МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ

Кафедра Комп'ютерних систем та мереж

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____Ігор ЖУКОВ
« ____ » _____ 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
"МАГІСТР"
ЗА СПЕЦІАЛЬНІСТЮ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

Тема: Комп'ютерна транспортна мережа муніципальної цифрової інфраструктури

Виконавець: Олександр БУЛАВЧИК

Керівник: Микола ГУЗІЙ

Нормоконтролер: Василь МАЛЯРЧУК

Засвідчую, що у кваліфікаційній роботі
немає запозичень із праць інших авторів
без відповідних посилань
Студент: _____Олександр БУЛАВЧИК

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж
Напрям (спеціальність) 123 "Комп'ютерна інженерія"
(шифр, найменування)

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерних систем та мереж
_____Ігор ЖУКОВ
« ____ » _____ 2023 р.

З А В Д А Н Н Я
на виконання кваліфікаційної роботи

Булавчика Олександра Сергійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема роботи: Комп'ютерна транспортна мережа муніципальної цифрової інфраструктури
затверджена наказом ректора від "29" серпня 2023 року № 1521/ст.

2.Термін виконання роботи: з 02.10.2023 до 31.12.2023

3.Вихідні дані до роботи: Метод та підходи до побудови мережі, схема архітектури транспортної мережі, схеми модулів, шаблони налаштувань, демонстраційний прототип мережі, рекомендації по апаратній частині

4.Зміст пояснювальної записки:
Опис необхідних мережевих технологій; метод побудови муніципальних мереж, головні ідеї, технології та принципи; підхід до налаштування, прототип та апаратна база;

5.Перелік обов'язкового графічного матеріалу:
Таблиці, рисунки, діаграми, графіки, презентація *PowerPoint*

6. Календарний план

№ п/п	Етапи виконання кваліфікаційної роботи	Термін виконання етапів	Примітка
1	Сформулювати мету, визначитись з предметом кваліфікаційної роботи у відповідності із завданням	02.10.23-06.10.23	
2	Провести аналіз технічної документації та спеціальної літератури	07.10.23-18.10.23	
3	Провести аналіз потреб, перспектив та тенденцій галузі інформаційних технологій	19.10.23-25.10.23	
4	Написати перший розділ кваліфікаційної роботи щодо необхідних мережевих технологій	26.10.23-06.11.23	
5	Написати другий розділ кваліфікаційної роботи щодо основних ідей, принципів та підходів методу	07.11.23-17.11.23	
6	Створити симуляцію прототипу мережі для тестування ефективності пропонованих ідей	18.11.23-25.11.23	
7	Написати третій розділ кваліфікаційної роботи щодо шаблонів налаштування модулів, перевірки демонстраційного прототипу та рекомендацій до підбору апаратної бази	26.11.23-08.12.23	
8	Оформити пояснювальну записку до кваліфікаційної роботи	09.12.23-17.12.23	
9	Підготовити графічний демонстраційний матеріал	18.12.23-21.12.23	
10	Представити на кафедру та захистити роботу	22.12.23-31.12.23	

7. Дата отримання завдання «02» жовтня 2023 р.

Керівник кваліфікаційної роботи Микола ГУЗІЙ
(підпис)

Завдання прийняв до виконання Олександр БУЛАВЧИК
(підпис студента)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи “Комп’ютерна транспортна мережа муніципальної цифрової інфраструктури”: 91 сторінка, 28 рисунків, 4 таблиці, 29 використаних джерел, 3 додатки.

ТРАНСПОРТНА МЕРЕЖА, МЕТОД, МАСШТАБОВАНІСТЬ, МОДУЛЬНІСТЬ, ШАБЛОННИЙ ПІДХІД, ПРОТОТИП.

Мета кваліфікаційної роботи – розробити метод побудови транспортних мереж для вирішення актуальних проблем цифровізації муніципальної інфраструктури міст, сформулювати принципи та підходи що лежать в основі методу, надати схеми архітектури та логічної структури мережі побудованої за описаним методом.

Об’єкт дослідження - комп’ютерна муніципальна мережа.

Предмет дослідження – методи побудови ефективної транспортної мережі муніципальної цифрової інфраструктури.

Методи дослідження – методи системного аналізу, методи оптимізації.

Результати – в кваліфікаційній роботі розроблено метод побудови транспортних мереж муніципальної цифрової інфраструктури та надано рекомендації що-до його реалізації.

Наукова новизна одержаних результатів – запропоновано уніфікований метод побудови муніципальних мереж, в основі якого покладено ідеї масштабування та зменшення трудовитрат на супроводження.

Прогнози щодо розвитку об’єкта дослідження – побудова мережі на основі розробленого методу у середовищі *H3C Cloud Lab*, подальша симуляція та перевірка прототипу мережі. Даний метод рекомендується використовувати при розробці нових чи модернізації існуючих муніципальних мереж компаніями-інтеграторами повного циклу.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

MAC – *Media Access Control* (Нагляд за доступом до середовища, фізична адреса)

КМ – Комп'ютерна мережа

IPv4 – *Internet Protocol version 4* (Інтернет протокол версії 4)

L2/L3 – *Другий та третій рівні моделі OSI*

LAN – *Local Area Network* (локальная мережа)

WAN – *Wide Area Network* (широкомасштабна мережа)

MAN – *Metropolitan Area Network* (регіональна/міська мережа)

DHCP – *Dynamic Host Configuration Protocol* (Протокол динамічного налаштування хостів)

MPLS – *Multi Protocol Label Switching (багатопротокольна комутація по міткам)*

LDP – *Label Distribution Protocol (протокол розповсюдження міток)*

VLAN – *Virtual Local Area Network* (Віртуальна локальна мережа)

TCP/IP – *Transmission Control Protocol/Internet Protocol* (протокол управління передачею/межмережевий протокол)

PAgP/ LACP – *Port Aggregation Protocol* (Протокол агрегації каналу) та *Link Aggregation Control Protocol* (Протокол керування агрегацією каналу)

L2/L3 VPN – *L2/L3 Virtual Private Network (віртуальні приватні мережі рівню 2 та 3 моделі OSI)*

SSH – *Secure Shell* (Безпечна оболонка, технологія захищеного віддаленого підключення)

RRPP – *Rapid Ring Protection Protocol (Протокол захисту швидкого кільця)*

PE – *Provider`s edge* (пристрій на границі мережі *MPLS*,

провайдерський пристрій)

P – *Provider`s device* (Пристрій провайдера)

CE – *Customer Edge* (Пристрій користувача)

OSPF – *Open Shortest Path First* (відкритий протокол пошуку найкоротших маршрутів)

ACL – *Access Control List*, Список керування досутпом (СКД)

AS – *Autonomous System* (Автономна система)

ISP – *Internet Servece Provider* (Постачальник послуг інтернету)

AAA – *Authentication Authorization Accounting*

ВСТУП

Засоби зв’язку завжди відігравали важливу роль у розвитку людства, розпочинаючи від появи письма та методів його передачі до сучасних комп’ютерних мереж. Цей еволюційний шлях не лише сприяв комунікації серед представників людської цивілізації, але й об'єднував наші громади та сім'ї у єдиний інформаційний простір.

В сучасності складно уявити життя без телекомунікацій, наш світ зазнав значних змін та прогресу від винайдення радіо-зв’язку, за допомогою якого, стало можливим керувати процесами та об’єднувати групи людей, ці задачі здаються легкими, допоки між керівником, оратором чи лідером та групою людей не встає простір, який потрібно пройти, щоб лише передати повідомлення в одну сторону. Такий простір створює затримки, за яких може відбутися будь-що, люди втрачають зв’язок, бажання та потребу у спілкуванні, у глобалізаціїї, а це призводить до консерватизму, що сповільнює прогрес людства.

Сьогодні всі галузі нашого життя так чи інакше пов’язані із світом технологій, технологій зв’язку. Всі сфери життя, від магазинів, навігатора й пошти, до навчання, торгів і виробництва наразі користуються засобами сучасного зв’язку.

Комп’ютерні мережі бувають різних видів, розмірів, призначень, проте єдине залишається незмінним – всі вони призначені для полегшення взаємодії людства, обміну інформацією чи надання послуг. Великі мережі провайдерів інтернет-послуг існують для об’єднання інформаційного простору людства, малі персональні мережі – щоб вам було легко користуватися розумними речами навколо вас, корпоративні мережі – щоб потоки важливої інформації не зупинялися й допомагали заробляти більше.

Муніципальні мережі хоч і не є найважливішими, проте вони завжди займали особливе місце у світі телекомунікацій, даючи змогу цілим громадам користуватися перевагами розумного, цифровізованого міста:

– купівля білетів та поїздок громадського транспорту;

– записи на прийом до лікаря, адміністративної установи, тощо;

– зв’язок громади із ресурсами міністерств;

– спрощення взаємодії з комунальними підприємствами;

– оперативна взаємодія із оперативними службами міста;

– забезпечення державної відео-охорони;

– взаємодія із актуальними, синхронізованими із міністерством освіти електронними ресурсами інститутів, шкіл, дитячих садків;

– керування розумними дорожними перекрестями та переходами для оптимізації потоків автомобільного транспорту;

– та багато інших прикладів цифрової інфраструктури міст.

Муніципальні мережі загалом покращують рівень життя громади у місті, де таку мережу активно використовують та розвивають. Проте у галузі муніципальних мереж не існує визначеного підходу до їх побудови, через що більшість проєктів розробляється індивідуально з нуля, переслідуючи різні цілі, вирішуючи одні й тіж самі проблеми кожного разу знову. При чому не завжди проекти таких мереж розробляються із ціллю невпинно розвиватися разом із суспільством, а тому – деякі муніципальні мережі, які розроблялися лише як вирішення поточних потреб через деякий час будуть потребувати або значних змін, або повного перепроектування, що вимагає додаткових вливань муніципального бюджету.

В сучасній інфраструктурі досить розповсюдженою є значна застарілість архітектури *WAN* мереж, в яких використовується не просто застаріле обладнання, а застарілі методи побудови мереж та засоби передачі даних. Досить яскравим прикладом застарілості мереж – є українські міста, в яких чи не існує таких муніципальних мереж, що об’єднували б соціальну, державну інфраструктуру, чи така інфраструктура є надзвичайно застарілою, що будувалася десятиліття тому назад. Саме через таку застарілість та потребу у підключенні все більшої кількості інфраструктури до мережі (для збільшення ефективності керування, та якості послуг міської інфраструктури) в Україні вже досить давно проводиться цифровізація з метою поліпшення цифрової інфраструктури, в тому числі й муніципальної цифрової інфраструктури.

У галузі мереж муніципальної цифрової інфраструктури відсутні певні уніфіковані процеси, що б допомагали створювати подібні мережі, із вже закладеними в їх можливості ідеями невпинного розвитку та еволюції.

В даній роботі розглядається проблематика підходів до проєктування та створення мереж муніципальної цифрової інфраструктури. Висувається пропозиція використовувати певний уніфікований метод їх побудови, що за потреби буде доповнюватися новими технологіями чи вирішувати нові проблеми без необхідності в майбутньому перебудовувати всю інфраструктуру з нуля.

В межах магістерської роботи висунуто пропозицію використовувати уніфікований метод побудови комп'ютерних мереж муніципальної інфраструктури, що відповідає актуальній проблематиці існуючих муніципальних мереж – застарілим підходам, індивідуальне проєктування кожної мережі, вирішення переважно поточних проблем без поступової еволюції можливостей мережі як основної направленості. Запропонований метод включає в себе детальний опис актуальної проблематики, ідей що мають стати серцевиною вирішення актуальних питань, актуальних принцип модульної організації архітектури мережі з її поділом на рівні із висхідною залежністю за-для кращої масштабованості. Окремо у розробленому методі надається деталізований шлях вирішення проблеми зменшення трудовитрат на супроводження мережі використанням шаблонного підходу до налаштування ієрархічно поділених на рівні пристроїв.

Основними ідеями розробленого методу є ефективна масштабованість та зменшення трудовитрат на створення, підтримку та супроводження шляхом введення політики шаблонів налаштувань обладнання мережі. Масштабованість є центральною ідеєю методу як обов'язкова необхідність для кожної мережі муніципальної інфраструктури через специфіку постійного зростання послуг, що надаються населенню так і зростання самого населення, що в свою чергу провокує поступове збільшення навантаження на сферу послуг (в даній роботі – послуг муніципальної цифрової інфраструктури). Зменшення трудовитрат на реалізацію та супроводження мережі покликане не тільки для зменшення грошових витрат на весь проєкт, а й для

полегшення підготовки спеціалістів, що будуть виконувати роль мережевих інженерів підтримки та супроводження для муніципальних мереж.

Ефективна масштабованість за розробленого методу досягається декількома шляхами:

1) так як муніципальна інфраструктура в своїй основі генерує трафік, що не направлено до конкретних кінцевих користувачів та їх ПК, не вимагає великих об’ємів доступу до глобальної мережі, не створює стрибків пікового навантаження як це відбувається в користувацьких мережах – потреби у використанні деяких технологій організації транспортування зміщуються в сторону тих, що дозволяють краще обробляти та комутувати однорідний потік мало-об’ємної інформації;

2) серед технологій що описані як необхідні в розробленому методі використовується вкрай ефективна в своїй основі транспортна мережа *MPLS*, що в комбінації з технологією *L3VPN* дає змогу на мінімальній кількості обладнання створити надійну мережу для передачі ізольованого на незалежні потоки трафіку, без необхідності створювати складні маршрутизовані надійні мережі;

3) в якості технологій що дозволяють ефективно організувати з’єднання територіально розподіленої інфраструктури з транспортною мережею в розробленому методі пропонується використання комбінації ефективного з точки зору резервованих портів протоколу *RRPP* для об’єднання інфраструктури в кільця, а протокол *VRRP* для надійного підключення кілець інфраструктури до транспортної мережі *MPLS* із використанням найменшої можливої кількості пристроїв що задіяні в мережі із дотриманням кількості зарезервованих портів під потреби архітектури на мінімально необхідному рівні;

4) модульна архітектура мережі що запропоновано в розробленому методі, в свою чергу дозволяє спростити процес інтеграції нового обладнання до мережі шляхом розділення логічної залежності за ієрархічними рівнями обладнання й організувавши перетворення трафіку в мережі в декілька рівнів, що розділені у відповідності із модулями мережі для зменшення впливу на логіку функціонування пристроїв що додаються до мережі; 5) крім того специфіка використання необхідних технологій та модульної архітектури дозволяє керувати тим, який тип обладнання

буде найчастіше нарощуватися, що дає можливість усунути складні налаштування із такого роду пристроїв спростивши процес нарощення мережі.

Зменшення трудовитрат на побудову та супроводження як одна із ключових ідей розробленого методу досягається шляхом двох підходів до організації архітектури мережі:

1) фізична архітектура мережі поділена на чіткі модулі із висхідною залежністю, де модулі вищого рівня не залежать своїми налаштуваннями та процесами перетворення трафіку від модулів нижчого ієрархічного рівня, даний підхід спрощує процес підготовки нових спеціалістів з підтримки та супроводження мережі т.я. уніфікує всю мережу, об'єднуючи логічну структуру в межах модулів, які залишаються архітектурно незмінними в процесі еволюції мережі – така фізична структура дозволяє спеціалістам не витрачати час на вивчення постійно змінюваних та незалежних частин мережі й, загалом, зменшити необхідний рівень кваліфікації спеціалістів;

2) програмна (чи логічна) частина мережі також поділяється на незалежні частини – шаблони налаштувань у відповідності до ролі обладнання у мережі та його відношення до конкретного модуля фізичної архітектури, що дозволяє значно спростити процес налаштування та підтримки мережі, так як все обладнання в межах одного ієрархічного рівня матиме само-подібні налаштування, в яких наявні відмінності лише для спеціальних значень та параметрів – це дозволяє спеціалісту не аналізувати логіку функціонування кожного окремого пристрою а лише порівнювати її із існуючим шаблоном, а у разі необхідності додавання нового екземпляру обладнання – буде достатнім лише застосувати відповідний шаблон із введенням тільки специфічної для даного екземпляру інформації. Такі підходи до зменшення трудовитрат не тільки дозволяють зменшити складність робіт по супроводженню, що зменшує загальну необхідну кількість персоналу підтримки, а й спростити процеси налаштування та введення нового обладнання у експлуатацію, що зменшує необхідний рівень кваліфікації спеціалістів.

Окремо варто звернути увагу на те, що використана комбінація технологій в розробленому методі надає досить широкий спектр можливості керування якості

надаваних послуг (*QoS*) через наявну множинну інкапсуляцію на різних рівнях мережі разом із розділенням на різні категорії трафіку шляхом поділу на *VPN* зони що розділяють трафік та його маршрутну інформацію.

Мета роботи полягає у розробці уніфікованого методу побудови комп'ютерних мереж муніципального призначення, що вирішує:

1) питання необхідності індивідуального проєктування такого типу мереж,

2) питання масштабування, що зазвичай покладається в проєкт як обов'язкова частина, проте не є основою проєкту,

3) питання зменшення трудовитрат на супроводження проєктів даного масштабу.

Об'єктом наукового дослідження даної магістерської роботи є сфера комп'ютерних мереж та їх багатогранні проблеми, галузь мереж що призначені для об'єднання муніципальної цифрової інфраструктури.

Предметом дослідження є метод, ідеї та принципи що пропонують перспективний уніфікований підхід до побудови, організації та підтримки комп'ютерних мереж муніципальної цифрової інфраструктури.

Методологія дослідження включає в себе структурний, принциповий, програмний та оптимізаційний аспекти розробки методу із подальшою перевіркою описаних ідей, принципів та підходів на основі побудованого демонстраційного прототипу.

Дана робота вказує на важливість впровадження ефективних та актуальних технологій, нових підходів та поглядів до побудови муніципальних мереж. Метод, розроблений в даній роботі дозволяє створити уніфіковану муніципальну мережу, що постійно розвивається й здатна задовольнити потреби постійно зростаючих міст, а за потреби – така мережа може бути використана в майбутньому для впровадження й переходу до передових мережевих технологій та принципів їх організації, як наприклад для надсучасної технології *SDN*.

У результаті магістерського дослідження вдалося розробити ефективний метод побудови комп'ютерних мереж муніципальної цифрової інфраструктури що не лише

вирішує актуальні потреби у галузі муніципальних мереж, а й є основою для інтеграції новітніх мережевих технологій.

Розроблений метод зосереджено на вирішенні питань невпинного масштабування за зменшення трудовитрат на побудову та супроводження мережі.

Функціональність методу орієнтована на муніципальну цифрову інфраструктуру, що має відділені потоки спеціалізованої інформації від загальних публічних мереж.

Завдяки розробленому методу, важливий процес цифровізації зростаючих міст стане уніфікованим та матиме на меті постійне вдосконалення, щоб дотримуватися сучасних вимог та потреб у сфері громадських послух. Уніфікація дозволить в подальшому позбутися залежності від компаній інтеграторів, що супроводжують кожну мережу окремо від інших, й перейти до повного контролю над мережею у державну власність, де вже спеціалісти, що працюють на державу будуть виконувати впровадження, супроводження й адаптацію уніфікованих муніципальних мереж.

РОЗДІЛ 1
ОПИС НЕОБХІДНИХ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ

1.1. Комп'ютерна мережа, загальний огляд

1.1.1. Загальні положення комп'ютерних мереж

Комп’ютерною мережею (КМ), або мережею ЕОМ, називається комплекс територіально розподілених ЕОМ, зв’язаних між собою каналами передачі даних та мережевим програмним забезпеченням.

Іншими словами Комп’ютерна мережа – це система розподіленої обробки інформації, що складається щонайменше з двох комп’ютерів, поєднаних засобами зв’язку. Комп’ютерна мережа являє собою сукупність територіально рознесених комп’ютерів, здатних обмінюватися між собою повідомленнями через середовище передачі даних [1].

В загальному випадку КМ складається з сукупності вкладених одна в одну підсистем:

– мережа робочих станцій;

– мережа серверів;

– базова мережа передачі даних.

Комп’ютер набуває нової назви: робоча станція, сервер, комутаційний комп’ютер.

Мережа робочих станцій – зовнішня оболонка КМ. Вона представлена сукупністю робочих станцій та засобів зв'язку, що забезпечують взаємодію робочих станцій із сервером і, можливо, між собою. Робоча станція (клієнтська машина, робоче місце, абонентський пункт, термінал) – це комп'ютер, за яким безпосередньо працює абонент КМ.

Мережа серверів - сукупність серверів та зв'язку, які забезпечують підключення серверів до базової мережі передачі [1].

Комп'ютер, який виконує загальні завдання КМ і надає послуги робочим станціям, називають сервером.

Базова мережа передачі - сукупність засобів передачі даних між серверами. Вона складається з каналів зв'язку та вузлів зв'язку [1].

Вузол зв'язку - сукупність засобів комутації та передачі даних в одному пункті. Вузол зв'язку приймає дані, що надходять каналами зв'язку, і передає дані в канали, що ведуть до абонентів. Характерним прикладом вузла є автоматична телефонна станція. Зауважимо, що перша у світі електрична мережа – телефонна. Саме вона лягла в основу базової мережі передачі даних та багато в чому визначила принципи побудови КМ. Вузол зв'язку реалізується на основі комутаційного комп'ютера та апаратури передачі даних.

Комутаційний комп'ютер керує прийомом та передачею даних. Базова мережа передачі є ядром КМ, що забезпечує фізичне об'єднання комп'ютерів та інших пристроїв [1].

1.1.2. Класифікація комп'ютерних мереж

Найбільші особливості реалізації КМ можна простежити за запропонованими базовими класифікаційними ознаками [1].

Таблиця 1.1

Класифікація мереж

Признак класифікації	**Вид КМ**
Занята територія	Локальна; глобальна
Логіка з’єднань	З жорсткою логікою; з програмованою логікою
Кількість рівнів ієрархії	Одноріневa; багаторівнева
Апаратно-програмна платформа мережі	Однорідна; неоднорідна
Призначення	Загального призначення; спеціального призначення

За територіальною ознакою мережі поділяються на локальні (*Local Area Network, LAN*) та глобальні (*Wide Area Network, WAN*). До локальних відносять 13 мережі, організовані в межах істотно обмеженої території (кімната, поверх, будинок, сусідні будинки). Глобальні мережі сягають відстані від десятків до десятків тисяч

кілометрів, переплітаються між собою і можуть об'єднувати сотні локальних мереж [1].

Що-до логіки з’єднань, традиційно в локальних мережах використовувалася жорстка логіка з'єднань: спеціальний канал зв'язку стандартної топології (шина, кільце, зірка), тоді як у глобальних мережах - логіка з'єднань, що програмується (комутується). Саме тому як істотна відмінність локальних мереж від глобальних до недавнього часу називався тільки один шлях доставки інформації.

Глобальні мережі реалізують багаторівневий принцип організації мережі. У таких мережах кожен наступний (від користувача) рівень продає заявки попереднього. У цьому сенсі кожен комп'ютер попереднього рівня, що надсилає заявки на послуги, розглядається як клієнт, а кожен комп'ютер наступного рівня, що надає послуги клієнтам сервер. У однорівневих мережах той самий комп'ютер (стосовно інших) може бути і клієнтом, і сервером.

З моменту створення першої КМ змінилося два покоління комп'ютерів, різко зросла кількість їх виробників та конструктивних рішень. Це було об'єктивною причиною появи неоднорідних КМ. «Переродження» однорідних мереж у неоднорідні слід як природний результат еволюційного розвитку будь-якої КМ.

Залежно від призначення КС поділяють на КС загального та спеціального призначення. Спеціалізація сучасних КС зазвичай провадиться на прикладному рівні (за рахунок прикладних програм користувачів). Тим не менш, у військовій галузі та банківській сфері є безліч прикладів спеціалізації мереж за рахунок конструктивних рішень. Зазвичай спеціалізовані КС є «персональними» мережами організації або корпоративними мережами [1].

1.2. Технологія *Ethernet*

Ethernet - сімейство технологій пакетної передачі даних між пристроями для комп'ютерних та промислових мереж.

Стандарти *Ethernet* визначають кабельні з’єднання та електричні сигнали на фізичному рівні, формат фреймів та протоколи керування доступом до середовища —

на канальному рівні моделі *OSI*. *Ethernet* в основному описується стандартами *IEEE* групи 802.3 [2].

Назва «*Ethernet*» (буквально «ефірна мережа» або «середовище мережі») відображає початковий принцип роботи цієї технології: все, що передається одним вузлом, одночасно приймається рештою (тобто є якась схожість з радіомовленням). В даний час практично завжди підключення відбувається через комутатори (*switch*), так що кадри, що відправляються одним вузлом, доходять лише до адресата (виняток становлять передачі на широкомовну адресу) - це підвищує швидкість роботи і безпеку мережі.

У стандарті перших версій зазначено, що як передавальне середовище використовується коаксіальний кабель, надалі з'явилася можливість використовувати кручену пару та оптичний кабель. Причиною переходу на оптичний кабель була потреба збільшити довжину сегмента без повторювачів.

Метод управління доступом (для мережі на коаксіальному кабелі) - множинний доступ з контролем несучої та виявленням колізій (*CSMA*/*CD*), швидкість передачі даних 10 Мбіт / с, розмір кадру від 64 до 1518 байт, описані методи кодування даних. Режим роботи напівдуплексний, тобто вузол не може одночасно передавати та приймати інформацію. Кількість вузлів в одному сегменті мережі, що розділяється, обмежена граничним значенням в 1024 робочих станції. У 1995 році прийнятий стандарт *IEEE* 802.3*u Fast Ethernet* зі швидкістю 100 Мбіт/с і з'явилася можливість роботи в режимі повний дуплекс. У 1997 році був прийнятий стандарт *IEEE* 802.3*z Gigabit Ethernet* зі швидкістю 1000 Мбіт/с для передачі по оптичному волокну і ще через два роки для передачі по крученій парі [2].

1.2.1. Формат фрейму

Існує кілька форматів *Ethernet*-кадру.

- Початковий *Version I* (більше не застосовується).

- *Ethernet Version* 2 або *Ethernet*-кадр *II*, ще званий *DIX* (абревіатура перших літер фірм-розробників *DEC, Intel, Xerox*) - найбільш поширена і використовується до цього дня (рис. 1.1). Часто використовується безпосередньо протоколом Інтернет [2].

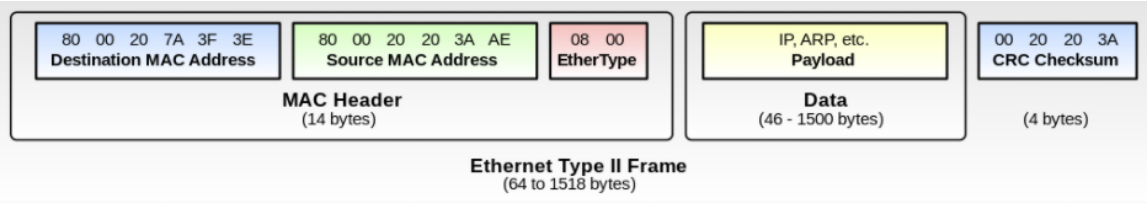

Рис. 1.1. Формат *Ethernet Version* 2 фрейму, 64-1518 байтів

– *Novell* — внутрішня модифікація *IEEE* 802.3 без *LLC* (*Logical Link Control*).

– Кадр *IEEE* 802.3 *LLC*.

– Кадр *IEEE 802.3 LLC/SNAP*.

*Я*к доповнення *Ethernet*-кадр може містити тег *IEEE* 802.1*Q* для ідентифікації *VLAN* (рис. 1.2), до якої він адресований, а в ньому *IEEE* 802.1*p* для вказівки на пріоритетність [2].

Різні типи кадру мають різний формат та значення *MTU*.

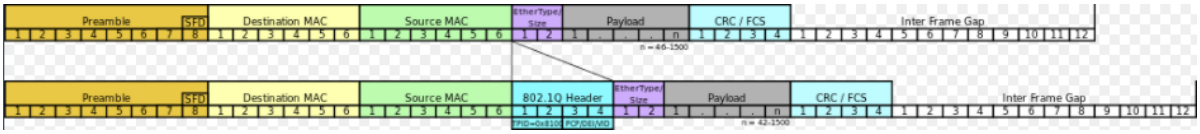

Рис. 1.2. Відмінність фрейму 802.1*Q* від фрейму *Version* 2

1.2.2. *MAC*-адреса

При проєктуванні стандарту *Ethernet* було передбачено, що кожна мережна карта (як і вбудований мережевий інтерфейс) повинна мати унікальний шестибайтовий номер (*MAC*-адреса), прошитий у ній при виготовленні. Цей номер використовується для ідентифікації відправника та одержувача кадру, і передбачається, що при появі в мережі нового комп'ютера (або іншого пристрою, здатного працювати в мережі) адміністратору мережі не доведеться налаштовувати *MAC*-адресу. Унікальність *MAC*-адрес досягається тим, що кожен виробник отримує в координуючому комітеті *IEEE Registration Authority* діапазон із шістнадцяти мільйонів (224) адрес, і в міру вичерпання виділених адрес може запросити новий діапазон. Тому за трьома старшими байтами *MAC*-адреси можна визначити виробника.

Існують таблиці, що дозволяють визначити виробника за *MAC*-адресою; зокрема, вони включені до програм типу *arpalert* [2].

MAC-адреса зчитується один раз з ПЗУ при ініціалізації мережевої карти, надалі всі кадри генеруються операційною системою. Усі сучасні операційні системи дозволяють змінити *MAC*-адресу. Для *Windows*, починаючи, як мінімум, з *Windows* 98, він змінювався у реєстрі. Деякі драйвери мережевих карток давали можливість змінити її в налаштуваннях, але зміна адреси працює абсолютно для будь-яких карток [2].

1.2.3. Технологія *GigabitEthernet* (1000*BASE-T*)

Залежно від швидкості передачі даних та передавального середовища існує кілька варіантів технології. Незалежно від способу передачі, стек мережного протоколу і програми працюють однаково практично у всіх випадках.

Гігабітний *Ethernet* (*Gigabit Ethernet*, 1 Гбіт/с), 1000*BASE-T, IEEE* 802.3*ab* - Основний гігабітний стандарт, опублікований в 1999р., використовує кручену пару категорії 5 та 5*e*. У передачі даних беруть участь 4 пари, кожна пара використовується одночасно для передачі по обох напрямках зі швидкістю - 250 Мбіт / с. Використовується метод кодування *PAM*5 (5-*level Phase Amplitude Modulation,* п'ятирівнева фазоамплітудна модуляція) з 4 лініями (4*D-PAM*5) та 4-мірною Трелліс-модуляцією (*TCM*), частота основної гармоніки - 62,5 МГц. Відстань - до 100 метрів.

1000*BASE-X* - загальний термін для позначення стандартів зі змінними приймачами у форм-факторах *GBIC* або *SFP* (оптично-волоконні кабелі) [2].

1.3. Комп'ютерна мережа муніципального призначення

Міська обчислювальна мережа (*metropolitan area network, MAN*) (від англ. «мережа великого міста») об'єднує комп'ютери в межах міста, являє собою мережу, за розмірами меншу, ніж *WAN*, але більшу, ніж *LAN*.

MAN застосовується для об'єднання одну мережу групи мереж, розташованих у різних будинках. У діаметрі така мережа може становити від 5 до 50 км. Як правило, *MAN* не належить будь-якій окремій організації, в більшості випадків її сполучні елементи та інше обладнання належить групі користувачів або провайдеру, хто бере плату за обслуговування. Про рівень обслуговування заздалегідь домовляються та обговорюють деякі гарантійні зобов'язання. *MAN* часто діє як високошвидкісна

мережа, щоб дозволити спільно використовувати регіональні ресурси (подібно до великої *LAN*). Це також часто використовується для забезпечення загальнодоступного підключення до інших мереж, використовуючи зв'язок з *WAN* [3].

В межах даної роботи під поняттям муніципальної мережі розуміється саме така мережа, що об’єднує в одну мережу групи мереж, що розташовані у різних будинках – інфраструктурних об’єктах. При чому саме для об’єднання міської інфраструктури, як наприклад: метро, ДНЗ, Школи, ВНЗ, відділки поліції, лікарні, камери міського відеоспостереження, тощо.

1.4. Трирівнева мережева архітектура

Трирівнева модель організації мережі компанії (ієрархічна модель мережі) вперше запропонована інженерами *Cisco Systems*. Поділяє архітектуру мережі на три рівня ієрархії з різними функціональними призначеннями: ядро мережі, рівень розподілу та рівень доступу (рис. 1.3).

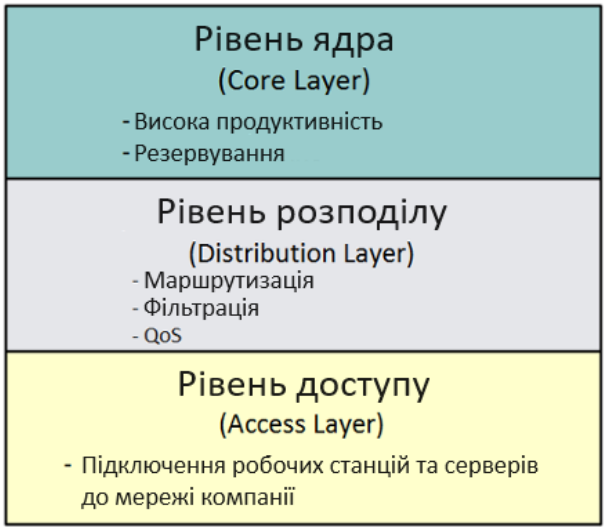

Рис. 1.3. Ієрархічна мережева модель
(трирівнева архітектура)

Рівень доступу слугує для підключення робочих станцій та серверів до мережі. У більшості випадків даний рівень представлено в мережі комутаторами другого рівня (але у деяких випадках – третього рівня). Зазвичай, для організації даного найпростішого рівня ієрархічної модулі використовуються оптимальні за ціною пристрої, що не вимагають складного налаштування. Основне призначення таких

пристроїв – забезпечити доступ кінцевим пристроям до наступного рівня ієрархії (рівня розподілу) [4].

Рівень розподілу, чи рівень робочої групи, розташовано між ядром мережі та рівнем доступу. На даному рівні вирішуються задачі агрегації широкорозсильних доменів та доменів маршрутизації, фільтрації та налаштування якості обслуговування (*QoS*), агрегації великих кабельних мереж в комутаційній шафі, забезпечення високого рівня доступності ядра для абонентів. На рівні розподілу використовуються маршрутизатори та/чи комутатори третього рівня.

Рівень ядра мережі представляє собою комплекс мережевих пристроїв (маршрутизаторів та комутаторів), що забезпечують резервацію каналів та високошвидкісну передачу даних між різними сегментами рівня розподілу. На даному рівні також реалізується функція забезпечення доступу до мережі Інтернет [4].

1.5. Технологія оптично-волоконних провідників даних

За використання звичних коаксіальних кабелів з часом постало питання – яким чином можливо збільшити пропускну здатність кабелю та збільшити дистанцію передачі даних? На це питання було дано відповідь – коаксіальний кабель не здатний до таких передач в силу своєї будови та фізичних законів. Тому йому на заміну прийшов кабель типу “Вита пара”, що є дешевшим, більш містким по пропускній здатності але все-ще з малою дальністю передачі даних – до 100м. Потрібно було шукати альтернативи, щоб прокладати лінії зв’язку на багато кілометів. Головною, і наразі популярною альтернативою став оптоволоконний кабель [5].

Оптоволоконний кабель — конструкція з одного або кількох ізольованих один від одного оптичних волокон, укладених в оболонку. Крім власне оптичних волокон і ізоляції може містити екран, силові елементи та інші конструктивні елементи. Також це фізичний медіум, що складається з певної кількості оптичних волокон, оточених спільною захисною оболонкою, та використовується для передачі світлового потоку.

Оптична кабельна лінія — лінія оптичних сигналів і складається з одного або декількох паралельних кабелів із з'єднувальними, стопорними та кінцевими муфтами (ущільненнями) та кріпильними деталями [5].

Оптичне волокно складається із:

– Серцевини;

– оптичної оболонки;

– захисного покриття;

– буферного покриття (опціонально).

Розрізняють одномодове і багатомодове волокно. Одномодове волокно (*SM*) найпоширеніших розмірів, буває: 8/125 і 9/125 мкм (це означає: діаметр серцевини — 8 мкм, діаметр волокна — 125 мкм тощо). Багатомодове (*MM*) найпоширеніших розмірів, буває: 50/125 і 62/125 мкм. Одномодове волокно дешевше за багатомодове, дозволяє передавати оптичний імпульс на великі відстані, з меншим розходженням сигналу на виході, але в той же час прямопередавальне устаткування для нього значно дорожче [5].

Основними перевагами оптоволоконного кабелю є швидкість передачі даних (швидкість носія даних – світла) та дистанція передачі даних – від 400м (ММ) до 300Км (*SM*) й більше. Хоча у даного провідника наявні два головних недоліки: при зламі провідника процес ремонту є трудомістким та вимагає дорогого обладнання, також проблемою є те, що вартість даного провідника є значно більшою за вартість кабельних провідників сигналу [5].

1.6. Інтерфейс *SFP*

SFP - промисловий стандарт модульних компактних приймачів (трансіверів), що використовуються для передачі та прийому даних у телекомунікаціях.

Модулі *SFP* (табл. 1.2) використовуються для приєднання плати мережевого пристрою (комутатора, маршрутизатора або подібного пристрою) до оптичного волокна або неекранованої кручений пари, що виступають в ролі мережевого кабелю. Модуль *SFP* прийшов на зміну громіздкішому модулю *GBIC*. Модуль має роз'єм, який

можна порівняти за розміром з роз'ємом 8*P*8*C*, тобто дозволяє на 1 юніті (1*U*) 19-дюймового телекомунікаційного обладнання розмістити до 48 оптичних портів (інтерфейсів) [6].

В основному, для підключення до модуля використовується один роз'єм типу *LC* або *SC* або два роз'єми *LC*. Оптичні модулі з одним рознімання мультиплексують сигнал, забезпечуючи дуплексну передачу по одному волокну. Такі модулі зазвичай містять у своїй назві маркування *Bi-Directional*, *BiDi*, або назву технології мультиплексування (*WDM, DWDM, CWDM*...). Також існують модулі з електричним інтерфейсом та роз'ємом *RJ*45 [6].

Таблиця 1.2

Різновиди *SFP*-модулів для волоконно-оптичних кабелів:

Довжина хвилі світлового променя – носія інформації	Максимальна відстань передачі даних	Позначення
850 нм	550 м	*MMF — SX*
1310 нм	10 км	*SMF — LX*
1550 нм	40, 80, 120 км	*EX, ZX, EZX (DWDM)*
1310/1550 нм	10 км	*SMF — BX*

1.6.1. Стандарт *SFP+*

SFP+ є розширеною версією приймача *SFP*, здатного підтримувати швидкості передачі даних від 4*Gbit/s* до 10 *Gbit/s*. *SFP+* було спочатку видано 9 травня 2006 р.; версія 4.1 було видано 6 липня 2009 р.

Звичайний модуль *SFP* не може бути використаний у роз'ємі *SFP+*, якщо інше не зазначено в специфікації обладнання. Для роз'ємів *X*2 є перехідники на один модуль *SFP+* або два модулі *SFP*. За рахунок малих габаритів кількість роз'ємів *SFP+* на стандартний 1*U* 19″ може бути значно більшою, ніж інших роз'ємів 10*G* [7].

1.6.2. Стандарт *QSFP*

QSFP служить інтерфейсом між платою мережевого пристрою (мережевої карти, комутатора, маршрутизатора) і трансівером, що найчастіше перетворює електричний сигнал на оптичний для передачі по оптоволокну. *QSFP* підтримується

безліччю виробників і дозволяє використовувати швидкості передачі від 40 Гбіт/с і більше (4 канали по 10 Гбіт/с кожен). Специфікація *QSFP* допускає використання *QSFP* з великими швидкостями, на травень 2013 року найшвидшим варіантом був *SFF*-8665 зі швидкістю 4*x*28 Гбіт/с (112 Гбіт/с) [8].

Модулі *QSFP* можуть використовуватися для передачі даних за протоколами *Ethernet*, *Fibre Channel*, *InfiniBand*, сумісні зі стандартами *SONET*/*SDH* з різними швидкостями. Приймачі *QSFP*+ можуть також використовуватися для передачі сигналів *Serial Attached SCSI*, 40 Гбіт *Ethernet*, *Infiniband QDR* (40 Гбіт/с) і *FDR* (56 Гбіт/с) *Infiniband* та інших. Модулі *QSFP* лише трохи ширші за модулі *SFP*/*SFP*+, і, порівняно з ними, дозволяють збільшити щільність портів у 3-4 рази.

Даний інтерфейс підключає мережевий пристрій (комутатор, маршрутизатор, медіаконвертер або подібний пристрій) до оптоволоконного або мідного кабелю [8].

Протокол безпечної оболонки *SSH*

SSH - мережевий протокол прикладного рівня, що дозволяє здійснювати віддалене керування операційною системою та тунелювання *TCP*-з'єднань (наприклад, для передачі файлів).

Схожий по функціональності з протоколами *Telnet* і *rlogin*, але, на відміну від них, шифрує весь трафік, включаючи паролі, що передаються [9].

1.7. Протокол динамічного налаштування вузлів *DHCP*

Для зв’язку між мережами очікується що кінцеві пристрої мають визначені *IP*-адреси. Але як кінцеві пристрої отримують дану інформацію? Їх можна налаштувати вручну, це трудомісткий процес, який часто призводить до помилок. Існує більш зручний спосіб: він називається *DHCP* [10].

Кожна мережа повинна мати *DHCP*-сервер, що відповідає за налаштування. Під час запуску, кожен комп’ютер має вбудовану в мережеву плату фізичну адресу, але не має *IP*-адреси. Для визначення своєї *IP*-адреси комп’ютер надсилає *Broadcast* повідомлення щоб встановити зв’язок з *DHCP*-сервером. Коли сервер отримує пакет, він виділяє вільний *IP*-адрес з певного адресного простору визначеного на сервері й відправляє пакет назад, кінцевому пристрою за його фізичним адресом. Постає

питання: на який час можливо виділити в автоматичному режимі *IP*-адресу з пулу? Якщо кінцевий пристрій покине мережу й не звільнить виділену адресу, то вона буде назавжди втрачена. Для запобігання таких втрат існує можливість видавати адреси на певний проміжок часу. Така технологія називається лізингом. Перед кінцем строку дійсності лізингу КП має надіслати до серверу запит о продовженні строку використання *IP*-адреси. Якщо такий запит не був надісланий чи у запиті відмовлено, КП не має права продовжувати використовувати виділену раніше адресу [10].

Протокол *DHCP* описано в стандартах *RFC* 2131 та 2132. Він широко використовується в Інтернеті для налаштування ряду параметрів (адреса шлюзу, адреса *DNS*-серверу, назва домену) й визначення *IP*-адрес. Окрім мереж підприємств та домашніх мереж, *DHCP* використовують інтернет-провайдери. З його допомогою вони налаштовують пристрої через інтернет-з'єднання, щоб абонентам не доводилось дізнаватися цю інформацію. Зазвичай з допомогою *DHCP* передаються дані про маску мережі, *IP*-адрес шлюзу за умовчанням, а також *IP*-адреса *DNS*-серверів та серверів часу [10].

Передача даних здійснюється за допомогою протоколу *UDP*. За замовчуванням запити від клієнта робляться до сервера на порт 67, сервер у свою чергу відповідає клієнту на порт 68, видаючи *IP*-адресу та іншу необхідну інформацію, таку, як мережеву маску, маршрутизатор і сервери *DNS* [11].

1.8. Віртуальні локальні мережі (*VLAN*)

Крім свого основного призначення – підвищення пропускної здатності з'єднань в мережі – комутатор дозволяє локалізувати потоки інформації в мережі, а також контролювати ці потоки й керувати ними, спираючись на механізм користувацьких фільтрів. Однак користувацький фільтр може заборонити передачу трафіку тільки по адресам, а *Broadcast*-трафік він передає всім сегментам мережі [12].

Технологія віртуальних локальних мереж (*Virtual LAN, VLAN*), дозволяє подолати вказане обмеження. Віртуальною мережею називається група вузлів мережі, трафік якої , в тому числі й *Broadcast*-трафік, на канальному рівні повністю ізольовано від інших вузлів мережі. Це означає, що передача фреймів між різними

віртуальними мережами на основі адреси канального рівня неможлива, незалежно від типу адреси – унікального, групового чи *Broadcast*-трафіу.

В той самий час, всередині віртуальної мережі фрейми передаються по технології комутації, тобто тільки на той порт, який зв'язаний з адресом призначення фрейму.

Призначення технології *VLAN* полягає в полегшенні процесу створення ізольованих мереж, які потім мають зв'язуватися за допомогою маршрутизаторів, що реалізують будь-який протокол мережевого рівня, наприклад *IP*. Така побудова мережі створює більш сильні бар'єри на шляху помилкового трафіку із однієї мережі в іншу. Технологія віртуальних мереж створює гнучку основу для побудови великої мережі, з'єднаної маршрутизаторами, так як комутатори дозволяють створювати повністю ізольовані сегменти програмним шляхом, не вдаючись до фізичної комутації [12].

Отже *VLAN* надає такі можливості:

– Логічне розподіл комутатора на кілька мереж, що не поєднуються між собою.

– Влаштування такого поділу на мережі з двома або більше комутаторами без вимоги проведення додаткових кабелів.

– Асиметричні *VLAN*. У цьому випадку порт (не *trunk*, по кабелю рухаються кадри без мітки 802.1*Q*) підключений до однієї внутрішньої *VLAN* комутатора з вхідних кадрів (вона називається *PVID*), і до більш ніж однієї внутрішньої *VLAN* комутатора з вихідних кадрів. При цьому може бути відсутнє підключення по вихідних кадрах до *PVID VLAN*. Також через даний пункт може бути реалізована і більш високорівнева абстракція *VLAN* інтерфейсів - *Promiscuous* / *Community* / *Isolated* порти. У цьому випадку використовується логічне вкладення кількох вторинних *VLAN* в одну первинну [12].

- *Promiscuous* порт (порт на первинній *VLAN*) може спілкуватися з будь-яким *Promiscuous*/*Community*/*Isolated* портом як у первинної, і будь-який вкладеної у ній вторинної *VLAN*.

- *Community* порт (порт на вторинній *VLAN*) може спілкуватися з будь-яким *Promiscuous* портом, а також з будь-яким *Community* портом в межах своєї вторинної *VLAN*.

- *Isolated* порт (теж порт на вторинній *VLAN*, але це спеціальна *isolated VLAN*, яка може бути тільки одна в даній первинній *VLAN*) може спілкуватися тільки з *Promiscous* портами, і не може спілкуватися навіть з іншими *Isolated* портами (функціонал «всі клієнти бачать сервер і не бачать один одного», часто використовується в «гостяних» *Wi-Fi* мережах).

- Дворівневе вкладення *VLAN* міток у кадрі, а також трансляція значень міток «на льоту». Ця технологія називається *QinQ*, і підтримується не у всіх пристроях з підтримкою *VLAN*.

1.9. Агрегація каналів передачі даних

1.9.1. Протоколи *PAgP* та *LAcP*

LACP — відкритий стандартний протокол агрегування каналів, описаний у документах *IEEE* 802.3*ad* та *IEEE* 802.1*aq*. Багато виробників для своїх продуктів використовують не стандарт, а патентовані або закриті технології, наприклад *Cisco* застосовує технологію *EtherChannel* (розроблену на початку 1990-х років компанією *Kalpana*[*en*]), а також нестандартний протокол *PAgP* [13].

Port Aggregation Protocol (*PAgP*) (Агрегування каналів) - пропрієтарний протокол компанії *Cisco Systems*, що служить для автоматизації агрегування фізичних *Ethernet* портів комутатора в один логічний (для маршрутизаторів є еквівалентна технологія – *Ling Aggregation Protocol*). Таке об'єднання дозволяє збільшувати пропускну здатність та надійність каналу.

Агрегування каналів може бути налаштовано між двома комутаторами, комутатором та маршрутизатором, між комутатором та хостом. Для агрегування каналів є інші назви: *port trunking* (у *Cisco trunk*'ом називається тегований порт, тому з цим терміном плутанини найбільше), *EtherChannel* (у *Cisco* так називається агрегування каналів, це може стосуватися як настроювання статичних агрегованих каналів, так і з використанням протоколів *LACP* або *PAgP*), *port channel, NIC bonding*.

За допомогою такої агрегації декількох з’єднань (лінків) група лінків отримуватиме спільні налаштування (всі налашьтування застосовані до групи автоматично налаштовуються на всіх лінках що входять до групи), крім того дана технологія забезпечує певний рівень надійності й відмово-захищеності, так як за поломки одного з лінків інші продовжать працювати.

Об’єднання (агрегація) каналів у єдиний логічний також дозволяє збільшити пропускну здатність так як навантаження рівномірно розподіляється по всім каналам що входять у єдину групу (а єдина група логічно є еквівалентною єдиному з’єданню)

1.9.2. Технологія *MC-LAG*

MC-LAG, або група агрегування каналу є типом групи агрегування каналу (*LAG*) із складовими портами, які завершуються на окремому комутаторі, перш за все з метою забезпечення резервування мережі у випадку, якщо один з комутаторів відмовляє чи вимкнено. Галузевий стандарт *IEEE* 802.1 *AX*-2008 для агрегування каналів не посилається на *MC-LAG*, але не виключає його. Його реалізація варіюється залежно від постачальника.

LAG є методом інверсного мультиплексування по декількох каналах локальних мереж, що збільшує пропускну здатність та надмірність. Це визначено стандартом *IEEE* 802.1 *AX*-2008, в якому описано наступне: «агрегування каналів дозволяє одному або декільком лінкам бути об'єднаними разом, для формування групи каналів, таким чином, щоб клієнт *MAC* міг обробити її, ніби це було поодиноке з'єднання». Канальний рівень доступу досягається за рахунок використання *LAG* разом з однією *MAC*-адресою для всіх портів пристрою групи. *LAG* може бути налаштований як статично, так і динамічно. Динамічна затримка використовує одноранговий протокол управління, званий протоколом управління агрегацією каналів (*LACP*). Цей протокол *LACP* також визначено у стандарті 802.1 *AX*-2008 [14].

1.10. Протокол захищеного кільця *RRPP* (*ERPS*)

RRPP (*ERPS*) - кільцевий протокол, що використовується для виключення утворення кілець у топології. Може бути заміною сімейства протоколів *STP*.

Принцип роботи наступний:

На всіх комутаторах, включених у фізичне кільце, призначається спеціальна *R-APS VLAN*, за якою передаватиметься службова інформація. Інші *VLAN*, що проходять по кільцю, перетворюються на *Protected VLANs*. Також вказуються *West*- та *East*-порти, причому *West* повинен дивитися на *East* і, відповідно, навпаки. Один з комутаторів (як правило, найдальший від входу в мережу, щоб вийшли дві приблизно рівні гілки) вибирається *RPL owner*'ом і один з його кільцевих портів призначається *RPL*-портом, на якому трафік блокуватиметься. Таким чином, якщо на одному з комутаторів на кільцевому порту зникає зв'язок, цей комутатор надсилає службове повідомлення про обрив через працюючий порт і таким чином сповіщає *RPL owner*'а, який, у свою чергу, включає порт, що не працює. При відновленні сигналу на порту, що впав, комутатор блокує його на час, зазначений у параметрі *WTR Time*, щоб при нестабільному сигналі з цього порту не доводилося постійно перебудовувати топологію [15].

Перевагою такого протоколу є простота реалізації на пристроях, що є розподіленими у просторі на великих відстанях один-від-одного. В межах даної роботи даний протокол використовується для організації рівня доступу мережі. рознесеними географічно пристроями. Саме через це в даній роботі не використовується протокол *STP*, за використання якого ефективним є формування надлишкових зв’язків, часто більше 2-х на пристрій, що значно збільшить вартість проекту за обставин, коли пристрої є рознесеними у просторі.

1.11. Протокол підвищення доступності маршрутизаторів *VRRP*

VRRP — мережевий протокол, призначений для збільшення доступності маршрутизаторів, що виконують роль шлюзу за умовчанням. Це досягається шляхом об'єднання групи маршрутизаторів в один віртуальний маршрутизатор і призначення групі пристроїв загальної *IP*-адреси, яка і використовуватиметься як стандартний шлюз для комп'ютерів в мережі [16].

Фактично, віртуальний маршрутизатор – це група інтерфейсів маршрутизаторів, які знаходяться в одній мережі та поділяють *Virtual Router Identifier* (*VRID*) та віртуальну *IP*-адресу. *VRRP*-маршрутизатор може перебувати у кількох

віртуальних маршрутизаторах, кожен із унікальною комбінацією *VRID*/*IP*-адресу. Відповідності між *VRID* та віртуальною *IP*-адресою мають бути однаковими на всіх маршрутизаторах в одній мережі. У будь-який момент часу лише один із фізичних маршрутизаторів виконує маршрутизацію трафіку, тобто стає *VRRP Master router*, решта маршрутизаторів у групі стає *VRRP Backup router*. *Я*кщо поточний *VRRP Master router* стає недоступним, його роль бере на себе один з *VRRP Backup* маршрутизаторів, той у якого найвищий пріоритет. Завдання пріоритету дозволяє визначити пріоритетніші шляхи адміністративно [16].

1.12. Технологія транспортної мережі *MPLS*

MPLS (багатопротокольна комутація за мітками) – механізм у високопродуктивній телекомунікаційній мережі, що здійснює передачу даних від одного вузла мережі до іншого за допомогою міток. *MPLS* є масштабованим та незалежним від будь-яких протоколів механізмом передачі даних.

У мережі, що базується на *MPLS*, пакетам даних присвоюються мітки. Рішення про подальшу передачу пакета даних іншому вузлу мережі здійснюється лише на підставі значення присвоєної мітки без необхідності вивчення самого пакета даних. За Завдяки цьому можливе створення наскрізного віртуального каналу, незалежного середовища передачі і використання будь-якого протоколу передачі даних [17].

Серед переваг технології виділяють:

– *MPLS* дозволяє легко створювати віртуальні канали між вузлами мережі;

– технологія дозволяє інкапсулювати різні протоколи передачі;

– незалежність від особливостей технологій канального рівня, таких як *ATM*, *Frame Relay*, *SONET*/*SDH* чи *Ethernet*;

– відсутність необхідності підтримки кількох мереж другого рівня, необхідні передачі різного роду трафіку. На вигляд комутації *MPLS* відноситься до мереж з комутацією пакетів.

Технологія *MPLS* ґрунтується на обробці заголовку *MPLS*, що додається до кожного пакету даних. Заголовок *MPLS* може складатися з однієї або кількох "міток". Декілька записів (міток) у заголовку *MPLS* - називаються стеком міток.

У *MPLS*-маршрутизаторі пакет з *MPLS*-міткою комутується на наступний порт після пошуку мітки в таблиці комутації замість пошуку таблиці маршрутизації. При розробці *MPLS* пошук міток та комутація за мітками виконувались швидше, ніж пошук за таблицею маршрутизації або *RIB* (англ. *routing information base* — інформаційна база маршрутизації), оскільки комутація може бути виконана безпосередньо на комутаційній фабриці замість центрального процесора. Маршрутизатори, розташовані на вході або виході *MPLS*-мережі, називаються *LER* (граничний маршрутизатор міток). *LER* на вході в *MPLS*-мережу додають мітку *MPLS* до пакета даних, а *LER* на виході з *MPLS*-мережі видаляє мітку *MPLS* з пакета даних [17].

Маршрутизатори, що виконують маршрутизацію пакетів даних, ґрунтуючись лише на значенні мітки, називаються *LSR* (англ. *label switching router* — комутуючий по мітках маршрутизатор). У деяких випадках пакет даних, що надійшов на порт *LER*, вже може містити мітку, тоді новий *LER* додає другу мітку пакет даних. Мітки між *LER* і *LSR* розподіляються за допомогою *LDP* (протокол розподілу міток). Для того, щоб отримати повну картину *MPLS*-мережі, *LSR* постійно обмінюються мітками та інформацією про кожен сусідній сайт, використовуючи стандартну процедуру. Віртуальні канали (тунелі), звані *LSP* (шляхи комутації міток), встановлюються провайдерами для вирішення різних завдань, наприклад, для організації *VPN* або для передачі трафіку через мережу *MPLS* по зазначеному тунелю. Багато в чому *LSP* нічим не відрізняється від *PVC* у мережах *ATM* або *Frame relay*, за винятком того, що *LSP* не залежить від особливостей технологій канального рівня. При описі віртуальних приватних мереж, заснованих на технології *MPLS*, *LER*, розташовані на вході або виході мережі, зазвичай називаються *PE*-маршрутизаторами (маршрутизатори провайдера) [17].

1.12.1. Динамічна організація шляхів за допомогою протоколу *LDP*

LDP (протокол розподілу міток) — протокол, за допомогою якого два *LER* (граничний маршрутизатор міток) у мережі *MPLS* обмінюються інформацією про відображення міток. Два *LER* називаються *LDP* бенкетами. Обмін інформацією між *LER* двонаправлений [18].

Протокол розподілу міток (*LDP*) надає *LSR* (маршрутизатор, що комутує мітки) засоби для запиту, поширення та випуску інформації про прив'язку префіксу мітки для однорангових маршрутизаторів у мережі. *LDP* дозволяє *LSR* виявляти потенційні однорангові вузли та встановлювати сеанси *LDP* із цими одноранговими вузлами з метою обміну інформацією про прив'язку міток. Іншими словами, *LDP* використовується для встановлення транспортних *LSP* (шляхи комутації міток) *MPLS*, коли керування трафіком не потрібно. Він встановлює *LSP*, які виконують існуючу таблицю *IP*-маршрутизації, і особливо добре підходить для створення повної мережі *LSP* між усіма маршрутизаторами в мережі. *LDP* може працювати в багатьох режимах відповідно до різних вимог; однак найбільш поширеним використанням є режим, який не запитується, який встановлює повну мережу тунелів між маршрутизаторами. У запитаному режимі вхідний маршрутизатор відправляє запит *LDP* маршрутизатору наступного переходу, як визначено з його таблиці *IP*-маршрутизації. Цей запит надсилається по мережі кожним маршрутизатором. Як тільки запит досягає вихідного маршрутизатора, генерується повідомлення у відповідь. Це повідомлення підтверджує *LSP* та повідомляє кожному маршрутизатору зіставлення міток для використання на кожному каналі для цього *LSP*. У незапитаному режимі вихідні маршрутизатори транслюють зіставлення міток для кожного зовнішнього каналу всім своїм сусідам. Ці широкомовні розсилки поширюються по кожному каналу в мережі, доки не досягнуть вхідних маршрутизаторів. На кожному етапі вони інформують *upstream* маршрутизатор про зіставлення міток, що використовується для кожного зовнішнього каналу, і шляхом лавинної розсилки мережі вони встановлюють *LSP* між зовнішніми посиланнями [18].

Основною перевагою *LDP* над *RSVP* є простота налаштування повної мережі тунелів з використанням непотрібного режиму, тому він найчастіше використовується в цьому режимі для установки базової мережі тунелів, необхідної для *VPN* рівня 2 і рівня 3.

1.12.2 Технології *L3VPN* та *L2VPN*

Технологія *MPLS* є популярною не тільки через можливість організувати транспортну мережу без використання маршрутизації, а й через можливості

організувати роздрібнене керування пересиланням категоризованого трафіку, що крім іншого може мати різні налаштування безпеки та *QoS*.

Технологія, що базується на основі транспортної мережі *MPLS* й дозволяє створити приватні віртуальні мережі (розділити з'єднання на незалежні категорії) називається *L3VPN*. Дана технологія працює наступним чином: кожному клієнту присвоюється власний ізольований ідентифікатор *VirtualRouting and Forwarding*, що дозволяє створювати окремі таблиці маршрутизації для кожного клієнта. При чому дані таблиці маршрутизації є можливим передавати між клієнтами з однієї віртуальної категорії за використання протоколу *MPBGP* (*BGP* версії 4).

Технологія *L2VPN*, як слідує з назви – дозволяє організувати ізольовану передачу трафіку на *L2* рівні мережі, при чому встановивши зв'язок на рівні *L2* між усіма абонентами однієї категорії *VPN*. Дана технологія дозволяє об'єднати на фізичному рівні інфраструктуру, що обов'язково має знаходитися в одній локальній *L2* мережі, але яку розподілено географічно.

L2VPN підтримує велике різноманіття технологій *L2* рівня, як наприклад: *Ethernet, Frame Relay, ATM* і т.п.

Логіка функціонування *L2VPN* через особливості зв'язку на *L2* рівні сильно відрізняється від звичайних міток *MPLS*: для організації зв'язку в межах однієї *broadcast*-мережі, необхідна наявна виділена лінія зв'язку, яку симулює *L2VPN* шляхом перепакування оригінального, поміченого *VLAN* (для розділу на *VPN* та категорії) фрейму інформації у дублюючий й подальша його передача як звичайного фрейму в іншу мережу. Саме дублюючий фрейм прийматиме змін за передачі даних по транспортній мережі, а коли дані надійдуть до межі віддаленої *broadcast*-мережі – оригінальний фрейм буде розпаковано й передано так, ніби-то пристрої знаходяться в справжній локальній *broadcast*-мережі.

1.13. Протокол динамічної маршрутизації *BGP*

BGP (протокол граничного шлюзу) протокол динамічної маршрутизації. Належить до класу протоколів маршрутизації зовнішнього шлюзу. На даний момент є основним протоколом динамічної маршрутизації в Інтернеті.

Протокол *BGP* призначений для обміну інформацією про досяжність підмереж між автономними системами, тобто групами маршрутизаторів під єдиним технічним та адміністративним управлінням, що використовують протокол внутрішньо-доменної маршрутизації для визначення маршрутів у собі та протокол міждоменної маршрутизації для визначення маршрутів доставки пакетів до інших АС. Передана інформація включає список АС, до яких є доступ через цю систему. Вибір найкращих маршрутів здійснюється з правил, прийнятих у мережі [19].

BGP підтримує безкласову адресацію та використовує сумування маршрутів для зменшення таблиць маршрутизації. З 1994 року діє четверта версія протоколу, всі попередні версії є застарілими. *BGP*, поряд із *DNS*, є одним із головних механізмів, що забезпечують функціонування Інтернету.

BGP є протоколом прикладного рівня та функціонує поверх протоколу транспортного рівня *TCP* (порт 179). Після встановлення з'єднання передається інформація про всі маршрути, призначені для експорту. Надалі передається лише інформація про зміни у таблицях маршрутизації. При закритті з'єднання видаляються всі маршрути, інформація про які передана протилежною стороною [19].

1.13.1. Списки контролю доступу та політики маршрутизації

Для контролю маршрутів що передаються та правил їх розповсюдження використовуються списки контролю доступу та політики маршрутизації (та *IP* -листи префіксів). Саме за допомогою даних технологій та протоколів забезпечується механізм безпеки та контролю з’єднань *BGP*. Без даних обмежень за допомогою протоколу *BGP* пристрій передаватиме всі відомі йому маршрути, що є шкідливим для функціонування мережі інтернет.

Крім того, в деякій мірі списки контролю доступу та політики маршрутизації доповнюють засоби контролю якості надання послуг (*QoS*).

1.13.2. Багатопротокольна версія *BGP*

Багатопротокольні розширення для *BGP* (*MBGP* або *MP-BGP*), які іноді називають *Multiprotocol BGP* або *Multicast BGP* і визначені в *IETF RFC* 4760, разом є розширенням *BGP*, яке дозволяє використовувати різні типи адрес (відомі як адресні сім’ї (*Address Families*)) для паралельного розподілу. У той час як стандартний *BGP*

підтримує лише одноадресні (*unicast*) адреси *IPv*4, багатопротокольний *BGP* підтримує адреси *IPv*4 та *IPv*6, а також одноадресні та багатоадресні варіанти кожного. Мультипротокольний *BGP* дозволяє обмінюватися інформацією про топологію *IP*-маршрутизаторів із підтримкою багатоадресної передачі окремо від топології звичайних одноадресних маршрутизаторів *IPv*4. Таким чином, це дозволяє використовувати топологію багатоадресної маршрутизації, відмінну від топології одноадресної маршрутизації. Незважаючи на те, що *MBGP* дозволяє обмінюватися інформацією про міждоменне багатоадресне пересилання, інші протоколи, такі як сімейство *Protocol Independent Multicast*, необхідні для побудови дерев і пересилання багатоадресного трафіку.

Багатопротокольний *BGP* також широко розгортається у випадку *MPLS L*3 *VPN*, щоб обмінюватися мітками *VPN*, отриманими для маршрутів із простору клієнтів через мережу *MPLS*, щоб розрізняти різні простори клієнтів, коли трафік з інших просторів клієнтів надходить до маршрутизатора провайдера (*PE*) [20].

1.14. Мережеве обладнання, комутатор та маршрутизатор

1.14.1. Комутатор

Мережевий комутатор - пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного або декількох сегментів мережі. Комутатор працює на канальному (другому) рівні мережевої моделі *OSI* [21].

Комутатори були розроблені з використанням мостових технологій та часто розглядаються як багато-портові мости. Для з'єднання кількох мереж на основі мережного рівня служать маршрутизатори (3 рівень *OSI*). На відміну від концентратора (1 рівень *OSI*), який поширює трафік від одного підключеного пристрою до всіх інших, комутатор передає дані лише безпосередньо одержувачу (виняток становить широкомовний трафік усім вузлам мережі та трафік для пристроїв, для яких невідомий вихідний порт комутатора). Це підвищує продуктивність і безпеку мережі, позбавляючи решту сегментів мережі необхідності (і можливості) обробляти дані, які їм не призначалися [21].

Комутатор зберігає у пам'яті таблицю комутації, у якій вказується відповідність вузла порту. При включенні комутатора ця таблиця порожня, і він працює у режимі навчання. У цьому режимі дані, що надходять на який-небудь порт, дані передаються на всі інші порти комутатора. При цьому комутатор аналізує кадри (кадри) і, визначивши *MAC*-адресу хоста-відправника, заносить його в таблицю на деякий час. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, *MAC*-адреса якого вже є в таблиці, цей кадр буде переданий тільки через порт, вказаний в таблиці.

Якщо *MAC*-адреса хоста-одержувача не асоційована з будь-яким портом комутатора, кадр буде відправлено на всі порти, за винятком того порту, з якого він був отриманий. Згодом комутатор будує таблицю для всіх активних *MAC*-адрес, у результаті трафік локалізується [21].

Існують декілька режимів комутації:

– З проміжним зберіганням (*Store and Forward*). Комутатор читає всю інформацію у кадрі, перевіряє його відсутність помилок, вибирає порт комутації і після цього посилає у нього кадр.

– Наскрізний (*cut-through*). Комутатор зчитує в кадрі тільки адресу призначення і виконує комутацію. Цей режим зменшує затримки передачі, але в ньому немає методу виявлення помилок.

– Безфрагментний (*fragment-free*) або гібридний. Цей режим є модифікацією наскрізного режиму, який частково вирішує проблему колізій. Теоретично пошкоджені кадри (зазвичай через зіткнень) часто коротше мінімального допустимого розміру кадру *Ethernet*, що дорівнює 64 байтам. Тому в цьому режимі комутатор відкидає кадри довжиною менше 64 байт, а решта після прочитання перших 64 байт у наскрізному режимі передає далі [21].

1.14.2. Маршрутизатор

Маршрутизатор або роутер (транслітерація англійського слова) - спеціалізований пристрій, який пересилає пакети між різними сегментами мережі на основі правил та таблиць маршрутизації.

Маршрутизатор може пов'язувати різноманітні мережі різних архітектур. Для прийняття рішень про надсилання пакетів використовується інформація про топологію мережі та певні правила, задані адміністратором [22].

Маршрутизатори працюють на «мережевому» (третьому) рівні мережевої моделі *OSI*, на відміну від комутаторів *L2* рівня *OSI* та концентраторів (хабів), які працюють відповідно на другому та першому рівнях моделі *OSI*.

Принцип роботи маршрутизаторів загалом наступний:

Зазвичай маршрутизатор використовує адресу одержувача, зазначену в заголовку пакета, і визначає за допомогою таблиці маршрутизації шлях, яким слід передати дані. Якщо в таблиці маршрутизації адреси немає описаного маршруту — пакет відкидається [22].

Існують інші способи визначення маршруту пересилання пакетів, коли, наприклад, використовується адреса відправника, використовувані протоколи верхніх рівнів та інша інформація, що міститься в заголовках пакетів мережного рівня. Нерідко маршрутизатори можуть здійснювати трансляцію адрес відправника і одержувача, фільтрацію транзитного потоку даних на основі певних правил з метою обмеження доступу, шифрування/розшифровування даних і т.д. [22].

Що-до таблиці маршрутизації:

Таблиця маршрутизації містить інформацію, на основі якої маршрутизатор приймає рішення про подальше пересилання пакетів. Таблиця складається з деякого числа записів — маршрутів, у кожному з яких міститься ідентифікатор мережі одержувача (що складається з адреси та маски мережі), адреса наступного вузла, якому слід передавати пакети, адміністративна відстань — ступінь довіри до джерела маршруту та деяка вага запису — метрика.

Метрики записів у таблиці грають роль обчисленні найкоротших маршрутів до різних одержувачам. Залежно від моделі маршрутизатора і протоколів маршрутизації, що використовуються, у таблиці (рис. 1.4) може міститися деяка додаткова службова інформація [22].

```
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
```

Рис. 1.4. Таблиця маршрутизації певного маршрутизатора

Таблиця маршрутизації може складатися двома способами:

1) Статична маршрутизація - коли записи в таблиці вводяться і змінюються вручну. Такий спосіб вимагає втручання адміністратора щоразу, коли відбуваються зміни у топології мережі. З іншого боку, він є найбільш стабільним і вимагає мінімум апаратних ресурсів маршрутизатора для обслуговування таблиці [22].

2) Динамічна маршрутизація - коли записи в таблиці оновлюються автоматично за допомогою одного або декількох протоколів маршрутизації - *RIP*, *OSPF*, *IGRP*, *EIGRP*, *IS-IS*, *BGP*, та ін.

Крім того, маршрутизатор завжди будує таблицю оптимальних шляхів до мереж призначення на основі різних критеріїв - кількості проміжних вузлів, пропускної спроможності каналів, затримки передачі даних і т. п.

Критерії обчислення оптимальних маршрутів найчастіше залежать від протоколу маршрутизації, а також, метрики є можливим задавати через налаштування конфігурації маршрутизатора. Такий спосіб побудови таблиці дозволяє автоматично тримати таблицю маршрутизації у актуальному стані та обчислювати оптимальні маршрути на основі поточної топології мережі. Однак динамічна маршрутизація надає додаткове навантаження на пристрої, а висока нестабільність мережі може призводити до ситуацій, коли маршрутизатори не встигають синхронізувати свої таблиці, що призводить до суперечливих відомостей про топологію мережі в різних її частинах і втрату даних [22].

1.15. Технологія *NAT*

Маршрутизація в комплексній мережі здійснюється на основі тих адрес призначення, які розміщені в заголовку пакетів. Як правило, ці адреси залишаються незмінними з моменту їх формування відправником й до моменту надходження на вузол призначення. Однак із цього правила є виключення. В широко використовуваній сьогодні технології трансляції мережевих адрес (*Network Address Translation, NAT*) передбачено пересування пакету у зовнішній, глобальній мережі на основі адрес, що відрізняються від використовуваних для маршрутизації пакетів у внутрішній корпоративній, муніципальній чи навіть локальній мережі [12].

Одною із найбільш популярних причин використання технології *NAT* є дефіцит публічних *IP*-адрес. Якщо по будь-яким причинам компанії інтегратору, підприємству, чи окремому користувачу у якого є потреба підключення до інтернету не вдається отримати від постачальника послуг необхідну кількість глобальних *IP*-адрес, то воно може скористатися технологією *NAT*. В даному випадку для адресації внутрішніх вузлів використовуються спеціально зарезервовані для даних цілей приватні пули адрес:

– великі *WAN* мережі: 10.0.0.0-10.255.255.255;

– *WAN* мережі провайдерів: 172.16.0.0-172.31.255.255;

– *MAN* та *LAN* мережі: 192.168.0.0-192.168.255.255;

Дані діапазони адрес зіставляють великий адресний простір, достатній для нумерації вузлів мереж практично будь-яких розмірів. Ці адреси виключені із більшості централізовано-розподілених, це означає, що пакети з даними адресами призначення будуть відкинуті маршрутизаторами на магістралях Інтернету. Для того щоб вузли з приватними адресами могли зв’язуватися між собою чи з вузлами що мають глобальний адрес через Інтернет – є необхідним використовувати технологію *NAT* [12].

Потреба у використанні трансляції адрес виникає і тоді, коли підприємство із поглядів безпеки бажає приховати адреси вузлів внутрішньої мережі, щоб не дати можливості зловмисникам зіставити план, вирахувати структуру і масштаб своєї мережі. В даному випадку технологія *NAT* також виявляється корисною [12].

1.16. Технології *AD-VPN, GRE* та *IPSec*

AD-VPN - це технологія, що призначена для створення зашифрованих *VPN* з'єднань між користувачами та корпоративною мережею. Вона існує для забезпечення безпеки та конфіденційності під час віддаленого доступу до ресурсів компанії. Дана технологія працює за принципом хабу та вітів – пристрої, що зберігають інформацію про шляхи до вітів називаються хабами, саме вони є центрами з'єднань для технології *AD-VPN*, більша частина налаштувань відбувається саме в них. Віти, в свою чергу – це пристрої яким необхідно встановити тунельоване, захищене підключення до іншого пристрою-віти по мережі, що не гарантовано є незмінною. Крім того – використання хабів дозволяє централізувати управління безпекою підключень й дозволяє ефективніше аналізувати стан існуючих чи проблемних підключень.

AD-VPN в основному використовує тунелі *GRE* (*Generic Routing Encapsulation*), які дозволяють з'єднувати віддалених користувачів з центральною мережею. Дана технологія створює віртуальний канал для безпечної передачі даних через ненадійні мережі, що забезпечує високу конфіденційність та цілісність інформації. Проте серед недоліків саме такого типу тунелів – відсутність вбудованих механізмів шифрування та аутентифікації інформації, що передається по тунелю, дана технологія працює на рівні маршрутизації й зазвичай використовуєтсья в комбінації з технологією захищених тунелів *IPSec*.

Тунелі, що будуються з використанням технології *IPSec* в свою чергу мають декілька переваг над *GRE*, оскільки включають в себе механізми надійного шифрування, аутентифікації та контролю цілісності даних (*AAA*). Це надає значно вищий рівень безпеки, захищаючи від несанкціонованого доступу інформацію, що пересилається через тунель.

Висновки за розділом

Мережеві технології та методи їх впровадження невпинно розвиваються, забезпечуючи світу все більше можливостей для створення та вдосконалення мереж. Різноманіття технологічних рішень широко відображає динаміку цього розвитку,

роблячи шляхи створення та ефективного впровадження мереж все більш варіативними. Цей постійний прогрес дозволяє створювати ефективні мережі, які задовольняють різноманітні потреби у сфері комунікаційних архітектур.

Кількість протоколів та технологій, використовуваних у будівництві, проєктуванні та реалізації мереж, відображає конкурентний характер цієї галузі та швидкий ріст попиту на мережеві підключення. Розмаїття комп'ютерних мереж, поділених за розмірами, призначенням та засобами передачі даних, стало повноцінною галуззю науки з власними дослідницькими інститутами та установами стандартизації.

Спеціалісти з розробки, підтримки, впровадження та розвитку мереж стають невід'ємною частиною сфер бізнесу, науки, розваг та послуг. Зростання числа користувачів мереж та збільшення потреб у існуючих мережах свідчать про важливість цієї галузі. Мережі не лише перспективні, але і актуальні в сучасному світі.

У цьому розділі кваліфікаційної роботи детально розглянуто важливі та необхідні технології для побудови муніципальних мереж. Велика кількість стандартів, протоколів та сервісів у сфері мереж відкриває широкі можливості, але велика конкуренція серед компаній, які надають мережеві послуги, підкреслює важливість та високий попит на розширення цього сегменту ринку. Лідерами у цій галузі на території України залишаються компанії *Cisco* та *HP* (*Hewlett-Packard*), які своїми прибутками що постійно зростають та щорічними технологічними нововведеннями ілюструють перспективи та динаміку розвитку мережевих технологій.

РОЗДІЛ 2
МЕТОД ПОБУДОВИ МУНІЦИПАЛЬНИХ МЕРЕЖ, КЛЮЧОВІ ІДЕЇ, ТЕХНОЛОГІЇ ТА ПРИНЦИПИ

2.1. Опис головної ідеї методу побудови транспортних мереж

Дана робота має на меті опис методу до побудови комп'ютерних транспортних мереж муніципальної цифрової інфраструктури. В даному розділі описується проблематика існуючих мереж та запропоновано ідеї та підходи з метою зменшення трудовитрат та збільшення ефективності масштабування.

2.1.1. Проблематика існуючих мереж

З плином часу більшість міст, як і їх населення, зростають, відповідно зростають й потреби населення цих міст, серед яких – потреба у якісних послугах зв'язку.

Застарілі методи комунікації заміщаються новими, все більше абонентів підключаються до світової мережі, а тому – необхідні ефективні рішення, що задовольняють потреби в якості, масштабованості та низькій вартості підключення. Для мереж муніципальної цифрової інфраструктури головною задачею є надання доступних послуг якомога більшій кількості абонентів, як наприклад абонентам: дошкільних, середніх та вищих навчальних закладів, лікарень, відеоспостереження, державних інститутів, об'єктів та сервісів.

Саме така транспортна мережа, яка об'єднує інфраструктуру міста, розробляється, змінюється, вдосконалюється та перероблюється – досить часто не проєктується із увагою на майбутнє масштабування та постійне супроводження. Мережі, що об'єднують державну інфраструктуру зазвичай розробляються незалежними підприємствами-інтеграторами у відповідь на державне замовлення, яке в свою чергу зазвичай обмежується вирішенням поточних проблем чи задач, без орієнтації на невплинний розвиток. Такий підхід не є ефективним, так як в своїй основі не враховує невплинний ріст кількості користувачів, разом з яким, паралельно, має невпинно розвиватися й інфраструктура.

Необхідність покладеної в проєкт масштабованості обумовлена тим, що за певного моменту, коли кількість користувачів досягає певного критичного значення – мережа, яку не орієнтовано на паралельне зростання разом із кількістю користувачів, потребує серйозної модернізації, заміни чи перепроєктування.

Дані процеси є як трудомісткими, а отже – часовитратними й вимагаючими залучення кваліфікованих спеціалістів, так і досить дорогими.

Для вирішення даної проблеми необхідно з самого початку підходити до проектування такої мережі, що має у своїй основі – здатність до ефективного масштабування та супроводження. Саме метод до побудови такої мережі й буде описано далі.

2.1.2. Варіанти вирішення проблеми масштабування

Проблему масштабування транспортних мереж муніципальної цифрової інфраструктури можна вирішити двома шляхами: 1) сучасним та ефективним, але дорогим та вкрай вибагливим; 2) відносно застарілим, який є надійним й перевіреним, хоча й вимагає більшої кількості персоналу підтримки.

Перший шлях – використовувати технології *SDN*, надсучасні принципи та апаратуру, що дозволяють створити, налаштувати, керувати та слідкувати за мережею, яка будується на основі вже існуючої мережевої інфраструктури. Керування, налаштування та моніторинг відбувається максимально централізовано – через використання спеціальних апаратних засобів, які містять в собі всі налаштування та є центрами керування мережею. Даний шлях є перспективним, але має критичні недоліки, які найбільш актуальні для міст, які тільки починають цифровізуватися, чи тільки почали нарощувати мережеву інфраструктуру. До таких міст відноситься, як наприклад, місто Київ. Серед даних недоліків – пряма залежність від вже існуючої інфраструктури й висока вартість придбання спеціалізованого обладнання та підписок програмного забезпечення. Місцеві мережі більшості міст світу не є сучасними, здатними забезпечити користувачів гігабітним інтернетом, або навіть в деяких містах далеко не вся державна інфраструктура має підключення до глобальної мережі. А використання *SDN* вимагає підключення сучасного обладнання до вже існуючої мережі, щоб використовуючи її – налаштувати та об’єднати

обладнання у нову мережу. Якщо ж вже існуюча мережа є застарілою – переваги *SDN* втрачаються й виникає потреба у побудові нової мережевої інфраструктури, що усуває одну із основних переваг *SDN* й мало чим відрізняє процес введення в експлуатацію *SDN* від звичайної розробки нової мережі. Зважаючи на це – доцільно буде розглянути саме варіант, за якого розробка нової мережі є основою підходу.

Другий шлях – шлях розробки нової мережевої інфраструктури на основі модульної, розподіленої організації з використанням класичних методів керування та підтримки мережі. Даний шлях включає в себе розробку такої мережі, коли керування апаратним забезпеченням відбувається за допомогою налаштувань кожного окремого екземпляру обладнання (класичний підхід), саме це й є головним недоліком даного шляху у порівнянні з *SDN*. Але дану проблему можна звести до мінімуму поєднавши модульну організацію мережі з шаблонним підходом до налаштування обладнання в середині модулів й інтеграцією системи моніторингу в мережу. Основною другого шляху є модульна організація мережі, коли рівні Ядра, Розподілу й Доступу є незалежними за своєю архітектурою один від одного й проектуються таким чином, щоб мережу можна було розширити в будь-який момент додавши до неї новий модуль на рівні, де необхідно розширити можливості.

2.1.3. Модульна організація мережі

Масштабування мережі – це проблема, що зустрічається в будь якій сфері, в якій з плином часу з’являється все більше нових користувачів. Зазвичай, якщо мережа більше не здатна надавати послуги більшій кількості абонентів, то в такій мережі можливі наступні зміни: заміна обладнання на більш потужне, з більшою кількістю портів, модернізація архітектури мережі чи перепроектування всієї мережі. Варіанти заміни обладнання й перепроектування мережі не є ефективними через те, що не вирішують проблему остаточно. Перепроектування є занадто затратним, а заміна обладнання на більш потужне – лише тимчасове вирішення проблеми.

Тому ефективним варіантом є модернізація мережі, або її супровід. Під вимоги масштабованості та супроводжуваності підпадає модульна організація мережі, яка об’єднує рівні мережі в однотипні модулі, додаванням цих модулів і відбувається масштабування.

Модульна організація передбачає на вищому рівні таку організацію, що не залежить від налаштуваннь нижчих рівнів. Така організація має своєю першоосновою – можливість збільшення мережі.

2.2. Технології необхідні для ефективної організації транспортної мережі

Отже організація мережі, а точніше - її архітектура, буде наступною:
Трирівнева модульна розподілена архітектура, в якій рівень ядра проектується незалежним від налаштувань нижчих рівнів, щоб дозволити можливість безперешкодного розширення кількості модулів нижчих рівнів без необхідності в переналаштуваннях ядра.

Тепер розглянемо технології та протоколи, за допомогою яких й буде будуватися логіка мережі.

На рівні доступу доцільно використовувати наступний мінімум технологій та протоколів:

1) DHCP, а точніше *DHCP Client* для автоматичного отримання базових параметрів *IP* та маски, даний протокол спростить взаємодію з обладнанням що додається у модуль рівня доступу без попередніх налаштувань. Крім того доцільно також використати *DHCP Relay*, для клієнтських підключень, які мають отримати параметри *IP* та маски від віддаленого серверу.

2) RRPP (або *Cisco REP*) / *STP* (його модифікації) для зв'язності пристроїв модулю рівня доступу за уникнення кілець.

На рівні розподілу та ядра необхідні можливості маршрутизації, керування та ізоляції трафіку, тому технології необхідні для даних рівнів такі:

1) VRRP – для надійності підключень модулів рівню *ACCESS* до модулів рівню *DISTRIBUTION*;

2) OSPF – для забезпечення динамічного знаходження сусідів та передачі маршрутної інформації для організації базису, на якому будується транспортна мережа.

3) MPLS – Для зменшення навантаження на обладнання та пришвидшення процесів передачі інформації, це досить популярна технологія для організації великих потоків даних. В даному методі, для транспортної мережі розглядається *MPLS LDP*.

4) BGP – для передачі маршрутної інформації за детально налаштованими політиками та для зв'язку із *ISP* (постачальником послуг інтернету). За даного методу також використовується *MPBGP* для ізоляції не тільки потоків даних, але й маршрутної інформації.

5) L2 та *L3 VPN*, які базуються на інкапсуляції повідомлень в *MPLS* заголовки, при чому використовуються спеціальні *VPNv4* заголовки, для керування розповсюдження маршрутної інформації та ізоляції потоків даних. *L2 VPN* дозволяє за необхідності з'єднати клієнтські підключення з віддаленим сервером, що підключений до транспортної мережі на рівні *L2*, так начебто вони в одній мережі *Ethernet*.

6) NAT – для організації виходу з транспортної мережі в *Internet*.

7) Stack/vPC – для об'єднання потужностей / розподілу навантаження між обладнанням модулів рівню ядра та розподілу.

8) LAcP/PAgP – для підвищення пропускної здатності та надійності ліній зв'язку між обладнанням.

Слід окремо зазначити, що на всіх рівнях присутні сервісні протоколи як наприклад *SSH, NTP, ACL, SNMP*, на яких не доречно загострювати увагу в межах даної роботи. Але необхідно зауважити, що *SNMP* грає значущу роль у супроводженні та підтримці мережі через те, що за використання системи моніторингу надає змогу ефективно слідкувати за станом мережевої інфраструктури та впроваджувати віялові зміни для груп пристроїв, що значно спрощує й зменшує у вартості роботу кваліфікованого персоналу підтримки чи мережевих інженерів.

2.3. Призначення транспортної мережі та її структура

Після опису ідей до організації мережі, її архітектури (модульна, трьохрівнева) та набору технологій для кожного рівня – стає можливим описати загальне

відображення методу побудови транспортних мереж у вигляді схеми логічної структури, що й буде описано далі, взявши до уваги наступне:

Так як в даній роботі описується метод до побудови транспортної мережі муніципальної цифрової інфраструктури, тобто - мережі що має надавати послуги транспортування даних для дошкільних, шкільних та вищих навчальних закладів, лікарень, інститутів, державних підприємств та підрозділів, громадського транспорту та закладів правоохорони – мережа має зв’язувати абонентів із серверами державних установ і, також, задовольняти потребу абонентів у доступі до глобальної мережі інтернету за відповідної необхідності.

При чому в якості абонентів виступають не кінцеві пристрої установ, як наприклад комп’ютери шкіл, а групи даних пристроїв об’єднані комутаторами\маршрутизаторами даних установ, тобто – контроль трафіку та упровадження сервісу транспортування надається не індивідуальному користувачу, а всій групі, тобто структура мережі початково має враховувати велику кількість підключень для кожного абоненту.

Примітка: дане пояснення не забороняє підключення до транспортної мережі окремого кінцевого пристрою, а лише підкреслює орієнтованість методу – забезпечення сервісами транспортування великої кількості абонентів, які в свою чергу містять також велику кількість кінцевих пристроїв.

Крім абонентів, які очікується завжди підключати до модулів рівню доступу, в транспортній мережі передбачається наявність державної інформаційної інфраструктури (сервери, тощо), яка інтегрується до транспортної мережі, шляхом прямого зв’язку з рівнем ядра. Державні установи обробки інформації, сервери, сховища даних (як наприклад хмара для камер відеоспостереження) очікується, що буде підключено до внутрішньої мережі, але з особливістю – підключення, як описано вище, відбувається напряму до рівня ядра. Таке підключення дозволяє сконцентрувати всі потоки даних муніципальної цифрової інфраструктури якомога ближче до рівня, на якому ці дані маршрутизуються.

Відображенням описаних вище ідей та принципів методу у вигляді логічної структури мережі буде наступна схема (рис. 2.1):

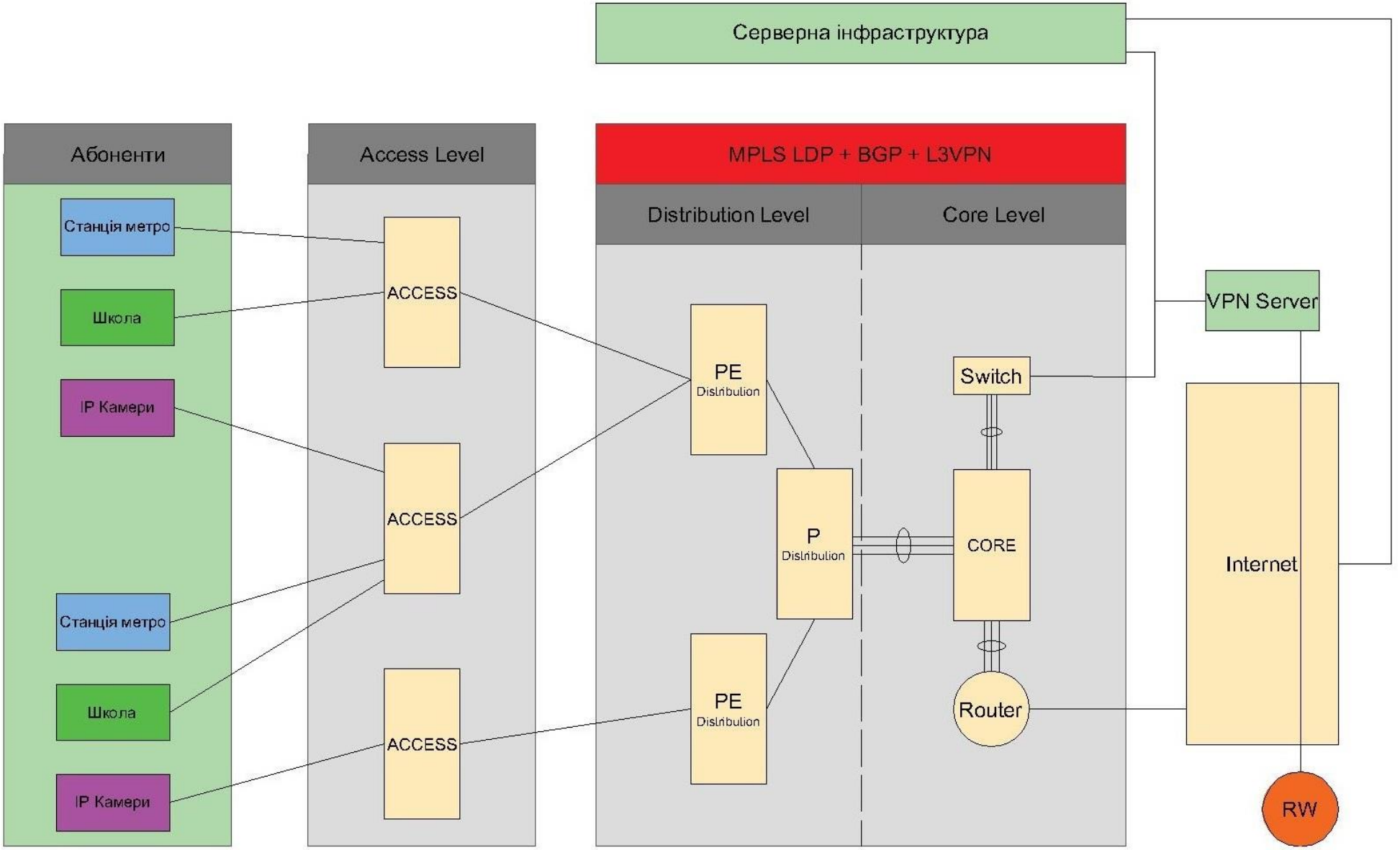

Рис. 2.1. Схема логічної структури транспортної мережі

На (див. рис. 2.1) зображено схему структури мережі, що відповідає вищезазначеним умовам та ідеям, жовтим кольором, в середині рівнів відображено блоки *Access, PE/P Distribution* та *Core*, які являють собою модулі відповідних рівнів.

Для доступу в інтернет передбачається використати множинне підключення до декількох *ISP* (за-для підвищення доступності та надійності), які аґрегуються на маршрутизаторі, що не є частиною транспортної мережі *MPLS*, але напряму пов'язаний з ядром. В разі недостачі кількості портів маршрутизатору – передбачається його розширення шляхом додавання у напрямку підключень *ISP* комутатора, який в такому випадку буде виконувати роль аґрегатора всіх з'єднаннь з глобальною мережею.

Дана схема, за бажанням, може бути доповнена засобами безпеки, як наприклад *IDS* (*intrusion detection system*), *Firewall* та *Spam* – аналізатор.

Серверна інфраструктура держави не обов'язково має безпосередньо підключатися до транспортної мережі, за-для безпеки є можливим варіант розташування між транспортною мережею та серверною інфраструктурою захисту у вигляді фаєрволу-ів.

Для забезпечення надійності з'єднання критичної інфраструктури, а саме – серверів та державних установ, передбачається окрема гілка з'єднання з *ISP*, яка використовується як резервна, для зовнішнього доступу та керування.

Адміністрування транспортною мережею планується здійснювати за допомогою *SSH*. Проте транспортна мережа в своїх межах використовує приватний пул адрес, який обумовлений досить великим розмахом даної інфраструктури, й крім того саме муніципальна цифрова інфраструктура не потребує зв'язку з глобальною мережею через те, що виконує лише роль інфраструктури і не є джерелом запитів до глобальної мережі. У зв'язку з цим використовувати публічні адреси для організації інфраструктури було б не доцільно та занадто витратно, тому – для керування обладнанням потрібно організувати *VPN* сервер, що напряму підключено до транспортної інфраструктури (модуля рівня ядра). Даному *VPN* серверу, як і серверам та абонентам, за допомогою *NAT* надається доступ до глобальної мережі, а отже – публічна адреса. Для керування транспортною інфраструктурою достатньо із

глобальної мережі підключитися до *VPN* серверу, а звідти вже в просторі приватних адрес транспортної мережі муніципальної інфраструктури керувати обладнанням за допомогою протоколу *SSH*.

Додатково слід відзначити, що за використання технології *L3VPN* потоки даних від шкіл\камер\метро та іншої муніципальної інфраструктури можна ізолювати настільки роздрібнено, що кожен тип інфраструктури матиме свою окрему таблицю маршрутизації та налаштування керування трафіку, що дозволяє поділити абонентів за рівнями критичності та пріоритетності трафіку.

2.4. Модульна структура транспортної мережі, архітектура модулів

Маючи чітке уявлення про архітектуру транспортної мережі, її призначення, функції та технології які дозволять її реалізувати – стає можливим описати логічну архітектуру модулів транспортної мережі. Кожен модуль побудовано таким чином, щоб займати мінімальну кількість портів у модуля вищого рівня, бо основна ідея методу – забезпечити ефективне масштабування.

2.4.1. Архітектура модулю рівня доступу, варіанти реалізації

Рівень доступу є найпростішим за логікою функціонування. Даний рівень складається з географічно розподілених комутаторів, основне призначення яких – надавати в користування свої порти доступу абонентам й забезпечувати надійне з'єднання з рівнем розподілу.

Рівень доступу ізолює дані лише на *L2* рівні, додаючи в *Ethernet* фрейм поле 802.1*Q* (інкапсуляція у *VLAN*), й за допомогою портів *TRUNK* зводить всі *VLAN* абонентів до рівня розподілу, де інкапсуляція доповнюється на рівні *L3* заголовками *MPLS* та *VPNv4*.

Бажано, щоб комутатори даного рівня були як мінімум *L2+*, з можливістю прописати статичні маршрути у напрямку рівня розподілу.

Архітектуру модуля даного рівня доцільно реалізувати за допомогою *STP*-гілок (рис. 2.2), де надійність забезпечується множинними надлишковими з'єднаннями між комутаторами. Такий підхід є більш надійним за інші, але займає більше портів та

іноді конвергентність такої архітектури довша ніж, наприклад, в топології кільце (обумовлено необхідністю проводити повторний розрахунок дерева *STP*).

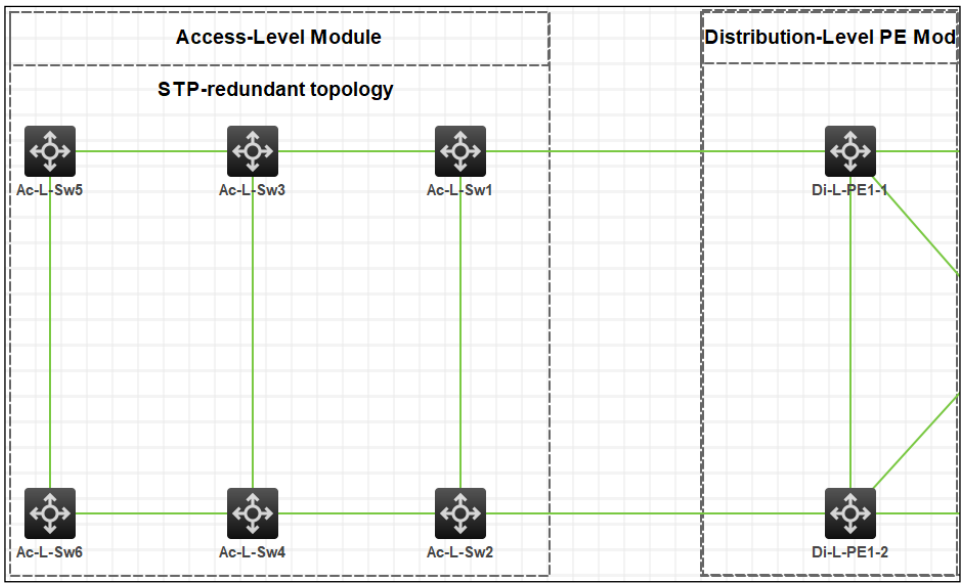

Рис. 2.2. Архітектура модулю рівня доступу, варіант протоколу *STP*

Альтернативно – архітектура модулю даного рівня може бути представлена через топологію кільця за використання протоколу *RRPP* (*Cisco REP*, протокол захищеного кільця) (рис. 2.3), що забезпечує меншу надійність підключення (бо комутатор з'єднується із сусідами лише за допомогою двох гілок і не більше) проте даний підхід водночас обмежує кількість зарезервованих портів (інтерфейсів) під потреби архітектури лише до 2-х на кожен комутатор рівня доступу, що є суттєвою перевагою для мереж, де більш пріоритетним є параметр масштабованості (кількість абонентів на один екземпляр пристрою в мережі)

Даний протокол було розроблено з увагою на швидкість конвергенції мережі після виникнення розриву однієї з гілок, що робить даний протокол більш переважним для підключень в яких досить важливою є висока доступність мережі.

У протоколі *RRPP* існує можливість розмежовувати групи кілець на домени що можуть як перетинатися, так і бути повністю незалежними. В межах одного домену завжди має бути визначене головне кільце нульового рівня. Кількість кілець в домені не обмежена, проте заради уникнення сповільнення конвергенції мережі рекомендується не збільшувати як кількість кілець в одному домені, так і кількість пристроїв в одному кільці більше 10.

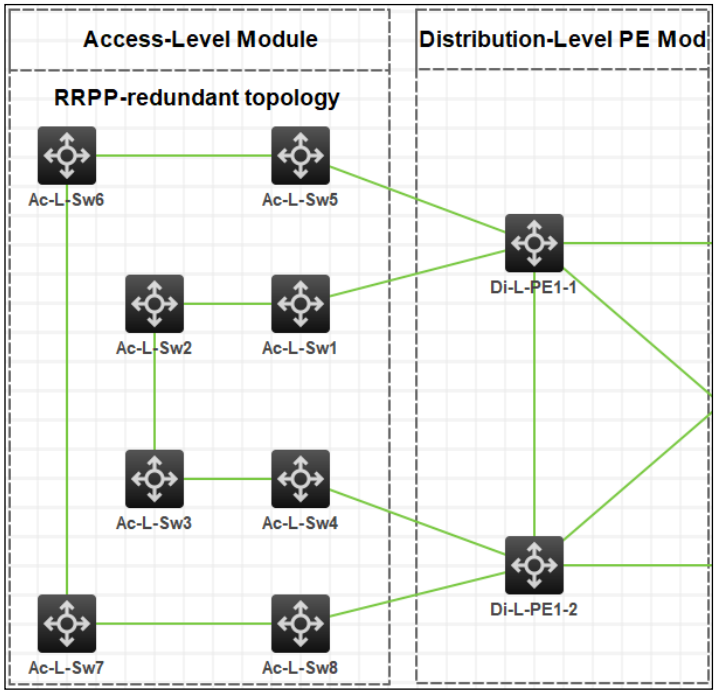

Рис. 2.3. Архітектура модулю рівня доступу, варіант з використанням кільцевої топології протоколу *RRPP*

2.4.2. Архітектура модулю рівня розподілу, варіанти реалізації

Через використання протоколу *MPLS* - пристрої рівня розподілу поділяються на ролі, а саме: *Provider`s edge* – пристрій на межі мережі *MPLS*; *Provider`s device*, або просто *P* – пристрій що цілковито розташовано всередині мережі *MPLS*, такий пристрій не пов'язаний з пристроями що не входять до мережі *MPLS*.

Отже в рівні розподілу розташовуються 2 модулі, що відповідають граничним пристроям і пристроям цілковито розташованим в межах мережі *MPLS*.

Пристрої *PE* за-для забезпечення надійності з'єднання мають підключати модулі рівня доступу як мінімум двома гілками, а так як основна увага методу приділяється саме масштабованості – то надлишкова надійність є менш пріоритетною за ефективне використання портів. Зважаючи на це – в модулі *PE* достатньо розташувати 2 пристрої, така пара пристроїв також має гілку зв'язку між собою для додаткової надійності ціною лише 1-го порту (рис. 2.4). Хоч для з'єднання рівня доступу з рівнем розподілу достатньо лише 2-х гілок, для з'єднання пристроїв *PE* з пристроями *P* бажано використати топологію *full-mesh*, так як до кожного модулю *PE* може підключатися множина модулів рівню доступу. Однак збільшення надійності значуще зменшує ефективність масштабування, тому доцільно буде піти на

компроміс – всі пристрої *PE*, в кожному модулі *PE* мають з'єднуватися як мінімум з двома пристроями *P*, при чому дані з'єднання мають бути налагоджені між пристроями *P* в різних модулях, якщо це можливо. Примітка: пристрої *PE* – обов'язково комутатори *L*3 рівня.

Пристрої *P* мають аґрегувати великі потоки даних від граничних пристроїв *PE*, а тому повинні мати як велику кількість портів, так і потужну комутуючу здатність, тому бажано, щоб такі пристрої представляли собою пару комутаторів об'єднаних в стек. Тому модуль пристроїв *P* складається з декількох однотипних комутаторів рівня *L*3, що об'єднано в стек (рис. 2.4).

Примітка: модуль пристроїв *P* представлено стеком однотипних комутаторів, а тому допускається модифікація даного модулю шляхом нарощування стеку. Така можливість присутня через базову властивість стеку – спільні налаштування та об'єднання потужностей всіх членів стеку, а отже – суть модулю незмінна за його нарощування.

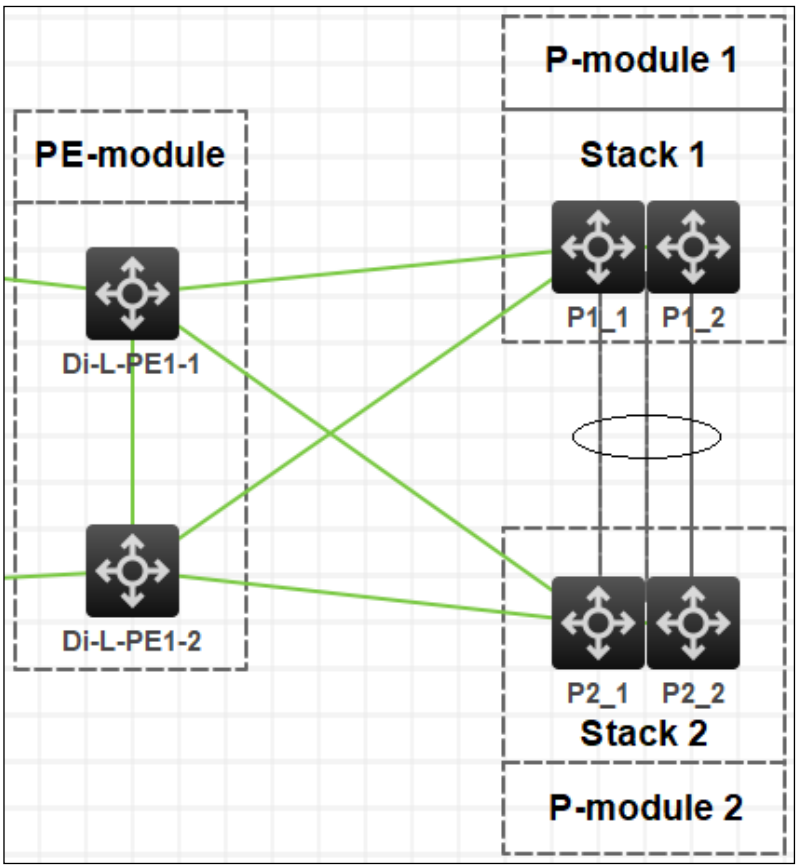

Рис. 2.4. Архітектура модулів рівня розподілу, на рисунку зображено один модуль *PE* (в лівій частині) та два однотипних модулі *P*, що представлені стеками з двох комутаторів

2.4.3. Архітектура модулю рівня ядра

Рівень ядра виконує одну з найважливіших ролей – розпакування ізольованих повідомлень та маршрутизація трафіку у відповідності із правилами та політиками компанії (чи замовника). Крім того, даний модуль виконує роль перенаправлення трафіку спрямованого до глобальної мереж, пересилаючи трафік на маршрутизатор (чи фаєрвол) границі автономної системи транспортної мережі та *ISP*. Передбачається, що даний модуль, на відміну від рівнів доступу та розподілу, буде складатися з надпотужних комутаторів *L3*, з розширеним списком можливостей, повністю заміщуючи можливості маршрутизатора.

Використання комутаторів дозволяє суттєво зменшити вартість побудови мережі, на відміну від реалізації проєкту мережі з використанням маршрутизаторів, вартість яких є на порядок більшою через дороге апаратне забезпечення маршрутизації для кожного з інтерфейсів маршрутизатора.

У більшості випадків, враховуючи специфічність службового трафіку муніципальної цифрової інфраструктури (трафік муніципальної інфраструктури переважно орієнтований на звернення до серверів міністерств, маловибагливий до наявності підключення до глобальної мережі й не має притаманних користувацьким підключенням стрибкам навантаження) - одного надпотужного комутатору буде достатньо для покриття муніципальної інфраструктури міста з населенням до півтора мільйона громадян (з врахуванням резервного запасу потужності), але для великих міст, як наприклад для Києву, потрібно об’єднати потужності двох таких надпотужних комутаторів (рис. 2.5).

Окрім того, для спрощення роботи комутаторів за збільшення рівню захисту всієї транспортної мережі допускається інтеграція потужних фаєрволів, здатних виконувати трансляцію мережевих адрес (*NAT*) – така інтеграція є бажаною. За додавання фаєрволу для захисту та проведення *NAT* – трафік у напрямку до інтернету пересилається до фаєрволу, де він сканується, відбувається *NAT*, повертається до ядра, а від нього маршрутизується до маршрутизатору границі автономної системи транспортної мережі та *ISP*.

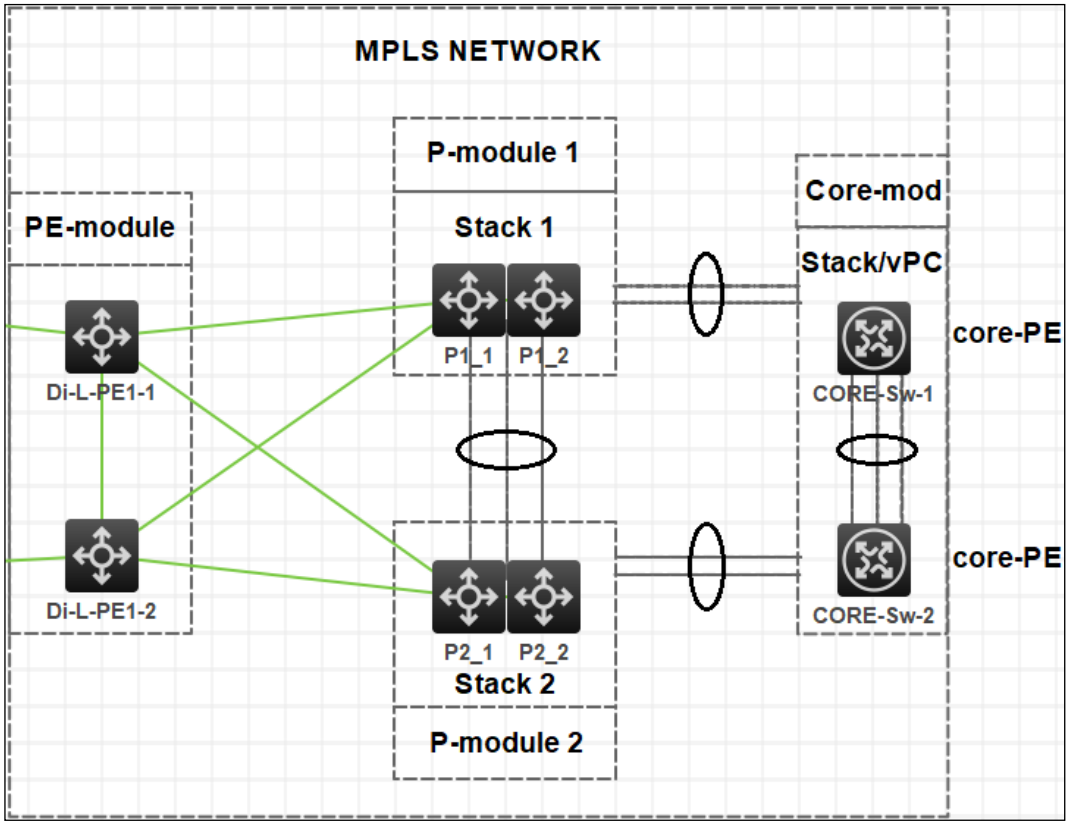

Рис. 2.5. Архітектура в межах *MPLS* мережі, на рисунку зображені модуль *PE*(ліва частина рисунку), два модулі *P* (центральна частина рисунку) та модульядра (права частина рисунку)

Примітка: Модуль ядра також має роль *PE* в мережі *MPLS*. Для переважної більшості випадків, за використання даного методу для побудови транспортної мережі муніципальної цифрової інфраструктури, достатньою є наявність одного модулю рівня ядра, що складається з одного-двох надпотужних комутаторів.

2.5. Можливості масштабування рівнів доступу та розподілу

Мережа, що побудована з використанням описаних вище модулів може бути масштабована для потреб муніципальної інфраструктури міста будь-якого розміру. При чому найбільша кількість нарощень пристроями буде відбуватися на рівні доступу, через те, що саме пристрої доступу будуть географічно рознесеними по місту за-для підключення об’єктів інфраструктури до транспортної мережі.

Вплив від масштабування кожного з модулів мережі не є однаковим, так наприклад - нарощення модулів доступу дозволить підключити стільки ж нових об’єктів, скільки було додано пристроїв. Вплив додавання пристроїв на різних рівнях

мережі можна побачити у відповідних таблицях - масштабованості кількості абонентів за нарощення модулю доступу (табл. 2.1) та масштабованість кілець доступу за нарощення кількості пристроїв розподілу (табл. 2.2):

Таблиця 2.1

Масштабованість максимальної кількості абонентів за нарощення модулю доступу

Модуль доступу				
Кількість кілець	Кількість пристроїв в кільці	Кількість портів для підключення об'єктів	Резерв архітектури	Резерв до вищого рівня
1	1	24	2	2
1	2	48	4	2
1	3	72	6	2
1	4	96	8	2
1	5	120	10	2
1	6	144	12	2
1	7	168	14	2
1	8	192	16	2
1	9	216	18	2
1	10	240	20	2
2	1	48	4	4
2	2	96	8	4
…	…	…	…	…
2	9	432	36	4
2	10	480	40	4
…	…	…	…	…
10	1	240	20	20
10	2	480	40	20
…	…	…	…	…
10	9	2160	180	20
10	10	2400	200	20

Таблиця 2.2

Масштабованість кілець доступу за нарощення кількості пристроїв рівню розподілу

Рівень розподілу							
№ п/п	Модулів *P*	Пристроїв в стеку P	Вільних портів P	Модулів *PE*	Кількість можливих кілець	Резерв архітектури PE	*Acess* / *Distribution devices*
1	2	3	4	5	6	7	9
1	1	1	16	1	23	6	76,667
2	1	1	12	2	46	12	92,000
3	1	1	8	3	69	18	98,571
4	1	1	4	4	92	24	102,222
5	1	1	0	5	115	30	104,545
6	1	2	24	5	115	30	95,833
7	1	2	20	6	138	36	98,571

Продовження таблиці 2.2

1	2	3	4	5	6	7	9
8	1	2	16	7	161	42	100,625
9	1	2	12	8	184	48	102,222
10	1	2	8	9	207	54	103,500
11	1	2	4	10	230	60	104,545
12	1	2	0	11	253	66	105,417
13	2	2	44	11	253	66	97,308
14	2	2	40	12	276	72	98,571
…	…	…	…	…	…	…	…
23	2	2	4	21	483	126	105,000
24	2	2	0	22	506	132	105,417
…	…	…	…	…	…	…	…
31	2	3	0	34	782	204	105,676

2.6. Шлях, обробка та захист трафіку в мережі

Для забезпечення високого рівня якості надаваних послуг є необхідним знати яким чином трафік що передається транспортною мережею змінюється, обробляється й перенаправляється. Кожен рівень інкапсуляції трафіку дозволяє відокремити його на категорії за пріоритетом, правилами обробки й маршрутизації.

Шлях трафіку муніципальної інфраструктури по мережі (рис. 2.6), що побудована з використанням вище описаних ідей, технологій та схеми логічної структури (див. рис. 2.1) поділяється на 6 основних проміжків у напряму від інфраструктури до серверів: 1) не оброблені дані, що генеруютья зі сторони об’єкту інфраструктури; 2) дані інкапсулюються у *VLAN* мітки по надходженню до рівню доступу й направлено до рівню розподілу; 3) на рівні розподілу трафік ділиться на категорії за міток *VLAN* та протоколу *L3VPN* й інкапсулюється мітками транспортування по *MPLS*-мережі у напряму ядра; 4) на рівні ядра з трафіку знімається мітка *MPLS* й переглядається таблиця категорій трафіку протоколу *L3VPN*, якщо трафік направлено до *ISP* – відбувається трансляція мережевої адреси й передача трафіку на маршрутизатор границі *AS*, альтернативно – з трафіку знімаються мітки (окрім *VLAN*) й дані передаються до комутатору серверної інфраструктури; 5) на комутаторі мережевої інфраструктури з трафіку знімається мітка *VLAN* й відбувається передача оригінальних даних у напрямку серверів, фаєрволів чи іншого обладнання серверної інфраструктури.

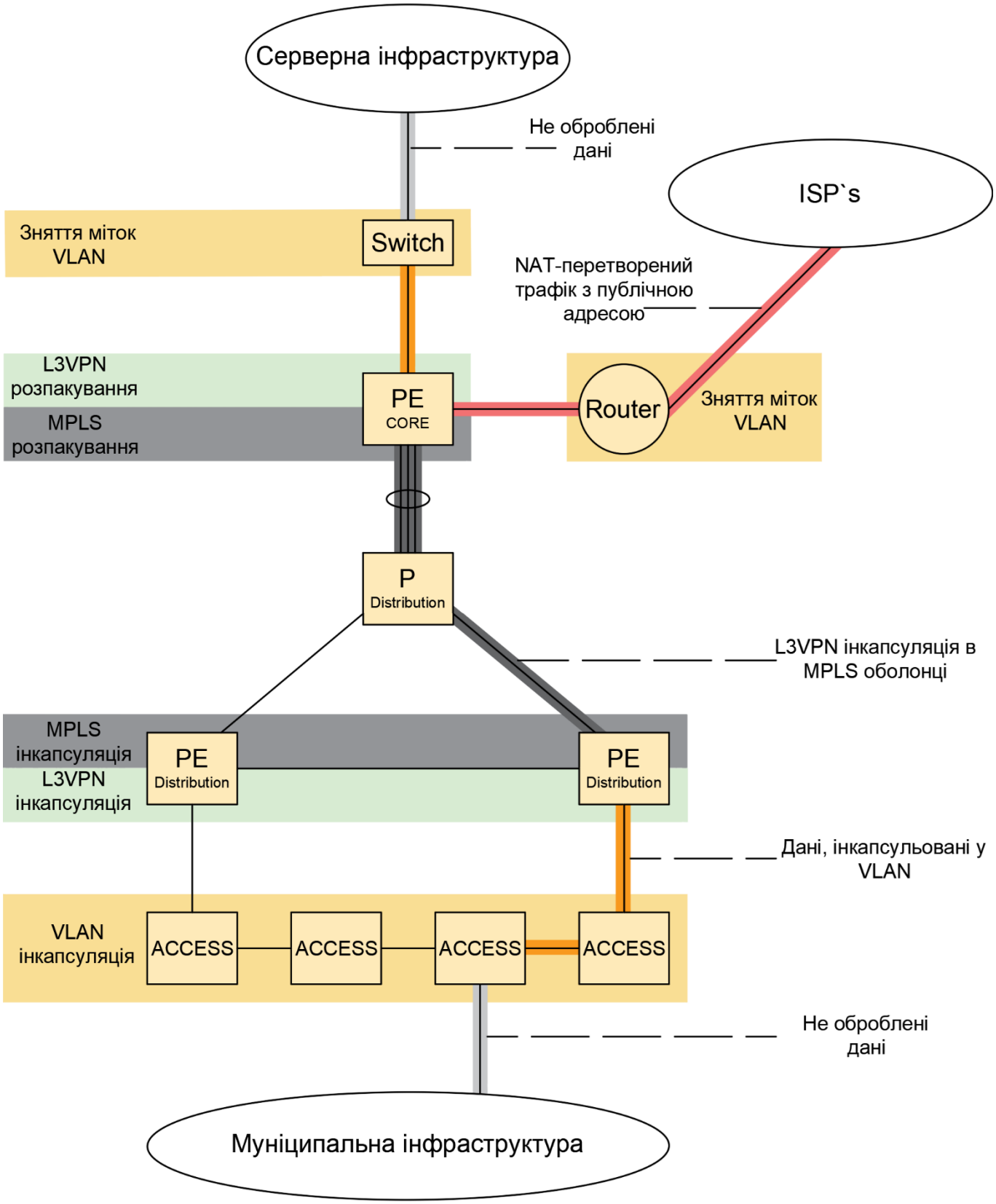

Рис. 2.6. Шлях та інкапсуляція трафіку у напряму від абонента до серверу

Схема трафіку із впровадженням додаткового захисту інформації за використання протоколів захищеного тунелювання *AD-VPN* та *IPSec* виглядає наступним чином (рис. 2.7):

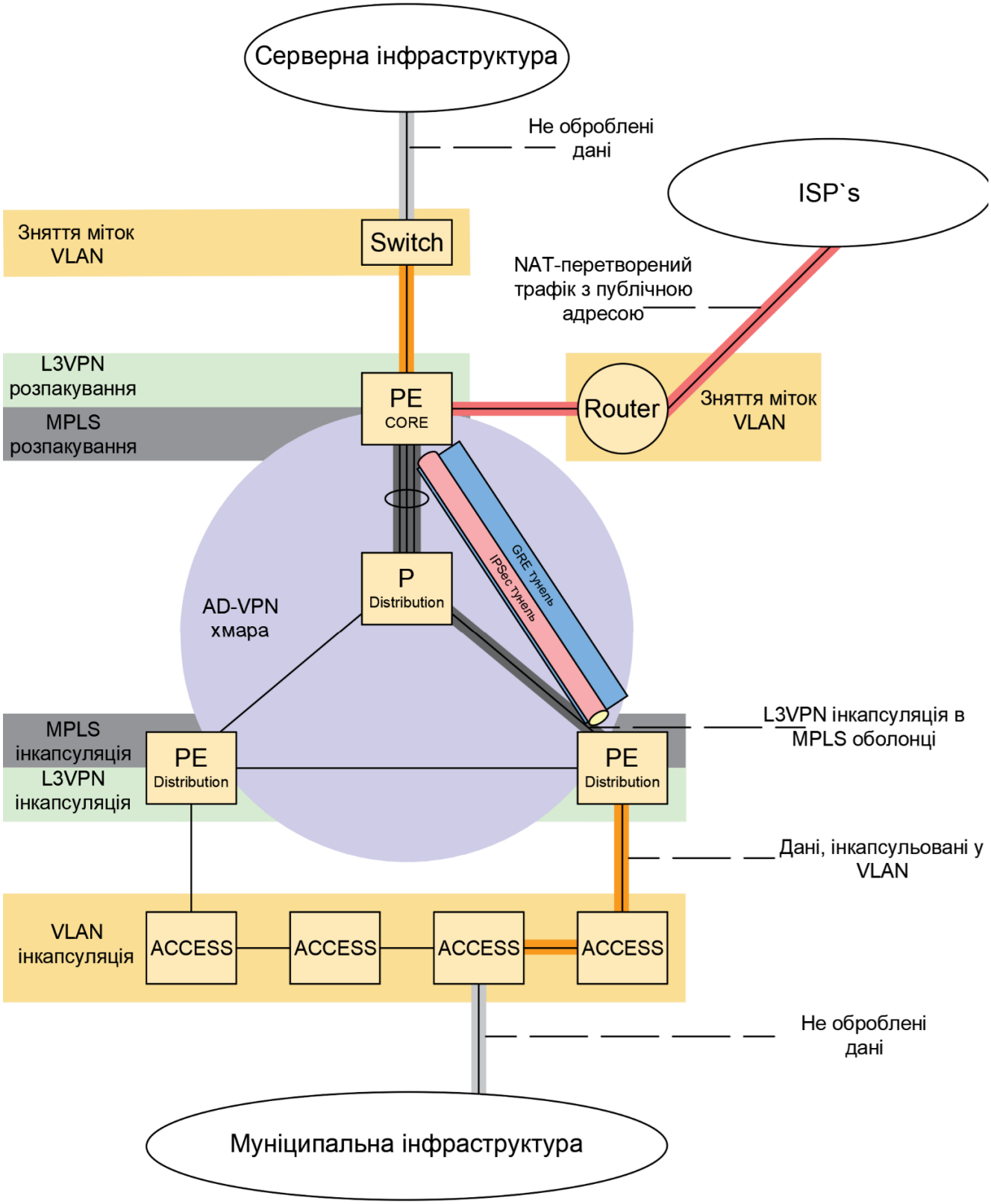

Рис. 2.7. Шлях та інкапсуляція трафіку за використання додаткових технологій захисту інформації.

Для покращення рівня захищеності трафіку в транспортній мережі доцільним кроком є інтеграція в архітектуру мережі протоколу захищених виділених з'єднань з використанням тунелювання – *AD-VPN* (див. рис. 2.7), - це дозволить додатково

ізолювати трафік на проміжку від пристроїв *PE* розподілу та пристроєм ядра. Крім того, протокол *AD-VPN* дозволяє централізувати знаходження проблемних ланок мережі, через те, що стан всіх ланок обробляється на ключових пристроях, як наприклад - пристрої ядра.

Якщо ж в мережі необхідно впровадити не тільки інкапсуляцію за паролем, а й надійне шифрування даних – протокол *AD-VPN*, що здатен будувати *GRE*-тунелі здатний поєднати два тунелі одночасно, доповнюючи простий тунель *GRE* шифрованим тунельним з'єднанням *IPSec*, що є стандартом у мережевій безпеці через велику роздрібненість можливостей налаштування сервісів *AAA*.

Висновки за розділом

Комп'ютерні мережі вже стали для людства буденністю, складно знайти людину, що б не користувалася послугами інтернету. Разом з цим все більше об'єктів реального світу занурюються в інтернет, все більше сервісів та послуг які можуть бути надані по мережі завойовують своє місце на ринку інформаційних послуг. А з розвитком послуг зв'язку, з цифровізацією України, виникає потреба у ефективних рішеннях для сучасних проблем.

Наразі мережі України є відносно застарілими і потребують досить значної модернізації. Ціллю модернізації є забезпечення нового, сучасного рівня доступу абонентів до послуг транспортування даних шляхом впровадження новітнього обладнання та технологій. Але на дану модернізацію не варто очікувати, потрібно знаходити рішення для поточної ситуації.

Міста України чекає значний ріст, хоч і не в найближчому майбутньому, але дана перспектива є міцною через те, що наша країна в найближчі десятиліття тільки почне бурхливий розвиток економіки та рівню життя. Разом із розвитком міст – зростає й кількість муніципальної цифрової інфраструктури.

Інфраструктуру муніципальної цифрової інфраструктури не є доцільним підключати як звичайних абонентів мережі – до інтернет провайдерів через необхідність спочатку обробити дані міністерствами та установами для безпеки, крім того вартість такого підключення є занадто великою.

Ефективним рішенням буде об’єднання державної міської інфраструктури у окрему мережу, що не залежить від застарілої інфраструктури системи зв’язку. Саме у сфері таких рішень на ринку не має поширених пропозицій, а ситуація з Українськими містами взагалі є не звичайною. Тому для вирішення даного питання потрібно сформувати певний проект, рішення, що підійшло б містам України, при чому буде тільки плюсом, якщо такий проект буде універсальним. Саме з такою ціллю в даній роботі розглядається, планується та аргументується вибір принципів, підходів та правил побудови мереж (іншими словами - методика), щоб отримати найефективніше рішення для Українських міст.

В даному розділі досить детально описано підхід, що є можливим використати при розвитку Українського міста будь-якого розміру.

РОЗДІЛ 3
ПІДХІД ДО НАЛАШТУВАННЯ, ПРОТОТИП ТА АПАРАТНА БАЗА

3.1. Опис підходу до налаштувань обладнання

Масштабованість в даному методі досягається за допомогою: обмеження на кількість використовуваних портів в модулях кожного рівня; використання модульної архітектури, що робить кожен рівень мережі незалежним від попереднього (налаштування верхніх рівнів не залежать від налаштувань нижніх), водночас - саме нижні рівні будуються відносно налаштувань верхніх рівнів; використання технологій (та протоколів) що дозволяють легко додавати нові апаратні модулі та організувати потоки даних великої кількості однотипних абонентів що географічно розподілені по значній території.

В свою чергу, простота налаштувань досягається за допомогою комбінації використаних протоколів, при чому увага приділяється низхідній залежності налаштувань, де саме нижні рівні мережі залежать від налаштувань верхніх рівнів, що дозволяє провести складні налаштування обладнання рівня Ядра лише один раз і "забути" про необхідність внесення змін за збільшення кількості модулів нижчих рівнів. Так само влаштовано рівень розподілу – пристрої *PE* мають налаштування, що дозволяють без внесення змін до основної логіки* додавати нові модулі рівня доступу.

* без внесення змін до основної логіки – єдині необхідні зміни – виділення новому модулю рівня доступу нового домену *STP*/*RRPP* та індивідуального набору *VLAN*, логіка маршрутизації, політики, надійність та зв'язність при цьому не змінні. Отже – зміни потрібно вносити тільки для параметрів *L*2 рівню, що виправдано додаванням ланцюгу *L*2 пристроїв, а на основну частину рівня розподілу (*L*3 рівень) додавання модулю рівня доступу впливу не має.

Примітка: надалі цей опис, так само як і всі аспекти описаного методу, буде використано при побудові демонстраційного прототипу.

3.2. Шаблонний підхід до налаштування обладнання

Крім масштабування, важливою частиною будь-якої великої мережі є її вартість: обслуговування, підтримки і, найважливіше – налаштування. Для зменшення витрат на дані заходи можна використати надсучасну архітектуру мереж на базі *SDN*, але такий підхід не є оптимальним для, наразі, розглянутих умов (відносна застарілість вже існуючої мережевої архітектури України). Окрім *SDN* є альтернативний метод суттєвого зменшення трудовитрат та вартості обслуговування мережі – використовувати шаблонний, само-подібний підхід до налаштувань обладнання.

В межах кожного рівня модулі матимуть ідентичні налаштування основної логіки. Така самоподоба між модулями дозволяє спеціалістам не витрачати час на дослідження логічної структури кожного модулю індивідуально, спеціалісту за такого підходу необхідно лише знати базову структуру налаштувань кожного модуля, а на основі цих знань легко виявити помилки допущені в налаштуваннях чи внести зміни у шаблон за потреби.

Крім того, важливою частиною такого підходу є те, що за модульної організації мережі та шаблонного підходу до налаштувань обладнання необхідний для супроводження мережі рівень кваліфікації спеціалістів стає нижчим, що також позитивно впливає на вартість супроводження такої мережі.

Але слід відмітити, що рівень самоподімності є обмеженим і неможливо налаштовувати всі модулі абсолютно ідентичними даними через відмінності у найпростіших значеннях, які не впливають на логіку функціонування, але мають бути визначені для кожного екземпляру модулю певного рівня. До таких параметрів належать наприклад: Системне ім’я пристрою, локальні паролі, набір *VLAN* (підхід до розподілу визначається політикою кожної організації індивідуально, в даній роботі далі буде наведено демонстраційний прототип із подібними параметрами, але не слід обмежуватися приведеним прикладом – імена, паролі та значення *VLAN* не мають чітких правил для їх ефективного задання та розподілу), Пул приватних адрес для протоколу *VRRP* та інші.

Примітка: Важливо відзначити, що логіка модулів залишається незмінною при визначенні індивідуальних параметрів перелічених вище.

3.2.1. Шаблон налаштувань модулів рівня доступу

Рівень доступу має найпростіші налаштування. Для побудови демонстраційного прототипу доцільним є варіант модуля з топологією “кільце” на основі протоколу *RRPP*. Отже, перелік налаштувань шаблону для кожного пристрою в модулі рівня доступу є таким:

1) Задати налаштування часу (по протоколу *ntp*, вказати адресу серверу *ntp*);

2) Задати індивідуальне ім’я для обладнання;

3) Створити набір *VLAN*-ів, що відповідають абонентам, які будуть підключені до обладнання (даний набір має відрізнятися від відповідних наборів в інших доменах, хоча й може мати однаковий розмір);

4) Створити *stp region-configuration*, додати до нього всі *VLAN* даного домена й активувати дані налаштування;

5) Створити віртуальний логічний *VLAN*-інтерфейс (необхідний для віддаленого підключення до даного обладнання), номер *VLAN* визначається згідно з політикою, визначеною в компанії чи за вимогами замовника;

6) Перевести порти, до яких буде підключено абонентів в режим доступу та назначити номер *VLAN* для даного типу абонентів (із урахуванням поточного домену) й додати опис (якщо необхідно);

7) Порти *Uplink* перевести в режим *Trunk*, визначити набір допустимих *VLAN* (даний набір має відповідати всім *VLAN*, що належать домену) та заборонити пропущення *VLAN* з номером 1. Вимкнути *STP* на даних портах (потрібно для налаштування *RRPP*);

8) Прописати статичний маршрут 0.0.0.0 у напрямку модуля *PE*, до якого підключено даний модуль рівня доступу;

9) Створити домен *RRPP*, задати контрольні *VLAN* (ці номери мають бути зарезервовані цілковито під домен *RRPP* й не використовуватися для підключень абонентів). Задати захищені *VLAN* (список номерів даного домену, за виключенням контрольних). Активувати *RRPP*;

10) Налаштувати профіль *SNMP* (згідно з політикою компанії чи вимогами замовника).

11) Налаштувати *SSH* для можливості віддаленого підключення.

12) Додатково: налаштувати *RADIUS*, списки контроль доступу, *DHCP snooping* та політики керування трафіку (для даних налаштувань не має чітких значень, бо вони визначаються цілковито політикою компанії та вимогами замовника).

Примітка: в кожному домені має бути свій набір *VLAN* для уникнення переміщення однакових даних по декільком доменам (захист від *broadcast*-шторму та кілець трафіку).

Даний шаблон налаштувань є спільним для всього обладнання модулю рівня доступу, але є деякі особливості, які потрібно описати окремо, а саме: в кожному кільці домену *RRPP* має бути визначено один пристрій який відповідатиме за контроль цілісності кільця.

3.2.2. Шаблон налаштувань модулів рівня розподілу та ядра

Перед розписом шаблону дій, необхідних для налаштування обладнання слід відмітити, що даний порядок дій є узагальненим переліком необхідних налаштувань, сам процес налаштувань вимагає значно більшої кількості дій, приклад конфігурацій повністю налаштованих пристроїв наведено в додатках. Крім того налаштування найбазовіших параметрів по типу імені, часу, профілів *SNMP* та іншого – упущено.

Налаштування модулів розділено на рівні *L*2 та *L*3 для зручності.

1) Налаштування модулів *PE* рівня розподілу:

Рівень *L*2:

1.1) Створити набір *VLAN* для категорій абонентів, при чому набори *VLAN* мають покривати всі домени модулів рівня доступу які планується підключати до даного модулю *PE*.

1.2) Створити *loopback* інтерфейс та задати йому адресу (за даною адресою та інтерфейсом відбувається керування даним пристроєм).

1.3) Створити *VLAN*-інтерфейси для *VLAN* які використовуються в доменах модулів рівня доступу (це необхідно для налаштування протоколу *VRRP* та, взагалі, для обробки й маршрутизації пакетів з даних *VLAN*).

1.4) Налаштувати регіон *RRPP* та визначити роль пристроїв модулю *PE* як *edge* та *assistant edge*;

1.5) Налаштувати порти до яких підключаються модулі рівня доступу (*Vlan*, безпека, захист від штормів та кілець);

1.6) Налаштувати *uplink* порти (дозволити влани);

Рівень *L*3:

1.7) Налаштувати *IP* зв'язність (прописати *IP* адреси необхідні для зв'язності пристроїв мережі *MPLS*);

1.8) Налаштувати *OSPF*, для організації обміну адресами та зв'язку між пристроями рівнів розподілу та ядра (дана зв'язність є основою для побудови ізольованих маршрутів *MPLS*);

1.9) Активувати *MPLS* та налаштувати автоматичне поширення шляхів за допомогою *LDP*. Переконатися у зв`язності по *MPLS*;

1.10) Налаштувати *BGP* (*iBGP*) та визначити один із пристроїв модулів *P* як *route-reflector* (зв'язність дистанційна через використання *loopback* інтерфейсу). *BGP* знадобиться для передачі маршрутів абонентів та керування;

1.11) Створити *VPN-instances* та пов'язати відповідні *VLAN*-інтерфейси з класами даних (*VPN-instances* є класами даних). Дане налаштування потрібне для увімкнення *L*3*VPN*, який дозволить ізолювати не тільки дані, а й їх потоки (і маршрутизацію) в залежності від класу даних;

1.12) Активувати *MPBGP* та налаштувати зв'язність *VPNv*4 між *PE* рівня розподілу та *PE* рівня ядра. Перевірити ізоляцію даних;

1.13) УВАГА, даний крок є умовним, так як кожна компанія чи замовник в своїх вимогах визначає це індивідуально: Налаштувати політики поширення маршрутів від абонентів у напрямку ядра;

2) Налаштування модулів *P* рівня розподілу. Дані пристрої мають схожі налаштування до модулів *PE* за відмінністю:

- Для пристроїв *P* не потрібно створювати *VLAN*-інтерфейси для клієнтських підключень та організовувати надійність за допомогою протоколу *VRRP*;

- Протокол *VRRP* можна використати для резервації зв’язку між декількома модулями *P*;

- Для пристроїв *P* не потрібно налаштовувати *RRPP*, *MPBGP* та *L3VPN*.

Окрім зазначених особливостей, модулі *P* налаштовуються ідентично до модулів *PE*. Мета модулів *P* – формувати простір для транспортування *MPLS*.

3) Налаштування модулів *PE* рівня Ядра відбувається ідентично до налаштувань модулів *PE* рівня розподілу за виключенням наступних особливостей:

- На рівні ядра не потрібно налаштовувати протоколи *VRRP* та *RRPP*.

Окрім того, на рівні ядра для забезпечення маршрутизації потоків ізольованих даних потрібно організувати політики розповсюдження та прийому маршрутів, списки контролю доступу для обмеження підключень та статичні маршрути для кожної сутності *L3VPN* (не обов’язково, але бажано) для направлення даних від абонентів до серверної інфраструктури держави.

Слід зазначити, що політики маршрутизації визначаються цілковито за потреби та політик налаштувань компанії чи конкретних вимог замовника; дані налаштування будуть упущені в демонстраційному прототипі.

3.3 Симулятор комп’ютерних мереж *H3C Cloud Lab*

Для побудови тестових стендів, перевірки концептів, тестування комбінацій налаштувань чи сценаріїв відпацювання – для цього всього доцільно скористатися відповідними середовищами, симуляторами та емуляторами.

Середовища - симулятори дозволяють точно моделювати різноманітні аспекти реальних сценаріїв та параметрів мережі, забезпечуючи більш достовірне відтворення реальних умов. В межах даної роботи є необхідним продемонструвати працездатність запропонованих ідей, принципів та підходів методу побудови муніципальних мереж з використанням середовища наближеного до реальних умов.

Серед безкоштовних та актуальних програмних засобів що функціонально відповідають потребам є середовище *H3C Cloud Lab*. Дане середовище призначене для навчання спеціалістів та тестування поєктів мереж із використанням основних типів пристроїв в мережах (комутаторів, маршрутизаторів, серверів та ПК).

Однією з основних відмінностей даного симулятору є те, що він використовує віртуальні машини для симуляції операційних систем кожного окремого екземпляру пристрою, що дозволяє проаналізувати роботу мережі у приближених до реальних умов.

Основними можливостями даного середовища є:

– Розміщення графічними засобами мережевого обладнання у віртуальному просторі;

– створення різноманітних топологій, шляхом проведення кабельних з'єднань різних типів;

– симуляція операційних систем пристроїв, та відповідна взаємодія з ними;

– налаштування симульованих пристроїв та їх операційних систем у повній відповідності до їх реальних аналогів;

– збереження, завантаження, імпорт та експорт тестових стендів;

– інтеграція альтернативних файлів операційних систем пристроїв;

– створення власного пристрою, задання його параметрів та операційної системи;

– в якості базових пристроїв – наявні комутатори та маршрутизатори компанії *HP* з базовими версіями операційних систем відповідних пристроїв;

– переводити екземпляри пристроїв в стани, що є відображеннями фізично увімкненого та вимкненого пристрою;

– за допомогою базових графічних засобів відокремлювати віртуальний простір, писати примітки, технічну інформацію, тощо;

– створювати знімки віртуального простору;

Для більшості випадків саме попередня побудова й тестування мереж й мають відбуватися в подібному просторі, де не має ризику пошкодити існуючу мережеву інфраструктуру. Даний простір також розповсюджується як рекомендований для самостійного навчання та дослідження можливостей протоколів, технологій, їх комбінацій.

Середовище *H3C Cloud Lab* безкоштовно можна завантажити з офіційного сайту компанії *H3C* у розділі підтримки, проте для його функціонування обов'язково

необхідно попередньо встановити середовище для запуску віртуальних машин *VirtualBox*-4.2.18.

Вікно симулятору із завантаженою топологією мережі для тестування протоколу *OSPF* виглядає наступним чином (рис. 3.1):

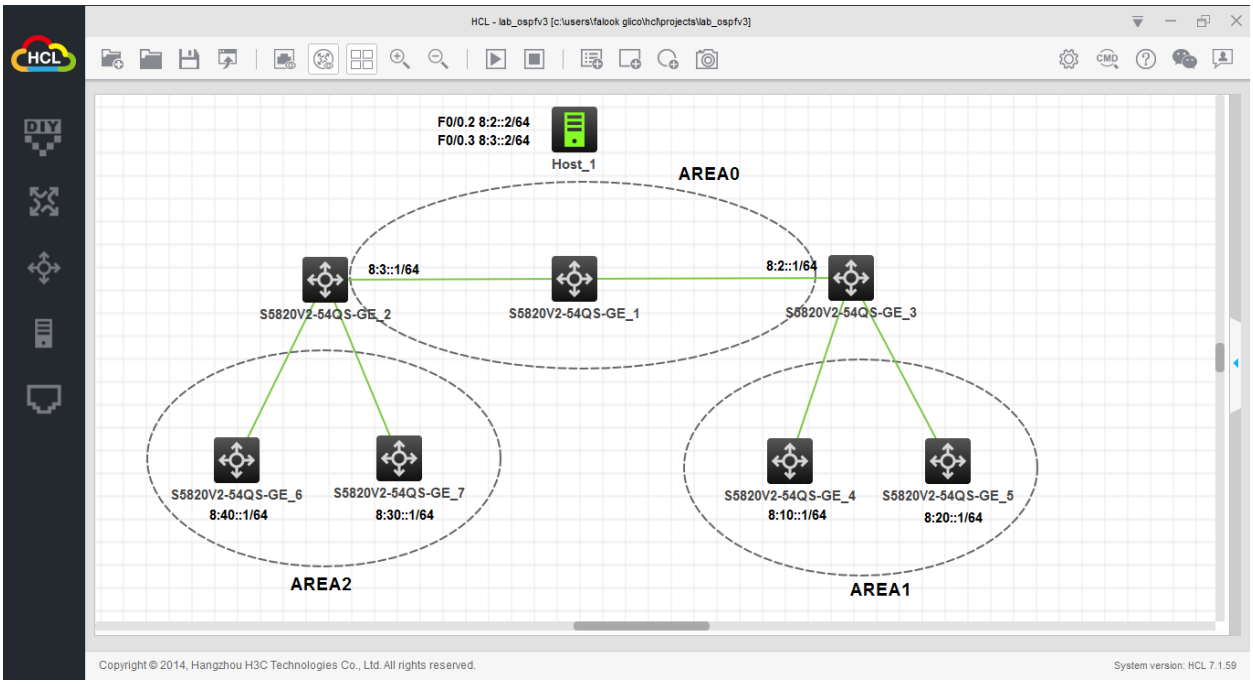

Рис. 3.1. Вікно симулятору із побудованою в ньому мережею

3.4. Побудова прототипу та його перевірка в середовищі *H3C Cloud Lab*

Для перевірки працездатності описаної в методі комбінації необхідних технологій, можливостей ефективного масштабування та шаблонного підходу до налаштувань (що призначено для зменшення трудовитрат) – доцільним є побудувати демонстраційний прототип транспортної мережі цілком за описаними в даній роботі ідеями, підходами, шаблонами налаштувань та схемою архітектури мережі.

Слід зазначити що деякі деталізовані налаштування, як наприклад AAA, *SNMP, NTP, NAT, Route-Policies* упущені через те, що дані налаштування доцільно робити тільки відштовхуючись від вимог замовника та наявних ресурсів, не доцільно вигадувати тестові дані подібного масштабу в межах прототипу.

Середовищем для створення та перевірки демонстраційного прототипу є симулятор *H3C Cloud Lab*. Серед представлених в демонстраційному прототипі модулів будуть: 2 кільця *RRPP* в складі одного модуля рівня доступу, 1 модуль *PE*

рівня розподілу (два комутатори на 24 порти), 1 модуль *P* рівня розподілу (1 стек комутаторів, що візуально представлено одним пристроєм (на 48 портів), 1 модуль рівня ядра (1 комутатор на 24 порти).

При чому за такої компоновки прототипу кількість абонентів що може бути підключена = (кількість вільних портів модулів *P* / 4) * 24 * 10. В прототипі використано 2 *uplink* порти модулю *P* для з'єднання з ядром, а тому за такого розкладу є можливим підключити 24/4 = 12 модулів *PE* рівня розподілу. До кожного модуля *PE* можна підключити до 24-ох кілець модулів рівня доступу, в кожному з яких розміщено по 10 пристроїв доступу, тому виходячи з цього: (24/4) * 12 * 24 * 10 = 2880 можливих абонентів.

Зважаючи що пристрої будуть розподілені географічно і зачасту розташовуватись так, щоб лише один пристрій було розміщено у абонента (об'єкта інфраструктури), то максимальну кількість абонентів вважаємо рівною кількості пристроїв рівня доступу = 2880. Однак варто взяти до уваги те, що довжина з'єднань, навіть оптичних, є обмеженою за утримання в певних межах вартості обладнання, а тому деяка кількість пристроїв рівня розподілу в межах кільця буде слугувати підсилювачами-комутаторами для об'єднання пристроїв на віддалених об'єктах в кільце, тому вважаємо кількість доступних пристроїв для підключення абонентів меншою, наприклад – в двічі ніж кількість пристроїв доступу 2880/2 = 1440 можливих абоненти.

Примітка: припущення про в двічі меншу кількість доступних пристроїв для підключення абонентів є грубим і неточним, не варто брати його як показник для реальних розрахунків.

Зіставимо кількість можливих абонентів із інфраструктурою, наприклад, міста Київ (дані застарілі): 491 школа + 52 станції метро + 50 лікарень + 55 поліклінік + 300 дошкільних навчальних закладів + 37 вищих навчальних закладів = 985 абонентів. Отже прототип, в теорії, здатен покрити інфраструктуру міста Київ (1440 > 985).

Логічну схему демонстраційного прототипу, побудованого за ідеями, схемами та шаблонами налаштування описаного методу виглядає наступним чином (рис. 3.2):

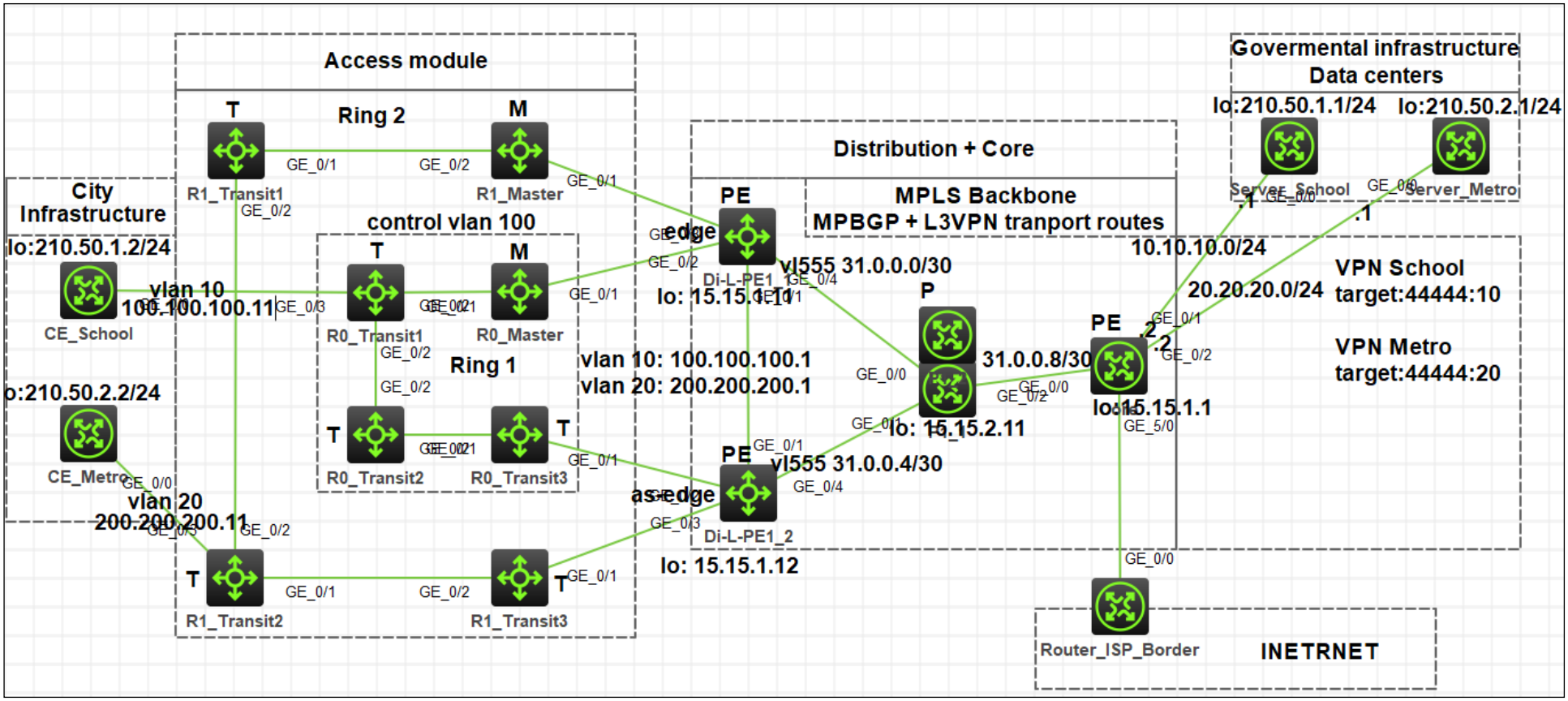

Рис. 3.2. Логічна схема демонстраційного прототипу із певними значеннями адрес, використаних для налаштування

На (див. рис. 3.2) зображено схему демонстраційного прототипу, що побудовано, налаштовано та протестовано в середовищі *H3C Cloud Lab*. В прототипі присутні всі описані модулі, схему зіставлено із урахуванням шаблонного налаштування й код файлу конфігурації ключових пристроїв наведено в додатках.

Що-до справності функціонування прототипу – далі буде наведено серію скріншотів із результатами вводу команд перевірки, на яких буде відображено стан основних технологій та протоколів використаних для побудови мережі.

```
<R1_master>disp rrpp v dom 1
 Domain ID      : 1
 Control VLAN   : Primary 100, Secondary 101
 Protected VLAN: Reference instance 1
 Hello timer    : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID        : 1
 Ring level     : 0
 Node mode      : Master
 Ring state     : Complete
 Enable status  : Yes, Active status: Yes
 Primary port   : GE1/0/1                    Port status: UP
 Secondary port: GE1/0/2                     Port status: BLOCKED

<R1_master>
```

Рис. 3.3. Статус зв’язності кільця модулю доступу (для даного модулю протокол захищеного кільця є найважливішим)

На (див. рис. 3.3) можна побачити назву пристрою, його роль у кільці протоколу *RRPP*, поточний стан цілісності кільця та блоковані порти для уникнення закільцьованості трафіку. Протокол захищеного кільця дозволяє організовувати великі ланцюги пристроїв із мінімальними затратами по кількості портів, часу налаштування та часу обслуговування. Окремо варто відзначити що даний протокол, як і топологія кільця, створювався для зменшення часу знаходження розриву ліній зв’язку й пришвидшення конвергенції мережі під час такої зміни топології.

Базові значення таймерів часу службових повідомлень протоколу *RRPP* не є оптимальними, їх рекомендовано змінити (шляхом симуляції та підбору значень за яких зберігається стабільна робота протоколу) на більш ефективні для поточної топології та кількості пристроїв у одному кільці.

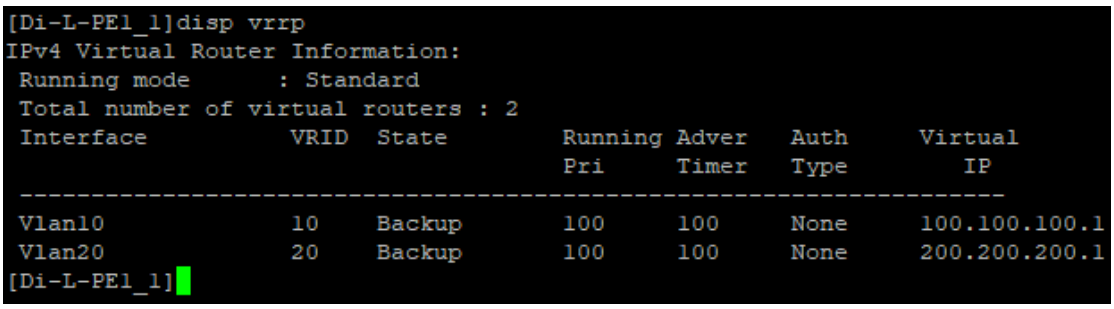

Рис. 3.4. Статус протоколу резервації доступності маршрутизаторів *VRRP*, що налаштовано між двома пристроями *PE* рівня розподілу

На (див. рис. 3.4) можна впевнитися, що зв'язок модулю рівня доступу зарезервовано протоколом *VRRP* між двома комутаторами з роллю *PE* рівня розподілу.

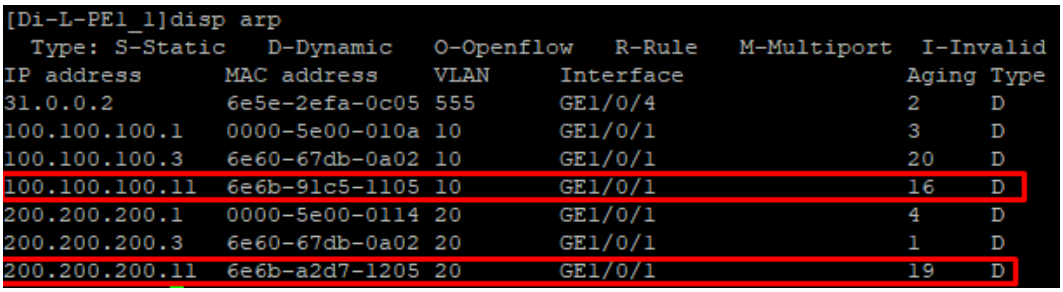

Рис. 3.5. *ARP* таблиця одного з *PE* рівню розподілу, червоним кольором виділено адреси абонентських підключень зі школи та метро

В свою чергу, (див. рис. 3.5) є підтвердженням як справного функціонування рівню доступу, так і наявної *L2* зв'язності між абонентами та *PE* рівню розподілу.

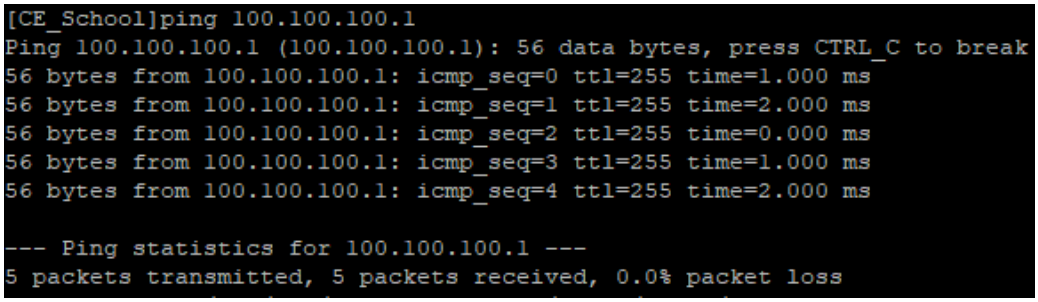

Рис. 3.6. *Ping*-запит від абонентського підключення школи до *PE* рівня розподілу

В свою чергу, (див. рис. 3.6) підтверджує справну зв'язність на рівні *L3* між абонентами та рівнем розподілу. На даному етапі можна заявити, що всі налаштування рівня доступу є справними. А налаштування *PE* рівня розподілу

достатні для організації надійного з'єднання модулів доступу з транспортною мережею *MPLS*.

```
<P1_1>sys
System View: return to User View with Ctrl+Z.
[P1_1]disp mpls ldp peer
Total number of peers: 3
Peer LDP ID              State         Role     GR   MD5  KA Sent/Rcvd
15.15.1.11:0             Operational   Active   Off  Off  311/308
15.15.1.12:0             Operational   Active   Off  Off  312/309
15.15.1.1:0              Operational   Active   Off  Off  312/312
[P1_1]
```

Рис. 3.7. Стан зв'язності мережі *MPLS*, виведений на модулі *P* рівня розподілу

На (див. рис. 3.7) можна побачити встановлену зв'язність між пристроями рівня розподілу та ядром за допомогою мережі *MPLS* (*MPLS Backbone*), це свідчить про справне налаштування *L3* для всіх пристроїв рівнів розподілу та ядра. За досягнутої зв'язності між пристроями з налаштованим *MPLS* також створюються відповідні шляхи комутації даних, відповідна таблиця виглядає наступним чином (рис. 3.8):

```
[Core]disp mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 4           Ingress: 3           Transit: 3           Egress: 1

FEC                In/Out Label        Nexthop         OutInterface
15.15.1.1/32       3/-
                   -/1151(L)
15.15.1.11/32      -/1149              31.0.0.10       GE0/0
                   1149/1149           31.0.0.10       GE0/0
15.15.1.12/32      -/1150              31.0.0.10       GE0/0
                   1150/1150           31.0.0.10       GE0/0
15.15.2.11/32      -/3                 31.0.0.10       GE0/0
                   1151/3              31.0.0.10       GE0/0
[Core]
```

Рис. 3.8. Опрацьовані та збережені шляхи мережі *MPLS*

```
[Core]disp bgp peer vpnv4

 BGP local router ID: 15.15.1.1
 Local AS number: 44444
 Total number of peers: 2                 Peers in established state: 2

  * - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  15.15.1.11           44444       29       26    0       4 00:20:52 Established
  15.15.1.12           44444       26       26    0       4 00:20:12 Established
[Core]
```

Рис. 3.9. Зв'язність *L3VPN* за допомогою *MPBGP* продемонстрована на пристрої ядра, на рисунку зображено 2 рядки встановленої зв'язності з пристроями *PE* рівня розподілу

На (див. рис. 3.9) можна побачити успішну зв'язність *L3VPN* за допомогою протоколу *MPBGP* з двома пристроями *PE* рівня розподілу. Ця інформація підтверджує не тільки успішність налаштувань *L3* між рівнями розподілу та ядра, а й означає що потоки даних відтепер не маршрутизуються а комутуються (*MPLS*). Крім того - дані повністю ізольовані по своїм категоріям (окремим *VPN*) (рис. 3.10), що значно підвищує захищеність даних та дозволяє керувати політиками доступу та якості обслуговування трафіку на рівні, що не уступає найсучаснішим засобам та технологіям керування якості надаваних послуг.

```
[Core]display ip routing-table vpn-instance School

Destinations : 14       Routes : 14

Destination/Mask   Proto   Pre  Cost        NextHop         Interface
0.0.0.0/32         Direct  0    0           127.0.0.1       InLoop0
10.10.10.0/24      Direct  0    0           10.10.10.2      GE0/1
10.10.10.0/32      Direct  0    0           10.10.10.2      GE0/1
10.10.10.2/32      Direct  0    0           127.0.0.1       InLoop0
10.10.10.255/32    Direct  0    0           10.10.10.2      GE0/1
100.100.100.0/24   BGP     255  0           15.15.1.11      GE0/0
127.0.0.0/8        Direct  0    0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0    0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0
210.50.1.0/24      BGP     255  0           10.10.10.1      GE0/1
224.0.0.0/4        Direct  0    0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0    0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0
```

Рис. 3.10. Маршрутна інформація про абонентів підключених до рівня доступу, що отримує пристрій ядра

```
[Server_School-bgp-ipv4]exit
[Server_School-bgp]exit
[Server_School]ping 100.100.100.11
Ping 100.100.100.11 (100.100.100.11): 56 data bytes, press CTRL_C to break
56 bytes from 100.100.100.11: icmp_seq=0 ttl=253 time=3.000 ms
56 bytes from 100.100.100.11: icmp_seq=1 ttl=253 time=1.000 ms
56 bytes from 100.100.100.11: icmp_seq=2 ttl=253 time=1.000 ms
56 bytes from 100.100.100.11: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 100.100.100.11: icmp_seq=4 ttl=253 time=4.000 ms

--- Ping statistics for 100.100.100.11 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
```

Рис. 3.11. Наявна зв'язність між сервером для шкіл та абонентом типу "Школа"

Останнім етапом перевірки є лістинг виконання команди *PING* (див. рис. 3.11), на якому видно наявну зв'язність між абонентським підключенням та відповідним сервером що підключено до ядра. Даний лістинг (див. рис. 3.11) є підтвердженням

справного налаштування всіх необхідних протоколів, необхідних для успішної побудови транспортної мережі муніципальної цифрової інфраструктури.

Окремо слід зазначити, що в даному прототипі упущені налаштування політик маршрутизації, що зачасту є надзвичайно важливими для фільтрування трафіку, маршрутної інформації та коректної взаємодії абонентів із серверними підключеннями. Таке упущення можливе лише в межах прототипу. В разі використання описаних ідей, підходів та рекомендацій для побудови справжньої мережі - слід надати матеріали даної роботи кваліфікованим мережевим інженерам для проектування мережі із урахуванням вимог компанії чи замовника.

3.5. Апаратна частина транспортної мережі, рекомендації та варіанти

Важливою частиною будь-якого проєкту є врахування фінансових затрат на його втілення, саме тому варто не тільки представити пояснення до проєкту, вказівки, схеми, а й його орієнтовні витрати із варіантами розрахованими на різний бюджет та сценарії розвитку.

Слід відмітити, що описаний в даній роботі метод створювався із увагою на відностно застарілі мережі та сумісність із більшістю поколінь обладнання. А тому - в реалізації мережі за описаним методом припускається використання: застарілого обладнання, обладнання що було у використанні, залишків зі складу та інших типів обладнання що розповсюджуються за уціненою вартістю. Але слід зауважити, що є дві важливі умови під час підбору обладнання: сумісність з протоколами описаними в ідеях методу як необхідні для побудови муніципальної мережі та сумісність обладнання з оптичними інтерфейсами швидкостей від 1*GE* (*SFP*) до 40*GE* (*QSFP*), в ідеалі обладнання рівня ядра має бути сумісним з оптичними інтерфейсами *QSFP*28 (100*G*).

3.5.1. Комутатори рівня доступу

Модуль рівня доступу є найменш вибагливим до налаштувань та характеристик обладнання. Так для даного рівня може підійти майже будь-який керований комутатор, від застарілих *Aruba* 2530 (350-600$) (рис. 3.12) до досить популярних *HP* 5130 (2800-4200$) (рис. 3.13)

Рис. 3.12. Комутатор *Aruba* 2530

Рис. 3.13. Комутатор *HP* 5130

Примітка: як підмічено вище – для рівня доступу підійде майже будь-який комутатор *L*2+, що підтримує протокол захищеного кільця та має можливість створення та налаштування віртуального інтерфейсу (для можливості віддаленого керування).

3.5.2. Комутатори рівня розподілу

На рівні розподілу вже потрібно використовувати досить потужні комутатори на велику кількість портів, що підтримують з'єднання *downlink* не менше 1*GE* (*SFP*) та *Uplink* не менше 10*GE* (*SFP+*) для задоволення потреби у транспортуванні великих об'ємів даних. Комутатори рівня розподілу обов'язково повинні бути *L*3 комутаторами та підтримувати всі протоколи динамічної маршрутизації, включаючи *MPBGP* (*BGP*4).

Серед популярних рішень рівня розподілу є досить широкий вибір від різних виробників. Так, наприклад, для побудови модулів рівня розподілу можна використати комутатори *HP* 5510 (7000$) (рис. 3.14), трохи менш потужний *HP* 3810*M* (5000$) та сучасний комутатор з приємною вартістю *HP* 6300*M* (4500$) (рис. 3.15). Однак хочу відмітити, що для рівня розподілу важливим параметром є можливість формувати стек. Гарними рішеннями в даному випадку є 5510 та 6300M.

Рис. 3.14. Комутатор *L*3 рівня *HP* 5510, що ідеально підходить для рівня розподілу

Рис. 3.15. Більш заощадливий екземпляр комутатору рівня розподілу *HP* 6300*M*

3.5.3. Комутатор рівня ядра

Найдорожчим екземпляром обладнанням є модуль ядра, що зазвичай представлено надпотужним комутатором (або стеком) до якого спрямовані потоки даних сотень, та навіть тисяч абонентських підключень (абонентське підключення – підключення об'єкту інфраструктури до мережі, а не індивідуальне підключення). Тому дане обладнання має бути надійним, та надзвичайно потужним.

Комутатор рівня ядра має бури навіть не *Enterprice* рівня, а виключно *DataCenter*–рішення через значні об'єми даних та необхідність обробляти дані схожим до маршрутизатор чином.

Досить надійним рішенням модуля рівня ядра, що входить до класу датацентрового обладнання є *HP FF* 12904*E Switch Chassis* (8000$) (рис. 3.16), що має потужність комутації в 11.5 *Tbps*. Даний комутатор є недорогим датацентровим рішенням, що задовольняє всім вимогам для побудови транспортної мережі муніципальної цифрової інфраструктури. Навіть одного екземпляру такого комутатору рівня ядра буде достатньо для більшості міст України. Але якщо брати до уваги перспективи зростання населення у містах, та заглянути у майбутнє на декілька десятиліть, то даного комутатору може бути недостатньо для покриття мегаполісів майбутнього.

Комутаторами, що здатні обробляти дані колосальних масштабів (ледве не об'єднати всю інфраструктуру країни) є *HP* 12908*E* (92*Tbps*, 14000$) та справжній монстр за своєю потужністю – *HP* 12916*E* (20000$) (рис. 3.17) з ємністю в 768 портів та комутаційною здатністю в 184 *Tbps* в межах одного корпусу.

Рис. 3.16. Комутатор *HP* 12904*E*

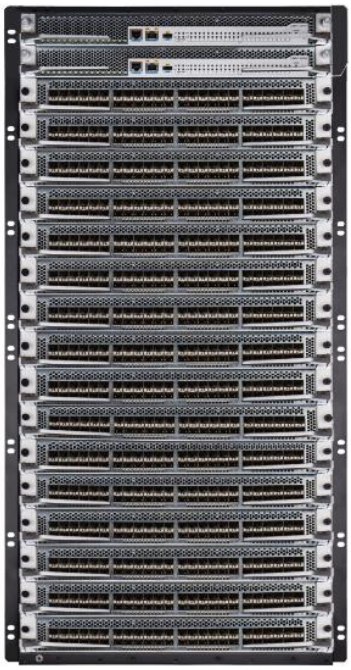

Рис. 3.17. Комутатор *HP* 12904*E*

Примітка: В межах даної роботи розглянуто лише пристрої компанії *HP* через досить широку розповсюдженість обладнання даного виробника в Україні, але обмежень на використання обладнання інших виробників не має, вибір відбувається цілковито за розсудом компанії-інтегратора та доступності обладнання виробників.

Висновки за розділом

Для того щоб рішення було втілене, воно повинне мати не лише чітке обґрунтування, гарну ідею та перспективи, рішення має також бути проаналізованим та протестованим. Тільки після цього стає доцільним взяти рішення для масової реалізації.

В даному розділі наведено: опис підходу до налаштувань та їх конкретні шаблони для кожного модулю; демонстраційний прототип та його перевірка у середовищі *H3C Cloud Lab*; рекомендації та варіанти по вибору апаратної бази транспортної мережі муніципальної цифрової інфраструктури. Демонстраційний прототип, схему якого наведено вище, побудовано цілковито за ідеями, підходами та схемами описаного методу, хоча в ньому і упущено деталізовані налаштування,

якими мережа доповнюється за бажанням, вимогами та специфікою окремої компанії, відповідальної за інтеграцію мереж.

Шаблони налаштування та демонстраційний прототип, як результати даного розділу - демонструють легку здатність до реалізації та перевірки з мінімальними трудовитратами. Детально розглянути прототип можна на відповідній схемі та у додатках з лістингами налаштувань обладнання.

Але що до удосконалення? – даний прототип мережі, як описано вище, є лише базисом, транспортною мережею, призначення якої – ефективне масштабування та об’єднання розподіленої інфраструктури, дану мережу можна змінювати та надбудовувати великою різноманітністю потреб. В транспортну мережу легко можна вбудувати засоби безпеки, керування, моніторингу, налаштувати політики безпеки та маршрутизації, адаптувати вибір обладнання та сервіси що транспортуються. Додатково варто сказати, що мережу, яку буде побудовано згідно ідей, підходів, схем та шаблонів даної роботи – в майбутньому буде доцільно використати як основу для побудови надсучасного типу мереж *SDN*.

ВИСНОВКИ

У даній магістерській роботі розроблено й запропоновано до використання уніфікований метод побудови комп'ютерних транспортних мереж муніципальної цифрової інфраструктури.

Запропонований метод включає детальний опис:

- актуальної проблематики та обґрунтування розробки методу;
- ключових ідей, що покладені в основу розроблюваного методу;
- специфіку використання мереж побудованих за використання розробленого методу;
- організації логічної структури та архітектури мережі з використанням поділу на модулі, незалежні за внутрішньою архітектурою;
- принципу ієрархічного поділу виконуваних логічних функцій мережі;
- шаблонного підходу до налаштування, підтримки, супроводження та інтеграції обладнання мережі;

Наведено детально описаний, побудований та протестований демонстраційний прототип що підтверджує працездатність та правдивість описаних ідей та підходів. Крім того в роботі наводяться рекомендації із вибору апаратної бази мережі з врахуванням можливих цінових категорій та потреб у потужності.

Мета роботи полягала в розробці методу побудови транспортних мереж для вирішення актуальних проблем цифровізації муніципальної інфраструктури міст із формулюванням відповідних принципів та підходів, що лежать в основі методу. Тому в даній роботі розроблено відповідний метод із приділенням уваги ключовим напрямам – масштабуванню та зменшенню трудовитрат на супроводження.

Особливу увагу в роботі приділено комбінації набору технологій та підходів їх використання, що допоможуть вирішити актуальні проблеми масштабування та зменшення трудовитрат на супроводження мережі за використання розробленого методу.

Ефективна масштабованість за використання розробленого методу досягається за рахунок декількох факторів:

1) специфіка трафіку муніципальної інфраструктури не вимагає великих об’ємів доступу до глобальної мережі, не створює стрибків пікового навантаження й не генерує хаотичні, непередбачувані все-сторонні запити, а отже – потреби у використанні певних технологій транспортування зміщуються в сторону тих, що ефективно обробляють та транспортують великий однорідний й передбачуваний потік інформації - саме така, направлена на ефективну взаємодію зі специфічним трафіком комбінація технологій й приводиться в розробленому методі;

2) серед технологій, описаних як необхідних приведено транспортну мережу *MPLS*, що в комбінації з технологією *L3VPN* дає змогу організувати ефективне транспортування ізольованого, поділеного на категорії трафіку з використанням мінімально-можливої надійної кількості обладнання в якості основи для транспортної мережі;

3) ефективна масштабованість, серед іншого, досягається шляхом зміщення топологічних змін при інтеграції нового обладнання в бік найнижчого рівню – розподілу, з метою усунення внесення логічних змін за інтеграції нового обладнання, нові налаштування необхідні тільки на новому екземплярі обладнання – все це можливо за комбінації модульного підходу до організації структури мережі й використанню протоколу надійного кільця *RRPP* в якості основного засобу забезпечення доступу до мережі;

Зменшення трудовитрат на побудову та супроводження мережі побудованої за розробленим методом досягається шляхом двох підходів:

1) фізична архітектура мережі поділена на модулі із висхідною залежністю, а модулі вищого рівня не залежать своїми налаштуваннями та процесами перетворення трафіку від модулів нижчого рівня - такий підхід спрощує процес підготовки нових спеціалістів (й зменшує необхідну кваліфікацію) з підтримки та супроводження мережі, оскільки уніфікує всю мережу, об’єднуючи логічну структуру в межах модулів, що залишаються архітектурно незмінними під час еволюції мережі.

2) програмна частина мережі також поділяється на незалежні частини – шаблони налаштувань у відповідності до ролі обладнання у мережі та його відношення до модуля архітектури - що значно спрощує процес налаштування та

підтримки мережі. Обладнання в межах одного рівня матиме ідентичні налаштування, відмінність в налаштуваннях існуватиме лише для спеціальних значень та параметрів, це дозволяє спеціалісту не аналізувати логіку функціонування окремого пристрою, а лише порівнювати її із існуючим шаблоном, у разі додавання нового обладнання - достатньо застосувати відповідний шаблон із введенням лише специфічної інформації для даного екземпляру.

Такі підходи до зменшення трудовитрат не тільки дозволяють зменшити складність робіт по супроводженню, зменшуючи загальну кількість персоналу підтримки, але й спрощують процеси налаштування та введення нового обладнання у експлуатацію, зменшуючи необхідний рівень кваліфікації спеціалістів.

За розробки методу важливо було не тільки надати опис ключових ідей, принципів та підходів побудови муніципальної мережі, а й привести рекомендації щодо реалізації певних моментів, серед таких рекомендацій:

1) інтегрувати за наявних ресурсів мережевий фаєрвол, на який буде передаватися вся інформація з пристрою ядра;

2) впровадити використання протоколів встановлення незалежних, захищених тунелів *AD-VPN* та безпечних тунелів вчасності – *GRE* та *IPSec*.

3) варіанти вибору апаратної бази для побудови муніципальної мережі, із урахуванням можливих цінових категорій та сценаріїв навантаження.

У роботі, серед іншого, приділено особливу увагу перевірці працездатності й можливості реалізації ідей, підходів та принципів, запропонованих у розробленому методі, як результат – в роботі наведено створення та деталізована перевірка працездатності демонстраційного прототипу муніципальної мережі із описом її можливостей та специфіки налаштування як прототипу.

У ході дослідження використано сучасні та актуальні протоколи та технології організації ефективних потоків обробки та передачі даних, серед інших, вартий особливої уваги популярний протокол *MPLS*, що використовується в багатьох муніципальних та *WAN* мережах, в якості його доповнення також використано технологію *L3VPN*, що є сучасним засобом організації ізоляції потоків маршрутної інформації.

Важливим аспектом під час вибору в якості підходу до налаштувань обладнання шаблонного підходу – є реальні складнощі під час організації процесу інтеграції нового обладнання та розвитку мережі в цілому. Процеси зміни мережі зачасту вимагають чіткого підходу, який має бути регламентованим для зменшення вірогідності внесення разом з налаштуваннями помилок. Саме для зменшення ризиків під час внесення змін до мережі та загального зменшення трудовитрат на супроводження в даній роботі пропонується шаблонний підхід но налаштувань обладнання.

Впровадження розробленого методу побудови комп'ютерних транспортних мереж муніципальної цифрової інфраструктури може допомогти в проведенні цифровізації міст та загальному покращенні якості мереж. Уніфікація мереж дозволяє переглянути відношення держави до мереж й змінити підходи до їх проєктування, побудови, експлуатації та розвитку з перекладання всіх процесів на сторонню компанію-інтегратора у область відповідальності інформаційного розвитку країни, що не тільки дозволить зменшити витрати через відсутність участі сторонніх компаній у створенні та підтримці мережі, а й дозволить створити робочі місця, де люди працюватимуть на країну.

В роботі коротко розглянуто шляхи переміщення й типові процеси перетворення трафіку на шляху від об'єктів муніципальної інфраструктури до серверного обладнання міністерств та державних установ. Запропоновано спосіб підвищення захищеності інформації в мережі через використання технології *AD-VPN* та захищених тунелів *GRE* та *IPSec*.

Отже дана магістерська робота є потенційно важливим кроком у розвитку галузі комп'ютерних мереж та саме мереж муніципального призначення. Розроблений метод створено з метою уніфікації процесу розробки та супроводу мереж, й може бути рекомендовано до використання міністерством цифрової трансформації під час загального покращення існуючих, створення нових мереж чи як готовий шаблон для реалізації проєктів компаній інтеграторів повного циклу. Метод розроблено із урахуванням майбутніх потреб із переходу на новий тип керування мережами, та муніципальну мережу, побудовану з використання розробленого уніфікованого

методу є доцільним в майбутньому використовувати як основу для впровадження мереж нового типу – *SDN* мереж.

Підсумовуючи, результатом даної роботи є уніфікований метод побудови комп'ютерних транспортних муніципальних мереж цифрової інфраструктури із детальним описом ключових ідей, підходів та принципів, покладених у метод та наведено рекомендації із організації безпеки передачі даних та підбору апаратної бази.

Для перевірки працездатності описаної комбінації технологій та підтвердження функціональності запропонованих ідей та підходів – було побудовано, проведено симуляцію та перевірено демонстраційний прототип муніципальної мережі.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Білоруський державний університет, Інформатика, теорія, тема 3: Комп'ютерні мережі. [Електронний ресурс]. – 2017. - Режим доступу: *https*://*studfile.net*/*preview*/6454542/ (дата звернення 10.12.23р). – Назва з екрана.

2. *Wikipedia*, *Ethernet* [Електронний ресурс]. - Режим доступу: *https*://*ru.wikipedia.org*/*wiki*/*Ethernet* (дата звернення 10.12.23р). – Назва з екрана.

3. *Wikipedia*, Муніципальна мережа [Електронний ресурс]. - Режим доступу: *https*://*ru.wikipedia.org*/*wiki*/%*D*0%93%*D*0%*BE*%*D*1%80%*D*0%*BE*%*D*0%*B*4%*D*1%81%*D*0%*BA*%*D*0%*B*0%*D*1%8*F*_%*D*0%*B*2%*D*1%8*B*%*D*1%87%*D*0%*B*8%*D*1%81%*D*0%*BB*%*D*0%*B*8%*D*1%82%*D*0%*B*5%*D*0%*BB*%*D*1%8*C*%*D*0%*BD*%*D*0%*B*0%*D*1%8*F*_%*D*1%81%*D*0%*B*5%*D*1%82%*D*1%8*C* (дата звернення 10.12.23р). – Назва з екрана.

4. Wikipedia, Ієрархічна модель мережі [Електронний ресурс]. - Режим доступу: *https*://*ru.wikipedia.org*/*wiki*/%*D*0%98%*D*0%*B*5%*D*1%80%*D*0%*B*0%*D*1%80%*D*1%85%*D*0%*B*8%*D*1%87%*D*0%*B*5%*D*1%81%*D*0%*BA*%*D*0%*B*0%*D*1%8*F*_%*D*0%*BC*%*D*0%*BE*%*D*0%*B*4%*D*0%*B*5%*D*0%*BB*%*D*1%8*C*_%*D*1%81%*D*0%*B*5%*D*1%82%*D*0%*B*8#:~:*text*=*Hierarchical*%20*internetworking*%20*model*)%20%*E*2%80%94%20%*D*1%82%*D*1%80%*D*1%91%*D*1%85%*D*1%83%*D*1%80%*D*0%*BE*%*D*0%*B*2%*D*0%*BD*%*D*0%*B*5%*D*0%*B*2%*D*0%*B*0%*D*1%8*F*%20%*D*0%*BC*%*D*0%*BE*%*D*0%*B*4%*D*0%*B*5%*D*0%*BB*%*D*1%8*C*,)%2*C*%20%*D*1%83%*D*1%80%*D*0%*BE*%*D*0%*B*2%*D*0%*B*5%*D*0%*BD*%*D*1%8*C*%20%*D*0%*B*4%*D*0%*BE*%*D*1%81%*D*1%82%*D*1%83%*D*0%*BF*%*D*0%*B*0%20(%*D*0%*B*0%*D*0%*BD*%*D*0%*B*3%*D*0%*BB* (дата звернення 10.12.23р). – Назва з екрана.

5. Wikipedia, Оптоволоконний кабель [Електронний ресурс]. - Режим доступу: *https*://*uk.wikipedia.org*/*wiki*/%*D*0%9*E*%*D*0%*BF*%*D*1%82%*D*0%*BE*%*D*0%*B*2%*D*0%*BE*%*D*0%*BB*%*D*0%*BE*%*D*0%*BA*%*D*0%*BE*%*D*0%*BD*%*D*0%*BD*%*D*0%*B*8%*D*0%*B*9_%*D*0%*BA*%*D*0%*B*0%*D*0%*B*1%*D*0%*B*5%*D*0%*BB*%*D*1%8*C* (дата звернення 10.12.23р). – Назва з екрана.

6. Wikipedia, *SFP* [Електронний ресурс]. - Режим доступу: *https*://*ru.wikipedia.org*/*wiki*/*SFP* (дата звернення 10.12.23р). – Назва з екрана.

7. Wikipedia, SFP+ [Електронний ресурс]. - Режим доступу: *https://ru.wikipedia.org/wiki/SFP%2B* (дата звернення 10.12.23р). – Назва з екрана.

8. Wikipedia, QSFP [Електронний ресурс]. - Режим доступу: *https://ru.wikipedia.org/wiki/QSFP* (дата звернення 10.12.23р). – Назва з екрана.

9. Wikipedia, SSH [Електронний ресурс] - Режим доступу: *https://ru.wikipedia.org/wiki/SSH* (дата звернення 10.12.23р). – Назва з екрана.

10. Andrew S. Tanenbaum Computer Networks, 5^{th} *Edition / Andrew S. Tanenbaum, David J. Wetherall; Prentice Hall,* 2011. – 960 *p.*

11. Wikipedia, DHCP [Електронний ресурс]. - Режим доступу: *https://ru.wikipedia.org/wiki/DHCP* (дата звернення 10.12.23р). – Назва з екрана.

12. В.Г. Оліфер Комп’ютерні мережі, принципи, технології, протоколи. 2-ге видання : Підручник для вищих навчальних закладів / В.Г. Оліфер, Н.А. Оліфер; Питер, 2020. – 1008с.

13. Wikipedia, Агрегація каналів [Електронний ресурс]. - Режим доступу: *https://ru.wikipedia.org/wiki/%D0%90%D0%B3%D1%80%D0%B5%D0%B3%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%BE%D0%B2* (дата звернення 10.12.23р). – Назва з екрана.

14. Wikipedia, MC-LAG [Електронний ресурс]. - Режим доступу: *https://ru.wikipedia.org/wiki/MC-LAG* (дата звернення 10.12.23р). – Назва з екрана.

15. Wikipedia, ERPS [Електронний ресурс]. - Режим доступу: *https://ru.wikipedia.org/wiki/ERPS#:~:text=ERPS%20(%D0%B0%D0%BD%D0%B3%D0%BB.,%D0%B1%D1%8B%D1%82%D1%8C%20%D0%B7%D0%B0%D0%BC%D0%B5%D0%BD%D0%BE%D0%B9%20%D1%81%D0%B5%D0%BC%D0%B5%D0%B9%D1%81%D1%82%D0%B2%D1%83%20%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%BE%D0%B2%20STP* (дата звернення 10.12.23р). – Назва з екрана.

16. Wikipedia, VRRP [Електронний ресурс]. - Режим доступу: *https://ru.wikipedia.org/wiki/VRRP* (дата звернення 10.12.23р). – Назва з екрана.

17. Wikipedia, MPLS [Електронний ресурс]. - Режим доступу: *https*://*ru.wikipedia.org*/*wiki*/*MPLS* (дата звернення 10.12.23р). – Назва з екрана.

18. Wikipedia, LDP [Електронний ресурс]. - Режим доступу: *https*://*ru.wikipedia.org*/*wiki*/*Label_Distribution_Protocol* (дата звернення 10.12.23р). – Назва з екрана.

19. Wikipedia, BGP [Електронний ресурс]. - Режим доступу: *https*://*ru.wikipedia.org*/*wiki*/*Border_Gateway_Protocol* (дата звернення 10.12.23р). – Назва з екрана.

20. Wikipedia, MPBGP [Електронний ресурс]. - Режим доступу: *https*://*en.wikipedia.org*/*wiki*/*Multiprotocol_BGP* (дата звернення 10.12.23р). – Назва з екрана.

21. Wikipedia, Мережевий комутатор [Електронний ресурс]. - Режим доступу: *https*://*ru.wikipedia.org*/*wiki*/%*D*0%*A*1%*D*0%*B*5%*D*1%82%*D*0%*B*5%*D*0%*B*2%*D*0%*BE* %*D*0%*B*9_%*D*0%*BA*%*D*0%*BE*%*D*0%*BC*%*D*0%*BC*%*D*1%83%*D*1%82%*D*0%*B*0%*D*1%82%*D*0%*BE*%*D*1%80 (дата звернення 10.12.23р). – Назва з екрана.

22. Wikipedia, Маршрутизатор [Електронний ресурс]. - Режим доступу: *https*://*ru.wikipedia.org*/*wiki*/%*D*0%9*C*%*D*0%*B*0%*D*1%80%*D*1%88%*D*1%80%*D*1%83%*D*1%82%*D*0%*B*8%*D*0%*B*7%*D*0%*B*0%*D*1%82%*D*0%*BE*%*D*1%80 (дата звернення 10.12.23р). – Назва з екрана.

23. Уенделл Одом *Cisco CCNA ICND*2 200-101, Маршрутизація та комутація: Офіційне керівництво по підготовці до сертифікаційних екзаменів: Академічне видання, *CCIE* №1624. – Вильямс, 2016. – 1008с.

24. Джеймс Куроуз Комп’ютерні мережі, Низхідний підхід, 6-е видання. / Джеймс Куроуз, Кіт Росс, – Ексмо, 2016. – 911 с.

25. ДСТУ 3008–95. Документація. Звіти у сфері науки і техніки. Структура іправила оформлення / Нац. стандарт України. – Вид. офіц. – [Чинний від 1995–02–23]. – Київ : Держспоживстандарт України, 1995. – 39 с.

26. *Hewlett-Packard HPE FlexNetwork* 5510 *HI Switch Series Configuration Guides, Release* 13*xx, Document version*: 6*W*100-20170315

27. *Hewlett-Packard HP* 5130 *EI Switch Series Configuration Examples, Part number*: 5998-7018

28. *GitBook,* Сети для самых маленьких [Електронний ресурс]. - Режим доступу: *https://linkmeup.gitbook.io/sdsm/* (дата звернення 10.12.23р). – Назва з екрана.

29. Слободян О. Положення про дипломні роботи (проєкти) випускників Національного авіаційного університету. – Київ: СМЯ НАУ, 2017. – 63 с.

ДОДАТОК А

Лістинг коду файлу конфігурації комутатора рівня розподілу

```
#
 version 7.1.059, Alpha 7159
#
 sysname R1_master
#
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 1
#
 lldp global enable
#
 system-working-mode standard
 xbar load-single
 password-recovery enable
 lpu-type f-series
#
vlan 1
#
vlan 10
#
vlan 20
#
stp region-configuration
 instance 1 vlan 10 20
 active region-configuration
#
 stp global enable
#
interface NULL0
#
interface FortyGigE1/0/53
 port link-mode bridge
#
interface FortyGigE1/0/54
 port link-mode bridge
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 combo enable fiber
 duplex full
 undo stp enable
 qos trust dot1p
 dhcp snooping trust
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 combo enable fiber
 duplex full
 undo stp enable
 qos trust dot1p
 dhcp snooping trust
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/7
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/8
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/9
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/11
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/12
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/13
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/14
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/15
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/16
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/17
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/18
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/19
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/20
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/21
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/22
 port link-mode bridge
 combo enable fiber
```

```
#
interface GigabitEthernet1/0/23
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/24
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/25
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/26
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/27
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/28
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/29
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/30
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/31
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/32
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/33
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/34
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/35
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/36
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/37
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/38
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/39
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/40
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/41
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/42
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/43
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/44
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/45
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/46
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/47
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/48
 port link-mode bridge
 combo enable fiber
#
interface M-GigabitEthernet0/0/0
#
interface Ten-GigabitEthernet1/0/49
 port link-mode bridge
 combo enable fiber
#
interface Ten-GigabitEthernet1/0/50
 port link-mode bridge
 combo enable fiber
#
interface Ten-GigabitEthernet1/0/51
 port link-mode bridge
 combo enable fiber
#
interface Ten-GigabitEthernet1/0/52
 port link-mode bridge
 combo enable fiber
#
 scheduler logfile size 16
#
line class aux
 user-role network-admin
#
line class tty
 user-role network-operator
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
line vty 0 63
 user-role network-operator
#
rrpp domain 1
 control-vlan 100
 protected-vlan reference-instance 1
 ring   1   node-mode   master   primary-port
GigabitEthernet1/0/1                    secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
 rrpp enable
#
radius scheme system
 user-name-format without-domain
#
domain system
```

```
#
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
return
```

ДОДАТОК Б

Лістинг коду файлу конфігурації комутатора *PE* рівня доступу

```
#
 sysname Di-L-PE1_1
#
ip vpn-instance Metro
 route-distinguisher 15.15.1.11:20
 vpn-target 44444:20 import-extcommunity
 vpn-target 44444:20 export-extcommunity
#
ip vpn-instance School
 route-distinguisher 15.15.1.11:10
 vpn-target 44444:10 import-extcommunity
 vpn-target 44444:10 export-extcommunity
#
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 1
#
 router id 15.15.1.11
#
ospf 1 router-id 15.15.1.11
 area 0.0.0.0
  network 15.15.1.11 0.0.0.0
  network 31.0.0.0 0.0.0.3
#
 mpls lsr-id 15.15.1.11
#
 lldp global enable
#
 system-working-mode standard
 xbar load-single
 password-recovery enable
 lpu-type f-series
#
vlan 1
#
vlan 10
#
vlan 20
#
vlan 555
 description to-P
#
stp region-configuration
 instance 1 vlan 10 20
 active region-configuration
#
 stp global enable
#
mpls ldp
#
interface NULL0
#
interface LoopBack0
 ip address 15.15.1.11 255.255.255.255
 ospf 1 area 0.0.0.0
#
interface Vlan-interface10
 ip binding vpn-instance School
 ip address 100.100.100.2 255.255.255.0
 vrrp vrid 10 virtual-ip 100.100.100.1
 vrrp vrid 10 preempt-mode delay 50
 dhcp select relay
 dhcp relay server-address 100.100.100.254
#
interface Vlan-interface20
 ip binding vpn-instance Metro
 ip address 200.200.200.2 255.255.255.0
 vrrp vrid 20 virtual-ip 200.200.200.1
 vrrp vrid 20 preempt-mode delay 50
 dhcp select relay
 dhcp relay server-address 200.200.200.254
#
interface Vlan-interface555
 description to-P
 ip address 31.0.0.1 255.255.255.252
 ospf network-type p2p
 ospf 1 area 0.0.0.0
 mpls enable
 mpls ldp enable
#
interface FortyGigE1/0/53
 port link-mode bridge
#
interface FortyGigE1/0/54
 port link-mode bridge
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 combo enable fiber
 duplex full
 undo stp enable
 qos trust dot1p
 dhcp snooping trust
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 combo enable fiber
 duplex full
 undo stp enable
 qos trust dot1p
 dhcp snooping trust
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 combo enable fiber
 duplex full
 undo stp enable
 qos trust dot1p
 dhcp snooping trust
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 description to-P
 port access vlan 555
 combo enable fiber
 undo stp enable
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/7
 port link-mode bridge
 combo enable fiber
```

```
#
interface GigabitEthernet1/0/8
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/9
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/11
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/12
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/13
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/14
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/15
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/16
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/17
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/18
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/19
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/20
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/21
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/22
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/23
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/24
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/25
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/26
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/27
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/28
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/29
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/30
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/31
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/32
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/33
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/34
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/35
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/36
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/37
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/38
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/39
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/40
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/41
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/42
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/43
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/44
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/45
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/46
```

```
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/47
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/48
 port link-mode bridge
 combo enable fiber
#
interface M-GigabitEthernet0/0/0
#
interface Ten-GigabitEthernet1/0/49
 port link-mode bridge
 combo enable fiber
#
interface Ten-GigabitEthernet1/0/50
 port link-mode bridge
 combo enable fiber
#
interface Ten-GigabitEthernet1/0/51
 port link-mode bridge
 combo enable fiber
#
interface Ten-GigabitEthernet1/0/52
 port link-mode bridge
 combo enable fiber
#
bgp 44444
 peer 15.15.1.1 as-number 44444
 peer 15.15.1.1 connect-interface LoopBack0
 #
 address-family vpnv4
  peer 15.15.1.1 enable
 #
 ip vpn-instance Metro
  peer 200.200.200.11 as-number 20
  #
  address-family ipv4 unicast
   peer 200.200.200.11 enable
 #
 ip vpn-instance School
  peer 100.100.100.11 as-number 10
  #
  address-family ipv4 unicast
   peer 100.100.100.11 enable
#
 scheduler logfile size 16
#
line class aux
 user-role network-admin
#
line class tty
 user-role network-operator
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
line vty 0 63
 user-role network-operator
#
rrpp domain 1
 control-vlan 100
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port
GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 0
 ring 1 enable
 ring 2 node-mode edge edge-port GigabitEthernet1/0/3
 ring 2 enable
#
 rrpp enable
#
radius scheme system
 user-name-format without-domain
#
domain system
#
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
return
```

ДОДАТОК В

Лістинг коду файлу конфігурації комутатора рівня Ядра

```
#
 sysname Core
#
ip vpn-instance Metro
 route-distinguisher 15.15.1.1:20
 vpn-target 44444:20 import-extcommunity
 vpn-target 44444:20 export-extcommunity
#
ip vpn-instance School
 route-distinguisher 15.15.1.1:10
 vpn-target 44444:10 import-extcommunity
 vpn-target 44444:10 export-extcommunity
#
 router id 15.15.1.1
#
ospf 1
 area 0.0.0.0
  network 15.15.1.1 0.0.0.0
  network 31.0.0.8 0.0.0.3
#
 mpls lsr-id 15.15.1.1
#
 system-working-mode standard
 xbar load-single
 password-recovery enable
 lpu-type f-series
#
vlan 1
#
mpls ldp
#
interface Serial1/0
#
interface Serial2/0
#
interface Serial3/0
#
interface Serial4/0
#
interface NULL0
#
interface LoopBack0
 ip address 15.15.1.1 255.255.255.255
 ospf 1 area 0.0.0.0
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 31.0.0.9 255.255.255.252
 ospf network-type p2p
 ospf 1 area 0.0.0.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip binding vpn-instance School
 ip address 10.10.10.2 255.255.255.0
#
interface GigabitEthernet0/2
 port link-mode route
 combo enable copper
 ip binding vpn-instance Metro
 ip address 20.20.20.2 255.255.255.0
#
interface GigabitEthernet5/0
 port link-mode route
 combo enable copper
#
interface GigabitEthernet5/1
 port link-mode route
 combo enable copper
#
interface GigabitEthernet6/0
 port link-mode route
 combo enable copper
#
interface GigabitEthernet6/1
 port link-mode route
 combo enable copper
#
bgp 44444
 peer 15.15.1.11 as-number 44444
 peer 15.15.1.11 connect-interface LoopBack0
 peer 15.15.1.12 as-number 44444
 peer 15.15.1.12 connect-interface LoopBack0
 #
 address-family vpnv4
  peer 15.15.1.11 enable
  peer 15.15.1.12 enable
 #
 ip vpn-instance Metro
  peer 20.20.20.1 as-number 200
  #
  address-family ipv4 unicast
   peer 20.20.20.1 enable
 #
 ip vpn-instance School
  peer 10.10.10.1 as-number 100
  #
  address-family ipv4 unicast
   peer 10.10.10.1 enable
#
 scheduler logfile size 16
#
line class aux
 user-role network-admin
#
line class tty
 user-role network-operator
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
line vty 0 63
 user-role network-operator
#
domain system
#
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
```

```
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
return
```