



---

---

## Monitoring Sistem Jaringan Dengan Protokol SNMP

### 1. SNMP ( Simple Network Management Protocol)

SNMP adalah sebuah protokol yang dirancang untuk memberikan kemampuan kepada pengguna untuk memantau dan mengatur jaringan komputernya secara sistematis dari jarak jauh atau dalam satu pusat kontrol saja. Pengolahan ini dijalankan dengan mengumpulkan data dan melakukan penetapan terhadap variabel-variabel dalam elemen jaringan yang dikelola.

### 2. Komponen utama dalam proses manajemen jaringan TCP/IP terdiri dari tiga elemen, yaitu:

#### 1. MIB (Management Information Database)

MIB Adalah struktur basis data variabel dari elemen jaringan yang dikelola. Pada kelompok interface terdapat variabel objek MIB yang mendefinisikan karakteristik interface diantaranya : *ifInOctets* mendefinisikan jumlah total byte yang diterima, *ifOutOctets* mendefinisikan jumlah total byte yang dikirim, *ifInErrors* mendefinisikan jumlah paket diterima yang dibuang karena rusak, *ifOutErrors* mendefinisikan jumlah paket dikirim yang dibuang karena usak, dan variable objek lainnya yang juga berkaitan dengan paket internet.

#### 2. Agen

Merupakan software yang dijalankan di setiap elemen jaringan yang dimonitor. Agen bertugas mengumpulkan seluruh informasi yang telah ditentukan dalam MIB.

#### 3. Manajer

Merupakan software yang berjalan di sebuah host di jaringan. Bertugas meminta informasi ke SNMP Agen. Manajer biasanya tidak meminta semua informasi yang dimiliki oleh agen, tetapi hanya meminta informasi tertentu saja yang akan digunakan untuk mengamati unjuk kerja jaringan. Manager biasanya menggunakan komputer yang memiliki tampilan grafis dan berwarna sehingga selain dapat menjalankan fungsinya sebagai Manager, juga untuk melihat grafik unjuk kerja dari suatu elemen jaringan yang dihasilkan oleh proses monitoring.

SNMP menggunakan UDP (User Datagram Protocol) sebagai protocol transport untuk mengirimkan pertanyaan dan menerima jawaban dari agen SNMP.

**3. SNMP terdiri dari dua jenis yakni:**

- Network Management Station, yang berfungsi sebagai pusat penyimpanan untuk pengumpulan dan analisa dari data manajemen jaringan.
- Peralatan yang dimanage menjalankan SNMP agent, yaitu proses background yang memonitor peralatan tersebut dan mengkomunikasikannya ke network management station.

Peralatan yang memiliki SNMP agent antara lain: CISCO router, Linux Server  
Untuk pencatatan data dapat digunakan aplikasi MRTG (Multi Router Traffic Grapher) ataupun The Dude dari vendor Mikrotik.

**4. PDU SNMPv1**

- *GetRequest*

Adalah jenis PDU yang dikirimkan dari manager kepada agent. PDU ini bertujuan untuk me-request data pada agent.

- *GetNextRequest*

Adalah jenis PDU yang dikirimkan dari manager kepada agent. Operasi ini hampir sama dengan operasi *GetRequest*, hanya saja, *GetNextRequest* ini meminta data setelahnya dari OID yang dispesifikasikan dalam paket *GetNextRequest*.

- *SetRequest*

Adalah jenis PDU yang dikirimkan dari manager kepada agent. PDU ini bertujuan untuk mengubah data pada agent.

- *GetResponse*

Adalah jenis PDU yang dikirimkan dari agent kepada manager. PDU ini bertujuan untuk me-reply data kepada manager sebagai response atas data yang diminta oleh manager melalui operasi *GetRequest*, *GetNextRequest*, dan *SetRequest*.

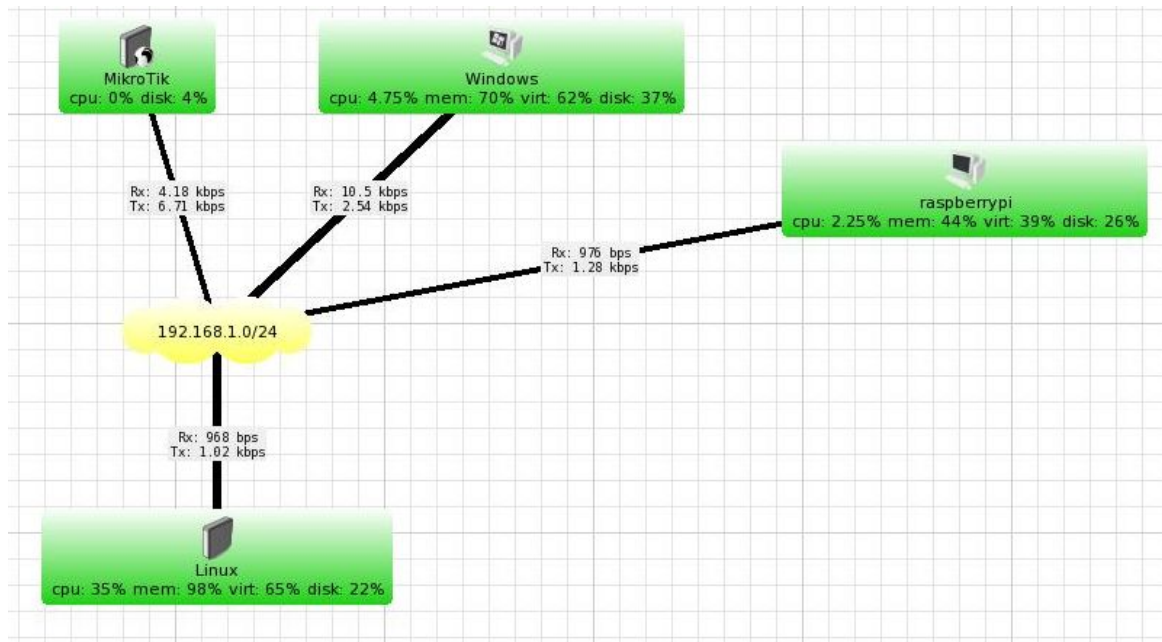
- *Trap*

Adalah jenis PDU yang dikirimkan dari agent kepada manager. SNMP trap ini adalah sebuah pesan yang diprakarsai oleh suatu elemen dalam jaringan (agent) dan dikirimkan kepada manager untuk memberitahu atau memberikan informasi kepada manager bahwa terjadi suatu event tertentu pada objek yang di-manage (managed device).

### 5. Tools Monitoring Jaringan : The Dude

The Dude adalah salah satu tools atau software yang digunakan buat memonitoring network jaringan komputer, yang dalam penggunaannya sangatlah penting bagi yang mempunyai pekerjaan memonitoring jaringan yang cukup besar dan rumit.

### 6. Topologi Percobaan

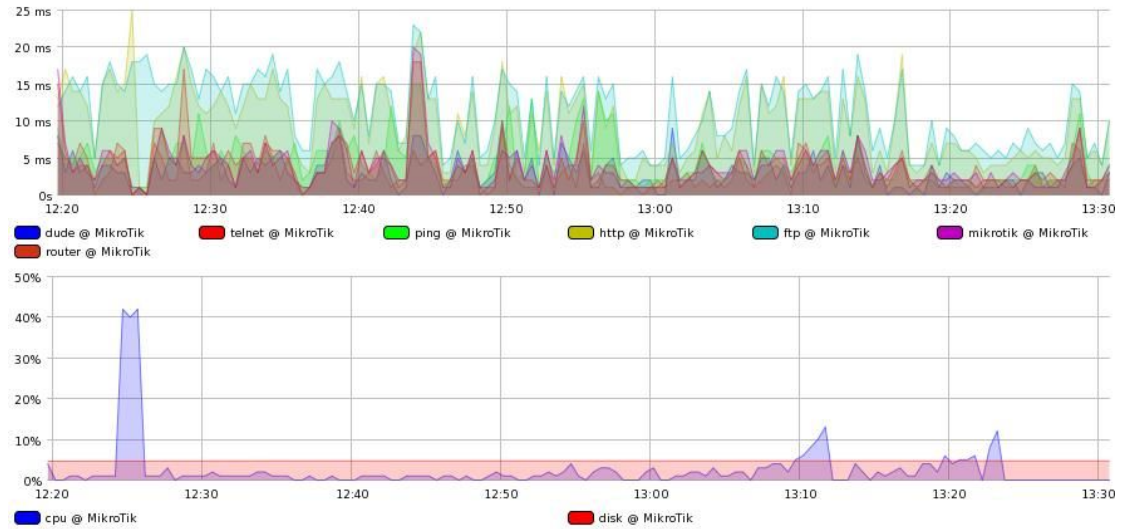


Keterangan Ip Address :

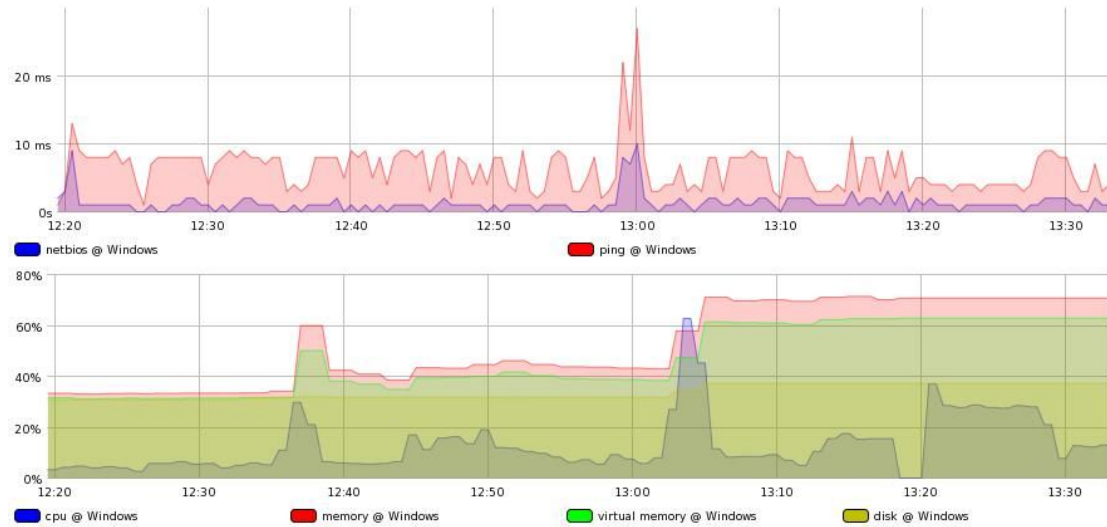
Perangkat	Function	Ip Address
Mikrotik	Manager	192.168.1.1
Windows	Agent	192.168.1.2
Linux	Agent	192.168.1.3
Raspberry	Agent	192.168.1.4

## 7. Traffic Percobaan

### ● Mikrotik

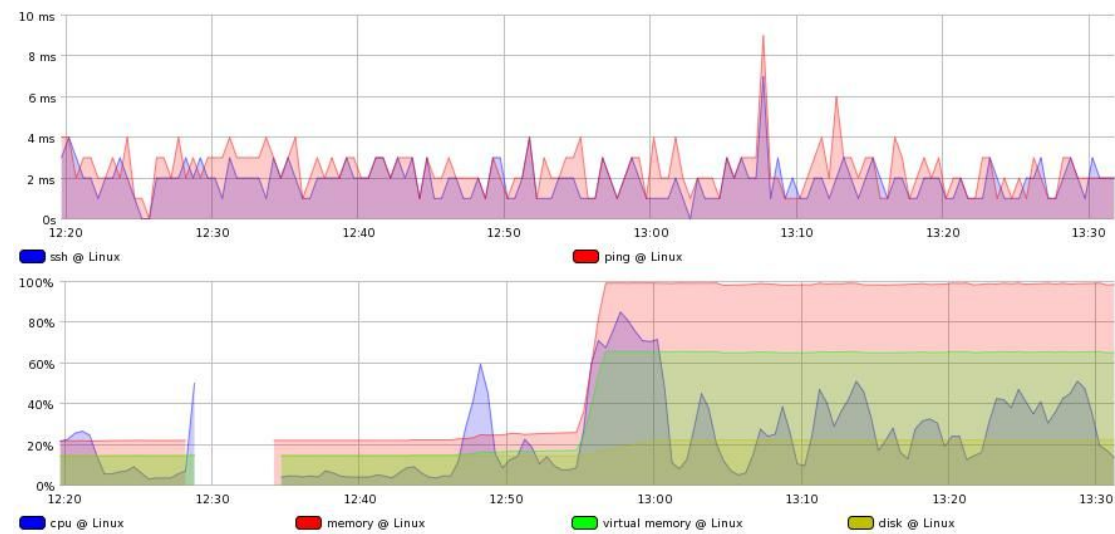


### ● Windows

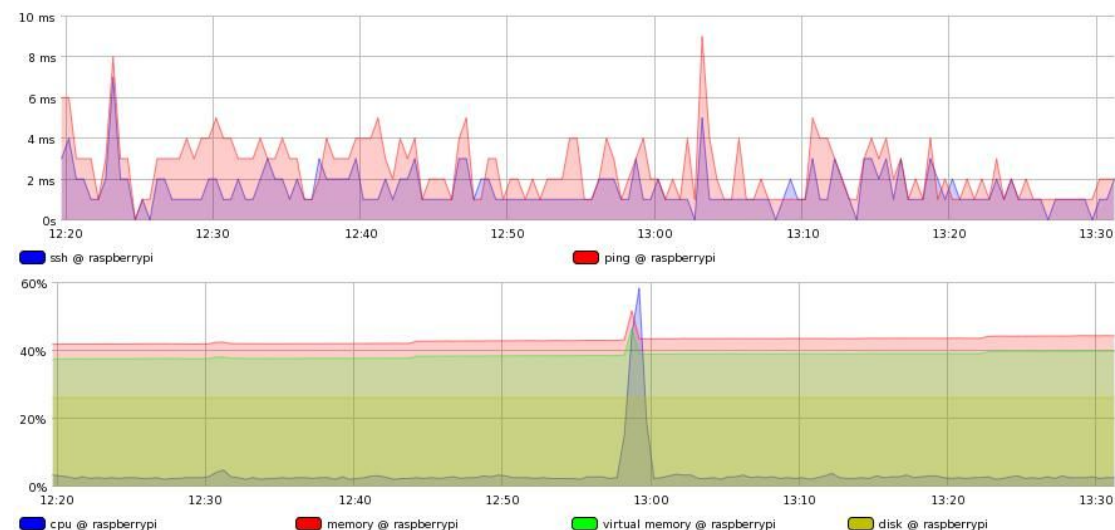


Nama : Johan Wahyudi  
NIM : 09011281320031

## ● Linux



## ● Raspberry Pi



## 8. Struktur MIB ()

- Setiap object mempunyai ID unik (OID).
- MIB mengasosiasikan setiap OID menggunakan label dan parameter lain.
- MIB bertindak sebagai kamus data yang digunakan untuk menyusun terjemahan pesan SNMP.

## **9. Object Identifier (OID)**

- Object Identifier (OID) merupakan sebuah pengenal yang digunakan untuk menamakan sebuah objek yang terdapat dalam MIB.
- OID bersifat unik untuk masing-masing objek.
- Secara struktural, sebuah OID terdiri dari sebuah node dalam namespace yang ditetapkan secara hirarki, yang didefinisikan secara formal menggunakan standar ASN.1.

**Contoh: 1.3.6.1.4.2682.1**  
**(Notasi titik tersebut membentuk hierarki)**

OID dapat didefinisikan dalam dua format, yaitu :

### **1. Textual OID**

Pendefinisian OID berdasarkan nama tiap node mulai dari root, dengan dipisahkan oleh titik (.).

Contoh : .iso.org.dod.internet.mgmt.mib.system.sysDescr

### **2. Numerical OID**

Pendefinisian OID berdasarkan angka integer sebagai pengganti nama, juga dipisahkan dengan titik (.).

Contoh : .1.3.6.1.2.1.1.1

#### **Masalah:**

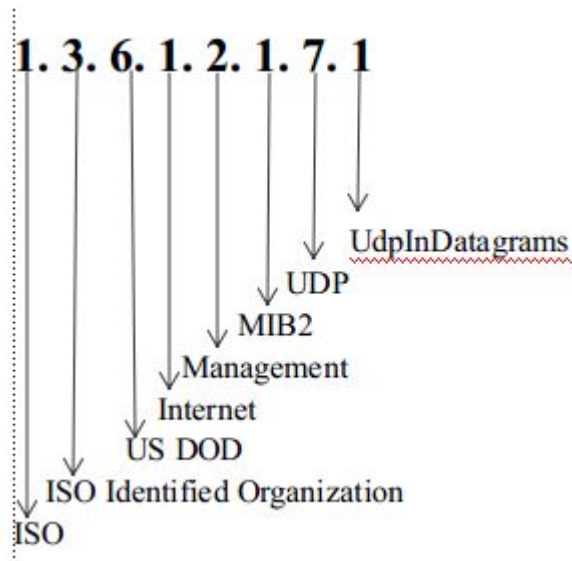
**bagaimana menamai setiap kemungkinan object standard (protocol, data.. dll) dalam setiap kemungkinan standard network.**

#### **Solusi:**

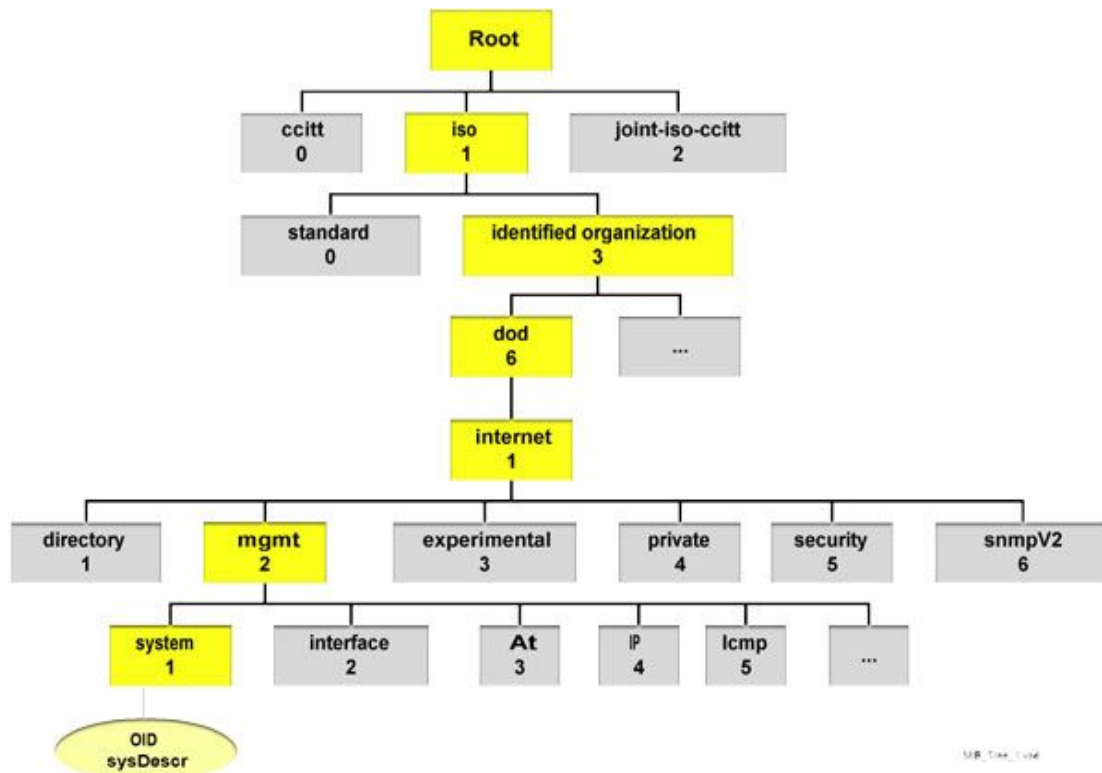
**menggunakan ISO Object Identifier tree.**

- **Setiap object terkait dalam struktur yang hierarki.**
- **Setiap cabang dan sub cabang mempunyai nama dan nomor.**

### 10. ISO Object Identifier (OID) Tree



### 11. MIB (Management Information Base) Tree



## 12. Format Pesan SNMPv1

Version	Community	SNMP PDU
---------	-----------	----------

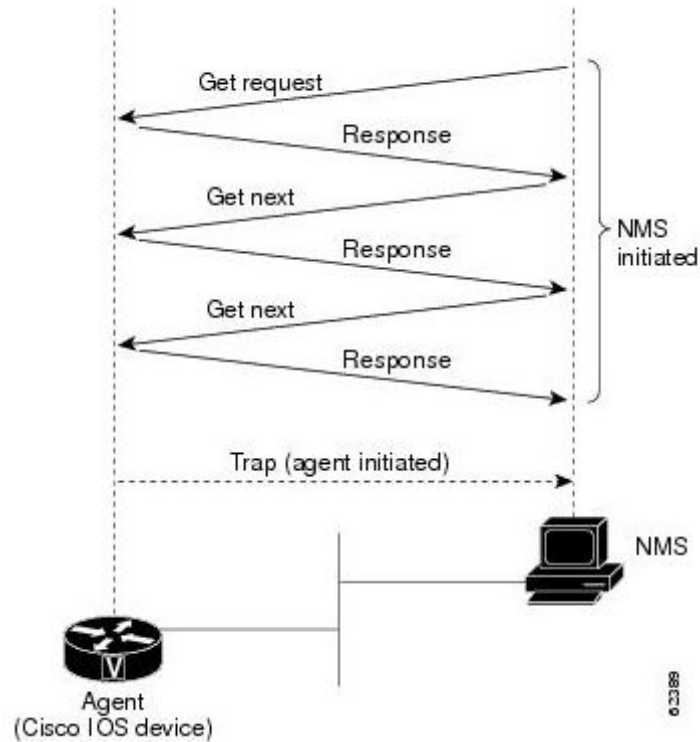
```
Frame 6: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0
  Ethernet II, Src: CadmusCo_6b:a6:48 (08:00:27:6b:a6:48), Dst: AsustekC_a3:05:d7 (f4:6d:04:a3:05:d7)
  Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.3 (192.168.1.3)
  User Datagram Protocol, Src Port: 57343 (57343), Dst Port: snmp (161)
  Simple Network Management Protocol
    version: version-1 (0)
    community: public
    data: get-request (0)
      get-request
        request-id: 176233
        error-status: noError (0)
        error-index: 0
        variable-bindings: 1 item
          1.3.6.1.2.1.25.2.3.1.6.1: Value (Null)
            Object Name: 1.3.6.1.2.1.25.2.3.1.6.1 (iso.3.6.1.2.1.25.2.3.1.6.1)
            Value (Null)
```

0000	f4 6d 04 a3 05 d7 08 00 27 6b a6 48 08 00 45 00	.m.....'k.H..E.
0010	00 49 00 00 40 00 40 11 b7 4f c0 a8 01 01 c0 a8	.I..@..0.....
0020	01 03 df ff 00 a1 00 35 b1 b6 30 2b 02 01 00 04	.....5..0+....
0030	06 70 75 62 6c 69 63 a0 1e 02 03 02 b0 69 02 01	.public.....i..
0040	00 02 01 00 30 11 30 0f 06 0b 2b 06 01 02 01 19	...0.0...+.....
0050	02 03 01 06 01 05 00	.....



### 13. SNMP Event Interaction and Timing



#### Get Request Object ID (OID) = 1.3.6.1.2.1.25.2.3.1.6.1

Source	Destination	Object ID (OID)
192.168.1.1	192.168.1.3	1.3.6.1.2.1.25.2.3.1.6.1

The screenshot shows a captured SNMP get-request packet. The packet details are highlighted in yellow:

- Simple Network Management Protocol
  - version: version-1 (0)
  - community: public
  - data: get-request (0)
    - get-request
      - request-id: 176233
      - error-status: noError (0)
      - error-index: 0
      - variable-bindings: 1 item
        - 1.3.6.1.2.1.25.2.3.1.6.1: Value (Null)
          - Object Name: 1.3.6.1.2.1.25.2.3.1.6.1 (iso.3.6.1.2.1.25.2.3.1.6.1)
          - Value (Null)

The hex dump at the bottom shows the raw packet data:

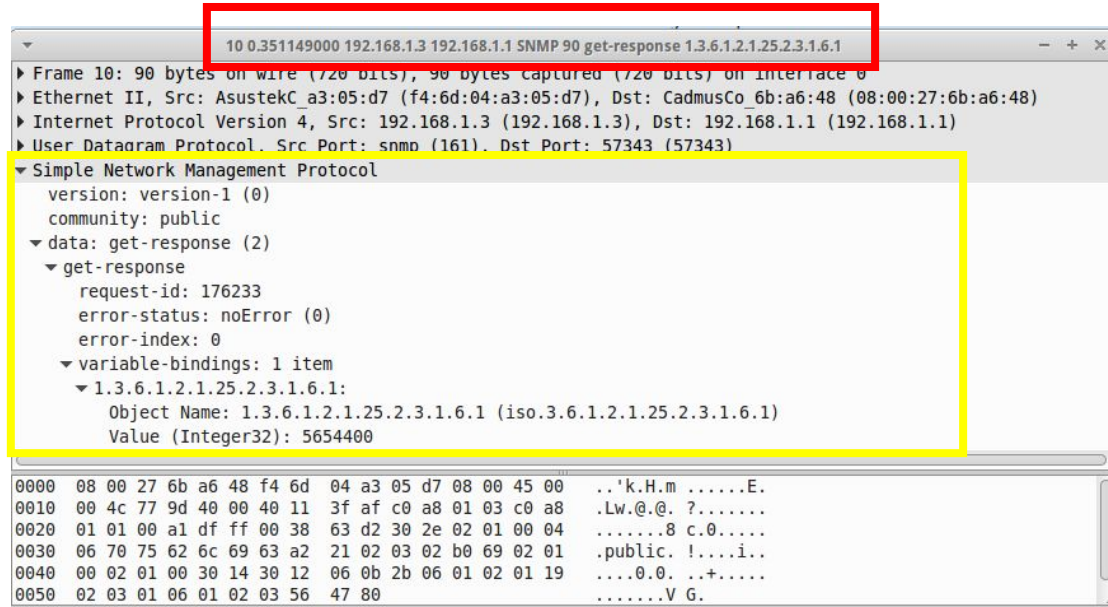
```

0000 f4 6d 04 a3 05 d7 08 00 27 6b a6 48 08 00 45 00 .m..... 'k.H..E.
0010 00 49 00 00 40 00 40 11 b7 4f c0 a8 01 01 c0 a8 .I.@.@. .0.....
0020 01 03 df ff 00 a1 00 35 b1 b6 30 2b 02 01 00 04 .....5 ..0+....
0030 06 70 75 62 6c 69 63 a0 1e 02 03 02 b0 69 02 01 .public. ....i..
0040 00 02 01 00 30 11 30 0f 06 0b 2b 06 01 02 01 19 ....0.0. .+.....
0050 02 03 01 06 01 05 00 .....
  
```

Nama : Johan Wahyudi  
NIM : 09011281320031

**Get Response Object ID (OID) = 1.3.6.1.2.1.25.2.3.1.6.1**

Source	Destination	Object ID (OID)
192.168.1.3	192.168.1.1	1.3.6.1.2.1.25.2.3.1.6.1



10 0.351149000 192.168.1.3 192.168.1.1 SNMP 90 get-response 1.3.6.1.2.1.25.2.3.1.6.1

- ▶ Frame 10: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
- ▶ Ethernet II, Src: AsustekC\_a3:05:d7 (f4:6d:04:a3:05:d7), Dst: CadmusCo\_6b:a6:48 (08:00:27:6b:a6:48)
- ▶ Internet Protocol Version 4, Src: 192.168.1.3 (192.168.1.3), Dst: 192.168.1.1 (192.168.1.1)
- ▶ User Datagram Protocol, Src Port: snmp (161), Dst Port: 57343 (57343)
- ▼ Simple Network Management Protocol
  - version: version-1 (0)
  - community: public
  - ▼ data: get-response (2)
    - ▼ get-response
      - request-id: 176233
      - error-status: noError (0)
      - error-index: 0
      - ▼ variable-bindings: 1 item
        - ▼ 1.3.6.1.2.1.25.2.3.1.6.1:
          - Object Name: 1.3.6.1.2.1.25.2.3.1.6.1 (iso.3.6.1.2.1.25.2.3.1.6.1)
          - Value (Integer32): 5654400

```
0000 08 00 27 6b a6 48 f4 6d 04 a3 05 d7 08 00 45 00  ..'k.H.m .....E.
0010 00 4c 77 9d 40 00 40 11 3f af c0 a8 01 03 c0 a8  .Lw.@.@. ?.....
0020 01 01 00 a1 df ff 00 38 63 d2 30 2e 02 01 00 04  .....8 c.0.....
0030 06 70 75 62 6c 69 63 a2 21 02 03 02 b0 69 02 01  .public. !....i..
0040 00 02 01 00 30 14 30 12 06 0b 2b 06 01 02 01 19  ....0.0. ..+.....
0050 02 03 01 06 01 02 03 56 47 80                    .....V G.
```

**Nama : Johan Wahyudi**  
**NIM : 09011281320031**

---

---

**Referensi :**

- <http://www.cisco.com/en/US/docs/routers/access/as5850/software/operations/guide/adm.html>
- <http://www.myloadtest.com/snmp-with-loadrunner/>
- <https://blogs.technet.microsoft.com/kevinholman/2015/02/03/snmp-trap-monitoring-with-scom-2012-r2/>
- [https://id.wikipedia.org/wiki/Protokol\\_Manajemen\\_Jaringan\\_Sederhana](https://id.wikipedia.org/wiki/Protokol_Manajemen_Jaringan_Sederhana)