Лабораторна робота №14

Налаштування SNMP-моніторингу.

Мета: розгорнути та налаштувати SNMP-сервер на базі Ubuntu, забезпечити його інтеграцію з агентами моніторингу та використати SNMP-інструменти для аналізу стану системи.

Інструменти: гіпервізор VirtualBox, модель комп'ютерної мережі.

Теоретичні відомості

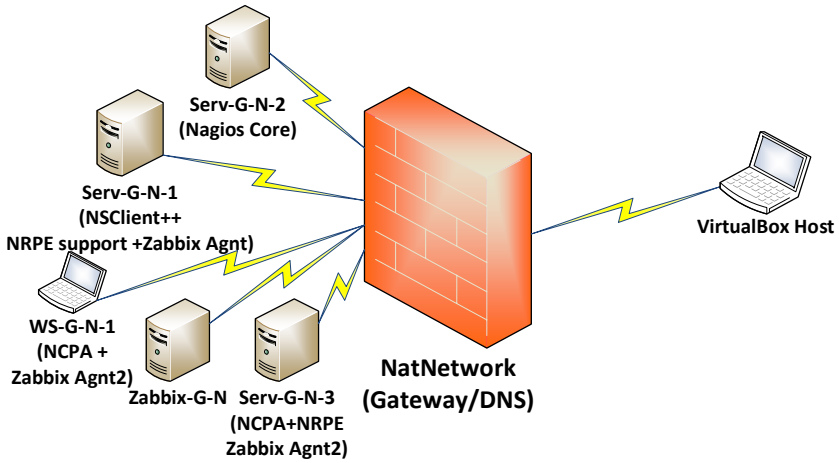

Рис. 14.1. Топологія мережі

На рис. 14.1 наведена модель комп'ютерної мережі, побудована під час виконання попередніх лабораторних робіт. На сервері Serv-G-N-2 розгорнуто систему моніторингу на базі Nagios 4.X. На сервері Zabbix-G-N працює сервер Zabbix з базовими налаштуваннями. В обох моніторингових системах налаштоване спостереження за Serv-G-N-1, WS-G-N-1, Serv-G-N-3.

Загальні відомості про SNMP (Simple Network Management Protocol)

SNMP – це протокол для моніторингу та управління мережевими пристроями, такими як маршрутизатори, комутатори, сервери, принтери тощо. Основні принципи SNMP-моніторингу:

Архітектура SNMP.

- Агент (Agent): ПЗ, яке працює на пристрої, що моніториться. Збирає дані пристрою та відповідає на запити.
- Менеджер (Manager): Централізована система, яка опитує агенти, отримує дані та аналізує їх.
- MIB (Management Information Base): БД об'єктів, які можуть бути керовані чи моніторені. Кожен об'єкт описується унікальним ідентифікатором (OID).

Основні операції SNMP

- Get: Менеджер запитує інформацію в агента.
- Set: Менеджер змінює налаштування на пристрої через агента.
- Trap: Агент самостійно надсилає повідомлення про важливу подію або проблему.
- Walk: Послідовний збір даних з MIB (наприклад, отримання всіх інтерфейсів пристрою).
- Bulk: Оптимізований збір великої кількості даних одним запитом.

Рівні версій SNMP

- SNMPv1: Початкова версія, базовий набір функцій, слабка безпека.
- SNMPv2c: Додано підтримку "bulk" операцій, але використовується лише «community string» для автентифікації.
- SNMPv3: Додана безпека (шифрування, автентифікація, контроль доступу).

Режими роботи

- Polling: Менеджер періодично опитує агентів для збору даних.
- Trap-орієнтований: Менеджер отримує тільки події (traps), що надсилаються агентами.

Ключові метрики

- Статистика інтерфейсів (трафік, помилки, статуси).
- Завантаження процесора та пам'яті.
- Стан дискових накопичувачів.
- Температура, вентилятори, живлення.

SNMP забезпечує ефективний спосіб централізованого контролю мережевих пристроїв і швидкого реагування на події.

Встановлення SNMP-сервера (snmpd) на Ubuntu

Для забезпечення ефективного вивчення принципів моніторингу SNMP існує широкий вибір безкоштовних інструментів, які можна адаптувати для різних рівнів складності та сценаріїв. Для базових навчальних стендів доцільно використовувати snmpd (Net-SNMP) або MiniSNMPd. Для моделювання складніших мережевих середовищ рекомендовано розгорнути SolarWinds SNMP Simulator або OpenNMS SNMP Mock. У випадках роботи з безпечним протоколом SNMPv3 зручно застосовувати iReasoning або Net-SNMP. А для тестування SNMP-трапів (повідомлень про події) варто скористатися спеціалізованим інструментом SNMPTT.

Встановимо у якості SNMP-сервера на Ubuntu snmpd та snmp(snmpwalk):

sudo apt update

sudo apt install snmpd

sudo apt install snmp

Для налаштування SNMP, редагуємо файл конфігурації SNMP демона ***/etc/snmp/snmpd.conf***, змінюючи такі параметри для базових налаштувань:

```
sysLocation  "System and network monitoring"
sysContact  "admin@falkovsky.net"
agentAddress udp:161
rocommunity public default -V systemonly
```

Перезапускаємо службу SNMP та перевіряємо, чи вона працює:

sudo systemctl restart snmpd

snmpwalk -v 2c -c public localhost

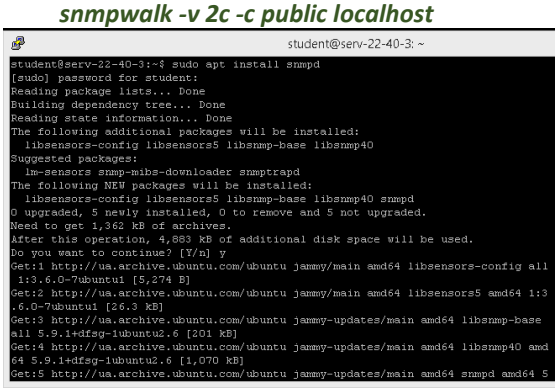

Рис. 14.2. Встановлення та налаштування SNMPD на сервері Serv-22-40-3

На рис.14.2 показаний процес встановлення, налаштування та перевірки працездатності SNMP-генератора на сервері Serv-G-N-3. Вивід команди snmpwalk є стандартним результатом запиту до SNMP-сервера і показує значення об'єктів, доступних через протокол SNMP.

iso.3.6.1.2.1... —OID (Object Identifier), який ідентифікує конкретний об'єкт в ієрархії MIB (Management Information Base).

= STRING, = INTEGER, = OID — тип значення об'єкта.

Значення справа від = — поточні дані, отримані з сервера.

Відредагуємо файл конфігурації SNMP демона ***/etc/snmp/snmpd.conf*** , щоб мати можливість отримати інформацію не тільки про системні об'єкти. Замінюємо systemonly на all, щоб мати доступ до всіх об'єктів MIB:

```
rocommunity public default -V all
```

Ми зможемо отримати інформацію не тільки про системні об'єкти, але й про інші компоненти, такі як мережеві інтерфейси, диски тощо.

Додаємо налаштування для моніторингу мережі - доступ до таблиці мережевих інтерфейсів:

```
view    all    included   .1
```

all — дає доступ до всього дерева OID (від кореня .1), що дозволить зібрати дані про трафік, стан інтерфейсів, швидкість тощо.

Додаємо налаштування для моніторингу дискових ресурсів:

```
disk       /     10%
disk       /var  10%
```

/ — коренева файлова система, 10% — мінімально доступний простір у відсотках (тривога, якщо менше 10%).

Для моніторингу критичних процесів додаємо:

```
proc  sshd
proc  snmpd
```

sshd, snmpd — приклади процесів, які потрібно перевіряти, якщо ці процеси не працюватимуть, буде сповіщення.

Додаємо налаштування для моніторингу використання пам’яті:

```
load   12 10 5
```

Значення: середнє завантаження CPU за 1, 5 та 15 хвилин. Якщо значення перевищує пороги, буде сповіщення.

Для захисту SNMP-сервера обмежуємо доступ тільки до певних IP-адрес (наприклад, сервера моніторингу):

```
agentAddress udp:161
acl my_networks 192.168.40.128/27
rocommunity public  my_networks
```

192.168.40.128/27 — підмережа, якій дозволено доступ.

Зберігаємо внесені зміни конфігурації, перезапускаємо службу SNMP та перевіряємо роботу snmpwalk

sudo systemctl restart snmpd
snmpwalk -v 2c -c public localhost

OID .1.3.6.1.4.1.2021 належить до UCD-SNMP-MIB, яка надає розширену інформацію про системні ресурси, включаючи використання пам'яті, CPU, файлових систем і процесів. У додатку 2 наведено приклади командних рядків snmpwalk для окремих перевірок з використанням OID .1.3.6.1.4.1.2021.

Для моніторингу мережевих інтерфейсів через SNMP використовується IF-MIB. Основний OID для цієї MIB — .1.3.6.1.2.1.2, що містить інформацію про всі інтерфейси. У додатку 3 цього документу наведено основні об'єкти IF-MIB для мережевих інтерфейсів.

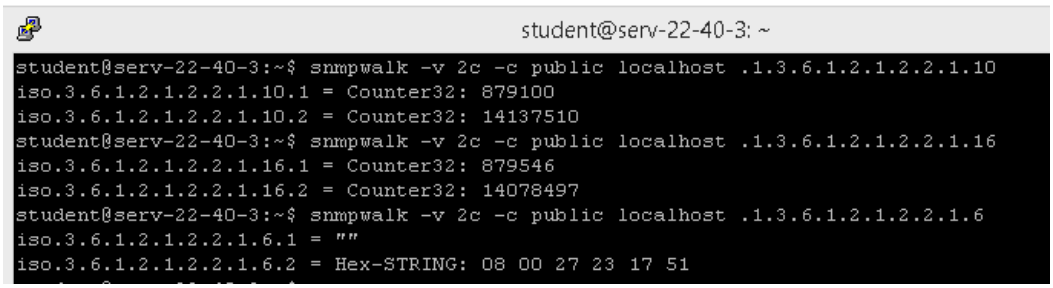

Рис. 14.3. SNMP-статистика на інтерфейсах Serv-22-40-3
.1.3.6.1.2.1.2.2.1.10 # прийняті байти,
.1.3.6.1.2.1.2.2.1.16 # передані байти,
.1.3.6.1.2.1.2.2.1.6 #MAC-адреси.

<u>Перевірка працездатності агентів моніторингу на сервері Serv-G-N-3</u>

Крім налаштованого SNMP на сервері повинні працювати агенти ncpa та nrpe, призначені для обміну інформацією з Ngios Core.Перевіряємо їх статус:

sudo service ncpa status
sudo service nrpe status

Якщо якийсь з сервісів не працює, відновлюємо його працездатність за алгоритмом, викладеним у додатку 1 цього документу.

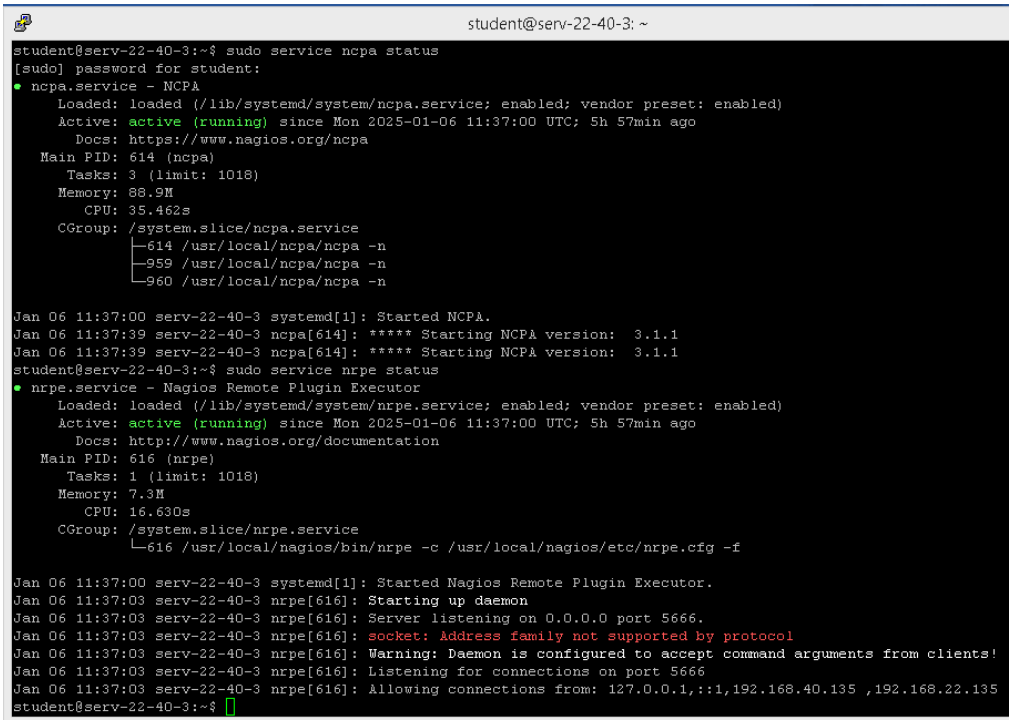

Рис. 14.4. Перевірка стану ncpa та nrpe на сервері Serv-40-22-3

На рис.14.4 «червоний» рядок

socket: Address family not supported by protocol

показує відсутність підтримки IPv6 на мережевих інтерфейсах.

Перевіряємо стан Zabbix Agent2 на цьому ж хості:

sudo systemctl status zabbix-agent2

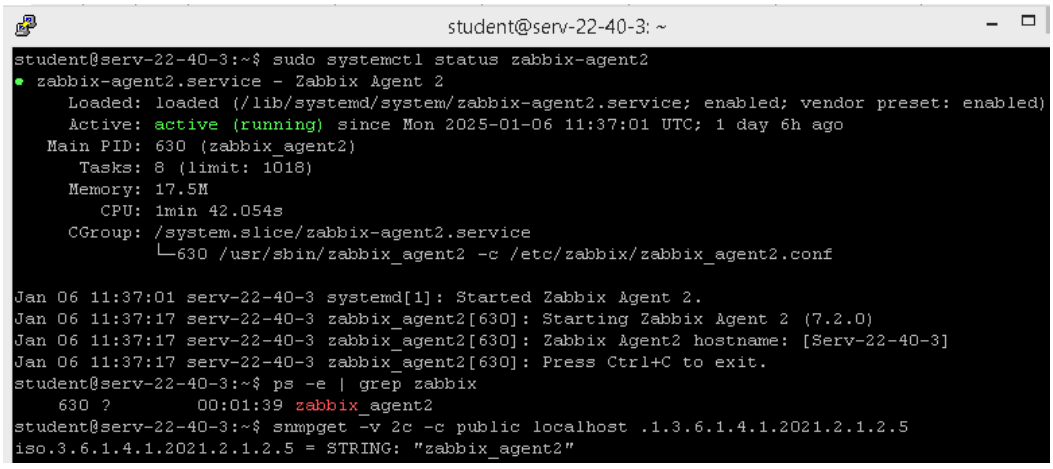

Рис. 14.5. Перевірка стану Zabbix Agent2 на сервері Serv-40-22-3

Ім’я процесу Zabbix Agent2 для додавання до систем моніторингу перевіряємо командою

ps -e | grep zabbix

Всі прямі перевірки працездатності сервісів на сервері Serv-40-22-3 виконано.

Зверніть увагу, що одним з завдань даної лабораторної роботи є налаштування SNMP-моніторингу працездатності даних сервісів. У прикладі ми виконали тільки пряму перевірку працездатності агентів моніторингу.

Завдання до лабораторної роботи

1. Встановіть та налаштуйте на сервері Ubuntu (Serv-G-N-3) SNMP-сервер на базі snmpd. Забезпечте службі snmpd доступ до всіх об'єктів MIB.
2. Перевірте працездатність раніше встановлених та налаштованих на сервері Serv-G-N-3 агентів моніторингу ncpa, nrpe, Zabbix Agent2
3. Змініть налаштування snmpd таким чином, щоб можна було додатково відслідковувати стан наступних процесів агентів моніторингу встановлених на сервері (ncpa, nrpe, zabbix-agent2).
4. Використовуючи SNMP-інструмент командного рядка snmpwalk, виконайте моніторинг характеристик серверу Serv-G-N-3 за наступними показниками: використання пам'яті, завантаження процесора, інформація про мережеві інтерфейси, статистика дисків, стан обраних процесів. Інтерпретуйте результати виконання кожної команди. Зробіть висновки щодо стану системи на основі отриманих метрик.

Звіт має містити:

- лістинг використаних команд;
- короткий опис редагування файлів конфігурації;
- скріншоти налаштувань та підключень;
- для кожної snmpwalk-команди наведіть:
    - використаний OID і його опис,
    - отриманий результат,
    - інтерпретацію значень,
- додайте загальний висновок щодо стану системи.

Корисні посилання

- How To Install and Configure an SNMP Daemon and Client on Ubuntu.

http://surl.li/uejoxx

- Linux snmpwalk: An Overview of SNMP and the snmpwalk Utility.

http://surl.li/hobszl

- Nagios. SNMP Monitoring.

http://surl.li/ypfjoe

Додаток 1.

Виправлення помилки з запуском клієнта Nagios на Ubuntu.

Виправлення помилки з роботою ncpa. Перевіряємо статус служби клієнта.

sudo service ncpa status

Вимикаємо автозапуск служби NCPA, щоб вона не запускалася під час перезавантаження системи.

sudo systemctl disable ncpa

sudo reboot

sudo service ncpa status

Змінюємо права доступу до файлу процесу ncpa.pid, щоб дозволити його видалення та видаляємо.

sudo chmod 777 /usr/local/ncpa/var/run/ncpa.pid

sudo rm /usr/local/ncpa/var/run/ncpa.pid

Перезапускаємо службу та відновлюємо її автозапуск.

sudo service ncpa restart

sudo systemctl enable ncpa

Це універсальний алгоритм відновлення та працює також з nrpe. Файл процесу nrpe-клієнта знаходиться по шляху /usr/local/nagios/var/nrpe.pid

Додаток 2.

Приклади командних рядків snmpwalk для окремих перевірок.

Таблиця 14.1.

snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021	Моніторинг ресурсів системи, включаючи використання пам'яті, CPU, файлових систем і процесів.
Приклади для перевірки дисків	
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.9	Перевірка дисків.
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.9.1.2	Ім'я файлової системи.
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.9.1.3	Тип файлової системи.
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.9.1.6	Загальний обсяг диску (KB).
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.9.1.7	Обсяг використаного місця (KB).
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.9.1.8	Вільний обсяг диску (KB).
Приклади для перевірки процесів	
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.2	Перевірка процесів
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.2.1.2	Перевірка процесу 1. Назва процесу.
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.2.1.5	Перевірка процесу 1. Статус процесу.
Приклади для перевірки завантаження CPU	
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.10	Перевірка завантаження CPU.
snmpwalk -v 2c -c public localhost.1.3.6.1.4.1.2021.10.1.3.1	Перевірка завантаження CPU за 1 хв
snmpwalk -v 2c -c public localhost.1.3.6.1.4.1.2021.10.1.3.2	Перевірка завантаження CPU за 5 хв
snmpwalk -v 2c -c public localhost.1.3.6.1.4.1.2021.10.1.3.3	Перевірка завантаження CPU за 15 хв
Приклади для перевірки використання пам’яті	
snmpwalk -v 2c -c public localhost.1.3.6.1.4.1.2021.4	Інформація про використання пам'яті (KB)
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.3	Сумарна фізична пам'ять (Total Swap Memory).
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.4	Сумарна RAM пам'ять.
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.5	Вільна фізична пам'ять (Free Swap Memory).
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.6	Вільна RAM пам'ять (Free RAM).
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.13	Сумарна буферна пам'ять (Buffer Memory).
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.14	Сумарна пам'ять у кеші (Cached Memory).
snmpwalk -v 2c -c public localhost .1.3.6.1.4.1.2021.4.15	Сумарна доступна пам'ять (Shared Memory).
snmpwalk -v 2c -c public localhost.1.3.6.1.4.1.2021.4.5.0	Загальний обсяг пам'яті (memTotalReal) (KB).
snmpwalk -v 2c -c public localhost.1.3.6.1.4.1.2021.4.6.0	Вільна пам'ять (memAvailReal) (KB).
snmpwalk -v 2c -c public localhost.1.3.6.1.4.1.2021.4.11.0	Використана пам'ять (memTotalReal - memAvailReal) (KB).
snmpwalk -v 2c -c public localhost.1.3.6.1.4.1.2021.4.3.0	Загальний розмір swap (KB).
snmpwalk -v 2c -c public localhost.1.3.6.1.4.1.2021.4.4.0	Вільний swap (KB).

Додаток 3.

Основні об'єкти IF-MIB для інтерфейсів.

Таблиця 14.2.

OID	Назва	Опис
.1.3.6.1.2.1.2.1.0	ifNumber	Кількість інтерфейсів у системі.
.1.3.6.1.2.1.2.2.1.1	ifIndex	Індекс інтерфейсу (унікальний для кожного).
.1.3.6.1.2.1.2.2.1.2	ifDescr	Опис інтерфейсу (наприклад, eth0, lo).
.1.3.6.1.2.1.2.2.1.3	ifType	Тип інтерфейсу (Ethernet, Loopback, etc.).
.1.3.6.1.2.1.2.2.1.4	ifMTU	Розмір MTU інтерфейсу.
.1.3.6.1.2.1.2.2.1.5	ifSpeed	Швидкість інтерфейсу (в бітах/сек).
.1.3.6.1.2.1.2.2.1.6	ifPhysAddress	MAC-адреса інтерфейсу.
.1.3.6.1.2.1.2.2.1.7	ifAdminStatus	Адміністративний статус (включений/виключений).
.1.3.6.1.2.1.2.2.1.8	ifOperStatus	Оперативний статус (активний/неактивний).
.1.3.6.1.2.1.2.2.1.9	ifLastChange	Час останньої зміни стану інтерфейсу.
.1.3.6.1.2.1.2.2.1.10	ifInOctets	Прийняті байти на інтерфейсі.
.1.3.6.1.2.1.2.2.1.11	ifInUcastPkts	Кількість прийнятих одноадресних пакетів.
.1.3.6.1.2.1.2.2.1.12	ifInNUcastPkts	Кількість прийнятих багатоадресних або широкомовних пакетів.
.1.3.6.1.2.1.2.2.1.13	ifInDiscards	Кількість відкинутих вхідних пакетів.
.1.3.6.1.2.1.2.2.1.14	ifInErrors	Кількість помилок у вхідних пакетах.
.1.3.6.1.2.1.2.2.1.15	ifInUnknownProtos	Кількість пакетів із невідомими протоколами.
.1.3.6.1.2.1.2.2.1.16	ifOutOctets	Передані байти на інтерфейсі.
.1.3.6.1.2.1.2.2.1.17	ifOutUcastPkts	Кількість переданих одноадресних пакетів.
.1.3.6.1.2.1.2.2.1.18	ifOutNUcastPkts	Кількість переданих багатоадресних або широкомовних пакетів.
.1.3.6.1.2.1.2.2.1.19	ifOutDiscards	Кількість відкинутих вихідних пакетів.
.1.3.6.1.2.1.2.2.1.20	ifOutErrors	Кількість помилок у вихідних пакетах.
.1.3.6.1.2.1.2.2.1.21	ifOutQLen	Довжина черги вихідних пакетів (у пакетах).
.1.3.6.1.2.1.31.1.1.1.1	ifName	Повна назва інтерфейсу (часто більш детальна, ніж ifDescr).
.1.3.6.1.2.1.31.1.1.1.15	ifHighSpeed	Швидкість інтерфейсу у Мбіт/сек (підтримує великі значення).
.1.3.6.1.2.1.31.1.1.1.18	ifAlias	Опис інтерфейсу (може бути визначений адміністратором).
.1.3.6.1.2.1.31.1.1.1.6	ifHCInOctets	Прийняті байти (64-бітовий лічильник для великих значень).
.1.3.6.1.2.1.31.1.1.1.10	ifHCOutOctets	Передані байти (64-бітовий лічильник для великих значень).