Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: **Методи та засоби оптимізації роботи в задачах побудови гетерогенних мереж різного призначення**

Виконав(ла): студент(ка) 6 курсу, групи САм-61
спеціальності 124 «Системний аналіз»
(шифр і назва спеціальності)

(підпис) Мурза Д.В.
(прізвище та ініціали)

Керівник (підпис) Марценко С.В.
(прізвище та ініціали)

Нормоконтроль (підпис) Мацюк О.В.
(прізвище та ініціали)

Завідувач кафедри (підпис) Боднарчук І.О.
(прізвище та ініціали)

Рецензент (підпис) Карпінський М.П.
(прізвище та ініціали)

Тернопіль
2020

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 124 «Системний аналіз»
(шифр і назва спеціальності)

студенту Мурзі Дмитру Васильовичу
(прізвище, ім'я, по батькові)

1. Тема роботи **Методи та засоби оптимізації роботи в задачах побудови гетерогенних мереж різного призначення**

Керівник роботи **Марценко Сергій Володимирович, к.т.н., доц.**
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «___» _____ 20___ року № _____

2. Термін подання студентом завершеної роботи _____

3. Вихідні дані до роботи технічне завдання на дослідження методів та засобів оптимізації роботи мереж

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 Аналіз предметної області; 1.1 Аналіз моделей побудови гетерогенних мереж; 1.2 Аналіз моделей безпеки гетерогенних мереж; 1.3 Постановка завдання оптимізації роботи в задачах побудови гетерогенних мереж різного призначення; 1.4 Висновки до першого розділу; 2 Розробка та впровадження методів та засобів оптимізації роботи в задачах побудови гетерогенних мереж різного призначення; 2.1 Оптимізація роботи мереж через віртуалізацію ресурсів; 2.2 Дослідження оптимізації роботи комутованих мереж…

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Мета, об'єкт, предмет дослідження; Завдання дослідження; Модель побудови гетерогенної локальної мережі; Модель безпеки гетерогенної мережі; Оптимізація комутованих мереж з VLAN; Оптимізація роботи з тунелюванням Geneve; Оптимізація магістральних MPLS мереж з інтеграцією SD-WAN; Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Мацюк О.В., доц. каф. КН		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст.викл. каф ОХ		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	21.09.20-27.09.20	*Виконано*
2.	Підбір наукових джерел щодо методів та засобів	28.09.20-04.10.20	*Виконано*
	оптимізації роботи мереж		
3.	Переклад та опрацювання наукових джерел щодо	05.10.20-11.10.20	*Виконано*
	методів та засобів оптимізації роботи мереж		
4.	Виконання дослідження щодо методів та засобів	12.10.20-18.10.20	*Виконано*
	оптимізації роботи мереж		
5.	Оформлення розділу «Аналіз предметної області»	19.10.20-25.10.20	*Виконано*
6.	Оформлення розділу «Розробка та впровадження	26.10.20-01.11.20	*Виконано*
	методів та засобів оптимізації роботи в задачах		
	побудови гетерогенних мереж різного призначення»		
7.	Оформлення розділу «Апробація прийнятих рішень»	02.11.20-08.11.20	*Виконано*
8.	Виконання завдання до підрозділу «Охорона праці»	09.11.20-15.11.20	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	16.11.20-22.11.20	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	23.11.20-29.11.20	*Виконано*
11.	Нормоконтроль	30.11.20-05.12.20	*Виконано*
12.	Перевірка на плагіат	07.12.2020	*Виконано*
13.	Попередній захист кваліфікаційної роботи	14.12.20	*Виконано*
14.	Захист кваліфікаційної роботи	21.12.2020	

Студент _____ Мурза Д.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Марценко С.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи та засоби оптимізації роботи в задачах побудови гетерогенних мереж різного призначення // Кваліфікаційна робота // Мурза Дмитро Васильович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно–інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група САм–61 // Тернопіль, 2020 // С. 74 , рис. – 16 , табл. – , кресл. – , додат. – 4 , бібліогр. – 50 .

Ключові слова: ОПТИМІЗАЦІЯ, ВІРТУАЛІЗАЦІЯ, ГЕТЕРОГЕННІ МЕРЕЖІ, МОДЕЛІ БЕЗПЕКИ, МОДЕЛІ МЕРЕЖ, ТЕХНОЛОГІЇ ОПТИМІЗАЦІЇ.

У роботі проведено дослідження методів та засобів оптимізації роботи в задачах побудови гетерогенних мереж різного призначення, що дало змогу на основі прийнятих рішень підвищити надійність, продуктивність та стійкість до мережевих атак.

В першому розділі кваліфікаційної роботи проведено аналіз моделей побудови гетерогенних мереж, що показало сильні та слабкі сторони мережевих дизайнів. На основі аналізу моделей безпеки визначено оптимальні методи для створення структури захисту мережевих ресурсів та користувачів. Здійснено постановку завдання оптимізації роботи гетерогенних мереж різного призначення.

Другий розділ кваліфікаційної роботи присвячений оптимізації мереж через віртуалізацію мережевих ресурсів. Це дало змогу пришвидшити розгортання мереж, впровадження нових сервісів, збільшити продуктивність та захищеність, що в свою чергу підвищило рівень задоволеності користувачів. Поділ мережі технологією VLAN дав змогу віртуалізувати користувацькі групи за їх призначенням, а не за місцем розташування і оптимізувати доступ до ресурсів необхідних цим групам. Досліджено

оптимізацію на основі протоколу Geneve, що є одним з самих сучасних рішень запропонований IETF у якості тунельного протоколу. На магістральних мережах одним з широковикористовуваних протоколів є MPLS, тому в роботі запропоновано оптимізацію цієї технології через гібридну систему з використанням рішень SD-WAN. Це уможливило вирішити питання статичності налаштувань MPLS і впровадити нові тенденції розвитку гетерогенних мереж. Досліджено переваги оптимізації з застосуванням протоколів HSRP, VRRP, GLBP для віртуалізації шлюзів за замовчуванням і балансування навантаження на маршрутизаторах.

В третьому розділі для апробації запропонованих рішень проведено моделювання оптимізації роботи мереж з використанням технології VLAN та протоколу HSRP, що дало змогу довести правильність пропозицій.

Метою дослідження є аналіз методів та засобів оптимізації в задачах побудови гетерогенних мереж різного призначення, що уможливить покращення продуктивності та захищеності мереж, спростить розгортання нових рішень та підвищень рівень задоволенсті користувачів. Досягнення поставленої мети передбачає виконання наступних завдань: здійснити аналіз моделей створення мережевих інфраструктур, моделей інформаційної безпеки; дослідити методи та засоби оптимізації роботи локальних та магістральних мереж; на основі проведеного аналізу внести пропозиції щодо оптимізації конкретних мережевих рішень.

Об’єкт дослідження – процес передавання, захисту та віртуалізації потоків інформації в мережах.

Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних.

ANNOTATION

Methods and means of work optimization in problems of multipurpose heterogeneous networks building // Diploma thesis Master degree // Murza Dmytro V. // Ternopil' Ivan Pul'uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science // Ternopil', 2020 // P. 74 , Tables – , Fig. – 16 , Diagrams – , Annexes. – 4 , References – 50.

The research has been carried out on the methods and means of work optimization in the tasks of building heterogeneous networks for different purposes, which allowed on the basis of decisions to increase the reliability, productivity and resistance to network attacks.

In the first section of the thesis, an analysis of models for building heterogeneous networks provided, which showed the strengths and weaknesses of network designs. Based on the analysis of security models, the best methods for creating a structure for the protection of network resources and users are identified. The problem of optimizing the operation of heterogeneous networks for various purposes is set.

The second section of the thesis is devoted to network optimization through virtualization of network resources. This has accelerated the deployment of networks, the introduction of new services, increased productivity and security, which in turn has increased user satisfaction. Separating the network with VLAN technology made it possible to virtualize user groups by their purpose rather than by location and to optimize access to the resources needed by these groups. The optimization based on the Geneve protocol, which is one of the most modern solutions proposed by the IETF as a tunnel protocol, is investigated. On backbone networks, one of the widely used protocols is MPLS, so the paper proposes the optimization of this technology through a hybrid system using SD-WAN solutions. This made it possible to resolve the issue of static MPLS settings and introduce

new trends in the development of heterogeneous networks. The advantages of optimization using HSRP, VRRP, GLBP protocols for default gateway virtualization and load balancing on routers are investigated.

In the third section, to test the proposed solutions, modeling of network optimization using VLAN technology and HSRP protocol was performed, which allowed to prove the correctness of the proposals.

The aim of the study is to analyze the methods and means of optimization in the tasks of building heterogeneous networks for different purposes, which will improve the performance and security of networks, simplify the deployment of new solutions and increase user satisfaction. Achieving this goal involves the following tasks: to analyze models of network infrastructures, information security models; to explore methods and means of optimizing the work of local and backbone networks; on the basis of the conducted analysis to make offers on optimization of concrete network decisions.

The object of research is the process of transmission, protection and virtualization of information flows in networks.

The subject of research - the theory of design of telecommunication networks, the theory of data transmission.

Key words: OPTIMIZATION, VIRTUALIZATION, HETEROGENEUS NETWORKS, SECURITY MODELS, NETWORK MODELS, OPTIMIZATION TECHNOLOGIES.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

WAN – Wide Area Network

SAS – Service and Application Security

QBS – QoS Based Security

QoS – Quality of Service

SD-WAN – Software Defined Wide Area Network

COTS – Commercial off the Self

HSRP – Hot Stanby Router Protocol

VRRP – Virtual Router Redundancy Protocol

GLBP – Gateway Load Balancing Protocol

ЗМІСТ

ВСТУП

Стрімкий розвиток новітніх технологій у великій мірі покладається на гетерогенні мережі різного призачення. Величезні об’єми даних, що передаються та накопичуються потребують нових підходів до побудови, захисту та експлуатації мереж.

Оптимізація мережі включає технології, інструменти та методи, які допомагають підтримувати, покращувати або максимізувати продуктивність у всіх мережевих доменах. Ці елементи використовуються для моніторингу, управління та оптимізації показників продуктивності, щоб допомогти забезпечити найвищий рівень обслуговування для користувачів у всій мережі.

Основними бізнес-цілями, що сприяють оптимізації, є такі технології, як SD-WAN, WiFi, великі дані, співпраця та багатохмарні хмари, мобільні та граничні обчислення.

Незважаючи на те, що мережеві технології продовжують розвиватися, вони все ще повинні працювати з існуючими системами. У недавньому опитуванні професіоналів NetOps було сказано, що перетворення мереж із застарілих архітектур на більш спритні (і менш затратні) є їх найбільшим пріоритетом на 2019 рік.

Однією з найбільших проблем, з якою стикається NetOps, є брак часу. Вони занадто зайняті вирішенням проблем у мережах, що як правило, складаються з різнорідних застарілих архітектур та безлічі інструментів моніторингу, щоб зосередитись на великих стратегічних проблемах. Оптимізація мережі пропонує варіант консолідованої архітектури, поліпшення загальної продуктивності мережі та єдиного наскрізного перегляду для NetOps.

З розвитком технологій все більше мережевих пристроїв, пристроїв IoT, додатків, хмарних мереж, віртуальних мереж, програмно визначених

мереж (SDN), з’являється ніж будь-коли раніше. І чим більше їх вводиться в мережу, тим більше шансів на порушення безпеки. В оптимізованій мережі NetOps має можливість допомогти мінімізувати вразливості для захисту конфіденційних даних від проникнення та атаки.

Актуальність теми. Оптимізація мережі важлива, оскільки наш взаємопов’язаний світ реального часу повністю залежить від надійної, безпечної, доступної цілодобової передачі даних. І з кожним роком до мереж ставлять все більше і більше вимог. Наш світ, керований даними, незаперечний. Кожен аспект нашого цифрового життя залежить від того, наскільки ефективно працює мережа, і саме тому оптимізація мережі є критично необхідною. Тому важливою та актуальною є задача оптимізації роботи гетерогенних мереж різного призначення як на етапі їх створенна, так і під час експлуатації.

Мета і завдання дослідження. Метою дослідження є аналіз методів та засобів оптимізації в задачах побудови гетерогенних мереж різного призначення, що уможливить покращення продуктивності та захищеності мереж, спростить розгортання нових рішень та підвищень рівень задоволеності користувачів. Досягнення поставленої мети передбачає виконання наступних завдань: здійснити аналіз моделей створення мережевих інфраструктур, моделей інформаційної безпеки; дослідити методи та засоби оптимізації роботи локальних та магістральних мереж; на основі проведеного аналізу внести пропозиції щодо оптимізації конкретних мережевих рішень.

Об’єкт дослідження – процес передавання, захисту та віртуалізації потоків інформації в мережах.

Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних.

Практичне значення одержаних результатів. Проаналізовано моделі дизайну мережевих архітектур гетерогенної структури, що дало змогу

визначити сучасні підходи в побудові та роботі мереж різного призначення. На основі проведеного аналізу стало можливим розробити вимоги до методів та засобів оптимізації роботи мереж з різнотипним обладнанням та різнорідними наборами даних. Запропоновано визначення характеристик оптимізації, що дасть змогу пропонувати покращені мережеві архітектури та концепції роботи гетерогенних мереж. Розглянуті моделі безпеки можуть бути використані для підвищення доступності та стійкості, підвищення надійності і захищеності ресурсів, даних та користувачів. Виконано постановку завдання оптимізації в задачах побудови мереж різного призначення. Запропоновано використання технології VLAN, як базового методу поділу на віртуалізовані широкомовні домени та покращення продуктивності через зменшення об’ємів трафіку і розділення рівнів доступу. Оскільки дана технологія дозволяє обмін між різними VLAN через маршрутизатор, то виникає можливість додавати політики управління та безпеки між різними підмережами комутованої мережі. Поділ мережі на VLAN в поєднанні з іншими протоколами дає змогу суттєво підвищити продуктивність та надає можливість управління потоками даних на 2-гому рівні. Наступним кроком оптимізації є використання протоколу Geneve прототипування якого наведено в даній роботі, а технічна реалізація можлива при наявності комерційного обладнання від виробників. Аналіз магістральної технології MPLS показав її обмеженість до вимог сучасного світу і як варіант вирішення цієї задачі запропоновано використання технології SD-WAN, що дає змогу додати віртуалізацію мережевих функцій та вирішити недоліки початкового протоколу MPLS. Запропоновано використання протоколів віртуалізації маршрутизаторів, що дасть змогу підвищити доступність шлюзів за замовчуванням і збільшити стійкість мережі до атак типу заборона сервісу. Проведено моделювання оптимізації роботи гетерогенної мережі через створення віртуальних мереж VLAN та поділ користувачів на віртуальні групи, оптимізовано використання ресурсів за допомогою

налаштувань протоколу Spanning Tree. Для гарантування доступності виходу назовні мережі проведено моделювання роботи протоколу HSRP з віртуалізацією IP адреси шлюзу за замовчуванням, що дало можливість прозоро для користувачів збільшити надійність.

Наукова новизна розробки: проведено прототипування мережевого рішення для оптимізації мережі гетерогенної структури на основі тунельного протоколу Geneve, розробкою якого займається група IETF, запропоновано створення гібридних магістральних мереж у поєднанні існуючих MPLS та SD-WAN рішень, що дасть змогу розширити можливості існуючих мереж та використовувати їх при побудові нових.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз моделей побудови гетерогенних мереж

Деякі типи гетерогенних мереж можуть бути розгорнуті у запланованому порядку, наприклад, розгортання мікровузлів у макромережі. Однак за інших обставин мережа може бути незапланованою. Прикладом цього є розгортання домашніх вузлів, які можуть керуватися споживачами. В обох випадках, і особливо там, де мережі не плануються, бажано, щоб мережа могла вживати заходів для оптимізації. Наприклад, перешкодами потрібно керувати, потенційно за допомогою регулювання рівнів потужності передачі вузлів. Крім того, коли вузли розгортаються незапланованим чином, мережа повинна отримати інформацію про топологію мережі, і зокрема, які вузли розташовані в безпосередній близькості один від одного, щоб правильно приймати рішення щодо мобільності. Таким чином, мережа і певною мірою стандартизація потребують засобів, що дозволяють мережі самооптимізуватися [1-50]. Подальший виклад матеріалу аналізує основні характеристики, переваги та недоліки моделей гетерогенних мереж в контексті їх застосування.

Неоднорідні мережі (гетерогенні, мультисервісні) – забезпечують більше одного окремого додатка чи послуги. Це передбачає не тільки декілька типів трафіку в мережі, але й здатність однієї мережі підтримувати всі програми без компрометації QoS. Існує два класи додатків: пропускна здатність та стійкий до затримки еластичний трафік (наприклад, моніторинг параметрів погоди при низьких частотах дискретизації) і пропускна здатність та чутливий до затримок нееластичний (в реальному часі) трафік (наприклад, шум або моніторинг трафіку), які додатково дискримінуються програмами, пов’язаними з даними (наприклад, відео з високою та низькою роздільною здатністю) з різними вимогами до якості обслуговування. Отже, необхідний

контрольований, оптимальний підхід для обслуговування різних мережевих трафіків, кожен із яких має власні потреби в QoS. Надати гарантії якості обслуговування в бездротових мережах непросто, оскільки сегменти часто становлять “прогалини” в гарантії ресурсів через обмеження розподілу ресурсів та можливостей управління у спільних бездротових носіях.

QoS у хмарних обчисленнях – ще одна велика область досліджень, яка потребуватиме більше уваги, оскільки дані та інструменти стануть доступними на хмарах. Зараз розробляються алгоритми динамічного планування та розподілу ресурсів, засновані на оптимізації рою частинок, але для додатків з великою потужністю та в міру зростання IoT це може стати вузьким місцем.

Однією з класичних мережевих моделей побудови великих гетерогенних мереж є трирівнева модель дизайну. На малюнку 1.1 показно приклад організації зв’язків в такій моделі.

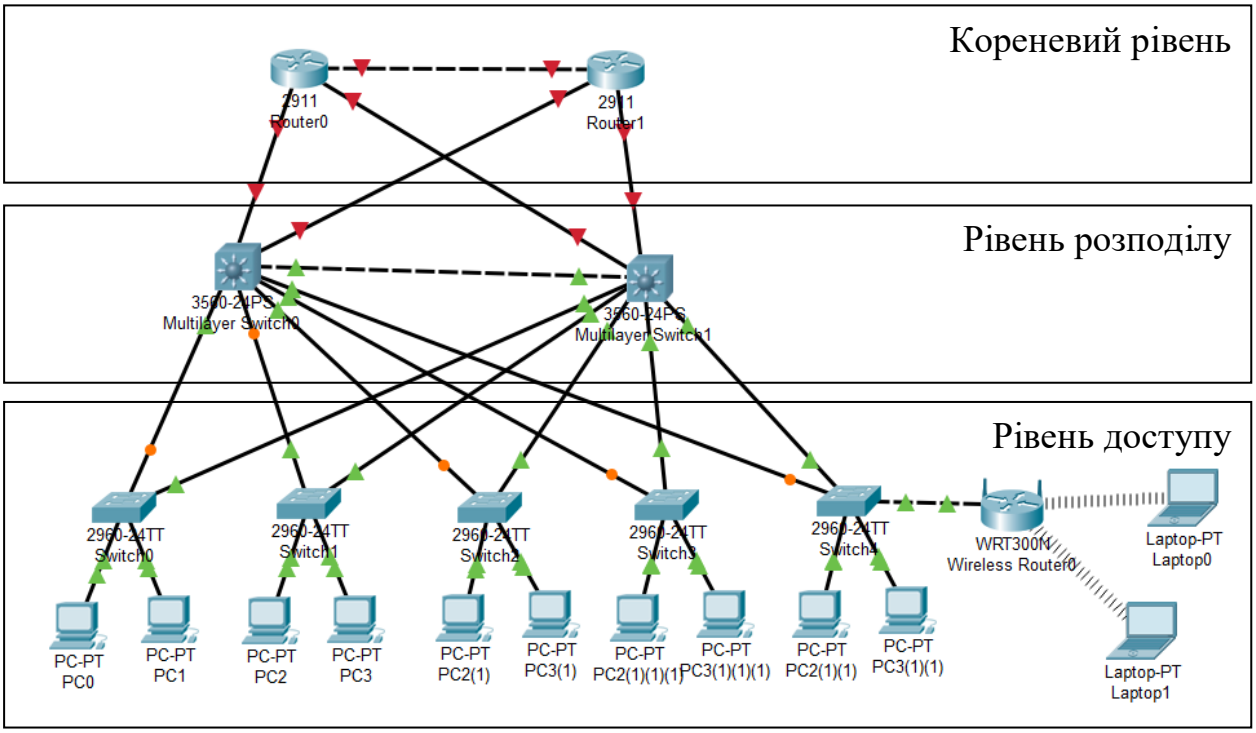

Рисунок 1.1 – Модель мережі на основі трирівневого дизайну

За такого варіанту організації мережевих ресурсів спостерігається взаємопов’язаність апаратно-програмних компонентів, що дає змогу гучко організовувати передавання даних між різними додатками програм та сервісами для забезпечення функціонування гетерогенності. За використання такого підходу спостерігається висока масштабованість за рахунок модульності компонентів. Розширення мережі відбувається без змін початкового дизайну. Вузли додаються на рівні доступу і при необхідності розширення використовується можливість збільшення рівня розподілу.

До основних недоліків такого дизайну можна віднести його статичність у відношенні до потреб організаційної структури. Якщо розглядати як приклад корпоративну мережу, то побудова мережі за цими принципами буде достатньо ефективною. У випадку мережі для сервіс провайдера – недоліком стане складність керування вимогами різних замовників послуг.

Вимогами нових мереж є:

– прозорість (методів сигналінгу, незалежність від протоколів);
– забезпечення функцій трафік інжиниринг;
– контроль доступу між вузлами з забезпечення якості послуг;
– гнучкість обслуговування.

Як частинний випадок трирівневого дизайну розглядають його спрощену версію у вигляді дворівневого без використання кореневого рівня. Такий підхід дає змогу зберегти кошти на купівлі обладнання використовуючи комутатори другого та третього рівнів для об’єднання функцій рівня розподілу та кореневого в один.

Для побудови магістральних мереж використовують технологію Multiprotocol Label Switching (MPLS). Комутація багатопротокольних міток (MPLS) – це механізм передачі даних, що застосовує “мітки” до пакетів даних. Існування цієї мітки оптимізує рішення щодо переадресації пакетів і

дозволяє співіснувати в мережі MPLS багато різних типів носіїв, усуваючи залежність від будь-якого конкретного протоколу передачі даних.

Послуги MPLS для кінцевого користувача рідко вимагають будь-яких додаткових можливостей, крім основних функцій маршрутизації. Всі теги MPLS та сегментація трафіку виконуються постачальником прозоро для кінцевого користувача. Через це практично будь-який маршрутизатор може бути підходящим для клієнта.

Річ у тім, що MPLS це техніка, а не послуга – тому вона може доставляти що завгодно, від IP VPN до метро Ethernet. Це дорого, тому з появою SD-WAN підприємства намагаються зрозуміти, як оптимізувати його використання порівняно з менш дорогими зв'язками, такими як Інтернет.

Ви коли-небудь замовляли щось через Інтернет у віддаленого продавця, а потім відстежували упаковку, оскільки вона робить дивні та на перший погляд нелогічні зупинки по всій країні.

Це схоже на спосіб роботи IP-маршрутизації в Інтернеті. Коли маршрутизатор Інтернету отримує IP-пакет, цей пакет не несе ніякої інформації, крім IP-адреси призначення. Немає вказівок про те, як цей пакет повинен дістатись до місця призначення або як слід поводитися з ним по дорозі.

Кожен маршрутизатор повинен приймати незалежне рішення щодо переадресації для кожного пакета, виходячи виключно із заголовка мережевого рівня пакета. Таким чином, кожного разу, коли пакет надходить на маршрутизатор, маршрутизатор повинен вирішити, куди направити пакет далі. Роутер робить це, посилаючись на складні таблиці маршрутизації.

Процес повторюється на кожному стрибку по маршруту, поки пакет врешті-решт не досягне місця призначення. Усі ці стрибки та всі ці індивідуальні рішення про маршрутизацію призводять до низької продуктивності програм, що чутливі до часу, таких як відеоконференції або передача голосу через IP (VoIP).

Багатопротокольна комутація міток (MPLS) вирішує цю проблему шляхом встановлення заздалегідь визначених високоефективних маршрутів.

З MPLS, коли пакет вперше потрапляє в мережу, він присвоюється певному класу еквівалентності переадресації (Forwarding equivalence class (FEC)), що позначається додаванням короткої послідовності бітів (мітки) до пакету.

Кожен маршрутизатор у мережі має таблицю, яка вказує, як обробляти пакети певного типу FEC, тому, як тільки пакет входить в мережу, маршрутизаторам не потрібно виконувати аналіз заголовків. Натомість наступні маршрутизатори використовують ярлик як індекс таблиці, яка надає їм новий FEC для цього пакета.

Це дає мережі MPLS можливість послідовно обробляти пакети з певними характеристиками (наприклад, що надходять з певних портів або переносять трафік певних типів програм). Пакети, що переносять трафік в режимі реального часу, такі як голос чи відео, можна легко зіставити з маршрутами з низькою затримкою по мережі – те, що є складним завданням при звичайній маршрутизації.

Краса MPLS полягає в тому, що він не пов’язаний з жодною базовою технологією. Він був розроблений ще за часів ATM та Frame Relay як метод накладання, спрощений та покращений показник – це частина “мультипротоколу”.

ATM та Frame Relay – це віддалені спогади, але MPLS живе в магістралях несучих та в корпоративних мережах. Найпоширенішими випадками використання є філії, мережі кампусів, служби метро Ethernet та підприємства, які потребують якості обслуговування (QoS) для додатків у реальному часі.

Ключовим архітектурним моментом у всьому цьому є те, що ярлики надають спосіб приєднати додаткову інформацію до кожного пакету – інформацію, яка перевищує те, що раніше мали маршрутизатори.

Існує велика плутанина щодо того, чи є MPLS службою рівня 2 або рівня 3. Але MPLS не вписується акуратно в семирівневу ієрархію OSI і іноді класифікується як рівень 2.5. Насправді однією з ключових переваг MPLS є те, що він відокремлює механізми переадресації від базової служби передачі даних. Іншими словами, MPLS можна використовувати для створення таблиць пересилання для будь-якого базового протоколу.

Зокрема, маршрутизатори MPLS встановлюють шлях із комутацією міток (Label Switched Path (LSP)), заздалегідь визначений шлях для маршрутизації трафіку в мережі MPLS, на основі критеріїв FEC. Лише після встановлення LSP може відбуватися переадресація MPLS. LSP є односпрямованими, що означає, що зворотний трафік надсилається через інший LSP.

Коли кінцевий користувач надсилає трафік у мережу MPLS, мітка MPLS додається вхідним маршрутизатором MPLS, який знаходиться на межі мережі. Мітка MPLS складається з чотирьох підрозділів:

Мітка: Мітка містить всю інформацію про маршрутизатори MPLS, щоб визначити, куди слід пересилати пакет.

Експериментальний: експериментальні біти використовуються для якості обслуговування (QoS), для встановлення пріоритету, який повинен мати позначений пакет.

Bottom-of-Stack: Bottom-of-Stack повідомляє маршрутизатору MPLS, якщо це останній етап подорожі, і немає більше ярликів, якими слід займатися. Зазвичай це означає, що маршрутизатор є вихідним маршрутизатором.

Час життя: визначає, скільки стрибків може зробити пакет, перш ніж його відкинути.

Перевагами MPLS є масштабованість, продуктивність, краще використання смуги пропускання, зменшення перевантаженості мережі та кращий досвід роботи кінцевих користувачів.

Сам MPLS не забезпечує шифрування, але він є віртуальною приватною мережею і як такий відокремлений від загальнодоступного Інтернету. Тому MPLS вважається безпечним видом транспорту. І він не вразливий до атак відмови в обслуговуванні, які можуть вплинути на мережі на основі чистого IP.

Негативним моментом є те, що MPLS – це послуга, яку потрібно придбати у провайдера і є набагато дорожчою, ніж відправка трафіку через загальнодоступний Інтернет.

По мірі виходу компаній на нові ринки їм може бути важко знайти постачальника послуг MPLS, який може забезпечити глобальне покриття. Як правило, постачальники послуг об’єднують глобальне покриття через партнерські відносини з іншими постачальниками послуг, що може коштувати дорого.

MPLS була розроблена в епоху, коли філії відправляли трафік назад до головного штабу або центру обробки даних, а не для сучасного світу, де працівники філій хочуть прямого доступу до хмари.

Провокаційне питання життєздатності MPLS було підняте ще в 2013 році і відповідь передбачає, що MPLS і надалі залишатиметься основною частиною ландшафту WAN, але більшість підприємств буде повільно переходити до гібридного середовища, що складається як з мереж MPLS, так і з публічного Інтернету.

MPLS продовжуватиме виконувати роль, що поєднує конкретні пункти “точка-точка”, такі як великі регіональні офіси, роздрібні магазини із системами торгових точок, регіональні виробничі потужності та численні центри обробки даних. І це потрібно для додатків у режимі реального часу.

Але архітекторам корпоративної глобальної мережі потрібно зробити розрахунок ризику/винагороди між першокласною, але дорогою продуктивністю MPLS порівняно з більш дешевою, але менш надійною

роботою Інтернету. Що підводить нас до захоплюючої нової технології під назвою SD-WAN.

1.2 Аналіз моделей безпеки для гетерогенних мереж

Майбутні системи зв’язку повинні забезпечувати повсюдне підключення, де користувачі завжди мають зв’язок будь коли та де завгодно. Потреба в безперервному з’єднання відповідає розробці та впровадженню ряду бездротових технологій, включаючи 3G / HSPDA, WLAN, із 802.11n

Однак широке розгортання бездротових мереж матиме значний вплив на розвиток Інтернет. Глобальна мережа буде виконувати функцію надшвидкої магістралі і ядра, в той час як інші будуть виконувати функції переферійних мереж.

Y-Comm – це архітектура для різнорідних мереж. Архітектура складається з двох каркасів як подано на малюнку 1.2.

Периферійний фреймворк займається проблемами периферійних мереж, тоді як основний фреймворк обробляє проблеми в базовій мережі

Рисунок 1.2 – Модель безпеки гетерогенної мережі

У цій архітектурі периферійний фреймворк та кореневий фреймворк щоб представити майбутнє телекомунікаційне середовище, яке підтримує неоднорідні пристрої, мережеві технології, мережеві оператори та послуги постачальників послуг. Однією з ключових цілей архітектури Y-Comm є більш комплексне вирішення питань безпеки порівняно з іншими парадигмами мереж, оскільки Y-Comm тісно інтегрує безпеку з архітектурою зв'язку.

Y-Comm використовує багаторівневу модель безпеки, яка повинна застосовуватися як до периферійної, так і до основної системи одночасно для забезпечення повної безпеки. Рівні безпеки повинні працювати разом в обох системах з метою повної інтеграції з новою архітектурою. Важливим моментом є те, що потрібно підтримувати неоднорідні мережі з відкритими архітектурами тому безпека повинна захищати не тільки дані, але й сутності.

Найвищий рівень безпеки знаходиться на сьомому рівні і називається Безпека сервісів та додатків (Service and application security (SAS)). У периферійній структурі SAS визначає функції AAAC на кінцевому пристрої та використовується для автентифікації користувачів та програм. SAS в Core Framework надає функції AAAC для послуг на платформі послуг у базовій мережі. Наступний рівень безпеки називається QoS-Based Security або QBS і стосується проблем якості обслуговування та мінливих вимог до якості обслуговування мобільного середовища, коли користувачі пересуваються. Крім того, для виконання своїх домовленостей про рівень обслуговування сервери можуть вибрати реплікацію послуг ближче до поточної позиції мобільного. Тому необхідно переконатись, що кінцеві точки та периферійні мережі не перевантажені. Рівень QBS також намагається блокувати атаки, пов'язані з QoS, такі як атаки Denial-of-Service (DoS) на мережі та сервери. Наступний рівень безпеки знаходиться на п'ятому рівні і називається Network Transport Security або NTS. У периферійній структурі NTS стосується доступу до і з кінцевих пристроїв та видимості цих пристроїв і

послуг в Інтернеті. У Core Framework NTS використовується для встановлення безпечних з'єднань через базову мережу. Отже, NTS в Core Framework передбачає встановлення захищених тунелів між основними кінцевими точками за допомогою механізмів, таких як IPsec, щоб забезпечити безпечне переміщення даних через основну мережу.

Нарешті, четвертий і останній рівень безпеки визначається на рівні чотири, але також може охоплювати рівні три і два. Це називається Network Architecture Security або NAS. У периферійній структурі він намагається вирішити проблеми безпеки, пов'язані з використанням певних мережевих технологій, та загрози безпеці, які виникають при використанні даної бездротової технології. Отже, коли мобільний пристрій бажає використовувати будь-яку дану мережу, викликається NAS, щоб гарантувати, що користувач має на це дозвіл. NAS також гарантує, що середовище локальної мережі є максимально безпечним. У Core Framework NAS використовується для забезпечення доступу до програмованої інфраструктури. NAS у цьому контексті визначає, які комутатори, маршрутизатори чи ресурси базової станції можуть використовуватися системою управління мережею. Повна архітектура Y-Comm, включаючи її рівні безпеки, показана на малюнку 1.3. Оскільки система безпеки інтегрована з Основною та периферійною структурами в рамках Y-Comm, ці функції безпеки, що є частиною архітектури зв'язку, можуть бути використані з набагато більшим ефектом, ніж попередні методи. Описані вище рівні безпеки стосуються управління безпечним транспортуванням даних та автентифікацією мобільних пристроїв та послуг. Однак, оскільки Y-Comm є відкритою архітектурою, необхідно також захищати такі об'єкти, як користувачі, сервери та мережева інфраструктура. Таким чином, Y-Comm може запропонувати три різні моделі мережевої безпеки.

Периферійний набір		Кореневий набір
Прикладні програми	SAS	Сервіси
Рівень QoS	QBS	QoS мережевого рівня
Кінцевий транспорт	NTS	Кореневий транспорт
Управління політиками	NAS	Управління мережами
Обслуговуваня		Конфігурування
Користувацьке обладнання		Обладнання провайдера
Апаратна платформа		Апаратна платформа

Рисунок 1.3 – Завершена Y-архітектура моделі безпеки мережі

Перша модель називається моделлю безпеки підключення, друга модель безпеки називається моделлю безпеки на основі кільця, а третя модель безпеки називається моделлю безпеки вертикальної передачі.

Модель безпеки підключення передбачає різні рівні захисту, які працюють разом, щоб встановити зв’язок між мобільним вузлом (MN) та службою, розміщеною на іншій стороні. Основна ідея полягає в тому, що кінцеві користувачі повинні використовувати рівні безпеки для підключення один до одного, і це дозволяє системі налаштовувати, підтримувати та контролювати з’єднання.

Можна показати, як використовується система безпеки, розглядаючи взаємодію, пов’язану з налаштуванням з’єднання. Зобразимо це у вигляді серії кроків:

– Крок 1: Сервер запущено. Модуль NAS на сервері розмовляє з модулем NAS у локальній мережі, щоб отримати доступ до своєї бездротової інфраструктури.

– Крок 2: Модуль безпеки QBS на сервері інформує модуль QBS в базовій мережі про свою Угоду про рівень обслуговування, яка містить QoS, пов’язану з підключенням до цієї послуги.

– Крок 3: запущено мобільний вузол. Модуль NAS у мобільному вузлі контактує з модулем NAS у периферійних мережах, щоб отримати доступ до бездротової інфраструктури.

– Крок 4: Коли мобільний вузол хоче скористатися послугою, модуль QBS у мобільному вузлі зв’язується з модулем QBS в базовій мережі та просить встановити з’єднання із сервером із заданою якістю обслуговування. Модуль QBS повертає дві основні кінцеві точки, які потрібно використовувати для встановлення з’єднання.

– Крок 5: Модуль NTS на мобільному вузлі зв’язується з модулем NTS в базовій мережі і повідомляє, що він хоче з’єднання з сервером, використовуючи основні кінцеві точки, QoS та параметри безпеки.

– Крок 6: Модуль NTS в базовій мережі зв’язується з модулем NTS на сервері, щоб сигналізувати про вхідний дзвінок. На цьому етапі сервер також може перевірити деталі безпеки клієнта, а також безпеку з’єднання.

– Крок 7: Якщо сервер приймає запит, то модуль NTS у базовій мережі приєднує дві основні кінцеві точки.

– Крок 8: Потім він сигналізує як клієнту, так і серверу, що встановлено підключення.

Безпека на основі кільця – це розширення Off-by-Default, ідея якої була представлена Баллані. Концепція Ring-Based не дозволяє серверам отримувати прямий доступ через глобальну мережу, таку як Інтернет, без початку взаємодії з мережевою інфраструктурою. Це робиться за допомогою концепції сфери дії, коли сервер діє лише в межах заданої області дії. Існує 3 сфери дії:

– Локальний: локальний сервер може використовувати лише процеси на одній машині. Це забезпечується рівнем SAS на локальній машині.

– LAN: Доступ до цих серверів дозволяється лише процесам в одній мережі. Це забезпечується рівнем NAS периферійної мережі. Ці сервери повинні зареєструватися в локальному DNS і стають доступними для мобільних пристроїв, коли користувачам дозволено використовувати периферійну мережу.

– Глобальний: Глобальні сервери доступні з будь-якої точки через базову мережу за допомогою Глобальних служб. Отже, це стосується основних рівнів NTS та QBS. Крім того, сервери повинні зареєструватися в глобальному DNS, яким також керує основна мережа, щоб дозволити доступ до глобальної мережі.

Механізми вертикальної передачі обслуговування передбачають отримання та вивільнення мережевих ресурсів у міру переміщення мобільних вузлів. У поточних стільникових мережах передача контролюється мережею, до якої приєднаний мобільний телефон. Однак такі механізми передачі, як Mobile IPv6 (MIPv6) та Fast Mobile IPv6 (FMIPv6), використовують хендовер на основі клієнта. Y-Comm також використовує передачу на основі клієнта для підтримки різнорідних мереж. За таких обставин необхідно переконатись, що мобільні вузли не намагаються зловживати мережевими ресурсами. Це мета моделі вертикальної передачі безпеки. Крім серверів автентифікації, авторизації, аудиту та вартості (AAAC), нові об’єкти беруть участь у Моделі безпеки вертикальної передачі (VHSM); брокери QoS (QoSB), які контролюють продуктивність мережі та проблеми, пов'язані з QoS; вони досягають цього за допомогою механізмів контролю за допуском та аудиту.

1.3 Постановка завдання оптимізації роботи в задачах побудови гетерогенних мереж різного призначення

Наведений вище огляд моделей дав змогу визначити сильні та слабкі сторони мережевих дизайнів, що застосовуються при побудові гетерогенних мереж. Методи та засоби оптимізації сучасних мереж різного призначення покликані вирішити ряд питань пов'язаних з масштабованістю, швидкодією, забезпеченням необхідних пропускних здатностей, захищеністю мережевих ресурсів, що в свою чергу підвищує рівень задоволеності користувачів цих послуг. Сучасні мережеві архітектури в великій мірі враховують статичні моменти цих показників, проте мають певні недоліки в динамічних середовищах де адаптація до нових умов повинна проходити у відповідності до змін.

Запропоновані методи та засоби оптимізації роботи мереж повинні включати:

– можливість віртуалізації мережевих ресурсів для гнучкого управління;

– розгортання ієрархічних надбудов для управління віртуалізованими мережами;

– засоби організації переходу до новітніх підходів управління мережами.

Віртуалізація мережевих ресурсів дає змогу утворювати набори фізичних пристроїв, що працюють як один елемент, що в свою чергу підвищує продуктивність роботи та збільшує протидію різного роду атакам на мережеві пристрої. Використання протоколів віртуалізації надає змогу використовувати стандартизовані механізми оптимізації роботи мережевих компонентів та швидке розгортання відповідних технічних рішень.

Іншим підходом до оптимізації є використання концепції програмно-конфігурованих мереж (Software Defined Networks). При цьому, вся мережа

віртуалізується і керується з однієї точки, що виконує роль контролера. Такий підхід суттєво спрощує реплікацію однотипних налаштувань пристроїв, створення карти шляхів та управління потоками даних. За допомогою програмних застосунків існує можливість динамічно керувати інформаційними потоками з врахуванням змін у стані мережевих компонентів та оперативно реагувати на завантаженість чи збої в роботі. Використання контролера управління мережею дає змогу здешевити мережеве обладнання, оскільки набір функцій суттєво зменшується і переноситься на інший пристрій. Комутатори та маршрутизатори виконують команди контролера і їх функція зводиться до передавання з порту на порт.

Надбудова, що має назву віртуалізації мережевих функцій (Network Function Virtualization) це мережева архітектура, що передбачає віртуалізацію цілих класів процесів мережевих вузлів, що може бути об’єднана в ланцюг для забезпечення певного сервісу.

Оптимізація роботи мережі також можлива через відхід від принципу передавання від вузла до вузла і перехід до інформаційно центрованих мереж (Information Centric Networks). Цей новий підхід дає змогу зосередитись на передаванні інформації як цінності і оптимізовувати мережеві ресурси у відношенні до запитів користувачів.

Розглянуті методи та засоби оптимізації роботи мереж дають змогу будувати гнучкі та надійні мережеві рішення, що покликані максимально задовольняти потреби користувачів.

1.4 Висновки до першого розділу

Перший розділ кваліфікаційної роботи присвячений аналізу моделей дизайну мережевих архітектур гетерогенної структури, що дало змогу визначити сучасні підходи в побудові та роботі мереж різного призначення. На основі проведеного аналізу стало можливим розробити вимоги до методів

та засобів оптимізації роботи мереж з різнотипним обладнанням та різнорідними наборами даних. В подальшому викладі матеріалу пропонується визначення характеристик оптимізації, що дасть змогу пропонувати покращені мережеві архітектури та концепції роботи гетерогенних мереж. Розглянуті моделі безпеки можуть бути використані для підвищення доступності та стійкості, підвищення надійності і захищеності ресурсів, даних та користувачів. Виконано постановку завдання оптимізації в задачах побудови мереж різного призначення.

2 РОЗРОБКА ТА ВПРОВАДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ОПТИМІЗАЦІЇ РОБОТИ В ЗАДАЧАХ ПОБУДОВИ ГЕТЕРОГЕННИХ МЕРЕЖ РІЗНОГО ПРИЗНАЧЕННЯ

2.1 Оптимізація роботи мереж через віртуалізацію ресурсів

Мережева віртуалізація (Network Virtualization (NV)) відноситься до абстрагування мережевих ресурсів, які традиційно передавались апаратно до програмного забезпечення. NV може об’єднати кілька фізичних мереж в одну віртуальну мережу, що базується на програмному забезпеченні, або може розділити одну фізичну мережу на окремі незалежні віртуальні мережі.

Програмне забезпечення для віртуалізації мережі дозволяє адміністраторам мережі переміщати віртуальні машини між різними доменами без переналаштування мережі. Програмне забезпечення створює мережеве накладання, яке може запускати окремі шари віртуальної мережі поверх тієї самої фізичної мережевої інфраструктури.

Мережева віртуалізація переписує правила доставки послуг, від програмно визначеного центру обробки даних (Software Defined Data Center SDDC), до хмари чи до граничного вузла. Цей підхід переміщує мережі від статичних, негнучких та неефективних до динамічних, рухливих та оптимізованих. Сучасні мережі повинні йти в ногу з вимогами до розміщених у хмарі розподілених додатків та зростаючими загрозами кіберзлочинців, забезпечуючи при цьому швидкість та спритність, необхідні для швидшого виходу на ринок програм. За допомогою віртуалізації мережі можна забути про витрачання днів чи тижнів на забезпечення інфраструктури для підтримки нового додатка. Програми можна розгорнути або оновити за лічені хвилини для збереження часу.

Мережева віртуалізація відокремлює мережеві послуги від базового обладнання та дозволяє здійснювати віртуальне забезпечення всієї мережі.

Це дає змогу програмно створювати, забезпечувати та керувати мережами в усьому програмному забезпеченні, при цьому продовжуючи використовувати базову фізичну мережу як нижній шар для переадресації пакетів. Фізичні мережеві ресурси, такі як комутація, маршрутизація, брандмауер, балансування навантаження, віртуальні приватні мережі (VPN) та багато іншого, об’єднуються та постачаються в програмному забезпеченні і вимагають переадресації пакетів IP-протоколу з базової фізичної мережі.

Мережі та служби безпеки в програмному забезпеченні розподіляються на віртуальний рівень (гіпервізори, у центрі обробки даних) і “приєднуються” до окремих робочих навантажень, таких як віртуальні машини або контейнери, відповідно до мережевих та безпекових політик, визначених для кожного підключеного застосування. Коли робоче навантаження переміщується на інший хост, мережеві служби та політики безпеки переміщуються разом із ним. І коли створюються нові робочі навантаження для масштабування програми, необхідні політики динамічно застосовуються до цих нових робочих навантажень, забезпечуючи більшу узгодженість політики та спритність мережі.

Мережева віртуалізація допомагає організаціям досягти значного прогресу в швидкості, маневреності та безпеці, автоматизуючи та спрощуючи багато процесів, що входять до роботи мереж центрів обробки даних та управління мережею чи безпекою в хмарі. Ось деякі ключові переваги віртуалізації мережі:

– скорочення часу побудови мережі з тижнів до хвилин;

– досягнення більшої операційної ефективності за допомогою автоматизації ручних процесів;

– розміщення та перерозподіл навантаження незалежно від фізичної топології;

– покращення мережевої безпеки в центрі обробки даних.

Одним із прикладів віртуалізації мережі є віртуальна локальна мережа (Virtual Local Area Network (VLAN)). VLAN - це підсекція локальної мережі (LAN), створена за допомогою програмного забезпечення, що об’єднує мережеві пристрої в одну групу, незалежно від фізичного місцезнаходження. VLAN можуть покращити швидкість та продуктивність зайнятих мереж та спростити зміни або доповнення до мережі.

Інший приклад – накладення мережі. Існують різні технології накладання. Одна стандартна в галузі технологія називається віртуальною розширюваною локальною мережею (Virtual Extensible LAN (VXLAN)). VXLAN забезпечує структуру для накладання віртуалізованих мереж рівня 2 на мережі рівня 3, визначаючи як механізм інкапсуляції, так і площину управління. Інша – загальна інкапсуляція мережевої віртуалізації (GENEVE), яка приймає ті самі поняття, але робить їх більш розширюваними завдяки гнучкості до декількох механізмів площини управління.

2.2 Дослідження оптимізації роботи комутованих мереж через використання технології VLAN

Технічно VLAN (віртуальна локальна мережа) може логічно розділити та виділити одну або кілька фізичних локальних мереж на кілька широкомовних доменів. Кожен широкомовний домен розглядається як одна VLAN. Як правило, лише пристрої з одним і тим же VLAN можуть взаємодіяти між собою.

До VLAN існував єдиний широкомовний домен через зазначену мережу, який називається локальною мережею. Під час обміну даними між двома хостами ініціатор відправляв ARP запит бродкастом у мережу. Цей запит потрапляв до всіх хостів та комутаторів в даній LAN спричинюючи непотрібну обробку даних і зачіпаючи велику кількість пристроїв.

Інколи виникала ситуація, що спричиняла бродкаст шторм, який зачіпав процесори та пам’ять пристроїв, генерував великий об’єм трафіку, який призводив до падіння продуктивності мережі або й взагалі зупинки роботи.

Настроюючи VLAN, мережа може бути сегментована на різні домени широкомовного мовлення (VLAN). Як і наведений вище випадок, широкомовний кадр буде обмежений для надсилання до порту в тій самій VLAN без відправки до портів в іншій VLAN. Таким чином, мережеві ресурси та пропускна здатність будуть значно заощаджені, щоб поліпшити гнучкість та продуктивність мережі.

На малюнку 2.1 показано будову VLAN кадру. За рахунок додавання мітки VLAN даний кадр буде зрозумілий тільки комутаторам, що підтримують технологію VLAN і повинен зніматись при виході з порту до хоста.

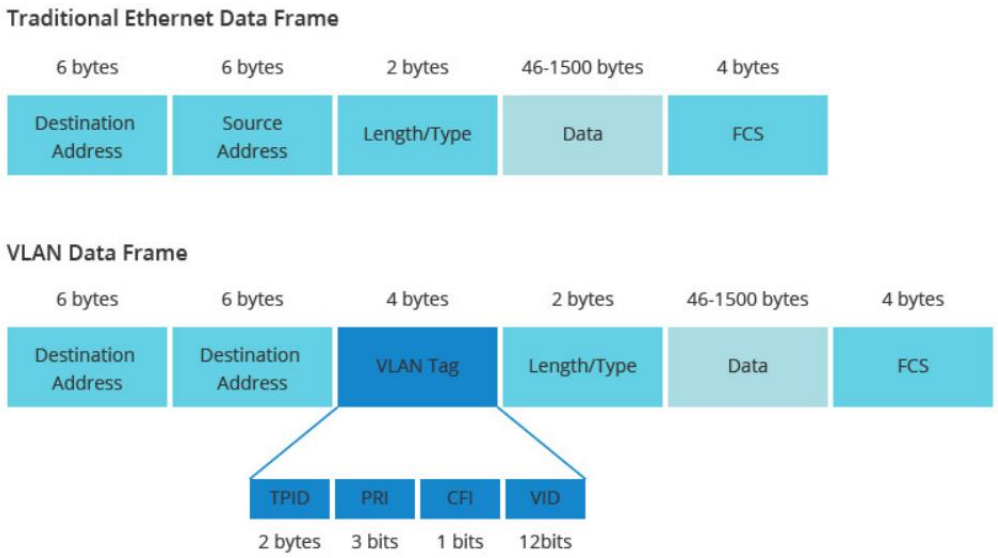

Рисунок 2.1 – Будова VLAN кадру

Тег VLAN: Це свого роду ідентифікатор VLAN, який інкапсульований у широкомовний кадр. Як тільки пакет даних увійде в порт комутатора у VLAN, тег VLAN буде інкапсульований. Однак, коли кадр із тегом VLAN

виходить з іншого порту, тег буде видалено. Зазвичай комутатор ідентифікує пакети з різних VLAN відповідно до інформації, що міститься в тегах VLAN. Протокол IEEE 802.1Q додає 4-байтовий тег VLAN між адресою джерела та полями довжина/тип кадру Ethernet.

Внутрішньо-VLAN зв’язок відноситься до спілкування користувачів у тому ж сегменті мережі та VLAN. Як правило, цей тип VLAN застосовується у двох сценаріях: внутрішньо-VLAN зв’язок через один і той же пристрій та внутрішньо-VLAN зв’язок через кілька пристроїв. Незалежно від типу, весь процес передачі в основному проходить наступні два етапи:

1. Запит ARP, надісланий від хост-джерела: Перед відправкою, хост-джерело порівняє свою IP-адресу з позначенням. Якщо хост-джерело виявить, що вони перебувають в одному сегменті мережі, він отримає MAC-адресу хоста призначення та заповнить отриману MAC-адресу поля MAC-адреси кадру. Однак, якщо хост-джерело виявляє, що вони не знаходяться в одному сегменті мережі, широкомовний пакет потрібно відправити на шлюз. MAC-адреса шлюзу буде використовуватися вихідним хостом як його MAC-адреса призначення.

2. Додавання та видалення тегів VLAN під час зв’язку між пристроями: Коли кадри обробляються в комутаторі, потрібно обробляти теги VLAN.

Оскільки широкомовні пакети обмежені в одній і тій же VLAN, хости в різних VLAN не можуть безпосередньо взаємодіяти один з одним на рівні 2. У реальних додатках комунікації для хостів у різних VLAN є широко розповсюдженими. Тому для вирішення цієї проблеми використовується маршрутизація між VLAN, яка може перенаправляти мережевий трафік з однієї VLAN на іншу.

Режим роботи маршрутизації між VLAN подібний до режиму внутрішньої мережі VLAN. Різниця полягає в тому, що маршрутизацію між VLAN потрібно досягти за допомогою маршрутизації рівня 3, яка може бути

реалізована за допомогою маршрутизатора або комутатора рівня 3. Існує три варіанти для того, щоб увімкнути маршрутизацію між різними VLAN:

Маршрутизація між VLAN з окремими фізичними інтерфейсами. Цей спосіб маршрутизації між VLAN полягає у підключенні додаткового порту від кожної VLAN до маршрутизатора. Кожна VLAN потребує одного фізичного порту на маршрутизаторі, що спричиняє велику вартість маршрутизаторів. Тому цей тип маршрутизації між VLAN рідко використовується через свою високу вартість та погану масштабованість.

Маршрутизація Router-on-a-stick Inter-VLAN. Цей тип маршрутизації VLAN набагато розумніший, ніж у вищезазначеного, що дозволяє одному фізичному інтерфейсу досягти переадресації трафіку між VLAN. Після налаштування з'єднання між маршрутизатором і комутатором як магістральної лінії, маршрутизатор може приймати кадри з тегами VLAN на інтерфейсі магістралі від підключеного комутатора і пересилати маршрутизовані пакети до міток призначення VLAN через той же інтерфейс.

Маршрутизація між VLAN із комутатором рівня 3. Останній спосіб полягає у використанні комутаторів рівня 3 з функцією маршрутизації. Користувачам потрібно створити SVI (Switch Virtual Interface) для кожної VLAN і налаштувати для неї IP-адресу. Цю IP-адресу можна використовувати для комп'ютерів як шлюз за замовчуванням. Таким чином, пакети від однієї VLAN будуть відправлені до SVI для перенаправлення до інших VLAN для реалізації взаємодії між VLAN.

На основі VLAN існують різні розширені конфігурації, розроблені для полегшення мережевого зв'язку, такі як використання VLAN для реалізації ізоляції рівня 2 та використання політики трафіку для реалізації контролю доступу між VLAN. Зазвичай існує п'ять основних типів VLAN: VLAN на основі інтерфейсу, VLAN на основі MAC-адреси, VLAN на основі підмережі IP, VLAN на основі протоколу та VLAN на основі політики.

VLAN на основі порту, який також називають VLAN на основі інтерфейсу – це технологія, яка дозволяє адміністраторам мережі вручну призначати VLAN для кожного порту комутатора. Такий спосіб підходить для невеликих мереж без необхідності часто змінювати мережеву інфраструктуру.

VLAN на основі MAC-адреси відноситься до присвоєння VLAN відповідно до вихідних MAC-адрес кадрів. Застосування цієї технології може значно покращити безпеку та гнучкість мережі. Навіть якщо користувачі часто змінюють своє фізичне місцезнаходження, адміністратору мережі не потрібно буде переналаштовувати VLAN.

VLAN на основі підмережі IP може призначати VLAN відповідно до IP-підмереж пристроїв. Це буде ефективним рішенням для загальнодоступної мережі з вищим попитом на мобільність та спрощеним управлінням та меншим попитом на безпеку. За допомогою цієї технології користувачі можуть автоматично приєднуватися до нового ідентифікатора VLAN після зміни їх IP.

Застосована до мережі з декількома протоколами, VLAN на основі протоколу може призначати VLAN відповідно до типів протоколів та форматів інкапсуляції кадрів.

VLAN, що базується на політиці, працює подібно до всіх вищезазначених методів. Але це також поєднання вищевказаних методів. Він може призначати VLAN відповідно до такої політики, як комбінація MAC-адрес та IP-адрес. Завдяки поєднанню політик для здійснення контролю доступу між VLAN, мережева безпека та гнучкість значно покращаться.

Створення віртуалізації мережевих ресурсів на основі технології VLAN є дуже базовим методом оптимізації мережі, проте і надзвичайно ефективним з точки зору поділу користувачів на віртуальні групи за призначенням чи типом роботи, а також ресурсами, що використовуються цими користувачами.

2.3 Дослідження оптимізації роботи на основі технології Geneve

Віртуалізація мережі передбачає співпрацю пристроїв з широким розмаїттям можливостей, таких як програмно-апаратні кінцеві точки тунелю, транзитні фабрики та централізовані кластери управління. В результаті їх ролі у зв'язуванні різних елементів у системі, всі ці компоненти впливають на вимоги до тунелів. Тому гнучкість є найважливішим аспектом тунельного протоколу, якщо він хоче йти в ногу з розвитком системи. Geneve (Generic Network Virtualization Encapsulation) – протокол, призначений розпізнати та врахувати ці мінливі можливості та потреби.

Мережа вже давно містить різноманітні механізми тунелювання, додавання міток та інших механізмів інкапсуляції. Однак поява мережевої віртуалізації спричинила сплеск відновленого інтересу та, відповідно, збільшення впровадження нових протоколів. Велика кількість протоколів у цьому просторі, починаючи від VLAN [IEEE.802.1Q_2014] і MPLS [RFC3031], закінчуючи новітніми VXLAN [RFC7348], NVGRE [RFC7637], часто призводить до питань про необхідність нової інкапсуляції. У той час як багато протоколів інкапсуляції прагнуть просто розділити інфраструктуру мережі або виступати мостом між двома доменами, мережева віртуалізація розглядає транзитну мережу як забезпечення зв'язку між декількома компонентами розподіленої системи. Багато в чому ця система схожа на шасі комутатора, де мережевий шар IP виконує роль з'єднувальної панелі та тунелю кінцевих точок на краю як лінійних карт. Якщо розглядати у такому світлі, вимоги, що пред'являються до тунельного протоколу, суттєво відрізняються з точки зору кількості необхідних метаданих та ролі транзитних вузлів.

Geneve призначений для підтримки випадків використання мережевої віртуалізації, де тунелі, як правило, встановлюються як з'єднувальна плата між віртуальними комутаторами, розташованими в гіпервізорах, фізичних

комутаторах, або проміжних боксах чи інших пристроях. Довільна мережа IP може бути використана як інфраструктура, хоча мережі Clos, складені за допомогою посилань ECMP (Equal Cost Multipath), є загальним вибором для забезпечення послідовної бісекційної пропускної здатності між усіма точками підключення. На рисунку 2.2 показаний приклад гіпервізора, комутатора верхньої стійки для підключення до фізичних серверів та висхідної лінії зв'язку WAN, підключеної за допомогою тунелів Geneve через спрощену мережу Clos. Ці тунелі використовуються для інкапсуляції та пересилання кадрів із приєднаних компонентів, таких як віртуальні машини або фізичні посилання.

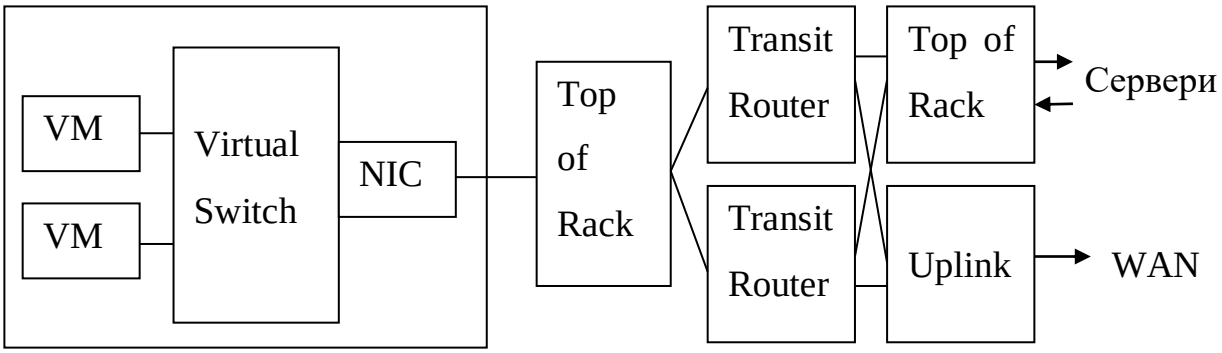

Рисунок 2.2 – Приклад Geneve тунелю між комутаторами

Для підтримки потреб віртуалізації мережі тунельний протокол повинен мати змогу скористатися різними можливостями кожного типу пристроїв як в інфраструктурній, так і в верхніх надбудовних мережах. Це призводить до того, що наступні вимоги ставляться до протоколу тунелювання площини даних:

– площина даних є загальною та достатньою для розширення, щоб підтримувати поточну та майбутню площини управління;

– тунельні компоненти ефективно реалізовувати як в апаратному, так і в програмному забезпеченні, не обмежуючи можливості найнижчим загальним знаменником;

– висока продуктивність порівняно з існуючими IP обробок.

Формат пакету Geneve складається з компактного заголовка тунелю, інкапсульованого в UDP через IPv4 або IPv6. Невеликий фіксований тунельний заголовок забезпечує інформацію про керування плюс базовий рівень функціональності та сумісності з акцентом на простоті. Потім цей заголовок супроводжується набором змінних параметрів, які дозволяють майбутні інновації. Нарешті, корисне навантаження складається з блоку даних протоколу зазначеного типу, наприклад, кадру Ethernet.

Параметри Geneve призначені для створення та обробки кінцевими точками тунелю. Однак варіанти можуть бути інтерпретовані транзитними пристроями вздовж траси тунелю. Транзитні пристрої, які не обробляють заголовки Geneve, повинні обробляти Geneve-пакети як будь-який інший пакет UDP і підтримувати послідовну поведінку пересилання.

У кінцевих точках тунелю генерація та інтерпретація опцій визначається площиною управління. Однак для забезпечення взаємодії між різнорідними пристроями пред’являються деякі вимоги до опцій та пристроїв, які їх обробляють:

– отримуючі кінцеві пристрої повинні знищувати пакети, що містять невідомі параметри з бітом 'C', встановленим у типі параметра. І навпаки, транзитні пристрої не повинні скидати пакети в результаті зустрічі з невідомими варіантами, включаючи ті, у яких встановлений біт «C».

– деякі опції можуть бути визначені таким чином, що позиція у списку опцій є значною. Опції чи їх впорядкування не повинні змінюватися транзитними пристроями.

– опція не повинна впливати на синтаксичний розбір або інтерпретацію будь-якої іншої опції.

При розробці опцій Geneve важливо врахувати, як ці опції будуть розвиватися в майбутньому. Після визначення опцій розумно очікувати, що

реалізації можуть залежати від конкретної поведінки. Як результат, обсяг будь-яких майбутніх змін повинен бути ретельно описаний заздалегідь.

Несподівано значні проблеми сумісності можуть виникнути внаслідок зміни довжини опції, яка була визначена як певний розмір. Вказується конкретна опція, яка має або фіксовану довжину і є постійною, або змінну довжину, яка може змінюватися з часом чи для різних випадків використання. Ця властивість є частиною визначення опції та передається за допомогою “Type”. Щодо параметрів фіксованої довжини, деякі реалізації можуть ігнорувати поле довжини в заголовку опції і замість цього проводити синтаксичний аналіз на основі добре відомої довжини, пов’язаної з типом. У цьому випадку перевизначення довжини вплине не тільки на синтаксичний аналіз відповідного варіанту, але й на будь-які наступні варіанти. Тому параметри, які визначено як фіксовану довжину за розміром, не повинні перевизначати на іншу довжину.

Вміщений в пакет UDP/IP, Geneve не має жодних власних механізмів безпеки. Як результат, зловмисник, який має доступ до основної мережі, що транспортує IP-пакети, має можливість підслуховувати або вводити пакети. Законні, але зловмисні кінцеві точки тунелю можуть також підробляти ідентифікатори у заголовку тунелю, щоб отримати доступ до мереж, що належать іншим орендарям.

У межах певного домену безпеки, наприклад центру обробки даних, який експлуатується одним постачальником послуг, найпоширенішим і найефективнішим механізмом захисту є ізоляція надійних компонентів. Тунельний трафік може передаватися через окрему VLAN і фільтруватися на будь-яких ненадійних межах. Крім того, кінцеві точки тунелю повинні експлуатуватися лише в середовищах, контрольованих постачальником послуг, таких як сам гіпервізор, а не всередині віртуальної машини клієнта.

При перетині ненадійного каналу, такого як загальнодоступний Інтернет, IPsec [RFC4301] може використовуватися для забезпечення

автентифікації та/або шифрування IP-пакетів, сформованих як частина інкапсуляції Geneve.

Geneve ніяк не впливає на безпеку інкапсульованих пакетів. Отже, оператор повинен зробити оцінку на основі свого мережевого середовища та визначити ризики, які стосуються їх конкретного середовища, та застосувати відповідні підходи до пом'якшення, залежно від ситуації.

Geneve – це протокол інкапсуляції накладеної віртуалізації мережі, призначений для встановлення тунелів між кінцевими точками віртуалізації мережі (Network Virtualization Endpoints (NVE)) через існуючу мережу IP. Він може бути використаний для розгортання мереж накладання декількох орендарів у існуючій мережі інфраструктури IP у загальнодоступному або приватному центрі обробки даних. Послуга накладання зазвичай надається постачальником послуг, наприклад, постачальником хмарних послуг або приватним оператором центру обробки даних. Через природу багатокористувацької оренди в таких середовищах система орендаря може очікувати конфіденційності даних, щоб переконатись, що в її пакетні дані не втручаються (активна атака) під час транзиту або несанкціонованого моніторингу (пасивна атака). Орендар може розраховувати, що постачальник послуг накладання надає конфіденційність даних як частину послуги, або орендар може запровадити власні механізми конфіденційності даних, такі як IPsec або TLS, щоб захистити дані в кінці між системами орендаря.

Якщо оператор визначить, що конфіденційність даних необхідна в його середовищі на основі їх аналізу ризику, наприклад, як у багатонаціональному середовищі, тоді слід використовувати механізм шифрування для шифрування даних орендаря в кінці між NVE. NVE можуть використовувати існуючі усталені механізми шифрування, такі як IPsec, DTL тощо. Оператор може вибрати не вмикати шифрування, якщо, наприклад, пакетні дані вже зашифровані системою орендаря.

2.4 Оптимізація MPLS з використанням технології SD-WAN

SD-WAN віртуалізує мережеві функції, які працюють в мережевій інфраструктурі, щоб вони могли працювати як програмне забезпечення на існуючому обладнанні. Технологія MPLS працює на власному обладнанні. З'єднання SD-WAN можуть бути виділеними лініями або загальнодоступними мережами, тоді як MPLS визначається виділеними лініями. У деяких випадках SD-WAN інтегровано з MPLS як одне із з'єднань SD-WAN.

MPLS працює аналогічно комутаторам і маршрутизаторам, перебуваючи між рівнями 2 і 3. (MPLS іноді вважається рівнем 2.5.). Він використовує технологію пересилання пакетів і мітки для прийняття рішень щодо пересилання даних. Мітка накладається між заголовками рівня 2 (лінія передачі даних) і рівня 3 (мережа).

Приклад організації SD-WAN з інтеграцією технології MPLS показано на рисунку 2.3.

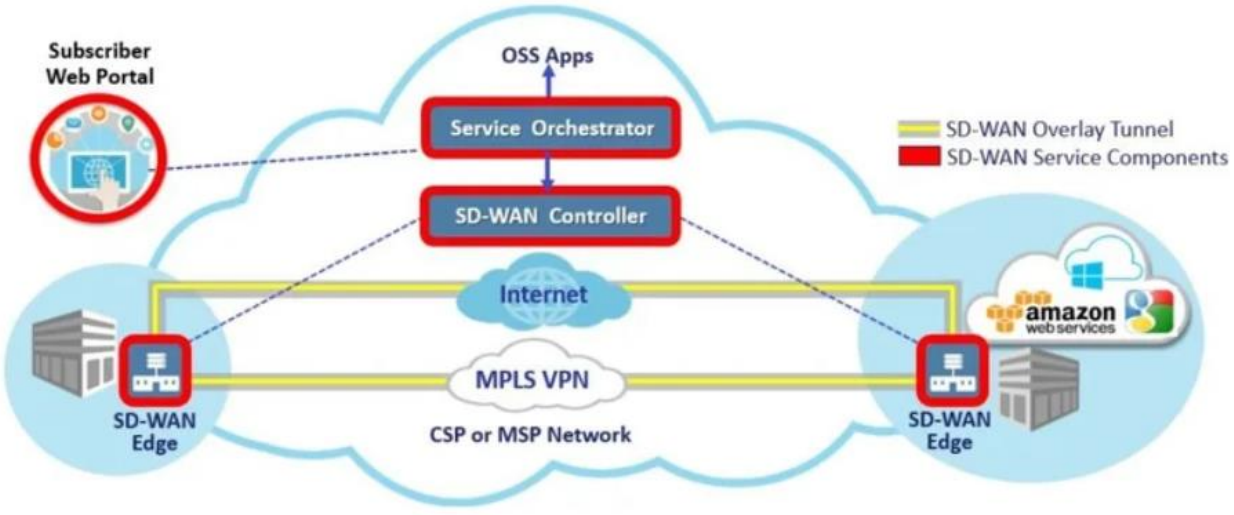

Рисунок 2.3 – SDWAN архітектура з інтеграцією MPLS

У цій віртуалізованій мережі є три основні компоненти: границя SD-WAN, контролер та оркестратор.

Границя SD-WAN – це місце, де розташовані кінцеві точки мережі. Це може бути філія, віддалений центр обробки даних або хмарна платформа.

SD-WAN Orchestrator – це віртуалізований менеджер мережі, який контролює трафік та застосовує політику та протокол, встановлені операторами.

Контролер SD-WAN централізує управління і дозволяє операторам бачити мережу через єдину точку, а також встановлює політику для виконання оркестратором.

Ці компоненти складають основну структуру SD-WAN. Крім того, існує три основних типи архітектури: локальна, хмарна та хмарна з магістраллю.

Локальний SD-WAN – це місце, де апаратне забезпечення SD-WAN знаходиться на місці. Мережеві оператори можуть безпосередньо отримувати доступ до мережі та апаратного забезпечення, в якому вона знаходиться, та керувати ними, і він не використовує хмару для своїх з'єднань. Це робить його ідеальним для конфіденційної інформації, яку неможливо надіслати через Інтернет.

SD-WAN з підтримкою хмари підключаються до віртуального хмарного шлюзу через Інтернет, що робить мережу більш доступною та забезпечує кращу інтеграцію та продуктивність із власними хмарними програмами.

З підтримкою хмари та Backbone SD-WAN дає організаціям додаткове резервне копіювання, підключаючи мережу до сусідньої точки присутності (PoP), наприклад, у центрі обробки даних. Це дозволяє трафіку переключатися із загальнодоступного Інтернету на приватне. Перехід до приватного з'єднання веде до більш безпечного SD-WAN і додає послідовності у випадку, якщо з'єднання перевантажене або не вдається.

Через свою віртуалізовану архітектуру SD-WAN не вимагає спеціального обладнання для спеціалізованих мережевих функцій. Натомість

інфраструктура складається з комерційного готового обладнання (commercial off-the-shelf (COTS)).

Деякі типи апаратних засобів COTS, такі як універсальне обладнання сторони клієнта (uCPE), можуть приймати різноманітні мережеві функції. Це спрощує управління мережею на межі мережі або в штаб-квартирі організації.

Підприємства можуть розгортати SD-WAN власноручно, коли бізнес володіє мережею та обладнанням і несе повну відповідальність за роботу та обслуговування мережі. У свою чергу, підприємства можуть використовувати керованого постачальника послуг, який володіє всім мережевим обладнанням і підтримує певний контроль над мережею, а також бере на себе основну відповідальність за управління мережею.

За прогнозами, глобальний ринок SD-WAN у 2023 році розростеться до 5,25 мільярда доларів, згідно з прогнозом IDC у липні 2019 року, оскільки все більше підприємств користуються перевагами віртуалізованої мережі.

Основні переваги включають:

– збільшена пропускна здатність за нижчою вартістю, оскільки мережевий трафік може бути забезпечений для оптимальної швидкості та розділення даних з низьким пріоритетом;

– централізоване управління в мережах філій за допомогою простої консолі управління, що зменшує необхідність ручного налаштування та IT-персоналу на місці;

– повна видимість мережі, оскільки контролер дає операторам цілісне уявлення про мережу;

– більше варіантів для типу підключення та вибору постачальника, оскільки мережа може працювати на апаратному забезпеченні COTS і використовувати як приватне, так і загальнодоступне підключення для маршрутизації свого трафіку.

Одним з найважливіших аспектів MPLS є те, як він може дуже надійно доставляти пакети до місця призначення пакетів. MPLS, як правило, пропонує високу якість обслуговування, коли мова йде про те, щоб уникнути втрати пакетів і зберегти найважливіший трафік організації. Ця надійність особливо важлива для підтримки якості протоколів у режимі реального часу, таких як Voice over IP (VoIP).

Надійність MPLS можлива завдяки міткам, які він використовує для пересилання. Мітки практично ізолюють пакети. Постачальники MPLS можуть також призначити вищий пріоритет певному мережевому трафіку. Ці переваги створюють відчуття передбачуваності трафіку в мережі. Мережеві шляхи заздалегідь визначені, тому пакети рухаються лише вздовж шляхів, до яких вони спрямовані.

Недоліком MPLS є вартість пропускної здатності. Сучасні споживачі дедалі більше цікавляться мультимедійним вмістом із обмеженою пропускною здатністю, таким як відео та доповнена реальність (AR), а також висока мегабітна вартість, яку вимагає MPLS, може бути недосяжною. Нарешті, мережа MPLS не пропонує вбудований захист даних, і якщо її неправильно реалізувати, вона може відкрити мережу для вразливостей.

Продовжуючи обговорення SD-WAN проти MPLS, SD-WAN пропонує кілька переваг перед традиційними мережами MPLS. Завдяки SD-WAN географічні межі стають менш актуальними, а ключові переваги, такі як видимість, масштабованість, продуктивність та контроль, покращуються.

На відміну від MPLS, SD-WAN не передбачає штрафних санкцій. Клієнти можуть легко оновити, додавши нові канали, без змін в інфраструктурі чи мережі. Мабуть, найбільшою перевагою SD-WAN є можливість економічно ефективно змішувати та поєднувати мережеві канали відповідно до типу вмісту або пріоритету. Широкосмугові та стільникові з’єднання з Інтернетом є менш дорогими, ніж MPLS, тому клієнти можуть

вибрати ці канали замість дорогої мережі MPLS для певних типів трафіку з нижчим пріоритетом.

Можливо, основною перевагою SD-WAN є віртуалізація безпеки. Сучасні організації надають перевагу мережевим архітектурам, що об'єднують безпеку, політики та організацію. Безпека SD-WAN охоплює ці основи, об'єднуючи підходи безпечного з'єднання. В архітектурі SD-WAN організація отримує вигоду від наскрізного шифрування по всій мережі, включаючи Інтернет. Усі пристрої та кінцеві точки повністю автентифіковані завдяки масштабованій функціональності обміну ключами та програмно визначеному захисту.

2.5 Оптимізація роботи маршрутизації через віртуалізацію обладнання

Протокол резервування маршрутизаторів, що створює віртуалізовані шлюзи, включає три протоколи: Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP) і Gateway Load Balancing Protocol (GLBP). Кожен протокол має своє призначення та має свої переваги та недоліки. First Hop Redundancy Protocol (FHRP) – це серія протоколів, що розроблені для зменшення втрат транспорту. Ці протоколи допомагають конкретній організації успішно відправляти трафік від джерела до пункту призначення без втрати багатьох пакетів. У разі виходу з ладу однієї системи існує резервна система, яка автоматично активується і продовжує надсилати трафік. Протокол HSRP та протокол GLBP є приватними Cisco, тоді як протокол VRRP є стандартом Інституту інженерів електрики та електроніки (IEEE). Порівняння дасть змогу показати, який протокол найкращий у якому сценарії, а який найкращий серед трьох протоколів. Ці протоколи працюють на пристроях рівня 3, які знаходяться на транспортному рівні. Протоколи

здатні передавати трафік, якщо один з маршрутизаторів мережі не працює через якусь технічну несправність.

Одним із способів досягти максимального часу безвідмовної роботи, тобто те, що мережа не виходить з ладу, є використання HSRP, який забезпечує надмірність мережі, щоб у разі відмови мережа якнайшвидше відновилася від втрати шлюза. Спільно використовуючи IP-адресу та MAC-адресу (рівень 2), два або більше маршрутизаторів можуть діяти як єдиний віртуальний маршрутизатор. Члени групи віртуального маршрутизатора постійно обмінюються повідомленнями про стан маршрутизатора, який живий, а який не працює. Несправність одного маршрутизатора дозволить іншому маршрутизатору взяти на себе мережеві обов'язки. Таким чином, пакети можна легко відправити або отримати.

HSRP – це власний протокол Cisco, який дозволяє мережевому інженеру додати більше одного резервного пристрою для досягнення надійності мережі. Різні маршрутизатори групи HSRP зв'язуватимуться, щоб вибрати один активний шлюз, який обробляє весь мережевий трафік. При налаштуванні маршрутизатора як активного маршрутизатора в цей момент також вибирається резервний маршрутизатор. Маршрутизатор в режимі очікування, так і активний маршрутизатор зв'язуються, надсилаючи повідомлення Hello, і визначають, чи активний маршрутизатор виходить з ладу. Коли відбувається збій, один із резервних маршрутизаторів виконує обов'язки активного маршрутизатора з мінімальною затримкою, і одночасно вибирається інший резервний маршрутизатор.

VRRP – це відкритий стандарт, який можна використовувати там, де існує обладнання різних компаній. Його робота майже така ж, як у HSRP, але відрізняється кількома нюансами. У VRRP, як і в HSRP, налаштована група маршрутизаторів, в яких мережевий інженер вибирає один головний маршрутизатор, а інший резервний маршрутизатор. Фізична IP-адреса головного маршрутизатора використовується клієнтами як шлюз за

замовчуванням. Члени резервної копії групи VRRP зв’язуватимуться з головним шлюзом за допомогою привітних повідомлень і прийматимуть на себе обов’язки головного маршрутизатора, коли головний маршрутизатор не працює або виникає якась помилка. Використана IP-адреса завжди належить головному маршрутизатору, який називається власником IP-адреси. Коли головний маршрутизатор відновлюється після помилки, він знову бере свої обов’язки назад і перенаправляє сам мережевий трафік.

VRRP додає групу маршрутизаторів, які можуть виступати в ролі мережевих шлюзів, що дозволяють трафіку проходити через ці шлюзи. Маршрутизатори групи VRRP обирають ведучого за допомогою механізму виборів VRRP, який виступатиме шлюзом. VRRP працює наступним чином:

– роль маршрутизаторів групи VRRP визначається їх IP-адресами та їх пріоритетами. Маршрутизатор з найвищим пріоритетом буде головним маршрутизатором, а інші з низьким пріоритетом – резервним. Якщо під час виборів маршрутизатори мають однаковий пріоритет, головним стає той, хто має найвищу IP-адресу. Головний регулярно надсилає повідомлення VRRP, щоб сповіщати резервні пристрої, щоб повідомити, що вони працюють належним чином, і кожен з резервних пристроїв запускає таймер для очікування повідомлення від головного.

– У режимі очікування, коли резервна копія отримує повідомлення VRRP, вона порівнює пріоритет у пакеті головного маршрутизатора зі своїм власним пріоритетом. У випадку, якщо пріоритет резервної копії вищий, ніж головного, тоді копія стане основною, інакше вона залишається резервним маршрутизатором в, група VRRP завжди має маршрутизатор з режимі очікування.

– У режимі очікування маршрутизатор групи VRRP залишається ведучим або резервним маршрутизатором, доки ведучий не виходить з ладу з якихось причин. Резервна пристрій не стає головним, навіть якщо він

налаштована з вищим пріоритетом, оскільки режим очікування допомагає уникнути частого переключення між головним та резервними копіями.

– Якщо таймер резервного маршрутизатора закінчується, але він все ще не отримує жодного повідомлення від головного, вважається, що останній не працює. У такому випадку резервний маршрутизатор вважає себе головним і надсилає Hello VRRP на всі інші маршрутизатори, щоб розпочати нові вибори.

Для досягнення розподілу навантаження між маршрутизаторами поряд із надлишковою надмірністю, Cisco має новий протокол, який називається GLBP. Це запатентований протокол компанією Cisco, який покращує ефективність FHRP, дозволяючи автоматичне вирівнювання навантаження.

LBP визначає протокол, який забезпечує балансування навантаження за кількома шлюзами через одну віртуальну IP-адресу. Active Virtual Gateway (AVG) обирається з членів групи GLBP. Інші учасники групи забезпечують резервну копію AVG, якщо з якихось причин він стане недоступний. AVG призначає віртуальну MAC-адресу кожному члену групи GLBP. Ці шлюзи стають Active Virtual Forwarder (AVF) для цієї віртуальної MAC-адреси, яка несе відповідальність за пересилання пакетів до інших маршрутизаторів або до пункту призначення.

2.6 Висновки до другого розділу

В другому розділі кваліфікаційної роботи для оптимізації роботи гетерогенних мереж різного призначення запропоновано використання технології VLAN, як базового методу поділу на віртуалізовані широкомовні домени та покращення продуктивності через зменшення об’ємів трафіку і розділення рівнів доступу. Оскільки дана технологія дозволяє обмін між різними VLAN через маршрутизатор, то виникає можливість додавати

політики управління та безпеки між різними підмережами комутованої мережі. Поділ мережі на VLAN в поєднанні з іншими протоколами дає змогу суттєво підвищити продуктивність та надає можливість управління потоками даних на 2-гому рівні. Наступним кроком оптимізації є використання протоколу Geneve прототипування якого наведено в даній роботі, а технічна реалізація можлива при наявності комерційного обладнання від виробників. Аналіз магістральної технології MPLS показав її обмеженість до вимог сучасного світу і як варіант вирішення цієї задачі запропоновано використання технології SD-WAN, що дає змогу додати віртуалізацію мережевих функцій та вирішити недоліки початкового протоколу MPLS. На завершення, запропоновано використання протоколів віртуалізації маршрутизаторів, що дасть змогу підвищити доступність шлюзів за замовчуванням і збільшити стійкість мережі до атак типу заборона сервісу.

3 АПРОБАЦІЯ ПРИЙНЯТИХ РІШЕНЬ

3.1 Моделювання мережі на основі технології VLAN

Для перевірки підвищення ефективності функціонування локальної мережі пропонується провести моделювання її роботи з врахуванням наступних параметрів:

– мережа є гетерогенною за своєю природою, містячи користувачів з різними вимогами до використання ресурсів;

– політики безпеки повинні бути застосовані до груп користувачів для розділення прав доступу до різних ресурсів мережі та сховищ даних;

– порти мають бути ефективно використані для забезпечення вищенаведених вимог.

Створення VLAN потребує аналізу наборів даних якими користувачі в мережі будуть обмінюватись між собою, розміщення серверного обладнання, визначення найкоротших шляхів у мережі для доступу до даних чи сервісів.

Аналіз шляхів обміну даними дає можливість організувати баланс навантаження на канали зв’язку, тим самим запобігаючи утворенню вузьких місць. Додавання надлишкових каналів разом з протоколом запобігання петлям Spannig Tree підвищує надійність роботи мережі та створює альтернативні шляхи передавання, які теж потрібно враховувати при створенні віртуалізованого поділу комутованої мережі.

Віртуалізація на основі VLAN стирає межі фізичного розміщення кінцевих користувачів по відношенню до їх доступу до інформації, спрощуючи конфігурування та реплікацію вибраних політик. Іншими словами, користувачі в одній VLAN мають ті ж самі права та набори даних у своїй роботі. Знаходячись в різних кімнатах чи навіть будівлях, але належачи одній VLAN віртуально вони знаходяться в тій самій IP підмережі.

Для моделювання оптимізації роботи мережі через впровадження технології віртуальних мереж VLAN використаємо програмний симулятор роботи мереж Cisco Packet Tracer 7. Даний продукт підтримує широку лінійку мережевого обладнання з можливістю візуалізації процесів, що відбуваються в мережі. Топологія модельованої мережі показана на малюнку 3.1.

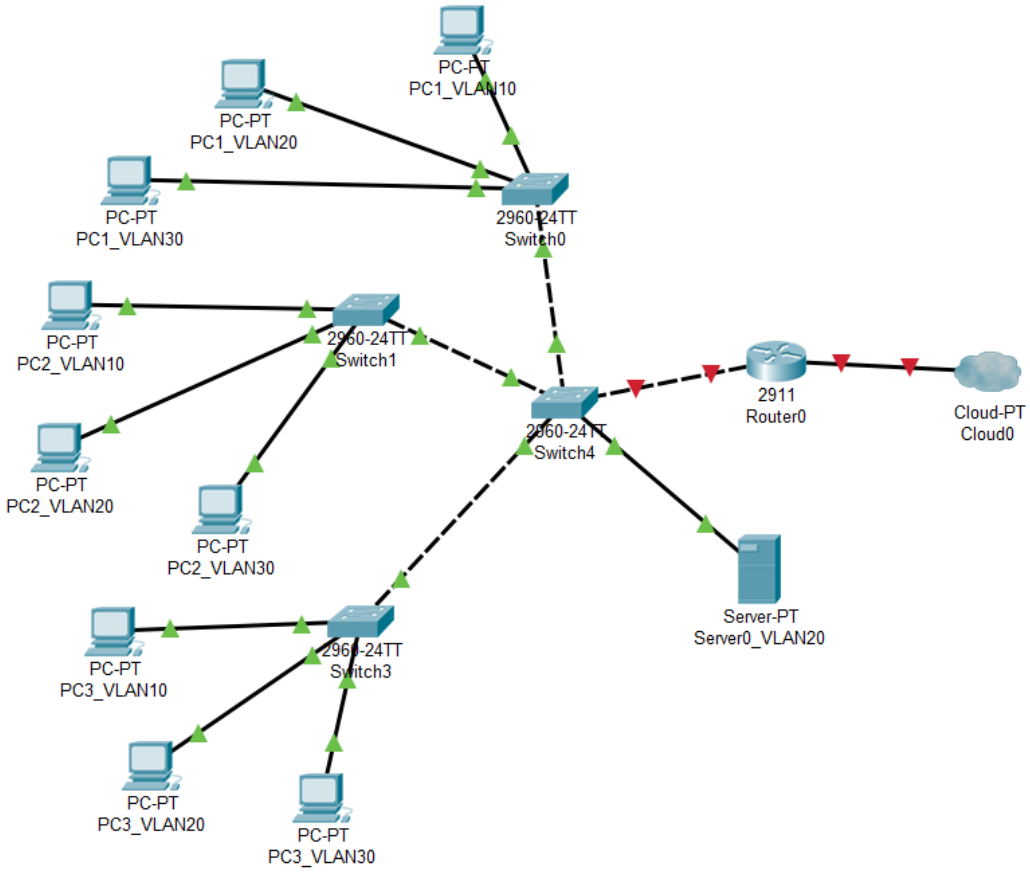

Рисунок 3.1 – Моделювання оптимізації роботи мережі з VLAN

Як видно з малюнку, створюється три VLAN з номерами 10, 20, 30, що відповідає трьом віртуальним групам користувачів. Також додано сервер доступ до якого за замовчуванням буде тільки в користувачів, які належать VLAN 20. Всі комутатори агрегуються через проміжний комутатор і магістральним портом під’єднуються до маршрутизатора. Всі обміни даними між VLAN будуть відбуватись через цей маршрутизатор і вихід назовні в

глобальні мережі також через нього. Така модель дає змогу впроваджувати на маршрутизаторі списки контролю доступу для розмежування привілеїв користувачів згідно обраних політик безпеки.

Лістинг 3.1 демонструє процес створення віртуальних мереж на комутаторах для розділення користувачів на групи. Спосіб призначення є статичне віднесення порту до відповідної VLAN.

Лістинг 3.1 – Створення віртуальних мереж на комутаторі

```
Switch>enable
Switch#configure terminal
Switch(config)#interface fastethernet 0/2
Switch(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
Switch(config-if)#switchport mode access
Switch(config-if)#interface fastethernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
Switch(config-if)#interface fastethernet 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
Switch(config-if)#interface fastethernet 0/1
Switch(config-if)#switchport mode trunk
```

Також показно, що інтерфейс під номером 1 буде виконувати роль магістрального для обміну даними між усіма VLAN. Такий варіант дасть змогу суттєво зекономити порти на комутаторі. У випадку недостатньої пропускної здатності через те, що всі VLAN будуть його використовувати як магістраль, існує можливість віртуалізувати декілька портів, щоб вони працювали як один логічний інтерфейс і не потрапляли під вплив протоколу запобігання петель. Пропускна здатність буде збільшеною у відповідності до пропускних здатностей портів, котрі будуть об’єднані. Також таке налаштування може уможливити баланс навантаження між фізичними інтерфейсами комутатора і покращити продуктивність оброблення кадрів даних.

Лістинг 3.2 показує створення віртуальних мереж на маршрутизаторі. Першим етапом відбувається активація підінтерфейсу, що буде обслуговувати відповідну VLAN і вказується який тег потрібно приймати від комутатора. Також, таке налаштування дає змогу маршрутизатору, що підтримує протокол 802.1Q додавати мітки при відправленні з порту до комутаторів і подальшої доставки до отримувача.

Лістинг 3.2 – Створення віртуальних мереж на маршрутизаторі

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/0.10
Router(config-subif)#
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gigabitEthernet 0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.11.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gigabitEthernet 0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.12.1 255.255.255.0
```

Правильне налаштування міток у відповідності до створених VLAN критично важливе для функціонування віртуальних мереж, оскільки кожен підінтефейс виконує роль шлюза за замовчуванням для всієї підмережі, що він обслуговує. Якщо шлюз працювати не буде, будь-які обміни даними між VLAN, чи з VLAN на зовні мережі стануть неможливими.

Змоделюємо ситуацію, коли потрібно здійснити обмін даними між хостами в одній VLAN та різних віртуальних мережах без задіювання маршрутизатора. Очікувано буде ситуація, що хости в одній віртуальній мережі знаходяться в одній IP мережі і тому зможуть виконати ARP запит на отримання MAC адреси отримувача даних. Результати перевірки з’єднання подано на малюнку 3.2.

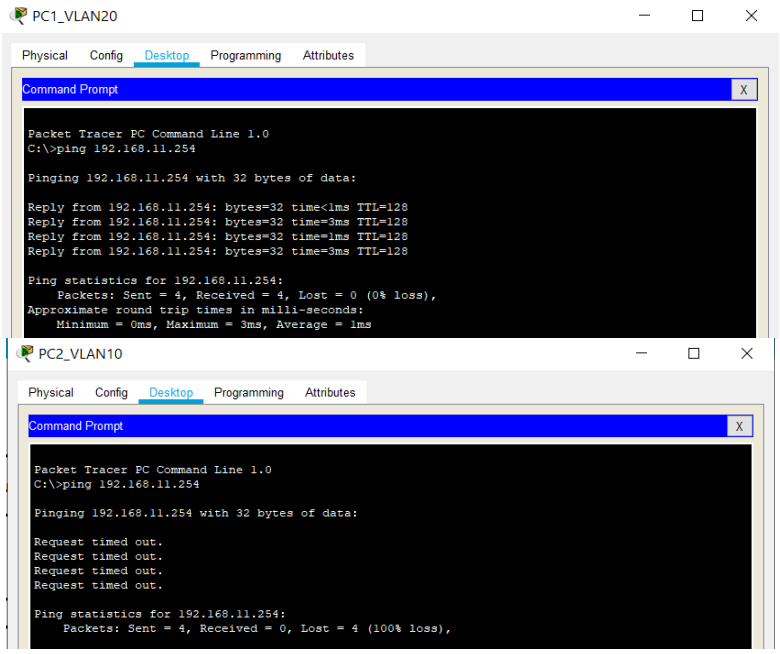

Рисунок 3.2 – Апробація відсутності з’єднання між різними віртуальними мережами

Хост у VLAN 10 спробував отримати з’єднання до хоста з VLAN 20 і результат виявився невдалим. Це тому, що для з’єднання з іншою VLAN потрібен маршрутизатор, який буде розуміти мітки VLAN та виконувати маршрутизацію. Відновимо з’єднання та повторимо спробу доступу до сервера. На малюнку 3.3 показано результат цих дій.

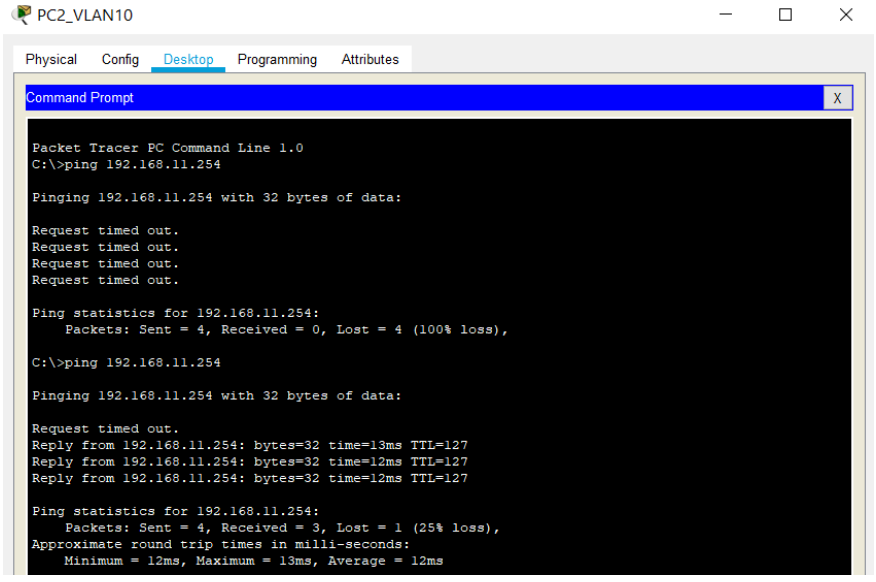

Рисунок 3.3 – Перевірка доступу до сервера з іншої VLAN

Результат перевірки показує, що тепер хост з VLAN 10 отримав доступ до сервера з VLAN 20. Це сталось тому, що маршрутизатор виконав функцію маршрутизації, оскільки всі його підмережі вже є в таблиці маршрутизації. Ніяких заборон на передавання даних між різними VLAN не було і це може стати проблемою, коли розглядається розмежування доступу. Малюнок 3.4 показує таблицю маршрутизації.

```
Router#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0.10
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/0.20
L       192.168.11.1/32 is directly connected, GigabitEthernet0/0.20
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/24 is directly connected, GigabitEthernet0/0.30
L       192.168.12.1/32 is directly connected, GigabitEthernet0/0.30
```

Рисунок 3.4 – Таблиця маршрутизації

Для встановлення розмежування доступів згідно політик безпеки організації потрібно використовувати списки контролю доступу. За допомогою цього тільки акредитовані сторони зможуть отримати ресурси, які їм призначені.

Певні труднощі можуть виникнути при неправильному налаштуванні портів доступу чи магістральних портів. Порти доступу повинні бути включені вручну, оскільки протокол Dynamic Trunking Protocol (DTP) має свої визначені стани і при під’єднані інших пристроїв може блокувати порт. Магістральний порт має параметр Native VLAN на який потрібно звертати увагу. Хоч даний параметр вже не є актуальним в наш час, він залишився з попередніх технологій і у випадку неспівпадання на двох кінцях магістралі буде блокувати з’єднання.

При роботі з віртуальними мережами потрібно перевіряти чи правильно хости присвоєні до відповідних VLAN. Результат перевірки показано на рисунку 3.5.

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   VLAN0010                         active    Fa0/2
20   VLAN0020                         active    Fa0/3
30   VLAN0030                         active    Fa0/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
```

Рисунок 3.5 – База даних VLAN

Перевірка правильності налаштування магістральних каналів показана на малюнку 3.6.

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30
```

Рисунок 3.6 – Параметри магістралі

Дослідження показало, що поділ мережі на VLAN може оптимізувати використання каналів. Це відбувається за допомогою протоколу Spannig Tree. Основна ідея такої оптимізації полягає в побудові найкоротших шляхів до ресурсів, які потрібні користувачам даної віртуальної групи. Протокол Spannig Tree будує окремі покриваючі дерева для кожної VLAN і вибирає кореневий комутатор. До цього кореневого комутатора всі інші повинні

побудувати найкоротші шляхи, а надлишкові повинні бути заблоковані для уникнення петель комутації. Якщо залишити цей процес неконтрольованим, то може виникнути ситуація коли кореневим для конкретної VLAN стане самий неоптимальний комутатор. Неоптимальні шляхи будуть навантажувати канали і відповідно буде спостерігатись погіршення продуктивності для користувачів інших віртуальних груп.

В модельованій топології агрегуючий комутатор з назвою Switch4 повинен бути кореневим для VLAN 20. Результати перевірки чи є даний пристрій головним в дереві показано на малюнку 3.7.

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.C919.4911
             Cost        19
             Port        4(FastEthernet0/4)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0060.3E04.26E6
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Root FWD 19        128.4    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/1            Desg FWD 19        128.1    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0007.EC37.48DC
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0060.3E04.26E6
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/1            Root FWD 19        128.1    P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    32788
             Address     0007.EC37.48DC
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
             Address     0060.3E04.26E6
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
```

Рисунок 3.7 – Перевірка кореневого комутатора для VLAN20 на Switch4

Як видно з поданого матеріалу комутатор Switch4 не є кореневим для VLAN20, оскільки MAC адреса кореневого комутатора не співпадає з MAC адресою даного пристрою.

Провівши налаштування кореневого комутатора для VLAN20 повторимо перевірку. Результати пропонованих рішень показано на малюнку 3.8.

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     0007.EC37.48DC
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0060.3E04.26E6
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/1            Root FWD 19        128.1    P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    24596
             Address     0060.3E04.26E6
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24596  (priority 24576 sys-id-ext 20)
             Address     0060.3E04.26E6
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/1            Desg FWD 19        128.1    P2p

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    32798
             Address     0007.EC37.48DC
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32798  (priority 32768 sys-id-ext 30)
             Address     0060.3E04.26E6
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
```

Рисунок 3.8 – Встановлення Switch4 кореневим для VLAN20

В той час як для інших VLAN параметри кореневого комутатора не змінились для VLAN 20 параметри Root ID та Bridge ID стали ідентичними, що свідчить про його призначення кореневим для цієї VLAN. Відповідно, шляхи до сервера під’єднаного до цього пристрою від інших комутаторів є найкоротшими, а продуктивність роботи для користувачів буде оптимальною

Використання віртуалізації на основі технології VLAN є одним з базових варіантів покращення роботи мережі, оптимізовуючи важливі параметри продуктивності, надійності та даючи змогу зекономити на дороговартісному обладнанні.

3.2 Моделювання оптимізації на основі маршрутизаторів

Роль маршрутизаторів в мережі є надзвичайно важливою, оскільки вони виконують функції перенаправлення трафіку та працюють шлязами за замовчуванням для хостів в мережі. Критично важливим стає питання постійної доступності цих пристроїв. В дослідженні методів оптимізації роботи гетерогенних мереж запропоновано використання протоколу HSRP для віртуалізації роботи маршрутизаторів. На малюнку 3.9 показано модифіковану топологію для моделювання оптимізації роботи мережі.

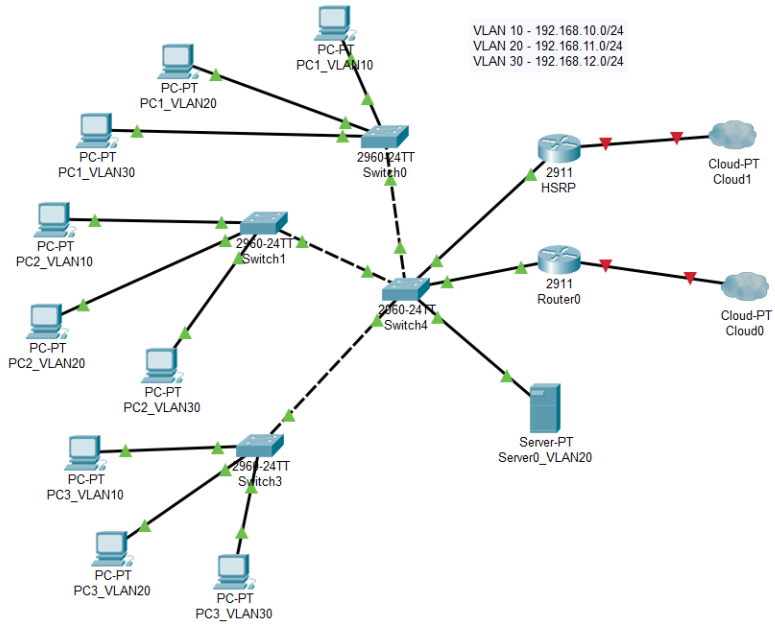

Рисунок 3.9 – Віртуалізація маршрутизаторів на основі HSRP

Як видно з малюнка, до основного маршрутизатора додано резервний з іменем HSRP. Під час своєї роботи два маршрутизатори будуть слідкувати за присутністю сусіда і у випадку, коли один з пристроїв вийде з ладу, візьмуть на себе функції маршрутизації. При цьому, процес зміни ролей між пристроями не буде видимий для користувачів і робота буде неперервною.

Лістинг 3.3 показує базові налаштування HSRP на маршрутизаторі. Віртуальна IP адреса використовується обома пристроями.

Лістинг 3.3 – Налаштування HSRP на маршрутизаторі

```
HSRP(config)#interface GigabitEthernet 0/0
HSRP(config-if)#ip address 192.168.10.253 255.255.255.0
HSRP(config-if)#no shutdown
HSRP(config-if)#standby ip 192.168.10.1
```

Перевірка присвоєння віртуальної адреси показана на малюнку 3.10.

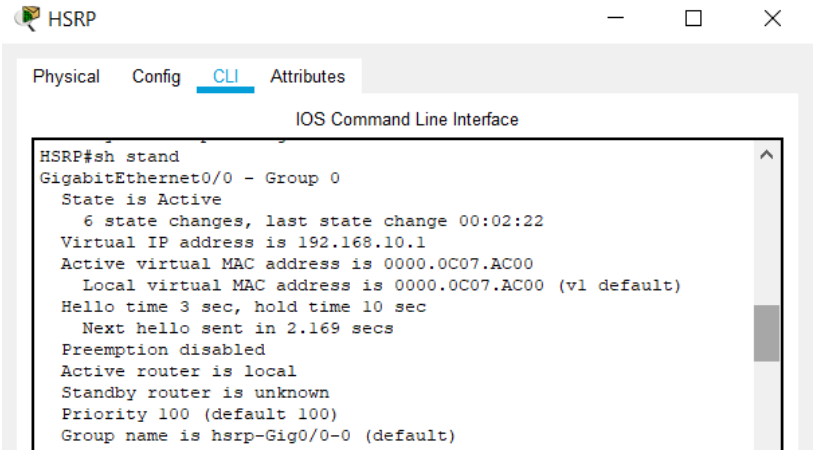

Рисунок 3.10 – Перевірка віртуалізації IP адреси на маршрутизаторі

Як видно з поданої перевірки, віртуальна адреса є 192.168.10.1 для всіх маршрутизаторів в одній групі. Проведена оптиміації роботи мережі дасть змогу підвищити стійкість маршрутизаторів до атак типу заборона сервісу.

3.3 Висновки до третього розділу

В даному розділі кваліфікаційної роботи проведено моделювання оптимізації роботи гетерогенної мережі через створення віртуальних мереж VLAN та поділ користувачів на віртуальні групи, оптимізовано використання ресурсів за допомогою налаштувань протоколу Spanning Tree. Для гарантування доступності виходу назовні мережі проведено моделювання роботи протоколу HSRP з віртуалізацією IP адреси шлюзу за замовчуванням, що дало можливість прозоро для користувачів збільшити надійність.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

4.1.1 Безпечні умови праці при монтажі комп'ютерної мережі

Законодавчими актами, що визначають основні положення про охорону праці є загальні закони України, а також спеціальні законодавчі акти. До загальних законів належать: Конституція України, Закони України: "Про охорону праці", "Про охорону здоров'я", "Про пожежну безпеку".

Приміщення, в яких встановлені персональні комп'ютери, повинні мати природне та штучне освітлення відповідно до СНиП II-4-79.

До початку робіт у комплексній бригаді проводиться первинний інструктаж з безпечного виконання робіт з основної та суміжних професій та ознайомлення з правилами надання першої допомоги.

Особи з простудними і хронічними захворюваннями верхніх дихальних шляхів до роботи з монтажу комп'ютерних мережі та заготовки і монтажу пластмасових труб не допускаються.

Роботи на висоті (при підйомі над поверхнею вище, ніж 1,3 м) виконуються тільки з риштувань або помостів.

Вимоги безпеки перед початком роботи передбачають, що до початку робіт з монтажу комп'ютерної мережі керівник зобов'язаний:

– перевірити ступінь готовності будівельних робіт;

– оцінити виробничі обставини, можливість взаємодії з іншими будівельно-монтажними організаціями у відповідності з проектом виконання робіт (ПВР); можливість безпечного застосування машин, механізмів, пристосувань, місця їх установки та порядок проїзду; можливість безпечного застосування піротехнічного інструменту, безпечної подачі електричних конструкцій, електротехнічних апаратів та інших блоків;

– узгодити з відповідними службами та, при необхідності, внести уточнення в ПВР.

– ознайомити працюючих з ПВР та технологічними картами на всі види робіт.

Керівник робіт повинен здійснити первинний інструктаж, який стосується:

– характеру та безпечних методів виконання робіт (у т.ч. за складних погодних умов); порядку проходів до кожного робочого місця;

– наявності небезпечних зон та відкритих каналів і траншей, відкритих прорізів, отворів у перекриттях та стінах;

– порядку розвантаження та складування матеріалів, устаткування та конструкцій;

– місць та порядку трансформаторів безпеки, електрифікованого інструменту, засобів електроосвітлення, випробувальних апаратів;

– порядку і місця установки вантажних лебідок та інших механізмів у монтажній зоні; порядку роботи з гідропідйомників, риштувань, підмостків, драбин; наявності діючих електроустановок та заборонених зон;

– надання першої допомоги, виклику швидкої медичної допомоги, пожежної охорони, керівника робіт чи роботодавця, представника служби охорони праці.

Перевірити наявність та термін дії посвідчень з охорони праці, електро-пожежобезпеки, посвідчень на право виконання спеціальних видів робіт (зварювання, монтаж кабельної арматури).

Видати наряд-допуск операторам на виконання робіт підвищеної небезпеки з проведенням цільового інструктажу та записом до журналу реєстрації інструктажів з питань охорони праці. Підписи інструкторів та інструктованих у журналі обов’язкові.

Попередити працюючих, що з’єднання та від’єднання від мережі обладнання, механізмів, інструменту, інвентарних шаф тощо (крім

оперативного вмикання і вимикання) в умовах будівельного майданчика виконуються тільки службою експлуатації власника мережі, якщо не існує іншої письмової домовленості з власником.

Вимоги безпеки під час виконання роботи:

– прокладання кабелів слід виконувати тільки в рукавицях.

– працювати ручними ударними інструментами слід із застосуванням захисних щитків або окулярів з непробивним склом.

– переносити чи перевозити інструмент з гострими кутами треба лише в чохлах.

– не дозволяється розміщувати кабель, барабан з кабелем та без нього, механізми, пристрої та інструменти безпосередньо біля бровки траншеї.

– перекочувати барабан з кабелем слід у напрямку стрілки, нанесеної фарбою на щоці барабана.

– переміщувати барабан з кабелем вручну дозволяється тільки по твердому ґрунту або надійному настилу по горизонтальній поверхні на відстань не більше .

Не дозволяється працюючим чи стороннім особам перебувати на шляху барабана, що переміщується. Під час піднімання барабана необхідно слідкувати за тим, щоб не пошкодити щоки барабана та втулку. Перед розмотуванням барабан встановити на домкрати (чи інший підіймальний пристрій). Барабан встановити так, щоб кабель розмотувався з його верхньої частини. Розмотувати кабель з барабана слід тільки за наявності гальмівного пристрою.

Прокладання кабелів і монтаж мережевого обладнання слід виконувати у захисному одязі з можливістю використання електростатичних браслетів.

Дотримання вимог безпечної роботи є необхідною умовою для успішного завершення побудови комп’ютерних мереж.

4.2 Безпека в надзвичайних ситуаціях

4.2.1 Функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуації мирного та воєнного часу

Моніторинг довкілля – це система спостереження, збирання та аналізу інформації про ситуацію, що може скластись під час надзвичайних ситуацій мирного та воєнного часу. Також це система спостереження за визначеними об’єктами, явищами та процесами з метою оперативного оцінювання їх стану, виявлення результатів впливу на них зовнішніх чинників та прийняття відповідних управлінських рішень (ДСТУ 3891:2013) (див. ДСТУ 7295:2013).

Моніторинг потенційно небезпечних об’єктів це спостереження, контролювання за зміною параметрів технологічних режимів з метою збирання, збереження, передавання та аналізування інформації щодо поточного стану потенційно небезпечних об’єктів, наявності та кількості порушень вимог безпеки, відпрацювання рекомендацій щодо проведення робіт із запобігання та ліквідування техногенних надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013).

Моніторинг джерел надзвичайних ситуацій це система спостереження за об’єктами, які можуть бути джерелами надзвичайних ситуацій, що має на меті виявлення небезпеки, збирання, узагальнення та аналізування оперативної інформації стосовно стану об’єктів моніторингу та розроблення науково-обґрунтованих рекомендацій щодо проведення заходів із запобігання та ліквідування надзвичайних ситуацій (ДСТУ 7295:2013).

Моніторинг довкілля це систематичні спостереження і контролювання, які проводять регулярно, за єдиною програмою для оцінювання стану довкілля, аналізування процесів, які відбуваються в ньому і своєчасне виявлення тенденцій його змінювання (ДСТУ 7295:2013).

Моніторинг надзвичайних ситуацій (НС) – система спостереження за об’єктами, які можуть бути джерелами надзвичайних ситуацій, що має на меті виявлення небезпеки, збирання, узагальнення та аналізування оперативної інформації щодо об’єктів моніторингу та розроблення науково обґрунтованих рекомендацій щодо проведення заходів із запобігання та ліквідування НС.

Моніторинг небезпечних явищ та процесів це система спостереження та контролювання за розвитком небезпечних та стихійних природних явищ і процесів, чинниками, які спричинюють їх формування та розвиток, аналізування, збереження та передавання інформації щодо виявлення тенденцій їх змінювання, розроблення комплексу заходів щодо запобігання природним надзвичайним ситуаціям та ліквідування їх наслідків. Небезпечні природні явища і процеси підрозділяють на геофізичні, геологічні, гідрологічні, метеорологічні, медико-біологічні та пожежі в природних екосистемах (ДСТУ 7295:2013).

Моніторинг пожеж в екосистемах це спостереження, контролювання, збирання, аналізування, збереження та передавання інформації щодо пожежної небезпеки в природних екосистемах (умов погоди, стану горючих матеріалів, інших пожежонебезпечних чинників), з метою своєчасного планування та здійснення заходів щодо запобігання виникненню і ліквідування пожеж та їх наслідків (ДСТУ 7295:2013).

Моніторинг радіаційної безпеки це спостереження і контролювання рівня радіоактивного забруднення місцевості, повітря, води, продовольства, об’єктів господарювання, дозових навантажень на населення з метою прийняття оперативних рішень щодо запобігання виникненню та ліквідування надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013).

Моніторинг хімічної небезпеки це спостереження, контролювання, збирання, аналізування, збереження та передавання інформації щодо визначення ступеня і характеру хімічного забруднення довкілля, санітарно-

гігієнічний нагляд за дотриманням установлених нормативів з метою виявлення джерела надходження небезпечних хімічних речовин, запобігання виникненню та ліквідування надзвичайних ситуацій та їх наслідків (ДСТУ 7295:2013)

Збір та аналіз інформації про стан довкілля під час мирного та воєнного стану дає можливість приймати оперативні рішння для адекватного реагування на ситуацію.

4.3 Висновки до четвертого розділу

В даному розділі кваліфікаційної роботи розглянуто питання безпечних умов праці при монтажі комп’ютерної мережі. В безпеці в надзвичайних ситуаціях висвітлено питання функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуацій мирного та воєнного часу.

ВИСНОВКИ

В кваліфікаційній роботі виконано дослідження методів та засобів оптимізації в задачах побудови гетерогенних мереж різного призначення. За результатами цього отримано наступні результати:

– досліджено моделі побудови гетерогенних мереж, що дало змогу визначити напрямки оптимізації їх характеристик;

– проаналізовано моделі безпеки гетерогенних мереж, що дало змогу сформулювати вимоги до комплексного захисту елементів мережі та даних;

– запропоновано виконати оптимізацію на основі віртуалізації мережевих ресурсів;

– здійснено підвищення ефективності роботи через створення віртуальних локальних мереж та описано додаткові налаштування для оптимізації роботи;

– виконано прототипування нового мережевого рішення, що базується на протоколі Geneve для створення віртуальних комутованих тунелів;

– запропоновано вдосконалення існуючої магістральної технології MPLS у вигляді гібридної з технологією SD-WAN;

– апробація прийнятих рішень здійснена через моделювання у середовищі Cisco Packet Tracer.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання безпечних умов праці при монтажі комп’ютерної мережі та функціонування державної системи спостереження, збирання, оброблення та аналізу інформації про стан довкілля під час надзвичайних ситуацій мирного та воєнного часу.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. E. Knipp et al., Managing Cisco Network Security. Elsevier Inc., 2002, ISBN: 978-1-931836-56-2

2. S. Wilkins and T. Smith, CCNP Security. SECURE 642-637 Official Cert Guide. Cisco Press, 2011, ISBN: 978-1-58714-2802.

3. V. Olifer and N. Olifer, Novye tekhnologii i oborudovanie IP-setei [New technologies and equipment of IP-networks]. St.-Peterburg, Russia: Bhv, 2000, ISBN: 5-8206-0053-3

4. A. D wankhade and P. N. Dr Chatur, “Comparison of Firewall and Intrusion Detection System,” Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 1, pp. 674–678, 2014, URL: http://ijcsit.com/docs/Volume 5/vol5issue01/ijcsit20140501145.pdf/.

5. T. King et al., “BLACKHOLE Community,” Internet Engineering Task Force (IETF), 2016. [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc7999. – Назва з екрану. – Дата звернення: 4.11.2020.

6. D. S. Ms. Charjan, P. S. Ms. Bochare, and Y. R. Bhuyar, “An Overview of Secure Sockets Layer,” Int. J. Comput. Sci. Appl., vol. 6, no. 2, pp. 388–393, 2013

7. “Cisco Network Admission Control (NAC) Solution Data Sheet - Cisco.” [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/nacappliance-cleanaccess/product_data_sheet0900aecd802da1b5.html. – Назва з екрану. – Дата звернення: 14.11.2020

8. M. Kozlova (AKA M. Kozlova, “7 luchshikh servisov zashchity ot DDoS-atak dlya povysheniya bezopasnosti [The 7 best services of protecting from DDoS- attacks for the increase of safety],” HOSTING.cafe, 2017. [Електронний

ресурс]. – Режим доступу: https://habrahabr.ru/company/hosting-cafe/blog/324848/. – Назва з екрану. – Дата звернення: 15.11.2020

9. Приїхав до Польщі – користуйся Інтернетом! [Електронний ресурс] – Режим доступу: http://naszwybir.pl/internet/. – Назва з екрану. – Дата звернення: 15.11.2020

10. V. F. Shangin, Informatsionnaya bezopasnost [Information Security]. Moscow, Russia: DMK Press, 2014.

11. Кулаков Ю.О. Комп'ютерні мережі / Ю.О. Кулаков – Юніор, 2005. – 397 с.

12. Вишневський В. М. Теоретичні основи проектування комп'ютерних мереж / В. М. Вишневський – Техносфера, 2004. – 512 с.

13. Cisco Systems Руководство по технологиям объединенных сетей / Cisco Systems - 3-е издание. СПб: “Вильямс”, 2002. – 1040 с.

14. Дебра Литтлджон Шиндер Основы компьютерных сетей / Дебра Литтлджон Шиндер - СПб: "Вильямс", 2002. – 656 с.

15. Коротыгин С. Стандарт IEEE 802.11 и его расширения / С. Коротыгин, А. Нежуренко - Сети и телекоммуникации, вып. 6(25), 2002 г.

16. Марк А. Спортак Компьютерные сети. Книга 1. High-Perfomance Networking. Энциклопедия пользователя / Марк А. – К.: ДиаСофт, 1999. – 432 с.

17. Марк А. Спортак Компьютерные сети. Книга 2: Networking Essentials. Энциклопедия пользователя / Марк А. – К.: ДиаСофт, 1999. – 432 с.

18. Беркман Л. Н. Архітектурна концепція побудови, принцип реалізації, ефективність застосування інтелектуальної телекомунікаційної мережі / Л. Н. Беркман, С. В. Толюпа // Зб. наук. праць ВІТІ НТУУ ―КПІ‖. – 2007. – №3. – С. 9-17.

19. Колченко В. О. Впровадження інтелекту в мережі наступного покоління (NGN) – перехід до мереж майбутнього покоління (FGN) / В. О. Колченко / Наукові записки УНДІЗ. – 2010. – №2(14). – С.80-85.

20. Беркман Л. Н. Проблеми створення сучасної конвергентної мережі на базі концепції FMC (Fixed-Mobile Convergence) / Л. Н. Беркман, О. І. Чумак, В. В. Григорович, П. Ю. Дещинський // Вісник УНДІЗ. – 2008. – №2. – С. 61-63.

21. Толюпа С. В. Структура інформаційної мережі та показники її ефективності / С. В. Толюпа, А. В. Сухін. // Зб. наук. праць КВІУЗ. – 2001. – №3. – С. 68-73.

22. Мурай А. В. Оценка качества телекоммуникационных услуг с учетом степени удовлетворения ожиданий и требований пользователей / А. В. Мурай // Наукові записки УНДІЗ. – 2013. – № 2(26). – С. 68-75.

23. Гребенніков В. О. Проблема загальнодоступності основних телекомунікаційних і інформаційних послуг в Україні та загальні підходи до її розв'язання / В. О. Гребенніков, Г. Ф. Колченко // Наукові записки УНДІЗ. – 2013. № 1(25). – С. 5-13.

24. Френк Г. Сети, связь и потоки / Г. Френк, И. Фриш ; пер. с англ. под ред. Д. А. Поспелова. – Москва : Связь, 1978. – 448 с.

25. Колченко Г. Ф. Розроблення нормативних документів для забезпечення функціонування системи оперативно-технічного управління телекомунікаційними мережами / Г. Ф. Колченко, І. В. Шестак // Наукові записки УНДІЗ. – 2012. – № 2(24). – С. 5-8.

26. Система управління сучасними телекомунікаційними мережами : монографія : у 2 ч. / [Кривуца В. Г., Беркман Л. Н., Климаш М. М. та ін.]. – Київ : ДУІКТ, 2009. – 268 с.

27. Шерстнева О. Г. Подходы к оценке качества управления связью / О. Г. Шестернева // Сети и системи связи. – 2008. – №11. – С. 35-41.

28. Стеклов В. К. Проектування телекомунікаційних мереж / В. К. Стеклов, Л. Н. Беркман. ; під ред. В. К. Стеклова – Київ : Техніка, 2002. – 792 с.

29. Кульгин М. Технология корпоративных сетей / М. Кульгин. – Санкт- Петербург : Питер, 1999. – 704 с.

30. Шварц М. Сети связи: протоколы, моделирование и анализ / М. Шварц. – ч.2. – Москва : Наука, 1992. – 272 с.

31. What is SD-WAN (Software-Defined Wide Area Network)? [Електронний ресурс]. – Режим доступу: https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/ – Назва з екрану. – Дата звернення: 12.11.2020.

32. SD-WAN vs MPLS: The Pros and Cons of Both Technologies)? [Електронний ресурс]. – Режим доступу: https://www.sdxcentral.com/networking/sd-wan/definitions/sd-wan-vs-mpls-pros-cons-technologies/ – Назва з екрану. – Дата звернення: 18.11.2020.

33. Cisco Software-Defined WAN (SD-WAN) FAQ [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sw-defined-wan-faq-cte-en.html?dtid=osscdc000283 – Назва з екрану. – Дата звернення: 18.11.2020.

34. Cisco Software-Defined WAN (SD-WAN) Cloud onRamp for Colocation At-a-Glance [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-on-ramp-aag-cte-en.html – Назва з екрану. – Дата звернення: 20.11.2020.

35. Draft-ietf-nvo3-geneve-08 [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/draft-ietf-nvo3-geneve-08 – Назва з екрану. – Дата звернення: 22.11.2020.

36. What Is Network Virtualization? [Електронний ресурс]. – Режим доступу: https://blog.gigamon.com/2018/01/04/network-virtualization-optimize/ – Назва з екрану. – Дата звернення: 22.11.2020.

37. Solving the Network Virtualization Conundrum [Електронний ресурс]. – Режим доступу: https://www.arista.com/en/solutions/network-virtualization – Назва з екрану. – Дата звернення: 23.11.2020.

38. Arregoces, Mauricio, and Maurizio Portolani. Data center fundamentals. Cisco Press, 2003

39. Long, James. Storage Networking Protocol Fundamentals. Pearson Education India, 2006.

40. F. Dad et al., “Optimal Path Selection Using Dijkstra’s Algorithm in Cluster-based LEACH Protocol,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 2, pp. 194–198, Feb. 2017.

41. Z. U. Rahman et al., “Investıgatıng the Pakıstan's Offshore Software Industry Infrastructure,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 3, pp. 237–243, Mar. 2017

42. Z. U. Rahman et al., “Magnetic Resonance Images Classification through Relevance Vector Machine,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 1, pp. 213–217, Jan. 2017

43. Membrey, Peter, Eelco Plugge, and David Hows. Practical Load Balancing: Ride the Performance Tiger. Apress, 2012.

44. Odom, Ccie Routing And Switching Exam Certi cation Guide, 4/E. Cisco press, 2004.

45. Kenyon, Tony. Data networks: routing, security, and performance optimization. Digital Press, 2002.

46. R. Froom, B. Sivasubramanian, and E. Frahim, Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide. Cisco press.

47. Popovic, Miroslav. Communication protocol engineering. CRC press, 2016. 277

48. J. Appl. Environ. Biol. Sci., 7(3)268-278, 2017

49. S. Tim, Cisco Telepresence Fundamentals. Pearson Education India, 2010.

50. Tate, Jon, et al. IBM Flex System and PureFlex System Network Implementation. IBM, International Technical Support Organization, 2013.

ДОДАТКИ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Національна академія наук України
Університет імені П'єра і Марії Кюрі (Франція)
Маріборский університет (Словения)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Шяуляйська державна колегія (Литва)
Жешувський політехнічний університет ім. Лукасевича (Польща)
Білоруський національний технічний університет (Республіка Білорусь)
Міжнародний університет цивільної авіації (Марокко)
Національний університет біоресурсів і природокористування України (Україна)
Наукове товариство ім. Шевченка
ГО «Асоціація випускників Тернопільського національного технічного університету імені Івана Пулюя»

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

Том ІІ

ІХ Міжнародної науково-технічної конференції молодих учених та студентів

25-26 листопада 2020 року

УКРАЇНА
ТЕРНОПІЛЬ – 2020

УДК 004.72

Д.В. Мурза, Ю.О. Круглик, С.В. Марценко, канд. техн. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

МЕТОДИ ТА ЗАСОБИ ОПТИМІЗАЦІЇ РОБОТИ МЕРЕЖ РІЗНОГО ПРИЗНАЧЕННЯ

D.V. Murza, Y.O. Kruhlyk, S.V. Martsenko, Ph.D., Assoc.

METHODS AND MEANS OF DIFFERENT PURPOSES NETWORKS OPTIMIZATION

Методи та засоби оптимізації сучасних мереж різного призначення покликані вирішити ряд питань пов'язаних з масштабованістю, швидкодією, забезпеченням необхідних пропускних здатностей, захищеністю мережевих ресурсів, що в свою чергу підвищує рівень задоволеності користувачів цих послуг. Сучасні мережеві архітектури в великій мірі враховують статичні моменти цих показників, проте мають певні недоліки в динамічних середовищах де адаптація до нових умов повинна проходити у відповідності до змін.

Запропоновані методи та засоби оптимізації роботи мереж повинні включати:

- можливість віртуалізації мережевих ресурсів для гнучкого управління;
- розгортання ієрархічних надбудов для управління віртуалізованими мережами;
- засоби організації переходу до новітніх підходів управління мережами.

Віртуалізація мережевих ресурсів дає змогу утворювати набори фізичних пристроїв, що працюють як один елемент, що в свою чергу підвищує продуктивність роботи та збільшує протидію різного роду атакам на мережеві пристрої. Використання протоколів віртуалізації надає змогу використовувати стандартизовані механізми оптимізації роботи мережевих компонентів та швидке розгортання відповідних технічних рішень.

Іншим підходом до оптимізації є використання концепції програмно-конфігурованих мереж (Software Defined Networks). При цьому, вся мережа віртуалізується і керується з однієї точки, що виконує роль контролера. Такий підхід суттєво спрощує реплікацію однотипних налаштувань пристроїв, створення карти шляхів та управління потоками даних. За допомогою програмних застосунків існує можливість динамічно керувати інформаційними потоками з врахуванням змін у стані мережевих компонентів та оперативно реагувати на завантаженість чи збої в роботі. Використання контролера управління мережею дає змогу здешевити мережеве обладнання, оскільки набір функцій суттєво зменшується і переноситься на інший пристрій. Комутатори та маршрутизатори виконують команди контролера і їх функція зводиться до передавання з порту на порт.

Надбудова, що має назву віртуалізації мережевих функцій (Network Function Virtualization) це мережева архітектура, що передбачає віртуалізацію цілих класів процесів мережевих вузлів, що може бути об'єднана в ланцюг для забезпечення певного сервісу. Оптимізація роботи мережі також можлива через відхід від принципу передавання від вузла до вузла і перехід до інформаційно центрованих мереж (Information Centric Networks). Цей новий підхід дає змогу зосередитись на передаванні інформації як цінності і оптимізовувати мережеві ресурси у відношенні до запитів користувачів. Розглянуті методи та засоби оптимізації роботи мереж дають змогу будувати гнучкі та надійні мережеві рішення, що покликані максимально задовольняти потреби користувачів.

УДК 004.72

Д.В. Мурза, Ю.О. Круглик, С.В. Марценко, канд. техн. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ДОСЛІДЖЕННЯ ВПРОВАДЖЕННЯ НОВИХ ПОСЛУГ У МЕРЕЖАХ ОПЕРАТОРІВ ЗВ'ЯЗКУ ТЕХНОЛОГІЇ 5G

D.V. Murza, Y.O. Kruhlyk, S.V. Martsenko, Ph.D., Assoc.

RESEARCH OF NEW SERVICES IMPLEMENTATION IN THE 5G TECHNOLOGY NETWORK OPERATORS

Розвиток сучасних технологій мобільного зв'язку надав суттєвий поштовх до впровадження та розширення наборів послуг для користувачів. В свою чергу це створило нові очікування якості, надійності, стабільності та об'єму сервісів, що надаються абонентам. Впровадження нових технологій в світі відбувається дуже швидкими темпами через кращу підготовленість як в технологічному плані, так і в фінансовому. Перспективи розгортання технології наступного покоління 5G в Україні потребують додаткового дослідження як в питаннях технічної можливості так і в обгрунтуванні доцільності впровадження нових послуг, що дадуть змогу в повній мірі використати усі її переваги.

Для вирішення поставлених завдань необхідно провести дослідження наступних аспектів:

- наявної ситуації частотного спектру для впровадження технології 5G;
- технічної підготовленості операторів мобільного зв'язку та економічної доцільності;
- провести аналіз наборів послуг, що надаються абонентам та перспектив їх покращення при використанні нової технології;
- можливості використання нових мереж в застосунках типу «Розумне місто», «Розумна країна» і т.д.

Якщо говорити про частотний спектр в Україні, то можна побачити, що на низьких частотах 900 МГц питання перерозподілу не вирішене до кінця, що ускладнює їх використання для цілей технології 5G. Використання високих частот призведе до виникнення труднощів покриття з перешкодами (будівлі, дерева, тощо). Таким чином, першим завданням при запровадженні нових послуг технології 5G повинно стати забезпечення необхідних частотних діапазонів відповідного рівня покриття. Аналізуючи ситуацію з покриттям технологіями 3G/4G, виникає картина недостатнього покриття операторами зв'язку віддалених регіонів, що також може ускладнити доцільність впровадження нових рішень, оскільки абоненти не будуть готові до їх використання. В такому світлі спостерігається певна непослідовність в діях наших телеком операторів, що до кінця не вирішивши попередні питання і взявшись за впровадження майбутніх технологій, можуть не отримати очікуваних результатів.

Одним з суттєвих поштовхів до впровадження технології наступного покоління 5G може стати правильне позиціонування переваг її використання. Оператори повинні надати відповідні набори послуг і підвищити економічну доцільність впровадження цієї технології задіявши механізми цифровізації країни, запропонувавши бізнес клієнтам спеціальні пакети послуг і створивши передумови до масового використання іншими абонентами.

Запровадження нових послуг операторами мобільного зв'язку технології 5G в Україні можливе при забезпеченні рівності доступу до технологій 3G/4G та розробці пакетів послуг, що уможливить отримання суттєвих доходів.