

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

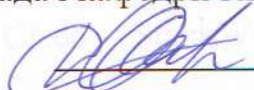
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект гетерогенної комутованої мережі з
використанням технологій стекування Cisco та
інтеграцією обладнання різних виробників.»

Виконав: студент 4-го курсу групи КІ-22-1
спеціальності 123 «Комп'ютерна інженерія»

 Богдан МЛИНСЬКИЙ

Керівник: старший викладач кафедри КІ та КБ

 Ольга ДЯЧУК

Рецензент: доцент кафедри КІ та КБ, к.т.н., доцент

 Юрій РОСІНСЬКИЙ

Житомир – 2026

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

2 лютого 2026 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Млинський Богдан Максимович

Тема роботи: «Проект гетерогенної комутованої мережі з використанням технологій стекування Cisco та інтеграцією обладнання різних виробників»

затверджена Наказом університету від 2 лютого 2026р. №97/с

Термін здачі студентом закінченої роботи 18 червня 2026р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єкт дослідження – процес побудови та функціонування комутованих мереж корпоративного рівня.

Предмет дослідження – технології стекування комутаторів Cisco, методи інтеграції обладнання різних виробників на основі стандартних протоколів і засоби централізованого моніторингу гетерогенної комутованої мережі.

Вихідні дані для роботи:

1. Структурна та логічна схеми гетерогенної комутованої мережі корпоративного рівня.
2. Технології стекування комутаторів Cisco – StackWise Plus (Catalyst 3750X) та FlexStack (Catalyst 2960S).
3. Вимоги до інтеграції обладнання різних виробників на основі відкритих стандартів – VLAN, STP/RSTP, агрегація каналів LACP (IEEE 802.3ad), SNMP.

4. Адресний план керуючого сегмента – мережа 192.168.1.0/24, керування через SVI VLAN 1.

5. Вимоги до централізованого моніторингу інфраструктури на базі системи Zabbix.

Обладнання та програмне забезпечення:

1. Комутатори Cisco Catalyst 2960S (WS-C2960S-F24TS-L) – 3 шт. (стек FlexStack).

2. Комутатори Cisco Catalyst 3750X (WS-C3750X-24P) – 2 шт. (стек StackWise Plus).

3. Комутатор ZTE ZXR10 5928.

4. Сервер для розгортання системи моніторингу Zabbix.

5. Операційна система Cisco IOS (версії 15.0 та 15.2).

6. Системне програмне забезпечення комутатора ZTE ZXR10 (підтримка smartgroup, SNMP).

7. Система моніторингу Zabbix з утилітою zabbix_sender.

8. Мова програмування Python із бібліотеками paramiko та netmiko (власний скрипт обробки подій стеку).

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Ефіменко А.А.	 2.02.26	 02.02.2026
2	Ефіменко А.А.	 2.02.26	 02.02.2026
3	Ефіменко А.А.	 2.02.26	 02.02.2026

Студент  Богдан МЛИНСЬКИЙ

Керівник  Ольга ДЯЧУК

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	02.02.2026 – 08.02.2026	Виконано
2	Аналіз технічної літератури та сучасних технологій побудови комутованих мереж	09.02.2026 – 22.02.2026	Виконано
3	Дослідження технологій стекування Cisco, гетерогенних мережевих середовищ і засобів моніторингу	23.02.2026 – 15.03.2026	Виконано
4	Аналіз вимог та розробка структури гетерогенної комутованої мережі	16.03.2026 – 29.03.2026	Виконано
5	Проектування стеків Cisco та інтеграції обладнання ZTE ZXR10	30.03.2026 – 12.04.2026	Виконано
6	Розробка адресного плану та логічної схеми мережі	13.04.2026 – 26.04.2026	Виконано
7	Налаштування мережевих пристроїв на лабораторному стенді	27.04.2026 – 10.05.2026	Виконано
8	Розгортання системи моніторингу Zabbix і розробка Python-скрипта обробки подій стеку	11.05.2026 – 24.05.2026	Виконано
9	Аналіз параметрів функціонування мережі та тестування рішення	25.05.2026 – 31.05.2026	Виконано
10	Оформлення пояснювальної записки та формування висновків	01.06.2026 – 10.06.2026	Виконано
11	Підготовка презентації та доповіді до захисту	11.06.2026 – 18.06.2026	Виконано

Студент  Богдан МЛИНСЬКИЙ

Керівник  Ольга ДЯЧУК

КККР 6 - 123 - 10 - 173

ФІКТ. Гр. А-22-1

АНОТАЦІЯ

Кваліфікаційна робота присвячена проектуванню гетерогенної комутованої мережі з використанням технологій стекування Cisco та інтеграцією обладнання різних виробників, що поєднує централізоване адміністрування, масштабованість, резервування каналів і мультивендорну сумісність у межах єдиної керованої інфраструктури з моніторингом на базі Zabbix.

Пояснювальна записка викладена на 110 сторінках, містить 28 рисунків, 11 таблиць, список використаних джерел із 20 найменувань, розміщений на 3 сторінках, та додатки.

Об'єкт дослідження – процес побудови та функціонування комутованих мереж корпоративного рівня.

Предмет дослідження – технології стекування комутаторів Cisco, методи інтеграції обладнання різних виробників на основі стандартних протоколів і засоби централізованого моніторингу гетерогенної комутованої мережі.

Метою роботи є проектування гетерогенної комутованої мережі зі стекуванням Cisco та інтеграцією мультивендорного обладнання для забезпечення ефективного управління, продуктивності, масштабованості та відмовостійкості. Застосовано методи аналізу технічної літератури, порівняння підходів до побудови мереж, структурного проектування, моделювання мережевої взаємодії та практичного налаштування й діагностики обладнання з контролем стану через SNMP.

У роботі проаналізовано архітектуру корпоративних мереж за ієрархічною моделлю та механізми Ethernet-комутації, VLAN, STP/RSTP, LACP (IEEE 802.3ad) і SNMP; досліджено технології стекування Cisco StackWise Plus і FlexStack. Розроблено структуру мережі з центральним вузлом на стеку Cisco Catalyst 3750X, вузлом доступу на стеку Cisco Catalyst 2960S та інтеграцією комутатора ZTE ZXR10 через логічний канал IEEE 802.3ad; визначено відповідність агрегації

					ККІК.КР.Б – 123 – 10 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект гетерогенної комутованої мережі з використанням технологій стекування Cisco та інтеграцією обладнання різних виробників.	Літ.	Арк.	Аркушів
Розроб.		Млинський Б.М.		17.06.26				
Керівник		Дячук О.Ю.		17.06.26			5	110
Реценз.		Росієнський Ю.М.		17.06.26		ФІКТ, Гр. КІ-22-1		
Н. контр.		Дячук О.Ю.		17.06.26				
Затверд.		Єфіменко А.А.		17.06.26				

Port-channel (Cisco) і smartgroup (ZTE) та адресний план керуючого сегмента 192.168.1.0/24 з керуванням через SVI VLAN 1.

На лабораторному стенді підтверджено працездатність рішення: учасники стеків перебувають у стані Ready з коректним розподілом ролей Master/Member, міжкомутаторні Port-channel/LACP та smartgroup працюють у режимі up/up з визначеним LACP-сусідством, верхній стек виконує роль кореневого мосту для VLAN 1, а лічильники помилок на логічних інтерфейсах нульові; водночас виявлено обмеження фізичного резервування стекового з'єднання Cisco Catalyst 3750X. Розгорнуто моніторинг Zabbix через SNMP і додатково реалізовано власний Python-скрипт, який через SSH аналізує show logging, виокремлює події Stack Manager (додавання/випадання учасника, готовність, зміну master-пристрою, стан stack-link) і передає їх у Zabbix засобами zabbix_sender із формуванням тригерів та email-сповіщень за інтервалу опитування 30 с.

Практична значущість роботи полягає в готовому проєктному рішенні гетерогенної мережі, придатному для побудови чи модернізації локальної мережі організації. Елементом практичної новизни є запропонований механізм моніторингу подій стекування Cisco на основі аналізу системного журналу, що доповнює стандартний SNMP-моніторинг і виявляє зміни складу стеку, не покриті типовими SNMP-шаблонами.

Результати роботи пройшли апробацію на 4 наукових конференціях (ІПРТК-2025, м. Київ; RS-2025, м. Дрогобич; «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир; «Інформаційно-комп'ютерні технології – 2026», м. Житомир) та опубліковані у 5 тезах доповідей.

Ключові слова: ГЕТЕРОГЕННА КОМУТОВАНА МЕРЕЖА, СТЕКУВАННЯ КОМУТАТОРІВ, CISCO CATALYST, STACKWISE PLUS, FLEXSTACK, LACP, VLAN, SNMP, ZABBIX, МУЛЬТИВЕНДОРНА ІНФРАСТРУКТУРА.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ANNOTATION

The qualification work is devoted to the design of a heterogeneous switched network using Cisco stacking technologies and the integration of equipment from different manufacturers, combining centralized administration, scalability, link redundancy and multi-vendor compatibility within a single managed infrastructure monitored with Zabbix.

The explanatory note is presented on 110 pages and contains 28 figures, 11 tables, a list of references with 20 items placed on 3 page, and appendices.

The object of research is the process of building and operating corporate-level switched networks. The subject of research is Cisco switch-stacking technologies, methods of integrating multi-vendor equipment on the basis of standard protocols, and means of centralized monitoring of a heterogeneous switched network.

The aim of the work is to design a heterogeneous switched network with Cisco stacking and multi-vendor integration to ensure efficient management, performance, scalability and fault tolerance. The applied methods include analysis of technical literature, comparison of network-design approaches, structural design, modelling of network interaction, and practical configuration and diagnostics of equipment with network-state control via SNMP.

The work analyses corporate-network architecture based on the hierarchical model and the mechanisms of Ethernet switching, VLAN, STP/RSTP, LACP (IEEE 802.3ad) and SNMP; Cisco StackWise Plus and FlexStack stacking technologies are studied. A network structure is designed with a central node on a Cisco Catalyst 3750X stack, an access node on a Cisco Catalyst 2960S stack and the integration of a ZTE ZXR10 switch via an IEEE 802.3ad logical channel; the correspondence of aggregation between Port-channel (Cisco) and smartgroup (ZTE) and the addressing plan of the management segment 192.168.1.0/24 with management via SVI VLAN 1 are defined.

The operability of the solution is confirmed on a laboratory bench: stack members are in the Ready state with a correct Master/Member role distribution, inter-switch Port-channel/LACP and smartgroup operate in up/up mode with detected LACP neighbours, the upper stack acts as the root bridge for VLAN 1, and error counters on the logical

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

interfaces are zero; at the same time, a limitation of the physical stack-link redundancy of the Cisco Catalyst 3750X is revealed. Zabbix monitoring via SNMP is deployed, and a custom Python script is additionally implemented that analyses show logging over SSH, extracts Stack Manager events (member addition/removal, readiness, master change, stack-link state) and forwards them to Zabbix via zabbix_sender, generating triggers and email notifications at a 30-second polling interval.

The practical significance of the work lies in a ready design solution for a heterogeneous network suitable for building or upgrading an organization's local network. An element of practical novelty is the proposed mechanism for monitoring Cisco stacking events based on system-log analysis, which complements standard SNMP monitoring and detects changes in stack composition not covered by typical SNMP templates.

The results were approbated at 4 scientific conferences (IIRTK-2025, Kyiv; RS-2025, Drohobych; "Computer Technologies: Innovations, Problems, Solutions", Zhytomyr; "Information and Computer Technologies – 2026", Zhytomyr) and published in 5 conference abstracts.

Keywords: HETEROGENEOUS SWITCHED NETWORK, SWITCH STACKING, CISCO CATALYST, STACKWISE PLUS, FLEXSTACK, LACP, VLAN, SNMP, ZABBIX, MULTI-VENDOR INFRASTRUCTURE.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	10
РОЗДІЛ 1 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ПОБУДОВИ КОМУТОВАНИХ МЕРЕЖ	15
1.1 Архітектурні принципи побудови корпоративних комп'ютерних мереж.....	15
1.2 Технології комутації в сучасних мережах.....	20
1.3 Технології стекування мережевих комутаторів.....	25
1.4 Особливості побудови гетерогенних мережевих середовищ.....	34
1.5 Системи моніторингу мережевої інфраструктури	37
Висновки до розділу	143
РОЗДІЛ 2 ПРОЄКТУВАННЯ ГЕТЕРОГЕННОЇ КОМУТОВАНОЇ МЕРЕЖІ.....	46
2.1 Аналіз вимог до мережевої інфраструктури організації	46
2.2 Розробка структури гетерогенної комутованої мережі	50
2.3 Проєктування стеку комутаторів Cisco	51
2.4 Інтеграція гетерогенного мережевого обладнання	56
2.5 Розробка адресного плану та сегментації мережі	60
Висновки до розділу	264
РОЗДІЛ 3 РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ РОБОТИ МЕРЕЖІ.....	66
3.1 Моделювання мережевої інфраструктури.....	66
3.2 Налаштування мережевих пристроїв.....	69
3.3 Розгортання системи моніторингу Zabbix.....	77
3.4 Аналіз параметрів функціонування мережі	87
Висновки до розділу 3	92
ВИСНОВКИ	95
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	98
ДОДАТКИ.....	101

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VLAN – Virtual Local Area Network

STP – Spanning Tree Protocol

RSTP – Rapid Spanning Tree Protocol

PVST – Per-VLAN Spanning Tree

LACP – Link Aggregation Control Protocol

SNMP – Simple Network Management Protocol

SSH – Secure Shell

IOS – Internetwork Operating System

SVI – Switch Virtual Interface

IP – Internet Protocol

MAC – Media Access Control

ARP – Address Resolution Protocol

OID – Object Identifier

ICMP – Internet Control Message Protocol

CPU – Central Processing Unit

RAM – Random Access Memory

CLI – Command Line Interface

VLAN ID – Virtual Local Area Network Identifier

ZTE – Zhongxing Telecommunication Equipment

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Сучасні корпоративні комп'ютерні мережі є невід'ємною складовою інформаційної інфраструктури підприємств, установ та організацій. Від стабільності та ефективності їх функціонування залежить доступ користувачів до інформаційних ресурсів, робота серверних служб, обмін даними між структурними підрозділами, функціонування систем моніторингу, безпеки та управління. Постійне збільшення кількості користувачів, цифрових сервісів, мережевих пристроїв і обсягів трафіку висуває підвищені вимоги до продуктивності, надійності, масштабованості та зручності адміністрування мережевої інфраструктури.

Одним із ключових елементів корпоративної мережі є комутувана інфраструктура. Саме комутатори забезпечують підключення кінцевих пристроїв, передавання кадрів у локальній мережі, логічну сегментацію за допомогою VLAN, взаємодію між окремими ділянками мережі та підключення до серверних або магістральних сегментів. У разі збільшення кількості вузлів мережі традиційне використання окремих комутаторів може ускладнювати адміністрування, підвищувати ризик помилок у конфігурації та знижувати гнучкість подальшого розширення інфраструктури.

Одним із ефективних способів вирішення цих завдань є застосування технологій стекування комутаторів. Стекування дає змогу об'єднати кілька фізичних пристроїв в єдину логічну систему, яка має спільну конфігурацію, єдину площину керування та централізоване адміністрування. Завдяки цьому спрощується керування портами, підвищується зручність масштабування мережі, зменшується складність обслуговування обладнання та створюються передумови для підвищення відмовостійкості мережевих з'єднань.

Разом із цим у реальних умовах мережеве середовище часто складається не лише з обладнання одного виробника. На практиці в одній інфраструктурі можуть одночасно використовуватися комутатори Cisco, ZTE та інших виробників. Така ситуація може бути зумовлена поступовою модернізацією мережі, обмеженнями бюджету, наявністю вже встановленого обладнання або потребою інтегрувати

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

окремі сегменти в єдину систему. У зв'язку з цим виникає необхідність побудови гетерогенних мережеских середовищ, у яких забезпечується коректна взаємодія пристроїв різних виробників.

Основою такої взаємодії є використання відкритих стандартів і поширених мережеских протоколів. До них належать VLAN для логічної сегментації мережі, STP або RSTP для запобігання петлям у комутованому середовищі, LACP для агрегації каналів між пристроями та SNMP для моніторингу стану мережеского обладнання. Використання стандартних механізмів дає змогу зменшити залежність від конкретного виробника обладнання та забезпечити сумісність різних пристроїв у межах однієї інфраструктури.

Окремого значення набуває питання моніторингу мережескої інфраструктури. Навіть правильно спроектована мережа потребує постійного контролю стану пристроїв, інтерфейсів, каналів зв'язку, завантаження портів, помилок передавання даних та інших параметрів. Для цього доцільно використовувати спеціалізовані системи моніторингу, зокрема Zabbix, який дозволяє централізовано отримувати інформацію з мережеских пристроїв за допомогою протоколу SNMP, аналізувати стан обладнання та своєчасно виявляти можливі проблеми.

Отже, розробка гетерогенної комутованої мережі з використанням технологій стекування Cisco та інтеграцією обладнання різних виробників є актуальним завданням. Такий підхід дозволяє поєднати переваги централізованого адміністрування, масштабованості, резервування каналів, мультивендорної сумісності та централізованого моніторингу мережескої інфраструктури.

Метою кваліфікаційної роботи є проектування гетерогенної комутованої мережі з використанням технологій стекування Cisco та інтеграцією обладнання різних виробників для забезпечення ефективного управління, високої продуктивності, масштабованості та відмовостійкості мережескої інфраструктури.

Для досягнення поставленої мети необхідно виконати такі завдання:

- провести аналіз сучасних технологій побудови комутованих мереж;
- розглянути архітектурні принципи побудови корпоративних комп'ютерних мереж;

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

- дослідити особливості технологій стекування комутаторів Cisco;
- проаналізувати принципи функціонування гетерогенних мережесередовищ;
- визначити способи інтеграції обладнання різних виробників за допомогою стандартних протоколів;
- розробити структуру гетерогенної комутованої мережі;
- спроектувати стек комутаторів Cisco та міжкомутаторні з'єднання;
- реалізувати механізми агрегації каналів за допомогою LACP;
- налаштувати взаємодію мережесвих пристроїв у межах єдиної інфраструктури;
- впровадити систему моніторингу мережі на базі Zabbix;
- оцінити ефективність запропонованого рішення з погляду масштабованості, керованості та відмовостійкості.

Об'єктом дослідження є процес побудови та функціонування корпоративних комутованих мереж.

Предметом дослідження є технології стекування комутаторів Cisco, засоби інтеграції обладнання різних виробників, протоколи взаємодії мережесвих пристроїв та системи моніторингу мережесвої інфраструктури.

У процесі виконання кваліфікаційної роботи використано методи аналізу технічної літератури та мережесвих технологій, метод порівняння підходів до побудови комутованих мереж, метод структурного проєктування мережесвої інфраструктури, метод моделювання мережесвої взаємодії, а також методи практичного налаштування та діагностики мережесвого обладнання. Для оцінки працездатності запропонованого рішення застосовано аналіз конфігурацій, перевірку стану стеків комутаторів, контроль роботи агрегованих каналів і моніторинг параметрів мережі через SNMP.

Наукова новизна одержаних результатів полягає в удосконаленні підходу до моніторингу стекованих комутаторів Cisco у гетерогенній мережі за рахунок поєднання стандартного SNMP-моніторингу з програмним механізмом виявлення подій стекування на основі аналізу системного журналу пристроїв. На відміну від

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

типових SNMP-шаблонів, які не відображають змін складу стеку, запропонований механізм через SSH аналізує вивід команди show logging, виокремлює події Stack Manager (додавання та випадання учасника стеку, готовність комутатора, зміну керуючого пристрою, зміну стану стекового з'єднання) і передає їх у систему Zabbix засобами zabbix_sender, що дає змогу формувати тригери та сповіщення для подій, які стандартними засобами автоматично не контролювалися, і скорочувати час їх виявлення.

Практична значущість роботи полягає у розробці проєкту гетерогенної комутованої мережі, яка поєднує стековані комутатори Cisco та обладнання іншого виробника в єдину керовану інфраструктуру. Запропоноване рішення може бути використане як основа для побудови або модернізації локальної мережі організації, де необхідно забезпечити централізоване адміністрування, резервування каналів зв'язку, логічну сегментацію мережі та контроль її стану за допомогою системи моніторингу.

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел і додатків.

У першому розділі розглянуто сучасні технології побудови комутованих мереж, принципи роботи комутаторів, технології стекування, особливості гетерогенних мережевих середовищ та засоби моніторингу мережевої інфраструктури.

У другому розділі виконано проєктування гетерогенної комутованої мережі, визначено вимоги до інфраструктури, розроблено її структуру, спроектовано стек комутаторів Cisco, описано інтеграцію обладнання різних виробників, адресний план і логічну схему мережі.

У третьому розділі наведено реалізацію та дослідження роботи мережі, описано налаштування мережевих пристроїв, розгортання системи моніторингу Zabbix, аналіз параметрів функціонування мережі та оцінку ефективності запропонованого рішення.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

РОЗДІЛ 1 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ПОБУДОВИ КОМУТОВАНИХ МЕРЕЖ

1.1 Архітектурні принципи побудови корпоративних комп'ютерних мереж

Корпоративна комп'ютерна мережа є основою інформаційної інфраструктури організації. Вона забезпечує передавання даних між робочими станціями, серверами, мережевими службами, системами зберігання інформації, засобами безпеки та іншими компонентами цифрового середовища. На відміну від невеликої локальної мережі, корпоративна мережа повинна підтримувати значну кількість користувачів, різні типи трафіку, централізоване адміністрування, контроль доступу, масштабування та стабільну роботу в умовах постійного навантаження.

Побудова такої мережі не може обмежуватися простим з'єднанням комутаторів між собою. Якщо інфраструктура розвивається без чіткої структури, з часом ускладнюється пошук несправностей, зростає кількість помилок у конфігурації, виникають проблеми з продуктивністю та резервуванням. Тому під час проєктування корпоративної інфраструктури важливо дотримуватися архітектурних принципів, які дозволяють розділити мережу на функціональні частини, визначити роль кожного пристрою та забезпечити передбачувану роботу всієї системи.

Одним із поширених підходів до побудови корпоративних мереж є ієрархічна модель. Її суть полягає в поділі мережі на кілька рівнів, кожен з яких виконує власні функції. Найчастіше виділяють рівень доступу, рівень розподілу та рівень ядра. У невеликих або середніх мережах окремі рівні можуть поєднуватися, однак сама логіка їх розподілу залишається важливою для правильного проєктування [1].

Рівень доступу є найближчим до кінцевих пристроїв і відповідає за їх фізичне підключення до мережі. Для цього рівня важливими є кількість доступних портів, підтримка VLAN, контроль стану підключень і зручність адміністрування. Якщо

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

кількість портів зростає, окремі комутатори доступу доцільно об'єднувати в стек, щоб не збільшувати кількість незалежних точок керування [4].

Особливістю рівня доступу є потреба в постійному розширенні. Якщо кількість користувачів або службових пристроїв зростає, організації доводиться додавати нові комутатори або збільшувати кількість доступних портів. У такій ситуації важливим стає не лише фізичне розширення мережі, а й збереження простоти керування. Саме тому на рівні доступу доцільно використовувати стекування комутаторів. Воно дозволяє об'єднати кілька фізичних пристроїв в один логічний комутатор, що спрощує налаштування, контроль портів і подальше масштабування.

Рівень розподілу виконує роль проміжної ланки між рівнем доступу та ядром мережі. Він агрегує трафік від комутаторів доступу, забезпечує взаємодію між окремими сегментами, може виконувати маршрутизацію між VLAN, фільтрацію трафіку, застосування політик безпеки та резервування каналів. У мережах, де використовується кілька комутаторів доступу, саме рівень розподілу дозволяє впорядкувати їх підключення та забезпечити централізовану взаємодію між різними частинами інфраструктури.

Рівень ядра призначений для швидкісного передавання трафіку між основними ділянками мережі. Його головними характеристиками є висока пропускна здатність, мінімальна затримка, надійність і стабільність роботи [2]. У великих мережах ядро є окремим функціональним рівнем, до якого підключаються пристрої рівня розподілу, серверні сегменти, зовнішні канали та інші критично важливі компоненти. У менших інфраструктурах функції ядра та розподілу можуть виконуватися одним рівнем обладнання, однак навіть у такому випадку необхідно враховувати резервування, агрегацію каналів і контроль навантаження [8].

Ієрархічна структура робить мережу зрозумілішою для адміністратора. Якщо кожен рівень виконує чітко визначені функції, легше планувати розвиток інфраструктури, аналізувати потоки трафіку, визначати точки можливих відмов і впроваджувати засоби моніторингу. Крім того, такий підхід спрощує

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

документування мережі, оскільки кожен комутатор, канал або логічний сегмент має зрозуміле місце у загальній архітектурі.

Для корпоративних мереж важливим є не тільки правильне розміщення обладнання, а й логічна організація трафіку. У межах однієї фізичної інфраструктури можуть працювати різні групи користувачів, адміністративні підрозділи, серверні ресурси, системи відеоспостереження, телефонія та службові пристрої. Якщо всі ці вузли знаходяться в одному ширококомовному домені, мережа стає менш керованою, а ширококомовний або помилковий трафік впливає на більшу кількість пристроїв. Для вирішення цієї проблеми застосовується логічна сегментація мережі.

Основним засобом логічної сегментації у комутованих мережах є VLAN. Використання VLAN дозволяє розділити одну фізичну мережу на кілька логічних сегментів. Кожен такий сегмент може відповідати окремому підрозділу, типу обладнання або службовому призначенню. Завдяки цьому зменшується розмір ширококомовних доменів, підвищується керованість мережі та створюються умови для застосування політик доступу між різними групами пристроїв.

Однак сама наявність VLAN не вирішує всі завдання побудови комутованої мережі. Потрібно також забезпечити правильну взаємодію між комутаторами, передавання трафіку через міжкомутаторні з'єднання та запобігання петлям на другому рівні моделі OSI. Якщо між комутаторами існує кілька фізичних шляхів і відсутні механізми контролю, у мережі можуть виникати комутаційні петлі. Вони призводять до дублювання кадрів, перевантаження каналів, нестабільності MAC-таблиць і втрати працездатності мережевого сегмента [3].

Для запобігання таким ситуаціям у комутованих мережах застосовуються протоколи сімейства Spanning Tree. Вони дозволяють побудувати логічну безпетельну топологію навіть тоді, коли фізично між комутаторами існують резервні з'єднання. Протокол визначає кореневий комутатор, аналізує вартість шляхів і переводить частину портів у стан блокування, якщо це необхідно для усунення петлі. У сучасних мережах часто використовується RSTP, який забезпечує швидшу перебудову топології порівняно з класичним STP [6].

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

У корпоративній мережі важливо поєднати резервування та контроль топології. З одного боку, резервні канали потрібні для підвищення надійності. З іншого боку, надлишкові з'єднання можуть створити петлі, якщо вони не контролюються відповідними протоколами. Тому проєктування комутованої інфраструктури передбачає поєднання резервування, протоколів запобігання петлям і механізмів агрегації каналів.

Агрегація каналів дозволяє об'єднати кілька фізичних з'єднань між комутаторами в один логічний канал. У результаті підвищується сумарна пропускна здатність і забезпечується вища стійкість до відмов окремих фізичних ліній. Одним із поширених стандартних механізмів агрегації є LACP. Його перевагою є можливість роботи між обладнанням різних виробників, якщо ці пристрої підтримують відповідний стандарт. Це робить LACP важливим елементом гетерогенних мережевих середовищ.

З погляду архітектури корпоративної мережі стекування комутаторів і агрегація каналів виконують різні функції. Стекування спрощує керування групою фізичних комутаторів і дозволяє розглядати їх як один логічний пристрій. Агрегація каналів забезпечує ефективніші міжкомутаторні з'єднання та може підвищувати надійність передавання даних між різними частинами мережі. У поєднанні ці технології дозволяють створити інфраструктуру, яка легше масштабується та простіше адмініструється.

Ще одним важливим архітектурним принципом є керованість мережі. Навіть правильно побудована інфраструктура не може ефективно експлуатуватися без постійного контролю її стану. Адміністратор повинен мати можливість бачити доступність комутаторів, стан портів, навантаження каналів, помилки передавання та зміни в роботі обладнання. Для цього використовуються системи моніторингу, які збирають інформацію з мережевих пристроїв і надають її у зручному для аналізу вигляді.

У гетерогенних мережах особливого значення набуває використання стандартних протоколів моніторингу. Якщо мережа побудована на обладнанні різних виробників, адміністратор не завжди може покладатися на один фірмовий

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

інструмент керування. Тому доцільно застосовувати універсальні засоби, які працюють із різними типами пристроїв. Одним із таких механізмів є SNMP. Він дозволяє отримувати від мережевого обладнання інформацію про його стан, інтерфейси, лічильники трафіку, помилки та інші параметри, важливі для експлуатації мережі.

Окрему увагу слід приділяти сумісності обладнання. У багатьох організаціях мережа формується поступово, тому в ній можуть одночасно використовуватися пристрої різних поколінь і різних виробників. Якщо інфраструктура залежить лише від пропрієтарних технологій одного виробника, інтеграція іншого обладнання може бути ускладненою. Саме тому під час побудови гетерогенної мережі важливо спиратися на стандартизовані механізми взаємодії.

Сумісність у комутованій мережі забезпечується насамперед через використання загальноприйнятих протоколів. VLAN дозволяє створювати логічні сегменти незалежно від виробника комутатора, STP або RSTP дає змогу контролювати петлі у мережах другого рівня, LACP використовується для агрегації каналів, а SNMP дозволяє підключати обладнання до єдиної системи моніторингу. Такий підхід зменшує технічні ризики та робить інфраструктуру більш гнучкою.

Під час проєктування корпоративної мережі також необхідно розділяти фізичну та логічну структуру. Фізична топологія показує, як саме з'єднані між собою комутатори, сервери, робочі станції та інші пристрої. Логічна структура описує, як організовано передавання трафіку, які VLAN використовуються, які пристрої виконують функції агрегації, де знаходяться керуючі адреси та які канали є основними. Для адміністратора важливо розуміти обидва рівні, оскільки фізично проста схема може мати складну логічну організацію.

Правильно спроектована мережа повинна мати чітку систему іменування пристроїв, зрозумілий адресний план і логічний поділ на сегменти. Імена комутаторів мають відображати їхню роль або місце в інфраструктурі. IP-адреси керування повинні бути впорядкованими та належати до визначеного керуючого сегмента. VLAN мають створюватися відповідно до функцій користувачів, служб

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

або типів обладнання. Такий підхід зменшує кількість помилок під час експлуатації та полегшує документування мережі.

Документування є важливою частиною архітектурного проектування. До документації доцільно включати структурну схему, логічну схему, адресний план, таблицю VLAN, опис міжкомутаторних з'єднань, інформацію про логічні канали, параметри моніторингу та короткий опис ролі кожного пристрою. Наявність такої інформації дозволяє швидше виконувати діагностику, планувати зміни та супроводжувати мережу після впровадження.

У межах даної роботи архітектурні принципи корпоративних мереж є основою для подальшого проектування гетерогенної комутованої інфраструктури. Проектована мережа повинна поєднувати структурованість, масштабованість, сумісність і керованість. Для досягнення цих властивостей використовуються стекування комутаторів Cisco, стандартні протоколи взаємодії, логічна сегментація та централізований моніторинг.

Отже, корпоративна комутована мережа повинна проектуватися як цілісна система, у якій кожен елемент має визначене функціональне призначення. Рівень доступу забезпечує підключення кінцевих пристроїв, рівень розподілу агрегує трафік і поєднує окремі сегменти, а рівень ядра або його функціональний аналог забезпечує швидкісну взаємодію між основними частинами інфраструктури. Розглянуті архітектурні принципи створюють основу для подальшого аналізу технологій комутації, стекування та побудови гетерогенних мережевих середовищ.

1.2 Технології комутації в сучасних мережах

Комутація визначає спосіб передавання Ethernet-кадрів усередині локальної мережі. На відміну від фізичного з'єднання пристроїв, комутація працює з адресною інформацією канального рівня та приймає рішення на основі MAC-адрес. Саме тому в цьому підрозділі розглядаються механізми формування MAC-таблиці, типи портів, VLAN, trunk-з'єднання та протоколи захисту від петель.

На відміну від концентраторів, які передавали отриманий сигнал на всі порти, комутатори аналізують службову інформацію в кадрах і приймають рішення про подальше передавання даних. Основою такого рішення є MAC-адреса пристрою

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

призначення. Комутатор не просто повторює сигнал, а визначає, через який порт доступний потрібний вузол. Завдяки цьому зменшується обсяг зайвого трафіку, ефективніше використовується пропускна здатність і знижується навантаження на кінцеві пристрої.

Основним механізмом роботи комутатора є формування таблиці MAC-адрес. Коли комутатор отримує кадр на певний порт, він аналізує MAC-адресу відправника та запам'ятовує, через який інтерфейс цей пристрій доступний. Надалі, якщо кадр призначений для відомої MAC-адреси, він передається лише через відповідний порт. Якщо адреса призначення ще невідома, комутатор тимчасово розсилає кадр на всі порти в межах відповідного широкомовного домену, крім порту, з якого кадр було отримано.

Таблиця MAC-адрес формується динамічно. Якщо пристрій переміщується з одного порту на інший, комутатор оновлює відповідний запис. Якщо пристрій тривалий час не передає дані, запис може бути видалений. У стабільній мережі ці процеси не помітні для користувачів. Проблеми виникають тоді, коли одна й та сама MAC-адреса починає з'являтися на різних портах. Найчастіше це пов'язано з петлями другого рівня або помилками в міжкомутаторних з'єднаннях. У такому випадку MAC-таблиця стає нестабільною, а передавання кадрів може порушуватися.

Комутатори працюють переважно на каналному рівні моделі OSI. На цьому рівні основними одиницями передавання є кадри, а адресація здійснюється за допомогою MAC-адрес. Водночас сучасні комутатори підтримують значно ширший набір функцій: VLAN, агрегацію каналів, протоколи Spanning Tree, засоби безпеки портів, моніторинг, списки контролю доступу та маршрутизацію між VLAN. Тому в корпоративній мережі комутатор є не лише пристроєм передавання кадрів, а й важливим елементом керування інфраструктурою.

Однією з переваг комутованих мереж є поділ середовища передавання на окремі колізійні домени. У мережах на базі концентраторів кілька пристроїв використовували спільне середовище, тому могли виникати колізії. У комутованій мережі кожен порт є окремим сегментом, а підключення зазвичай працює в

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

повнодуплексному режимі. Це означає, що пристрій може одночасно передавати й отримувати дані. Для стабільної роботи важливо, щоб обидва кінці з'єднання мали узгоджені параметри швидкості та дуплексу, інакше можливі помилки кадрів, повторні передавання та зниження продуктивності.

Швидкість інтерфейсів має значення не тільки для кінцевих підключень, а й для міжкомутаторних каналів. У реальних інфраструктурах можуть одночасно використовуватися Fast Ethernet, Gigabit Ethernet і швидші інтерфейси. Для робочих станцій може бути достатньо меншої швидкості, тоді як міжкомутаторні з'єднання, серверні підключення та магістральні ділянки потребують більшої пропускної здатності. Якщо канал між комутаторами перевантажений, він стає вузьким місцем для всього сегмента.

Важливим елементом комутованої мережі є тип порту. Access-порт використовується для підключення кінцевого пристрою та належить до однієї VLAN. Trunk-порт застосовується для передавання трафіку кількох VLAN між комутаторами або між комутатором та іншим мережевим пристроєм. Помилка в налаштуванні типу порту може призвести до недоступності частини сегментів або некоректного передавання трафіку.

Логічна сегментація за допомогою VLAN є однією з основних технологій сучасної комутації. Без VLAN усі пристрої в межах однієї локальної мережі можуть належати до одного широкомовного домену. Для невеликої мережі це може бути прийнятним, але зі збільшенням кількості вузлів такий підхід ускладнює адміністрування. VLAN дозволяє розділити одну фізичну інфраструктуру на кілька логічних сегментів, зменшити розмір широкомовних доменів і створити основу для застосування політик доступу.

VLAN дозволяє розділити одну фізичну комутовану інфраструктуру на кілька логічних сегментів. Кожен сегмент може мати власне призначення: користувацький трафік, керування обладнанням, серверні підключення або службові системи. Для передавання кількох VLAN між комутаторами використовуються trunk-порти та тегування кадрів. Завдяки цьому одна фізична лінія може передавати трафік кількох логічних мереж.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Для передавання трафіку кількох VLAN між комутаторами використовується тегування кадрів. До кадру додається службова інформація, яка визначає належність до конкретної VLAN. Завдяки цьому один міжкомутаторний канал може передавати трафік кількох логічних сегментів. Це зменшує потребу в окремих фізичних лініях для кожної VLAN і робить мережу гнучкішою для подальшого розширення.

Використання VLAN потребує правильної документації. Адміністратор повинен розуміти, які VLAN створені, які порти до них належать, які міжкомутаторні з'єднання працюють у trunk-режимі та які сегменти передаються через ці канали. Без такої інформації пошук несправностей може суттєво ускладнитися, особливо в мережі з обладнанням різних виробників.

Окрему увагу в комутованих мережах потрібно приділяти запобіганню петлям на каналному рівні. Петля може виникнути тоді, коли між комутаторами існує кілька фізичних шляхів, а механізм контролю топології не налаштований або працює некоректно. У такій ситуації кадри можуть багаторазово передаватися між комутаторами. Це призводить до перевантаження каналів, нестабільності MAC-таблиць і порушення роботи мережевого сегмента.

Для запобігання таким проблемам застосовуються протоколи сімейства Spanning Tree. Їхнє завдання полягає у створенні логічної безпетельної топології навіть тоді, коли фізично в мережі є резервні з'єднання. Протокол визначає кореневий комутатор, аналізує доступні шляхи та переводить окремі порти у відповідні стани. Завдяки цьому мережа може мати надлишкові фізичні зв'язки, але залишатися стабільною на другому рівні.

Класичний STP забезпечує базовий захист від петель, однак перебудова топології після зміни стану каналу може займати помітний час. У сучасних мережах часто застосовуються швидші варіанти, зокрема RSTP або реалізації, побудовані на його принципах. Для обладнання Cisco поширеним режимом є Rapid PVST+, який дозволяє використовувати швидку перебудову топології окремо для VLAN.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

У цій роботі STP і RSTP розглядаються як механізми забезпечення стабільності комутованої інфраструктури. Це важливо для мережі, у якій використовуються стековані комутатори та кілька міжкомутаторних з'єднань. Водночас потрібно враховувати фактичні налаштування конкретних пристроїв.

Ще однією технологією сучасних комутованих мереж є агрегація каналів. Її призначення полягає в об'єднанні кількох фізичних з'єднань в один логічний канал. Такий підхід може підвищити сумарну пропускну здатність між пристроями та зменшити вплив відмови окремої фізичної лінії. Для адміністратора агрегований канал відображається як один логічний інтерфейс, хоча фактично може складатися з кількох портів.

Одним із поширених стандартних механізмів агрегації є LACP. Його перевага полягає в тому, що він дозволяє автоматично узгоджувати формування агрегованого каналу між пристроями. Якщо обидві сторони підтримують LACP і налаштовані коректно, вони обмінюються службовими повідомленнями та визначають, які порти входять до складу логічного каналу. Це зменшує ризик помилок порівняно зі статичним об'єднанням інтерфейсів.

Для гетерогенних мереж LACP має окреме значення, оскільки є стандартним механізмом і може використовуватися між обладнанням різних виробників. У такій інфраструктурі не завжди можливо застосовувати фірмові протоколи одного виробника. Стандартна агрегація дозволяє підготувати підключення Cisco до обладнання іншого виробника, зберігаючи передбачувану логіку міжкомутаторного з'єднання. У практичній частині цієї роботи важливо розділяти проєктну можливість агрегації та фактичний стан підключення, оскільки до ZTE використовується один фізичний канал, хоча сама логіка підключення може бути розширена.

Під час налаштування агрегованих каналів порти, які входять до одного логічного інтерфейсу, повинні мати узгоджені параметри. Вони мають працювати з однаковою швидкістю, сумісним режимом дуплексу, однаковим типом порту та відповідною VLAN-конфігурацією. Якщо параметри фізичних інтерфейсів відрізняються, канал може не сформуватися або працювати нестабільно. Тому

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

діагностика EtherChannel або LACP повинна включати перевірку стану логічного інтерфейсу, його фізичних учасників, лічильників помилок і LACP-сусідів.

Технології комутації пов'язані також із моніторингом і діагностикою. Комутатор повинен не лише передавати кадри, а й надавати адміністратору інформацію про стан інтерфейсів, швидкість, кількість переданих і отриманих пакетів, помилки, стан логічних каналів і доступність пристрою. Без такої інформації складно оцінити реальний стан мережі та своєчасно виявити проблеми.

Для отримання службової інформації з мережевих пристроїв часто використовується SNMP. Він дозволяє системі моніторингу звертатися до комутатора та отримувати параметри його роботи. У гетерогенних мережах SNMP є корисним, оскільки підтримується багатьма виробниками обладнання та дозволяє об'єднати моніторинг різних пристроїв у межах однієї системи. Детальніше роль SNMP і Zabbix розглядається в підрозділі 1.5.

Отже, технології комутації є технічною основою корпоративної мережі. Вони забезпечують передавання кадрів, формування MAC-таблиць, логічну сегментацію за допомогою VLAN, передавання трафіку між комутаторами через access- і trunk-порти, захист від петель за допомогою STP або RSTP, а також можливість використання LACP для логічного об'єднання фізичних каналів. Для цієї кваліфікаційної роботи ці механізми мають практичне значення, оскільки проєктована мережа поєднує стековані комутатори Cisco, обладнання ZTE та централізований моніторинг.

1.3 Технології стекування мережевих комутаторів

Стекування комутаторів використовується тоді, коли кілька фізичних пристроїв потрібно об'єднати в один логічний вузол керування. Для адміністратора такий вузол виглядає як один комутатор із загальною конфігурацією, єдиною системою керування та спільною логікою роботи інтерфейсів. У цій роботі стекування є ключовим механізмом організації Cisco-частини мережі, оскільки дозволяє замінити групу окремих комутаторів двома логічними стекованими вузлами.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Стекування полягає в об'єднанні кількох фізичних комутаторів у єдину логічну систему. Для адміністратора така група пристроїв відображається як один комутатор із загальною конфігурацією, єдиною системою керування та спільною логікою роботи. Фізично в мережі може бути встановлено кілька пристроїв, але з погляду адміністрування вони працюють як один керований вузол. Це особливо корисно на рівні доступу, де зазвичай потрібна велика кількість портів.

Основна перевага стекування полягає не лише у збільшенні кількості портів. Звичайне додавання окремого комутатора також розширює мережу, але кожен такий пристрій залишається окремим об'єктом адміністрування. Він має власну конфігурацію, окремі параметри доступу, моніторингу та службових протоколів. У стеку ці пристрої об'єднуються в одну систему, що зменшує кількість точок керування та робить мережу більш впорядкованою.

Стек комутаторів має спільну площину керування. Налаштування більшості параметрів виконується централізовано через один логічний пристрій. Адміністратор може переглядати стан портів усіх комутаторів стеку, налаштовувати VLAN, перевіряти інтерфейси, контролювати таблиці MAC-адрес і виконувати діагностику без окремого підключення до кожного фізичного комутатора.

У стеку один із комутаторів зазвичай виконує роль головного пристрою. Він відповідає за керування стеком, обробку конфігурації та координацію роботи інших учасників. Інші комутатори працюють як члени стеку. У низці реалізацій також передбачена резервна роль, коли один із пристроїв може прийняти функції керування у разі відмови головного. Така побудова зменшує залежність від одного фізичного вузла [5].

Розподіл ролей у стеку має практичне значення. Головний комутатор забезпечує логіку керування, але інші пристрої не є пасивними. Вони обслуговують підключені до них порти, передають трафік і залишаються частинами одного логічного комутатора. Нумерація інтерфейсів у стеку зазвичай відображає номер фізичного комутатора, номер модуля та номер порту. Завдяки цьому можна визначити, на якому саме пристрої розташований потрібний інтерфейс.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Стекування спрощує масштабування. Якщо потрібно збільшити кількість портів, до стеку можна додати сумісний комутатор. Загальна кількість портів зростає, але логіка адміністрування залишається централізованою. Це зручно для мереж, які розширюються поступово і не повинні перетворюватися на набір окремих слабо пов'язаних пристроїв.

Стекування також зменшує складність внутрішніх міжкомутаторних з'єднань. Якщо кілька окремих комутаторів з'єднані звичайними Ethernet-портами, адміністратор повинен контролювати trunk-з'єднання, STP, VLAN і можливі петлі між ними. У стеку взаємодія між фізичними пристроями реалізується через спеціалізовані стекові з'єднання або модулі. Завдяки цьому група комутаторів працює як єдиний пристрій, а внутрішня взаємодія не потребує такої самої логіки, як звичайні міжкомутаторні Ethernet-з'єднання.

Стекування корисне не тільки на рівні доступу, а й у вузлах розподілу. На рівні доступу воно дозволяє отримати більшу кількість портів і зберегти єдину точку керування. На рівні розподілу стек може виконувати роль центрального комутаційного вузла, до якого підключаються нижчі сегменти або обладнання іншого виробника. У такій схемі важливими стають правильне розташування uplink-підключень, контроль стекових портів і моніторинг стану вузла.

З погляду відмовостійкості стекування має переваги, але не замінює всі інші механізми резервування. Фізична відмова одного комутатора не обов'язково означає повну втрату роботи всього логічного вузла, оскільки інші члени стеку можуть продовжувати обслуговувати свої порти. Якщо стек підтримує резервування керування, інший пристрій може прийняти роль головного. Водночас критичні підключення не слід зосереджувати на одному фізичному члені стеку, оскільки його відмова все одно може вплинути на важливу частину мережі.

Для підвищення надійності важливі з'єднання доцільно розподіляти між різними членами стеку. Наприклад, логічний канал може використовувати фізичні порти, розташовані на різних комутаторах одного стеку, якщо така можливість підтримується платформою. У цьому випадку відмова одного фізичного комутатора не обов'язково призводить до повної втрати логічного з'єднання.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Стекування також полегшує документування. Замість опису кількох незалежних комутаторів можна описувати один логічний вузол із зазначенням фізичного складу стеку, ролей його членів, номерів пристроїв, портів і міжкомутаторних підключень. Така документація спрощує експлуатацію та допомагає швидше визначити, до якого пристрою належить конкретний порт.

Водночас стекування має обмеження. Не всі моделі комутаторів підтримують роботу в стеку. Навіть у межах одного виробника можуть існувати різні технології стекування, які не є взаємозамінними. Комутатори мають бути сумісними за апаратною платформою, стековими модулями, кабелями та програмним забезпеченням. Якщо ці умови не виконуються, пристрої не зможуть працювати як єдиний стек або робота стеку буде нестабільною.

Ще одним обмеженням є залежність від стекових з'єднань. Якщо стекові кабелі або модулі працюють некоректно, це впливає на взаємодію між членами стеку. Тому під час експлуатації потрібно контролювати склад стеку, ролі комутаторів, стан стекових портів і наявність сусідів. Крім того, помилка в конфігурації логічного вузла може вплинути одразу на всі комутатори стеку, тому стекування не скасовує потреби в перевірці змін і документуванні налаштувань.

Однією з поширених технологій стекування Cisco є StackWise. Вона використовується в комутаторах сімейства Cisco Catalyst і дозволяє об'єднувати кілька фізичних пристроїв в один логічний комутатор. У такій схемі керування стеком здійснюється через одну конфігурацію, а порти різних фізичних комутаторів відображаються як інтерфейси одного пристрою.

Для комутаторів Cisco Catalyst 3750X використовується StackWise Plus. Ця технологія передбачає використання спеціалізованої стекової шини та окремих стекових інтерфейсів, через які комутатори обмінюються службовою інформацією, даними керування та трафіком між членами стеку. На відміну від звичайного з'єднання через Ethernet-порти, стекові інтерфейси призначені саме для внутрішньої взаємодії учасників стеку.

Архітектурно StackWise Plus використовує кільцеву топологію. Кожен комутатор має два стекові порти, що дозволяє сформувати замкнене кільце. Якщо

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

один стековий канал виходить з ладу, стек може продовжити роботу через альтернативний шлях, однак внутрішня пропускна здатність і стійкість такої схеми зменшуються. Тому під час експлуатації важливо контролювати стан усіх стекових портів і підтримувати кільцеву структуру, якщо це можливо.

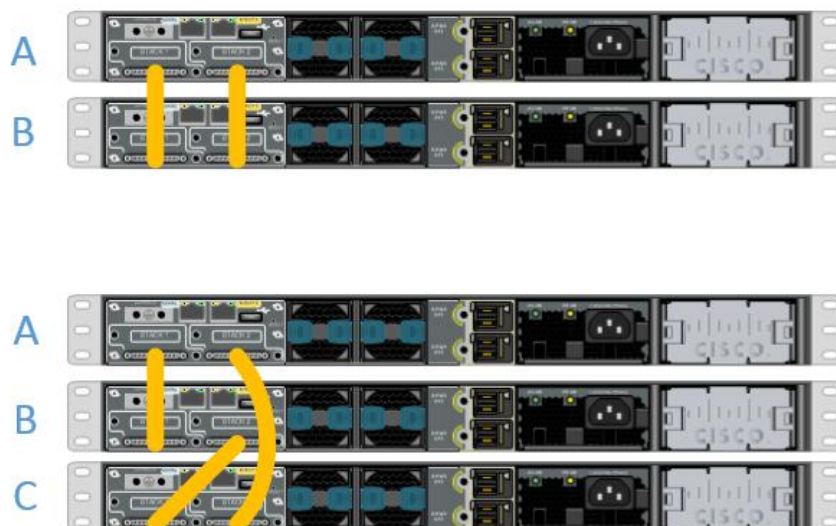


Рисунок 1.1 – Схема з'єднання комутаторів у StackWise

У стеку Cisco керуюча роль може називатися master або active залежно від покоління обладнання. Її сутність однакова: головний комутатор координує роботу стеку та обробляє керуючі функції. Інші пристрої працюють як члени стеку. У деяких реалізаціях передбачений standby-комутатор, який може прийняти керування у разі відмови основного пристрою

Таблиця 1.1

Основні ролі комутаторів у стеку Cisco

Роль	Призначення
Master (Active)	Керує стеком, обробляє конфігурацію та службові процеси
Standby	Резервний керуючий вузол, готовий перебрати функції master
Member	Звичайний член стеку, який обслуговує власні інтерфейси
Provisioned	Попередньо зарезервований запис для майбутнього комутатора

Вибір головного комутатора залежить від пріоритету, MAC-адреси, часу запуску, наявності збереженої конфігурації та особливостей конкретної платформи. Адміністратор може впливати на цей процес, задаючи пріоритети учасникам стеку. Це потрібно для того, щоб керуючу роль отримував пристрій, який є найбільш доцільним з погляду фізичного розміщення, стабільності живлення або підключення ключових каналів.

Для діагностики StackWise використовуються команди, які дозволяють перевірити склад стеку, ролі учасників, стан стекових портів і версію програмного забезпечення.

Таблиця 1.2

Основні команди діагностики StackWise

Команда	Призначення
show switch	Перегляд складу стеку та ролей комутаторів
show switch detail	Детальна інформація про членів стеку
show switch stack-ports	Стан стекових портів
show switch neighbors	Інформація про сусідні комутатори стеку
show platform stack-manager all	Детальна діагностика стекового менеджера
show version	Перевірка версії IOS та ролі пристрою

Якщо один із комутаторів не відображається у складі стеку або стековий порт має проблемний стан, це може свідчити про несправність кабелю, стекового модуля або самого пристрою. Такі параметри потрібно перевіряти не лише під час первинного налаштування, а й у процесі експлуатації.

Важливою можливістю StackWise є підтримка Cross-Stack EtherChannel. У такому режимі фізичні інтерфейси одного Port-channel можуть належати різним комутаторам стеку. Це дозволяє будувати більш стійкі uplink-з'єднання без окремої складної схеми резервування. У разі відмови одного фізичного комутатора логічний канал може продовжити роботу через інший інтерфейс, якщо така схема правильно налаштована.

Окремо слід розглянути FlexStack, яка використовується для стекування комутаторів Cisco Catalyst 2960S. За концепцією вона також дозволяє об'єднати кілька фізичних комутаторів в один логічний пристрій, однак орієнтована переважно на рівень доступу. Для реалізації FlexStack використовуються спеціальні стекові модулі та кабелі, які забезпечують взаємодію комутаторів через окремі стекові з'єднання.

FlexStack створює єдину площину керування для групи комутаторів доступу. Адміністратор може переглядати стан усіх фізичних пристроїв стеку, їхні ролі, номери, порти та загальний стан. Порівняно зі StackWise Plus ця технологія має скромніші характеристики щодо кількості учасників і пропускної здатності внутрішньої стекової шини, однак для рівня доступу цього зазвичай достатньо.

Таблиця 1.3

Порівняння StackWise Plus та FlexStack

Характеристика	StackWise Plus	FlexStack
Максимальна кількість комутаторів	До 9	До 4
Тип застосування	Рівень розподілу, ядро	Рівень доступу
Стекова архітектура	Кільцева	Кільцева
Підтримка Cross-Stack EtherChannel	Так	Так
Централізоване керування	Так	Так
Резервування керування	Так	Так

Основна різниця між StackWise Plus і FlexStack полягає в апаратній платформі, продуктивності стекового з'єднання, кількості підтримуваних учасників і типовому призначенні. StackWise Plus більше підходить для продуктивніших сценаріїв, зокрема для вузлів розподілу. FlexStack доцільніше використовувати на рівні доступу, де головними вимогами є кількість портів, централізоване керування та простіше розширення.

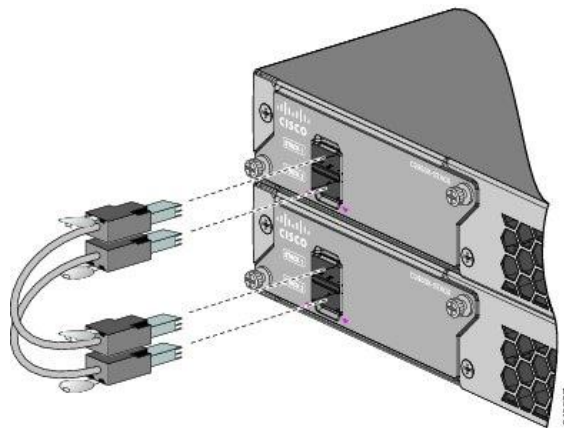


Рисунок 1.2 – Об'єднання у FlexStack

Стекування не є єдиним способом побудови масштабованої комутаційної інфраструктури. Альтернативою можуть бути традиційні міжкомутаторні з'єднання з використанням LACP та протоколів Spanning Tree. У цьому випадку кожен комутатор залишається окремим пристроєм зі своєю конфігурацією, а зв'язок між ними організовується через логічні або резервні канали. Такий підхід простіший з погляду сумісності, але складніший в адмініструванні.

Інший клас альтернатив становлять технології віртуалізації комутаторів, які використовуються різними виробниками: Cisco Virtual Switching System, Cisco StackWise Virtual, HPE IRF, Aruba VSF або Juniper Virtual Chassis. Вони можуть забезпечувати єдину площину керування і вищий рівень відмовостійкості, але зазвичай потребують іншого класу обладнання та складнішого проектування.

Таблиця 1.4

Порівняння стекування та альтернативних технологій

Технологія	Єдина конфігурація	Віддалене розташування вузлів	Відмовостійкість
StackWise	Так	Ні	Висока
FlexStack	Так	Ні	Висока
VSS	Так	Частково	Дуже висока
StackWise Virtual	Так	Так	Дуже висока
IRF	Так	Так	Висока
EtherChannel	Ні	Так	Середня

У гетерогенній мережі стекування Cisco не вирішує всі питання сумісності, але створює зручну основу для побудови керованої Cisco-частини інфраструктури. Усередині стеку адміністратор отримує єдину систему керування, а взаємодія з обладнанням іншого виробника повинна будуватися за допомогою стандартних протоколів, таких як IEEE 802.1Q, LACP, STP/RSTP та SNMP.

Поєднання стекування з LACP має практичне значення для побудови міжкомутаторних з'єднань. Якщо агрегований канал формується між стекованим вузлом і іншим комутатором, фізичні порти можуть бути логічно об'єднані в один канал. Якщо ці порти розміщені на різних членах стеку, мережа отримує додаткову стійкість до відмови окремого комутатора. Водночас у конкретній реалізації потрібно розрізняти можливість такого підходу та фактичну кількість задіяних фізичних каналів.

Для експлуатації стекованих систем важливо контролювати не тільки звичайні Ethernet-порти, а й внутрішні стекові з'єднання. Діагностика повинна включати перевірку складу стеку, ролей учасників, стану стекових портів, використання стекової шини, завантаження процесора та журналів системних подій. Система моніторингу може бачити стек як один мережевий пристрій із багатьма інтерфейсами, але адміністратор повинен розуміти, які інтерфейси належать до яких фізичних комутаторів.

У проєктованій мережі використання двох різних підходів до стекування Cisco дозволяє розділити ролі обладнання. Стек Cisco Catalyst 3750X може виконувати роль верхнього комутаційного вузла, а стек Cisco Catalyst 2960S – роль вузла доступу та розширення портової ємності. У результаті замість п'яти окремих комутаторів Cisco адміністратор працює з двома логічними стекованими вузлами. Це спрощує налаштування, документування, моніторинг і подальшу діагностику.

Отже, StackWise Plus і FlexStack є важливими технологіями Cisco для побудови масштабованих комутуваних мереж. Вони дозволяють об'єднати кілька фізичних пристроїв у логічний комутатор, централізувати керування, спростити розширення мережі та зменшити кількість окремих точок адміністрування. Водночас ці технології потребують сумісного обладнання, справних стекових

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

модулів або кабелів і регулярної перевірки стану стеку. У поєднанні зі стандартними протоколами взаємодії вони створюють основу для побудови керованої гетерогенної інфраструктури.

1.4 Особливості побудови гетерогенних мережевих середовищ

Гетерогенне мережеве середовище - це інфраструктура, у якій одночасно використовуються пристрої різних виробників, апаратних платформ або поколінь обладнання. На практиці така ситуація є поширеною, оскільки мережі організацій зазвичай розвиваються поступово. Частина обладнання закуповується раніше, частина модернізується пізніше, а окремі сегменти можуть будуватися на основі інших технічних рішень. У результаті в одній мережі можуть одночасно працювати комутатори Cisco, ZTE, HPE, Juniper, MikroTik або інших виробників.

Перевагою такого підходу є гнучкість. Організація не прив'язується повністю до одного постачальника, може поступово оновлювати інфраструктуру та використовувати вже наявне обладнання. Це особливо важливо тоді, коли повна заміна мережевої платформи є економічно недоцільною. Водночас гетерогенна мережа складніша в адмініструванні, оскільки різні пристрої мають різний синтаксис команд, різні назви інтерфейсів, різний формат діагностики та не завжди однаково реалізують однакові стандарти [7].

Основною вимогою до мультивендорної мережі є використання стандартизованих протоколів. Пропрієтарні механізми можуть бути зручними в межах обладнання одного виробника, але вони не завжди придатні для інтеграції інших платформ. Наприклад, стекування Cisco дозволяє об'єднати сумісні комутатори Cisco в один логічний вузол, але комутатор іншого виробника не може бути включений до такого стеку. Тому взаємодія між Cisco та ZTE повинна будуватися через стандартні механізми канального рівня та протоколи керування.

Для комутованої гетерогенної мережі ключове значення мають VLAN, STP або RSTP, LACP та SNMP. У цьому підрозділі ці технології розглядаються не як окремі механізми роботи комутатора, а як засоби сумісності між обладнанням різних виробників. Саме вони дозволяють поєднати фірмові можливості Cisco-

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

інфраструктури з обладнанням ZTE без повної залежності від однієї апаратної платформи.

У випадку VLAN для гетерогенної мережі важлива не сама наявність цієї технології, а однакова логіка її обробки на різних платформах. Потрібно узгодити режим порту, native VLAN, список дозволених VLAN і спосіб тегування кадрів. Помилка на одному боці з'єднання може призвести до того, що окремий сегмент буде недоступним або трафік потрапить не в той логічний домен. Тому під час інтеграції різного обладнання необхідно перевіряти не лише фізичне підключення, а й фактичну VLAN-конфігурацію.

Окремої уваги потребує робота Spanning Tree. У мультивендорній мережі різні пристрої можуть використовувати різні режими STP або RSTP. Це не завжди створює проблему, але потребує перевірки. Адміністратор повинен розуміти, який пристрій є кореневим мостом, які порти перебувають у forwarding-стані, які можуть блокуватися та чи немає ознак нестабільної топології. Для проєктованої мережі логічно, щоб центральну роль у L2-топології виконував верхній стек Cisco Catalyst 3750X, оскільки саме він є основним комутаційним вузлом.

Для опису міжкомутаторних з'єднань у мультивендорній мережі потрібно враховувати різницю в термінології. На Cisco логічний агрегований канал описується як Port-channel, а на ZTE подібну роль може виконувати smartgroup. У межах цієї роботи така відповідність розглядається як проєктна можливість для подальшого розширення підключення, а не як твердження про вже реалізовану багатоканальну агрегацію до ZTE.

LACP у гетерогенній мережі має практичну цінність саме тому, що є стандартним механізмом. Він дозволяє узгоджувати параметри логічного каналу між пристроями різних виробників. Проте для коректної роботи необхідно, щоб обидві сторони мали сумісні параметри: швидкість, дуплекс, тип порту, VLAN-конфігурацію та режим агрегації. Якщо одна сторона очікує LACP, а інша працює в статичному режимі, або якщо відрізняється режим access/trunk, з'єднання може працювати некоректно.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

У гетерогенному середовищі діагностика має більше значення, ніж у мережі з обладнанням одного виробника. Сам факт фізичного з'єднання не означає, що логічна взаємодія налаштована правильно. Потрібно перевіряти стан портів, VLAN, Spanning Tree, LACP-сусідів або відповідних логічних інтерфейсів, а також помилки на фізичних інтерфейсах. Помилки CRC, drops, нестабільна швидкість або періодичне перемикання стану порту можуть свідчити про проблеми з кабелем, портом або узгодженням параметрів.

Для контролю обладнання різних виробників потрібен спільний механізм моніторингу. У цій роботі таким механізмом є SNMP, оскільки він підтримується як Cisco, так і ZTE та дозволяє отримувати дані про доступність пристроїв, стан інтерфейсів і лічильники трафіку.

Окремим питанням є безпека керування. Усі пристрої гетерогенної мережі повинні мати узгоджену політику адміністративного доступу. Віддалене керування потрібно обмежувати лише довіреними вузлами або керуючим сегментом. Для SNMP бажано використовувати доступ тільки на читання, якщо цього достатньо для моніторингу. Надмірні права або слабкі параметри доступу можуть створити ризик для всієї інфраструктури, навіть якщо проблема стосується лише одного пристрою.

У межах даної роботи гетерогенність проявляється через поєднання стекованих комутаторів Cisco та комутатора ZTE ZXR10. Стекування використовується всередині Cisco-частини мережі, а взаємодія з ZTE будується через стандартні мережеві механізми. Такий підхід дозволяє поєднати переваги централізованого керування Cisco-стеками з можливістю інтеграції обладнання іншого виробника.

Отже, побудова гетерогенної мережі потребує не лише фізичного підключення пристроїв, а й перевірки їхньої логічної сумісності. Основою такої сумісності є VLAN, STP або RSTP, LACP та SNMP. Для стабільної роботи також потрібні документація, діагностика, узгоджена політика доступу та моніторинг. Розглянуті особливості створюють основу для подальшого аналізу систем

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

моніторингу, які дозволяють контролювати стан обладнання різних виробників в єдиному середовищі.

1.5 Системи моніторингу мережевої інфраструктури

Моніторинг мережевої інфраструктури є важливою складовою експлуатації корпоративної мережі. Навіть правильно спроектована та налаштована інфраструктура потребує постійного контролю, оскільки її стан може змінюватися через навантаження, відмови обладнання, помилки конфігурації, пошкодження кабельних ліній або некоректну роботу окремих сервісів. Без системи моніторингу адміністратор часто дізнається про проблему вже після звернення користувачів.

Основне завдання моніторингу полягає в отриманні, збереженні та аналізі інформації про стан мережевих пристроїв і каналів зв'язку. До таких параметрів належать доступність комутаторів, стан інтерфейсів, обсяг вхідного та вихідного трафіку, помилки на портах, завантаження каналів, час відповіді та події, що виникають під час роботи обладнання. Наявність цих даних дозволяє не лише реагувати на аварії, а й заздалегідь помічати ознаки можливих проблем.

У комутованій мережі моніторинг має контролювати не тільки загальну доступність пристрою. Важливо бачити стан окремих портів, логічних інтерфейсів, стекованих вузлів і міжкомутаторних з'єднань. Пристрій може залишатися доступним, але окремий інтерфейс може бути вимкнений, перевантажений або мати помилки. Такі ситуації складно виявити без централізованого збору даних.

Для стекованих комутаторів моніторинг має додаткове значення. Стек може відображатися як один логічний пристрій, але фактично складається з кількох фізичних комутаторів. Тому адміністратор повинен розуміти, до якого члена стеку належить конкретний інтерфейс, і мати можливість контролювати не лише логічний вузол загалом, а й окремі порти. Це важливо для діагностики, коли проблема виникає не з усім стеком, а з конкретним підключенням.

У гетерогенній мережі роль моніторингу ще важливіша. Якщо в інфраструктурі використовуються пристрої різних виробників, адміністратору складніше постійно перевіряти їхній стан вручну. Кожна платформа може мати

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

власний синтаксис команд, назви інтерфейсів і формат діагностичної інформації. Система моніторингу зменшує цю складність, оскільки збирає дані з різного обладнання та подає їх в одному інтерфейсі.

Одним із найпоширеніших протоколів для моніторингу мережевого обладнання є SNMP. Його призначення полягає в обміні службовою інформацією між системою моніторингу та мережевими пристроями. Система моніторингу надсилає запити до пристрою, а пристрій повертає значення певних параметрів. Це можуть бути дані про стан інтерфейсу, кількість переданих пакетів, помилки, uptime, назву пристрою, місце розташування та інші характеристики.

SNMP є зручним для гетерогенних середовищ, оскільки підтримується обладнанням різних виробників. У такій схемі система моніторингу не повинна використовувати командний синтаксис кожного пристрою окремо. Вона працює з параметрами, які пристрій надає через SNMP. Це спрощує централізований контроль і дозволяє уніфікувати підхід до спостереження за мережею.

Основою роботи SNMP є модель взаємодії між менеджером і агентом. Менеджером виступає система моніторингу, а агентом є мережевий пристрій, який надає інформацію про свій стан. Агент зберігає або формує дані, доступні для опитування, а менеджер періодично звертається до нього для отримання потрібних значень. Такий підхід дозволяє регулярно збирати інформацію та будувати історію зміни параметрів у часі.

Дані в SNMP організовані у вигляді об'єктів, які мають унікальні ідентифікатори OID. Окремі OID можуть відповідати за опис інтерфейсу, його адміністративний стан, операційний стан, кількість вхідних або вихідних октетів, помилки та інші показники. У гетерогенній мережі важливо враховувати, що різні виробники можуть підтримувати як стандартні OID, так і власні розширення.

Крім SNMP, у мережевому моніторингу можуть використовуватися Syslog і потоковий аналіз трафіку. Syslog призначений для передавання повідомлень про події від мережевих пристроїв до централізованого сервера. Це можуть бути зміни стану інтерфейсів, повідомлення про помилки, автентифікацію або зміни конфігурації. Потоковий аналіз, наприклад NetFlow або подібні механізми,

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

дозволяє оцінювати структуру трафіку, однак його доступність залежить від можливостей конкретного обладнання.

У межах цієї роботи основна увага приділяється SNMP-моніторингу, оскільки він є універсальним і придатним для контролю обладнання різних виробників. Для проєктованої мережі це особливо важливо, оскільки інфраструктура поєднує стековані комутатори Cisco та комутатор ZTE. Використання SNMP дозволяє підключити ці пристрої до єдиної системи моніторингу без необхідності постійного ручного входу на кожен комутатор.

Однією з поширених систем моніторингу є Zabbix. Вона дозволяє контролювати сервери, мережеві пристрої, служби, додатки та інші компоненти інфраструктури. Для мережевих пристроїв Zabbix може використовувати SNMP, ICMP-перевірки, агентські перевірки, зовнішні скрипти та інші способи отримання даних. У контексті комутованої мережі найбільш важливими є контроль доступності пристроїв, автоматичне виявлення інтерфейсів, збір статистики трафіку, фіксація помилок і побудова графіків.

Архітектура Zabbix складається з кількох основних компонентів. Центральним елементом є сервер Zabbix, який виконує обробку даних, зберігання історії, перевірку тригерів і формування подій. Для збереження інформації використовується база даних. Веб-інтерфейс забезпечує доступ адміністратора до налаштувань, графіків, подій і панелей моніторингу. У більших мережах можуть також застосовуватися Zabbix проху, які збирають дані з окремих сегментів і передають їх на центральний сервер.

Для обґрунтування вибору системи моніторингу доцільно порівняти Zabbix з іншими поширеними рішеннями. У корпоративних мережах можуть використовуватися PRTG Network Monitor, Nagios Core, LibreNMS, Prometheus із Grafana та інші системи. Для цієї роботи важливими є підтримка SNMP, можливість роботи з обладнанням різних виробників, автоматичне виявлення інтерфейсів, наявність тригерів і графіків, а також можливість розширення за допомогою власних шаблонів або скриптів.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

Порівняння систем моніторингу мережевої інфраструктури

Система	Підтримка SNMP	Автоматичне виявлення	Тригери / сповіщення	Графіки та дані	Розширення функціональності
Zabbix	+	Підтримується виявлення інтерфейсів та інших об'єктів через правила discovery	Підтримуються тригери, події та сповіщення	Підтримується збереження історії та побудова графіків	Шаблони, користувацькі елементи даних, зовнішні скрипти
PRTG Network Monitor	+	Підтримується виявлення пристроїв і сенсорів	Підтримуються сповіщення за станом сенсорів	Підтримується збереження статистики та побудова графіків	Налаштування сенсорів, скриптові сенсори
Nagios Core	+(через плагіни)	Залежить від додаткових компонентів і налаштувань	Підтримуються перевірки стану та сповіщення	Базові можливості залежать від установлених доповнень	Плагіни та зовнішні скрипти
LibreNMS	+	Підтримується автоматичне виявлення мережевих пристроїв	Підтримуються правила сповіщень	Підтримується збереження історії та побудова графіків	Шаблони, модулі виявлення, інтеграції
Prometheus + Grafana	Потребує експортерів для SNMP	Залежить від налаштування експортерів і service discovery	Підтримується через Alertmanager	Grafana забезпечує візуалізацію метрик	Експортери, правила збору метрик, панелі Grafana

За наведеними критеріями для проєкту обрано Zabbix. Це рішення підтримує SNMP-моніторинг, автоматичне виявлення інтерфейсів, створення тригерів, побудову графіків і збереження історичних даних. Крім того, Zabbix дозволяє використовувати шаблони та власні перевірки, що важливо для мережі з обладнанням різних виробників. У межах проєкту ці можливості потрібні для контролю стекованих комутаторів Cisco, комутатора ZTE ZXR10, стану інтерфейсів і параметрів доступності пристроїв.

Важливою можливістю Zabbix є автоматичне виявлення мережевих інтерфейсів. У комутованих мережах ручне додавання кожного порту до системи моніторингу потребує значного часу, оскільки комутатор може мати десятки

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

фізичних інтерфейсів, а стекований вузол фактично об'єднує порти кількох фізичних пристроїв. Автоматичне виявлення дозволяє системі отримати перелік інтерфейсів через SNMP і створити для них відповідні елементи даних, графіки та тригери.

Для стекованих комутаторів така функція має практичне значення. Оскільки стек відображається як один логічний пристрій, кількість доступних інтерфейсів може бути значною. Система моніторингу може отримати список портів, їхні назви, індекси, адміністративний і операційний стан. Це дозволяє контролювати не лише доступність стеку, а й роботу кожного окремого інтерфейсу.

Окреме місце в системах моніторингу займають тригери. Тригер визначає умову, за якої певний параметр вважається проблемним. Наприклад, тригер може спрацьовувати, якщо пристрій недоступний, інтерфейс перейшов у стан down, кількість помилок перевищила допустиме значення або завантаження каналу наблизилося до критичного рівня. Завдяки тригерам система моніторингу не лише збирає інформацію, а й допомагає швидше виявляти події, які потребують уваги адміністратора.

У комутованій мережі тригери потрібно налаштовувати з урахуванням ролі інтерфейсів. Не кожен порт у стані down є проблемою. Якщо порт не використовується, його вимкнений стан може бути нормальним. Натомість для uplink-з'єднань, портів підключення серверів, керуючих інтерфейсів і міжкомутаторних каналів недоступність є важливою подією. Такий підхід дозволяє уникнути зайвих сповіщень і зосередити увагу на критичних елементах інфраструктури.

Графіки в Zabbix дають змогу аналізувати зміну параметрів у часі. Для мережевих інтерфейсів це можуть бути графіки вхідного та вихідного трафіку, кількості помилок, завантаження каналу або інших показників. Такі дані корисні не лише для пошуку несправностей, а й для планування розвитку мережі. Якщо певний канал регулярно наближається до межі своєї пропускнуєї здатності, це може свідчити про потребу в модернізації або зміні топології.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

У гетерогенній мережі стандартних шаблонів Zabbix іноді недостатньо для повного контролю всіх параметрів. Це пов'язано з тим, що різні виробники обладнання можуть по-різному надавати SNMP-дані або використовувати власні OID для окремих характеристик. У таких випадках адміністратор може доповнювати систему власними елементами даних, правилами виявлення або скриптами. Опис таких скриптів доцільно виконувати в практичній частині роботи, а повний код винести в додатки.

Централізований моніторинг також допомагає швидше виявляти інциденти. Якщо комутатор стає недоступним, інтерфейс змінює стан або на порту з'являються помилки, система може сформувати подію та відобразити її в інтерфейсі адміністратора. Це скорочує час реагування та зменшує залежність від ручної перевірки. У корпоративній мережі швидкість виявлення проблеми безпосередньо впливає на стабільність роботи користувачів і сервісів.

Моніторинг не замінює технічну документацію, але доповнює її фактичними даними. У системі можна бачити перелік пристроїв, їхні IP-адреси, інтерфейси, шаблони, групи, графіки та поточний стан. Якщо документація показує проєктну структуру мережі, то моніторинг відображає її реальний стан під час експлуатації. Поєднання цих двох підходів робить інфраструктуру більш керованою.

Під час впровадження моніторингу потрібно враховувати безпеку. SNMP community або інші параметри доступу не повинні бути відкритими для всіх вузлів мережі. Доступ до SNMP бажано обмежувати сервером моніторингу або адміністративним сегментом. Якщо для моніторингу достатньо режиму читання, не слід використовувати права запису. Це зменшує ризик несанкціонованого впливу на мережеве обладнання.

У межах цієї роботи система моніторингу розглядається як обов'язкова складова гетерогенної комутованої мережі. Вона дозволяє контролювати стан стекованих комутаторів Cisco, обладнання ZTE та міжкомутаторних з'єднань. Завдяки використанню SNMP і Zabbix адміністратор отримує єдину точку контролю, що особливо важливо для мережі з різними апаратними платформами.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Отже, моніторинг мережевої інфраструктури є необхідним елементом сучасної корпоративної мережі. Він забезпечує контроль доступності пристроїв, аналіз стану інтерфейсів, виявлення помилок, оцінку навантаження та накопичення історичних даних. Для гетерогенної мережі Zabbix є доцільним рішенням, оскільки поєднує підтримку SNMP, автоматичне виявлення, тригери, графіки та можливість розширення за допомогою власних шаблонів або скриптів.

Висновки до розділу 1

У першому розділі було розглянуто теоретичні основи побудови корпоративних комутованих мереж, технології стекування комутаторів, особливості гетерогенних середовищ та підходи до моніторингу мережевої інфраструктури. Проведений аналіз показав, що сучасна корпоративна мережа повинна проєктуватися як цілісна система, у якій кожен пристрій має визначену функціональну роль, а взаємодія між елементами інфраструктури є передбачуваною та контрольованою.

Розглянуто ієрархічний підхід до побудови корпоративних мереж. Встановлено, що поділ інфраструктури на рівень доступу, рівень розподілу та рівень ядра дозволяє впорядкувати структуру мережі та спростити її подальший розвиток. Для мереж невеликого або середнього масштабу окремий рівень ядра може не виділятися фізично, однак його функції частково виконує центральний комутаційний вузол. Такий підхід є прийнятним за умови, що ролі пристроїв, міжкомутаторні з'єднання та логічна структура мережі чітко визначені.

Проаналізовано базові технології комутації, які забезпечують роботу локальних мереж. Комутатори виконують передавання Ethernet-кадрів на основі MAC-адрес, формують таблиці комутації та дозволяють ефективніше використовувати пропускну здатність порівняно з простим повторенням трафіку на всі порти. Окрему увагу приділено access- і trunk-портам, VLAN, тегуванню кадрів, STP/RSTP та LACP. Ці механізми є необхідними для логічної сегментації, передавання трафіку між комутаторами і організації міжкомутаторних з'єднань.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Встановлено, що VLAN є базовим інструментом логічного поділу мережі. Вони дозволяють розділяти трафік різних груп пристроїв у межах спільної фізичної інфраструктури та зменшувати розмір широкомовних доменів. Водночас застосування VLAN потребує правильного налаштування trunk-з'єднань і документації, оскільки помилки в режимах портів або списках дозволених VLAN можуть призвести до недоступності окремих сегментів.

Розглянуто роль протоколів STP і RSTP у забезпеченні стабільності комутованої мережі. Надлишкові фізичні з'єднання можуть підвищувати відмовостійкість, але без контролю топології вони створюють ризик петель другого рівня. Тому під час проєктування мережі необхідно визначати центральний вузол L2-топології, контролювати стан портів і враховувати фактичний режим роботи Spanning Tree на конкретному обладнанні.

Стекування дозволяє об'єднати кілька фізичних комутаторів у один логічний пристрій із централізованим керуванням. Це зменшує кількість окремих точок адміністрування, спрощує налаштування портів, полегшує документування та дозволяє масштабувати мережу без значного ускладнення її структури. У межах теми роботи особливе значення мають StackWise Plus для комутаторів Cisco Catalyst 3750X та FlexStack для Cisco Catalyst 2960S.

Порівняння StackWise Plus і FlexStack показало, що ці технології мають спільну мету, але орієнтовані на різні сценарії використання. StackWise Plus доцільно застосовувати у продуктивніших вузлах, які виконують функції верхнього рівня комутації або розподілу. FlexStack більше відповідає завданням рівня доступу, де головними вимогами є збільшення кількості портів і централізоване адміністрування. Водночас ефективність стекування залежить від сумісності обладнання, стану стекових з'єднань, розподілу ролей між учасниками стеку та правильного розміщення критичних підключень.

Було визначено, що стекування не замінює всі інші механізми побудови надійної мережі. Воно спрощує керування групою комутаторів і може підвищити зручність експлуатації, але потребує поєднання з VLAN, STP/RSTP, LACP і засобами моніторингу. Особливо важливо контролювати стан стекових портів, ролі

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

комутаторів у стеку та належність інтерфейсів до конкретних фізичних пристроїв, оскільки логічне об'єднання не скасовує фізичної структури мережі.

Розглянуто особливості побудови гетерогенних мережевих середовищ. Встановлено, що використання обладнання різних виробників є типовим для реальних корпоративних мереж, які розвиваються поступово. Основою сумісності в такому середовищі є використання стандартних механізмів: VLAN, STP/RSTP, LACP і SNMP.

Для гетерогенної мережі важливо розділяти фірмові та стандартні технології. Стекування Cisco є ефективним механізмом організації Cisco-частини інфраструктури, але обладнання іншого виробника не може бути включене до такого стеку. Тому взаємодія з комутатором ZTE ZXR10 повинна будуватися через стандартні мережеві механізми. У цьому контексті важливими є узгодження режимів портів, VLAN, параметрів Spanning Tree, можливість використання LACP та правильне документування відповідності термінів між платформами, наприклад Port-channel на Cisco і smartgroup на ZTE.

Порівняння систем моніторингу показало, що для даного проєкту доцільним рішенням є Zabbix. Його перевагами є автоматичне виявлення інтерфейсів, використання шаблонів, побудова графіків, налаштування тригерів і можливість розширення за допомогою власних перевірок або скриптів. Це важливо для мережі, у якій одночасно використовуються стековані комутатори Cisco та ZTE.

Отже, результати теоретичного аналізу підтверджують доцільність побудови гетерогенної комутованої мережі на основі поєднання стекування Cisco та стандартних протоколів взаємодії. Стекування забезпечує централізоване керування Cisco-комутаторами, VLAN і STP/RSTP формують стабільну логічну структуру другого рівня, LACP може використовуватися для організації та подальшого розширення міжкомутаторних з'єднань, а SNMP і Zabbix забезпечують централізований контроль стану інфраструктури. Розглянуті теоретичні положення створюють основу для подальшого проєктування мережі, визначення її структури, адресного плану, логіки інтеграції обладнання різних виробників і практичної перевірки працездатності рішення.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

РОЗДІЛ 2 ПРОЄКТУВАННЯ ГЕТЕРОГЕННОЇ КОМУТОВАНОЇ МЕРЕЖІ

2.1 Аналіз вимог до мережевої інфраструктури організації

Проектування комутованої мережі організації починається з визначення вимог до її структури, продуктивності, масштабованості, відмовостійкості та керованості. Мережа має забезпечувати стабільну роботу підключених пристроїв, підтримку службових сервісів, можливість подальшого розширення та зручність адміністрування. У разі відсутності чітко визначених вимог подальше налаштування обладнання може бути несистемним, а пошук несправностей і модернізація інфраструктури ускладнюються.

У межах кваліфікаційної роботи проєктується гетерогенна комутована мережа, у якій поєднуються стековані комутатори Cisco та комутатор ZTE ZXR10. Така структура відповідає умовам корпоративних мереж, де обладнання може належати до різних апаратних платформ і використовуватися в межах однієї інфраструктури. Тому вимоги до мережі охоплюють не лише роботу Cisco-сегмента, а й коректну інтеграцію обладнання іншого виробника.

Першою вимогою є достатня портова ємність. На рівні доступу мережа має забезпечувати підключення користувацьких і службових пристроїв без необхідності повної перебудови топології під час розширення. Для цього використовується стек Cisco Catalyst 2960S, який виконує роль вузла доступу та дозволяє об'єднати кілька фізичних комутаторів в один логічний пристрій. Такий підхід зменшує кількість незалежних конфігурацій і спрощує супровід портів.

Другою вимогою є наявність центрального комутаційного вузла. У проєктованій мережі цю роль виконує стек Cisco Catalyst 3750X. Він використовується як верхній комутаційний вузол, до якого підключаються стек доступу, комутатор ZTE ZXR10 та сервер моніторингу. Такий розподіл ролей робить структуру мережі зрозумілою: стек доступу забезпечує портову ємність, а верхній стек агрегує основні підключення.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

Важливою вимогою є масштабованість. Мережа повинна допускати збільшення кількості портів, додавання нових сегментів і розширення службової інфраструктури без повної зміни архітектури. Стекування Cisco вирішує це завдання за рахунок об'єднання кількох фізичних комутаторів у логічні вузли. У результаті адміністратор працює не з набором окремих пристроїв, а з двома стекованими комутаційними вузлами, що спрощує керування та подальше розширення.

Окремою вимогою є продуктивність між комутаторних з'єднань. Канали між основними вузлами не повинні ставати вузьким місцем під час передавання трафіку між сегментами. Для цього структура мережі передбачає логічно впорядковані міжкомутаторні підключення та можливість їх подальшого розширення. Використання стандартних механізмів другого рівня дозволяє зберегти сумісність між Cisco та ZTE і забезпечити передбачувану роботу з'єднань між ними.

Відмовостійкість є однією з основних вимог до мережевої інфраструктури. Відмова окремого порту, кабельної лінії або комутатора не повинна призводити до повної втрати працездатності всієї мережі. Стекування дозволяє зменшити кількість незалежних точок адміністрування та підвищити керованість комутаційних вузлів. Для підвищення стійкості також важливо правильно розподіляти критичні підключення між фізичними членами стеку, контролювати стан стекових портів і перевіряти роботу міжкомутаторних з'єднань.

Для гетерогенної інфраструктури важливою є сумісність обладнання. Оскільки в проєкті використовуються Cisco та ZTE, взаємодія між ними будується на стандартних механізмах, а не на фірмових технологіях одного виробника. До таких механізмів належать VLAN, STP або RSTP, LACP як можливість організації логічного каналу та SNMP для моніторингу. Це дозволяє поєднати стекування Cisco всередині Cisco-сегмента з підключенням обладнання іншого виробника.

Наступною вимогою є керованість інфраструктури. Усі ключові пристрої повинні мати керуючі IP-адреси, бути доступними для адміністрування та підтримувати механізми моніторингу. У проєкті використовується єдиний керуючий сегмент, через який адміністратор може отримувати доступ до

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

комутаторів і сервера моніторингу. Така схема спрощує контроль стану обладнання та створює основу для централізованого збору службових параметрів.

Для контролю стану мережі використовується SNMP та система Zabbix. Такий підхід дозволяє контролювати доступність пристроїв, стан інтерфейсів, завантаження каналів і помилки на портах. Для гетерогенної мережі це особливо важливо, оскільки Cisco та ZTE мають різну командну логіку, але можуть передавати службові параметри через спільний протокол моніторингу.

Окремою вимогою є можливість діагностики. Під час експлуатації адміністратор повинен мати змогу перевірити склад стеку, ролі його учасників, стан стекових портів, параметри Spanning Tree, доступність пристроїв, стан інтерфейсів і коректність міжкомутаторних з'єднань. Це дозволяє підтвердити працездатність проєктної схеми та швидше виявляти причини можливих несправностей.

Також потрібно враховувати логічну сегментацію мережі. Навіть якщо на початковому етапі використовується базовий керуючий сегмент, структура повинна допускати подальше впровадження окремих VLAN для користувачів, серверів, моніторингу або службового обладнання. Це дозволить розділяти трафік за призначенням і зменшити залежність усіх пристроїв від одного широкомовного домену.

Важливою вимогою є безпечне адміністрування. Доступ до керування комутаторами та SNMP-параметрів повинен бути обмежений відповідно до потреб експлуатації. Для моніторингу достатньо використовувати доступ на читання, якщо не передбачено окремих задач зміни конфігурації. Такий підхід зменшує ризик небажаного впливу на мережеве обладнання.

Проектована мережа також повинна бути зручною для документування. Необхідно зафіксувати склад стеків, ролі пристроїв, IP-адреси керування, міжкомутаторні підключення, логіку взаємодії з ZTE, параметри VLAN і моніторингу. Документація потрібна для подальшої діагностики, модернізації та супроводу мережі.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Основні вимоги до гетерогенної комутованої мережі

Вимога	Зміст вимоги	Реалізація в проєкті
Портова ємність	Забезпечення достатньої кількості портів для підключення пристроїв	Стек Cisco Catalyst 2960S на рівні доступу
Центральний комутаційний вузол	Агрегація основних підключень мережі	Стек Cisco Catalyst 3750X
Масштабованість	Можливість подальшого розширення портів, VLAN і підключень	Використання стекування та впорядкованої структури
Продуктивність	Недопущення перевантаження ключових міжкомутаторних з'єднань	Проектування основних каналів із можливістю подальшого розширення
Відмовостійкість	Зменшення впливу відмов окремих портів або пристроїв	Стекування, контроль стану портів і міжкомутаторних з'єднань
Сумісність	Робота обладнання різних виробників в одній мережі	Використання VLAN, STP/RSTP, LACP та SNMP
Керованість	Централізований доступ до мережевих пристроїв	Керуючий сегмент і IP-адреси пристроїв
Моніторинг	Контроль доступності, інтерфейсів, трафіку та помилок	SNMP і Zabbix
Безпека адміністрування	Обмеження службового доступу до пристроїв	Контроль доступу до керування та SNMP
Документування	Фіксація структури, адресації, ролей і підключень	Схеми, таблиці адресації та опис вузлів

Отже, аналіз вимог показав, що для побудови гетерогенної комутованої мережі необхідно забезпечити масштабованість, достатню портову ємність, керованість, сумісність обладнання різних виробників, можливість моніторингу та контроль стану ключових з'єднань. Для реалізації цих вимог у проєкті використовуються стековані комутатори Cisco, комутатор ZTE ZXR10, стандартні мережеві протоколи та система централізованого моніторингу. На основі визначених вимог у наступному підрозділі розробляється структура гетерогенної комутованої мережі.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

2.2 Розробка структури гетерогенної комутованої мережі

На основі визначених вимог розроблено структуру гетерогенної комутованої мережі, яка поєднує стековані комутатори Cisco, комутатор ZTE ZXR10 та сервер моніторингу Zabbix. Основна логіка проєктного рішення полягає в поділі мережі на кілька функціональних вузлів, кожен із яких виконує окрему роль у загальній інфраструктурі.

До складу проєктованої мережі входять чотири основні компоненти: стек Cisco Catalyst 3750X, стек Cisco Catalyst 2960S, комутатор ZTE ZXR10 та сервер Zabbix. Стек Cisco Catalyst 3750X використовується як центральний комутаційний вузол. Стек Cisco Catalyst 2960S працює як окремий стекований вузол Cisco. Комутатор ZTE ZXR10 додає до структури обладнання іншого виробника. Сервер Zabbix забезпечує централізований контроль стану мережевих пристроїв.

Стек Cisco Catalyst 3750X побудований на базі двох фізичних комутаторів. У структурі мережі він займає центральне положення, оскільки через нього організовується взаємодія між іншими елементами інфраструктури. До цього стеку підключаються стек Cisco Catalyst 2960S, комутатор ZTE ZXR10 та сервер моніторингу. Така побудова дозволяє зосередити основні міжвузлові зв'язки в одному логічному комутаційному центрі [10].

Стек Cisco Catalyst 2960S складається з трьох фізичних комутаторів, які працюють як один логічний пристрій. У загальній структурі він розглядається як окремий Cisco-вузол, пов'язаний із верхнім стеком Cisco Catalyst 3750X. Детальні параметри стекування, ролі комутаторів і особливості організації цього стеку розглядаються в наступному підрозділі.

Комутатор ZTE ZXR10 включено до структури як гетерогенний елемент. Він не є частиною стеку Cisco та працює як окремий комутаційний пристрій. Його підключення до Cisco-інфраструктури реалізується через стандартні Ethernet-механізми, що дозволяє уникнути залежності від пропрієтарних технологій одного виробника. У подальшому таке підключення може бути розширене за рахунок використання логічного каналу, однак у структурі мережі ZTE розглядається саме як окремий вузол іншої апаратної платформи.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

Сервер Zabbix розміщується в мережі як службовий компонент. Він не бере участі в передаванні основного трафіку між комутаційними вузлами, але має доступ до керуючих адрес мережевих пристроїв [18]. Завдяки цьому сервер може отримувати службові параметри через SNMP та відображати стан обладнання в єдиній системі моніторингу.

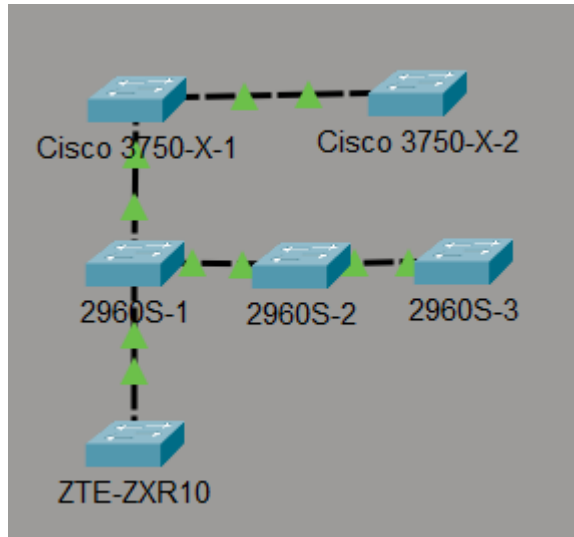


Рисунок 2.1 – Структурна схема гетерогенної комутованої мережі

У цій структурі логічна Cisco-частина представлена двома стекованими вузлами, хоча фізично вона складається з п'яти комутаторів. Комутатор ZTE ZXR10 показує інтеграцію обладнання іншого виробника, а сервер Zabbix забезпечує службовий контроль стану мережі. Такий опис структури є основою для подальшого розгляду стеків, інтеграції ZTE, адресації та логічної схеми мережі.

2.3 Проєктування стеку комутаторів Cisco

У проєктованій гетерогенній комутованій мережі стекування Cisco використовується як один із ключових механізмів організації комутаційної інфраструктури. Його застосування дозволяє об'єднати кілька фізичних комутаторів у логічні вузли, спростити адміністрування та зменшити кількість окремих пристроїв, які потрібно налаштовувати й контролювати незалежно один від одного. У межах проєкту передбачено два стековані вузли Cisco: верхній стек Cisco Catalyst 3750X та стек доступу Cisco Catalyst 2960S [9].

Верхній стек Cisco Catalyst 3750X складається з двох комутаторів Cisco WS-C3750X-24P. У структурі мережі цей стек виконує роль центрального

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

комутаційного вузла, через який організовується взаємодія між основними елементами інфраструктури. Його доцільно розміщувати на верхньому рівні проєктованої схеми, оскільки саме він забезпечує агрегацію підключень, зв'язок зі стеком доступу та підключення гетерогенного обладнання.

Використання двох комутаторів у складі верхнього стеку дозволяє отримати один логічний комутаційний вузол замість двох окремих пристроїв. Для адміністратора це означає спільну конфігурацію, єдину точку керування та узгоджену роботу портів. Такий підхід зменшує складність експлуатації центральної частини мережі та полегшує подальше документування підключень.

У межах верхнього стеку один комутатор виконує роль головного пристрою, а другий працює як член стеку. Головний комутатор відповідає за керування логічним вузлом, обробку конфігурації та координацію роботи стеку. Комутатор-член обслуговує власні фізичні інтерфейси та працює як частина спільної комутаційної системи. Такий розподіл ролей дозволяє поєднати централізоване керування з фізичним розподілом портів між двома пристроями.

Стек доступу Cisco Catalyst 2960S складається з трьох комутаторів Cisco WS-C2960S-F24TS-L. Його основне призначення полягає у збільшенні кількості доступних портів і підключенні нижчих сегментів мережі. Саме на рівні доступу найчастіше виникає потреба у більшій кількості портів, оскільки до мережі можуть підключатися кінцеві пристрої, службові вузли, додаткові комутатори або обладнання для тестування.

У разі використання трьох окремих комутаторів адміністратор мав би працювати з трьома незалежними конфігураціями. Це ускладнює керування, збільшує кількість можливих помилок і потребує більше часу на супровід. Стекування дозволяє об'єднати ці пристрої в один логічний вузол, у якому всі порти відображаються в межах єдиної системи керування. Саме тому застосування стеку Cisco Catalyst 2960S є доцільним для рівня доступу.

У стеку доступу один комутатор виконує роль головного, а два інші працюють як члени стеку. Така структура дозволяє зберегти чітку логіку керування та водночас отримати більшу портову ємність. Для адміністратора важливо, що

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

кожен фізичний комутатор у стеку залишається ідентифікованим, а його порти мають власну нумерацію. Це спрощує пошук фізичних підключень і подальше обслуговування мережі.

Таблиця 2.2

Структура стекованих вузлів Cisco

Логічний вузол	Обладнання	Кількість комутаторів	Функціональна роль
Стек Cisco Catalyst 3750X	Cisco WS-C3750X-24P	2	Центральний комутаційний вузол
Стек доступу Cisco Catalyst 2960S	Cisco WS-C2960S-F24TS-L	3	Вузол доступу та розширення портової ємності

Під час проектування стеків важливо враховувати не тільки кількість комутаторів, а й їхню роль у загальній структурі мережі. Верхній стек має виконувати функцію основного вузла агрегації, тому саме через нього доцільно організовувати підключення до інших комутаційних блоків. Стек доступу має підпорядковану роль і забезпечує розширення кількості портів. Такий розподіл функцій відповідає ієрархічній моделі побудови корпоративної мережі.

Окрему увагу потрібно приділити пріоритетам комутаторів у стеку. Пріоритет впливає на вибір головного пристрою під час формування стеку. Якщо пріоритети не визначені або визначені випадково, роль головного комутатора може отримати пристрій, який не є оптимальним з погляду розміщення або підключень. Тому у проєкті передбачається логічний розподіл ролей, за якого головним пристроєм має бути комутатор, що займає центральне місце в роботі відповідного стеку.

Стан стекових з'єднань є важливим показником працездатності всієї стекованої системи. Через стекові порти комутатори обмінюються службовою інформацією та працюють як єдиний логічний пристрій. Якщо стекові з'єднання організовані коректно, система має вищу стабільність і краще переносить окремі

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

фізичні порушення. Якщо один зі стекових каналів не працює, стек може залишатися працездатним, але його внутрішня відмовостійкість зменшується.

Під час експлуатації стеків необхідно контролювати склад стеку, ролі його учасників і стан стекових портів. У практичній частині роботи ці параметри доцільно підтвердити результатами діагностичних команд. Такий підхід дозволить не лише описати проєктне рішення, а й показати, що стекові вузли фактично сформовані та готові до роботи.

Важливо враховувати, що стекування не приховує фізичну структуру повністю. Хоча адміністратор працює з одним логічним вузлом, кожен порт усе одно належить конкретному фізичному комутатору в стеку. Нумерація інтерфейсів дає змогу визначити, на якому саме члені стеку розташований порт. Це має практичне значення під час підключення кабелів, пошуку несправностей і складання схеми мережі.

Під час проєктування слід уникати ситуації, коли всі важливі з'єднання підключені до одного фізичного комутатора в стеку. Якщо критичні канали зосереджені на одному пристрої, його відмова може вплинути на значну частину мережі. Тому важливі підключення доцільно розподіляти між різними членами стеку. Це стосується uplink-з'єднань, каналів між комутаційними вузлами та підключення обладнання, яке має значення для всієї інфраструктури.

У проєктованій мережі верхній стек Cisco Catalyst 3750X використовується як точка взаємодії між основними елементами інфраструктури. Стек доступу Cisco Catalyst 2960S підключається до нього як нижчий функціональний рівень. Такий підхід дозволяє зробити топологію зрозумілою: верхній стек агрегує трафік, а стек доступу забезпечує розширення портової ємності. Це спрощує подальше масштабування мережі та полегшує її супровід.

Для взаємодії між стекованими вузлами доцільно використовувати логічні міжкомутаторні з'єднання. У цьому підрозділі вони розглядаються лише на рівні проєктного рішення, без детального опису команд налаштування. Детальна реалізація агрегованих каналів і взаємодія з обладнанням іншого виробника

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

розглядаються в наступних підрозділах та практичній частині роботи. Такий розподіл матеріалу дозволяє уникнути дублювання й зберегти логіку викладу.

Робота стеків також повинна узгоджуватися з логікою запобігання петлям у мережі другого рівня. У схемі, де є кілька комутаційних вузлів, важливо заздалегідь визначити центральну роль верхнього стеку. Саме він має бути основним вузлом, через який проходить взаємодія між частинами мережі. Такий підхід робить логічну топологію більш передбачуваною та спрощує діагностику у випадку змін або несправностей.

Для стеку доступу основною задачею є підключення нижчих сегментів і передавання трафіку до верхнього комутаційного вузла. Він не повинен створювати надлишкових неконтрольованих шляхів, які можуть ускладнити роботу протоколів другого рівня. Тому його підключення до верхнього стеку має бути чітко визначене, задокументоване та перевірене під час реалізації.

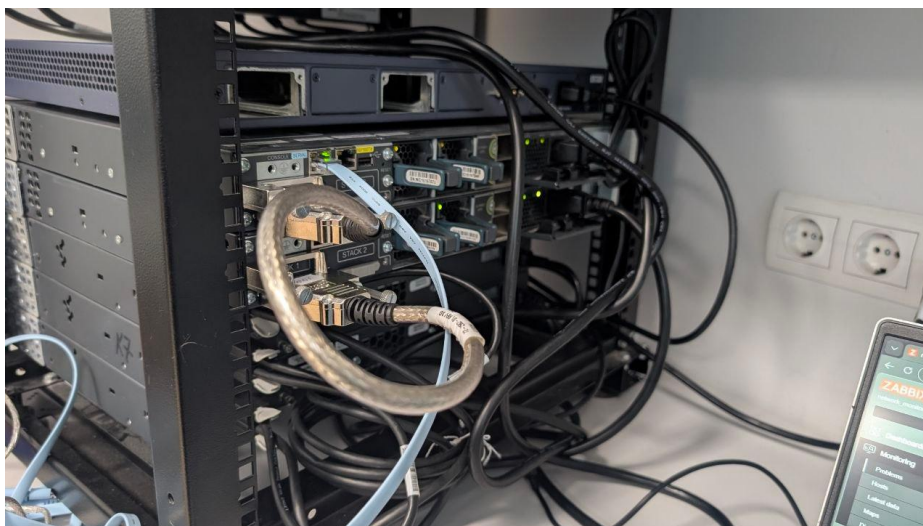


Рисунок 2.2 – Стекування комутаторів Cisco

У підсумку проєктування стеків Cisco спрямоване на підвищення керованості, масштабованості та структурованості мережі. Верхній стек Cisco Catalyst 3750X виконує роль центрального комутаційного вузла, а стек доступу Cisco Catalyst 2960S забезпечує розширення портової ємності. Замість п'яти окремих комутаторів у структурі мережі використовуються два логічні вузли, що значно спрощує адміністрування та документування.

Таким чином, використання двох стекованих вузлів Cisco дозволяє побудувати зручну для експлуатації комутовану інфраструктуру. Стекування

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

забезпечує централізоване керування, спрощує масштабування, зменшує кількість незалежних пристроїв і створює основу для подальшої інтеграції гетерогенного обладнання.

2.4 Інтеграція гетерогенного мережевого обладнання

У проєктованій мережі гетерогенність реалізується через інтеграцію комутатора ZTE ZXR10 з комутаційною інфраструктурою Cisco. Основна частина мережі побудована на стекованих комутаторах Cisco, однак для забезпечення мультивендорної сумісності до загальної структури включено комутатор іншого виробника. Таке рішення дозволяє показати, що мережа не обмежується обладнанням однієї платформи та може бути розширена за рахунок пристроїв, які підтримують стандартні мережеві протоколи.

Комутатор ZTE ZXR10 підключається до верхнього стеку Cisco Catalyst 3750X як окремий комутаційний вузол. Оскільки обладнання ZTE не може бути включене до стеку Cisco, його інтеграція виконується через стандартні Ethernet-з'єднання. Для організації такого з'єднання в проєкті передбачено використання механізму агрегації каналів на основі стандарту IEEE 802.3ad. Це дозволяє застосовувати єдину логіку побудови міжкомутаторного з'єднання незалежно від виробника обладнання.

На стороні Cisco для реалізації логічного агрегованого з'єднання використовується інтерфейс Port-channel. На стороні ZTE аналогічну роль виконує інтерфейс smartgroup. Незважаючи на різні назви в командному інтерфейсі, обидва механізми мають однакове функціональне призначення: вони дозволяють об'єднувати фізичні інтерфейси в один логічний канал. Це спрощує проєктування, документування та подальше розширення міжкомутаторного з'єднання.

Використання LACP у такій схемі є доцільним, оскільки цей протокол забезпечує динамічне узгодження параметрів агрегованого каналу між пристроями. У порівнянні зі статичним об'єднанням портів LACP дає адміністратору більше можливостей для контролю стану каналу. Пристрої обмінюються службовими повідомленнями, визначають сумісність параметрів і формують логічне з'єднання

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

лише за умови коректного налаштування обох сторін. Це особливо важливо в гетерогенній мережі, де використовуються різні платформи та різний синтаксис конфігурації.

У проєкті передбачено можливість подальшого розширення з'єднання між Cisco та ZTE шляхом додавання додаткових фізичних інтерфейсів до відповідного логічного каналу. Такий підхід дозволяє не змінювати загальну архітектуру мережі під час модернізації. Якщо в майбутньому виникне потреба збільшити пропускну здатність або підвищити стійкість підключення, до Port-channel на Cisco та smartgroup на ZTE можна буде додати ще один або кілька фізичних портів за умови підтримки відповідних параметрів обома пристроями.

Для коректної роботи такої схеми необхідно забезпечити відповідність параметрів на обох сторонах з'єднання. Фізичні інтерфейси, які входять до логічного каналу, повинні мати сумісну швидкість, режим дуплексу, однаковий тип порту та узгоджену VLAN-конфігурацію. Якщо один бік з'єднання налаштований як access-порт, а інший як trunk, передавання трафіку може відбуватися некоректно. Тому під час інтеграції Cisco та ZTE необхідно перевіряти не тільки сам факт фізичного підключення, а й логіку роботи порту на каналному рівні.

У межах базової реалізації з'єднання між ZTE ZXR10 і верхнім стеком Cisco Catalyst 3750X може використовуватися як один фізичний канал, включений до логічної групи. Такий варіант дозволяє перевірити сумісність LACP між різними виробниками, підтвердити правильність налаштування smartgroup на ZTE та Port-channel на Cisco, а також підготувати інфраструктуру до подальшого розширення. У цьому випадку основним результатом є не збільшення пропускну здатності, а створення правильної логічної основи для масштабованого міжкомутаторного підключення.

З технічної точки зору така побудова є зручною нашого проєкту, оскільки дозволяє показати не лише поточне фізичне підключення, а й архітектурну можливість розвитку мережі. Якщо використовується один фізичний канал, мережа вже може працювати та передавати трафік між Cisco та ZTE. Якщо до логічної групи в майбутньому додати ще один фізичний інтерфейс, структура з'єднання

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

залишиться тією самою, але зросте пропускна здатність або з'явиться додаткова стійкість до відмови одного з кабелів.

Для гетерогенної мережі важливо правильно описати відповідність термінів між платформами. На Cisco логічний агрегований інтерфейс позначається як Port-channel, а фізичний порт додається до нього через channel-group. На ZTE логічний агрегований інтерфейс позначається як smartgroup, а фізичний інтерфейс включається до цієї групи відповідною командою. Незважаючи на різний синтаксис, обидва пристрої працюють за спільною логікою IEEE 802.3ad.

Таблиця 2.3

Відповідність елементів LACP на Cisco та ZTE

Функція	Cisco	ZTE ZXR10
Логічний канал	Port-channel	smartgroup
Додавання фізичного порту	channel-group	smartgroup на фізичному інтерфейсі
Режим динамічного узгодження	active	active
Стандарт	IEEE 802.3ad	IEEE 802.3ad
Призначення	Міжкомутаторне з'єднання	Міжкомутаторне з'єднання

Під час інтеграції обладнання різних виробників необхідно враховувати, що однакова технологія може по-різному відображатися в командному інтерфейсі. Для Cisco адміністратор перевіряє стан EtherChannel, Port-channel, LACP-сусідів і фізичних учасників каналу. Для ZTE потрібно перевіряти стан smartgroup, фізичних інтерфейсів і режим їхньої участі в логічній групі. Тому в практичній частині роботи доцільно окремо показати конфігураційні фрагменти та діагностику з обох сторін.

Крім LACP, інтеграція ZTE ZXR10 потребує узгодження VLAN. У базовому варіанті з'єднання може працювати в межах одного логічного сегмента. Така схема є простою та зручною для перевірки працездатності. Якщо в майбутньому через це з'єднання потрібно буде передавати трафік кількох VLAN, обидві сторони

необхідно перевести у trunk-режим і узгодити список дозволених VLAN. Це дозволить використовувати один логічний канал для передавання трафіку кількох мережевих сегментів.

Важливою умовою стабільної роботи є контроль петель на другому рівні. Якщо ZTE підключений до верхнього стеку Cisco одним логічним з'єднанням, ризик утворення петлі є мінімальним. Проте у разі додавання додаткових фізичних або логічних шляхів необхідно перевіряти роботу STP або сумісних механізмів запобігання петлям. Центральну роль у такій топології доцільно залишати за верхнім стеком Cisco Catalyst 3750X, оскільки він виконує функцію основного комутаційного вузла.

Окрему увагу потрібно приділити документуванню підключення ZTE. У документації необхідно зазначити, до якого стеку Cisco підключений комутатор ZTE, який логічний канал використовується, які фізичні порти беруть участь у з'єднанні та який режим роботи застосовується. Це дозволить швидше виконувати діагностику та спростить подальше розширення каналу. У гетерогенній мережі така документація особливо важлива, оскільки різні виробники використовують різну термінологію для подібних функцій.

Для подальшої експлуатації ZTE ZXR10 повинен бути доступним для моніторингу. Оскільки мережа проєктується як керована інфраструктура, пристрої Cisco та ZTE мають контролюватися в єдиній системі. Для цього доцільно використовувати SNMP та систему Zabbix. У межах цього підрозділу достатньо зазначити, що ZTE передбачений як окремий вузол моніторингу, а детальне налаштування SNMP, шаблонів і перевірок буде розглянуто в практичному розділі.

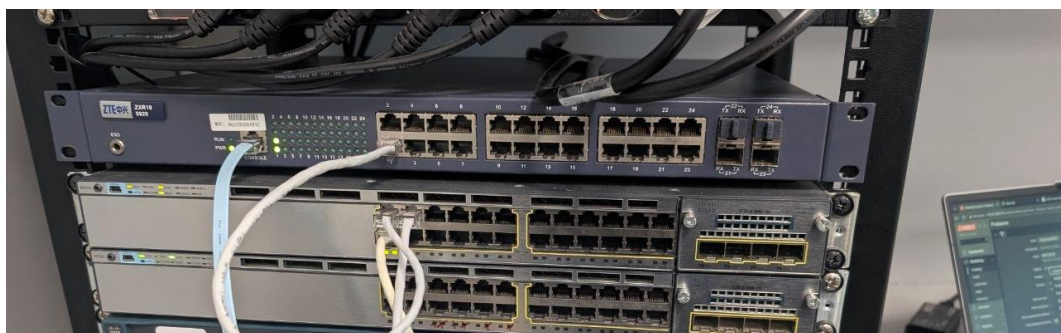


Рисунок 2.3 – Інтеграція комутатора ZTE ZXR10 у гетерогенну мережу

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

У підсумку інтеграція ZTE ZXR10 у проєктовану мережу базується на використанні стандартних механізмів канального рівня. Cisco-частина інфраструктури організована за допомогою стекування, а взаємодія із ZTE реалізується через логічний канал на основі IEEE 802.3ad [13]. Такий підхід дозволяє зберегти сумісність між обладнанням різних виробників, підготувати мережу до подальшого розширення та спростити адміністрування міжкомутаторного підключення.

Таким чином, комутатор ZTE ZXR10 інтегрується до гетерогенної комутованої мережі як окремий мультивендорний вузол. Його підключення до верхнього стеку Cisco Catalyst 3750X проєктується з урахуванням можливості використання LACP та подальшого розширення фізичних каналів. Це забезпечує технічну гнучкість, підтримку стандартної міжвендорної взаємодії та створює основу для централізованого моніторингу всієї інфраструктури.

2.5 Розробка адресного плану та сегментації мережі

Адресний план є важливою частиною проєктування комутованої мережі, оскільки він визначає порядок ідентифікації пристроїв, логіку керування обладнанням і можливість подальшого моніторингу. У межах даного проєкту адресація використовується насамперед для керування мережевими пристроями, виконання діагностики та підключення обладнання до системи моніторингу. Тому адресний план повинен бути простим, зрозумілим і придатним для подальшого розширення.

У проєктованій мережі використовується керуючий сегмент на основі мережі 192.168.1.0/24. У цьому сегменті розміщуються основні мережеві пристрої: верхній стек Cisco Catalyst 3750X, стек доступу Cisco Catalyst 2960S, комутатор ZTE ZXR10 та сервер моніторингу. Використання одного керуючого сегмента спрощує доступ до обладнання, перевірку зв'язності та налаштування SNMP-моніторингу.

Для керування стекованими комутаторами Cisco використовуються SVI-інтерфейси VLAN 1. Верхній стек Cisco Catalyst 3750X має керуючу адресу 192.168.1.2 з маскою 255.255.255.0. Стек доступу Cisco Catalyst 2960S має керуючу

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

адресу 192.168.1.4 з такою самою маскою. Комутатор ZTE ZXR10 також має адресу в цьому сегменті, що дозволяє адмініструвати його разом із пристроями Cisco в межах єдиної керуючої мережі.

Таблиця 2.4

Адресний план керуючого сегмента мережі

Пристрій	Функціональна роль	IP-адреса	Маска підмережі	Призначення
Стек Cisco Catalyst 3750X	Центральний комутаційний вузол	192.168.1.2	255.255.255.0	Керування та моніторинг
Стек Cisco Catalyst 2960S	Вузол доступу	192.168.1.4	255.255.255.0	Керування та моніторинг
ZTE ZXR10	Гетерогенний комутаційний вузол	192.168.1.7	255.255.255.0	Керування та моніторинг
Сервер Zabbix	Система моніторингу	192.168.1.9	255.255.255.0	Збір даних через SNMP

Використання адрес у межах однієї підмережі дозволяє виконувати базову перевірку доступності між пристроями без додаткової маршрутизації. Це зручно для лабораторної або проектної реалізації, оскільки адміністратор може швидко перевірити зв'язок між сервером моніторингу та мережевими вузлами. У разі розширення інфраструктури адресний план може бути доповнений окремими підмережами для користувачів, серверів, службових пристроїв або інших сегментів.

У поточній структурі VLAN 1 використовується як базовий керуючий VLAN. Через нього забезпечується доступ до керуючих інтерфейсів комутаторів і взаємодія з сервером моніторингу [17]. Такий підхід є простим і достатнім для демонстрації працездатності мережі, інтеграції обладнання різних виробників і

перевірки SNMP-доступу. Водночас у промисловій експлуатації доцільно виділяти окремий службовий VLAN для керування, щоб відокремити адміністративний трафік від користувацького.

З погляду подальшого розвитку мережі адресний план повинен передбачати можливість сегментації. Якщо мережа буде використовуватися для підключення різних груп пристроїв, доцільно створити окремі VLAN для користувачів, серверів, мережевого обладнання, систем відеоспостереження або бездротової інфраструктури. Такий підхід дозволить зменшити розмір широкомовних доменів і підвищити керованість мережі [11].

Таблиця 2.5

Можлива структура VLAN для подальшого розширення мережі

VLAN	Назва сегмента	Призначення	Орієнтовна підмережа
1		Керування мережевими пристроями	192.168.1.0/24
10		Робочі станції користувачів	192.168.10.0/24
20		Серверне обладнання	192.168.20.0/24
30		Службові системи моніторингу	192.168.30.0/24
40		Гостьові або тестові підключення	192.168.40.0/24

Наведена структура VLAN є проєктним варіантом для розвитку мережі. У межах базової реалізації основна увага приділяється керуючому сегменту та взаємодії мережевого обладнання. Проте закладена логіка сегментації дозволяє в майбутньому розділити трафік за функціональним призначенням. Це важливо для мережі, яка може поступово масштабуватися та обслуговувати різні типи пристроїв.

Для передавання трафіку між комутаторами необхідно правильно визначити типи портів. Якщо через міжкомутаторне з'єднання передається лише один сегмент, порт може працювати в режимі access. Якщо в майбутньому потрібно буде передавати кілька VLAN, міжкомутаторні з'єднання необхідно перевести в trunk-режим. У такому випадку один фізичний або логічний канал зможе передавати

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

трафік кількох VLAN, а кожен кадр буде ідентифікований відповідним VLAN-тегом.

У поточній схемі базовим є простий варіант з одним керуючим сегментом. Це спрощує початкове налаштування та перевірку працездатності мережі. Для нашого проєкту такий підхід є доцільним, оскільки основною метою є демонстрація стекування Cisco, інтеграції ZTE, роботи LACP-механізмів і підключення пристроїв до моніторингу. Водночас проєктна структура не обмежує подальше впровадження додаткових VLAN.

Особливу увагу потрібно приділити адресації сервера моніторингу. Сервер Zabbix повинен бути доступний до всіх мережевих пристроїв, які контролюються через SNMP. Якщо сервер перебуває в тій самій підмережі, що й керуючі інтерфейси комутаторів, збір даних можна організувати без додаткової маршрутизації. Це зменшує складність схеми та полегшує початкове впровадження моніторингу.

Під час розширення мережі можливі два варіанти організації моніторингу. Перший варіант полягає в тому, що сервер Zabbix залишається в керуючому сегменті та напряму опитує мережеві пристрої. Другий варіант передбачає винесення системи моніторингу в окремий службовий VLAN, доступ до якого контролюється правилами маршрутизації або списками доступу. Другий підхід є більш правильним для промислової мережі, однак для базової реалізації достатньо першого варіанта.

З погляду безпеки використання VLAN 1 як керуючого сегмента не є оптимальним для великої виробничої мережі. У реальній експлуатації рекомендується створювати окремий management VLAN і переносити керуючі адреси пристроїв саме в нього. Це дозволяє відокремити адміністративний доступ від звичайного користувацького трафіку. У межах даного проєкту VLAN 1 використовується як базовий сегмент для демонстрації роботи мережі, але структура адресації передбачає можливість подальшого переходу до окремого службового VLAN.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Для забезпечення коректної роботи гетерогенного середовища всі пристрої повинні мати узгоджену VLAN-конфігурацію на міжкомутаторних з'єднаннях. Якщо ZTE ZXR10 підключається до верхнього стеку Cisco в межах одного логічного сегмента, обидві сторони повинні однаково обробляти цей трафік. У разі переходу до trunk-режиму необхідно буде узгодити native VLAN, список дозволених VLAN і режим роботи портів. Це важливо, оскільки різні виробники можуть мати відмінності в стандартних параметрах портів.

У підсумку адресний план проєктованої мережі побудований навколо керуючого сегмента 192.168.1.0/24. У ньому розміщені основні мережеві пристрої та сервер моніторингу. Такий варіант забезпечує просту схему адміністрування, зручну перевірку доступності та можливість централізованого збору даних через SNMP. Водночас структура передбачає можливість подальшої сегментації мережі за допомогою додаткових VLAN.

Таким чином, розроблений адресний план забезпечує базову керованість гетерогенної комутованої мережі та створює основу для її подальшого розвитку. Використання єдиного керуючого сегмента спрощує початкову реалізацію, а можливість виділення окремих VLAN дозволяє масштабувати мережу відповідно до потреб організації. У наступному підрозділі доцільно узагальнити структурну та логічну схему мережі, показавши взаємозв'язок стеків Cisco, комутатора ZTE та системи моніторингу.

Висновки до розділу 2

У другому розділі кваліфікаційної роботи виконано комплексне проєктування архітектури гетерогенної комутованої мережі організації, визначено ключі технічні вимоги до інфраструктури та сформовано логіку її функціонування. Проведений аналіз дозволив обґрунтувати такі критичні параметри, як відмовостійкість, портова ємність, масштабованість та міжвендорна сумісність. Сформована ієрархічна структура мережі дозволила чітко розмежувати функції агрегації трафіку й підключення кінцевих точок доступу, мінімізуючи ризики виникнення «вузьких місць» у магістральних каналах.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Важливим етапом проектування стало розгортання технології стекування на базі обладнання Cisco, що дозволило консолідувати два комутатори Cisco Catalyst 3750X на рівні ядра/агрегації та три пристрої Cisco Catalyst 2960S на рівні доступу у два логічні вузли адміністрування. Таке рішення не лише редукує кількість незалежних конфігурацій і точок керування, а й оптимізує роботу протоколів другого рівня (STP/RSTP) та суттєво підвищує внутрішню стійкість системи до фізичних відмов ліній зв'язку або окремих шасі. Водночас інтеграція гетерогенного комутатора ZTE ZXR10 до центрального стеку реалізована за допомогою відкритого стандарту агрегації каналів IEEE 802.3ad (LACP). Визначена мапа відповідності інтерфейсів Port-channel та smartgroup забезпечує балансування навантаження та стабільну роботу мультивендорного середовища без прив'язки до пропрієтарних технологій конкретного виробника.

Розроблений адресний план та модель логічної сегментації фіксують створення виділеного сегмента керування (Management Plane) у межах підмережі 192.168.1.0/24 на базі VLAN 1. Розміщення інтерфейсів SVI комутаторів та сервера моніторингу Zabbix в одному логічному просторі дозволяє виконувати пряме SNMP-опитування та ICMP-діагностику без залучення транзитної маршрутизації. Задля безпечного масштабування інфраструктури та обмеження широкомовних доменів у перспективі спроектовано структуру додаткових VLAN для робочих станцій, серверів, систем моніторингу та гостей підключень із розрахунком на перехід до Inter-VLAN маршрутизації. Сформовані у цьому розділі структурно-логічні рішення є вичерпною базою для практичної реалізації, написання конфігураційних лістингів для обладнання Cisco та ZTE, а також розгортання системи централізованого моніторингу в наступному розділі роботи.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ РОБОТИ МЕРЕЖІ

3.1 Моделювання мережевої інфраструктури

Практична частина роботи виконувалася на лабораторному стенді з використанням фізичного мережевого обладнання Cisco та ZTE. Основою моделі стали два стековані вузли Cisco, окремий комутатор ZTE ZXR10 та сервер моніторингу Zabbix. Такий формат реалізації дозволив виконати налаштування на реальних пристроях, отримати фактичні виводи діагностичних команд і перевірити роботу системи моніторингу за реальними подіями обладнання.

Для побудови моделі не використовувалася лише програмна емуляція. Це пов'язано з тим, що в роботі досліджуються функції, які залежать від фізичного обладнання: стекові з'єднання Cisco, ролі учасників стеку, стан stack-портів, системні повідомлення Stack Manager, LACP-сусідство та SNMP-опитування реальних інтерфейсів. Тому лабораторний стенд був використаний як основне середовище моделювання та перевірки.

До складу стенда увійшли два комутатори Cisco WS-C3750X-24P, три комутатори Cisco WS-C2960S-F24TS-L, комутатор ZTE ZXR10 та сервер Zabbix. Комутатори Cisco WS-C3750X-24P були об'єднані в один стек з іменем SW-1-UPPER. Комутатори Cisco WS-C2960S-F24TS-L були об'єднані в окремий стек з іменем SW-29. Комутатор ZTE ZXR10 працював як окремий пристрій іншого виробника. Сервер Zabbix використовувався для контролю доступності пристроїв, SNMP-опитування, збору параметрів інтерфейсів і приймання додаткових подій від скрипта моніторингу стеків.

Для керування обладнанням було використано адресний сегмент 192.168.1.0/24. У цьому сегменті були розміщені керуючі адреси обох стеків Cisco, комутатора ZTE та сервера моніторингу. Стек SW-1-UPPER отримав адресу 192.168.1.2, стек SW-29 - адресу 192.168.1.4, комутатор ZTE ZXR10 - адресу 192.168.1.7, сервер Zabbix - адресу 192.168.1.9.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

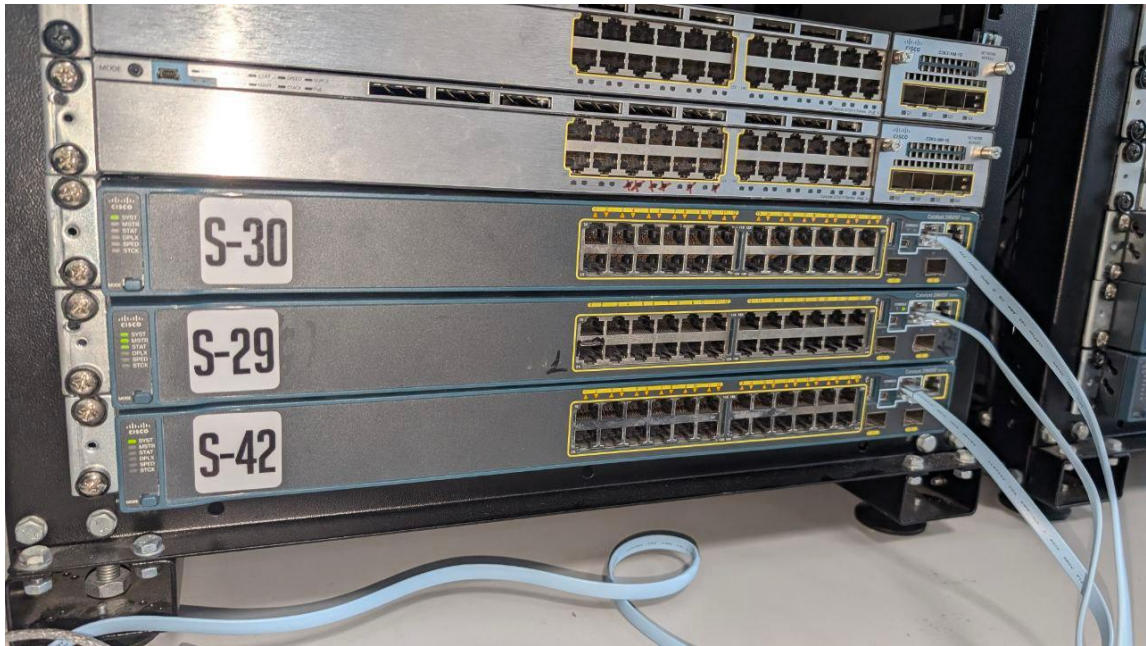


Рисунок 3.1 – Зібрані на стенді стеки Cisco

Комутатор ZTE ZXR10 був підключений до Cisco-частини мережі як окремий пристрій. У його конфігурації використовувалася VLAN 1, керуючий інтерфейс з адресою 192.168.1.7 та інтерфейс smartgroup2 для організації логічного підключення. Це дозволило перевірити взаємодію між Cisco та ZTE через стандартну логіку Ethernet і LACP.

Сервер Zabbix був розміщений у тому самому керуючому сегменті. З нього виконувалася перевірка доступності хостів. Після підтвердження мережевої доступності пристрої були підготовлені до SNMP-опитування. Надалі цей сервер використовувався не лише для базового SNMP-моніторингу, а й для приймання даних від власного Python-скрипта, який аналізує системні журнали Cisco.

Перед основним налаштуванням було перевірено стартові параметри стенда. На Cisco-пристроях перевірялися версії IOS, склад стеків, інвентарні дані, VLAN, Spanning Tree, EtherChannel, LACP-сусідство, таблиці MAC-адрес, ARP-таблиця та стан керуючих інтерфейсів. На ZTE перевірялися керуючий інтерфейс, smartgroup, фізичні порти, SNMP-параметри та доступність пристрою в мережі.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		67



Рисунок 3.2 – Фізичне розміщення обладнання в лабораторному стенді

У моделі використовувалася VLAN 1. На Cisco-комутаторах та ZTE керуючі адреси були налаштовані на SVI-інтерфейсах VLAN 1. Це забезпечило єдиний керуючий сегмент для всіх основних пристроїв стенда. Для перевірки доступності використовувалися ICMP-запити, ARP-таблиці та дані Zabbix.

Окремо в моделі було передбачено перевірку подій стеку Cisco. Для цього використовувався журнал пристрою. У журналі фіксуються системні повідомлення, пов'язані з роботою стеку, зокрема додавання або випадання учасника, готовність комутатора, зміна master-пристрою та зміна стану stack-link. Ці події стали основою для подальшої кастомізації моніторингу в Zabbix.

Практична модель була побудована так, щоб кожен етап можна було підтвердити технічними даними. Стан стеків підтверджувався командами Cisco, стан міжкомутаторних з'єднань - EtherChannel і LACP-командами, доступність

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

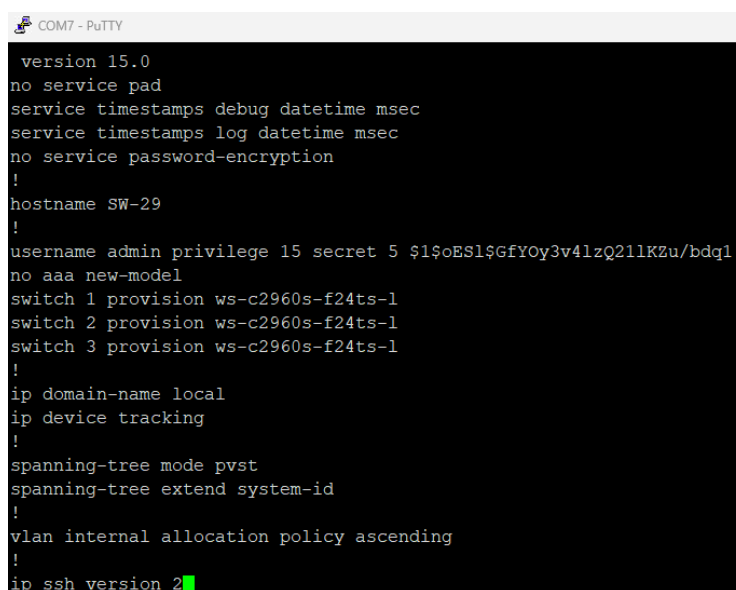
керуючого сегмента - ICMP та ARP, а робота моніторингу - даними Zabbix. Такий підхід дозволив перейти від загальної схеми до фактичної перевірки працездатності обладнання.

У результаті було створено робочу лабораторну топологію гетерогенної комутованої мережі. Отримані діагностичні дані стали основою для подальшого опису конфігурації мережевих пристроїв, розгортання моніторингу, аналізу параметрів роботи та перевірки відмовостійкості.

3.2 Налаштування мережевих пристроїв

Після створення лабораторної топології було виконано налаштування мережевих пристроїв, які входять до складу стенда. Основна конфігурація виконувалася на двох стекованих вузлах Cisco та комутаторі ZTE ZXR10. На Cisco-комутаторах було налаштовано стекування, керуючі інтерфейси, SSH-доступ, Spanning Tree, EtherChannel/LACP і SNMP. На ZTE ZXR10 було налаштовано керуючий інтерфейс, smartgroup, фізичний порт підключення, SSH і SNMP.

Першим було налаштовано стек Cisco Catalyst 2960S з іменем SW-29. Його конфігурація містить службові параметри IOS, hostname, локального адміністративного користувача, дані про трьох учасників стеку, налаштування Spanning Tree, SSH, Port-channel, керуючого інтерфейсу VLAN 1 та SNMP.



```

COM7 - PuTTY
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW-29
!
username admin privilege 15 secret 5 $1$oESl$GfY0y3v4lzQ21lKZu/bdq1
no aaa new-model
switch 1 provision ws-c2960s-f24ts-1
switch 2 provision ws-c2960s-f24ts-1
switch 3 provision ws-c2960s-f24ts-1
!
ip domain-name local
ip device tracking
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2

```

Рисунок 3.3 – Налаштування на SW-29

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

Локальний користувач admin має 15 рівень привілеїв, що дозволяє виконувати повне адміністрування пристрою. Команди switch provision визначають склад стеку. У цьому випадку стек складається з трьох комутаторів моделі ws-c2960s-f24ts-l. Порти першого комутатора відображаються як FastEthernet1/0/x, другого - як FastEthernet2/0/x, третього - як FastEthernet3/0/x.

Режим Spanning Tree для SW-29 - spanning-tree mode pvst [16]. Команда spanning-tree extend system-id додає ідентифікатор VLAN до Bridge ID. У практичній схемі це використовується для роботи VLAN 1 і контролю топології другого рівня [15]. SSH версії 2 увімкнено, а доменне ім'я local використовується для службової генерації параметрів SSH.

```

COM7 - PuTTY
SW-29#show switch
Switch/Stack Mac Address : c07b.bcbf.cd80

Switch#  Role  Mac Address      Priority Version  Current State
-----
*1      Master c07b.bcbf.cd80    15      1      Ready
2       Member 1c1d.86bc.e200    10      1      Ready
3       Member 5017.ffae.4c80    5       1      Ready
  
```

Рисунок 3.4 – Перевірка комутаторів, які входять до стеку

Після базової конфігурації було перевірено фактичний склад стеку SW-29. Команда show switch показала, що всі три учасники стеку перебувають у стані Ready.

```

COM7 - PuTTY
SW-29#show switch detail
Switch/Stack Mac Address : c07b.bcbf.cd80

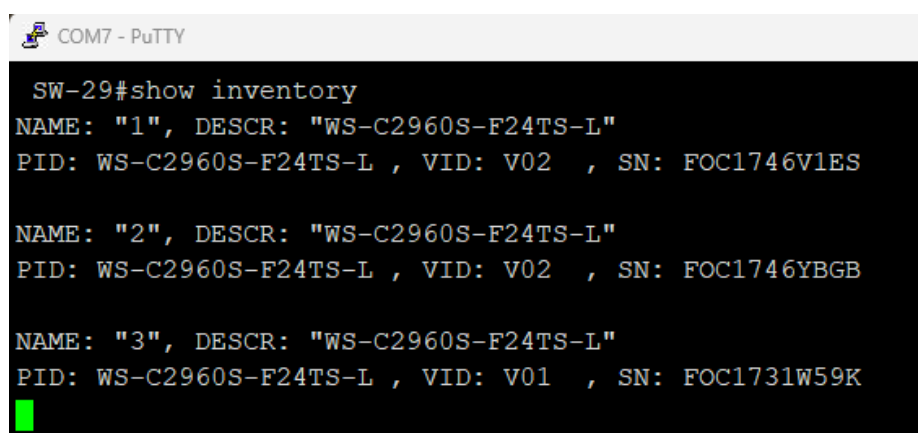
Switch#  Role  Mac Address      Priority Version  Current State
-----
*1      Master c07b.bcbf.cd80    15      1      Ready
2       Member 1c1d.86bc.e200    10      1      Ready
3       Member 5017.ffae.4c80    5       1      Ready

Stack Port Status      Neighbors
Switch#  Port 1  Port 2      Port 1  Port 2
-----
1        Ok     Ok          2        3
2        Ok     Ok          1        3
3        Ok     Ok          1        2
  
```

Рисунок 3.5 – Перевірка стек портів

Усі stack-порти мають стан Ok. Для кожного учасника також відображені сусіди по стекових з'єднаннях. Це підтверджує, що стекові з'єднання між трьома комутаторами працюють і комутатори бачать один одного в межах FlexStack.

Цей результат підтверджує робочий стан обох стекових портів на кожному учаснику. Для стеку з трьох комутаторів це важливо, оскільки порушення одного стекового з'єднання може не зупинити роботу логічного вузла, але вплине на його внутрішню стійкість. На SW-29 також було створено Port-channel-інтерфейс. Port-channel2 працює в access-режимі. Фізичний порт FastEthernet3/0/1 входить до channel-group 2 у режимі active, тобто бере участь у формуванні LACP-каналу.



```

COM7 - PuTTY
SW-29#show inventory
NAME: "1", DESCR: "WS-C2960S-F24TS-L"
PID: WS-C2960S-F24TS-L , VID: V02 , SN: FOC1746V1ES

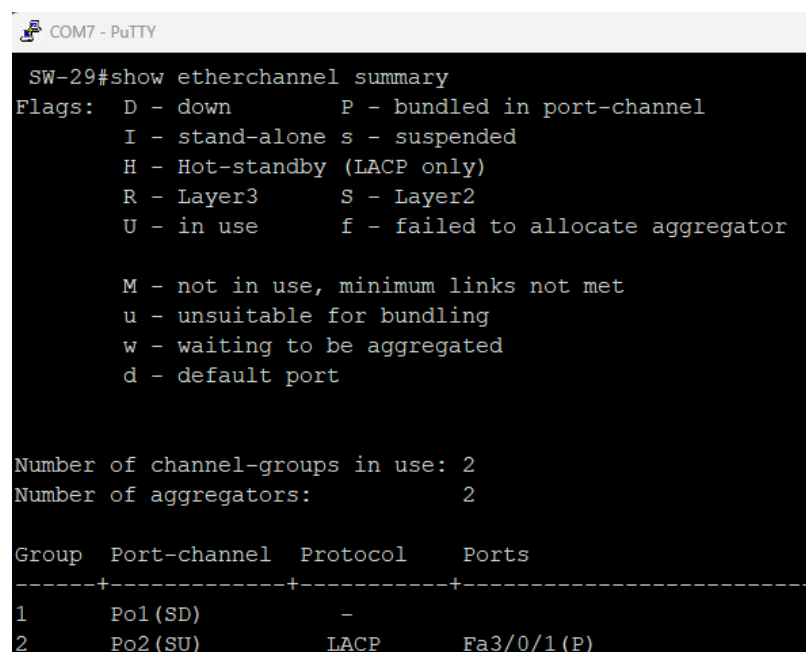
NAME: "2", DESCR: "WS-C2960S-F24TS-L"
PID: WS-C2960S-F24TS-L , VID: V02 , SN: FOC1746YBGB

NAME: "3", DESCR: "WS-C2960S-F24TS-L"
PID: WS-C2960S-F24TS-L , VID: V01 , SN: FOC1731W59K

```

Рисунок 3.6 – Перевірка апаратного складу стеку

Стан EtherChannel було перевірено командою show etherchannel summary:



```

COM7 - PuTTY
SW-29#show etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1       Po1 (SD)        -           -
2       Po2 (SU)        LACP        Fa3/0/1 (P)

```

Рисунок 3.7 – Перевірка апаратного складу стеку

Позначення Po2(SU) означає, що Port-channel2 є L2-каналом і перебуває у використанні. Позначення Fa3/0/1(P) показує, що фізичний порт FastEthernet3/0/1 успішно включений до складу Port-channel2.

```

COM7 - PuTTY
SW-29#show lacp neighbor
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode           P - Device is in Passive mode

Channel group 2 neighbors

Partner's information:

Port      Flags    LACP port      Dev ID      Age    Admin  Oper  Port  Port
Fa3/0/1   SA      32768         a493.4c9d.f480  19s    0x0    0x2   0x103 0x3D
SW-29#
  
```

Рисунок 3.8 – Перевірка сусідства через LACP-групу

У цьому виводі видно, що порт Fa3/0/1 має LACP-сусіда з Dev ID a493.4c9d.f480. Цей ідентифікатор відповідає сусідньому стеку Cisco Catalyst 3750X. Отже, між SW-29 і верхнім стеком сформовано LACP-взаємодію через Port-channel2. Для перевірки проходження трафіку було переглянуто динамічну таблицю MAC-адрес.

```

COM7 - PuTTY
SW-29#show mac address-table dynamic
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       00e0.4c36.0395   DYNAMIC   Po2
1       a493.4c9d.f482   DYNAMIC   Po2
1       a493.4c9d.f4c0   DYNAMIC   Po2
Total Mac Addresses for this criterion: 3
SW-29#
  
```

Рисунок 3.9 – Перевірка таблиці MAC-адрес

Другим було налаштовано верхній стек Cisco Catalyst 3750X з іменем SW-1-UPPER. Його конфігурація містить дані двох комутаторів, налаштування Rapid

PVST+, Port-channel-інтерфейси, керуючий інтерфейс VLAN 1, SSH-доступ і SNMP.

Фрагмент базової конфігурації SW-1-UPPER має такий вигляд:

```
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname SW-1-UPPER
username admin privilege 15 secret <encrypted_password>
no aaa new-model
switch 1 provision ws-c3750x-24p
switch 2 provision ws-c3750x-24p
system mtu routing 1500
ip domain-name local
spanning-tree mode rapid-pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip ssh version 2
```

```
COM6 - PuTTY
SW-1-UPPER#show switch
Switch/Stack Mac Address : a493.4c9d.f480

Switch#  Role  Mac Address      Priority Version  Current State
-----
*1      Master a493.4c9d.f480    15      3      Ready
2       Member 70ca.9b56.7200    1       3      Ready
```

Рисунок 3.10 – Фактичний склад стеку

У стеку SW-1-UPPER присутні два комутатори. Перший має роль Master і пріоритет 15, другий працює як Member із пріоритетом 1. Обидва учасники перебувають у стані Ready.

Команда show switch detail показала стан stack-портів:

```

COM6 - PuTTY

SW-1-UPPER#show switch detail
Switch/Stack Mac Address : a493.4c9d.f480

Switch#  Role  Mac Address      Priority  H/W  Current
          Version  State
-----
*1      Master  a493.4c9d.f480    15       3     Ready
 2      Member  70ca.9b56.7200    1        3     Ready

Switch#  Stack Port  Status      Neighbors
          Port 1  Port 2      Port 1  Port 2
-----
 1        Ok     Down        2        None
 2        Ok     Down        1        None

```

Рисунок 3.11 – Стан портів стеку

У цьому стеку перший stack-порт на кожному комутаторі має стан Ok, а другий - Down. Це означає, що між двома комутаторами є робоче стекове з'єднання, але кільцева схема не замкнена другим stack-каналом. Такий стан не завадив формуванню стеку, оскільки обидва комутатори визначаються як Ready, але кільце можливе при додаванні нових юнітів.

```

COM6 - PuTTY

SW-1-UPPER#show inventory
NAME: "1", DESCR: "WS-C3750X-24P"
PID: WS-C3750X-24P-L , VID: V02 , SN: FDO1620R0WK

NAME: "Switch 1 - Power Supply 1", DESCR: "FRU Power Supply"
PID: PWR-C1-715WAC , VID: V01D , SN: DCB1849G265

NAME: "Switch 1 - FRULink Slot 1 - FRULink Module", DESCR: "FRULink 1G Module"
PID: C3KX-NM-1G , VID: V01 , SN: FDO17032JFX

NAME: "2", DESCR: "WS-C3750X-24P"
PID: WS-C3750X-24P-L , VID: V02 , SN: FDO1539K03J

NAME: "Switch 2 - Power Supply 1", DESCR: "FRU Power Supply"
PID: C3KX-PWR-715WAC , VID: V02D , SN: DTN1626K03B

NAME: "Switch 2 - FRULink Slot 1 - FRULink Module", DESCR: "FRULink 1G Module"
PID: C3KX-NM-1G , VID: V01 , SN: FDO17030Z91

SW-1-UPPER#

```

Рисунок 3.12 – Апаратний склад стеку

```

COM6 - PuTTY

interface GigabitEthernet1/0/1
switchport mode access
channel-group 1 mode active
!
interface GigabitEthernet1/0/2
switchport mode access
channel-group 1 mode active
!
interface GigabitEthernet1/0/3
switchport mode access
speed 100
channel-group 2 mode active
!
interface GigabitEthernet1/0/4
switchport mode access
speed 100
channel-group 2 mode active
!
interface GigabitEthernet1/0/5
switchport mode access
speed 100
channel-group 2 mode active

```

Рисунок 3.13 – Конфігурація фізичних інтерфейсів

У цьому фрагменті інтерфейси додані до відповідних channel-group у режимі active. Це означає використання LACP. У фактичному стані, за результатами діагностики, активними учасниками були Gi1/0/1 у Port-channel1 та Gi1/0/2 у Port-channel2.

```

COM6 - PuTTY

SW-1-UPPER#show etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1 (SU)        LACP       Gi1/0/1 (P)
2      Po2 (SU)        LACP       Gi1/0/2 (P)

```

Рисунок 3.14 – Стан EtherChannel на SW-1-UPPER

Команда `show lacp neighbor` показала LACP-сусідів для обох channel-group:

```

COM6 - PuTTY
Channel group 1 neighbors
Port      Flags    Priority  Dev ID      Age  Admin key Oper Key Port Number State
Gi1/0/1   SA       32768    0022.935b.a81c 3s   0x0      0x211    0x1      0x3D
Channel group 2 neighbors
Port      Flags    Priority  Dev ID      Age  Admin key Oper Key Port Number State
Gi1/0/2   SA       32768    c07b.bcbf.cd80 21s   0x0      0x2      0x302    0x3D
  
```

Рисунок 3.15 – Перегляд LACP-сусідств

Для Port-channel2 сусід має Dev ID `c07b.bcbf.cd80`, що відповідає стеку SW-29. Це підтверджує LACP-взаємодію між SW-1-UPPER і SW-29. Для Port-channel1 визначено окремого LACP-сусіда, що відповідає підключенню іншого мережевого вузла.

Третім пристроєм було налаштовано комутатор ZTE ZXR10. Його конфігурація відрізняється від синтаксису Cisco, але основні задачі залишаються тими самими: керуюча адреса, фізичні інтерфейси, smartgroup, SSH і SNMP.

Фрагмент конфігурації керуючого інтерфейсу ZTE ZXR10:

```

hostname ZXR10
interface vlan 1
ip address 192.168.1.7 255.255.255.0
out_index 27
vlan list 1
ztp vlan 1
  
```

Адреса 192.168.1.7 використовується для доступу до ZTE ZXR10 і його підключення до моніторингу. Інтерфейс VLAN 1 розміщений у тому самому керуючому сегменті, що й комутатори Cisco та сервер Zabbix.

Для організації логічного підключення на ZTE було створено smartgroup2:

```

interface smartgroup2
out_index 29
switchport access vlan 1
smartgroup mode 802.3ad
  
```

Smartgroup2 є логічним інтерфейсом ZTE, який відповідає ідеї агрегованого каналу. Для нього вказано VLAN 1 і режим `802.3ad`, тобто LACP. У Cisco аналогом такого логічного інтерфейсу є Port-channel.

Фізичний інтерфейс gei_1/1 було додано до smartgroup2:

```
interface gei_1/1
  out_index 3
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
  smartgroup 2 mode active
```

Команда smartgroup 2 mode active додає фізичний інтерфейс gei_1/1 до smartgroup2 в активному режимі LACP. У поточній схемі використовується один фізичний інтерфейс, тому логічний канал працює з одним активним учасником. Така конфігурація дозволяє узгодити LACP-взаємодію з Cisco-стороною та залишає структуру каналу зрозумілою для діагностики.

Після налаштування Cisco та ZTE було виконано перевірку взаємодії між пристроями. На Cisco-комутаторах перевірялися Port-channel, LACP-сусідство, STP, MAC-таблиці та ARP. На ZTE перевірялися smartgroup, фізичний інтерфейс gei_1/1 і керуюча адреса.

У результаті налаштування було отримано робочу конфігурацію стенда. Стек SW-29 сформований із трьох комутаторів Cisco 2960S, має активний керуючий інтерфейс 192.168.1.4, робочі stack-порти, Port-channel2 на основі LACP і SNMP-доступ. Стек SW-1-UPPER сформований із двох комутаторів Cisco 3750X, має адресу 192.168.1.2, працює як root bridge для VLAN 1, має активні Port-channel1 і Port-channel2 та SNMP-доступ. Комутатор ZTE ZXR10 має адресу 192.168.1.7, smartgroup2 з інтерфейсом gei_1/1, SSH-доступ і SNMP-конфігурацію. Отримані конфігурації та діагностичні виводи стали основою для подальшого підключення обладнання до Zabbix і аналізу роботи мережі.

3.3 Розгортання системи моніторингу Zabbix

Після налаштування мережевих пристроїв було розгорнуто систему моніторингу Zabbix. Сервер моніторингу мав адресу 192.168.1.9 і був розміщений у тому самому керуючому сегменті, що й комутатори Cisco та ZTE. Це дозволило виконувати SNMP-опитування пристроїв без додаткової маршрутизації та використовувати Zabbix як єдину точку контролю стану лабораторної мережі.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

У системі Zabbix були створені окремі хости для стеку Cisco Catalyst 3750X, стеку Cisco Catalyst 2960S та комутатора ZTE ZXR10. Для зручності ідентифікації використовувалися імена, які відповідають фактичним пристроям у стенді: SW-1-UPPER для стеку Cisco Catalyst 3750X, SW-FLEX для стеку Cisco Catalyst 2960S та ZXR10 для комутатора ZTE. Слід зазначити, що стек Cisco Catalyst 2960S, налаштований з іменем SW-29, у системі Zabbix зареєстровано як хост SW-FLEX, тому далі обидві назви позначають той самий стек. Основним інтерфейсом для опитування було обрано SNMP.

Name ▲	Interface	Availability	Tags
<u>SW-1-UPPER</u>	192.168.1.2:161	SNMP	class: network target: cisco target: cisco-ios
<u>SW-FLEX</u>	192.168.1.4:161	SNMP	class: network target: cisco target: cisco-ios
<u>Zabbix server</u>	127.0.0.1:10050	ZBX	class: os class: software subclass: logging ...
<u>ZTE-SW</u>	192.168.1.7:161	SNMP	class: network target: snmp

Рисунок 3.16 – Список мережевих пристроїв у Zabbix

Перед додаванням пристроїв до Zabbix на них було перевірено SNMP-конфігурацію. На пристроях було задано SNMP-доступ у режимі читання (RO), обмежений списком доступу лише адресою сервера моніторингу 192.168.1.9, а також місце розташування й контакт адміністратора:

```
snmp-server community <community> RO SNMP-NMS
snmp-server location ServerRoom
snmp-server contact admin
```

На стеку Cisco Catalyst 3750X було використано аналогічну логіку SNMP-налаштування:

```
snmp-server community <community> RO SNMP-NMS
snmp-server location ServerRoom
snmp-server contact admin
```

У конфігурації комутатора ZTE ZXR10 було задано SNMP engine-id, community, SNMP view та ввімкнено службові повідомлення SNMP:

```
snmp-server packetsize 1400
snmp-server engine-id 830900020300010289d64401
snmp-server community <community> view allview ro
snmp-server view AllView internet included
```

```
snmp-server view DefaultView system included
snmp-server enable trap SNMP
snmp-server enable trap RMON
snmp-server enable trap STALARM
```

Після додавання хостів було виконано перевірку доступності SNMP-інтерфейсів. Для цього використовувалися стандартні елементи даних Zabbix, які перевіряють доступність пристрою, отримують базову інформацію про систему та визначають список інтерфейсів. Для комутаторів Cisco було використано SNMP-шаблони, які дозволяють отримувати інформацію про інтерфейси, трафік, помилки та стан портів. Для ZTE було використано SNMP-опитування за стандартними OID та доступними параметрами пристрою.

Рисунок 3.17 – Налаштування SNMP-інтерфейсу хоста SW-1-UPPER

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

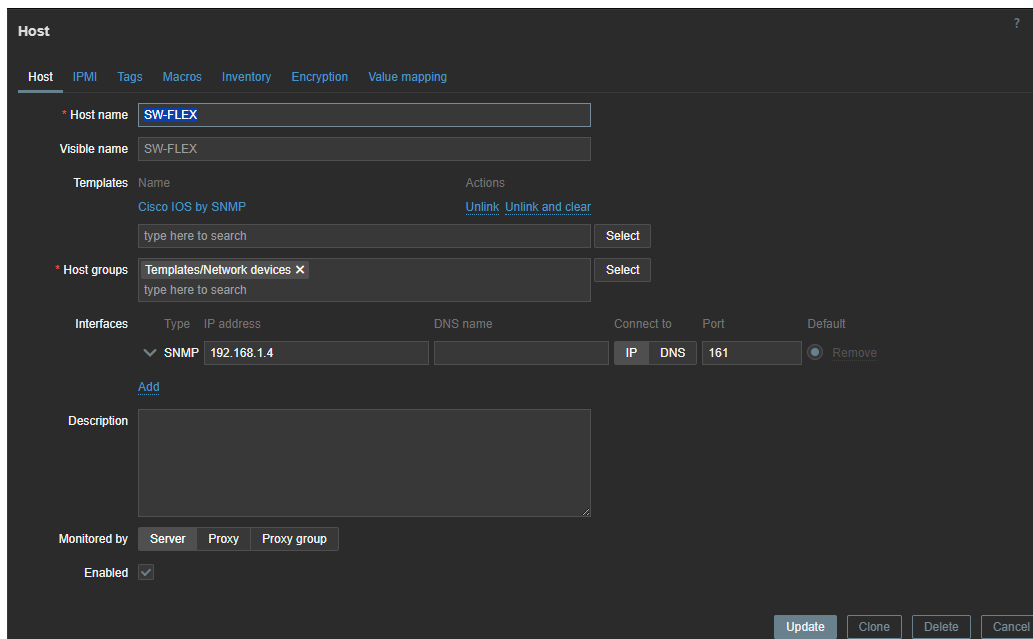


Рисунок 3.18 – Налаштування SNMP-інтерфейсу хоста SW-FLEX

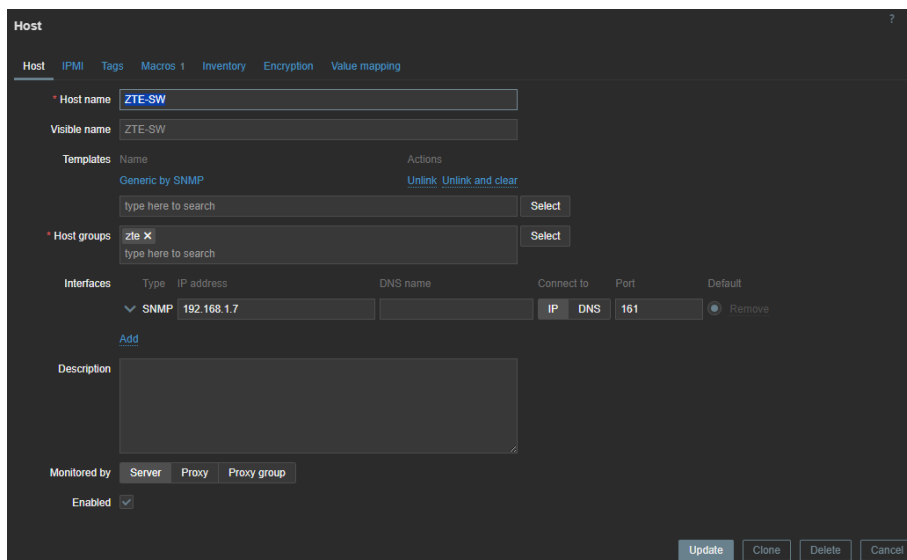


Рисунок 3.19 – Налаштування SNMP-інтерфейсу хоста ZXR10

Після прив'язки шаблонів у Zabbix було отримано перелік інтерфейсів пристроїв. Для стекованих комутаторів Cisco це особливо важливо, оскільки один логічний хост містить інтерфейси кількох фізичних комутаторів. Наприклад, на стеку Cisco Catalyst 2960S інтерфейси мають нумерацію з урахуванням номера учасника стеку: FastEthernet1/0/x, FastEthernet2/0/x та FastEthernet3/0/x. У Zabbix ці інтерфейси відображалися як елементи одного хоста SW-FLEX.

Для стеку Cisco Catalyst 3750X у Zabbix відображалися фізичні інтерфейси обох учасників стеку, а також логічні Port-channel-інтерфейси. Це дозволило контролювати не лише доступність пристрою загалом, а й стан конкретних

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

підключень. Особливу увагу було приділено Port-channel1 і Port-channel2, оскільки вони використовуються для міжкомутаторної взаємодії.

Для базового моніторингу були використані такі групи параметрів: доступність хоста, стан інтерфейсів, вхідний і вихідний трафік, помилки на інтерфейсах, зміна операційного стану порту та службова інформація SNMP. Отримані дані дозволили побудувати графіки завантаження каналів і відстежувати стан основних підключень.

- stack.ssh.status (Numeric) – Стан SSH-опитування пристрою;
- stack.event.stack_added (Numeric) – Подія додавання учасника стеку;
- stack.event.stack_removed (Numeric) – Подія випадання учасника стеку;
- stack.event.stack_ready (Numeric) – Подія готовності учасника стеку;
- stack.event.stack_master (Numeric) – Подія, пов'язана з master-пристроєм;
- stack.event.stack_link (Numeric) – Подія зміни стану stack-link;
- stack.last_event (Text) – Текст останньої події стеку;
- stack.severity (Numeric) – Загальний рівень важливості останньої події.

Стандартний SNMP-моніторинг забезпечив контроль доступності пристроїв та інтерфейсів. Однак під час налаштування було виявлено, що стандартні шаблони не дають потрібної деталізації для контролю системних подій стеку Cisco. Зокрема, базові шаблони не формували окремі події для випадання учасника стеку, додавання учасника, готовності комутатора, зміни master-пристрою або зміни стану stack-link. Ці події фіксуються в журналі Cisco, але не відображаються як окремі зручні параметри в стандартному SNMP-шаблоні.

Для закриття цієї задачі було розроблено власний Python-скрипт, який працює як додатковий механізм моніторингу стеків Cisco. Скрипт підключається до комутаторів через SSH, виконує команду show logging, аналізує отримані рядки журналу, шукає події Stack Manager і передає результат у Zabbix через zabbix_sender.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

У скрипті було визначено список пристроїв, які потрібно опитувати. Для кожного пристрою вказано його IP-адресу та відповідне ім'я хоста в Zabbix. Це потрібно тому, що ім'я хоста в Zabbix повинно точно збігатися з іменем, яке використовується під час передавання даних через zabbix_sender.

Фрагмент налаштування відповідності між IP-адресами та хостами Zabbix:

```
ZABBIX_SERVER = "127.0.0.1"
ZABBIX_HOST_MAP = {
    "192.168.1.4": "SW-FLEX",
    "192.168.1.2": "SW-1-UPPER",
}
SWITCHES = [
    {"name": "SW-FLEX", "host": "192.168.1.4"},
    {"name": "SW-1-UPPER", "host": "192.168.1.2"},
]
```

У цьому фрагменті стек Cisco Catalyst 2960S відповідає хосту `SW-FLEX`, а стек Cisco Catalyst 3750X - хосту `SW-1-UPPER`. Саме ці імена використовуються під час передавання значень у Zabbix. Якщо ім'я в скрипті не збігається з іменем хоста в Zabbix, сервер не прийме значення для відповідного item.

Для підключення до комутаторів використовувалися бібліотеки `paramiko` та `netmiko`. Оскільки в стенді застосовуються старіші моделі Cisco, у скрипті було додано налаштування сумісності SSH-обміну. Це дало змогу встановлювати SSH-з'єднання з пристроями, які підтримують застаріліші алгоритми обміну ключами.

Фрагмент налаштування SSH-сумісності:

```
paramiko.transport.Transport._preferred_kex = (
    "diffie-hellman-group14-sha1",
    "diffie-hellman-group-exchange-sha1",
    "diffie-hellman-group1-sha1",
)
```

Цей блок не змінює конфігурацію комутаторів, а впливає лише на роботу Python-клієнта. Він був потрібний для того, щоб скрипт міг стабільно підключатися до Cisco IOS через SSH та отримувати журнал командою show logging.

Для пошуку подій стеку було створено набір регулярних виразів. Кожен вираз відповідає окремому типу події Stack Manager:

```
PATTERNS = {
```

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		82

```

"STACK_ADDED": re.compile(r"%STACKMGR-.*SWITCH_ADDED", re.I),
"STACK_REMOVED": re.compile(r"%STACKMGR-.*SWITCH_REMOVED", re.I),
"STACK_READY": re.compile(r"%STACKMGR-.*SWITCH_READY", re.I),
"STACK_MASTER": re.compile(r"%STACKMGR-.*MASTER_READY", re.I),
"STACK_LINK": re.compile(r"%STACKMGR-.*STACK_LINK_CHANGE", re.I),
}

```

Подія `STACK\_ADDED` відповідає появі учасника стеку. Подія `STACK\_REMOVED` відповідає випадінню учасника зі стеку. Подія `STACK\_READY` фіксує готовність комутатора. Подія `STACK\_MASTER` використовується для визначення зміни або готовності керуючого пристрою. Подія `STACK\_LINK` відповідає зміні стану стекового з'єднання.

Для кожного типу події було задано числовий рівень важливості. Це значення передається в Zabbix і може використовуватися в тригерах [19]:

```

SEVERITY_MAP = {
    "STACK_ADDED": 1,
    "STACK_REMOVED": 3,
    "STACK_READY": 1,
    "STACK_MASTER": 2,
    "STACK_LINK": 2,
}

```

У цій шкалі значення 1 використовується для інформаційних подій, 2 - для попереджень, 3 - для критичніших подій. Найвищий рівень у цьому наборі отримує `STACK\_REMOVED`, оскільки випадання учасника стеку безпосередньо впливає на фізичний склад логічного вузла.

Передавання даних у Zabbix виконується через `zabbix\_sender`. Для цього в скрипті реалізовано функцію `send\_to\_zabbix`, яка формує команду з адресою Zabbix-сервера, іменем хоста, ключем item та значенням:

```

def send_to_zabbix(zabbix_host, item_key, value):
    cmd = [
        "zabbix_sender",
        "-z", ZABBIX_SERVER,
        "-s", zabbix_host,
        "-k", item_key,
        "-o", str(value),
    ]
    result = subprocess.run(cmd, capture_output=True, text=True, timeout=10)

```

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

Ця функція використовується для передавання як числових, так і текстових значень. Наприклад, числовий item `stack.severity` отримує рівень важливості події, а текстовий item `stack.last\_event` отримує короткий опис останньої знайденої події.

Підключення до Cisco-комутатора та отримання журналу виконується функцією `get\_logs`. Вона встановлює SSH-з'єднання, переходить у привілейований режим і виконує команду `show logging`:

```
def get_logs(host, retries=3):
    conn = ConnectHandler(
        device_type="cisco_ios_ssh",
        host=host,
        username=USERNAME,
        password=PASSWORD,
        conn_timeout=30,
        banner_timeout=30,
        auth_timeout=30,
        fast_cli=False,
    )
    conn.enable()
    output = conn.send_command("show logging", read_timeout=120)
    conn.disconnect()
    return output.splitlines()
```

У разі помилки підключення скрипт передає в Zabbix значення `0` для item `stack.ssh.status`. Якщо журнал успішно отримано, у Zabbix передається значення `1`. Це дозволяє окремо контролювати не тільки події стеку, а й доступність комутатора для SSH-опитування.

Основний аналіз журналу виконується у функції `analyze`. Вона проходить по рядках журналу, перевіряє їх за регулярними виразами та після збігу передає дані в Zabbix:

```
def analyze(device, logs):
    host = device["host"]
    zabbix_host = ZABBIX_HOST_MAP.get(host, device["name"])
    if logs:
        send_to_zabbix(zabbix_host, "stack.ssh.status", 1)
    for line in logs:
        line = line.strip()
        for event, pattern in PATTERNS.items():
            if pattern.search(line):
```

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

```

severity = SEVERITY_MAP.get(event, 1)
send_to_zabbix(
    zabbix_host,
    f"stack.event.{event.lower()}",
    severity
)
send_to_zabbix(
    zabbix_host,
    "stack.last_event",
    f"{event}:{line[:100]}"
)

send_to_zabbix(
    zabbix_host,
    "stack.severity",
    severity
)

```

У цьому блоці для кожної знайденої події оновлюються три типи item. Перший item має вигляд `stack.event.<тип\_події>` і зберігає рівень важливості конкретної події. Другий item `stack.last\_event` зберігає текст останньої події. Третій item `stack.severity` зберігає загальний рівень критичності останньої знайденої події.

Для уникнення повторної обробки одного й того самого рядка журналу в скрипті використовується множина `processed`. У ній зберігається комбінація IP-адреси пристрою та рядка журналу. Якщо такий запис уже був оброблений, скрипт не надсилає його повторно в Zabbix. Це зменшує кількість дубльованих подій.

Опитування пристроїв виконується в циклі з інтервалом 30 секунд:

```

def main():
    print("STACK monitor STARTED → Zabbix mode")
    while True:
        for sw in SWITCHES:
            logs = get_logs(sw["host"])
            analyze(sw, logs)
        time.sleep(30)

```

Інтервал 30 секунд визначає максимальну затримку між появою події в журналі Cisco та її виявленням скриптом. Після виявлення події значення одразу передається в Zabbix через `zabbix\_sender`.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

Для приймання даних від скрипта в Zabbix були створені окремі trapper-items. Вони не опитуються самим Zabbix, а очікують значення, які надсилає зовнішній скрипт. Для кожного стеку Cisco було створено однаковий набір item.

На основі item `stack.severity` було створено тригер, який спрацьовує при появі події з підвищеним рівнем важливості. Для окремого контролю випадання учасника стеку також використовувався item `stack.event.stack\_removed`. Такий підхід дозволяє формувати подію в Zabbix навіть тоді, коли SNMP-параметри пристрою ще залишаються доступними, але в журналі Cisco вже зафіксовано зміну складу стеку.

Рисунок 3.20 – Тригер Zabbix для подій стеку Cisco

Окремо було налаштовано дію Zabbix для надсилання повідомлень на електронну пошту. Після спрацювання тригера система формує повідомлення адміністратору із зазначенням хоста, рівня важливості та тексту останньої події. Текст події береться з item `stack.last\_event`, який оновлюється Python-скриптом.

Формат повідомлення містить ім'я хоста, тип події, час спрацювання та короткий опис із журналу Cisco. Це дозволяє одразу зрозуміти, на якому стеку виникла подія та до якого типу вона належить. Для подій `STACK\_REMOVED`

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

повідомлення має підвищену важливість, оскільки воно означає втрату учасника стеку.

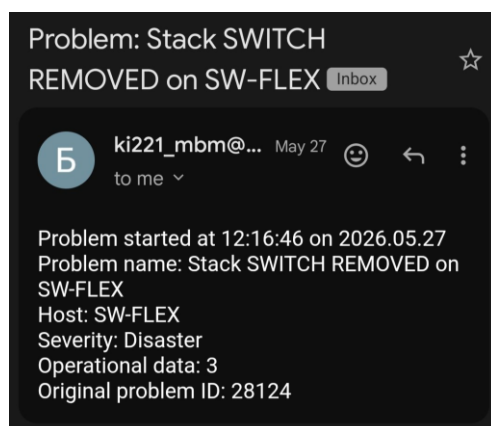


Рисунок 3.21 – Email-повідомлення про подію стеку Cisco

Після налаштування базового SNMP-моніторингу та власного механізму обробки подій стеку система Zabbix почала виконувати дві функції. Перша функція - стандартний контроль мережевих пристроїв: доступність, стан інтерфейсів, трафік і помилки. Друга функція - контроль спеціалізованих подій стеку Cisco через журнал `show logging` і зовнішній Python-скрипт. Поєднання цих двох механізмів дозволило контролювати як поточні параметри інтерфейсів, так і події, пов'язані зі зміною складу стеку.

3.4 Аналіз параметрів функціонування мережі

Після налаштування мережевих пристроїв і підключення їх до Zabbix було виконано перевірку фактичної роботи мережі. Аналіз проводився за трьома напрямками: перевірка комутаційної частини через, контроль параметрів у Zabbix та тестування реакції системи на події стеку Cisco.

Для кожного мережевого пристрою контролювалася доступність, стан інтерфейсів, наявність вхідного та вихідного трафіку, а також помилки на портах. Основна увага приділялася інтерфейсам, які беруть участь у міжкомутаторній взаємодії: Port-channel2 на SW-29, Port-channel1 і Port-channel2 на SW-1-UPPER, а також smartgroup2 на ZTE ZXR10.

У Zabbix було перевірено, що хости SW-1-UPPER, SW-FLEX і ZXR10 перебувають у доступному стані. Для Cisco-пристроїв додатково контролювалися SNMP-інтерфейси, які відповідають фізичним портам і логічним Port-channel. Для

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

ZTE контролювався стан доступності пристрою та інтерфейсу, пов'язаного з підключенням до Cisco-частини мережі.

Окремим напрямом аналізу була перевірка роботи власного механізму виявлення подій стеку Cisco. Стандартний SNMP-контроль показував стан пристроїв та інтерфейсів, але події зміни складу стеку було винесено в окремий механізм. Python-скрипт опитував обидва Cisco-стеки через SSH, виконував `show logging`, знаходив повідомлення Stack Manager і передавав результат у Zabbix.

Для перевірки цього механізму контролювалися такі item: `stack.ssh.status`, `stack.event.stack\_added`, `stack.event.stack\_removed`, `stack.event.stack\_ready`, `stack.event.stack\_master`, `stack.event.stack\_link`, `stack.last\_event` і `stack.severity`.

Для перевірки виявлення відмов було виконано контрольовану зміну стану стеку. Після появи відповідного запису в журналі Cisco скрипт визначав тип події за регулярним виразом і передавав її в Zabbix. Якщо подія відповідала випадінню учасника стеку, оновлювався item `stack.event.stack\_removed`, item `stack.last\_event` отримував текст останнього повідомлення, а `stack.severity` отримував підвищене числове значення.



Рисунок 3.22 – Зміна складу стеку та його автоматичне відновлення

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

Схема обробки події мала такий вигляд: подія з'являється в журналі Cisco, скрипт отримує журнал через SSH, визначає тип події, надсилає значення через `zabbix\_sender`, Zabbix оновлює item, після чого спрацьовує відповідний тригер. У разі налаштованої дії Zabbix формує email-повідомлення адміністратору [12].

The screenshot shows the Zabbix monitoring interface. The top part displays a list of problems with columns for Time, Severity, Recovery time, Status, Info, Host, Problem, Duration, Update, Actions, and Tags. The bottom part shows a detailed view of a specific problem, including its history and actions.

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
04:00:56 PM	Information		PROBLEM		SW-FLEX	Cisco IOS: 2: Device has been replaced (new serial number received)	1h 6m 54s	Update		class: network component: system scope: notice
04:00:06 PM	Average		PROBLEM		SW-FLEX	Cisco IOS: Interface Fa1/0/1(): Link down				
Today										
2026-05-27 12:16:46 PM	Disaster		PROBLEM		SW-FLEX	Stack SWITCH REMOVED on SW-FLEX				

Time	User/Recipient	Action	Message/Command	Status	Info
2026-06-05 05:07:18 PM	Admin (Zabbix Administrator)		e		
2026-06-05 04:00:56 PM	Admin (Zabbix Administrator)		ALERTS	Sent	
2026-06-05 04:00:56 PM					

Рисунок 3.23 – Спрацювання тригера та поява проблеми Zabbix після події стеку

Для оцінки швидкості виявлення подій було враховано інтервал роботи скрипта. У конфігурації скрипта основний цикл виконується з паузою 30 секунд. Тому максимальна затримка між появою події в журналі Cisco та її виявленням скриптом визначається цим інтервалом. Передавання значення в Zabbix після виявлення виконується через `zabbix\_sender`, тобто без очікування наступного SNMP-опитування.

Окремо перевірялася подія, пов'язана зі зміною керуючого комутатора стеку. У разі втрати master-пристрою стек виконує вибір нового керуючого учасника. Після завершення цього процесу в журналі Cisco з'являється повідомлення, яке визначається скриптом як `STACK\_MASTER`. Для цієї події встановлено рівень важливості `2`, тобто попередження.

Для доповнення якісного аналізу роботи мережі було виконано кількісну оцінку параметрів, які безпосередньо перевірялися на лабораторному стенді. Основну увагу приділено часу відновлення керування стеком Cisco та часу виявлення відповідної події системою моніторингу Zabbix. Ці показники розглядаються окремо, оскільки відновлення роботи стеку відбувається засобами самого обладнання Cisco, а фіксація події в Zabbix залежить від інтервалу роботи додаткового Python-скрипта. Під час перевірки було встановлено, що у випадку втрати поточного master-пристрою стек Cisco виконує переобрання нового керуючого учасника приблизно за 3 секунди. Після цього стек продовжує роботу з новим master-пристроєм. Подія зміни керуючого пристрою фіксується в

системному журналі Cisco, після чого Python-скрипт отримує журнал через SSH, аналізує повідомлення Stack Manager і передає результат у Zabbix через zabbix_sender. Інтервал опитування журналу Cisco у скрипті становить 30 секунд. Тому максимальний час виявлення події системою моніторингу не перевищує одного циклу опитування. Це означає, що фактичне відновлення керування стеком відбувається швидше, ніж подія потрапляє до Zabbix, однак система моніторингу фіксує сам факт зміни та формує повідомлення адміністратору.

Таблиця 3.1

Кількісна оцінка відновлення та виявлення подій стеку Cisco

Сценарій перевірки	Показник	Отримане значення	Метод оцінки
Втрата master-пристрою	Час переобрання нового master	≈ 3 с	Спостереження за станом стеку та журналом Cisco
Виявлення зміни master у Zabbix	Максимальний час фіксації події	до 30 с	Інтервал опитування Python-скрипта
Випадання учасника стеку	Максимальний час виявлення події	до 30 с	Подія `SWITCH_REMOVED` у `show logging`
Повернення учасника стеку	Максимальний час виявлення події	до 30 с	Події `SWITCH_ADDED` / `SWITCH_READY` у `show logging`
Зміна стану stack-link	Максимальний час виявлення події	до 30 с	Подія `STACK_LINK_CHANGE` у `show logging`

Таким чином, кількісна оцінка підтвердила, що стек Cisco здатний швидко відновити керуючу роль після втрати master-пристрою, а система Zabbix разом із Python-скриптом забезпечує автоматичне виявлення подій стеку протягом одного циклу опитування. Для поточної реалізації час переобрання master становив

приблизно 3 секунди, а максимальний час виявлення події в Zabbix — до 30 секунд.

Під час аналізу такої події перевірялися два результати. Перший результат - поява нового master-пристрою у виводі `show switch`. Другий результат - передавання події в Zabbix і формування повідомлення. Це дозволило перевірити не лише автоматичне відновлення керування стеком, а й роботу зовнішнього механізму контролю цієї зміни.

Email-повідомлення містило ім'я хоста, рівень важливості та текст останньої події, отриманий із `stack.last\_event`. Завдяки цьому адміністратор отримує не просто факт спрацювання тригера, а короткий опис події з журналу Cisco. Для подій `STACK\_REMOVED` це дозволяє швидко визначити, що проблема пов'язана саме зі зміною складу стеку, а не лише з недоступністю пристрою або інтерфейсу.

Це все підтверджує працездатність міжкомутаторного з'єднання в межах стенда. Контроль помилок показав, що на логічних Port-channel-інтерфейсах критичних помилок не зафіксовано.

Перевірка відмов і подій стеку показала, що власний механізм моніторингу дозволяє отримувати події, які не зводяться лише до стану інтерфейсу. Випадання учасника стеку, повернення учасника, зміна master-пристрою або stack-link фіксуються на рівні системного журналу Cisco, після чого передаються в Zabbix. Це дозволяє скоротити час виявлення проблеми до інтервалу опитування скрипта та часу обробки події в Zabbix.

У результаті аналізу було встановлено, що мережа працює стабільно в базовому режимі. Cisco-стеки перебувають у стані Ready, міжкомутаторні Port-channel працюють, LACP-сусідство визначається, керуючі адреси доступні, MAC-і ARP-таблиці підтверджують фактичний обмін трафіком, а Zabbix отримує дані від пристроїв і формує події за результатами роботи скрипта. Це створює основу для оцінки ефективності запропонованого рішення.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		91

Висновки до розділу 3

У третьому розділі було виконано практичну реалізацію та перевірку роботи гетерогенної комутованої мережі на лабораторному стенді. До складу стенда увійшли два стековані вузли Cisco, комутатор ZTE ZXR10 та сервер моніторингу Zabbix. Практична перевірка виконувалася на фізичному обладнанні, що дозволило отримати реальні конфігурації, діагностичні виводи, дані SNMP-моніторингу та події з журналів Cisco.

Було налаштовано стек Cisco Catalyst 2960S з іменем SW-29. За результатами діагностики стек складався з трьох комутаторів Cisco WS-C2960S-F24TS-L. Перший комутатор виконував роль Master, другий і третій працювали як Member. Усі учасники перебували у стані Ready, а stack-порти мали стан Ok. Це підтвердило коректне формування стеку та працездатність FlexStack-з'єднань.

Також було налаштовано верхній стек Cisco Catalyst 3750X з іменем SW-1-UPPER. До його складу увійшли два комутатори Cisco WS-C3750X-24P. Перший комутатор виконував роль Master, другий працював як Member, обидва пристрої перебували у стані Ready. Під час перевірки було встановлено, що один stack-порт на кожному комутаторі має стан Ok, а другий – Down.

Слід окремо зауважити, що верхній стек Cisco Catalyst 3750X сформовано з використанням одного стекового з'єднання, унаслідок чого один зі stack-портів кожного комутатора перебуває у стані Down, а стекове кільце залишається незамкненим. У такій конфігурації стек функціонує коректно як єдиний логічний вузол (обидва учасники у стані Ready, ролі Master/Member розподілені), однак внутрішнє резервування стекової шини є неповним: за стандартом StackWise Plus повне резервування й подвоєна пропускна здатність стекового кільця досягаються підключенням другого стекового кабелю між двома комутаторами, що не потребує додаткового обладнання чи третього пристрою. Для умов лабораторного стенда обрана конфігурація є прийнятною, оскільки відмовостійкість на рівні передавання даних забезпечується незалежно від стану стекового кільця – за рахунок агрегованих міжкомутаторних каналів LACP/Port-channel між стеками, роботи Spanning Tree та резервування висхідних підключень. З огляду на це, як напрям

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		92

подальшого вдосконалення інфраструктури рекомендовано замкнути стекове кільце 3750X другим кабелем StackWise, що дозволить досягти повного внутрішнього резервування стеку та усунути єдину виявлену точку зниженої стійкості.

Для керування пристроями було використано сегмент 192.168.1.0/24. Стек SW-1-UPPER мав адресу 192.168.1.2, стек SW-29 – 192.168.1.4, комутатор ZTE ZXR10 – 192.168.1.7, сервер Zabbix – 192.168.1.9. Перевірка керуючих інтерфейсів, ARP-таблиць і доступності пристроїв підтвердила, що всі основні вузли були доступні в межах спільного керуючого сегмента.

Під час налаштування міжкомутаторних з'єднань було використано Port-channel та LACP на Cisco, а також smartgroup у конфігурації ZTE [14]. На стеку SW-29 активним був Port-channel2, до якого входив інтерфейс FastEthernet3/0/1. На стеку SW-1-UPPER активними були Port-channel1 і Port-channel2. Діагностика показала стан SU для активних Port-channel, наявність LACP-сусідів і роботу логічних каналів у режимі up/up. Для ZTE ZXR10 було налаштовано smartgroup2 з фізичним інтерфейсом gei_1/1 у режимі active [20].

Перевірка Spanning Tree показала, що для VLAN 1 верхній стек SW-1-UPPER виконував роль кореневого мосту. На стеку SW-29 Port-channel2 мав роль Root і перебував у стані Forwarding. Це підтвердило узгоджену роботу логічної топології другого рівня та відсутність блокування основного шляху між стекованими вузлами Cisco.

Для контролю стану мережі було розгорнуто сервер Zabbix. До системи моніторингу були додані стек SW-1-UPPER, стек SW-29 та комутатор ZTE ZXR10. Через SNMP контролювалися доступність пристроїв, стан інтерфейсів, вхідний і вихідний трафік, а також помилки на портах. Це дозволило отримати централізоване відображення стану обладнання без постійного ручного підключення до кожного комутатора.

Окремо було реалізовано додатковий механізм моніторингу подій стеку Cisco. Стандартний SNMP-моніторинг забезпечував контроль доступності та інтерфейсів, але не давав потрібної деталізації для подій StackWise/FlexStack із

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		93

журналу Cisco. Для цього було розроблено Python-скрипт, який через SSH підключається до стеків Cisco, виконує команду show logging, аналізує повідомлення Stack Manager і передає результат у Zabbix через zabbix_sender.

Скрипт обробляв події додавання учасника стеку, випадання учасника стеку, готовності комутатора, зміни master-пристрою та зміни стану stack-link. Для кожного типу події було задано окремий шаблон пошуку та числовий рівень важливості. У Zabbix для приймання цих даних були створені trapper-items, зокрема stack.ssh.status, stack.last_event, stack.severity та окремі item для подій стеку.

Під час тестування було перевірено роботу тригерів і email-сповіщень. Після появи відповідної події в журналі Cisco скрипт передавав її в Zabbix, після чого система формувала подію та надсилала повідомлення на електронну пошту адміністратора. Інтервал опитування журналів у скрипті становив 30 секунд, тому час виявлення події обмежувався цим інтервалом та часом обробки події в Zabbix.

Аналіз роботи мережі показав, що міжкомутаторні канали працювали без критичних помилок. Port-channel2 на SW-29 і SW-1-UPPER перебував у стані up/up, лічильники помилок на логічних інтерфейсах мали нульові значення.

У результаті практичної реалізації було підтверджено працездатність запропонованої гетерогенної комутованої мережі. Cisco-стеки були сформовані та перевірені діагностичними командами, комутатор ZTE ZXR10 був інтегрований у спільний керуючий сегмент, SNMP-моніторинг у Zabbix забезпечив контроль доступності та інтерфейсів, а власний Python-скрипт доповнив систему моніторингу контролем подій стеку Cisco. Отримані результати підтвердили можливість централізованого керування, моніторингу та оперативного виявлення подій у гетерогенній мережевій інфраструктурі.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		94

ВИСНОВКИ

У кваліфікаційній роботі було розроблено проєкт гетерогенної комутованої мережі з використанням стекування Cisco та інтеграцією обладнання ZTE. Мета роботи досягнута: спроектовано структуру мережі, виконано налаштування стекованих комутаторів, підключено обладнання іншого виробника, розгорнуто моніторинг Zabbix і перевірено роботу мережі на лабораторному стенді.

У першому розділі було розглянуто технології, необхідні для побудови такої мережі: Ethernet-комутацію, VLAN, STP/RSTP, LACP, SNMP, StackWise Plus, FlexStack та засоби моніторингу. Було визначено, що стекування Cisco доцільно використовувати для об'єднання сумісних комутаторів в один логічний вузол, а взаємодію з обладнанням іншого виробника потрібно будувати на стандартних протоколах.

У другому розділі було виконано проєктування мережі. До її складу увійшли стек Cisco Catalyst 3750X, стек Cisco Catalyst 2960S, комутатор ZTE ZXR10 та сервер Zabbix. Для керування пристроями було використано сегмент 192.168.1.0/24. Було визначено адреси пристроїв, логіку підключень, роль кожного вузла та можливість подальшого розширення мережі.

У практичній частині було налаштовано стек SW-29 на базі трьох комутаторів Cisco Catalyst 2960S. Діагностичні команди підтвердили, що всі три учасники перебувають у стані Ready, перший комутатор виконує роль Master, а stack-порти мають стан Ok. Також було налаштовано стек SW-1-UPPER на базі двох комутаторів Cisco Catalyst 3750X. Обидва учасники стеку перебували у стані Ready, однак діагностика показала, що в цьому стеку активним є лише один stack-шлях.

Було налаштовано міжкомутаторні з'єднання з використанням Port-channel і LACP на Cisco та smartgroup на ZTE. Перевірка показала активний стан Port-channel, наявність LACP-сусідів і роботу логічних каналів. Для VLAN 1 верхній стек SW-1-UPPER виконував роль кореневого мосту, а стек SW-29 мав активний шлях до нього через Port-channel2.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

Для контролю мережі було розгорнуто Zabbix. Через SNMP виконувалося спостереження за доступністю пристроїв, станом інтерфейсів, трафіком і помилками. Оскільки стандартні SNMP-шаблони не давали потрібної деталізації для подій стеку Cisco, було розроблено Python-скрипт, який через SSH отримує `show logging`, визначає події Stack Manager і передає їх у Zabbix через `zabbix\_sender`.

Кількісна оцінка показала, що переобрання master-пристрою в стеку Cisco відбувається приблизно за 3 с, а виявлення подій стеку в Zabbix через Python-скрипт виконується в межах одного циклу опитування, тобто до 30 с.

Скрипт обробляв події додавання та випадання учасника стеку, готовності комутатора, зміни master-пристрою і зміни стану stack-link. Для цих подій у Zabbix були створені окремі trapper-items, тригери та email-сповіщення. Інтервал опитування журналу становив 30 секунд, тому подія могла бути виявлена протягом наступного циклу роботи скрипта.

За результатами перевірки встановлено, що запропоноване рішення є працездатним. Cisco-стеки сформовані, ZTE ZXR10 інтегрований у спільний керуючий сегмент, міжкомутаторні з'єднання працюють, Zabbix отримує дані від пристроїв, а власний скрипт дозволяє відстежувати події стеку, які не покриваються стандартним SNMP-моніторингом.

Результати кваліфікаційної роботи пройшли апробацію на 4 наукових конференціях (ІРТК-2025, м. Київ; RS-2025, м. Дрогобич; «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир; «Інформаційно-комп'ютерні технології – 2026», м. Житомир) і опубліковані у 5 тезах доповідей: «Архітектура та відмовостійкість стеків Cisco Catalyst 2960-SF: аналіз FlexStack/FlexStack-Plus»; «Аналіз архітектури протоколу LISP як засобу підвищення масштабованості та гнучкості сучасних IP-мереж»; «Мережева діагностика та самовідновлення в мультивендорних архітектурах за допомогою ZABBIX та NETDEVOPS-підходів»; «Кросплатформенні технології стекування комутаторів у мультивендорних середовищах: підходи, сценарії, перспективи віртуалізації»; «Особливості забезпечення відмовостійкості в розподілених

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		96

мережевих системах: аналіз проблеми SPLIT-BRAIN та порівняння з автономними архітектурами».

Запропоноване рішення може бути використане як основа для побудови або модернізації локальної мережі організації. Його можна розширити шляхом винесення керування в окремий VLAN, додавання резервних фізичних каналів, замикання стекового кільця на Cisco Catalyst 3750X та доповнення Zabbix новими тригерами для контролю мережевої інфраструктури.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		97

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Млинський Б.М., Дячук О.Ю. Архітектура та відмовостійкість стеків cisco catalyst 2960-sf: аналіз flexstack/flexstack-plus. Тези VIII Всеукраїнської науково-технічної конференції "Комп'ютерні технології: інновації, проблеми, рішення". м. Житомир, 02-03 грудня 2025 р. – Житомир: Житомирська політехніка, 2025. С. 187-188.
2. Млинський Б.М., Дячук О.Ю. Аналіз архітектури протоколу LISP як засобу підвищення масштабованості та гнучкості сучасних IP-мереж. Матеріали 1-ї Міжнародної науково-практичної конференції «Стійкі системи: безпечні цифрові технології та критична інфраструктура (RS-2025)». м. Дрогобич, 27 червня 2025 р. – Дрогобич: Донецький національний технічний університет, 2025. С. 131-135.
3. Дячук О.Ю., Колощук М.С., Млинський Б.М. Мережева діагностика та самовідновлення в мультивендорних архітектурах за допомогою ZABBIX та NETDEVOPS-підходів. Матеріали 1-ї Міжнародної науково-практичної конференції «Стійкі системи: безпечні цифрові технології та критична інфраструктура (RS-2025)». м. Дрогобич, 27 червня 2025 р. – Дрогобич: Донецький національний технічний університет, 2025. С. 125-130.
4. Дячук О.Ю., Колощук М.С., Млинський Б.М. Кросплатформенні технології стекування комутаторів у мультивендорних середовищах: підходи, сценарії, перспективи віртуалізації. Тези міжнародної науково-практичної конференції "Інтегровані інтелектуальні робототехнічні комплекси" (ІРТК-2025). м. Київ, 20-21 травня 2025 р. – Київ: Київський авіаційний інститут, 2025. С. 414-416.
5. Млинський Б.М., Дячук О.Ю., Колощук М.С. Особливості забезпечення відмовостійкості в розподілених мережових системах: аналіз проблеми SPLIT-BRAIN та порівняння з автономними архітектурами. Інформаційно-комп'ютерні технології – 2026: матеріали XVI Міжнародної науково-технічної конференції, м. Житомир, 2–3 квіт. 2026 р. Житомир: Державний університет «Житомирська політехніка», 2026. С. 305–307.

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				98
Змн.	Арк.	№ докум.	Підпис	Дата		

6. Bonaventure O. Computer Networking: Principles, Protocols and Practice (3rd ed.). Université catholique de Louvain, 2019. URL: <https://www.computer-networking.info/index.html> (дата звернення: 14.03.2026).
7. Byers K. Netmiko: Multi-vendor library to simplify CLI connections to network devices. GitHub Repository, 2025. URL: <https://github.com/ktbyers/netmiko> (дата звернення: 10.03.2026).
8. Case J., Fedor M., Schoffstall M., Davin J. Simple Network Management Protocol (SNMP) : RFC 1157. Internet Engineering Task Force, 1990. URL: <https://datatracker.ietf.org/doc/html/rfc1157> (дата звернення: 05.03.2026).
9. Cisco Catalyst 2960-S Switch Software Configuration Guide, Cisco IOS Release 15.2(1)E and Later. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/15-2_1_e/configuration/guide/2960_scg.html (дата звернення: 14.03.2026).
10. Cisco Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Cisco IOS Release 15.2(1)E and Later. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-2_1_e/configuration/guide/scg3750x.html (дата звернення: 14.03.2026).
11. Dordal P. L. An Introduction to Computer Networks (2nd ed.). Loyola University Chicago, 2020. URL: <https://intronetworks.cs.luc.edu/> (дата звернення: 14.03.2026).
12. Forcier J. Paramiko: A SSH2 protocol library for Python. URL: <https://www.paramiko.org/> (дата звернення: 11.03.2026).
13. Gerhards R. The Syslog Protocol : RFC 5424. Internet Engineering Task Force, 2009. URL: <https://datatracker.ietf.org/doc/html/rfc5424> (дата звернення: 07.03.2026).
14. IEEE Std 802.1AX-2020: IEEE Standard for Local and Metropolitan Area Networks – Link Aggregation (LACP). New York : IEEE, 2020. 195 p.
15. IEEE Std 802.1Q-2022: IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks. New York : IEEE, 2022. 2132 p. URL: <https://standards.ieee.org/ieee/802.1Q/10323/> (дата звернення: 14.03.2026).

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				99
Змн.	Арк.	№ докум.	Підпис	Дата		

16. Peterson L., Davie B. Computer Networks: A Systems Approach (6th ed.). Open Source Community Project, 2020. URL: <https://book.systemsapproach.org/> (дата звернення: 14.03.2026).

17. Presuhn R. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) : RFC 3416. RFC Editor, 2002. URL: <https://www.rfc-editor.org/info/rfc3416> (дата звернення: 17.06.2026).

18. Tanenbaum A. S., Wetherall D. J. Computer Networks (5th ed.). Prentice Hall, 2011. 960 p. URL: https://ia803105.us.archive.org/view_archive.php?archive=/3/items/calibre_ebook_libraries/calibre_libraries/202.203.132.245.zip&file=Computer%20Networks%20%285e%29%20-%20Andrew%20S.%20Tanenbaum%20%26%20DAVID%20J._29.pdf (дата звернення: 14.03.2026).

19. Zabbix Documentation 7.0 LTS. Zabbix Sender Utility Usage. URL: <https://www.zabbix.com/documentation/7.0/en/manual/concepts/sender> (дата звернення: 22.02.2026).

20. ZTE Corporation. ZXR10 5928 Series Command Reference (Configuration and Management). Version 5.0. Shenzhen : ZTE, 2022. 412 p. URL: <https://www.manualslib.com/products/Zte-Zxr10-5928-9807801.html> (дата звернення: 14.03.2026).

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				100
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				101
Змн.	Арк.	№ докум.	Підпис	Дата		

Конфігураційні файли пристроїв

```

SW-29#sh run
Building configuration...
Current configuration : 3761 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW-29
!
boot-start-marker
boot-end-marker
!
!
username admin privilege 15 secret 5
$1$oESI$GfYOy3v4lzQ21lKZu/bdq1
no aaa new-model
switch 1 provision ws-c2960s-f24ts-l
switch 2 provision ws-c2960s-f24ts-l
switch 3 provision ws-c2960s-f24ts-l
!
!
ip domain-name local
ip device tracking
!
!
crypto pki trustpoint TP-self-signed-3166686592
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-
3166686592
revocation-check none
rsakeypair TP-self-signed-3166686592
!
!
crypto pki certificate chain TP-self-signed-3166686592
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
!
interface Port-channel1
switchport mode trunk
!
interface Port-channel2
switchport mode access
!
interface FastEthernet0
no ip address
!
interface FastEthernet1/0/1
!
interface FastEthernet1/0/2
!
interface FastEthernet1/0/3
!
interface FastEthernet1/0/4
!
interface FastEthernet1/0/5
!
interface FastEthernet1/0/6
!
interface FastEthernet1/0/7
!
interface FastEthernet1/0/8
!
interface FastEthernet1/0/9
!
interface FastEthernet1/0/10
!
interface FastEthernet1/0/11
!
interface FastEthernet1/0/12
!
interface FastEthernet1/0/13
!
interface FastEthernet1/0/14
!
interface FastEthernet1/0/15
!
interface FastEthernet1/0/16
!
interface FastEthernet1/0/17
!
interface FastEthernet1/0/18
!
interface FastEthernet1/0/19
!
interface FastEthernet1/0/20
!
interface FastEthernet1/0/21
!
interface FastEthernet1/0/22
!
interface FastEthernet1/0/23
!
interface FastEthernet1/0/24
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
!
interface FastEthernet2/0/1
switchport mode trunk
!
interface FastEthernet2/0/2
!
interface FastEthernet2/0/3
!
interface FastEthernet2/0/4
!
interface FastEthernet2/0/5
!
interface FastEthernet2/0/6
!

```

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				102
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface FastEthernet2/0/7
!
interface FastEthernet2/0/8
!
interface FastEthernet2/0/9
!
interface FastEthernet2/0/10
!
interface FastEthernet2/0/11
!
interface FastEthernet2/0/12
!
interface FastEthernet2/0/13
!
interface FastEthernet2/0/14
!
interface FastEthernet2/0/15
!
interface FastEthernet2/0/16
!
interface FastEthernet2/0/17
!
interface FastEthernet2/0/18
!
interface FastEthernet2/0/19
!
interface FastEthernet2/0/20
!
interface FastEthernet2/0/21
!
interface FastEthernet2/0/22
!
interface FastEthernet2/0/23
!
interface FastEthernet2/0/24
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface FastEthernet3/0/1
switchport mode access
channel-group 2 mode active
!
interface FastEthernet3/0/2
!
interface FastEthernet3/0/3
!
interface FastEthernet3/0/4
!
interface FastEthernet3/0/5
!
interface FastEthernet3/0/6
!
interface FastEthernet3/0/7
!
interface FastEthernet3/0/8
!
interface FastEthernet3/0/9
!
interface FastEthernet3/0/10
!
interface FastEthernet3/0/11
!
interface FastEthernet3/0/12
!
interface FastEthernet3/0/13
!
interface FastEthernet3/0/14
!
interface FastEthernet3/0/15
!
interface FastEthernet3/0/16
!
interface FastEthernet3/0/17
!
interface FastEthernet3/0/18
!
interface FastEthernet3/0/19
!
interface FastEthernet3/0/20
!
interface FastEthernet3/0/21
!
interface FastEthernet3/0/22
!
interface FastEthernet3/0/23
!
interface FastEthernet3/0/24
!
interface GigabitEthernet3/0/1
!
interface GigabitEthernet3/0/2
!
interface Vlan1
ip address 192.168.1.4 255.255.255.0
!
ip http server
ip http secure-server
!
ip access-list standard SNMP-NMS
permit host 192.168.1.9
ip access-list standard VTY-MGMT
permit 192.168.1.0 0.0.0.255
!
snmp-server community flex RO SNMP-NMS
snmp-server location ServerRoom
snmp-server contact admin
!
line con 0
line vty 0 4
access-class VTY-MGMT in
login local
transport input ssh
line vty 5 15
access-class VTY-MGMT in
login local
transport input ssh
!
end
SW-29#

```

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				103
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-1-UPPER#show running-config
Building configuration...
Current configuration : 4962 bytes
!
! Last configuration change at 01:00:42 UTC Mon Jan 2
2006
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW-1-UPPER
!
boot-start-marker
boot-end-marker
!
!
username admin privilege 15 secret 5
$1$UnXW$wYftUnbHOWAu3VaulOkom0
no aaa new-model
switch 1 provision ws-c3750x-24p
switch 2 provision ws-c3750x-24p
system mtu routing 1500
!
ip domain-name local
!
crypto pki trustpoint TP-self-signed-1285420160
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-
1285420160
revocation-check none
rsakeypair TP-self-signed-1285420160
!
!
crypto pki certificate chain TP-self-signed-1285420160
certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609
  2A864886 F70D0101 05050003
  31312F30 2D060355 04031326 494F532D 53656C66
  2D536967 6E65642D 43657274
  69666963 6174652D 31323835 34323031 3630301E
  170D3036 30313032 30303031
  33385A17 0D323030 31303130 30303030 305A3031
  312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469
  66696361 74652D31 32383534
  32303136 3030819F 300D0609 2A864886 F70D0101
  01050003 818D0030 81890281
  8100A6C4 9A369FAC C53AFF4C 305B8794
  BDEFEE119 5A328A55 003C2F1C 404ADC91
  B4870601 A6323E73 39A718CE 32A3321C
  54BDF96B 61FFF340 3250288D 28858F72
  39A58630 0B8FE9AB B54987CE D15B3FA4
  60ED30A5 3BE76509 2AA64665 63F174A0
  2E43F4FF DF0792DD 478EBED7 08E0E7B7
  33C80504 CB2493D5 3AFB646E 67222A04
  E7C90203 010001A3 53305130 0F060355 1D130101
  FF040530 030101FF 301F0603
  551D2304 18301680 149FAE19 2791662E 6B39793A
  66F1C405 BCEF083F 2D301D06

```

```

03551D0E 04160414 9FAE1927 91662E6B 39793A66
F1C405BC EF083F2D 300D0609
  2A864886 F70D0101 05050003 81810057 76B9ECC0
  5D6F1E54 1BF6C42C 8C085ABB
  60D0E109 9DE30291 DE62D3EE 996A6714
  347AF270 48A5C21A 991254B0 82468965
  B60DCC87 F0F75AE4 D53E833B 54253B6A
  A1F5C968 CE2641EB B077B7E1 A5D6E62C
  C7349005 49E8CE3D BD68B10E BD2D1ACB
  3563E4ED 7F15DAF0 0EC988DB DB9987E7
  8AC534D0 591F7BBC E4001733 EDDF28
quit
license boot level lanbase
license boot level lanbase switch 2
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface Port-channel1
 switchport mode access
!
interface Port-channel2
 switchport mode access
!
interface FastEthernet0
 no ip address
 no ip route-cache
 shutdown
!
interface GigabitEthernet1/0/1
 switchport mode access
 channel-group 1 mode active
!
interface GigabitEthernet1/0/2
 switchport mode access
 speed 100
 duplex full
 channel-group 2 mode active
!
interface GigabitEthernet1/0/3
!
interface GigabitEthernet1/0/4
!
interface GigabitEthernet1/0/5
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!

```

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				104
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface TenGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/1/2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
!
interface GigabitEthernet2/0/4
!
interface GigabitEthernet2/0/5
!
interface GigabitEthernet2/0/6
!
interface GigabitEthernet2/0/7
!
interface GigabitEthernet2/0/8
!
interface GigabitEthernet2/0/9
!
interface GigabitEthernet2/0/10
!
interface GigabitEthernet2/0/11
!
interface GigabitEthernet2/0/12
!
interface GigabitEthernet2/0/13
!
interface GigabitEthernet2/0/14
!
interface GigabitEthernet2/0/15
!
interface GigabitEthernet2/0/16
!
interface GigabitEthernet2/0/17
!
interface GigabitEthernet2/0/18
!
interface GigabitEthernet2/0/19
!
interface GigabitEthernet2/0/20
!
interface GigabitEthernet2/0/21
!
interface GigabitEthernet2/0/22
!
interface GigabitEthernet2/0/23
!
interface GigabitEthernet2/0/24
!
interface GigabitEthernet2/1/1
!
interface GigabitEthernet2/1/2
!
interface GigabitEthernet2/1/3
!
interface GigabitEthernet2/1/4
!
interface TenGigabitEthernet2/1/1
!
interface TenGigabitEthernet2/1/2
!
interface Vlan1
ip address 192.168.1.2 255.255.255.0
no ip route-cache
!
ip http server
ip http secure-server
ip ssh version 2
!
ip access-list standard SNMP-NMS
permit host 192.168.1.9
ip access-list standard VTY-MGMT
permit 192.168.1.0 0.0.0.255
!
snmp-server community 01052005 RO SNMP-NMS
snmp-server location ServerRoom
snmp-server contact admin
!
line con 0
line vty 0 4
access-class VTY-MGMT in
exec-timeout 30 0
login local
transport input ssh
line vty 5 15
access-class VTY-MGMT in
exec-timeout 30 0
login local
transport input ssh
!
end
SW-1-UPPER#
ZXR10#

```

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		105

```

ZXR10#
ZXR10#
ZXR10#show version
ZXR10 Router Operating System Software, ZTE
Corporation
ZXR10 ROS Version V4.08.23
ZXR10_5928 Software, Version ZXR10 5900
V2.8.23.A.19.P01, RELEASE SOFTWARE
Copyright (c) 2000-2011 by ZTE Corporation
Compiled Apr 13 2011, 16:27:13
System image files are flash:<flash/img/zxr10.zar>
System uptime is 0 days, 1 hours, 23 minutes

```

```

[MPU]
Main processor: ZXR10 MPC8270, 450M - PCI with
256M bytes of memory
8K bytes of non-volatile configuration memory
16M bytes of processor board System flash (Read/Write)
ROM: System Bootstrap, Version: V1.23 , RELEASE
SOFTWARE
Hardware Version: V1.3, CPLD Version: V1.4
System serial: 4294967295

```

System temperature(Celsius):32

ZXR10#nfig

^

% Invalid input detected at '^' marker.

ZXR10#show system

```

System Description: ZXR10 ROS Version V4.08.23
ZXR10_5928 Software, Version ZXR10 5900
V2.8.23.A.19.P01
Copyright (c) 2000-2011 by ZTE Corporation
Compiled Apr 13 2011, 16:27:13
System ObjectID:

```

```

.iso.org.dod.internet.private.enterprises.zte.zxr10.zxr10-
objectID.zxr10Switch5928SysID

```

Started before: 5001 Seconds

Contact with: +86-25-52870000

System name: ZXR10

Location: No.68 Zijinghua Rd. Yuhuatai District,
Nanjing, China

This system primarily offers a set of 78 services

ZXR10#show clock

13:26:32 Fri Jun 5 2026 UTC

ZXR10#

ZXR10#

ZXR10#shi

% Unrecognized command

ZXR10#sh

ZXR10#show run

ZXR10#show vlan

VLAN Name	IsDynamic	PvidPorts
UntagPorts	TagPorts	

1	VLAN0001	NO	gei_1/1-24,
		smartgroup1	
		-2	

ZXR10#show vlan 1

^

% Invalid input detected at '^' marker.

ZXR10#

ZXR10#

ZXR10#

ZXR10#show lacp neighbors

Smartgroup 1 neighbors

Actor Port	Partner System ID	Partner Port No.	Port Priority	Oper Key	Port State

Smartgroup 2 neighbors

Actor Port	Partner System ID	Partner Port No.	Port Priority	Oper Key	Port State

gei_1/1	0x8000,a493.4c9d.f480	258	0x8000	0x1	0x3d
---------	-----------------------	-----	--------	-----	------

ZXR10#show lacp counters

Smartgroup:1

Actor Port	LACPDU Tx	Marker	LACPDU Rx	Marker

Port	Tx	Rx	Tx Rx	Err	Err

Smartgroup:2

Actor Port	LACPDU Tx	Marker	LACPDU Rx	Marker

Port	Tx	Rx	Tx Rx	Err	Err

gei_1/1	165	150	0	0	0	0
---------	-----	-----	---	---	---	---

ZXR10#show lacp sys-id

0x8000,0022.935b.a81c

ZXR10#show smartgroup

^

% Invalid input detected at '^' marker.

ZXR10#show smartgroup1

^

% Invalid input detected at '^' marker.

ZXR10#show interface gei_1/1

gei_1/1 is up, line protocol is up

Description is none

The port is electric

Duplex full

Mdi type:auto

MTU 1500 bytes BW 1000000 Kbits

Last clearing of "show interface" counters never

20 seconds input rate : 96 Bps, 0

pps

20 seconds output rate: 18 Bps, 0

pps

Interface peak rate :

input 1655 Bps, output 80 Bps

Interface utilization: input 0%, output 0%

Input:

Packets : 3682 Bytes : 650189

Unicasts : 668 Multicasts: 2998

Broadcasts : 16 Undersize : 0

Oversize : 0 CRC-ERROR : 0

Dropped : 0 Fragments : 0

Jabber : 0 MacRxErr : 0

Output:

		Млинський Б.М.		
		Дячук О.Ю.		
Змн.	Арк.	№ докум.	Підпис	Дата

ККІКБ.КР.Б – 123 – 10 – ПЗ

Арк.

106

Packets : 523 Bytes : 71860
 Unicasts : 220 Multicasts: 303
 Broadcasts : 0 Collision : 0

ZXR10#how interface brief

^
 % Invalid input detected at '^' marker.
 ZXR10#show interface statistics

^
 % Invalid input detected at '^' marker.
 ZXR10#show interface brief
 Interface portattribute mode BW(Mbits) Admin Phy
 Prot Description
 gei_1/1 electric Duplex/full 1000 up up up
 none
 gei_1/2 electric Duplex/full 1000 up down
 down none
 gei_1/3 electric Duplex/full 1000 up down
 down none
 gei_1/4 electric Duplex/full 1000 up down
 down none
 gei_1/5 electric Duplex/full 1000 up down
 down none
 gei_1/6 electric Duplex/full 1000 up down
 down none
 gei_1/7 electric Duplex/full 1000 up down
 down none
 gei_1/8 electric Duplex/full 1000 up down
 down none
 gei_1/9 electric Duplex/full 1000 up down
 down none
 gei_1/10 electric Duplex/full 1000 up down
 down none
 gei_1/11 electric Duplex/full 1000 up down
 down none
 gei_1/12 electric Duplex/full 1000 up down
 down none
 gei_1/13 electric Duplex/full 1000 up down
 down none
 gei_1/14 electric Duplex/full 1000 up down
 down none
 gei_1/15 electric Duplex/full 1000 up down
 down none
 gei_1/16 electric Duplex/full 1000 up down
 down none
 gei_1/17 electric Duplex/full 1000 up down
 down none
 gei_1/18 electric Duplex/full 1000 up down
 down none
 gei_1/19 electric Duplex/full 1000 up down
 down none
 gei_1/20 electric Duplex/full 1000 up down
 down none
 gei_1/21 electric Duplex/full 1000 up down
 down none
 gei_1/22 electric Duplex/full 1000 up down
 down none
 gei_1/23 electric Duplex/full 1000 up down
 down none
 gei_1/24 electric Duplex/full 1000 up down
 down none
 smartgroup1 up up down none
 smartgroup2 1000 up up up none

ZXR10#show spanning-tree
 % Incomplete command.
 ZXR10#show ssh server

^
 % Invalid input detected at '^' marker.
 ZXR10#show snmp-server
 ^
 % Invalid input detected at '^' marker.
 ZXR10#show users
 Line User Host(s) Idle Location
 * 0 con 0 idle 00:00:00
 ZXR10#ping 192.168.1.2
 sending 5,100-byte ICMP echoes to 192.168.1.2,timeout
 is 2 seconds.
 .!!!!
 Success rate is 80 percent(4/5),round-trip min/avg/max=
 1/2/3 ms.
 ZXR10#ping 192.168.1.4
 sending 5,100-byte ICMP echoes to 192.168.1.4,timeout
 is 2 seconds.
 .!!!!
 Success rate is 80 percent(4/5),round-trip min/avg/max=
 1/16/59 ms.
 ZXR10#
 ZXR10#
 ZXR10#
 ZXR10#
 ZXR10#
 ZXR10#
 ZXR10#
 ZXR10#
 ZXR10#show snmp
 Contact : +86-25-52870000
 Location: No.68 Zijinghua Rd. Yuhuatai District,
 Nanjing, China
 117 SNMP packets input
 0 Bad SNMP version errors
 0 Unknown community name
 0 Illegal operation for community name supplied
 0 Number of requested variables
 0 Number of altered variables
 117 Get-request PDUs
 0 Get-next PDUs
 0 Set-request PDUs
 117 SNMP packets output
 0 Too big errors (Maximum packet size 1400)
 0 No such name errors
 0 Bad values errors
 0 General errors
 117 Response PDUs
 0 SNMP trap PDUs
 ZXR10# show run
 Building configuration...
 !
 !
 vlan list 1
 !
 !
 !
 !
 !
 !
 !

```

interface vlan 1
  ip address 192.168.1.7 255.255.255.0
  out_index 27
!
interface null1
  out_index 1
!
interface smartgroup1
  out_index 28
  switchport access vlan 1
  smartgroup mode on
!
interface smartgroup2
  out_index 29
  switchport access vlan 1
  smartgroup mode 802.3ad
!
interface gei_1/1
  out_index 3
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
  smartgroup 2 mode active
!
interface gei_1/2
  out_index 4
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/3
  out_index 5
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/4
  out_index 6
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/5
  out_index 7
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/6
  out_index 8
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/7
  out_index 9
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/8
  out_index 10
  negotiation auto

```

```

switchport access vlan 1
switchport qinq normal
!
interface gei_1/9
  out_index 11
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/10
  out_index 12
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/11
  out_index 13
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/12
  out_index 14
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/13
  out_index 15
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/14
  out_index 16
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/15
  out_index 17
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/16
  out_index 18
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/17
  out_index 19
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!
interface gei_1/18
  out_index 20
  negotiation auto
  switchport access vlan 1
  switchport qinq normal
!

```

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				108
Змн.	Арк.	№ докум.	Підпис	Дата		

```
*****
**
Welcome to ZXR10 5928 Switch of ZTE
Corporation

*****
**
@
!
!
!
!
snmp-server location No.68 Zijinghua Rd. Yuhuatai
District, Nanjing, China
snmp-server contact +86-25-52870000
snmp-server packetsize 1400
snmp-server engine-id 830900020300010289d64401
snmp-server community ztemon view allview ro
snmp-server view AllView internet included
snmp-server view DefaultView system included
snmp-server enable inform SNMP
snmp-server enable inform VPN
snmp-server enable inform BGP
snmp-server enable inform OSPF
snmp-server enable inform RMON
snmp-server enable inform STALARM
snmp-server enable trap SNMP
snmp-server enable trap VPN
snmp-server enable trap BGP
snmp-server enable trap OSPF
snmp-server enable trap RMON
snmp-server enable trap STALARM
```

ККИКБ.КР.Б – 123 – 10 – ПЗ

```

!
!
!
protect
tcp synflood-protect disable
tcp synflood-protect defence 0 waittime 30 num 1
tcp synflood-protect max-connect high 90 low 60
tcp synflood-protect one-minute high 80 low 50
!
no ftp-server enable listen 21
ftp-server top-directory /flash/
!
logging on
logging buffer 200
logging mode fullcycle
logging console notifications
logging level notifications
logging timestamps datetime localtime
alarm cpuload-on
alarm cpuload-interval 30
alarm cpuload-threshold high-grade 95 middle-grade 85
low-grade 75
syslog-server facility local0
!
line console idle-timeout 120
line console absolute-timeout 1440
line telnet idle-timeout 120
line telnet absolute-timeout 1440
line telnet max-link 16

```

```

!
ssh server enable
ssh server authentication ispgroup 1
ssh server authentication mode local
ssh server authentication type chap
no ssh server only
ssh server version 1
!
!
radius auto-change off
!
!
!
!
tacacs disable
tacacs-server timeout 5
tacacs-server packet 1024
!
!
!
control-plane-security enable
!
!
end
ZXR10#

```

		Млинський Б.М.			ККІКБ.КР.Б – 123 – 10 – ПЗ	Арк.
		Дячук О.Ю.				
Змн.	Арк.	№ докум.	Підпис	Дата		110