

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

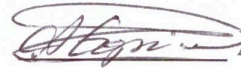
до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту системи
моніторингу мережної інфраструктури
побудованої на базі протоколу SNMP»

Виконав студент 4-го курсу групи КБ-2
спеціальності 125 «Кібербезпека»



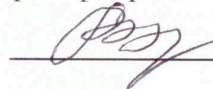
Богдан Яворенко

Керівник зав. кафедри КІ та КБ, к.т.н., доцент



Андрій Єфіменко

Рецензент професор кафедри КІ та КБ, д.т.н., доцент



Володимир Воротніков

Житомир – 2022

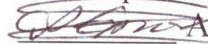
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Яворенко Богдан Олександрович

Тема роботи: «Проект підсистеми захисту системи моніторингу мережної інфраструктури побудованої на базі протоколу SNMP»

затверджена Наказом університету від 1 березня 2022 р. № 128/с

Термін здачі студентом закінченої роботи 25 червня 2022 р.

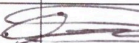
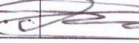
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Захист системи моніторингу
2. Протокол SNMP

Обладнання та програмне забезпечення:

1. Маршрутизатори Cisco 3995 та Cisco 3660
2. Комутатор Cisco 2960
3. Операційні системи Windows 7, Kali Linux, Cisco IOS
4. Топологія мережі

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 05.03.2022	 05.03.2022
2	Єфіменко А.А.	 14.04.2022	 14.04.2022
3	Єфіменко А.А.	 15.05.2022	 15.05.2022

Студент  Богдан Яворенко

Керівник  Андрій Єфіменко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	05 березня 2022	Виконано
2	Пошук інформації щодо реалізації системи моніторингу	12 березня 2022 – 15 березня 2022	Виконано
3	Аналіз технологій захисту систем моніторингу	18 березня 2022 – 20 березня 2022	Виконано
4	Проектування загальної топології	23 березня 2022 – 26 березня 2022	Виконано
5	Розробка IP-адресації та вибір обладнання	02 квітня 2022 – 06 квітня 2022	Виконано
6	Налаштування пристроїв мережі	09 квітня 2022 – 14 квітня 2022	Виконано
7	Тестування налаштованої мережі на проникнення	18 квітня 2022 – 24 квітня 2022	Виконано
8	Налаштування засобів захисту підсистеми моніторингу	30 квітня 2022 – 08 травня 2022	Виконано
9	Перевірка закритих вразливостей	13 травня 2022 – 16 травня 2022	Виконано
10	Написання пояснювальної записки	26 травня 2022 – 08 червня 2022	Виконано
11	Підготовка додаткових матеріалів	10 червня 2022 – 12 червня 2022	Виконано
12	Отримання відгуку та рецензії на кваліфікаційну роботу	14 червня 2022 – 15 червня 2022	Виконано
13	Захист кваліфікаційної роботи	25 червня 2022	Виконано

Студент Б. Яворенко Богдан Яворенко

Керівник А. Єфіменко Андрій Єфіменко

АНОТАЦІЯ

Кваліфікаційна робота містить опис повного циклу проектування, розробки та налаштування проекту підсистеми захисту системи моніторингу мережної інфраструктури побудованої на базі протоколу SNMP. Пояснювальна записка складається з вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 77 сторінках друкованого тексту. Пояснювальна записка має 20 сторінок додатків. Список використаних джерел містить 25 найменувань і займає 2 сторінки. В роботі наведено 59 рисунків та 8 таблиць. Загальний обсяг роботи – 97 сторінок.

Метою роботи є розробка та налаштування проекту підсистеми захисту системи моніторингу мережної інфраструктури побудованої на базі протоколу SNMP.

У роботі проаналізовано прикладні реалізації використання протоколу SNMP для моніторингу мережі, порівняно варіанти реалізації моніторингу за допомогою додатків на базі ОС Windows та Linux. Спроектовано загальну топологію мережі та проекти локальних ділянок, розроблено схему адресації всіх пристроїв мережі з урахуванням можливості розширення, здійснено вибір відповідного проекту топології обладнання мережі. Побудовано модель загроз мережі організації. Налаштовано мережу у відповідності до проекту та перевірено правильність функціонування налаштованих протоколів. Проведено тестування на проникнення та реалізовано атаки відповідно до виявлених проблем безпеки, після чого налаштовано засоби захисту від атак на протоколи та механізми мережі.

Ключові слова: МЕРЕЖА, ЗАХИСТ ТРАФІКУ, МЕНЕДЖЕР, АГЕНТ, СЕРВЕР, КЛІЄНТ, МОНІТОРИНГ, ПРОТОКОЛ, КОРИСТУВАЧ, АТАКА, ПРОНИКНЕННЯ, ТЕСТУВАННЯ, SNMP, ЗАГРОЗА, РЯДОК СПІЛЬНОТИ, ШИФРУВАННЯ.

					КІК.КР.Б – 125 – 26 – ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту системи моніторингу мережної інфраструктури побудованої на базі протоколу SNMP	Літ.	Арк.	Аркуші
Розроб.	Яворенко Б.О.	55	10.06				4	77
Керівник	Єфіменко А.А.	55	20.06					
Реценз.	Воротніков В.В.	55	20.06					
Пр.експ.	Єфіменко А.А.	55	20.06					
Затверд.	Єфіменко А.А.	55	20.06			ФІКТ, Гр. КБ-2		

ANNOTATION

The qualification work contains a description of the full cycle of design, development and configuration of the security subsystem of the network infrastructure monitoring system built on the basis of the SNMP protocol. The explanatory note consists of an introduction, three chapters, conclusions, a list of references and appendices. The text is set out on 77 pages of printed text. The explanatory note has 20 pages of appendices. The list of used sources contains 25 names and occupies 2 pages. The paper contains 59 figures and 8 tables. The total volume of the work is 97 pages.

The purpose of the work is to develop and configure the project of the protection subsystem of the network infrastructure monitoring system built on the basis of the SNMP protocol.

There are analyzes the application implementations of the SNMP protocol for network monitoring at explanatory note, compares the implementation options for monitoring using applications based on Windows and Linux. The general network topology and projects of local areas are designed, the scheme of addressing of all devices of a network taking into account possibility of expansion is developed, the choice of the corresponding project of topology of the network equipment is made. The model of threats of the organization's network is built. The network was configured in accordance with the project and the correct operation of the configured protocols was checked. Intrusion testing was performed and attacks were implemented in accordance with the identified security issues, after which the means of protection against attacks on protocols and network mechanisms were configured.

Keywords: NETWORK, TRAFFIC PROTECTION, MANAGER, AGENT, SERVER, CLIENT, MONITORING, PROTOCOL, USER, ATTACK, PENETRATION, TESTING, SNMP, COMMUNITY STRING, ENCRYPTION.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ЗАСТОСУВАННЯ ПРОТОКОЛУ SNMP ДЛЯ ПОБУДОВИ СИСТЕМИ МОНІТОРИНГУ ПРИСТРОЇВ КОМП'ЮТЕРНОЇ МЕРЕЖІ	9
1.1 Принципи побудови та функціонування протоколу SNMP.....	9
1.2 Застосування протоколу SNMP для моніторингу пристроїв мережної інфраструктури	16
1.3 Проблеми безпеки протоколу SNMP	24
1.4 Застосування протоколу SNMP для побудови систем кіберзахисту	30
РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ МОНІТОРИНГУ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА БАЗІ ПРОТОКОЛУ SNMP ТА АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ	33
2.1 Проектування підсистеми моніторингу вразливостей та комп'ютерної мережі	33
2.2 Аналіз загроз підсистеми моніторингу	39
2.3 Побудова моделі загроз підсистеми моніторингу	44
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ПІДСИСТЕМИ МОНІТОРИНГУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ.....	47
3.1 Вибір мережевого обладнання	47
3.2 Налагодження комп'ютерної мережі та підсистеми моніторингу	51
3.3 Дослідження рівня захищеності підсистеми моніторингу.....	65
3.4 Налагодження засобів захисту та дослідження стійкості системи моніторингу.....	69
ВИСНОВКИ.....	75
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	76
ДОДАТКИ.....	78

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

ІКС – інформаційно-комунікаційна система

ПК – персональний комп'ютер

IP – Internet Protocol

EIGRP – Enhanced Interior Gateway Protocol

DUAL – Diffusing Update Algorithm

DHCP – Dynamic Host Configuration Protocol

HTTP – HyperText Transfer Protocol

DNS – Domain Name System

AAA – Authentication, Authorization, Accounting

SNMP – Simple Network Management Protocol

OID – Object identifier

MIB – management information base

NMS – Network management system

SSH – Secure Shell

UDP – User Datagram Protocol

TCP – Transmission Control Protocol

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В сучасному світі практично всі процеси перейшли в віртуальний простір, доступність мережних рішень дала змогу великому бізнесу полегшити повсякденні задачі, а ІКС є базисом для функціонування різних корпорацій. Тому задача побудови універсальних мереж, що здібні однаково ефективно надавати послуги різних типів і при цьому бути максимально захищеними, з кожним днем стає все більш актуальною. Не менш важливим є можливість моніторингу мережі, оскільки це дозволяє знизити ризики перебоїв мережі.

Метою кваліфікаційної роботи є проектування, розробка та налаштування підсистеми захисту системи моніторингу мережної інфраструктури побудованої на базі протоколу SNMP.

Визначена мета обумовлює наступні завдання:

- аналіз та дослідження технологій моніторингу та їх захисту;
- розробка проекту системи захисту підсистеми моніторингу;
- налаштування та тестування спроектованої мережі в емуляторі;
- тестування стійкості до загроз та налаштування засобів захисту.

Об'єктом дослідження є процес побудови підсистеми захисту системи SNMP-моніторингу мережної інфраструктури.

Предметом дослідження є протокол SNMP, питання безпеки протоколу SNMP та питання застосування протоколу у мережах малого та середнього розмірів, а також можливості протоколу для проведення процедур моніторингу мережних пристроїв та мережних вузлів.

У процесі виконання кваліфікаційної роботи було розроблено проект підсистеми захисту системи моніторингу мережної інфраструктури на базі протоколу SNMP, досліджено його можливості, реалізовано безпекові рішення, а також протестовано стійкість цього протоколу до атак.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ЗАСТОСУВАННЯ ПРОТОКОЛУ SNMP ДЛЯ ПОБУДОВИ СИСТЕМИ МОНІТОРИНГУ ПРИСТРОЇВ КОМП'ЮТЕРНОЇ МЕРЕЖІ

1.1 Принципи побудови та функціонування протоколу SNMP

Simple Network Management Protocol (SNMP) – це протокол прикладного рівня, він уможливорює обмін даними між мережними пристроями [1]. Він являє собою стандартний інтернет-протокол для керування пристроями в IP-мережах на основі архітектур TCP/UDP, який дозволяє відслідковувати керовані мережеві пристрої, включаючи маршрутизатори, мережеві комутатори, сервери, принтери та інші пристрої, що включені через IP через єдину систему керування/програмне забезпечення. SNMP - це не продукт, а зведення правил. Він визначений Радою з архітектури Інтернету та є частиною пакету TCP/IP. SNMP керується та підтримується Інженерною групою Інтернету (IETF).

Спочатку протокол повинен був надати системним адміністраторам інструмент управління інтернетом. Однак, гнучка архітектура SNMP дозволила проводити моніторинг всіх мережевих пристроїв та керувати ними з однієї консолі. Це стало причиною поширення SNMP. Протокол дозволяє системному адміністратору проводити моніторинг, контролювати продуктивність мережі та змінювати конфігурацію підключених пристроїв. SNMP використовують у мережах будь-якого розміру: чим більша мережа, тим краще розкриваються переваги протоколу. Він дозволяє переглядати, контролювати та керувати вузлами через єдиний інтерфейс з функціями пакетних команд та автоматичного оповіщення. Таким чином, SNMP позбавляє адміністратора необхідності введення команд вручну. Усього були розроблені та розгорнуті три версії:

- SNMPv1
- SNMPv2c
- SNMPv3

Першу версію протоколу створено у 80-х роках XX століття. Легка в налаштуванні – потрібен лише рядок community [2]. Версія широко використовується досі.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

Друга версія протоколу SNMP з'явилася 1993 року. Розробники додали до неї новий запит GetBulk та пастку Inform, а також удосконалили безпеку.

У цій версії є два способи спілкування з пристроями, що підтримують SNMPv1: двомовна система мережного управління та проксі-агенти. Проксі-агенти виконують роль майстер-агентів, а двомовній системі управління менеджер визначає, яку версію SNMP підтримує агент, і зв'язується з ним через SNMPv2c.

Третя версія вийшла 1998 року. Розробники додали в SNMP криптографічний захист, полегшили віддалену настройку та адміністрування об'єктів [3]. Цього вдалося досягти за рахунок визначення набору стандартизованих об'єктів управління, які називаються об'єктами MIB віддаленого мережевого моніторингу - RMON MIB.

Таблиця 1.1 – Порівняння версій протоколу SNMP

	SNMPv1	SNMPv2c	SNMPv3
Контроль доступу	На основі назв спільнот та MIB	На основі назв спільнот та MIB	Контроль доступу на основі користувача, групи користувачів та подання MIB
Аутентифікація та конфіденційність	На основі назв спільнот	На основі назв спільнот	Режим автентифікації: MD5/SHA Режим шифрування: DES56/AES128/AES192 /AES256/3DES
Trap	Підтримує	Підтримує	Підтримує
Inform	Не підтримує	Підтримує	Підтримує
GetBulk	Не підтримує	Підтримує	Підтримує
Додаток	Підходить для невеликих мереж із низькими вимогами до безпеки	Підходить для різного розміру мереж з низькими вимогами до безпеки	Підходить для великих та надгігантських підприємств із суворими вимогами безпеки

Всі вони використовуються досі, а найпоширенішою стала друга – SNMPv2c, яка і використовувалась більшу частину історії протоколу.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

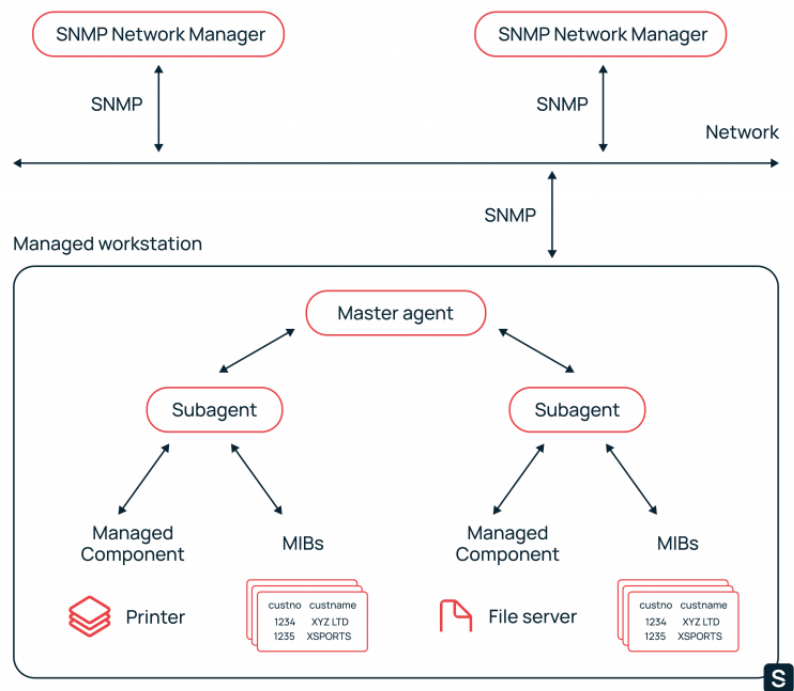


Рисунок 1.1 – Схема функціонування протоколу SNMP

Протокол SNMP для функціонування використовує три основні компоненти:

- Мережна станція управління, що включає мережного менеджера.
- Агенти.
- Керовані компоненти.

Кожен з компонентів системи несе важливу роль у функціонуванні системи та виконує певний функціонал [4]. Важливим є кожен з них.

Мережна станція управління (NMS, Network Management Station) – це консоль системи, NMS віддалено моніторить керовані пристрої, отримує дані, зібрані майстер-агентами, відстежує продуктивність і представляє отриману інформацію у графічному вигляді. Вбудований менеджер NMS відповідає за зв'язок із агентами.

Агент SNMP отримує запити від диспетчера SNMP та передає йому відповіді.

Крім того, агент SNMP здійснює обмін даними з усіма субагентами DPI2 та вузлами SMUX у системі. Агент SNMP управляє деякими змінними MIB, і всі субагенти DPI2 та вузли SMUX реєструють свої змінні MIB на агенті SNMP. Існує два види агентів:

- Майстер-агент.
- Субагент.

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

Майстер-агент – це програма, що пов'язує мережевих менеджерів та субагентів. Майстер-агент аналізує запити, що надходять, мережевого менеджера NMS і пересилає їх субагентам, отримують інформацію, створюють відповідь і відправляють його менеджеру. Майстер агент повідомляє менеджера, якщо запит некоректний, неправильно сформульований або запитана інформація недоступна.

Субагент – це програма, що поставляється вендором разом з мережевим пристроєм, використовуються в конкретній базі інформації, що управляє (MIB). Субагент збирає інформацію про майстер-агент, налаштовує параметри майстер-агента, відповідає на запити менеджера. Кожен керований компонент має відповідний субагент.

Керовані компоненти є підключеними до мережі комп'ютерами або програмним забезпеченням із вбудованим субагентом. До таких пристроїв відносяться не тільки маршрутизатори, комутатори та сервери, а й IP-відеокамери, МФУ та IP-телефони. До програмним забезпеченням із субагентами також відносяться антивірусні програми, системи резервного копіювання, ПЗ для систем ДБЖ.

Крім того, SNMP включає базу керуючої інформації (MIB) і ідентифікатор об'єкта (OID). MIB - це база даних управління інформацією про пристрої, де зберігаються інформація про стан керованого пристрою, доступна для систем управління. У кожного типу пристрою своя MIB-таблиця, і завдяки MIB менеджер знає, яку інформацію може запросити у агента пристрою. OID – ідентифікатор об'єкта. MIB надає власний унікальний ID, що дозволяє вам ідентифікувати пристрій. OID є цифровим еквівалентом шляху до файлу, частина OID містить дані про виробника обладнання, що дозволяє швидко отримати деяку інформацію про пристрій.

Менеджери та агенти обмінюються даними через протокол UDP. За замовчуванням SNMP використовує порти UDP 161 і 162. Менеджер надсилає запити на порт 161 агента. З порту 161 агент надсилає відповідь менеджеру. При надсиланні запиту менеджер додає до нього ID, а агент вставляє цей ID у відповідь, щоб менеджер міг зв'язати свій запит із відповіддю агента.

Пастки агент висилає на порт 162 менеджерів. Якщо використовується DLTS або TLS, агент надсилає повідомлення на порт 10162, а менеджер — на порт 10161.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

Адміністратор може змінити порти SNMP, які використовуються за замовчуванням, на будь-які інші.

Для реалізації моніторингу та менеджменту протоколом використовує спеціальні повідомлення. В обміну беруть участь два основних компоненти:

- База керуючої інформації – MIB
- Ідентифікатор об'єкту – OID

База керуючої інформації (MIB) – це ієрархічна база даних із відомостями про пристрій. У кожного типу пристрою своя MIB-таблиця: у принтера міститься інформація про стан картриджів, а у комутатора - дані про трафік. Завдяки MIB менеджер знає, яку інформацію може запросити у агента пристрою.

Кожен об'єкт у MIB має свій унікальний ідентифікатор - ідентифікатор об'єкту (OID), який представлений у числовому форматі та має ієрархічну структуру. OID – це числовий еквівалент шляху до файлу. Він надає значення кожної таблиці в MIB, кожному стовпцю в таблиці та кожному значенню в стовпці.

Наприклад, OID 1.3.6.1.4.868.2.4.1.1.1.3.3562.3. означає iso.org.dod.internet.private.transition.products.chassis.card.slotCps.cpsSlotSummary.cpsModuleTable.cpsModuleEntry.cpsModuleModel.3562.3.

Використовуючи перші 6 цифр цього OID, можна пройти дерево на схемі.

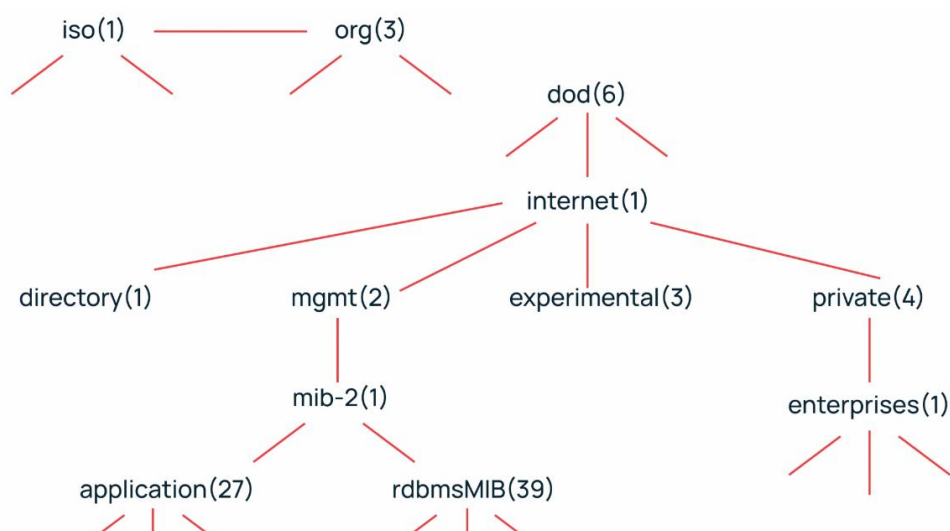


Рисунок 1.2 – Схематичне представлення дерева OID

Частина значень OID містить дані про виробника пристрою, що дозволяє швидко отримати певну інформацію про девайс.

Деревоподібна ієрархія MIB і OID у SNMP виглядає дещо заплутаною, але має свої переваги. Це проста та гнучка система організації мережевих пристроїв, вона працює незалежно від розміру мережі.

Замість протоколу UDP може використовуватися TCP, IPX або протокол MAC-рівня. Обмін даними базується на Protocol Data Unit (PDU).

Усього в SNMP сім PDU:

- GET – запит менеджера NMS на отримання даних із пристрою.
- GETNEXT – запит, аналогічний GET. Відмінність лише тому, що менеджер запитує дані, що є наступному рівні ієрархії OID, в MIB.
- SET – за допомогою цього запиту менеджер змінює або привласнює нові дані.
- RESPONSE – повідомлення від агента, що надсилається у відповідь на запит даних.
- TRAP – це повідомлення про подію або помилку. Агент відправляє його відразу після настання події, не чекаючи на запит менеджера. Менеджер не підтверджує отримання повідомлення, що може стати проблемою.
- GETBULK – запит агенту на вилучення з масиву даних. Це покращений варіант запиту GETNEXT.
- INFORM – повідомлення, подібне до TRAP, але з підтвердженням отримання. Агент надсилатиме повідомлення, поки менеджер не підтвердить, що воно дійшло.
- TRAP, GETBULK – є лише у другій та третій версіях протоколу SNMP.

Таблиця 1.2 – Схема PDU в SNMP

IP-заголовок	TCP/IP	TCP/IP
UDP-заголовок	TCP/IP	TCP/IP
Версія SNMP	v1/v2/v3	PDU

Продовження таблиці 1.2 – Схема PDU в SNMP

Рядок спільноти	Public, Private	PDU
Тип PDU	Get, GetNext, Response, Set, Trap, GetBulk, Inform	PDU
ID запиту	Ідентифікатор запиту	PDU
Статус помилки	0, 1, 2, 3, 4, 5	PDU
Індекс помилки	0, 1	PDU
Зв'язані змінні	Одна або декілька змінних у запиті	PDU

Для полегшення діагностики помилок під час передачі даних розроблено 6 статусів помилок:

- 0 - noError – Процес завершено успішно.
- 1 - tooBig — Об'єкт занадто великий і не міститься у Response.
- 2 - noSuchName - Для запитів GET і SET: запитана змінна не існує в базі MIB. Для запитів GETNEXT: не має приймача в дереві MIB.
- 3 - badValue — Для запитів SET: зроблено помилку в синтаксисі або встановлено неприпустиме значення.
- 4 - readOnly – Помилка не визначена.
- 5 - genErr - Інші помилки, наприклад, спроба надати значення, що перевищує межі реалізації.

Унікальною особливістю протоколу SNMP є використання спеціальних пакетів – пасток. Пастка (Trap) – це найважливіший спосіб комунікації у SNMP. Менеджер відповідає за багато пристроїв, на багатьох з них може бути кілька керованих компонентів. Агент відправляє пастку з власної ініціативи, коли потрібно повідомити менеджеру про подію. Наприклад, пастка може надіслати звіт про перегрівання машини або про те, що в тонері закінчилося чорнило.

Отримавши повідомлення, менеджер вибирає потрібну дію, наприклад, опитує агента, щоб отримати повне уявлення про те, що сталося. Перелік повідомлень, які надсилає пастка:

- 0 – coldStart – Холодний запуск пристрою.
- 1 - warmStart - Гарячий запуск пристрою.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

- 2 - linkDown - Інтерфейс відключився.
- 3 - linkUp - Інтерфейс увімкнувся.
- 4 — authenticationFailure — Менеджер надіслав повідомлення з неправильним рядком спільноти.
- 5 - egpNeighborLoss - Агент втратив зв'язок з хостом за протоколом Exterior Gateway Protocol (EGP).
- 6 - enterpriseSpecific - Сталася подія, характерна для виробника цього пристрою.

У SNMP є два типи пасток: Trap та Inform. Trap та Inform – це спонтанні дії керованого пристрою. Коли виникає умова спрацювання переривання, керований пристрій надсилає переривання NMS для повідомлення. Inform схожий на Trap, але для Inform потрібне підтвердження від NMS, а для Trap – ні. Якщо керований пристрій не отримує підтвердження, він зберігає Inform у буфері або повторює операцію Inform, доки NMS не поверне підтвердження. Як тільки кількість повторних надсилань досягне максимальної межі, керований пристрій запише журнал для запиту на інформування. Якщо повідомлення не дійшло менеджера, агент про це не дізнається.

1.2 Застосування протоколу SNMP для моніторингу пристроїв мережної інфраструктури

Протокол простого керування мережею (SNMP) був створений для полегшення можливості моніторингу мережі, який мережеві адміністратори можуть використовувати для різних моделей пристроїв та отримують змогу виявлення різних аспектів продукту. Таку інформацію, як завантаження процесора, таблиці маршрутизації та статистику мережевого трафіку та якість підключення з'єднання між пристроями мережі, серед багатьох інших, можна отримати віддалено за допомогою SNMP. Можна також використовувати SNMP для встановлення конфігурацій на пристроях, що підтримують його.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

Зчитування в SNMP здійснюється за допомогою функції рядку community. Першочергове завдання адміністратора – налаштування такого рядку. Після підключення до пристрою потрібно "витягнути" його для моніторингу за допомогою OID.

Для моніторингу пристроїв використовуються в основному робочі станції на базі ОС Windows та Linux з встановленим на нього програмним забезпеченням [5]. В сучасності існує досить багато таких реалізацій від різних розробників. Одними з найбільш популярних є:

- MRTG.
- Cacti.
- Network Performance Monitor
- ManageEngine SNMP Bandwidth Monitoring
- PRTG

Multi Router Traffic Grapher або MRTG є одним з найбільш давніх інструментів моніторингу за протолом SNMP. Він існує з 1995 року і все ще широко використовується в сучасності. Це абсолютно безкоштовна система із відкритим вихідним кодом. MRTG не найкрасивішим та найзручнішим, але, можливо, найгнучкішим. Окрім смуги пропускання MRTG може контролювати безліч параметрів. Фактично, він може відстежувати, реєструвати та відображати будь-які параметри SNMP.

Два основних компоненти MRTG - це скрипт Perl, який зчитує дані SNMP з цільових пристроїв, та програма на C який бере дані, зберігає їх у базі даних циклічного перебору та створює веб-сторінки з використанням смуги пропускання графіки. Той факт, що він в основному написаний на Perl, дозволяє налаштувати будь-яке програмне забезпечення під свої конкретні потреби. MRTG доступний для Windows або Linux. Початкове налаштування може бути більш складним, ніж у аналогічного ПЗ, але MRTG має досить доступну документацію.

Для встановлення MRTG необхідно спочатку встановити та налаштувати Perl. Існує спосіб запустити MRTG у Windows замість певної програми, але це вимагає додаткових маніпуляцій, включаючи деякі зміни реєстру. Після встановлення MRTG налаштовується шляхом редагування файлу конфігурації в старому стилі

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Linux. Адміністратори, які звикли до налаштування графічного інтерфейсу, можуть зіткнутися з певними проблемами на даному етапі.

MRTG найкраще завантажувати прямо з сайту розробника. Він доступний як ZIP-файл для Windows або тарбол для Linux.

Найважливішим аргументом щодо MRTG є той факт, що це перша система моніторингу, і вона все ще існує, що свідчить про її цінність.

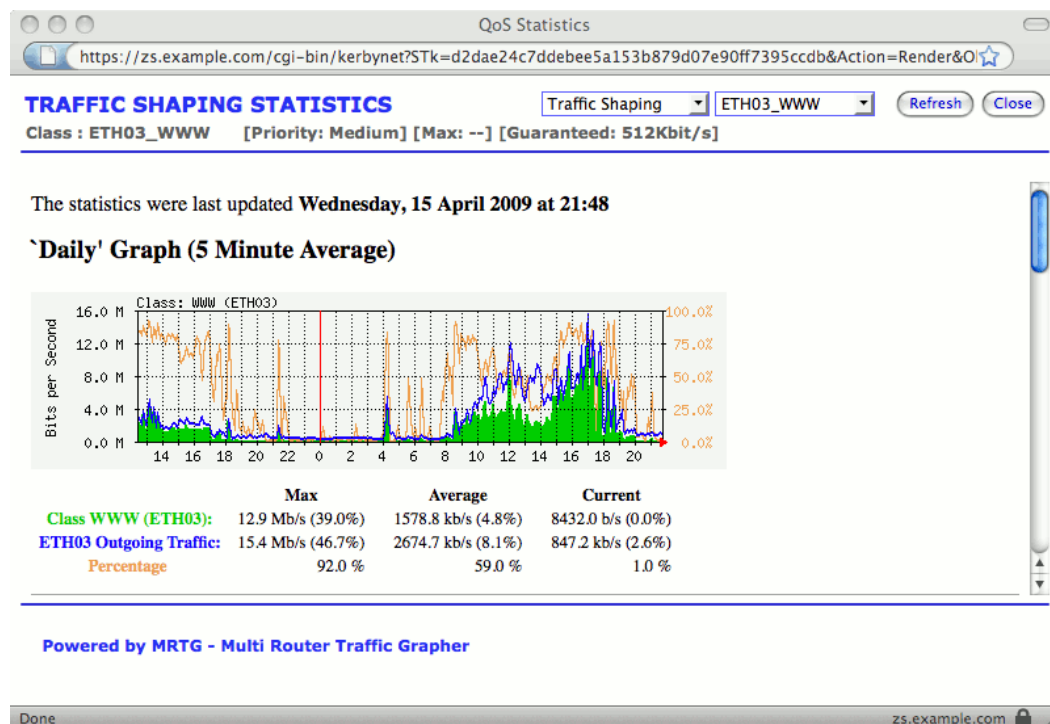


Рисунок 1.3 – Приклад моніторингу трафіку за допомогою ПЗ MRTG

Sacti вважається покращеною версією MRTG. Візуально та функціонально будь-який з графіків Sacti схожий з MRTG. Sacti створений на основі RRDTools, розробленої тим самим розробником і є прямим нащадком MRTG.

Sacti більш досконалий, ніж MRTG, з веб-інтерфейсом конфігурації, який дозволяє проводити налаштування простіше та інтуїтивніше. Це повний пакет моніторингу та побудови мережі. Інструмент забезпечений швидким опитуванням, розширеними шаблонами пристроїв та графіків, декількома методами збору даних та функціями керування користувачами. Це чудово підходить для невеликих локальних мереж, але так само добре для складних мереж із тисячами пристроїв на кількох сайтах.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

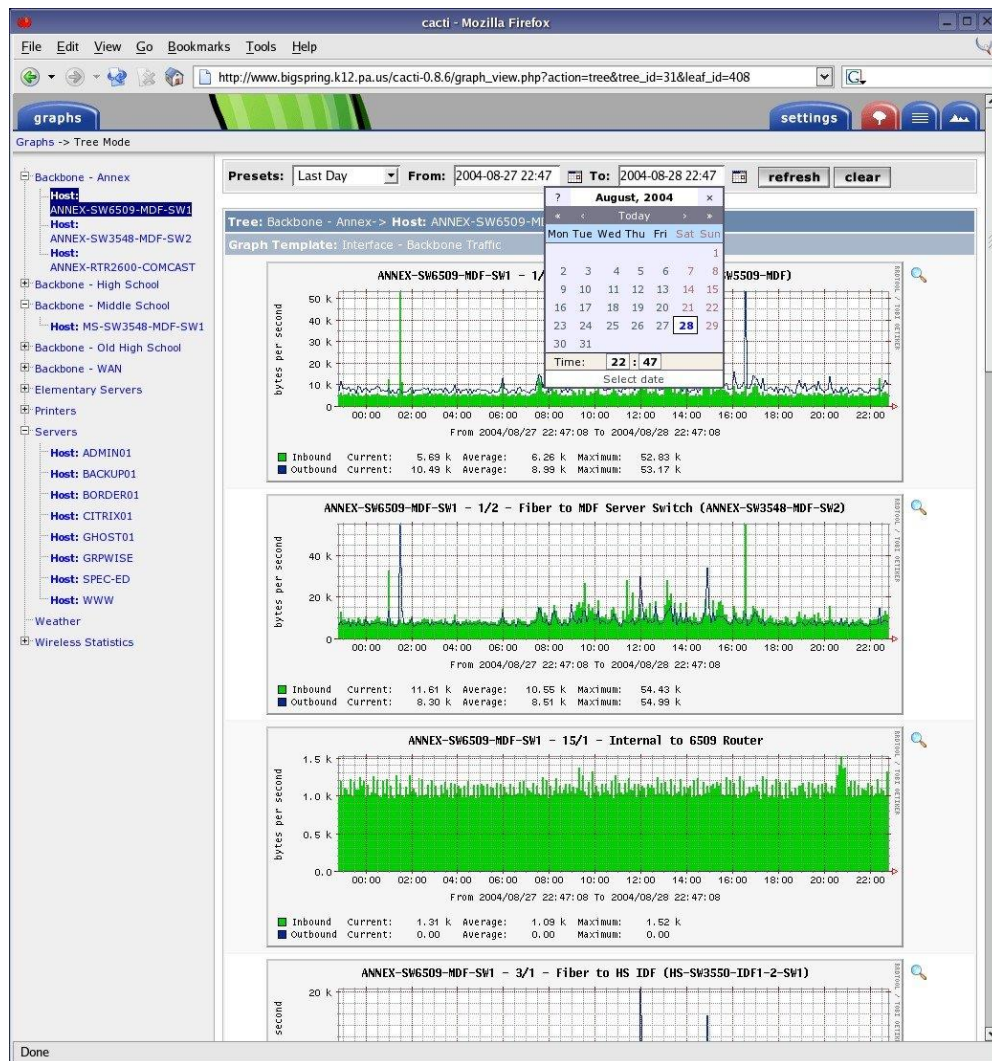


Рисунок 1.4 – Приклад моніторингу трафіку за допомогою ПЗ Cacti

Cacti створено на основі ПЗ RRDtool. За словами його розробника, «RRDtool – це галузевий стандарт OpenSource, високопродуктивна система реєстрації та відображення даних для тимчасових рядів. RRDtool може бути легко інтегрований у сценарії оболонки, програми Perl, Python, Ruby, Lua або Tcl». RRDtool є прямим нащадком MRTG. RRDTool є розвитком програмного додатку MRTG на С.

Підсумовуючи Cacti – це інтерфейс RRDTool. Він зберігає необхідні дані для створення графіків та заповнення їх даними у базі даних MySQL. Він повністю написаний на мові програмування PHP. Програмне забезпечення підтримує свої графіки, джерела даних та циклічні архіви у базі даних, а також обробляє збір даних, залишаючи графіки для RRDTool. Багато користувачів Cacti є колишніми користувачами MRTG.

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

SolarWinds Network Performance Monitor - це програма для Windows, яка використовує SNMP для опитування декількох мережевих пристроїв та отримання статистики трафіку від їх інтерфейсів. Результати візуально відображаються на графіках, що відображають статистику використання кожного інтерфейсу. Адміністратор може додати пристрій до інструмента, просто вказавши його IP-адресу та рядок спільноти SNMP. Потім інструмент відправляє запит до пристрою і перераховує всі доступні параметри та дозволяє йому вирішити, які з них адміністратор хоче включити до своїх графіків. Наприклад, мережний комутатор виставлятиме кожному інтерфейсу трафік і лічильники помилок.

Монітор продуктивності мережі має багато інших функцій. Одним з основних є його масштабованість. Інструмент працюватиме з невеликими мережами, але легко масштабується до великих мереж, що з десятків тисяч вузлів, розподілених за різними адресами. NPM також може створювати карти мережі та відображати наочне уявлення про критичний шлях між двома пристроями або службами.

Насправді SolarWinds NPM – це набір з безлічі інструментів, які включають один із найкращих інструментів моніторингу мережі SNMP.

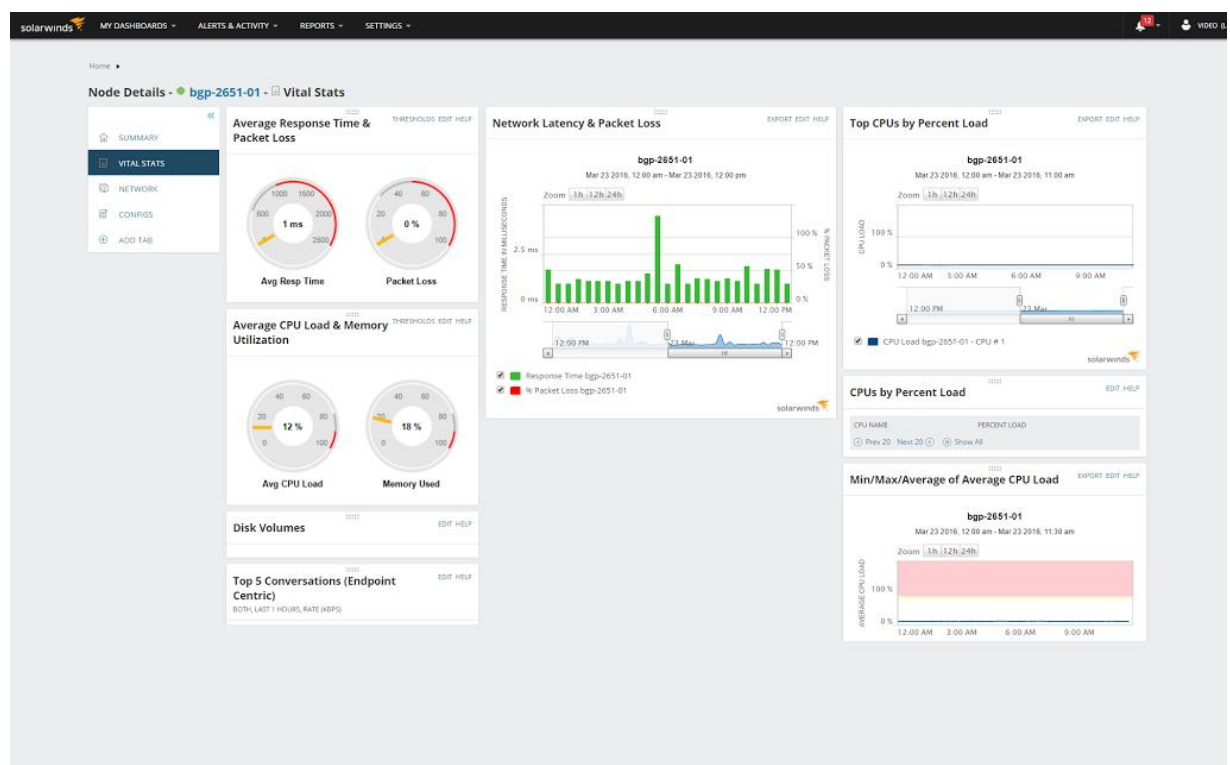


Рисунок 1.5 – Приклад моніторингу трафіку за допомогою ПЗ SolarWinds NPM

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

ІТ-компанія ManageEngine пропонує комплексні та прості рішення навіть для найскладніших завдань управління ІТ. ManageEngine добре відомий своїм високоякісним програмним забезпеченням, включаючи кілька інструментів моніторингу мережі.

SNMP Bandwidth Monitoring – це програмне забезпечення для моніторингу пропускної здатності SNMP. Він є частиною безкоштовного пакету ManageEngine OpUtils, який включає набір з 16 утиліт управління мережею. Програмне забезпечення працює як у Windows, так і на Linux. Кожен користувач має можливість отримати безкоштовну версію, яка дозволяє відстежувати до 10 пристроїв та їх інтерфейсів. ManageEngine SNMP Bandwidth Monitoring також має платну версію без обмежень пристрою. А розробники пропонують безкоштовну 30-денну версію повного програмного забезпечення OpsUtil.

Налаштування інструменту досить просте, потрібно лише вказати підмережу для сканування, а також рядок спільноти SNMP для використання. Відразу після попередніх налаштувань інструмент автоматично виявляє пристрої у вказаній підмережі, які відповідають зазначеному рядку. Після виявлення пристроїв на вкладці «Інвентаризація» можна переглянути стан інтерфейсів кожного пристрою. І, звичайно, можна відображати графіки використання пропускної здатності мережі за одиницю часу.

Звіти – це ще один сильний бік цього інструменту. Наприклад, можливо створювати звіти про використання пропускної смуги за останні 12 годин – один місяць. Крім цього оповіщення інструменту є досить потужним. У адміністратора мережі є можливість встановити порогові значення та отримувати повідомлення електронною поштою або SMS-повідомленнями, коли вони перевищені.

ManageEngine SNMP Bandwidth Monitoring є одним з найкращих сучасних рішень моніторингу для мереж середнього та великого розміру за рахунок великої кількості протоколів та технологій, що підтримуються даним програмним застосуванням.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

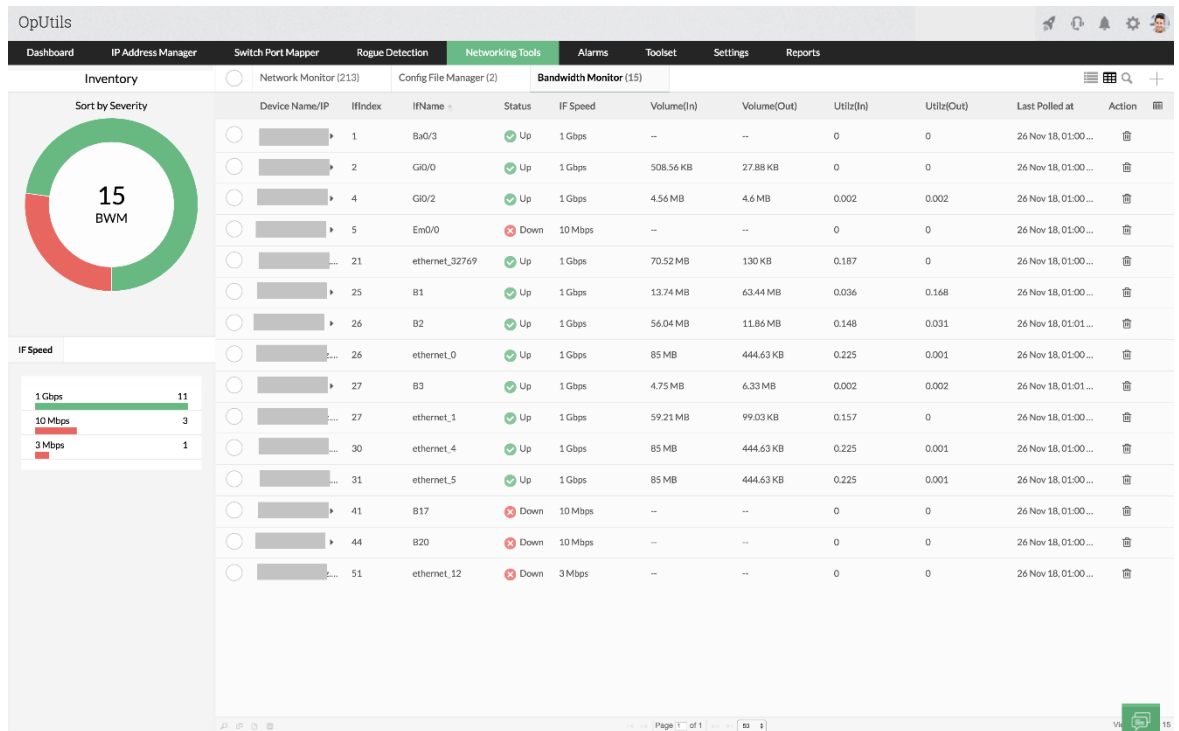


Рисунок 1.6 – Приклад моніторингу трафіку за допомогою ПЗ ManageEngine SNMP Bandwidth Monitoring

Raessler – німецька компанія – пропонує одне з найкращих рішень для моніторингу, яке дуже нагадує Cacti або навіть MRTG. Однак, PRTG має більш професійний вигляд та функціонал.

За словами розробників Raessler, адміністратор може налаштувати PRTG за декілька хвилин. Налаштування продукту є винятково легким, що є досить великим плюсом.

PRTG Desktop — це альтернативний інтерфейс, який можна використовувати для підключення до основного сервера PRTG або екземпляра PRTG Hosted Monitor, щоб проводити налаштування, переглядати результати моніторингу та стежити за своєю мережею.

PRTG Desktop — це кросплатформна програма для швидкого доступу до даних та керування моніторингом.

Кількість особливостей та той досвід, що вони дають користувачу досить вражаючі. По-перше, ПЗ дає можливість вибирати між декількома різними інтерфейсами користувача. Тут є корпоративна консоль Windows, веб-інтерфейс на основі

Аяx, а також мобільні програми для Android та iOS. Одна з особливостей мобільних програм – це можливість сканувати ярлик QR-коду. Тобто, будь-який користувач може роздрукувати з програмного забезпечення та прикріпити до пристроїв, щоб негайно приєднати ці пристрої до графіків.

Графіки у PRTG вважаються одними з найкращих серед подібного програмного забезпечення. PRTG може не тільки відстежувати пристрої та використання пропускної смуги. Він може записувати багато інших параметрів, використовуючи SNMP, WMI, NetFlow та Sflow. Інструмент має кілька чудових звітів, які можна запускати на вимогу або планувати, а потім переглядати у форматі HTML або PDF. Крім цього, є можливість експортувати звіти у формати CSV або XML для зовнішньої обробки.

Веб-сайт Paessler дозволяє вибирати між двома різними версіями PRTG. Існує безкоштовна версія або безкоштовна 30-денна пробна версія. Перша обмежить ваші можливості моніторингу до 100 датчиків. Paessler враховує кожен параметр, який контролюється як один датчик. Наприклад, для моніторингу смуги пропускання на кожному порту 48-портового комутатора потрібно 48 датчиків.

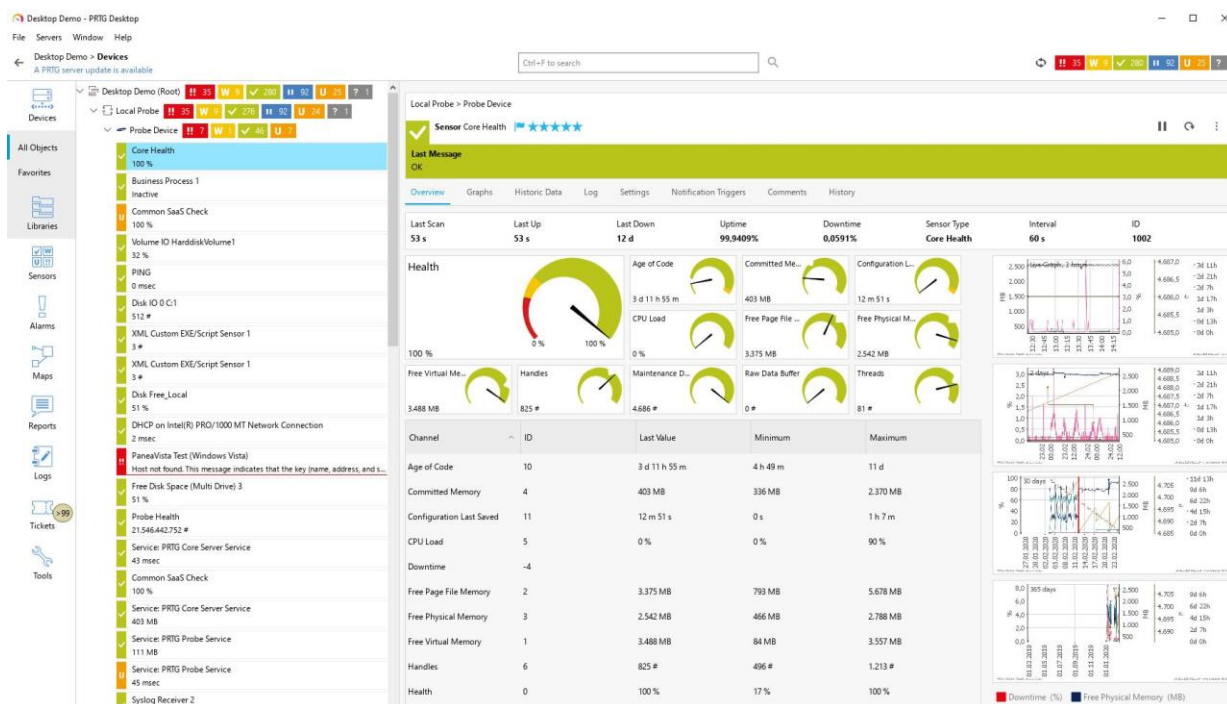


Рисунок 1.7 – Приклад моніторингу трафіку за допомогою ПЗ PRTG

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3 Проблеми безпеки протоколу SNMP

На момент написання дипломного проекту існує 3 основні версії протоколу SNMP. Під час кожного з етапів еволюції версій було значно покращено захист протоколу. Важливим є детально розглянути проблеми безпеки кожної з версій [6].

Один з найбільш помітних недоліків SNMP v1 – відсутність розвиненої системи захисту даних на рівні, необхідному для мереж масштабу підприємства.

У SNMPv1 захист адміністративної інформації трактувався надто спрощено: вона базувалася на використанні колективного імені (Community Name), яке, перебуваючи у заголовку SNMP, несло у собі всі можливості захисту повідомлень. Цей засіб (відомий під назвою тривіальний протокол) вимагав, щоб програма-агент і менеджер впізнали однакове колективне ім'я, перш ніж продовжити виконання операцій мережевого адміністрування. В результаті багато адміністраторів мереж обмежувалися у своїй роботі лише функціями моніторингу, забороняючи видачу команди SET, здатної змінювати параметри конфігурації віддаленого пристрою. Це призвело до того, що користувачі уникали команд SET: такий примітивний засіб захисту, як колективне ім'я, міг дати можливість особам, які не наділені відповідними повноваженнями, змінювати параметри, про що користувачі могли навіть не дізнатися. До того ж, вся критично важлива інформація передавалася у відкритому вигляді.

У зв'язку з цим було розроблено пропозиції щодо вдосконалення захисту у межах SNMPv1, подані у липні 1992 р.; вони становили основу структури захисту для SNMPv2. Протягом 1993 було опубліковано 11 RFC, які визначали нові стандарти SNMP. Перший з них, RFC 1441 є введенням в SNMP версії 2 (SNMPv2).

Стандартами захисту SNMPv2 визначаються методи аутентифікації (DAP – Digest Authentication Protocol) та забезпечення конфіденційності (SPP – Symmetric Privacy Protocol) інформації адміністративного характеру. В основі лежить концепція учасника (party) - унікального набору параметрів захисту, який може включати розташування мережі, протоколи аутентифікації та забезпечення конфіденційності, що використовуються між агентом і менеджером.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Новий тип пакетів get-bulk-request дозволяє менеджеру ефективно обробляти великі блоки даних. Ще один новий тип пакетів inform-request дозволяє одному менеджеру надсилати інформацію іншому менеджеру. Визначено два нових MIB: MIB SNMPv2 та MIB SNMPv2-M2M (менеджер-менеджер). SNMPv2 надає покращену секретність порівняно з SNMPv1. У SNMPv1 ім'я спільноти передається від менеджера до агента як відкритого пароля. SNMPv2 надає аутентифікацію та розширену секретність.

Однак друга версія SNMP не була підтримана виробниками мережного обладнання та поширення не набула. Але останнім часом розробники стандартів із IETF намагаються переламати ситуацію, запропонувавши специфікацію третьої версії SNMP. Істотні покращення протоколу, що забезпечують гнучке адміністрування агентів систем управління та захист керуючої інформації, зворотна сумісність із системами на основі базової версії SNMPv1, а також відкрита архітектура дозволяють авторам SNMPv3 сподіватися на успішне практичне втілення версії.

При розробці SNMPv3 чимало уваги було приділено безпеці протоколу. Починаючи з даної версії стала підтримуватися модель, орієнтована на користувача (User-BasedSecurityModel (скорочено USM) завдяки якій стало можливим додавання модулів аутентифікації і шифрування без зміни базової архітектури. Модель USM включає в себе модуль аутентифікації, модуль шифрування і модуль контролю часу. При цьому, модуль аутентифікації і шифрування займаються захистом даних, а модуль контролю часу синхронізує час між сутностями SNMP.

Основні проблеми, які необхідно було вирішити за допомогою моделі USM:

- Можливість відкладання яких дій на невизначений час або повторення одних і тих же дій з довільними інтервалами;
- Зміна даних сутностями не пройшли аутентифікацію;
- Можливість заблокувати обмін даними між сутностями;
- Можливість перехоплення трафіку при передачі між сутностями;
- Можливість «маскараду», тобто сутність не пройшла аутентифікацію, могла прикинутися сутністю пройшла аутентифікацію.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

Проблему було вирішено таким чином: для кожного мережевого пристрою пароль перетвориться в деякий унікальний ключ. Це забезпечує додаткову безпеку тому навіть у тому випадку, якщо ключ буде перехоплений, зломисник отримає доступ тільки до одного мережного пристрою. Для шифрування пароля використовується алгоритм MD5, але розробники вирішили, що це не забезпечить достатнього захисту пароля і тому блок PDU двічі хешується за допомогою двох різних ключів, які в свою чергу генеруються з закритого ключа. Пізніше, перші 12 октетів використовуються як код аутентифікації повідомлення, який додається до повідомлення. Такий же процес потрібно проводити на іншій стороні, але тільки у зворотному порядку. Незважаючи на всю складність і енергоємність процесу передачі даних між сутностями SNMP, на думку розробників, алгоритм шифрування (DES) насправді не забезпечує достатнього захисту інформації, тому надалі передбачається використовувати інші алгоритми.

Розробниками передбачено 3 рівня безпеки:

- noAuthNoPriv - паролі передаються у відкритому вигляді, конфіденційність даних відсутня.
- authNoPriv - аутентифікація без конфіденційності. Більшість користувачів використовує саме цей рівень захищеності тому, що він вже досить високий, а мережеві пристрої не перевантажуються шифруванням даних.
- authPriv - аутентифікація і шифрування. Максимальний рівень захищеності.

Як правило, адміністратори спочатку вибирають другий рівень безпеки і лише деякі з них, потім починають використовувати третій. Однією з причин, по якій не використовується третій рівень, є те, що він перевантажує мережеві пристрої.

На даний момент закінчена розробка нової специфікації DataOverCableServiceInterfaceSpecification, а для управління ключами багато користувачів вже використовують алгоритми Діффі-Хеллмана (Diffie-Hellman) і Kerberos замість DES. Це означає, що скоро можна буде очікувати вихід нової версії протоколу SNMP.

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Тобто, третя версія являє собою найбільш захищений на даний момент варіант протоколу SNMP. Щоб дослідити проблеми безпеки саме цієї версії потрібно розглянути основні атаки на протокол.

Основними вразливостями та атаками на протокол SNMP є:

- Вразливість у стандартній конфігурації Windows SNMP-сервісу.
- Проблема в OS Solaris версії до 2.6.
- SNMP Amplification (DDOS-атака).

Вразливість у стандартній конфігурації Windows SNMP сервісу дозволяє віддалено конфігурувати мережеві параметри, які впливають на безпеку та правильне функціонування системи (якщо адміністратор сам запустив SNMP Service)

При конфігурації за замовчуванням, SNMP service відповідає стандартне community (ім'я) "public", яке має права читання і запис. Community - це ім'я, яке має такі ж функції, як логін і пароль в системах.

Протокол SNMP надає два рівні повноважень: read-only and read-write, проте до виходу SP4 Windows NT SNMP Service не дозволяв конфігурувати communities доступу, відмінному від read-write!

Якщо спробувати убезпечити SNMP Service шляхом перейменування community для доступу, система залишиться незахищеною від крякера, що має обліковий запис на машині, так як параметри SNMP Service знаходяться в реєстрі і доступні всім користувачам на читання. Також Windows NT SNMP Service має можливість обмежити доступ для списків IP-адрес. На перший погляд, це дозволяє захиститися від атак невідомих систем, однак це не є проблемою для крякерів (що необхідно розуміти будь-якому адміністратору), оскільки протокол SNMP використовує UDP протокол для обміну інформацією, а він є протоколом без встановлення з'єднання, тому можлива заміна вихідної адреси (але для цього доведеться переробити вихідні дані SNMP менеджерів під Unix і вивчити UDP spoofing)

SNMP "set" операції (дозволяють змінювати значення змінних) можуть бути з заміною зворотного адреси будь-якої, оскільки відповідь не потрібний. Однак якщо включено обмеження довірених IP адрес, але доведеться знайти акаунт на системі, що атакується, і витягти довірену інформацію з реєстру.

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

Завдяки налаштованому за промовчанням Windows NT SNMP Сервісу ми можемо отримати за допомогою SNMP менеджера майже всі інформацію щодо пристроїв, що дає змогу зловмиснику проводити різні маніпуляції з ними.

В OS Solaris версії до 2.6 виходячи з ISS Security Advisory (November 2nd, 1998), в агенті SNMP, який за замовчуванням запущений у цій системі, існують реальні загрози отримати доступ на рівні рута, маніпулювати процесами та параметрами машини.

Для доступу до MIB-інформації існує прихована "undocumented community string", яка дозволить атакуючому змінити більшість системних параметрів.

На жаль, саме це community не називається, проте ISS Internet Scanner і ISS RealSecure real-time intrusion detection можуть детектувати цю проблему, тобто. можна подивитися і в їх вихідних файлах.

Суть атаки SNMP Amplification полягає в тому, щоб ініціювати багаторазово збільшену відповідь на SNMP-запит. Спочатку розроблені для автоматизації отримання табличних даних при мінімізації кількості пакетів, що відправляються, BULK-запити стали досить ефективним інструментом проведення DDoS-атак в руках зловмисників. Як говорить RFC3416, GetBulkRequest, реалізований в SNMP версії 2, призначений для можливості запросити великий обсяг даних, чим і користуються атакуючі, залучаючи неправильно настроєні сервери в інтернеті.

Якщо встановити максимальну кількість рядків, що повертаються в таблиці 20000 і виконати запит на адресу неправильно налаштованого сервера/пристрою відповідь видасть приблизно таке: *iso.3.6.1.6.3.18.1.1.1.8.123.123.12.123.123.12.123.123.12 .123.123.12 = No more variables left in this MIB View (It is past the end of the MIB tree).*

У відповідь на запит розміром близько 70 байт з урахуванням заголовків сервер повертає відповідь розміром близько 10 кілобайт, тобто майже в 150 разів більше. Коефіцієнт посилення не фіксований і може приймати як більше (досягаючи 1700 разів), так і менше значення, залежно від типу ОС та параметрів конфігурації пристрою. Якщо під час формування подібного запиту використовувати

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

заміну IP-адреси відправника на адресу жертви та високу інтенсивність звернень до вразливого сервера, DDoS-атака буде успішно виконана.

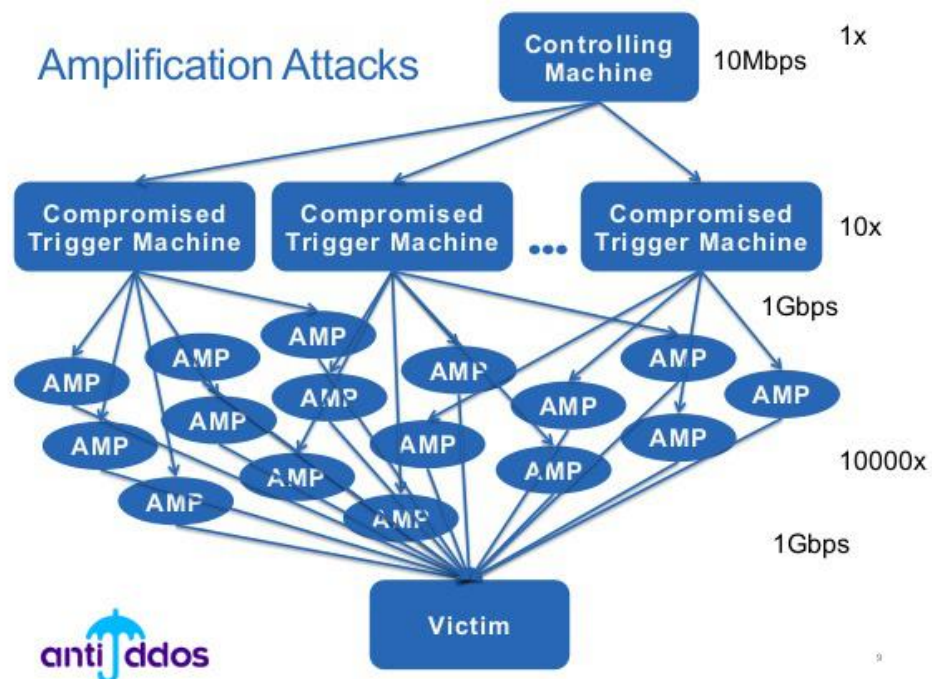


Рисунок 1.8 – Схематичне зображення атаки SNMP Amplification

Захист від DDoS атак типу SNMP Amplification передбачає усунення можливостей підміни адрес та усунення вразливостей протоколу UDP. Загальні рекомендації для вразливих атак з використанням заміни адреси протоколів на базі UDP надані в BCP38 і RFC2827.

Специфічні для SNMP рекомендації щодо забезпечення безпеки сервера або мережного обладнання можна поділити на такі напрямки:

- Архітектурне: дозвіл обробки запитів лише на інтерфейсах, недоступних із не довірених мереж.
- Зміна community на більш непередбачуване.
- Обмеження IP-адрес керуючих станцій.
- Обмеження гілки OID, доступної для отримання/зміни SNMP.
- Мінімізація чи відмова від використання community читання і запис.

- Перехід на SNMP версії 3 за допомогою додаткових параметрів аутентифікації та шифрування.
- Вимкнення SNMP, якщо не використовується.

1.4 Застосування протоколу SNMP для побудови систем кіберзахисту

Simple Network Management Protocol (SNMP) був розроблений для віддаленого моніторингу мережевих пристроїв через IP-мережі. SNMP використовується для збору інформації з мережевих пристроїв, таких як маршрутизатори, комутатори, а також для Windows і IBM Power Systems, а також для конфігурації та модифікації. Використовуючи SNMP, компанії можуть перехоплювати повідомлення всередині рішень SIEM або моніторингу та сповіщати когось про отримання певного повідомлення. Оскільки SNMP також можна використовувати для модифікації пристрою, компанії мають можливість відповідати на конкретне повідомлення, щоб виправити проблему, що підтримує автоматизацію.

Найближчим по функціоналу рішенням замість протоколу SNMP вважається Syslog [7]. Саме тому досить важливим є порівняння даних протоколів.

Ось основні відмінності між SNMP та системним журналом:

- Сповіщення в режимі реального часу порівняно з історичними даними – SNMP був розроблений, щоб попередити вас про подію в режимі реального часу. Syslog був розроблений, щоб забезпечити спосіб централізації інформації журналу для історичних цілей.
- Pull або push – SNMP надсилає запит на пристрій, який шукає інформацію, тоді як сервер системного журналу просто є сховищем інформації, яку потім можна запитати для отримання більш детальної інформації.
- Надійність – пристрої системного журналу не можуть гарантувати, що їхнє повідомлення надходить до сервера системного журналу. SNMP опитує пристрій, щоб отримати інформацію, і тому не може втратити дані.
- Проактивне проти реактивного – SNMP може реагувати на пастку і вживати певних заходів. Syslog не може цього зробити.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

- Зміна статусу або детальна інформація – SNMP попереджає про зміну статусу, наприклад, рядок тепер недоступний. Syslog може містити більш детальну інформацію про те, чому щось сталося.

- Безпечні проти незахищених – SNMP-повідомлення безпечні і не можуть бути підроблені. Хоча Syslog не захищений, і повідомлення можна підробити.

Незважаючи на поштовх до підвищення безпеки, компанії також хочуть покращити свою автоматизацію. SNMP дозволяє компаніям проявляти активність у реагуванні на проблеми здоров'я системи, що має вирішальне значення для доступності та продуктивності системи. SNMP пропонує можливість опитування щодо певної події та реагування на основі відповіді. Якщо сталася подія, адміністратор може вжити заходів, щоб її виправити. Велика перемога для бізнесу.

За допомогою syslog компанії можуть централізувати всю аудиторську інформацію в одному місці. Це особливо корисно для складання аудиторських звітів. Потім вони можуть використовувати рішення для моніторингу, наприклад AbsMessage, щоб попередити когось про отримання певного повідомлення або автоматично ініціювати відповідь, забезпечуючи реагування на загрози безпеці в режимі реального часу, зменшуючи ризик.

Хороша новина полягає в тому, що користувачам не потрібно вибирати між SNMP і syslog. Головне — знайти рішення для моніторингу, які підтримують формати SNMP і syslog, щоб підвищити безпеку, працездатність та продуктивність IBM i.

Підсумовуючи, протокол SNMP являє собою одне з найкращих рішень для моніторингу мережі. У будь-якій системі кіберзахисту моніторинг мережі є одним з найважливіших етапів розслідування інцидентів кібербезпеки. Також дуже важливим є кількість джерел з яких підсистема моніторингу черпає інформацію, тому SNMP чудово підходить за даним критерієм. Крім того, версія SNMPv3 є досить захищеною, що дозволяє використовувати її в системах кіберзахисту. Дана практика вже використовується великими корпораціями у процесах обміну.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до першого розділу

У першому підрозділі було розглянуто основні теоретичні відомості щодо протоколу SNMP, наведено архітектуру, основні реалізації обміну повідомленнями. Також наведено порівняння основних версій протоколу в порядку зростання.

У другому підрозділі було наведено прикладні реалізації використання протоколу SNMP для моніторингу мережі. Було порівняно варіанти реалізації моніторингу за допомогою додатків на базі ОС Windows та Linux. В результаті порівняння з'ясовано, що найкращим рішенням буде використання ПО ManageEngine SNMP Bandwidth Monitoring або PRTG.

У третьому підрозділі проаналізовано основні проблеми безпеки протоколу SNMP. З'ясовано, що незважаючи на досить сильний захист протоколу третьої версії все ж існують певні проблеми, які найчастіше зв'язані з бекдорами ПО на різних ОС.

У четвертому підрозділі розглянуто роль протоколу SNMP у проектуванні та будівництві системи кібрзахисту на базі моделі додатків SIEM.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ МОНІТОРИНГУ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА БАЗІ ПРОТОКОЛУ SNMP ТА АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ

2.1 Проектування підсистеми моніторингу вразливостей та комп'ютерної мережі

При проектуванні було використано трьохрівневу модель мережі від компанії Cisco Systems [8]. Дана модель є ієрархічною та передбачає, що мережа будується з використанням трьох безпосередньо залежних один від одного рівнів. Це такі рівні:

- рівень ядра;
- рівень розподілу;
- рівень доступу.

Глобальну мережу організації було спроектовано за допомогою графічного редактору Draw.io. Загальну топологію мережі наведено на рис. 2.1:

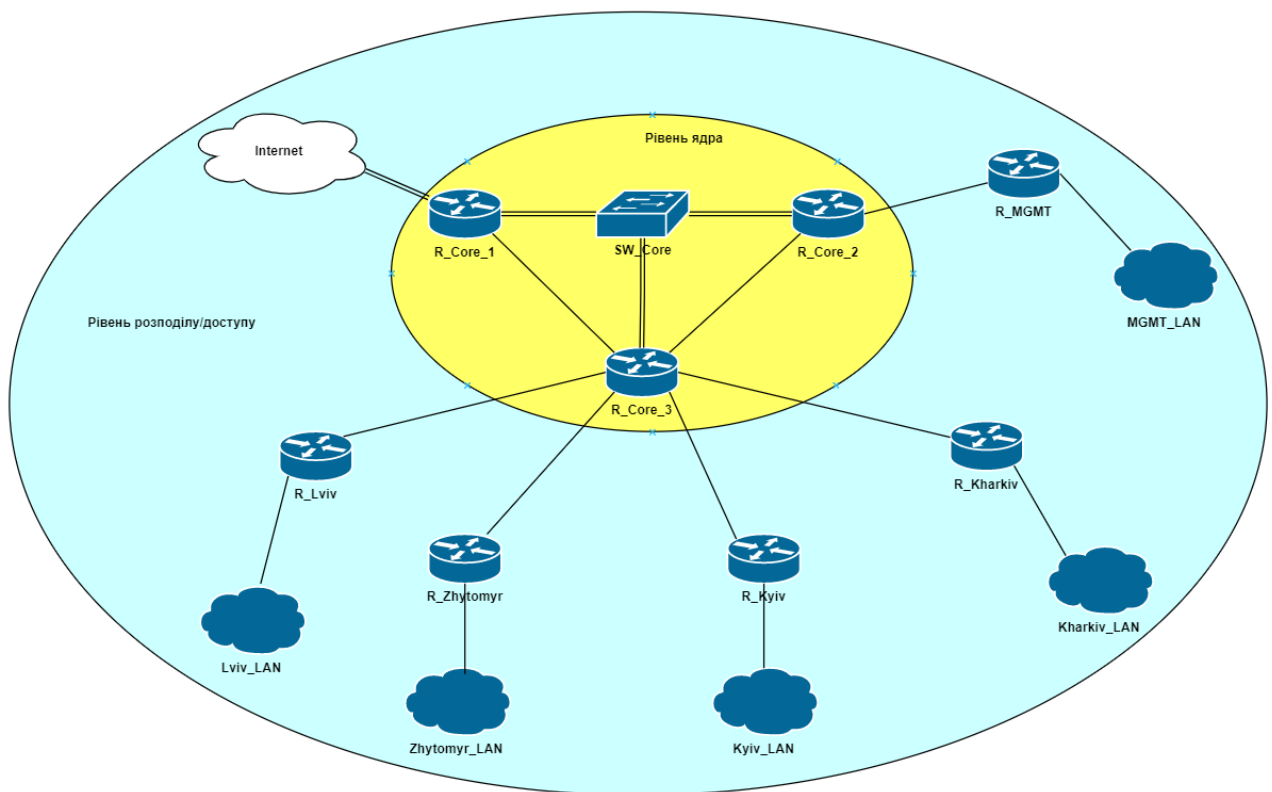


Рисунок 2.1 – Загальна топологія мережі

Рівень ядра складається з 3 маршрутизаторів та 1 комутатора, з'єднаних між собою високошвидкісними каналами зв'язку на базі технології Gigabit Ethernet. Канали між роутерами до комутатора проагреговано для збільшення пропускної здатності мережі. Також до одного з маршрутизаторів реалізовано вихід в глобальну мережу за допомогою транляції адрес за протоколом NAT.

Рівень розподілу та доступу представляє собою набір з 5 маршрутизаторів, що під'єднані до ядра мережі та кінцевого устаткування. Дані пристрої є ключовими під час передачі трафіку віддалених мереж. З'єднання з ядром мережі виконано за допомогою витої пари Gigabit Ethernet. Канали між роутерами розподілу та роутерами ядра проагреговано для збільшення продуктивності мережі. Також одна з локальних мереж являє собою мережу для адміністрування пристроїв за допомогою протоколу SNMP.

В загальному у мережі використано 8 маршрутизаторів, 6-ти комутаторів. Мережа складається з 5 локальних мереж.

До кожного маршрутизатора доступу підключено 1-2 мережі. Розглянемо детальніше кожну з них.

Від маршрутизатора R_Zhytomyr виходить локальна мережа LAN_Zhytomyr. Проект даної ділянки зображено на рисунку 2.2.

У своєму складі мережа LAN_Zhytomyr має 186 ПК та 9 комутаторів на 24 порти, до кожного комутатора підключено 21 ПК, один порт SW_Zhytomyr задіяний для підключення до R_Zhytomyr та по 2 порти кожного комутатора для агрегованого каналу між ними, оскільки у подібній топології пропускна здатність є дуже важливим аспектом. На всіх комутаторах, окрім з'єднуючого з R_Zhytomyr, 1 порт залишається вільним. Підключення до маршрутизатора виконане за допомогою витої пари технології Gigabit Ethernet. Всі інші підключення даних мереж реалізовані за допомогою технології Fast Ethernet та знову ж витої пари. На прикладі даної мережі побудовано ще декілька LAN'ів для міст з можливістю розширення. Дані мережі являють собою LAN'и до яких підключаються користувачі мережі.

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

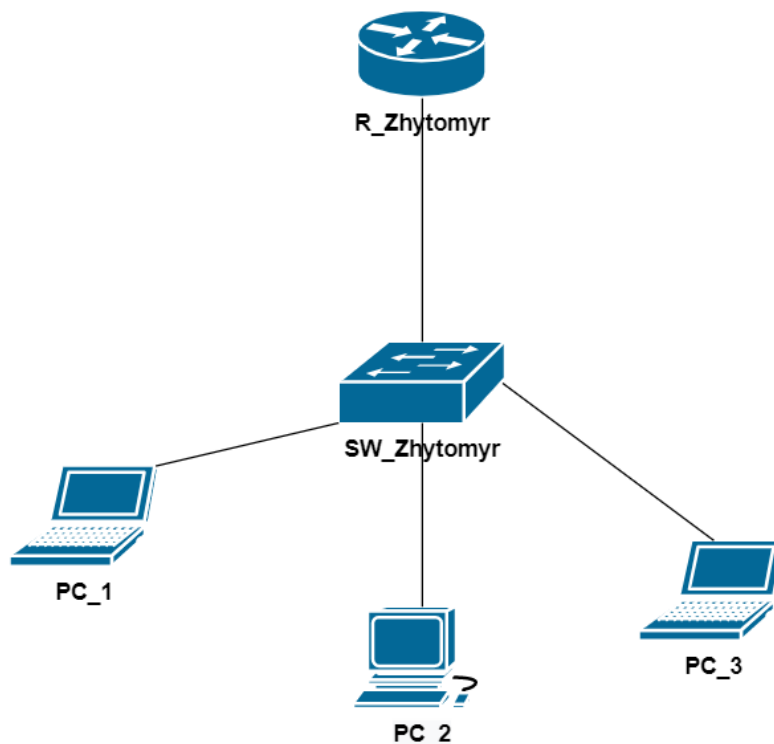


Рисунок 2.2 – Загальний вигляд мережі LAN_Zhytomyr

Маршрутизатор R_Core_1 представляє собою з'єднуюче звено між топологією та глобальною мережею. На маршрутизаторі налаштовано трансляцію адрес локальних мереж за протоколом PAT(NAT). Адресу для доступу до мережі отримано за допомогою протоколу динамічної адресації DHCP. Проект даної ділянки зображено на рисунку 2.3.

Дана мережа представлена 1 маршрутизатором та хмарою, яка представляє Інтернет. Маршрутизатор в даній мережі є частиною ядра мережі, що дозволяє всім пристроям топології отримати доступ до глобальної мережі. Для надання доступу налаштовано динамічну маршрутизацію за допомогою протоколу EIGRP.

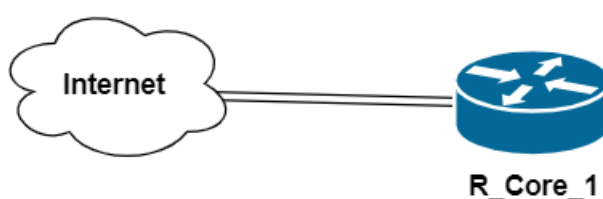


Рисунок 2.3 – Загальний вигляд ділянки доступу до WAN

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

Від маршрутизатора R_MGMT виходить 1 мережа - MGMT. Дана мережа використовується для віддаленого адміністрування, моніторингу та тестування безпеки мережі. Проект даної ділянки зображено на рисунку 2.5.

Мережа MGMT представлена 28 ПК та 2 комутаторами на 26 портів, до кожного комутатора підключено 14 ПК, по 1 порту задіяно для підключення до R_MGMT та між комутаторам. На комутаторах по 10 портів є вільними, тобто виступають резервними. Підключення до маршрутизатора та між комутаторами виконане за допомогою витої пари технології Gigabit Ethernet. Всі інші підключення даної мережі реалізовані за допомогою технології Fast Ethernet та знову ж витої пари.

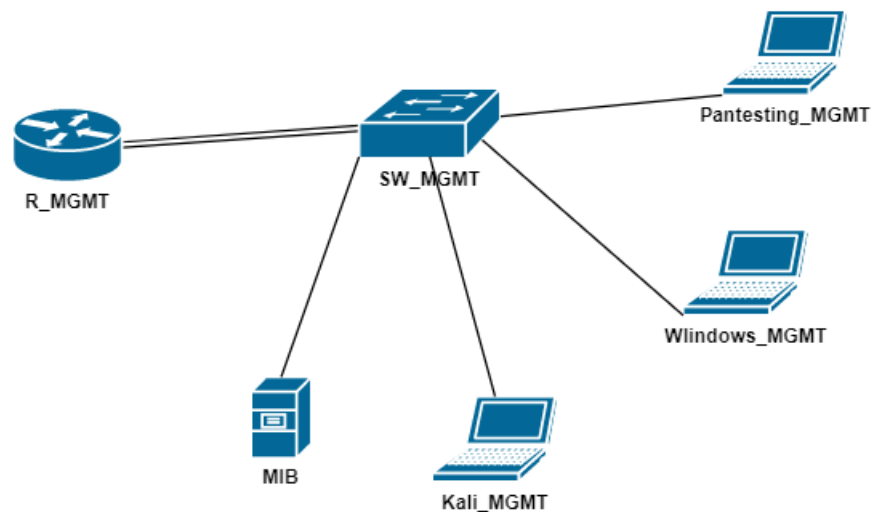


Рисунок 2.4 – Загальний вигляд мережі MGMT

Одним з найважливіших етапів під час проектування топології є розробка схеми адресації мережі для уникнення дублікатів адрес та можливих проблем в функціонуванні мережі.

Під час розробки схему адресації, увагу було звернено в першу чергу на оптимальну кількість IP-адрес, не забуваючи про можливість розширення поточних мереж.

Для пристроїв рівня ядра було розраховано наступні IP-адреси мереж. Частина IP-адрес будуть належати пристроям рівня розподілу/доступу для взаємодії між ними. Розрахунки подано у вигляді таблиці 2.1.

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.1 – Параметри адресації пристроїв ядра

Пристрої	Мережа
R_Core_1, R_Core_2, R_Core_3	192.168.1.0/28
R_Core_1, Internet	DHCP (192.168.122.0/24)
R_Core_2, R_MGMT	192.168.20.0/30
R_Core_3, R_Lviv	192.168.10.0/30
R_Core_3, R_Zhytomyr	192.168.11.0/30
R_Core_3, R_Kyiv	192.168.12.0/30
R_Core_3, R_Kharkiv	192.168.13.0/30

Більш детального огляду потребує розрахунок IP-адрес локальних мереж. Результати розрахунків подано у вигляді таблиць 2.2 – 2.6.

Таблиця 2.2 – Параметри адресації мережі LAN_Lviv

Призначення	IP-адреса
Адреса мережі	192.168.110.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса вузла	192.168.110.1
Максимальна адреса вузла	192.168.110.254
Широкомовна адреса	192.168.110.255
Шлюз по замовчуванню	192.168.110.1
Діапазон статичних адрес	192.168.110.10 – 192.168.110.10
Діапазон адрес майбутніх ПК	192.168.110.11 – 192.168.110.156
Діапазон вільних адрес	192.168.110.157 – 192.168.110.254

Таблиця 2.3 – Параметри адресації мережі LAN_Zhytomyr

Призначення	IP-адреса
Адреса мережі	192.168.111.0

Продовження таблиці 2.3 – Параметри адресації мережі LAN_Zhytomyr

Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса вузла	192.168.111.1
Максимальна адреса вузла	192.168.111.254
Широкомовна адреса	192.168.111.255
Шлюз по замовчуванню	192.168.111.1
Діапазон статичних адрес	192.168.111.10 – 192.168.111.10
Діапазон адрес майбутніх ПК	192.168.111.11 – 192.168.111.206
Діапазон вільних адрес	192.168.111.207 – 192.168.111.254

Таблиця 2.4 – Параметри адресації мережі LAN_Kyiv

Призначення	ІР-адреса
Адреса мережі	192.168.112.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса вузла	192.168.112.1
Максимальна адреса вузла	192.168.112.254
Широкомовна адреса	192.168.112.255
Шлюз по замовчуванню	192.168.112.1
Діапазон статичних адрес	192.168.112.10 – 192.168.112.10
Діапазон адрес майбутніх ПК	192.168.112.11 – 192.168.112.171
Діапазон вільних адрес	192.168.112.172 – 192.168.112.254

Таблиця 2.5 – Параметри адресації мережі LAN_Kharkiv

Призначення	ІР-адреса
Адреса мережі	192.168.113.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса вузла	192.168.113.1
Максимальна адреса вузла	192.168.113.254
Широкомовна адреса	192.168.113.255
Шлюз по замовчуванню	192.168.113.1
Діапазон статичних адрес	192.168.113.10 – 192.168.113.10
Діапазон адрес майбутніх ПК	192.168.113.11 – 192.168.113.171

Продовження таблиці 2.5 – Параметри адресації мережі LAN_Kharkiv

Діапазон вільних адрес	192.168.113.172 – 192.168.113.254
------------------------	-----------------------------------

Таблиця 2.6 – Параметри адресації мережі LAN_MGMT

Призначення	ІР-адреса
Адреса мережі	192.168.254.0
Маска мережі	255.255.255.224/27
Інвертована маска	0.0.0.31
Мінімальна адреса вузла	192.168.254.1
Максимальна адреса вузла	192.168.254.30
Широкомовна адреса	192.168.254.31
Шлюз по замовчуванню	192.168.254.1
Діапазон статичних адрес	192.168.254.1 – 192.168.254.30
Діапазон адрес майбутніх ПК	–
Діапазон вільних адрес	–

2.2 Аналіз загроз підсистеми моніторингу

Аналіз загроз підсистеми моніторингу полягає у детальному огляді протоколів та технологій налаштованих на пристроях мережі та перевірці можливих атак на них. У спроектованій топології будуть функціонувати наступні протоколи:

- DHCP
- SNMPv3
- EIGRP, який “з коробки” є досить захищеним
- SSHv2
- ARP

Окрім атак на протоколи також можливе проникнення до адміністративних панелей пристроїв мережі з метою отримання привілеїв з подальшою шкодою для системи.

Одним з перших протоколів, на який можливі атаки є DHCP, оскільки його виведення з ладу дозволить зловмиснику “відрізати” локальні мережі з великою

кількістю пристроїв від мережі або ж перехопивши трафік заволодіти критично важливою інформацією. Основними реалізаціями атак на протокол DHCP у спроектованій топології є:

- DHCP Starvation
- DHCP Spoofing

При атаках виснаження ресурсів DHCP зловмисник створює лавинне розсилання із DHCP-запитів на DHCP-сервер, щоб використовувати всі доступні IP-адреси, які може призначити сервер DHCP [10]. Після розподілу всіх IP-адрес, які можуть бути призначені DHCP-сервером, відбувається відмова в обслуговуванні (DoS-атака), оскільки нові клієнти не можуть отримати доступ до мережі. DoS-атака — це будь-яка атака, яка використовується для навантаження конкретних пристроїв та мережевих сервісів несанкціонованим трафіком, внаслідок чого дозволений трафік не може отримати доступу до цих ресурсів.

Під час DHCP-спуфінгу зловмисник налаштовує в мережі несправжній DHCP-сервер, щоб видавати для клієнтів DHCP-адреси. Мета цієї атаки - змусити клієнтів використовувати помилкову службу доменних імен (DNS) і Windows-службу імен Internet (сервер WINS), а також використовувати вузол або пристрій зловмисника як стандартний шлюз [10].

Перед DHCP-спуфінгом часто використовується атака виснаження ресурсів DHCP для відмови від обслуговування санкціонованого DHCP-сервера, завдяки чому набагато простіше впровадити в мережу фіктивний DHCP-сервер.

Незважаючи на досить сильний захист протоколу SNMPv3 все ж деякі варіанти атак можливо провести, отримавши певні авторизаційні дані. Загрозу становлять наступні вразливості та атаки:

- SNMP Amplification
- Вразливість у реалізації SNMPv3 у продуктах Cisco

Суть атаки SNMP Amplification полягає в тому, щоб ініціювати багаторазово збільшену відповідь на SNMP-запит. Спочатку розроблені для автоматизації отримання табличних даних при мінімізації кількості пакетів, що відправляються,

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

BULK-запити стали досить ефективним інструментом проведення DDoS-атак в руках зловмисників. Цитуючи RFC3416, GetBulkRequest, реалізований в SNMP версії 2 [11], призначений для можливості запросити великий обсяг даних, чим і користуються атакуючі, залучаючи неправильно настроєні сервери в мережі.

Якщо встановити максимальну кількість рядків, що повертаються в таблиці 20000 і виконати запит на адресу неправильно налаштованого сервера/пристрою то у відповідь на запит розміром близько 70 байт з урахуванням заголовків сервер повертає відповідь розміром близько 10 кілобайт, тобто майже в 150 разів більше. Коефіцієнт посилення не фіксований і може приймати як більше (досягаючи 1700 разів), так і менше значення, залежно від типу ОС та параметрів конфігурації пристрою. Якщо під час формування подібного запиту використовувати заміну IP-адреси відправника на адресу жертви та високу інтенсивність звернень до вразливого сервера, DDoS-атака готова.

Вразливість у реалізації SNMPv3 у продуктах Cisco існує в кодї аутентифікації у різних реалізаціях протоколу SNMPv3. Віддалений користувач може за допомогою спеціально сформованого пакету SNMPv3, що використовує HMAC-MD5-96 або HMAC-SHA-96 як аутентифікаційний протокол, зробити спуфінг атаки і отримати доступ до деяких даних або змінити конфігурацію пристрою.

SSHv2 – це безпечний протокол зв'язку, який охоплює кілька рівнів архітектури, але за час його використання було знайдено декілька безпекових дір, які дозволяють провести атаки мережі. Такими атаками є:

- SSH Brute-force
- MITM-атака
- Timing attack

Однією з найпопулярніших атак на протокол SSH є атака методом перебору паролів (Brute-force). Найчастіше використовується додаткове ПЗ та певна відкрита база даних паролів (словник). Якщо запустити сервіс SSH, доступ до якого можливий з Інтернету, то в журналі автентифікації користувачів можна спостерігати багато записів невдалого підключення користувача admin/root, так начебто він

постійно вводить невірний пароль. Саме так і виглядає атака методом перебору паролів, більш відома як bruteforce. Найпростішим способом захисту може бути написання правила, що блокує весь доступ. Але це призведе до ряду проблем, першим з яких – як надати доступ до сервісу легітимним користувачам. Інший варіант – переведення роботи протоколу на інший порт. Статистика цього підходу показує, що зміна порта SSH на порт з верхнього діапазону, в значній мірі зменшує кількість спроб несанкціонованого доступу, але звичайно не виключає їх. Важливо відмітити, що той хто сканував порт 22 з таким же успіхом може знайти і порт 22222, на який, ймовірно, буде налаштовано роботу SSH [12]. Однак це слугує одним із запобіжних заходів для досягнення успіху. Також бажано використовувати нестандартні ім'я користувача і паролі, щоб зменшити ефективність brute-force атаки.

MITM-атака – це вид атаки, що ґрунтується на перенаправленні трафіка між двома комп'ютерами для перехоплення інформації, в подальшому її вивчення, знищення або модифікації, тобто порушення цілісності та конфіденційності інформації. Атакуюча сторона отримує дані авторизації користувача і здійснює журналювання усього сеансу зв'язку, запуск команд та їх виконання.

Атака по часу (timing attack) представляє собою атаку стороннім каналом, в якій нападник загрожує криптосистемі, аналізуючи час, потрібний для виконання різних операцій. Кожна дія на комп'ютері вимагає певного часу, і цей час може різнитися залежно від даних на вході. У випадку атаки по часу на SSH зломисник може дізнатися коли користувач вводить дані авторизації і перехопити їх. На рис. 1 зображено, що після натискання клавіші виконується певна операція відправлення символу на SSH сервер.

В даному випадку зломисник може переглянути коли користувач використовував команду “su” яка виглядає як два 20 бітові пакети після яких слідує пакет “Password:” розміром 28 біт, всі наступні пакети до пакету “Prompt” є символами паролю, діставши які зломисник може отримати доступ до серверу.

Незважаючи на механізми шифрування та автентифікації, які використовує протокол SSH, він має дві слабкості, які уможливлюють атаки по часу: по-перше,

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

передані пакети обмежені лише восьми байтами (у випадку блокового шифру), який показує приблизний розмір вихідних даних. По-друге, в інтерактивному режимі, кожне натискання клавіші, яке користувач відправляє на віддалену машину, надсилається в окремому IP-пакеті відразу після того, як натиснута кнопка, що розкриває інформацію про часові інтервали між натискання різних клавіш.

Протокол ARP є одним з найважливіших під час передачі даних у мережі та функціонує на канальному рівні. Виведення з ладу даного протоколу призведе до унеможливлення обміну трафіком мережі, тому його захист має високий пріоритет. Основними атаками на ARP є:

- ARP-spoofing
- ARP-poisoning

Спуфінг ARP (ARP-spoofing) — це тип атаки, під час якої зловмисник надсилає фальсифіковані повідомлення ARP (протоколу розпізнавання адрес) через локальну мережу. Це призводить до пов'язування MAC-адреси зловмисника з IP-адресою законного комп'ютера або сервера в мережі. Як тільки MAC-адреса зловмисника буде підключена до аутентичної IP-адреси, зловмисник почне отримувати будь-які дані, призначені для цієї IP-адреси. Підробка ARP може дозволити зловмисникам перехоплення, змінення або навіть зупинку передачі даних. Атаки підробки ARP можуть відбуватися лише в локальних мережах, які використовують протокол розділення адрес.

Отруєння ARP (ARP-poisoning) – тип атак, націлений на локальні мережі, метою яких є відправлення шкідливих ARP-пакетів на шлюз. Мета атаки - зміна пар "IP-адреса - MAC-адреса". Спочатку ARP був розроблений виключно для максимально ефективної роботи та принципи безпеки не бралися до уваги.

Сама атака є відправкою підробленої ARP-відповіді з метою асоціювати MAC-адресу атакуючого з IP-адресою жертви і навпаки. Як тільки шлюз отримує таку відповідь, відбувається широкомовне надсилання змін і всі пристрої в мережі отримують підроблені дані. Цей крок дозволяє перенаправляти трафік через комп'ютер зловмисника. В результаті, до отримання пакетів реальною IP-адресою призначення вони обробляються/модифікуються атакуючим. Користуючись цим,

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

атакуючий може з легкістю здійснювати шкідливі дії, поки у нього буде доступ до комп'ютера в локальній мережі. Крім атак МІТМ, таким чином організується атака типу "відмова в обслуговуванні", шляхом перенаправлення або відкидання вхідного/вихідного трафіку.

2.3 Побудова моделі загроз підсистеми моніторингу

Для того, щоб мережа працювала без проблем важливо проаналізувати всі можливі загрози на етапі проектування. Найбільш ефективним варіантом реалізації для засвоєння є графічне моделювання. Такий підхід дозволяє наглядно побачити які саме елементи системи є вразливими, під час яких саме процесів та хто становить загрозу мережі.

Моделювання ризиків – це неперервний процес, який допомагає знаходити та зменшувати кількість загроз в системі шляхом прийняття певних дій. Перевага моделювання інформаційних ризиків полягає в тому, що ми отримуємо розуміння реальних атак, чітко визначаємо зв'язок компонентів системи, отримуємо сценарії та ймовірності використання вразливостей та отримуємо розуміння впливу на систему проведення атаки.

Для повного розуміння безпекових аспектів мережі потрібно визначити при моделюванні наступне:

- вимоги безпеки;
- загрози безпеці та потенційні вразливості;
- оцінити критичність загроз і вразливостей.

В результаті моделювання визначено повний перелік можливих загроз мережі. Проаналізовано основні процеси, бази даних та користувачів на стійкість до різного роду загроз, оцінивши критичність кожного з них.

Загрози спроектованій мережі можна описати за їх природою, тобто об'єктивні та суб'єктивні. До об'єктивних загроз належать всі атаки на процеси та від користувачів мережі, хакерів, інших зловмисників. До суб'єктивних різного роду природні явища, катастрофи.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

Для кожної з загроз мережі визначено які властивості інформації вона порушує, які можливі способи її реалізації та джерела виникнення.

В спроектованій мережі об'єктивні загрози становлять хакери, зловмисники, кримінальні ланки та спецслужби. Суб'єктивними загрозами є природні та техногенні явища.

На моделі загроз вказано основні потоки трафіку та взаємодії між елементами мережі. Проаналізовано рівень захищеності та можливі загрози для кожного з елементів.

Результати моделювання схеми загроз за допомогою ПЗ OWASP Threat Dragon [13] наведено на рисунку 2.5.

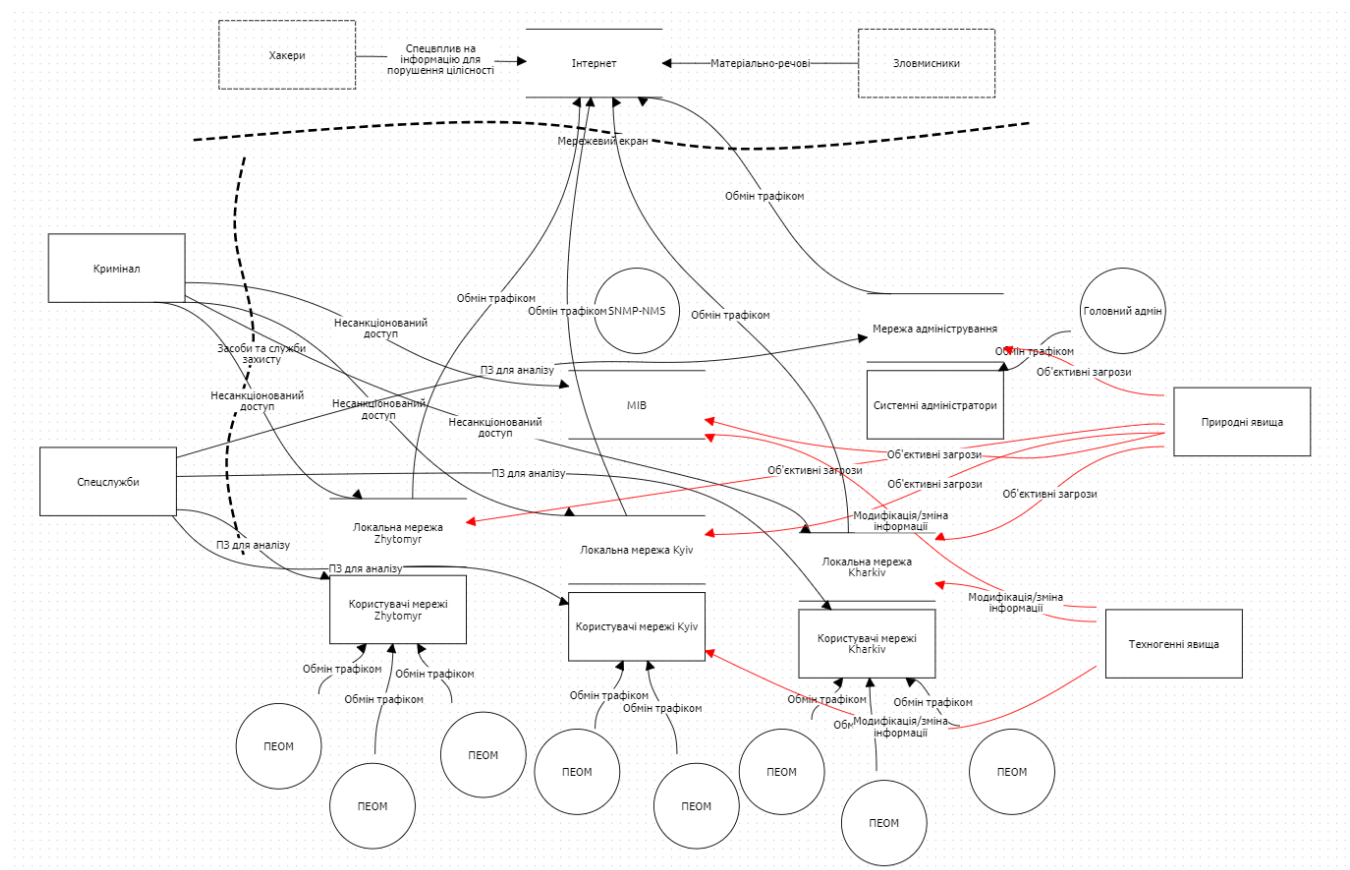


Рисунок 2.5 – Модель загроз мережі організації

Висновки до другого розділу

У першому підрозділі було спроектовано загальну топологію мережі та проекти локальних ділянок за допомогою графічного редактору Draw.io. Розроблено схему адресації всіх пристроїв мережі з урахуванням можливості розширення.

У другому підрозділі було наведено аналіз можливих загроз мережі відповідно до протоколів, які будуть функціонувати у спроектованій мережі. Для кожного з протоколів наведено найбільш поширені варіанти атак та визначено їх можливу шкоду.

У третьому підрозділі побудовано модель загроз мережі організації за допомогою OWASP Threat Dragon. Визначено загроз, класифікуючи кожен з них за природою виникнення. Наведено найбільш критичні ділянки мережі.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ПІДСИСТЕМИ МОНІТОРИНГУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

3.1 Вибір мережевого обладнання

Для реалізації спроектованої комп'ютерної мережі було вирішено використовувати мережеве обладнання компанії Cisco Systems, inc.

При виборі моделі маршрутизатора важливо врахувати його можливості в маршрутизації пакетів складних глобальних мереж. Маршрутизатор повинен відповідати певним вимогам: бути сучасним, містити достатню кількість портів, забезпечити максимально надійну роботу та легке розширення мережі, працювати на необхідній швидкості для передачі та обробки даних.

На рівні ядра потрібен маршрутизатор, який підтримує технологію Gigabit Ethernet, протоколи EIGRP та SNMP, мав додаткові можливості, потрібні в сучасних умовах. Для таких задач найбільш оптимальним варіантом буде маршрутизатор CISCO3945/K9 (рис. 3.1).



Рисунок 3.1 – Маршрутизатор CISCO3945/K9

Маршрутизатор CISCO3945/K9 [9] - це пристрій з інтегрованими сервісами другого покоління ISR G2 (Integrated Services Router Generation 2), що характеризується високою надійністю, посиленням захистом, високою продуктивністю і масштабованістю, і швидкістю маршрутизації до 350Мбіт/с.

До переваг CISCO3945/K9 можна віднести модульну конфігурацію з великою кількістю слотів розширення під EHWIC модуля, сумісні з WIC / VWIC /

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

HWIC, слоти розширення під модулі SM (Service Modules), сумісні з модулями попереднього покоління NM, внутрішні роз'єми під модулі ISM (Internal Service Modules), які замінюють AIM модулі попереднього покоління (Сумісність з AIM немає); внутрішні роз'єми під модулі цифрової обробки сигналів (DSP) - PVDM3 для підтримки голосових і відео функцій (сумісні з PVDM2), а також можливість установки модуля WLAN-контролера для управління до 25 точок доступу Cisco Unified Access Point. Даний маршрутизатор може мати до 4-х вбудованих гігабітних мережевих з'єднань, і можливість установки процесорного модуля SPE (Service Performance Engine). На маршрутизаторі CISCO3945/K9 встановлена версія універсального ПО Cisco IOS Release 15.0 M, всі функції якого доступні в одній повній прошивці, а окремі елементи відкриваються.

На рівні розподілу/доступу потрібен маршрутизатор, який по функціоналу подібний до того, що використовується на рівні ядра. Але на даному рівні можна використати більш доступний пристрій з підтримкою протоколів SNMP та EIGRP та достатнім захистом. Ідеальним вибором буде маршрутизатор Cisco 3660 (рис. 3.2).



Рисунок 3.2 – Маршрутизатор Cisco 3660

Cisco 3660 – надзвичайно гнучка платформа, з широким спектром мережевих модулів. [9]

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Мережеві модулі, що використовуються в серії, сумісні з платформами Cisco 1600, 1700, 2600 та 3600, що забезпечує захист інвестицій та зменшує витрати на підтримку мережі та навчання фахівців.

Відмінними рисами Cisco 3660 є наявність резервного джерела живлення та можливості гарячої заміни модулів. Інтегровані порти на материнській платі Cisco 3660 звільняють наявні 6 слотів для досягнення вищої щільності WAN-портів або для мультисервісного агрегування.

Наявність додаткових слотів у Cisco 3660, у поєднанні з дедалі більшим спектром мережних модулів відкривають нові можливості для застосування, наприклад як мультисервісний концентратор з високою щільністю портів, або маршрутизатора для підключення філії до АТМ-мережі, зі швидкостями від T1/E1 Inverse Multiplexing для АТМ (IMA) до OC-3.

Cisco 3660 постачається у кількох конфігураціях. Базовий комплект забезпечує:

- шість слотів розширення для встановлення мережних модулів
- два Advanced Integration module (AIM) слота
- підтримку резервування джерела живлення
- один консольний порт
- один додатковий (AUX) порт
- два слоти PCMCIA для зберігання програмного забезпечення та конфігурації

Cisco 3660 може бути замовленим у варіанті з одним та двома Fast Ethernet портами, та забезпечує гарячу заміну мережних модулів та резервних джерел живлення.

Широкі можливості керування досягаються з використанням програм CiscoWorks, CiscoView, і CiscoView Stack Management Interface.

Ці ж системи використовуються для управління широким спектром продуктів Cisco, які вже використовуються в корпоративних мережах, забезпечуючи адміністраторів єдиним інтерфейсом системи управління.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

Особливості:

- модульна архітектура забезпечує гнучкість у побудові рішення та можливість поступового нарощування потужності
- широкий набір підтримуваних інтерфейсів, що варіюються від 300bps асинхронного послідовного каналу до АТМ ОС-3, підтримується підключення до мереж IP, АТМ, Frame Relay, TDM, що дозволяє задовольнити потреби будь-якої великої філії
- забезпечується ефективно за вартістю рішення, у якому можуть поєднуватись висока щільність голосових портів та набір додаткових інтерфейсів. Наприклад, типова конфігурація Cisco 3660 для віддаленої філії може виглядати так:
 - два інтерфейси T1 або digital voice, підключені до телефонної станції або телефонної мережі
 - магістральний канал 8xT1/E1 АТМ ІМА для підключення до центрального офісу
 - 30 цифрових модемів для забезпечення віддаленого доступу
 - послідовні порти для підключення інших пристроїв

Під час вибору комутатора увагу звернено на кількість портів. Їх повинна бути достатня кількість, оскільки мережа є глобальною. Також потрібно, щоб дані порти функціонували на достатній швидкості та була можливість налаштування VLAN'ів, тобто комутатор повинен бути керованим. Оптимальним вибором буде комутатор Cisco WS-C2960-24TC-S (рис. 3.3).



Рисунок 3.3 - Комутатор Cisco WS-C2960-24TC-S

Cisco WS-C2960-24TC-S - керований комутатор з 24 портами Fast Ethernet портів і 2 Gigabit Ethernet. Даний комутатор підтримує передачу голосу, відео і даних

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

з високими стандартами безпеки доступу. Крім того, вони забезпечують масштабоване управління відповідно до потреб бізнесу.

Комутатор Cisco WS-C2960-24TC-S підтримує Intelligent features (створення складних списків управління доступом, розширена безпека), комбіновані гігабітні порти. Також даний комутатор підтримує QoS, покроковий Rate Limiting, ACL (на базі MAC або IP адрес, портів UDP / TCP) і multicast services, можливість регулювати швидкість передачі на кожному порту з кроком 64 Кбіт, Link Aggregation для організації більш швидкісних з'єднань між комутаторами і серверами, можливість організації транкових з'єднань на кожному порту за допомогою тегів 802.1q, до 255 VLAN на комутатор, до 4000 VLAN ID.

3.2 Налагодження комп'ютерної мережі та підсистеми моніторингу

Для того, щоб мережа функціонувала правильно важливо налаштувати все у правильному порядку та використовуючи правильні параметри. В даному випадку використано ті, які розраховано при проектуванні топології.

Для початку налаштовано параметри IP-адресації на всіх пристроях мережі. Розглянемо на прикладі роутера ядра R_Core_3:

```
R_Core_3#configure terminal
R_Core_3(config)#interface fastEthernet0/0
R_Core_3(config-if)#description link_to_SW_Core
R_Core_3(config-if)#ip address 192.168.1.3 255.255.255.240
R_Core_3(config-if)#no shutdown
R_Core_3(config-if)#exit
R_Core_3(config)#int ethernet1/0
R_Core_3(config-if)#description link_to_R_Lviv
R_Core_3(config-if)#ip address 192.168.10.1 255.255.255.252
R_Core_3(config-if)#no shutdown
R_Core_3(config-if)#exit
R_Core_3(config)#int ethernet1/0
```

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_Core_3(config-if)#description link_to_R_Zhytomyr
R_Core_3(config-if)#ip address 192.168.11.1 255.255.255.252
R_Core_3(config-if)#no shutdown
R_Core_3(config-if)#exit
R_Core_3(config)#int ethernet1/0
R_Core_3(config-if)#description link_to_R_Kyiv
R_Core_3(config-if)#ip address 192.168.12.1 255.255.255.252
R_Core_3(config-if)#no shutdown
R_Core_3(config-if)#exit
R_Core_3(config)#int ethernet1/0
R_Core_3(config-if)#description link_to_R_Kharkiv
R_Core_3(config-if)#ip address 192.168.13.1 255.255.255.252
R_Core_3(config-if)#no shutdown
R_Core_3(config-if)#exit
R_Core_3#write

```

Роутери доступу налаштовано, як DHCP-сервери. Приклад налаштування показано на основі R_Zhytomyr:

```

R_Zhytomyr#configure terminal
R_Zhytomyr(config)#ip dhcp excluded-address 192.168.111.1 192.168.111.10
R_Zhytomyr(config)#ip dhcp pool LAN_Zhytomyr
R_Zhytomyr(dhcp-config)#network 192.168.111.0 255.255.255.0
R_Zhytomyr(dhcp-config)#default-router 192.168.111.1
R_Zhytomyr(dhcp-config)#dns-server 8.8.8.8
R_Zhytomyr(dhcp-config)#domain-name yavorenko.local
R_Zhytomyr(dhcp-config)#end

```

На всіх маршрутизаторах налаштовано маршрутизацію на основі протоколу EIGRP. На роутерах доступу переведено інтерфейси, які переходять у LAN`и, у пасивний стан. На маршрутизаторі ядра, який має вихід у глобальну мережу, також

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

налаштовано статичний маршрут та за допомогою редистрибуції протоколу EIGRP додано його у загальну таблицю маршрутизації. Приклад налаштування на R_Core_3:

```
R_Core_3#configure terminal
R_Core_3(config)#router eigrp 1
R_Core_3(config-router)#no auto-summary
R_Core_3(config-router)#network 192.168.1.0 0.0.0.15
R_Core_3(config-router)#network 192.168.10.0 0.0.0.3
R_Core_3(config-router)#network 192.168.11.0 0.0.0.3
R_Core_3(config-router)#network 192.168.12.0 0.0.0.3
R_Core_3(config-router)#network 192.168.13.0 0.0.0.3
R_Core_3(config-router)#end
```

Для реалізації доступу до глобальної мережі на одному з маршрутизаторів ядра налаштовано трансляцію адрес мережі за протколом PAT(NAT). IP-адресу з глобальної мережі отримано за протколом DHCP. Крім цього налаштовано статичний маршрут для маршрутизації даного маршруту іншим пристроям мережі та додано його у глобальну таблицю маршрутизації за допомогою редистрибуції статичних маршрутів. Показано на прикладі R_Core_1:

```
R_Core_1#configure terminal
R_Core_1(config)#interface FastEthernet0/0
R_Core_1(config-if)#ip address dhcp
R_Core_1(config-if)#ip nat outside
R_Core_1(config-if)#exit
R_Core_1(config)#interface FastEthernet0/1
R_Core_1(config-if)#ip nat inside
R_Core_1(config-if)#exit
R_Core_1(config)#access-list 1 permit any
R_Core_1(config)#ip nat inside source list 1 interface FastEthernet0/0 overload
R_Core_1(config)#ip route 0.0.0.0 0.0.0.0 fastEthernet0/1
```

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_Core_1(config)#router eigrp 1
R_Core_1(config-router)#redistribute static
R_Core_1(config-router)#end
R_Core_1#write

```

Для реалізації моніторингу та менеджменту мережі використовується протокол SNMP. На маршрутизаторах та комутаторах критичного рівня (ядра) налаштовано SNMP-сервер за протолом третьої версії, як найбільш захищений варіант. Реалізовано доступ до серверу лише з ПК головного адміністратора мережі MGMT за допомогою списків контролю доступу. Показано на прикладі комутатора SW_Core:

```

SW_Core#configure terminal
SW_Core(conf)#ip access-list standard YAVORENKO_SNMP_ACL
SW_Core(config-std-nacl)#permit 192.168.254.3
SW_Core(config-std-nacl)#exit
SW_Core(conf)#snmp-server group ADMIN v3 priv match exact write YAVORENKO_SNMP-RW access YAVORENKO_SNMP_ACL
SW_Core(conf)#snmp-server view YAVORENKO_SNMP-RW iso included
SW_Core(conf)#snmp-server user YAVORENKO_ADMIN ADMIN v3 auth md5
cisco12345 pri des cisco54321
SW_Core(conf)#snmp-server location Ukraine_WAN
SW_Core(conf)#snmp-server contact admin@yavorenko.local.net
SW_Core(conf)#snmp-server enable traps
SW_Core(conf)#end
SW_Core#write

```

На рівні доступу реалізовано сервери менеджменту та моніторингу за протоколом SNMP версії 2с. Для кожної з задач реалізовано відповіді рядки спільноти з розгалуженням доступу до мережі відповідно до прав доступу. Таким чином, менеджмент дозволений лише з ПК головного адміністратора мережі MGMT, а

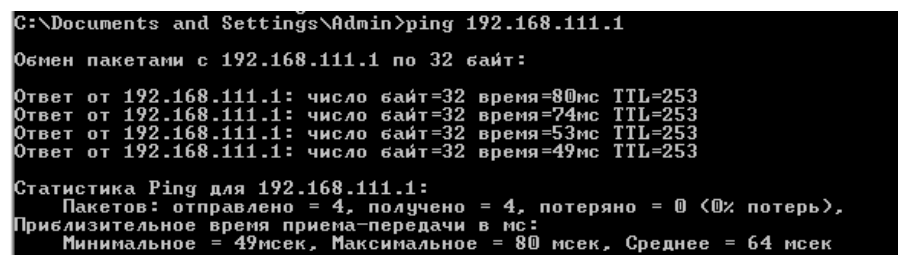
		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

моніторинг доступний всім адміністраторам цієї ж мережі. Приклад налаштування на R_Kyiv:

```
R_Kyiv#configure terminal
R_Kyiv(conf)#ip access-list standard ADMIN_SNMP_ACL
R_Kyiv(config-std-nacl)#permit 192.168.254.3
R_Kyiv(config-std-nacl)#exit
R_Kyiv(conf)#ip access-list standard SNMP_ACL
R_Kyiv(config-std-nacl)#permit 192.168.254.0 0.0.0.31
R_Kyiv(config-std-nacl)#exit
R_Kyiv(conf)#snmp-server community SNMP_MONITOR_RO RO SNMP_ACL
R_Kyiv(conf)#snmp-server community SNMP_MANAGER_RW RW ADMIN_SNMP_ACL
R_Kyiv(conf)#snmp-server location Kyiv_LAN
R_Kyiv(conf)#snmp-server contact admin@kyiv.yavorenko.net
R_Kyiv(conf)#snmp-server host 192.168.254.3 version 2c SNMP_MONITOR_RO
R_Kyiv(conf)#end
```

Після реалізації налаштувань на пристроях створеної топології важливо перевірити працездатність мережі.

Перш за все, у створеній топології потрібно перевірити наявність наскрізного з'єднання між віддаленими вузлами мереж. Перевіряємо за допомогою команд `tracert` та `ping` (рис. 3.4 – 3.6).



```
C:\Documents and Settings\Admin>ping 192.168.111.1
Обмен пакетами с 192.168.111.1 по 32 байт:
Ответ от 192.168.111.1: число байт=32 время=80мс TTL=253
Ответ от 192.168.111.1: число байт=32 время=74мс TTL=253
Ответ от 192.168.111.1: число байт=32 время=53мс TTL=253
Ответ от 192.168.111.1: число байт=32 время=49мс TTL=253

Статистика Ping для 192.168.111.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 49мсек, Максимальное = 80 мсек, Среднее = 64 мсек
```

Рисунок 3.4 – Перевірка зв'язку між PC_Zhytomyr_1 та R_Zhytomyr

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

```

C:\Documents and Settings\Admin>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по 32 байт:

Ответ от 192.168.1.1: число байт=32 время=157мс TTL=253
Ответ от 192.168.1.1: число байт=32 время=49мс TTL=253
Ответ от 192.168.1.1: число байт=32 время=45мс TTL=253
Ответ от 192.168.1.1: число байт=32 время=50мс TTL=253

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
    Приблизительное время приема-передачи в мс:
        Минимальное = 45мсек, Максимальное = 157 мсек, Среднее = 75 мсек

C:\Documents and Settings\Admin>ping 192.168.112.11

Обмен пакетами с 192.168.112.11 по 32 байт:

Ответ от 192.168.112.11: число байт=32 время=108мс TTL=61
Ответ от 192.168.112.11: число байт=32 время=138мс TTL=61
Ответ от 192.168.112.11: число байт=32 время=68мс TTL=61
Ответ от 192.168.112.11: число байт=32 время=86мс TTL=61

Статистика Ping для 192.168.112.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
    Приблизительное время приема-передачи в мс:
        Минимальное = 68мсек, Максимальное = 138 мсек, Среднее = 100 мсек

```

Рисунок 3.5 – Перевірка зв'язку між PC_Zhytomyr_1 та R_Core_1, PC_Kyiv_3

```

C:\Documents and Settings\Admin>tracert 192.168.1.2

Трассировка маршрута к 192.168.1.2 с максимальным числом прыжков 30

 1      9 ms    22 ms    20 ms    192.168.111.1
 2     28 ms    31 ms    32 ms    192.168.11.1
 3     91 ms    73 ms    86 ms    192.168.1.2

Трассировка завершена.

C:\Documents and Settings\Admin>tracert 192.168.112.11

Трассировка маршрута к 192.168.112.11 с максимальным числом прыжков 30

 1      20 ms    21 ms    10 ms    192.168.111.1
 2      32 ms    53 ms    32 ms    192.168.11.1
 3      76 ms    53 ms    74 ms    192.168.12.2
 4      91 ms    86 ms    74 ms    192.168.112.11

Трассировка завершена.

C:\Documents and Settings\Admin>

```

Рисунок 3.6 – Перевірка зв'язку між PC_Zhytomyr та R_Core_2, PC_Kyiv_1

Для перевірки функціонування DHCP кінцеве устаткування налаштовано як DHCP-клієнти. Результат отримання пристроями IP-адрес наведено на рис. 3.7 – 3.9.

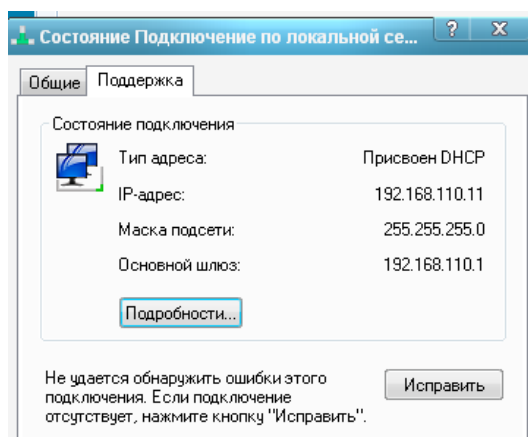


Рисунок 3.7 – Отримання IP-адреси клієнтом PC_Lviv_1

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

```

C:\Documents and Settings\Admin>ipconfig

Настройка протокола IP для Windows

Подключение по локальной сети 2 - Ethernet адаптер:

    DNS-суффикс этого подключения . . : yavorenko.local
    IP-адрес . . . . . : 192.168.111.12
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . : 192.168.111.1

C:\Documents and Settings\Admin>

```

Рисунок 3.8 – Перевірка IP-адреси клієнтом PC_Zhytomyr_2

```

PC_Kyiv_3> ip dhcp
DORA IP 192.168.112.11/24 GW 192.168.112.1

PC_Kyiv_3> show ip

NAME       : PC_Kyiv_3[1]
IP/MASK    : 192.168.112.11/24
GATEWAY    : 192.168.112.1
DNS        : 8.8.8.8
DHCP SERVER : 192.168.112.1
DHCP LEASE  : 86347, 86400/43200/75600
DOMAIN NAME : yavorenko.local
MAC        : 00:50:79:66:68:05
LPORT      : 20093
RHOST:PORT  : 127.0.0.1:20094
MTU        : 1500

PC_Kyiv_3>

```

Рисунок 3.9 – Перевірка IP-адреси клієнтом PC_Kyiv_3

Для перевірки правильної роботи протоколу EIGRP виведено таблиці маршрутизації, топології та сусідів. Показано на основі маршрутизатора ядра R_Core_2. На рисунку 3.10 виведено таблицю маршрутизації. На рисунку 3.11 виведено таблицю сусідів.

```

R_Core_2#show ip route eigrp
 192.168.12.0/30 is subnetted, 1 subnets
D    192.168.12.0 [90/284160] via 192.168.1.3, 01:50:13, FastEthernet0/1
 192.168.13.0/30 is subnetted, 1 subnets
D    192.168.13.0 [90/284160] via 192.168.1.3, 01:50:05, FastEthernet0/1
D    192.168.110.0/24 [90/286720] via 192.168.1.3, 01:50:18, FastEthernet0/1
D    192.168.111.0/24 [90/286720] via 192.168.1.3, 02:29:48, FastEthernet0/1
 192.168.10.0/30 is subnetted, 1 subnets
D    192.168.10.0 [90/284160] via 192.168.1.3, 01:50:23, FastEthernet0/1
 192.168.11.0/30 is subnetted, 1 subnets
D    192.168.11.0 [90/284160] via 192.168.1.3, 03:01:34, FastEthernet0/1
 192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
D    192.168.20.0/24 is a summary, 03:01:36, Null0
D    192.168.113.0/24 [90/286720] via 192.168.1.3, 01:50:00, FastEthernet0/1
D    192.168.112.0/24 [90/286720] via 192.168.1.3, 01:50:10, FastEthernet0/1
D    192.168.254.0/24 [90/30720] via 192.168.20.2, 03:01:34, FastEthernet0/0
 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
D    192.168.1.0/24 is a summary, 03:01:37, Null0
D*EX 0.0.0.0/0 [170/30720] via 192.168.1.1, 03:01:27, FastEthernet0/1
R_Core_2#

```

Рисунок 3.10 – Таблиця маршрутизації протоколу EIGRP на R_Core_2

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_Core_2#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                Interface    Hold Uptime    SRTT    RTO  Q  Seq
   (sec)              (ms)
3   192.168.1.4            Fa0/1       14 02:46:23    27    200  0  14
2   192.168.1.1            Fa0/1       11 03:02:10    34    204  0  17
1   192.168.1.3            Fa0/1       10 03:02:12    37    222  0  49
0   192.168.20.2           Fa0/0       12 03:02:12    39    234  0  11
R_Core_2#

```

Рисунок 3.11 – Таблиця маршрутизації протоколу EIGRP на R_Core_2

Для перевірки налаштувань SNMP-серверів використано наступні технології: програмні додатки для ОС Windows PowerSNMP Free Manager від Dart [14] та MIB Browser Free Tool від ManageEngine [15], для ОС Linux утиліту SNMP-Check. Моніторинг мереж більш зручний у першому додатку для ОС Windows, крім того він підходить для протоколу третьої версії. Для початку потрібно додати SNMP-агенти до NMS. Для цього потрібно ввести IP-адресу, порт, обрати версію та ввести параметри аутентифікації протоколу (рис. 3.12). Якщо дані введено вірно – додаток виведе пристрій з мінімальними відомостями про нього у попередньому перегляді (рис. 3.13). Після цього пристрій можна додати до групи агентів, що дозволить його подальший моніторинг (рис. 3.14). За допомогою OID протоколу можна отримати різні відомості про пристрій, наприклад його локацію (рис. 3.15). Окрім цього, додаток дозволяє виводити великі об'єми значень у вигляді таблиць. Для прикладу виведено таблицю IP-адресації пристрою R_Lviv (рис. 3.16). Для зручності є можливість стежити за змінами значень OID та додати їх на головний екран (рис. 3.17 - 3. 18). Також додаток дозволяє стежити за пропускнуою здатністю мережі, що також є досить зручною опцією, оскільки швидкість мережі – один з найважливіших моментів (рис. 3. 19).

Рисунок 3.12 – Вікно додавання нового агента

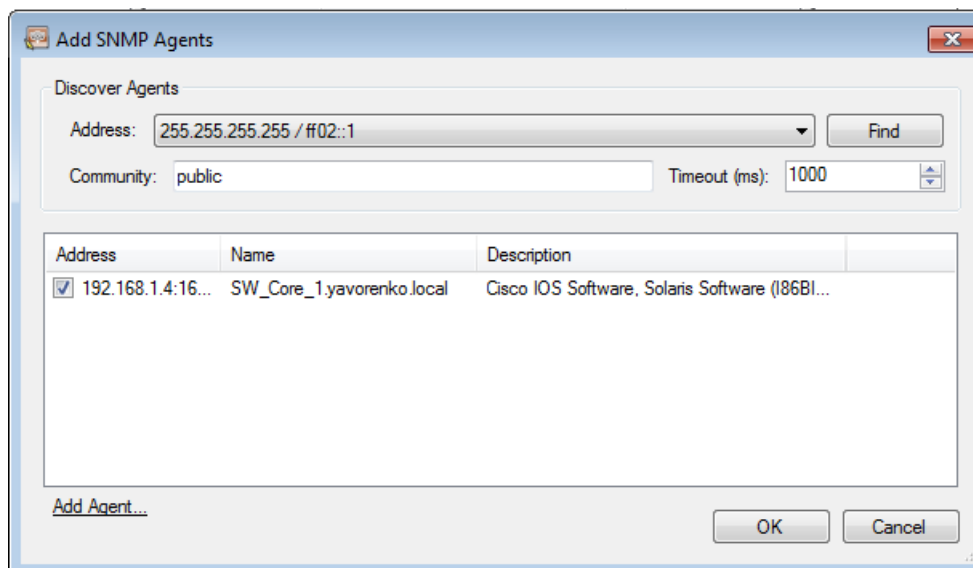


Рисунок 3.13 – Попередній перегляд агентів, що додаються

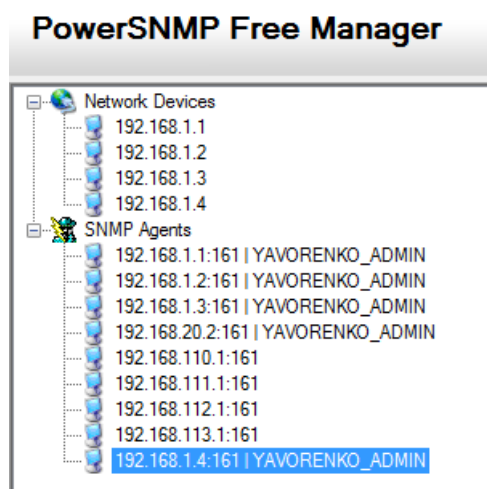


Рисунок 3.14 – Список доданих SNMP-агентів

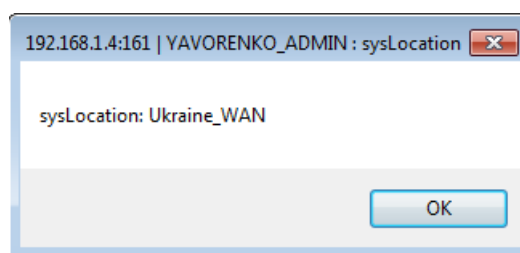


Рисунок 3.15 – Виведення інформації з агенту за допомогою GET-запиту

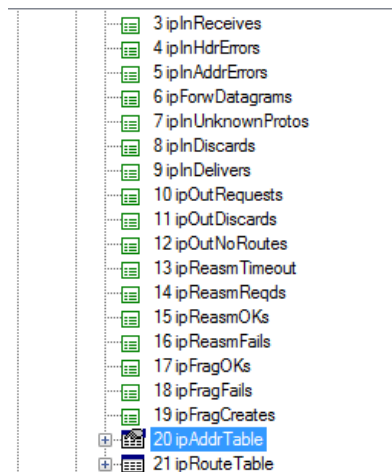


Рисунок 3.16 – Список доступних об'єктів у human-readable форматі замість OID

ipAdEntAddr	ipAdEntIfIndex	ipAdEntNetMask	ipAdEntBcastAddr	ipAdEntReasmMaxSize
192.168.10.2	1	255.255.255.252	1	18024
192.168.110.1	2	255.255.255.0	1	18024

Рисунок 3.17 – Виведення таблиці IP-адресації на R_Lviv за допомогою GET-запиту

Рисунок 3.18 – Додавання змінної для постійного моніторингу

Device Address	Variable/IID	Value
Variable Watches		
192.168.1.1:161	sysName (1.3.6.1.2.1.1.5.0)	R_Core_1.yavorenko.local
192.168.1.1:161	sysUpTime (1.3.6.1.2.1.1.3.0)	1167866
192.168.1.4:161	sysName (1.3.6.1.2.1.1.5.0)	SW_Core_1.yavorenko.local
192.168.1.4:161	sysUpTime (1.3.6.1.2.1.1.3.0)	1459414
192.168.1.4:161	sysLocation (1.3.6.1.2.1.1.6.0)	Ukraine_WAN
192.168.1.4:161	sysContact (1.3.6.1.2.1.1.4.0)	admin@yavorenko.local.net

Рисунок 3.19 – Список поточних змінних, які моніторяться

Ping Watches	
192.168.1.1	54 ms
192.168.1.2	31 ms
192.168.1.3	48 ms
192.168.1.4	37 ms

Рисунок 3.20 – Список пристроїв, у яких тестується пропускна здатність (затримка під час передачі трафіку)

Для реалізації менеджменту використано інший додаток – ManageEngine MIB Browser Free Tool. Процес налаштування схожий з попереднім додатком. Для початку потрібно додати SNMP-агент, записавши його IP-адресу, порт, параметри аутентифікації та рівень захисту хоста (рис. 3.21). В результаті до бази користувачів та агентів буде додано новий запис (рис. 3.22). Після цього з'являється можливість повного керування агентом за допомогою SET-запитів, обравши OID та записавши нове значення параметру (рис. 3.23 – 3.24).

Рисунок 3.21 – Налаштування нового SNMPv3-агента

Рисунок 3.22 – Результат додавання нового SNMPv3-агента

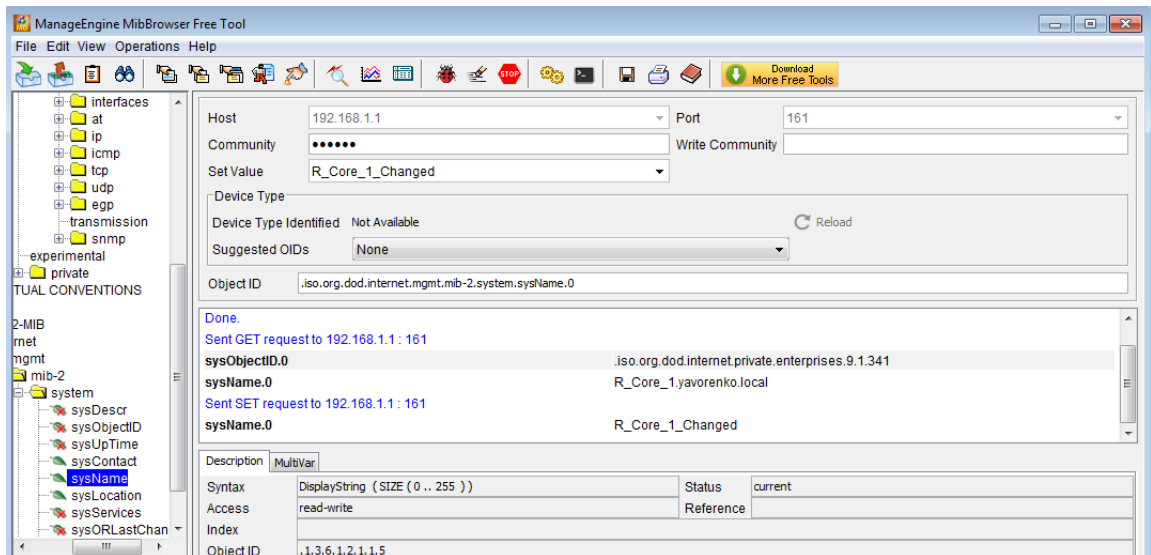


Рисунок 3.23 – Результат виконання GET та SET-запитів до агента

```
R_Core_1#
*Mar  1 03:20:50.831: %SYS-5-CONFIG-I: Configured from 192.168.254.3 by snmp
R_Core_1#
R_Core_1_Changed#
R_Core_1_Changed#
```

Рисунок 3.24 – Результат менеджменту R_Core_1 за протоколом SNMP

Для менш критичних пристроїв налаштовано протокол SNMPv2c з використанням рядків спільнот, як механізму аутентифікації. За рахунок розповсюдженості даної версії з'явилася велика кількість зручних рішень для моніторингу та менеджменту. Процес додавання нових агентів також спрощено. Для цього потрібно вказати IP-адресу, версію та рядок спільноти (рис. 3.25). В результаті з'являється можливість моніторингу та менеджменту, ідентична третій версії протоколу (рис 3.26). Для реалізації менеджменту потрібно вказати рядки спільнот для різних режимів – read та write, або тільки write (рис 3.27 – 3.28).

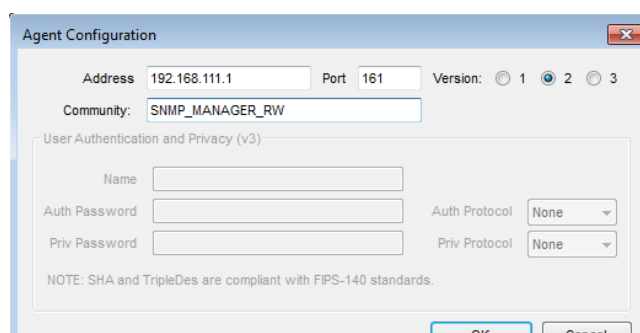


Рисунок 3.25 – Додавання нового агента за протоколом SNMPv2c

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

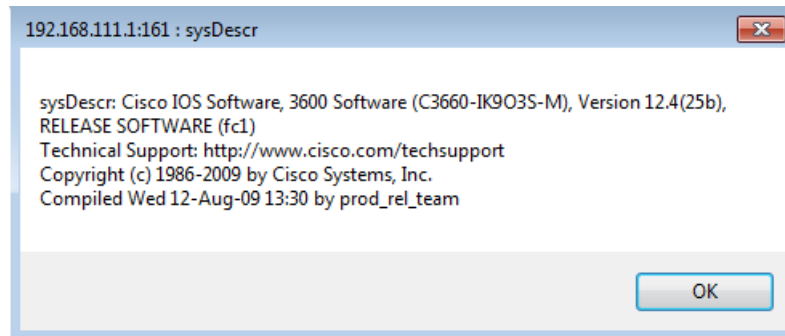


Рисунок 3.26 – Виведення значення об'єкту sysDescr

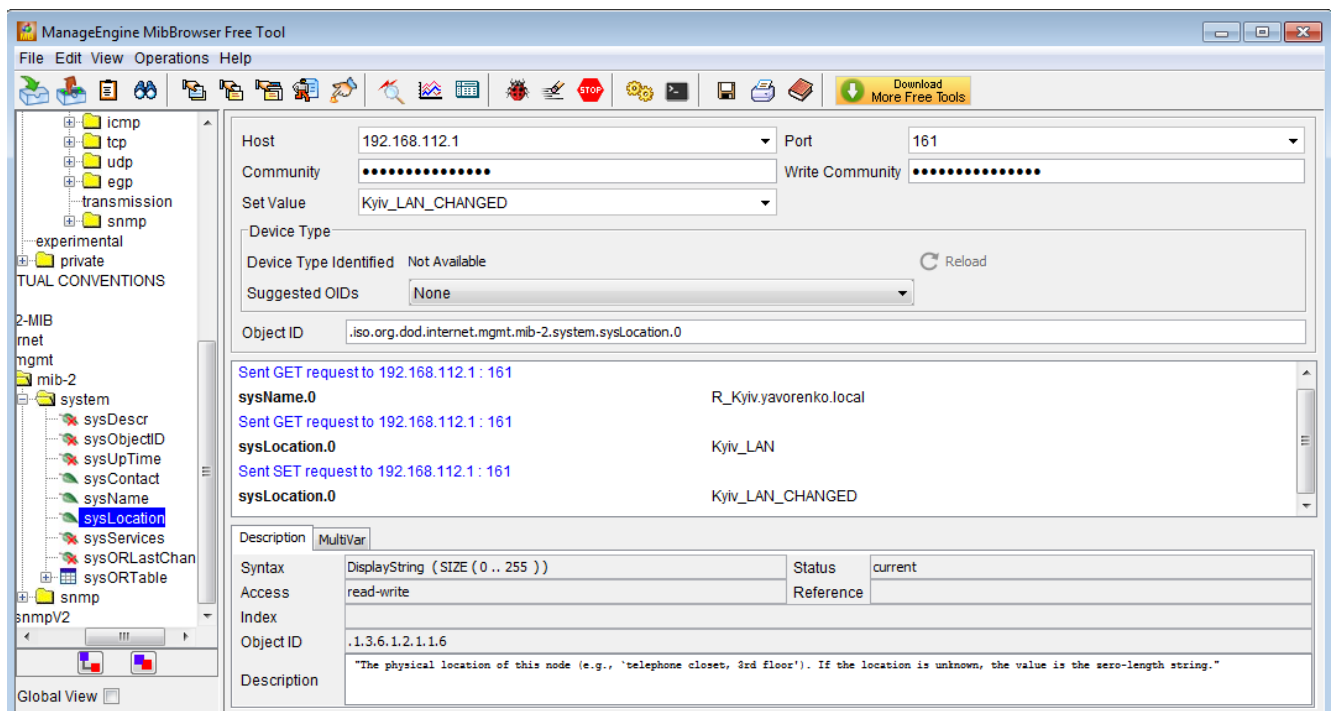


Рисунок 3.27 – Виведення та зміна значення об'єкту sysLocation

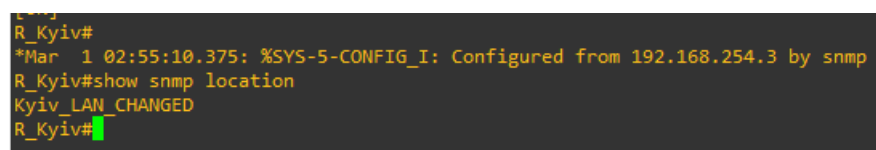


Рисунок 3.28 – Результат зміни значення об'єкту sysLocation на R_Kyiv

На ОС Linux чудовим інструментом для моніторингу агентів є утиліта SNMP-Check, яка дозволяє виводити важливі об'єкти за протоколом версії 2с у зручному вигляді. В якості параметрів лише потрібно передати порт, версію протоколу, рядок спільноти та IP-адресу (рис. 3.29 – 3.30).

```

(kali@kali)-[~]
$ snmp-check -p 161 -v 2c -c SNMP_MONITOR_RO 192.168.112.1
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.112.1:161 using SNMPv2c and community 'SNMP_MONITOR_RO'

[*] System information:

Host IP address      : 192.168.112.1
Hostname             : R_Kyiv.yavorenko.local
Description          : Cisco IOS Software, 3600 Software (C3660-IK903S-M),
Wed 12-Aug-09 13:30 by prod_rel_team
Contact              : admin@kyiv.yavorenko.net
Location             : Kyiv_LAN
Uptime snmp          : noSuchObject
Uptime system        : 02:56:17.41
System date          : -

[*] Network information:

IP forwarding enabled : yes
Default TTL           : 255
TCP segments received : 0
TCP segments sent     : 0
TCP segments retrans  : 0
Input datagrams       : 3402
Delivered datagrams   : 3279
Output datagrams      : 3810

[*] Network interfaces:

Interface            : [ up ] FastEthernet0/0
Id                   : 1
Mac Address          : cc:08:2f:b8:00:00
Type                 : ethernet-csmacd
Speed                : 100 Mbps
MTU                  : 1500
In octets             : 191637
Out octets            : 310282

Interface            : [ up ] FastEthernet0/1
Id                   : 2
Mac Address          : cc:08:2f:b8:00:01
Type                 : ethernet-csmacd
Speed                : 100 Mbps
MTU                  : 1500
In octets             : 405999
Out octets            : 249731

```

Рисунок 3.29 – Результат виведення інформації утилітою SNMP-Check (частина)

```

[*] Network IP:

Id      IP Address      Netmask      Broadcast
1       192.168.12.2     255.255.255.252  1
2       192.168.112.1   255.255.255.0   1

[*] Routing information:

Destination      Next hop      Mask          Metric
0.0.0.0          192.168.12.1  0.0.0.0       33280
192.168.1.0      192.168.12.1  255.255.255.240 30720
192.168.10.0     192.168.12.1  255.255.255.252 284160
192.168.11.0     192.168.12.1  255.255.255.252 284160
192.168.12.0     192.168.12.2  255.255.255.252 0
192.168.13.0     192.168.12.1  255.255.255.252 284160
192.168.20.0     192.168.12.1  255.255.255.0   33280
192.168.110.0    192.168.12.1  255.255.255.0   286720
192.168.111.0    192.168.12.1  255.255.255.0   286720
192.168.112.0    192.168.112.1 255.255.255.0   0
192.168.113.0    192.168.12.1  255.255.255.0   286720
192.168.254.0    192.168.12.1  255.255.255.0   35840

[*] Listening UDP ports:

Local address      Local port
192.168.12.2       162
192.168.12.2       57001
192.168.112.1      67
192.168.112.1      161

[*] File system information:

Index              : noSuchObject
Mount point        : noSuchObject
Access             : noSuchObject
Bootable           : noSuchObject

```

Рисунок 3.30 – Результат виведення інформації утилітою SNMP-Check (частина)

3.3 Дослідження рівня захищеності підсистеми моніторингу

Після налаштування мережі та перевірки правильності функціонування пристроїв важливо проаналізувати мережу на безпечність. Найкращим інструментом для реалізації тестування є Kali Linux.

Kali Linux — це дистрибутив Linux, розроблений для цифрової криміналістичної експертизи та тестування на проникнення [16]. Він підтримується та фінансується Offensive Security.

Kali Linux має близько 600 програм (інструментів) для тестування на проникнення, включаючи Armitage (графічний інструмент керування кібератаками), Nmap (сканер портів), Wireshark (сніфер пакетів), metasploit (фреймворк тестування на проникнення), John the Ripper (утиліта для зламу паролів), sqlmap (автоматична ін'єкція SQL та інструмент захоплення бази даних), Aircrack-ng (набір програм для тестування на проникнення бездротових локальних мереж), пакет Burp і сканери безпеки веб-додатків OWASP ZAP тощо.

Першим етапом перевірки є аналіз відкритих портів мережі, що може дати змогу зловмиснику провести атаки на систему. Для перевірки портів використано утиліту nmap. Перевірено відкриті UDP та TCP-порти на маршрутизаторі доступу R_Lviv за допомогою параметру (рис. 3.31 – 3.32). Першим з портів, який був би цікавий зловмиснику – це 161, порт на якому функціонує протокол SNMP. Отримання інформації з нього дало б змогу проводити різні маніпуляції, крім того, якщо протокол налаштовано невірно хакер може змінити будь-які дані пристрою та, наприклад, перенаправити важлий трафік собі на робочу станцію, що може дати йому повний доступ та призвести до виведення з ладу всієї мережі.

З результатів сканування видно, що пристрій використовує 3-тю версію протоколу, хоча насправді на пристрої налаштована версія 2с. Дана версія використовує рядки спільноти для аутентифікації в різні режими роботи. Тому першим, що варто перевірити, можливість зламу рядка спільноти за допомогою атаки грубої сили з використанням заготовленого словника [17] найбільш використовуваних рядків спільнот (рис. 3.23).

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

```
(kali㉿kali)-[~]
└─$ sudo nmap 192.168.110.1 -Pn -sU -sV
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-21 14:41 EDT
Nmap scan report for 192.168.110.1
Host is up (0.096s latency).
Not shown: 996 filtered ports
PORT      STATE      SERVICE  VERSION
67/udp    open|filtered dhcp
161/udp   open      snmp      Cisco SNMP service; ciscoSystems SNMPv3 server
162/udp   open|filtered snmptrap
4500/udp  open|filtered nat-t-ike

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.63 seconds
```

Рисунок 3.31 – Сканування UDP-портів за допомогою nmap

```
(kali㉿kali)-[~]
└─$ sudo nmap 192.168.110.1 -Pn -sV
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-21 14:44 EDT
Nmap scan report for 192.168.110.1
Host is up (0.089s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Cisco router telnetd
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

Рисунок 3.32 – Сканування TCP-портів за допомогою nmap

```
(kali㉿kali)-[~]
└─$ sudo onesixtyone -c common-community-strings.txt -p 161 192.168.110.1
Scanning 1 hosts, 121 communities

(kali㉿kali)-[~]
└─$
```

Рисунок 3.33 – Результат виконання атаки грубої сили на SNMP-сервер

З результату, отриманого після виконання брут-форс атаки, зроблено висновок, що SNMP-сервер досить надійно захищений та можливість його зламу не висока. Крім того, на більш критичних пристроях налаштовано третю версію протоколу, яка “з коробки” вже має гарний захист та шифрування. Крім цього, під час проведення атак сервер отримує діагностичну інформацію щодо підозрілих пакетів (рис. 3.34), що дає змогу адміністратору мережі вчасно зреагувати та заблокувати робочу станцію зломисника.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_Lviv#
*Mar 1 02:06:52.983: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x83951194(220758460), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:14:30.183: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x911C1194(243453588), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:16:21.339: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x911D1194(243460134), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:17:29.471: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x1000(4096), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:18:59.915: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x21D8876(35490678), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:20:19.911: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x10002(65538), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:21:39.595: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x1800003D(45298489), srcaddr=192.168.254.4
R_Lviv#
*Mar 1 02:23:21.111: %CRYPTO-4-RECD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.110.1, prot=17, spi=0x3CDE39A1(102119675), srcaddr=192.168.254.4

```

Рисунок 3.34 – Виведення діагностичної інформації на R_Lviv

Наступним вразливим місцем мережі є протокол DHCP. Якщо на пристроях не налаштовано захист від атак на даний протокол зловмисник може провести деякі типи атак, наприклад, DHCP-starvation та підміна за допомогою DHCP Rogue Server. Для перевірки гіпотези здійснено спробу провести атаку з підміною сервера за допомогою Metasploit. Для початку задано параметри майбутнього DHCP-серверу та здійснено його запуск у мережі, яка використовується для моніторингу топології (рис 3.35). Після запуску, на одній з станцій LAN-у виконано налаштування IP-адресації за протоколом DHCP (рис. 3.36). Під час обміну трафіком перехоплено пакети за допомогою сніферу Wireshark, в яких міститься інформація, яка була відправлена з серверу зловмисника (рис. 3.37). Також під час атаки було виведено діагностичну інформацію щодо підозрілих пакетів (рис. 3.38), що дає змогу вчасно зреагувати, але при цьому, нажаль, не є варіантом стримання. Крім цього, в результаті проведення атаки, LAN втрачає можливість обміну інформацією через невірні адреси, отримані в підставного серверу (рис 3.39).

```

msf6 auxiliary(server/dhcp) > set srvhost 192.168.110.1
srvhost => 192.168.110.1
msf6 auxiliary(server/dhcp) > set netmask 255.255.255.0
netmask => 255.255.255.0
msf6 auxiliary(server/dhcp) > set DHCPSTART 192.168.110.201
DHCPSTART => 192.168.110.201
msf6 auxiliary(server/dhcp) > set DHCPEND 192.168.110.210
DHCPEND => 192.168.110.210
msf6 auxiliary(server/dhcp) > exploit
[*] Auxiliary module running as background job 1.

[*] Starting DHCP server ...
msf6 auxiliary(server/dhcp) >

```

Рисунок 3.35 – Створення DHCP-серверу для підміни у Metasploit

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

```
PC1> ip dhcp
DORA IP 192.168.110.202/24 GW 192.168.110.1
PC1>
```

Рисунок 3.36 – Результат отримання IP-адреси однією з станцій мережі

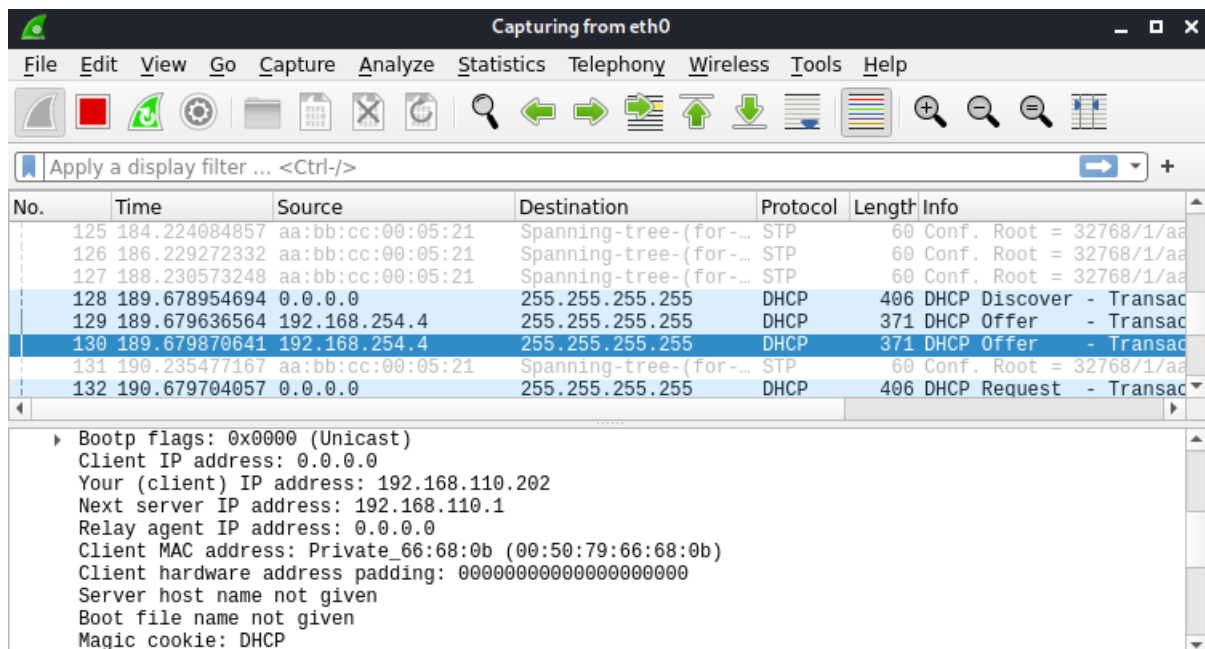


Рисунок 3.37 – Перехоплений пакет DHCP Offer

```
R_MGMT#
*Mar 1 05:10:59.142: %CRYPTO-4-RECDV_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0xF3121194(407804763
6), srcaddr=192.168.254.4
R_MGMT#
*Mar 1 05:12:01.274: %CRYPTO-4-RECDV_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0x1000(4096), srcadd
r=192.168.254.4
R_MGMT#
*Mar 1 05:13:30.230: %CRYPTO-4-RECDV_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0x2000000(33554432),
srcaddr=192.168.254.4
R_MGMT#
*Mar 1 05:14:30.334: %CRYPTO-4-RECDV_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0x303A0201(809107969
), srcaddr=192.168.254.4
R_MGMT#
*Mar 1 05:15:33.642: %CRYPTO-4-RECDV_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0x1E000130(503316784
), srcaddr=192.168.254.4
R_MGMT#
*Mar 1 05:16:37.030: %CRYPTO-4-RECDV_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0x405000(4214784), s
rcaddr=192.168.254.4
R_MGMT#
*Mar 1 05:18:01.126: %CRYPTO-4-RECDV_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=192.168.254.1, prot=17, spi=0x2E62197D(778180989
), srcaddr=192.168.254.4
R_MGMT#
```

Рисунок 3.38 – Виведення діагностичної інформації на R_MGMT

```
(kali@kali)-[~]
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
^C
--- 192.168.1.1 ping statistics ---
43 packets transmitted, 0 received, 100% packet loss, time 43182ms
```

Рисунок 3.39 – Спроба інформаційного обміну після проведення атаки

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

Також критичним моментом мережі є віддалений доступ за допомогою протоколу Telnet. У протоколі не передбачено використання ні шифрування, ні перевірки достовірності даних [18]. Тому він вразливий для будь-якого виду атак, до яких вразливий його транспорт, тобто протокол ТСП. Крім цього, на даний момент на пристроях не налаштовано механізми авторизації та аутентифікації, що дозволяє зловмиснику після отримання доступу до пристрою виконувати будь-які команди та налаштовувати мережу, що є відритою проблемою безпеки. Критично важливо використати більш захищений протокол віддаленого доступу та налаштувати паролі на пристроях мережі.

```
(kali㉿kali)-[~]
└─$ telnet -a 192.168.110.1
Trying 192.168.110.1...
Connected to 192.168.110.1.
Escape character is '^]'.

Password required, but none set
Connection closed by foreign host.

(kali㉿kali)-[~]
└─$
```

Рисунок 3.40 – Спроба підключення за протоколом Telnet до R_Lviv

3.4 Налагодження засобів захисту та дослідження стійкості системи моніторингу

В результаті аналізу у попередньому підрозділі з'ясовано критичні моменти у захисті мережі, для яких доцільно налаштувати функції захисту. Після чого важливо перевірити стійкість мережі та з'ясувати ефективність дій.

Однією з найважливіших проблем у захисті були можливі атаки на протокол DHCP [19]. Тому, в першу чергу, потрібно забезпечити безпеку саме цієї ділянки мережі. Для цього потрібно налаштувати функцію DHCP Snooping на комутаторах мережі. Великим плюсом такої реалізації захисту є те, що DHCP snooping регулює лише повідомлення DHCP і не може безпосередньо впливати на трафік користувачів або інші протоколи. Для правильного налаштування потрібно вказати надійні

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

порти (ті, які підключені до комутаторів або DHCP-серверів) та ненадійні (до яких підключені клієнти). Приклад налаштування на SW_MGMT:

```
SW_MGMT#configure terminal
SW_MGMT(config)#int range eth0/1-3
SW_MGMT(config-if)#ip dhcp snooping trust
SW_MGMT(config-if)#ip dhcp snooping limit rate 256
SW_MGMT(config-if)#end
SW_MGMT#write
```

Після налаштування захисту від DHCP-атак здійснено повторну спробу підміни DHCP-серверу. Спочатку виведено діагностичну інформацію на комутаторі щодо функціонування DHCP Snooping (рис. 3.41). Після створення підставного серверу на одній з робочих станцій здійснено спробу отримання IP-адреси (рис. 3.42), що не дало ніякого результату, оскільки обмін DHCP-пакетами з ненадійними портами неможливий. В результаті мережу захищено від атак на даний протокол.

```
SW_MGMT#show ip dhcp snooping
Switch DHCP snooping is disabled
DHCP snooping is configured on following VLANs:
none
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: aabb.cc00.0500 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface           Trusted    Allow option    Rate limit (pps)
-----
Ethernet0/0         yes       yes             256
  Custom circuit-ids:
Ethernet0/1         yes       yes             256
  Custom circuit-ids:
Ethernet0/2         yes       yes             256
  Custom circuit-ids:
Interface           Trusted    Allow option    Rate limit (pps)
-----
Ethernet0/3         yes       yes             256
  Custom circuit-ids:
```

Рисунок 3.41 – Виведення статистичних даних щодо функціонування DHCP Snooping

```
PC1> ip dhcp
DDD
Can't find dhcp server
```

Рисунок 3.42 – Спроба отримання IP-адреси з підставного серверу після налаштування DHCP Snooping

Для забезпечення безпеки таблиць маршрутизації доцільно налаштувати аутентифікацію протоколу EIGRP. Без даних налаштувань при появі невідомого маршрутизатора в мережі, на якому функціонує протокол EIGRP з тим же номером автономної системи, пристрій почне обмін таблицею маршрутизації з маршрутизатором зломисника, що може призвести до непоправних наслідків. Приклад налаштування на базі R_Kharkiv:

```
R_Kharkiv(config)#key chain EIGRP_KeyChain_Protected
R_Kharkiv(config-keychain)#key 1
R_Kharkiv(config-keychain-key)#key-string 123qwerty123
R_Kharkiv(config-keychain-key)#exit
R_Kharkiv(config-keychain)#exit
R_Kharkiv(config)#interface fastEthernet 0/0
R_Kharkiv(config-if)#ip authentication mode eigrp 1 md5
R_Kharkiv(config-if)#ip authentication key-chain eigrp 1 EIGRP_KeyChain_Protected
R_Kharkiv(config-if)#end
R_Kharkiv#write
```

Також важливим є налаштування механізму паролів та привілеїв на пристроях мережі для того, щоб зменшити ризик несанкціонованого доступу до пристроїв. Крім цього, важливо замінити протокол віддаленого адміністрування Telnet на більш сучасний та захищений. Основним протоколом, який надає такий функціонал, є SSH другої версії [20]. Також гарним рішенням буде фільтрація доступу до

даного протоколу за допомогою списків контролю доступу таким чином, щоб доступ до нього був лише з мережі, яка відповідає за менеджмент, тобто LAN_MGMT.

Приклад налаштування на основі R_Core_2:

```
R_Core_2#configure terminal
R_Core_2(config)#enable secret qwerty123
R_Core_2(config)#username admin privilege 15 secret qwerty123
R_Core_2(config)#username user privilege 1 secret qwerty123
R_Core_2(config)#crypto key generate rsa general-keys modulus 1024
R_Core_2(config)#ip ssh version 2
R_Core_2(config)#ip ssh time-out 90
R_Core_2(config)#ip ssh authentication-retries 3
R_Core_2(config)#banner motd #Unauthorized access is prohibited. For legal
users only.#
R_Core_2(config)#privilege exec level 4 ping
R_Core_2(config)#privilege exec level 4 show
R_Core_2(config)#privilege exec level 4 traceroute
R_Core_2(config)#ip access-list standard SSH_MGMT
R_Core_2(config-std-nacl)#permit 192.168.254.0 0.0.0.31
R_Core_2(config-std-nacl)#exit
R_Core_2(config)#line con 0
R_Core_2(config-line)#password qwerty123
R_Core_2(config-line)#logging synchronous
R_Core_2(config-line)#login local
R_Core_2(config-line)#exit
R_Core_2(config)#line vty 0 15
R_Core_2(config-line)#login local
R_Core_2(config-line)#transport input ssh
R_Core_2(config-line)#transport output none
R_Core_2(config-line)#access-class SSH_MGMT in
R_Core_2(config-line)#end
```

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

Для перевірки правильності налаштувань виконано підключення до мережі з однієї з робочих станцій LAN_MGMT. Перевірено можливість підключення під обліковими записами користувачів з різним рівнем привілеїв та можливості виконання ними налаштувань пристрою (рис 3.43 – 3.44). На пристрої, який використовувався для віддаленого менеджменту перевірено результат налаштувань (рис. 3.45). Також перевірено можливість підключення з пристрою мережі, яка не дозволена в ACL, налаштованому на маршрутизаторі (рис. 3.46). В результаті перевірки стійкості зроблено висновок, що мережа захищена від несанкціонованого доступу, тобто механізм контролю доступу та авторизації налаштований вірно. Крім цього дані які передаються під час обміну трафіком зашифровані, що блокує доступ до sniffінгу.

```
(kali@kali)-[~]
$ ssh -l admin 192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
RSA key fingerprint is SHA256:R3Sq5SLJOEc6rmkkaIzh6J9oii3InDI8D62ojSXbqGw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.2' (RSA) to the list of known hosts.
Password:
Unauthorized access is prohibited. For legal users only
R_Core_2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_Core_2(config)#int fa0/0
R_Core_2(config-if)#description link_to_R_MGMT
R_Core_2(config-if)#end
R_Core_2#exit
Connection to 192.168.1.2 closed.
```

Рисунок 3.43 – Підключення за протоколом SSHv2 під обліковим записом адміна

```
(kali@kali)-[~]
$ ssh -l user 192.168.1.2
Password:
Unauthorized access is prohibited. For legal users only
R_Core_2>en
Password:
R_Core_2#show run
Building configuration...

Current configuration : 4732 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_Core_2
```

Рисунок 3.44 – Підключення за протоколом SSHv2 під обліковим записом звичайного користувача

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_Core_2#
*Mar  1 02:32:28.227: %SYS-5-CONFIG_I: Configured from console by admin on vty0 (192.168.254.4)
R_Core_2#sh int fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is cc02.2f56.0000 (bia cc02.2f56.0000)
  Description: link to R MGMT
  Internet address is 192.168.20.1/30
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec

```

Рисунок 3.45 – Перевірка змін на маршрутизаторі R_Core_2

```

R_Kyiv#ssh -l admin 192.168.1.2
% Connection refused by remote host
R_Kyiv#

```

Рисунок 3.46 – Спроба підключення по SSHv2 до R_Core_2 з пристрою, який не належить до дозволених LAN

Висновки до третього розділу

У першому підрозділі здійснено аналіз мережного обладнання, яке відповідає вимогам проекту мережі. Здійснено вибір маршрутизаторів та комутаторів від компанії Cisco Systems, inc.

У другому підрозділі було налаштовано параметри IP-адресації, DHCP та SNMP серверів, маршрутизацію за протоколом EIGRP та статичними маршрутами комп'ютерної мережі. Досліджено та перевірено правильність функціонування налаштованих протоколів.

У третьому підрозділі було проаналізовано основні безпекові проблеми налаштованої мережі. Проведено тестування на проникнення та виявлення можливих інцидентів кібербезпеки. Реалізовано атаки відповідно до виявлених проблем безпеки.

У четвертому підрозділі налаштовано засоби захисту від атак на протоколи та механізми мережі. Здійснено повторні спроби атаки, перевірено правильність налаштувань та функціонування безпекових рішень.

		Яворенко Б.О.			KIK.KP.B – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

ВИСНОВКИ

В результаті виконання випускної кваліфікаційної роботи було повністю спроектовано підсистему захисту системи моніторингу мережної інфраструктури та реалізовано проект мережі за допомогою емулятора GNS3. Досліджено особливості функціонування та захисту протоколу SNMP версій 2с та 3. Проаналізовано та вирішено проблеми безпеки та вразливості під час побудови мережі.

У першому розділі було розглянуто основні теоретичні відомості щодо протоколу SNMP, наведено архітектуру, основні реалізації обміну повідомленнями, порівняно основні версії протоколу. Проаналізовано прикладні реалізації використання протоколу SNMP для моніторингу мережі, порівняно варіанти реалізації моніторингу за допомогою додатків на базі ОС Windows та Linux, з'ясовано яке з рішень підходить найкраще мережі. Виявлено основні проблеми безпеки протоколу SNMP.

У другому розділі було спроектовано загальну топологію мережі та проекти локальних ділянок, розроблено схему адресації всіх пристроїв мережі з урахуванням можливості розширення. Наведено аналіз можливих загроз мережі відповідно до протоколів, які будуть функціонувати у спроектованій мережі, наведено найбільш поширені варіанти атак та визначено їх можливу шкоду. Побудовано модель загроз мережі організації за допомогою OWASP Threat Dragon.

У третьому розділі здійснено вибір відповідного проекту топології обладнання мережі. Було налаштовано мережу у відповідності до проекту та перевірено правильність функціонування налаштованих протоколів. Проаналізовано основні безпекові проблеми налаштованої мережі. Проведено тестування на проникнення та реалізовано атаки відповідно до виявлених проблем безпеки. Налаштовано засоби захисту від атак на протоколи та механізми мережі. Перевірено правильність функціонування безпекових рішень.

Враховуючи реалізацію проекту його можна використовувати для організації малого та середнього розмірів з можливістю розширення.

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is SNMP | SNMP Monitoring [Електронний ресурс] – Режим доступу до ресурсу: <https://www.site24x7.com/network/what-is-snmp.html>
2. IBM Docs - SNMPv1 & SNMPv3 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ibm.com/docs/en/aix/7.2>
3. C. Riggs, Network perimeter security. ст. 112-113.
4. What is SNMP? Basic Tutorial on NMS, MIBs, OIDs, Traps & Agents - PC & Network Downloads - PCWDLD.com [Електронний ресурс] – Режим доступу до ресурсу: <https://www.pcwdld.com/what-is-snmp-and-tutorial>
5. D. Perkins and E. McGinnis, Understanding SNMP MIBs. Upper Saddle River, N.J.: Prentice Hall PTR, 1997, ст. 136 - 143.
6. The Definitive Guide to SNMP [Електронний ресурс] – Режим доступу до ресурсу: <https://www.comparitech.com/net-admin/snmp/>
7. Common SNMP Vulnerability: 9-Step Guide to Protect Your Network [Електронний ресурс] – Режим доступу до ресурсу: <https://www.comparitech.com/net-admin/common-snmp-vulnerabilities/>
8. Differences Between SNMP and Syslog [Електронний ресурс] – Режим доступу до ресурсу: <https://www.dpstele.com/blog/differences-between-snmp-and-syslog.php>
9. R. Bates, Network management SNMP. New York: McGraw-Hill, 2002, ст. 23 - 25.
10. Cisco three-layer hierarchical model [Електронний ресурс] – Режим доступу до ресурсу: <https://study-ccna.com/cisco-three-layer-hierarchical-model>
11. Cisco Routers List [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/products/routers/branch-routers/index.html>
12. DHCP Starvation attacks and DHCP spoofing attacks – Режим доступу до ресурсу: <https://www.omnisecu.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php>
13. L. Allen and K. Cardwell, Advanced penetration testing for highly-secured environments. ст. 41 - 49.

		Яворенко Б.О.			<i>KIK.KP.B – 125 – 26 – ПЗ</i>	Арк.
		Єфіменко А.А.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

14. What is SNMP Reflection and Amplification | DDoS Attack Glossary | Imperva [Електронний ресурс] – Режим доступу до ресурсу: <https://www.imperva.com/learn/ddos/snmp-reflection>
15. Inside SSH-2 (SSH, The Secure Shell: The Definitive Guide) [Електронний ресурс] – Режим доступу до ресурсу: https://docstore.mik.ua/oreilly/networking_2ndEd/ssh/ch03_05.html
16. Threat Modeling Process | OWASP Foundation [Електронний ресурс] – Режим доступу до ресурсу: https://owasp.org/www-community/Threat_Modeling_Process
17. SNMP - How can I test SNMP [Електронний ресурс] – Режим доступу до ресурсу: <https://store.chipkin.com/articles/snmp-how-can-i-test-snmp>
18. S. Prowell, R. Kraus and M. Borkin, Seven Deadliest Network Attacks. Burlington: Elsevier Science, 2010, ст. 12 - 26.
19. POPUP How to use MIB Broweser [Електронний ресурс] – Режим доступу до ресурсу: <https://pitstop.manageengine.com/portal/en/kb/articles/how-to-use-mib-browser>
20. What is Kali Linux [Електронний ресурс] – Режим доступу до ресурсу: <https://www.educative.io/answers/what-is-kali-linux>
21. SNMP – Simply Not My Problem. Or is it? | Pen Test Partners [Електронний ресурс] – Режим доступу до ресурсу: <https://www.pentestpartners.com/security-blog/snmp-simply-not-my-problem-or-is-it>
22. F. Swiderski and W. Snyder, Threat modeling. Redmond, Wash.: Microsoft Press, 2004, ст. 67-73.
23. Secure Telnet Connection - Information Technology [Електронний ресурс] – Режим доступу до ресурсу: <https://it.mst.edu/policies/secure-telnet/>
24. What is DHCP Snooping [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/snoodhcp.pdf>
25. Cisco Content Hub - Configuring SSHv2 and Telnet [Електронний ресурс] – Режим доступу до ресурсу: https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/www.cisco.com/content/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/security/security_Book/sec_ssh_cgr1000.html.xml

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

Детальна схема побудованої мережі в GNS3

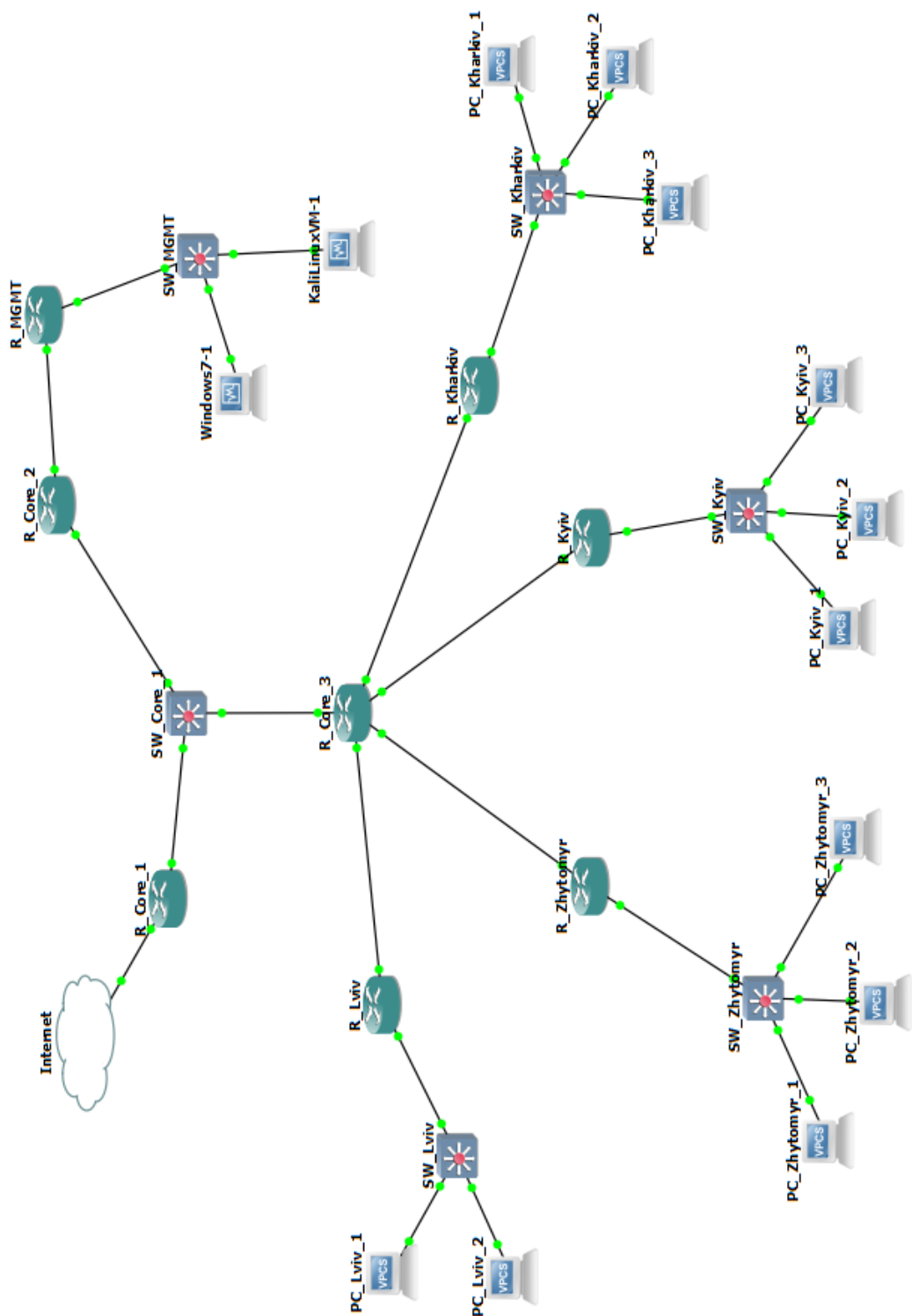


Рисунок А.1 – Схема побудованої мережі в емуляторі GNS3

Модель загроз мережі організації

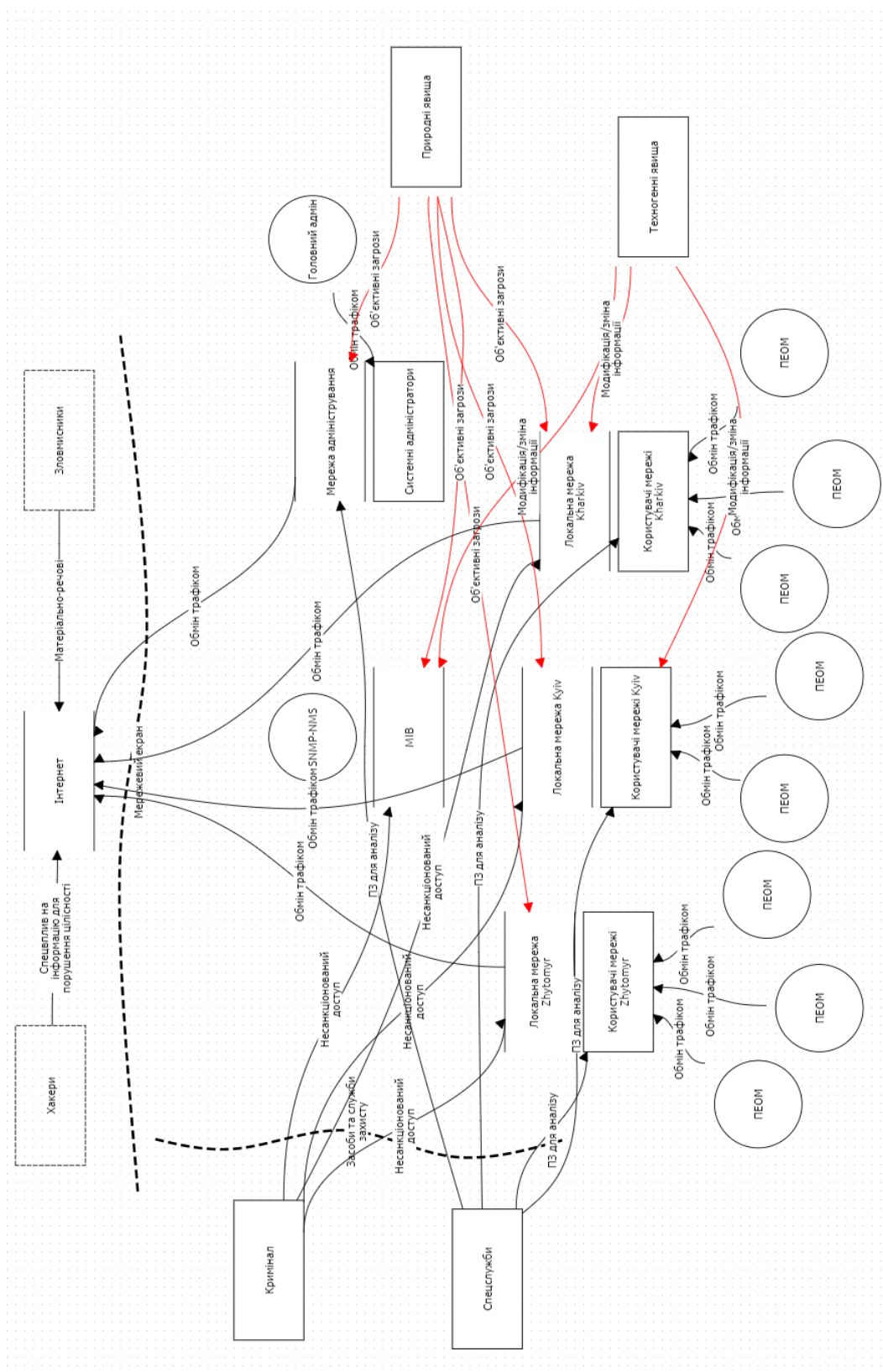


Рисунок Б.1 – Модель загроз мережі організації

		Яворенко Б.О.		
		Єфіменко А.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

КІК.КР.Б – 125 – 26 – ПЗ

Арк.

80

Лістинг конфігураційних файлів всіх пристроїв мережі

```

R_Core_1#sh run
Building configuration...
Current configuration : 4875 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R_Core_1
boot-start-marker
boot-end-marker
enable secret 5
$1$3b4F$Fs/riOYBBFAK7VjZ.nrgd.
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip domain name yavorenko.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
key chain EIGRP_KeyChain_Protected
  key 1
    key-string 123qwerty123
username admin privilege 15 secret 5
$1$c4QG$hqkEfbK/Mj/vnQFs8v1of0
username user secret 5
$1$WLT7$IyKRZsDhAsrG6ZdXTIwCg1
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface FastEthernet0/0
  ip address dhcp
  ip nat outside
  ip virtual-reassembly
  duplex auto
  speed auto
interface FastEthernet0/1
  ip address 192.168.1.1 255.255.255.240
  ip nat inside
  ip virtual-reassembly
  duplex auto
  speed auto
router eigrp 1
  redistribute static
  network 192.168.1.0 0.0.0.15
  no auto-summary
  no ip http server
  no ip http secure-server
  ip forward-protocol nd
  ip nat inside source list 1 interface FastEthernet0/0
  overload
  ip access-list standard SSH_MGMT
    permit 192.168.254.0 0.0.0.31
  ip access-list standard
    YAVORENKO_SNMP_ACL
    permit 192.168.254.3
  access-list 1 permit any
snmp-server group ADMIN v3 priv match exact
write YAVORENKO_SNMP-RW access
YAVORENKO_SNMP_ACL
snmp-server view YAVORENKO_SNMP-RW iso
included
snmp-server location Ukraine_WAN
snmp-server contact admin@yavorenko.local.net
snmp-server enable traps snmp authentication
linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps xgcp
snmp-server enable traps cnpd
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps icsudsu
snmp-server enable traps ds3
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps config-copy
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps bgp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-
change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-
change shamlink interface-old
snmp-server enable traps ospf cisco-specific state-
change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific
retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps pim neighbor-change rp-
mapping-change invalid-pim-message
snmp-server enable traps ipmulticast
snmp-server enable traps mvpn
snmp-server enable traps msdp
snmp-server enable traps rsvp

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

```

snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server enable traps stun
snmp-server enable traps dlsr
snmp-server enable traps bstun
snmp-server enable traps pppoe
snmp-server enable traps l2tun session
snmp-server enable traps atm subif
snmp-server enable traps dial
snmp-server enable traps dsp card-status
snmp-server enable traps ipmobile
snmp-server enable traps vtp
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps event-manager
snmp-server enable traps voice poor-qov
snmp-server enable traps voice fallback
snmp-server enable traps dnis
no cdp log mismatch duplex
control-plane
mgcp behavior g729-variants static-pt
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C
privilege exec level 4 traceroute
privilege exec level 4 ping
privilege exec level 4 show
line con 0
exec-timeout 0 0
privilege level 15
password qwerty123
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
transport output none
line vty 5 15
login local
transport input ssh
transport output none
end

```

```

R_Core_2#sh run
Building configuration...
Current configuration : 4791 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R_Core_2
boot-start-marker
boot-end-marker
enable secret 5
$1$FCNY$d4teznAMs3EYVSJP4bxuw1
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip domain name yavorenko.local
ip name-server 8.8.8.8
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
key chain EIGRP_KeyChain_Protected
key 1
key-string 123qwerty123
username admin privilege 15 secret 5
$1$s0.f$ICbssp/Cp36qafIrEeaf/
username user secret 5
$1$8HWN$V9q2XwXVyvu6TsnhT4oWf1
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface FastEthernet0/0
description link_to_R_MGMT
ip address 192.168.20.1 255.255.255.252
duplex auto
speed auto
interface FastEthernet0/1
ip address 192.168.1.2 255.255.255.240
duplex auto
speed auto
router eigrp 1
network 192.168.1.0 0.0.0.15
network 192.168.20.0 0.0.0.3
auto-summary
no ip http server
no ip http secure-server
ip forward-protocol nd
ip access-list standard SSH_MGMT
permit 192.168.254.0 0.0.0.31
ip access-list standard
YAVORENKO_SNPMP_ACL
permit 192.168.254.3
snmp-server group ADMIN v3 priv match exact
write YAVORENKO_SNPMP-RW access
YAVORENKO_SNPMP_ACL
snmp-server view YAVORENKO_SNPMP-RW iso
included
snmp-server location Ukraine_WAN

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

```

snmp-server contact admin@yavorenko.local.net
snmp-server enable traps snmp authentication
linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps xgcp
snmp-server enable traps cnpd
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps icsudsu
snmp-server enable traps ds3
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps config-copy snmp-server
enable traps flash insertion removal
snmp-server enable traps envmon
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps bgp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-
change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-
change shamlink interface-old
snmp-server enable traps ospf cisco-specific state-
change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific
retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps pim neighbor-change rp-
mapping-change invalid-pim-message
snmp-server enable traps ipmulticast
snmp-server enable traps mvpn
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server enable traps stun
snmp-server enable traps dlsr
snmp-server enable traps bstun
snmp-server enable traps pppoe
snmp-server enable traps l2tun session
snmp-server enable traps atm subif
snmp-server enable traps dial

```

```

snmp-server enable traps dsp card-status
snmp-server enable traps ipmobile
snmp-server enable traps vtp
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps event-manager
snmp-server enable traps voice poor-qov
snmp-server enable traps voice fallback
snmp-server enable traps dn timer
no cdp log mismatch duplex
control-plane
mgcp behavior g729-variants static-pt
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C
privilege exec level 4 traceroute
privilege exec level 4 ping
privilege exec level 4 show
line con 0
exec-timeout 0 0
privilege level 15
password qwertY123
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
transport output none
line vty 5 15
login local
transport input ssh
transport output none
end

R_Core_3#sh run
Building configuration...
Current configuration : 5152 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R_Core_3
boot-start-marker
boot-end-marker

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

```

enable secret 5
$1$krI1$RE4xYFrF9uM0dJgIB/dmd1
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip domain name yavorenko.local
ip name-server 8.8.8.8
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
key chain EIGRP_KeyChain_Protected
key 1
  key-string 123qwerty123
username admin privilege 15 secret 5
$1$67QG$2CO325i2q5Sd9N/jIpO0N0
username user secret 5
$1$m5VT$JiErPgBNYONc3FOqc7Gz.1
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface FastEthernet0/0
  ip address 192.168.1.3 255.255.255.240
  duplex auto
  speed auto
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
interface Ethernet1/0
  ip address 192.168.10.1 255.255.255.252
  half-duplex
interface Ethernet1/1
  ip address 192.168.11.1 255.255.255.252
  half-duplex
interface Ethernet1/2
  ip address 192.168.12.1 255.255.255.252
  half-duplex
interface Ethernet1/3
  ip address 192.168.13.1 255.255.255.252
  half-duplex
router eigrp 1
  network 192.168.1.0 0.0.0.15
  network 192.168.10.0 0.0.0.3
  network 192.168.11.0 0.0.0.3
  network 192.168.12.0 0.0.0.3
  network 192.168.13.0 0.0.0.3
  no auto-summary
  no ip http server
  no ip http secure-server
  ip forward-protocol nd
  ip access-list standard SSH_MGMT
    permit 192.168.254.0 0.0.0.31
  ip access-list standard
    YAVORENKO_SNMP_ACL
    permit 192.168.254.3

```

```

snmp-server group ADMIN v3 priv match exact
write YAVORENKO_SNMP-RW access
YAVORENKO_SNMP_ACL
snmp-server view YAVORENKO_SNMP-RW iso
included
snmp-server location Ukraine_WAN
snmp-server contact admin@yavorenko.local.net
snmp-server enable traps snmp authentication
linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps xgcp
snmp-server enable traps cnpd
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps icsudsu
snmp-server enable traps ds3
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps config-copy
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps bgp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-
change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-
change shamlink interface-old
snmp-server enable traps ospf cisco-specific state-
change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific
retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps pim neighbor-change rp-
mapping-change invalid-pim-message
snmp-server enable traps ipmulticast
snmp-server enable traps mvpn
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server enable traps stun

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

```

snmp-server enable traps dlsw
snmp-server enable traps bstun
snmp-server enable traps pppoe
snmp-server enable traps l2tun session
snmp-server enable traps atm subif
snmp-server enable traps dial
snmp-server enable traps dsp card-status
snmp-server enable traps ipmobile
snmp-server enable traps vtp
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps event-manager
snmp-server enable traps voice poor-qov
snmp-server enable traps voice fallback
snmp-server enable traps dnis
no cdp log mismatch duplex
control-plane
mgcp behavior g729-variants static-pt
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C
privilege exec level 4 traceroute
privilege exec level 4 ping
privilege exec level 4 show
line con 0
exec-timeout 0 0
privilege level 15
password qwerty123
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
transport output none
line vty 5 15
login local
transport input ssh
transport output none
end

R_MGMT#sh run
Building configuration...
Current configuration : 4800 bytes
version 12.4
service timestamps debug datetime msec

```

```

service timestamps log datetime msec
no service password-encryption
hostname R_MGMT
boot-start-marker
boot-end-marker
enable secret 5
$1$Q9L2$LNEKhUWl2814Td4KMZo7m.
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip domain name yavorenko.local
ip name-server 8.8.8.8
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
key chain EIGRP_KeyChain_Protected
key 1
key-string 123qwerty123
username admin privilege 15 secret 5
$1$GCca$e8SeEy/nJD9rgM8yiFRme.
username user secret 5
$1$JTiU$4BLUXCpMGYwrZGbbApz9i.
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface FastEthernet0/0
ip address 192.168.20.2 255.255.255.252
duplex auto
speed auto
interface FastEthernet0/1
ip address 192.168.254.1 255.255.255.224
duplex auto
speed auto
router eigrp 1
passive-interface FastEthernet0/1
network 192.168.20.0 0.0.0.3
network 192.168.254.0 0.0.0.31
auto-summary
no ip http server
no ip http secure-server
ip forward-protocol nd
ip access-list standard SSH_MGMT
permit 192.168.254.0 0.0.0.31
ip access-list standard
YAVORENKO_SNMP_ACL
permit 192.168.254.3
snmp-server group ADMIN v3 priv match exact
write YAVORENKO_SNMP-RW access
YAVORENKO_SNMP_ACL
snmp-server view YAVORENKO_SNMP-RW iso
included
snmp-server location Ukraine_WAN
snmp-server contact admin@yavorenko.local.net
snmp-server enable traps snmp authentication
linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps ds1

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

```

snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps xgcp
snmp-server enable traps cnpd
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps icsudsu
snmp-server enable traps ds3
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps config-copy
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps bgp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-
change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-
change shamlink interface-old
snmp-server enable traps ospf cisco-specific state-
change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific
retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps pim neighbor-change rp-
mapping-change invalid-pim-message
snmp-server enable traps ipmulticast
snmp-server enable traps mvpn
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server enable traps stun
snmp-server enable traps dlsr
snmp-server enable traps bstun
snmp-server enable traps pppoe
snmp-server enable traps l2tun session
snmp-server enable traps atm subif
snmp-server enable traps dial
snmp-server enable traps dsp card-status
snmp-server enable traps ipmobile
snmp-server enable traps vtp
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete

```

```

snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps event-manager
snmp-server enable traps voice poor-qov
snmp-server enable traps voice fallback
snmp-server enable traps dnis
no cdp log mismatch duplex
control-plane
mgcp behavior g729-variants static-pt
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C
privilege exec level 4 traceroute
privilege exec level 4 ping
privilege exec level 4 show
line con 0
exec-timeout 0 0
privilege level 15
password qwerty123
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
transport output none
line vty 5 15
login local
transport input ssh
transport output none
end

R_Lviv#sh run
Building configuration...
Current configuration : 2325 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R_Lviv
boot-start-marker
boot-end-marker
enable secret 5 $1$fwtl$Zs3P37.y7J0Yl/iWc1QXz0
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip domain name yavorenko.local

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

```

ip name-server 8.8.8.8
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.110.1
192.168.110.10
ip dhcp pool LAN_Lviv
    network 192.168.110.0 255.255.255.0
    default-router 192.168.110.1
    dns-server 8.8.8.8
    domain-name yavorenko.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
key chain EIGRP_KeyChain_Protected
    key 1
        key-string 123qwerty123
username admin privilege 15 secret 5
$1$F99y$Q9vqvFjOA3ew9.e46zucN1
username user secret 5
$1$fHfY$h4fD8VCpE5AiM/EJoR2e41
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface FastEthernet0/0
    ip address 192.168.10.2 255.255.255.252
    duplex auto
    speed auto
interface FastEthernet0/1
    ip address 192.168.110.1 255.255.255.0
    duplex auto
    speed auto
router eigrp 1
    network 192.168.10.0 0.0.0.3
    network 192.168.110.0
    no auto-summary
no ip http server
no ip http secure-server
ip forward-protocol nd
ip access-list standard ADMIN_SNMP_ACL
    permit 192.168.254.3
ip access-list standard SNMP_ACL
    permit 192.168.254.0 0.0.0.31
ip access-list standard SSH_MGMT
    permit 192.168.254.0 0.0.0.31
snmp-server community SNMP_MONITOR_RO
RO SNMP_ACL
snmp-server community SNMP_MANAGER_RW
RW ADMIN_SNMP_ACL
snmp-server location Lviv_LAN
snmp-server contact admin@lviv.yavorenko.net
snmp-server host 192.168.254.3 version 2c
SNMP_MONITOR_RO
no cdp log mismatch duplex
control-plane
mgcp behavior g729-variants static-pt
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C
privilege exec level 4 traceroute
privilege exec level 4 ping

```

```

privilege exec level 4 show
line con 0
    exec-timeout 0 0
    privilege level 15
    password qwerty123
    logging synchronous
    login local
line aux 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line vty 0 4
    login local
    transport input ssh
    transport output none
line vty 5 15
    login local
    transport input ssh
    transport output none
end

R_Zhytomyr#sh run
Building configuration...
Current configuration : 2354 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R_Zhytomyr
boot-start-marker
boot-end-marker
enable secret 5
$1$7mOF$XukUEUZ6jDnz8xEDIFvDz0
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip domain name yavorenko.local
ip name-server 8.8.8.8
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.111.1
192.168.111.10
ip dhcp pool LAN_Zhytomyr
    network 192.168.111.0 255.255.255.0
    default-router 192.168.111.1
    dns-server 8.8.8.8
    domain-name yavorenko.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
key chain EIGRP_KeyChain_Protected
    key 1
        key-string 123qwerty123
username admin privilege 15 secret 5
$1$Fk8z$WF/y8qcujj01Rcxb0xhiT/
username user secret 5
$1$m.hP$IAw00Pzb.uuWQtYyciOAG0
ip tcp synwait-time 5

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

```

ip ssh time-out 90
ip ssh version 2
interface FastEthernet0/0
ip address 192.168.11.2 255.255.255.252
duplex auto
speed auto
interface FastEthernet0/1
ip address 192.168.111.1 255.255.255.0
duplex auto
speed auto
router eigrp 1
 redistribute static
 network 192.168.11.0 0.0.0.3
 network 192.168.111.0
 no auto-summary
 no ip http server
 no ip http secure-server
 ip forward-protocol nd
 ip access-list standard ADMIN_SNMP_ACL
 permit 192.168.254.3
 ip access-list standard SNMP_ACL
 permit 192.168.254.0 0.0.0.31
 ip access-list standard SSH_MGMT
 permit 192.168.254.0 0.0.0.31
 snmp-server community SNMP_MONITOR_RO
 RO SNMP_ACL
 snmp-server community SNMP_MANAGER_RW
 RW ADMIN_SNMP_ACL
 snmp-server location Kyiv_LAN
 snmp-server contact admin@kyiv.yavorenko.net
 snmp-server host 192.168.254.3 version 2c
 SNMP_MONITOR_RO
 no cdp log mismatch duplex
 control-plane
 mgcp behavior g729-variants static-pt
 banner motd ^CUnauthorized access is prohibited.
 For legal users only.^C
 privilege exec level 4 traceroute
 privilege exec level 4 ping
 privilege exec level 4 show
 line con 0
 exec-timeout 0 0
 privilege level 15
 password qwerty123
 logging synchronous
 login local
 line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 line vty 0 4
 login local
 transport input ssh
 transport output none
 line vty 5 15
 login local
 transport input ssh

```

```

transport output none
end

```

```

R_Kyiv#sh run
Building configuration...
Current configuration : 2322 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R_Kyiv
boot-start-marker
boot-end-marker
enable secret 5
$1$MvB6$gPhGyJLV9W9B91zJbVST70
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip domain name yavorenko.local
ip name-server 8.8.8.8
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.112.1
192.168.112.10
ip dhcp pool LAN_Kyiv
 network 192.168.112.0 255.255.255.0
 default-router 192.168.112.1
 dns-server 8.8.8.8
 domain-name yavorenko.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
key chain EIGRP_KeyChain_Protected
key 1
 key-string 123qwerty123
username admin privilege 15 secret 5
$1$gqG5$4Pzi.twy7Ybih6Wcv58CF.
username user secret 5
$1$M.Xo$oj7Q/y.FH8stIqNqlfiBs.
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.252
duplex auto
speed auto
interface FastEthernet0/1
ip address 192.168.112.1 255.255.255.0
duplex auto
speed auto
router eigrp 1
 network 192.168.12.0 0.0.0.3
 network 192.168.112.0
 auto-summary
no ip http server
no ip http secure-server
!
ip forward-protocol nd

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		88

```

ip access-list standard ADMIN_SNMP_ACL
 permit 192.168.254.3
ip access-list standard SNMP_ACL
 permit 192.168.254.0 0.0.0.31
ip access-list standard SSH_MGMT
 permit 192.168.254.0 0.0.0.31
snmp-server community SNMP_MONITOR_RO
RO SNMP_ACL
snmp-server community SNMP_MANAGER_RW
RW ADMIN_SNMP_ACL
snmp-server location Kyiv_LAN
snmp-server contact admin@kyiv.yavorenko.net
snmp-server host 192.168.254.3 version 2c
SNMP_MONITOR_RO
no cdp log mismatch duplex
control-plane
mgcp behavior g729-variants static-pt
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C
privilege exec level 4 traceroute
privilege exec level 4 ping
privilege exec level 4 show
line con 0
 exec-timeout 0 0
 privilege level 15
 password qwerty123
 logging synchronous
 login local
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login local
 transport input ssh
 transport output none
line vty 5 15
 login local
 transport input ssh
 transport output none
end

R_Kharkiv#sh run
Building configuration...
Current configuration : 2328 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R_Kharkiv
boot-start-marker
boot-end-marker
enable secret 5 $1$P2B0$LSRgYc-
nTRlhUeT4HqzYGC/
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable

ip cef
ip domain name yavorenko.local
ip name-server 8.8.8.8
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.113.1
192.168.113.10
ip dhcp pool LAN_Kharkiv
 network 192.168.113.0 255.255.255.0
 default-router 192.168.113.1
 dns-server 8.8.8.8
 domain-name yavorenko.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
key chain EIGRP_KeyChain_Protected
 key 1
  key-string 123qwerty123
username admin privilege 15 secret 5
$1$dDMj$4Kn6GtfX1zRJmuBuquGOi.
username user secret 5
$1$y49s$HUyDq6uk5bSOBxZVLX4U10
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 192.168.113.1 255.255.255.0
 duplex auto
 speed auto
router eigrp 1
 network 192.168.13.0 0.0.0.3
 network 192.168.113.0
 auto-summary
no ip http server
no ip http secure-server
ip forward-protocol nd
ip access-list standard ADMIN_SNMP_ACL
 permit 192.168.254.3
ip access-list standard SNMP_ACL
 permit 192.168.254.0 0.0.0.31
ip access-list standard SSH_MGMT
 permit 192.168.254.0 0.0.0.31
snmp-server community SNMP_MONITOR_RO
RO SNMP_ACL
snmp-server community SNMP_MANAGER_RW
RW ADMIN_SNMP_ACL
snmp-server location Kyiv_LAN
snmp-server contact admin@kyiv.yavorenko.net
snmp-server host 192.168.254.3 version 2c
SNMP_MONITOR_RO
no cdp log mismatch duplex
control-plane
mgcp behavior g729-variants static-pt
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				89
Змн.	Арк.	№ докум.	Підпис	Дата		

```

privilege exec level 4 traceroute
privilege exec level 4 ping
privilege exec level 4 show
line con 0
exec-timeout 0 0
privilege level 15
password qwerty123
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
transport output none
line vty 5 15
login local
transport input ssh
transport output none
end

```

```

SW_Core_1#sh run
Building configuration...
Current configuration : 5641 bytes
! Last configuration change at 01:13:22 UTC Wed
Jun 22 2022
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname SW_Core_1
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
username admin privilege 15 secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
username user secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
ip domain-name yavorenko.local
ip name-server 8.8.8.8
no ipv6 cef
ipv6 multicast rpf use-bgp
key chain EIGRP_KeyChain_Protected

```

```

key 1
key-string 123qwerty123
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface Ethernet0/0
duplex auto
interface Ethernet0/1
duplex auto
interface Ethernet0/2
duplex auto
interface Ethernet0/3
duplex auto
interface Ethernet1/0
duplex auto
interface Ethernet1/1
duplex auto
interface Ethernet1/2
duplex auto
interface Ethernet1/3
duplex auto
interface Vlan1
ip address 192.168.1.4 255.255.255.240
router eigrp 1
network 192.168.1.0 0.0.0.15
ip default-gateway 192.168.1.1
no ip http server
ip access-list standard SSH_MGMT
permit 192.168.254.0 0.0.0.31
ip access-list standard YA-
VORENKO_SNMP_ACL
permit 192.168.254.3
snmp-server group ADMIN v3 priv write YA-
VORENKO_SNMP-RW access YA-
VORENKO_SNMP_ACL
snmp-server view YAVORENKO_SNMP-RW iso
included
snmp-server location Ukraine_WAN
snmp-server contact admin@yavorenko.local.net
snmp-server enable traps snmp authentication link-
down linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-
change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-
change shamlink interface

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

```

snmp-server enable traps ospf cisco-specific state-
change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific re-
transmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps ethernet cfm cc mep-up
mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck
mep-missing mep-unknown service-up
snmp-server enable traps pw vc
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps ether-oam
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps mpls rfc traffic-eng
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute pro-
tected
snmp-server enable traps ethernet evc status create
delete
snmp-server enable traps auth-framework sec-viola-
tion
snmp-server enable traps dot1x auth-fail-vlan guest-
vlan no-auth-fail-vlan no-guest-vlan
snmp-server enable traps bridge newroot topology-
change
snmp-server enable traps stpx inconsistency root-in-
consistency loop-inconsistency
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps bfd
snmp-server enable traps bgp
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps cef resource-failure peer-
state-change peer-fib-state-change inconsistency
snmp-server enable traps dls
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps msdp
snmp-server enable traps mvpn

```

```

snmp-server enable traps pim neighbor-change rp-
mapping-change invalid-pim-message
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps slb real virtual csrp
snmp-server enable traps syslog
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps mpls vpn
snmp-server enable traps vrfmib vrf-up vrf-down
vnet-trunk-up vnet-trunk-down
control-plane
privilege exec level 4 traceroute
privilege exec level 4 ping
privilege exec level 4 show
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C
line con 0
exec-timeout 0 0
privilege level 15
password qwerty123
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
transport output none
end

```

```

SW_Lviv#sh run
Building configuration...
Current configuration : 2794 bytes
Last configuration change at 01:18:21 UTC Wed
Jun 22 2022
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname SW_Lviv
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
username admin privilege 15 secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

```

username user secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
ip domain-name yavorenko.local
ip name-server 8.8.8.8
no ipv6 cef
ipv6 multicast rpf use-bgp
key chain EIGRP_KeyChain_Protected
key 1
key-string 123qwerty123
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface Ethernet0/0
duplex auto
interface Ethernet0/1
duplex auto
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet0/2
duplex auto
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet0/3
duplex auto
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet1/0
duplex auto
interface Ethernet1/1
duplex auto
interface Ethernet1/2
duplex auto
interface Ethernet1/3
duplex auto
interface Vlan1
ip address 192.168.110.2 255.255.255.0
router eigrp 1
network 192.168.110.0
no ip http server
ip access-list standard ADMIN_SNMP_ACL
permit 192.168.254.3
ip access-list standard SNMP_ACL
permit 192.168.254.0 0.0.0.31
ip access-list standard SSH_MGMT
permit 192.168.254.0 0.0.0.31
snmp-server community SNMP_MONITOR_RO
RO SNMP_ACL
snmp-server community SNMP_MANAGER_RW
RW ADMIN_SNMP_ACL
snmp-server location Kharkiv_LAN

```

```

snmp-server contact admin@kharkiv.yavorenko.net
snmp-server host 192.168.254.3 version 2c
SNMP_MONITOR_RO
control-plane
privilege exec level 4 traceroute
privilege exec level 4 ping
privilege exec level 4 show
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C
line con 0
exec-timeout 0 0
privilege level 15
password qwerty123
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
transport output none
end

```

```

SW_Zhytomyr#sh run
Building configuration...
Current configuration : 2779 bytes
Last configuration change at 01:20:59 UTC Wed
Jun 22 2022
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname SW_Zhytomyr
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
username admin privilege 15 secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
username user secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
ip domain-name yavorenko.local
ip name-server 8.8.8.8
no ipv6 cef

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ipv6 multicast rpf use-bgp
key chain EIGRP_KeyChain_Protected
key 1
  key-string 123qwerty123
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface Ethernet0/0
interface Ethernet0/1
  duplex auto
  ip dhcp snooping limit rate 256
  ip dhcp snooping trust
interface Ethernet0/2
  duplex auto
  ip dhcp snooping limit rate 256
  ip dhcp snooping trust
interface Ethernet0/3
  duplex auto
  ip dhcp snooping limit rate 256
  ip dhcp snooping trust
interface Ethernet1/0
  duplex auto
interface Ethernet1/1
  duplex auto
interface Ethernet1/2
  duplex auto
interface Ethernet1/3
  duplex auto
interface Vlan1
  ip address 192.168.111.2 255.255.255.0
router eigrp 1
  network 192.168.111.0
no ip http server
ip access-list standard ADMIN_SNMP_ACL
  permit 192.168.254.3
ip access-list standard SNMP_ACL
  permit 192.168.254.0 0.0.0.31
ip access-list standard SSH_MGMT
  permit 192.168.254.0 0.0.0.31
snmp-server community SNMP_MONITOR_RO
RO SNMP_ACL
snmp-server community SNMP_MANAGER_RW
RW ADMIN_SNMP_ACL
snmp-server location Kyiv_LAN
snmp-server contact admin@kyiv.yavorenko.net
snmp-server host 192.168.254.3 version 2c
SNMP_MONITOR_RO
control-plane
privilege exec level 4 traceroute
privilege exec level 4 ping
privilege exec level 4 show
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C
line con 0

```

```

exec-timeout 0 0
privilege level 15
password qwerty123
logging synchronous
login local
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login local
  transport input ssh
  transport output none
end

```

```

SW_Kyiv#sh run
Building configuration...
Current configuration : 2705 bytes
Last configuration change at 01:22:44 UTC Wed
Jun 22 2022
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname SW_Kyiv
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
username admin privilege 15 secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
username user secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
ip domain-name yavorenko.local
ip name-server 8.8.8.8
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface Ethernet0/0
interface Ethernet0/1
  duplex auto

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				93
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet0/2
duplex auto
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet0/3
duplex auto
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet1/0
duplex auto
interface Ethernet1/1
duplex auto
interface Ethernet1/2
duplex auto
interface Ethernet1/3
duplex auto
interface Vlan1
ip address 192.168.112.2 255.255.255.0
router eigrp 1
network 192.168.112.0
no ip http server
ip access-list standard ADMIN_SNMP_ACL
permit 192.168.254.3
ip access-list standard SNMP_ACL
permit 192.168.254.0 0.0.0.31
ip access-list standard SSH_MGMT
permit 192.168.254.0 0.0.0.31
snmp-server community SNMP_MONITOR_RO
RO SNMP_ACL
snmp-server community SNMP_MANAGER_RW
RW ADMIN_SNMP_ACL
snmp-server location Kyiv_LAN
snmp-server contact admin@kyiv.yavorenko.net
snmp-server host 192.168.254.3 version 2c
SNMP_MONITOR_RO
control-plane
privilege exec level 4 traceroute
privilege exec level 4 ping
privilege exec level 4 show
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C
line con 0
exec-timeout 0 0
privilege level 15
password qwerty123
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
transport output none

```

```

end

SW_Kharkiv#sh run
Building configuration...
Current configuration : 2778 bytes
Last configuration change at 01:24:11 UTC Wed
Jun 22 2022
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname SW_Kharkiv
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
username admin privilege 15 secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
username user secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
ip domain-name yavorenko.local
ip name-server 8.8.8.8
no ipv6 cef
ipv6 multicast rpf use-bgp
key chain EIGRP_KeyChain_Protected
key 1
key-string 123qwerty123
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface Ethernet0/0
interface Ethernet0/1
duplex auto
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet0/2
duplex auto
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet0/3
duplex auto
ip dhcp snooping limit rate 256
ip dhcp snooping trust

```

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				94
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet1/0
duplex auto
interface Ethernet1/1
duplex auto
interface Ethernet1/2
duplex auto
interface Ethernet1/3
duplex auto
interface Vlan1
ip address 192.168.113.2 255.255.255.0
router eigrp 1
network 192.168.113.0
no ip http server
ip access-list standard ADMIN_SNMP_ACL
permit 192.168.254.3
ip access-list standard SNMP_ACL
permit 192.168.254.0 0.0.0.31
ip access-list standard SSH_MGMT
permit 192.168.254.0 0.0.0.31
snmp-server community SNMP_MONITOR_RO
RO SNMP_ACL
snmp-server community SNMP_MANAGER_RW
RW ADMIN_SNMP_ACL
snmp-server location Kyiv_LAN
snmp-server contact admin@kyiv.yavorenko.net
snmp-server host 192.168.254.3 version 2c
SNMP_MONITOR_RO
control-plane
privilege exec level 4 traceroute
privilege exec level 4 ping
privilege exec level 4 show
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C
line con 0
exec-timeout 0 0
privilege level 15
password qwerty123
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
transport output none
end

SW_MGMT#sh run
Building configuration...
Current configuration : 5759 bytes
Last configuration change at 01:27:03 UTC Wed
Jun 22 2022
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec

no service password-encryption
service compress-config
hostname SW_MGMT
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
username admin privilege 15 secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
username user secret 4
qefKtK/CXVSxbl0BYS7eza8/qgXxc.YEE8SapvqP
EvI
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
ip domain-name yavorenko.local
ip name-server 8.8.8.8
no ipv6 cef
ipv6 multicast rpf use-bgp
key chain EIGRP_KeyChain_Protected
key 1
key-string 123qwerty123
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
ip ssh time-out 90
ip ssh version 2
interface Ethernet0/0
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet0/1
duplex auto
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet0/2
duplex auto
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet0/3
duplex auto
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet1/0
duplex auto
interface Ethernet1/1
duplex auto
interface Ethernet1/2
duplex auto
interface Ethernet1/3
duplex auto

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Vlan1
  no ip address
  shutdown
no ip http server
ip access-list standard SSH_MGMT
  permit 192.168.254.0 0.0.0.31
ip access-list standard YA-
VORENKO_SNMP_ACL
  permit 192.168.254.3
snmp-server group ADMIN v3 priv write YA-
VORENKO_SNMP-RW access YA-
VORENKO_SNMP_ACL
snmp-server view YAVORENKO_SNMP-RW iso
included
snmp-server location Ukraine_WAN
snmp-server contact admin@yavorenko.local.net
snmp-server enable traps snmp authentication link-
down linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-
change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-
change shamlink interface
snmp-server enable traps ospf cisco-specific state-
change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific re-
transmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps ethernet cfm cc mep-up
mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck
mep-missing mep-unknown service-up
snmp-server enable traps pw vc
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps ether-oam
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps mpls rfc traffic-eng
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute pro-
tected
snmp-server enable traps ethernet evc status create
delete
snmp-server enable traps auth-framework sec-viola-
tion
snmp-server enable traps dot1x auth-fail-vlan guest-
vlan no-auth-fail-vlan no-guest-vlan

```

```

snmp-server enable traps bridge newroot topology-
change
snmp-server enable traps stpx inconsistency root-in-
consistency loop-inconsistency
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps bfd
snmp-server enable traps bgp
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps cef resource-failure peer-
state-change peer-fib-state-change inconsistency
snmp-server enable traps dlsw
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps pim neighbor-change rp-
mapping-change invalid-pim-message
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps slb real virtual csrp
snmp-server enable traps syslog
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps mpls vpn
snmp-server enable traps vrfmib vrf-up vrf-down
vnet-trunk-up vnet-trunk-down
control-plane
privilege exec level 4 traceroute
privilege exec level 4 ping
privilege exec level 4 show
banner motd ^CUnauthorized access is prohibited.
For legal users only.^C
line con 0
  exec-timeout 0 0
  privilege level 15
  password qwerty123
  logging synchronous
  login local
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous

```

		Яворенко Б.О.			KIK.KP.Б – 125 – 26 – ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		96

line vty 0 4
login local
transport input ssh

transport output none
end

		Яворенко Б.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Єфіменко А.А.				97
Змн.	Арк.	№ докум.	Підпис	Дата		