

Tugas UAS

Konfigurasi Acces point Achmad



Nama : Rifqi Fadil Fahrial
NIM : 1222646

Mata Kuliah: Komputer dan jaringan dasar
Dosen Pengampu: Dani Pradana Kartaputra, S.Si., M.T

TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
STMIK BANDUNG
2024

1 Tugas

Pada sebuah kantor seorang manajer bernama Achmad menginginkan ruangnya memiliki jaringan hotspot tersendiri, berbeda dengan bawahannya. Achmad menginginkan hanya ada 6 clients saja yang dapat terkoneksi dengan access point tersebut. meskipun sudah dibatasi dengan penggunaan *mac filtering* pada 6 clients, Achmad masih tidak puas dan menginginkan hotspotnya memiliki *password security*. . . Achmad mengetahui bahwa ada bawahannya yang mengerti tentang *hacking* pada jaringan *wireless*. . . Pada suatu waktu Achmad menyadari bahwa hotspotnya memiliki pengunjung gelap. Achmad mengetahui *mac address* pengunjung gelap tersebut dan menginginkan pengunjung gelap tersebut tidak dapat terkoneksi ke hotspot miliknya. Koneksi internet hotspot tersebut didapat dari *access point* di ruang IT. kedua *access point* (AP IT dan AP ruangan Achmad) harus di konfigurasi terlebih dahulu agar ruangnya memiliki koneksi internet. Berikanlah solusi untuk hal tersebut. diatas

2 Penyelesaian

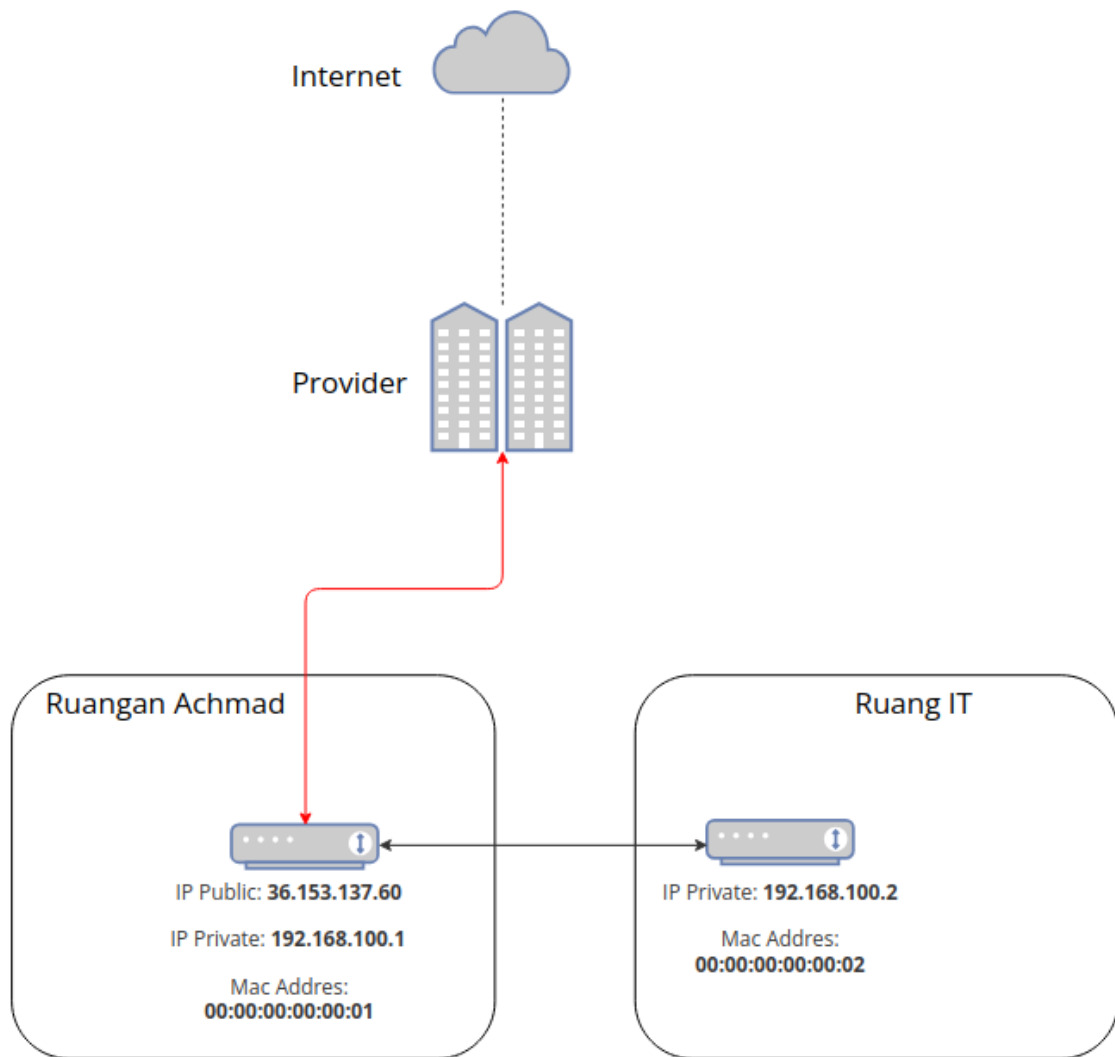
2.1 Penjabaran

Berdasarkan informasi diatas maka harus mengkonfigurasi:

1. Mengkonfigurasi *Access Point* agar terkoneksi dengan internet. . .
2. membatasi pengguna maksimal 6 pengguna dengan *Mac filtering*. . .
3. menambahkan *password security* pada *access point*. . .
4. mengatasi *hacker* pada jaringan di *access point* Ruang IT agar tidak terhubung dengan hotspot. . .

2.2 Mengkonfigurasi *Access Point* agar terhubung dengan internet

Untuk menghubungkan jaringan ini dengan internet maka harus ditentukan dahulu Host dari jaringan ini dan Acces point lainnya sebagai *repeater* agar memudahkan proses konfigurasi. . . oleh sebab itu maka Ruangan Achmad menjadi Hostnya dan Ruangan IT menjadi Repeaternya kemudian *access point* Achmad terhubung dengan koneksi fiber dengan provider internet untuk mendapatkan koneksi internet dan menerima *IP Public* untuk menjelajah internet. . .



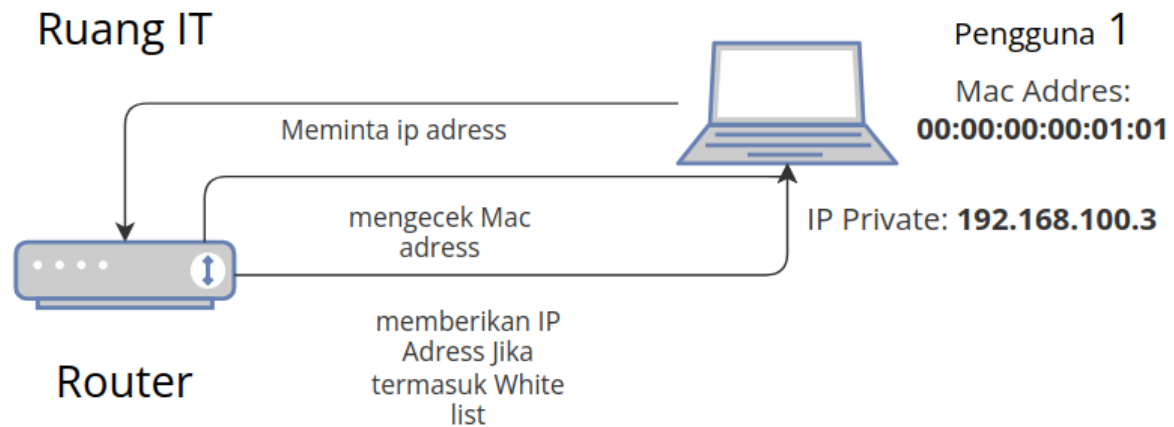
Gambar 1: Gambar Koneksi antara *Access Point* ruang Acmhad dan Ruang IT agar terhubung dengan internet

berdasarkan gambar 1 dapat terlihat bahwa *access point* ruang Acmhad dan Ruang IT terhubung dengan internet...

2.3 Membatasi pengguna maksimal 6 pengguna dengan *Mac filtering*

Kemudian untuk Pengguna dari jaringan ini maka diberlakukan sistem *Mac Filtering* yang bekerja sebagai penjaga dari koneksi dari perangkat yang tidak dikenal... hal ini dapat dikonfigurasi pada *Acces Point* pada Ruang it jika 6 perangkat itu ada pada ruang IT dan tidak ada pada ruang Acmhad...

untuk membatasi pengguna menggunakan *Mac Filtering* maka diberlakukan *Whitelist* dan *Blacklist* dari *Mac Address* yang terhubung dengan *access point*, jika *Mac Adress* dari perangkat berada pada *whitelist* maka perangkat tersebut dapat terhubung ke *access point* dan sebaliknya dengan *Blacklist*...



Gambar 2: Gambaran Mac Filtering

misalkan ada perangkat baru yang dimiliki oleh Abidin ingin terhubung dengan *Acces Point* di ruang IT maka abidin meminta IP Address kepada *Acces Point* yang kemudian membaca *Mac Address* dari perangkat abidin, Jika *Mac Address* nya berada pada *Blacklist* maka perangkat Abidin Tidak dapat terhubung dengan *Access Point* dan menerima koneksi internet, namun jika berada dalam *Whitelist* maka dapat terhubung dengan *Acces Point* dan menerima Koneksi Internet... Misalkan ada 6 perangkat yang diizinkan maka dapat dibuatkan *Whitelist* pada *Acces Point* seperti Berikut:

Perangkat	Mac Addres	Status
Perangkat 1	00:00:00:00:01:01	Diizinkan
Perangkat 2	00:00:00:00:01:02	Diizinkan
Perangkat 3	00:00:00:00:01:03	Diizinkan
Perangkat 4	00:00:00:00:01:04	Diizinkan
Perangkat 5	00:00:00:00:01:05	Diizinkan
Perangkat 6	00:00:00:00:01:06	Diizinkan

2.4 Menambahkan *password security* pada *Access Point*

Kemudian Untuk menambahkan Keamanan dari *Acces Point* maka diberlakukannya sistem Password untuk Perangkat baru yang ingin terhubung dengan *Acces Point* untuk mencegah dari perangkat yang tidak dikenal terhubung dan melakukan kejahatan pada Jaringan ini... Untuk menambahkan *password security* pada *Acces Point* pada ruang IT dan ruang Acmhad maka diberlakukannya *Password Security* seperti berikut:

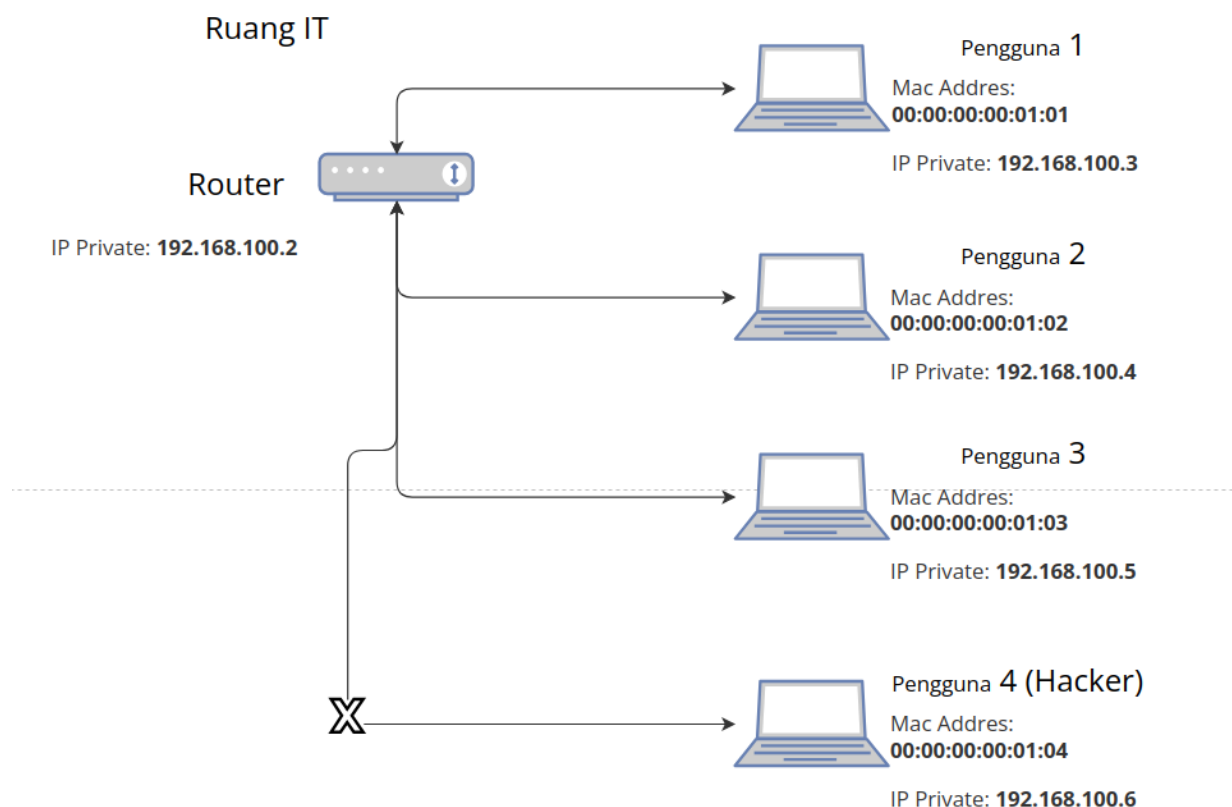
Nama Acces Point	Sistem password	Password
Access Point Achmad	WPA2-PSK	Admin#1234
Acces Point Ruang IT	WPA2-PSK	password

yang nantinya jika ada perangkat baru yang ingin melakukan koneksi dengan *Access Point* maka akan diminta password untuk terhubung dengan *Access Point*, jika benar memasukan password yang benar maka perangkat tersebut akan menerima koneksi internet dan sebaliknya...

2.5 Mengatasi *hacker* pada *Access Point*

Kemudian untuk mengatasi hacker yang terhubung pada jaringan maka cara mengatasinya adalah dengan mengidentifikasi dari perangkat mana yang terindikasi Hacker kemudian carilah *Mac Address* dari hacker tersebut dan kemudian masukan pada *Blacklist* pada *Access Point* sehingga hacker tersebut tidak dapat terhubung dengan *Access Point* meskipun mengetahui password dari *Access Point* yang kemudian dapat diketahui siapa yang menjadi hacker tersebut dari perangkatnya yang tidak terhubung dengan *Access Point*... untuk melakukan *Blacklist* maka perlu dilakukan pengisian *Blacklist* pada *Access Point* yang kemudian diisi oleh *Mac Address* dari perangkat hacker yang terindikasi, contohnya:

Nama Pengguna	Mac Address	Status
Pengguna 4	00:00:00:00:01:04	Diblokir



Gambar 3: Simulasi *Blacklist*

berdasarkan gambar 3 dapat terlihat jika perangkat yang terindikasi hacker telah teridentifikasi dan *Mac Address* dari perangkat hacker telah ditemukan kemudian dimasukan ke dalam *Blacklist* pada *Access Point*...