



**UNIVERSITAS INDONESIA**

**IMPLEMENTASI APLIKASI BERBASIS WEB SEBAGAI  
SISTEM PENDETEKSI ROGUE ACCESS POINT DENGAN  
*WIRED-SIDE SOLUTION***

**SKRIPSI**

**ADITYO ABDI NUGROHO**

**NPM. 0806459665**

**FAKULTAS TEKNIK  
PROGRAM STUDI TEKNIK KOMPUTER  
DEPARTEMEN TEKNIK ELEKTRO  
UNIVERSITAS INDONESIA  
DEPOK**

**JULI 2012**



**UNIVERSITAS INDONESIA**

**IMPLEMENTASI APLIKASI BERBASIS WEB SEBAGAI  
SISTEM PENDETEKSI ROGUE ACCESS POINT DENGAN  
*WIRED-SIDE SOLUTION***

**SKIRPSI**

**Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana**

**ADITYO ABDI NUGROHO**

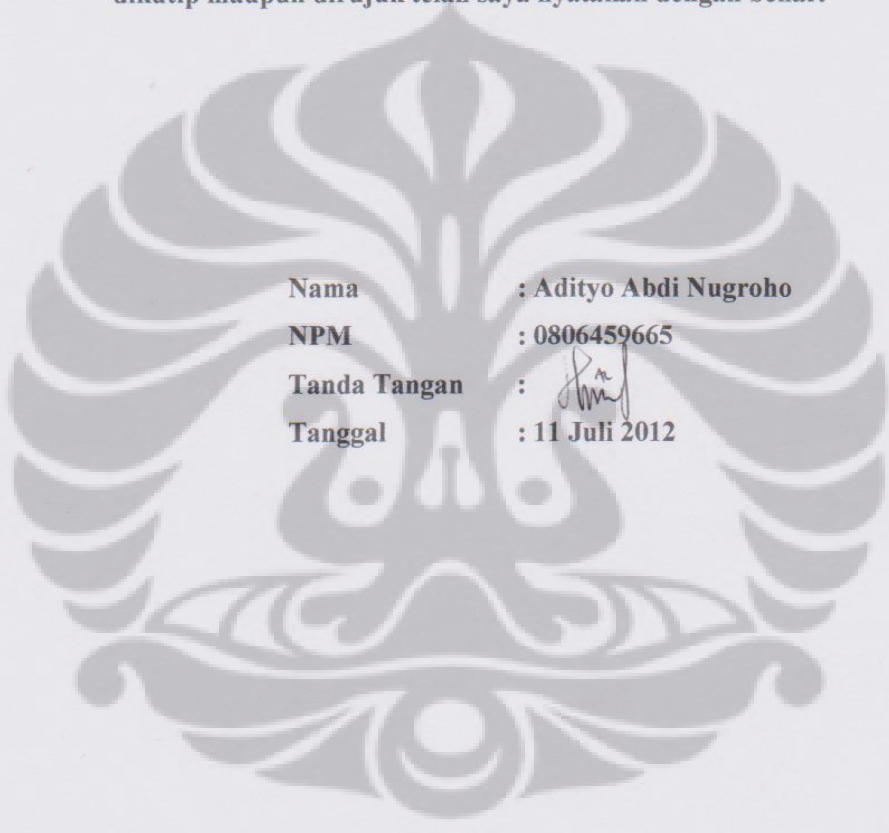
**NPM. 0806459665**


**FAKULTAS TEKNIK  
PROGRAM STUDI TEKNIK KOMPUTER  
DEPARTEMEN TEKNIK ELEKTRO  
UNIVERSITAS INDONESIA  
DEPOK**

**JULI 2012**

## HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.



Nama : Adityo Abdi Nugroho  
NPM : 0806459665  
Tanda Tangan :   
Tanggal : 11 Juli 2012

## HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :

Nama : Adityo Abdi Nugroho  
NPM : 0806459665  
Program Studi : Teknik Komputer  
Judul Skripsi : Implementasi Aplikasi Berbasis Web Sebagai Sistem  
Pendeteksi Rogue Access Point dengan Wired-Side  
Solution

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer, Fakultas Teknik, Universitas Indonesia

### DEWAN PENGUJI

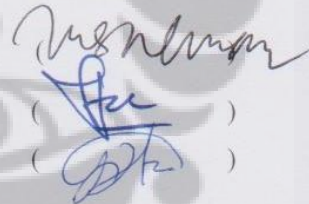
Pembimbing : Muhammad Salman S.T., M.IT

Penguji : Yan Maraden ST. MSc.

Penguji : I Gde Dharma Nugraha ST. MT

Ditetapkan di : Depok

Tanggal : 11 Juli 2012



Three handwritten signatures in blue ink are present. The top signature is the largest and most legible, appearing to be 'Muhammad Salman'. Below it are two smaller signatures, each enclosed in parentheses, likely representing the examiners Yan Maraden and I Gde Dharma Nugraha.

## UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kepada Allah SWT karena hanya dengan rahmat-Nya, saya mampu menyelesaikan skripsi ini. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat menyelesaikan studi Sarjana Teknik Program Studi Teknik Komputer, Fakultas Teknik Universitas Indonesia. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak baik moril maupun material, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada :

1. Muhammad Salman ST, M.IT, selaku dosen pembimbing yang telah bersedia meluangkan waktu, tenaga dan pikiran untuk memberikan pengarahan, diskusi dan bimbingan serta persetujuan penulisan skripsi ini.
2. Teman-Teman S1 Teknik Elektro, khususnya Angkatan 2008 yang telah berjuang bersama, saling memberikan dukungan dan pembelajarannya.
3. Seluruh keluarga dan saudara saya : Ibu saya Renvilla, mas uki, mas kongko, mas bowo, mas sulis, mas yoko, mas pram, mas dwi, mba ria, mba rini, mba yani, mba dewi, mba devi. Dan yang spesial untuk almarhum Ayah saya yang telah memberikan dukungannya.
4. Semua pihak yang tidak dapat penulis sebutkan satu persatu, yang juga memberikan dukungan dalam penyelesaian skripsi ini.

Akhir kata, semoga Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu demi kelancaran penulisan skripsi ini. Semoga tulisan ini membawa manfaat untuk pembaca bagi pengembangan ilmu.

Depok, 11 Juli 2012

Adityo Abdi Nugroho

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI**  
**TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS**

---

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Adityo Abdi Nugroho

NPM : 0806459665

Program Studi : Teknik Komputer

Departemen : Teknik Elektro

Fakultas : Teknik

Jenis karya : Tugas akhir

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif** (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul:

**Implementasi Aplikasi Berbasis Web Sebagai Sistem Pendeteksi Rogue  
Access Point dengan Wired-Side Solution**

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Depok

Pada tanggal: 11 Juli 2012

Yang menyatakan,



( Adityo Abdi Nugroho )

## ABSTRAK

Nama : Adityo Abdi Nugroho  
Program Studi : Teknik Komputer  
Judul : Implementasi Aplikasi Berbasis Web Sebagai Sistem Pendeteksi Rogue Access Point dengan Wired-Side Solution  
Pembimbing : Muhammad Salman, ST, MIT

*Rogue Access Point (RAP)* menjadi salah satu ancaman dalam keamanan jaringan *Wireless Local Area Network (WLAN)*. RAP merupakan perangkat yang menciptakan sebuah jaringan wireless yang tidak dilegitimasi oleh network admin jaringan tersebut. Beberapa metode digunakan untuk mendeteksi RAP, yaitu berbasis hardware misalnya : perangkat sensor khusus untuk mendeteksi keberadaan RAP dan berbasis software, misalnya dibuatnya sistem berbasis aplikasi yang mampu mendeteksi RAP seperti sistem aplikasi berbasis web ini. Ada 2 bentuk model yang dapat terciptanya perangkat RAP yaitu RAP *Unauthorized AP*, RAP *Bridging Connection*. Sistem ini menggunakan 3 parameter yaitu IP, MAC Address dan *Round Trip Time (RTT)*. Parameter ini menjadi penentu terdeteksinya suatu perangkat palsu yang termasuk RAP dalam skala satu jaringan. ketiga parameter itu akan diukur dengan cara membandingkan antara legal dan illegal. Perangkat yang legal telah didaftarkan oleh network admin kemudian melakukan deteksi terhadap jaringan tersebut, setelah itu dilakukan komparasi antara kedua data tersebut, perangkat yang tidak terdefiniskan dalam database merupakan perangkat yang ilegal. Sistem akan memberikan output berupa alarm dalam website. Dari hasil pengujian bahwa, waktu rata-rata *Load Time* yang dibutuhkan 5213.5569 milidetik untuk mendeteksi satu jaringan. Selain itu, juga diketahui bahwa tingkat akurasi sistem untuk model *unauthorized AP* sebesar 53,3% , sedangkan *model Bridging Connection* sebesar 90% mampu mendeteksi secara sempurna.

Kata kunci : RAP, WLAN, Rogue access point, unauthorized AP, Bridging Connection

## ABSTRACT

Name : Adityo Abdi Nugroho  
Study Program : Computer Engineering  
Title : Implementation of Web Application For Rogue Access Point Detection System with Wired-Side Solution.  
Supervisor : Muhammad Salman, ST, MIT

Rogue Access Point (RAP) is one network security threat in Wireless Local Area Network (WLAN). RAP is a device that creates a wireless network that is not legitimized by admin network. Some of the methods used to detect RAP, which is based on hardware such as sensor devices for detecting and RAP-based on software, for example detection system that can detect RAP applications such as web-based application systems. There are two model that RAP-Unauthorized AP and RAP-Bridging Connection. This system uses three parameters, IP, MAC Address and Round Trip Time (RTT). This parameter determines the detection of a prosthetic device that includes a RAP-scale networks. All parameter will be compare between legal and illegal device. Legal devices that have been registered by the network admin and then perform detection on the network, after that, it carried out a comparison between the data, the device is not in the database, It mean that an illegal device. The system will give alarm output from the website. From the results of that testing, the average time needed 5213.5569 milliseconds Load Time to detect a network. In addition, it is also known that the accuracy of a model system for unauthorized APs of 53.3%, while the Connection Bridging the model is able to detect 90% perfectly.

Keyword : *RAP, WLAN, Rogue access point, unauthorized AP, Bridging Connection*



## DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS.....	i
HALAMAN PENGESAHAN.....	ii
UCAPAN TERIMA KASIH .....	iii
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI.....	iv
ABSTRAK .....	v
ABSTRACT.....	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR .....	x
BAB I.....	1
PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Tujuan Penulisan .....	4
1.4 Batasan Masalah.....	4
1.5 Metode Penelitian.....	4
1.6 Sistematika Penulisan.....	5
BAB II.....	6
WIRELESS SECURITY DAN ROGUE ACCESS POINT .....	6
2.1 Wireless Security.....	6
2.1.1 Rogue AP (Rogue Access Point) .....	6
2.1.2 Wireless Intruders .....	7
2.1.3 Misconfigured AP .....	7
2.1.4 Evil Twin AP .....	7
2.1.5 Wireless Phishing.....	8
2.2 Rogue Access Point.....	8
2.3 Klasifikasi Rogue Access Point .....	9
2.4 Tipe Rogue Access Point .....	9
2.5 Struktur Posisi Rogue Access Point .....	10
BAB III .....	13
PERANCANGAN SISTEM DETEKSI ROGUE ACCESS POINT .....	13

3.1	Topologi Jaringan.....	13
3.2	Komponen Perangkat Lunak .....	14
3.2.1	Sistem Operasi .....	14
3.2.2	Program Pembangun <i>Webserver</i> dan <i>Database Server</i> .....	15
3.3	Komponen Perangkat Keras .....	16
3.4	Rancangan Cara Kerja Sistem .....	18
3.4.1	Parameter Pendeteksian Rogue Access Point .....	19
3.4.2	Mode Pendeteksian .....	20
o	Mode Automatic .....	20
o	Mode Manually .....	20
3.4.3	Metoda Pengambilan Nilai Parameter .....	21
3.5	Diagram-Diagram <i>Unified Modelling Language (UML)</i> .....	23
3.5.1	Use Case Diagram.....	23
3.5.2	<i>Activity Diagram</i> .....	24
3.5.3	<i>Sequence Diagram</i> .....	25
3.5.4	<i>Component Diagram</i> .....	26
BAB IV	.....	28
IMPLEMENTASI SISTEM DAN ANALISIS HASIL	.....	28
4.1	Implementasi Sistem Testbed.....	28
4.1.1	Access point .....	28
4.1.2	Internet Akses/IP Public.....	28
4.1.3	Traffic Generator.....	28
4.1.4	Internal LAN .....	29
4.2	Metode RAP .....	29
4.2.1	Access Point ilegal ( <i>Unauthorized AP</i> ).....	29
4.2.2	Bridging Connection .....	30
4.3	Aplikasi Deteksi RAP .....	30
4.4	Server Scripting .....	32
4.5	Pengujian dan Analisa .....	33
4.5.1	Hasil Pengukuran dan Analisa RTT Terhadap RAP dan AP.....	33
4.5.2	Pengukuran Load Time Deteksi Perangkat Online.....	36
4.5.3	Pengukuran Load Time Deteksi Perangkat Offline .....	37

4.5.4	Pengukuran Load Time/Network.....	38
4.5.5	Perbandingan Akurasi Pendeteksian RAP dan AP .....	39
BAB V.....		42
KESIMPULAN.....		42
REFERENSI .....		43
Lampiran .....		45

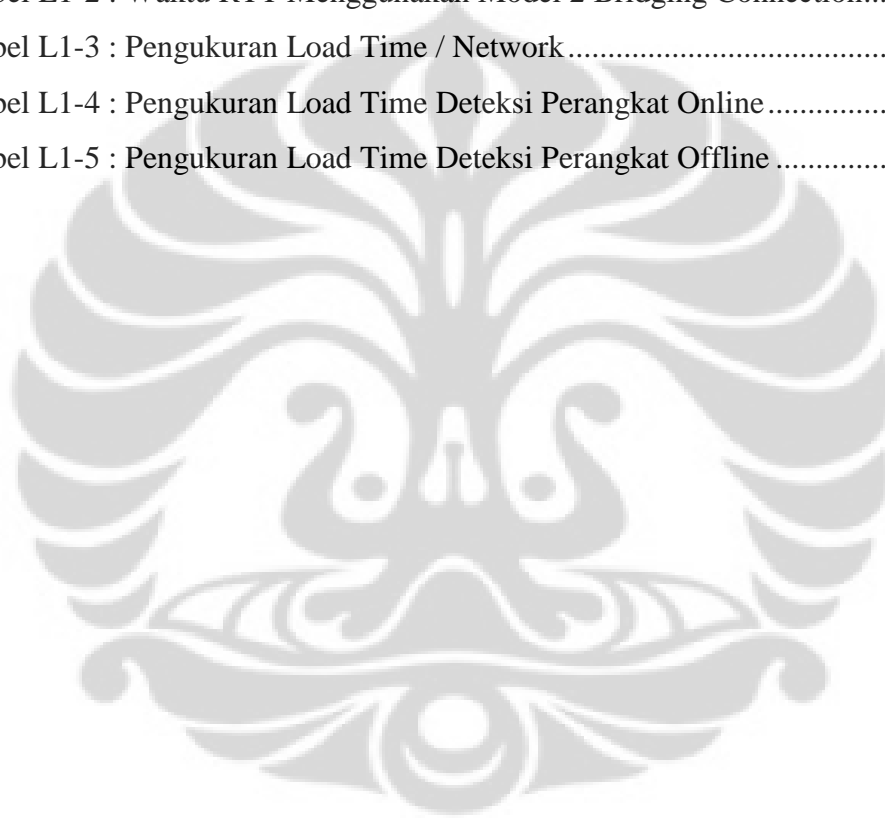


## DAFTAR GAMBAR

Gambar 1-1 : RAP Detection Road Map, dan efektifitas model tipe solusi RAP Detection [13].....	2
Gambar 2-1 : Lapisan Layer Networking [6].....	11
Gambar 2-2 : Posisi umum Rogue Access Point [4].....	12
Gambar 3-1 : Topologi Jaringan .....	14
Gambar 3-2 : Diagram Alur Kerja Secara Umum .....	19
Gambar 3-3 : Alogaritma Mode Response Rogue AP.....	21
Gambar 3-4 : Contoh Ping di command prompt.....	22
Gambar 3-5 : Contoh arp di command prompt.....	22
Gambar 3-6 : <i>Use Case Diagram</i> .....	24
Gambar 3-7 : <i>Activity Diagram</i> .....	25
Gambar 3-8 : <i>Sequence Diagram</i> .....	26
Gambar 3-9 : <i>Component Diagram</i> .....	27
Gambar 4-1 : <i>Topologi Jaringan : Model 1 Unauthorized AP</i> .....	29
Gambar 4-2 : <i>Topologi Jaringan : Model 2 Bridging Connection</i> .....	30
Gambar 4-3 : <i>Interface Add device Form</i> .....	31
Gambar 4-4 : <i>Interface List Device Form</i> .....	32
Gambar 4-5 : <i>Interface Check RAP</i> .....	32
Gambar 4-6 : <i>Pseudocode Server Scripting Deteksi RAP</i> .....	33
Gambar 4-7 : <i>Grafik Perbandingan Waktu RTT antara RAP dan AP melalui model unauthorized</i> .....	34
Gambar 4-8 : <i>Grafik Perbandingan Waktu RTT antara RAP dan AP melalui model Bridging Connection</i> .....	35
Gambar 4-9 : <i>Grafik Pengukuran Load Time Untuk Mendeteksi Perangkat yang Online</i> .....	36
Gambar 4-10 : <i>Grafik Pengukuran Load Time untuk mendeteksi perangkat yang Offline</i> .....	37
Gambar 4-11 : <i>Grafik Pengukuran Load Time untuk mendeteksi perangkat dalam satu network</i> .....	38
Gambar 4-12 : <i>Grafik Perbandingan Akurasi Model Unauthorized AP</i> .....	39
Gambar 4-13 : <i>Grafik Perbandingan Akurasi Model Bridging Connection</i> .....	40

## DAFTAR TABEL

Tabel 2-1 : Klasifikasi Rogue Access Point.....	9
Tabel 2-2 : Rogue AP Taxonomy dan Scenario [10].....	10
Tabel 3-1 : Daftar Alamat IP Perangkat pada Topologi Jaringan.....	13
Tabel 3-2 : Parameter pengukuran dan Potensi Rogue AP .....	20
Tabel L1-1 : Waktu RTT Menggunakan Model 1 <i>Unauthorized AP</i> .....	45
Tabel L1-2 : Waktu RTT Menggunakan Model 2 Bridging Connection.....	45
Tabel L1-3 : Pengukuran Load Time / Network.....	46
Tabel L1-4 : Pengukuran Load Time Deteksi Perangkat Online.....	46
Tabel L1-5 : Pengukuran Load Time Deteksi Perangkat Offline .....	47



# BAB I

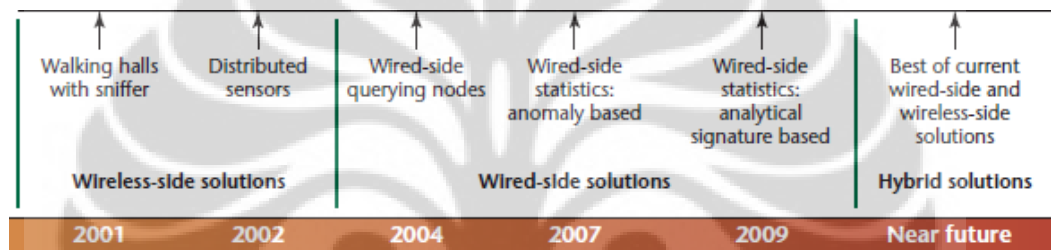
## PENDAHULUAN

### 1.1 Latar Belakang

Wireless Local Area Network (WLAN) telah berkembang dan sudah banyak digunakan diberbagai sektor. Banyak orang yang memperoleh keuntungan dari WLAN seperti kemudahan instalasi, fleksibel, mobilitas, pengurangan pendanaan (*reduced cost*), dan jangkauan yang cukup luas (*Scalability*). Akan tetapi dari berbagai kelebihan yang disebutkan, WLAN memiliki beberapa ancaman keamanan sehingga pengguna harus lebih sadar dalam implementasi jaringan nirkabel (WLAN). Saat Sekarang ini, banyak organisasi, perusahaan, institusi dari berbagai bidang menggunakan jaringan Wireless LAN untuk menyediakan akses internet, seperti Hotspot, dan wi-fi. Hampir 50% dari perusahaan laptop saat ini mendukung WLAN mulai tahun 2006 [1]. Hal itu akan terlihat dari berkembangnya jaringan dari waktu ke waktu yang menjadikan jaringan memiliki fleksibilitas, mobilitas and terintegrasi. Selain itu, karena karyawan atau pegawai yang memiliki mobilitas yang tinggi untuk mampu berpindah dari tempat ke tempat lainnya untuk mendapatkan akses internet sehingga menjadikan alasan WLAN harus segera dikembangkan dan digunakan. Dari kebutuhan itu berbagai teknologi dilakukan untuk melakukan improvisasi jaringan wireless. Sementara itu, komunikasi *peer to peer* dan akses internet harus tetap terpelihara artinya selalu dilakukan *maintenance* agar jaringan yang telah dibuat tidak perlu di instalasi ulang melainkan dijaga dan dipelihara dengan baik. Disamping itu, mengingat keamanan dalam suatu akses jaringan sangat penting agar terhindar dari perusakan atau hal-hal yang tidak diinginkan, maka harus dilakukan perhatian khusus untuk menangani masalah keamanan jaringan.

WLAN memiliki beberapa ancaman keamanan (*Security Threat*) yaitu *Denial of Service*, *spoofing and Session Hijacking*, dan *Eavesdropping* [1]. Dengan cara-cara seperti itu dapat dilakukan perusakan atau pencurian data, selain itu ada yang langsung menyerang para pengguna, salah satunya ialah *Rogue Access Point* . Menurut definisinya Rogue AP ialah Wi-Fi Akses point yang

dibuat oleh *attacker* yang bertujuan untuk melihat akses traffic jaringan (*sniffing wireless network traffic*) [2]. Rogue AP ialah sebuah Akses Point palsu yang tidak legal terkoneksi dalam jaringan yang bertujuan untuk mengambil informasi yang terkandung didalamnya khususnya untuk pengguna. Seiring dengan perkembangan Wireless LAN, Banyak kasus Rogue AP yang meluas ke perusahaan atau institusi. Yang mana bertujuan untuk mengontrol atau mengambil informasi dari pengguna. Akibat yang didapatkan pengguna atau perusahaan jika Rogue AP ini berhasil dilakukan ialah *MAC Spoofing*, pengambilan data/informasi yang bersifat rahasia, dan perusakan sistem. Berita ini sering dibahas pada beberapa waktu lalu untuk diberikan solusi dan cara/metode untuk mengurangi kejadian Rogue AP yang merugikan pengguna atau perusahaan.



Gambar 1-1 : RAP Detection Road Map, dan efektifitas model tipe solusi RAP Detection [13]

Seperti dalam gambar 1.1 penyerangan menggunakan Rogue AP sudah banyak dan banyak pula yang telah membuat solusi dengan segala macam kelemahan dan kelebihan yang dimiliki. Dibutuhkan suatu rancangan sistem yang lebih baik untuk mendeteksi Rogue AP. Salah satunya ialah konsep sistem pendeteksi *Rogue Access Point*. Pada umumnya, RAP dideteksi menggunakan perangkat lunak/keras menggunakan 3 macam pendekatan. Pertama menggunakan Pendekatan *wireless*, Pendekatan *Wired*, dan Pendekatan *Hybrid*. Dari ketiga pendekatan tersebut sebagian besar deteksi RAP dilakukan dengan melibatkan peran dari Network administrator dan memerlukan *deployment* perangkat deteksi RAP kedalam infrastruktur jaringan yang akan dideteksi [11]. Perangkat deteksi umumnya sangat mahal dan sulit untuk digunakan untuk semua kalangan. Oleh karena itu, penulis memiliki gagasan untuk merancang sebuah sistem yang mudah berbasis web untuk mendeteksi melalui pendekatan berbasis kabel (*wired*). *Wired-side*

*solution* menjadi salah satu cara yaitu melakukan manajemen jaringan dengan memanfaatkan parameter yang dimiliki oleh masing-masing perangkat.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya bahwa ancaman yang didapat dari Rogue AP ini cukup variatif, khususnya untuk pengguna dari suatu perusahaan atau institusi yang primitif. Pencurian informasi menjadi sangat mudah dilakukan jikalau tidak dilindungi dengan keamanan jaringan yang baik. Oleh karena itu, dibutuhkan cara atau metode untuk mendeteksi Rogue AP. Deteksi RAP dipilih melalui pendekatan kabel (*wired*). *Wired-Side Solution* memanfaatkan parameter yang dimiliki untuk mendeteksi perangkat yang bersifat ilegal. Sampel kasus diambil dalam area *Network Administrator* dalam menjaga keamanan jaringannya, khususnya dari ancaman Rogue AP. Pada umumnya, dari sisi *wired* Rogue AP itu tercipta dalam suatu jaringan melalui distribusi layer yang sama. Ada 2 model RAP dilihat melalui pendekatan *wired* :

- *Attacker* menggunakan *Wireless Access Point* dari berbagai merk (Cisco, TP-Link, D-Link) untuk menciptakan jaringan nirkabel (*wireless*) baru, model ini disebut juga model *Unauthorized AP*
- *Attacker* menggunakan PC Client (laptop atau PC Desktop) dengan bantuan *Wireless Card* untuk menciptakan jaringan nirkabel (*wireless*) baru (*bridging Connection*). Model ini disebut juga model *Bridging Connection*

Oleh karena itu, akan dibuat sebuah sistem yang mampu melakukan manajemen jaringan, pendeteksian Rogue AP dan dibuatkan dalam bentuk antarmuka website, untuk mempermudah *network administrator* dalam menganalisa keadaan jaringan.



### 1.3 Tujuan Penulisan

Tujuan dari penelitian ini adalah :

1. Membangun sebuah sistem yang mampu mendeteksi *Rogue Access Point* menggunakan pendekatan *wired* dengan cara membandingkan parameter-parameter dan hasilnya akan divisualisasikan dalam bentuk website yang akan digunakan oleh network administrator untuk melakukan tindakan lebih lanjut.
2. Mengukur Akurasi dan efektivitas deteksi *Rogue Access Point* menggunakan pendekatan *wired* melalui parameter-parameter tertentu.

### 1.4 Batasan Masalah

Seperti yang dijelaskan di latar belakang bahwa batasan masalah akan lebih spesifik dan berfokus untuk satu kasus yang dibentuk dalam 2 model RAP yaitu *unauthorized AP* dan *Bridging Connection*. Seorang *network administrator* sebagai *super user* jaringan tersebut menjadi pengontrol jaringan. Kemudian pendeteksian RAP dilakukan dengan mengumpulkan identitas informasi dari sebuah perangkat melalui pendekatan *wired*. Menurut definisi Rogue AP ialah AP yang tidak terdefiniskan/bersifat ilegal dalam jaringan yang telah dibuat oleh *network administrator*. *Network administrator* memiliki database perangkat dimana masing-masing dari perangkat memiliki identitas informasi berisi IP, MAC dan RTT.

### 1.5 Metode Penelitian

Metode penelitian yang digunakan dalam penulisan skripsi ini ialah studi literatur , perancangan dan *testbed*. Studi literatur dilakukan dengan mencari, mengembangkan dan mendiskusikan isu dan masalah yang ada dalam bidang Teknologi informasi khususnya jaringan. Selain itu, akan menjadi teori awal yang digunakan untuk melakukan perancangan simulasi/testbed, setelah itu juga dilakukan analisa dari keadaan jaringan, Rogue AP, dan *resource*. Perancangan yang dilakukan ialah dengan memilih metode yang tepat dengan merancang beberapa topologi untuk *testbed* yang mungkin digunakan sebagai percobaan serta

menghasilkan data-data yang valid dan mampu dilakukan. *Testbed* ialah melakukan percobaan dengan membuat rancangan jaringan yang sama lengkap dengan *attacker* dan sistem deteksi dan tindakan lanjut Rogue AP. Testbed dilakukan sesuai standar, artinya minimal memiliki keadaan jaringan (*testbed*) yang sama dengan keadaan jaringan sebenarnya.

## 1.6 Sistematika Penulisan

Sistematika dari penulisan skripsi ini adalah sebagai berikut:

### Bab 1 PENDAHULUAN

Berisi Latar Belakang sebagai dasar penelitian, perumusan masalah, tujuan penulisan, batasan penelitian, dan Sistematika Penulisan.

### Bab 2 TINJAUAN PUSTAKA

Bab ini memberikan pengantar mengenai berbagai teori yang digunakan dalam perancangan sistem, yang terdiri dari bahasan mengenai Dasar jaringan, WLAN, definisi serta ancaman dan keadaan rogue AP. Dasar teori ini ialah modal awal untuk dapat melakukan perancangan.

### Bab 3 PERANCANGAN

Bab ini membahas mengenai metodologi rancang testbed sistem deteksi dan tindakan lanjut yang berisi flow chart, algoritma. Selain itu, membuat skenario sesuai paramater/variabel yang digunakan untuk *testbed*.

### Bab 4 IMPLEMENTASI DAN ANALISIS

Bab ini dibahas mengenai implementasi sistem deteksi Rogue AP, berupa beberapa metode pengujian yang dilakukan. Bentuk implementasinya ialah dilakukan *testbed* dengan mengkondisikan keadaan jaringan sesuai parameter tertentu. Analisis hasil diperlihatkan dalam bentuk grafik.

### Bab 5 KESIMPULAN

Bab ini berisikan kesimpulan dari hasil pengujian yang telah dilakukan.

## BAB II

### WIRELESS SECURITY DAN ROGUE ACCESS POINT

#### 2.1 Wireless Security

Wireless Local Area Network (WLAN) sedang berkembang dan banyak digunakan oleh pengguna internet. Implementasi WLAN sudah dilakukan oleh beberapa perusahaan dan institusi dari berbagai bidang, pendidikan, pemerintahan, perdagangan dan lain-lain. Alasan penggunaan WLAN ialah menyediakan pengguna untuk dapat akses internet/mendapatkan informasi di lokasi manapun karena bersifat mobilitas yang tinggi, beberapa perusahaan dan institusi lebih banyak memilih dan menggunakan WLAN. WLAN tidak terbatas oleh geografis atau batasan luas wilayah. WLAN menyediakan fleksibilitas untuk para pengguna termasuk untuk kolaborasi yang dapat diakomodasi oleh *wireless* yang dapat mencakup client yang lebih banyak. Disamping itu, dari kelebihan dari WLAN, ada ancaman yang mengakibatkan WLAN tidak fungsional, tidak reliable, dan tidak terlindungi dengan baik. Beberapa ancaman keamanan WLAN (*security attack*) sudah banyak dilakukan dari waktu ke waktu, dimana berbanding lurus dengan evolusi dari keamanan jaringan (*security network*). Ada 5 Ancaman keamanan jaringan WLAN, yaitu :

##### 2.1.1 Rogue AP (Rogue Access Point)

*Attacker* masuk kedalam jaringan dengan cara penetrasi menggunakan AP palsu. Penetrasi dapat dilakukan dengan menyamakan antara *Legitimate AP* dan *Unlegitimate AP* sehingga pengguna tidak mengetahui mana yang benar dan yang salah. Luas dan banyaknya bagian dari perusahaan mengakibatkan sulitnya melakukan pendeksian, beberapa menggunakan perangkat tambahan untuk dapat mendeteksi perangkat yang palsu (RAP). Hal itu cukup efektif mengurangi Rogue AP, ditambahkan WIPS mampu membedakan antara perangkat *legitimate* dan *Unlegitimate*. Dengan cara itu perangkat yang palsu akan terdeteksi dan dilakukan suatu pemblokiran akses, sehingga RAP secara tidak langsung tidak akan terhubung kembali.

### 2.1.2 Wireless Intruders

Wireless IPS produk seperti Motorola AirDefense, AirMagnet, dan perangkat lainnya juga dapat mendeteksi *Unlegitimate AP* yang beroperasi di suatu area yang umum, area perusahaan, instansi atau tempat umum. *Wireless Intruder* lebih cenderung mencari target tertentu dalam area yang bersifat umum, dan menggunakan *resource* atau akses internet. Namun, jika menggunakan WIPS sensor jaringan *wireless* untuk mampu memiliki keamanan jaringan yang efektif memerlukan *update* database yang akan digunakan WIPS sensor. Secara khusus, 802.11a/b/g sensor harus diperbarui untuk memantau saluran baru 5 GHz, 802.11n, dan mencari metode-metode serangan baru 802.11n . karena 802.11n mampu menjangkau lebih jauh.

### 2.1.3 Misconfigured AP

AP dilakukan konfigurasi oleh network admin untuk dapat mampu berfungsi sesuai kebutuhan. Fungsional konfigurasi AP menjadi hal yang sangat vital untuk keamanan AP. Kesalahan konfigurasi menimbulkan ancaman keamanan yang signifikan. Sebagian besar perusahaan WLAN yang dikelola terpusat memiliki kordinasi atau audit secara berkala terhadap konfigurasi atau *maintenance* AP tujuannya ialah meningkatkan kehandalan, dan mengurangi risiko. Selain itu, dibutuhkan dokumentasi untuk setiap konfigurasi AP, sehingga memudahkan network admin untuk *maintenance* dan mencari kesalahan dalam konfigurasi.

### 2.1.4 Evil Twin AP

AP palsu dapat dengan mudah dibuat dengan nama jaringan yang sama (SSID) sebagai hotspot yang asli atau sah dan dekatnya *client* di area Wi-Fi mengakibatkan *client* terhubung secara prioritas. Dengan nama SSID yang sama atau mengkloningkan AP tetangganya membuat *client* tidak mampu membedakan antara yang *Legitimate* atau *unlegitimate*. Software yang berbasis *opensource* juga sudah banyak menyediakan untuk kemungkinan pembuatan *evil twin AP*. Tidak hanya itu, penggunaan hardware yang tidak sulit juga dapat memudahkan *attacker* untuk menciptakan AP ini, bahkan, melalui rute atau sumber yang sama dengan yang aslinya.

### 2.1.5 Wireless Phishing

Selain metode *man in the middle*, serangan wireless berbasis aplikasi juga dilakukan oleh *attacker* yang terus mengembangkan metode baru yaitu Wi-Fi *Phishing*. Sebagai contoh, *attacker* meracuni Wi-Fi cache browser Web klien, selama melakukan penyerangan dapat masuk ke dalam sesi Web masa lalu (*history*) atau seperti dengan menggunakan Evil Twin di sebuah hotspot terbuka. Setelah diambil data *history*, kemudian *client* diarahkan ke situs *phishing* lama setelah meninggalkan area hotspot, bahkan ketika terhubung ke jaringan lainnya. Salah satu teknik untuk mengurangi ancaman ini adalah menghapus cache browser *client* setelah selesai menggunakan internet.

### 2.2 Rogue Access Point

Keamanan jaringan menjadi topik perbincangan yang cukup banyak dalam perkembangan teknologi jaringan. Satu dari banyaknya tantangan terhadap keamanan jaringan dalam IT saat ini ialah *Rogue Access Point*. Sebagai standarisasi yang cukup banyak dan berkembang secara cepat, saat ini teknologi yang digunakan untuk standarisasi ialah 802.11 yang telah menjadi lebih populer, lebih murah dan mudah digunakan oleh pengguna atau instalasi, disamping itu ancaman terhadap jaringan di perusahaan-perusahaan dan tempat lainnya juga ikut meningkat sehingga memunculkan standar yang lainnya yaitu 802.11 a/b/g/n untuk menuntut kesempurnaan keamanan jaringan *wireless*.

*Rogue Access Point* terkadang didefinisikan sangat sederhana, yaitu Access point yang diletakan secara bebas dan tidak terotorisasi dan menggunakan SSID yang sama atau mirip, padahal tidak sesederhana itu dalam kenyataannya. *Rogue Access Point* dapat lebih kompleks dari itu dan dengan metode-metode yang baru dan sulit. *Rogue Access Point* adalah Wi-fi Access Point yang terhubung ke dalam jaringan anda tanpa otorisasi (*Authorization*). *Rogue Access point* itu berada diluar dari manajemen jaringan administrator dan kebijakan keamanan jaringan. Sebuah *Rogue Access Point* mengizinkan siapapun pengguna yang memiliki teknologi Wi-fi (perangkat NIC Card) untuk terhubung kedalam suatu jaringan. IT *Resources* menjadi hal yang sangat rentan untuk dilakukan manipulasi termasuk kejahatan dalam jaringan (*Sniffer, criminal hacker*).[3]

### 2.3 Klasifikasi Rogue Access Point

Access Point dapat dibagi menjadi dua kategori: Access Point yang baik (*Good*) dan jahat (*Rogue*). Access Point yang baik biasanya mampu menyediakan layanan-layanan secara baik seperti akses Internet untuk pengguna yang memiliki Wireless Card, layanan DHCP, Layanan Sharing data dan lain-lain. Sebelum dapat terhubung antara Node nirkabel (Wireless Card) dibutuhkan informasi jaringan untuk mengakses layanan-layanan melalui Access Point. Informasi jaringan tersebut adalah: alamat IP, subnet mask yang membagi bit untuk jaringan dan host, gateway dan alamat IP dari sistem nama domain (DNS) server.

Semua jaringan *wireless* yang menggunakan media perangkat AP dapat diklasifikasikan berdasarkan Valid, Interfering, Known Interfering, Suspect-Unsecured, Unsecured/Rogue, or Denial Of Service (DoS).

Tabel 2-1 : Klasifikasi Rogue Access Point

Tipe Access Point	Deskripsi
<b>Valid AP</b>	Sebuah AP yang telah dikendalikan dari pusat dan telah diberi tanda valid secara manual.
<b>Interfering AP</b>	Sebuah <i>Unlegitimate AP</i> , tetapi belum dikategorikan sebagai AP yang bersifat jahat, karena hanya diklasifikasikan sebagai pengganggu.
<b>Known-Interfering AP</b>	Sebuah <i>Unlegitimate AP</i> secara manual yang diklasifikasikan sebagai pengganggu. Seperti <i>Legitimate AP</i> , dan secara otomatis juga bukan disebut sebagai Access Point yang bersifat jahat
<b>Suspect Unsecured AP</b>	Sebuah <i>Unlegitimate AP</i> yang dapat menjadi AP Jahat, tetapi kepastian tidak 100%
<b>Rogue AP</b>	Sebuah <i>Unlegitimate AP (fixed)</i> yang mentransmisikan frame yang menjadi pengganggu dari alamat MAC yang valid (jika bekerja di Layer 2), atau yang dapat mengganggu alamat IP (jika Bekerja di Layer 3).
<b>DoS</b>	Sebuah <i>Unlegitimated AP</i> yang secara manual telah bersifat jahat dengan cara melakukan penghentian suatu layanan.

### 2.4 Tipe Rogue Access Point

*Rogue Access Point* merupakan salah satu ancaman terbesar dalam keamanan jaringan khususnya pada WLAN. Bahkan, dalam beberapa waktu hampir 20% dari perusahaan telah terinfeksi Rogue AP [9]. Sama halnya, konfigurasi AP yang tidak benar dan *phising AP* dan dideteksi seperti ancaman

keamanan yang sama sekali dimanipulasi oleh *attacker*. Bagaimanapun, hal seperti itu juga dapat dianggap sebagai Rogue AP, dan lebih pentingnya lagi sebenarnya ada beberapa tipe rogue AP yang disebut *compromised AP*, yang mana tipe itu yang paling bahaya karena dapat selalu ikut serta dalam komoditas jaringan WLAN. Karena tipe *compromised AP* ini ialah tipe perusak, atau punya niat yang tidak baik, sehingga akan selalu dilakukan cara apapun untuk merusak. Cara yang dilakukan berbeda-beda untuk menjadi *Rogue Access Point*, untuk lebih detail taxonomy Rogue AP ialah sebagai berikut :

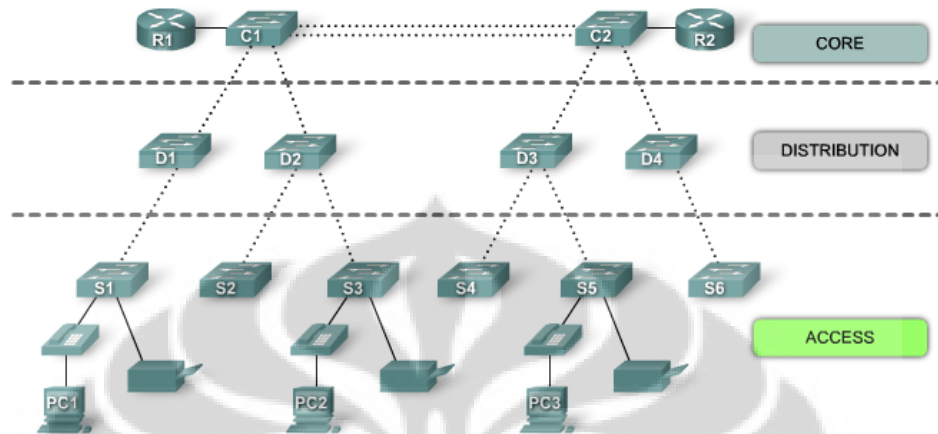
Tabel 2-2 : Rogue AP Taxonomy dan Scenario [10]

Rogue AP Class	Kemungkinan cara yang dilakukan ( <i>Possible Scenarios</i> )
1. Improperly Configured	Tidak cukup menguasai keamanan jaringan, kerusakan pada driver, cacat fisik perangkat, adanya multi NIC CARD
2. Unauthorized	Koneksi internal LAN tanpa persetujuan, Eksternal AP yang mirip dengan aslinya.
3. Phising	Pengelabuhan oleh musuh atau membuat sesuatu yang secara fisik sama, namun isinya berbeda.
4. Compromised	Pengungkapan keamanan jaringan yang dilakukan oleh <i>attacker</i> untuk target.

## 2.5 Struktur Posisi Rogue Access Point

Sebuah Access Point bekerja pada area access network, dimana access point ini berdekatan dengan *end user*. Desain jaringan hirarki melibatkan membagi jaringan ke dalam lapisan diskrit. Setiap lapisan menyediakan fungsi tertentu yang mendefinisikan perannya dalam jaringan secara keseluruhan. Dengan memisahkan berbagai fungsi yang ada pada jaringan, desain jaringan menjadi modular, yang memfasilitasi skalabilitas dan kinerja. Model desain khas hirarki dibagi dalam tiga lapisan: *Access*, *Distribution*, dan *Core*. Dalam urutan *Physical Network*, layer core network itu merupakan jaringan backbone yang merupakan pusat jaringan, layer distribution network merupakan area distribusi jaringan, karakteristiknya ialah menggunakan perangkat router, switch layer 3 atau sejenisnya dan layer

access network ini ialah jalur yang memberikan akses kepada user, karakteristiknya ialah menggunakan perangkat switch, dan access point, atau sejenisnya. Seperti halnya switch di kabel , Access Point memiliki peran yang sama dalam memberikan akses jaringan untuk pengguna.



Gambar 2-1 : Lapisan Layer Networking [6]

#### - Core Layer

Desain hirarki dari *Core Layer* adalah backbone yang berkecepatan tinggi dari *internetwork*. Dimana Backbone adalah bagian dari suatu jaringan yang menjadi sebagai jalur utama traffic dari sumber (*Sources*) atau tujuan (*destination*) dan menuju jaringan lainnya . *Internetwork* dikenal juga sebagai internet, atau jaringan yang terkoneksi dengan router dan perangkat lainnya yang berfungsi secara umum sebagai sebuah jaringan sendiri (*single network*).[6]

#### - Distribution Layer

*Distribution Layer* mendapatkan data yang diterima dari lapisan akses switch (*Access Layer*) sebelum ditransmisikan ke lapisan inti (*Core Layer*) untuk *routing* ke tujuan akhir. *Distribution Layer* mengontrol arus lalu lintas jaringan dengan menggunakan kebijakan dan *broadcast domain* yang mana dilakukan oleh fungsi *routing* antara virtual LAN (VLAN) yang didefinisikan pada *Access layer* . VLAN memungkinkan Anda untuk segmen lalu lintas pada beralih ke subnetwork yang terpisah. Sebagai

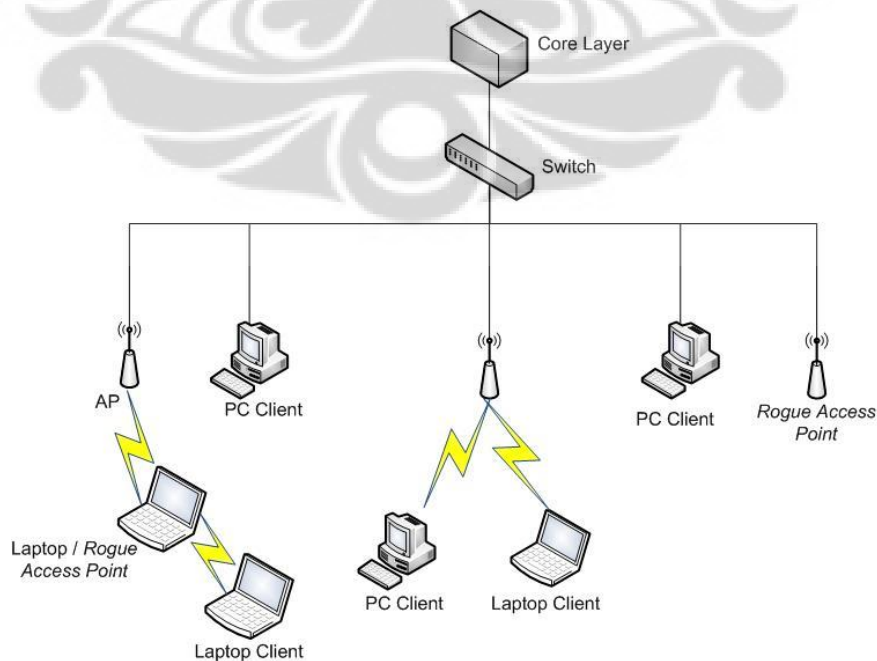


contoh, di universitas, Anda bisa memisahkan lalu lintas sesuai dengan fakultas, mahasiswa, dan tamu. *Distribution Layer* switch biasanya tinggi kinerja perangkat yang memiliki ketersediaan tinggi dan redundansi untuk memastikan kehandalan. Anda akan mempelajari lebih lanjut tentang VLAN, *broadcast domain*, dan inter-VLAN routing kemudian dalam kursus ini. [6]

#### - Access layer

*Interface Access Layer* dengan perangkat akhir, seperti PC, printer, dan telepon IP, untuk menyediakan akses ke seluruh jaringan. *Access Layer* dapat termasuk router, switch, *bridge*, hub, dan jalur akses nirkabel (*Access Point*). Tujuan utama dari lapisan akses adalah untuk menyediakan sarana untuk menghubungkan perangkat ke jaringan dan mengendalikan perangkat yang diizinkan untuk berkomunikasi pada jaringan.[6]

*Rogue Access Point* seperti yang didefinisikan sebelumnya bahwa ada banyak kemungkinan posisi dari *Rogue Access Point*, yaitu ada yang tergabung dalam satu sumbu access network yang sama, atau berbeda access network tetapi dalam *Core* dan *Distribution layer* area yang sama.



Gambar 2-2 : Posisi umum Rogue Access Point [4]

## BAB III

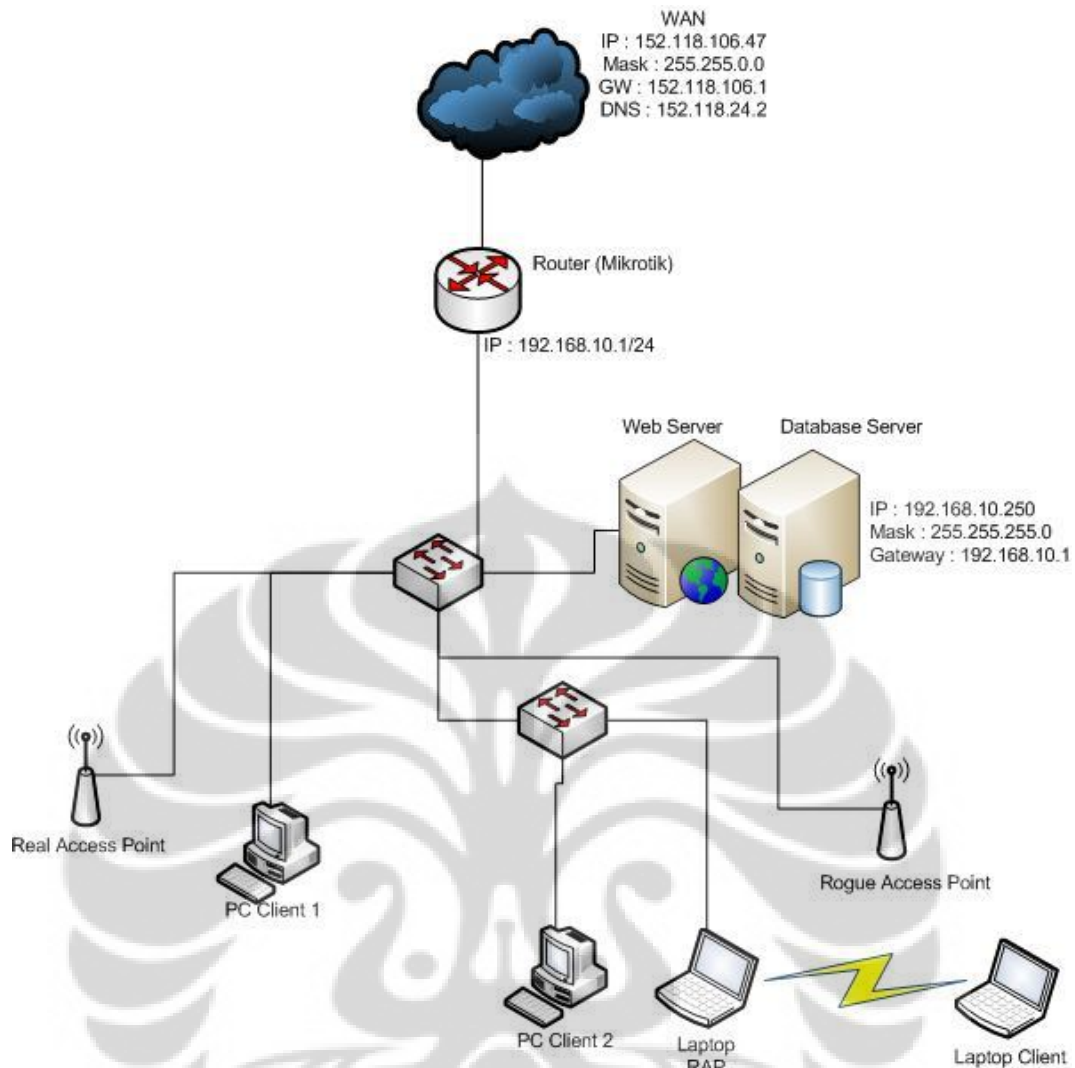
### PERANCANGAN SISTEM DETEKSI ROGUE ACCESS POINT

#### 3.1 Topologi Jaringan

Model topologi jaringan dirancang memiliki keadaan yang sama dengan keadaan sebenarnya. Dari penjelasan sebelumnya disebutkan bahwa ada 2 tipe jenis *Rogue Access Point* pada umumnya, sehingga sistem deteksi ini diharapkan dapat mencakup keduanya. Pengujian pada tugas akhir ini terdiri dari perangkat-perangkat yang terhubung satu sama lain di jaringan Mercator Multimedia Laboratory Engineering Center Universitas Indonesia. Topologi jaringan dibuat seperti jaringan pada umumnya atau yang sering digunakan institusi, laboratorium, dan perusahaan. Komposisi topologi jaringan terdiri dari *PC Client*, *Switch*, *server*, *Router* dan *AP*. *Server* terdiri dari 2 fungsi yaitu *Web Server* dan *Database Server*. Jaringan. Untuk akses internet di jaringan lokal, *Router* mendapatkan IP Statis 152.118.106.47/16 yang merupakan IP Public dari Universitas Indonesia. *Router* akan melakukan *Network Address Translation* untuk jaringan lokal sehingga membentuk jaringan lokal dengan *Network* 192.168.10.0/24. IP lokal yang diberikan *client* bersifat *Dynamic* yaitu menggunakan *DHCP Service*.

Tabel 3-1 : Daftar Alamat IP Perangkat pada Topologi Jaringan

No.	Nama Perangkat	Alamat IP/Netmask	Keterangan
1	Router : Ethernet to Public	152.118.106.47/16	Ethernet 1
2	Router : Ethernet to local	192.168.10.1/24	Ethernet 2
3	Server	192.168.10.250/24	
4	Client (PC, Laptop, AP)	192.168.10.2-254/24	IP exclude : 192.168.10.250/24 (IP Server)



Gambar 3-1 : Topologi Jaringan

## 3.2 Komponen Perangkat Lunak

### 3.2.1 Sistem Operasi

#### - Windows

Semua perangkat yang masuk dalam topologi jaringan kecuali router menggunakan Sistem operasi windows XP Service Pack 3 32-bit. Sistem operasi ini dipilih dengan pertimbangan karena konfigurasi jaringan dalam topologi jaringan tidak terlalu kompleks dan mencoba untuk melakukan hal yang standar untuk pengguna *PC Client* yaitu menggunakan OS Windows karena dianggap

lebih *User friendly*. Selain itu, *Server* ini berperan sebagai *web* dan *database server* dimana konfigurasi yang tidak terlalu kompleks dalam perancangan *server* sehingga penulis lebih memilih menggunakan windows dibandingkan yang lain.

#### - **Linux**

Selain windows yang dipilih sebagai sistem operasi, linux juga digunakan untuk beberapa perangkat. Laptop RAP yang menggunakan Linux Ubuntu 11.10 32-bit. Sistem operasi ini dipilih karena bersifat *customize* untuk melakukan apapun termasuk melakukan *bridging connection* untuk menciptakan RAP. Seri 32-bit dipilih karena ketersediaan dan kompatibilitas aplikasi-aplikasi lebih banyak digunakan.

### 3.2.2 Program Pembangun *Webserver* dan *Database Server*

Program ini dijalankan di *server* yang berfungsi sebagai “brain” dalam memasukkan, mengolah, menghapus dan memproses data. Beberapa program berkolaborasi sehingga menghasilkan antarmuka yang bersifat *User Friendly*.

#### 1. **XAMPP**

XAMPP merupakan kompilasi dari beberapa program yang terdiri atas program apache *HTTP Server*, *Mysql*, dan dapat ditulis dengan bahasa pemrograman PHP dan perl. Semua itu adalah komponen utama dalam membangun *Web Server*. Perangkat lunak ini tersedia dalam *General Public Liscence (GNL)* Merupakan web server yang mudah digunakan yang dapat melayani tampilan halaman web yang dinamis. XAMPP singkatan yang masing-masing hurufnya adalah :

**X** : Program ini dapat dijalankan dibanyak sistem operasi

**A** : *Apache*, merupakan aplikasi *web server*. Tugas utama Apache adalah menghasilkan halaman web yang benar kepada pengguna berdasarkan kode PHP yang dituliskan oleh pembuat web.

**M** : *Mysql*, merupakan aplikasi *Database Server*. *Mysql* dapat digunakan untuk membuat dan mengelola database beserta isinya.

**P** : PHP, Bahasa pemrograman web. PHP yang membuat fungsi-fungsi untuk halaman web yang bersifat dinamis

**P** : Perl, Adalah sebagai menyelesaikan masalah-masalah umum seperti program-program *Common Gateway interface* (CGI) dan berbagai protokol internet lainnya.

## 2. Hypertext Preprocessor (PHP)

PHP merupakan singkatan dari *Hypertext Preprocessor*, adalah sebuah bahasa *Scripting* yang terpasang pada HTML. PHP merupakan bahasa pemrograman web yang dapat menyatu dengan HTML. Kelebihan PHP :

1. PHP mendukung sistem database : *Oracle, Mysql, PostgreSQL*
2. PHP bersifat *flexible* karena dapat berjalan di berbagai sistem operasi
3. PHP merupakan aplikasi yang berbasis *Open Source* atau tidak berbayar
4. PHP bersifat *Customize*, artinya dapat dikembangkan sendiri atau membuat fungsi-fungsi baru.
5. PHP memiliki tingkat keamanan yang cukup tinggi
6. PHP memiliki waktu eksekusi yang lebih cepat dibandingkan dengan bahasa pemrograman lainnya.

## 3. Notepad ++

Notepad ++ merupakan pendukung para *programmer* untuk melakukan kemudahan dalam saat *coding*. Aplikasi ini memberikan tanda-tanda dengan memberikan perbedaan warna pada setiap code atau pemrograman yang berbeda. Aplikasi ini juga berbasis *open source* dan dapat didownload secara gratis baik dalam *install* dan *portable version*.

### 3.3 Komponen Perangkat Keras

Komponen perangkat keras yang digunakan dalam topologi jaringan ini adalah sebagai berikut :

#### 1. Server

Spesifikasi Komponen Server adalah sebagai berikut :

- Motherboard : MSI ASUS

- LAN CARD : 3Com Etherlink XL 10/100 PCI
- HDD Seagate 40 Gb PATA
- RAM 758 MB
- NVIDIA Geforce4 MX 440
- Prosesor AMD Athlon (1,26 GHz, Cache 2 Mb L2, LGA 775)

## 2. Router

- Tipe Router : Mikrotik Rb750, Router Indoor
- 5 Port Ethernet
- RAM 32 Mb
- CPU AR7241 400Mhz
- Main Storage 64 Mb

## 3. Switch 3com

- Memory 1 Mb
- Ports 8 x 10/100
- Interfaces 8 x Ethernet 10Base-T/100Base-TX RJ-45

## 4. Kabel UTP tipe CAT 5-e dengan connector RJ-45 1Gbps

## 5. 2 buah Access Point

- Tipe AP : D-Link DWL-900+ dan Linksys WAP54G
- Support 802.11 b/g/n 11,54,100Mbps
- Channel : 11 Channel

## 6. 2 buah PC Client

- Compaq Presario CQ5600 Series Desktop PC
- Prosesor Dual-Core CPU
- RAM 1 Gb
- Hard drive 250 Gb
- Realtek PCIe FE Family Controller 100Mbps

## 7. 2 buah Laptop

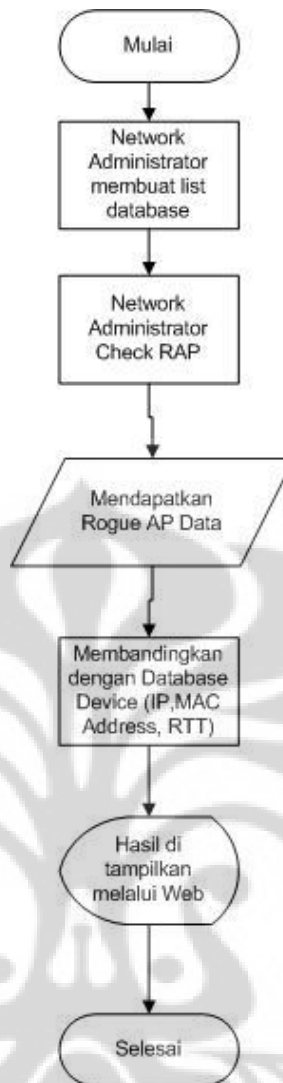
- **Laptop sebagai RAP**
  - Toshiba Satellite L640
  - Operating System Linux Ubuntu 11.10
  - Prosesor Intel Core i3 @2.4Ghz (4 CPU)

- RAM 3 Gb
- Atheros AR8152 PCI-E FastEthernet Controller
- Broadcom 802.11g/n Network Adapter 100Mbps
- **Laptop sebagai Client**
  - Toshiba Satellite M200
  - Windows Vista Home Basic
  - Prosesor Intel Core 2 Duo T5450 @1.66Ghz (2 CPU)
  - RAM 2 Gb
  - Marvell Yukon 88E8039 PCI-E FastEthernet Controller
  - Intel PRO/Wireless 3945ABG Network 802.11g 54Mbps

### 3.4 Rancangan Cara Kerja Sistem

Sistem deteksi ini dirancang melalui pendekatan *wired*, dimana pada umumnya semua akan bermuara pada distribusi layer yang sama. Jalur *wired* dapat dimanfaatkan menjadi salah satu cara untuk mendapatkan nilai parameter dari masing-masing perangkat. Parameter itu ialah *IP*, *MAC Address* dan *RTT*. *IP* merupakan alamat yang dimiliki oleh masing-masing perangkat yang terhubung ke dalam jaringan. *MAC Address* adalah terdiri dari kombinasi huruf dan angka yang mendeksripsikan suatu perangkat, atau disebut juga identitas perangkat. *RTT* adalah kependekan dari *Round Trip Time*, merupakan waktu yang dibutuhkan untuk mengirimkan antara pengirim dan penerima.

Oleh karena itu, pada awalnya *network administrator* sebagai *super user* dalam sistem ini akan membuat database sistem yang berkaitan dengan keberadaan semua divais jaringan yang ada termasuk *PC Client*, Laptop, *AP*, *Server*, dan *Router*. Semua perangkat memiliki 3 parameter yang akan disimpan didatabase sebagai data acuan. Perangkat dapat ditambahkan, diubah (*update*) dan dihapus. Sistem ini mencakup semua yang berada dalam 1 distribusi layer yang sama atau disebut juga area untuk *network administrator*. Secara *real time* sistem mampu melakukan *checking* untuk semua perangkat yang aktif dan dibandingkan dengan daftar database yang ada. Algoritma sistem ini untuk bersifat asli atau valid akan memenuhi kebenaran dalam 3 parameter itu.



Gambar 3-2 : Diagram Alur Kerja Secara Umum

### 3.4.1 Parameter Pendeteksian Rogue Access Point

Pendeteksian *Rogue Access Point* dapat dilakukan hanya jika telah terdefiniskan *Rogue Access Point* tersebut, hal yang paling mudah untuk mendefinisikan *Rogue Access Point* dapat dilakukan dengan membandingkan parameter-parameter yang dimiliki *Access Point*. Parameter-parameter yang digunakan ialah, IP, MAC Address, dan RTT. Sedangkan akses internet hanya mampu dilihat dari sisi *client*, dimana RAP dapat mengalirkan akses internet maupun tidak kepada *client* sehingga mendapatkan indikasi terhadap kemungkinan palsu atau asli.



Tabel 3-2 : Parameter pengukuran dan Potensi Rogue AP

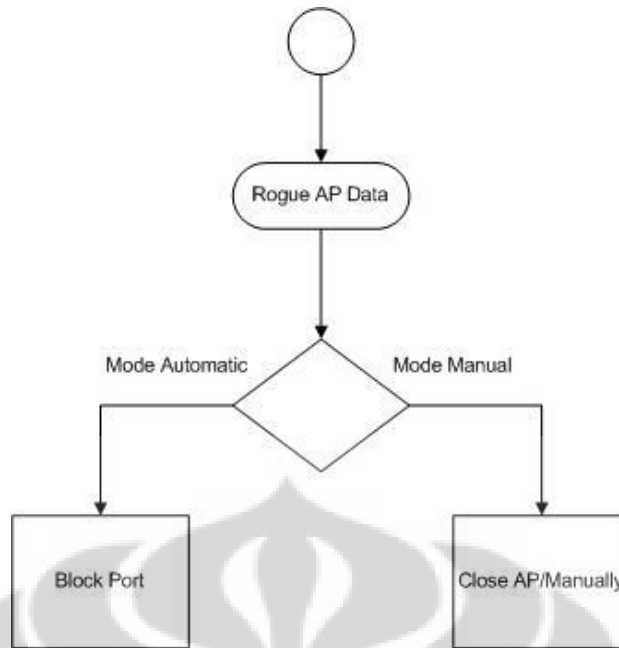
Parameter Pengukuran Rogue AP	Potensi Kejadian
IP	<ul style="list-style-type: none"> <li>• Memiliki IP, atau Wireless MAC yang tidak sesuai dengan telah didefinisikan di jaringan</li> <li>• Tidak Memiliki Akses internet</li> <li>• Memiliki Waktu RTT yang tidak normal</li> </ul>
MAC Address	
Akses Internet	
RTT ( <i>Round Trip Time</i> )	

### 3.4.2 Mode Pendeteksian

Potensi yang mungkin terjadi dari *Rogue Access Point* sangat banyak, tetapi dapat dibatasi dan didefinisikan lebih praktis untuk memastikan bahwa itu rogue AP atau tidak. Ada 2 mode yang dapat dilakukan untuk mendeteksi Rogue AP :

- **Mode Automatic**  
Mode bersifat otomatis dimana parameter-parameter yang ada dalam database dibandingkan dengan data terkini (pada saat itu). Setelah itu, secara otomatis akan memblok port AP tersebut. Mode ini sangat mengkhawatirkan dimana *false positive* akan banyak terjadi.
- **Mode Manually**  
Mode bersifat secara manual (*one click*) dimana *network administrator* mendeteksi Rogue AP dengan melihat parameter-parameter pendeteksian Rogue AP. Jika anomali dan dicurigakan, *network administrator* akan menganalisa. Mode ini lebih akurat dibandingkan dengan mode *automatic*, karena dapat mereduksi *false positive*.

Akan tetapi dalam sistem ini hanya diterapkan metode *manually*. Sehingga dalam browser nanti sebagai interface data pendeteksian AP, *network administrator* hanya dapat menggunakan metode manual.



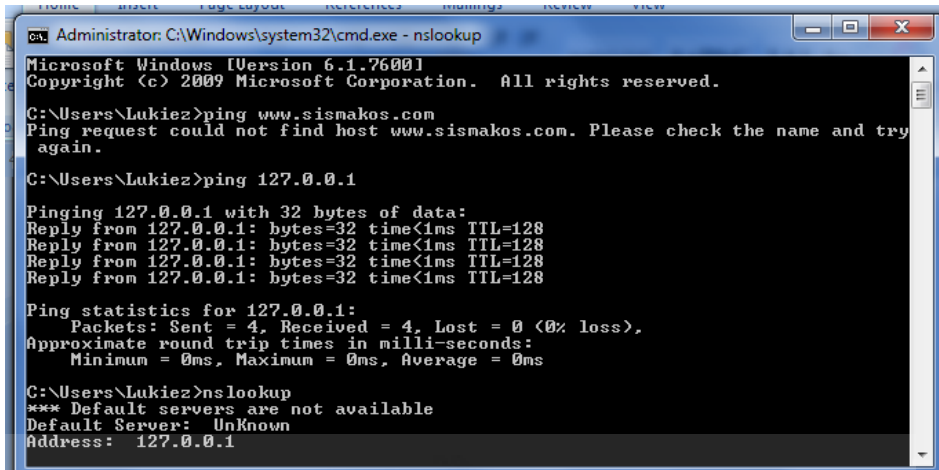
Gambar 3-3 : Alogoritma Mode Response Rogue AP

### 3.4.3 Metoda Pengambilan Nilai Parameter

Parameter yang dibuat merupakan kepastian yang dimiliki oleh setiap perangkat jaringan, yaitu IP, *MAC Address* dan *RTT (Round Trip Time)*. IP didapatkan dari masing-masing divais melalui *DHCP service* oleh *router*. *MAC Address* merupakan nilai yang unik dan bersifat identik untuk setiap perangkat atau sudah didapatkan dari produsennya. *RTT* merupakan waktu yang dibutuhkan sebuah perangkat untuk berkomunikasi satu sama lain (*peer to peer*) dari paket pengiriman sampai paket yang diterima (*reply packet*). Ada beberapa metode untuk melihat nilai parameter melalui command prompt adalah sebagai berikut :

- Ping Command

Ping merupakan suatu metode pengiriman paket “hello” dari pengirim ke penerima dan pengirim menerima *reply packet* yang menandakan antara pengirim dan penerima telah terhubung. Dalam normal besarnya paket ping yang dikirimkan 64 bytes, tetapi digunakan besarnya paket 1500 bytes. Dengan menggunakan Ping akan mendapatkan nilai *RTT*. Ping dapat dilakukan di command prompt, dengan format : ping <ip>, misalnya : ping 192.168.10.20. Contoh hasilnya akan seperti ini :



```
Administrator: C:\Windows\system32\cmd.exe - nslookup
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Lukiez>ping www.sismakos.com
Ping request could not find host www.sismakos.com. Please check the name and try
again.

C:\Users\Lukiez>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

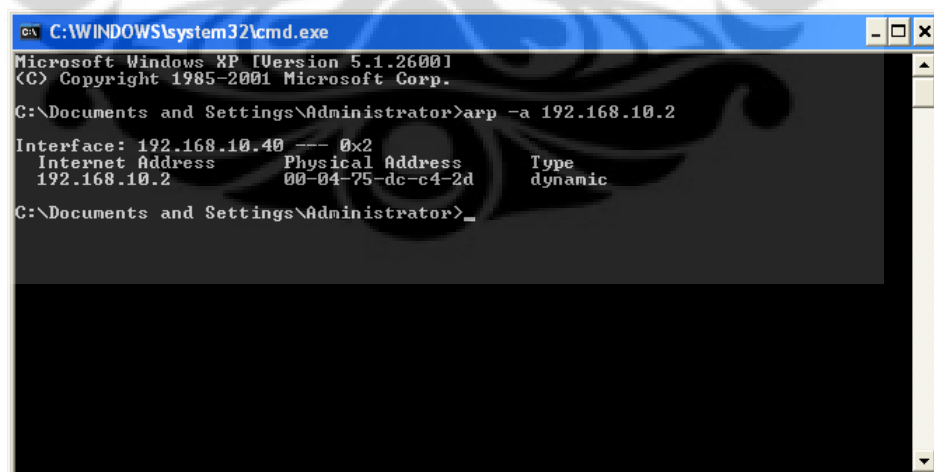
Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Lukiez>nslookup
*** Default servers are not available
Default Server: UnKnown
Address: 127.0.0.1
```

Gambar 3-4 : Contoh Ping di command prompt

- ARP Command

ARP merupakan kependekan dari *Address Resolution Protocol*. ARP merupakan paket yang digunakan untuk *broadcasting* dalam jaringan untuk membentuk sebuah *mapping*. Melalui ARP akan didapatkan informasi *MAC address* dari masing-masing perangkat. ARP akan bekerja sesaat setelah perangkat dinyalakan dan akan rutin dilakukan pengiriman untuk memastikan perangkat tersebut tetap aktif dalam *mapping* yang telah dibuat. Format pemanggilan paket ARP : `arp -a 192.168.10.2`



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>arp -a 192.168.10.2

Interface: 192.168.10.40 --- 0x2
 Internet Address      Physical Address      Type
 192.168.10.2          00-04-75-dc-c4-2d    dynamic

C:\Documents and Settings\Administrator>_
```

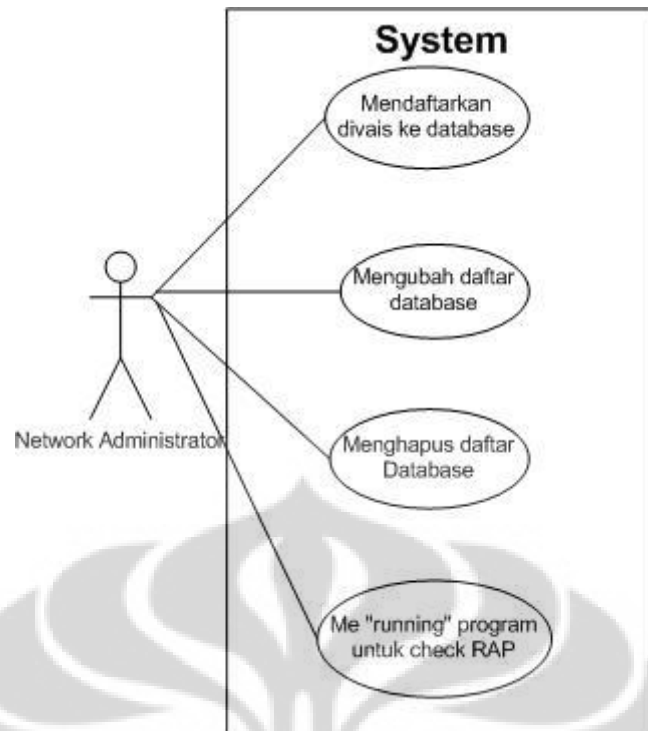
Gambar 3-5 : Contoh arp di command prompt

### 3.5 Diagram-Diagram *Unified Modelling Language* (UML)

*Unified Modelling Language* (UML) merupakan sebuah metode yang merepresentasikan atau mendeskripsikan desain perangkat lunak atau perangkat keras ke dalam notasi-notasi grafis yang bersifat standar. UML memudahkan dalam membaca alur desain, dan dalam membuat dokumentasi aplikasi. Dengan UML, rancangan perangkat lunak dapat direpresentasikan ke dalam diagram-diagram yang memiliki fungsi masing-masing. Berikut ini adalah diagram-diagram yang merepresentasikan rancangan dari modul yang akan dibuat, meliputi *use case diagram*, *activity diagram*, *sequence diagram*, dan *component diagram*.

#### 3.5.1 Use Case Diagram

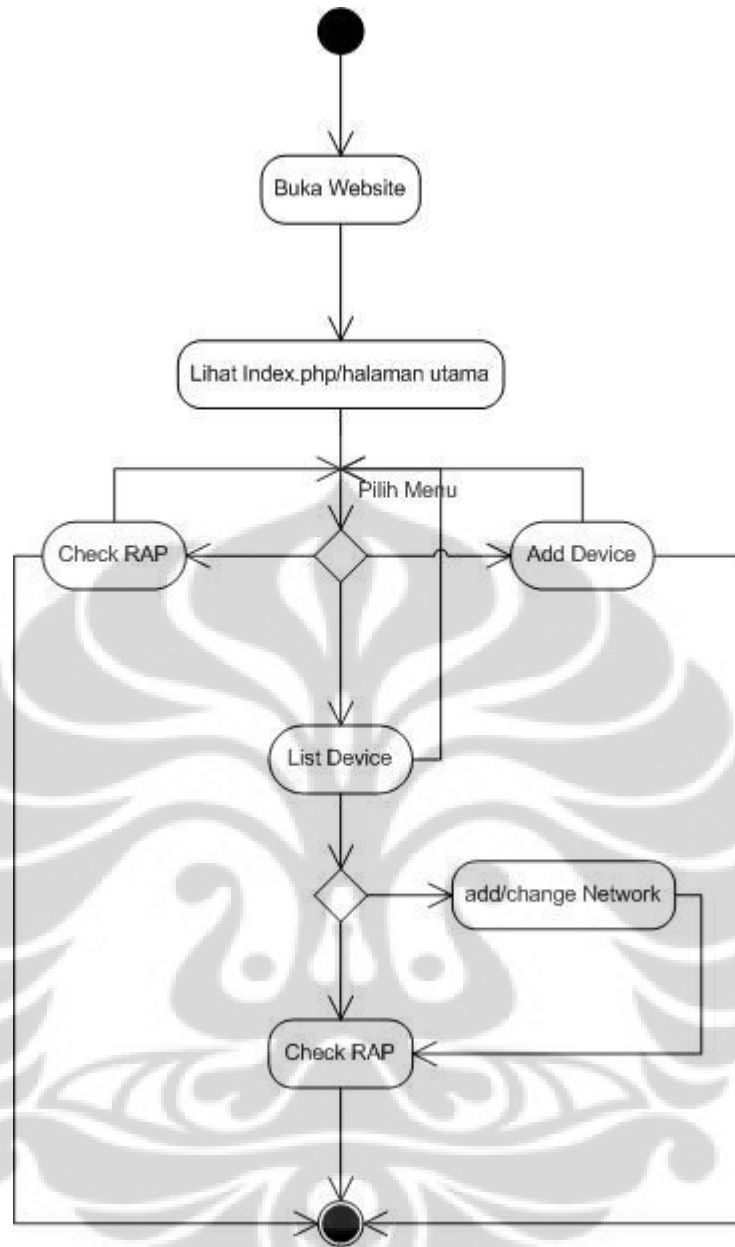
*Use Case Diagram* digunakan untuk mewakili fungsionalitas dari sistem [12]. Diagram ini menggambarkan interaksi antara pengguna, yang diwakili dengan notasi *actor* (subjek manusia) dengan sistem untuk mencapai tujuannya. *Use Case Diagram* untuk sistem ini ada dalam gambar 3. Dari gambar 3.3 dapat dilihat bahwa pengguna hanya dapat digunakan oleh *network administrator*, dimana memiliki 4 aktifitas yang dapat dilakukan pertama, mendaftarkan perangkat yang berada dalam topologi jaringannya ke dalam database, *network administrator* juga harus mendaftarkan IP dari semua yang berada dalam topologinya sedangkan *MAC address* dan *RTT time* akan secara otomatis didapatkan melalui sistem. Kedua, mengubah daftar database yang telah ada, misalnya *MAC address* diganti atau *RTT* waktunya yang normal berubah akibat jaringan yang memiliki *traffic* yang padat. Ketiga, menghapus daftar database yang ada di topologi jaringan merupakan hak dari *network administrator*. Keempat, melakukan proses pengecekan akan adanya RAP. Dengan hanya menekan tombol (*one Click*) dapat menunggu dalam beberapa waktu kemudian akan terlihat hasilnya di antarmuka.



Gambar 3-6 : Use Case Diagram

### 3.5.2 Activity Diagram

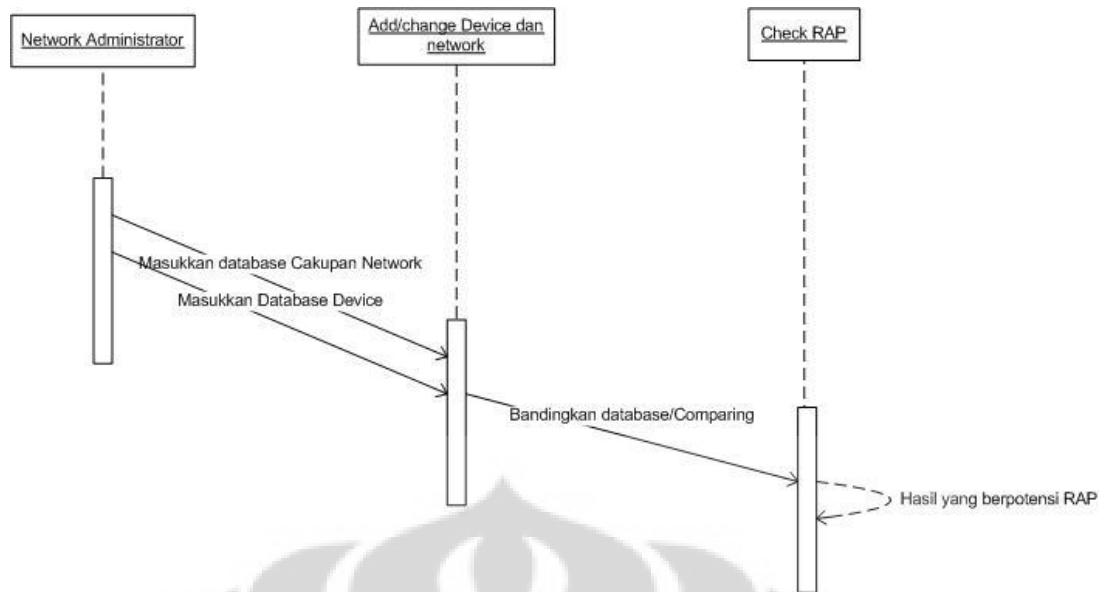
Activity Diagram merupakan diagram UML yang digunakan untuk merepresentasikan logika, *Business process*, atau alur kerja program [12]. Karena outputnya ialah interface antarmuka maka, pada gambar 3.7 diberikan Activity Diagram untuk menunjukkan alur dari mulai akses web yang dibuat. Activity diagram terdiri dari 3 menu, Check RAP, Add Device dan List Device. Dalam List Device ada add/change network, itu berarti cakupan check RAP hanya dalam jaringan tertentu.



Gambar 3-7 : Activity Diagram

### 3.5.3 Sequence Diagram

Sequence Diagram merupakan *interaction diagram* yang digunakan untuk menggambarkan perilaku dari objek-objek yang terlibat dalam sistem dan pesan-pesan antar objek yang berada dalam *use cases* [12].

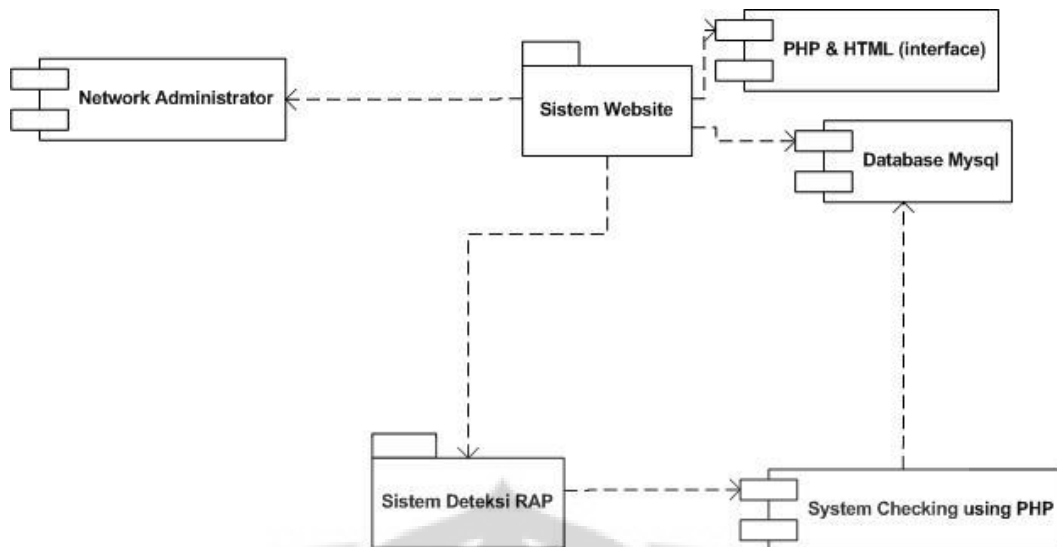


Gambar 3-8 : *Sequence Diagram*

Dari gambar diatas dapat dilihat sequence diagram sistem ini, network administrator memasukkan database berupa cakupan network dan daftar perangkat. Jaringan telah teridentifikasi melalui daftar database yang disimpan oleh network administrator, kemudian dilakukan check RAP, dengan mengirimkan paket-paket untuk menguji divais mana yang sedang aktif dan tidak dikenal (*unauthorization*). Hasil divais yang sedang aktif akan dibandingkan dengan database, akan terlihat yang berpotensi terjadinya RAP dengan cara melihat 3 parameter IP, MAC address dan RTT yang bersifat tidak normal, atau tidak terdaftar.

#### 3.5.4 *Component Diagram*

*Component diagram* merupakan definisi untuk menggambarkan objek dalam sistem dan hubungan dari objek tersebut. Pada sistem ini, setidaknya terdapat 4 component, dimana 2 *component* membentuk *package* sistem website, dan 1 component membentuk *package* sistem deteksi RAP. 1 component lainnya yang independent ialah network administrator, tetapi network administrator akan menjadi peranan penting dalam kedua *package*.



Gambar 3-9 : *Component Diagram*

### 1. *Package* Sistem Website

Sistem website terdiri dari 2 component yaitu database (Mysql) dan desain antarmuka (PHP & HTML). Kedua komponen itu saling memberikan input untuk sistem website agar terbentuk sistem website yang baik dalam interface dan databasenya.

### 2. *Package* Sistem Deteksi RAP

Sistem deteksi RAP ini terdiri dari 1 component yaitu PHP khusus untuk mendeteksi keberadaan *device* yang ada dalam jaringan. Kemudian untuk memastikan adanya RAP, maka hasil deteksi perangkat dibandingkan dengan database mysql.

### 3. *Component* Network Administrator

*Network administrator* adalah orang yang berperan dalam menjaga jaringan, konfigurasi dan melakukan deteksi antara legal dan ilegal *device* yang terhubung ke dalam jaringan.



## BAB IV

### IMPLEMENTASI SISTEM DAN ANALISIS HASIL

#### 4.1 Implementasi Sistem Testbed

Setelah dilakukan perancangan perangkat keras dan lunak, implementasi testbed yang menggambarkan kondisi jaringan yang digunakan sebelum tahap pengujian sesuai dengan topologi jaringan. Pengujian ini dilakukan di Mercator Multimedia Laboratory Engineering Center Universitas Indonesia. Seperti dalam gambar 3.1 topologi jaringan yang akan digunakan dalam pengujian. Topologi jaringan ini hanya memiliki satu jaringan yaitu internal LAN. Berikut penjelasan lebih rinci tentang kondisi topologi jaringan :

##### 4.1.1 Access point

Access point yang digunakan ialah AP D-Link Access Point DWL-900AP+ (sebagai RAP) dan AP Linksys WAP54G (Sebagai *legitimate AP*). Kedua wireless access point ini menggunakan standar 802.11b dengan kecepatan 11Mbps. Dalam implementasi kedua AP tersebut menggunakan kanal frekuensi radio yang berbeda, tujuannya agar tidak terjadi interferensi. Access point D-Link menggunakan channel 11, sedangkan Linksys menggunakan Channel 6. Perbedaan kanal yang lebih dari 1 diharapkan lebih baik.

##### 4.1.2 Internet Akses/IP Public

Dalam topologi ini digunakan IP Public yang merupakan berasal dari Source UI. *IP Public* dikonfigurasi secara *static* yaitu IP : 152.118.106.47. Selain itu, UI juga menggunakan *Proxy* dengan konfigurasi IP 152.118.24.10 port 8080 untuk dapat akses internet. Internet akses ini digunakan untuk mengkondisikan jaringan secara normal , artinya host dapat melakukan akses *traffic* internet.

##### 4.1.3 Traffic Generator

*Traffic generator* digunakan untuk membuat kondisi jaringan seperti *traffic* normal atau pada umumnya. Kondisi jaringan dibuat seperti ini untuk memastikan bahwa aplikasi dapat dijalankan dalam kondisi normal atau bukan idle. Beban yang dibuat oleh *traffic generator* sebesar rate normal.

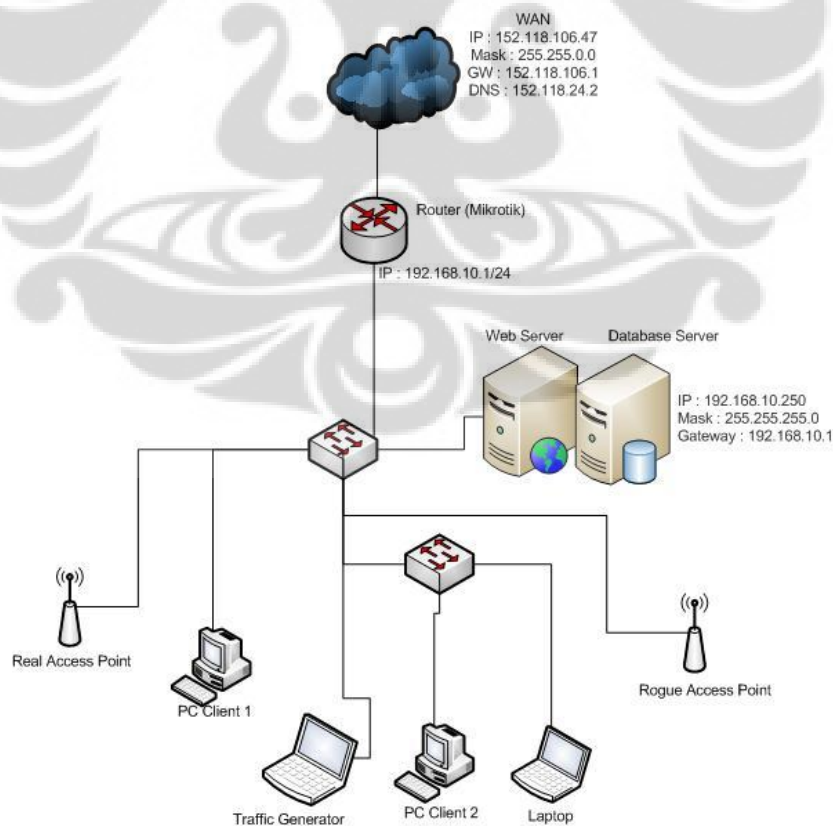
#### 4.1.4 Internal LAN

Pengujian ini hanya digunakan dalam 1 jaringan. Internal LAN mengkonfigurasi alamat jaringan 192.168.10.0/24. Jaringan LAN ini menghubungkan antara host komputer, laptop, access point, dan *server* dengan media kabel Cat 5-e 1 Gbps serta NIC *card* dengan *bandwith* maksimum 100Mbps. LAN kemudian terhubung ke internet menggunakan port Ethernet dari router.

#### 4.2 Metode RAP

##### 4.2.1 Access Point ilegal (*Unauthorized AP*)

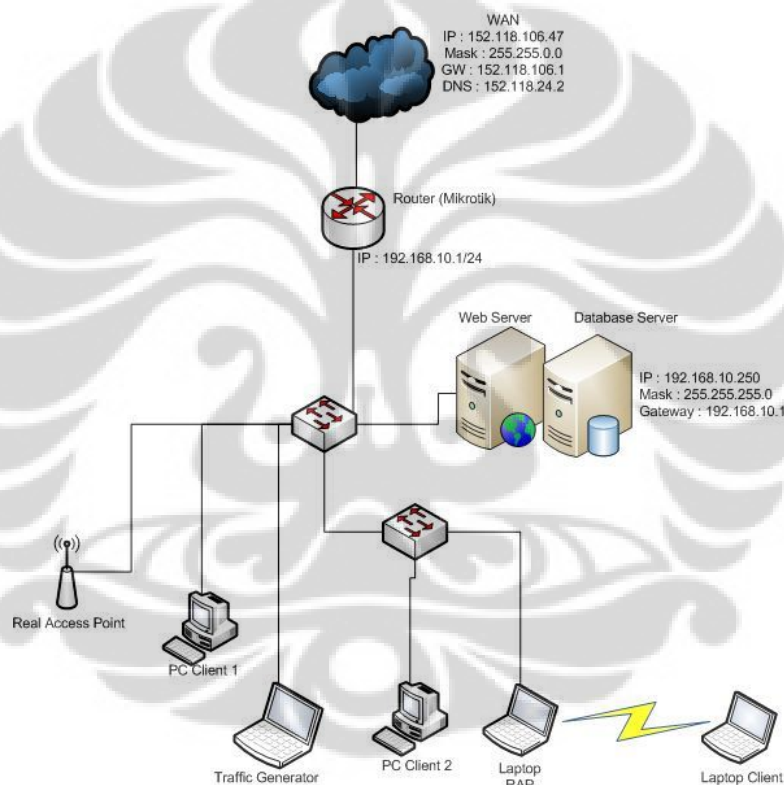
Access point ilegal merupakan salah satu cara *attacker* untuk menciptakan RAP. Metode ini disebut model 1 *Unauthorized AP*. Bentuk kategori Access Point ilegal ini ialah Access point yang di"create" tanpa diketahui oleh network administrator dan *attacker* mengendalikan AP tersebut. Bentuk perangkatnya ialah perangkat AP. Dalam pengujian ini digunakan AP D-Link Access Point DWL-900AP+ dan AP Linksys WAP54G



Gambar 4-1 : Topologi Jaringan : Model 1 Unauthorized AP

#### 4.2.2 Bridging Connection

*Bridging connection* merupakan salah satu cara *attacker* untuk dapat menciptakan RAP dengan cara menjadi MITM (*man in the middle*). Modelnya RAP berada ditengah-tengah antara pengguna dan *accessor*. Metode ini disebut model 1 *Bridging Connection AP*. Umumnya RAP ini menggunakan SSID yang sama sehingga *client* dianggap terhubung pada access point yang ilegal. Perangkat yang digunakan ialah Laptop Toshiba Satellite L640 menggunakan OS Linux. Selain itu, dapat dilakukan dengan cara menjadikan AP sebagai *extended AP* menggunakan laptop/ *Wireless Client*.



Gambar 4-2 : Topologi Jaringan : Model 2 Bridging Connection

#### 4.3 Aplikasi Deteksi RAP

Pembuatan aplikasi berbasis web ini menggunakan bahasa pemrograman PHP untuk melakukan eksekusi dalam pendeteksian RAP. Aplikasi ini hanya dapat digunakan oleh *network administrator*, karena dalam *use case* aplikasi ini hanya dapat digunakan oleh *network administrator*. *network administrator* melakukan manajemen terhadap semua perangkat yang aktif dalam jaringannya,

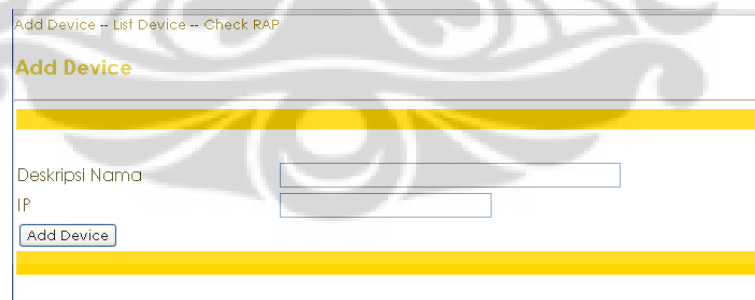
kemudian dilakukan eksekusi berupa pengaktifan code untuk mendeteksi RAP. Eksekusi aplikasi ini dengan cara *one click* yang berarti mengaktifkan ping dan arp packet setelah itu akan mengeluarkan hasil/output yang akan dianalisis oleh *network administrator*.

- Database

Database berfungsi sebagai *storage* data perangkat. Setelah program dieksekusi akan merekam semua perangkat yang didaftarkan oleh network admin. Database terdiri dari 2 tabel yaitu tabel network (field : id, ip\_first, ip\_last, mask) dan tabel device\_list (field : no, deskripsi, hostname, ip, mac, rtt). Data tabel yang dibuat untuk aplikasi ini ada didalam lampiran gambar L1-11

- Interface

Dalam aplikasi ini memiliki 3 menu yaitu, *add device*, *list device* dan *check RAP*. *Add device* digunakan untuk menambahkan perangkat device yang ada dalam jaringan, *list device* digunakan untuk melihat daftar perangkat yang telah teregistrasi/aktif. *Check RAP* digunakan untuk mendeteksi RAP yang ada di jaringan dengan cara membandingkan 3 Parameter yaitu IP, MAC Address dan RTT untuk semua perangkat yang aktif dalam jaringan dengan perangkat yang telah teregistrasi oleh *network administrator*.



The image shows a web-based form titled "Add Device". At the top, there is a navigation bar with the text "Add Device -- List Device -- Check RAP". Below this, the main heading "Add Device" is displayed. The form contains two input fields: "Deskripsi Nama" and "IP". Below the "IP" field, there is a button labeled "Add Device". The form is styled with a light background and a yellow border.

Gambar 4-3 : Interface Add device Form

NETWORK : 192.168.10.2 - 192.168.10.200  
 MASK : 255.255.255.0  
 Change

Host Name	Deskripsi	IP Address	MAC Address	RTT Time	Update	Delete
SERVER	SERVER	192.168.10.2	00-04-75-dc-c4-2d	2ms		
	Access Point 1	192.168.10.3	00-90-4c-91-00-01	6ms		
DORTMUND	Dortmund	192.168.10.40	d4-85-64-0b-75-8f	2ms		
PRINTER	PRINTER	192.168.10.5	00-15-99-44-e0-ab	4ms		
ESSEIN	Essein	192.168.10.54	d4-85-64-10-5d-e7	4ms		
	Access point DWL	192.168.10.6	00-80-c8-17-27-ea	1ms		

Gambar 4-4 : Interface List Device Form

Check

Check

Check

Host Name	IP Address	MAC Address	Status	RTT Time	Alarm
SERVER	192.168.10.2	00-04-75-dc-c4-2d	Online	0ms (0%)	Benar--tidak ada
-	192.168.10.3	00-90-4c-91-00-01	Online	2ms (100%)	Benar--RTT Normal
-	192.168.10.4	00-01-e6-a6-a8-1d	Online	ssms (0%)	Masalah--tidak ada
PRINTER	192.168.10.5	00-15-99-44-e0-ab	Online	1ms (100%)	Benar--RTT Normal
-	192.168.10.6	00-80-c8-17-27-ea	Online	26ms (0%)	Masalah--tidak ada
-	192.168.10.7	e8-39-df-f3-90-43	Offline	Time out	Masalah--tidak ada
MO-LAPTOP	192.168.10.8	00-1c-bf-aa-e5-db	Online	28ms (0%)	Masalah--tidak ada

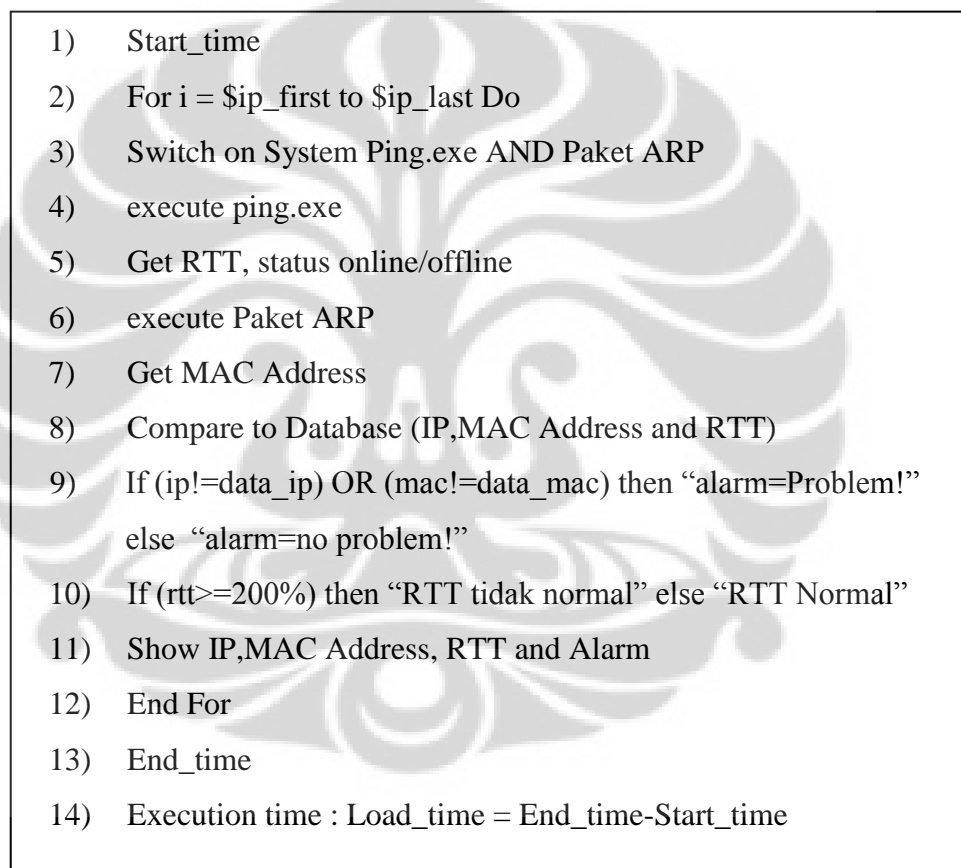
Page loads: 44.1091 sec. Check

Gambar 4-5 : Interface Check RAP

#### 4.4 Server Scripting

Script yang dibuat akan melakukan eksekusi untuk mendeteksi perangkat yang ilegal dengan cara menggunakan *command ping.exe* dan *arp*. *Ping.exe* digunakan untuk mendapatkan waktu RTT dan packet *reply*. Hasil packet *reply* itu akan memastikan keaktifan (*online*) sebuah perangkat. Kemudian *script* ini akan menghitung dan mencatat durasi waktu antara mulai eksekusi *command ping.exe* hingga saat diterima respon/*acknowledgement*, durasi waktu inilah yang disebut *Round Trip Time* (RTT) dan akan dijadikan sebagai parameter penentuan RAP. *Ping.exe* dilakukan 1 kali per *IP Address*, hal ini dilakukan untuk mempercepat proses pendeteksian. Seperti yang diketahui bahwa, pada kondisi normal *command ping.exe* melakukan 4 *sending*. Disamping itu, ada n perangkat (karena subnet *prefix /24* maka  $n=254$ ) yang harus dideteksi, maka dilakukan secara berulang-ulang sejumlah n kali untuk memperoleh kondisi perangkat yang aktif

dalam jaringan tersebut. Aplikasi ini menggunakan 3 parameter untuk mendeteksi perangkat yaitu, waktu RTT, *MAC Address* dan *IP Address*. Dalam database telah ada perangkat-perangkat yang bersifat legal yang telah didaftarkan, sehingga setelah melakukan deteksi server akan membandingkan (*Comparasion*) data perangkat yang ada dalam database. Perangkat-perangkat akan diolah dengan cara mencocokkan parameter perangkat yang legal dengan yang dideteksi. Perangkat yang tidak sesuai atau tidak dalam database akan memberikan alarm dan dianggap sebagai perangkat ilegal. Gambar 4-4 menunjukkan pseudocode dari server scripting.



```

1) Start_time
2) For i = $ip_first to $ip_last Do
3) Switch on System Ping.exe AND Paket ARP
4) execute ping.exe
5) Get RTT, status online/offline
6) execute Paket ARP
7) Get MAC Address
8) Compare to Database (IP,MAC Address and RTT)
9) If (ip!=data_ip) OR (mac!=data_mac) then "alarm=Problem!"
   else "alarm=no problem!"
10) If (rtt>=200%) then "RTT tidak normal" else "RTT Normal"
11) Show IP,MAC Address, RTT and Alarm
12) End For
13) End_time
14) Execution time : Load_time = End_time-Start_time

```

Gambar 4-6 : *Pseudocode Server Scripting Deteksi RAP*

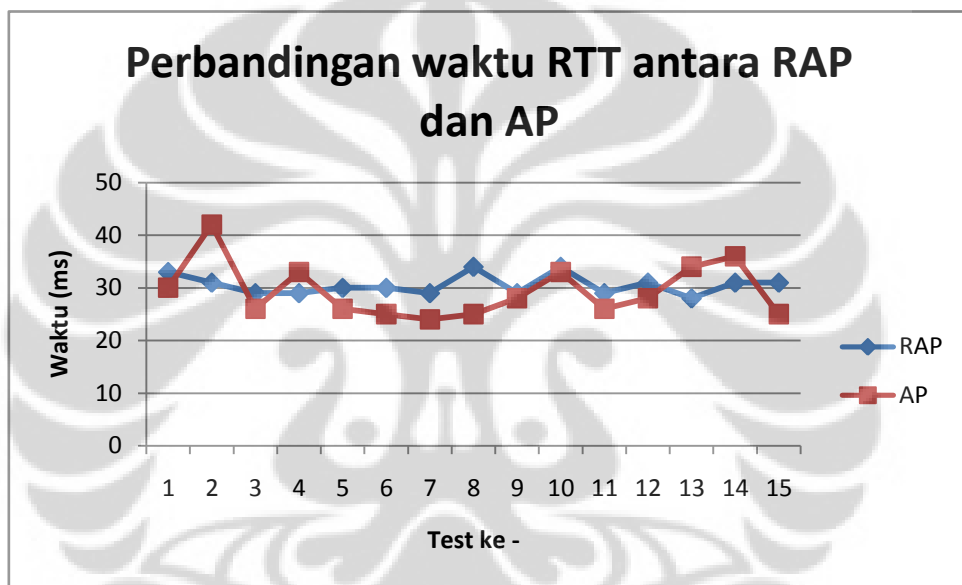
## 4.5 Pengujian dan Analisa

### 4.5.1 Hasil Pengukuran dan Analisa RTT Terhadap RAP dan AP

Implementasi aplikasi deteksi RAP ini membutuhkan nilai parameter RTT sebagai nilai standar/ambang batas untuk menentukan apakah perangkat

itu sebuah AP atau RAP. Untuk mendapatkan nilai itu maka dilakukan pengukuran testbed menggunakan command ping.exe. RTT didapatkan dari proses pengiriman paket “hello” dari RAP dan AP ke server pendeteksi atau dari server pendeteksi ke RAP dan AP. Seperti yang dijelaskan sebelumnya bahwa ada 2 model yang terdefiniskan dalam RAP yaitu *unauthorized AP* dan *Bridging Connection AP* sehingga pengukuran ini dilakukan sebanyak 2 kali. Dari hasil pengukuran AP dan RAP menggunakan model 1 ditunjukkan pada gambar 4-5.

- Model 1 *Unauthorized AP*

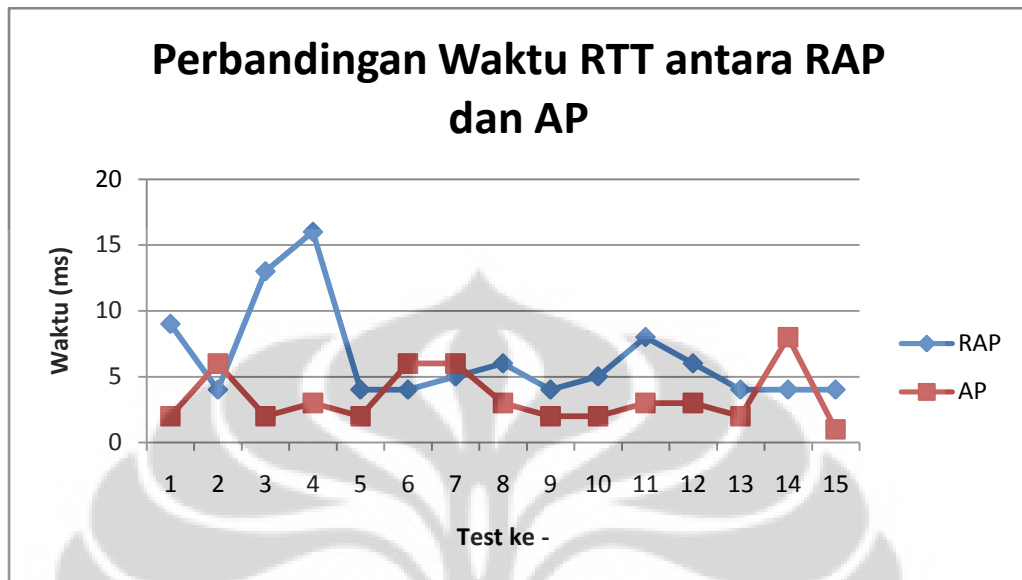


Gambar 4-7 : Grafik Perbandingan Waktu RTT antara RAP dan AP melalui model *unauthorized*

Pada model 1 ini seperti dengan perkiraan awal bahwa perbedaan waktu RTT tidak akan terlalu jauh, atau bahkan sama karena posisi RAP dan AP hampir sama, hal itu ditunjukkan pada grafik pada gambar dimana letak kordinat RTT yang berhimpit. RAP ini memiliki hop yang sama dengan AP, karena RAP juga terhubung dalam satu distribusi layer yang sama. Nilai rata-rata RTT RAP 30,533 ms dan RTT AP 29,4 ms. Nilai RTT sangat tidak jauh hanya selisih 2,03 ms. Dalam selisih waktu sekecil itu tidak ada jaminan bahwa RAP akan jelas terlihat melalui waktu RTT. Oleh karena itu, pada model ini tidak dapat ditentukan nilai ambang batas atau standar untuk mendeteksi RAP pada model 1. Secara *logical*

network, posisi RAP dan AP dalam model ini akan sama, terlepas dari nilai fluktuasi grafik.

- Model 2 *Bridging Connection*



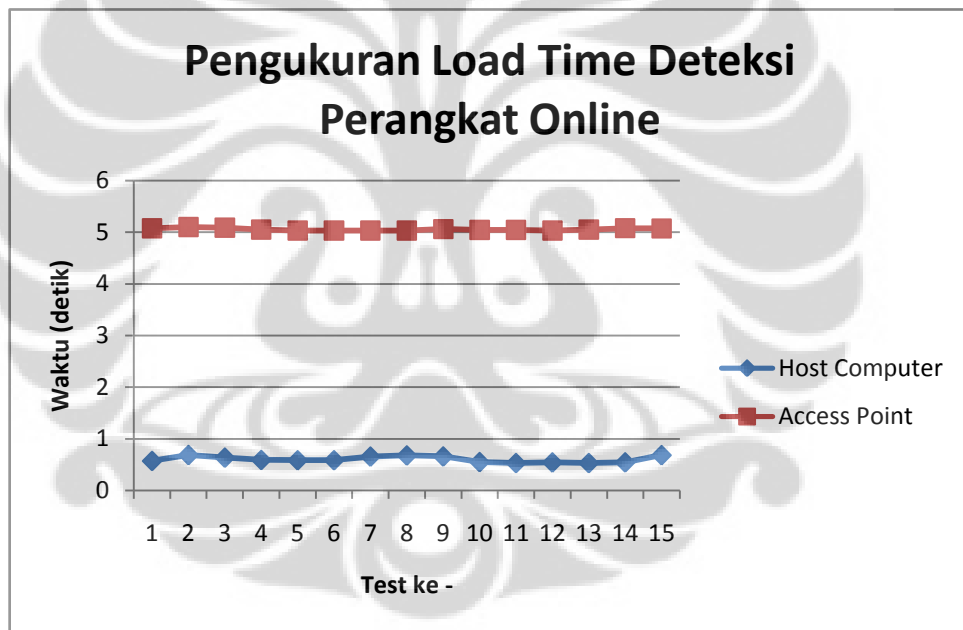
Gambar 4-8 : Grafik Perbandingan Waktu RTT antara RAP dan AP melalui model *Bridging Connection*

Pada model 2 ini perbandingan waktu RTT antara RAP dan AP menggunakan *bridging connection* sangat jelas terlihat. RAP ini tercipta melalui akses sumber yang sama, namun membuat sebuah jaringan sendiri sebagai jaringan palsu untuk host. RAP memiliki perbedaan hop sehingga waktu yang dibutuhkan lebih lama. Berdasarkan nilai rata-rata RTT RAP 6,4 ms, dan RTT AP 3,4 ms. Hal itu jelas dapat menjadi bukti bahwa RAP menggunakan model ini dapat memanfaatkan waktu RTT sebagai parameter penentuan RAP. Waktu RTT ini dijadikan nilai standar/ambang batas untuk implementasi aplikasi deteksi RAP berbasis web. Seperti yang dilihat dalam gambar 4-6 range grafik antara RAP dan AP tidak terlalu berhimpit sehingga didapatkan nilai ambang batas :  $(6,4/3,4) \cdot 100\% = 188,35\%$  . Pengambilan data dilakukan dalam kondisi *traffic* normal atau bukan kondisi *idle*, seperti yang dijelaskan sebelumnya bahwa kondisi jaringan dibuat dengan *traffic generator*.



#### 4.5.2 Pengukuran Load Time Deteksi Perangkat Online

Pengukuran *load time* ini ialah mendeteksi perangkat yang aktif atau *online* atau bukan dalam keadaan mati. *Load time* ini dihitung ketika deteksi perangkat sudah melalui web aplikasi RAP, yang berarti waktu yang dibutuhkan ketika eksekusi script deteksi untuk satu perangkat hingga selesai eksekusi script. Pengukuran ini dimaksudkan untuk mengetahui estimasi waktu yang dibutuhkan untuk mendeteksi perbedaan status perangkat, *online* atau *offline*. Pengertian status perangkat ini menentukan keberadaan suatu perangkat, yaitu AP dan *Host Computer*. Karena perangkat ini yang digunakan dalam pengujian ini. Dengan cara itu dapat diketahui nilai dari waktu yang dibutuhkan untuk mendeteksi Access Point dan host computer yang aktif. Gambar 4-7 menunjukkan pengukuran load time deteksi perangkat online dan dilakukan sebanyak 15 kali.

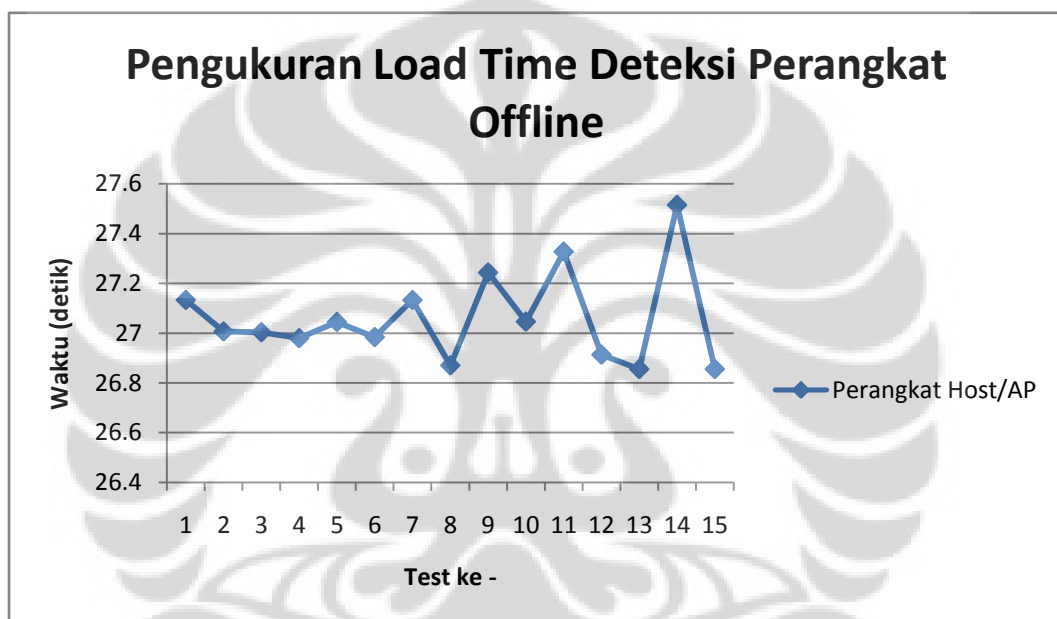


Gambar 4-9 : Grafik Pengukuran Load Time Untuk Mendeteksi Perangkat yang Online

Pada pengukuran *load time* yang dilakukan 2 perangkat ini seperti yang terlihat dalam grafik menunjukkan range nilai yang berbeda. *Host computer* memiliki waktu yang lebih cepat dibandingkan AP. Artinya perangkat *host computer* memiliki respon yang lebih cepat dibandingkan dengan AP, selisih waktu keduanya hingga 5 detik. Perangkat yang aktif biasanya akan jauh lebih cepat, karena mendapatkan *acknowledgement* paket *reply* yang lebih cepat dari penerima.

### 4.5.3 Pengukuran Load Time Deteksi Perangkat Offline

Pengukuran *load time* ini untuk mendeteksi perangkat *offline* atau tidak terhubung. Secara status perangkat pasti berbeda, karena antara ketersediaan perangkat atau tidak. Pengukuran perangkat *offline* dilakukan untuk melihat berapa waktu yang dibutuhkan untuk mendeteksi suatu perangkat jikalau dalam keadaan *offline*. Karena deteksi perangkat yang aktif dalam satu jaringan akan mencakup perangkat yang *online* dan *offline*. Sehingga dapat diestimasikan waktu yang dihabiskan untuk mendeteksi perangkat *offline*. Gambar 4-8 menunjukkan pengukuran grafik *load time* deteksi perangkat *offline* dilakukan sebanyak 15 kali.



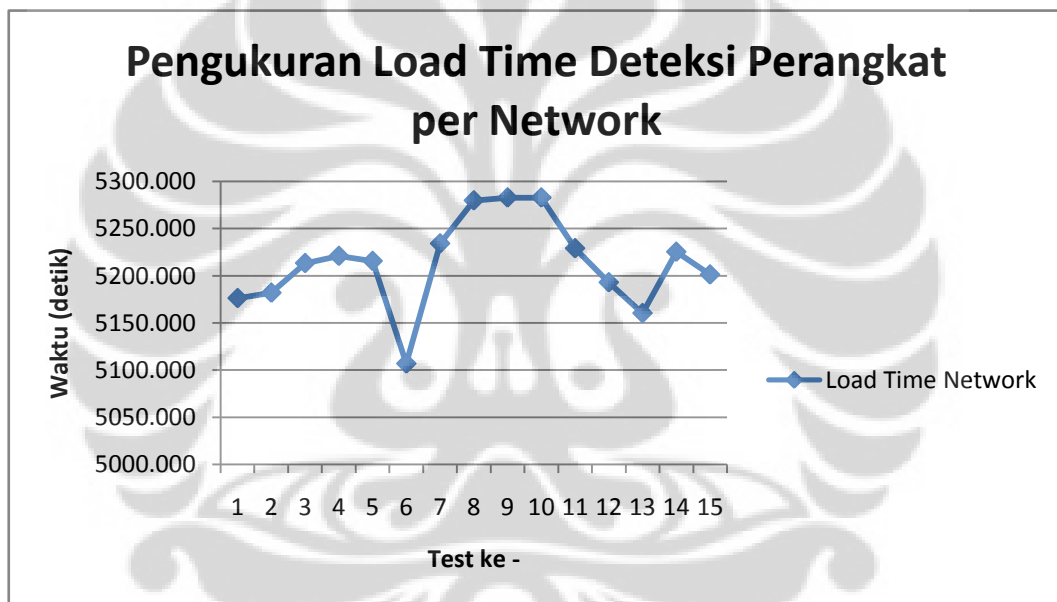
Gambar 4-10 : Grafik Pengukuran Load Time untuk mendeteksi perangkat yang Offline

Pada pengukuran *load time* dalam mendeteksi perangkat *offline* ini dapat dilihat grafik bahwa butuh waktu 25-27 detik untuk mengetahui bahwa IP tersebut tidak terhubung atau tidak ada perangkat. Hal ini sudah dalam perkiraan awal bahwa, ketika melakukan *command ping.exe* dan paket *ARP*, dikirimkan paket “hello” yang akan diterima oleh penerima sekaligus memberikan balasan paket untuk pengirim. Jika tidak ada perangkat yang terhubung dalam IP tersebut pemberi akan melakukan *re-send* paket hingga sampai akhirnya pengirim tidak melakukan toleransi atau sudah dianggap tidak terhubung. Oleh karena itu, untuk mendeteksi perangkat *offline* akan jauh lebih lama. Selain itu, perangkat *offline* ini tidak akan

mendapatkan nilai parameter MAC dan RTT karena dalam paket ARP perangkat tersebut tidak terdeteksi.

#### 4.5.4 Pengukuran Load Time/Network

Aplikasi deteksi RAP yang dibuat ialah untuk melihat keaktifan dari suatu perangkat. Dengan cara itu dapat diketahui semua informasi jaringannya. Skala yang digunakan ialah satu *network*, karena subnet yang digunakan ialah 255.255.255.0 atau prefix /24, maka jumlah host IP yang dapat digunakan ialah 254 IP/host. Seperti dalam topologi percobaan yang dilakukan ada 6 perangkat yang aktif. Seperti dalam gambar 4-9 pengukuran load time dilakukan sebanyak 15 kali.



Gambar 4-11 : Grafik Pengukuran Load Time untuk mendeteksi perangkat dalam satu network

Dalam eksekusi aplikasi ini dibutuhkan waktu pendeteksian per satu perangkat, artinya jika ada 254 perangkat yang harus dideteksi tentunya membutuhkan waktu yang lebih lama. Dalam pengukuran ini hanya dilakukan hingga host ke 200 yang dideteksi hanya ada 6 perangkat yang aktif untuk dideteksi. Rata-rata waktu yang dibutuhkan untuk mendeteksi semua perangkat dalam satu jaringan ialah 5213.5569 detik. Untuk setiap iterasi deteksi akan memakan waktu  $\pm 5000$  detik. Hal ini jelas terlihat jikalau dilihat dari gambar 4-8 yang menunjukkan waktu yang dibutuhkan untuk mendeteksi perangkat *offline*. Dari 200 perangkat yang

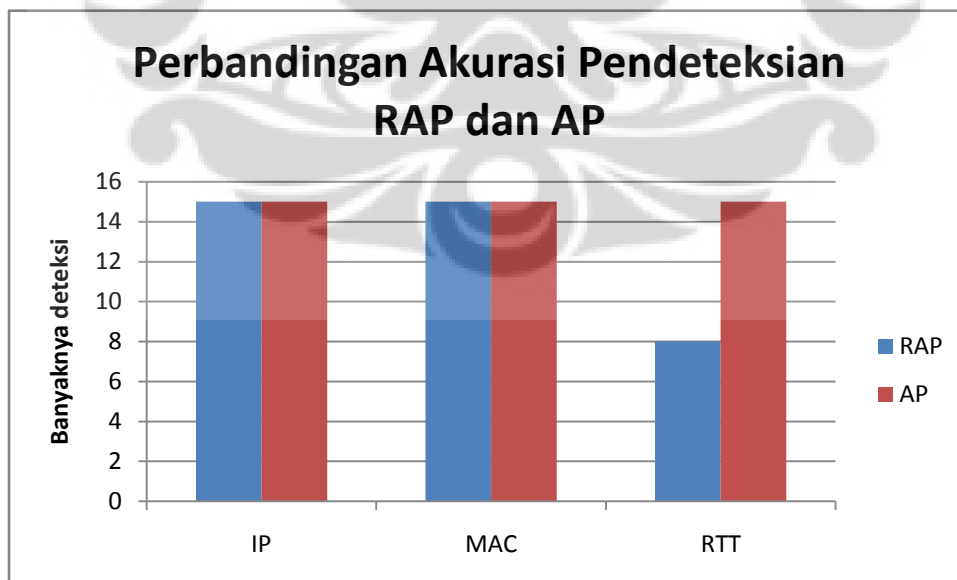
ada, dan 200 iterasi dilakukan hanya ada 6 perangkat yang *online* dan 194 perangkat *offline*.

#### 4.5.5 Perbandingan Akurasi Pendeteksian RAP dan AP

Aplikasi yang dibuat untuk pendeteksian memiliki 3 parameter khusus untuk mengetahui apakah perangkat tersebut legal atau illegal. Oleh karena itu, dilakukan beberapa percobaan pendeteksian dan akan mendapatkan seberapa besar akurasi untuk mendeteksi RAP dan AP melalui 3 parameter tersebut. Percobaan ini dilakukan untuk mendapatkan nilai akurasi terhadap kesempurnaan sistem untuk dapat mendeteksi 3 parameter dalam suatu perangkat. Ketidakefektifan deteksi diakibatkan oleh *error code*, *bug*, *error output* dan lain-lain. Kemudian parameter manakah yang menjadi prioritas untuk dapat dijadikan referensi awal. Percobaan ini dilakukan sebanyak 15 kali. Perbandingan akurasi pendeteksian ini menggunakan 2 model yang berbeda. Yaitu model *Unauthorized AP* dan *Bridging Connection*.

- Model 1 (*Unauthorized AP*)

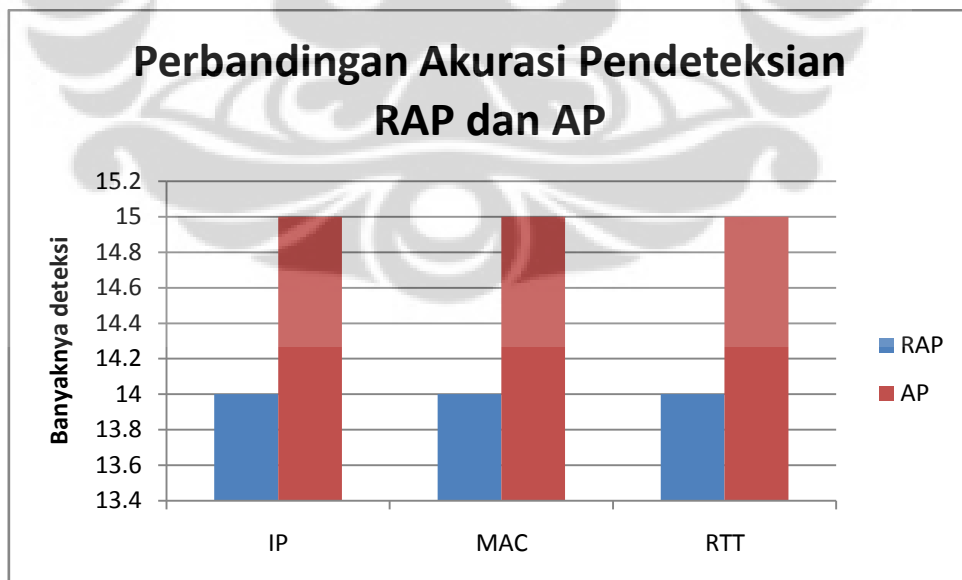
Gambar 4-12 menunjukkan perbandingan akurasi pendeteksian menggunakan aplikasi ini antara RAP dan AP.



Gambar 4-12 : Grafik Perbandingan Akurasi Model *Unauthorized AP*

Pengukuran ini dilakukan untuk mendapatkan nilai akurasi dari aplikasi ini. Dalam model ini dilakukan 15 kali percobaan antara AP dan RAP. Tingkat akurasi dalam percobaan ini dilakukan untuk memastikan kesempurnaan dalam mendeteksi 3 parameter yang dimiliki perangkat, sehingga analisa dan hasil akhir dapat dilakukan dengan baik oleh *network administrator*. AP dilakukan eksekusi dan menghasilkan 3 parameter, IP terdeteksi dengan baik sebanyak 15 kali termasuk apakah IP tersebut legal atau ilegal. *MAC Address* terdeteksi dengan baik sebanyak 15 kali kemudian mampu menentukan apakah MAC tersebut ilegal atau legal. RTT juga dilakukan mampu mendeteksi sebanyak 15 kali, karena RTT dalam model ini tidak memiliki ambang batas nilai sehingga tidak perlu untuk melakukan perbandingan. RAP dalam model ini ialah murni menjadi sebagai perangkat ilegal, artinya RAP ini bukan tercipta dari perangkat yang sudah terdaftar oleh *network administrator*. Sehingga secara penuh, perangkat ini akan diberikan alarm karena 3 parameter tersebut tidak terpenuhi. Dari 15 kali percobaan IP dan MAC selalu terdeteksi dengan sempurna, hanya saja 8 kali dari 15 kali percobaan, RTT tidak dapat terdeteksi dengan sempurna.

- Model 2 (*Bridging Connection*)



Gambar 4-13 : Grafik Perbandingan Akurasi Model *Bridging Connection*

Dalam model ini RAP dibuat menggunakan laptop yang dilakukan *Bridging Connection*. Lebih tepatnya menciptakan *MAC Bridge* antara *LAN Card* dan

*Wireless Card*. Konsep model ini ialah dimana Laptop menjadi RAP dengan menjadikan sebagai MAC Bridge, artinya komunikasi antara Laptop (RAP) dan host yang terhubung ke RAP hanya melewati layar 2 saja, yaitu melalui MAC Address, sehingga seakan-akan dalam satu jaringan sama. Dalam percobaannya sebanyak 15 kali, parameter IP, dan RTT menjadi prioritas kedua, dimana MAC Address akan terlihat seperti *MAC Spoofing*. IP address dari RAP akan sama, tetapi pada host yang terkoneksi akan memiliki IP yang berbeda tetapi MAC Address yang didapatkan dari RAP, hal itu karena fungsi *bridging connection* mengakibatkan *ARP Proxy*. Hasil Akurasi kesempurnaan sistem mendeteksi suatu perangkat sebesar 90%.



## BAB V

### KESIMPULAN

1. Sistem Pendeteksi *Rogue Access Point* berbasis web mampu menjadi solusi ancaman *Rogue Access Point* dengan 2 model yang digunakan yaitu, *Bridging Connection* dan *Unauthorized AP*.
2. Sistem Pendeteksian menggunakan 3 Parameter penting untuk mengukur dan efektifitas pendeteksian RAP : IP, MAC Address dan RTT (Round Trip Time)
3. Rata-rata Waktu yang dibutuhkan untuk mendeteksi sebuah perangkat yang *Online* ialah 0,601 detik untuk *Host Computer* dan 5,05 detik untuk *Access Point*
4. Rata-rata waktu yang dibutuhkan untuk mendeteksi sebuah perangkat yang *Offline* ialah 27,06 detik untuk *Host Computer/AP*. Hasil ini lebih lama dibandingkan perangkat *online* karena membutuhkan pengiriman secara berulang-ulang.
5. Rata-rata waktu *Load Time* untuk mendeteksi semua perangkat (*Online* dan *Offline*) dalam satu segment network ialah 5213,55 detik
6. Hasil pengujian model *Unauthorized AP* memiliki akurasi 53% untuk RTT hanya 8 kali percobaan yang mampu terdeteksi secara sempurna, 7 percobaan lainnya tidak terdeteksi secara sempurna. Sedangkan IP dan MAC mampu terdeteksi secara sempurna. Sehingga prioritas pendeteksi pada model ini ialah IP dan *MAC Address*
7. Hasil Pengujian pada model *Bridging Connection* memiliki akurasi 90% untuk paramater IP, MAC Address dan RTT yang mampu mendeteksi secara sempurna. Sehingga prioritas pendeteksian pada model ini ialah *MAC Address* dan RTT.

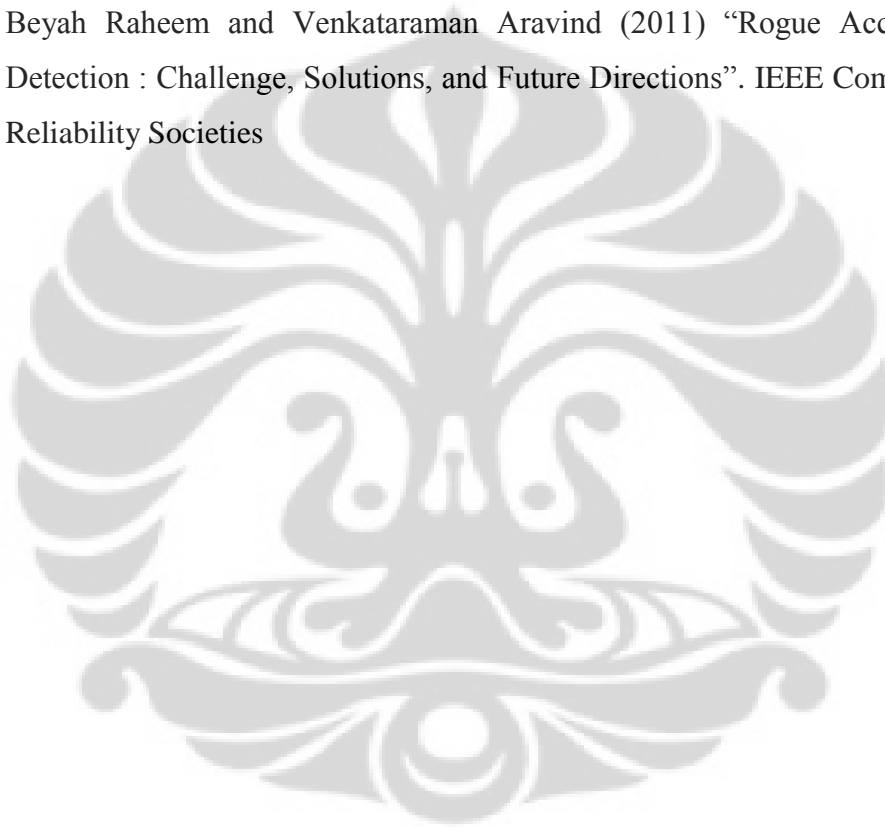
## REFERENSI

- [1] Abdul Hamid Rafidah (2003). *Wireless LAN : Security Issues and Solutions. Reading Room, SANS Institute, Page 3, 2006.*
- [2] Srilasak, Songrit, Wongthavarawat, Kitti, & Phonphoem (2008). *Integrated Wireless Rogue Access Point Detection and Counterattack. 2008 International Conference on Information Security and Assurance*
- [3] White Paper (2004), “Rogue Access Point Detection : Automatically Detect and Manage Wireless Threats to Your Network”. Proxim Corporation
- [4] Kim, Sang-Eon, Chang, Byung-Soo, Lee, Hong Sang, “Rogue AP Detection in The Wireless LAN For Large Scale Deployment”. Volume 4 - Number 5. SYSTEMATICS, CYBERNETICS AND INFORMATICS
- [5] Aruba Networks (2008), “Retail Wireless Networks Validated Reference Design”. Version 3.3 Solution Guide.
- [6] CCNA Exploration 4.0, “LAN Switching and Wireless”. Cisco Network Academy, copyright © 2007 Cisco Systems, Inc.
- [7] Lisa Philfer (2010), Top Ten Wi-Fi Security Threat, <http://www.esecurityplanet.com/views/article.php/3869221/Top-Ten-Wi-Fi-Security-Threats.htm>. diakses tanggal 19 Desember 2011.
- [8] “Wired Equivalent Protocol”. [www.unsri.ac.id/upload/arsip/WEP.doc](http://www.unsri.ac.id/upload/arsip/WEP.doc), Computer System Faculty, Sriwijaya University.(2008)
- [9] N, Gopinath K, and Chaskar, Hemant. “All you wanted to know about WiFi Rogue Access Points : A quick reference to rogue AP security threat, Rogue AP detection and mitigation”. <http://www.rogueap.com/rogue-ap-docs/RogueAP-FAQ.pdf> . AirTight Networks 2009.
- [10] Ma, Liran, Teymorian, Amin Y and Cheng, Xiuzhen. “A Hybrid Rogue Access Point Protection Framework for commodity Wi-fi Networks”. *IEEE*



*Communications Society subject matter experts for publication in the IEEE INFOCOM 2008 proceedings.*

- [11] Muhammad Farid Abdillah (2011) “Sistem Pendeteksi Rogue Access Point Menggunakan Aplikasi Berbasis Web dengan Metoda Pengukuran Round Trip Time”. Universitas Indonesia
- [12] Fowler, Martin. (2003). *UML Distilled : A brief Guide to the Standard Object Modelling Language*, Third Edition. USA : Addison Wesley
- [13] Beyah Raheem and Venkataraman Aravind (2011) “Rogue Access Point Detection : Challenge, Solutions, and Future Directions”. IEEE Computer and Reliability Societies



## Lampiran

Tabel L1-1 : Waktu RTT Menggunakan Model 1 *Unauthorized AP*

RAP		AP	
Banyaknya	Waktu (ms)	Banyaknya	Waktu (ms)
Test 1	33	Test 1	30
Test 2	31	Test 2	42
Test 3	29	Test 3	26
Test 4	29	Test 4	33
Test 5	30	Test 5	26
Test 6	30	Test 6	25
Test 7	29	Test 7	24
Test 8	34	Test 8	25
Test 9	29	Test 9	28
Test 10	34	Test 10	33
Test 11	29	Test 11	26
Test 12	31	Test 12	28
Test 13	28	Test 13	34
Test 14	31	Test 14	36
Test 15	31	Test 15	25
<b>Rata-Rata</b>	<b>30.5333333</b>	<b>Rata-Rata</b>	<b>29.4</b>

Tabel L1-2 : Waktu RTT Menggunakan Model 2 *Bridging Connection*

RAP		AP	
Banyaknya	Waktu (ms)	Banyaknya	Waktu (ms)
Test 1	9	Test 1	2
Test 2	4	Test 2	6
Test 3	13	Test 3	2
Test 4	16	Test 4	3
Test 5	4	Test 5	2
Test 6	4	Test 6	6
Test 7	5	Test 7	6
Test 8	6	Test 8	3
Test 9	4	Test 9	2
Test 10	5	Test 10	2
Test 11	8	Test 11	3
Test 12	6	Test 12	3
Test 13	4	Test 13	2
Test 14	4	Test 14	8
Test 15	4	Test 15	1
<b>Rata-Rata</b>	<b>6.4</b>	<b>Rata-Rata</b>	<b>3.4</b>

Tabel L1-3 : Pengukuran Load Time / Network

<b>Banyaknya</b>	<b>Waktu (detik)</b>
Test 1	5176.2566
Test 2	5181.9396
Test 3	5213.3207
Test 4	5220.9356
Test 5	5215.5899
Test 6	5106.9453
Test 7	5234.1384
Test 8	5279.7276
Test 9	5282.7683
Test 10	5282.7683
Test 11	5229.0163
Test 12	5192.9770
Test 13	5160.3956
Test 14	5225.3215
Test 15	5201.2531
<b>Rata-Rata</b>	<b>5213.5569</b>

Tabel L1-4 : Pengukuran Load Time Deteksi Perangkat Online

Load time Host Computer		Load time AP	
<b>Banyaknya</b>	<b>Waktu (Detik)</b>	<b>Banyaknya</b>	<b>Waktu (detik)</b>
Test 1	0.5714	Test 1	5.0767
Test 2	0.6847	Test 2	5.1017
Test 3	0.6344	Test 3	5.0898
Test 4	0.5897	Test 4	5.0513
Test 5	0.5835	Test 5	5.0308
Test 6	0.5844	Test 6	5.0329
Test 7	0.6547	Test 7	5.0312
Test 8	0.6766	Test 8	5.0335
Test 9	0.6573	Test 9	5.0602
Test 10	0.5496	Test 10	5.0444
Test 11	0.5309	Test 11	5.0428
Test 12	0.5425	Test 12	5.0339
Test 13	0.5305	Test 13	5.0493
Test 14	0.5438	Test 14	5.0782
Test 15	0.682	Test 15	5.073
<b>Rata-Rata</b>	<b>0.60106667</b>	<b>Rata-Rata</b>	<b>5.055313333</b>

Tabel L1-5 : Pengukuran Load Time Deteksi Perangkat Offline

<b>Banyaknya</b>	<b>Waktu (Detik)</b>
Test 1	27.1327
Test 2	27.0061
Test 3	27.0029
Test 4	26.9791
Test 5	27.0442
Test 6	26.9835
Test 7	27.1324
Test 8	26.8696
Test 9	27.2431
Test 10	27.0456
Test 11	27.327
Test 12	26.9128
Test 13	26.8549
Test 14	27.5147
Test 15	26.855
<b>Rata-rata</b>	<b>27.06024</b>

