу бездротового доступу:

– прикордонний маршрутизатор;

– базові станції (також часто називаються точки доступу);

– і, нарешті, дуже важливий елемент - система білінгу: з її допомогою проводиться облік наданих послуг, їх тарифікація, виставлення рахунків абонентам.

– система управління мережею - допоможе вирішити завдання експлуатації мережі як єдиної системи;

– сервери надання додаткових мережевих послуг - дозволять не тільки надавати доступ в Інтернет, а й організувати ряд локальних послуг - телефонія, ігри, музичні портали;

– система гарантованого електроживлення - дозволить Вашому обладнанню працювати без перерв в разі перерв в електропостачанні;

– інші системи. Фантазія розробників породила велику кількість потрібних, і практично непотрібних систем для операторів. Але на початковому етапі, в рамках обмеженого бюджету старт-апу, вони Вам навряд чи знадобляться.

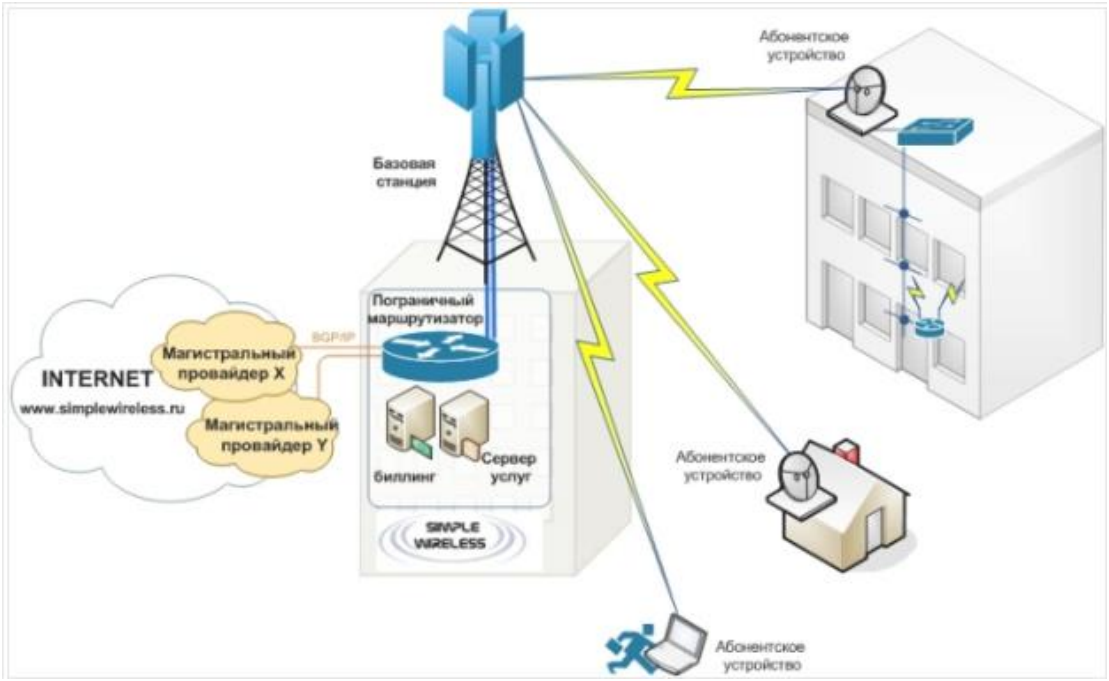


Рис. 1.2. Схематично зображені перераховані пристрої, пов'язані в єдину систему

Схему будемо розглядати в напрямку від джерела каналу до його споживачам. Як підключитися до магістрального провайдеру? Для цього зазвичай використовується прикордонний маршрутизатор. Термін «прикордонний» говорить сам за себе - він знаходиться на кордоні між магістральним провайдером і провайдером мережі доступу. «Маршрутизатор» дозволяє передавати дані через кордон двох мереж: магістральної мережі і мережі доступу.

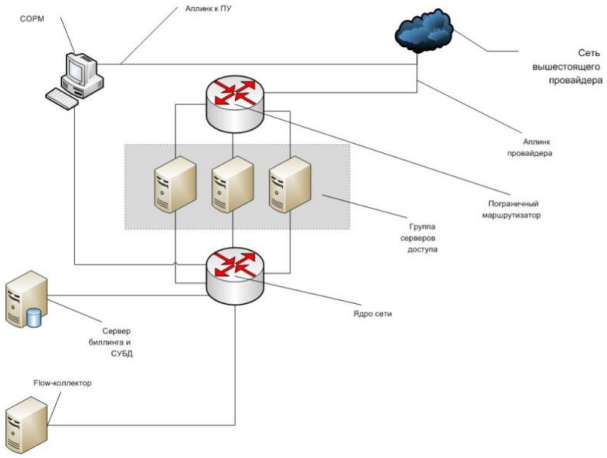


Рис. 1.3. Логічна схема побудови інтернет-провайдера

1.1.2 Стандартні сервіси інтернет-провайдера

Для того, щоб надавати доступ до мережі Інтернет тисячам абонентів, недостатньо просто протягнути локальну мережу до кожного з них. Необхідно налаштувати авторизацію, білінг, фільтрацію і ще безліч важливих сервісів, які відповідають за якість і повноту наданих послуг. Стандартний набір сервісів, що використовуються інтернет-провайдером, виглядає так: DHCP-сервер; DNS-сервер; сервер AAA (radius або diameter); сервер білінгу; сервер баз даних; сервер зберігання flow-статистики і білінгової інформації; сервер моніторингу мережі; СОРМ; пристрою фільтрації трафіку; BRAS; сервіси розваг для користувачів (опціонально);

Основне завдання DHCP-сервера - видавати IP-адреси клієнтам. Кожен оператор сам вирішує, як це робити - статично прив'язувати mac-адресу клієнта з IP-адресою, або по порту комутатора (в разі використання dhcp option 82), або пулом адрес, що виділяються на підмережу. Іноді зустрічаються реалізації з AAA-серверами. Найпопулярнішою реалізацією є ISC DHCP Server, так як він безкоштовний і має досить легкий синтаксис налаштування. У деяких мережах реалізується на маршрутизаторах, але частіше в якості динамічної видачі адрес. Завдання DNS-сервера - відповідати на DNS-запити абонентів і перетворювати їх в IP-адреси. По виконуваних функцій DNS-сервери поділяються на кілька груп; сервер певної конфігурації може відноситися відразу до декількох типів:

– Авторитативний DNS-сервер - сервер, який відповідає за будь-яку зону.

– Кешуючий DNS-сервер - обслуговує запити клієнтів (отримує рекурсивний запит, виконує його за допомогою нерекурсивних запитів до авторитативним серверів або передає рекурсивний запит вищестоящому DNS-серверу).

– Перенаправляючий DNS-сервер - перенаправляє отримані рекурсивні запити вищестоящому кешуючому у вигляді рекурсивних запитів.

Сервер доступу являє собою маршрутизатор або сервер, який забезпечує клієнтам доступ до мережі Інтернет. Як правило, це досить продуктивне обладнання, так як дуже сильно впливає на якість послуг, що надаються і вимагає від системного адміністратора певної кваліфікації для налаштування та обслуговування даного сервера. Загальних рекомендацій, на чому саме реалізувати сервер доступу немає, але для здешевлення будівництва мережі використовують саме серверне обладнання, а не маршрутизатори, оскільки в разі апгрейда заміна сервера буде більш вигідна, ніж заміна маршрутизатора. Однак програмне забезпечення для серверів не завжди працює стабільно і у випадку з UNIX-подібними системами іноді призводить до проблем в ядрі (kernel panic)[30].

Технології доступу різні, і провайдер сам вибирає, що використовувати. Останнім часом на піку популярності знаходиться технологія IPoE. Також досить широко застосовуються протоколи PPPoE, IPSec, L2TP, а ось протокол PPTP все сильніше втрачає популярність. Це обумовлено сучасними вимогами безпеки. Більшість протоколів використовують NAT (Network Address Translation), так як дозволяє економити реальні (білі) IP-адреси, зокрема IPv4.

Сервер аутентифікації, авторизації та аккаунтинга. З назви - сервер, який проводить ідентифікацію користувачів, видає користувачам привілеї або забирає їх, веде облік доступу. Найбільш часто реалізується засобами FreeRADIUS. Переваги - безкоштовний, простий в налаштуванні і має досить широку функціональність.

Authentication (аутентифікація) - зіставлення персони (запиту) існуючого облікового запису в системі безпеки. Здійснюється за логіном, паролем, сертифікату, смарт-карти.

Authorization (авторизація, перевірка повноважень, перевірка рівня доступу) - зіставлення облікового запису в системі (і персони, що пройшла аутентифікацію) і певних повноважень (або заборони на доступ). У загальному випадку авторизація може бути «негативною» (користувачеві А заборонений доступ до серверів компанії).

Accounting (облік) - стеження за споживанням ресурсів (переважно мережевих) користувачем. У accounting включається також і запис фактів отримання доступу до системи (англ. Access logs).

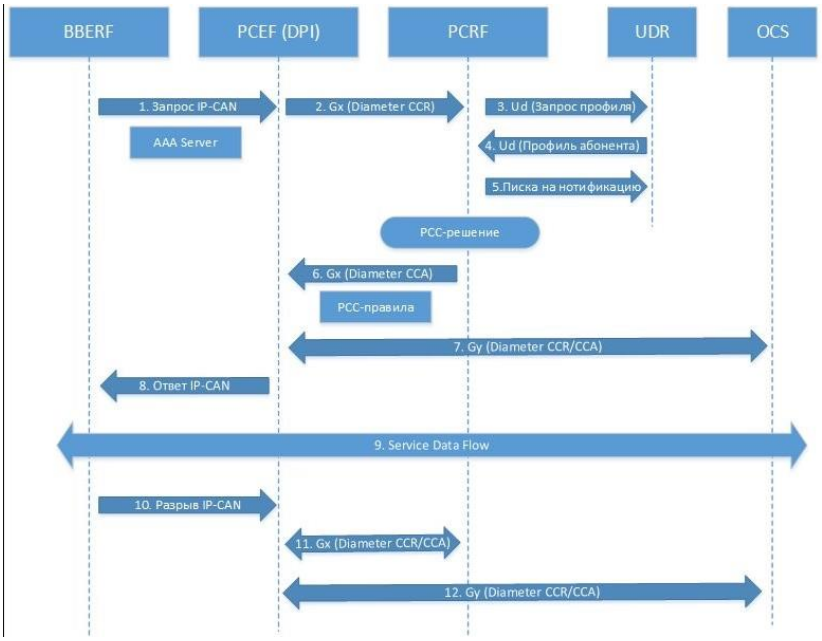


Рис. 1.4. Схема роботи AAA-сервера

Сервер білінгу можна назвати центром мережі, так як сервер управляє обліковими записами даних клієнтів оператора, а саме - додавання і видалення користувачів, списання абонентської плати, зміна відомостей про тарифи і багато іншого. Дуже сильно залежить від сервера бази даних. На ринку багато програмного забезпечення для виконання ролі АСР (автоматизована система розрахунків).

Сервісний шлюз BRAS - серверна функція, яка дозволяє оператору широкосмугового доступу здійснювати контроль доступу абонентів до мережі Інтернет і застосовувати політики тарифних планів і додаткових тарифних опцій. У своїх пристроях її реалізували такі виробники, як Cisco, Juniper, Huawei, Ericsson, але продукцію цих підприємств можуть собі дозволити тільки великі оператори зв'язку. Невеликі інтернет-провайдери використовують в якості BRAS програмне рішення (BRAS на Mikrotik OS, BRASFil від SoftM, СКАТ DPI від VAS Experts), так як це значно дешевше і може бути встановлено на стандартний сумісний x86-сервер.

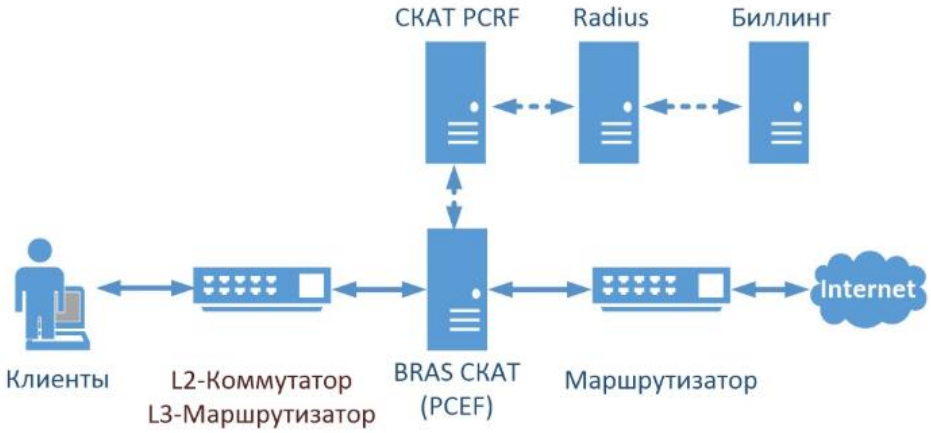


Рис. 1.5. Схема роботи BRAS

СОРМ - програмно-апаратна платформа для реалізації системи оперативно-розшукових заходів для силових відомств. На сьогоднішній день актуальні СОРМ другого і третього покоління. Як правило, оператор зв'язку тільки оплачує вартість обладнання та його установку в серверну стійку, але доступу до інтерфейсу обладнання не має. Основне завдання даного обладнання - реалізація деяких федеральних законів по контролю зв'язку.

Слід зазначити, що СОРМ є невід'ємною частиною мережі, без неї здати проект мережі до відповідних контролюючих органів неможливо. Також слід враховувати, що flow-статистика, як і дані про платежі, є білінгової інформацією, яку оператор зв'язку зобов'язаний зберігати 3 роки.

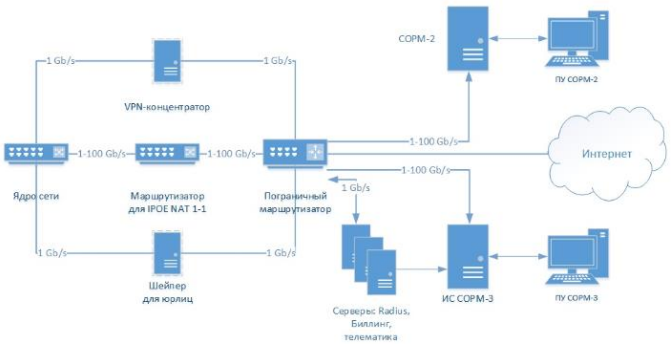


Рис. 1.6. Схема роботи СОРМ

1.1.3 Характеристики та особливості рівнів моделі побудови мережі інтернет-провайдера

На рис. 1.7 наведена еталонна модель побудови мережі. Вона являє собою топологію «дерево» (об'єднання декількох топологій «зірка») з додатковими надлишковими зв'язками. Схема не тільки компенсує головний недолік даної топології (відмова одного з вузлів впливає на роботу всієї мережі), а й збільшує без того надмірну витрату кабелю вдвічі. Для зменшення витрат на кабель багато організацій «підсилюють» тільки найбільш значущі частини мережі.

Слід пам'ятати, що це всього лише модель, а отже, розподіл на рівні може бути умовним - деякі пристрої можуть реалізовувати відразу обидва рівня, а якісь рівні можуть бути зовсім відсутніми.

Як видно, дана модель складається з чотирьох рівнів:

– рівень доступу;

– рівень агрегації;

– рівень ядра мережі;

– серверний рівень.

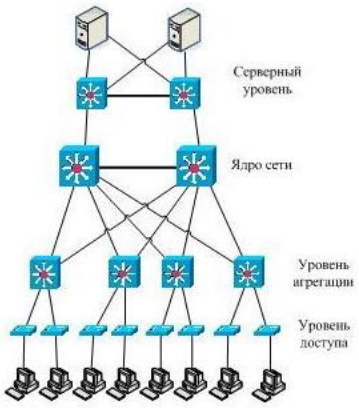


Рис. 1.7. Еталонна модель побудови мережі

Головним процесом на рівні доступу є підключення обладнання клієнта (комп'ютер, Wi-Fi-маршрутизатор) до мережі провайдера. Тут обладнанням провайдера є комутатори (якщо це локальна мережа і планується підключення за допомогою дротового середовища) або базові станції (якщо підключення відбувається через бездротову середу). Як правило, для організації керованої мережі використовують комутатори другого рівня (L2), рідше - третього (L3). Деякі провайдери на етапі будівництва локальної мережі віддають перевагу некерованим комутаторам, згодом це може позначитися на якості послуг, що надаються[7].

Також для здешевлення вартості підключення використовуються пристрої з максимальною кількістю фізичних інтерфейсів 24/48. У ролі керованих комутаторів другого рівня добре зарекомендували себе Cisco Catalyst серій 2900, 3500 і 3700.



Рис. 1.8. Комутатор Cisco Catalyst

Комутатори L3 на рівні доступу зустрічаються досить рідко, так як вони дорожче, ніж L2, і їх розміщення в технічних приміщеннях багатоповерхівок пов'язано з певними ризиками. Якщо комутатори L3 і зустрічаються на рівні доступу, то лише в об'єднанні рівня доступу і рівня агрегації. Приватним прикладом використання є кабінет в офісі або відділ, а у випадку з провайдером - багатоквартирний будинок або житлова секція в цьому будинку.

Варто відзначити, що при будівництві мережі кожен провайдер сам вибирає ступінь її сегментування. Сегмент мережі, або VLAN (Virtual Local Area Network), дозволяє об'єднати групу користувачів в одну логічну мережу або відокремити кожного окремо. Вважається дуже поганим прикладом, коли мережа рівна, тобто клієнти, комутатори, маршрутизатори і сервери знаходяться в одному логічному сегменті. Така мережа має дуже багато недоліків. Більш правильним рішенням є поділ цілої мережі на більш дрібні підмережі, в ідеальному варіанті - виділяти VLAN для кожного клієнта.

Ріень агрегації - проміжний рівень між ядром мережі і рівнем доступу. Як правило, цей рівень реалізується на L3-комутаторах, рідше - на маршрутизаторах через їх високу вартість і, знову ж таки, особливостей експлуатації в приміщеннях певного типу. Основне завдання обладнання зводиться до об'єднання «лінків» від комутаторів рівня доступу на «магістральному» комутаторі по топології «зірка».

Відстань від комутаторів доступу до комутаторів цієї групи може досягати декількох кілометрів. Якщо на рівні доступу використовуються L2-комутатори, а мережа сегментована, то на цьому рівні організовуються L3-інтерфейси для VLAN, прописаних на рівні доступу. Такий підхід здатний трохи розвантажити ядро мережі, так як в цьому випадку ядро не має записів про самих VLAN і параметрах VLAN-інтерфейсів, а має тільки маршрут до кінцевої підмережі.

Найбільш популярне обладнання, що використовується провайдерами для реалізації роботи цього рівня, - Cisco Catalyst серії 3750 і 3550, зокрема WS-C3550-24-FX-SMI.



Рис. 1.9. Комутатор Cisco Catalyst

Ядро є невід'ємною частиною будь-якої мережі. Даний рівень реалізується на маршрутизаторах, рідше - на високопродуктивних L3-комутаторах (знову ж таки, для зменшення вартості самої мережі.) Як було сказано раніше, в залежності від архітектури мережі, ядро може «тримати» статичні маршрути або мати налаштування для динамічної маршрутизації.

Серверний рівень реалізується, як зрозуміло з назви, серверами мережі. Реалізація може бути як на серверних платформах, так і на спеціалізованому обладнанні. ПО для серверних платформ на сьогоднішній день представлено різними виробниками і під різними видами ліцензій, так само як і ОС, на яких буде працювати це програмне забезпечення.

Прикордонний рівень зазвичай відсутній на схемах, наведених на самому початку, так як працює поза основної мережі, хоча і може бути реалізований на рівні ядра. Але краще для цих цілей виділити самостійний пристрій. На даному рівні відбувається обмін трафіком між провайдером і вищим провайдером або між AS (автономною системою) оператора з іншими автономними системами (в разі використання BGP). На початку будівництва мережі рівень може бути реалізований і на сервері доступу, але згодом, як тільки виникне необхідність додавання ще одного сервера доступу, постане питання про підмережі з власних реальних адрес.

Дану потребу можна реалізувати на маршрутизаторах або на L3-комутаторах - досить отримати доступ до зовнішнього пулу адрес з власної зовнішньої підмережі на IP-адресу, що видається провайдером при підключенні.

Підсумкова схема мережі інтернет-провайдера може виглядати так, але на практиці вона модифікується під певні завдання.

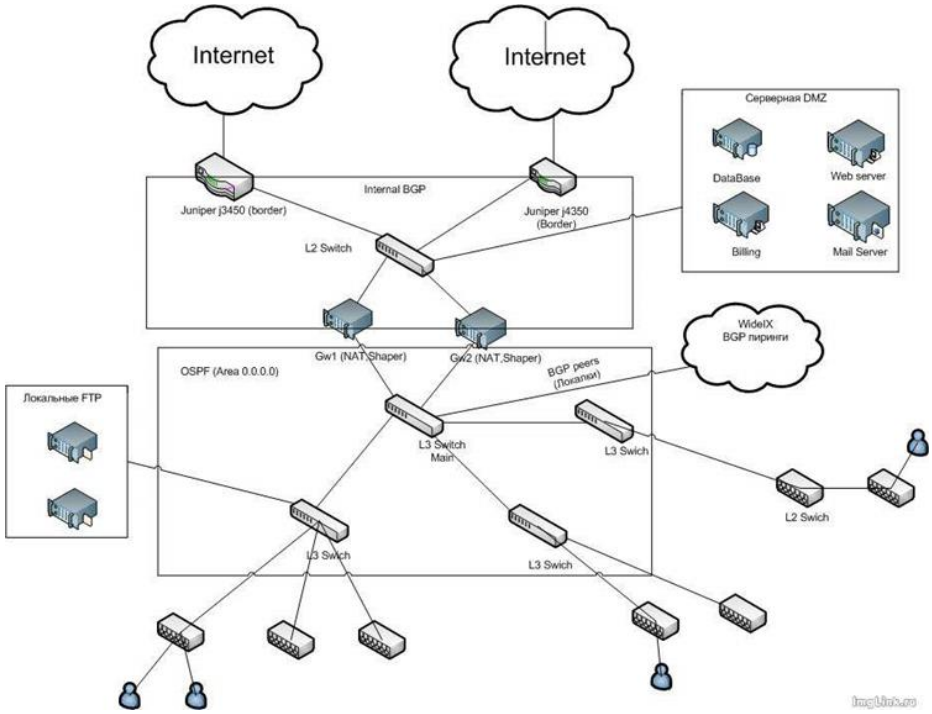


Рис. 1.10. Підсумкова схема мережі інтернет-провайдера

Пристрій 1-го рівня як прикордонний маршрутизатор, використовуються два Juniper j4350 до кожної з яких підключений свій магістральний «аплінк», взаємодія з «аплінк» відбувається за допомогою BGP протоколу (тобто віддаємо мережі закріплені за нашою AS (автономна система) і отримуємо від них повний список маршрутів в мережі Інтернет(full-view).

Між маршрутизаторами і комутаторами 3-го рівня використовується протокол OSPF для обміну внутрішньомережевими маршрутами. Маршрутизатор 1 має метрику 100, Маршрутизатор 2 має метрику 200, тобто в разі відмови одного з маршрутизаторів - всі пакети підуть через резервні (інтервал перемикання близько 10 секунд).

1.2 Протоколи та технології побудови мереж інтернерт-провайдерів

Transmission Control Protocol/Internet Protocol (TCP/IP) - це набір протоколів передачі даних. Часто ці протоколи, через їхній тісний зв'язок, іменуються разом - TCP/IP. TCP - це промисловий стандарт стека протоколів, розроблений для глобальних мереж. Стандарти TCP/IP опубліковані в серії документів, названих Request for Comment (RFC). Документи RFC описують внутрішню роботу мережі Internet. Деякі RFC описують мережеві сервіси або протоколи і їх реалізацію, в той час як інші узагальнюють умови застосування. Стандарти TCP/IP завжди публікуються у вигляді документів RFC, але не всі RFC визначають стандарти[20]. TCP/IP - це сімейство мережевих протоколів, орієнтованих на спільну роботу. До складу сімейства входить кілька компонентів:

– IP (Internet Protocol-міжмережевий протокол) - забезпечує транспортування пакетів даних з одного комп'ютера на інший;

– ICMP (Internet Control Message Protocol - протокол керуючих повідомлень в мережі Internet) - відповідає за різні види низькорівневої підтримки протоколу IP, включаючи повідомлення про помилки, допоміжні маршрутизирующие запити і підтвердження про отримання повідомлень;

– ARP (Address Resolution Protocol - протокол перетворення адрес) - виконує трансляцію IP-адрес в апаратні MAC-адреси;

– UDP (User Datagram Protocol - протокол передачі дейтаграм користувача) і TCP (Transmission Control Protocol - протокол управління передачею) - забезпечують доставку даних конкретним додатків на вказаному комп'ютері. Протокол UDP реалізують передачу окремих повідомлень без підтвердження доставки, тоді як TCP гарантує надійний повнодуплексний канал зв'язку між процесами на двох різних комп'ютерах з можливістю управління потоком і контролю помилок.

– Лідируюча роль стека TCP/IP пояснюється наступними його властивостями:

– Це найбільш завершений стандартний і в той же час популярний стек мережевих протоколів, що має багаторічну історію.

– Майже всі великі мережі передають основну частину свого трафіку за допомогою протоколу TCP / IP.

– Цей стек є основою для створення intranet-корпоративної мережі, що використовує транспортні послуги Internet і гіпертекстову технологію WWW, розроблену в Internet.

– Всі сучасні операційні системи підтримують стек TCP/IP.

– Це гнучка технологія для з'єднання різнорідних систем як на рівні транспортних підсистем, так і на рівні прикладних сервісів.

На транспортному рівні функціонують протокол управління передачею TCP (Transmission Control Protocol) і протокол дейтаграм користувача UDP (User Datagram Protocol). Протокол TCP забезпечує надійну передачу повідомлень між віддаленими прикладними процесами за рахунок утворення віртуальних з'єднань. Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним способом, як і IP, і виконує тільки функції сполучної ланки між мережним протоколом і численними прикладними процесами. Для того щоб забезпечити надійну доставку даних, протокол TCP передбачає встановлення логічного з'єднання, що дозволяє йому нумерувати пакети, підтверджувати їх, в разі втрати організовувати повторні передачі, розпізнавати і знищувати дублікати, доставляти прикладному рівню пакети в тому порядку, в якому вони були відправлені. Завдяки цьому протоколу об'єкти на хості-відправника та хості-одержувачі можуть підтримувати обмін даними в дуплексному режимі.

У функції протоколів TCP і UDP входить також виконання ролі сполучної ланки між прилеглими до транспортному рівню прикладним і мережевим рівнями. Від прикладного протоколу транспортний рівень приймає завдання на передачу даних з тим чи іншим якістю прикладному рівню-одержувачу. Програмні модулі, що реалізують протоколи TCP і UDP, подібно модулів протоколів прикладного рівня, встановлюються на хостах.

Існує два класи протоколів маршрутизації всередині автономних систем: Distance Vector, до якого відносяться RIP, EIGRP і Link State, до якого відносяться OSPF і IS-IS. Ідеологія Link State має на увазі, що кожен маршрутизатор повинен не просто знати найкращі маршрути в усі вилучені мережі, але і мати в пам'яті повну карту мережі з усіма існуючими зв'язками між іншими маршрутизаторами в тому числі.

OSPF - найбільш поширений протокол маршрутизації. Це пов'язано з тим, що його основний конкурент EIGRP аж до 2013 року був закритим протоколом і міг використовуватися тільки на обладнанні Cisco, в той час, як OSPF - це відкритий протокол, і він спочатку підтримувався як Cisco, так і іншими виробниками[11]. Таким чином, OSPF завоював популярність не дивлячись на деякі його недоліки в порівнянні з EIGRP: меншу гнучкість, відсутність чіткого опису механізму підрахунку метрики, підвищені вимоги до ресурсів маршрутизатора. В той же час, стандартне значення адміністративної дистанції для протоколу OSPF - 110, що означає, що його маршрути вважаються більш пріоритетними ніж IS-IS, RIP, External EIGRP, IBGP, але менш пріоритетними ніж IGRP. Така адміністративна дистанція - швидше преференція з боку Cisco до своїх протоколах. Так як з точки зору всіх існуючих протоколів, OSPF, звичайно краще RIP, в сучасних мережах, але він так само має бути і краще IGRP, який, в силу свого віку є класовим протоколом маршрутизації. OSPF є безкласовим (classless) протоколом маршрутизації, що означає передачу разом з апдейтами інформацію про масці підмережі (префікс), в той час, як старі класові протоколи маршрутизації, спираються на стандартні класи мереж (A, B, C) і з цієї причини в нині малозастосовні. MPLS (Multiprotocol label switching) є протоколом для прискорення і формування потоків мережевого трафіку, що, по суті, означає сортування MPLS і розстановку пріоритетів в ваших пакетах даних на основі їх клас обслуговування (наприклад, IP-телефон, відео або дані Skype). При використанні протоколів MPLS доступна використовувана пропускна здатність збільшується, а критично важливі програми, такі як передача голосу і відео, гарантують 100% безперебійну роботу.

MPLS це метод маркування пакетів, який встановлює пріоритетність даних. CE маршрутизатор, який використовується з боку вузла клієнта, який безпосередньо підключається до маршрутизатора оператора[1].

CE взаємодіє з маршрутизатором з боку оператора (PE) і обмінюється маршрутами всередині PE. Використовуваний протокол маршрутизації може бути статичним або динамічним (протокол внутрішнього шлюзу, такий як OSPF, або протокол зовнішнього шлюзу, такий як BGP). PE маршрутизатор - граничний маршрутизатор з боку оператора (MPLS домену), до якого підключаються пристрої CE[5]. Приставка PE до маршрутизатора, означає те, що він охоплює обладнання, здатне до роботи з широким діапазоном протоколів маршрутизації, зокрема:

– Протокол прикордонного шлюзу BGP(зв'язок PE-PE або PE-CE);

– Протокол динамічної маршрутизації OSPF(зв'язок між маршрутизатором і PE);

– Багатопротокольна комутація по мітках MPLS(зв'язок між маршрутизатором PE і P).

P-маршрутизатор - внутрішній маршрутизатор мережі оператора (провайдера) MPLS домену. У багатопротокольній комутації по мітках (MPLS) маршрутизатор P функціонує як транзитний маршрутизатор базової мережі. Маршрутизатор P зазвичай підключений до одного або декількох маршрутизаторів PE[2]. Щоб зрозуміти принцип роботи методики MPLS слід зазначити, що в традиційній IP-мережі кожному маршрутизатора доводиться виконувати пошук IP, шляхом постійного пошуку його в таблицях з пакетами даних з метою пересилки на наступний рівень поки пакети даних не досягнуть потрібного пункту призначення. MPLS технологія привласнює мітку всім IP-пакетам, а тим часом вже самі маршрутизатори приймають рішення про передачу пакету далі на наступний пристрій завдяки потрібного значення мітки[4].

1.3 Безпека мереж провайдерів

VPN (англ. Virtual Private Network - віртуальна приватна мережа) - логічна мережа, створювана поверх іншої мережі, наприклад Internet. Незважаючи на те, що комунікації здійснюються по публічних мережах 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.

За своєю суттю VPN володіє багатьма властивостями виділеної лінії, проте розгортається вона в межах загальнодоступної мережі, наприклад Інтернету. За допомогою методики тунелювання пакети даних транслюються через загальнодоступну мережу як за звичайним двоточковим з'єднанням. Між кожною парою «відправник-одержувач» даних встановлюється своєрідний тунель - безпечне логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого. Основними компонентами тунелю є:

– ініціатор;

– маршрутизована мережа;

– тунельний комутатор;

– Перш ніж перейти до порівняння, позначимо коло завдань, вирішення яких лягає на будь-яку віртуальну приватну мережу:

– Необхідно маркувати вузли віртуальної мережі та здійснювати коректну адресацію пакетів, призначених конкретним клієнтам.

– Щоб зберегти конфіденційність переданих по мережі даних, потрібна ефективне шифрування, а також повне виключення проходження інформації у відкритому вигляді.

– Для забезпечення цілісності VPN також необхідні аутентифікація учасників при підключенні до мережі і перевірка джерел даних для захисту мережі від попадання в неї несанкціонованих вузлів і пакетів.

Існують різні варіанти побудови VPN. При виборі рішення потрібно враховувати фактори продуктивності засобів побудови VPN. Наприклад, якщо маршрутизатор і так працює на межі потужності свого процесора, то додавання тунелів VPN і застосування шифрування/дешифрування інформації можуть зупинити роботу всієї мережі через те, що цей маршрутизатор не справлятиметься з простим трафіком, не кажучи вже про VPN. Досвід показує, що для побудови VPN найкраще використовувати спеціалізоване обладнання, однак якщо є обмеження в засобах, то можна звернути увагу на чисто програмне рішення. Розглянемо деякі варіанти побудови VPN.

VPN на базі маршрутизаторів. Іншим способом побудови VPN є застосування для створення захищених каналів маршрутизаторів. Так як вся інформація, яка виходить із локальної мережі, проходить через маршрутизатор, то доцільно покласти на цей маршрутизатор і завдання шифрування. Прикладом обладнання для побудови VPN на маршрутизаторах є обладнання компанії Cisco Systems. Починаючи з версії програмного забезпечення IOS 11.3, маршрутизатори Cisco підтримують протоколи L2TP і IPSec. Крім простого шифрування інформації, що проходить Cisco підтримує і інші функції VPN, такі як ідентифікація при встановленні тунельного з'єднання і обмін ключами. Для підвищення продуктивності маршрутизатора може бути використаний додатковий модуль шифрування ESA. Крім того, компанія Cisco System випустила спеціалізований пристрій для VPN, яке так і називається Cisco 1720 VPN Access Router (маршрутизатор доступу до VPN), призначене для установки в компаніях малого і середнього розміру, а також у відділеннях великих організацій.

VPN на базі програмного забезпечення. Наступним підходом до побудови VPN є чисто програмні рішення. При реалізації такого рішення використовується спеціалізоване програмне забезпечення, яке працює на виділеному комп'ютері, і в більшості випадків виконує роль проксі-сервера. Комп'ютер з таким програмним забезпеченням може бути розташований за брандмауером.

Також на канальному рівні для організації тунелів може використовуватися технологія MPLS (від англійського Multiprotocol Label Switching - мультипротокольна комутація по мітках - механізм передачі даних, який емулює різні властивості мереж з комутацією каналів поверх мереж з комутацією пакетів). MPLS працює на рівні, який можна було б розташувати між канальним і третім мережевим рівнями моделі OSI, і тому його зазвичай називають протоколом канально-мережевого рівня. Він був розроблений з метою забезпечення універсальної служби передачі даних як для клієнтів мереж з комутацією каналів, так і мереж з комутацією пакетів. За допомогою MPLS можна передавати різний трафік, такий як IP-пакети, ATM, SONET і кадри Ethernet.

Для вирішення ідентичних завдань раніше були розроблені такі технології, як Frame Relay і ATM. Багато інженерів вважали, що технологія ATM буде замінена іншими протоколами з меншими накладними витратами на передачу даних і при цьому забезпечують передачу пакетів даних змінної довжини з встановленням з'єднання між вузлами мережі. Технологія MPLS розроблялася з урахуванням сильних і слабких сторін ATM. В даний час обладнання з підтримкою MPLS замінює на ринку обладнання з підтримкою вищезгаданих технологій. Ймовірно, що в майбутньому MPLS повністю витіснить дані технології. Зокрема, MPLS обходиться без комутації осередків і набору сигнальних протоколів, характерних для ATM. При розробці MPLS прийшло розуміння того, що на рівні ядра сучасної мережі немає необхідності в осередках ATM маленького фіксованого розміру, оскільки сучасні оптичні мережі мають таку велику швидкість передачі даних, що навіть пакет даних максимальної довжини в 1500 байт відчуває незначну затримку в чергах буферів комутаційного обладнання (необхідність скорочення таких затримок, наприклад, для забезпечення заданої якості голосового трафіку, вплинула на вибір осередків малого розміру, характерних для ATM).

У той же час в MPLS спробували зберегти механізми оптимізації та управління трафіком (англ. Teletraffic engineering) і управління окремо від

переданого потоку даних, які зробили технології Frame relay і ATM привабливими для впровадження в великих мережах передачі даних. Незважаючи на те, що перехід на MPLS дає переваги управління потоками даних (поліпшення надійності і підвищення продуктивності мережі), існує проблема втрати контролю потоків даних, що проходять через мережу MPLS, з боку звичайних IP-додатків.

Шифрований транспортний VPN для шифрованої групи Cisco (GET VPN) - це набір функцій, необхідних для забезпечення захисту групового трафіку IP або одноадресної передачі через приватну мережу WAN, яка бере свій початок на пристрої Cisco IOS або протікає через нього[3]. GET VPN поєднує груповий протокол інтерпретації протоколів керування (GDOI) з шифруванням захисту IPsec, щоб надати користувачам ефективний метод захисту IP багатоадресної передачі або одноадресного трафіку. GET VPN дає змогу маршрутизатору застосувати шифрування до невідкритих (тобто "рідних") IP-пакетів багатоадресної передачі та одноадресної передачі та виключає вимогу налаштовувати тунелі для захисту багатоадресної та одноадресної передачі[9].

VPN для шифрованого транспорту Cisco Group забезпечує такі переваги:

– Забезпечує безпеку даних та автентифікацію транспорту, допомагаючи дотримуватися дотримання безпеки та внутрішнього регулювання, шифруючи весь трафік WAN;

– Вмикає масштабні мережеві сітки та виключає складне управління одноранговими ключами з груповими ключами шифрування;

– Для мереж Multiprotocol Label Switching (MPLS) підтримує мережевий інтелект, такий як повне з'єднання, шлях маршрутизації та якість обслуговування(QoS);

– Забезпечує просте управління членством за допомогою централізованого сервера ключів;

– Допомагає забезпечити низьку затримку, забезпечуючи постійний прямий зв’язок між сайтами, не вимагаючи транспорту через центральний концентратор;

– Зменшує навантаження на трафік на обладнання пристрою для клієнтів (CPE) та пристрої шифрування на крайньому рівні постачальника, використовуючи основну мережу для реплікації багатоадресного трафіку, уникаючи реплікації пакетів на кожному окремому веб-сайті однорангової мережі[10].

Завдяки GET Cisco надає тунельну VPN, яка виключає потребу в тунелях. Мережі, усуваючи потребу в тунелях «point-to-point», можуть збільшуватись, зберігаючи функції мережевого інтелекту, важливою для якості голосу та відео. GET - модель безпеки на основі стандартів, що базується на концепції «довірених» членів групи. Перевірені маршрутизатори членів використовують загальну методологію безпеки, яка не залежить від будь-якого взаємозв'язку між тунелями IPsec. Крім того, "будь-які" мережі, використовуючи довірені групи замість тунелів "point-to-point", можуть збільшувати масштаби, зберігаючи функції мережевого інтелекту (такі як QoS, маршрутизація та багатоадресна передача), мережі на основі GET можуть використовуватися в різних середовищах WAN, включаючи IP та MPLS. VPN-адреси MPLS, які використовують цю технологію шифрування, є високомасштабними, керованими та економічно ефективними, і вони відповідають вимогам шифрування, передбачених урядом. Гнучка природа GET дозволяє підприємствам, орієнтованим на безпеку, або керувати власною мережевою безпекою через послугу WAN постачальника послуг, або завантажувати послуги шифрування на своїх провайдерів. GET спрощує безпеку великих Layer2 або MPLS мереж, які потребують часткового або повного зв'язку.

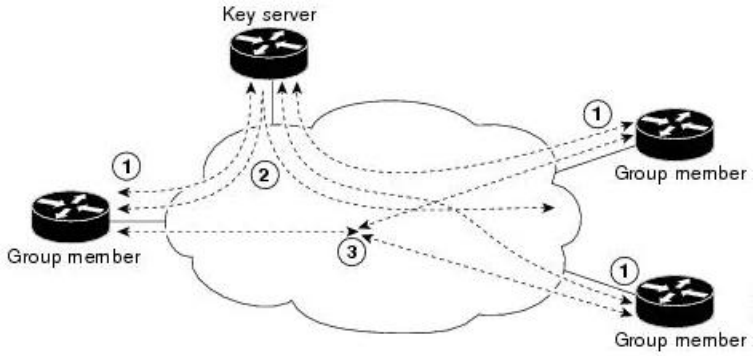


Рис. 1.12. Схема роботи GETVPN

Нововведенням GET VPN є введення поняття "довіреної групи", всі члени якої поділяють одну і ту ж IPSec SA(security association). Це дозволяє будь-якому члену групи (GM, group member) розшифрувати трафік, зашифрований будь-яким іншим GM. Крім того, оскільки розшифрувати наше повідомлення може кожен GM, ми можемо розсилати мультикаст.

Для всіх GM визначаються одні і ті ж ключі шифрування. Реалізується це за допомогою протоколу GDOI(Group Domain of Interpretation). Використовується два різних ключі: один для шифрування даних, інший для шифрування контрольних повідомлень. Пакет, який потрібно надіслати, інкапсулюється ESP з допомогою отриманого загального ключа. За синхронізацію і оновлення ключів відповідають сервера ключів (KS , key servers). Всі політики шифрування, використовувані протоколи, «цікавий» трафік, таймери та ін. налаштовуються на KS і поширюються по всьому GM. GM спочатку автентифіковані в IKE Phase 1, а потім отримують необхідні дані від KS під час реєстрації. Крім того, оскільки KS фактично стає точкою відмови для всієї мережі, передбачена можливість створення декількох KS, звані COOP KS (cooperative KS), з можливістю підхоплювати функції в режимі «холодного» резерву.

Висновки з першого розділу

При виконанні даного розділу кваліфікаційної роботи було проаналізовано поставлене завдання. Досліджено MPLS-мережу та було зроблено висновок, що це механізм передачі даних, який емулює різні властивості мереж з комутацією каналів через мережі з комутацією пакетів. Також було виявлено головні переваги та недоліки GET VPN. Було розглянуто BGP як єдиний протокол маршрутизації між автономними системами в глобальній мережі Інтернет. Це протокол міждоменної маршрутизації використовується усіма інтернет-провайдерами, а також великими компаніями та організаціями, які мають власні публічні номери автономних систем.

РОЗДІЛ 2. ВИБІР ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВСТАНОВЛЕННЯ ВІРТУАЛЬНИХ МАШИН ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ

2.1 Вибір програми для налаштування схеми та її встановлення

GNS3 - це графічний симулятор мережі, який дозволяє змоделювати віртуальну мережу з маршрутизаторів і віртуальних машин. Незамінний інструмент для навчання та тестів. Працює практично на всіх платформах. Дуже добре підходить для створення стендів на десктоп машинах. Залежно від апаратної платформи, на якій буде використовуватися GNS3, можлива побудова комплексних проектів, що складаються з маршрутизаторів Cisco, Cisco ASA, Juniper, а також серверів під управлінням мережевих операційних систем. Насправді GNS3 НЕ симулятор, а емулятор! Варто розуміти різницю між цими поняттями. Емулятор дозволяє створити модель комп'ютера або іншого пристрою і запускати всередині оригінальне програмне забезпечення. Емулюються всі основні компоненти пристрою, в тому числі процесор, пам'ять і пристрої введення/виводу. У випадку з Cisco, емулятор створює модель маршрутизатора і запускає всередині реальну операційну систему Cisco IOS. Таким чином ми отримуємо повнофункціональний маршрутизатор. Симулятор ж імітує поведінку системи і її інтерфейсу. Яскравий приклад - Cisco Packet Tracer. Програмісти цього ПО просто створили пристрої з схожим інтерфейсом і схожими командами. Переваги GNS3:

– Перша і найголовніша причина - повний функціонал емульованого пристроїв. Тобто запустивши той же маршрутизатор Cisco, нам будуть доступні практично всі функції, які працюють на реальному маршрутизаторі. Якщо згадати Cisco Packet Tracer, то там значна частина функціоналу недоступна, тому що це всього лише симулятор.

– Можливість побудови гетерогенних мереж. Мається на увазі, що ми можемо зібрати схему де будуть не тільки пристрої Cisco, а й Juniper, Mikrotik, CheckPoint і т.д. Погодьтеся, це більш схоже на реальне життя.

– Додавання в мережу повноцінних робочих станцій і серверів. Знову ж таки, якщо брати те й же самий Cisco Packet Tracer, то там в якості кінцевих пристроїв були доступні клієнтські комп'ютери або сервери з дуже обмеженим функціоналом. У GNS3 ми можемо додати повноцінний комп'ютер з Windows 7 або Ubuntu. Чи можемо використовувати в схемі Windows Server або RedHat. Забігаючи трохи вперед, можу сказати що робиться це за допомогою технологій віртуалізації (VirtualBox або VMWare) або підключивши GNS3 до реальної мережі. Таким чином ми можемо перевірити в лабораторній роботі установку VPN клієнта на робочу станцію, аутентифікацію користувачів через сервер AAA, використовувати справжній браузер при підключенні до цього Інтернету. Загалом що завгодно, як в реальному житті[23].

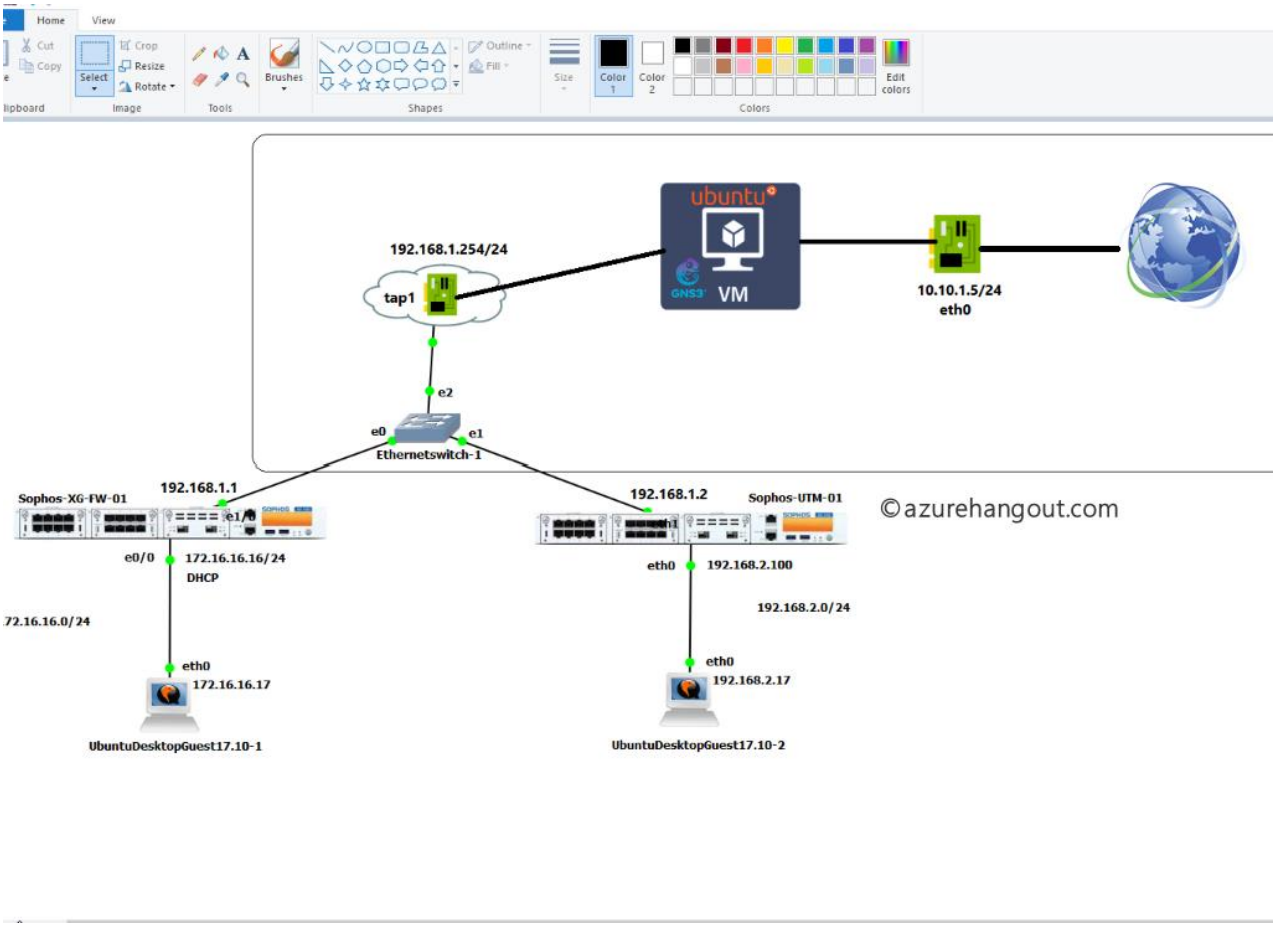


Рис. 2.1. Приклад робочої схема в емуляторі GNS3

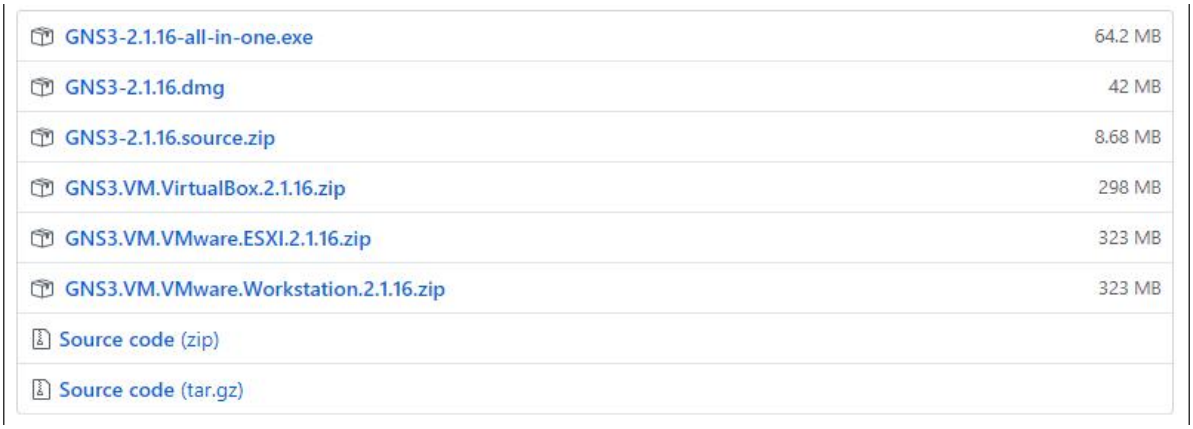


Рис. 2.2. Вибір потрібних файлів для скачування

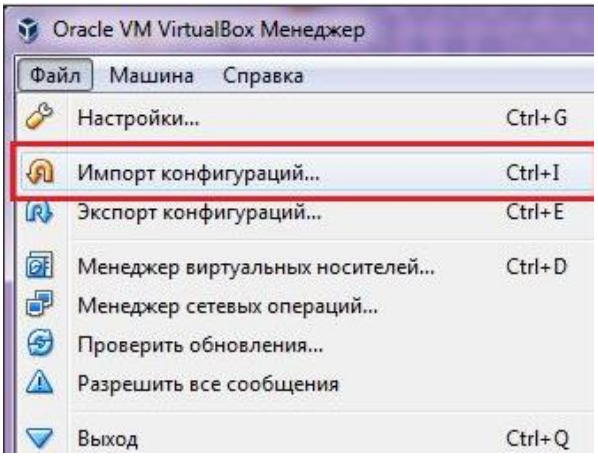


Рис. 2.3. Імпортування образу в Virtual Box

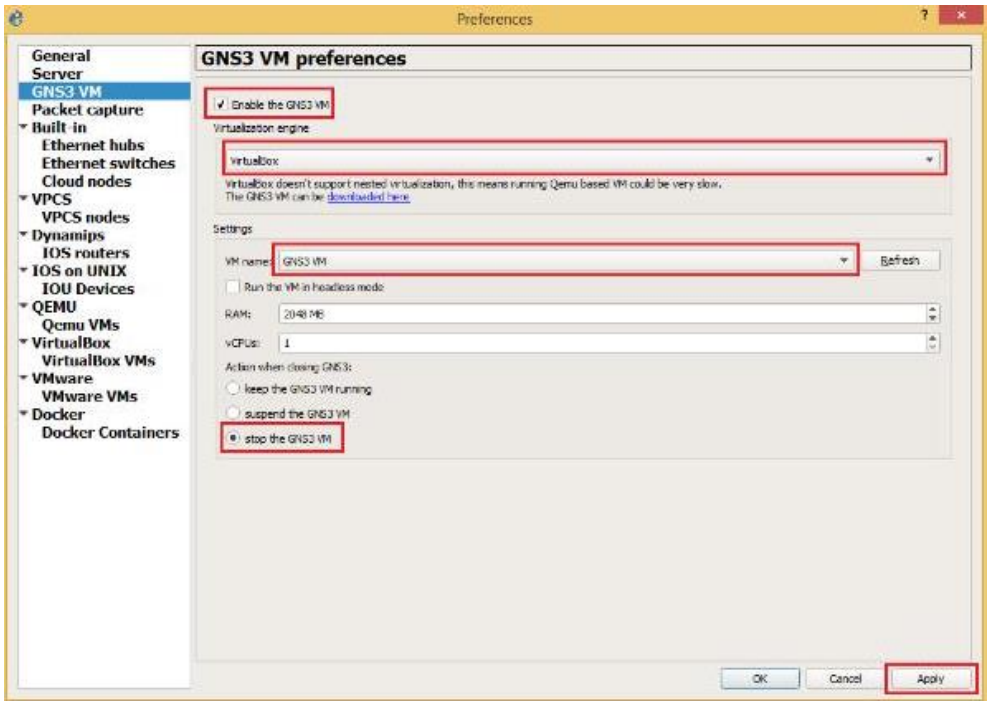


Рис. 2.4. Налаштування GNS3

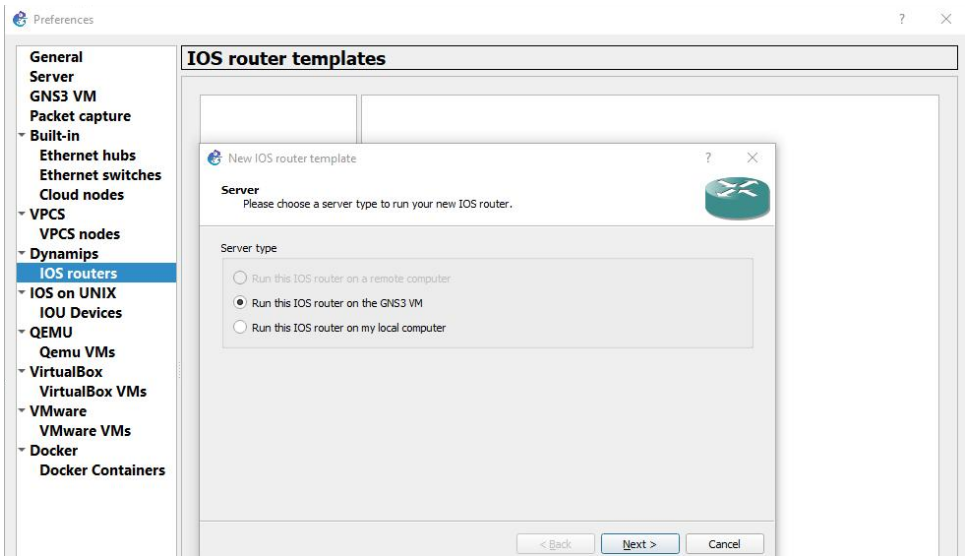


Рис. 2.5. Налаштування роутера в емуляторі GNS3

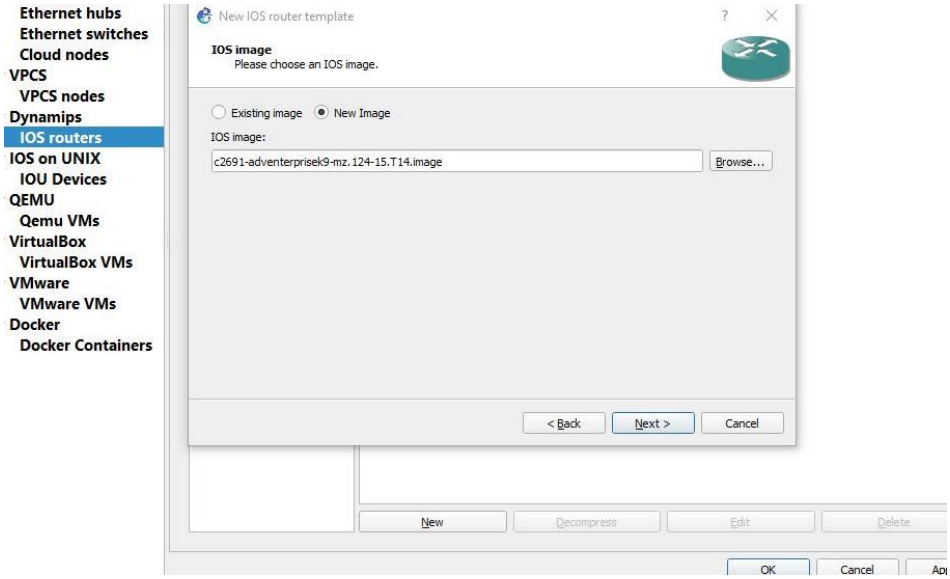


Рис. 2.6. Налаштування роутера в емуляторі GNS3

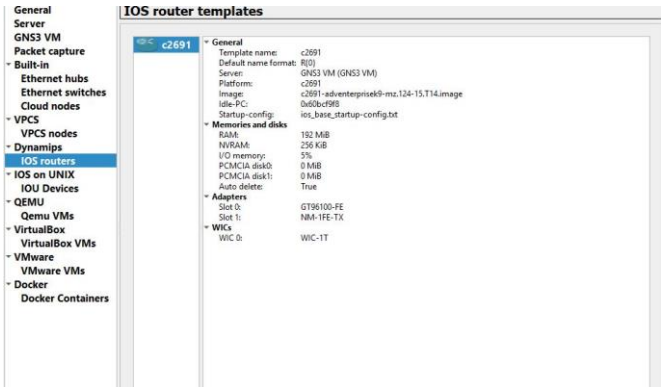


Рис. 2.7. Налаштування роутера в емуляторі GNS3

2.2. Завантаження та налаштування Virtual Box

Віртуальна машина (Virtual Machine) - програма, що емулює апаратне забезпечення комп'ютера, тобто це такий собі віртуальний комп'ютер, на який можна встановлювати операційну систему і все супутнє програмне забезпечення, при цьому ніяких змін у Вашій основній операційній системі не буде.

А навіщо ж нам потрібна ця сама віртуальна машина? Особисто я знайшов в цьому дві, але дуже важливі причини:

– Всім же коли-небудь хотілося побачити, як виглядають інші операційні системи такі як: Linux, Solaris, та й просто інші версії Windows. Але зносити свою систему не охота, так як раптом Вам нова ОС не сподобається і доведеться переставляти заново. Тому є таке рішення як віртуальна машина, за допомогою якої Ви легко можете встановлювати в ній інші ОС, а відповідно і тестувати їх, без перевстановлення своєї системи.

– Підійде для тих, хто вже опанував основами комп'ютера і хоче знати більше, наприклад, як налаштовується комп'ютерна мережа? Як налаштовуються різні служби сервера і так далі, на допомогу Вам прийде все та ж сама віртуальна машина, за допомогою якої Ви можете встановити кілька операційних систем (причому різних!) і так сказати проводити досліди, без шкоди своїй операційній системі. Це відмінно допомагає в освоєння комп'ютерних технологій, так як віртуальна машина допомагає практикуватися, якщо звичайно у Вас вдома є кілька комп'ютерів (3-4), то це інша ситуація[24].

Тепер перейдемо до встановлення та налаштування VirtualBox. Саме встановлення програми абсолютно стандартне і Ви її можете встановити без проблем.

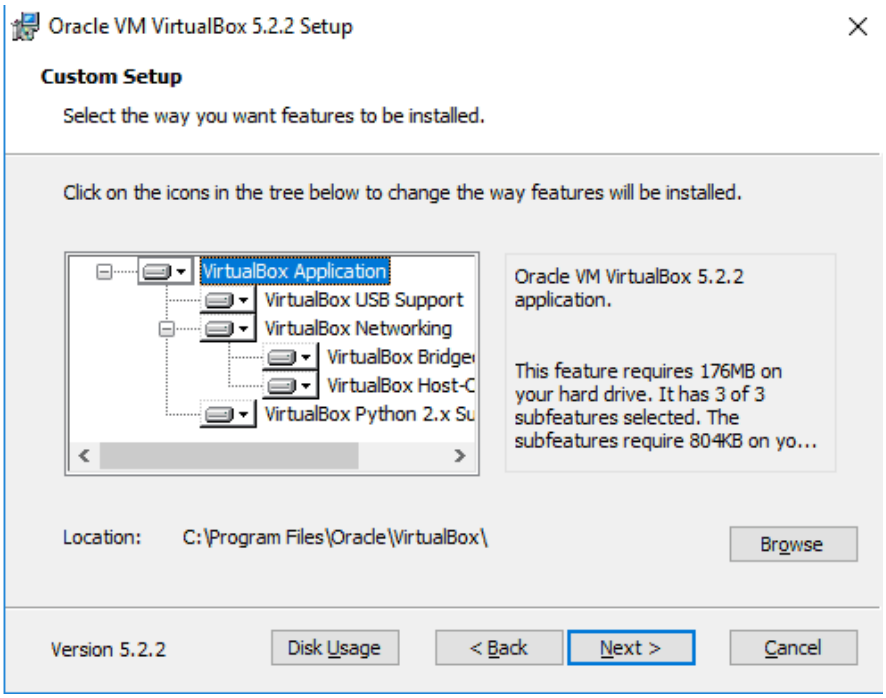


Рис. 2.8. Встановлення Virtual Box

Примітка: для роботи віртуальних машин потрібно, щоб на комп'ютері була включена віртуалізація VT-x або AMD-V в БІОС. Зазвичай вона включена за замовчуванням, але, якщо щось піде не так, враховуйте цей момент.

Тепер давайте створимо свою першу віртуальну машину. У прикладі далі використовується VirtualBox, запущена в Windows, як гостьова ОС (тієї, яка віртуалізується) буде Windows 10.

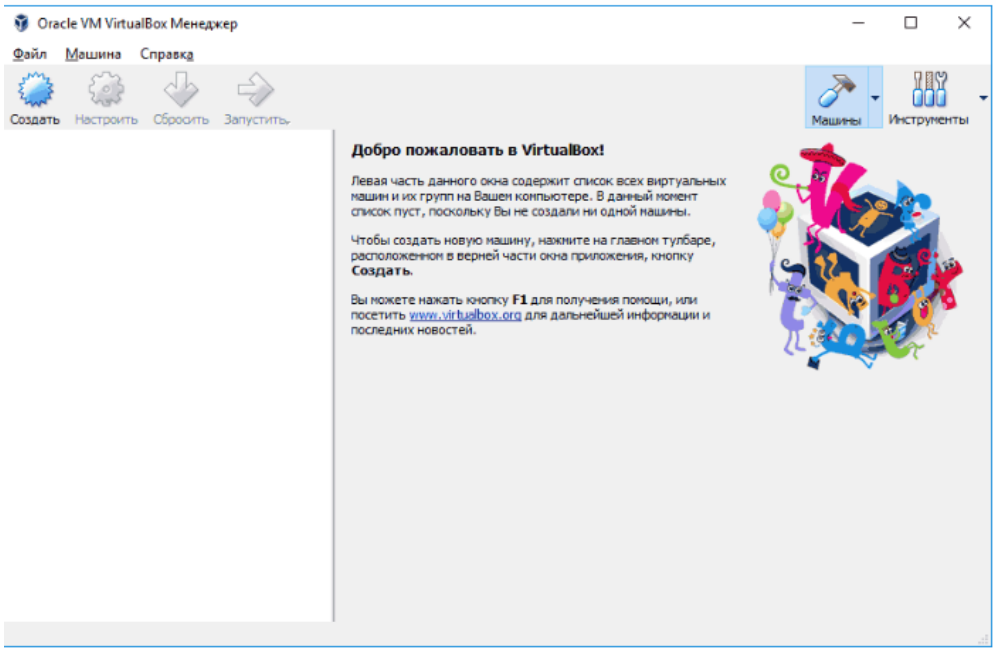


Рис. 2.9. Робоче вікно програми Virtual Box

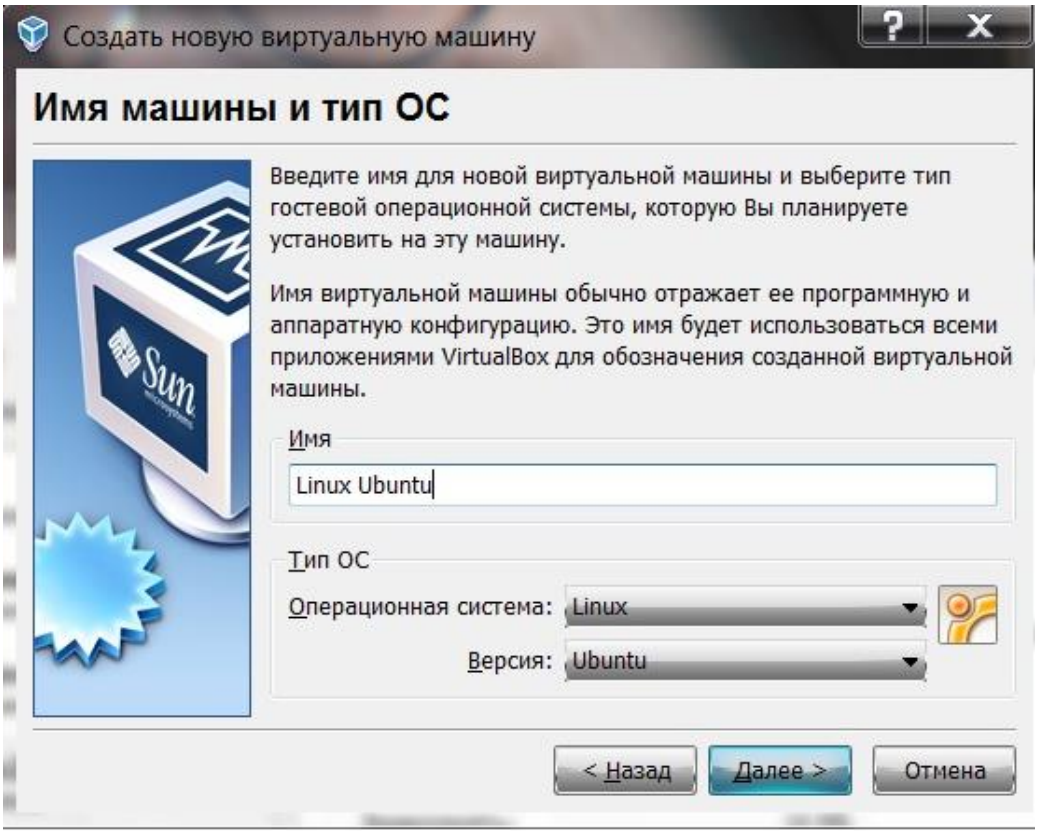


Рис. 2.10. Встановлення операційної системи

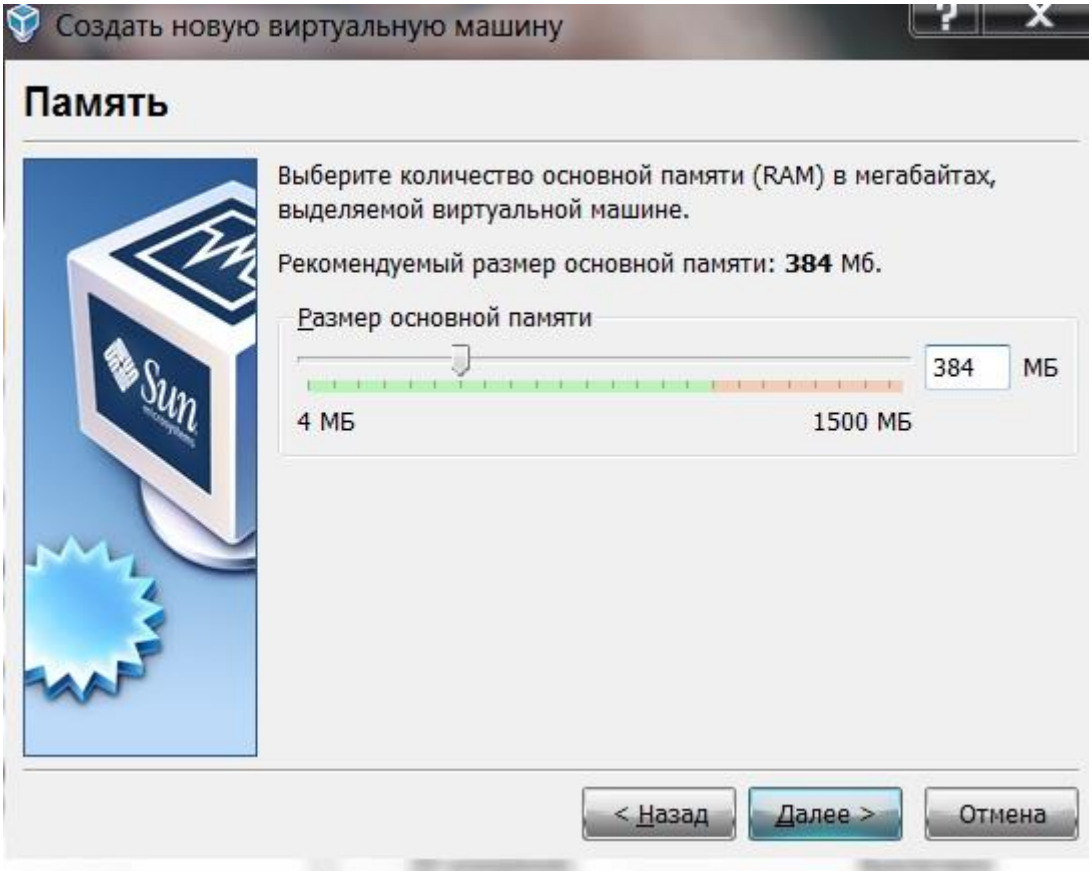


Рис. 2.11. Встановлення операційної системи

2.3 Опис та встановлення обладнання Juniper Networks в схему інтернет-провайдера

Juniper Networks - американська компанія, виробник телекомунікаційного устаткування , переважно для інтернет-провайдерів , корпорацій і державного сектора.

З моменту створення і по теперішній час, Juniper Networks спеціалізується на розробці швидкісних рішень по обробці потокових даних для вищого рівня мережевих рішень. Більшість продуктів компанії використовує мережеві процесори власної розробки і працює під управлінням JUNOS - операційної системи, заснованої на FreeBSD і містить повний набір POSIX - сумісних команд і інструментів. JUNOS також відома високим ступенем регрес-тестування[16].

JunOS OS - це FreeBSD, яку переробили інженери Juniper. JunOS, на відміну від IOS (НЕ IOS XR) має модульну архітектуру - складається з ядра і процесів, які відповідають тільки за свою окрему функцію. Під кожен процес виділяється частина пам'яті. Що це нам дає? Якщо у нас ламається якийсь із процесів, припустимо процес, який відповідає за vrrp, то він не тягне за собою всі інші процеси і той же rpd або ppmd процеси будуть працювати.

Ядро виконує базові функції ОС - керування процесами і взаємодія між ними, за поділ доступу процесів до пам'яті, процесору і іншим ресурсам RE. За інші функції - управління обладнанням, маршрутизацію, моніторинг стану заліза і т.д. відповідають спеціальні процеси (daemons), які стартують при завантаженні системи.

Якщо якийсь із процесів при завантаженні не може запуститися з якихось причин, то він буде перезапущений. Якщо перезапуск не приведе до позитивного результату, то інформація про проблему з цим процесом буде згенеровано в лог для того, що б інженери могли розібратися з причиною виникнення проблеми і виправити її. У JunOS OS дуже багато різних процесів, тому ми розберемо найважливіші з них:

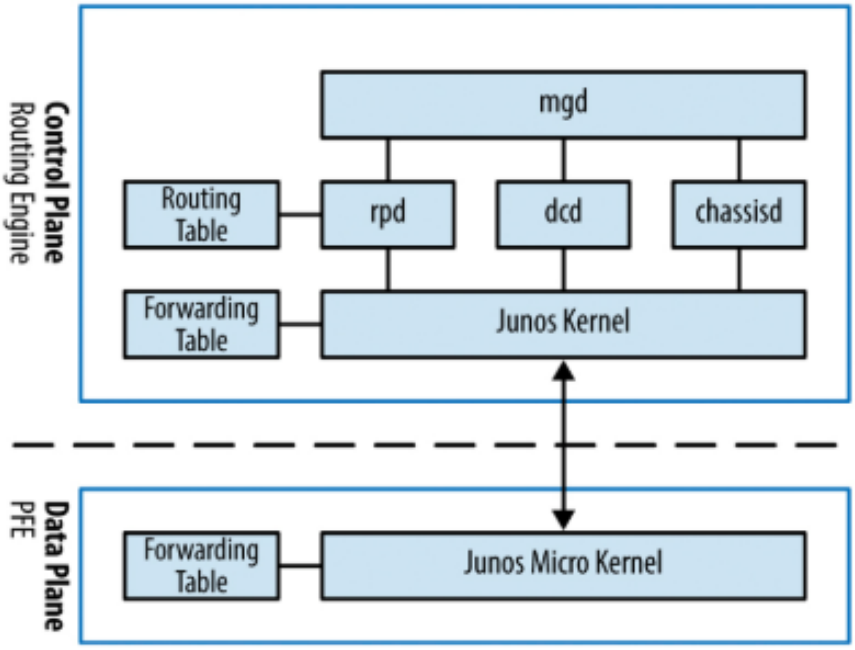


Рис. 2.12. Найголовніші процеси операційної системи JUNOS

mgd - management daemon. Даний процес відповідає за управління обладнанням та іншими процесами, CLI є його клієнтом. Саме завдяки mgd ми можемо користуватися такими функціями, як rollback, private conguration mode, виводити частину конфігурації в inacive або застосовувати apply-групи.

dcd - Device control daemon. Даний процес відповідає за конфігурацію інтерфейсів. Саме він дозволяє нам конфігурувати неіснуючий інтерфейс. Даний демон передасть в routing socket інформацію про сконфігуровані інтерфейси, що б rpd згодом зміг додати маршрут в таблицю маршрутизації.

chassisd - chassis daemon. Один з найбільш важливих процесів в JunOS. Саме він відповідає за моніторинг стану всіх компонентів маршрутизатора (від напруги на різних вузлах маршрутизатора до швидкості обертання вентиляторів). У разі будь-яких проблем даний процес відключить плату або / і маршрутизатор в уникненні поломки або передасть інформацію про проблему alarmd / craftd процесам, а вони в свою чергу, згенерують повідомлення в лог і включать будь-який індикатор craft-панелі маршрутизатора.

rpd- routing protocol daemon. Даний процес відповідає за всі протоколи маршрутизації, від rip до bgp. Він відповідає за підтримання сусідства між пристроями і обмін між ними маршрутною інформацією, вибір кращого маршруту, складання таблиць маршрутизації і таблиці форвардинга, яка використовується безпосередньо для просування пакетів.

PFE обробляє весь трафік, включаючи і трафік управління (якщо управління здійснюється не через console або management порт на самому RE). PFE складається з програмованих чіпів, які дозволяють виробляти аппаратано:

- пошук next-hop;
- виконувати ip / mpls / mac lookup;
- застосовувати QoS;
- застосовувати фільтрацію;
- туннелювання.

PFE встановлений на інтерфейсній карті. Є плати з 1-м, 2-ма або 4-ма PFE, кожен PFE обслуговує тільки свою групу інтерфейсів і взаємодіє з іншими PFE через SCB. У складі інтерфейсної карти є CPU, який керує всіма PFE. Зв'язок між PFE і RE проводиться через вбудований в плату SCB гігабітний свіч.

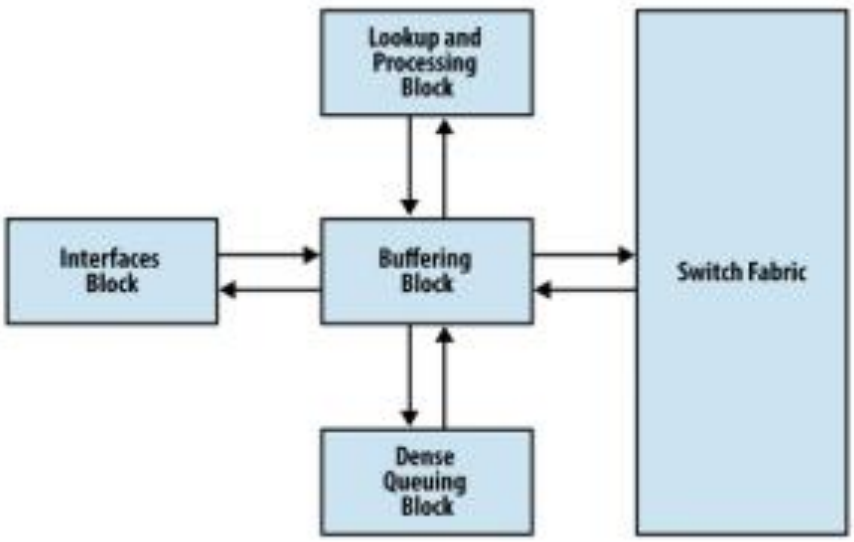


Рис. 2.13. Склад PFE

Memory and Buffering block - даний блок забезпечує взаємодію між усіма іншими блоками. У звичайних платах (без індексу Q) виконує і функції блоку черг (природно в більш урізаному варіанті), а в платах з великою ємністю виконує функцію блоку інтерфейсів.

Lookup block - багатоядерний чіп, який виконує ip або mpls lookup, виробляє зміну заголовків пакету, застосування фільтрів, шейпер, QoS. Саме цей блок є центром PFE. Блок працює з заголовками пакетів і може аналізувати заголовки розміром до 256 байт (що дозволяє реалізувати різні сервіси, типу захисту від DDOS).

Interface block - даний блок присутній на платах з малою пропускною здатністю і виконує функцію попередньої класифікації вхідних пакетів. Якщо даний блок відсутній, то цю функцію виконує блок буферизації.

Dense Queuing block - блок розширених черг. Представлений на платах з індексом Q і дозволяє реалізувати H-QoS. При відсутності даного блоку його функції переходять на блок буферизації.

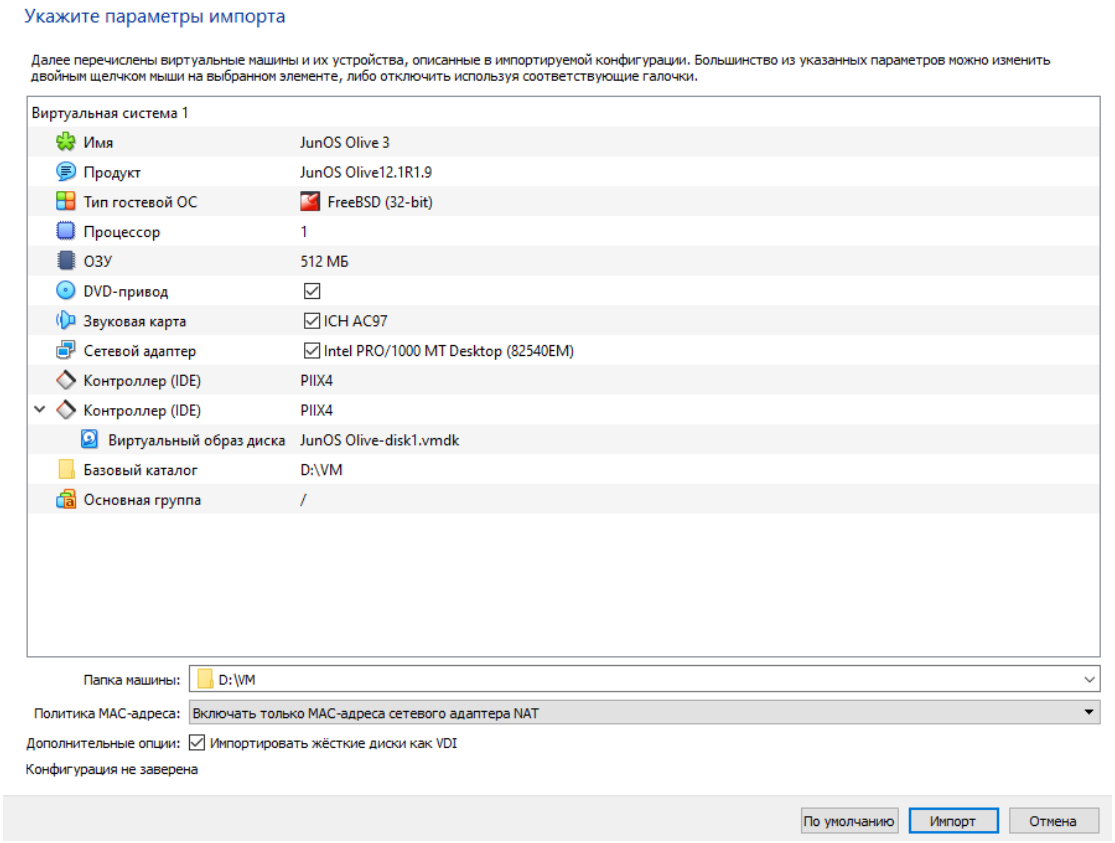


Рис. 2.14. Імпортування операційної системи JUNOS в Virtual Box

2.4. Розробка схеми адресації пристроїв

Таблиця 2.1.

Параметри адресації мережі

Мережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	Префікс
Підмережа A	-	1.1.1.0	255.255.255.0	/24
Підмережа B	-	1.1.2.0	255.255.255.0	/24
Підмережа C	-	3.3.3.0	255.255.255.0	/24
Підмережа D	-	2.2.2.0	255.255.255.0	/24
Підмережа E	-	2.2.1.0	255.255.255.0	/24
Підмережа F	-	192.2.12.0	255.255.255.0	/24
Підмережа G	-	172.2.12.0	255.255.255.0	/24
Підмережа H	-	172.2.13.0	255.255.255.0	/24
Підмережа I	-	192.2.13.0	255.255.255.0	/24
Підмережа J	-	202.2.2.0	255.255.255.0	/24
Підмережа K	-	202.2.3.0	255.255.255.0	/24
Підмережа L	-	202.2.4.0	255.255.255.0	/24
Підмережа M	-	182.2.2.0	255.255.255.0	/24

Продовження Табл. 2.1.

Параметри адресації мережі

Підмережа N	-	182.2.3.0	255.255.255.0	/24
Підмережа O	-	182.2.4.0	255.255.255.0	/24
Підмережа P	-	182.2.5.0	255.255.255.0	/24
Маршутизатор JunOS-ASBR	Інтерфейс L0	1.1.0.1	255.255.255.255	/32
	Інтерфейс Eth0	1.1.1.1	255.255.255.0	/24
	Інтерфейс Eth1	3.3.3.1	255.255.255.0	/24
Маршутизатор Cisco-ASBR	Інтерфейс L0	2.2.0.2	255.255.255.255	/32
	Інтерфейс Fa0/0	2.2.2.1	255.255.255.0	/24
	Інтерфейс Fa0/1	3.3.3.2	255.255.255.0	/24
Маршутизатор JunOS-P	Інтерфейс L0	1.1.0.3	255.255.255.255	/32
	Інтерфейс Eth0	1.1.1.2	255.255.255.0	/24
	Інтерфейс Eth1	1.1.2.2	255.255.255.0	/24
Маршутизатор JunOS-PE	Інтерфейс L0	1.1.0.4	255.255.255.255	/32

Продовження Табл. 2.1.

Параметри адресації мережі

	Інтерфейс Eth0	192.2.12.1	255.255.255.0	/24
	Інтерфейс Eth2	172.2.12.1	255.255.255.0	/24
	Інтерфейс Eth1	1.1.2.1	255.255.255.0	/24
Маршутизатор Cisco-P	Інтерфейс L0	2.2.0.5	255.255.255.255	/32
	Інтерфейс Fa0/0	2.2.2.2	255.255.255.0	/24
	Інтерфейс Fa0/1	2.2.1.2	255.255.255.0	/24
Маршутизатор Cisco-PE	Інтерфейс L0	2.2.0.6	255.255.255.255	/32
	Інтерфейс Fa1/0	192.2.13.1	255.255.255.0	/24
	Інтерфейс Fa1/1	172.2.13.1	255.255.255.0	/24
	Інтерфейс Fa0/1	2.2.1.1	255.255.255.0	/24
Маршутизатор BGroupMember 1	Інтерфейс Fa0/0	192.2.12.2	255.255.255.0	/24
	Інтерфейс Fa0/1	202.2.2.1	255.255.255.0	/24
Маршутизатор AGroupMember 1	Інтерфейс Fa0/0	172.2.12.2	255.255.255.0	/24
	Інтерфейс Fa0/1	182.2.2.1	255.255.255.0	/24
Маршутизатор PrimaryKeyServer	Інтерфейс Fa0/0	172.2.13.2	255.255.255.0	/24

Продовження Табл. 2.1.

Параметри адресації мережі

	Інтерфейс Fa0/1	182.2.3.1	255.255.255.0	/24
Маршутизатор SecondaryKeyServer	Інтерфейс Fa0/0	172.2.13.3	255.255.255.0	/24
	Інтерфейс Fa0/1	182.2.4.1	255.255.255.0	/24
Маршутизатор AGroupMember 2	Інтерфейс Fa0/0	172.2.13.4	255.255.255.0	/24
	Інтерфейс Fa0/1	182.2.5.1	255.255.255.0	/24
Маршутизатор BGroupMember 2	Інтерфейс Fa0/0	192.2.13.3	255.255.255.0	/24
	Інтерфейс Fa0/1	202.2.4.1	255.255.255.0	/24
Маршутизатор KeyServer	Інтерфейс Fa0/0	192.2.13.2	255.255.255.0	/24
	Інтерфейс Fa0/1	202.2.3.1	255.255.255.0	/24

Висновки з другого розділу

При виконанні даного розділу кваліфікаційної роботи було проаналізовано можливі програми для виконання проекту. Було обрано GNS3, оскільки доступний повний функціонал емульованих пристроїв. Тобто запустивши той же маршрутизатор Cisco, нам будуть доступні практично всі функції, які працюють на реальному маршрутизаторі. Було проаналізовано обладнання Juniper Networks та обрано найкраще з них для схеми інтеренет-провайдера. Зроблено висновок, що JunOS OS - це FreeBSD, яку переробили інженери Juniper. Також розроблено схему адресації пристроїв мережі.

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

3.1. Налагодження MPLS L3VPN Inter-AS Option B

Опорна мережа оператора побудована на базі маршрутизаторів Cisco 7200 серії та Juniper з використанням технології MPLS.

```
    }
    em1 {
        unit 0 {
            family inet {
                address 1.1.2.2/24;
            }
            family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 1.1.0.3/32;
            }
        }
    }
}
routing-options {
    router-id 1.1.0.3;
}
protocols {
    mpls {
        icmp-tunneling;
        interface em0.0;
        interface em1.0;
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface em0.0 {
                interface-type p2p;
            }
            interface em1.0 {
                interface-type p2p;
            }
        }
    }
    ldp {
        interface em0.0;
        interface em1.0;
    }
```

Рис. 3.1. Налагодження маршрутизатора JUNOS-P

```
!
interface Loopback0
 ip address 2.2.0.5 255.255.255.255
 ip ospf 1 area 0
!
interface FastEthernet0/0
 ip address 2.2.2.2 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet0/1
 ip address 2.2.1.2 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
 duplex auto
 speed auto
 mpls ip
!
```

Рис. 3.2. Налагодження маршрутизатора CISCO-P

JunOS-P та Cisco-P - маршрутизатори всередині мережі оператора (MPLS домену). P-пристрої в схемі виконують функції LSR, тобто виконують комутацію по міткам. На них було налаштовано базову маршрутизацію та проколи mpls та ldp. У мережі MPLS-VPN для P-маршрутизаторів використовується дворівневий стек міток, за допомогою якого пакети передаються по магістралі з одного сайту VPN в інший.

```
routing-options {
    router-id 1.1.0.1;
    autonomous-system 65100;
}
protocols {
    mpls {
        icmp-tunneling;
        label-switched-path toPE {
            to 1.1.0.4;
        }
        interface em0.0;
        interface em1.0;
    }
    bgp {
        group IBGP {
            type internal;
            local-address 1.1.0.1;
            family inet-vpn {
                unicast;
            }
            neighbor 1.1.0.4 {
                export next-hop-self;
            }
        }
        group EBGP {
            type external;
            family inet-vpn {
                unicast;
            }
            peer-as 65200;
            neighbor 3.3.3.2;
        }
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface em0.0 {
                interface-type p2p;
            }
        }
    ldp {
        interface em0.0;
        interface em1.0;
    }
}
policy-options {
    policy-statement next-hop-self {
        term A {
            from {
                protocol bgp;
                neighbor 3.3.3.2;
            }
            then {
                next-hop self;
            }
        }
    }
}
```

Рис. 3.3. Налагодження маршрутизатора JUNOS-ASBR

ASBR - прикордонний роутер автономної системи OSPF, знаходиться на кордоні з іншою автономною системою. На маршрутизаторі було налаштовано базову маршрутизацію, протокол BGP(IBGP та EBGP). IBGP (Internal BGP) - використовується для з'єднання сусідів BGP в одній автономній системі. IBGP працює всередині автономної системи для обміну BGP інформацією, так що всі BGP-роутери мають однакову BGP маршрутну інформацію про зовнішні автономні системи. Коли BGP працює між маршрутизаторами різних автономних систем, це називається EBGP. За замовчуванням, маршрутизатори, на яких працює EBGP, мають пряме з'єднання один з одним.

```
router bgp 65200
 bgp router-id 2.2.0.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 no bgp default route-target filter
 neighbor 2.2.0.6 remote-as 65200
 neighbor 2.2.0.6 update-source Loopback0
 neighbor 3.3.3.1 remote-as 65100
 !
 address-family ipv4
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.0.6 activate
  neighbor 2.2.0.6 send-community extended
  neighbor 2.2.0.6 next-hop-self
  neighbor 3.3.3.1 activate
  neighbor 3.3.3.1 send-community extended
 exit-address-family
!
```

Рис. 3.4. Налагодження EBGP і IBGP на маршрутизаторі Cisco-ASBR

```
interface FastEthernet0/1
 ip address 3.3.3.2 255.255.255.0
 duplex auto
 speed auto
 mpls bgp forwarding
```

Рис. 3.5. Команда mpls bgp forwarding на інтерфейсі

Вузол повинен розуміти, чи може він надсилати/приймати пакет з міткою через будь-яку взаємодію. Коли LDP використовується як протокол розподілу міток, включення "mpls ip" не тільки дозволить LDP (контрольна площина), але також дозволяє LSR надсилати/приймати пакет з міткою через інтерфейс. У випадку варіанта B Inter-AS, BGP використовується як протокол розподілу міток між ASBR. Таким чином, команда "mpls bgp forwarding" дозволяє ASBR

надсилати/приймати мічений пакет через налаштований інтерфейс (що спрямовано до іншого ASBR)[27]. Коли ви налаштовуєте LDP на маршрутизаторі з комутацією міток (LSR), маршрутизатор починає надсилати повідомлення виявлення LDP з усіх інтерфейсів, що підтримуються LDP. Коли сусідній LSR отримує повідомлення про виявлення LDP, він встановлює базовий сеанс TCP[26].

Next-hop в BGP відрізняється від IGP протоколів. У BGP next-hop, як правило, вказує на eBGP-сусіда, який відправив оновлення в локальну автономну систему. Відповідно, для iBGP-маршрутизаторів, next-hop знаходиться не в безпосередньо приєднаній мережі.

Для того щоб отриманий маршрут був обраний як найкращий в таблиці BGP і був поміщений в таблицю маршрутизації, необхідно щоб зазначений next-hop був доступний. Перевірка доступності next-hop фактично змушує маршрутизатор двічі переглядати таблицю маршрутизації для того щоб визначити доступність цього маршруту - це і називається рекурсивною маршрутизацією . Для того щоб перевірка доступності next-hop була пройдена, необхідно щоб в IGP протоколі, який працює в локальній автономній системі, був маршрут до цього next-hop. Якщо next-hop для певного маршруту недоступний, то цей маршрут буде збережений в таблиці BGP, але він не може бути поміщений а таблицю маршрутизації.

```
router bgp 65200
 bgp router-id 2.2.0.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 no bgp default route-target filter
 neighbor 2.2.0.6 remote-as 65200
 neighbor 2.2.0.6 update-source Loopback0
 neighbor 3.3.3.1 remote-as 65100
 !
```

Рис. 3.6. Команда no bgp default route-target filter на інтерфейсі

Коли BGP отримує маршрут VPN-IPv4 або VPN-IPv6 від іншого маршрутизатора PE, BGP зберігає цей маршрут у своїй локальній таблиці маршрутів, лише якщо принаймні один VRF імпортує route target цього маршруту. Якщо VRF не імпортує жодну з route target маршруту, BGP відкидає

маршрут; ця функція називається автоматичною фільтрацією за цільовим маршрутом. Намір полягає в тому, щоб BGP відслідковував маршрути тільки для безпосередньо підключених VPN, а також відкидав усі інші маршрути VPN-IPv4 або VPN-IPv6 для збереження пам'яті. Ми можемо скористатися командою no bgp default route-target filter, щоб вимкнути автоматичну фільтрацію для всіх VRF.

```
routing-instances {
    A {
        instance-type vrf;
        interface em2.0;
        route-distinguisher 65101:65201;
        vrf-target target:65101:65201;
        routing-options {
            router-id 172.2.12.1;
        }
        protocols {
            ospf {
                export BGP-to-OSPF;
                area 0.0.0.0 {
                    interface em2.0 {
                        interface-type p2p;
                    }
                }
            }
            ldp {
                interface em2.0;
            }
        }
    }
    B {
        instance-type vrf;
        interface em0.0;
        route-distinguisher 65102:65202;
        vrf-target target:65102:65202;
        routing-options {
            router-id 192.2.12.1;
        }
        protocols {
            ospf {
                export BGP-to-OSPF;
                area 0.0.0.0 {
                    interface em0.0 {
                        interface-type p2p;
                    }
                }
            }
            ldp {
                interface em0.0;
            }
        }
```

Рис. 3.7. Налаштування VRF на маршрутизаторі JunOS-PE

```
policy-options {
    policy-statement BGP-to-OSPF {
        term BGP {
            from protocol bgp;
            then accept;
        }
        term BGP1 {
            then reject;
        }
    }
```

Рис. 3.8. Policy-options на JunOS

```
!
router ospf 65201 vrf B
 router-id 192.2.13.1
 redistribute bgp 65200 subnets
!
router ospf 65200 vrf A
 router-id 172.2.13.1
 redistribute bgp 65200 subnets
!
router ospf 1
 router-id 2.2.0.6
!
router bgp 65200
 bgp router-id 2.2.0.6
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 2.2.0.2 remote-as 65200
 neighbor 2.2.0.2 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.0.2 activate
  neighbor 2.2.0.2 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf A
  redistribute connected
  redistribute ospf 65200 match internal external 1
 exit-address-family
 !
 address-family ipv4 vrf B
  redistribute connected
  redistribute ospf 65201 match internal external 1
 exit-address-family
```

Рис. 3.9. Налаштування на Cisco-PE

VRF - технологія, яка дозволяє реалізовувати на базі одного фізичного маршрутизатора мати кілька віртуальних - кожного зі своєю незалежною таблицею маршрутизації. Перевагою віртуальної маршрутизації є повна ізоляція маршрутів як між двома віртуальними маршрутизаторами, так і між віртуальним і реальним[29]. Ми створюємо списки імпорту route-target та списки експорту route-target для кожного VRF. Цілі маршруту, які ви розміщуєте у списку експорту route-target, додаються до кожного маршруту,

розміщеного на інших маршрутизаторах PE. Коли маршрутизатор PE отримує маршрут від іншого маршрутизатора PE, він порівнює route-target, приєднані до кожного маршруту, зі списком імпорту route-target, визначеним для кожного його VRF. Якщо будь-який route-target, приєднаний до маршруту, відповідає списку імпорту для VRF, то маршрут імпортується до цього VRF. Якщо жоден route-target не відповідає списку імпорту, маршрут відхиляється для цього VRF.

3.2. Налагодження Cisco Group Encrypted Transport Virtual Private Network (GET VPN)

```
R2(config)#$export rsa getvpn-export-general pem terminal 3des myrsakeypasswd
% Key name: getvpn-export-general
   Usage: General Purpose Key
   Key data:
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQChv7C3PwhMstU8FJnsWd2/80JS
mnYeL8SonJQEy2rRznTGLo3i9VSyq5uWmmruSN0ZA+LyTehNeVk7rULaJNRr5EQq
cYx7QInjTaORPjTTm7OlJFUTtCF8gFi3iA98MLfCaY7q/GMy8KqlocA5yI+CjzI6
t6rd/UApK/9wzFtl6wIDAQAB
-----END PUBLIC KEY-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,34A284EF005A1FCB

VFX5zpUEJWK3ShESCSFdZDoEdAZz2i/bZttKRVlueHhGTAxH7GWyVu7bxcERi29e
5trIQ9zBtEVZYXhxZhFgx0EG/Eqobr8lLR+vWhNFmHEjijJfSXcBhCZb+7HJsNje
oq6j7pL8gE0QdPo/wSVOX9YsW/A5jKyolsIqDm3GKVTG26C3XDyLjuw6IZ6vMelL
mEekpVCTCrsUQRuxt9JV6wBfOOvl7O/BEqrAvSQ7E0A6DzKlIg4UyJc8XliYRE60
vg57xO7U2DmcAE1SSoHuGZEaKHW3HlzoU4TeDxljuwrPx2NVZiZXLRGnmRpY7/ob
pjoqzLMNB2VHHAd/TffltOFDcgoitIOuBl3j56Vwr0owG9/nTnDvFpkpFDchzfBo
7ccZ8R2ANdQHEHrhy0ev5dCtlwCS6CbJR1TzPJudRvN+fATbY8C+0UQ2ZN8i7jCl
MKU78/SuMBoaVddvqhD+T2OfpocpVOMV5kknpR8Xs+k0+kcQF5nelLxRwF2Nz8Fh
5TpFomlVvecCidpvLjnw/kSqHGXIP+lxWtZ+lrzF6twl/f44BmlWCILexZAgo6vD
Q7+xIUpH59QU88qMbctvqWfWf8xi+oT2/xtakhUs9NExkxCqJbk56Zxhsrw3w+lz
B4aZ6+7lqhZ8POFnlP4BxORvMshy2X0uqjrlbvTkDpZMlLYCrRqjBeham3BtVS+G
TRr/SAmJ5H3IJqUYg2w7Mi/UksawpSRtkzN+2DeAsi0XpLdjG+fu0NI4VrEj6Gz5
c4lD9xpPi+B5OD4xeL7MGryfNrhw4mza3V4ZBWDWGHD6lch9TpkloQ==
-----END RSA PRIVATE KEY-----

R2(config)#
```

Рис. 3.10. Генерування ключів на головному Key Server

```
R3(config)#$ getvpn-export-general pem exportable terminal myrsakey
% Enter PEM-formatted public General Purpose key or certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQChv7C3PwhMstU8FJnsWd2/80JS
mnYeL8SonJQEy2rRznTGLo3i9VSyq5uWmmruSN0ZA+LyTehNeVk7rULaJNRr5EQq
cYx7QInjTaORPjTTm7OlJFUTtCF8gFi3iA98MLfCaY7q/GMy8KqlocA5yI+CjzI6
t6rd/UApK/9wzFtl6wIDAQAB
-----END PUBLIC KEY-----
quit
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,07E2B5257B485293

0/jBdfVY3LB2cRXR4mi/TEZG1JTUNuDYdbxtOnmdjL+yTHrB9JwH6mIow0hM6D+i
SHJGh+CYK46u8BZU1jfasAXqkHX3bpOjUTklEOTTVxQq7XIVQqSLFGIrIKNA53n7
KMon+uDQwUOn7zekgtt5qqB2SRAohuAELuCvOJmBAaWMQyPJI1UPBSksvsw+Uc9R
txX3zgb1HH43piqyRBb3JKdX8ADGh5iDaLQEGLrsfc2LiFZ03jSzNr6rx3ZQuE/F
V/R/K+wDh3QyPmby4cX+cz2U2osXbi3Xk3Ozg8Nu2eT0kjP8o6pzll9EDgdtgQQt
OmZmyBppUZ3n6eyuHRZ3HuNPsMWmMWyqIsL5mA+f3x25cHwGkcQvGOdKi8ZATi0v
lejY2+BuRx4EUPRlpI7PK3uqjHVbprVt3U3qjql+Qj0A4HvCsQQLG+B80KMElcup
GJV7akKw2FGseHcpNiYzJR+MaSYq+jb/T1Nj4+ZApiTl2RXDw5C2NTbRrH3JN18F
WGn9+GVEtA6j09CvJ+0490nvz5YvLNUqCgV25IfxbWzfGE1DTCURtTvpcEGwjmjR
P2O0v3jeLEvowkYg4hkYMUkt/o8V+F88ZjaevnUNcPEmF2bbfVKz7hobTPXFHtua
yWLXJS0kxqpWpo7VmqGhS40w+NEj3J1F+RdREdCQwbGbBrlhhZpAqvIpEhXUKJlE
6Gtlmh3JOa9wF0YIEztFAw2JWGDikEIJVJ1pjLEAdJ0ADHJ1ydx//2/Xn3QrQTix
l2SiLsvDsJ9ObTHvHo+wGhi3QTpwWqNGbq3zxl9+vLhMUl5Tq9nvrQ==
-----END RSA PRIVATE KEY-----
quit
% Key pair import succeeded.

R3(config)#
*Jun  7 13:39:51.655: %SSH-5-ENABLED: SSH 1.99 has been enabled
R3(config)#
```

Рис. 3.11. Імпорт ключів на запасному Key Server

Оскільки KS фактично стає точкою відмови для всієї мережі, передбачена можливість створення декількох KS, так звані COOP KS (cooperative KS), з можливістю підхоплювати функції в режимі «холодного» резерву.

Як уже згадувалося, ми можемо налаштувати кілька KS, один з яких буде основним, а інші - підхоплювати його функції при падінні. Отже, щоб налаштувати COOP KS потрібно наступне:

– Необхідно налаштувати RSA ключі на основному KS і експортувати обидва ключа (приватний і публічний) на всі COOP KS;

– Необхідно налаштувати власне redundancy.

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key $3cur3dG3tVpNK3Y address 172.2.0.0
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec transform-set GDOI-TRANS esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile GDOI-PROFILE
 set security-association lifetime seconds 7200
 set transform-set GDOI-TRANS
!
!
crypto gdoi group GETVPN-GROUP
 identity number 1234
 server local
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa getvpn-export-general
  rekey transport unicast
  sa ipsec 1
   profile GDOI-PROFILE
   match address ipv4 GETVPN-ACL
   replay time window-size 5
  address ipv4 172.2.13.2
  redundancy
   local priority 100
   peer address ipv4 172.2.13.3
```

Рис. 3.12. Налаштування головного сервера мережі

В обов'язки сервера ключів входить підтримка політики, створення та підтримка ключів для групи. Коли учасник групи реєструється, сервер ключів завантажує цю політику та ключі до члена групи. Сервер ключів також відновлює групу до закінчення терміну дії існуючих ключів. Ключовий сервер має два обов'язки: обслуговування запитів на реєстрацію та відправлення rekey. Член групи може зареєструватися в будь-який час та отримати найактуальнішу

політику та ключі. Коли учасник групи реєструється на сервері ключів, сервер ключів перевіряє ідентифікатор групи, який член групи намагається приєднати. Якщо цей ідентифікатор є дійсним ідентифікатором групи, сервер ключів відправляє політику SA члену групи. Після того як член групи визнає, що він може обробляти завантажену політику, сервер ключів завантажує відповідні ключі.

Існує два типи ключів, які сервер ключів може завантажувати: ключ шифрування ключа (KEK) та ключ шифрування трафіку (TEK). TEK стає IPsec SA, з яким спілкуються члени групи в межах однієї групи. KEK шифрує повідомлення rekey.

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key $3cur3dG3tVpNK3Y address 172.2.0.0
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec transform-set GDOI-TRANS esp-aes 256 esp-sha-hmac
 mode transport
!
crypto ipsec profile GDOI-PROFILE
 set security-association lifetime seconds 7200
 set transform-set GDOI-TRANS
!
!
crypto gdoi group GETVPN-GROUP
 identity number 1234
 server local
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa getvpn-export-general
  rekey transport unicast
  sa ipsec 1
   profile GDOI-PROFILE
   match address ipv4 GETVPN-ACL
   replay time window-size 5
  address ipv4 172.2.13.3
  redundancy
   local priority 75
   peer address ipv4 172.2.13.2
```

Рис. 3.13. Налаштування запасного сервера мережі

Повідомлення rekey також можуть періодично передаватися для обліку можливих втрат пакету. Втрата пакетів може статися через те, що повідомлення надсилаються без використання надійного транспорту. Якщо механізм повторної передачі є багатоадресним, не існує ефективного механізму зворотного зв'язку, за допомогою якого одержувачі можуть вказувати, що вони не отримали повідомлення про повторну передачу, тому повторна передача прагне довести всіх приймачів до актуальних даних. Якщо механізм повторної

передачі є одноадресним, одержувачі відправлять повідомлення про підтвердження.

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key $3cur3dG3tVpNK3Y address 172.2.13.2
crypto isakmp key $3cur3dG3tVpNK3Y address 172.2.13.3
!
!
!
!
crypto gdoi group GETVPN-GROUP
 identity number 1234
 server address ipv4 172.2.13.2
 server address ipv4 172.2.13.3
!
!
crypto map GETVPN-MAP 10 gdoi
 set group GETVPN-GROUP
!
```

Рис. 3.14. Налаштування AGroupMember1

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key $3cur3dG3tVpNK3Y address 172.2.13.2
crypto isakmp key $3cur3dG3tVpNK3Y address 172.2.13.3
!
!
!
!
crypto gdoi group GETVPN-GROUP
 identity number 1234
 server address ipv4 172.2.13.2
 server address ipv4 172.2.13.3
!
!
crypto map GETVPN-MAP 10 gdoi
 set group GETVPN-GROUP
!
```

Рис. 3.15. Налаштування AGroupMember1

Налаштування маршрутизатора IOS для використання IPsec починається з конфігурації політики ISAKMP та ключових даних аутентифікації ISAKMP маршрутизатора.

Cisco рекомендує використовувати AES, як найкращий за співвідношенням криптостійкість/ресурси процесора. Рекомендоване значення для rekey - 1200 с. Cisco рекомендує робити його в діапазоні 15-30 хвилин, з дефолтом в 20.

Команда crypto map використовується для створення або зміни записів криптографічних карт. Записи в криптографічних картах встановлюють параметри IPsec SA шифрування або аутентифікації трафіку. Якщо потрібно створити більше одного запису в криптографічного карті, то слід враховувати, що обробка трафіку буде проводитися в відповідністю з пріоритетами записів.

Команда crypto isakmp policy використовується для створення IKE політики, в якій зазначаються бажані алгоритми і параметри створюваного захищеного каналу, які будуть запропоновані партнеру для узгодження. Цей канал буде забезпечувати захист частині обмінів інформацією першої фази і всі обміни другої фази IKE. Таких політик може бути зазначено кілька з присвоєнням їм пріоритету.

```
encryption = gost (ГОСТ 28147-89)
hash = gost (ГОСТ Р34.11-94)
authentication = gost-sig
group = vko (VKO ГОСТ Р 34.10-2001)
lifetime = 86400
```

Рис. 3.16. Параметри за замовчуванням команди crypto isakmp policy

Член групи реєструються на сервері ключів, щоб отримати IPsec SA або SA, необхідні для зв'язку з групою. Член групи надає ідентифікатор групи на сервер ключів, щоб отримати відповідну політику та ключі для цієї групи. Ці дані періодично оновлюються, і до закінчення терміну дії поточних сертифікатів IPsec, щоб не було втрати трафіку. Висновок команди show crypto isakmp sa detail покаже аутентифікацію асоціації безпеки (SA) як "rsig", тому що підпис RSA використовується для автентифікації ключа перешифровки ключа (KEK) в GET VPN.

3.3. Тестування роботи схеми мережі

Схема складається с 10 маршрутизаторів Cisco та 3 маршрутизаторів Juniper. В схемі налаштовано MPLS L3VPN Inter-AS Option B та GETVPN. Між ASBR піднімається vpnv4 сесія, в рамках якої проводиться обмін vpnv4 маршрутами (необхідно налаштовувати фільтрацію префіксів на ASBR, що б не віддати або не одержати щось зайве).

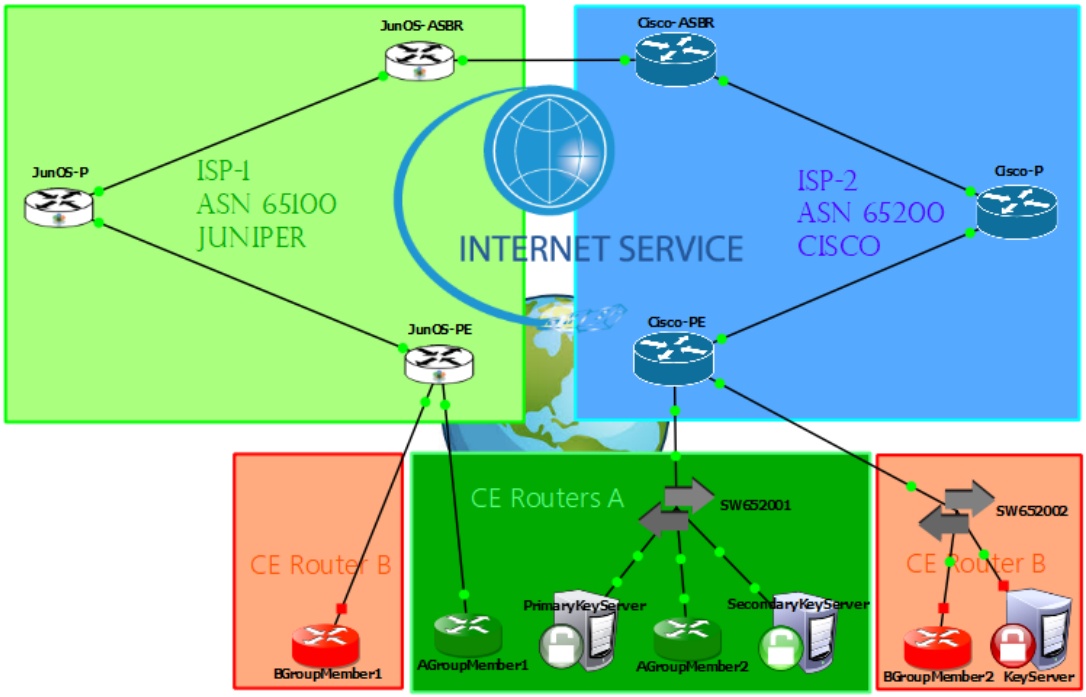


Рис. 3.17. Схема мережі провайдера

```
13:04:17.159: %BGP-5-ADJCHANGE: neighbor 3.3.3.1 Up
13:04:17.575: %LDP-5-NBRCHG: LDP Neighbor 2.2.0.5:0 (1) is UP
13:04:43.191: %BGP-5-ADJCHANGE: neighbor 2.2.0.6 Up
```

Рис. 3.18. Підняття bgp та ldp сусідів

```
AGroupMember1#ping 182.2.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.2.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/180/336 ms
AGroupMember1#traceroute 182.2.5.1
Type escape sequence to abort.
Tracing the route to 182.2.5.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.2.12.1 12 msec 20 msec 20 msec
  2 1.1.2.2 [MPLS: Labels 299792/300048 Exp 0] 140 msec 128 msec 116 msec
  3 1.1.1.1 [MPLS: Label 300048 Exp 0] 140 msec 92 msec 168 msec
  4 3.3.3.2 [MPLS: Label 25 Exp 0] 732 msec 296 msec 120 msec
  5 2.2.2.2 [MPLS: Labels 17/22 Exp 0] 140 msec 96 msec 148 msec
  6 172.2.13.1 [MPLS: Label 22 Exp 0] 132 msec 80 msec 76 msec
  7 172.2.13.4 172 msec 156 msec 84 msec
AGroupMember1#
```

Рис. 3.19. Перевірка зв’язку між кінцевими пристроями мережі

```
AGroupMember2#ping 182.2.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 182.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 124/168/220 ms
AGroupMember2#traceroute 182.2.2.1
Type escape sequence to abort.
Tracing the route to 182.2.2.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.2.13.1 488 msec 16 msec 36 msec
  2 2.2.1.2 [MPLS: Labels 16/20 Exp 0] 152 msec 48 msec 100 msec
  3 2.2.2.1 [MPLS: Label 20 Exp 0] 180 msec 144 msec 120 msec
  4 3.3.3.1 [MPLS: Label 299952 Exp 0] 124 msec 148 msec 184 msec
  5 1.1.1.2 [MPLS: Labels 299776/299824 Exp 0] 52 msec 120 msec 32 msec
  6 1.1.2.1 [MPLS: Label 299824 Exp 0] 104 msec 84 msec 104 msec
  7 172.2.12.2 152 msec 116 msec 160 msec
AGroupMember2#
```

Рис. 3.20. Перевірка зв'язку між кінцевими пристроями мережі

З вищенаведеного виводу traceroute ми бачимо, що для забезпечення доступності від одного клієнта до іншого використовуються три різних LSP (Label Switch Path).

У середовищах Multiprotocol Label Switching (MPLS) команда traceroute поводиться інакше, ніж у середовищах, що не є MPLS. Команда traceroute MPLS працює дещо інакше, ніж звичайна команда traceroute, оскільки маршрутизатори, на яких працює MPLS, обмінюються мітками для прийняття рішень про переадресацію замість інформації про маршрутизацію IP.

```
Cisco-PE#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  2.2.0.5/32       0             Fa0/1      2.2.1.2
17         16         2.2.0.2/32       0             Fa0/1      2.2.1.2
18         Pop Label  2.2.2.0/24       0             Fa0/1      2.2.1.2
```

Рис. 3.21. show mpls forwarding-table

```
Cisco-ASBR#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  2.2.0.5/32       0             Fa0/0      2.2.2.2
17         Pop Label  2.2.1.0/24       0             Fa0/0      2.2.2.2
18         Pop Label  3.3.3.1/32       0             Fa0/1      3.3.3.1
19         17         2.2.0.6/32       0             Fa0/0      2.2.2.2
```

Рис. 3.22. show mpls forwarding-table

```
Cisco-P#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  2.2.0.2/32       10494         Fa0/0      2.2.2.1
17         Pop Label  2.2.0.6/32       9849          Fa0/1      2.2.1.1
Cisco-P#
```

Рис. 3.23. show mpls forwarding-table

Local label показує локальне значення мітки для префікса, зазначеного в полі Prefix or Tunnel Id. Outgoing label вказує вихідну мітку або дію зроблену з міткою. Pop label означає видалення мітки з пакета (в даному випадку видаляється мітка 16). Поле Bytes label switched показує кількість переданих байтів з цією міткою.

```
Cisco-PE#show mpls ldp neighbor
    Peer LDP Ident: 2.2.0.5:0; Local LDP Ident 2.2.0.6:0
        TCP connection: 2.2.0.5.646 - 2.2.0.6.18737
        State: Oper; Msgs sent/rcvd: 87/86; Downstream
        Up time: 01:08:40
        LDP discovery sources:
          FastEthernet0/1, Src IP addr: 2.2.1.2
        Addresses bound to peer LDP Ident:
          2.2.2.2         2.2.0.5         2.2.1.2
Cisco-PE#
```

Рис. 3.24. show mpls ldp neighbor

За допомогою цієї команди ми можемо побачити ідентифікатор сусіда, ідентифікатор маршрутизатора, інформацію про з'єднання TCP між локальним маршрутизатором і сусідом, час існування сесії, кількість переданих пакетів.

```
Cisco-PE#show mpls ldp parameters
LDP Feature Set Manager: State Initialized
  LDP features:
    Basic
    IP-over-MPLS
    TDP
    IGP-Sync
    Auto-Configuration
    TCP-MD5-Rollover
Protocol version: 1
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 90 sec; interval: 10 sec
Downstream on Demand max hop count: 255
LDP for targeted sessions
LDP initial/maximum backoff: 15/120 sec
LDP loop detection: off
Cisco-PE#
```

Рис. 3.25. show mpls ldp parameters

У висновку команди show mpls ldp parameters виводиться інформація про версію протоколу, діапазон використовуваних міток, тимчасових параметрах протоколів TDP / LDP.

show ip bgp vpnv4 all - показує всі префікси VPNv4, запамятовані за допомогою BGP.

```
Cisco-PE#show ip bgp vpnv4 all
BGP table version is 13, local router ID is 2.2.0.6
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
Route Distinguisher: 65101:65201 (default for vrf A)
 *>i 172.2.12.0/24    2.2.0.2                  0    100      0 65100 i
 *>  172.2.13.0/24    0.0.0.0                  0         32768 ?
 *>  172.2.13.2/32    172.2.13.2               1         32768 ?
 *>  172.2.13.3/32    172.2.13.3               1         32768 ?
 *>  172.2.13.4/32    172.2.13.4               1         32768 ?
 *>i 182.2.2.0/24     2.2.0.2                  0    100      0 65100 i
 *>  182.2.3.1/32     172.2.13.2               1         32768 ?
 *>  182.2.4.1/32     172.2.13.3               1         32768 ?
 *>  182.2.5.1/32     172.2.13.4               1         32768 ?
Route Distinguisher: 65102:65202 (default for vrf B)
 *>  192.2.13.0       0.0.0.0                  0         32768 ?
Cisco-PE#
```

Рис. 3.26. show ip bgp vpnv4 all

```
Cisco-ASBR#show ip bgp vpnv4 all
BGP table version is 11, local router ID is 2.2.0.2
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
Route Distinguisher: 65101:65201
 *>  172.2.12.0/24    3.3.3.1                                0 65100 i
 *>i 172.2.13.0/24    2.2.0.6                  0    100      0 ?
 *>i 172.2.13.2/32    2.2.0.6                  1    100      0 ?
 *>i 172.2.13.3/32    2.2.0.6                  1    100      0 ?
 *>i 172.2.13.4/32    2.2.0.6                  1    100      0 ?
 *>  182.2.2.0/24     3.3.3.1                                0 65100 i
 *>i 182.2.3.1/32     2.2.0.6                  1    100      0 ?
 *>i 182.2.4.1/32     2.2.0.6                  1    100      0 ?
 *>i 182.2.5.1/32     2.2.0.6                  1    100      0 ?
Route Distinguisher: 65102:65202
 *>i 192.2.13.0       2.2.0.6                  0    100      0 ?
Cisco-ASBR#
```

Рис. 3.27. show ip bgp vpnv4 all

IGP відповідають за створення та збереження інформації про маршрутизацію в домені AS, і тому вони вважаються "внутрішніми". Ці протоколи будують структуру AS, і, враховуючи їх застосування в більш широких мережах, як і Інтернет-провайдери, найважливішими характеристиками, які вони повинні мати, є надійність та оптимізація трафіку, генерованого протоколами.

```
root@JUNOS-PE> show route protocol bgp

inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

A.inet.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.2.13.0/24       *[BGP/170] 01:45:05, localpref 100, from 1.1.0.1
                      AS path: 65200 ?
                     > to 1.1.2.2 via eml.0, Push 299824, Push 299776(top)
172.2.13.2/32       *[BGP/170] 01:45:05, localpref 100, from 1.1.0.1
                      AS path: 65200 ?
                     > to 1.1.2.2 via eml.0, Push 299840, Push 299776(top)
172.2.13.3/32       *[BGP/170] 01:45:05, localpref 100, from 1.1.0.1
                      AS path: 65200 ?
                     > to 1.1.2.2 via eml.0, Push 299856, Push 299776(top)
172.2.13.4/32       *[BGP/170] 01:45:05, localpref 100, from 1.1.0.1
                      AS path: 65200 ?
                     > to 1.1.2.2 via eml.0, Push 299872, Push 299776(top)
182.2.3.1/32        *[BGP/170] 01:45:05, localpref 100, from 1.1.0.1
                      AS path: 65200 ?
                     > to 1.1.2.2 via eml.0, Push 299888, Push 299776(top)
182.2.4.1/32        *[BGP/170] 01:45:05, localpref 100, from 1.1.0.1
                      AS path: 65200 ?
                     > to 1.1.2.2 via eml.0, Push 299904, Push 299776(top)
182.2.5.1/32        *[BGP/170] 01:45:05, localpref 100, from 1.1.0.1
                      AS path: 65200 ?
                     > to 1.1.2.2 via eml.0, Push 299920, Push 299776(top)

B.inet.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.2.13.0/24       *[BGP/170] 01:45:05, localpref 100, from 1.1.0.1
                      AS path: 65200 ?
                     > to 1.1.2.2 via eml.0, Push 299936, Push 299776(top)

mpls.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)

bgp.l3vpn.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```

Рис. 3.28. show route bgp

```
root@JUNOS-ASBR> show route advertising-protocol bgp 3.3.3.2 detail

bgp.l3vpn.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
* 65101:65201:172.2.12.0/24 (1 entry, 1 announced)
 BGP group EBGP type External
     Route Distinguisher: 65101:65201
     VPN Label: 299808
     Nexthop: Self
     Flags: Nexthop Change
     AS path: [65100] I
     Communities: target:65101:65201

* 65101:65201:182.2.2.0/24 (1 entry, 1 announced)
 BGP group EBGP type External
     Route Distinguisher: 65101:65201
     VPN Label: 299808
     Nexthop: Self
     Flags: Nexthop Change
     AS path: [65100] I
     Communities: target:65101:65201 rte-type:0.0.0.0:1:0

root@JUNOS-ASBR>
```

Рис. 3.29. show route advertising-protocol bgp 3.3.3.2 detail

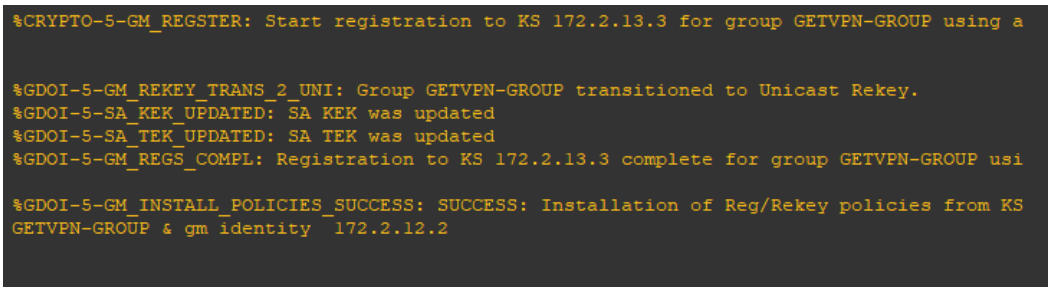


Рис. 3.30. Повідомлення на GroupMember

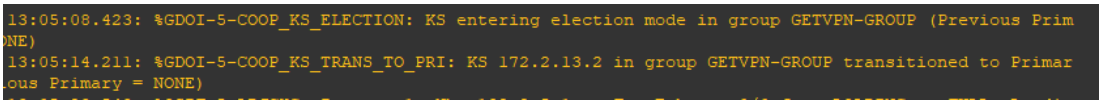


Рис. 3.31. Повідомлення на KeyServer

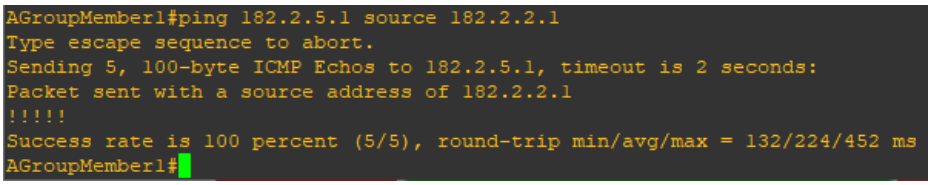


Рис. 3.32. Проходження трафіку між GroupMember

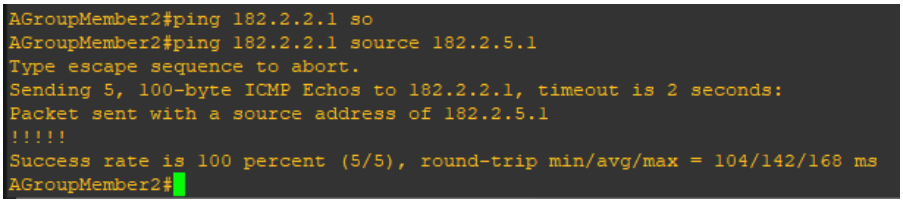


Рис. 3.33. Проходження трафіку між GroupMember

Цікавий трафік ініціює процес IPSec - трафік вважається цікавим, коли політика безпеки IPSec, сконфігурована у членів IPSec, запускає процес IKE. Передача даних - дані передаються між колегами IPSec на основі параметрів IPSec та ключів, що зберігаються в базі даних SA. Визначення того, який тип трафіку вважається цікавим, є частиною формулювання політики безпеки для використання VPN. Потім політика реалізується в інтерфейсі конфігурації для кожного конкретного партнера IPSec. Наприклад, у маршрутизаторах Cisco використовуються списки доступу для визначення трафіку для шифрування. Списки доступу присвоюються таким чином, що заяви дозволу вказують на те, що вибраний трафік повинен бути зашифрований, а заяви про заборону можна використовувати для вказівки на те, що вибраний трафік повинен надсилатися незашифрованим.

Команда show crypto ipsec sa використовується для виведення на екран інформації про IPsec з'єднання.

```
AGroupMember1#sh cry ipsec sa

interface: FastEthernet0/0
    Crypto map tag: GETVPN-MAP, local addr 172.2.12.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (182.2.0.0/255.255.0.0/0/0)
   remote ident (addr/mask/prot/port): (182.2.0.0/255.255.0.0/0/0)
   current_peer 0.0.0.0 port 848
     PERMIT, flags={}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #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.: 172.2.12.2, remote crypto endpt.: 0.0.0.0
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x3E8821FB(1049108987)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x3E8821FB(1049108987)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 5, flow_id: SW:5, sibling_flags 80000000, crypto map: GETVPN-MAP
        sa timing: remaining key lifetime (sec): (203)
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
        replay detection support: Y  replay window size: 5
        Status: ACTIVE(ACTIVE)
      spi: 0xCB405E2(213124578)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 7, flow_id: SW:7, sibling_flags 80000000, crypto map: GETVPN-MAP
        sa timing: remaining key lifetime (sec): (6659)
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
        replay detection support: Y  replay window size: 5
        Status: ACTIVE(ACTIVE)
```

Рис. 3.34. show crypto ipsec sa

```
AGroupMember2#sh cry ipsec sa

interface: FastEthernet0/0
    Crypto map tag: GETVPN-MAP, local addr 172.2.13.4

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (182.2.0.0/255.255.0.0/0/0)
   remote ident (addr/mask/prot/port): (182.2.0.0/255.255.0.0/0/0)
   current_peer 0.0.0.0 port 848
     PERMIT, flags={}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #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.: 172.2.13.4, remote crypto endpt.: 0.0.0.0
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x3E8821FB(1049108987)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x3E8821FB(1049108987)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 5, flow_id: SW:5, sibling_flags 80000000, crypto map: GETVPN-MAP
        sa timing: remaining key lifetime (sec): (135)
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
        replay detection support: Y  replay window size: 5
        Status: ACTIVE(ACTIVE)
      spi: 0xCB405E2(213124578)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 7, flow_id: SW:7, sibling_flags 80000000, crypto map: GETVPN-MAP
        sa timing: remaining key lifetime (sec): (6583)
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
        replay detection support: Y  replay window size: 5
        Status: ACTIVE(ACTIVE)
```

Рис. 3.35. show crypto ipsec sa

В даний час не існує автоматичної синхронізації конфігурації між первинними та вторинними KS, тому вони повинні бути виправлені вручну. Оскільки COOP є важливою (і майже завжди обов'язковою) конфігурацією для GETVPN, важливо переконатися, що COOP працює правильно, а ролі COOP KS є правильними:

```
PrimaryKeyServer#sh crypto gdoi ks coop
Crypto Gdoi Group Name :GETVPN-GROUP
        Group handle: 2147483650, Local Key Server handle: 2147483650

        Local Address: 172.2.13.2
        Local Priority: 100
        Local KS Role: Primary   , Local KS Status: Alive
        Local KS version: 1.0.4
        Primary Timers:
                Primary Refresh Policy Time: 20
                Remaining Time: 11
                Antireplay Sequence Number: 998

        Peer Sessions:
        Session 1:
                Server handle: 2147483651
                Peer Address: 172.2.13.3
                Peer Version: 1.0.4
                Peer Priority: 75
                Peer KS Role: Secondary , Peer KS Status: Alive
                Antireplay Sequence Number: 2

                IKE status: Established
                Counters:
                    Ann msgs sent: 997
                    Ann msgs sent with reply request: 1
                    Ann msgs recv: 0
                    Ann msgs recv with reply request: 2
                    Packet sent drops: 0
                    Packet Recv drops: 1
                    Total bytes sent: 675760
                    Total bytes recv: 823
```

Рис. 3.36. show crypto gdoi ks coop

```
SecondaryKeyServer#sh crypto gdoi ks coop
Crypto Gdoi Group Name :GETVPN-GROUP
        Group handle: 2147483650, Local Key Server handle: 2147483650

        Local Address: 172.2.13.3
        Local Priority: 75
        Local KS Role: Secondary , Local KS Status: Alive
        Local KS version: 1.0.4
        Secondary Timers:
                Sec Primary Periodic Time: 30
                Remaining Time: 18, Retries: 0
                Invalid ANN PST recvd: 2
                New GM Temporary Blocking Enforced?: No
                Antireplay Sequence Number: 3

        Peer Sessions:
        Session 1:
                Server handle: 2147483651
                Peer Address: 172.2.13.2
                Peer Version: 1.0.4
                Peer Priority: 100
                Peer KS Role: Primary   , Peer KS Status: Alive
                Antireplay Sequence Number: 998

                IKE status: Established
                Counters:
                    Ann msgs sent: 1
                    Ann msgs sent with reply request: 2
                    Ann msgs recv: 996
                    Ann msgs recv with reply request: 1
                    Packet sent drops: 0
                    Packet Recv drops: 2
                    Total bytes sent: 1470
                    Total bytes recv: 675220


SecondaryKeyServer#
```

Рис. 3.37. show crypto gdoi ks coop

Коли процес реєстрації починається вперше, GM та KS домовляються про сесію обміну ключами (IKE), щоб захистити трафік GDOI. Щодо GM, перевіряємо чи IKE успішно встановлено:

```
PrimaryKeyServer#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.2.13.2      172.2.13.4      GDOI_IDLE         1003 ACTIVE
172.2.13.2      172.2.13.3      GDOI_IDLE         1001 ACTIVE
172.2.13.3      172.2.13.2      GDOI_IDLE         1002 ACTIVE

IPv6 Crypto ISAKMP SA

PrimaryKeyServer#
```

Рис. 3.38. show crypto gdoi ks coop

```
AGroupMember1#show crypto isa sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.2.13.3      172.2.12.2      GDOI_IDLE         1001 ACTIVE
172.2.12.2      172.2.13.2      GDOI_REKEY        1002 ACTIVE

IPv6 Crypto ISAKMP SA
```

Рис. 3.39. show crypto gdoi ks coop

Висновки з третього розділу

При виконанні даного розділу кваліфікаційної роботи було обрано моделі пристроїв для мережі, сладено схему. Також було проведене базове налуштування пристроїв, MPLS L3VPN Inter-AS Option B, GET VPN. Виконане повне тестування правильності налаштування пристроїв мережі. Було досліджено MPLS-мережу та зроблено висновок, що це механізм передачі даних, який емулює різні властивості мереж з комутацією каналів через мережі з комутацією пакетів. Були переглянуті важливі команди діагностики схеми під час роботи GETVPN, щоб переконатися, що все працює правильно.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було спроектовано та налаштовано схему базового інтернет-провайдера на обладнанні Cisco та Juniper:

1. Досліджено MPLS-мережу та було зроблено висновок, що це механізм передачі даних, який емулює різні властивості мереж з комутацією каналів через мережі з комутацією пакетів. MPLS (Multiprotocol Label Switching) являється дуже актуальною технологією сучасних віртуальних приватних мереж. Однією з сильних сторін технології MPLS є те, що вона може використовуватися спільно з різними протоколами рівня 2. Серед цих протоколів - PPP, ATM, Frame Relay, Ethernet. Протокол PPP (Point-to-Point Protocol) застосовується для передачі IP-пакетів по комутованих і виділених каналах. Маршрутизатор з підтримкою MPLS використовує вміст мітки MPLS для вказівки маршруту, грунтуючись на вимогах додатка до рівня якості обслуговування QoS. Усередині мережі MPLS вміст заголовка IP-пакета більше не потребує розгляду для визначення маршруту.
2. Cisco GET VPN - нова технологія від Cisco, покликана забезпечити безпеку тунелів через провайдерські з'єднання, що володіє рядом корисних особливостей. Ми маємо нову технологію, що дозволяє шифрувати з'єднання між офісами. Основна область застосування - підвищення конфіденційності MPLS VPN. Переваги - підтримка spoke-to-spoke з'єднань, висока масштабованість і підтримка мультикаст. Недоліки - прямий наслідок з відсутності тунелів - обмежена до неможливості робота через public Internet. Особливістю є наявність загальних IPSec ключів, що дозволяють всім членам групи розшифровувати повідомлення, надіслані іншими членами цієї групи. Були переглянуті важливі команди діагностики схеми під час роботи GETVPN, щоб переконатися, що все працює правильно.

3. Було проаналізовано можливі програми для виконання проекту. Було обрано GNS3, оскільки доступний повний функціонал емульованих пристроїв. Тобто запустивши той же маршрутизатор Cisco, нам будуть доступні практично всі функції, які працюють на реальному маршрутизаторі. Емулюються всі основні компоненти пристрою, в тому числі процесор, пам'ять і пристрої введення / виводу. У випадку з Cisco, емулятор створює модель маршрутизатора і запускає всередині реальну операційну систему Cisco IOS. Було проаналізовано обладнання Juniper Networks та обрано найкраще з них для схеми інтеренет-провайдера. Зроблено висновок, що JunOS OS - це FreeBSD, яку переробили інженери Juniper.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гольдштейн А.Б. Технология и протоколы MPLS / А.Б. Гольдштейн, Б.С. Гольдштейн. — СПб. : БХВ – Санкт-Петербург, 2005. — 304 с
2. Олвейн В. Структура и реализация современной технологии MPLS. Руководство Cisco / Вивек Олвейн. — М. : Вильямс, 2004. — 480 с.
3. GETVPN [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/84120/
4. Бараш Л. Виртуальные частные сети на базе MPLS / Леонид Бараш // Компьютерное Обозрение. — 2004. — № 17. — с. 14–16.
5. Trace Route in MPLS Network [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/200510-Trace-route-in-MPLS-network.html
6. BGP Inter-AS [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/302600/\
7. Как построена сеть интернет-провайдера [Електронний ресурс] – Режим доступу до ресурсу: https://vasexperts.ru/blog/seti/kak-postroena-set-internet-provajdera/
8. MPLS L3VPN [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/273679/
9. Cisco Group Encrypted Transport VPN Configuration Guide [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get-vpn-xe-3s-book/sec-get-vpn.html
10. Group Encrypted Transport VPN (GETVPN) [Електронний ресурс] – Режим доступу до ресурсу: https://networklessons.com/cisco/ccie-routing-switching-written/group-encrypted-transport-vpn-getvpn

11. Configuring OSPF Areas [Електронний ресурс] – Режим доступу до ресурсу: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/configuring-ospf-areas.html#id-example-configuring-a-single-area-ospf-network

12. Group VPN Overview [Електронний ресурс] – Режим доступу до ресурсу: https://www.juniper.net/documentation/en_US/release-independent/nce/topics/concept/nce-134-group-vpn-mx-overview.html

13. Постачальник послуг Інтернету [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Постачальник_послуг_Інтернету

14. Basic MPLS Configuration [Електронний ресурс] – Режим доступу до ресурсу: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/mpls-basic-configuration.html#id-mpls-configuration-overview

15. Example: Configuring MPLS-Based Layer 3 VPNs [Електронний ресурс] – Режим доступу до ресурсу: https://www.juniper.net/documentation/en_US/junos/topics/example/mpls-qfx-series-vpn-layer3.html

16. Настройка mpls l3 vpn в junos [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/sandbox/80039/

17. SIMPLE JUNIPER MPLS CORE WITH L3VPN [Електронний ресурс] – Режим доступу до ресурсу: https://juniperlabs.wordpress.com/2014/01/16/simple-juniper-mpls-core-with-l3vpn/

18. Томас Т. Структура и реализация сетей на основе протокола OSPF. Руководство Cisco / Том Томас. — М. : Вильямс, 2004. — 816 с.

19. Rosen, E. Multiprotocol Label Switching Architecture / E. Rosen, A. Viswanathan, R. Callon. — RFC 3031, 2001. — 61 с.

20. TCP/IP (Transmission Control Protocol/Internet Protocol) [Електронний ресурс] – Режим доступу до ресурсу: https://ru.bmstu.wiki/index.php?title=TCP/IP_(Transmission_Control_Protocol/Internet_Protocol)&mobileaction=toggle_view_mobile

21. How to configure OSPF on Juniper [Електронний ресурс] – Режим доступу до ресурсу: https://www.letsconfig.com/how-to-configure-ospf-on-juniper/

22. MPLS Inter AS Option B [Електронний ресурс] – Режим доступу до ресурсу: http://wiki.kemot-net.com/mpls-inter-as-option-b

23. Основы GNS3. Обзор [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/266503/

24. VirtualBox [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/VirtualBox

25. GET (Group Encrypted Transport) VPN [Електронний ресурс] – Режим доступу до ресурсу: https://sites.google.com/site/amitsciscozone/home/ipsec/get-vpn

26. LDP Overview [Електронний ресурс] – Режим доступу до ресурсу: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/ldp-overview.html

27. MPLS LDP Configuration Guide [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/12-4m/mp-ldp-12-4m-book.pdf

28. Label Distribution Protocol [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Label_Distribution_Protocol

29. Описание, настройка и пример использования VRF на Cisco [Електронний ресурс] – Режим доступу до ресурсу: http://ciscotips.ru/vrf#:~:text=VRF%20–%20технология%2C%20позволяющая%20реализовывать%20на,со%20своей%20независимой%20таблицей%20маршрутизации.

30. Основные сервисы в сетях интернет-провайдера [Електронний ресурс] – Режим доступу до ресурсу: https://vasexperts.ru/blog/seti/osnovnye-servisy-v-setyax-internet-provajdera/

ДОДАТКИ

Додаток А

Cisco маршрутизатори

```
Cisco-PE#show run
Building configuration...

Current configuration : 2682 bytes
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Cisco-PE
boot-start-marker
boot-end-marker
vrf definition A
 rd 65101:65201
 address-family ipv4
  route-target export 65101:65201
  route-target import 65101:65201
 exit-address-family
vrf definition B
 rd 65102:65202
 address-family ipv4
  route-target export 65102:65202
  route-target import 65102:65202
 exit-address-family
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
redundancy
ip tcp synwait-time 5
interface Loopback0
 ip address 2.2.0.6 255.255.255.255
 ip ospf 1 area 0
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 2.2.1.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
 duplex auto
 speed auto
 mpls ip
interface FastEthernet1/0
 vrf forwarding B
 ip address 192.2.13.1 255.255.255.0
 ip ospf network point-to-multipoint
 ip ospf 65201 area 0
 duplex auto
 speed auto
!
interface FastEthernet1/1
 vrf forwarding A
 ip address 172.2.13.1 255.255.255.0
 ip ospf network point-to-multipoint
 ip ospf 65200 area 0
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
```

```
 duplex auto
 speed auto

interface FastEthernet2/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router ospf 65201 vrf B
 router-id 192.2.13.1
 redistribute bgp 65200 subnets
!
router ospf 65200 vrf A
 router-id 172.2.13.1
 redistribute bgp 65200 subnets
!
router ospf 1
 router-id 2.2.0.6
!
router bgp 65200
 bgp router-id 2.2.0.6
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 2.2.0.2 remote-as 65200
 neighbor 2.2.0.2 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.0.2 activate
  neighbor 2.2.0.2 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf A
  redistribute connected
  redistribute ospf 65200 match internal external 1
 exit-address-family
 !
 address-family ipv4 vrf B
  redistribute connected
  redistribute ospf 65201 match internal external 1
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
 transport input all
end
```

```
Cisco-ASBR#show run
Building configuration...

Current configuration : 1998 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Cisco-ASBR
boot-start-marker
boot-end-marker
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
redundancy
ip tcp synwait-time 5
interface Loopback0
 ip address 2.2.0.2 255.255.255.255
 ip ospf 1 area 0
!
interface FastEthernet0/0
 ip address 2.2.2.1 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet0/1
 ip address 3.3.3.2 255.255.255.0
 duplex auto
 speed auto
 mpls bgp forwarding
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router ospf 1
 router-id 2.2.0.2
!
router bgp 65200
 bgp router-id 2.2.0.2
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 no bgp default route-target filter
```

```
 neighbor 2.2.0.6 remote-as 65200
 neighbor 2.2.0.6 update-source Loopback0
 neighbor 3.3.3.1 remote-as 65100
address-family ipv4
 exit-address-family
address-family vpnv4
  neighbor 2.2.0.6 activate
  neighbor 2.2.0.6 send-community extended
  neighbor 2.2.0.6 next-hop-self
  neighbor 3.3.3.1 activate
  neighbor 3.3.3.1 send-community extended
 exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
!mgcp profile default
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
 transport input all
end
PrimaryKeyServer#show run
Building configuration...
Current configuration : 2289 bytes
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname PrimaryKeyServer
boot-start-marker
boot-end-marker
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
redundancy
ip tcp synwait-time 5
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key $3cur3dG3tVpNK3Y address
172.2.0.0
crypto isakmp keepalive 10 periodic
crypto ipsec transform-set GDOI-TRANS esp-aes 256
esp-sha-hmac
 mode transport
crypto ipsec profile GDOI-PROFILE
 set security-association lifetime seconds 7200
 set transform-set GDOI-TRANS
crypto gdoi group GETVPN-GROUP
 identity number 1234
 server local
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa getvpn-export-
general
  rekey transport unicast
```

```
 sa ipsec 1
  profile GDOI-PROFILE
  match address ipv4 GETVPN-ACL
  replay time window-size 5
 address ipv4 172.2.13.2
 redundancy
  local priority 100
  peer address ipv4 172.2.13.3
interface FastEthernet0/0
 ip address 172.2.13.2 255.255.255.0
 ip ospf network point-to-multipoint
 ip ospf 1 area 0
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 182.2.3.1 255.255.255.0
 ip ospf network point-to-multipoint
 ip ospf 1 area 0
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet2/1
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 router-id 182.2.3.1
ip forward-protocol nd
no ip http server
no ip http secure-server
ip access-list extended GETVPN-ACL
 permit ip 182.2.0.0 0.0.255.255 182.2.0.0 0.0.255.255
no cdp log mismatch duplex
control-plane
gcp profile default
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
 transport input all
```

Додаток Б

Juniper маршрутизатори

```
root@JUNOS-ASBR# show
version 12.1R1.9;
system {
    host-name JUNOS-ASBR;
    root-authentication {
        encrypted-password
"$1$oTJQnXWw$V5NCbpJgRbOVU9hsIOQy11"; ##
SECRET-DATA
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
interfaces {
    em0 {
        unit 0 {
            family inet {
                address 1.1.1.1/24;
            }
            family mpls;
        }
    }
    em1 {
        unit 0 {
            family inet {
                address 3.3.3.1/24;
            }
        family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 1.1.0.1/32;
            }
        }
    }
routing-options {
    router-id 1.1.0.1;
    autonomous-system 65100;
}
protocols {
    mpls {
        icmp-tunneling;
        label-switched-path toPE {
            to 1.1.0.4;
        }
        interface em0.0;
        interface em1.0;
    }
    bgp {
        group IBGP {
            type internal;
            local-address 1.1.0.1;
            family inet-vpn {
                unicast;
            }
            neighbor 1.1.0.4 {
```

```
export next-hop-self;
            }
        }
        group EBGP {
            type external;
            family inet-vpn {
                unicast;
            }
            peer-as 65200;
            neighbor 3.3.3.2;
        }
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface em0.0 {
                interface-type p2p;
            }
        }
    }
    ldp {
        interface em0.0;
        interface em1.0;
    }
}
policy-options {
    policy-statement next-hop-self {
        term A {
            from {
                protocol bgp;
                neighbor 3.3.3.2;
            }
            then {
                next-hop self;
            }
        }
    }
}

[edit]
root@JUNOS-PE# show
version 12.1R1.9;
system {
    host-name JUNOS-PE;
    root-authentication {
        encrypted-password
"$1$Q1dUWvO8$c1nDuNznNSULmZ5WUg51i1"; ##
SECRET-DATA
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
interfaces {
    em0 {
        unit 0 {
            family inet {
                address 192.2.12.1/24;
            }
            family mpls;
```

```
    }
    }
    em1 {
        unit 0 {
            family inet {
                address 1.1.2.1/24;
            }
            family mpls;
        }
    }
    em2 {
        unit 0 {
            family inet {
                address 172.2.12.1/24;
            }
            family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 1.1.0.4/32;
            }
        }
    }
}
routing-options {
    router-id 1.1.0.4;
    autonomous-system 65100;
}
protocols {
    mpls {
        icmp-tunneling;
        label-switched-path toASBR {
            to 1.1.0.1;
        }
        interface em1.0;
        interface em2.0;
        interface em0.0;
    }
    bgp {
        group IBGP {
            type internal;
            local-address 1.1.0.4;
            family inet-vpn {
                unicast;
            }
            neighbor 1.1.0.1;
        }
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface em1.0 {
                interface-type p2p;
            }
        }
    }
    ldp {
        interface em1.0;
    }
}
policy-options {
    policy-statement BGP-to-OSPF {
        term BGP {
            from protocol bgp;
            then accept;
        }
        term BGP1 {
```

```
            then reject;
        }
    }
    policy-statement OSPF-to-BGP {
        term OSPF {
            from protocol ospf;
            then accept;
        }
    }
}
routing-instances {
    A {
        instance-type vrf;
        interface em2.0;
        route-distinguisher 65101:65201;
        vrf-target target:65101:65201;
        routing-options {
            router-id 172.2.12.1;
        }
        protocols {
            ospf {
                export BGP-to-OSPF;
                area 0.0.0.0 {
                    interface em2.0 {
                        interface-type p2p;
                    }
                }
            }
            ldp {
                interface em2.0;
            }
        }
    }
    B {
        instance-type vrf;
        interface em0.0;
        route-distinguisher 65102:65202;
        vrf-target target:65102:65202;
        routing-options {
            router-id 192.2.12.1;
        }
        protocols {
            ospf {
                export BGP-to-OSPF;
                area 0.0.0.0 {
                    interface em0.0 {
                        interface-type p2p;
                    }
                }
            }
            ldp {
                interface em0.0;
            }
        }
    }
}

[edit]
```