

TUGAS  
MANAJEMEN JARINGAN



NAMA : MUHAMMAD FACHRURROJI ILHAM S

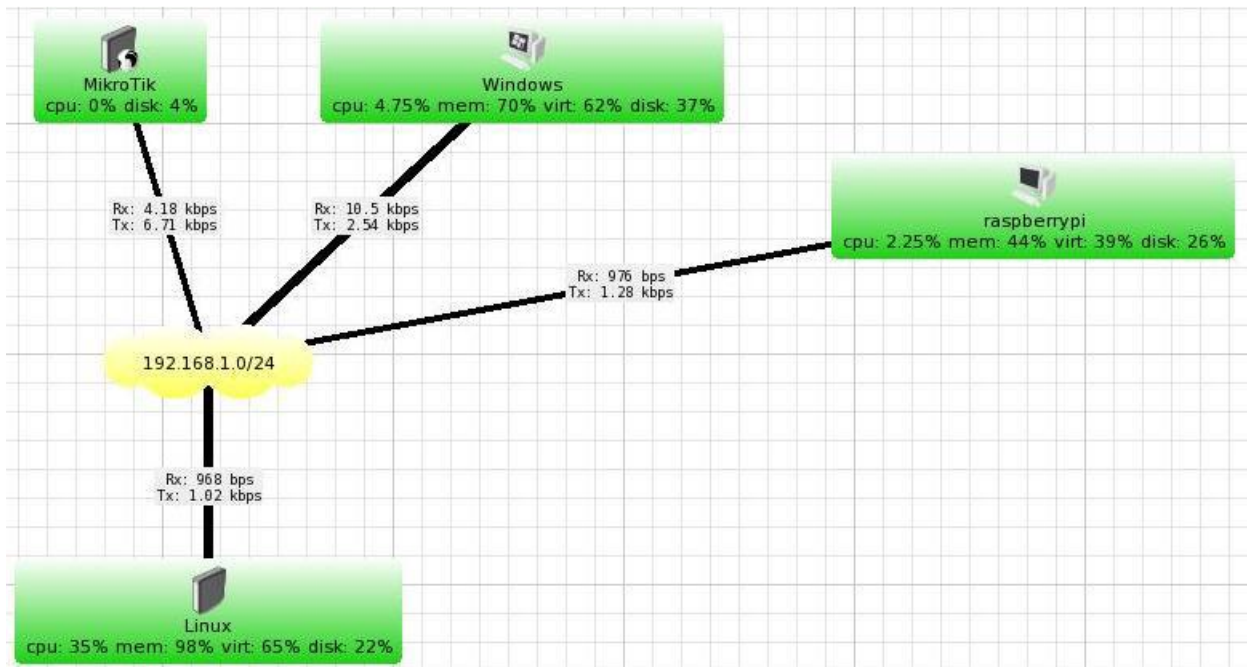
NIM : 09011181320025

JURUSAN SISTEM KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS SRIWIJAYA

2016

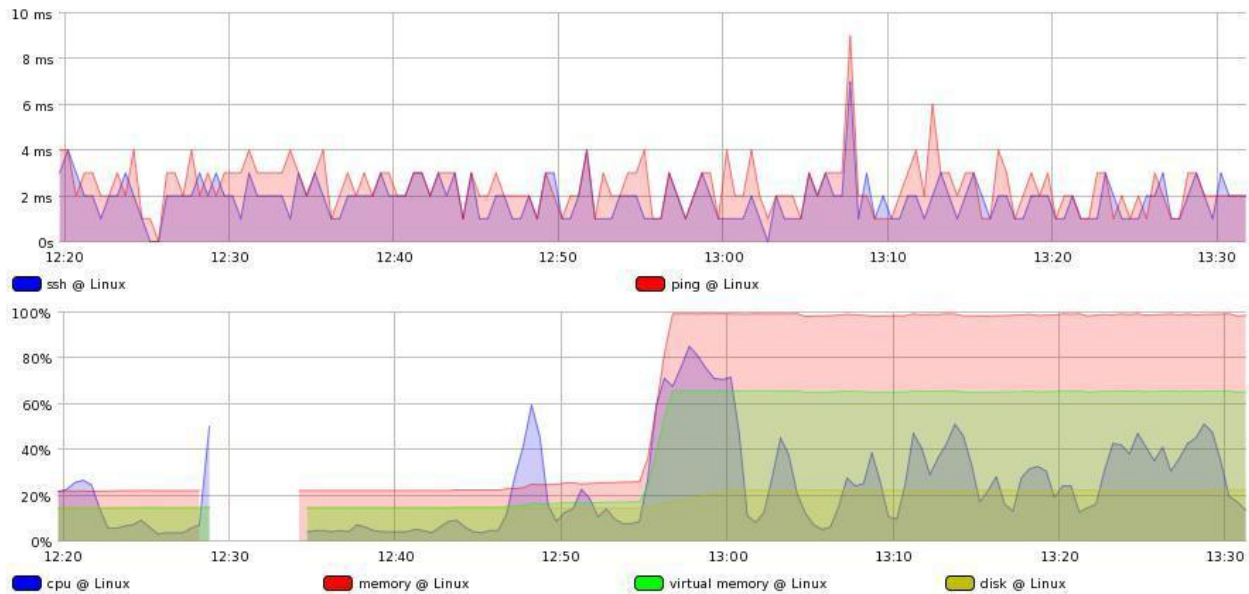
SNMP merupakan sebuah protokol yang dirancang untuk memberikan kemampuan kepada pengguna untuk memantau dan mengatur jaringan komputernya secara sistematis dari jarak jauh atau dalam satu pusat kontrol saja. Dengan menggunakan protokol kita bisa mendapatkan informasi tentang status dan keadaan dari suatu jaringan. Pengolahan ini dijalankan dengan mengumpulkan data dan melakukan penetapan terhadap variabel-variabel dalam elemen jaringan yang dikelola.

## Topologi SNMP



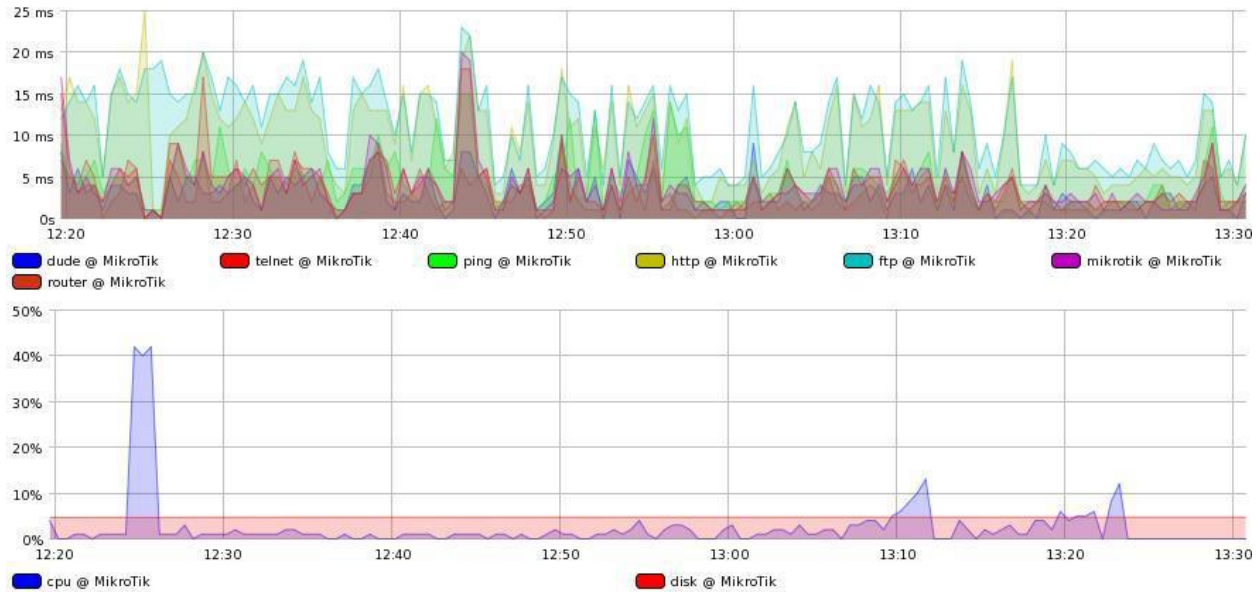
Penjelasan gambar topologi SNMP diatas SNMP digunakan untuk manajemen network. SNMP merupakan protokol untuk manajemen peralatan yang terhubung dalam jaringan IP. Aada beberapa alat yang digunakan yaitu switch, router, modem, komputer, server dan lain-lain. Dari gambar diatas bahwa internet protocol mengirim data melalui beberapa perangkat komputer yaitu mikrotik, windows, raspberry pi dan data yang dikirim 6.71 kbps dan data yang diterima 4.18 kbps, sedangkan pada windows data yang dikirim 2.54 kbps dan data yang diterima 10.5 kbps dan pada raspberry pi data yang dikirim 1.28kbps dan data yang diterima 976 bps. Pada linux sendiri, internet protocol mengirim data 1.02 kbps dan menerima data 968 bps.

## Traffic linux



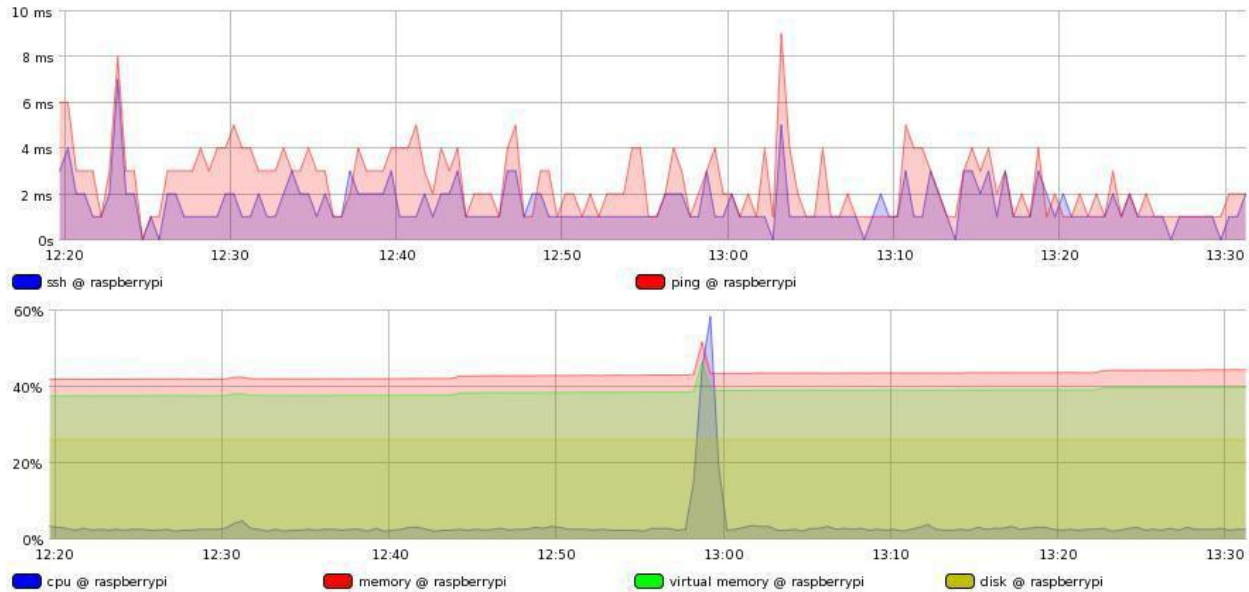
Dari gambar di atas traffic yang pertama kita bisa lihat terdapat 2 warna pada traffic yaitu warna biru dan merah, pada warna biru warna itu adalah statistic ssh dan warna merah adalah statistic ping. Pada pukul 13.10 dapat kita lihat itu adalah traffic tertinggi dengan kecepatannya 6 ms, kemudian traffic mengalami penurunan dengan kecepatan 0 ms dan traffic tersebut normal pada pukul 12.20 dengan kecepatan trafficnya 4 ms. Pada gambar traffic yang kedua terdapat 4 bagian warna yaitu merah biru, hijau dan kuning, pada warna biru menunjukkan statistik cpu, warna merah statistik memory, warna hijau trafik virtual memory dan warna kuning trafik disk. Pada warna biru statistik tertinggi pada pukul 13:00 yaitu sekitar lebih dari 80% dan statistik terendah pada pukul 12:30 sampai dengan pukul 12:30 dengan persentasenya 0%. Pada warna merah statistik tertinggi yaitu pada pukul 13:00 dengan presentasinya 100% dan statistik terendah pada pukul 12:20 dengan presentasinya 20%. Pada warna hijau statistik tertinggi pada pukul 13:00 dengan presentasinya 60% dan statistik terendah pada pukul 12:30 dengan presentasinya 0%. Pada warna yang terakhir yaitu kuning, statistik terendah pada pukul 12:20 dan mengalami penurunan kemudian netral kembali pada pukul 12:40 dengan presentasinya 20% dan statistik tertinggi pada pada pukul 13:00 dan kembali netral pada pukul 13:30 dengan presentasinya lebih dari 20%.

## Traffic Mikrotik



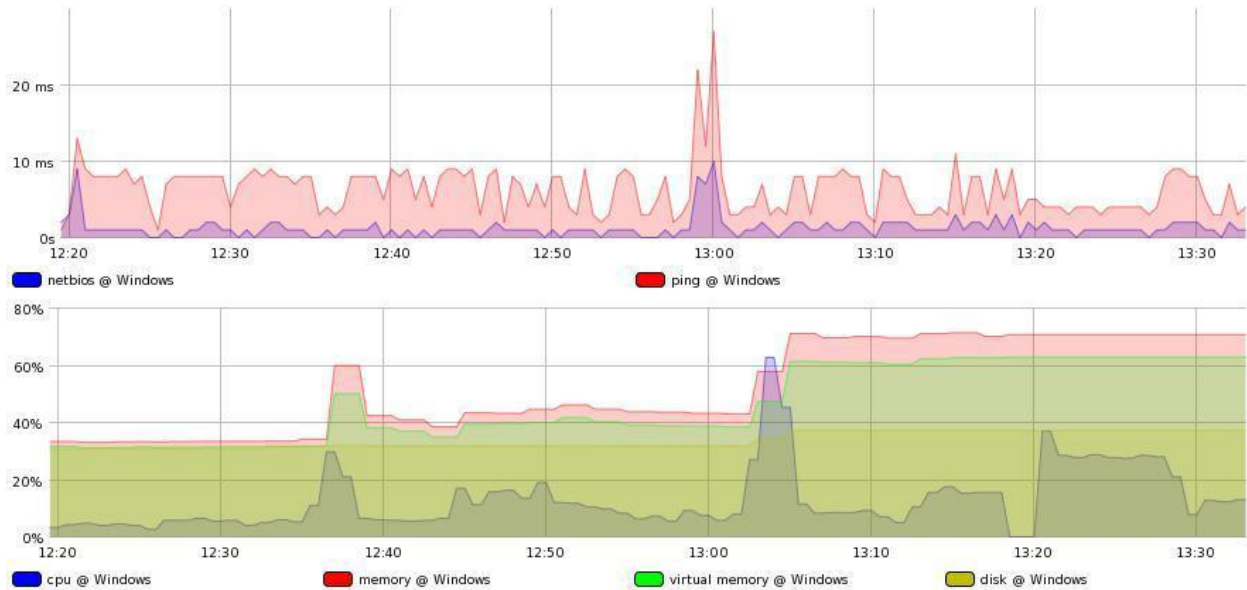
Dari gambar diatas, kita bias lihat warna biru sebagai statistic nude, warna merah sebagai talnet, warna hijau sebagai ping, warna kuning sebagai http, warna biru muda sebagai ftp, warna ungu sebagai mikrotik dan warna merah tua sebagai router. Pada statistik dude, statistik tertinggi pada pukul 13:00 dengan kecepatan data kurang dari 10 ms. Pada ping, statistik tertinggi pukul 13:00 dengan kecepatan data kurang dari 15 ms. Pada http, statistik tertinggi pada pukul lebih 12:40 dengan kecepatan data lebih dari 20 ms. Pada ftp, statistik tertinggi pada pukul 12:40 dengan kecepatan data lebih dari 20 ms. Pada mikrotik, statistik tertinggi pukul 12:40 dengan kecepatan data 20 ms. Kemudian traffic kedua, warna biru sebagai cpu dan warna merah sebagai disk. Pada cpu, statistik tertinggi pada pukul 12:20 dengan presentase data lebih dari 40% dan statistik terendah pada pukul 12:20. Netral kembali pukul 12:20 sampai dengan waktu 13:30.

## Traffic Raspberry pi



Pada gambar traffic atas yang pertama, warna biru yaitu ssh dan warna merah statistik ping. Pada statistik ssh, statistik tertinggi terdapat pada pukul 12:20 dengan kecepatan data 6 ms dan statistik terendah pada pukul 12:30 dengan kecepatan data 0 ms sedangkan statistik netral kembali pada kecepatan 2 ms. Pada traffic kedua, warna biru yaitu sebagai cpu, warna merah statistik memory, warna hijau statistik virtual memory dan warna kuning statistik disk. Pada cpu, statistik tertinggi pukul 13:00 dengan presentase data yang diterima 60%. Pada memory, statistik tertinggi pukul 13:00 dengan presentase data yang diterima 60% dan statistik terendah pukul 12:20 dengan presentase data yang diterima 40%. Pada virtual memory, statistik tertinggi pukul 13:00 dengan data yang diterima lebih dari 40% dan statistik terendah pukul 12:20 dengan data yang diterima kurang dari 40%. Pada disk, statistik netralnya pukul 12:20 -13:30 dengan data yang diterima lebih dari 20%.

## Traffic windows 8



Pada gambar traffic atas yang pertama, warna biru sebagai netbios dan warna merah sebagai ping. Pada netbios, statistik tertinggi pukul 13:00 dengan kecepatan data 10 ms dan terendah pukul 12:30, jam 12:40, jam 12:50, jam 13:10, jam 13:20 kecepatan data yang diperoleh 0 s. Pada ping, statistik tertinggi pukul 13:00 kecepatan data lebih dari 20 ms dan statistik terendah pukul 12:20 kecepatan data 0 s. Pada traffic yang kedua, warna biru sebagai cpu, warna merah sebagai memory, warna hijau sebagai virtual memory dan warna kuning sebagai disk. Di cpu, statistik tertinggi pukul 13:00 dengan data lebih dari 60 % dan terendah pukul 13:20 dengan data 0%. Kemudian di memory, tertingginya pukul 13:10 dengan data 60% dan terendah pukul 12:20-12:40 dengan data 40%. Pada virtual memory, tertinggi pukul 13:10-13:30 dengan data 60% terendah pukul 12:40 dengan data 40%. Dan yang terakhir pada disk, tertinggi pukul 13:10-13:30 dengan data 40%, terendah pukul 12:20-13:00 dengan data 20%.

## PCAPS dari topologi SNMP

The screenshot displays a Wireshark capture of network traffic. The packet list pane shows the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
4951	124.355411	192.168.1.4	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.3.3.1.2.196611
4952	124.356318	192.168.1.1	192.168.1.4	SNMP	89	get-next-request 1.3.6.1.2.1.25.3.3.1.2.196611
4953	124.357235	192.168.1.4	192.168.1.1	SNMP	90	get-response 1.3.6.1.2.1.25.3.4.1.1.262145
4954	124.361870	CadmusCo_6b:a6:48	Broadcast	ARP	60	who has 192.168.1.213? Tell 192.168.1.1
4955	124.403215	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.5.31
4956	124.404219	192.168.1.3	192.168.1.1	SNMP	91	get-response 1.3.6.1.2.1.25.2.3.1.5.31
4957	124.404794	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.5.3
4958	124.405502	192.168.1.3	192.168.1.1	SNMP	91	get-response 1.3.6.1.2.1.25.2.3.1.5.3
4959	124.406634	192.168.1.1	192.168.1.3	SNMP	87	get-request 1.3.6.1.2.1.25.2.3.1.5.1

The packet details pane for packet 4955 shows the following structure:

- Frame 4955: 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)
  - Destination: AsustekC\_a3:05:d7 (f4:6d:04:a3:05:d7)
  - Source: CadmusCo\_6b:a6:48 (08:00:27:6b:a6:48)
  - Type: IP (0x0800)
- Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.3 (192.168.1.3)
  - Version: 4
  - Header Length: 20 bytes
  - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  - Total Length: 73
  - Identification: 0x0000 (0)
  - Flags: 0x02 (Don't Fragment)
  - Fragment offset: 0
  - Time to live: 64
  - Protocol: UDP (17)
  - Header checksum: 0xb74f [validation disabled]
  - Source: 192.168.1.1 (192.168.1.1)
  - Destination: 192.168.1.3 (192.168.1.3)
  - [Source GeoIP: Unknown]
  - [Destination GeoIP: Unknown]
- User Datagram Protocol, Src Port: 57343 (57343), Dst Port: 161 (161)
  - Source Port: 57343 (57343)
  - Destination Port: 161 (161)
  - Length: 53
  - Checksum: 0x8135 [validation disabled]
  - [Stream index: 0]
- Simple Network Management Protocol
  - version: version-1 (0)
  - community: public
  - data: get-request (0)
    - get-request
      - request-id: 180971
      - error-status: noError (0)
      - error-index: 0
      - variable-bindings: 1 item
        - 1.3.6.1.2.1.25.2.3.1.5.31: value (Null)
        - object Name: 1.3.6.1.2.1.25.2.3.1.5.31 (iso.3.6.1.2.1.25.2.3.1.5.31)
        - value (Null)

Dari gambar pcaps di atas dapat dijelaskan IP destination yang digunakan adalah 192.168.1.3 dan IP source nya adalah 192.168.1.1, SNMP request-id: 180971 error-status: noError (0) error-index: 0. Pada variabel bindings terdapat 1 item yaitu: 1.3.6.1.2.1.25.2.3.1.5.31: value (Null) object name: 1.3.6.1.2.1.25.2.3.1.5.31 (iso.3.6.1.2.1.25.2.3.1.5.31) value (Null).