

ВІДЗІВ НАУКОВОГО КЕРІВНИКА НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ

студента Дмитренка Дениса Олеговича
представлену на здобуття освітнього ступеня бакалавр
зі спеціальності 123 «Комп'ютерна інженерія»

1. Робота виконана на тему „Проект підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP”.

2. Актуальність роботи зумовлено зростанням складності мереж і, як наслідок, утрудненням їх адміністрування, потребою у якісному моніторингу задля своєчасного реагування на проблеми, що виникають.

3. Основний зміст пояснювальної записки роботи викладено на 53 сторінках тексту, пояснювальна записка містить 1 таблицю, 30 ілюстрацій та додатки. Список використаних літературних джерел налічує 20 найменувань. До складу роботи входить реалізований у середовищі моделювання GNS3 проект підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP.

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

Розділ 1 присвячений теоретичним основам організації управління мережею на основі протоколу SNMP. У розділі розглянуто загальні аспекти організації управління мережею, теоретичні основи роботи протоколу SNMP та NETCONF.

Розділ 2 присвячений проектуванню мережі організації на базі протоколу SNMP. У розділі подано проект мережі організації, проект політики безпеки, проект сценаріїв тестування функціоналу безпеки.

Розділ 3 присвячений налагодженню та дослідженню підсистеми управління мережею. Розділ містить базове налагодження пристроїв мережі, налагодження підсистеми управління комп'ютерною мережею організації на базі SNMP, тестування виконаних налаштувань.

5. Висновки містять сумарні результати проведеної роботи.

6. Список використаних літературних джерел має достатній для даного виду робіт обсяг та оформлений загалом правильно.

7. Додатки містять топологію спроектованої мережі.

8. Таблиці та ілюстрації оформлені досить якісно та є інформативними.

9. Якість оформлення роботи є досить високою.

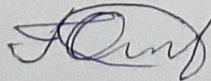
10. Основне зауваження - неповна реалізація студентом адміністрування комп'ютерною мережею організації.

11. Ставлення студента до виконання випускної кваліфікаційної роботи – відносно відповідальне.

12. У цілому у процесі написання випускної кваліфікаційної роботи студент Дмитренко Д. О. виявив необхідні знання, уміння і навички. Також студент Дмитренко Д. О. показав вміння працювати з інформаційними джерелами, здійснювати проектування мереж, оформити свої розробки та напрацювання як випускну кваліфікаційну роботу.

Випускна кваліфікаційна робота студента Дмитренка Д. О. написана на достатньому рівні та може бути допущена до захисту в Екзаменаційній комісії.

Науковий керівник
к.пед.н., доцент кафедри КІ та КБ
26 червня 2020 року



О. С. Головня

РЕЦЕНЗІЯ
на кваліфікаційну роботу
студента 4 курсу групи КІ-2 спеціальності 123 «Комп'ютерна інженерія»
факультету інформаційно-комп'ютерних технологій
Державного університету «Житомирська політехніка»
Дмитренка Дениса Олеговича
на тему: „Проект підсистеми управління комп'ютерною мережею організації
на базі протоколу SNMP”

Кваліфікаційну роботу студента Дмитренка Д. О. “Проект підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP” присвячено актуальній тематиці - розробленню підсистеми управління мережею організації.

Робота містить проект підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP, виконаний у середовищі віртуалізації GNS3. До складу пояснювальної записки входить вступ, три розділи основного тексту, висновки, список використаної літератури та додатки.

У першому розділі пояснювальної записки розглянуто теоретичні основи управління мережею, теоретичні аспекти протоколу SNMP та NETCONF.

У другому розділі пояснювальної записки виконано проектування підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP.

У третьому розділі пояснювальної записки здійснено налаштування пристроїв мережі, налагодження підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP, виконано тестування налаштувань.

Зміст роботи загалом відповідає поставленому завданню. Тему роботи розкрито досить повно. Студентом продемонстровано достатні теоретичні знання та практичні навички. Пояснювальну записку загалом сформовано логічно, науково й технічно грамотно. Функціонал проекту мережі реалізовано майже в повному обсязі.

Позитивний бік роботи полягає у тому, що одержані результати можуть бути застосовані для налаштування реального обладнання мережі та для дослідження аналогічних мереж. Водночас, робота має недоліки, серед яких: неповна реалізація управління спроектованої мережі, відсутність висновків до третього розділу, мовленнєві та стилістичні помилки, недоліки оформлення.

У цілому кваліфікаційна робота студента Дмитренка Дениса Олеговича “Проект підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP” відповідає вимогам рівня вищої освіти “бакалавр” спеціальності 123 “Комп'ютерна інженерія” і рекомендується до захисту в ЕК.

Пропонована оцінка «задовільно»

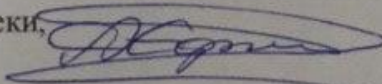
Рецензент:

завідувач кафедри

комп'ютерної інженерії та кібербезпеки,

к. т. н.

26 червня 2020 р.



А. А. Єфіменко

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

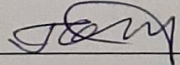
до випускної кваліфікаційної роботи бакалавра
на тему:

«Проект підсистеми управління комп'ютерною мережею
організації на базі протоколу SNMP»

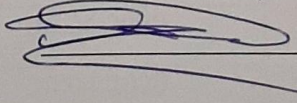
Виконав студент 4-го курсу, групи КІ-2
спеціальності 123 «Комп'ютерна інженерія»

 Дмитренко Д.О.

Керівник, доцент кафедри КІ та КБ, к.пед.н.

 Головня О.С.

Рецензент, завідувач кафедри КІ та КБ, к.т.н.

 Єфіменко А. А.

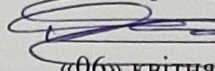
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії

та кібербезпеки

 Єфіменко А. А.

«06» квітня 2020 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента **Дмитренка Дениса Олеговича**

Тема роботи: **Проект підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP**

затверджена Наказом по університету від «06» квітня 2020 р. № 98с

Термін здачі студентом закінченої роботи – **1 червня 2020 р.**

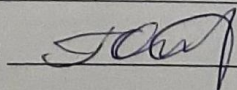
Вихідні дані для роботи:

1. Фізична топологія мережі
2. Маршрутизатори Cisco 7200
3. Комутатори Cisco 2960
4. Операційна система, Windows 7
5. Графічний симулятор мереж GNS3

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Головня О.С.	06.04.2020	06.04.2020
2	Головня О.С.	20.04.2020	20.04.2020
3	Єфіменко А. А.	11.05.2020	11.05.2020

Керівник



Головня О.С.

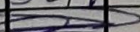
РЕФЕРАТ

Кваліфікаційна робота складається з проекту підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP та пояснювальної записки до нього. Пояснювальна записка до роботи містить 53 сторінки, 30 ілюстрацій та 1 таблиці.

Метою роботи є проект підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP.

В роботі визначено основні завдання на розробку підсистеми, яка забезпечить моніторинг та управління комп'ютерною мережею. Також в роботі проаналізована організація моніторингу периметру мереж на базі SNMP, обґрунтовано актуальність даної системи та описана сфера її використання, обґрунтований вибір виробника обладнання – Cisco. Розроблені, сформовані та налагоджені загальний проект мережі та проект підсистеми управління. Наведено, загальна топологія мережі, опис конкретних серій обладнання, що будуть використані при побудові даного проекту захисту, опис політики функціонування протоколу та тестування проекту. Також наводяться результати тестування підсистеми управління.

КЛЮЧОВІ СЛОВА: SNMP, МЕРЕЖА, NETCONF, CISCO, ПІДСИСТЕМИ УПРАВЛІННЯ, КОМП'ЮТЕРНА МЕРЕЖА.

					КІК.КР.Б – 123 – 20 – ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP Пояснювальна записка	Літ.	Арк.	Аркушів
Розроб.		Дмитренко Д.О.					4	55
Керівник		Головня О.С.				Державний університет «Житомирська політехніка», група КІ-2		
Н. контр		Сфіменко А. А.						
Рецензент		Сфіменко А. А.						
Зав. каф.		Сфіменко А. А.						

ABSTRACT

The qualification work consists of a project for the organization's computer network management subsystem based on the SNMP Protocol and an explanatory note to it. The explanatory note to the work contains 53 pages, 30 illustrations and 1 table.

The purpose of this work is to design a subsystem for managing an organization's computer network based on the SNMP Protocol.

The paper defines the main tasks for the development of a subsystem that will provide monitoring and management of a computer network. The paper also analyzes the organization of network perimeter monitoring based on SNMP, substantiates the relevance of this system and describes the scope of its use, the reasonable choice of the equipment manufacturer – Cisco. A common network project and a management subsystem project have been developed, formed and set up. The General network topology, description of specific hardware series that will be used in the construction of this security project, description of the Protocol functioning and testing of the project are given. The results of testing the control subsystem are also provided.

KEYWORDS: SNMP, NETWORK, NETCONF, CISCO, MANAGEMENT SUBSYSTEMS, COMPUTER NETWORK.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	7
ВСТУП	8
РОЗДІЛ 1. СУЧАСНІ ПРОТОКОЛИ УПРАВЛІННЯ МЕРЕЖЕЮ	10
1.1. ОРГАНІЗАЦІЯ УПРАВЛІННЯ МЕРЕЖЕЮ.....	10
1.2. SIMPLE NETWORK MANAGEMENT PROTOCOL	12
1.3. NETWORK CONFIGURATION PROTOCOL.....	18
ВИСНОВКИ ДО РОЗДІЛУ 1	20
РОЗДІЛ 2. ПРОЕКТ ПІДСИСТЕМИ УПРАВЛІННЯ МЕРЕЖЕЮ.....	21
2.1. ПРОЕКТ МЕРЕЖІ ОРГАНІЗАЦІЇ.....	21
2.2. ПРОЕКТ ПОЛІТИКИ БЕЗПЕКИ.....	26
2.3. ПРОЕКТ СЦЕНАРІЇВ ТЕСТУВАННЯ ФУНКЦІОНАЛУ ПІДСИСТЕМИ	29
ВИСНОВКИ ДО РОЗДІЛУ 2	36
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ УПРАВЛІННЯ МЕРЕЖЕЮ	38
3.1. БАЗОВЕ НАЛАГОДЖЕННЯ ПРИСТРОЇВ МЕРЕЖІ.....	38
3.2. НАЛАГОДЖЕННЯ ПІДСИСТЕМИ УПРАВЛІННЯ КОМП'ЮТЕРНОЮ МЕРЕЖЕЮ ОРГАНІЗАЦІЇ НА БАЗІ ПРОТОКОЛУ SNMP	40
3.3. ТЕСТУВАННЯ НАЛАШТУВАНЬ.	45
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	52
ДОДАТКИ.....	54

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACL – Access Control List

ОС – операційна система

OSI – Open Systems Interconnection

TCP – Transmission Control Protocol

IP – Internet Protocol

LAN – Local Area Network

MAC – Media Access Control

SNMP – Simple Network Management Protocol

NETCONF – Network Configuration Protocol

MIB – Management Information Bases

IETF – Internet Engineering Task Force

ПЗ – програмне забезпечення

ВСТУП

Актуальність теми. Соціальність являється незмінною складовою кожного з нас. Комунікаційні технології та зокрема Інтернет дозволяють нам завжди залишатись на зв'язку з оточуючими. Розвиток глобальної мережі йде з наростаючою швидкістю і в недалекому майбутньому саме вона стане основою усіх комунікаційних мереж. Можливості об'єднаних мереж, що утворюють Інтернет та втілення в життя все нових і нових ідей, які здавалися раніше недосяжними, будуть грати все більш зростаючу роль в реалізації цих проектів.

До основних потреб людини можна віднести спілкування з оточуючими. Використання мереж, як ніколи зв'язує нас один з одним вже не одне десятиліття. Для втілення своїх ідей в життя, ми просто і легко можемо миттєво зв'язуватися з іншими людьми та ділитися ними. За лічені секунди, новини та відкриття стають відомими у всьому світі. Комунікації відкрили безліч можливостей сучасної людини, таких як миттєвий обмін повідомленнями, доступність до мережі з будь-якої точки світу.

Зростання складності мереж ускладнює процес їх адміністрування, який включає в себе такі завдання, як:

- пошук та усунення несправностей апаратної частини;
- установка нових служб і протоколів;
- налаштування програмного забезпечення;
- пошук шляхів оптимізації роботи мережі.

Актуальність обраної теми полягає в тому, що дуже важливим завданням при адмініструванні мереж є своєчасне реагування на виникаючі проблеми та своєчасне їх усунення в мінімально можливі терміни. Для ефективного і оперативного вирішення завдань адміністрування необхідна достовірна інформація про роботу систем мережі та її компонентів. Саме ця інформація може бути зібрана і оброблена, зокрема, за допомогою спеціальних програмних систем моніторингу.

Метою кваліфікаційної роботи є проект підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP.

Встановлена мета обумовлює наступні завдання:

- організація управління мережею;
- вибір засобів реалізації підсистеми;
- перевірка працездатності сервісів та служб, запущених в мережі;
- вибір сучасного технічного забезпечення системи;
- реалізація підсистеми захисту мережі.

Об'єктом дослідження є процес управління комп'ютерною мережею.

Предметом дослідження є засоби і методи використання моніторингу та управління комп'ютерною мережею.

В процесі виконання кваліфікаційної роботи був розроблений проект підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP. При цьому були використані маршрутизатори експертного рівня.

РОЗДІЛ 1. СУЧАСНІ ПРОТОКОЛИ УПРАВЛІННЯ МЕРЕЖЕЮ

1.1. Організація управління мережею

Діяльність сучасних організацій тісно пов'язана з використанням інформаційних технологій, будь то комп'ютер на робочому місці менеджера дрібної фірми або корпоративна мережа великої компанії - системного інтегратора. І чим більше організація та чим важливіше її функції, тим вище вимоги до комп'ютерних систем, які забезпечують виконання даних задач, та тим дорожча ціна кожного збою в роботі. Ефективність діяльності компанії стає все більш і більш залежною від якості роботи її комп'ютерного та телекомунікаційного обладнання.

Особливо гостро постає питання про надійність і максимальну ефективність функціонування обчислювальних мереж. Банки, фінансові, транспортні та телекомунікаційні компанії несуть величезні збитки від мережевих неполадок, що призводять до втрати даних, різкого падіння продуктивності, блокування серверів і інших неприємностей. Отже, особливої актуальності набуває проблема управління мережею.

Управління мережею - це комплекс заходів, спрямований на підвищення ефективності функціонування мережі, виявлення та усунення помилок в її роботі, правильне її розвиток і модернізацію, і скорочення витрат в кінцевому підсумку. Прийнято розділяти функції управління мережею на дві групи:

Управління елементами мережі:

1. Управління конфігурацією:

- реєстрація пристроїв мережі,
- їх мережевих адрес і ідентифікаторів;
- визначення параметрів мережевої операційної системи і опис конфігурації елементів мережі, а також протоколів мережевих взаємодій;
- графічне відображення схеми мережі.

2. Управління безпекою:

					КІК.КР.Б – 123 – 20 – ПЗ	
						10

- контроль доступу і управління повноваженнями користувачів;
- контроль і управління параметрами міжмережевої взаємодії;
- захист від несанкціонованого доступу ззовні;
- управління цілісністю даних (архівуванням і живленням).

3. Управління ресурсами:

- реєстрація ліцензій і облік використання програмних засобів і мережевих ресурсів;
- управління пріоритетами користувачів і прикладних задач.

Управління комунікаціями:

1.Обробка збоїв:

- пошук, виявлення, локалізація і усунення несправностей і помилок;
- попередження і профілактика збоїв;
- спостереження за кабельною системою;
- моніторинг віддалених сегментів і міжмережевих зв'язків.

2.Управління продуктивністю:

- збір та аналіз статистичних даних про функціонування мережі, аналіз трафіку;
- планування та оцінка ефективності використання ресурсів мережі;
- аналіз і інтерпретація протоколів;
- планування розвитку мережі, управління сегментацією.

В даний час для управління мережами використовуються програми, що працюють на базі платформ мережевого управління, таких як системи HP OpenView фірми Hewlett-Packard, NetView for AIX (IBM), SunNet Manager (Sun), Spectrum (Cabletron Systems), NetWare Management Systems (Novell) та інші різноманітні крос-платформні засоби управління. В основі цих засобів лежить використання протоколу SNMP (Simple Network Management Protocol). Протокол SNMP призначений для збору і передачі службової інформації (status information) між різними комп'ютерами.

1.2. Simple Network Management Protocol

SNMP - це протокол прикладного рівня, розроблений для стека TCP/IP, хоча є його реалізації і для інших стеків, наприклад IPX/SPX. Він використовується для отримання від мережевих пристроїв інформації про їх статус, продуктивності і інших характеристиках, які зберігаються в базі даних керуючої інформації MIB (Management Information Base). Простота SNMP багато в чому визначається простотою SNMP MIB, особливо їх перших версій MIB I і MIB II. Крім того, сам протокол також досить нескладний.

Агент в протоколі SNMP - це обробний елемент, який забезпечує менеджерам, розміщеним на керуючих станціях мережі, доступ до значеннями змінних MIB і тим самим дає їм можливість реалізовувати функції з управління і спостереження за пристроєм.

Основні операції з управління винесені в менеджер, а агент SNMP виконує найчастіше пасивну роль, передаючи в менеджер по його запиті значення накопичених статистичних змінних. При цьому пристрій працює з мінімальними витратами на підтримання керуючого протоколу. Воно використовує майже всю свою обчислювальну потужність для виконання своїх основних функцій маршрутизатора, мосту або концентратора, а агент займається збором статистики і значень змінних стану пристрої та передачею їх менеджеру системи управління.

SNMP - це протокол типу «запит-відповідь», тобто на кожен запит, що надійшов від менеджера, агент повинен передати відповідь. Особливістю протоколу є його надзвичайна простота - він включає в себе лише кілька команд.

Команда Get-request використовується для отримання менеджером від агента значення якого-небудь об'єкта за його імені.

Команда GetNext-request використовується менеджером для вилучення значення наступного об'єкта (без зазначення його імені) при послідовному перегляді таблиці об'єктів.

З допомогою команди Get-response SNMP агент передає менеджеру відповідь на команди Get-request або GetNext-request.

Команда Set використовується для зміни менеджером значення будь-якого об'єкта. За допомогою команди Set відбувається власне управління пристроєм. Агент повинен розуміти сенс значень об'єкта, який використовується для управління пристроєм, і на підставі цих значень виконувати реальне керуючий вплив - відключити порт, приписати порт певною VLAN і т. п. Команда Set придатна також для установки умови, при виконання якого SNMP агент повинен надіслати відповідне менеджеру повідомлення. Може бути визначена реакція на такі події, як ініціалізація агента, рестарт агента, обрив зв'язку, відновлення зв'язку, невірна аутентифікація і втрата найближчого маршрутизатора. Якщо відбувається будь-яке з цих подій, то агент ініціалізує переривання.

Команда Trap використовується агентом для повідомлення менеджеру про виникнення особливої ситуації.

Версія SNMP v.2 додає до цього набору команду GetBulk, яка дозволяє менеджеру отримати кілька значень змінних за один запит.

В системах управління, побудованих на основі протоколу SNMP, стандартизуються наступні елементи:

- протокол взаємодії агента і менеджера;
- мова опису моделей MIB і повідомлень SNMP - мова абстрактної синтаксичної нотації ASN.1 (стандарт ISO 8824:1987, рекомендації ITU-T X.208);
- кілька конкретних моделей MIB (MIB-I, MIB-II, RMON, RMON 2), імена об'єктів яких реєструються в дереві стандартів ISO. Все інше віддається на відкуп розробнику системи управління. Протокол SNMP і тісно пов'язана з ним концепція SNMP MIB були розроблені для управління маршрутизаторами Internet як тимчасове рішення. Але, як це часто буває з усім тимчасовим, простота і ефективність рішення забезпечили успіх цього протоколу, і сьогодні він використовується при управлінні практично будь-якими видами обладнання та програмного забезпечення обчислювальних мереж. І хоча в області

управління телекомунікаційними мережами спостерігається стійка тенденція застосування стандартів ITU-T, в які входить протокол CMIP, і тут є досить багато прикладів успішного використання SNMP-управління. Агенти SNMP вбудовуються в аналогові модеми, модеми ADSL, комутатори ATM і т. д.

Формат повідомлень SNMP

Протокол SNMP обслуговує передачу даних між агентами і станцією, що управляє мережею. SNMP використовує транспортний дейтаграммний протокол UDP, не забезпечує надійної доставки повідомлень. Протокол, який організовує надійну передачу дейтаграм на основі з'єднань TCP, дуже завантажує керовані пристрої, які на момент розробки протоколу SNMP були не дуже потужні, тому від послуг протоколу TCP вирішили відмовитися.

SNMP часто розглядають тільки як рішення для управління мережами TCP/IP. Хоча SNMP найчастіше і працює над UDP (він може також працювати і над TCP), він може працювати і над транспортними мережними протоколами стека OSI - TPO, TP4, CNLS, а також над протоколами MAC - рівня. Зростає підтримка протоколу SNMP і в інших транспортних середовищах. Наприклад, фірма Novell почала підтримувати протокол SNMP з версії NetWare 3.11, а деякі виробники обладнання (наприклад, Bay Networks) реалізують у своїх пристроях передачу повідомлень SNMP за допомогою як IP, так і IPX.

Повідомлення SNMP, на відміну від багатьох інших повідомлень комунікаційних протоколів, не мають заголовків з фіксованими полями. Згідно з нотацією ASN.1, повідомлення SNMP складається з довільної кількості полів, перед кожним полем вказується його тип і розмір.

Будь-яке повідомлення SNMP складається з трьох основних частин: версії протоколу (version), ідентифікатора спільноти (community), що використовується для групування пристроїв, керованих певним менеджером, і області даних, в якій власне і містяться описані вище команди протоколу, імена об'єктів і їх значення. Область даних ділиться на блоки даних протоколу (Protocol Data Unit, PDU).

Контроль роботи мережі. Моніторинг і аналіз локальних мереж.

Постійний контроль за роботою локальної мережі, необхідний для підтримання її в працездатному стані.

Контроль - це необхідний перший етап, який повинен виконуватися при управлінні мережею. Зважаючи на важливість цієї функції її часто відокремлюють від інших функцій систем управління і реалізують спеціальними засобами. Такий поділ функцій контролю і власне управління корисно для невеликих і середніх мереж, для яких встановлення інтегрованої системи управління економічно недоцільна. Використання автономних засобів контролю допомагає адміністратору мережі виявити проблемні ділянки та пристрої мережі, а їх відключення або реконфігурацію він може виконувати у цьому випадку вручну.

Процес контролю роботи мережі зазвичай ділять на два етапи - моніторинг і аналіз.

На етапі моніторингу виконується більш проста процедура - процедура збору первинних даних про роботу мережі: статистики про кількість інформації, що циркулює в мережі, кадрів і пакетів різних протоколів, стан портів концентраторів, комутаторів і маршрутизаторів і т. п.

Далі виконується етап аналізу, під яким розуміється більш складний і інтелектуальний процес осмислення зібраної на етапі моніторингу інформації, співставлення її з даними, отриманими раніше, та вироблення припущень про можливі причини сповільненої або ненадійної роботи мережі.

Завдання моніторингу вирішуються програмними і апаратними вимірниками, тестерами, мережними аналізаторами, вбудованими засобами моніторингу комунікаційних пристроїв, а також агентами систем управління. Завдання аналізу вимагає більш активної участі людини і використання таких складних засобів, як експертні системи, які акумулюють практичний досвід багатьох мережеских фахівців.

Все різноманіття засобів, що застосовуються для аналізу та діагностики обчислювальних мереж, можна розділити на декілька великих класів.

– Агенти систем управління, що підтримують функції однією з стандартних MIB і постачають інформацію по протоколу SNMP або CMIP. Для отримання даних від агентів зазвичай потрібна наявність системи управління, що збирає дані від агентів автоматичному режимі.

– Вбудовані системи діагностики і управління (Embedded systems). Ці системи виконуються у вигляді програмно-апаратних модулів, встановлюються в комунікаційне обладнання, а також у вигляді програмних модулів, вбудованих в операційні системи. Вони виконують функції діагностики і управління тільки одним пристроєм, і в цьому їх основна відмінність від централізованих систем управління. Прикладом засобів цього класу може служити модуль управління мультисегментним повторювачем Ethernet, що реалізує функції автосегментації портів при виявленні несправностей, приписування портів внутрішніми сегментами повторювача і деякі інші. Як правило, вбудовані модулі управління «за сумісництвом» виконують роль SNMP-агентів, які постачають дані про стан пристрою для систем управління.

– Аналізатори протоколів (Protocol analyzers). Представляють собою програмні або апаратно-програмні системи, які обмежуються, на відміну від систем управління лише функціями моніторингу і аналізу трафіку у мережах. Хороший аналізатор протоколів може захоплювати і декодувати пакети великої кількості протоколів, що застосовуються в мережах, - зазвичай кілька десятків. Аналізатори протоколів дозволяють встановити деякі логічні умови для захоплення окремих пакетів і виконують повне декодування захоплених пакетів, тобто показують в зручній для фахівця формі вкладеність пакетів різних протоколів рівнів один в одного з розшифровкою змісту окремих полів кожного пакета.

– Експертні системи. Цей вид систем акумулює знання технічних фахівців про виявлення причин аномальної роботи мереж і можливі способи приведення мережі в працездатний стан. Експертні системи часто реалізуються у вигляді окремих підсистем різних засобів моніторингу та аналізу мереж: систем управління мережами, аналізаторів протоколів, мережевих аналізаторів.

Найпростішим варіантом експертної системи є контекстно-залежна система допомоги. Більш складні експертні системи являють собою, так звані бази знань, що володіють елементами штучного інтелекту. Прикладами таких систем є експертні системи, вбудовані в систему управління Spectrum компанії Cabletron і аналізатора протоколів Sniffer компанії Network General. Робота експертних систем полягає в аналізі великої кількості подій, та видачі користувачу звіту про причини несправності мережі.

- Обладнання для діагностики і сертифікації кабельних систем. Умовно це устаткування можна поділити на чотири основні групи: мережеві монітори, прилади для сертифікації кабельних систем, кабельні сканери і тестери.

- Мережеві монітори (звані також мережевими аналізаторами) призначені для тестування кабелів різних категорій. Мережеві монітори збирають також дані про статистичних показники трафіку - середньої інтенсивності загального трафіку мережі, середньої інтенсивності потоку пакетів з певним типом помилки і т. п. Ці пристрої є найбільш інтелектуальними пристроями з усіх чотирьох груп пристроїв даного класу, оскільки працюють не тільки на фізичному, але і на канальному, а іноді і на мережевому рівнях.

- Пристрої для сертифікації кабельних систем виконують сертифікацію згідно з вимогами одного з міжнародних стандартів на кабельні системи.

- Кабельні сканери використовуються для діагностики мідних кабельних систем.

- Тестери призначені для перевірки кабелів на відсутність фізичного розриву.

- Багатофункціональні портативні пристрої аналізу і діагностики. У зв'язку з розвитком технології великих інтегральних схем з'явилася можливість виробництва портативних приладів, які поєднували функції декількох пристроїв: кабельних сканерів, мережевих моніторів і аналізаторів протоколів.

1.3. Network configuration protocol

В кінці 80-х IETF розробив SNMP, який став дуже популярним. Незважаючи на те, що SNMP надавав можливість конфігурування пристроїв, цим протоколом користувалися за великим рахунком для моніторингу мереж. У 2002 році Рада по архітектурі Інтернету і ключові члени IETF-спільноти об'єдналися з операторами зв'язку, щоб обговорити цю ситуацію. Результати обговорення опубліковані в RFC 3535. На той момент оператори зв'язку використовували пропрієтарний командний інтерфейс для конфігурування пристроїв. Інтерфейс мав безліч зручностей, на відміну від SNMP. До того ж, багато виробників не дозволяли повністю конфігурувати свої пристрої через SNMP. Мережеві інженери в основному писали сценарії, які допомагали їм управляти пристроями, однак, командний інтерфейс в цьому випадку є причиною багатьох труднощів. Найбільш значущою з яких є непередбачуваність висновку, що формується мережевим пристроєм. Вміст і форматування виводу має схильність до змін у не завжди потрібний бік.

У той же час компанія Juniper Networks використовувала засновану на XML конфігурацію. Це було запропоновано в IETF і поширено серед спільноти.

Ці два факти послужили причиною створення протоколу, який задовольняв би вимогам як мережевих операторів і постачальників обладнання.

Мережний протокол конфігурації, NETCONF, є протоколом мережного управління пристроями. Він був розроблений в рамках робочої групи NETCONF і вперше опублікований в RFC 4741, який був перероблений в RFC 6241 в червні 2011.

NETCONF надає механізми установки, управління і видалення конфігурації мережевих пристроїв за допомогою віддаленого виклику процедур (RPC. NETCONF використовує XML як засіб надання конфігурації і як засіб формування повідомлень протоколу, який реалізується поверх транспортного.

Базова функціональність NETCONF може бути розширена за допомогою доповнень. При установці сесії клієнт і сервер обмінюються один з одним інформацією про встановлені розширення.

Основною особливістю протоколу NETCONF є те, що функціональність протоколу керування досить точно відображає функціональність самого пристрою. Це знижує витрати на реалізацію і забезпечує своєчасний доступ до нових можливостей. Крім того, програми можуть отримувати доступ до семантичного і синтаксичного вмісту природного інтерфейсу керування пристроєм.

Можливість передплати та отримання асинхронних повідомлень опублікована в RFC 5277. Вона визначає запит типу <create-subscription>, який включає можливість підписки на повідомлення реального часу. У свою чергу повідомлення відправляються за допомогою інструкції <notification>. RFC також визначає можливість: interleave, яка спільно з: notification допомагає обробляти різні NETCONF запити під час включеної підписки.

NETCONF використовує комунікаційну парадигму на основі RPC. Клієнт відправляє серію з одного або декількох повідомлень запиту RPC до сервера, який дає відповідь серією RPC-відповідей.

Протокол NETCONF може бути накладено на будь-транспортний протокол, який надає необхідний набір функціональних можливостей. Він не прив'язаний до жодного з певних транспортних протоколів, але може бути реалізований за будь-якого з них.

У даний момент робоча група працює над підтримкою повідомлень, що дозволяють обмінюватися шаблонами (XML Schema, Relax NG, etc.), які визначають дерево NETCONF.

Висновки до розділу 1

В результаті аналізу протоколів управління мережею було розглянуто 2 протоколи – SNMP та NETCONF. Також, проведено пошук детальної інформації по дієздатності даних протоколів, та досліджено переваги, які вони надають.

РОЗДІЛ 2. ПРОЕКТ ПІДСИСТЕМИ УПРАВЛІННЯ МЕРЕЖЕЮ

2.1. Проект мережі організації

В даній роботі була розглянута мережа організації, що представлена одним офісом. Офіс складається з робочих станцій, п'яти комутаторів, та п'яти маршрутизаторів. Також є можливість збільшувати кількість кінцевих пристроїв за рахунок підключення до вільних портів комутаторів.

Для підключення пристроїв мережі між собою використовуються високошвидкісні порти FastEthernet. Дані порти відрізняються від інших своєю пропускною здатністю в 100 Мбіт/сек, що є досить високою швидкістю пропускання навіть для сучасних мереж.

Таблиця 2.1

Параметри інтерфейсів пристроїв

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Маршрутизатор R2	Fa0/1	Комутатор IOU1	E0/1
	Fa0/0	Комутатор IOU2	E0/0
Маршрутизатор R3	Fa0/1	Комутатор IOU3	E0/0
	Fa0/0	Маршрутизатор R4	Fa0/1
Маршрутизатор R4	Fa0/0	Комутатор IOU4	E0/0
	Fa1/0	Маршрутизатор R1	Fa1/0
	Fa2/0	Комутатор IOU2	E0/2
	Fa0/1	Маршрутизатор R3	E0/0
Маршрутизатор R1	Fa1/0	Маршрутизатор R4	Fa1/0
	Fa0/0	Комутатор IOU2	E0/1
	Fa0/1	Маршрутизатор R5	Fa0/0
Маршрутизатор R5	Fa0/0	Маршрутизатор R1	Fa0/1
	Fa0/1	Комутатор IOU5	E0/0
Комутатор IOU1	E0/2	Робоча станція Win7-1	E0
	E0/0	Робоча станція Pc2	E0
	E0/1	Маршрутизатор R2	Fa0/1

Продовження таблиці 2.1

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Комутатор IOU2	E0/0	Маршрутизатор R2	Fa0/0
	E0/1	Маршрутизатор R1	Fa0/0
	E0/2	Маршрутизатор R4	Fa2/0
Комутатор IOU3	E0/0	Маршрутизатор R3	Fa0/1
	E0/1	Робоча станція Pc3	E0
Комутатор IOU4	E0/0	Маршрутизатор R4	Fa0/0
	E0/1	Робоча станція Pc4	E0
Комутатор IOU5	E0/0	Маршрутизатор R5	Fa0/1
	E0/1	Робоча станція Pc1	E0

Для забезпечення функціонування даної мережі організації було обрано оптимальні маршрутизатори і комутатори корпорації Cisco, котрі мають адаптованість під модернізацію модулями.

Так як доступу до реального обладнання немає, то мережа розробляється в графічному симуляторі. Через це, конкретні моделі пристроїв назвати важко. Тому нижче охарактеризовані серії пристроїв, які були використані для побудови мережі.

Маршрутизація мережі побудована на базі маршрутизатора Cisco з серії 7200.

Маршрутизатори Cisco 7200 Series є найбільш розповсюдженими універсальними рішеннями для агрегації сервісів – значна кількість компаній довірили свій мережевий інтерфейс цим пристроям. Дана серія маршрутизаторів має велику кількість інтерфейсів, тому активно використовується не тільки підприємствами-початківцями, але і великими компаніями, адже від цього значною мірою буде залежати майбутній розвиток офісу підприємства.

Завдяки високій продуктивності, маршрутизатори здатні відправляти дані в кілька потоків, а отже, такий прийом передачі сприяє підвищенню швидкості обміну інформацією. Це досягається за рахунок чіпів Cisco 7200 NPE-G2. Даний процесор допомагає створити мережну платформу, здатну не тільки швидко

передавати дані, але й справлятися із завантаженістю на каналах передачі. У разі її виникнення, в дію приходить магістральна передача інформації, яка допомагає відправити надлишок пакетів протягом короткого періоду часу. Також на вибір на користь даних пристроїв впливає широкий набір підтримуваних з'єднань, легкість в управлінні та обслуговуванні, та збільшена гнучкість і масштабованість завдяки новій карті адаптера портів.

Спільно з чіпами Cisco 7200 NPE-G2 створюється мережева платформа, здатна не тільки швидко передавати дані, але також і справлятися із завантаженістю на каналах передачі. У таких випадках включається Магістральна передача інформації, яка допомагає відправити надлишок пакетів протягом короткого періоду. Якщо врахувати яку кількість пакетів відправляється в секунду, то можна зрозуміти, що даний продукт повністю виправдовує вкладені інвестиції. Лінійка маршрутизаторів серії 7200 оснащена новою функцією IP / MPLS. Вона дозволяє користувачеві використовувати широкосмугову комутацію, постійний доступ, а також агрегацію всіх підключень. Залежно від складності проектів адміністратор може сам підбирати прийнятний для виконання завдань інтерфейс. Початковий рівень завдання буде використовувати інтерфейс DS 0, а в міру розвитку користувач сам повинен підбирати підходящий варіант роботи. Сімейство маршрутизаторів Series 7200 підтримує термінацію PPP і L2TP , а також 16 тисяч абонентських сесій. Маршрутизатор Cisco 7201 підтримує ряд додатків, важливих для безпеки і відмовостійкості комунікації. Для безперебійної роботи використовуються здвоєні джерела струму, а в разі збою обладнання спрацьовує вбудована сигналізація. В системі існують монітори оточення для коригування дій перед відключенням, а також є можливість вилучення та інсталяції адаптерів в режимі онлайн.

Стосовно Cisco Catalyst серії 2960, то це лінійка мережевого обладнання, що підтримує передачу найпопулярніших типів інформації, в тому числі відео та голос. Продукти даної серії відповідають сучасним нормам і використовуються багатьма компаніями, як засіб для передачі всіх типів інформації. Багато

підприємств останнім часом стали використовувати бездротові мережі, оскільки такий тип передачі інформації істотно полегшує роботу підприємства, скорочує витрати на дроти, а також залишає багато вільного місця в робочому офісі. Комутатори серії Cisco 2960 відрізняються своїми "інтелектуальними" можливостями. Користувачеві в першу чергу необхідно вказати темпи, а також важливі пріоритети, тип передачі інформації і швидкість виконання всіх операцій. Звичайно, при виконанні складних завдань продуктивність даних комутаторів може скорочуватися, але за рахунок впроваджених технологій система швидко справляється з великим навантаженням.

Саме Cisco Catalyst 2960 можуть використовуватися в різних типах зв'язку, тобто, підтримуються, як провідна мережа, так і бездротова, тому ці продукти отримали таке широке поширення.

Для комутації мережі доречно використовувати сімейство комутаторів Cisco Catalyst 2960. Це сімейство фіксованої конфігурації з великою різноманітністю моделей для організації рівня доступу локальної мережі (безпосереднє підключення комп'ютерів/робочих станцій/мережевих принтерів).

У лінійці представлені моделі на 8, 24 або 48 портів 10/100 Ethernet + 2-4 порти Fast Ethernet. Для живлення IP-телефонів, або бездротових точок доступу, порти комутаторів оснащені технологією PoE (Power over Ethernet). Також наявна підтримка надлишкового модуля живлення Cisco Redundant Power System 2300.

Серед можливостей комутаторів даної лінійки виділяють можливість регулювати швидкість передачі на кожному інтерфейсі з кроком в 64 Кбіт/с, підтримку об'єднання портів (Link Aggregation) для організації більш швидкісних з'єднань між комутаторами і серверами та можливість організації транкових з'єднань на кожному інтерфейсі за допомогою тегів 802.1q.

Майже всі серії Cisco Catalyst 2960 не підтримують маршрутизацію, натомість, вміють фільтрувати трафік, ґрунтуючись на інформації 3-го рівня – IP. Комутатори володіють можливістю стекування, починаючи від серії Cisco Catalyst 2960S.

					КІК.КР.Б – 123 – 20 – ПЗ	
						24

Не так давно Cisco представила нову серію комутаторів Cisco Catalyst 2960-X/XR в даному сімействі. Оновлену серію розробники наділили відмінними технічними характеристиками, зробивши її більш продуктивною та інтелектуальною, а також приділили велику увагу «зеленим» технологіям.

Ця серія прийшла на зміну серії Catalyst 2960-S/SF, яка на сьогоднішній день є однією з найпоширеніших і широко використовуваної серій комутаторів в світі. Апаратна платформа 2960-S/SF дозволяє за допомогою технології FlexStack організувати стек комутаторів на швидкості 40 гбіт/с, достатню для об'єднання чотирьох комутаторів. У серії 2960-X інженери Cisco домоглися майже дворазового поліпшення показників платформи 2960-S і додали ряд опцій, що дозволяють поліпшити безпеку, забезпечити простоту впровадження та обслуговування. При цьому стекування серії 2960-X можливо з серією 2960-S. Таким чином, сумісність комутаторів 2960-X і 2960-S/SF при роботі в стеці дозволяє домогтися додаткового захисту інвестицій за рахунок зворотної сумісності і можливості міграції між серіями.

Комутатори Cisco Catalyst 2960-XR виділені в особливу групу і наділені наступними додатковими можливостями:

- можливість установки другого блоку живлення;
- підтримка Layer 3 і динамічної маршрутизації;
- 8 черг на порт, що налаштовуються;
- 48 груп EtherChannel.

Для забезпечення функціонування спрощеної топології мережі, перш за все було виконано розрахунок параметрів IP-адресації. Під час розрахунку параметрів IP-адресації особлива увага була приділена економії IP-адрес, а також було приділено увагу можливості розширення внутрішньої мережі. Внутрішня адресація мережі буде налагоджена за рахунок протоколу динамічного налаштування вузла – Dynamic Host Configuration Protocol (DHCP). Внутрішні мережі для зручності налаштування та підвищення безпеки будуть поділені на віртуальні локальні мережі – Virtual Local Area Network (VLAN).

2.2. Проект політики безпеки

Маршрутизатори серії 7200 корпорації Cisco (рис. 2.1) пропонують солідний набір сервісів, що забезпечують не лише захист самого маршрутизатора, а й допомагають захистити локальну мережу за ним.



Рис. 2.1. Маршрутизатор Cisco серії 7200

Перш за все це досягається за рахунок вбудованих служб безпеки, системою локальної автентифікації та розширеними можливостями AAA (Authentication, Authorization, Accounting).

Також маршрутизатори даної серії пропонують інтегрований пакет рішень IPsec/ME/IPS.

ME на базі маршрутизаторів Cisco 7200 дозволяють:

- контролювати пакети та виявляти невідповідність політиці безпеки;
- проводити розширену перевірку вмісту протоколів IPv4 та IPv6;
- проводити URL-фільтрацію (Websense & N2H2);
- налаштовувати користувацький ME;
- проводити аутентифікацію/авторизацію користувачів для протоколів HTTP/HTTPS, FTP і Telnet;
- фільтрувати трафік додатків;

– виявляти та запобігати відмові в обслуговуванні (DoS) тощо.

Основою для захисту внутрішньої мережі можна вважати NAT та ACL. Ці технології дозволяють отримати надійний захист на третьому рівні моделі OSI.

Для захисту ж самого маршрутизатора використовується технологія AutoSecure, розділений на ролі доступ до командного рядка та зовнішнє управління.

В другому офісі для забезпечення периметрового захисту внутрішньої мережі застосовано дворівневий захист з використанням граничного екрануючого маршрутизатора та ME експертного рівня. Дана схема допомагає відфільтровувати трафік ще до експертного ME, що дозволяє забезпечити захист не тільки внутрішньої мережі, але й самого пристрою експертного ME.

Комутатори серії 2960 корпорації Cisco можуть мати консольні порти 10/100 та 10/100/1000.

Порти 10/100 можуть бути налаштовані для роботи зі швидкістю 10 або 100 Мбіт/с в повнодуплексному, або напівдуплексному режимі. Також ці порти можуть використовуватися для підвищення швидкості і дуплексного автоузгодження. За замовчуванням встановлено режим автоузгодження. При використанні порту для виконання автоузгодження він запитує відомості про швидкість і настройки дуплексного режиму підключеного пристрою і відправляє відомості про свої можливості. Якщо підключений пристрій також підтримує автоузгодження, порт комутатора вибирає оптимальні параметри підключення (тобто максимальну швидкість передачі даних по лінії, доступну для обох пристроїв, повнодуплексну передачу, якщо підключений пристрій її підтримує) і встановлює відповідні налаштування.



Рис. 2.2. Комутатор Cisco серії 2960

Порти 10/100 на комутаторах Catalyst 2960-24PC-L, 2960-48PST-L, 2960-48pst-S і

2960-24PC-S, комутатори і порти з нумерацією від 1 до 8 портів 10/100 на комутаторах

Catalyst 2960-24LT-L і 2960-24LC-S забезпечують підтримку PoE для пристроїв, відповідають вимогам стандарту IEEE 802.3 af. Попередній стандарт PoE компанії Cisco також підтримується для IP-телефонів Cisco і точок доступу Cisco Aironet. Кожен з портів PoE на комутаторах Catalyst 2960 забезпечує живлення потужністю до 15,4 Вт по кабелю Ethernet.

Комутатори Catalyst 2960-24PC-L, 2960-48PST-L, 2960-48PST-S і 2960-24PC-S забезпечують максимальну потужність живлення PoE приблизно 370 Вт.

Комутатори Catalyst 2960-24LT-L і 2960-24LC-S забезпечують максимальну потужність живлення PoE приблизно 124 Вт.

Для кожного порту PoE Catalyst 2960 можна вказати, чи буде він автоматично подавати живлення при підключенні IP-телефону або точки доступу. Диспетчер пристроїв Network Assistant і інтерфейс командного рядка визначають параметри PoE для кожного порту PoE 10/100.

Автоматично: при виборі автоматичної настройки порт забезпечує живлення тільки при підключенні допустимого пристрою, відповідного стандарту IEEE 802.3 af, IP-телефону або точки доступу Cisco, що відповідають

вимогам попереднього стандарту Cisco. Автоматична настройка призначена за замовчуванням.

Ніколи: при виборі цієї настройки порт не подає живлення навіть при підключенні IP-телефону Cisco або точки доступу.

Також, наявний порт подвійного призначення, який можна налаштувати як Порт 10/100/1000 або порт модуля SFP. Кожен порт являє собою єдиний інтерфейс з двома входами: роз'ємом RJ-45 і роз'ємом для модуля SFP. Два входи не є резервними інтерфейсами по відношенню один до одного. Комутатор активує тільки один роз'єм одночасно. За замовчуванням комутатор динамічно вибирає тип інтерфейсу, що використовувався при першому підключенні. Однак можна використовувати команду конфігурації інтерфейсу `media-type` для призначення вручну роз'єму RJ - 45 або роз'єму для модуля SFP. Для отримання інформації про налаштування швидкості і дуплексного режиму для порту каскадування подвійного призначення.

Кожен порт каскадування має 2 індикатора: один відображає стан порту RJ-45, інший - стан порту модуля SFP. Індикатор порту горить тільки у активного роз'єму.

2.3. Проект сценаріїв тестування функціоналу підсистеми

Для тестування дієздатності системи було проаналізовано декілька ПЗ.

1. Zabbix

Zabbix - це повномасштабний інструмент для мережевого та системного моніторингу мережі, який об'єднує кілька функцій в одній веб-консолі. Він може бути налаштований для моніторингу та збору даних з різних серверів і мережевих пристроїв, забезпечуючи обслуговування і моніторинг продуктивності кожного об'єкта.

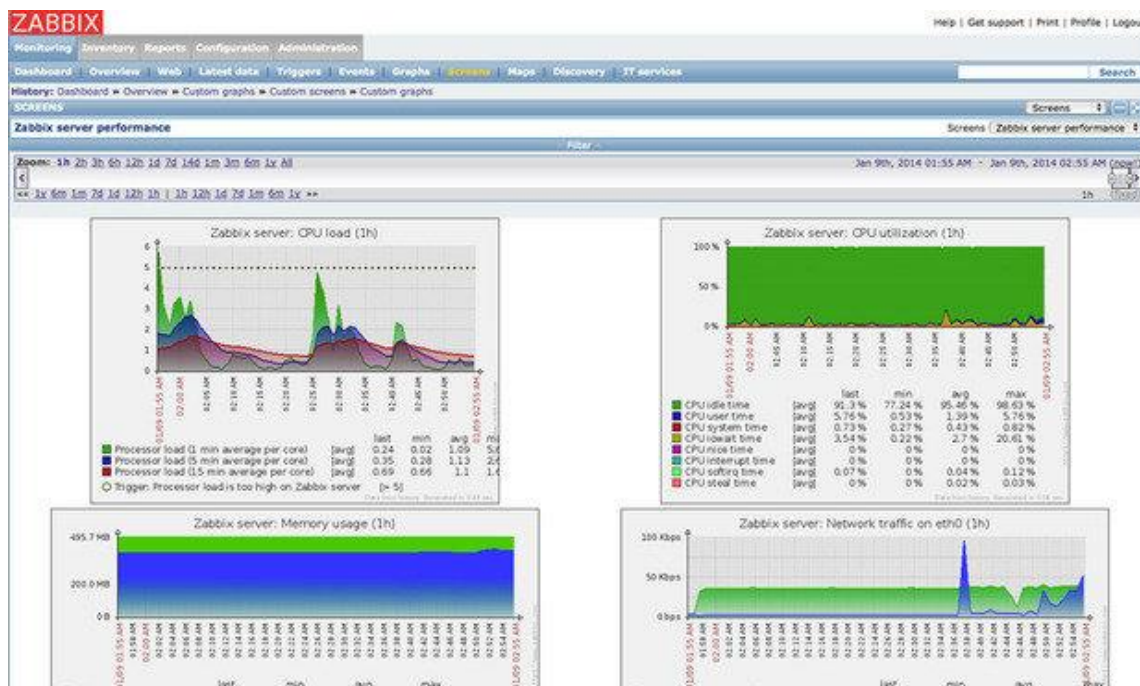


Рис. 2.3. Інтерфейс ПЗ Zabbix

В основному, Zabbix працює з програмними агентами, запущеними на контрольованих системах. Але це рішення також може працювати і без агентів, використовуючи протокол SNMP або інші можливості для здійснення моніторингу. Zabbix підтримує VMware та інші гіпервізори віртуалізації, надаючи докладні дані про продуктивність гіпервізора і його активності. Особлива увага також приділяється моніторингу серверів додатків Java, веб-сервісів і баз даних.

Хости можуть додаватися вручну або через процес автоматичного виявлення. Широкий набір шаблонів за замовчуванням застосовується до найбільш поширених варіантів використання, таким як Linux, FreeBSD і Windows-сервера; широко-використовувані служби, такі як SMTP і HTTP, а також ICMP і IPMI для докладного моніторингу апаратної частини мережі. Крім того, користувацькі перевірки, написані на Perl, Python або майже на будь-якій іншій мові, можуть бути інтегровані в Zabbix.

Zabbix може бути складним для реалізації на початковому етапі, але розумне використання автоматичного виявлення та різних шаблонів може частково полегшити труднощі з інтеграцією.

2. Observium

Observium - це програма для моніторингу мережевого обладнання та серверів, яка має величезний список підтримуваних пристроїв, що використовують протокол SNMP. Як програмне забезпечення, що належить до LAMP, Observium відносно легко встановлюється і налаштовується, вимагаючи звичайних установок Apache, PHP і MySQL, створення бази даних, конфігурації Apache і тому подібного. Він встановлюється як власний сервер з виділеною URL-адресою.

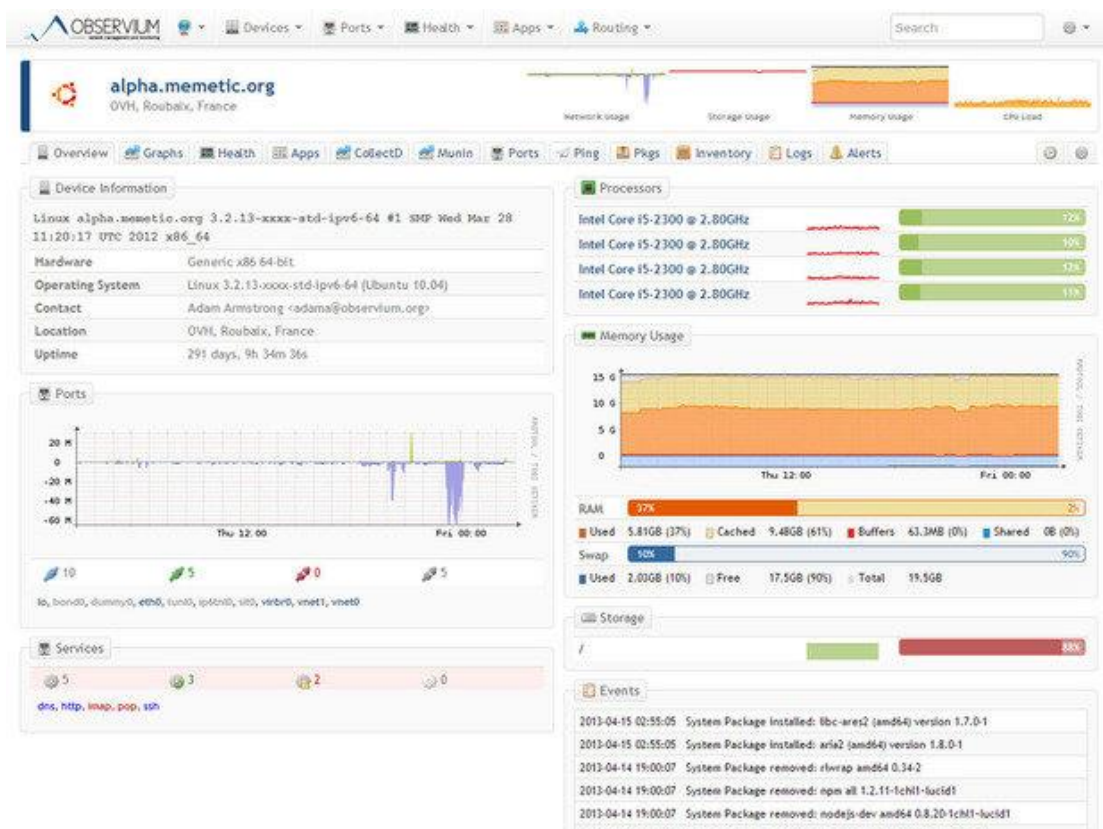


Рис. 2.4. Інтерфейс ПЗ Observium

Ви можете увійти в графічний інтерфейс і почати додавати хости і мережі, а також задати діапазони для автоматичного виявлення і дані SNMP, щоб Observium міг досліджувати його навколишні мережі і збирати дані по кожній виявленій системі. Observium також може виявляти мережеві пристрої через протоколи CDP, LLDP або FDP, а віддалені агенти хостів можуть бути розгорнуті на Linux-системах, щоб допомогти в зборі даних.

Вся ця зібрана інформація доступна через легкий у використанні інтерфейс, який надає просунуті можливості для статистичного відображення

даних, а також у вигляді діаграм і графіків. Ви можете отримати що завгодно: від часу відгуку ping і SNMP до графіків пропускної здатності, фрагментації, кількості IP-пакетів і т.д. залежно від пристрою, ці дані можуть бути доступні аж для кожного виявленого порту.

3. Icinga

Icinga починалася як відгалуження від системи моніторингу Nagios, але нещодавно була переписана в самостійне рішення, відоме як Icinga 2. На даний момент обидві версії Програми знаходяться в активній розробці і доступні до використання, при цьому Icinga 1.x сумісна з великою кількістю плагінами і конфігурацією Nagios. Icinga 2 розроблялася менш громіздкою, з орієнтацією на продуктивність, і більш зручною у використанні. Вона пропонує модульну архітектуру і багатопотоковий дизайн, яких немає ні в Nagios, ні в Icinga.



Рис. 2.5. Інтерфейс ПЗ Icinga

Як і Nagios, Icinga може бути використана для моніторингу всього, що говорить на мові IP, настільки глибоко, наскільки ви можете використовувати SNMP, а також настраюються плагіни і доповнення.

Існує кілька варіацій веб-інтерфейсу для Icinga, але головною відмінністю цього програмного рішення для моніторингу від Nagios є конфігурація, яка може бути виконана через веб-інтерфейс, а не через файли конфігурації. Для тих, хто вважає за краще керувати своєю конфігурацією поза командним рядком, ця функціональність стане справжнім подарунком.

4. Nagios

Nagios - це самостійна програмна система для моніторингу мережі, яка вже багато років знаходиться в активній розробці. Написана на мові C, вона дозволяє робити майже все, що може знадобитися системним і мережевим адміністраторам від пакету прикладних програм для моніторингу. Веб-інтерфейс цієї програми є швидким і інтуїтивно зрозумілим, в той час його серверна частина — надзвичайно надійною.

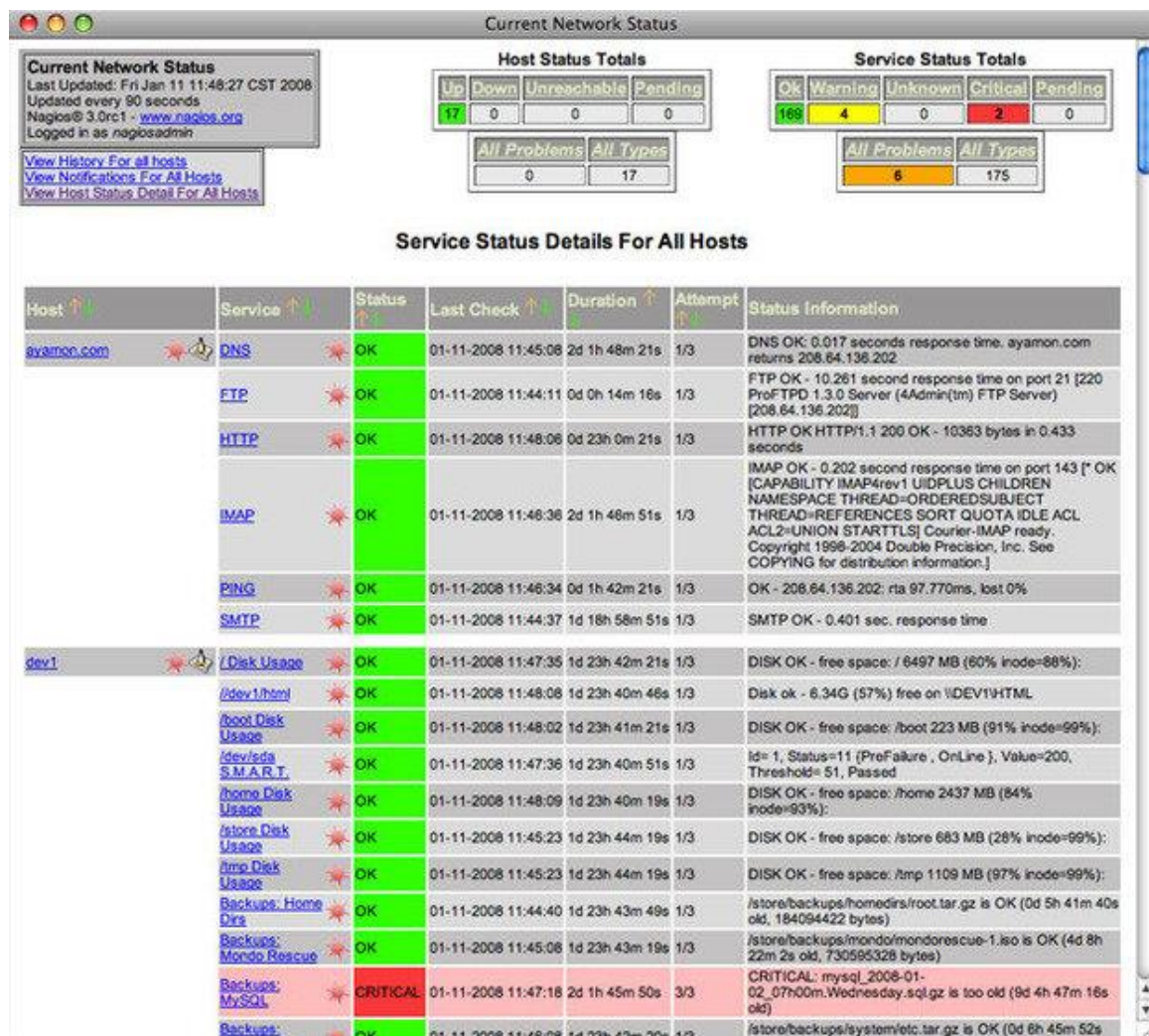


Рис. 2.6. Інтерфейс ПЗ Nagios

Як і Sacti, дуже активна спільнота підтримує Nagios, тому існують різні плагіни для величезної кількості апаратних засобів і програмного забезпечення. Від найпростіших ping-перевірок до інтеграції зі складними програмними рішеннями, такими як, наприклад, написаним на Perl безкоштовним програмним інструментарієм WebInject для тестування веб-додатків і веб сервісів. Nagios

дозволяє здійснювати постійний моніторинг стану серверів, сервісів, мережних каналів і всього іншого, що розуміє протокол мережевого рівня IP. Наприклад, ви можете контролювати використання дискового простору на сервері, завантаженість ОЗУ і ЦП, використання ліцензії FLEXlm, температуру повітря на виході сервера, затримки в WAN і Інтернет-каналі і багато іншого.

Недоліком Nagios є конфігурація, так як її найкраще виконувати через командний рядок, що значно ускладнює навчання новачків. Хоча люди, знайомі зі стандартними файлами конфігурації Linux/Unix, не повинні відчувати особливих проблем.

5. Cacti

Cacti - це безкоштовна програма, що входить в LAMP-набір серверного програмного забезпечення, яке надає стандартизовану програмну платформу для побудови графіків на основі практично будь-яких статистичних даних. Якщо будь-який пристрій або сервіс повертає числові дані, то вони, швидше за все, можуть бути інтегровані в Cacti. Існують шаблони для моніторингу широкого спектру обладнання-від Linux-і Windows-серверів до маршрутизаторів і комутаторів Cisco - в основному все, що спілкується на SNMP. Існують також колекції шаблонів від сторонніх розробників, які ще більше розширюють і без того величезний список сумісних з Cacti апаратних засобів і програмного

забезпечення.

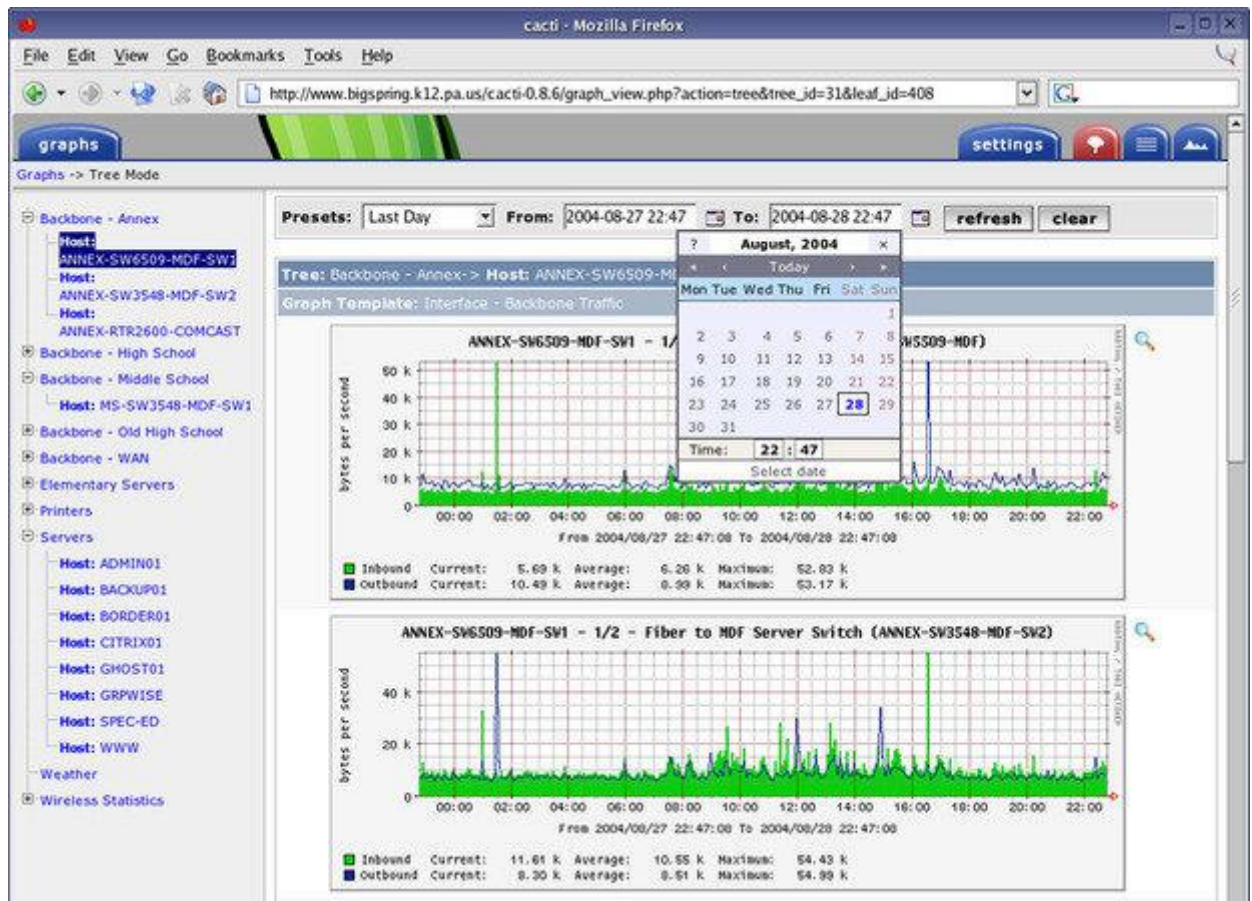


Рис. 2.7. Інтерфейс ПЗ Састі

Незважаючи на те, що стандартним методом збору даних Састі є протокол SNMP, також для цього можуть бути використані сценарії на Perl або PHP. Фреймворк програмної системи вміло розділяє на дискретні екземпляри збір даних і їх графічне відображення, що дозволяє з легкістю повторно обробляти і реорганізовувати існуючі дані для різних візуальних уявлень. Крім того, ви можете вибрати певні часові рамки і окремі частини графіків просто клікнувши на них і перетягнувши.

Таким чином, Састі - це інструментарій з великими можливостями для графічного відображення та аналізу тенденцій продуктивності мережі, який можна використовувати для моніторингу практично будь-якої контрольованої метрики, представленої у вигляді графіка. Дане рішення також підтримує практично безмежні можливості для налаштування, що може зробити його надто складним при певних застосуваннях.

6.Power SNMP Free Manager

PowerSNMP Free Manager - це безкоштовна програма, яка дозволяє легко відстежувати пристрої у вашій мережі за допомогою SNMP-запитів або відгуку пристроїв за допомогою ping-запитів.

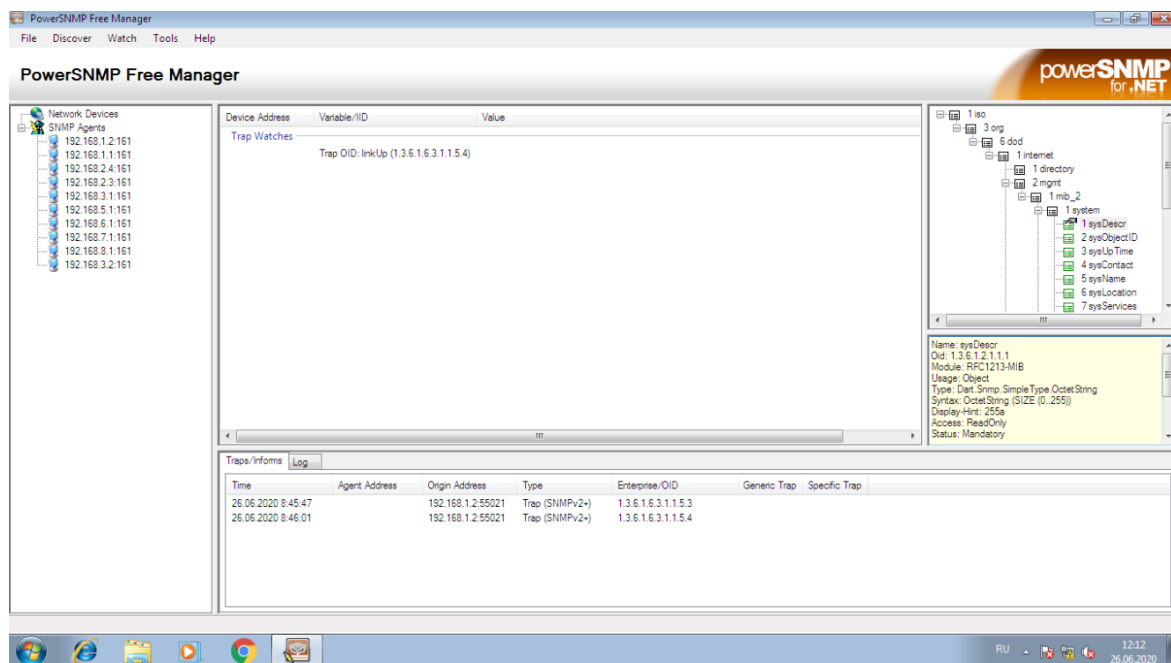


Рис. 2.7. Інтерфейс ПЗ Power SNMP Free Manager

Крім того, можна налаштувати елементи спостереження, які будуть завжди попереджати вас про виникнення незвичайної події. SNMP-пастки, змінні агента, які виходять за межі діапазону, або пінг пристроїв – все це можна контролювати за допомогою зручного інтерфейсу. Також, можливе налаштування для відправлення повідомлень про спрацьовані пастки SNMP на електронну пошту. Дане програмне забезпечення рекомендується для тих, хто тільки знайомиться з даним протоколом.

Висновки до розділу 2

Була спроектована мережа організації, що складається з одного офісу. Сформовано таблицю параметрів інтерфейсів пристроїв та адресації підмереж для наявного офісу.

Обрані пристрої, на яких базуватиметься підсистема управління. Описані можливості обладнання, які можуть використовуватись для поставленого

завдання, обрані та обґрунтовані основні з них. Також, проведено аналіз програмного забезпечення для моніторингу SNMP.

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ УПРАВЛІННЯ МЕРЕЖЕЮ

3.1. Базове налагодження пристроїв мережі

В даному пункті розглянуто базові налаштування пристроїв мережі. Для зручності конфігурування, та повного розуміння, який пристрій налаштовується, й перевірки зв'язку між пристроями по імені стандартні імена елементів мережі були змінені на ті, які відповідають проекту (рис. 3.1).

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host switch1
switch1(config)#
```

Рис. 3.1. Налаштування імені на комутаторі switch1

Адресація є основою будь-якої мережі, тому після зміни імен було налаштовано статичну адресацію інтерфейсів мережі. Пристрої будуть знаходити один одного у мережі за відповідною адресою.

Розрізняють «сірі» та «білі» IP-адреси. Перші зазвичай застосовуються для внутрішніх (локальних) мереж і існують тільки там. Другі – застосовуються в глобальній мережі і є загальнодоступними для зв'язку з Інтернету. Із-за цього вони, навідміну від «білих» адрес, можуть повторюватись. У фрагменті лістингу показане налаштування «сірої» адреси на інтерфейсі vlan1 комутатора IOU2 для з'єднання з глобальною мережею (рис. 3.2). Для зручності віддаленого керування комутаторами були налаштовані IP-адреси інтерфейсів VLAN1 на кожному з них (рис. 3.3).

```
IOU2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
IOU2(config)#int vlan1
IOU2(config-if)#ip add 192.168.1.2 255.255.255.0
IOU2(config-if)#no sh
IOU2(config-if)#
*May 19 19:28:04.911: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*May 19 19:28:05.917: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
IOU2(config-if)#
```

Рис. 3.2. Налаштування статичної IP-адреси на комутаторі IOU2

Статичні IP-адреси також використовуються для ідентифікації пристрою у процесі віддаленого керування.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int fa0\1
      ^
% Invalid input detected at '^' marker.

R2(config)#int fa0/1
R2(config-if)#ip add 192.168.1.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#
*Mar  1 00:19:56.095: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:19:57.095: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R2(config-if)#exit
R2(config)#exit
R2#
*Mar  1 00:20:04.927: %SYS-5-CONFIG_I: Configured from console by console
R2#copy ru st
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```

Рис. 3.3. Налаштування статичної IP-адреси для інтерфейсу Fast Ethernet0/1 на маршрутизаторі R2

За рахунок відповідних масок IP-адрес підмереж віддалене підключення до комутаторів можливе лише з одного пристрою, та лише зсередини відповідної локальної мережі. Це міра для зменшення ймовірності зловмисних дій щодо корегування роботи комутаторів.

Далі були сконфігуровані IP-адреси кінцевих пристроїв. Вони були згенеровані за рахунок протоколу динамічного конфігурування вузлів DHCP. Даний протокол дозволяє автоматично видавати для кінцевого пристрою всі потрібні налаштування мережі – маску підмережі, IP-адресу, адресу DNS (Domain Name Server), шлюз за замовчуванням, та ім'я домену підмережі. Для реалізації відповідних дій на маршрутизуючих пристроях, які мають підключення до підмереж через комутатори, був налагоджений цей протокол (рис. 3.4).

```

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.3
Router(config)#ip dhcp pool pool1
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# domain-name inet.com
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)#

```

Рис. 3.4. Налаштування DHCP на маршрутизаторі Router

Для взаємодії різних мереж між собою використовуються статичні маршрути або динамічні протоколи маршрутизації. Так як мережа одного офісу складається з багатьох підмереж, то раціонально використовувати останні.

Для маршрутизації в мережі Інтернет використовується протокол динамічної маршрутизації OSPF (Open Shortest Path First), заснований на технології відстеження стану каналу (link-state technology), що використовує для знаходження найкоротшого шляху алгоритм Дейкстри. Щоб забезпечити взаємодію локальної мережі із глобальною слід «розповісти» про свою мережу сусідньому маршрутизатору із глобальної мережі.

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.2 255.255.255.0 area 0
Router(config-router)#no network 192.168.1.2 255.255.255.0 area 0
Router(config-router)#network 192.168.1.0 255.255.255.0 area 0
Router(config-router)#network 192.168.2.0 255.255.255.0 area 0
Router(config-router)#

```

Рис. 3.5. Налаштування протоколу динамічної маршрутизації OSPF на маршрутизаторі Router

3.2. Налаштування підсистеми управління комп'ютерною мережею організації на базі протоколу SNMP

Налаштування SNMP — досить цікава тема, так як протокол SNMP є потужним інструментом у руках системного адміністратора і критично необхідним у великій мережі. Мережним пристроєм буде виступати маршрутизатор CISCO (рис. 3.6).

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#snmp-server community GROUP1 rw SNMP_ACL
Router(config)#ip access-list standard SNMP_ACL
Router(config-std-nacl)#permit host 192.168.1.3
Router(config-std-nacl)#exit
Router(config)#snmp-server community GROUP1 ro SNMP_ACL
Router(config)#snmp-server host 192.168.1.3 version 2c GROUP1
Router(config)#snmp-server enable traps snmp
Router(config)#
```

Рис. 3.6. Налаштування функціонування протоколу SNMP на маршрутизаторі
Router

```
switch1(config)#$aps snmp authentication linkdown linkup coldstart warmstart
switch1(config)#snmp-server host 192.168.1.3 version 2c GROUP1
switch1(config)#ip access-list standard SNMP_ACL
switch1(config-std-nacl)# permit 192.168.1.3
switch1(config-std-nacl)#!
switch1(config-std-nacl)#!
switch1(config-std-nacl)#snmp-server community GROUP1 RO SNMP_ACL
switch1(config)#snmp-server chassis-id
```

Рис. 3.7. Налаштування функціонування протоколу SNMP на комутаторі
switch1

Для моніторингу стану мережі було використано програмне забезпечення PowerSNMP Free Manager 2.0.0. Цей додаток ідеально підходить для легких та помірних завдань управління мережею. Він має простий у використанні інтерфейс, запит та контроль агентів, та монітор пасток SNMP. Також має можливість для налаштування автоматизованих повідомлень на електронну пошту у разі спрацювання пінг тайм-ауту та пасток SNMP. Програмне забезпечення PowerSNMP – це набір засобів управління для менеджменту мережевих пристроїв і додатків за допомогою стандартів SNMPv1/v2 і ASN.1, що гарантує високу сумісність і швидкість роботи. Засоби управління Agent та Manager у складі колекції PowerSNMP for ActiveX здійснюють передачу повідомлень по мережі, а комплект доповнюють об'єктів надає інформацію MIB і підтримку кодування/декодування.

Особливості PowerSNMP for ActiveX:

- Засіб управління Manager кодує пакети SNMPv1/v2, відправляє їх на будь-який агент, декодує відповідь і представляє його в додаток користувача у вигляді простого COM-об'єкта.

- Просте створення користувацьких SNMP-агентів, які передають певну інформацію MIB на віддалені мережеві менеджери.
- Програма для стиснення MIB комбінує кілька MIB в єдиний стиснутий файл, який зручно і легко поширювати.
- Компонент Service дає можливість встановлювати агентську або менеджерський додаток в якості системного сервісу.
- Об'єкти підтримки (DartStream, SnmpMessage, SnmpTable, SnmpTableRow, SnmpTrap, SnmpTraps, SnmpVariable, SnmpVariables) надають об'єктні моделі, спрощують використання SNMP.
- Підтримка служби компонентів COM+.
- Можливість роботи в мультипоточному середовищі.

На нижченаведеному рисунку можна побачити стартове вікно встановлення даної програми (рис. 3.8).



Рис. 3.8. Стартове вікно встановлення ПЗ PowerSNMP

Після натискання кнопки “Next >” відкривається наступне вікно, де описана ліцензійна угода даного ПЗ.



Рис. 3.9. Вікно з ліцензійною угодою ПЗ PowerSNMP

Наступним кроком, після погодження з ліцензійними умовами, є вибір кореневої директорії для встановлення ПЗ (рис. 3.10).

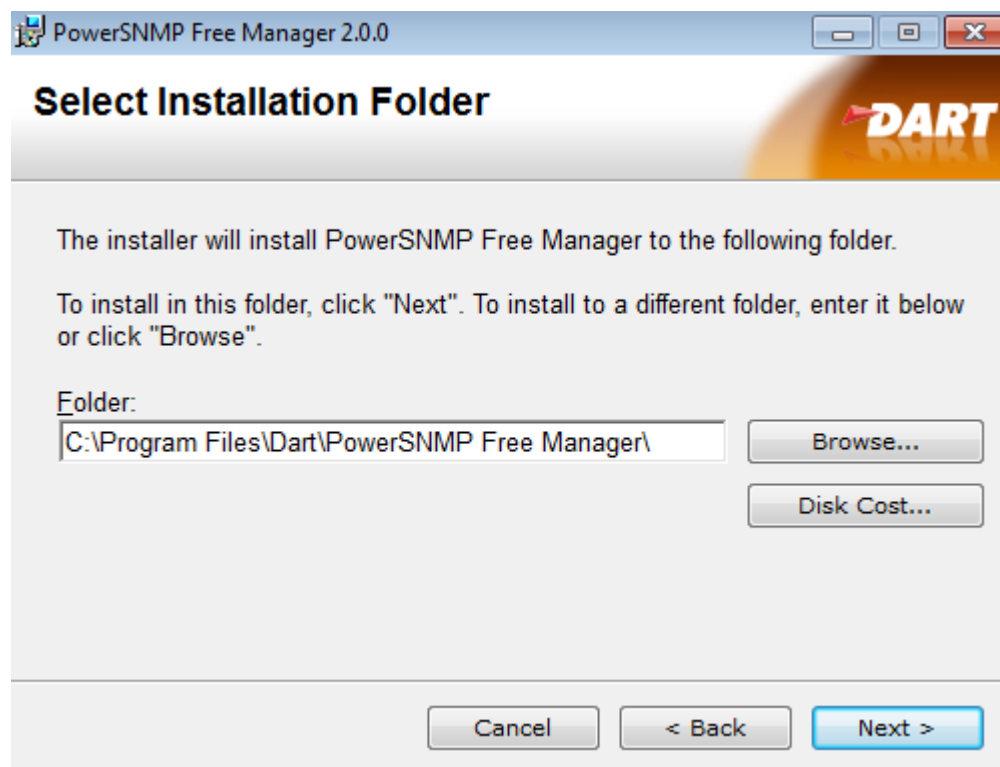


Рис. 3.10. Вибір кореневої директорії для встановлення ПЗ PowerSNMP

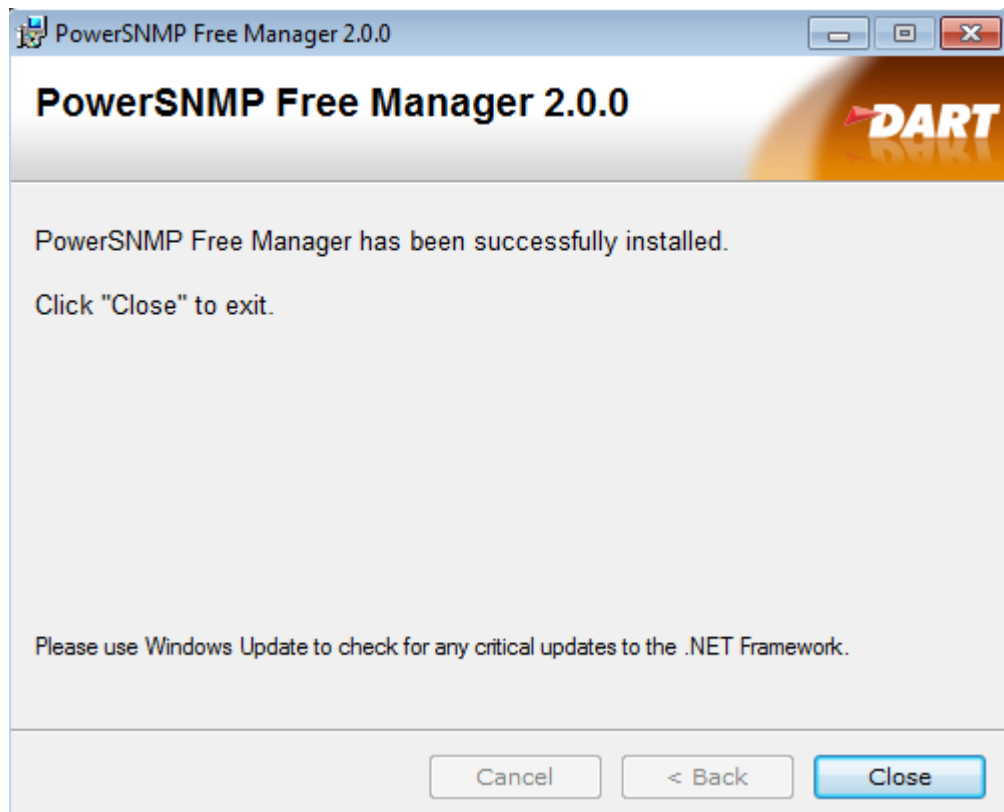
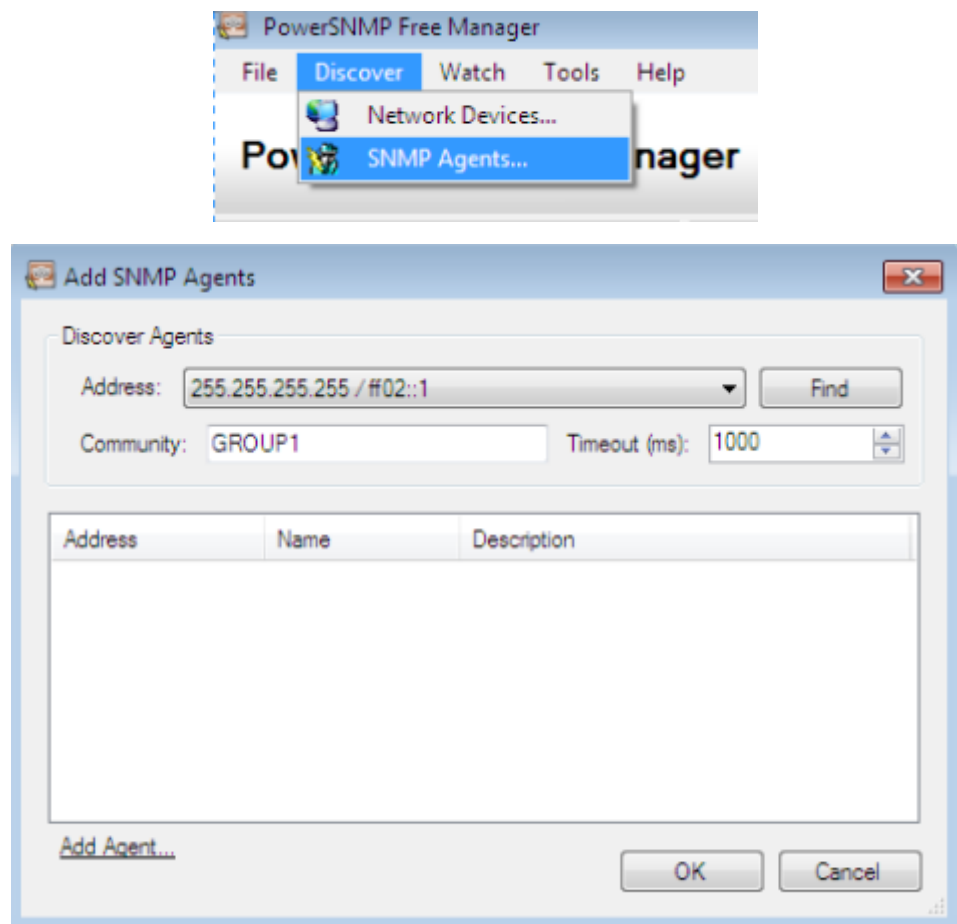


Рис. 3.8 – 3.11. Процес встановлення ПЗ



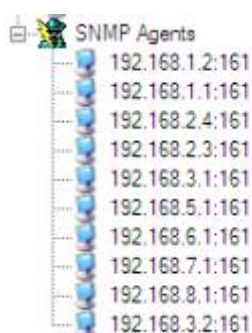
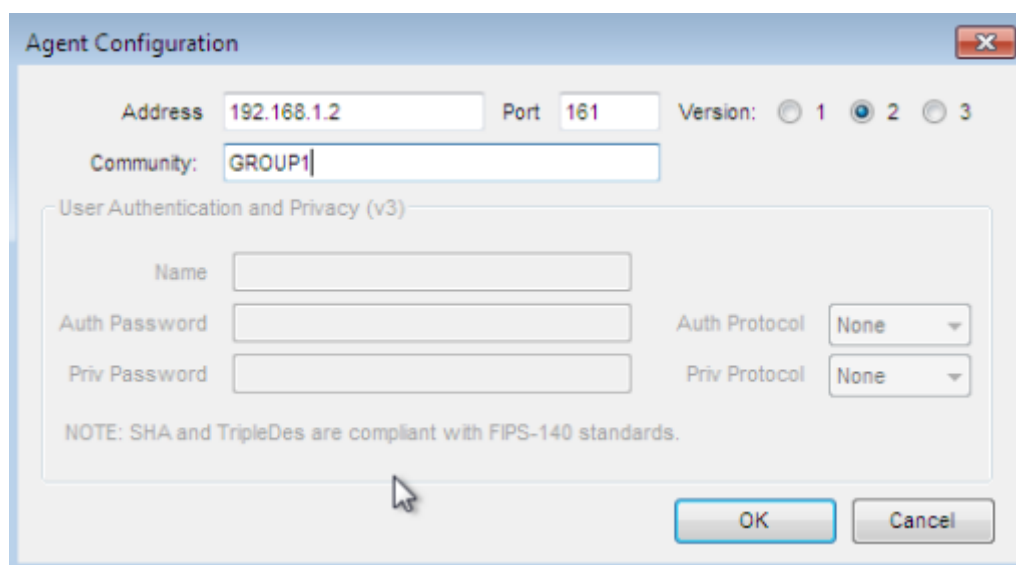


Рис.3.12 – 3.15. Додавання SNMP агентів

Для додавання агента SNMP слід скористатися вкладкою Discover, та натиснути на «SNMP Agents». Ця дія викличе відповідне вікно налаштувань. Після цього, в ньому слід вказати адресу та назву групи, обравши відповідну версію SNMP (у даному випадку – 2). Після додавання, агент буде відображено у списку з лівої сторони.

3.3. Тестування налаштувань.

Для тестування правильної роботи протоколу, було проведено дослідження дієздатності пасток SNMP.

На віртуальній машині було запущено програмне забезпечення Power SNMP Free Manager, налаштоване на моніторинг стану мережі. Після цього, переконавшись, що мережа знаходиться в активному стані було протестоване налагодження протоколу SNMP на мережних пристроях.

Для перевірки належної працездатності протоколу було проведено тестування, результати якого, наведені на рисунках 3.16 – 3.22.

Так, на рис. 3.16 показано вимкнення та увімкнення одного з інтерфейсів маршрутизатора, а саме – F0/1 на маршрутизаторі Router. Це було виконано для того, щоб перевірити працездатність пастки SNMP на цю дію.

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int f0/1
Router(config-if)#shut
Router(config-if)#
*Mar 1 00:55:10.587: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
*Mar 1 00:55:11.587: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet
0/1, changed state to downn sh
Router(config-if)#
*Mar 1 00:56:07.083: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to
up
*Mar 1 00:56:08.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet
0/1, changed state to up
```

Рис. 3.16. Вимкнення та увімкнення інтерфейсу F0/1 на маршрутизаторі Router

Як видно на рис. 3.17, пастка на SNMP-сервері успішно спрацювала і вивела відповідне повідомлення у діалогове вікно Traps/Informs програми PowerSNMP. В даному повідомленні видно не всю, а лише основну інформацію про пастку.

Traps/Informs Log						
Time	Agent Address	Origin Address	Type	Enterprise/OID	Generic Trap	Specific Trap
26.06.2020 7:48:26		192.168.1.1:59754	Trap (SNMPv2+)	1.3.6.1.6.3.1.1.5.3		
26.06.2020 7:48:26		192.168.1.1:59754	Trap (SNMPv2+)	1.3.6.1.6.3.1.1.5.4		

Рис. 3.17 Моніторинг стану інтерфейса F0/1

Для того, щоб подивитись детальну інформацію щодо конкретної пастки, що спрацювала слід двічі натиснути лівою клавiшею миші на відповідне повідомлення пастки SNMP. Ілюстративно це виглядає так, як показано на рис. 3.18-3.19 (повідомлення про вимкнення та увімкнення відповідно).

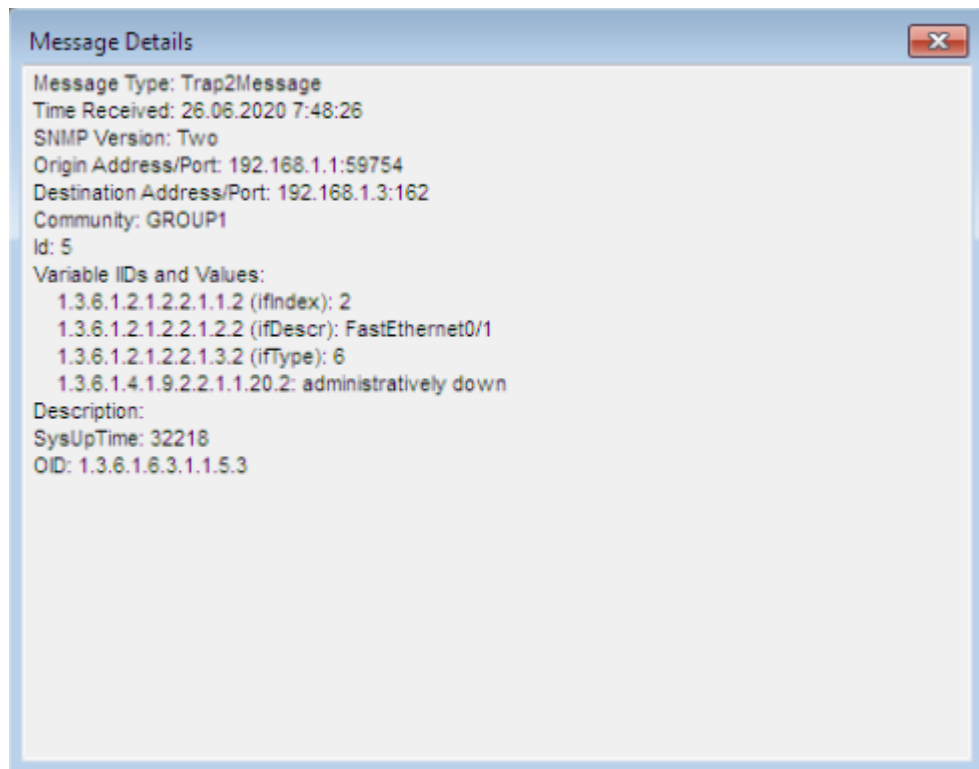


Рис. 3.18. Детальна інформація з пастки SNMP про вимкнення інтерфейсу F0/1

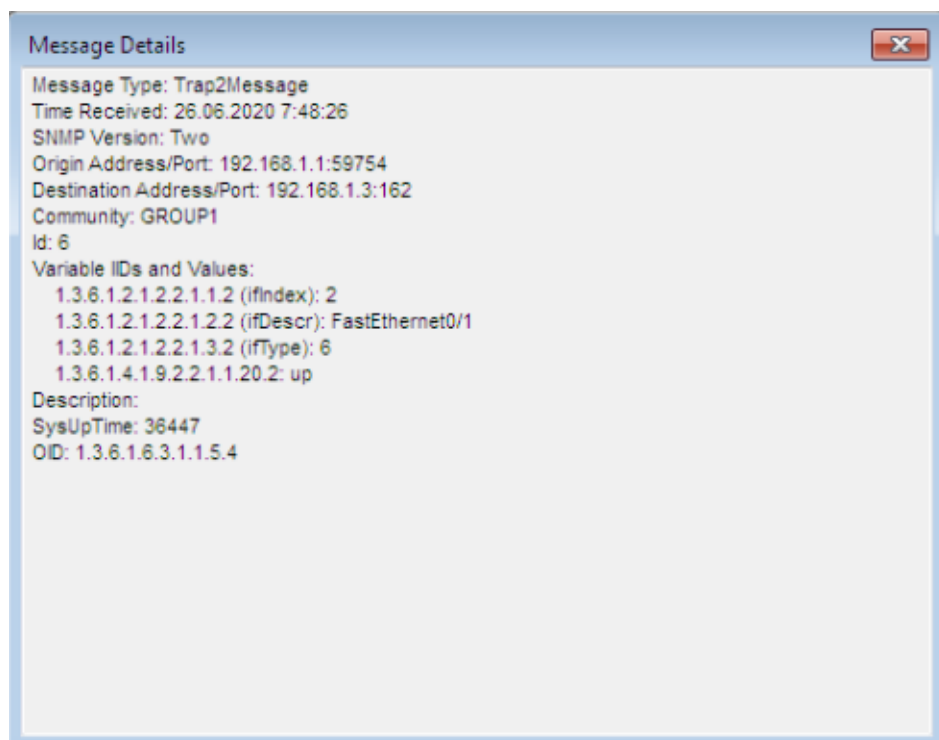


Рис. 3.19. Детальна інформація з пастки SNMP про увімкнення інтерфейсу F0/1

В детальній інформації можна побачити такі поля:

- тип повідомлення;
- час отримання;
- версія SNMP;
- адреса та порт інтерфейсу, з якого надійшло повідомлення;
- адреса та порт інтрефейсу, на який надходять повідомлення;
- назва спільноти до якої належить мережа;
- id повідомлення;
- код та його розшифровка в MIB;
- час роботи в системі;
- OID повідомлення.

Проаналізувавши зміст повідомлень, приходимо до висновку, що протокол на маршрутизаторах функціонує належним чином.

Аналогічні дії проведемо і для тестування налаштувань на комутаторах (рис. 3.20-3.23).

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int e0/1
Switch(config-if)#shut
Switch(config-if)#
*Jun 24 11:59:12.766: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
*Jun 24 11:59:13.766: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
Switch(config-if)#n sh
Switch(config-if)#
*Jun 24 11:59:51.838: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
Switch(config-if)#
*Jun 24 11:59:53.854: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
Switch(config-if)#
```

Рис. 3.20. Вимкнення та увімкнення інтерфейсу E0/1 на комутаторі Switch

Traps/Informs		Log				
Time	Agent Address	Origin Address	Type	Enterprise/OID	Generic Trap	Specific Trap
26.06.2020 8:45:47		192.168.1.2:55021	Trap (SNMPv2+)	1.3.6.1.6.3.1.1.5.3		
26.06.2020 8:46:01		192.168.1.2:55021	Trap (SNMPv2+)	1.3.6.1.6.3.1.1.5.4		

Рис. 3.21. Моніторинг стану інтерфейса E0/1

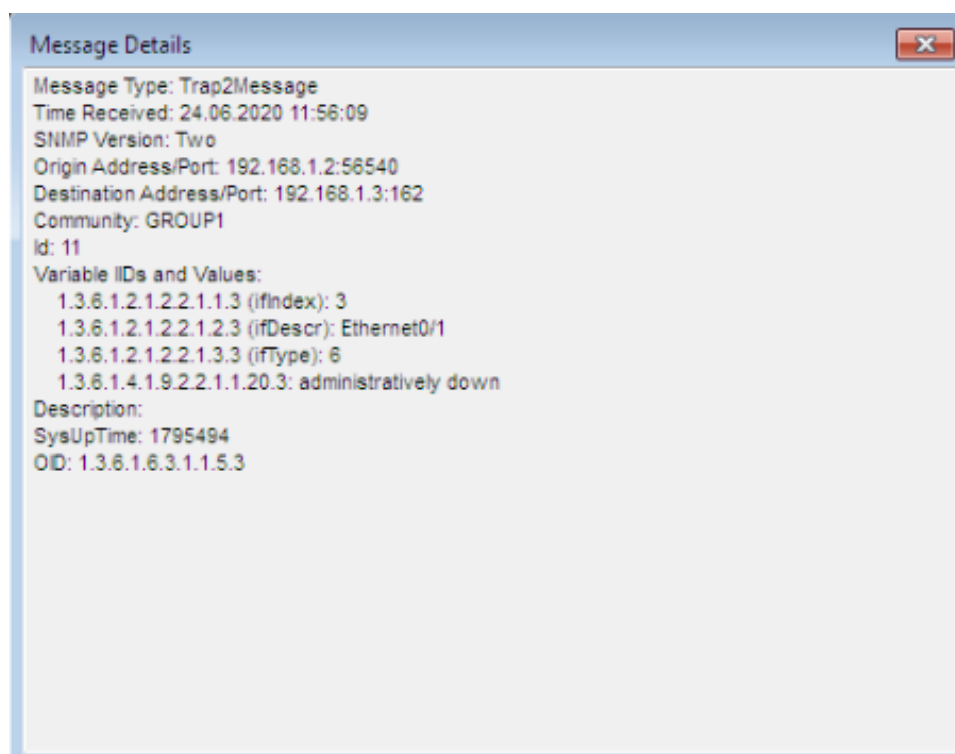


Рис.3.22. Детальна інформація з пастки SNMP про вимкнення інтерфейсу F0/1



Рис.3.23. Детальна інформація з пастки SNMP про увімкнення інтерфейсу F0/1

Як бачимо, налаштування на комутаторах також є коректними, про що свідчать наведені вище рисунки.

ВИСНОВКИ

В даній кваліфікаційній роботі за результатами аналізу підсистеми під управлінням комп'ютерною мережею організації на базі протоколу SNMP визначено основні принципи функціонування мережі. Розроблено підсистему управління комп'ютерною мережею організації на базі протоколу SNMP.

Було розглянуто 6 існуючих програмних засобів для моніторингу стану мережі та проаналізовані їх переваги та недоліки. Дослідження даних засобів показали, що для даного проекту слід використовувати ПЗ Power SNMP Free Manager.

Також були розглянуті вироби провідного виробника мережного обладнання – корпорації Cisco. Проаналізований асортимент, можливості налаштувань та експлуатації обладнання для локальних мереж.

Також в роботі була спроектована мережа організації, що складається з одного офісу. Сформована таблиця параметрів інтерфейсів пристроїв та адресації підмереж для даної мережі.

Обрані пристрої, на яких базується дана підсистема управління. Описані можливості обладнання, які використовуються для поставленого завдання, обрані та обґрунтовані основні з них.

Були описані базові налаштування пристроїв мережі: статична та динамічна адресація, маршрутизація по протоколу OSPF. Для зручності роботи з обладнанням були налаштовані імена пристроїв.

На мережних пристроях було проведене налагодження списків доступу в мережі.

Проведено тестування функціонування протоколу SNMP. Проведено аналіз результатів тестування та сформовано висновки щодо модернізації та можливостей покращення роботи мережі.

Реалізована мережа є повністю готовим макетом реальної реалізації проекту. Конфігурації можуть бути застосовані для налаштування реального обладнання мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основы организации сетей Cisco / Вито Амато., 2004. – 464 с. – ("Вильямс").
2. Access control list [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Access_control_list
3. Configuring IP Access Lists [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html>
4. Simple Network Management Protocol [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/SNMP>
5. Кевин Шмидт и Дуглас Мауро / Основы SNMP., 2012. – 520 с.
6. Розвивайте бізнес за допомогою IT-рішень Cisco [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/dam/global/uk_ua/solutions/small-business/pdf/Cisco_SMB_Buyers_Guide_final.pdf
7. Cisco 7200 Series Routers [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/products/routers/7200-series-routers/index.html>
8. Cisco 7200 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.nstor.ru/ru/catalog/net/oborudovanie-cisco/marshrutizatory-cisco/2026.html>
9. Cisco Catalyst 2960-X and 2960-XR Series Switches Data Sheet [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet_c78-728232.html
10. Cisco Catalyst 2960-X - возможности и преимущества [Електронний ресурс] – Режим доступу до ресурсу: http://stornet.ru/articles/cisco_catalyst_2960x_vozmojnosti_i_preimushhestva/

11. Настройка доступа в Интернет на маршрутизаторе Cisco [Электронный ресурс] – Режим доступа до ресурсу: <https://netclo.ru/nastroyka-dostupa-v-internet-na-marshr/#more-1671>

12. Мілінський М. ACL: списки контролю доступу в Cisco IOS [Електронний ресурс] / Микола Мілінський. – 2011. – Режим доступу до ресурсу: <https://habr.com/en/post/121806/?mobile=no>.

13. Налагодження та дослідження засобів віддаленого доступу та адміністрування [Електронний ресурс] – Режим доступу до ресурсу: https://learn.ztu.edu.ua/pluginfile.php/60583/mod_resource/content/1/KM_KIKB_LR-08-2019-2020_KI-3_KB-2-1_KB-2-2_KBK-19-1.pdf

14. Основы работы с керованими комутаторами Cisco та мережною операційною системою Cisco IOS [Електронний ресурс] – Режим доступу до ресурсу:
https://learn.ztu.edu.ua/pluginfile.php/40477/mod_resource/content/1/KM_KIKB_LR-04-2018-2019_KI-2KB-1.pdf

15. Campus LAN and Wireless LAN Design Guide, 2018. – 60 с.

16. Guide to Networks / Jill West, Tamara Dean, Jean Andrews, 2016. – 783 с.

17. Cisco Enterprise Campus Infrastructure. Best Practices Guide, 2014. – 45 с

18. Введение в SNMP [Електронний ресурс] – Режим доступу до ресурсу:
<https://cacaoadmin.com/vvedenie-v-snmp-prostoj-protokol-setevogo-upravleniya/>

19. Настройка SNMP [Електронний ресурс] – Режим доступу до ресурсу:
<https://army.ru/network/nastroyka-snmp/>

20. Введение в SNMP [Електронний ресурс] – Режим доступу до ресурсу:
http://network.xsp.ru/6_1.php

ДОДАТКИ

					КІК.КР.Б – 123 – 20 – ПЗ	
						54

Топологія мережі

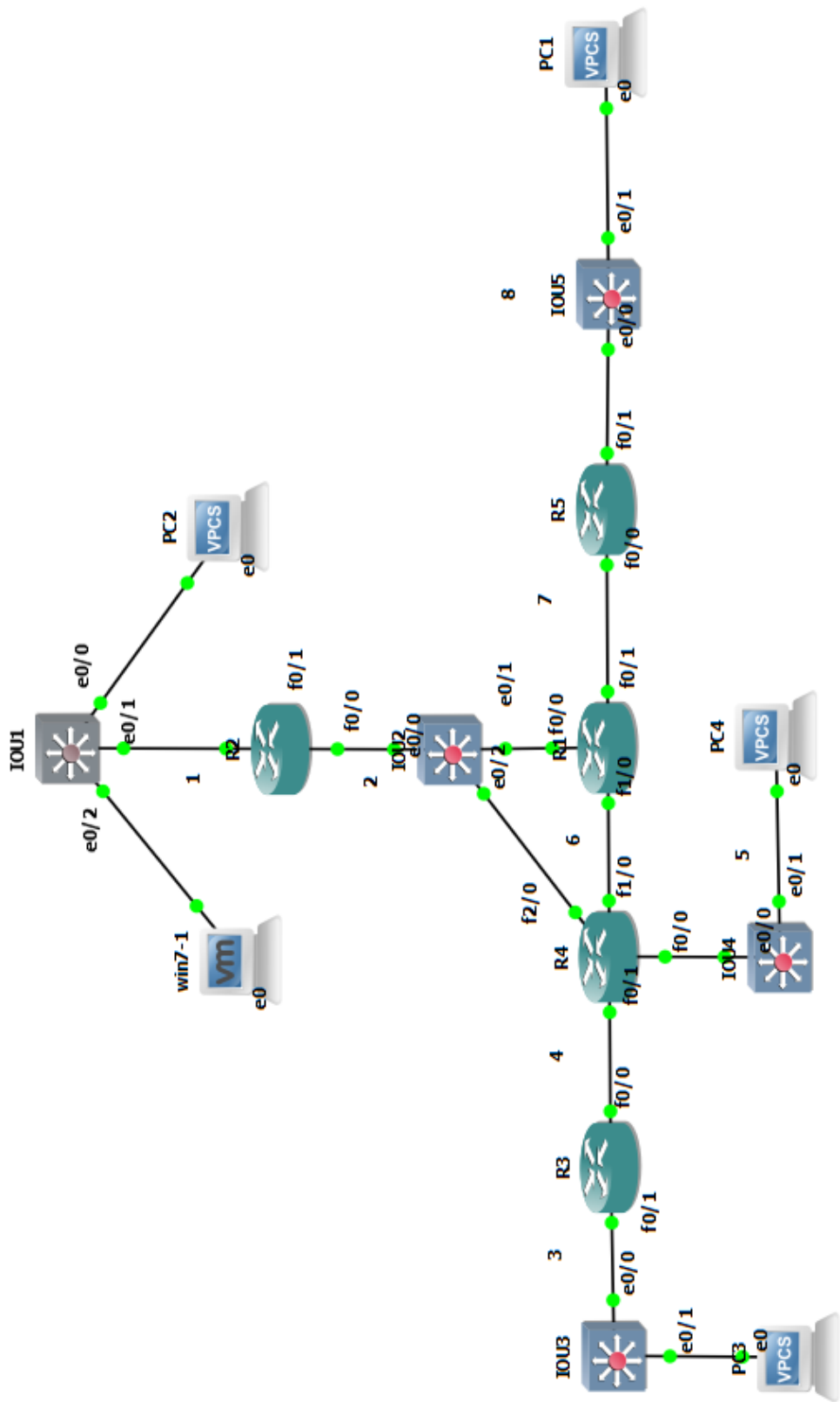


Рис. А.1. Загальна топологія мережі

					КІК.КР.Б – 123 – 20 – ПЗ	
						56