ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження методів моніторингу мережі Cisco, включаючи системи моніторингу пропускної спроможності, утилізації ресурсів та виявлення проблем у реальному часі»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Володимир ЛИСАК
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав:
здобувач вищої освіти Володимир ЛИСАК
група КСДМ-61

Керівник: Наталія ЛАЩЕВСЬКА
науковий ступінь, вчене звання к.т.н., доцент

Рецензент: _____
науковий ступінь, вчене звання

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерної інженерії

Ступінь вищої освіти Магістр

Спеціальність Комп'ютерна інженерія

Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою КІ

_____ Наталія ЛАЩЕВСЬКА
«_____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Лисаку Володимиру Павловичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Дослідження методів моніторингу мережі Cisco, включаючи системи моніторингу пропускної спроможності, утилізації ресурсів та виявлення проблем у реальному часі

керівник кваліфікаційної роботи Наталія ЛАЩЕВСЬКА к.т.н., доцент,
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» 10.2023р. №145

2. Строк подання кваліфікаційної роботи «28» грудня 2023р.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, методи моніторингу мереж, статті про інструменти моніторингу мереж.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Дослідження методів моніторингу комп'ютерних мереж
Аналіз інструментів моніторингу мереж та можливостей застосування
Реалізація моніторингу мережі Cisco

5. Перелік графічного матеріалу: *презентація*

1. Тема дипломної роботи
2. Об'єкт, предмет, мета, новизна роботи
3. Наукова новизна та практичне значення
4. Актуальність дослідження
5. Загальний аналіз методів моніторингу мереж
6. Метрики моніторингу
7. Утилізація ресурсів
8. Інструменти моніторингу мережі
9. Реалізація системи моніторингу за допомогою емулятора мережі EVE-NG та інтеграція з системою моніторингу Paessler PRTG
10. Перегляд результатів у PRTG
11. Висновки
12. Список публікацій

6. Дата видачі завдання «19» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	19.10-05.11.23	Виконано
2	Вивчення матеріалів для аналізу методів моніторингу мережі Cisco	05.11-12.11.23	Виконано
3	Аналіз методів моніторингу пропускної спроможності, утилізації ресурсів та виявлення проблем у реальному часі	13.11-19.11.23	Виконано
4	Дослідження інструментів моніторингу мереж	20.11-25.11.23	Виконано
5	Дослідження технологій емуляції мережі	27.11-03.12.23	Виконано
6	Реалізація моніторингу мережі Cisco	04.12-10.12.23	Виконано
7	Оформлення роботи: вступ, висновки, реферат	11.12-20.12.23	Виконано
8	Розробка демонстраційних матеріалів	21.12-29.12.23	Виконано

Здобувач вищої освіти _____ Володимир ЛИСАК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Наталія ЛАЩЕВСЬКА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 82 стор., 2 табл., 12 рис., 30 джерел.

Мета роботи – дослідження сучасних методів моніторингу мережі Cisco та надання рекомендацій щодо їх успішного впровадження на практиці.

Об'єкт дослідження – вивчення методів моніторингу мережі Cisco, що охоплює перевірку систем моніторингу пропускної здатності, використання ресурсів і виявлення проблем у реальному часі в контексті мережевої інфраструктури Cisco.

Предмет дослідження – дослідження та аналіз інструментів і методів, що використовуються для моніторингу мереж Cisco, з особливою увагою на вимірюванні пропускної спроможності, управлінні використання ресурсів, а також виявлення та вирішення проблем у режимі реального часу.

Короткий зміст роботи: У роботі проведено дослідження методів та інструментів моніторингу мережі Cisco. Проаналізовано основні технології моніторингу мереж. Проаналізовано методи моніторингу пропускної спроможності, утилізації ресурсів та виявлення проблем у реальному часі.

КЛЮЧОВІ СЛОВА: МЕРЕЖІ CISCO, МОНІТОРИНГ МЕРЕЖІ, ПРОПУСКНА СПРОМОЖНІСТЬ, УТИЛІЗАЦІЯ РЕСУРСІВ, ІНСТРУМЕНТИ МОНІТОРИНГУ.

ABSTRACT

Text part of the master's qualification work: 91 pages, 19 pictures, 1 table, 37 sources.

The purpose of the work research is researching modern methods of Cisco network monitoring and providing recommendations for their successful implementation in practice..

Object of research – study of Cisco network monitoring methods, including testing of bandwidth monitoring systems, resource utilization, and real-time problem detection in the context of Cisco network infrastructure..

Subject of research – research and analysis of tools and techniques used to monitor Cisco networks, with a particular focus on measuring bandwidth, managing resource utilization, and identifying and resolving problems in real time.

Summary of the work: The work studies the methods and tools for monitoring the Cisco network. The main technologies of network monitoring are analyzed. The methods of monitoring bandwidth, resource utilization and real-time problem detection are analyzed.

KEYWORDS: CISCO NETWORKS, NETWORK MONITORING, BANDWIDTH, RESOURCE UTILIZATION, MONITORING TOOLS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Термін	Значення
CDP	Cisco Discovery Protocol
CLI	Command Line Interface
ICMP	Internet Control Message Protocol
QoS	Quality of Service
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
TAP	Test Access Point
TCA	Threshold Crossing Alert
TCP	Transmission Control Protocol
VoIP	Voice over IP

ВСТУП

Актуальність теми. У сучасному світі, інформаційні технології стають невід’ємною частиною кожного бізнесу та організації, мережева інфраструктура є основою для забезпечення ефективної та безперебійної роботи. Мережа Cisco вважається однією з найбільш широко використовуваних і ефективних систем зв'язку в багатьох галузях. Середовища мереж стають все більш складними, це вимагає розробки та впровадження ефективних методів моніторингу для забезпечення надійності, безпеки та оптимальної продуктивності.

Проведення даного дослідження є актуальним, оскільки в контексті стрімкого розвитку технологій та зростаючої важливості ефективного управління мережами, з ускладненням мереж і зростаючою важливістю їх стабільності та ефективності щодо бізнес-процесів моніторинг мережевої інфраструктури стає актуальним та необхідним для забезпечення їх стабільності та ефективності.

Використання апробованих методів моніторингу мережі Cisco дозволяє на практиці вдосконалити роботу мережі, забезпечуючи оптимальну пропускну спроможність та ефективне використання ресурсів. Моніторинг у реальному часі дозволяє виявляти та реагувати на потенційні проблеми безпеки мережі, запобігаючи можливим загрозам. Розуміння утилізації ресурсів дозволяє оптимізувати їх використання, що веде до економії коштів та забезпечення високої продуктивності. В результаті, дослідження цієї теми може значно поліпшити ефективність мережі підприємства, знизити ризики та сприяти загальному успіху організації.

Мета і завдання дослідження. Метою даного дослідження є дослідження та аналіз існуючих методів моніторингу рішень Cisco для мережі, а також розробка та впровадження оригінальних підходів, які підвищать ефективність та продуктивність управління мережею. Висвітлення цих аспектів у контексті сучасних труднощів і тенденцій у сфері мережевих технологій має вирішальне

значення для просування сучасних методів моніторингу та управління мережевими ресурсами.

В процесі дослідження вирішувались наступні завдання:

- провести аналіз існуючих рішень та підходів моніторингу мережевого обладнання Cisco;
- дослідити та проаналізувати методи моніторингу пропускної спроможності, утилізації ресурсів та виявлення проблем у реальному часі;
- проаналізувати інструменти моніторингу мережі від виробника Cisco та від сторонніх виробників;
- застосувати технології емуляції мережі для проведення лабораторних досліджень;
- реалізувати систему моніторингу мережі Cisco.

Об`єкт дослідження. Вивчення методів моніторингу мережі Cisco, що охоплює перевірку систем моніторингу пропускної здатності, використання ресурсів і виявлення проблем у реальному часі в контексті мережевої інфраструктури Cisco.

Предмет дослідження. Дослідження та аналіз методів, інструментів і методів, що використовуються для моніторингу мереж Cisco, з особливим акцентом на вимірюванні пропускної спроможності, управлінні використання ресурсів, а також виявленні та вирішенні мережевих проблем у режимі реального часу.

Методи дослідження. Аналіз літератури, структурування отриманих даних, системний підхід, оцінка досліджуваних методів моніторингу, структурний аналіз, методи порівняння.

Наукова новизна та практична значущість отриманих результатів полягає в тому, що вперше здійснено комплексне дослідження методів моніторингу пропускної спроможності, утилізації ресурсів та виявлення проблем в

реальному часі у мережах на основі обладнання Cisco. Реалізовані та впроваджені методи моніторингу, які сприяють оптимізації роботи мережі, забезпечуючи її максимальну продуктивність та надійність.

Апробація результатів та публікації. Надається в 1 статті, 1 тезисах доповіді на науково-практичній конференції.

Стаття: Лисак В.П., Катков Ю.І. РОЗРОБЛЕННЯ КЛАСИФІКАЦІЇ ІНСТРУМЕНТІВ СИСТЕМНОГО АДМІНІСТРУВАННЯ СЕРВЕРІВ // Державний університет телекомунікацій. // Зв'язок. №2, 2022 с.12-21

Тези доповідей: Лисак В.П., Лащевська Н.О ПОРІВНЯННЯ СИСТЕМ МОНІТОРИНГУ МЕРЕЖІ CISCO/ IV НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «ПРОБЛЕМИ КОМП’ЮТЕРНОЇ ІНЖЕНЕРІЇ».

1 ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ МОНІТОРИНГУ КОМПЮ’ТЕРНИХ МЕРЕЖ

1.1 Поняття про системи моніторингу мереж

Системи моніторингу мережі включають програмні та апаратні засоби, які можуть відстежувати різні аспекти мережі та її роботу, такі як трафік, використання пропускної спроможності та час безвідмовної роботи. Ці системи можуть виявляти пристрої та інші елементи, які складають мережу, і надавати оновлення стану.

Багато великих корпоративних організацій розгортають продукти та мережеві пристрої Cisco. Це включає комутатори та маршрутизатори Cisco та багато інших типів мережевих пристроїв. Компанія пропонує різноманітне мережеве обладнання, яке включає шлюзи, брандмауери та бездротові точки доступу. Незалежно від того, чи складається ваша мережа виключно з мережевих пристроїв і програм Cisco, чи з суміші продуктів постачальника, вам знадобиться система моніторингу мережі для моніторингу та керування всіма мережевими компонентами [1].

Мережеві адміністратори покладаються на системи моніторингу мережі, які допомагають їм швидко виявляти збої в роботі пристроїв або з'єднань, а також такі проблеми, як вузькі місця в трафіку, що обмежують потік даних. Здатність виявляти проблеми поширюється на частини мережі, які традиційно знаходяться за межами їх демаркаційних кордонів. Ці системи можуть сповіщати адміністраторів про проблеми електронною поштою або текстом і надавати звіти за допомогою мережевої аналітики [2].

Системи моніторингу мережі відстежують і контролюють мережеві пристрої та сервери для збору даних про за допомогою стандартних протоколів, таких як [1]:

а) Simple Network Management Protocol (SNMP) — це протокол прикладного рівня, який входить до набору Інтернет-протоколів, набору найбільш часто використовуваних протоколів зв’язку в Інтернеті. SNMP використовується для збору інформації про зміни в мережі або для оцінки стану підключених до неї пристроїв Cisco. Моніторинг SNMP полегшує проактивне виявлення всіх керованих пристроїв і програм. У разі перевищення порогових значень для певних значень програмне забезпечення може попередити системних адміністраторів про проблему, дозволяючи їм докладніше вивчати дані та шукати рішення.

б) Internet Control Message Protocol (ICMP) використовується спеціально для звітування про помилки мережевого трафіку. Мережеві пристрої покладаються на ICMP для передачі повідомлень про помилки, наприклад, у випадку, коли неможливо отримати доступ до хоста чи клієнта, або якщо запитувана інформація недоступна. На відміну від SNMP, ICMP не використовується в ситуаціях, коли інформація передається між різними системами. Натомість він часто використовується мережевими експертами та адміністраторами для усунення несправностей підключення до Інтернету за допомогою діагностичних засобів, таких як traceroute або ping. Серед типових повідомлень про помилки ICMP: "Перевищено час", "Адресат недосяжний", "Завеликий пакет", "Проблема з параметрами".

в) Cisco Discovery Protocol (CDP) працює на канальному рівні на всіх маршрутизаторах, мостах, серверах доступу та комутаторах Cisco. CDP дозволяє застосункам керування мережею виявляти пристрої Cisco, які є сусідами існуючих пристроїв, що працюють за

протоколами нижчого рівня. CDP дозволяє додаткам керування мережею дізнаватися типи пристроїв і адреси агентів SNMP інших сусідніх пристроїв і надсилати запити до цих пристроїв.

Схема роботи протоколу CDP зображена на рисунку 1.1

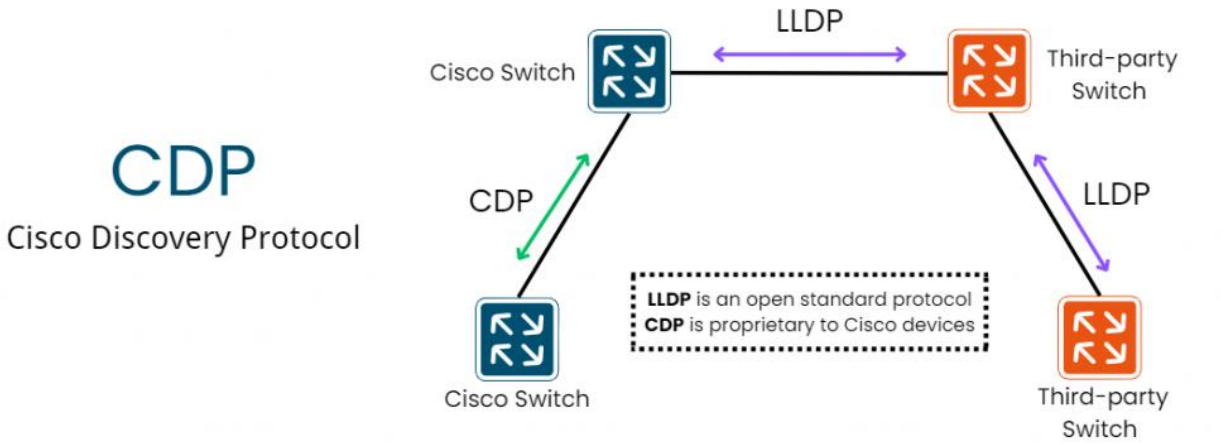


Рисунок 1.1 – Схема роботи протоколу CDP

Системи моніторингу мереж призначені для забезпечення безперебійної роботи та продуктивності мережі. Вони збирають та аналізують дані про стан мережі, щоб виявляти та попереджати про потенційні проблеми.

Основні цілі систем моніторингу мереж:

- Забезпечення безперебійної роботи мережі. Системи моніторингу мереж можуть виявляти та попереджати про потенційні проблеми, такі як збої обладнання, перевантаження мережі та атаки. Це допомагає запобігти збоям у мережі та підтримує роботу мережі.
- Підвищення ефективності роботи мережі. Системи моніторингу мережі можна використовувати для спостереження за використанням мережі та визначення регіонів, де продуктивність мережі можна покращити. Це може включати оптимізацію маршрутизації, балансування навантаження та ефективне використання ресурсів.
- Забезпечення безпеки мережі. Системи моніторингу мереж можуть використовуватися для моніторингу безпеки мережі та виявлення

потенційних загроз. Це може включати виявлення вторгнення, аналіз безпеки та моніторинг журналів.

Конкретні цілі систем моніторингу мережі можуть відрізнятися залежно від потреб організації. Наприклад, організація, яка використовує мережу для передачі важливої фінансової інформації, може зосередитися на цілях безпеки. Організація, яка використовує мережу для передачі відеоконтенту, може зосередитися на досягненні цілей, пов’язаних із продуктивністю.

Системи моніторингу мережі є корисними для організацій будь-якого розміру. Вони можуть допомогти організаціям зберегти продуктивність мережі, забезпечити її безперебійну роботу та захистити від потенційних загроз.

Системи моніторингу мають ряд проблем, які можуть перешкоджати їх ефективному функціонуванню. Основні проблеми систем моніторингу:

- Визначення правильних метрик для моніторингу. Не всі метрики важливі для всіх систем. Дуже важливо вибрати показники, які найбільше відповідають конкретній системі та її передбачуваним цілям.
- Збір та обробка даних. Системи моніторингу можуть генерувати великі обсяги даних. Дуже важливо переконатися, що дані збираються та обробляються ефективним чином, це дозволить виявити проблеми.
- Аналіз даних. Дані, зібрані в процесі моніторингу, необхідно вивчати, щоб розпізнати потенційні проблеми. Це може бути складним завданням, особливо для великих обсягів даних.
- Повідомлення про проблеми. Системи моніторингу повинні мати можливість якнайшвидше виявляти потенційні проблеми, що дозволить вжити коригувальні дії.
- Розв'язання проблем. Коли системи моніторингу виявляють потенційні проблеми, необхідно вирішити їх. Це може бути складним завданням, особливо для складних систем.

Інші проблеми, які можуть бути специфічними для систем моніторингу, включають проблеми, пов’язані з конкретним типом системи, яка контролюється. Наприклад, системам моніторингу мережі може бути важко розпізнавати атаки, а системам моніторингу безпеки може бути важко розпізнавати вторгнення.

Для вирішення питань систем моніторингу необхідно вжити ефективних заходів. Ці заходи можуть включати:

- Розробка плану моніторингу. План моніторингу повинен визначати, які метрики необхідно збирати, як їх збирати та як аналізувати.
- Використання спеціальних інструментів для моніторингу. Спеціалізовані інструменти можуть полегшити збір, обробку та аналіз даних.
- Розробка процедур для вирішення проблем. Процедурам вирішення проблем слід визначати, хто відповідальний за вирішення проблем, і які кроки необхідно вжити.

Впровадження відповідних заходів може допомогти в підвищенні ефективності систем моніторингу та зменшенні ризиків, пов'язаних з їх використанням.

1.2 Методи моніторингу мереж

Щоденна робота мережі складається з потоку трафіку, використання пропускної здатності та доступу до ресурсів. Ці показники визначають нормальну поведінку мережі [3].

Щоб визначити типову поведінку мережі, важливо реалізувати моніторинг мережі. Для спостереження за мережею використовуються такі інструменти, як IDS, аналізатори пакетів, SNMP, NetFlow та інші.

Існує два поширених методи, які використовуються для захоплення трафіку та надсилання його на пристрої моніторингу мережі [3]:

а) Мережеві TAP, іноді відомі як Test Access Point.

б) Віддзеркалення трафіку за допомогою Switch Port Analyzer (SPAN) або іншого віддзеркалення портів.

Мережевий розгалужувач — це пасивний роздільний пристрій, вбудований між пристроєм, який вас цікавить, і мережею. TAP пересилає весь трафік, у тому числі помилки фізичного рівня, на аналізуючий пристій, дозволяючи трафіку досягти пункту призначення.

На рисунку 1.2 TAP одночасно надсилає дані передачі (TX) із внутрішнього маршрутизатора та дані прийому (RX) на внутрішній маршрутизатор по окремих виділених каналах.

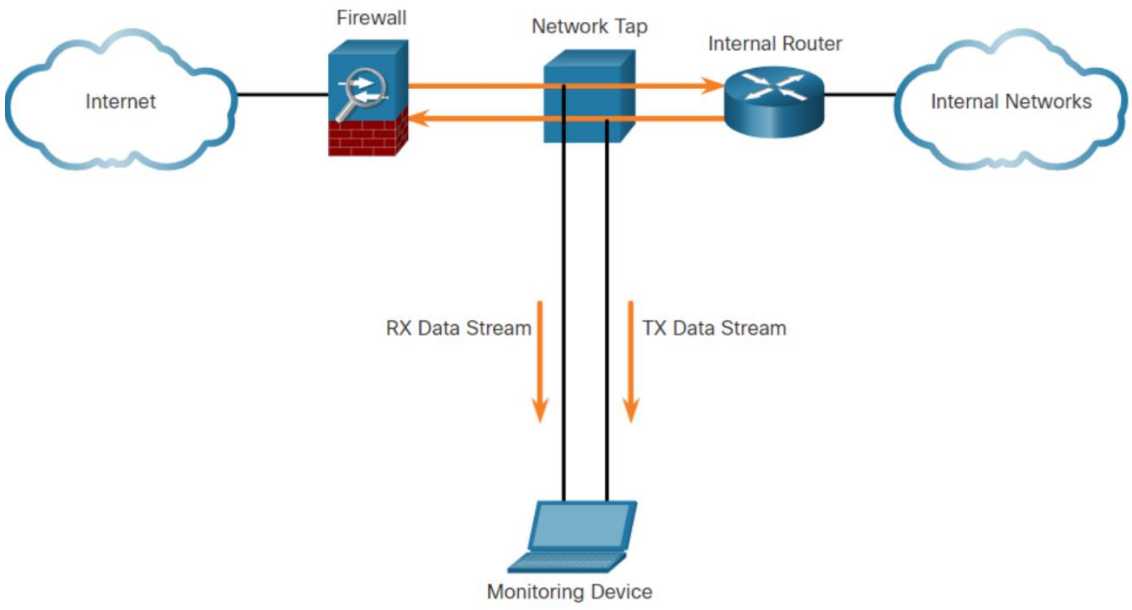


Рисунок 1.2 – Застосування TAP в простій мережі

Це гарантує, що всі дані надходять на пристрій моніторингу в режимі реального часу. TAP є відмовостійким, що означає, що трафік між брандмауером і внутрішнім маршрутизатором не пошкоджений [3].

Резюмуючи, проаналізовану інформацію можна відмітити наступні характеристики TAP:

- TAP створюють повну 100% копію двонаправленого мережевого трафіку, забезпечуючи максимальну точність моніторингу мережі.
- TAP не змінюють часові співвідношення між кадрами, інтервалом та часом відгуку, що особливо важливо при аналізі VoIP та Triple Play, включаючи аналіз FDX.
- TAP не вносять додаткового джиттера чи фальсифікації, що важливо під час аналізу VoIP/відео.
- TAP пропускають весь трафік: IPv4 або IPv6, пакети з помилками, короткі або великі кадри, неправильні кадри CRC, міжкадровий інтервал не відкидається та не змінюється, будь-які пакети не відкидаються незалежно від смуги пропускання.
- TAP відмовостійкі.
- TAP не є адресними мережевими пристроями, тому не можуть бути зламані.
- TAP не потрібно налаштовувати та оновлювати, отримання всіх даних гарантовано та заощаджує час персоналу.

Збір даних для моніторингу мережі вимагає, щоб увесь трафік був захоплений. Для обходу сегментації мережі, що накладається мережевими комутаторами, слід застосовувати спеціальні методи, наприклад віддзеркалення портів. Віддзеркалення портів дає змогу комутатору копіювати кадри, отримані на одному або кількох портах, до порту аналізатора портів комутатора (SPAN), підключеного до пристрою аналізу.

Зв’язок між портами джерела та портом призначення називається сеансом SPAN. Під час одного сеансу можна контролювати один або декілька портів. У кількох комутаторах Cisco сеансовий трафік можна скопіювати на декілька портів призначення. Можна вказати вихідний VLAN, у який усі порти вихідного VLAN стануть джерелами трафіку SPAN. Також існує варіант SPAN

під назвою Remote SPAN (RSPAN) дозволяє адміністратору мережі використовувати гнучкість VLAN для моніторингу трафіку на віддалених комутаторах [3].

Підсумовуючи, проаналізовану інформацію можна відмітити наступні характеристики SPAN:

- При використанні SPAN створюються пакети даних, що дублюються, що знижує ефективність інструментів моніторингу.
- SPAN може легко перепідписатися, відкидаючи пакети, також спостерігаються втрати пакетів у разі перевантаження портів або помилок. В результаті «некоректної роботи» мережевий фахівець упускає з поля зору користувача трафіку, що не дозволяє виявити серйозні помилки в роботі мережі. Крім того, фахівці з інформаційної безпеки можуть пропустити вірусний трафік або атаки зловмисників.
- Дані 1 рівня, пошкоджені та некоректні пакети, неправильний CRC, міжкадровий інтервал та інші нестандартні дані не пересилаються на SPAN-порти. Отже, SPAN не підходить для моніторингу, захоплення та аналізу протоколу реального часу (RTP), особливо в сучасних стратегіях оцінки середнього значення якості голосу або відео та якості сприйняття в цілому (QoE).
- Теги VLAN не завжди надсилаються через порт SPAN, і це залежить від налаштувань. Тому це може призвести до виявлення помилкових проблем та утруднення пошуку проблем VLAN.
- SPAN-порти надають лише узагальнені дані.
- SPAN-порти змінюють тимчасові мітки пакетів.
- Доведено, що SPAN-порти можна зламати, тому вони можуть становити загрозу безпеці.
- SPAN-порт має найнижчий пріоритет на комутаторі, коли справа доходить до вибору між основним трафіком та трафіком SPAN.

- SPAN-порти вимагають програмування через інтерфейс командного рядка і можуть бути неправильно налаштовані, що призводить до утворення сліпих зон для моніторингу та збоїв.
- У деяких країнах SPAN не відповідає вимогам закону для випадків законного перехоплення.
- Кількість SPAN-портів у комутаторі обмежена порівняно з кількістю, необхідною для моніторингу. Різним фахівцям потрібні копії трафіку для вирішення таких завдань, як безпека , фільтрація вмісту, виявлення вторгнень, діагностика та усунення несправностей.

Як мережеві TAP, так і SPAN мають свої переваги та недоліки, коли справа доходить до захоплення мережевого трафіку. Сучасні високошвидкісні мережі мають TAP як рекомендований варіант через відсутність втрати або затримки пакетів. Коли швидкість і надійність мають суттєве значення, TAP є найбільш прийнятним варіантом. Однак вони можуть бути дорожчими та менш масштабованими, ніж SPAN. Як наслідок, TAP може бути неефективним у певних випадках.

SPAN — це економічне та масштабоване рішення, яке підходить для нерегулярного та швидкого усунення несправностей у зв’язках, що не використовуються. Така простота конфігурації та відсутність початкових витрат робить віддзеркалення портів привабливою пропозицією для організацій, які роблять перші кроки до моніторингу мережі [4].

1.3 Метрики моніторингу

Моніторинг мереж та IT-інфраструктури став першочерговим у зв’язку з цифровою трансформацією, яка відбувається в діловому світі. Моніторинг мережі передбачає як якісні, так і кількісні засоби спостереження та визначення

поведінки мережі та може надавати інформацію в реальному часі про збої та помилки, а також потенційні проблеми у вашій мережі. Крім того, моніторинг продуктивності мережі може допомогти вам зрозуміти заплановані майбутні робочі процеси шляхом розпізнавання вимог кінцевого користувача. Щоб максимально використати переваги цих функцій, вам знадобиться розширений інструмент моніторингу мережі та інфраструктури.

Моніторинг мережі дозволяє приймати рішення на основі отриманих даних. Ці дані дозволяють побудувати бізнес-модель, яка обіцяє високу ефективність інвестицій в інфраструктуру, продуктивність мережі та параметри попиту користувачів. Побудова відповідної структури вимагає моніторингу основних показників мережі, які допоможуть вам точно визначити продуктивність мережі.

Відстеження правильних метрик прокладає шлях до більш ефективних результатів щодо продуктивності мережі та IT-інфраструктури. Це полегшує вашій організації приймати правильні інвестиційні рішення в довгостроковій перспективі, а командам у різних відділах краще розуміти потреби та очікування користувачів. З іншого боку, необхідно підкреслити, чому важливо відстежувати основні мережеві показники перед впровадженням усіх цих функцій у вашій організації [5].

Показники продуктивності мережі допомагають розрізняти проблеми з додатками та проблеми з передачею даних, щоб легше вирішувати потенційні проблеми. Цей підхід включає два основні показники, відомі як час зворотного зв’язку та час відповіді сервера, які обчислюються на основі пасивного спостереження за мережевим трафіком [6]:

а) Час передачі даних: час передачі, який потрібен пакету даних, щоб досягти місця призначення, і час, потрібний для підтвердження отримання пакета. Щоб обчислити час передачі даних, необхідно встановити TCP-сеанс.

б) Час відповіді сервера: час відповіді сервера – це кількість часу, необхідного для обробки запиту та відповіді на нього.

Моніторинг метрик продуктивності мережі пропонує кілька переваг, які можуть допомогти покращити всю продуктивність мережі, наприклад [6]:

а) Забезпечує повну видимість мережі: необхідно відстежувати кожен біт мережевого трафіку та підключених до нього пристроїв. Інструменти моніторингу мережі можуть забезпечити повні можливості моніторингу та звітності з ключовими показниками продуктивності, які забезпечують повну видимість вашої мережі та допомагають забезпечити безперебійне надання послуг кінцевим користувачам.

б) Запобігає простою мережі: показники продуктивності мережі допомагають передбачити та запобігти простою мережі, визначаючи потенційні та несподівані помилки та збої.

в) Використовуючи рішення для моніторингу мережі, ви можете відстежувати мережевий трафік і пов’язані з ним пристрої. Це допомагає миттєво виправляти помилки та максимально підвищити доступність послуг.

г) Спостерігайте за використанням пропускної здатності: використання пропускної здатності є одним із найважливіших показників продуктивності. Це допоможе визначити, яку пропускну здатність використовує мережа. Крім того, рішення для моніторингу сповіщають, коли ці показники досягають критичних рівнів, щоб вчасно вжити заходів.

Під час огляду мережі вкрай важливо враховувати кілька ключових показників, щоб забезпечити її ефективність і безпеку. Ось декілька основних:

- Максимальна пропускна здатність: максимальна швидкість передачі даних за певний період часу. Щоб максимізувати ефективність мережі, найефективнішим способом зробити це є максимізація

використовуваної пропускної здатності без перевищення порогових значень. Інструменти продуктивності мережі полегшують моніторинг смуги пропускання, яку використовує мережа. Ці інструменти також можуть повідомляти адміністраторів в режимі реального часу, надсилаючи сповіщення про перевищення пропускної здатності.

- Втрата пакетів: кількість пакетів даних, втрачених під час передачі від одного пункту призначення до іншого. Це впливає на послуги кінцевих користувачів, оскільки запити на дані не можуть бути виконані в певний час. Втрата пакетів можлива через кілька причин, зокрема проблеми з програмним забезпеченням, перевантаження мережі або низьку продуктивність маршрутизатора. Протокол керування передачею (TCP) може знаходити втрачені пакети даних і гарантувати, що вони досягнуть місця призначення. Важливо уважно стежити за всією процедурою.
- Повторна передача: втрачені або скинуті пакети даних мають бути передані повторно, щоб завершити запит даних. Повторні передачі допомагають визначити перевантаження мережі, вимірюючи швидкість втрати пакетів даних..
- Пропускна здатність: процес вимірювання пропускної здатності, який обчислює фактичну швидкість передачі даних у різних областях мережі. У той час як пропускна здатність використовується для визначення теоретичного обмеження для передачі даних, пропускна здатність використовується для визначення фактичної кількості пакетів даних, які успішно передано до місця призначення через мережу. Пропускна здатність може відрізнятися залежно від зони мережі. Низька пропускна здатність вказує на те, що скинуті пакети потрібно повторно передати.
- Затримка: затримка мережі вимірюється в мілісекундах, а затримка мережі є середнім із цих значень. Декілька факторів, включаючи чергування пакетів у комутованих мережах і показник заломлення

оптоволоконного кабелю, відповідають за збільшення затримки мережі. Постійна буферизація або аномальне збільшення затримки свідчить про значну проблему з продуктивністю мережі.

- Доступність мережі: доступність мережі є одним із найважливіших показників для визначення ступеня безвідмовної роботи мережі протягом тривалого періоду часу. Час безвідмовної роботи – це загальна кількість часу, протягом якого ваша мережа використовується. Наявність мережі життєво важлива для забезпечення постійного надання послуг споживачам.
- З'єднання: дуже важливо перевірити зв'язок між пристроями та станціями у мережі. Якщо пристрій несправний або мережа не може з'єднатися з пристроєм, різні служби можуть не працювати через простої або низьку продуктивність. Проблеми з підключенням зазвичай виникають через зловмисне програмне забезпечення, націлене на певні вузли, щоб вплинути на продуктивність певної області мережі.
- Джитер: джитер можна визначити як часову затримку або різницю в часі між надсиланням кожного пакета даних через мережу. Це порушення нормальної послідовності пакетів даних і може виникнути через перевантаження мережі або зміни маршруту.
- Утилізація ресурсів: утилізація ресурсів або використання ресурсів в мережі вказує на те, наскільки ефективно обладнання та інфраструктура використовуються для передачі та обробки даних. Ось деякі ключові аспекти використання ресурсів:
- Використання пропускної здатності: вимірює обсяг передачі даних через мережу відносно її максимальної пропускної здатності. Високе використання може призвести до затримок та втрати пакетів.
- Використання процесора: показник, що вказує на те, як ефективно обладнання обробляє дані. Високе використання процесора може призвести до зниження продуктивності та затримок у обробці.

- Використання пам'яті: вказує на те, наскільки інтенсивно використовується доступна пам'ять. Перевищення обсягу пам'яті може викликати сильні затримки та навіть витоки.
- Використання мережевих інтерфейсів: вимірює обсяг трафіку, що проходить через мережеві інтерфейси. Це важливо для визначення насиченості мережі та виявлення можливих точок перевантаження.

Наприкінці, важливо зазначити значення виявлення проблем у реальному часі. Це включає в себе вчасне сповіщення про відмови, затримки або інші аномалії, які можуть виникнути в мережі. Моніторинг, який підтримує систему оперативної інформації про стан мережі, дозволяє миттєво реагувати на наявність проблем і усувати їх, що мінімізує збитки для користувачів. Це може мати важливе значення для функціонування бізнес-процесів і підтримки високої доступності. Використання систем моніторингу в реальному часі дозволяє негайно реагувати на проблеми та навіть запобігати їм завдяки використанню аналізу тенденцій і попереджувальних сигналів.

Моніторинг ключових показників мережі є критично важливим елементом для забезпечення ефективності, безпеки та стабільності сучасних інформаційних систем. Інструменти моніторингу дозволяють оперативно реагувати на проблеми та забезпечують надійність функціонування мереж.

2 ДОСЛІДЖЕННЯ ІНСТРУМЕНТІВ МОНІТОРИНГУ МЕРЕЖІ

2.1 Аналіз інструментів моніторингу мережі від Cisco

2.1.1 Cisco Network Assistant

Компанія Cisco, ймовірно, є найвідомішим, надійним і довіреним постачальником у всьому світі мережевих систем і технологій. Але незалежно від того, обладнання якого постачальника використовується або скільки кінцевих точок у вас є, інструменти моніторингу мережі та усунення несправностей забезпечують підтримку вашого середовища і дуже важливо, щоб вони були [7].

Більшість мереж великих підприємств у тій чи іншій формі використовують продукти Cisco у своїй IT-інфраструктурі, якщо не в усьому обладнанні. Гігант уніфікованих комунікацій вважається надійним і стабільним і має широкий асортимент продукції [8].

Деяке обладнання, як маршрутизатори, комутатори або брандмауери Cisco, мають в комплекті поставки Cisco Network Assistant (CNA). CNA — це застосунок, розроблений для ПК з ОС Windows для керування мережами. Він розроблений для сумісності з дротовими та бездротовими мережами та малими і середніми організаціями. Cisco Network Assistant має внутрішній зручний інтерфейс, який забезпечує централізоване відображення мережі [9].

Ця реалізація робить конфігурацію, керування та усунення несправностей простим повсякденним завданням для адміністраторів мережі. Вони також мають можливість маніпулювати загальними службами, створювати звіти про інвентаризацію та синхронізувати паролі на маршрутизаторах, комутаторах, контролерах локальної мережі та точках доступу Cisco.

Основні технічні характеристики Cisco Network Assistant [9]:

а) Конфігурація мережі. Ключовою розширеною перевагою використання Cisco Network Assistant є можливість, яку він надає мережевим адміністраторам, налаштовувати та підтримувати максимум 80 маршрутизаторів, комутаторів, бездротових контролерів і точок доступу одночасно. Кількома кліками миші користувач може запустити внутрішній диспетчер пристроїв або розпочати сеанс Telnet за допомогою інтуїтивно зрозумілого графічного інтерфейсу.

б) Управління мережею: ще однією дуже важливою перевагою Cisco Network Assistant є можливість спростити поточне керування мережею. Точніше кажучи, це дозволяє мережевим адміністраторам створювати звіти про інвентаризацію та скидати паролі. Нарешті, чудовим варіантом є вбудоване оновлення програмного забезпечення Cisco IOS за допомогою процесу перетягування.

в) Усунення несправностей мережі: Cisco Network Assistant пропонує перегляд топології пов’язаної мережі, де проблеми підсвічені. Цей прийом допомагає усунення несправностей з боку адміністраторів, щоб легко вчасно виявити причину проблем з мережею. Іншою передовою технологічною функцією є графічне представлення на графіках тенденцій. Ці діаграми представляють автоматично виявлені проблеми мережі, такі як несправності кабелю та помилки конфігурації.

г) Оптимізація мережі. Однією з найкращих функцій, які Cisco Network Assistant надає користувачеві, є здатність зменшувати ризики мережі. Ця послуга здійснюється шляхом перегляду конфігурації мережі. Потім програмне забезпечення рекомендує зміни щодо якості послуг (QoS), впровадження безпеки та доступності мережі відповідно до найкращих галузевих практик.

д) Підтримка пристроїв і кількох мов. Нарешті, Cisco розробила Network Assistant із багатьма цінними функціями, такими як підтримка кількох мов і пристроїв. Окрім англійської, GUI реалізований німецькою,

французькою, іспанською, італійською, китайською та японською мовами. Крім того, Cisco зберігає оновлений список програмного забезпечення для комутаторів Catalyst, контролерів локальної мережі, маршрутизаторів ISR і точок доступу, які можна знайти на офіційному сайті Cisco.

Найпоширенішим використанням CNA є налаштування пристроїв. Багато людей відчувають себе зручніше, використовуючи графічний інтерфейс користувача для налаштування своїх пристроїв Cisco порівняно з використанням CLI. Щоб налаштувати пристрої, натисніть «Налаштувати» на панелі функцій. Це екран, на якому показано різні способи налаштування пристроїв. Ви побачите Smartports як перший вибір у списку завдань, які ви можете виконати. Розумні порти — це попередньо створені конфігурації для певних типів портів. Наприклад, якщо комутатор пов’язано з маршрутизатором, іншим комутатором, ПК або телефоном VoIP, для цих пристроїв уже є попередньо встановлені конфігурації. Кожна категорія складається з кількох конфігурацій. У деяких категоріях є майстри, наприклад Майстер безпеки та Майстер AVVID. Ви можете налаштувати більшість будь-яких параметрів комутатора за допомогою CNA Configure Tools [10].

Також Cisco Network Assistant використовується для моніторингу мережі. Усередині вкладки моніторинг є можливість створювати звіти про інвентаризацію свого пристрою, статистику портів на кожному пристрої, графіки посилань, інформацію про якість обслуговування, сповіщення про події та системні повідомлення. Найбільш інформативними в категорії Monitor є Bandwidth Graphs і Link Graphs. За допомогою цього інструменту можна контролювати пропускну здатність кожного порту вашого комутатора або маршрутизатора.

За допомогою категорії Troubleshoot (Усунення несправностей) можна виконати графічний ping і traceroute. Існують варіанти виконання трасування

рівня 2-го і 3-го рівня. Унікальною функцією є можливість відстеження рівня 2 (MAC-адреса Ethernet) [10].

У категорії обслуговування є багато потужних інструментів. Існує можливість створення резервної копії конфігурації, оновлення програмного забезпечення IOS, перезавантаження пристрою або підключення Telnet до консолі. Найвигіднішими аспектами Cisco Network Assistant є його здатність копіювати конфігурацію та оновлювати програмне забезпечення IOS [10].

Cisco Network Assistant (CNA) був корисним інструментом для адміністрування та моніторингу мережі, особливо щодо апаратного забезпечення Cisco. Його графічний інтерфейс робив його доступним для користувачів з різним рівнем досвіду, спрощуючи конфігурацію та відслідковування стану мережевих пристроїв. Однак недоліки CNA, такі як обмеженість функціоналу та припинена підтримка, визначають його як застарілий інструмент. Застарілість може створити проблеми у використанні новітнього обладнання та можливостей, що доступні в більш сучасних рішеннях.

Висновок полягає в тому, що, розглядаючи швидко змінюючись світ мережевих технологій, користувачам слід розглядати альтернативи, які надають актуальні функціональні можливості та підтримку для нових технологій.

2.1.2 Cisco Prime Infrastructure

Cisco Prime Infrastructure — це комплексне рішення для повного керування життєвим циклом дротового та бездротового зв’язку. За допомогою Cisco Prime Infrastructure ви можете здійснювати конвергентне управління для полегшення моніторингу, усунення несправностей і створення звітів. Ви можете отримати покращене керування конфігурацією, змінами та відповідністю для нижчої сукупної вартості володіння. Cisco Prime for Enterprise — це інноваційна стратегія та портфоліо продуктів управління, які

дають IT-відділам змогу ефективніше керувати своїми мережами та послугами, які вони надають. Cisco Prime спрощує керування мережею, покращує ефективність операцій, зменшує кількість помилок і робить надання мережевих послуг більш передбачуваним [11].

Cisco Prime Infrastructure спрощує й автоматизує багато повсякденних завдань, пов'язаних із підтримкою та керуванням наскрізною мережевою інфраструктурою. Нове конвергентне рішення надає всі існуючі бездротові можливості для керування радіочастотами, видимості доступу користувачів, звітування та усунення несправностей разом із функціями життєвого циклу мережевої інфраструктури, такими як виявлення, інвентаризація, конфігурація та керування образами, звітування про відповідність, інтегровані передові методи та звітування [12].

Нова модель операційного робочого процесу, заснована на процесах життєвого циклу, узгоджує функціональність продукту з тим, як оператори мережі виконують свою роботу [12]:

а) Проектування – оцінка, планування та створення конфігурацій, необхідних для розгортання нових мережевих послуг і технологій. Створення шаблонів, які використовуються для моніторингу ключових мережевих ресурсів, пристроїв і атрибутів. Шаблони за замовчуванням і найкращі практичні розробки надаються для швидкого готового впровадження, автоматизації роботи, необхідної для використання перевірених Cisco дизайнів і найкращих практик.

б) Розгортання – планування розгортання та впровадження мережевих змін. Це може включати розгортання нових шаблонів конфігурації або моніторингу, створених на етапі проектування, оновлення образів програмного забезпечення та підтримку ініційованих користувачем спеціальних змін і оновлень відповідності. Це прискорює розгортання служби, мінімізує ймовірність помилок і має високу масштабованість. Крім того, інфраструктура Cisco Prime Infrastructure забезпечує

простий набір керованих і розширених потоків для масового надання нових пристроїв, включаючи конвергентні комутатори доступу в мережі, і початкової конфігурації, щоб привести пристрій у робочий стан протягом кількох хвилин, таким чином скорочуючи IT витрати.

в) Експлуатація – попередньо встановлені інформаційні панелі забезпечують оновлений моніторинг загального стану мережі. Прості робочі процеси одним клацанням миші та 360-градусний огляд покращують усунення несправностей і скорочують час вирішення проблем з мережею. Уніфікований дисплей тривоги надає корисну інформацію та можливість автоматично відкривати запити на обслуговування в Центрі технічної підтримки Cisco.

г) Звітність – надає широкий спектр попередньо визначених звітів для актуальної інформації про мережу, включаючи детальну інвентаризацію, відповідність, аудит, ємність, кінець продажу, вразливі місця в безпеці та багато іншого.

Політики моніторингу контролюють, як Prime Infrastructure стежить за вашою мережею, керуючи: атрибутами мережі та пристроїв, які моніторить Prime Infrastructure, швидкістю оновлення параметрів моніторингу, прийнятними значеннями для запитуваних атрибутів, виявленням проблем у реальному часі та сигналами тривоги, якщо порогові значення показників перевищенні [13].

Політики моніторингу важливі, оскільки окрім контролю за тим, що відстежується, вони визначають, які дані можна відображати у звітах, на інформаційних панелях та в інших областях Prime Infrastructure. Політики моніторингу не вносять жодних змін на пристрої. За замовчуванням, увімкнено лише моніторинг стану пристрою (тобто політику моніторингу стану пристрою). Моніторинг справності інтерфейсу не ввімкнено за замовчуванням, щоб захистити продуктивність системи у великих розгортаннях.

У цих кроках коротко описано, як можна налаштувати політику моніторингу [13]:

а) Використовуйте тип політики моніторингу як шаблон для своєї політики моніторингу та дайте політиці відповідне ім’я. Типи політик включені в пакет Prime Infrastructure і дозволяють легко розпочати моніторинг різних технологій і послуг.

б) Налаштуйте частоту опитування своєї політики або взагалі вимкніть опитування для певних параметрів.

в) Укажіть сигнали тривоги про перевищення порогу (TCA), які має генерувати Prime Infrastructure у разі перевищення порогового значення параметра. Деякі TCA налаштовані за замовчуванням; ви можете налаштувати або вимкнути їх, а також налаштувати нові TCA.

г) Укажіть пристрої, які ваша політика має контролювати. Пристрої фільтруються залежно від типу політики.

д) Активуйте свою політику. Дані опитування відображаються на інформаційних панелях, у звітах, таблиці «Сигнали та події» та в інших областях веб-інтерфейсу користувача.

У таблиці 2.1 представлені параметри, які Cisco Prime Infrastructure може моніторити автоматично.

Показники	Опитувані пристрої	Інформаційна база управління	Включені об’єкти ІБУ
Доступність пристроїв	Всі SNMP пристрої, пристрої сторонніх розробників	SNMPv2-MIB	sysUpTime

Використання ЦП	Пристрої Cisco IOS, усі підтримувані пристрої Nexus, пристрої Cisco UCS	CISCO-PROCESS-MIB	cpmCPUTotalPhysicalIndex cpmCPUTotal1minRev
	Пристрої Cisco ASR	CISCO-ENTITY-QFP-MIB	
Використання пулу пам'яті	Пристрої Cisco IOS, пристрої ISR	CISCO-MEMORY-POOL-MIB	ciscoMemoryPoolName ciscoMemoryPoolType ciscoMemoryPoolUsed ciscoMemoryPoolFree
	Усі підтримувані пристрої Cisco Nexus, пристрої Cisco UCS, пристрої Cisco IOS XE	CISCO-PROCESS-MIB	cpmCPUTotalIndexcpmCPUMemoryUsedcpmCPUMemoryFree
	Пристрої Cisco ASA, пристрої	CISCO-ENHANCED-	cempMemPoolTypecempMemPoolNamece

	IOS XR та Edison	MEMPOOL-MIB	mpMemPoolUsedcempMemPoolFree
	Пристрої Cisco IOS ASR	CISCO-ENTITY-QFP-MIB	ceqfpMemoryResTypeceqfpMemoryResInUseceqfpMemoryResFree
Температура середовища	ASR, усі підтримувані пристрої Nexus, пристрої Cisco UCS	CISCO-ENVMON-MIB	entSensorValue
	Catalyst 2000, 3000,4000,6000, ISR	CISCO-ENVMON-MIB	ciscoEnvMonTemperatureStatusValue

Таблиця 2.1 - Метрики автоматичного моніторингу параметрів пристрою

У таблиці 2.2 представлені параметри інтерфейсу, які Cisco Prime Infrastructure може моніторити автоматично.

Показники	Опитувані пристрої	Інформаційна база управління	Включені об’єкти ІБУ
Доступність інтерфейсу	Пристрої Cisco IOS, усі підтримувані пристрої Nexus та пристрої	IF-MIB	ifOperStatus

	сторонніх виробників		
Використання вхідних даних	Пристрої Cisco IOS, пристрої сторонніх виробників	IF-MIB, Old-CISCO-Interface-MIB	ifHCInBroadcastPkts, ifHCInMulticastPkts, ifInErrors, ifInDiscards, ifInUnknownProtos ifHCInBroadcastPkts, ifHCInMulticastPkts, locIfInputQueueDrops
Використання вихідних даних	Пристрої Cisco IOS, пристрої сторонніх виробників	IF-MIB, Old-CISCO-Interface-MIB	ifHCOutBroadcastPkts, ifHCOutMulticastPkts, ifHCOutUcastPkts, ifOutDiscards, ifOutUnknownProtos, locIfOutputQueueDrops
Відсоток падіння на клас QoS	Пристрої Cisco IOS	IF-MIB, Old-CISCO-Interface-MIB	cbQosCMDropBitRate,cbQosCMPrePolicyBitRate

Таблиця 2.2 - Метрики автоматичного моніторингу параметрів інтерфейсу

Політики моніторингу інфраструктури Prime відстежують показники мережевих пристроїв і сповіщають вас про зміну умов до того, як проблеми вплинуть на їх роботу. За замовчуванням Prime Infrastructure опитує показники справності пристроїв на підтримуваних маршрутизаторах, комутаторах і

концентраторах і пристроях сторонніх розробників, а також показники справності інтерфейсів на інтерфейсах WAN, з'єднаннях і магістральних портах. Він не опитується на накопичувачах і пристроях серії UCS. Якщо порогове значення порушується три рази, Prime Infrastructure генерує критичний сигнал тривоги, який відображається на сторінці «Сигнали та події».

Prime Infrastructure надає різноманітні інформаційні панелі для моніторингу пристроїв і мережі. Декілька прикладів того, що можуть надати інформаційні панелі [13]:

а) Інформація про стан усієї мережі в реальному часі, як-от недоступні пристрої, несправні інтерфейси та останні тривоги.
б) Зведена історична інформація, наприклад, тривоги, що виникають найчастіше, а також пристрої та інтерфейси з найбільшим використанням пам'яті та ЦП.
в) Інформація про пристрій, як-от історія доступності пристрою, використання, статистика інтерфейсу та сигнали тривоги.

Cisco Prime Infrastructure є дієвим інструментом для моніторингу та управління мережею, зокрема, щодо пропускної спроможності, утилізації ресурсів та виявлення проблем у реальному часі. Враховуючи його функціональні можливості, він може бути ефективним вибором для підприємств, які прагнуть забезпечити стабільну та продуктивну роботу своєї мережі. Однак при виборі системи моніторингу слід враховувати складність налаштування та великий обсяг необхідних ресурсів.

2.1.3 Cisco DNA Center

Cisco DNA Center – це програма для керування та автоматизації, яка використовується як контролер для Cisco DNA. Він використовується як платформа керування як для SD Access та мереж на основі намірів, так і для

існуючих традиційних мереж. Cisco DNA Center — це сучасна платформа керування мережею Cisco для корпоративних мереж [14].

Завдяки ефективній інформаційній панелі Cisco DNA Center дуже легко використовувати мережевим інженерам. Завдяки багаторазовим шаблонам, ефективним робочим процесам, політикам тощо це спрощує мережеві операції, налаштування та усунення несправностей. З DNA Center мережа відчуває зручність мережевої автоматизації. Вашою мережею легко керувати, мережеві операції виконуються ефективно, а час простою мережі зменшується.

Основні функції та переваги Cisco DNA Center [15]:

а) Автоматизація мережі: Cisco DNA Center автоматизує завдання налаштування мережі вручну, зменшуючи ймовірність людських помилок і економлячи дорогоцінний час. Це спрощує розгортання нових пристроїв, оновлень програмного забезпечення та політик безпеки в мережі.

б) Гарантія мережі: Завдяки можливостям моніторингу Cisco DNA Center забезпечує видимість продуктивності мережі в реальному часі. Він проактивно виявляє та вирішує проблеми з мережею, забезпечуючи оптимальну доступність і продуктивність мережі.

в) Контроль доступу на основі політик: Cisco DNA Center дозволяє визначати та застосовувати політики доступу до мережі на основі ролей користувачів, пристроїв і програм. Це спрощує керування контролем доступу, полегшуючи захист вашої мережі від несанкціонованого доступу.

г) Мережева аналітика: Cisco DNA Center збирає та аналізує мережеві дані, щоб надати цінну інформацію про мережевий трафік, використання програм і поведінку користувачів. Ці знання допоможуть вам приймати зважені рішення та вдосконалювати вашу мережу.

д) Програмно-визначена мережа (SDN): Cisco DNA Center підтримує принципи програмно-визначеної мережі, що дозволяє керувати мережевими пристроями та налаштовувати їх за допомогою програмного забезпечення, а не вручну. Це забезпечує гнучкість, масштабованість і динамічність в управлінні мережевою інфраструктурою.

Щоб використовувати Cisco DNA Center, вам потрібно буде інсталювати його на виділеному сервері, який відповідає вимогам до апаратного та програмного забезпечення, визначеним Cisco. Після встановлення ви можете отримати доступ до інтерфейсу Cisco DNA Center через веб-браузер. Там ви знайдете зручну інформаційну панель з інтуїтивно зрозумілими меню та навігацією. Різноманітні обов'язки, як-от реєстрація пристрою, конфігурація мережі, керування політикою безпеки та усунення несправностей, можна виконувати на панелі керування. Крім того, Cisco DNA Center поєднується з іншими рішеннями Cisco, такими як Identity Services Engine (ISE) і Application Policy Infrastructure Controller (APIC), щоб розширити можливості керування мережею [15].

За допомогою можливості ефективного моніторингу Cisco DNA Center може відслідковувати продуктивність вашої мережі наскрізно. Cisco DNA Center пропонує різноманітні послуги моніторингу, які допомагають організаціям зрозуміти стан працездатності їхньої мережі. Ці послуги включають:

- Моніторинг пропускної спроможності: Платформа полегшує організаціям моніторинг пропускної здатності мережі в режимі реального часу. Це допомагає виявляти потенційні проблеми з продуктивністю мережі.
- Моніторинг утилізації ресурсів: Платформа надає організаціям можливість спостерігати за використанням мережевих ресурсів. Це

допомагає виявляти потенційні проблеми з продуктивністю пристроїв.

- Виявлення проблем у реальному часі: Платформа використовує AI для виявлення потенційних проблем у мережі до того, як вони виникнуть. Це допомагає організаціям запобігти перебоям у роботі мережі.

Cisco DNA Center пропонує потужні можливості моніторингу, які допомагають організаціям отримувати уявлення про стан своєї мережі. Платформа забезпечує всеосяжну видимість мережі, включаючи пристрої, додатки, дані та процеси. Це полегшує організаціям отримання повного розуміння справності своєї мережі та розпізнавання потенційних проблем до їх виникнення.

Платформа також використовує штучний інтелект для максимального підвищення ефективності використання мережі. Це може допомогти організаціям заощадити гроші на комунікаційних витратах і підвищити продуктивність. Крім того, платформа забезпечує централізоване управління безпекою мережі. Це полегшує організаціям захист своєї мережі від шкоди.

Cisco DNA Center - це потужний інструмент, який надає комплексні можливості для моніторингу та управління мережею. Його переваги включають централізоване управління, автоматизацію, інтеграцію та розширені аналітичні можливості. Неспростовність налаштувань та вартість можуть бути недоліками, але при правильному впровадженні Cisco DNA Center стає потужним інструментом для вдосконалення та оптимізації мережевої інфраструктури.

2.1.4 Cisco IP SLA

IP SLA — це функція моніторингу продуктивності мережі операційної системи Cisco IOS, яка дозволяє IT-фахівцям збирати інформацію про продуктивність мережі в реальному часі. IP SLA дозволяє спостерігати та звітувати про продуктивність мережі за допомогою показників. IP SLA генерує

та постійно відстежує трафік у мережі, тому це вважається активним методом моніторингу мережі [16].

Маршрутизатор Cisco IOS IP SLA може постійно збирати дані про різні аспекти мережі, зокрема [16]:

а) Час відповіді.
б) Затримка.
в) Джиттер.
г) Втрата пакетів.
д) Якість оцінки голосу.
е) Підключення

Вся ця інформація надає мережевому адміністратору базові відомості про продуктивність мережі. Вона також дозволяє перевірити рівень якості обслуговування (QoS) мережі та швидко виявити причину проблеми, якщо рівень продуктивності падає.

IP SLA на пристроях Cisco IOS - це корисний спосіб моніторингу та забезпечення продуктивності мережі. Ця функція також дозволяє мережевим інженерам та адміністраторам досліджувати проблеми мережі та виявляти їх першопричини за допомогою реальної статистики.

Інженери можуть використовувати IP SLA для моніторингу шляхів трафіку до місця призначення, щоб підтвердити, що певний веб-сервер приймає з'єднання. Широкомасштабні мережі (WAN), які з'єднують декілька географічних регіонів і потребують моніторингу з одного центрального місця, можуть отримати вигоду від IP SLA.

IP SLA також використовується для маршрутизації на основі політик - методу перенаправлення пакетів даних на основі певних політик або фільтрів. Політики можуть застосовуватися на основі певних параметрів, таких як розмір пакета, адреса джерела, адреса призначення або тип трафіку, щоб покращити можливості мережі з обробки трафіку та її загальну гнучкість [16].

Cisco IP SLA можна поєднувати з іншими інструментами моніторингу, включаючи SNMP і NetFlow, ця комбінація дозволить визначити причину проблем з мережею. Використання агента SNMP для опитування маршрутизатора IP SLA полегшить отримання звітів IP SLA і зробить їх більш зрозумілими та менш складними для людей. Крім того, агенти полегшують запис, побудову графіків і перегляд історичної інформації щодо результатів IP SLA. До популярних агентів SNMP належать Cacti, SolarWinds і PRTG.

Коли організації інтегрують IP SLA з системою управління мережею (NMS), вони можуть отримувати візуальні сповіщення про порушення порогових значень в режимі реального часу. IP SLA також можна інтегрувати зі статичними маршрутами - заздалегідь визначеними шляхами, які пакети даних повинні пройти, щоб досягти мережі або хоста призначення. IP SLA також можна поєднувати з протоколами маршрутизації, такими як OSPF або EIGRP [16].

IP SLA виступає як цінний допоміжний інструмент в мережевому адмініструванні, здатний вимірювати та моніторити ключові параметри ефективності мережі. Його переваги включають вимірювання затримки, джиттера, пропускної спроможності та доступності, допомагаючи адміністраторам забезпечити високу якість обслуговування.

Однак IP SLA слід розглядати як складову частину більш широкої мережевої стратегії, оскільки він не здатний моніторити утилізацію ресурсів пристроїв. Для комплексного моніторингу, інтеграція IP SLA з більш потужними моніторинговими системами, такими як Cisco Prime Infrastructure чи інші рішення, що підтримують SNMP, може бути корисною стратегією.

2.2 Аналіз інструментів моніторингу мережі від сторонніх виробників

2.2.1 SolarWinds Network Performance Monitor

SolarWinds Network Performance Monitor (NPM) — це потужна та доступна система моніторингу мережі, розроблена, щоб допомогти вам у досягненні всебічного моніторингу, починаючи з відкриття. Сканер мережевих пристроїв NPM автоматично знаходить пристрої у вашій мережі, що полегшує вам контроль за моніторингом. Ви також можете візуалізувати з'єднання між пристроями, програмами та з'єднаннями за допомогою інструментів відображення топології мережі. Це допомагає покращити видимість і може допомогти у вирішенні проблем [17].

Відстеження пристроїв у мережі має вирішальне значення. NPM спрощує виявлення пристроїв, усуваючи необхідність використання команд CLI для виявлення та ідентифікації пристроїв Cisco у мережі. За допомогою функцій моніторингу пристроїв Cisco NPM може автоматично виявляти та контролювати пристрої Cisco. Використовуючи інтуїтивно зрозумілу інформаційну панель SolarWinds NPM, щоб увімкнути будь-які критичні вузли, які ви хочете контролювати, а потім додаються відповідні пристрої Cisco до свого інвентарю. За допомогою інструментів мережевого моніторингу NPM ви можете контролювати стан і продуктивність будь-якого пристрою з підтримкою SNMP [18].

Відображення мережевих пристроїв вручну може зайняти багато часу, особливо якщо намагатися встигати за зміною топології, і чим більшою та динамічнішою є мережа, тим складніше стає підтримувати актуальну карту топології мережі. Завдяки функціям моніторингу пристроїв ви можете легко створювати динамічні користувацькі карти топології мережі, які відображають показники продуктивності пристрою, підключення та використання каналів. Це означає, що ви можете візуалізувати всю продуктивність вашої мережі з одного погляду, що полегшує відстеження показників продуктивності. Функції

відображення програмного забезпечення для моніторингу мережі дозволяють візуалізувати та збирати дані в інтуїтивно зрозумілий спосіб, щоб ви могли швидко виявити першопричину проблем — навіть у складних мережах [18].

Монітор продуктивності мережі SolarWinds спрощує моніторинг мережевих пристроїв Cisco за допомогою повністю настроюваних інформаційних панелей і діаграм, які дозволяють миттєво переглядати продуктивність і доступність пристроїв Cisco. Щоб контролювати пристрої Cisco в мережі, NPM опитує MIBS на ваших пристроях і отримує критичні показники продуктивності. Потім NPM відображає цю інформацію у зручних графіках, які ви можете змінити відповідно до своїх особистих уподобань. Цей інструмент може допомогти забезпечити продуктивність і доступність брандмауерів Cisco ASA. Ця потужна функція програмного забезпечення Cisco для моніторингу пристроїв може бути представлена на інформаційній панелі PerfStack, що дозволяє порівнювати різні типи даних, співвідносити ваші дані на загальній шкалі часу та обмінюватися даними між командами [18].

SolarWinds NPM пропонує комплексний моніторинг пристроїв Cisco, тому ви можете інтегрувати свій підхід до моніторингу мережі Cisco в єдиний інструмент. NPM забезпечує підтримку пристроїв Cisco, включаючи пристрої ACI, як-от комутатори Spine Switch і Nexus leaf. Цей інструмент дозволяє переглядати загальний стан членів Cisco SwitchStack, швидко знаходити комутатори з проблемами та контролювати підключення даних учасників. Ви також можете відстежувати продуктивність пристрою Nexus і брандмауери Cisco ASA, забезпечуючи детальну видимість інфраструктури ASA, щоб ви могли гарантувати доступність послуг. Завдяки функції автоматичного виявлення пристроїв Cisco NPM ідентифікація, зіставлення та моніторинг усіх компонентів Cisco мережі не може бути простішою.

SolarWinds Network Performance Monitor містить широкий спектр функцій усунення несправностей мережі, які об’єднують ваші пристрої Cisco та інші мережеві компоненти в односторінковий аналіз шляху. Це спрощує усунення несправностей, що дає змогу швидше визначити першопричину

проблем. З центральної інформаційної панелі керування NPM можна відстежувати продуктивність, деталі конфігурації пристрою та трафік, консолідуючи свої дії з усунення несправностей та аналізу. Щоб звести до мінімуму кількість непотрібних отриманих сповіщень, NPM також має можливості інтелектуального оповіщення мережі з урахуванням топології. Систему сповіщень можна персоналізувати, щоб ви не отримували некритичні сповіщення у неробочий час. Завдяки розширеним функціям усунення несправностей і інтелектуальним сповіщенням Network Performance Monitor ви можете залишатися в курсі подій і швидко вирішувати проблеми [18].

SolarWinds NPM можна встановити лише в ОС Windows. Пакет створює дві служби, які є сервером додатків і сервером бази даних. Ці дві частини не можна встановити на одній машині. Вимоги до апаратного забезпечення системи збільшуються з підвищенням рівня можливостей моніторингу елементів. Тобто для запуску NPM SL2000 потрібен більш потужний комп'ютер, ніж для запуску NPM SL100. Для цього потрібна Windows Server 2012 або Windows Server 2016 для обох елементів системи. Середовище бази даних має базуватися на Microsoft SQL Server 2012, 2014 або 2016. Комп'ютер, на якому ви хочете запустити монітор, потребує принаймні чотирьох-ядерного процесора з тактовою частотою 2,5 ГГц. Ця швидкість має становити принаймні 3 ГГц для версії SLX. Комп'ютер, на якому розміщено базу даних, також повинен мати чотирьох-ядерний процесор, але потрібна швидкість принаймні 3 ГГц навіть для NPM SL100 [19].

Хоча може виникнути бажання спробувати Network Performance Monitor для невеликої мережі, його функціональність краще підходить для середніх і великих систем. Його додаткові функції та візуалізації дійсно підвищать продуктивність адміністрування та стабільність мережі для великих і складних мереж.

У SolarWinds Network Performance Monitor є кілька дуже приємних додаткових функцій, які зазвичай не очікуються від цієї категорії програмного забезпечення для моніторингу мережі. Вони включають можливість

установлювати налаштовані умови сповіщення з об’єднаних мережевих джерел даних, тож ви не просто записуєте статуси окремих пристроїв. Модуль NetPath — ще одна чудова утиліта, яка розширює можливості усунення несправностей Network Performance Monitor на територію аналізатора пропускної здатності. Можливість моніторингу віртуальних середовищ, бездротових мереж та інтернет-маршрутів доповнює функції моніторингу локальної мережі, щоб створити справді глобальну службу моніторингу, яка дуже добре працюватиме для гібридних і складних мережевих топологій [19].

SolarWinds NPM для моніторингу мережі Cisco є ефективним інструментом для підтримки високого рівня продуктивності мережі. Завдяки розширеним можливостям моніторингу та аналізу ви можете швидко виявляти, точно визначати та вирішувати проблеми, заощаджуючи час і ресурси. Завдяки його засобам ви можете ефективно контролювати свою мережу, щоб забезпечити надійність і ефективність.

2.2.2 ManageEngine NetFlow Analyzer

Моніторинг обсягу мережевого трафіку та використання пропускної здатності за допомогою NetFlow має вирішальне значення для будь-якого типу мережі. Отримання видимості трафіку користувачів, трафіку додатків і потоків даних дозволяє мережевим інженерам, адміністраторам і фахівцям із безпеки виявляти вузькі місця – перевантаження мережі, незвичні моделі трафіку, контролювати угоди SLA з провайдерами, перевіряти доступність пропускної здатності, виявляти проблеми з якістю обслуговування (QoS), моніторинг мережі Wi-Fi та багато іншого [20].

Netflow — це мережевий протокол, розроблений Cisco, який використовується для збору інформації про IP-трафік і моніторингу мережевого трафіку. Він використовується та підтримується майже в будь-якій мережі та став галузевим стандартом.

NetFlow Analyzer — це інструмент аналізу смуги пропускання та трафіку, який полегшує моніторинг використання смуги пропускання у вашій мережі та аналіз конкретних даних про те, хто, коли та що стосується вашого мережевого

трафіку. Він використовує технологію потоку, щоб забезпечити видимість вашої мережі в режимі реального часу, і підтримує всі основні формати потоку, такі як netflow, sflow, jflow, IPFIX і appflow. Це допоможе ретельно ознайомитися з деталями на рівні інтерфейсу, щоб виявити шаблони трафіку та відстежувати продуктивність пристрою, розпізнавати та класифікувати нестандартні програми, які перевантажують пропускну здатність мережі, і виявляти загрози безпеці. Використання інструменту моніторингу пропускної здатності мережі, такого як NetFlow Analyzer, дозволяє контролювати всі ці важливі параметри в реальному часі [20].

Основні функції NetFlow Analyzer, які допомагають ефективно контролювати пропускну здатність мережі Cisco [21]:

а) Виявлення пристрою. NetFlow Analyzer дає вам уявлення про всі потокові та непотокові експортуючі пристрої Cisco у вашій інфраструктурі, від серверів до комутаторів, маршрутизаторів до брандмауерів та інтерфейсів. Також можна контролювати всі бездротові пристрої Cisco у вашій інфраструктурі, такі як контролери та точки доступу. Отримання широкої видимості відсотка трафіку пов’язаних SSID, IP-адрес клієнта та MAC-адрес, а також їхніх програм. Ви також можете ізолювати несанкціоновані пристрої або обмежити їм доступ до вашої мережі.

б) Використання пропускної здатності на рівні програми. За допомогою NetFlow Analyzer ви можете отримати видимість того, яка програма завантажує пропускну здатність вашої мережі та знижує продуктивність критично важливих для бізнесу програм. Відстеження рівню 4 і трафіку користувацьких або домашніх програм, відображаючи програми за допомогою можливостей рішення. Завдяки технології Cisco NBAR2 NetFlow Analyzer можна також контролювати програми рівня 7 за допомогою динамічних портів і знаходити їх використання для оптимізації продуктивності мережі.

в) Виявлення аномалій поведінки мережі (NBAD). Діагностика та усунення будь-яких загроз безпеці у середовищі Cisco, виявляючи відомі та невідомі атаки безпеки. За допомогою аналізу поведінки мережі або виявлення аномалій поведінки мережі можна знайти нові та незвичні дії в мережі та виявити, чи становлять вони потенційну загрозу безпеці організації.

г) Глибока перевірка пакетів. Відстежуйте продуктивність серверів Cisco організації за допомогою глибокої перевірки пакетів (DPI) NetFlow Analyzer. Ви можете встановити DPI до десяти пристроїв і отримати час відповіді додатків і мережі в реальному часі для додатків і розмов TCP, а також знайти обсяг трафіку UDP. Це може визначити основну причину проблеми перевантажень, чи це через програму, чи на стороні мережі.

д) Формування трафіку. Керування тим, як має використовуватися пропускна здатність мережі, за допомогою параметрів формування трафіку, таких як QoS, список контролю доступу (ACL) і політика обслуговування. Підвищення продуктивності мережі, обмеживши або заблокувавши певні ресурсомісткі програми, які забирають пропускну здатність. Може визначати пріоритетність трафіку відповідно до вимог підприємства та переконатися, що всі критично важливі програми отримують достатню пропускну здатність. Перевірте відповідність і ефективність застосованих політик за допомогою карт класів QoS (CBQoS).

е) Управління ризиками за допомогою сповіщень. Зменшення впливу мережевих проблем, перш ніж вони підірвуть продуктивність, налаштувавши сповіщення про випадки, коли використання пропускної здатності стає нижче або вище базової продуктивності. За допомогою сповіщень у режимі реального часу та зведених сповіщень можна встановити порогове значення, серйозність і дію, щоб отримувати сповіщення, коли використання даних відповідає

пороговому значенню. NetFlow Analyzer також має попередньо налаштоване сповіщення Link Down для сповіщення, коли будь-який з інтерфейсів пристроїв виходить з ладу. Щоб отримувати сповіщення про подію, ви можете вибрати будь-який шаблон сповіщень, як-от електронна пошта, SMS, чат або залогувати тікет.

ж) Групування пристроїв. Зменшення середнього часу отримання інформації для усунення несправностей моніторингу пропускної здатності Cisco, згрупувавши пристрої на основі відділів або філій. NetFlow Analyzer допомагає створювати логічні групи пристроїв, IP-адрес, інтерфейсів і точок доступу, щоб ефективно контролювати та керувати використанням пропускної здатності. Також можна призначати певні ролі користувачів, наприклад адміністраторів, операторів і гостей, для кращої доступності та безпеки.

ManageEngine NetFlow Analyzer — це потужний інструмент для моніторингу та аналізу мережевого трафіку у середовищі Cisco. Це сприяє ефективній ідентифікації та вирішенню мережевих проблем, оптимізації ресурсів і підвищенню продуктивності. З фінансової точки зору це може знизити витрати на розширення мережі та підтримувати стабільну роботу інфраструктури.

2.2.3 Zabbix

Моніторинг мережевих параметрів, працездатності сервера та продуктивності є основною відповідальністю програмного забезпечення Zabbix. Zabbix використовує гнучкий механізм сповіщень, який дозволяє користувачам налаштовувати сповіщення електронною поштою майже про будь-яку подію. Це покращує нашу здатність оперативно реагувати на проблеми з сервером. Zabbix надає чудові можливості звітності та візуалізації даних на основі збережених даних. Zabbix підтримує як опитування, так і перехоплення. Усі звіти та статистика Zabbix, а також параметри конфігурації доступні через веб-інтерфейс. Веб-інтерфейс дозволяє оцінювати стан мережі

та продуктивність сервера з будь-якого місця. Якщо Zabbix правильно налаштований, він може мати значний вплив на моніторинг вашої технологічної інфраструктури. Він підходить як для невеликих організацій з кількома серверами, так і для великих підприємств з великою кількістю серверів. [22].

Zabbix збирає дані з різних пристроїв і систем у мережі, аналізує ці дані та забезпечує моніторинг у реальному часі та оповіщення [23]:

а) Збір даних. Zabbix використовує агенти, які є невеликими програмними модулями, встановленими на пристроях, які потрібно контролювати (таких як сервери, маршрутизатори та комутатори). Ці агенти збирають відповідні дані, такі як системні показники, мережевий трафік і продуктивність програм, з пристроїв. Крім того, Крім того, Zabbix також може збирати інформацію за допомогою автоматичних методів, таких як SNMP та IPMI.

б) Обробка даних. Зібрані дані надсилаються на сервер Zabbix для обробки та аналізу. Сервер збирає та зберігає дані в базі даних для подальшого використання та аналізу. Zabbix також підтримує віддалений моніторинг за допомогою проксі, які можна встановити у віддалених місцях для збору та передачі даних на центральну платформу.

в) Моніторинг і тригери. Zabbix постійно відстежує зібрані дані в режимі реального часу. Він порівнює дані з попередньо визначеними пороговими значеннями та правилами, встановленими адміністраторами. Ці порогові значення визначають прийнятний діапазон значень для певних показників. Якщо метрика перевищує або падає нижче визначеного порогу, Zabbix запускає подію.

г) Оповіщення та повідомлення. Коли спрацьовує подія, Zabbix генерує сповіщення та сповіщення. Він може надсилати сповіщення через різні канали, такі як електронна пошта, SMS, обмін миттєвими

повідомленнями або спеціальні сценарії. Адміністратори можуть визначати різні методи сповіщення залежно від серйозності події, це забезпечить швидке сповіщення відповідних людей.

д) Візуалізація та звітність. Zabbix надає зручний веб-інтерфейс, де адміністратори можуть створювати налаштовані інформаційні панелі, графіки та звіти для візуалізації зібраних даних. Ці візуальні представлення допомагають визначати тенденції, аналізувати історичні дані та отримувати уявлення про продуктивність і стан мережі.

Впровадження Zabbix для моніторингу мережі має кілька власних переваг і недоліків [23]:

а) Відкритий вихідний код. Zabbix є безкоштовним у використанні, усуваючи витрати на ліцензування та дозволяючи організаціям інвестувати ресурси в інші місця.

б) Активна спільнота. Zabbix має велику та активну спільноту користувачів, яка надає доступ до обширних ресурсів, підтримку та обмін знаннями.

в) Гнучкість. Гнучкість Zabbix дозволяє йому адаптуватися до різноманітних мережевих середовищ, що робить його придатним для компаній зі складною інфраструктурою.

г) Налаштування: Zabbix дозволяє створювати власні шаблони моніторингу, правила та сповіщення відповідно до конкретних вимог.

Серед недоліків Zabbix можна виділити наступне:

а) Витратність ресурсів: Zabbix може споживати значні ресурси сервера, особливо під час моніторингу великої кількості пристроїв і збору великої кількості даних. Може знадобитися належне планування обладнання та налаштування продуктивності.

б) Накладні витрати на технічне обслуговування: для безперебійної роботи Zabbix необхідне регулярне технічне обслуговування, таке як

очищення бази даних та оновлення програмного забезпечення. Нехтування завданнями технічного обслуговування може з часом призвести до проблем з продуктивністю.

Zabbix відстежує мережі, сервери та програми. Послуги моніторингу Cisco в цьому пакеті надаються для загального моніторингу пристроїв на основі SNMP і служб аналізу трафіку, які застосовуються до всіх марок мережевих пристроїв. Однак Zabbix також пропонує шаблони, які пропонують певний доступ до пристроїв Cisco. Шаблони, доступні для обладнання Cisco, надають канали для прямого підключення до пристроїв Cisco, запитів до них і оновлення їхніх налаштувань. Існують шаблони для всіх типів обладнання Cisco, включаючи брандмауери. Ці шаблони доступні безкоштовно в спільноті користувачів. Інформаційна панель служби є одночасно привабливою та конфігурованою. Ви отримуєте сторінку карти мережі, яка автоматично оновлюється на основі регулярних перевірок стану SNMP. Ви також отримуєте інвентаризацію пристроїв на інформаційній панелі. Статуси та події обладнання відображаються на екрані у вигляді тексту, а також у кольорових діаграмах і графіках. Монітор постачається з кількома стандартними звітами, але також може створювати власні або отримувати їх від спільноти користувачів [24].

Zabbix вимагає як фізичної, так і дискової пам’яті. 128 МБ фізичної пам’яті та 256 МБ вільного дискового простору можуть бути хорошою відправною точкою. Однак обсяг необхідної дискової пам'яті, очевидно, залежить від кількості хостів і параметрів, які контролюються. Якщо ви маєте намір зберігати довгу історію параметрів моніторингу, вам слід мати принаймні декілька гігабайт пам’яті для зберігання історії в базі даних. Кожен процес демона Zabbix асоціюється з декількома підключеннями до сервера бази даних. Обсяг пам’яті, виділеної для з’єднання, залежить від конфігурації механізму бази даних. Zabbix і особливо база даних Zabbix можуть вимагати значних ресурсів процесора залежно від кількості параметрів, що

відстежуються, і вибраного механізму бази даних. Для використання підтримки SMS-повідомлень у Zabbix потрібні послідовний порт зв’язку та послідовний модем GSM. Перетворювач USB-serial також буде працювати [25].

Zabbix - це ефективна система моніторингу мереж Cisco. Забезпечує розширений моніторинг пропускної здатності, використання ресурсів і можливості виявлення проблем у реальному часі. З огляду на економічні фактори, це може бути вигідним варіантом для компаній, які шукають потужне та ефективне рішення для моніторингу мережі.

2.2.4 Paessler PRTG

PRTG — це комплексна програма моніторингу мережі для систем на базі Windows. Він підходить для мереж будь-якого розміру та підтримує моніторинг LAN, WAN, WLAN та VPN. Також може контролювати фізичний або віртуальний веб-сервер, поштовий і файловий сервери, системи Linux, клієнти Windows, маршрутизатори та багато іншого. PRTG відстежує доступність мережі та використання пропускної здатності, а також різноманітні інші параметри мережі, такі як якість обслуговування, завантаження пам’яті та використання ЦП, навіть на віддалених машинах. PRTG надає системним адміністраторам дані в реальному часі та періодичні тенденції використання для оптимізації ефективності, компонування та налаштування виділених ліній, маршрутизаторів, брандмауерів, серверів та інших мережевих компонентів [26].

Програмне забезпечення відстежує мережу, яка використовує протокол (SNMP), інструментарій керування Windows (WMI), аналізатор пакетів, Cisco NetFlow, IPFIX, sFlow, jFlow та багато інших галузевих стандартних протоколів. Він працює на машині під керуванням Windows у мережі протягом 24 годин на добу. PRTG постійно записує параметри використання мережі та доступність мережевих систем. Записані дані зберігаються у внутрішній базі даних для подальшого аналізу.

Ключові особливості Paessler PRTG [27]:

а) Висока продуктивність: система бази даних зберігає необроблені результати моніторингу, а також журнали, топ-листи та заявки. Це перевершує сервери мови структурованих запитів (SQL) для моніторингу даних. Ви можете розподілити високі навантаження між кількома зондами, а також отримати доступ до бази даних через PRTG API.

б) Низькі системні вимоги: для роботи PRTG Network Monitor достатньо середньостатистичного ПК не старше 2 років. Навіть нетбук може контролювати більше тисячі датчиків. PRTG Hosted Monitor не потребує апаратного забезпечення для основного сервера PRTG.

в) Високі стандарти безпеки: захищені з’єднання та веб-сервери Secure Sockets Layer (SSL) та Transport Layer Security (TLS), безпечні шифри, персоналізоване керування правами користувачів і багато іншого.

г) Захищений SSL/TLS веб-сервер із підтримкою HTTP та HTTPS для веб-інтерфейсу PRTG. Це діє як односторінкова програма (SPA), щоб уникнути тривалого перезавантаження сторінки. Сервер ретрансляції електронної пошти для автоматичної доставки електронної пошти.

д) Настроювані сповіщення для конкретних потреб: Різні методи сповіщення: електронна пошта, push-повідомлення, текстові повідомлення SMS, повідомлення системного журналу та перехоплення протоколу простого керування мережею (SNMP), запити HTTP, журнали подій, служба простих сповіщень Amazon (SNS), сценарії виконання.

е) Кілька способів ініціювання сповіщень: сповіщення про статус, сповіщення про обмеження, сповіщення про порогове значення, сповіщення про кілька умов, сповіщення про ескалацію. Поступові залежності, щоб уникнути затоплення тривог, підтвердження певних тривог, щоб уникнути подальших сповіщень, і планування сповіщень.

ж) Глибокий генератор звітів для створення звітів на вимогу або запланованих звітів у HTML, як .pdf, .csv або .xml. За замовчуванням доступні кілька шаблонів звітів.

з) Графічний механізм для зручних живих графіків і графіків історичних даних.

и) Модулі аналізу мережі для автоматичного пошуку мережевих пристроїв і датчиків.

к) Розподілений моніторинг для моніторингу кількох мереж у різних місцях.

л) Спеціальні функції для постачальників керованих послуг (MSP) для моніторингу мереж клієнтів і підвищення якості обслуговування.

м) Публікація даних за допомогою інформаційних панелей у режимі реального часу, включаючи живу інформацію про продуктивність і статус.

н) Налаштування: PRTG API дозволяє розробляти власні функції. Крім того, ви можете створювати спеціальні датчики, сповіщення та шаблони пристроїв відповідно до ваших потреб.

Cisco пропонує потужні рішення в кількох сферах, від керування мережею та уніфікованого зв’язку до управління маршрутизацією та комутацією. Професійно відстежуючи параметри, пов'язані з Cisco, можна вичерпати всі його можливості. Також надається доступ до всіх датчиків Cisco у безкоштовній версії PRTG. Щоб почати необхідно лише активувати датчики та почати моніторинг пристроїв мережі [28].

Комутатори Cisco відомі своєю безвідмовною конструкцією та стабільністю, але це не означає, що вони не можуть створювати проблеми. Несправний комутатор Cisco може призвести до незліченних проблем з мережею, включаючи пошкодження ЦП і проблеми з підключенням. Багато системних адміністраторів використовують командний рядок для швидкого запиту, наприклад, чи доступний певний мережевий компонент. Однак професійний моніторинг йде набагато далі. Професійний інструмент

моніторингу використовує такі протоколи, як SNMP, NetFlow і IPFIX, щоб постійно стежити за всіма найважливішими мережевими пристроями. PRTG постачається з кількома датчиками SNMP, а також із вбудованими датчиками Cisco. Серед іншого, моніторинг комутатора Cisco за допомогою PRTG дозволяє контролювати ЦП, температуру, час безвідмовної роботи, трафік і порти. За допомогою PRTG ви контролюватимете всі свої мережеві пристрої – незалежно від виробника – з однієї центральної панелі інструментів. PRTG також постачається з настроюваною системою сповіщень, яка негайно подає звуковий сигнал у разі виникнення проблем [29].

Маршрутизатори Cisco надзвичайно стабільні та забезпечують високий рівень безпеки. Багато системних адміністраторів використовують маршрутизатори Cisco для своїх мереж. Завдяки PRTG можна легко контролювати маршрутизатори Cisco за допомогою NetFlow або SNMP. Датчик трафіку SNMP відображає вхідний і вихідний трафік, а також загальний трафік. Моніторинг трафіку відбувається за допомогою протоколу NetFlow. Датчик Cisco IP SLA відстежує якість обслуговування вашої мережі. Серед іншого, він вимірює втрату пакетів і джиттер. PRTG контролює різні швидкості та значення затухання підключення ADSL. Він дозволяє встановлювати власні порогові значення та сповіщає вас, якщо ці значення перевищено. Як наслідок, можна переконатися, що у вас завжди є достатня пропускна здатність. За допомогою датчику Cisco Health Sensor система моніторингу PRTG надає можливість моніторингу утилізації ресурсів таких як: оперативна пам’ять, завантаженість центрального процесору та інших [30].

Виходячи з наступних переваг Paessler PRTG є чудовим засобом моніторингу Cisco мереж [28]:

а) Висока якість завдяки приналежності до співтовариства розробників Cisco: член мережі розробників Cisco, PRTG надає індивідуальні датчики для вашої мережі Cisco, тож ви завжди можете бути в безпеці.
б) Простий порівняльний аналіз VoIP: оскільки вони особливо схильні до затримок і втрат даних, певні параметри попередньо

розраховуються прямо на етапі аналізу (наприклад, ICPIF, MOS). Це дає можливість проводити порівняльний аналіз безпосередньо, без додаткових розрахунків.

в) Повний моніторинг гарантії якості: об’єднавши всі відповідні параметри лише з кількома датчиками, ви можете легко виміряти якість обслуговування вашої мережі Cisco та використовувати свої висновки для прийняття обґрунтованих рішень.

г) Високопродуктивний моніторинг через SNMP: використовуючи технологію SNMP, можна збирати такі параметри, як статистичні дані про використання процесора та підключення ADSL маршрутизатора Cisco за мінімального споживання пропускної здатності.

д) Огляд усіх VPN-з’єднань IPsec: для пристроїв Cisco з Adaptive Security Appliance (ASA) ви отримаєте легкий для читання огляд трафіку, користувачів і захищених IPsec VPN-з’єднань.

е) Швидке створення кількох датчиків для підключень VPN: активувавши датчики ASA VPN, ви можете швидко налаштувати додаткові підключення VPN для моніторингу. Це звільняє вас від необхідності створювати окремий датчик для кожного окремого підключення.

ж) Короткий огляд справності системи: за допомогою PRTG ви отримуєте чіткий і надійний огляд усіх необхідних значень, включаючи температуру, навантаження ЦП, блок живлення та доступну пам’ять.

з) Ідеальна сумісність із технологією Cisco NetFlow: шість датчиків допомагають мережам із високим трафіком контролювати трафік даних і забезпечують високу продуктивність мережі. Датчики, як у стандартній, так і в настроюваній версіях, сумісні з протоколами NetFlow IPFIX, NetFlow 9 і NetFlow 5.

и) Автоматичні сповіщення: якщо станеться помилка або буде перевищено один із визначених вами порогів, ви отримаєте сповіщення негайно, де б ви не були.

к) Автоматизація для зменшення робочого навантаження: завдяки датчикам і сповіщенням PRTG вам більше не потрібно витрачати час на перевірку кожного пристрою вручну.

л) Краща мережева безпека: завдяки спеціальним датчикам Cisco та надзвичайно чіткому моніторингу ви швидше помітите лазівки в безпеці своїх пристроїв Cisco.

На основі вищезазначених спільних аспектів PRTG тепер можна сміливо підсумувати, що PRTG є чудовим і доступним інструментом моніторингу мережі Cisco з безліччю датчиків моніторингу, зручним інтерфейсом та чималою кількістю додаткових функцій, які спрощують сучасний процес моніторингу мережі.

2.3 Вибір системи моніторингу мережі між постачальником та стороннім виробником

Моніторинг пристроїв Cisco за допомогою інструментів моніторингу Cisco може бути єдиною підтримкою, яка потрібна підприємствам. Однак багато вбудованих програм моніторингу та готових інструментів для усунення несправностей не мають локального інтерфейсу користувача. Деякі мережі складаються з тисяч людей і пристроїв кількох постачальників, які розтягуються на багатьох фізичних сайтах. Це може зробити ефективне керування мережею важкою роботою для IT-відділів, створюючи ситуації, коли один пристрій не спілкуватиметься з іншим або застаріває та створює збої в мережі [8].

Незалежно від того, обладнання якого постачальника використовується або скільки користувачів і кінцевих точок у мережі, моніторинг і усунення несправностей у корпоративному середовищі є життєво важливими. Інструменти моніторингу постачальників створені спеціально для певного обладнання; вони відстежують лише рішення конкретного постачальника. Що стосується сторонніх інструментів моніторингу, ви отримуєте набагато більше. Інструменти управління продуктивністю сторонніх розробників мають ширший погляд на обладнання та середовище, які вони збираються контролювати та керувати [8].

Якщо брати до уваги уніфіковані комунікації, потрібно враховувати набагато більше речей. Тому що, уніфіковані комунікації являють собою мережу, обладнання безпеки, таке як SBC, відеокомпоненти, включені до UC, це все стосується програм, апаратного забезпечення аналізу. Отже, це справді складне середовище, у якому сторонні інструменти моніторингу та керування допоможуть забезпечити більшу видимість. У випадку використання інструмента керування стороннього виробника, він дає видимість усіх пристроїв мережі, незалежно від виробника пристрою.

Найкращий спосіб підвищення ефективності моніторингу мережі – це використання єдиного програмного забезпечення для моніторингу продуктивності мережі та єдиним інтерфейсом користувача. Це означає, що не потрібно встановлювати, завантажувати та вивантажувати кілька клієнтів програмного забезпечення або перемикатися з одного набору термінології на інший, вивчати ярлики та отримувати глибокі знання про різні продукти. Управління декількома постачальниками повинно бути достатньо гнучким, щоб дозволити точно налаштувати моніторинг для однієї платформи і в той же час використовувати напрацювання, зроблені вами на іншій платформі. Інструменти моніторингу мережі Cisco ефективні лише для моніторингу пристроїв Cisco. Для управління та налаштування декількох мережевих пристроїв мережеві інженери та команди повинні бути навчені роботі з CLI/API/GUI та іншими інтерфейсами [7].

Коли мова йде про рішення для управління мережею, вони завжди дають можливість використовувати можливості декількох постачальників, в той час як рішення конкретного постачальника завжди зосереджені на чомусь одному, що поставляється від постачальника. Дуже важливо, щоб у вас було сертифіковане рішення, тому що це дає вам впевненість, що інструмент буде працювати з обладнанням, яке ви намагаєтесь контролювати.

Вибираючи інструмент моніторингу мережі від Cisco, наразі найкраще використовувати Cisco Prime Infrastructure, оскільки він централізує керування пристроями Cisco через єдиний інтерфейс, також надає інформацію щодо використання пропускної здатності та критичних подій, усі вони відбуваються в режимі реального часу та надають сповіщення про ці події.

Серед систем моніторингу від сторонніх виробників для моніторингу мереж на основі обладнання Cisco найбільш підходящим вибором буде Paessler PRTG, оскільки він об’єднує в собі необхідні характеристики, які спростять робочий процес, дозволяючи контролювати всю інфраструктуру. Вбудовані датчики охоплюють багато основних випадків використання, без необхідності купувати додаткові, тому вони можуть контролювати пристрої Cisco, а також мережу, сервіси, сервери, пристрої IoT, хмарну інфраструктуру, бази даних і багато іншого. Крім того, їх можна розширювати, а це означає, що можна розгортати датчики сторонніх виробників або навіть розробляти власні, щоб задовольнити конкретні потреби.

3 ТЕХНІЧНЕ ОБГРУНТУВАННЯ ЕФЕКТИВНОГО ПРОЦЕСУ МОНІТОРИНГУ МЕРЕЖІ

3.1 Вибір обладнання та програмного забезпечення для моніторингу мережі Cisco

Адміністратори мереж часто стикаються з необхідністю моніторингу та аналізу мережної активності. Для цього можливо використати кілька різних пристроїв Cisco, які мають велику кількість можливостей моніторингу мережі. Комутатори Cisco Catalyst, які призначені для корпоративних комунікацій, мають першочергове значення для цього.

Дані комутатори підтримують протоколи NetFlow – протокол моніторингу трафіку в мережі та протокол SNMP версії 3, що дозволяє збирати інформацію про керовані пристрої в IP-мережі та подальшого моніторингу мережі.

Також для моніторингу мережі може використовуватись Cisco ASA Firewall. Cisco ASA - це пристрій безпеки, який забезпечує видимість характеру вхідного і вихідного трафіку і дозволяє більш ефективно управляти політиками безпеки. Моніторинг та аналіз трафіку Cisco ASA відіграє важливу роль у захисті мережі від зловмисних дій, моніторинг та аналіз мережевого трафіку виконується за допомогою функцій аналізу трафіку FirePOWER.

Cisco WLC (Wireless LAN Controller) – керовані бездротові контролери, які дозволяють виконувати моніторинг бездротової мережі. Вони надають можливість аналізу мережного трафіку, виявлення та виправлення проблем у бездротовій мережі, а також надають детальну статистику використання ресурсів.

При виборі обладнання Cisco для моніторингу мережі необхідно враховувати вимоги вашої мережі і конкретні завдання, які перед вами стоять. Крім того, важливо враховувати бюджет і наявні ресурси, щоб вибрати найбільш відповідне обладнання.

Вибір програмного забезпечення моніторингу мережі Cisco — це вибір між рішенням Cisco або стороннім програмним продуктом, який повністю сумісний з апаратним забезпеченням Cisco. Рішенням від компанії Cisco є Cisco Prime Infrastructure. Він надає можливість спостерігати за мережею в режимі реального часу, збирати дані про трафік, виявляти проблеми з мережею та негайно вживати заходів для їх усунення. Одним з найкращих рішень від сторонніх виробників, буде використання Paessler PRTG, оскільки він сумісний з пристроями Cisco, надає можливість налаштування сенсорів моніторингу спеціально розроблених для пристроїв Cisco, які спростять робочий процес, дозволяючи контролювати всю інфраструктуру.

3.2 Реалізація моніторингу мережі Cisco

Для реалізації моніторингу мережі Cisco, необхідне відповідне програмне забезпечення. Реалізація буде відбуватись за допомогою програми емуляції мережі EVE-NG. Дане рішення надає змогу експериментувати з мережевими конфігураціями, протоколами та технологіями без використання фізичних пристроїв, з можливістю взаємодіяти з реальною мережею. Також даний емулятор має можливість інтеграції з програмним забезпеченням для моніторингу мережі Paessler PRTG, яке виконує моніторинг мережі, використовуючи протокол SNMP.

Першим кроком, необхідно налаштувати SNMP-протокол на маршрутизаторі Cisco, для збору даних з пристроїв мережі. Для початку

необхідно встановити комунікаційний рядок (community string) для доступу до пристроїв. Далі увімкнути SNMP-службу на всіх пристроях. Після цього налаштувати пристрій в якості SNMP-агента, який буде відповідати на SNMP-запити, відправлені мережевим менеджером. Також необхідно налаштувати відправку SNMP-пасток на PRTG, використовуючи UDP-порти 161 та 162. Конфігурація SNMP на маршрутизаторі Cisco виглядатиме наступним чином:

R1(config)#snmp-server community IIIPRTG RO

R1(config)#snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart

R1(config)#snmp-server enable traps license

R1(config)#snmp-server enable traps memory bufferpeak

R1(config)#snmp-server enable traps cpu threshold

R1(config)#snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config

R1(config)#snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up

R1(config)#snmp-server enable traps ethernet cfm alarm

R1(config)#snmp-server host 192.168.0.50 version 2c comp-comm

На рисунку 3.1 продемонстровано конфігурацію маршрутизатора Cisco.

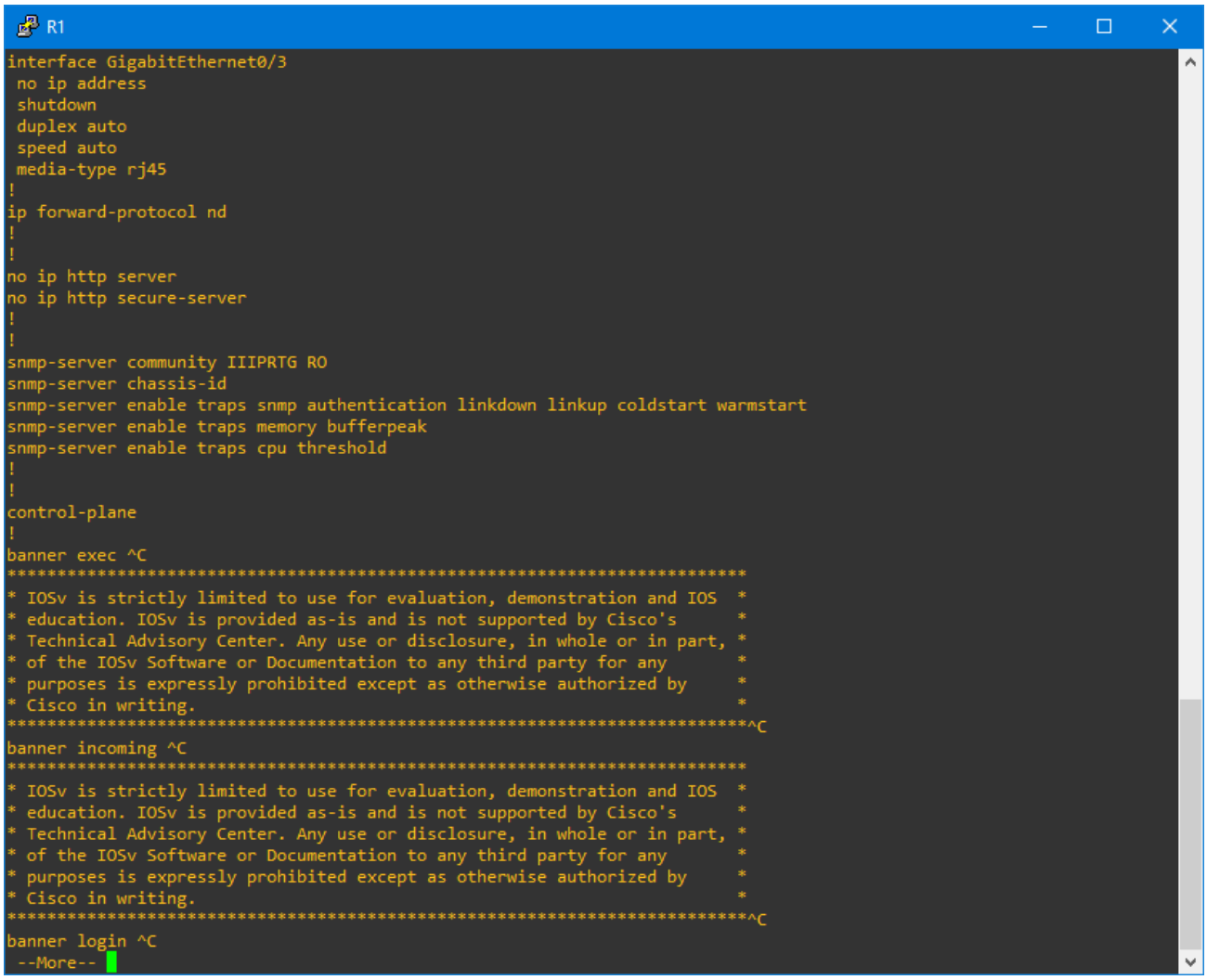


Рисунок 3.1 – Конфігурація маршрутизатора Cisco

Другим кроком, необхідно налаштувати програмне забезпечення моніторингу, яке буде збирати та аналізувати отримані дані. В якості програмного забезпечення використовується Paessler PRTG. Для цього в моніторинговому ПЗ необхідно додати попередньо налаштований маршрутизатор.

Додавання нового пристрою в Paessler PRTG відображено на рисунку 3.2.

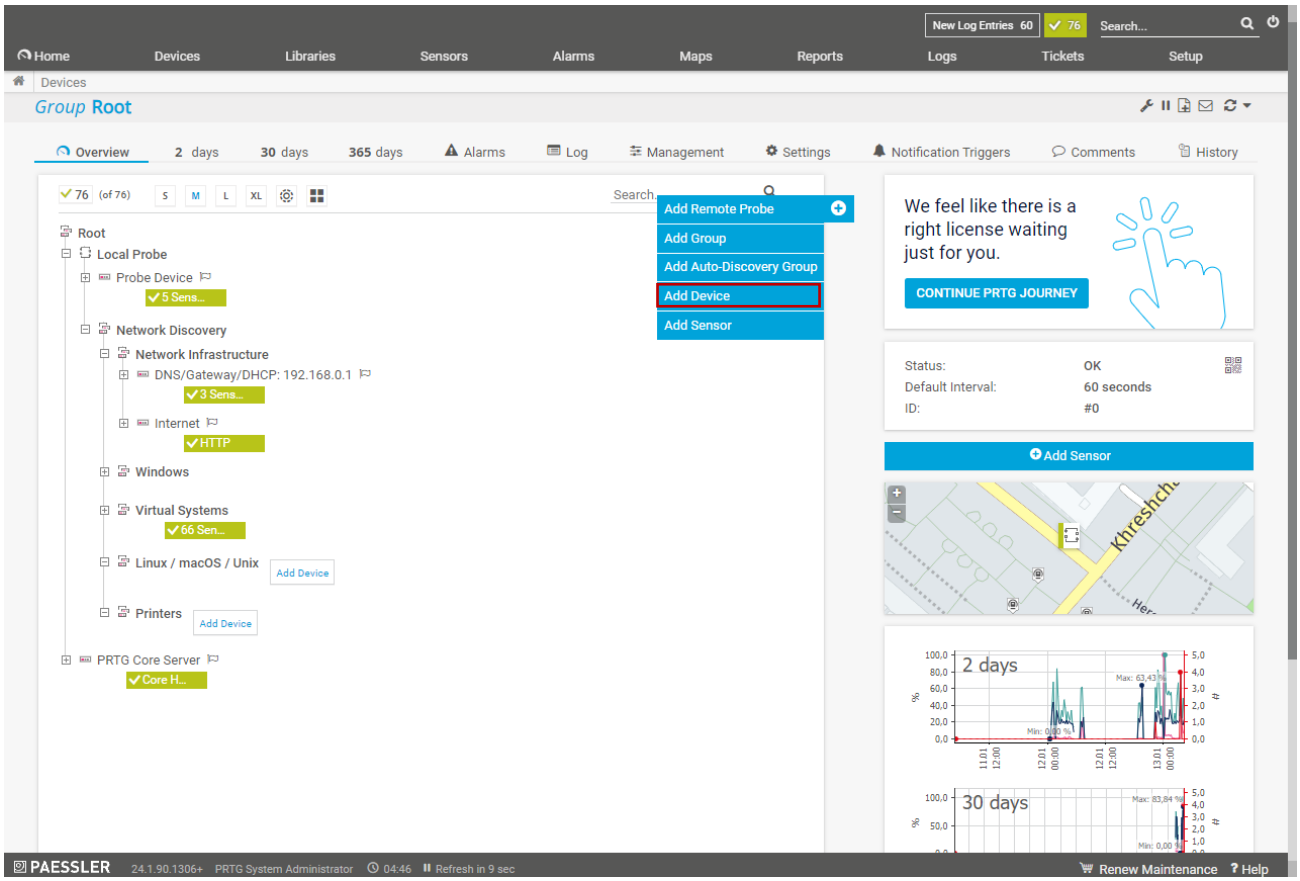


Рисунок 3.2 – Додавання нового пристрою

Налаштування нового пристрою показані на рисунку 3.3.

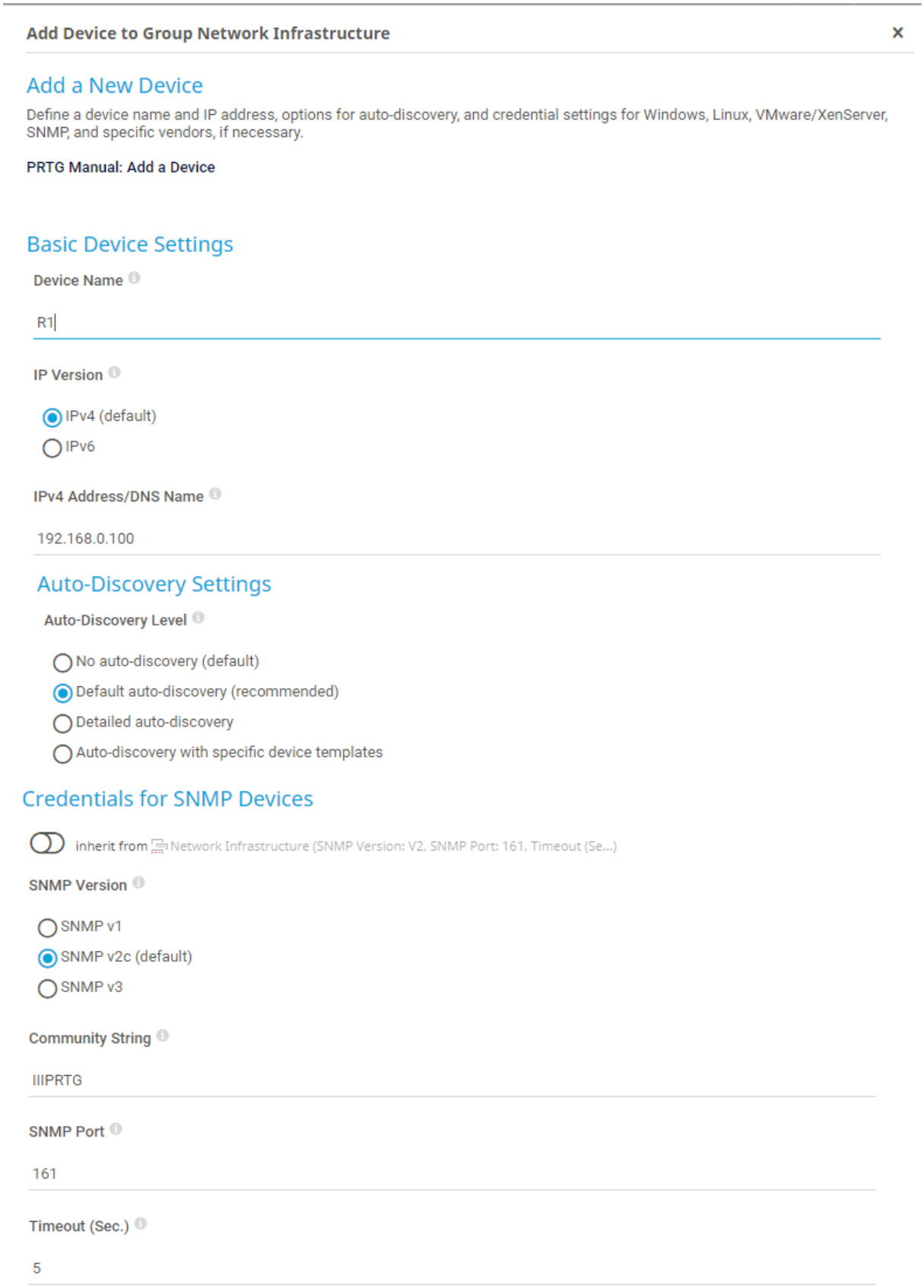


Рисунок 3.3 – Налаштування нового пристрою

Після цього доданий пристрій доступний для моніторингу. За налаштуванням відображаються наступні параметри для моніторингу: ping, моніторинг трафіку портів GigabitEthernet0/0 та 0/1, час безперервної роботи (uptime), завантаженість ЦП, працездатність системи. Також існує можливість встановлення додаткових сенсорів. На рисунку 3.4 показано моніторингові показники маршрутизатора R1.

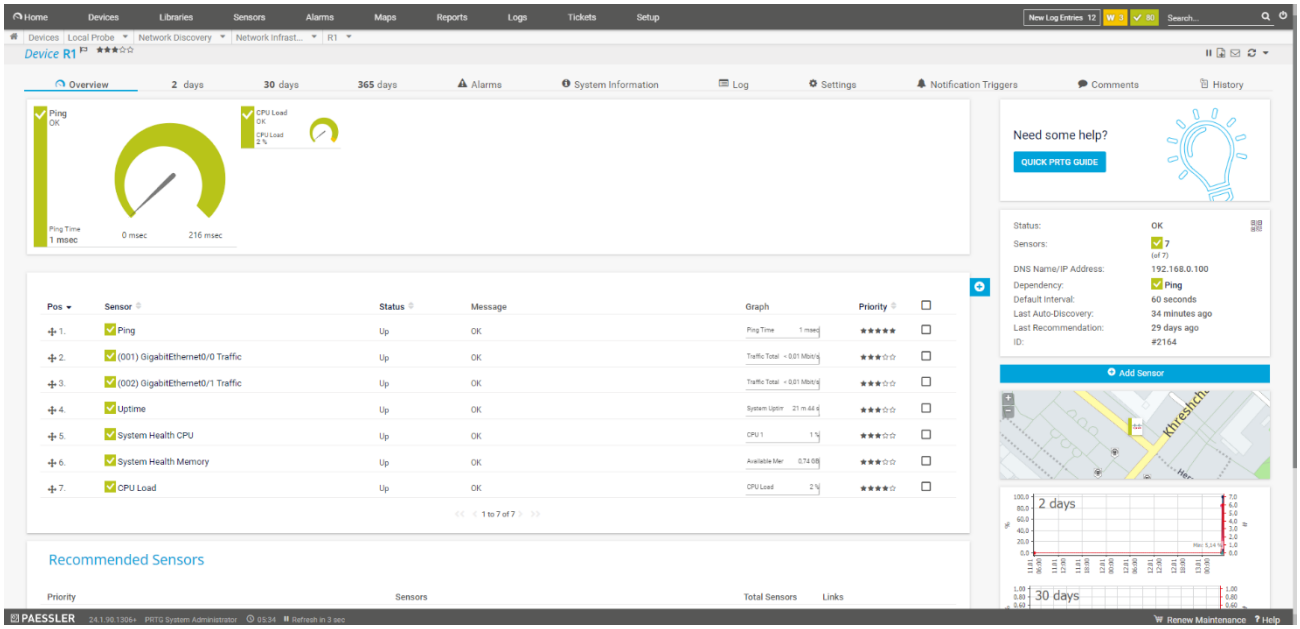


Рисунок 3.4 – Моніторингові показники маршрутизатора R1

Далі необхідно провести перевірку моніторингу мережі, щоб переконатися, що вона працює належним чином. Тестуватися будуть наступні показники моніторинг пропускної здатності, використання ресурсів таких як ЦП та пам’ять, можливості моніторингу в реальному часі за допомогою налаштування оповіщень.

Моніторинг пропускної здатності буде протестовано за допомогою відправлення на інтерфейс ICMP пакетів. На рисунку 3.5 показано початкові значення використання пропускної здатності порту GigabitEthernet0/0.

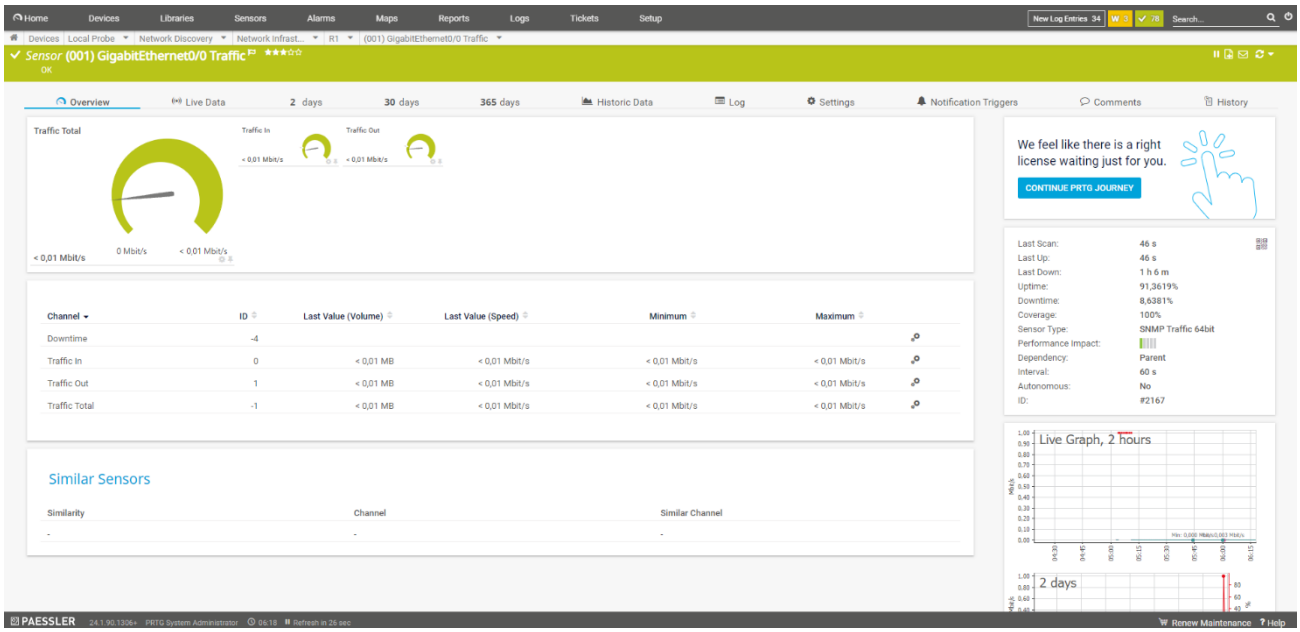


Рисунок 3.5 – Початкові показники використання пропускної здатності порту GigabitEthernet0/0

Після виконання команди ping одночасно з двох пристроїв, використання пропускної здатності помітно зросло з 0,01 Мбіт/с до 0,09 Мбіт/с. На рисунку 3.6 продемонстровані показники використання пропускної здатності порту GigabitEthernet0/0 під час виконання команди ping.

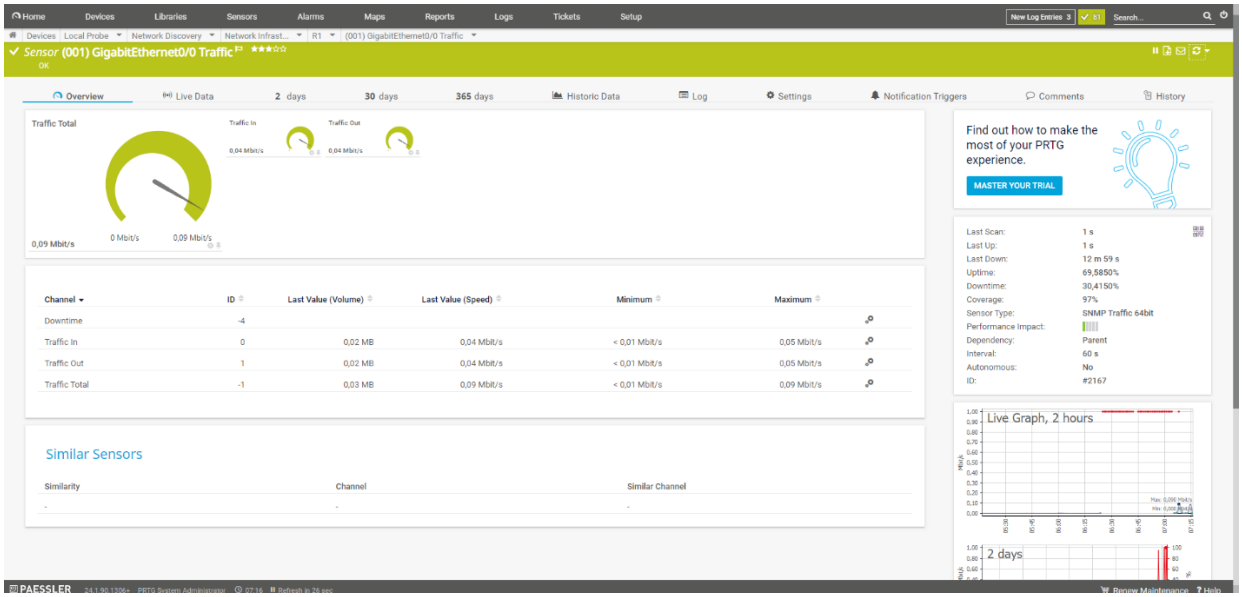


Рисунок 3.6 - Показники використання пропускної здатності порту GigabitEthernet0/0

Моніторинг утилізації ресурсів ЦП буде протестовано за допомогою написання IP SLA тестів, які дозволяють створювати трафік та вимірювати різні параметри мережевої продуктивності. В даному випадку IP SLA тест буде застосовано для генерації трафіку та спостереження за змінами утилізації ЦП на маршрутизаторі Cisco. На рисунку 3.7 показано початкові показники використання ЦП.

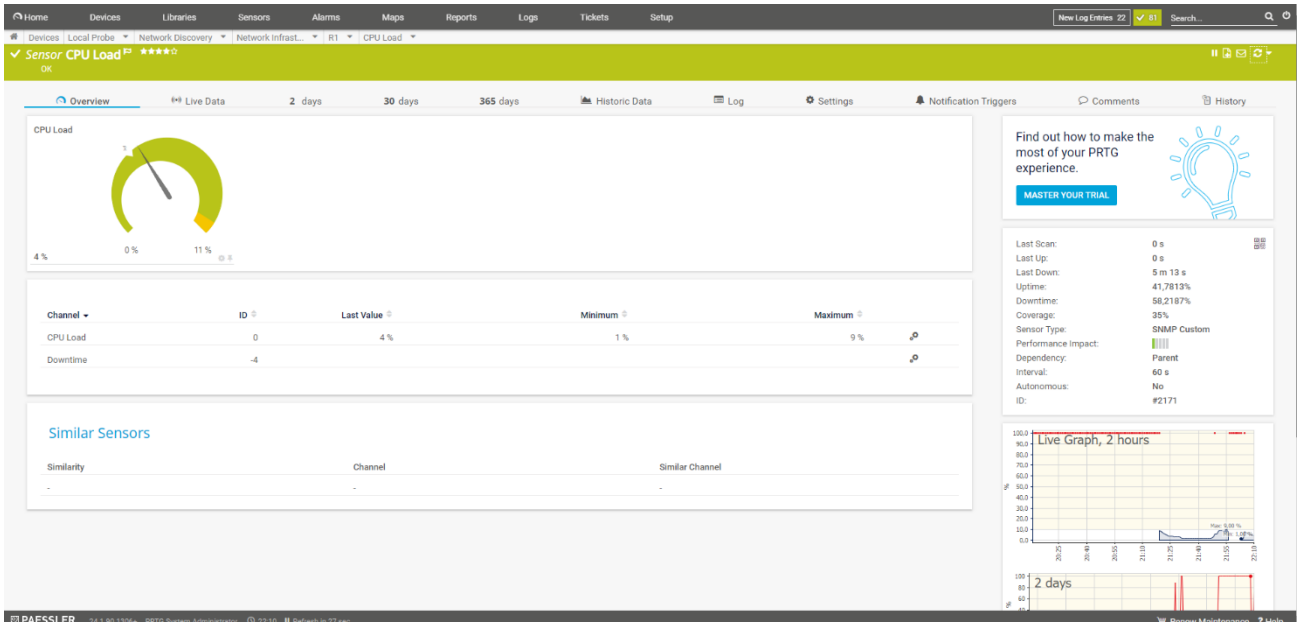


Рисунок 3.7 – Початкові показники використання ЦП

Під час виконання IP SLA тесту, використання ЦП зросло з 4% до 11%, оскільки перед цим було налаштовано, що у разі перевищення навантаження більше ніж 10%, то спрацює попередження. Одночасно, відбувалась фіксація показників використання пам’яті, але суттєвих змін не було виявлено. Демонстрація показників ЦП під час IP SLA тесту на рисунку 3.8. На рисунку 3.9 показано використання пам’яті.

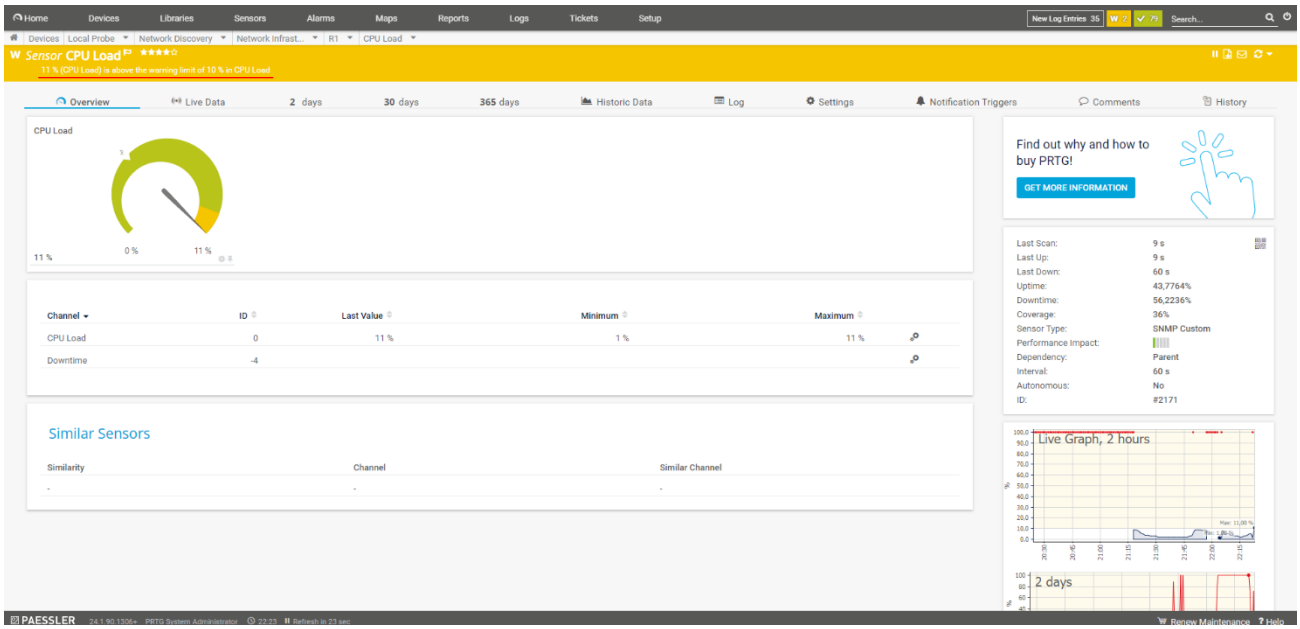


Рисунок 3.8 – Показники ЦП під час виконання IP SLA тесту

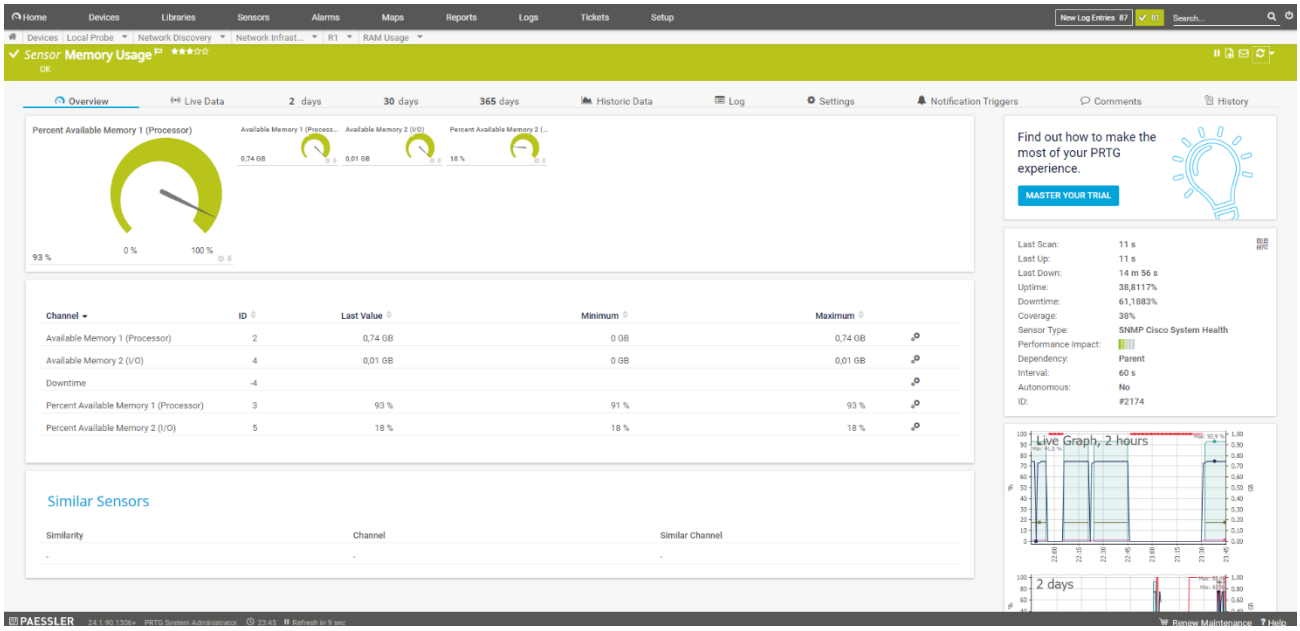


Рисунок 3.9 – Показники використання пам’яті під час виконання IP SLA тесту

У разі припинення роботи маршрутизатора усі датчики моніторингу перестануть отримувати дані та надсилатимуть відповідні повідомлення. На рисунку 3.10 показано статус сенсорів маршрутизатора у випадку припинення його роботи.

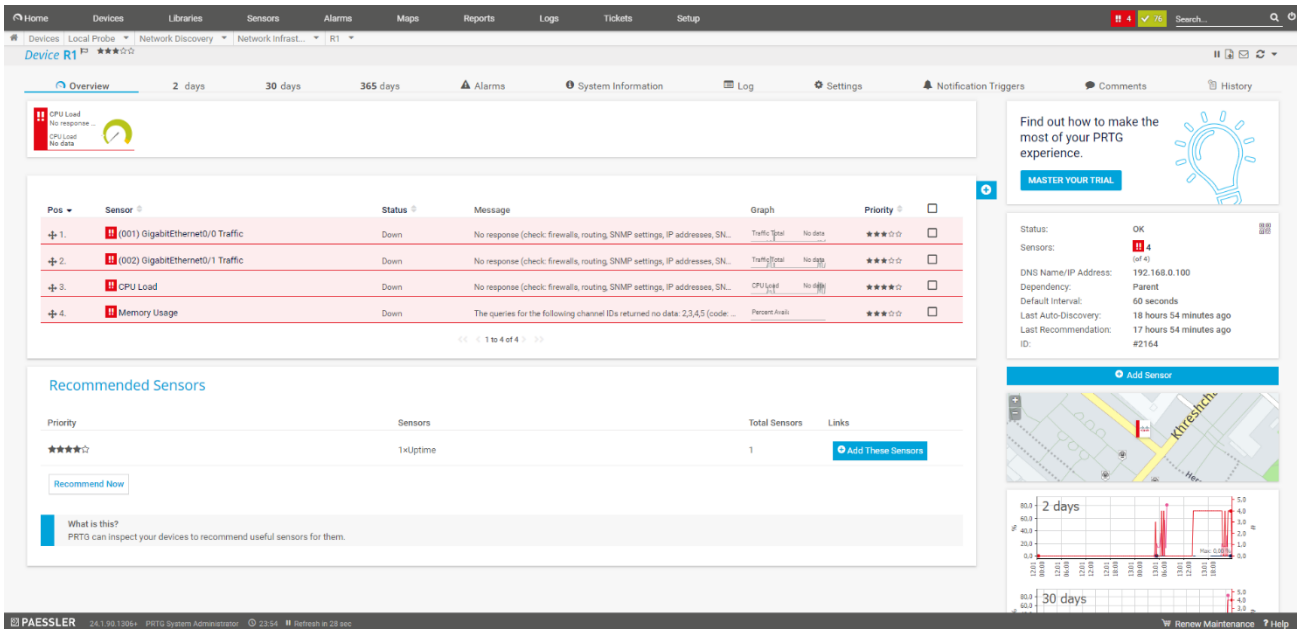


Рисунок 3.10 – Статус датчиків після припинення роботи маршрутизатора

Таким чином, використовуючи емулятор мережі EVE-NG та інтегрувавши його з системою моніторингу Paessler PRTG, надається можливість моніторингу мережі Cisco, використовуючи протокол SNMP. Використовуючи сенсори для моніторингу пропускної здатності, використання ресурсів маршрутизатора таких як ЦП та ОЗП та завдяки налаштованим сповіщенням продемонстрована можливість моніторингу даних показників в режимі реального часу.

ВИСНОВКИ

Магістерська робота включала широке дослідження методів моніторингу мережі Cisco, включаючи пропускну здатність, використання ресурсів та виявлення проблем у реальному часі. Також було проаналізовано існуючі системи моніторингу та їх функціональність по відношенню до мережевої інфраструктури Cisco.

З отриманих результатів можна зробити висновок, що ефективне впровадження систем моніторингу забезпечить стабільну та надійну роботу мережі. Інструменти моніторингу пропускної здатності можуть бути використані для швидкого виявлення та вирішення проблем, пов'язаних з перевантаженням мережевих каналів, що сприяє підвищенню продуктивності та скороченню часу відновлення сервісів.

Системи моніторингу використання ресурсів також вивчалися для ефективного розподілу завдань і оптимізації мережевих обчислювальних ресурсів Cisco. Це стає ключовим фактором забезпечення ефективності та економії ресурсів, що впливає на продуктивність всієї організації.

Також продовжуються дослідження способів виявлення проблем в режимі реального часу, що є важливим аспектом забезпечення безперебійної роботи мережі. Системи виявлення та аналізу можуть бути використані для швидкого реагування на можливі порушення та забезпечення високої надійності та доступності мережевих сервісів.

Загалом отримані результати свідчать про те, що використання сучасних методів моніторингу мережі Cisco має вирішальне значення для стабільності, продуктивності та ефективності інформаційних систем. Щоб максимально підвищити ефективність програмного забезпечення для керування мережею Cisco, рекомендується комплексне рішення, яке включає всі аспекти моніторингу мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Optimize Efficiency with Cisco Network Monitoring Tools [Електронний ресурс]. Режим доступу: https://www.ir.com/guides/optimize-efficiency-cisco-network-monitoring-tools
2. What Is Network Monitoring? [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html
3. Network Monitoring and Tools [Електронний ресурс]. Режим доступу: https://netacad.fit.vutbr.cz/wp-content/uploads/ccna/cyberops/CA_Module_15.pdf
4. TAP vs. SPAN: Which Option is Right for You? [Електронний ресурс]. Режим доступу: https://community.fs.com/article/tap-vs-span-which-option-is-right-for-you.html
5. Network Performance Metrics: 5 Essential Network Metrics to Monitor [Електронний ресурс]. Режим доступу: https://krontech.com/network-performance-metrics-5-essential-network-metrics-to-monitor
6. What are Network Performance Metrics? [Електронний ресурс]. Режим доступу: https://www.solarwinds.com/resources/it-glossary/network-metrics
7. What is Network Monitoring? Third party vs Cisco Network Monitoring Tools [Електронний ресурс]. Режим доступу: https://www.ir.com/blog/communications/cisco-network-monitoring-tools
8. The Importance of Cisco Network Monitoring [Електронний ресурс]. Режим доступу: https://www.ir.com/blog/communications/the-importance-of-cisco-network-monitoring
9. What is Cisco Network Assistant (CNA)? [Електронний ресурс]. Режим доступу: https://networkinterview.com/what-is-cisco-network-assistant-cna/
10. Cisco Network Assistant (CNA) – Configure, Monitor, Troubleshoot & Maintain your Devices [Електронний ресурс]. Режим доступу: https://petri.com/csc_cisco_network_assistant/

11. Cisco Prime Infrastructure Vs Cisco DNA Center [Електронний ресурс]. Режим доступу: https://www.thenetworkdna.com/2021/01/cisco-prime-infrastructure-vs-cisco-dna.html
12. Cisco Prime Infrastructure [Електронний ресурс]. Режим доступу: https://www.secureitstore.com/Prime-Infrastructure.asp
13. Cisco Prime Infrastructure 3.9 User Guide [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-9/user/guide/bk_CiscoPrimeInfrastructure_3_9_0_UserGuide/monitor_device_and_network_health_and_performance.html
14. Cisco DNA Center [Електронний ресурс]. Режим доступу: https://ipcisco.com/lesson/cisco-dna-center/#Effective_Monitoring
15. Cisco DNA Center [Електронний ресурс]. Режим доступу: https://www.linkedin.com/pulse/cisco-dna-center-snell-ondzaghe-mba/
16. IP SLA (Cisco) [Електронний ресурс]. Режим доступу: https://www.techtarget.com/whatis/definition/IP-SLA-Cisco
17. SolarWinds Network Monitoring System [Електронний ресурс]. Режим доступу: https://www.solarwinds.com/network-performance-monitor/use-cases/network-monitoring-system
18. Cisco Network Device Monitoring Software [Електронний ресурс]. Режим доступу: https://www.solarwinds.com/network-performance-monitor/use-cases/cisco-monitoring-analytics?irgwc=1&CMP=BIZ-TAD-PCWDLD-SW_WW_X_X_PPD_LD_EN_0_0-NPM-X_0_X_X_X_X-X
19. SolarWinds Network Performance Monitor (NPM) Review [Електронний ресурс]. Режим доступу: https://www.comparitech.com/net-admin/solarwinds-network-performance-monitor-review/
20. Netflow: Monitor Bandwidth & Network Utilization. Detect LAN, WAN, Wi-Fi Bottlenecks, Unusual Traffic Patterns, Problems And More [Електронний ресурс]. Режим доступу: https://www.firewall.cx/networking/network-protocols/netflow/netflow-monitor-network-bandwidth-application-traffic.html

21. Cisco Bandwidth Monitoring Software [Електронний ресурс]. Режим доступу: https://www.manageengine.com/products/netflow/cisco-bandwidth-monitoring.html#cbm1
22. Overview of Zabbix [Електронний ресурс]. Режим доступу: https://www.zabbix.com/documentation/1.8/en/manual/about/overview_of_zabbix
23. Driving Efficiency and Performance: Zabbix Implementation for Network Monitoring [Електронний ресурс]. Режим доступу: https://blogs.halodoc.io/driving-efficiency-and-performance-halodocs-zabbix-implementation-for-network-monitoring/
24. The Best Cisco Network Monitoring Tools [Електронний ресурс]. Режим доступу: https://www.comparitech.com/net-admin/cisco-network-monitoring-tools/
25. Zabbix Requirements [Електронний ресурс]. Режим доступу: https://www.zabbix.com/documentation/4.0/es/manual/installation/requirements
26. PRTG Manual: Welcome to PRTG [Електронний ресурс]. Режим доступу: https://www.paessler.com/manuals/prtg/welcome_to_prtg
27. PRTG Manual: Key Features [Електронний ресурс]. Режим доступу: https://www.paessler.com/manuals/prtg/key_features
28. Cisco Monitoring [Електронний ресурс]. Режим доступу: https://www.paessler.com/cisco-monitoring
29. Cisco switch monitoring [Електронний ресурс]. Режим доступу: https://www.paessler.com/cisco-switch-monitoring
30. Cisco router monitoring [Електронний ресурс]. Режим доступу: https://www.paessler.com/cisco-router-monitoring

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

Державний університет інформаційно-комунікаційних технологій

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра «Комп'ютерної інженерії»

ДОСЛІДЖЕННЯ МЕТОДІВ МОНІТОРИНГУ МЕРЕЖІ CISCO, ВКЛЮЧАЮЧИ СИСТЕМИ МОНІТОРИНГУ ПРОПУСКНОЇ СПРОМОЖНОСТІ, УТИЛІЗАЦІЇ РЕСУРСІВ ТА ВИЯВЛЕННЯ ПРОБЛЕМ У РЕАЛЬНОМУ ЧАСІ

Виконав: **Лисак В.П.**
Група КСДМ-61

Керівник: **Лащевська Н.О.**, к.т.н., доцент

Об'єкт, предмет, мета, новизна роботи

- Об'єкт дослідження – методи моніторингу мережі Cisco, що охоплює перевірку систем моніторингу пропускної здатності, використання ресурсів і виявлення проблем у реальному часі.
- Предмет дослідження – застосування програмного забезпечення для моніторингу мереж Cisco, з особливою увагою на вимірюванні пропускної спроможності, управлінні використання ресурсів, виявлення та вирішення проблем у режимі реального часу.
- Мета роботи - дослідження сучасних методів та способів моніторингу мережі Cisco.

Наукова новизна та практичне значення

- Наукова новизна та практична значущість отриманих результатів полягає в тому, що здійснено комплексне дослідження методів моніторингу пропускної спроможності, утилізації ресурсів та виявлення проблем в реальному часі у мережах на основі обладнання Cisco. Досліджено інструменти моніторингу мережі Cisco. Реалізовані та впроваджені методи моніторингу, які сприяють оптимізації роботи мережі, забезпечуючи її максимальну продуктивність та надійність.

Актуальність дослідження

- Актуальність роботи визначається за рахунок того, мережеві середовища стають дедалі складнішими, а обсяги передачі даних збільшуються, що вимагає дослідження та впровадження ефективних методів моніторингу для забезпечення надійності, безпеки та оптимальної продуктивності.

Загальний аналіз методів моніторингу мереж

- 1. SNMP (Простий протокол керування мережею)
- *Опис:* SNMP є одним з основних протоколів для моніторингу мережевих пристроїв. Він дозволяє збирати інформацію про стан та параметри пристроїв.
- *Переваги:* Простий у використанні, підтримується багатьма виробниками обладнання.
- *Недоліки:* Обмежений в забезпеченні повного контролю та відсутність механізмів безпеки.

Загальний аналіз методів моніторингу мереж

- 2. Flow-based моніторинг:
- *Опис:* Оцінка трафіку на основі даних про потоки, які передаються через мережу, таких як NetFlow або sFlow.
- *Переваги:* Дозволяє виявляти та аналізувати патерни трафіку, ідентифікувати проблеми у пропускній спроможності.
- *Недоліки:* Потребує підтримки мережевих пристроїв, може вимагати великого обсягу даних.

Метрики моніторингу

- 1. Пропускна спроможність - кількість даних, які можуть бути передані через мережу за певний період часу.
- 2. Утилізація ресурсів - визначає, наскільки ефективно використовуються різні компоненти мережевої інфраструктури. Це включає в себе використання пропускної спроможності, обчислювальних ресурсів, пам'яті, а також інших ресурсів на різних рівнях мережі.
- 3. Затримка - Час, який затрачається на передачу сигналу від відправника до отримувача.

Утилізація ресурсів

- 1. Пропускна спроможність - утилізація пропускної спроможності визначає, наскільки велика частина доступної мережевої пропускної спроможності використовується для передачі даних. Висока утилізація може призвести до перевантаження мережі, зниження продуктивності та збільшення затримок.
- 2. Утилізація мережевих інтерфейсів - вказує на те, наскільки використовуються мережеві інтерфейси на різних пристроях. Дозволяє ідентифікувати перевантажені інтерфейси та розподілити трафік ефективніше.
- 3. Використання CPU та пам’яті - Утилізація центрального процесора (CPU) та оперативної пам'яті визначає, наскільки завантажені ці ресурси на мережевих пристроях. Висока утилізація CPU або пам'яті може вказувати на перевантаження та потенційні проблеми з продуктивністю.

Інструменти моніторингу мережі

- Cisco Prime Infrastructure - інтегрована платформа для моніторингу, управління та оптимізації мережевої інфраструктури Cisco.

1. Моніторинг пропускної спроможності:

- *Можливості:*
  - Відслідковування пропускної спроможності на рівні мережевих інтерфейсів.
  - Графічне відображення та аналіз трафіку мережі.
  - Виявлення змін в пропускній спроможності та адаптація до нових умов.

2. Утилізація ресурсів:

- *Можливості:*
  - Моніторинг використання CPU та пам'яті на мережевих пристроях.
  - Автоматичне сповіщення при досягненні певного рівня утилізації.
  - Глибокий аналіз роботи пристроїв для ідентифікації причин перевантажень.

3. Виявлення проблем у реальному часі:

- *Можливості:*
  - Система оповіщень та журнал подій для виявлення проблем.
  - Миттєва реакція на події та автоматичне виконання зазначених дій.
  - Засоби діагностики для виявлення та вирішення проблем у реальному часі.

Інструменти моніторингу мережі

- Paeesler PRTG - програмне забезпечення моніторингу мережі та систем, що надає великий набір інструментів для вимірювання та аналізу параметрів мережі.

1. Моніторинг пропускної спроможності:

- *Можливості:*
  - Використання сенсорів, таких як SNMP Traffic, NetFlow, або sFlow для точного моніторингу трафіку.
  - Визначення та аналіз пристроїв, які споживають більше пропускної спроможності.
  - Вивчення патернів та прогнозування навантаження на мережу.

2. Утилізація ресурсів:

- *Можливості:*
  - Сенсори для моніторингу використання CPU, пам'яті та інших ресурсів на серверах та мережевих пристроях.
  - Сповіщення при перевищенні заданих порогових значень утилізації.
  - Аналіз історії використання ресурсів для прогнозування їхнього майбутнього навантаження.

3. Виявлення проблем у реальному часі:

- *Можливості:*
  - Система сповіщень, яка негайно реагує на події та проблеми.
  - Автоматичні сценарії відповіді на конкретні ситуації.
  - Графічний інтерфейс для швидкого визначення та аналізу проблем у реальному часі.

Реалізація системи моніторингу за допомогою емулятора мережі EVE-NG та інтеграція з системою моніторингу Paessler PRTG

1. Підготовка інфраструктури:
- Запуск та конфігурація EVE-NG для емуляції мережевого обладнання.
- Створення віртуальних мережевих пристроїв (роутерів, комутаторів) для емуляції реальної мережі.

2. Встановлення та налаштування Paessler PRTG:
- Встановлення сервера Paessler PRTG у віртуальному чи фізичному середовищі.
- Налаштування основних параметрів, таких як IP-адреса та доступи до інтерфейсу.

3. Створення сенсорів у Paessler PRTG:
- Додавання сенсорів, які будуть моніторити віртуальні пристрої в EVE-NG.
- Використання SNMP, NetFlow або інших протоколів для збору даних з емульованих пристроїв.

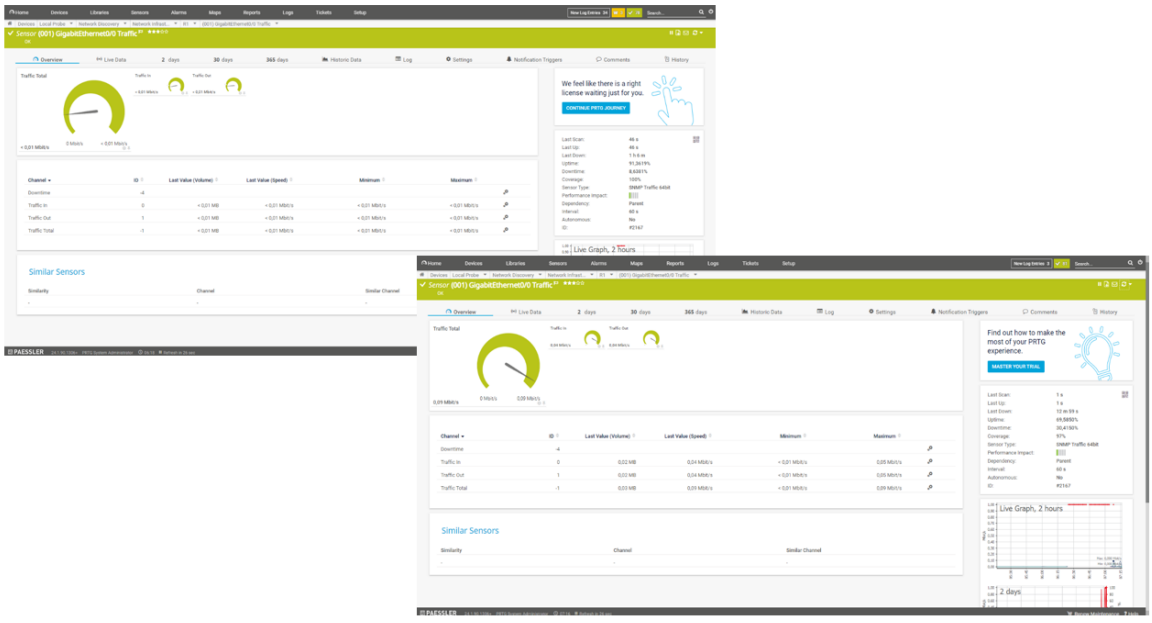
4. Налаштування SNMP на віртуальних пристроях:
- Включення та налаштування SNMP на емульованих маршрутизаторах та комутаторах.
- Визначення параметрів безпеки, таких як community strings.

5. Інтеграція EVE-NG із Paessler PRTG:
- Введення IP-адрес сервера Paessler PRTG у налаштуваннях EVE-NG.
- Вказання Paessler PRTG як сервера моніторингу для емульованих пристроїв.

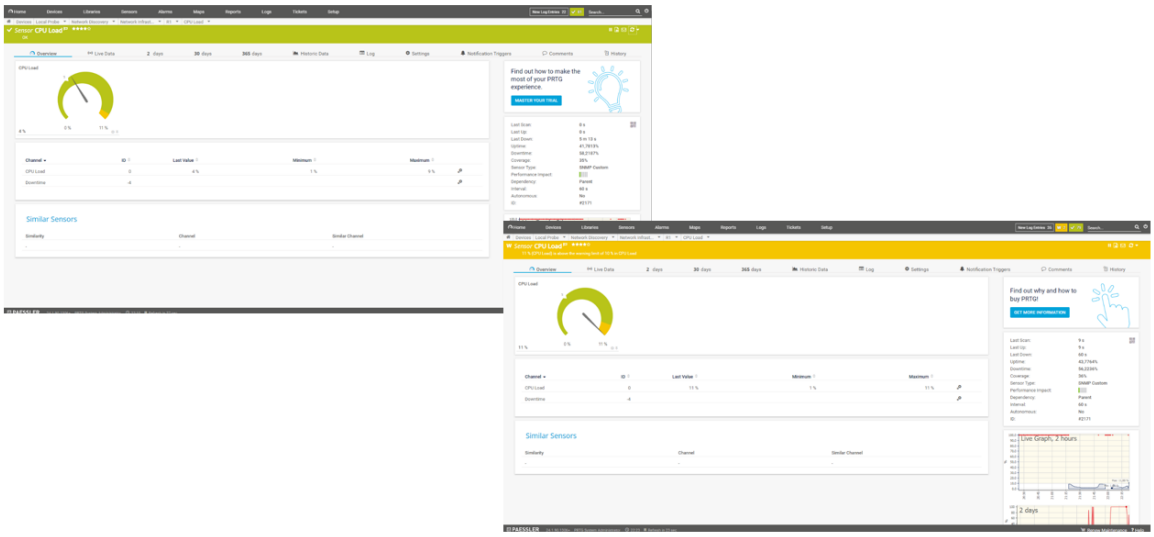
6. Моніторинг та аналіз даних:
- Спостереження за роботою сенсорів в Paessler PRTG для отримання інформації про пропускну спроможність, утилізацію ресурсів та інші параметри.
- Використання графіків та звітів для аналізу та виявлення проблем у мережі.

7. Налаштування сповіщень:
- Налаштування сповіщень в Paessler PRTG для оперативного реагування на проблеми.

Перегляд результатів у PRTG



Перегляд результатів у PRTG



Висновки

- В даній роботі було досліджено методи моніторингу мережі Cisco, включаючи пропускну здатність, використання ресурсів та виявлення проблем у реальному часі. Також було проаналізовано існуючі системи моніторингу та їх функціональність по відношенню до мережевої інфраструктури Cisco.
- EVE-NG забезпечив реалістичне тестування та моделювання робочих умов для мережевого обладнання. Це дозволило ефективно перевіряти функціонал Paessler PRTG та його реакцію на різні сценарії мережевого трафіку та навантаження.
- Дослідження показало, що інтеграція EVE-NG та Paessler PRTG має практичну застосованість у тестуванні, аналізі та управлінні віртуальними та реальними мережами. Цей підхід може бути ефективно використаний для підготовки та оптимізації мережевих інфраструктур у реальних умовах експлуатації.

Список публікацій

- *Апробація результатів роботи*. Результати роботи були апробовані на IV науково-практична конференції «ПРОБЛЕМИ КОМП’ЮТЕРНОЇ ІНЖЕНЕРІЇ», 1 грудня 2023, ДУІКТ, Київ, Україна.
- *Публікації.* Лисак В.П., Катков Ю.І. РОЗРОБЛЕННЯ КЛАСИФІКАЦІЇ ІНСТРУМЕНТІВ СИСТЕМНОГО АДМІНІСТРУВАННЯ СЕРВЕРІВ Державний університет телекомунікацій. Зв'язок. №2, 2022