УДК 004.738 DOI: 10.30977/BUL.2219-5548.2022.96.0.14

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ МОНІТОРИНГУ ТА АНАЛІЗУ СТАНУ IP-МЕРЕЖІ НА ОСНОВІ ВИКОРИСТАННЯ ПРОТОКОЛУ SNMP

Голубничий Д. Ю., Коцюба В. П.
Харківський національний економічний університет ім. С. Кузнеця

Анотація. *Проведений аналіз технологій контролю, діагностики та моніторингу обладнання комп'ютерних мереж. Обґрунтовано, що найбільш ефективним і надійним засобом, що дозволяє виконувати завдання з управління IP-мережними пристроями, є протокол SNMP. Наведені архітектура й компоненти SNMP та алгоритми практичного налаштування SNMP на комп'ютері з ОС Windows та Linux.*

Ключові слова: *системи моніторингу, управління обладнанням, протокол мережного моніторингу, налаштування SNMP, MIB.*

Вступ

Сучасні комп'ютерні мережі дозволяють передавати потоковий трафік (передачу даних, відео, голосу тощо) будуються на основі застосування інфокомунікаційних технологій, які об'єднали в собі системи електрозв'язку, передачі даних, автоматизовані системи управління, засоби комп'ютерних мереж, оброблення даних, інформаційно-вимірювальні системи, бази даних та ін.

Підтримувати надійне функціонування та взаємодію глобальних та локальних (відомчих) комп'ютерних мереж, забезпечення виконання визначених вимог щодо надійності й ефективності їхньої роботи та складових елементів можливе за рахунок застосування систем і засобів контролю, керування, моніторингу та аналізу стану IP-мереж [1].

Аналіз публікацій

Системи моніторингу здійснюють управління комп'ютерною мережею в автоматизованому режимі, а рішення, що базуються на основі підготовленої інформації системою моніторингу про роботу обладнання (хостів, комутаторів, маршрутизаторів, серверів, модемів тощо) приймає адміністратор мережі.

Перевірку підключеного мережного обладнання та його доступність в IP-мережі можна здійснити за допомогою утиліти ping, яка використовується із стандартними скриптами. Для моніторингу мережі відправляються ICMP-запити й зворотно присилаються ICMP-відповіді, що устаткування доступне й підключене в єдину IP-мережу [2].

Програмне забезпечення Ping infoview є невеликою утилітою для опитування вузлів за іменами або IP-адресами з можливістю встановлення кількості та інтервалів пінгування. Вона є аналогом стандартної консольної програми ping.exe.

Звичайно, такий спосіб простий, надійний і часто застосовується тими, хто займається налагодженням цифрового обладнання IP-мереж та мережними адміністраторами, але якщо потрібно стежити за значеннями конкретних параметрів мережного обладнання, відповідністю параметрів і помилок, необхідно використовувати більш складні та надійні системи контролю.

На сучасному етапі для аналізу й діагностики комп'ютерних мереж застосовуються такі технології, програми та протоколи:

1. Вбудовані системи діагностики й управління (Embedded systems) – система управління та моніторингу обладнання локальних IP-мереж System Center Operations Manager (SCOM), яка забезпечує збір даних, їхній аналіз та зберігання на сервері баз даних Microsoft SQL Server. Ці системи виконуються у вигляді програмно-апаратних модулів, що встановлюються в комунікаційне обладнання, а також у вигляді програмних модулів, вбудованих в операційні системи Windows, UNIX та Linux.

Однак у цієї системи є низка недоліків, а саме система моніторингу охоплює багато загальних показників системи, але не придатна для стеження за визначеними параметрами, специфічність й складність під час налаштування [2, 3].

2. Система моніторингу Zabbix використовується для комплексного моніторингу мережного обладнання, серверів та сервісів. Складається із сервера моніторингу (ядра), що виконує періодичне опитування та отримання даних, обробляє їх, аналізує й здійснює запуск скриптів для розсилання повідомлень. Zabbix-проксі є надійним рішенням для централізованого віддаленого монітори-

нгу місць, філій, мереж, що не мають локальних адміністраторів й автоматичне виявлення за діапазоном IP-адрес.

Система моніторингу Zabbix має специфічні недоліки, такі як громіздкість сервісу, необхідність установлення програмного забезпечення на все обладнання мережі тощо [3].

3. Система моніторингу Nagios – програма для моніторингу систем і мереж, працює також і під Sun Solaris, FreeBSD, AIX і HPUX. За допомогою цієї програми доступний моніторинг стану хостів (завантаження процесора, використання диска, системні логи тощо), підтримка віддаленого моніторингу через шифровані тунелі SSH або SSL, можливість побудови карт мереж виявлення проблем відразу після їхнього виникнення та моніторинг безпеки системи [2, 3].

4. Система моніторингу Cacti дозволяє збирати статичні дані за певні часові інтервали й відтворювати їх у графічному вигляді за допомогою RRDtool-утиліти, написана в інфраструктурі Apache-PHP-MySql, дозволяє налаштовувати збір і відображення даних моніторингу на основі вебінтерфейсу й заздалегідь складеного набору графіків даних за останній день, тиждень, місяць і рік. Є можливість довільно задавати часовий проміжок, за який буде згенерований графік.

Недоліками системи Cacti є швидке наростання кількості однотипних налаштувань у разі значної кількості середовищ і серверів, а також обмежена продуктивність деяких JMX рішень для Cacti.

5. Аналізатори протоколів (Protocol analyzers) є програмними або апаратно-програмними системами. Програмне забезпечення аналізатора складається з ядра, що підтримує роботу мережного адаптера та програмного забезпечення, який декодує протоколи канального рівня й протоколи верхніх рівнів, таких як IP, TCP, ftp, telnet, HTTP тощо. Суттєвим недоліком аналізаторів є те, що вони обмежуються лише функціями моніторингу й аналізу трафіку в мережах.

6. Одним із найбільш зручних, надійних, простих і швидких засобів, який дозволяє виконувати практично весь спектр завдань управління мережними пристроями, є протокол для управління пристроями в IP-мережах Simple Network Management Protocol (SNMP).

SNMP визначений Інженерною радою інтернету (IETF) як компонент стеку TCP/IP.

Основною концепцією протоколу є те, що вся необхідна для управління пристроєм інформація зберігається на самому пристрої – будь то сервер, модем або маршрутизатор – у так званій адміністративній базі даних. Ці змінні можуть відтворювати такі параметри, як кількість пакетів оброблених пристроєм, стан його інтерфейсів, час й особливості функціонування пристрою тощо [3, 4].

За своєю сутністю моніторинг – це комплекс швидкого знаходження проблеми, оповіщення про неї адміністратора й діагностики, що дає повну й точну інформацію про несправну роботу IP-мережі. Необхідність вчасного прогнозування, запобігання поломок, оповіщення про них, зберігання інформації про стан обладнання в комп'ютерній мережі та оперативне усунення виявлених несправностей підтверджує актуальність цієї роботи.

Мета та постановка завдання

Метою роботи є аналіз принципів застосування технологій, програм і протоколів, що дозволяють керувати обладнанням і підтримувати надійну роботу комп'ютерної мережі.

Для досягнення поставленої мети необхідно розкрити особливості функціонування системи моніторингу мережного обладнання, побудованого на основі архітектур UDP/TCP та застосування мережних протоколів контролю й управління – SNMP відповідно до змісту рекомендації RFC 1155, 3584, 3411 тощо [4–7].

Виклад основного матеріалу

Усю необхідну інформацію протокол SNMP отримує з бази керуючої інформації Management Information Base (MIB). MIB є базою даних стандартизованої структури. База даних має деревоподібну структуру, а всі змінні класифіковані за тематикою. Кожне піддерево містить певну тематичну підгрупу змінних. Найбільш важливі компоненти, що відповідають за роботу мережних вузлів, об'єднані в підгрупі MIB-II. Існують два типи MIB: стандартні й фірмові. Стандартні MIB визначені комісією з діяльності інтернет Internet Activity Board (IAB), а фірмові – виробником пристрою.

У таблиці 1 наведено перелік найбільш поширених стандартів баз керуючої інформації. У базах даних, зазначених у таблиці 1, є багато змінних, які можуть бути корисні для діагностування мережі та мережного обладнання.

Наприклад, використовуючи MIB-II, можливо отримати відомості про загальну кількість пакетів, переданих мережним інтерфейсом, а за допомогою MIB-повторювача можна дізнатися інформацію про кількість колізій порту.

Таблиця 1 – Перелік основних стандартів баз керуючої інформації

База	Призначення
MIB-II	Задає значну кількість об'єктів, що можуть бути використані для управління мережними інтерфейсами
MIB-повторювача	Включена до підмножини MIB-II. Установлює об'єкти, які можна використовувати для керування повторювачем
MIB-мосту	Включена до підмножини MIB-II. Задає дані, які можна використовувати для керування мостом
RMON MIB	Вказує об'єкти даних, які можна використовувати для управління мережею загалом за допомогою протоколу Remote Network MONitoring (RMON)

У MIB кожен об'єкт має ім'я та тип. Ім'я об'єкта характеризує його становище в дереві MIB. У цьому разі ім'я дочірнього вузла містить ім'я батьківського вузла й задається цілим числом [6].

Компоненти SNMP

Для найменування змінних бази MIB і однозначного визначення їхніх форматів використовується додаткова специфікація, що називається SMI – Структура управління інформацією. Наприклад, специфікація SMI включається як стандартне ім'я IpAddress і визначає його формат як рядок з 4 байтів. Інший приклад – ім'я Counter, для якого визначено формат у вигляді цілого числа в діапазоні від 0 до 2^{32}.

Існує три компоненти SNMP, за допомогою яких він виконує свої основні завдання, наведені на рис. 1.

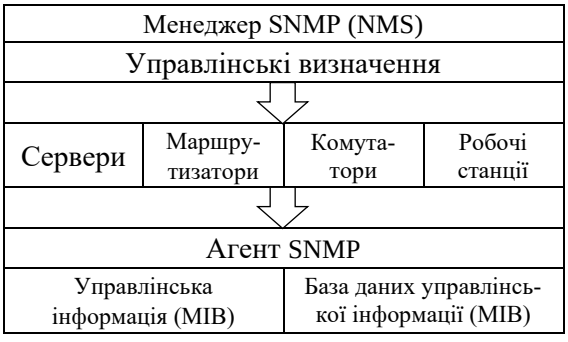

Рис. 1. Структура SNMP

1) Менеджер SNMP. Це централізована система вузлів на основі графічного інтерфейсу, яка використовується для моніторингу мережі. Її також називають Системою управління мережею Network management system (NMS). Він взаємодіє з двоспрямованим потоком інформації між вузлом NMS та елементами мережі. Елементами мережі можуть бути комутатори, комп'ютери (хости), маршрутизатори, сервери, IP-телефони, модеми, IP-відеокамери тощо.

2) Агент SNMP. Агент – це модуль програмного забезпечення для управління мережею, який встановлюється на мережному пристрої, такому як хост, сервер, маршрутизатор тощо. Агент підтримує базу даних про елементи мережі, які дистанційно керуються. Коли NMS запитує будь-яку інформацію, вона повертається разом із даними, що зберігалися в базі даних до NMS.

Якщо будь-яка пастка або помилка зустрічається агентом на керованому пристрої, він надсилає повідомлення про пастку менеджеру SNMP із зазначенням стану в реальному часі.

3) База даних управлінської інформації (MIB). Кожен з агентів SNMP підтримує інформаційну базу даних для керованих пристроїв, яка пояснює параметри пристроїв.

Менеджер SNMP використовує цю базу даних, щоб запитати в агента інформацію про конкретний пристрій для NMS. Отже, ця спільна інформація між агентом та менеджером відома як База даних MIB.

Структура MIB:

− це група інформації, що містить змінні, що містять значення, відповідні параметрам елемента мережі в його сховищах. Ці змінні відомі як керовані об'єкти та ідентифікуються ідентифікатором об'єкта (OID);

− MIB – це сукупність ідентифікаторів об'єктів у ієрархічному форматі, і кожен може ідентифікувати змінну, яку SNMP може встановити або прочитати;

− OID бувають двох видів – скалярні та табличні. Скаляр повідомляє лише про один випадок події, що означає, що результат – лише один. Приклад: текст або номер;

− табличний об'єкт – це таблиця, яка є пулом усіх пов'язаних OID і, отже, дає кілька результатів для одного значення об'єкта. Наприклад: для подвійного процесора центрального процесора це призведе до отримання двох значень.

Оскільки SNMP працює на прикладному рівні пакета протоколів TCP/IP, тому всі по-

відомлення SNMP будуть транспортуватися через протокол UDP (User Datagram Protocol). UDP-порт 161 використовується агентом SNMP для отримання запиту від менеджера. Однак менеджер може також надіслати запит на будь-який інший порт, який доступний крім цього.

Менеджер отримує відповідь у вигляді повідомлень, таких як повідомлення «Trap» та «Inform» на порт 162 UDP. NMS буде виконувати всі операції моніторингу та управління мережними пристроями / елементами та надавати основні дані, які використовуються для управління мережею [5, 6].

Агент SNMP, пов'язаний з кожним із керованих у мережі елементів, перекладає локальні дані MIB, такі як дані про продуктивність, інформацію про помилки, появу будь-якої події, у зручну форму для NMS. Для цього агент використовує Get-Requests, що доставляють дані до програмного забезпечення NMS. Мережні елементи, такі як маршрутизатори, комутатори, комп'ютери, модеми тощо, збирають і зберігають дані MIB, а за допомогою агента SNMP він робить їх доступними для сумісних із ними систем управління (рис. 2).

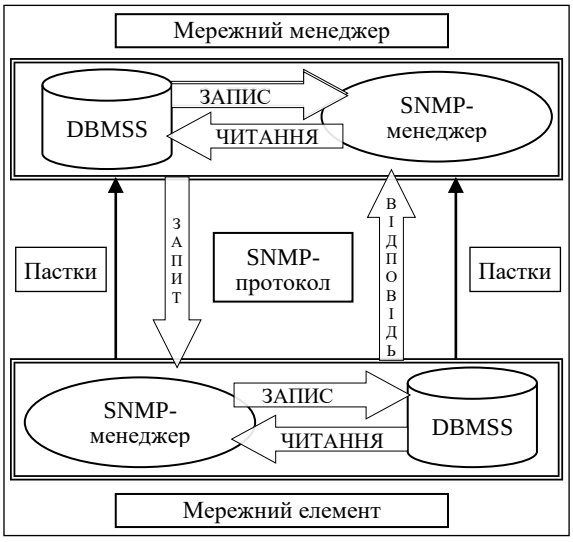

Рис. 1. Схема архітектури SNMP

Network Manager – це програмне забезпечення з відкритим кодом, таке як Solar winds та Cisco IOS. Для запуску SNMP менеджер мережі має встановити це програмне забезпечення на сервері. Основним завданням менеджера простого управління мережним протоколом є запит та отримання даних від агента для управління та моніторингу елементів мережі (рис. 2). Крім того, є можливість редагування конфігурації, коли це потрібно відповідно до вимог мережі.

Іншим важливим завданням є отримання повідомлень «Trap» та «Inform» щодо несправностей і виникнення подій у мережі.

Команди SNMP.

Розгортаючи SNMP, елементами мережі керують за допомогою трьох команд: читання, запис та пастка:

− команда читання використовується NMS для моніторингу керованих мережних елементів, таких як маршрутизатори, комутатори тощо. Цю дію завершує NMS, вивчаючи різні змінні, що підтримуються елементами мережі;

− команда запису використовується NMS для управління мережними елементами. За допомогою цієї команди NMS може змінювати значення змінних, що зберігаються в керованих мережних елементах;

− команда пастка використовується керованими мережними елементами, щоб повідомляти про випадки й помилки в системі управління [3, 7].

Повідомлення запиту SNMP, які є PDU, передбачають такі операції, як отримати, GetNext та GetBulk:

− Отримати. Використовуючи це повідомлення, запит NMS на отримання понад однієї змінної з агента SNMP;

− GetNext. Ця операція дозволяє новій системі управління отримувати одну або більше наступних змінних з агента SNMP;

− GetBulk. Ця операція відповідає послідовній операції GetNext. За допомогою цього набору повідомлень запитів ми можемо отримати базу даних від агента.

Відповідь: він повертає змінну одиницю даних від агента до NMS у відповідь на PDU запит на отримання та встановлення (рис. 3).

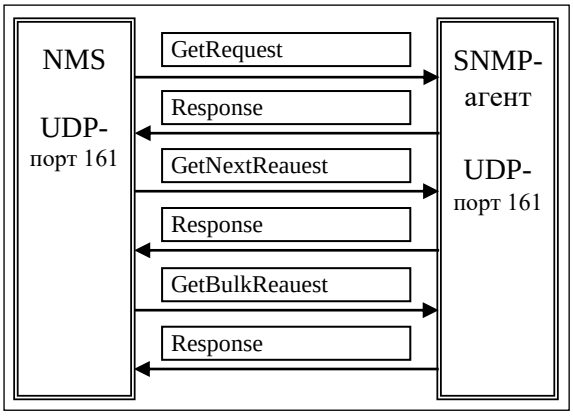

Рис. 2. Схема взаємодії за протоколом SNMP

Пастка. Ця команда ініціюється агентами SNMP. Коли подія відбувається, агент надсилає сигнал менеджеру SNMP для підтвердження події у формі цього PDU.

InformRequest. Його функція така сама, як і в команди «Trap». Він містить підтвердження отримання пакету від менеджера SNMP.

Коли в мережі відбувається подія, тоді SNMP «Trap» повідомляє про це менеджеру SNMP.

Наприклад, перехід порту зі стану DOWN у стан UP у маршрутизаторі. Інформація SNMP – це також пастки SNMP, які є квитанцією про підтвердження від менеджера.

На рис. 4 показано зв'язок між керованими SNMP елементами мережі та менеджером надсилання пасток і повідомлень. Функціональність «Trap» та «Inform» відрізняється.

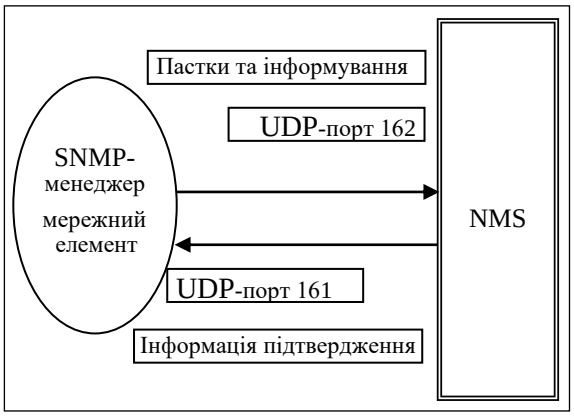

Рис. 3. SNMP-пастки

Повідомлення про захоплення SNMP надсилається лише один раз, а також відкидається, коли воно надсилається. Вони не зберігаються в пам'яті для отримання відповіді від менеджера. Повідомлення «Inform» надсилається знову й знову, поки не отримає відповідь від NMS або запит не закінчиться.

Якщо хост-пристрій не отримає відповіді від NMS, тоді він буде надсилати запит «Inform» кілька разів, поки не отримає необхідного результату. Отже, «Inform» використовує більше ресурсів пам'яті в мережі та мережних пристроях [8].

Протокол SNMP v3

Уніфікований протокол мережного моніторингу SNMP версії 3 (SNMP v3) завдяки сучасній модульній архітектурі, удосконаленим протоколам управління, зокрема протокол прикладного рівня, схему баз даних і набір об'єктів даних, можливістю шифрувати трафік, підтримці SNMP версії 1 та версії 2 й покращеному віддаленому налаштуванню широко застосовується для моніторингу та аналізу мережного устаткування, для знаходження й вирішення багатьох мережних проблем.

У SNMP v3 не застосовуються терміни «агент» і «менеджер», тепер використовується термін «сутності». Як і раніше, одна сутність знаходиться на керованому пристрої, а друга займається опитуванням застосунків.

У сутностей-агентів і сутностей-менеджерів є ядро, що виконує чотири основні функції (рис. 5):

- функції диспетчера;
- оброблення повідомлень;
- функції безпеки;
- контроль доступу.

Диспетчер – це система управління вхідним та вихідним трафіком. Для кожного вихідного блоку даних (PDU) він визначає тип необхідного оброблення (SNMP v1, SNMP v2, SNMP v3) та передає блок даних відповідного модуля в системі оброблення повідомлень.

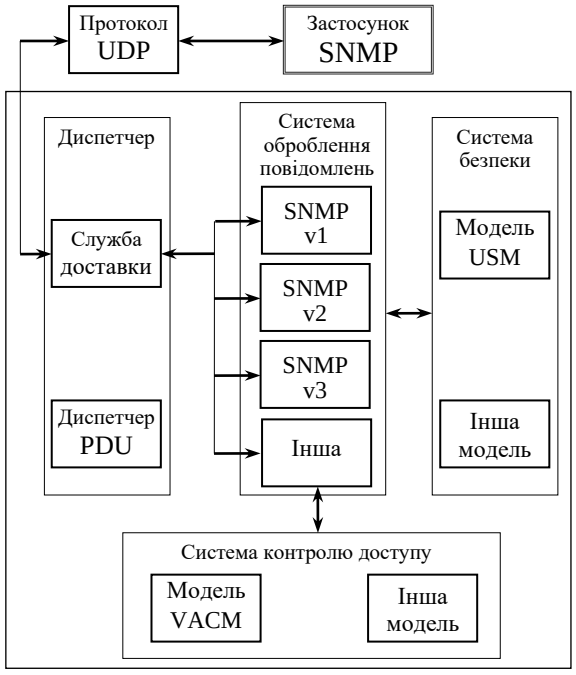

Рис. 4. Схема роботи ядра SNMP v3

Після того як система оброблення повідомлень поверне повідомлення, яке містить визначений блок даних, Диспетчер відправить його на рівень транспорту для подальшої передачі. Для вхідних повідомлень Диспетчер проводить зворотну операцію.

Система оброблення повідомлень отримує дані від Диспетчера PDU, додає до них відповідний заголовок та повертає їх назад Диспетчеру. Система безпеки відповідає за шифрування та автентифікацію.

Усі вихідні повідомлення перед відправленням спочатку передаються із системи оброблення повідомлень у систему безпеки, де шифруються поля в заголовку повідомлення, PDU, генерується код автентифікації та додається до заголовка повідомлення.

Система контролю доступу керує службами автентифікації контролю доступу до MIB із вмісту PDU. Теоретично система контролю доступу може працювати з різними моделями контролю доступу, але в RFC 2275 описана тільки одна модель View-Based Access Control Model (VACM) .

За допомогою цих команд та стандартної бази MIB можна отримати найрізноманітнішу інформацію.

Наприклад: кількість прийнятих та надісланих пакетів по TCP, IP, UDP або ICMP. А ще можна дізнатися про кількість помилок, що були виявлені під час надсилання або отримання пакетів.

У процесі розроблення SNMP v3 достатньо уваги було приділено безпеці протоколу. Тепер стала підтримуватися модель, орієнтована на користувача User-Based Security Model, (USM) завдяки якій можна додавати модулі автентифікації та шифрування без зміни базової архітектури [7].

Практичне застосування протоколу SNMP. Налаштування SNMP у Windows. Налаштування даних агента SNMP

Пуск → Панель управління → Адміністрування → Управління комп'ютером.

1. У дереві консолі необхідно розгорнути вузол «Служби та застосунки» й обрати пункт «Служби».

2. У ділянці праворуч двічі клацнути елемент «Служба SNMP».

3. Потім відкрити вкладку «Агент».

4. Ввести ім'я користувача або адміністратора комп'ютера в полі «Контакт», а потім ввести фізичне розташування комп'ютера або контакту в полі «Розташування». Ці коментарі обробляються як текст і є не обов'язковими.

5. У розділі «Служба» потрібно встановити прапорці поруч зі службами, що надаються комп'ютером, і натиснути кнопку «Так».

Налаштування співтовариства та пасток SNMP

Пуск → Панель управління → Адміністрування → Управління комп'ютером.

1. У дереві консолі потрібно розгорнути вузол «Служби та застосунки» й обрати пункт «Служби».

2. У ділянці праворуч двічі клацнути елемент «Служба SNMP».

3. Відкрити вкладку «Трепінг».

4. У полі «Ім'я співтовариства» ввести ім'я співтовариства й натиснути кнопку «Додати в список».

5. У розділі «Адресати пасток» натиснути кнопку «Додати».

6. У полі «Host Name» ввести ім'я, IP-адресу вузла й натиснути кнопку «Додати». Ім'я вузла або його адреса з'явиться в списку призначення пасток.

7. Натиснути кнопку «Так» [7, 9].

Налаштування безпеки SNMP

Пуск → Панель управління → Адміністрування → Управління комп'ютером.

1. У дереві консолі потрібно розгорнути вузол «Служби та застосунки» й обрати пункт «Служби».

2. У ділянці праворуч двічі клацнути елемент «Служба SNMP».

3. Відкрити вкладку «Безпека».

4. Установити прапорець «Пересилання пасток перевірки достовірності», якщо необхідно, щоб агент відправляв пастку в разі порушення перевірки достовірності.

5. У розділі «Прийнятні імена співтовариств» потрібно натиснути кнопку «Додати».

6. У полі «Права співтовариства» обрати дозволи, щоб вказати, як вузол оброблятиме запити SNMP від обраного співтовариства.

7. У полі «Ім'я співтовариства» ввести потрібне ім'я співтовариства з урахуванням регістру, а потім натиснути кнопку «Додати».

8. Потім для того, щоб приймати запити SNMP від будь-якого вузла мережі, незалежно від його статусу, потрібно вибрати варіант «Приймати пакети SNMP з будь-якого вузла».

9. Щоб обмежити прийняття пакетів SNMP, потрібно натиснути «Приймати пакети SNMP із цих комп'ютерів», потім натиснути «Додати» й ввести в поле ім'я вузла, IP-адресу або IPX-адресу відповідного вузла. Натиснути «Додати», а потім кнопку «Так».

Налаштування SNMP у Linux
Налаштування SNMP у CentOS 7

Спочатку потрібно встановити останні оновлення за допомогою yum/dnf

```
yum update
```

Потім встановити SNMP

```
yum install net-snmp net-snmp-utils
```

та створити копію конфігураційного файлу

```
mv /etc/snmp/snmpd.conf
/etc/snmp/snmpd.conf.orig
```

Тепер потрібно відредагувати налаштування агента

```
nano /etc/snmp/snmpd.conf
```

та додати рядки

```
community public syslocation
MyLocation syscontact
admin@example.com
```

Доцільніше вказувати дійсні назви про локацію та в email.

Потім необхідно додати сервіс в автозавантаження та перезапустити його

```
systemctl enable snmpd.service
systemctl start snmpd
```

Як перевірити, що сервіс запущений:

```
systemctl status snmpd
```

Опитування агента за допомогою утиліти snmpwalk:

```
snmpwalk -v 2c -c public –O e 127.0.0.1
```

Опитування сервера локальною командою:

```
snmpwalk -v2c -c public localhost system
```

Налаштування SNMP у Linux Debian

Насамперед потрібно встановити демона, клієнта та файли [9]

```
apt install snmpd snmp libsnmp-dev
```

Після встановлення переходимо до налаштування SNMP у Debian.

Файлом налаштування SNMP-агента за замовчуванням є /etc/snmp/snmpd.conf. Агент SNMP може бути запущений з налаштуваннями за замовчуванням. Проте для включення віддаленого моніторингу потрібно зробити декілька змін. Для цього необхідно створити резервну копію файлу

```
cp /etc/snmp/snmpd.conf
/etc/snmp/snmpd.conf.orig
```

Тепер потрібно змінити директиву agentAdress. Її поточні налаштування дозволяють доступ тільки з локального комп'ютера. Для включення віддаленого моніторингу необхідно визначити IP-адресу інтерфейсу

```
vim /etc/snmp/snmpd.conf
###################################
###########
#
# AGENT BEHAVIOUR
#

# Listen for connections from the
local system only agentAddress udp:
127.0.0.1:161,udp:192.168.43.62:161
```

Для налаштування автентифікації

```
directive community [source [OID]]
```

Rocommunity надає доступ тільки до читання, а rwcommunity – до читання / запису. У Access Control section потрібно помістити рядок

rocommunity S3CUrE 192.168.43.100.

Крім того, можна включити запит із локального хосту rocommunity S3CUrE localhost

```
rouser authOnlyUser
rwuser authPrivUser priv
rocommunity S3CUrE localhost
rocommunity S3CUrE 192.168.43.100
```

Потім потрібно перезапустити SNMP

```
systemctl restart snmpd
```

Щоб додати сервіс в автозавантаження, необхідно ввести

```
systemctl enable snmpd
```

Висновки

Наведений аналіз сучасних способів моніторингу та контролю мережного обладнання, показані переваги та недоліки основних технологій моніторингу та діагностування обладнання IP-мереж.

Розглянуті особливості функціонування, системи моніторингу мережного обладнання, побудованого на основі архітектури UDP/TCP із застосування мережного протоколу контролю та управління SNMP.

Показана структура та компоненти SNMP, наведена архітектура та схема роботи ядра SNMP v3 й детальний опис його роботи.

Наведені алгоритми практичного налаштування SNMP у Windows та Linux.

Література

1. Методи наукових досліджень в телекомунікаціях: навч. посібник: у 2 т. / за ред. проф. В.В. Поповского. Харків: Компанія СМІТ, 2013. Т. 1. 390 с.
2. SNMP. URL: https://znaimo.com.ua/
3. Кордяк В., Дронюк І., Федевич О. Інформаційна технологія моніторингу та аналізу трафіку у комп'ютерних мережах. Національний університет «Львівська політехніка» 2015. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/31297/1/07-35-42.pdf.

4. Взаємозв'язок між протоколами SNMP версії 1, версії 2 та версії 3 стандартної комп'ютерної мережі. URL: https://datatracker.ietf.org/doc/rfc3584/
5. Структура та ідентифікація керуючої інформації в мережах на основі стеку протоколів TCP/IP. URL: https://www.rfc-editor.org/info/rfc1155.
6. RFC 3411. MIB та архітектура SNMP. URL: https://www.arc-it.net/html/archuse/archuse.html.
7. Протокол управління SNMP. URL: https://selectel.ru/blog/snmp/
8. Обробка і відправлення повідомлень для SNMP. URL: https://www.arc-it.net/html/resources/resources.html.
9. Протоколи управління SNMP. URL: https://selectel/blog/snmp/

References

1. Research methods in telecommunications. In 2 volumes. Volume 1: textbook manual / ed. prof. V.V. Popovsky. Harkiv: SMITH Company, 2013. 390 p.
2. SNMP. URL: https://znaimo.com.ua/
3. Kordyak V., Dronyuk I., Fedevich O. Information technology for monitoring and analysis of traffic in computer networks. Lviv Polytechnic National University, 2015. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/31297/1/07-35-42.pdf.
4. Interconnection between SNMP versions 1, version 2 and version 3 of the standard computer network. URL: https://datatracker.ietf.org/doc/rfc3584/
5. Structure and identification of control information in networks based on the TCP / IP protocol stack. URL: https://www.rfc-editor.org/info/rfc1155.
6. RFC 3411. MIB and SNMP architecture. URL: https://www.arc-it.net/html/archuse/archuse.html.
7. SNMP management protocol. URL: https://selectel.ru/blog/snmp/
8. Processing and sending messages for SNMP. URL: https://www.arc-it.net/html/resources/resources.html.
9. SNMP Management Protocols. URL: https://selectel/blog/snmp/

Голубничий Дмитро Юрійович, к.т.н., доц. каф. інформаційних систем, Харківський національний економічний університет ім. С. Кузнеця, dmytro.holubnychyi@ hneu.net, тел. +38 093-900-38-96,

Коцюба Василь Петрович, к.т.н., доц. каф. інформаційних систем, Харківський національний економічний університет ім. С. Кузнеця, vasyl.kotsyuba@gmail.com,
тел. +38 067-573-27-89.

Applying technologies of monitoring and condition analysis of IP-networks based on the use of the SNMP protocol

Abstract. Problem. *Monitoring, security, condition analysis and control of telecommunications networks remains the most important part of system and network administration. Monitoring systems controls the network in an automated mode, and complex decisions based on the prepared information of the network monitoring system are made by the network administrator.* ***Goal.*** *The purpose of the work is to analyze the principles of applying technologies, programs and protocols that allow you to manage equipment and maintain reliable operation of the computer network. To consider features of functioning, the systems of monitoring of the network equipment are built on the basis of UDP/TCP architecture on application of the network protocol of control and management of SNMP.* ***Methodology.*** *Analytical methods of studying technologies of principles and approaches to network monitoring and management are used. The structure and components of SNMP are shown, the architecture and scheme of operation of SNMP v3 kernel and the detailed description of its work are resulted.* ***Results.*** *The analysis of modern methods of monitoring and control of network equipment is given, the advantages and disadvantages of the main technologies of monitoring and diagnosing the equipment of IP networks are shown. It is substantiated that the most effective and reliable tool that allows you to perform tasks on the management of IP network devices is the SNMP protocol.* ***Originality****. The monitoring system allows you to provide a set of solutions that maintain automatic monitoring of networks implemented on the basis of different technologies (data and speech, video), providing different services and built on equipment from different manufacturers.* ***Practical value.*** *The structure and components of SNMP are shown, the architecture and scheme of operation of SNMP v3 kernel and the detailed description of its work are resulted. Algorithms for practical SNMP configuration in Windows are presented, SNMP agent, trap and security data settings, configuring SNMP on Linux, SNMP settings in CentOS 7 and Debian 10.*

Key words: *monitoring systems, equipment management, network monitoring protocol, SNMP settings, MIB.*

Dmitro Holubnychyi, Ph.D., assoc. prof. kaf. information systems, Semyon Kuznets Kharkiv National University of Economics, tel. +38 38 093-900-38-96. dmytro.holubnychyi@hneu.net,

Vasily Kotsyuba, Ph.D., assoc. prof.kaf. information systems, Semyon Kuznets Kharkiv National University of Economics, vasyl.kotsyuba@gmail.com,
tel. +38 067-573-27-89.