

TUGAS 3 MID

MANAJEMEN JARINGAN



BRAMANTIO RIZKI NUGROHO

NIM 09121001044

SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2016

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) adalah spesifikasi manajemen jaringan yang dikembangkan oleh Internet Engineering Task Force (IETF), sebuah bagian dari Internet Activities Board (IAB), pada pertengahan tahun 1980-an sebagai standar manajemen untuk produk-produk jaringan berbasis LAN, seperti bridge, router, dan wiring concentrator. SNMP didesain untuk mengurangi tingkat kompleksitas dari manajemen jaringan dan banyaknya sumber daya yang dibutuhkan untuk mendukung manajemen tersebut. Adanya SNMP memungkinkan manajemen jaringan yang tersentralisasi, kuat, dan kompatibel pada semua platform. Selain itu, SNMP memberikan fleksibilitas untuk manajemen informasi-informasi yang dimiliki oleh vendor produk tertentu. SNMP merupakan spesifikasi komunikasi yang menjelaskan bagaimana informasi manajemen dipertukarkan antara aplikasi manajemen jaringan dengan agen manajemen. Terdapat beberapa versi dari SNMP, tetapi yang populer adalah SNMPv1 dan SNMPv2. Terdapat 3 konsep dasar pada SNMP, yaitu : manager, agent, dan management information based (MIB). Pada beberapa konfigurasi di titik manager menjalankan suatu software management, dimana perangkat yang dapat dimanage seperti bridges, routers, servers dan workstations yang dapat integrasikan dengan sebuah modul software agent. Agent bertanggung jawab untuk menyediakan akses ke lokal MIB dari object resources dan aktivitas node tersebut. Agen tersebut juga akan bereaksi terhadap perintah manager untuk mendapat kembali nilai-nilai dari MIB dan untuk menetapkan nilai-nilai di dalam MIB. Satu contoh dari suatu obyek didapat kembali dari suatu perhitungan dari banyaknya paket-paket pengirim dan penerima pada sebuah node. Manager dapat memonitor nilai yang di load pada jaringan tersebut. Software Agent berada pada di devices tersebut, beberapa agent menerima pesan yang masuk dari manager, pesan permintaan tersebut di baca atau ditulis pada data device tersebut. Agent akan mengirimkan kembali respon yang diterima, dimana agent tidak harus menunggu untuk bertanya tentang sebuah informasi. Namun pada beberapa kasus tertentu agent akan mengirimkan sebuah pesan notifikasi untuk melakukan trap ke satu atau lebih manager. Software Management pada sebuah station management akan mengirimkan pesan request ke agent dan menerima respon dan trap dari agent. Protocol UDP yang biasa digunakan sebagai pembawa paket tersebut dengan karakteristiknya yang hemat dengan bandwidth, namun protocol pembawa lainnya juga dapat digunakan.

SNMP Versi 1

SNMP versi 1 adalah standar protokol SNMP yang pertama kali dibuat, SNMP dibuat untuk digunakan sebagai alat manajemen jaringan untuk jaringan dan mengoperasikan internetworking TCP/IP. (Stallings, 2007,p761). SNMP sebenarnya digunakan untuk merujuk kepada kumpulan spesifikasi manajemen

jaringan yang mencakup protocol itu sendiri, definisi database, dan konsep-konsep yang terkait. Model manajemen jaringan yang digunakan untuk SNMP mencakup elemen-elemen utama sebagai berikut:

1. Management station atau Manager
2. Agent
3. Management Information Base
4. Network Management Protocol

SNMP Versi 2

SNMPv2 menyediakan framework dimana dapat dibangun aplikasi manajemen jaringan dan menyediakan infrastruktur untuk manajemen jaringan. (Stallings, 2007, p765). Fungsi-fungsi pada SNMP v1 masih sama dengan yang digunakan pada SNMP v2, namun ada fungsi-fungsi yang dikembangkan, seperti pada fungsi trap. SNMP v2 juga memperkenalkan 2 protokol baru yaitu GetBulk dan Inform. GetBulk digunakan oleh NMS untuk mendapatkan data yang berukuran besar dengan efisien. Operasi Inform memungkinkan NMS untuk saling mengirimkan informasi trap. Dari segi keamanan SNMP v2 juga dikembangkan sehingga lebih aman dibanding SNMP v1.

SNMP Versi 3

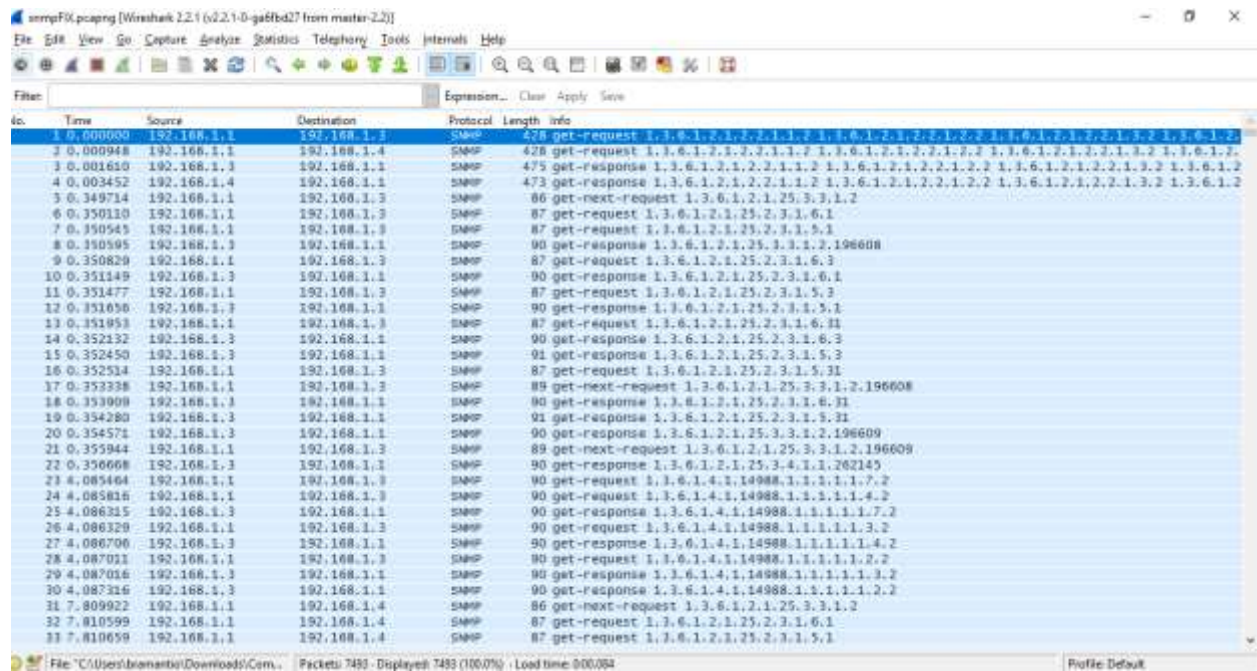
SNMPv3 menyediakan 3 layanan penting yaitu authentication, privacy, dan access control, Authentication dan privacy adalah bagian dari User-Based Security Model (USM) dan access control didefinisikan dalam View-Based Access Control Model (VACM). (Stallings, 2007, p769).

Management Information Base (MIB)

Management information base (MIB) adalah koleksi dari objek-objek atau variable data-data yang merupakan salah satu aspek dari managed agent. (Stallings, 2007, p762). Setiap perangkat memiliki unique object identifier (OID) yang terdiri dari angka – angka yang dipisahkan oleh titik. OID secara alami akan membentuk tree. MIB menghubungkan setiap OID dengan label dan parameter lain yang berhubungan dengan objek yang bersangkutan. MIB kemudian bertindak sebagai kamus atau buku kode yang digunakan untuk menghubungkan dan menerjemahkan SNMP.

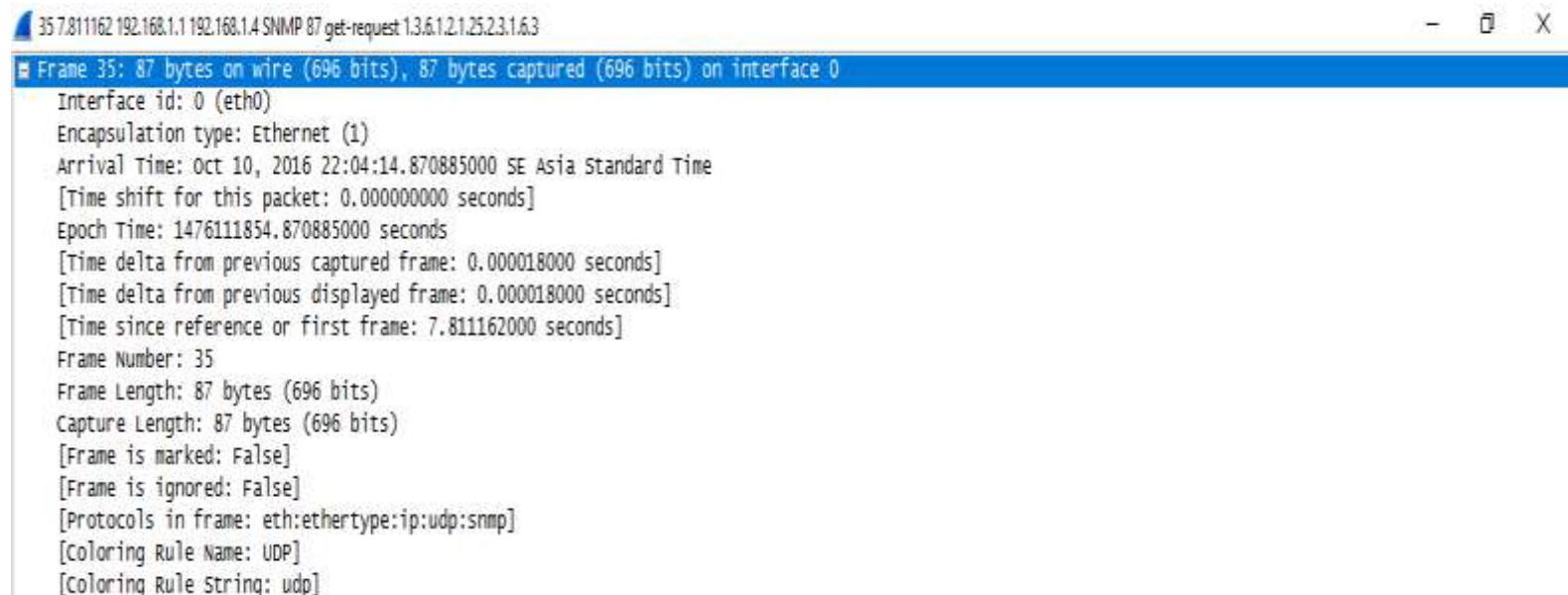
Analisa Packet Capture Pada Wireshark

Hasil capture packet dengan "Wiresharks"



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	192.168.1.4	SNMP	478	get-request 1.3.6.1.2.1.25.2.3.1.2.196608
2	0.000948	192.168.1.1	192.168.1.4	SNMP	478	get-request 1.3.6.1.2.1.25.2.3.1.2.196608
3	0.001810	192.168.1.3	192.168.1.1	SNMP	473	get-response 1.3.6.1.2.1.25.2.3.1.2.196608
4	0.003452	192.168.1.4	192.168.1.1	SNMP	473	get-response 1.3.6.1.2.1.25.2.3.1.2.196608
5	0.0049714	192.168.1.1	192.168.1.3	SNMP	86	get-next-request 1.3.6.1.2.1.25.2.3.1.2
6	0.050110	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.6.1
7	0.050545	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.6.1
8	0.050595	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.2.3.1.6.1
9	0.050829	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.6.3
10	0.051149	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.2.3.1.6.1
11	0.051477	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.6.3
12	0.051650	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.2.3.1.6.1
13	0.051953	192.168.1.4	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.6.31
14	0.052132	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.2.3.1.6.3
15	0.052450	192.168.1.3	192.168.1.1	SNMP	91	get-response 1.3.6.1.2.1.25.2.3.1.5.3
16	0.052534	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.5.31
17	0.053338	192.168.1.1	192.168.1.3	SNMP	89	get-next-request 1.3.6.1.2.1.25.2.3.1.2.196608
18	0.053909	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.2.3.1.6.31
19	0.054280	192.168.1.3	192.168.1.1	SNMP	91	get-response 1.3.6.1.2.1.25.2.3.1.5.31
20	0.054571	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.2.3.1.2.196609
21	0.055944	192.168.1.1	192.168.1.3	SNMP	89	get-next-request 1.3.6.1.2.1.25.2.3.1.2.196609
22	0.056668	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.2.3.1.2.262145
23	4.085464	192.168.1.1	192.168.1.3	SNMP	90	get-request 1.3.6.1.4.1.14988.1.1.1.1.1.7.2
24	4.085816	192.168.1.1	192.168.1.3	SNMP	90	get-request 1.3.6.1.4.1.14988.1.1.1.1.1.4.2
25	4.086315	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.4.1.14988.1.1.1.1.1.7.2
26	4.086329	192.168.1.1	192.168.1.3	SNMP	90	get-request 1.3.6.1.4.1.14988.1.1.1.1.1.3.2
27	4.086700	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.4.1.14988.1.1.1.1.1.4.2
28	4.087011	192.168.1.1	192.168.1.3	SNMP	90	get-request 1.3.6.1.4.1.14988.1.1.1.1.1.2.2
29	4.087016	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.4.1.14988.1.1.1.1.1.3.2
30	4.087316	192.168.1.3	192.168.1.1	SNMP	90	get-response 1.3.6.1.4.1.14988.1.1.1.1.1.2.2
31	7.809922	192.168.1.1	192.168.1.4	SNMP	86	get-next-request 1.3.6.1.2.1.25.2.3.1.2
32	7.810599	192.168.1.1	192.168.1.4	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.6.1
33	7.810659	192.168.1.1	192.168.1.4	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.5.1

Paket No. 35 digunakan sebagai sample.



```
35 7.811162 192.168.1.1 192.168.1.4 SNMP 87 get-request 1.3.6.1.2.1.25.2.3.1.6.3
Frame 35: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 10, 2016 22:04:14.870885000 SE Asia Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1476111854.870885000 seconds
[Time delta from previous captured frame: 0.000018000 seconds]
[Time delta from previous displayed frame: 0.000018000 seconds]
[Time since reference or first frame: 7.811162000 seconds]
Frame Number: 35
Frame Length: 87 bytes (696 bits)
Capture Length: 87 bytes (696 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:snmp]
[Coloring rule Name: UDP]
[Coloring rule String: udp]
```

35 7.811162 192.168.1.1 192.168.1.4 SNMP 87 get-request 1.3.6.1.2.1.25.2.3.1.6.3

Frame 35: 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: Raspberr_4e:56:9b (b8:27:eb:4e:56:9b)

- Destination: Raspberr_4e:56:9b (b8:27:eb:4e:56:9b)
 - Address: Raspberr_4e:56:9b (b8:27:eb:4e:56:9b)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Source: CadmusCo_6b:a6:48 (08:00:27:6b:a6:48)
 - Address: CadmusCo_6b:a6:48 (08:00:27:6b:a6:48)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

35 7.811162 192.168.1.1 192.168.1.4 SNMP 87 get-request 1.3.6.1.2.1.25.2.3.1.6.3

Frame 35: 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: Raspberr_4e:56:9b (b8:27:eb:4e:56:9b)

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.4

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - 0000 00.. = Differentiated Services Codepoint: Default (0)
 -00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
- Total Length: 73
- Identification: 0x0000 (0)
- Flags: 0x02 (Don't Fragment)
 - 0... = Reserved bit: Not set
 - .1.. = Don't fragment: Set
 - ..0. = More fragments: Not set
- Fragment offset: 0
- Time to live: 64
- Protocol: UDP (17)
- Header checksum: 0xb74e [validation disabled]
 - [Header checksum status: Unverified]
- Source: 192.168.1.1
- Destination: 192.168.1.4
 - [Source GeoIP: Unknown]
 - [Destination GeoIP: Unknown]

35 7.811162 192.168.1.1 192.168.1.4 SNMP 87 get-request 1.3.6.1.2.1.25.2.3.1.6.3

Frame 35: 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: Raspberr_4e:56:9b (b8:27:eb:4e:56:9b)

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.4

User Datagram Protocol, Src Port: 57343, Dst Port: 161

- Source Port: 57343
- Destination Port: 161
- Length: 53
- Checksum: 0xaf8c [unverified]
 - [Checksum Status: Unverified]
- [Stream index: 1]

Simple Network Management Protocol

```
Frame 35: 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: Raspberr_4e:56:9b (b8:27:eb:4e:56:9b)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.4
User Datagram Protocol, Src Port: 57343, Dst Port: 161
Simple Network Management Protocol
  version: version-1 (0)
  community: public
  data: get-request (0)
    get-request
      request-id: 176274
      error-status: noError (0)
      error-index: 0
    variable-bindings: 1 item
      1.3.6.1.2.1.25.2.3.1.6.3: value (Null)
        Object Name: 1.3.6.1.2.1.25.2.3.1.6.3 (iso.3.6.1.2.1.25.2.3.1.6.3)
        value (Null)
```

Device	IP Address	Fungsi
Mikrotik (Server)	192.168.1.1	Manager
Windows (Client)	192.168.1.2	Agent
Linux (Client)	192.168.1.3	Agent
Raspberry Pi (Client)	192.168.1.4	Agent