Міністерство освіти і науки, молоді та спорту України

Тернопільський національний педагогічний університет

імені Володимира Гнатюка

Кафедра інформатики та

методики її викладання

Моніторинг мережного трафіку засобами протоколу SNMP ОС Linux

Виконав:

Студент фізико-

математичного факультету

Групи І-24

Федірко Сергій

Науковий керівник:

Олексюк Василь Петрович

Тернопіль – 2013

Зміст

Вступ

Дана робота присвячена протоколу SNMP (SimpleNetworkManagementProtocol) - одному з протоколів моделі OSI,який ми не вивчали на курсі «Комп'ютерні мережі». Я спробую заповнити цей вакуум, надавши вамгрунт для роздумів і самовдосконалення, щодо цього питання. Цяробота висвітлює аспекти роботи з даним протоколом, показує його слабкі місця, уразливості в системі "security", вказує які цілі переслідували творціта пояснює його призначення. Також дослідивши цю роботу ви зможете одержати уміння та навички роботи з моніторингу вузлів мережі, серверів і активного мережевого обладнання засобами SNMP.

Для успішного адміністрування мережі необхідно знати стан кожного її елемента з можливістю змінювати параметри його функціонування. Зазвичай мережа складається з пристроїв різних виробників, і управляти нею було б нелегким завданням, якби кожен з мережевих пристроїв розумів тільки свою систему команд. Тому виникла необхідність у створенні єдиної мови управління мережевими ресурсами, яку б розуміли всі пристрої, і яка в силу цього, використовувалася усіма пакетами управління мережею для взаємодії з конкретними пристроями.Подібною мовою стала SNMP – SimpleNetworkManagementProtocol.

SNMP виконує такі функції:

- відправлення та прийом пакетів SNMP через протокол IP;
- збір інформації про статус і поточну конфігурацію мережевих пристроїв;
- зміна конфігурації мережевих пристроїв.

Призначення

Протокол SNMP був розроблений з метою перевірки функціонування мережевих маршрутизаторів і мостів. Згодом сфера дії протоколу охопила і інші мережеві пристрої, такі як хаби, шлюзи,термінальні сервера, LAN Manager сервера, машини під управліннямиWindows NT і т.д. Крім того, протокол допускає можливість внесення змін у функціонування зазначених пристроїв.Розроблена для систем, орієнтованих під операційну систему UNIX, вона стала фактично загальноприйнятим стандартом мережевих систем управління та підтримується переважною більшістю виробників мережевого устаткування в своїх продуктах. В силу своєї назви – Простий Протокол Мережевого Управління – основним завданням при його розробці було домогтися максимальної простоти реалізації. У результаті виник протокол, що включає мінімальний набір команд, проте дозволяє виконувати практично весь спектр завдань управління мережевими пристроями – від отримання інформації про місцезнаходження конкретного пристрою до можливості виконувати його тестування.

Протокол SNMP

ПротоколSNMP створений в 1988 р. з метою управління великою кількістю мережевих пристроїв. З того моменту протокол набрав відповідну популярність і став стандартом. З моменту розробки протокол SNMP був 3 рази перероблений з версії SNMPv1, SNMPv2 і SNMPv3. Насправді, версій було більше, наприклад v2 була переглянута 2 рази (або навіть більше). Так само варто відзначити, що крім SNMP були й інші спроби створити комерційні і не комерційні протоколи управління (CORBA, TMN...) не увінчалися успіхом.

Крім управління пристроями, завжди SNMP використовують для моніторингу. SNMP може отримувати різну інформацію від будь-яких мережевих пристроїв, будь то роутер, свіч або просто комп'ютер (в яких є підтримка даного протоколу. Вміст одержуваної інформації може бути дуже різноманітно, наприклад : час аптайм, різні лічильники продуктивності CPU, мережі та ін, мережеві параметри пристроїв...

Архітектура протоколу SNMP

Мережа, що використовує SNMP для управління містить три основні компоненти:

- **SNMP менеджер** - ПЗ, яке встановлюється на ПК адміністратора (системи моніторингу)
- **SNMP агент** - ПО, запущене на мережевому вузлі, за якими здійснюється моніторинг.
- **SNMP MIB** - MIB це Managementinformationbase. Цей компонент системи забезпечує структурованість даних, якими обмінюються агенти та менеджери. По суті - це якась база даних у вигляді текстових фалів.

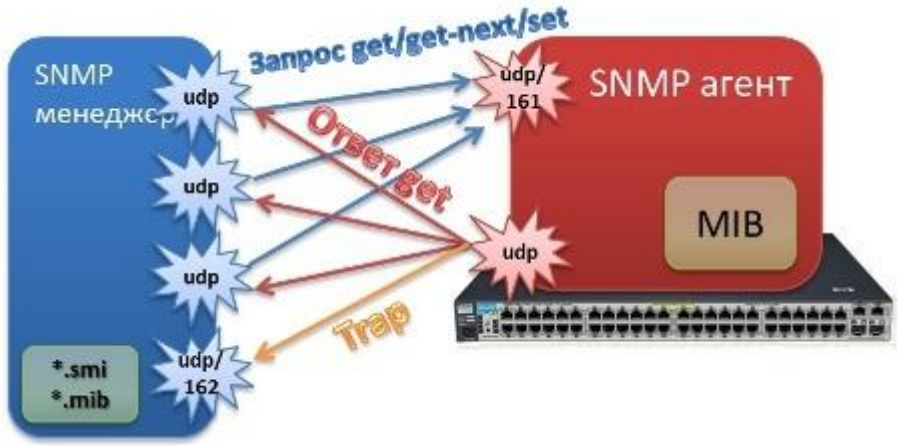
Для розуміння призначення компонентів, можна сказати, що SNMP менеджер є прошарком (інтерфейсом) між оператором \ адміністратором і мережевим вузлом із запущеним SNMP агентом. Так само, можна сказати,

що SNMP агент - це інтерфейс між SNMP менеджером і залізним обладнанням на мережевому вузлі. Якщо провести аналогію протоколу SNMP з клієнт-серверної архітектурою (наприклад, веб-сервера) то веб-сервер працює як служба на деякій порту, а користувач силами браузера звертається до веб-сервера як клієнт. Це чітко позначена архітектура з вираженим клієнтом і сервером. У разі SNMP ролі клієнта і сервера дещо розмиті. Наприклад, SNMP агент є свого роду службою, яка працює на пристрої (за яким проводиться моніторинг) і обробляє запити на певному портіudp/161, тобто фактично є сервером. А SNMP менеджер є свого роду клієнтом, який звертається до сервера SNMP агенту. У SNMP існує так званийTrap. Це запит від агента до менеджера. Точніше навіть не запит, а повідомлення. При відправці даного повідомлення, агент і менеджер "міняються ролями". Тобто, менеджер в такому випадку повинен бути сервером, працюючому на портіudp/162, а агент є клієнтом. В останніх версіях SNMP trap може називатися як сповіщення (notification).

SNMP працює на 7 рівні моделі OSI, тобто є службою прикладного рівня. Взаємодія агента і менеджера на рівні протоколу SNMP організовується за допомогою т.зв. пакетів об'єктів PDU (ProtocolDataUnit), які інкапсуліруются в транспортний протокол. Хоча, SNMP підтримує різні види транспорту, в 99% випадків використовується - UDP. При цьому, кожне повідомлення PDU містить певну команду (на читання змінної, запис значення змінної, або відповідь \trap агента). У цілому, взаємодію вузлів по SNMP можна представити в наступній послідовністю: менеджер -> SNMP (PDU) - UDP -IP - Ethernet -IP - UDP - SNMP (PDU) -> агент. При використанні шифрування в SNMP, за замовчуванням використовуються порт для запитів \ відповідей udp/10161, а Trap відправляються на udp/10162. Агенти, що працюють на хостах, збирають інформацію про пристрої і записують зібрані лічильники в значення змінних в базу даних MIB. Тим самим роблячи її доступною для менеджерів.

Давайте розглянемо схему взаємодії SNMP-агент - SNMP-менеджер:

Схема 1



SNMP менеджер відправляє запити агенту на порт udp/161 з довільного порту з ефемерного діапазону. У запиті SNMP менеджера вказується порт і адресу джерела. Далі агент приймає пакет і обробляє. У процесі обробки, формується відповідь, який відправляється на порт взятий з вихідного запиту. Відповідь відправляється з udp/161 порту. Можна сказати, що SNMP агент таким чином надає доступ SNMP менеджерові до даних, що зберігаються в базі MIB. При цьому, в момент відправки, SNMP менеджер вставляє в PDU якийсь ID (RequestID), а агент у відповідному PDU вставляє даний ID без зміни, для того щоб менеджер не плутав пакети від різних агентів. SNMP агент може бути налаштований на посилку Trap повідомлень, яку він виконує з ефімерного порту на udp/162 порт SNMP менеджера.

Логіка роботи протоколу SNMP

Розглянувши основні одиниці обміну SNMP, можна обговорити логіку роботи SNMP при виконанні даних запитів \ відповідей. Деякі загальні особливості роботи протоколу SNMP, які варто враховувати:

- Приймаюча сторона першою справою намагається декодувати повідомлення. Якщо приймаючої сторони не вдається розкодувати PDU, то пакет відкидається без будь-яких дій.
- Якщо версія SNMP в пакеті, що прийшов не відповідає версії сервера, то пакет так само Дропана.
- Після цього, звіряється аутентифікаційна інформація (або значення

рядка community, або інформація користувача). Можуть застосовуватися зовнішні модулі для аутентифікації.

- Далі, відбувається обробка повідомлення. Якщо необхідно - генерується відповідь.

MIB

Керуюча інформація та параметри комутатора зберігаються в інформаційній базі управління (ManagementInformationBase – MIB). MIB є набором змінних, що характеризують стан об'єкта управління. Ці змінні можуть відображати такі параметри, як кількість пакетів, оброблених пристроєм, стан його інтерфейсів, час функціонування пристрою і т.п. Кожен виробник мережевого устаткування, крім стандартних змінних, включає в MIB ряд параметрів, специфічних для даного пристрою. Однак при цьому не порушується принцип представлення та доступу до адміністративної інформації – всі вони будуть змінними в MIB. Тому SNMP як безпосередньо мережевий протокол надає тільки набір команд для роботи зі змінними MIB. Цей набір включає наступні операції:

Таблиця 1

get-request	Використовується для запиту одного чи більше параметрів MIB
get-next-request	Використовується для послідовного читання значень. Зазвичай використовується для читання значень із таблиць.
set-request	Використовується для встановлення значення однієї або більше змінних MIB
get-response	Повертає відповідь на запит get-request, get-next-request або set-request
trap	Повідомлення про події типу cold або warmrestart або "падіння" деякого link'у.

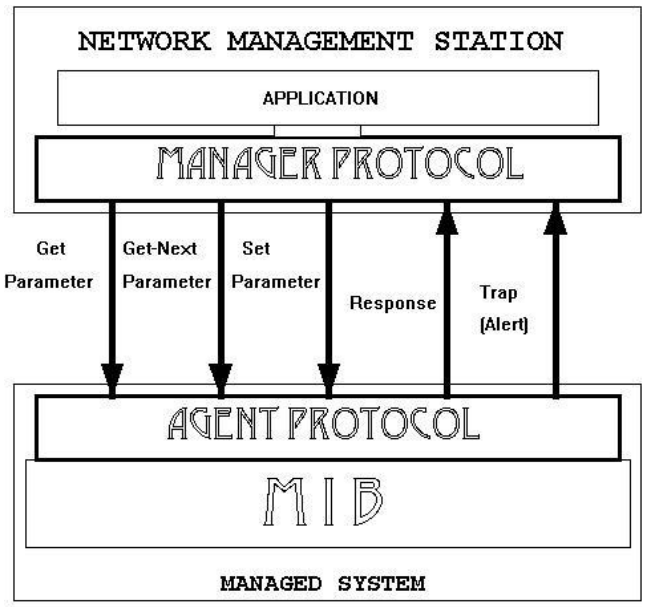
Для того, щоб проконтролювати роботу деякого пристрою мережі, необхідно просто отримати доступ до його MIB, яка постійно оновлюється

самим пристроєм, і проаналізувати значення деяких змінних.

Комутатор використовує стандартний модуль інформаційної бази управління MIB-II. Отже, значення, які входять до MIB-об'єктів можуть бути отримані за допомогою будь-яких засобів мережного управління, що базуються на SNMP. Крім стандарту MIB-II, комутатор також підтримує власну MIB у вигляді розширеної інформаційної бази управління. Об'єкти цієї MIB також можуть бути отримані шляхом зазначення менеджером OID MIB (ObjectIdentifier, ідентифікатор об'єкту MIB). Значення об'єктів MIB можуть бути як відкритими тільки для читання (read-only), так і для читання і для запису (read-write). Об'єктиread-only MIB можуть бути константами, якізапрограмовані в комутаторі, абозмінними, якізмінюються в процесіроботикомутатора. Прикладами констант read-only є кількістьпортів та їхтипи. Прикладами змінних read-only є статистичнізначення, такі як кількістьдопущенихпомилок, абоскільки Кбайт данихбулоотримано й передано через порт. Об'єктиread-write MIB зазвичайпов'язані з налаштуваннями, здійснюваними користувачем.

Як відбувається адресація в MIB до деякоїїїзмінної? За своєю структурою MIB являє собою дерево, зображене на рис. 1.

Рис. 1



Кожному елементу відповідає числовий і символьнийідентифікатор. В ім'язмінноївключаєтьсяповний шлях до неївідкореневогоелементуroot. Наприклад, час роботи пристрою з моменту перезавантаженнязберігається в змінній, щознаходиться в розділіsystemпід номером 3 і називаєтьсяsysUpTime. Відповідно, ім'язмінної буде включати весь шлях: iso (1). Org (3). Dod (6). Internet (1). Mgmt (2). Mib-

2 (1). System (1). SysUpTime (3) ;або на мові чисел: 1.3.6.1.2.1.1.3. Слідзауважити, що при цьомувузли дерева розділяютьсякрапками. Існує стандартна гілку MIB, щовідноситься до розділууправліннямgmt, яку зазвичайпідтримуютьвсімережевіпристрої. Поряд з цимкоженвиробникабоорганізаціяможерозробитисвійвласнийнабірзмінних і "підвішати" їх до дерева MIB. Однак, церобитьсятільки в суворовизначеномуїїмісці. Якщоорганізаціярозробляє свою базу MIB, то настадіїекспериментівзмінніможутьпоміщатися в розділехperimental. Однак для
офіційноїреєстраціїструктуриданихдеякоїорганізаціїїйнеобхіднотриматривласний номер в розділіprivate-enterprises. Всізмінні, адресовані вниз по гілціданоїорганізації, відносяться до продуктів тільки даного виробника.

Установка и настройка SNMP

Для роботи із протоколом SNMP потрібно для початку встановити цей протокол і його демона (агента). Оскільки тема стосується Linux, то розглянемо команди для даної операційної системи. Розглянемо установку по кроках. Але перед тим як приступити до роботи нам потрібно отримати права root. Для цього, вводимо відому для нас, команду:

```
sudo –s(цю команду потрібно буде підтвердити паролем).
```

Після того як ми отримали root-достум приступимо до роботи.

1) Ставимо пакет SNMP. Для цього ми використовуємо команди:

```
apt-get install snmpsnmpd

snmpconf –g basic-setup
```

Після успішної інсталяції програмного забезпечення з’явилась доступність до програм:

```
snmpget

snmpset

snmpgetnext

snmpwalk

snmpbulkwalk

snmpcheck

snmptest

snmpdelta

snmpnetstat

snmpstatus

snmptable

snmptrap

snmptranstat

і демон snmptrapd
```

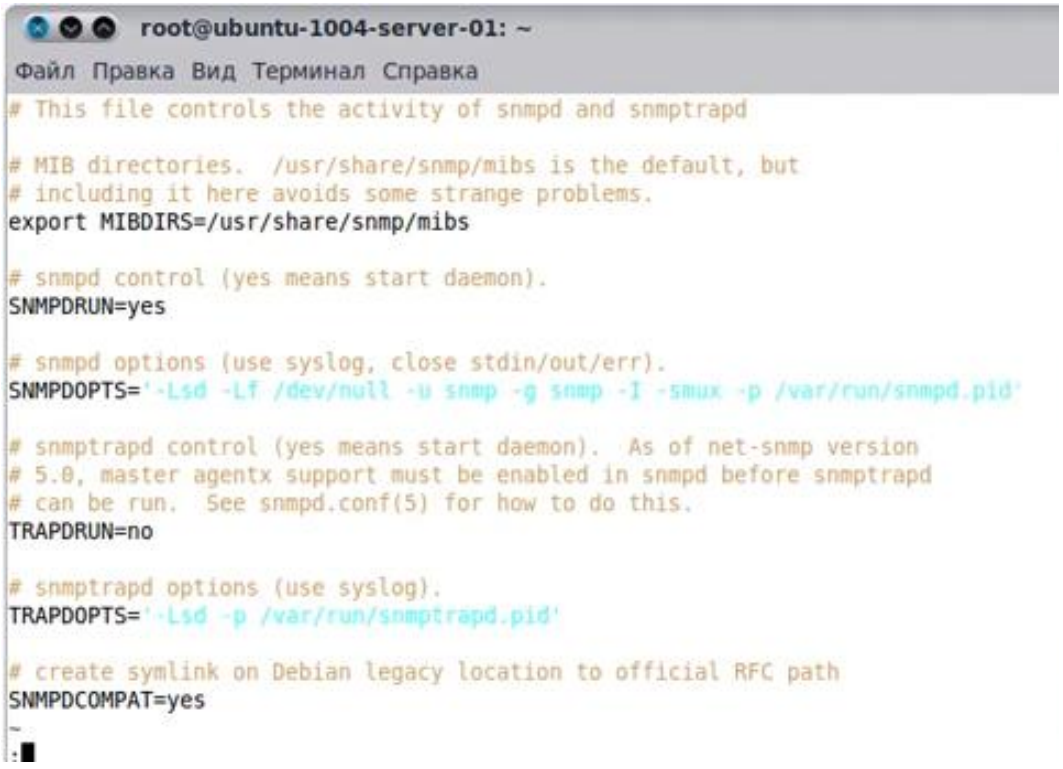
2) Перше, щопотрібно -переконатися в тому, щоSNMPDтількизбираєтьсячекатиз'єднання на локальний хост.Дляцього, редагуємофайл***/etc/default/SNMPD***. Зазамовченнямдемон SNMPD слухаєзверненнятільки з localhost: 127.0.0.1. Для того щоб слухав усі напрями змінюємо рядок

```
SNMPDRUN=yes

SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid 127.0.0.1'
```

до такого вигляду:

```
SNMPDRUN=yes

SNMPDOPTS='-Lsd -Lf /dev/null -p /var/run/snmpd.pid'
```

Рис. 2



3) Після установки пакету нам потрібно встановити конфігурацію для SNMPD. Для цього нам потрібно редагувати файл **«*snmpd.conf*»,** який знаходиться в ***/etc/snmp***. Це можна реалізувати двома способами:

- Можна ввести вручну, використовуючи команду:

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

На екран виведе вікно для форматування даного тексту.

o Також можна через графічний редактор, використовуючи команду ***«mc»***. Дальше переходимо по вказаному адресу і знаходимо даний файл і нажимаємо ***«F4»*** для редагування файлу.

Редагуємо даний файл до наступного вигляду:

```
syslocation Belle-notebook

syscontactAdminstrator
```

4) Перезапустимо SNMPD.

```
/etc/init.d/snmpdrestart
```

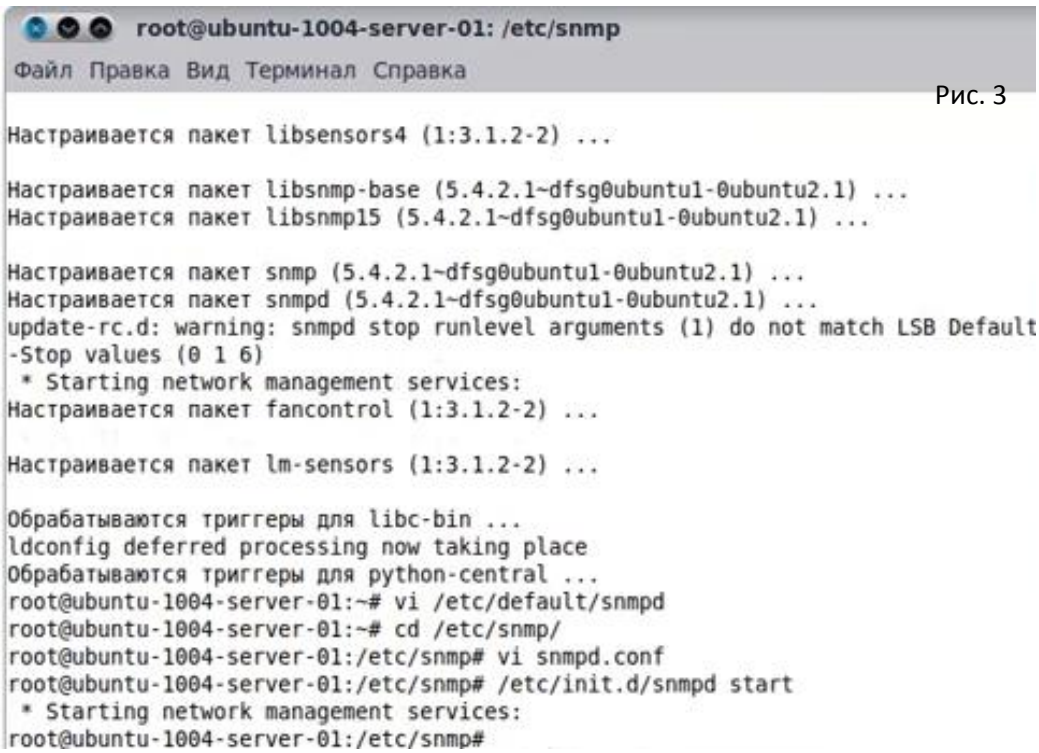


Рис. 3

5) Перевіримо роботу SNMPD сервера.

Якщо ми усе правильно зробили, то першим рядком у нас буде щось подібне до наступного рядка:

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux bt 3.2.6 #1 SMP Fri Feb 17 10:34:20 EST 2012
x86_64
```

Якщо дана команда викине рядок

```
Timeout: No Response from localhost
```

значить не правильно прокоментували файл.

6) Ми налаштували протокол SNMP. Дальше ми можемо приступати до системи моніторингу ***cacti,*** який працює на протоколі SNMP.

Висновок

На підставі вищевикладеного залишається зробити висновок про те, що адміністратор мережі може знайти в особі протоколу SNMP гарного помічника, маючи повний доступ до описів змінних MIB різних мережних пристроїв і потужний пакет, який би полегшував роботу з громіздкими іменами змінних в SNMP.

Отже, у статті я постарався якомога зрозуміліше розповісти про SNMP, щоб застосовувати цю технологію в мережах моніторингу. Підводячи короткий підсумок протокол SNMP базується на кількох основних принципах:

- Менеджер звертається до агента, запитуючи інформацію, яка характеризує стан пристрою, на якому працює агент.
- Менеджер може вказати агенту виконати зміну конфігурації віддаленого хоста, задавши значення змінної.
- Агент може сам повідомляти менеджеру про подію важливу подію.
- Вся інформація про вузол зберігатися в структурі дерева бази MIB.

Список використанихджерел

1) Установка и настройка SNMP протокола на LinuxDebian / Ubuntu / BackTrack.:[Електронний ресурс]. – Режим доступу до документа: http://alex-zone.nnover.ru/lin/6443984.html
2) Установка и нстройка SNMP на LinuxDebian/Ubuntu.:[Електронний ресурс]. – Режим доступу до документа: http://mannix.ru/prilozhenia/ustanovka-i-nastrojka-snmp-na-linux-debianubuntu.html
3) SNMP протокол - принципы, безопасность, применение.:[Електронний ресурс]. – Режим доступу до документа:http://www.opennet.ru/base/net/snmp_art.txt.html
4) SNMP протокол (основы).:[Електронний ресурс]. – Режим доступу до документа: http://www.k-max.name/linux/snmp-protocol/