

UTS
MANAJEMEN JARINGAN



OLEH :

NICA HARTUTI

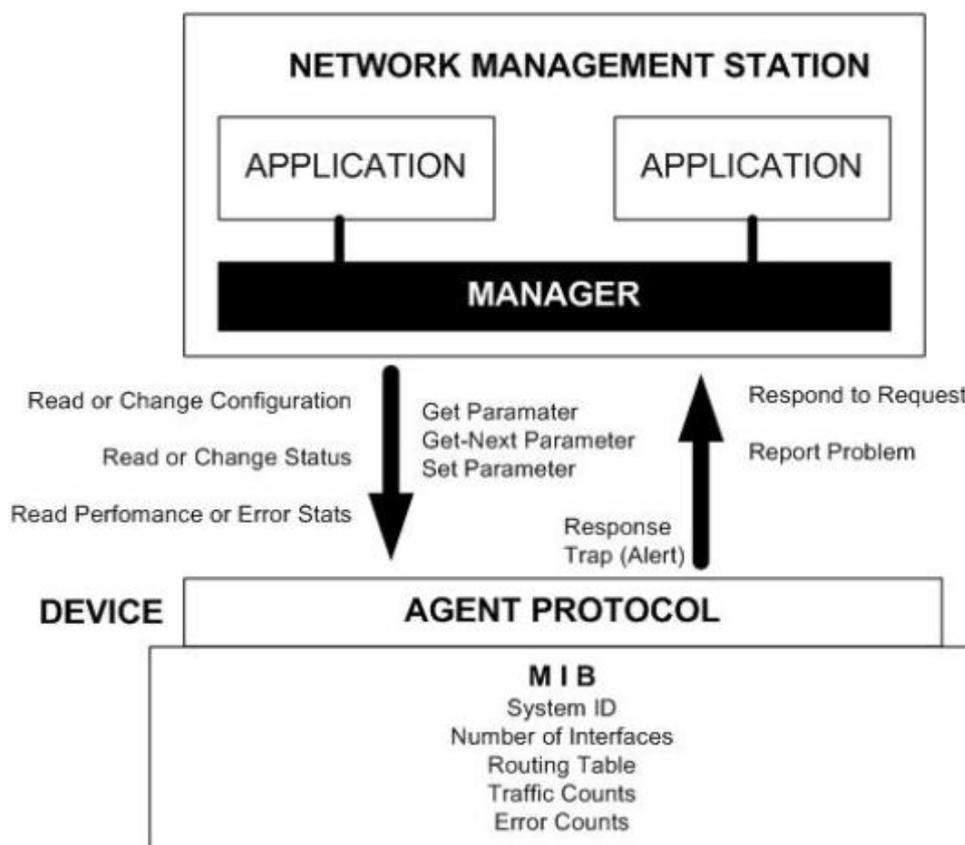
09011181320044

SK7B

SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
INDRALAYA
2016

Monitoring jaringan adalah salah satu fungsi dari *management* yang berguna untuk menganalisa apakah jaringan masih cukup layak untuk digunakan atau perlu tambahan kapasitas . Network Management Station, yang berfungsi sebagai pusat penyimpanan untuk pengumpulan dan analisa dari data manajemen jaringan.

Manajer juga disebut Network Management Station atau NMS. Perangkat lunak yang digunakan untuk membuat NMS bervariasi dalam fungsi serta beban. Fungsi lain dari NMS termasuk fitur pelaporan, pemetaan topologi jaringan dan mendokumentasikan, alat untuk memungkinkan Anda untuk memonitor lalu lintas pada jaringan Anda, dan sebagainya. Beberapa konsol manajemen juga dapat menghasilkan laporan analisis trend. Jenis laporan dapat membantu Anda melakukan perencanaan kapasitas dan menetapkan tujuan jangka panjang.



Gambar 5. Interaksi antara manager dan agent [18].

ELEMEN SNMP

1. Manajer

- ❖ software yang berjalan di sebuah host di jaringan.
- ❖ meminta informasi ke Agent.
- ❖ Manajer ini terdiri atas satu proses atau lebih yang berkomunikasi dengan agen-agensya dan dalam jaringan.
- ❖ Manajer akan mengumpulkan informasi dari agen 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.

2. Agent

- ❖ Agent merupakan perangkat lunak yang dijalankan disetiap elemen jaringan yang dikelola.
- ❖ Setiap agen mempunyai basis data variabel yang bersifat lokal yang menerangkan keadaan dan berkas aktivitasnya dan pengaruhnya terhadap operasi.

3. MIB (*Management Information Base*)

- ❖ Management Information Base, merupakan struktur basis data variabel dari elemen jaringan yang dikelola.
- ❖ Struktur ini bersifat hierarki dan memiliki aturan sedemikian rupa sehingga informasi setiap variabel dapat dikelola atau ditetapkan dengan mudah.
- ❖ 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,

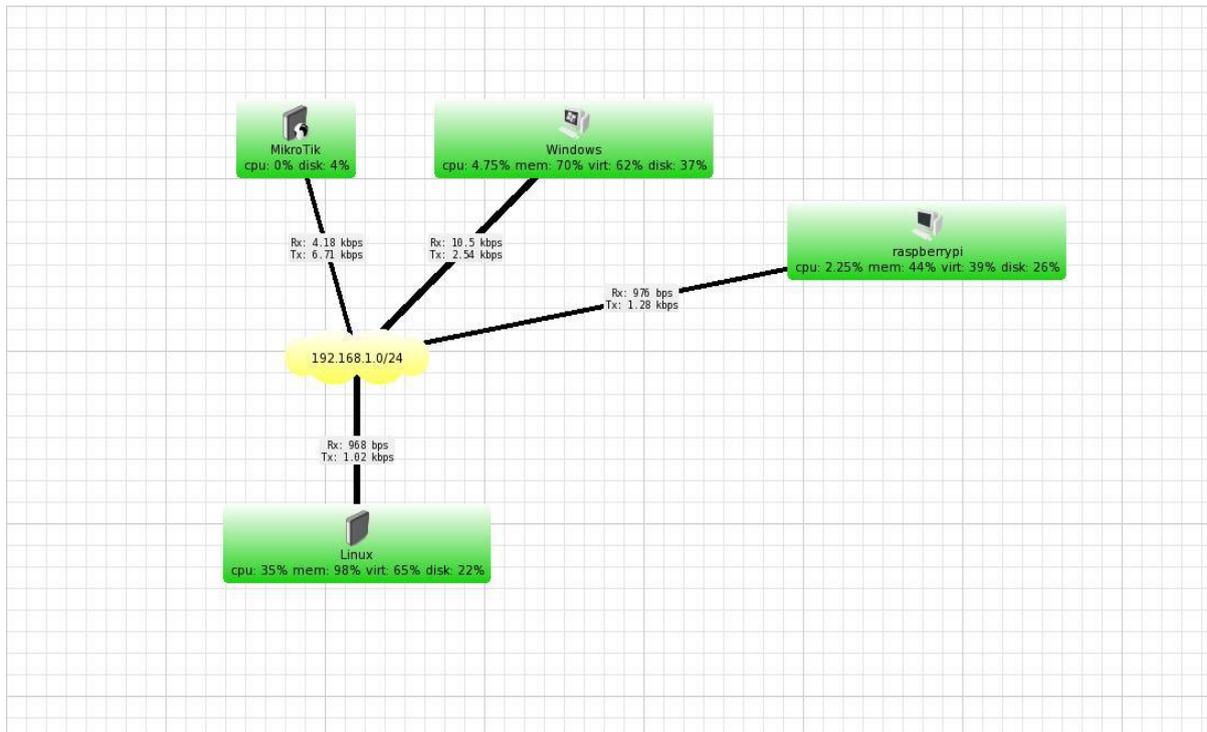
ifInErrors mendefinisikan jumlah paket diterima yang dibuang karena rusak,

ifOutErrors mendefinisikan jumlah paket dikirim yang dibuang karena rusak,

dan variable

- ❖ MIB di akses menggunakan protokol network-manajemen seperti SNMP. MIB terdiri dari managed objek dan di identifikasi oleh object identifier (pengidentifikasi objek).

TOPOLOGI PADA LINUX , MIKROTIK , WINDOWS , RSPBERRY .



Keterangan :

Pada gambar diatas adalah SNMP yang merupakan SNMP adalah protokol populer untuk melakukan network manajemen. SNMP digunakan untuk mengumpulkan informasi, dan mengkonfigurasi, peralatan jaringan, seperti, server, printer, hub, switch, dan router di jaringan berbasis Internet Protocol (IP). SNMP dapat mengumpulkan informasi seperti kondisi CPU, temperatur chasis, dan hampir tidak ada batas akan apa yang dapat dikonfigurasi oleh SNMP.

UDP lebih mudah di gunakan daripada menggunakan protokol yang lebih kompleks seperti TCP. Walau demikian, UDP mampu memberikan banyak fungsi yang memungkinkan komputer pusat manajemen untuk berkomunikasi dengan agen remote yang terdapat pada managed device. Sementara yang terjadi dalam pencatatan di peralatan biasanya pada siklus waktu periodik, tidak masalah jika ada data yang hilang karena nantinya akan tetap di update dengan data yang baru. Hal lain yang

menyebabkan UDP menarik untuk digunakan adalah karena sangat sederhana, tidak memakan bandwidth jaringan terlalu besar tidak seperti TCP.

Pada wireshark pcap SNMP

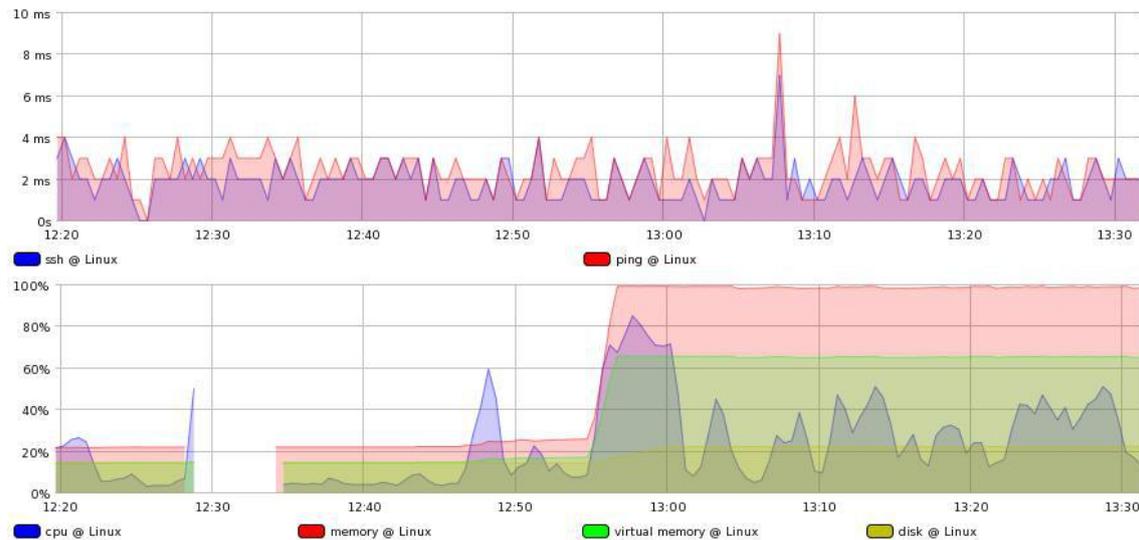
1	0.00000000	192.168.1.1	192.168.1.3	SNMP	428	get-request	1.3.6.1.2.1.2.2.1.1.2	1.3.6.1.2.1.2.2.1.2.2	1.3.6.1.2.1.2.2.1.2.2	1.3.6.1.2.1.2.2.1.3.2	1.3.6.1.2.1.2.2.1.4
2	0.00094800	192.168.1.1	192.168.1.4	SNMP	428	get-request	1.3.6.1.2.1.2.2.1.1.2	1.3.6.1.2.1.2.2.1.1.2	1.3.6.1.2.1.2.2.1.2.2	1.3.6.1.2.1.2.2.1.3.2	1.3.6.1.2.1.2.2.1.4
3	0.00161000	192.168.1.3	192.168.1.1	SNMP	475	get-response	1.3.6.1.2.1.2.2.1.1.2	1.3.6.1.2.1.2.2.1.1.2	1.3.6.1.2.1.2.2.1.2.2	1.3.6.1.2.1.2.2.1.3.2	1.3.6.1.2.1.2.2.1.4
4	0.00345200	192.168.1.4	192.168.1.1	SNMP	473	get-response	1.3.6.1.2.1.2.2.1.1.2	1.3.6.1.2.1.2.2.1.1.2	1.3.6.1.2.1.2.2.1.2.2	1.3.6.1.2.1.2.2.1.3.2	1.3.6.1.2.1.2.2.1.4
5	0.34971400	192.168.1.1	192.168.1.3	SNMP	86	get-next-request	1.3.6.1.2.1.25.3.3.1.2				
6	0.35011000	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	0.35054500	192.168.1.1	192.168.1.3	SNMP	87	get-request	1.3.6.1.2.1.25.2.3.1.5.1				
8	0.35059500	192.168.1.3	192.168.1.1	SNMP	90	get-response	1.3.6.1.2.1.25.3.3.1.2.196608				
9	0.35082900	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	0.35114900	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	0.35147700	192.168.1.1	192.168.1.3	SNMP	87	get-request	1.3.6.1.2.1.25.2.3.1.5.3				
12	0.35165600	192.168.1.3	192.168.1.1	SNMP	90	get-response	1.3.6.1.2.1.25.2.3.1.5.1				
13	0.35193300	192.168.1.1	192.168.1.3	SNMP	87	get-request	1.3.6.1.2.1.25.2.3.1.6.31				
14	0.35213200	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	0.35243000	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	0.35254400	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	0.35333800	192.168.1.1	192.168.1.3	SNMP	89	get-next-request	1.3.6.1.2.1.25.3.3.1.2.196608				
18	0.35390900	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	0.35428000	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	0.35457100	192.168.1.3	192.168.1.1	SNMP	90	get-response	1.3.6.1.2.1.25.3.3.1.2.196609				
21	0.35594400	192.168.1.1	192.168.1.3	SNMP	89	get-next-request	1.3.6.1.2.1.25.3.3.1.2.196609				
22	0.35668800	192.168.1.1	192.168.1.1	SNMP	90	get-response	1.3.6.1.2.1.25.3.4.1.1.262145				
23	0.08546400	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	0.08581600	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	0.08631500	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	0.08632900	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	0.08670600	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	0.08701100	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	0.08701600	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	0.08731600	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	7.80992200	192.168.1.1	192.168.1.4	SNMP	86	get-next-request	1.3.6.1.2.1.25.3.3.1.2				
32	7.81059900	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	7.81065900	192.168.1.1	192.168.1.4	SNMP	87	get-request	1.3.6.1.2.1.25.2.3.1.5.1				
34	7.81114400	192.168.1.4	192.168.1.1	SNMP	90	get-response	1.3.6.1.2.1.25.3.3.1.2.196608				
35	7.81116200	192.168.1.1	192.168.1.4	SNMP	87	get-request	1.3.6.1.2.1.25.2.3.1.6.3				
36	7.81193500	192.168.1.1	192.168.1.4	SNMP	87	get-request	1.3.6.1.2.1.25.2.3.1.5.3				
37	8.12268000	192.168.1.1	192.168.1.4	SNMP	87	get-request	1.3.6.1.2.1.25.2.3.1.6.31				

10.351149000 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: 161 (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:

Pada gambar diatas,dengan menggunakan protocol SNMP ,dimana dengan IP 192.168.1.3 dan Simple network management protocol version : -version -1 , community :public , data : get - response , request -id : 176233 , error status : noerror , error-index :0 , variable-buildings 1.3.6.2.1.25.2.3.1.6.1.

TRAFFIC PADA LINUX



Analisa :

pada traffik pad linux diatas :

warna biru ssh ,warna merah adalah ping, dan taffic dibawah warna biru adalah cpu linux,warna merah adalah memory linux ,warna hijau adalah virtual memory,dan warna kuning adalah disk linux.

Pada ssh linux

- ❖ pada waktu 12.30 dengan kecepatan 3ms , dan pada waktu 13.30 dengan kecepatan 3ms dan menurun dengan kecepatan 2 ms

Pada ping linux

- ❖ pada waktu 12.20 dengan kecepatan 3 ms , waktu 12.30 dengan kecepatan 3 ms , waktu 12.40 dengan kecepatan 3 ms , waktu 12.50 dengan kecepatan 0 ms , dan waktu 13.00 dengan kecepatan 4 ms , waktu 13.10 kecepatan 8 ms , waktu 13.20 kecepatan 3 ms , waktu 13.30 kecepatan 3 ms .

Pada cpu linux

- ❖ Waktu 12.20 dengan presentasi 20 % . waktu 12.30 presentasi 0% , waktu 12.40 presentasi 0% , waktu 12.50 presentasi 60%, waktu 13.00 presentasi 80%, waktu 13.10 presentasi 70 % , waktu 13.10 presentasi 40% , waktu 13.20 presentasi 30 % , waktu 13.30 presentasinya 50%.

Pada memory linux

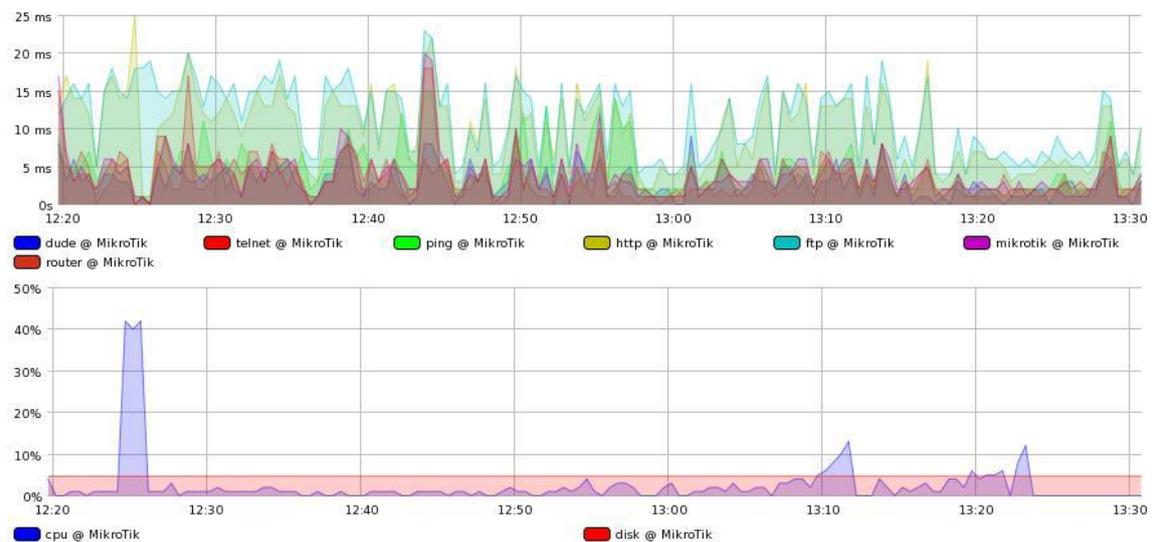
- ❖ Waktu 12.20 dengan presentasi 20 % . waktu 12.30 presentasi 0% , waktu 12.40 presentasi 20% , waktu 12.50 presentasi 20%, waktu 13.00 presentasi 100%, waktu

13.10 presentasi 100 % , waktu 13.10 presentasi 100% , waktu 13.20 presentasi 100 % , waktu 13.30 presentasinya 100%

Pada virtual memory

- ❖ Waktu 12.20 dengan presentasi 20 % . waktu 12.30 presentasi 0% , waktu 12.40 presentasi 20% , waktu 12.50 presentasi 20%, waktu 13.00 presentasi 60%, waktu 13.10 presentasi 60 % , waktu 13.10 presentasi 60% , waktu 13.20 presentasi 60 % , waktu 13.30 presentasinya 60%.

PADA MIKROTIK



Analisa :

pada traffik pada mikrotik diatas :

warna biru dude ,warna merah adalah telnet ,dan warna hijau adalah ping warna kuning adalah http , warna biru adalah ftp , warna ungu adalah mikrotik , warna merah adalah router.

Pada dude

- ❖ pada waktu 12.20 dengan kecepatan 5 ms , waktu 12.30 dengan kecepatan 5 ms , waktu 12. 40 dengan kecepatan 5 ms , waktu 12.50 dengan kecepatan 5 ms , dan waktu 13.00 dengan kecepatan 4 ms , waktu 13.10 kecepatan 5ms , waktu 13.20 kecepatan 3 ms , waktu 13.30 kecepatan 0 ms .

Pada ping

- ❖ pada waktu 12.20 dengan kecepatan 15 ms , waktu 12.30 dengan kecepatan 17 ms , waktu 12. 40 dengan kecepatan 7 ms , waktu 12.50 dengan kecepatan 10 ms , dan

waktu 13.00 dengan kecepatan 0 ms , waktu 13.10 kecepatan 5 ms , waktu 13.20 kecepatan 3 ms , waktu 13.30 kecepatan 2 ms .

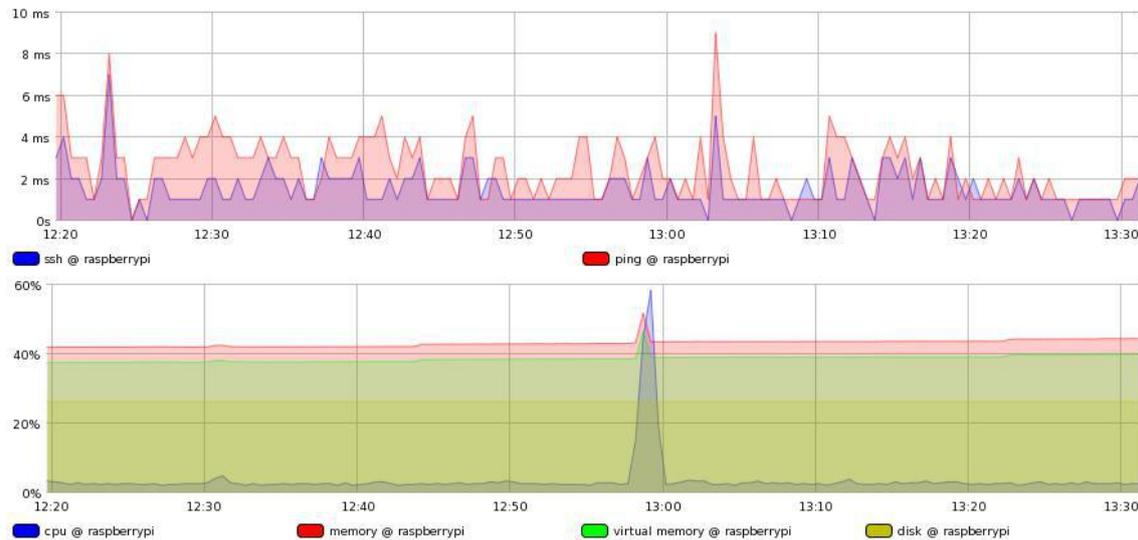
Pada ftp

- ❖ pada waktu 12.20 dengan kecepatan 15 ms , waktu 12.30 dengan kecepatan 5 ms , waktu 12.40 dengan kecepatan 15 ms , waktu 12.50 dengan kecepatan 17ms , dan waktu 13.00 dengan kecepatan 15 ms , waktu 13.10 kecepatan 15 ms , waktu 13.20 kecepatan 10 ms , waktu 13.30 kecepatan 10 ms .

Pada disk

- ❖ pada waktu 12.20, 12.30 , 12.40 ,12.50 , 13.00 ,13.10 ,13.20 ,13.30 presentasi 5%

PADA RASPBERRY PI



Analisa :

pada traffik pada raspberry diatas :

warna biru ssh ,warna merah adalah ping @raspberry ,dan warna biru cpu , warna merah adalah memory , warna hijau adalah virtual memory , warna kuning adalah disk @raspberry.

Pada ssh raspberrypi

- ❖ pada waktu 12.20 dengan kecepatan 6 ms , waktu 12.30 dengan kecepatan 5 ms , waktu 12.40 dengan kecepatan 4 ms , waktu 12.50 dengan kecepatan 3 ms , dan

waktu 13.00 dengan kecepatan 4 ms , waktu 13.10 kecepatan 5ms , waktu 13.20 kecepatan 3 ms , waktu 13.30 kecepatan 2 ms

Pada ping

- ❖ pada waktu 12.20 dengan kecepatan 6 ms , waktu 12.30 dengan kecepatan 5 ms , waktu 12.40 dengan kecepatan 4 ms , waktu 12.50 dengan kecepatan 3 ms , dan waktu 13.00 dengan kecepatan 4 ms , waktu 13.10 kecepatan 5ms , waktu 13.20 kecepatan 3 ms , waktu 13.30 kecepatan 2 ms
- ❖ pada waktu 12.20 dengan kecepatan 6 ms , waktu 12.30 dengan kecepatan 5 ms , waktu 12.40 dengan kecepatan 4 ms , waktu 12.50 dengan kecepatan 3 ms , dan waktu 13.00 dengan kecepatan 4 ms , waktu 13.10 kecepatan 5ms , waktu 13.20 kecepatan 4 ms , waktu 13.30 kecepatan 2 ms

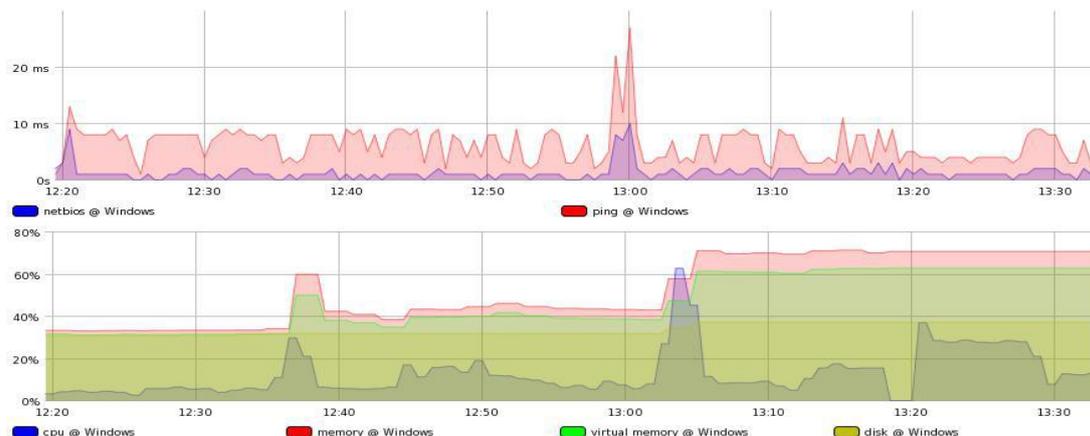
Pada memory

- ❖ Waktu 12.20 dengan presentasi 40 % . waktu 12.30 presentasi 40% , waktu 12.40 presentasi 40% , waktu 12.50 presentasi 40%, waktu 13.00 presentasi 40%, waktu 13.10 presentasi 40 % , waktu 13.10 presentasi 40% , waktu 13.20 presentasi 40 % , waktu 13.30 presentasinya 40%.

Pada virtual memory

- ❖ Waktu 12.20 dengan presentasi 40 % . waktu 12.30 presentasi 40% , waktu 12.40 presentasi 40% , waktu 12.50 presentasi 40%, waktu 13.00 presentasi 40%, waktu 13.10 presentasi 40 % , waktu 13.10 presentasi 40% , waktu 13.20 presentasi 40 % , waktu 13.30 presentasinya 40%.

PADA WINDOWS



Analisa :

pada trafik pada windows diatas :

warna biru adalah netbios , warna merah adalah ping @raspberry ,dan warna biru cpu@windows , warna merah adalah memory@windows, warna hijau adalah virtual memory@windows , warna kuning adalah disk @windows.

Pada ping

- ❖ pada waktu 12.20 dengan kecepatan 12 ms , waktu 12.30 dengan kecepatan 8 ms , waktu 12.40 dengan kecepatan 8 ms , waktu 12.50 dengan kecepatan 7 ms , dan waktu 13.00 dengan kecepatan 27 ms , waktu 13.10 kecepatan 8ms , waktu 13.20 kecepatan 8 ms , waktu 13.30 kecepatan 8 ms.

Pada memory@windows

- ❖ Waktu 12.20 dengan presentasi 30 %. waktu 12.30 presentasi 30% ,waktu 12.40 presentasi 40% , waktu 12.50 presentasi 40%, waktu 13.00 presentasi 40%, waktu 13.10 presentasi 60 % , waktu 13.10 presentasi 40% , waktu 13.20 presentasi 60 % , waktu 13.30 presentasinya 60%.

Pada virtual @windows

- ❖ Waktu 12.20 dengan presentasi 30 %. waktu 12.30 presentasi 30% ,waktu 12.40 presentasi 30% , waktu 12.50 presentasi 40%, waktu 13.00 presentasi 40%, waktu 13.10 presentasi 60 % , waktu 13.10 presentasi 40% , waktu 13.20 presentasi 40 % , waktu 13.30 presentasinya 40%.

Pada disk @windows

- ❖ Waktu 12.20 dengan presentasi 30 %. waktu 12.30 presentasi 30% ,waktu 12.40 presentasi 30% , waktu 12.50 presentasi 40%, waktu 13.00 presentasi 30%, waktu 13.10 presentasi 40 % , waktu 13.10 presentasi 40% , waktu 13.20 presentasi 40 % , waktu 13.30 presentasinya 40%.

KESEIMPULAN

- ❖ SNMP merupakan sebuah protokol jaringan yang didesain bagi pengguna khususnya administrator jaringan untuk memonitor aktifitas jaringan komputer dan mengontrol sebuah komputer atau server secara sistematis dari jarak jauh.

- ❖ *Network Monitoring System* (NMS) merupakan sebuah sub sistem dalam manajemen jaringan (*Network Management System*) yang melibatkan penggunaan perangkat lunak dan perangkat keras.
- ❖ Manajer ini terdiri atas satu proses atau lebih yang berkomunikasi dengan agen-agensya dan dalam jaringan.
- ❖ Manajer akan mengumpulkan informasi dari agen 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.
- ❖ Agent merupakan perangkat lunak yang dijalankan disetiap elemen jaringan yang dikelola
- ❖ Setiap agen mempunyai basis data variabel yang bersifat lokal yang menerangkan keadaan dan berkas aktivitasnya dan pengaruhnya terhadap operasi.