

Monitoring Terintegrasi Jaringan WLAN: Studi Kasus Dormitory Network Telkom University



Umar Ali Ahmad, ST, MT

Program Studi S1 Sistem Komputer – Universitas Telkom

Jl. Telekomunikasi Terusan Buah Batu Bandung

umar@telkomuniversity.ac.id

Abstrak

System monitoring atau sistem pemantauan merupakan fungsi inti sistem administrasi dari sebuah manajemen jaringan komputer. Perangkat monitoring yang baik dapat menginformasikan kepada user terkait potensi masalah mungkin timbul, sehingga penanganan dapat dipersiapkan sedini mungkin. Karakteristik jaringan komputer untuk lingkungan asrama seperti di Universitas Telkom yang terdiri dari gedung bertingkat yang tersebar, membutuhkan fungsi monitoring yang handal, dapat diandalkan, dan mudah dalam pengawasannya. Sehingga penyediaan layanan internet dapat tetap terjaga kualitasnya. Nagios telah menjadi solusi monitoring berbasis open source terkemuka, hanya saja seiring berjalan waktu, telah terjadi perkembangan yang cukup signifikan terkait dengan pengumpulan data dan penjadwalannya. Paper ini menjelaskan penggunaan Nagios sebagai tools monitoring berbasis protokol SNMP pada environment asrama/dormitory, dan penggunaan fungsi alerting untuk masing masing service alert.

Abstract

System monitoring is a core function of the system administration of a computer network management. Good monitoring tools are able to inform the user about the related potential problems that may arise, so every form of treatment could be prepared as early as possible. Characteristic of computer network in dormitory environment such as in Telkom University consist of several building located in different location, so its required monitoring function that are reliable, dependable and easy to control. So the provision of internet services can be maintained its quality. Nagios-based solutions have become the leading open source solution for network monitoring, as the development of the technology, there has been a significant growth for its techniques related to data collection and its scheduling. This paper describes the use of Nagios as a monitoring tool based on SNMP Protocol for high density campus environment such as hostel/dormitory, and the use of alerting function for each service alerts.

Keywords- Nagios, Open Source Monitoring, SNMP, Alerting.

pendahuluan

Sistem pemantauan jaringan komputer saat ini telah mencapai perkembangan yang cukup signifikan, dimana semakin besar area cakupan jaringan yang perlu diawasi, membutuhkan *tools* yang cukup handal untuk dapat mengawasi setiap perangkat dan elemen jaringan, sehingga dapat diambil keputusan sedini mungkin terkait dengan insiden yang memungkinkan terganggunya operasi jaringan komputer. ***System monitoring atau sistem pemantauan merupakan fungsi inti sistem administrasi dari sebuah manajemen jaringan komputer. Perangkat monitoring yang baik dapat menginformasikan kepada user terkait potensi masalah mungkin timbul, sehingga penanganan dapat dipersiapkan sedini mungkin [6]. Semakin lengkap informasi yang disediakan oleh tools monitoring, akan mendapatkan gambaran lebih lengkap terkait cara penanganan masalah yang timbul.***

Sebagai bagian dari penyelenggaraan fasilitas akademik, Universitas Telkom menyediakan 16 Tower Asrama yang diperuntukan untuk mahasiswa tingkat pertama. Selain fasilitas dasar yang disediakan,

penyelenggaraan fasilitas Internet merupakan hal yang penting untuk mendukung fungsi belajar dan mengajar diluar perkuliahan. Untuk mengelola jaringan internet pada Asrama Universitas Telkom membutuhkan mekanisme pengawasan dimana perangkat yang harus dimonitor banyak dan tersebar di beberapa lokasi. Oleh karena itu dibutuhkan system monitoring jaringan komputer atau yang biasa disebut *Network Monitoring System (NMS)* yang mampu mengawasi status perangkat, trafik komunikasi data, dan status penggunaan oleh user, sehingga memerlukan pengambilan keputusan seketika apabila memerlukan tindakan penanganan lebih lanjut yang dapat mempengaruhi penyediaan layanan internet.

Terdapat banyak aplikasi *monitoring* jaringan yang tersedia saat ini, ada yang sifatnya : open source, maupun proprietary. Dalam penelitian kali ini, penulis akan mengulas model *Monitoring System* menggunakan Nagios. Adapun objek pemantauannya adalah pemantauan *host* berupa *wireless access point* yang tersebar di masing masing koridor ruang asrama. Untuk memudahkan pemantauan kinerja dari masing masing *access point* tersebut yang secara fisik tersebar di beberapa lokasi terpisah, sehingga membutuhkan

adanya *system monitoring* yang dapat diandalkan oleh administrasi jaringan dalam menjaga ketersediaan akses secara kontinyu.

Metodologi Penelitian

Jaringan komputer yang baik dapat diukur berdasarkan kinerjanya, adapun kinerja jaringan komputer yang baik menurut Dr. Kornel Terplan [8], manajemen jaringan yang baik antara lain :

- *User Level Criteria* : Kriteria berdasarkan waktu respon (waktu dimana paket dikirim dengan benar) dan kehandalan (keadaan dimana ketersediaan system terjaga pada suatu tugas pengiriman paket data).
- *Network Level Criteria* : Kriteria berdasarkan waktu respon rata rata terhadap penundaan satu jalur paket dan pemakaian link untuk menghitung waktu respon rata rata pemakai.
- *Specific Level Criteria* : Kriteria khusus berdasarkan performansi dan delay.

Selain itu, jaringan yang baik harus mempunyai kemampuan untuk menyembuhkan dirinya sendiri disaat terjadi kegagalan system, atau dapat memberitahukan lebih dini kepada admin jaringan terhadap situasi yang berpotensi mengakibatkan kegagalan tersebut [5].

Nagios merupakan aplikasi monitoring jaringan komputer (*Network, Host, and Services*) yang dapat memberikan informasi secara real time tentang status jaringan dari masing masing *interface* yang terhubung. Nagios di desain untuk beroperasi pada Linux *Operating System*, dan bisa berjalan pada varian Unix lainnya. Nagios diciptakan oleh Ethan Galstad (<http://nagios.org>) dan pertama diluncurkan pada tahun 1999. Nagios mengawasi host host dan servis yang telah ditetapkan, memberi peringatan jika keadaan memburuk, dan memberi tahu kapan keadaan tersebut membaik (*recovered*). [1]

Ketersediaan dalam jaringan komputer seringkali karena adanya masalah yang terjadi dalam jaringan, yang mana terkait dengan konektifitas dan kinerja jaringan itu sendiri. Masalah yang berkaitan dengan konektifitas terjadi apabila suatu *end station* (seperti komputer, *hub*, *switch*, atau *router*) tidak berkomunikasi sebagaimana mestinya, sehingga timbul *lose of connectivity* ataupun *intermittent connectivity*. Masalah kinerja jaringan yang buruk dan tidak segera diperbaiki akan menimbulkan masalah lain yang berdampak jauh lebih besar terutama pada keberlangsungan layanan, untuk itu diperlukan cara dan prosedur yang tepat [2].

Dalam ulasan ini, Nagios diimplementasikan pada sistem operasi Linux Ubuntu versi 13, yang ditempatkan pada level tertinggi (core network) dari jaringan komputer asrama.

Perancangan Sistem

Perancangan Jaringan Akses

Jaringan komputer pada asrama Universitas Telkom didesain agar mampu mengakomodir kebutuhan penghuni asrama, dengan sebaran *user* sebagai berikut :

Informasi	Asrama Putra	Asrama Putri
Jumlah Gedung	8	8
Jumlah Lantai	4 Lt/Gedung	4 Lt/Gedung
Jumlah User	88 User/Lt	88 User/Lt
Total User	2816	2816

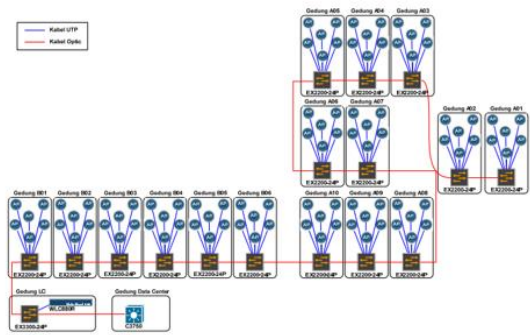
Tabel 1 : Skema distribusi *user*

Dengan pertimbangan akses *backbone* dan kebutuhan material pendukung, topologi yang dipilih adalah topologi *bus*, menggunakan *backbone* serat optik *single-mode 6 core*.



Gambar 1. Topologi Jaringan

Mempertimbangkan kebutuhan bandwidth lokal minimum jika setiap user mendapatkan 1Mbps adalah $5216 \text{ user} \times 1\text{Mbps} = 5,1\text{Gbps}$, sehingga dibutuhkan akses *backbone* dengan kapasitas maksimum 10Gbps. Untuk dapat mengakomodasi akses internet yang dapat diakses oleh seluruh kamar asrama tiap lantai, pilihan memudahkan akses sebagai pertimbangan utama, akses jaringan komputer nirkabel (*wireless*) dipilih untuk meminimalisir perangkat akses yang dibutuhkan. Dengan menggunakan 802.11n dual radio WLAN high-density access point yang mempunyai karakteristik 2x2MIMO, sebuah *access point* mampu mengakomodir antara 40-60 user. Sehingga untuk dapat menjangkau seluruh user di asrama Universitas Telkom diperlukan kebutuhan minimal 16 tower x 4 lantai x 2 AP = 128 Unit *Access Point* (asumsi user tiap lantai antara 50-80 user).



Gambar2 : High Level Design Dorm Network [10]

Selain itu, dalam menghitung kapasitas jaringan dalam standar IEEE 802.11 [9], beberapa hal yang harus diperhatikan antara lain :

- Packet Error Rate
- Jumlah dari Streams
- Channel Bandwidth
- Overhead (Multiple Channel Sharing)
- Background Traffic (beacons, probes, and management application)

Berikut persamaan yang dapat digunakan untuk menghitung waktu transmisi dari paket data tunggal [9] :

$$T_{XTIME} = T_{LEG_PREMABLE} + T_{L_SIG} + T_{VHTSIG-A} + T_{VHT_PREMABLE} + T_{VHTSIG-B} + T_{SYM} \times \left(\frac{T_{SYM} \times N_{SYM}}{T_{SYM}} \right)$$

$$T_{LEG_PREMABLE} = T_{L_STF} + T_{L_LTF}$$

$$T_{VHT_PREMABLE} = T_{VHT_STF} + N_{VHTLTF} \times T_{VHT_LTF}$$

$$N_{SYM} = m_{STBC} \times \left(\frac{8 \times DATA_LENGTH + N_SERVICE + N_{tail} \times N_{EX}}{m_{STBC} \times N_DBPS} \right)$$

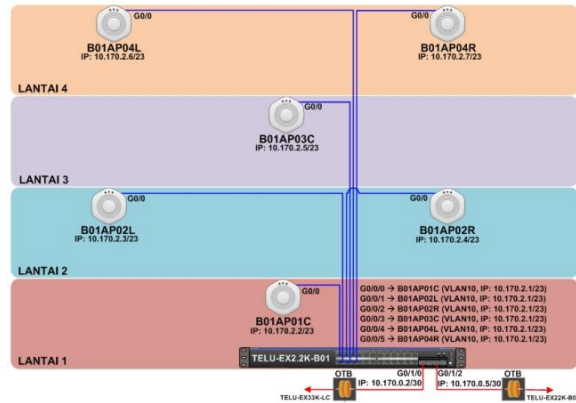
Perancangan Pengalaman Jaringan

Dengan memperhatikan aspek kehandalan system, dimana system harus mudah ditangani apabila terjadi gangguan/kegagalan, untuk itu dirancang pengalaman jaringan asrama (IP Address) yang dapat memudahkan implementasi dan pelaksanaan operasi jaringan komputer. Tipe pengalaman jaringan menggunakan IP Address kelas A yang dipecah kedalam sub-network yang lebih kecil. Dengan memperhatikan desain Sebuah Controller (10.170.1.x/30) sebagai central dari fungsi manajemen access point, dan Core Switch (10.170.1.x/30) yang menjadi terminasi awal dengan ISP, dan distribusi trafik ke setiap gedung, dimana gedung pertama yang terhubung (10.170.2.x/23).

No	Hostname	Interface	IP Address	Subnet	Loopback
1	WLC	G0/0/0	10.170.1.2/30	10.170.1.0/30	
		G0/0/0	10.170.1.1/30	10.170.1.0/30	
2	EX3.3K	G0/1/0	10.254.0.22/30	10.0.0.20/30	9.9.9.32
		G0/1/1	10.170.0.1/30	10.170.0.0/30	
3	B01....16	G0/0/0	10.170.0.1/30	10.170.0.0/30	
	B02....16	G0/0/0	10.170.0.2/30	10.170.0.3/30	9.1.2.1/32

Tabel 2. Pengalaman Jaringan

Untuk mengantisipasi perkembangan jaringan asrama ke depannya, dan memecah traffic broadcast agar tidak menjadi beban di seluruh jaringan, Virtual LAN dipilih sebagai salah satu metoda memecah traffic per masing masing gedung, dan juga untuk menghindari ancaman keamanan jaringan yang datangnya dari user.



Gambar 3. Low Level Design [10]

Perencanaan Kanalisasi & Power Access Point

Untuk menghindari interferensi berlebihan antar access point, pengaturan dilakukan berdasarkan pembagian kanal dan pengaturan Tx Power yang berbeda untuk operasi kanal 2.4GHz, dan kanal 5GHz[4] dengan pengaturan sebagai berikut :

No	Hostname	Channel 2.4GHz	Tx Power 2.4GHz	Channel 5GHz	Tx Power 5 GHz
1	AP01C	1	14	36	16
2	AP02L	6	15	40	16
3	AP02R	11	15	44	16
4	AP03C	1	14	46	16
5	AP04L	11	15	36	16
6	AP04R	6	15	40	16

Tabel 3 : Pengaturan Kanalisasi & Tx Power AP

Dengan konfigurasi pengaturan kanalisasi pada JUNOS [3] sebagai berikut :

```
set ip route default 10.170.1.1
set system name TELU-WLC880R-LC
set system ip-address 10.170.1.2
set system countrycode GB
set service-profile Telkom-University ssid-name TelkomUniversity
set service-profile Telkom-University ssid-type clear
set service-profile Telkom-University proxy-arp enable
set service-profile Telkom-University no-broadcast enable
set service-profile Telkom-University auth-fallthru last-resort
set service-profile Telkom-University backup-ssid mode dual
set service-profile Telkom-University wpa-ie auth-dot1x disable
set service-profile Telkom-University rsn-ie auth-dot1x disable
set service-profile Telkom-University attr vlan-name default
set radio-profile default power-policy max-coverage
set radio-profile default service-profile Telkom-University
set remote-site TELU local-switching mode enable
set remote-site TELU wlc-polling enable
set remote-site TELU cached-config on
set ap 1 serial-id pb3514343386 model WLA322-WW
set ap 1 name B01AP01C
set ap 1 fingerprint
9c:c4:1e:0d:cc:01:28:e8:53:c7:8c:5b:48:22:c4
```

Perancangan Sistem Monitoring

Sistem monitoring berbasis Nagios, diimplementasikan pada operating system LINUX Ubuntu, dengan kapasitas hardware dan software sebagai berikut :

No	Perangkat	Keterangan
1	Processor	Intel Atom Processor D410
2	Memory	1 GB
3	Harddisk	80GB

4	NIC Card	Wireless LAN 802.11a/b/n
5	Sistem Operasi	Ubuntu Server 13.10
6	NMS	Nagios
7	Browser	Google Chrome
8	Database	MySQL
9	Web Server	Apache
10	Scripting Language	PHP

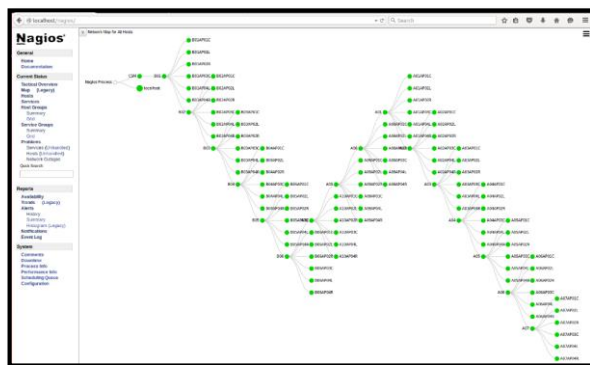
Tabel 4 : Kebutuhan hardware dan software

Instalasi paket pada Ubuntu yang dipakai antara lain : build-essential, apache2, php5-gd, wget, libgd2-xpm, libgd2-xpm-dev, libapache2-mod-php5, daemon. Adapun untuk menambahkan *host* pada system Nagios menggunakan penambahan terminal pada file konfigurasi untuk mendefinisikan *device IP, host, hostname, service, hostgroup, dan service group*.

Hasil Pengujian

Pengujian pada sistem ini dengan cara melakukan pengukuran berbasis protokol SNMP (*Simple Network Management Protocol*). SNMP digunakan untuk mengatur perangkat yang berada dalam suatu jaringan komputer dengan menggunakan protocol TCP/IP, SNMP menggunakan konsep *manager* dan *agent*, dimana *manager* (biasanya berupa *host*) mengendalikan dan memantau sekumpulan *agent*. Untuk mendapatkan informasi yang terdapat pada *database agent (Management Information Based)* dilakukan dengan cara mengakses *query*, dan *agent* akan mengirimkan respon dari *query* tersebut dengan sebuah pesan yang disebut *TRAP* (pesan yang dikirimkan dari *agent* ke *manager* sebagai laporan dari adanya *event*)[2].

Selain SNMP, Nagios juga mendukung pemantauan protokol *service* jaringan lainnya seperti SMTP, POP3, HTTP, NNTP, dll. Berikut adalah tampilan dari antarmuka aplikasi pemantauan jaringan menggunakan Nagios, dimana terdapat 96 buah *access point* yang dijadikan sebagai *host* yang dipantau oleh *manager SNMP (Host Agent)*.



Gambar 4 : Map Access Point Monitoring

Fitur lain yang dapat didukung oleh nagios dalam pemantauan jaringan komputer yaitu : *link traffic, network interface, kapasitas partisi harddisk, beban prosesor, penggunaan memori, space of disk, dan utilisasi CPU*. Map atau Peta merupakan salah satu cara Nagios menampilkan hasil pemantauan pengumpulan data secara *real time* sehingga mampu

menjadikan sebuah *Alert*. Adapun pengumpulan data tersebut disimpan dalam sebuah *database*, yang mana sangat membantu apabila akan dilakukan pengukuran kembali sesuai waktu yang ditentukan.

Ada 3 macam klasifikasi *Alert* pada Nagios, antara lain:

- *Down* : *host* atau *service* dalam keadaan *down* (mati/gagal), ditampilkan keterangan “*check time out*”
- *OK* : *host* atau *service* bekerja normal dan terhubung dengan baik.
- *Warning* : *host* atau *service* dalam keadaan peringatan dimana akan ambang batas minimal yang ditetapkan. (contoh : melebihi minimum *packet loss*)
- *Critical* : *host* atau *service* berada pada situasi kritis dimana sudah melebihi ambang batas minimal yang ditetapkan.

Host	Status	Services	Actions
A03AP01C	UP	1 OK	[Icons]
A03AP02L	UP	1 WARNING	[Icons]
A03AP02R	UP	1 OK	[Icons]
A03AP03C	UP	1 CRITICAL	[Icons]
A03AP04L	UP	1 OK	[Icons]
A03AP04R	UP	1 WARNING	[Icons]

Gambar 5: Monitoring Status Host

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
A03AP01C	91.605% (91.605%)	0.000% (0.000%)	8.395% (8.395%)	0.000%
A03AP02L	91.663% (91.663%)	0.000% (0.000%)	8.337% (8.337%)	0.000%
A03AP02R	91.686% (91.686%)	0.000% (0.000%)	8.314% (8.314%)	0.000%
A03AP03C	91.667% (91.667%)	0.000% (0.000%)	8.333% (8.333%)	0.000%
A03AP04L	91.622% (91.622%)	0.000% (0.000%)	8.378% (8.378%)	0.000%
A03AP04R	91.661% (91.661%)	0.000% (0.000%)	8.339% (8.339%)	0.000%
Average	91.651% (91.651%)	0.000% (0.000%)	8.349% (8.349%)	0.000%

Gambar 6: Monitoring Status Host Groups

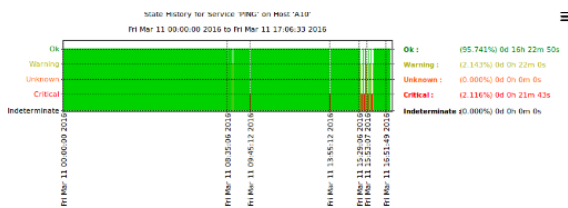
Untuk mendapatkan hasil yang lebih akurat dari sisi pemantauan, pengujian *alerting* dilakukan secara lebih mendalam dari suatu *host* yang akan dipantau. Dalam hal ini penulis melakukan pengujian langsung yang direkam pada tanggal 11 maret 2016 17:00pm, dimana didapat indikator masing masing *host*, berikut status *alerting*. Adapun untuk *service alert* menginformasikan adanya status *warning* untuk *host* yang mendapatkan *ping reply (round trip ping dari host ke agent)* diatas ambang batas Time yang ditetapkan (RTA Result>100ms).

```

[03-11-2016 17:02:11] SERVICE ALERT: A03AP04R:PING:WARNING:HARD:2:PING:WARNING - Packet loss = 0%, RTA = 424.79 ms
[03-11-2016 17:01:24] SERVICE ALERT: A06AP01C:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 7.03 ms
[03-11-2016 17:01:24] SERVICE ALERT: A08AP04R:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 8.19 ms
[03-11-2016 17:01:21] SERVICE ALERT: A03AP01C:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 2.36 ms
[03-11-2016 17:01:21] SERVICE ALERT: A03AP03C:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 2.55 ms
[03-11-2016 17:01:20] SERVICE ALERT: B06AP02R:PING:OK:SOFT:2:PING:OK - Packet loss = 16%, RTA = 5.89 ms
[03-11-2016 17:01:17] SERVICE ALERT: B04AP03C:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 4.96 ms
[03-11-2016 17:01:16] SERVICE ALERT: B06AP04L:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 15.16 ms
[03-11-2016 17:01:13] SERVICE ALERT: A03AP03C:PING:OK:HARD:2:PING:OK - Packet loss = 0%, RTA = 3.38 ms
[03-11-2016 17:01:08] SERVICE ALERT: B03AP02R:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 5.11 ms
[03-11-2016 17:00:46] SERVICE ALERT: B03:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 3.41 ms
[03-11-2016 17:00:44] SERVICE ALERT: B02AP02R:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 9.16 ms
[03-11-2016 17:00:28] SERVICE ALERT: A08AP02R:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 2.10 ms
[03-11-2016 17:00:19] SERVICE ALERT: B03AP03C:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 2.67 ms
[03-11-2016 17:00:15] SERVICE ALERT: B06:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 4.01 ms
[03-11-2016 17:00:15] SERVICE ALERT: A05:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 4.74 ms
[03-11-2016 17:00:14] SERVICE ALERT: A09AP01C:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 2.62 ms
[03-11-2016 17:00:14] SERVICE ALERT: A09AP04L:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 2.32 ms
[03-11-2016 17:00:13] SERVICE ALERT: A03AP04R:PING:CRITICAL:HARD:2:PING:CRITICAL - Packet loss = 16%, RTA = 546.06 ms
[03-11-2016 17:00:12] SERVICE ALERT: B02AP03C:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 2.15 ms
[03-11-2016 17:00:12] SERVICE ALERT: A04AP01C:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 2.44 ms
[03-11-2016 17:00:10] SERVICE ALERT: A04AP02R:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 2.05 ms
[03-11-2016 17:00:09] SERVICE ALERT: A03AP03C:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 2.03 ms
[03-11-2016 17:00:09] SERVICE ALERT: B01AP02R:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 1.92 ms
[03-11-2016 17:00:09] SERVICE ALERT: A03AP02L:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 2.17 ms
[03-11-2016 17:00:08] SERVICE ALERT: A03:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 3.95 ms
[03-11-2016 17:00:05] SERVICE ALERT: A02AP02R:PING:OK:SOFT:2:PING:OK - Packet loss = 0%, RTA = 2.15 ms
    
```

Gambar 7 : Service Alert Nagios

Nagios juga menyediakan fungsi pemantauan yang lengkap, apabila kita menginginkan adanya hasil analisa pengukuran yang lebih mendalam terhadap suatu *host group* yang spesifik, hal ini bisa dipantau melalui fasilitas *state history* untuk masing masing *service* yang dijalankan. Adapun contoh berikut adalah *State History* untuk *service* PING yang dilakukan pada *host* A10, dan didapatkan resume dari performansi layanan PING pada rentang waktu yang ditentukan sesuai dengan status masing masing *service level*.



Gambar 8 : State History Service PING

Nagios menyimpan *history* dari setiap *alert* yang dihasilkan oleh masing masing *host*[7]. Sebagai bagian dari fungsi pengambilan keputusan untuk status masing masing elemen jaringan / *host*, pengambilan data bisa dilakukan dengan *scheduled* (terjadwal) maupun *unscheduled* (Tidak Terjadwal). Dan dapat menampilkan total performansi pemantauan untuk rentang waktu pemantauan yang dimaksud, atau disebut sebagai *alert summary report*. Dengan adanya informasi yang lebih lengkap dari *alert summary report*, pengelola jaringan komputer dapat melakukan evaluasi secara berkala terhadap kondisi jaringan komputer yang dipantau, agar dapat meningkatkan layanan *availability* dan *accessibility* dari layanan jaringan komputer tersebut.

State	Type / Reason	Time	% Total Time	% Known Time
OK	Unscheduled	0d 16h 46m 35s	98.055%	98.055%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 16h 46m 35s	98.055%	98.055%
WARNING	Unscheduled	0d 0h 9m 59s	0.973%	0.973%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 9m 59s	0.973%	0.973%
UNKNOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
CRITICAL	Unscheduled	0d 0h 9m 59s	0.973%	0.973%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 9m 59s	0.973%	0.973%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	0d 17h 6m 33s	100.000%	100.000%

Gambar 9 : Alert Summary Report

Kesimpulan

Pada paper ini telah dibahas beberapa aspek dalam melakukan pemantauan jaringan nirkabel dengan studi kasus pada Asrama Universitas Telkom. Didapat beberapa kesimpulan antara lain :

1. Jaringan komputer yang baik harus memiliki system pemantauan yang dapat diandalkan, dimana dapat diambil pengambilan keputusan secara cepat terkait potensi gangguan ataupun keadaan yang mengakibatkan terganggunya ketersediaan jaringan.
2. Kehandalan sistem bukan merupakan suatu hal yang sifatnya parsial, melainkan menyeluruh. Mulai dari perancangan, sampai dengan implementasi akan menentukan faktor yang dapat membuat pemantauan jaringan komputer tersebut handal.
3. Nagios menyediakan sistem pemantauan yang cukup handal, dimana setiap elemen dari jaringan komputer dapat ditugaskan sebagai *host* ataupun *agent* untuk dilakukan pemantauan secara real time.
4. Status masing masing elemen dapat dibaca dengan kondisi dan juga performansinya, tidak hanya ditampilkan sebagai kondisi *UP* dan *DOWN*, status lain juga bisa ditentukan untuk memonitor apabila berada pada ambang batas minimal (status *critical* dan *warning*).
5. Status yang berpotensi menimbulkan kegagalan fungsi jaringan (*alert*), dapat dilengkapi dengan sebuah parameter minimal untuk setiap *service alert* yang terjadi, sehingga berbagai macam potensi kegagalan terkait dapat diantisipasi sedini mungkin.
6. Hasil pemantauan dapat disimpan dalam sebuah basis data yang lengkap, sehingga dapat dijadikan sumber evaluasi untuk menentukan tren kondisi jaringan, dan pengembangan terkait yang diperlukan untuk meningkatkan ketersediaan sistem yang dapat dipantau dengan sistem pemantauan yang handal menggunakan Nagios.

Saran

1. Setelah memiliki fungsi pemantauan jaringan yang baik, hal selanjutnya adalah melakukan evaluasi secara terus menerus, dan berkala untuk memastikan jaringan komputer berada pada kondisi prima untuk setiap masing masing *service alert*.
2. Peningkatan alert pada tahap selanjutnya adalah berupa notifikasi yang dapat dikirimkan melalui media seperti SMS, *email*, *alarm*, ataupun fitur *messaging* lainnya.
3. Dengan adanya notifikasi tersebut, diharapkan mampu memberikan masukan lebih dini dan real time untuk setiap kondisi jaringan, dan memutuskan penanganannya secara cepat.

daftar pustaka

[1] Ammur, Hidra. Defni, et. Al. "Perancangan dan Implementasi Network Monitoring Sistem

Jurnal ICT Penelitian dan Penerapan Teknologi

- Menggunakan Nagios dengan Email dan SMS Alert". Poli Rekayasa Vol 10, Nomor1, Okt 2014.
- [2] Fatria, Frima Bobby."Pengembangan Fitur Nagios Untuk Pemantauan Jaringan Berbasis SMS (Short Message Service)". Tugas Akhir Sarjana pada Universitas Islam Negeri Sultan Syarif Kasim Riau. 2011
- [3] Juniper Wireless WLA322 Product Documentation.
http://www.juniper.net/techpubs/en_US/release-independent/wireless/information-products/topic-collections/wla-series/wla322/wla322.pdf
[29.2.2012]
- [4] Proxim White Paper. "Voice Over Capacity Wifi Capacity Planning" Proxim Wireless Network. 2004
- [5] Pervilla, Miko. "Using Nagios to monitor faults in a self-healing environment"Helsinki University. 2007
- [6] Reams, Jonathan. "Extensible Monitoring with Nagios and Messaging MiddleWare". 26th Large Installation System Administration Conference (LISA 12). Usenix Associations.2012
- [7] Saputro, Dhani. "Analisis dan Implementasi Sistem Monitoring Jaringan Berbasis Linux Ubuntu Server RT RWNET ARDHANET". STMIK AMIKOM YOGYAKARTA. 2014
- [8] Terplan, Kornel. "Network Management Control". Springer US. 1990
- [9] Timo Vanhatupa, Phd. "Wifi Capacity Analysis For 802.11ac and 802.11n Theory and Practice". Ekahau WiFi Design White Paper. 2013. Pp:9-10
- [10] Uji Terima Laporan Pembangunan Infrastruktur Jaringan Wireless Internet di Asrama Universitas Telkom. PT. Jaringan Solusi Utama. 2015