Простий протокол управління мережею - це широко використовуваний протокол управління для зв'язку з мережевими пристроями, такими як маршрутизатори, комутатори, концентратори, IP-телефони, сервери тощо через IP-мережу.

***Він забезпечує обмін мережею та інформацією про продуктивність між мережевими елементами за допомогою портів UDP 161 і 162. Мережа, керована SNMP, складається з системи управління, що називається NMS, агента та керованих пристроїв.***



У цьому посібнику ми розглянемо основні будівельні блоки цього протоколу за допомогою команд, що використовуються для порту 161 та порту 162 для зв'язку. Крім того, ми побачимо концепцію SNMP Traps and Informs коротко за допомогою діаграм.

На додаток до цього, цей посібник також пояснює деякі популярні засоби моніторингу SNMP з їх функціями та зображеннями. Для кращої ясності теми прочитайте деякі відповіді на поширені запитання.

Що ви дізнаєтесь:

[C # Об'єктно-Орієнтовані Концепції Програмування](https://uk.myservername.com/oops-concepts-c-object-oriented-programming-concept-tutorial)

* [Простий протокол управління мережею](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#Simple_Network_Management_Protocol)
  + [Компоненти SNMP](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#SNMP_Components)
  + [Як працює простий протокол управління мережею](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#How_Simple_Network_Management_Protocol_Works)
  + [Команди SNMP](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#SNMP_Commands)
  + [SNMP-пастки](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#SNMP_Traps)
  + [Прості версії протоколів управління мережею](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#Simple_Network_Management_Protocol_Versions)
  + [Прості номери портів протоколів управління мережею](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#Simple_Network_Management_Protocol_Port_Numbers)
  + [Використання простого протоколу управління мережею](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#Uses_Of_Simple_Network_Management_Protocol)
* [Засоби моніторингу SNMP](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#SNMP_Monitoring_Tools)
  + [# 1) Мережевий монітор Paessler PRTG](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#1_Paessler_PRTG_Network_Monitor)
  + [# 2) Монітор продуктивності мережі Solar Winds](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#2_Solar_Winds_Network_Performance_Monitor)
  + [# 3) Управління двигуном Op Manager](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#3_Manage_Engine_Op_Manager)
* [Проста конфігурація протоколу управління мережею](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#Simple_Network_Management_Protocol_Configuration)
  + [Часті запитання](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#Frequently_Asked_Questions)
* [Висновок](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#Conclusion)
  + [Рекомендована література](https://uk.myservername.com/java-copy-array-how-copy-clone-an-array-java#Recommended_Reading)

**Простий протокол управління мережею**

SNMP використовується на прикладному рівні архітектури TCP / IP, і, як випливає з назви, він використовується для управління та моніторингу несправностей мережі та мережі. Іноді він також використовується для модифікації конфігурації віддалених кінцевих пристроїв мережі.

Приладами, сумісними з Протоколом простого управління мережею, є модеми, маршрутизатори, комутатори, принтери та сервери тощо.

**Компоненти SNMP**

**Існує три компоненти SNMP, за допомогою яких він виконує свої основні завдання. Вони такі:**

**# 1) Менеджер SNMP**

Це централізована система вузлів на основі графічного інтерфейсу, яка використовується для моніторингу мережі, а також її називають Системою управління мережею (NMS). Він взаємодіє з двонаправленим потоком інформації між вузлом NMS та елементами мережі.

Тут елементами мережі є комутатори, маршрутизатори, сервери, модеми, комп'ютерний хост, телефонні та відеокамери на базі IP-адрес тощо.

**# 2) Агент SNMP**

Агент - це модуль програмного забезпечення для управління мережею, який встановлюється на мережевому пристрої, такому як хост-ПК, сервер, маршрутизатор тощо. Агент підтримує базу даних про керовані елементи мережі. Коли NMS запитує будь-яку інформацію, вона повертається разом із даними який зберігався в базі даних до НМС.

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

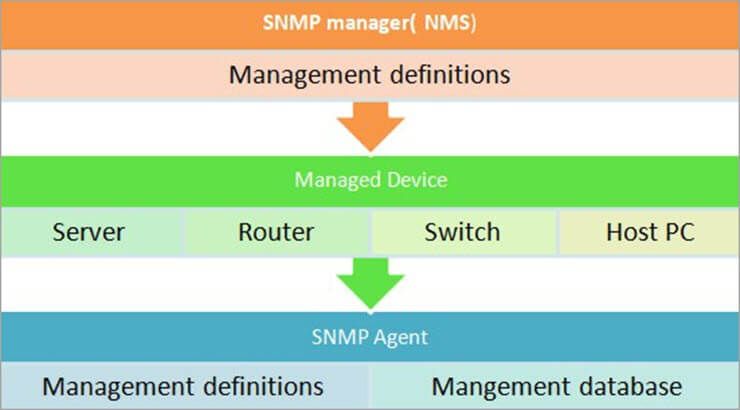
**# 3) База даних управлінської інформації (MIB)**

Кожен з агентів SNMP підтримує інформаційну базу даних для керованих пристроїв, яка пояснює параметри пристроїв.

Менеджер SNMP використовує цю базу даних, щоб запитати у агента інформацію про конкретний пристрій для NMS. Таким чином, ця спільна інформація між агентом та менеджером відома як База даних управлінської інформації (MIB).

**Структура MIB:**

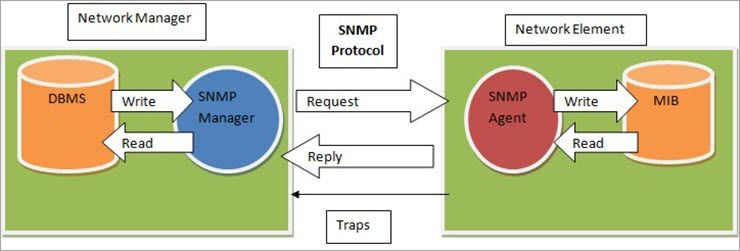
* Це група інформації, що включає змінні, що містять значення, відповідні параметрам елемента мережі в його сховищах. Ці змінні відомі як керовані об'єкти та ідентифікуються ідентифікатором об'єкта (OID).
* MIB - це сукупність ідентифікаторів об'єктів в ієрархічному форматі, і кожен може ідентифікувати змінну, яку SNMP може встановити або прочитати.
* OID бувають двох видів, скалярні та табличні. Скаляр повідомляє лише про один екземпляр події, що означає, що результат - лише один. **Приклад:** текст або номер.
* Табличний об’єкт - це таблиця, яка є пулом усіх пов’язаних OID і, таким чином, дає кілька результатів для одного значення об’єкта. **Наприклад:** Для подвійного процесора центрального процесора це призведе до двох значень.



**Як працює простий протокол управління мережею**

* Оскільки він працює на прикладному рівні пакета протоколів TCP / IP, таким чином усі повідомлення 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 доступний порт, який доступний крім цього.
* Менеджер отримує відповідь у вигляді повідомлень, таких як повідомлення «Trap» та «Inform» на порту 162 UDP.
* NMS буде виконувати всі операції моніторингу та управління мережевими пристроями / елементами та надавати основні дані, які використовуються для управління мережею.
* Агент SNMP, який пов'язаний з кожним з керованих мережами елементів, перекладає локальні дані MIB, такі як дані про продуктивність, інформацію про помилки, появу будь-якої події, у читабельну форму для NMS.
* Для цього агент використовує Get-Requests, які доставляють дані до програмного забезпечення NMS.
* Мережеві 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 з ними систем управління.

**Це можна зрозуміти за допомогою наведеного нижче малюнка: Схема архітектури SNMP**



* Network Manager - це програмне забезпечення з відкритим кодом, таке як Solar winds та Cisco IOS. Для запуску SNMP менеджер мережі повинен встановити це програмне забезпечення на сервері.
* Як ми бачимо з наведеного малюнка, основним завданням менеджера простого управління мережевим протоколом є запит та отримання даних від агента для управління та моніторингу елементів мережі. Крім того, для редагування конфігурації, коли це потрібно відповідно до вимог мережі.
* Іншим важливим завданням є отримання повідомлень Trap and Inform щодо несправностей та виникнення подій у мережі.

**Команди SNMP**

Розгортаючи SNMP, елементами мережі керують за допомогою трьох команд: Читання, Запис та Захоплення.

* **Команда читання** розгортається NMS для моніторингу керованих мережевих елементів, таких як маршрутизатори, комутатори тощо. Цю дію завершує NMS, вивчаючи різні змінні, які підтримуються елементами мережі **.**
* **Команда написання** розгортається НМС для управління мережевими елементами. За допомогою цієї команди NMS може змінювати значення змінних, які зберігаються в керованих мережевих елементах.
* **Пастка** **команди** використовується керованими мережевими елементами, щоб повідомляти про випадки та помилки в нову систему управління.

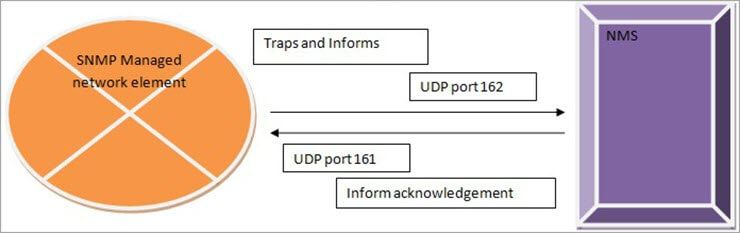
**Повідомлення запиту SNMP, які є PDU, включають такі операції, як „Отримати”, „Отримати” та „Отримати”.**

* **Отримати:** Використовуючи це повідомлення, запит NMS на отримання більш ніж 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 навалом.
* **Відповідь:** Він повертає змінну одиницю даних від агента до NMS у відповідь на PDU запиту на отримання та встановлення.
* **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 ж, як і у команди Trap. Він включає підтвердження отримання пакету від менеджера SNMP.



**SNMP-пастки**

**Порти та команди UDP, що використовуються NMS та керованими пристроями:**



* Коли в мережі відбувається подія, тоді SNMP Traps повідомлять 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 рисунку вище показано зв’язок між керованими SNMP елементами мережі та менеджером надсилання пасток та повідомлень. Функціональність Trap and Inform відрізняється.
* 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. Поки Inform надсилається знову і 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 жодного результату, таким чином Informs споживає більше ресурсів і пам'яті в мережі та мережевих пристроях.

**Прості версії протоколів управління мережею**

* **SNMPv1 (версія 1):** Це початкова версія протоколу. Він забезпечує найменшу кількість функцій управління мережею. Його автентифікація базується на іменах спільнот, тому вона також повертає менше кодів контролю помилок, які забезпечують дуже низький рівень безпеки.
* **SNMPv2 (версія 2):** Це перероблена версія SNMPv1, яка має імпровізацію в галузі безпеки, управління мережею та управління продуктивністю. Це створило нове повідомлення PDP, „GetBulkRequest”, яке використовується для вилучення великих даних від агента в одному запиті. SNMPv2c, який називають простою мережевою версією управління на основі спільноти версії 2, сумісний із моделлю безпеки інших версій.
* **SNMPv3 (версія 3):** Ця версія надає додаткову функцію криптографічного захисту, що робить її більш ефективною, ніж попередні версії. Він також має можливість віддаленого управління мережею та налаштування мережевих елементів і базується на Модулі безпеки на основі користувача (USM), а також на Моделі контролю доступу на основі перегляду (VACM).

**Прості номери портів протоколів управління мережею**

Пакети даних SNMP використовують UDP для зв'язку і мають два номери портів за замовчуванням, тобто порт 161 і порт 162.

|  |  |
| --- | --- |
| **Порт 161** | **Порт 162** |
| Маршрутизатор> увімкнути | Увійдіть у режим привілеїв |
| Цей порт використовується, коли NMS надсилає агенту пакети PDU Get, GetNext, GetBulk та Set Request. і агент надсилає відповідь на ці запити. | Це використовується агентом SNMP для відправки пастки та інформування пакета PDU до менеджера SNMP. |  |
| Менеджер SNMP отримує відповідь від агента на цьому порту. | Агент генерує повідомлення, щоб повідомити про будь-яку помилку або помилку з цього порту менеджеру SNMP. |  |
| Це використовується для зв'язку між менеджером SNMP та агентом SNMP для налаштування та моніторингу. | Це використовується для повідомлення агента SNMP про випадки подій менеджеру SNMP. |  |
| Повідомлення надсилається знову і знову по цьому порту до часу очікування запиту, якщо воно не отримає відповіді. | Як тільки повідомлення відправляється на цей порт, вони відкидаються без будь-якого підтвердження. |  |

**Використання простого протоколу управління мережею**

**Використання полягає в наступному:**

* Він використовується для моніторингу та налаштування мереж, включаючи глобальну мережу, мережі LAN та мережеві пристрої, такі як маршрутизатори, комутатори, мультиплексори, PDH та SDH-лінії, сервери та концентратори тощо.
* SNMP описує дані управління в режимі змінних на керованих мережевих пристроях, які детально визначають продуктивність мережі, конфігурацію та параметри стану.
* Крім того, ці змінні можуть запитуватися системою управління (NMS), встановлюючи та керуючи інструментом та програмами моніторингу.

**Таким чином, параметри, які ми можемо зрозуміти звідси:**

1. Відстежуйте загальну продуктивність мережі
2. Аудит використання ресурсів
3. Виявити несправність мережі та сигнали тривоги
4. Налаштування віддалених посилань та пристроїв
5. Конфігурація WAN-посилань
6. Діагностуйте несанкціонований доступ та втручання в мережу

**Засоби моніторингу SNMP**

Інструмент SNMP забезпечує мережу для моніторингу та управління мережевими елементами, дозволяючи модифікувати та збирати дані, що стосуються мережі та поведінки пристрою. Він забезпечує точність, якість обслуговування та ефективність для підтримки здорової та безперебійної роботи мережі та обслуговування.

Хороші інструменти моніторингу можуть допомогти користувачам ефективніше керувати мережею, регулярно отримуючи значення основних факторів моніторингу, таких як несправність, конфігурація та параметри продуктивності.

**Деякі засоби моніторингу SNMP:**

**# 1) Мережевий монітор Paessler PRTG**

Це гнучкий інструмент моніторингу мережі, який пропонує три види методів моніторингу, включаючи нюхання пакетів та Netflow, а також мережевий монітор SNMP. Цей інструмент кращий серед інших доступних на ринку інструментів завдяки різним датчикам, які він використовує для контролю різних елементів мережі.



**Особливості:**

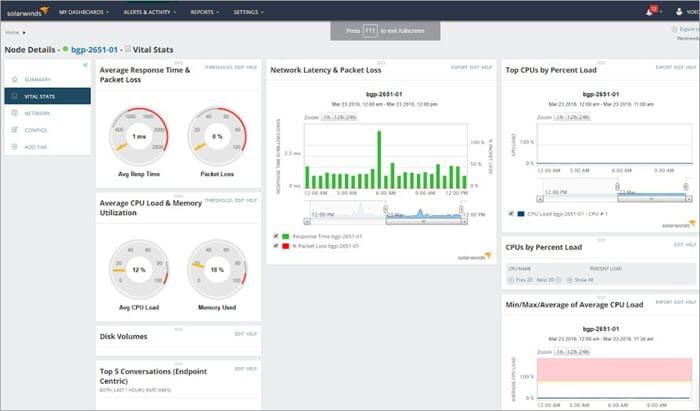
* Він забезпечує надійність мережі для моніторингу SNMP, пропонуючи різні мережеві датчики, які також сумісні з різними версіями протоколу SNMP. (SNMPV1, SNMPV2c та SNMPV3).
* Він пропонує моніторинг мережі та мережевих пристроїв за допомогою мінімальної пропускної здатності. Таким чином, навантаження на лінії STM та WAN стає мінімізованою, а операції стають більш плавними.
* Цей інструмент сумісний з широким спектром виробників мережевих пристроїв, таких як Cisco, Dell, HP тощо, що полегшує його використання та впровадження.
* Це незалежний від платформи інструмент. Таким чином, він може бути реалізований на Windows, Linux та Mac OS без будь-яких проблем.

**Ціна: Монітор мережі PRTG 500:** 1750 доларів

**Офіційна URL-адреса: [Песслер](https://www.paessler.com/prtg" \t "_blank)**

**# 2) Монітор продуктивності мережі Solar Winds**

Цей інструмент відрізняється від інших, оскільки він автоматично виявляє мережеві пристрої, присутні в мережі, та забезпечує інтерактивну платформу інформаційної панелі для перевірки стану мережі та звіту про продуктивність.



**Особливості:**

* Вбудований інструмент виявлення пристроїв - сканер Simple Network Management Protocol може автоматично знаходити, відображати та налаштовувати мережеві пристрої після встановлення програмного забезпечення в мережеву систему.
* Він розроблений таким чином, що діагностика, виявлення та усунення несправностей мережі буде відновлено до виникнення відключень. Це було спрощено завдяки великому відображенню мережевих параметрів у формі налаштованих інформаційних панелей та діаграм.
* Цей інструмент моніторингу продуктивності мережі здатний забезпечити 99,99% доступності мережі у вашій мережі та корисний для задоволення бізнес-потреб на вимогу щодо доброго стану мережі.
* Це дуже легко встановити в мережі і легко зрозуміти. Також сумісний з усіма версіями протоколу.

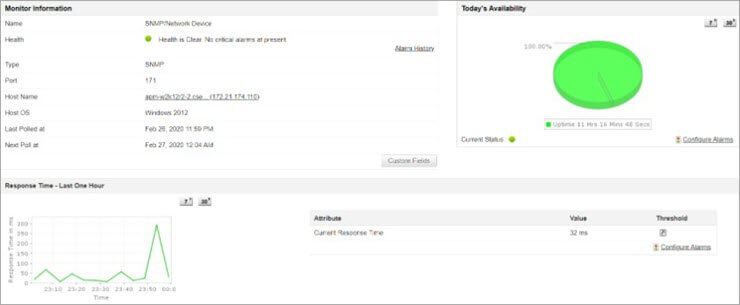
**Ціна: NPM SL 100:** 1583 дол

**Офіційна URL-адреса** : [**Сонячні вітри**](https://www.solarwinds.com/network-performance-monitor/use-cases/snmp-monitoring)

**# 3) Управління двигуном Op Manager**

Це програмне забезпечення може контролювати мережеві пристрої з підтримкою SNMP і сумісне з усіма трьома версіями Простого протоколу управління мережею. Моніторинг здійснюється шляхом управління агентами SNMP за допомогою програмного додатка.

Крім того, можна встановити індивідуальну базу даних MIB, і завдяки цьому користувач може отримувати SNMP-пастки від програми.



**Особливості:**

* Як пояснювалося вище, користувачеві потрібно лише встановити базу даних MIB у програму, і він / вона може вибрати параметри, які потрібно контролювати. Потім інструмент автоматично генерує графічний вигляд та інформаційну панель звітів та продуктивності.
* Це зручний програмний інструмент, таким чином користувач може встановити пороговий рівень для сигналізацій та несправностей, щоб отримувати сповіщення про помилку. Це допомагає своєчасно вживати коригувальні заходи та мінімізує відключення.
* Він також підтримує прослуховувач трапів SNMP. Він може надсилати та обробляти SNMP-пастки та SNMP-інформи та складати зведений звіт про всі події, що відбулися в мережі.
* Він сумісний з Windows і Linux і може повідомляти такі важливі параметри, як затримка, втрата пакетів, швидкість, навантаження процесора, навантаження пам'яті тощо.

**Ціна** : **Стандартна версія (10 пристроїв):** $ 245

**Офіційна URL-адреса** : [**Управління двигуном**](https://www.manageengine.com/products/applications_manager/snmp-manager.html)

**Проста конфігурація протоколу управління мережею**

**Для управління мережею SNMP доступні різні типи команд і типів конфігурації. Основні параметри конфігурації пояснюються в таблиці нижче:**

|  |  |  |
| --- | --- | --- |
| **Кроки** | **Команда** | **Опис і призначення** |
| **Крок 1** | Маршрутизатор # Налаштування терміналу | Для початку перейдіть у режим конфігурації |
| **Крок 2** | Маршрутизатор (конфігурація) # snmp-серверний контактний текст | Щоб налаштувати контактну інформацію SNMP |
| **Крок 3** | Маршрутизатор (конфігурація) # snmp-server location text | Щоб налаштувати інформацію про місцезнаходження |
| **Крок 4** | Маршрутизатор (конфігурація) # snmp-server chassis-id number | Налаштування ідентифікаційного номера шасі на сервері |
| **Крок 5** | Маршрутизатор (конфігурація) # snmp-server string community [view view-name] [ro | rw] [access-list-number] | Ця команда використовується для налаштування спільноти SNMP. У назві подання буде вказана кількість змінних, що використовуються для доступу до агента SNMP за допомогою рядка спільноти. Номер списку доступу буде містити IP-адреси номера менеджера SNMP, уповноваженого отримати доступ до агента SNMP. |
| **Крок 6** | Маршрутизатор (конфігурація) # кінець | Для виходу з режиму конфігурації маршрутизатора |
| **Крок 8** | Термінал налаштування маршрутизатора # | Увійдіть у режим конфігурації |
| **Крок 9** (конфігурація для Trap and Inform) | Маршрутизатор (конфігурація) # хост хосту snmp-сервера [traps | інформує] [versionpriv]] ім'я спільноти | Він використовується для налаштування місця, куди будуть надсилатися SNMP-пастки або Інформація. |
| **Крок 10** | Маршрутизатор (конфігурація) # snmp включити пастки [тип повідомлення] | Увімкнення агента SNMP для надсилання пасток SNMP або інформування з хостом. |
| **Крок 11** | Маршрутизатор (конфігурація) # кінець | Вийти з режиму конфігурації |

ad

**Часті запитання**

**Q # 1) Що таке SNMP V3?**

**Відповідь:** Це пов'язано з широкомасштабним впровадженням мереж для управління несправностями мереж глобальної мережі. Це захищена версія Простого протоколу управління мережею з можливістю віддаленого налаштування віддалених елементів мережі.

**Q # 2) Що таке SNMP Trap?**

**Відповідь:** Це пильне сповіщення або повідомлення, надіслане елементом мережі або пристроєм менеджеру мережі, повідомляючи про помилку або тривогу, яка сталася як висока температура.

**Запитання №3) SNMP TCP або UDP?**

**Відповідь** : Простий протокол управління мережею використовує протокол UDP (User Datagram Protocol) для зв'язку через порти 161 та порт 162. Це порти за замовчуванням. Він віддає перевагу UDP, оскільки не використовується TCP накладних витрат.

**Q # 4) Яка мета SNMP?**

**Відповідь:** Основна мета - дистанційне та централізоване управління мережевою системою або великими мережами адміністраторами мережі. Він розроблений таким чином, що менеджери мереж можуть централізовано керувати та контролювати мережеві пристрої.

**Q # 5) Чи безпечний SNMP?**

**Відповідь** : Це захищено чи ні, залежить від архітектури мережі та версії простого протоколу управління мережею, який ви використовуєте. Але SNMP V3 є більш безпечним, ніж інші дві версії, оскільки використовує зашифрований режим для зв'язку.

**Висновок**

Менеджер мережі, база даних MIB та елементи мережі - три основні компоненти, завдяки яким відбувається загальний процес спілкування та управління.

Також розглянули різні версії, методи конфігурації та інструменти, що використовуються для простого протоколу управління мережею. Порт, який використовується для зв'язку, відіграє надзвичайно важливу роль у завершенні зв'язку між менеджером SNMP та агентом SNMP.

Також проаналізовано табличну різницю між двома портами за замовчуванням SNMP, тобто портом 161 і портом 162