Wireless Access Management

Certified Mikrotik Training Advance Wireless Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

Training Outline

Access Management :

- Access List
- Connect List
- Centralized Access List Management:
  - Radius Mac Authentication

VAP !

Access Management

- **default-forwarding** (on AP) – pilihan dimana wireless client boleh berkomunikasi dengan client yang lain secara langsung atau tidak. (bisa dikonfigurasi lebih detail per client di **access-list**).
- **default-authentication** – kebijakan yang diambil untuk wireless client atau wireless AP yang tidak dikonfigurasi secara khusus di Access-list atau di **connect-list**.
- Kedua opsi tersebut menjadi tidak berfungsi atau diabaikan jika setting khusus terhadap sebuah wireless client atau bisa juga wireless AP yang dilakukan di access-list dan connect-list.

Access Management

- Sangat dimungkinkan untuk memasang beberapa filter untuk mac-address yang sama dan juga satu rule untuk semua mac-address.
- Sebuah rule filter mac-adress bisa diterapkan pada sebuah interface wireless saja atau bisa juga untuk semua interface.
- Jika tidak ada rule yang sesuai maka akan digunakan default policy (**default authentication** & **default forward**) dari wireless interface tersebut.

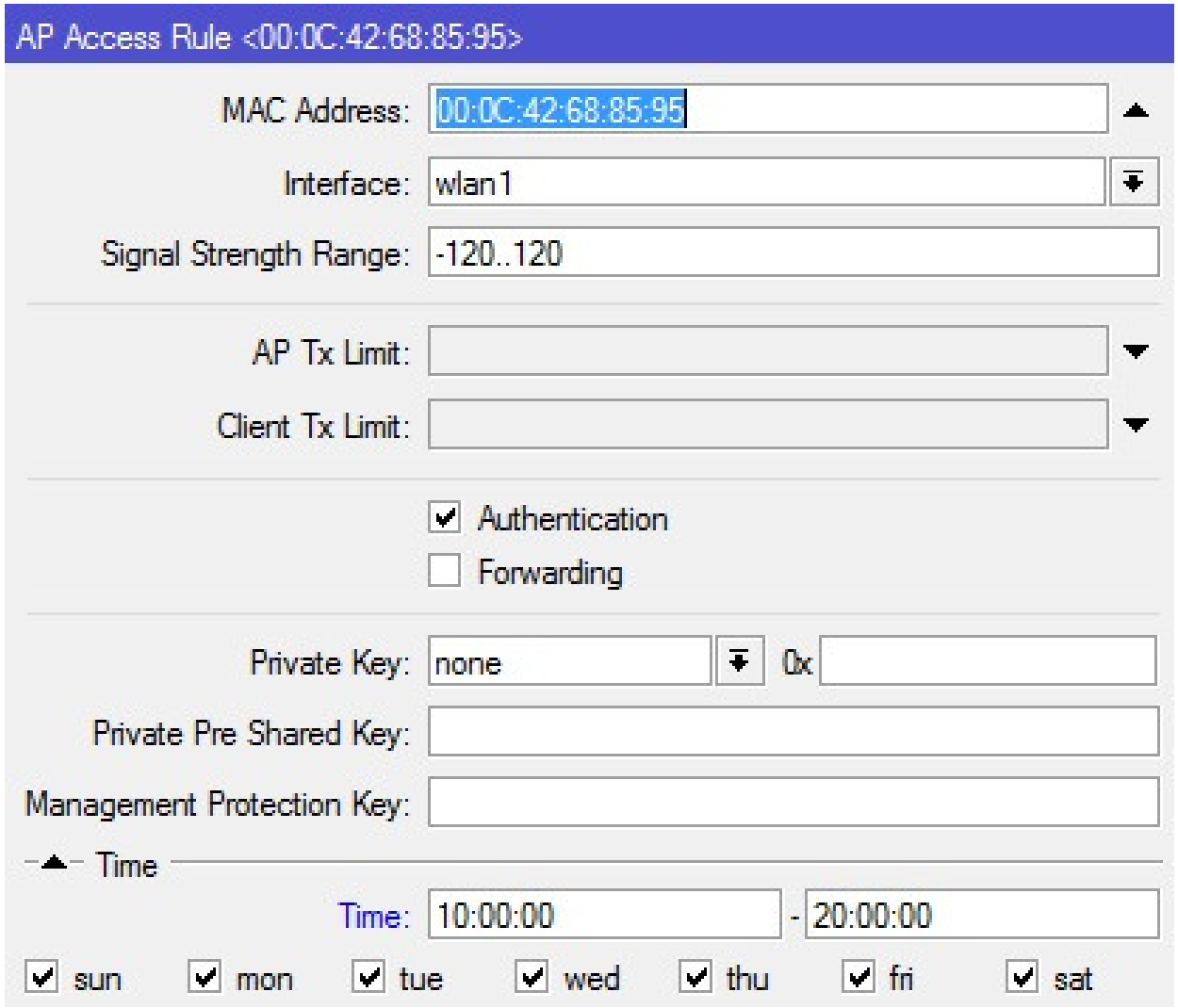
Wireless Access/Connect Lists

- **Access List** – adalah filter autentikasi sebuah AP (mode Access Point) terhadap client yang terkoneksi.
- **Connect List** – adalah filter autentikasi sebuah wireless client (mode Station) terhadap AP mana yang ingin terkoneksi.
- Rule autentikasi atau filter autentikasi dibaca secara terurut dari atas ke bawah seperti halnya sebuah filter firewall sampai request autentikasi mencapai kecocokan.

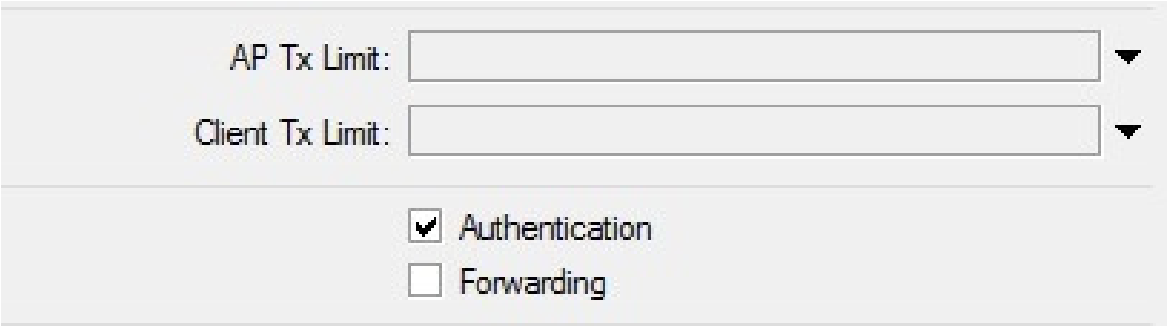
Wireless Access List

- Mampu membatasi autentikasi client tertentu berdasarkan kekuatan signalnya (signal stregth).
  - **Contoh**: hanya memperbolehkan client dengan signal bagus yang boleh terkoneksi jika tidak maka client tidak bisa terkoneksi sama sekali.
- Mampu untuk membatasi autentikasi client tertentu berdasarkan waktu yang sudah ditentukan.
  - **Contoh**: hanya memperbolehkan client bisa terkoneksi pada hari weekend saja.
- Mampu untuk membatasi autentikasi client berdasarkan ketentuan security tertentu.
  - **Contoh**: memperbolehkan client hanya bisa terkoneksi menggunakan WPA key tertentu.

Access List

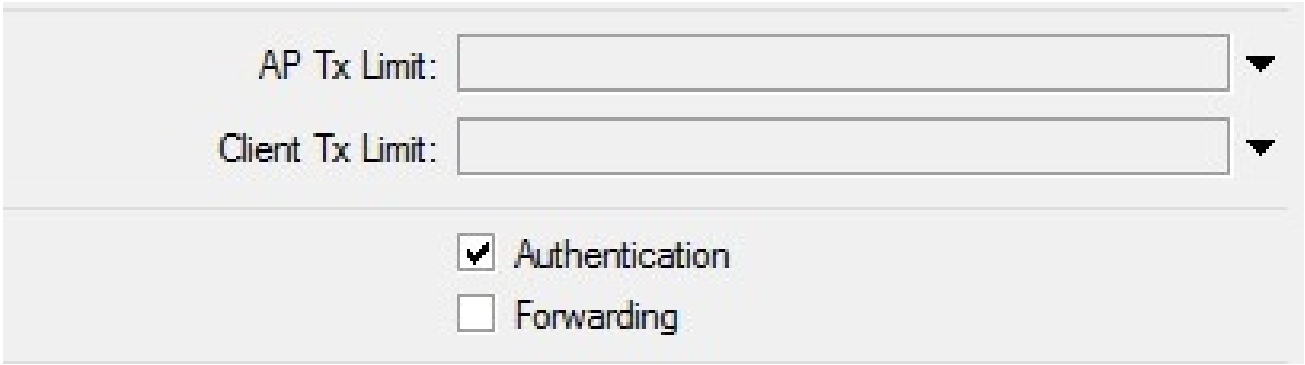

AP Access Rule <00:0C:42:68:85:95>
MAC Address: 00:0C:42:68:85:95
Interface: wlan1
Signal Strength Range: -120..120
AP Tx Limit:
Client Tx Limit:
Authentication
Forwarding
Private Key: none 0x
Private Pre Shared Key:
Management Protection Key:
Time
Time: 10:00:00 - 20:00:00
sun mon tue wed thu fri sat

Autentication



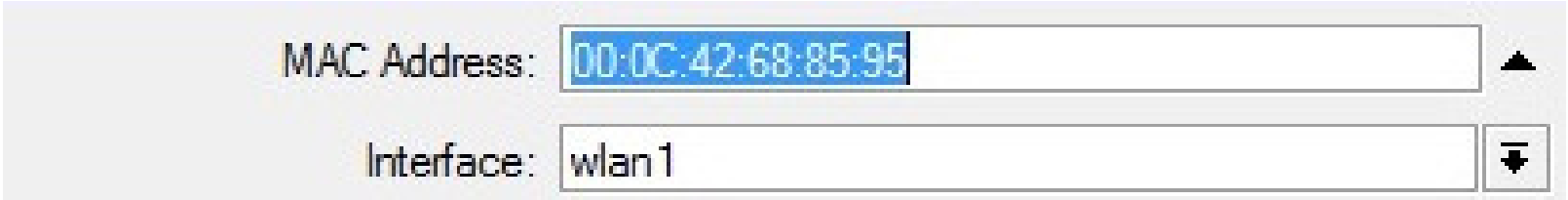
- **authentication** (yes or no) :
  - **no** – client tidak akan pernah terkoneksi.
  - **yes** – akan mengautentikasi client dan akan dilanjutkan dengan meminta prosedur keamanan sesuai dengan parameter **security-profile** di interface.
- **forwarding** (yes or no) :
  - **no** – client tidak akan bisa mengirimkan frame ke client yang lain walaupun masih terkoneksi dengan AP yang sama.
  - **yes** – client bisa mengirimkan frame data ke client lain yang terkoneksi ke AP yang sama.

Limit



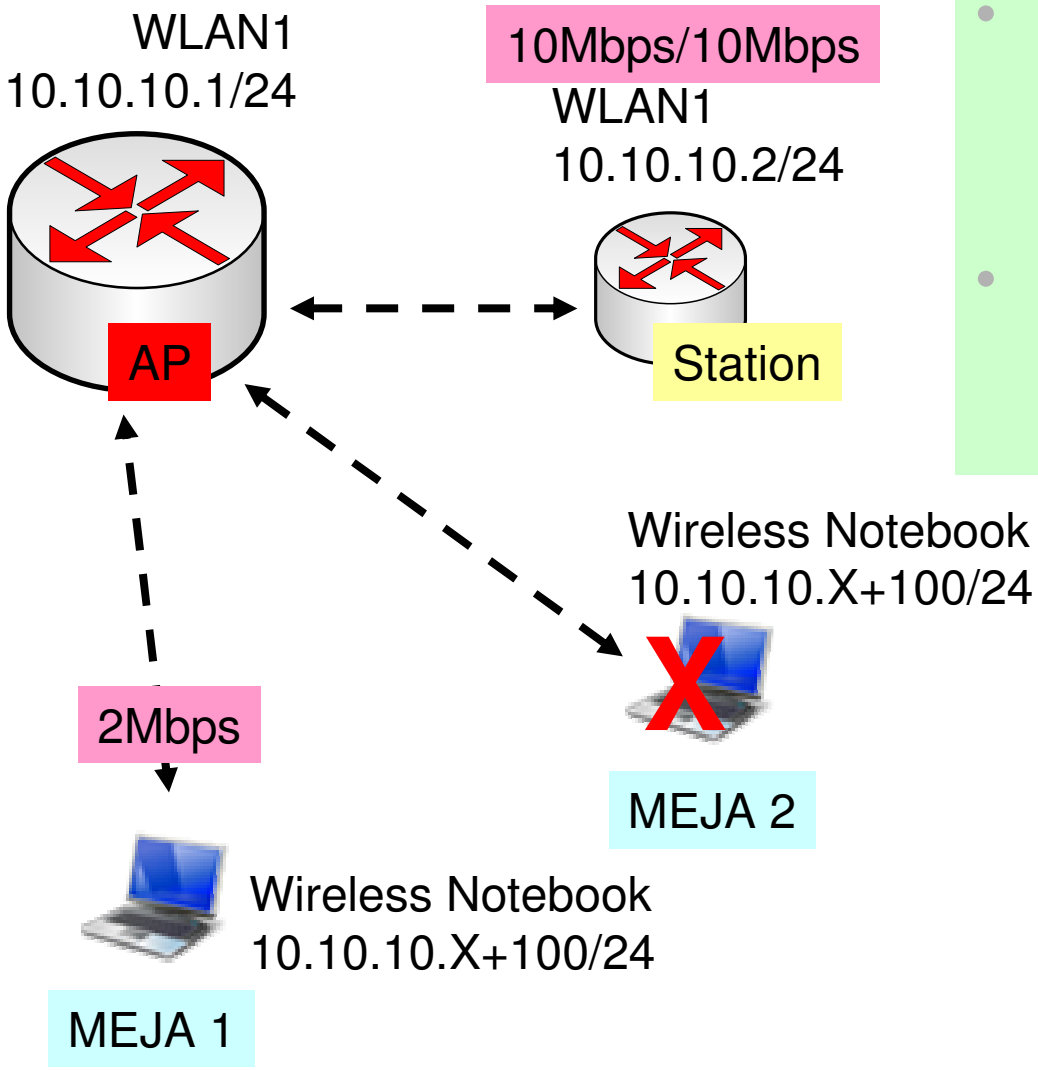
- **ap-tx-limit** (default : 0) : limit kecepatan data dari ap ke client. Nilai 0 berarti tidak terlimit.
- **client-tx-limit** (default : 0) : akan meminta client untuk membatasi kecepatan transmisinya. Nilai 0 berarti tidak terlimit. Fungsi in hanya berjalan di sesama RouterOS

Mac-address & Interface



- **mac-address** (default: 00:00:00:00:00:00) : Adalah parameter Untuk memasang filter terhadap client yang menggunakan mac-address tertentu.
  - Nilai default yaitu 00:00:00:00:00:00 melambangkan semua mac-address.
- **interface** (default: all) : adalah parameter untuk menetukan interface mana yang akan menggunakan filter tersebut.
  - Nilai default **All** berarti rule ini akan digunakan di semua interface di router.

[LAB-1] Access List Mac filter

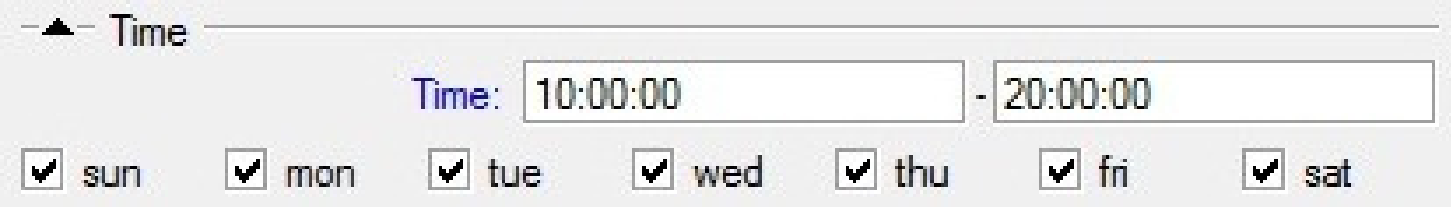


- Gunakan filter Mac-address untuk menetukan client yang terkoneksi.
- Aktifkan rate limit berbeda untuk tiap client.

Range Signal

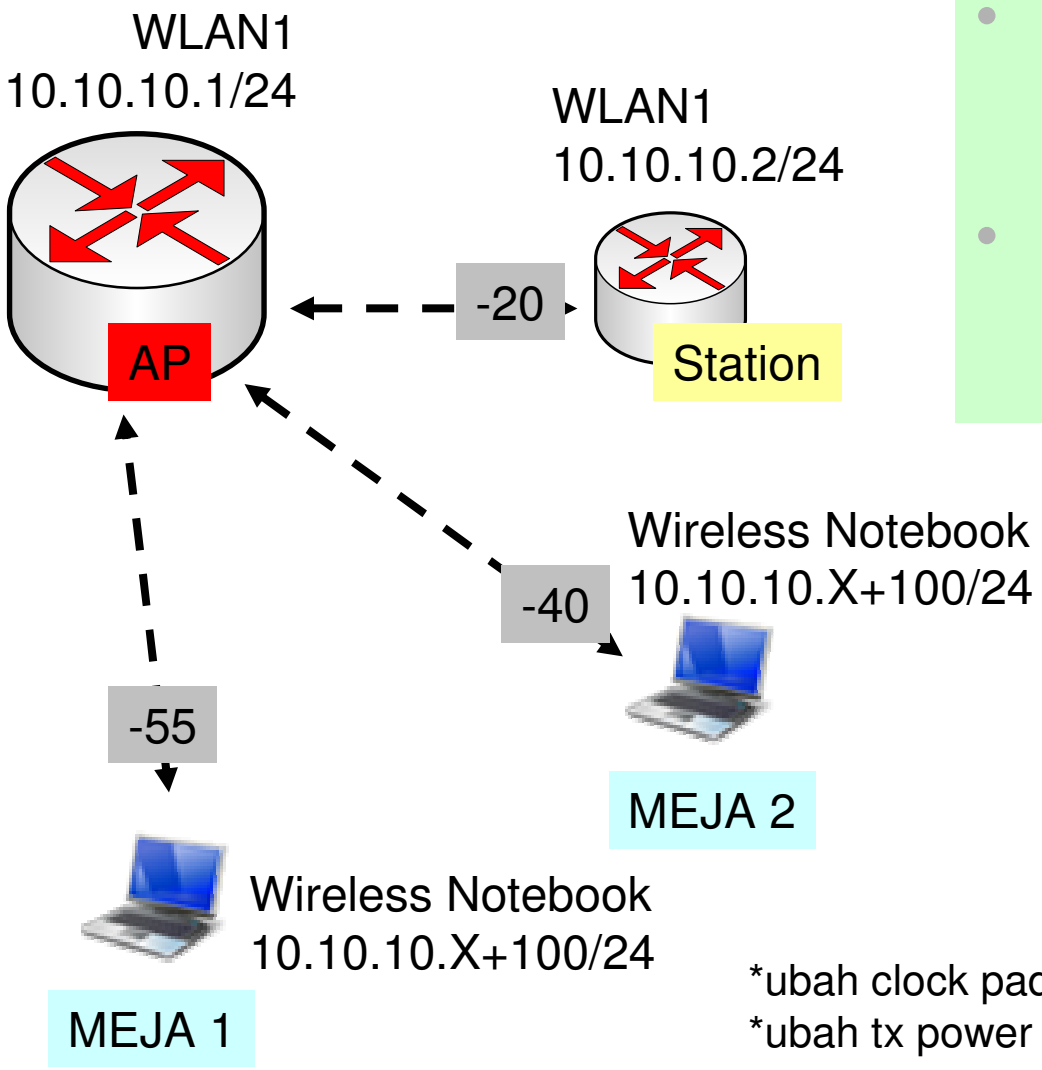
- **signal-range** (NUM..NUM – kedua parameter NUM adalah range antara -120..120; default : -120..120) : adalah paremeter untuk membatasi client yang terkoneksi dengan kekuatan signal tertentu.
  - Client hanya bisa terkoneksi jika signal strength yang didapatkannya masuk dalam range yang sudah ditentukan. Jika signal mengalami perubahan dan tidak masuk dalam range maka client akan diputus koneksinya.

Time



- **time** (TIME-TIME,sun,mon,tue,wed,thu,fri,sat - TIME adalah interval waktu 0..86400 seconds) : Rule ini akan dijalankan sesuai dengan waktu dan hari yang sudah ditentukan.

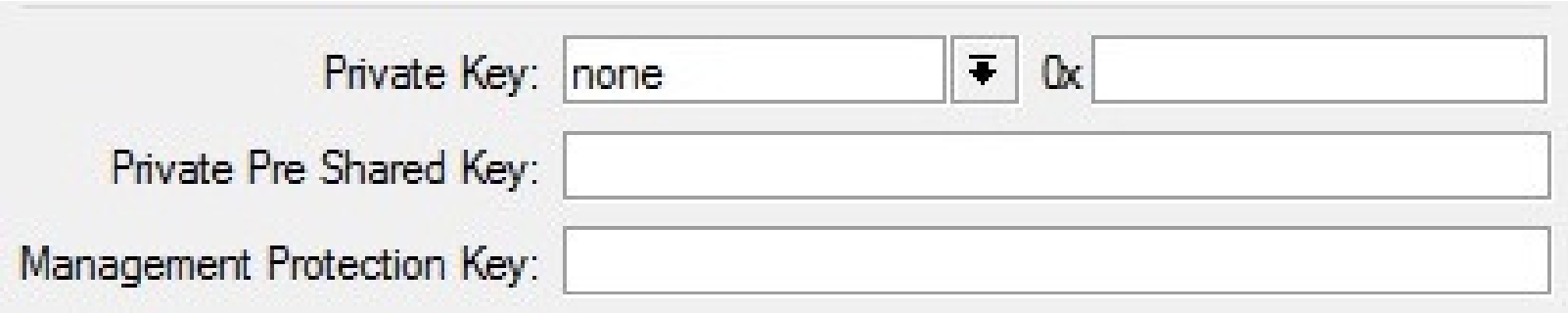
[LAB-2] Access List Signal filter



- Gunakan filter Signal untuk menetukan client yang terkoneksi
- Tentukan waktu koneksi yang berbeda untuk tiap client

*ubah clock pada router untuk test pada seting time
*ubah tx power supaya mempengaruhi signal

Security Policy

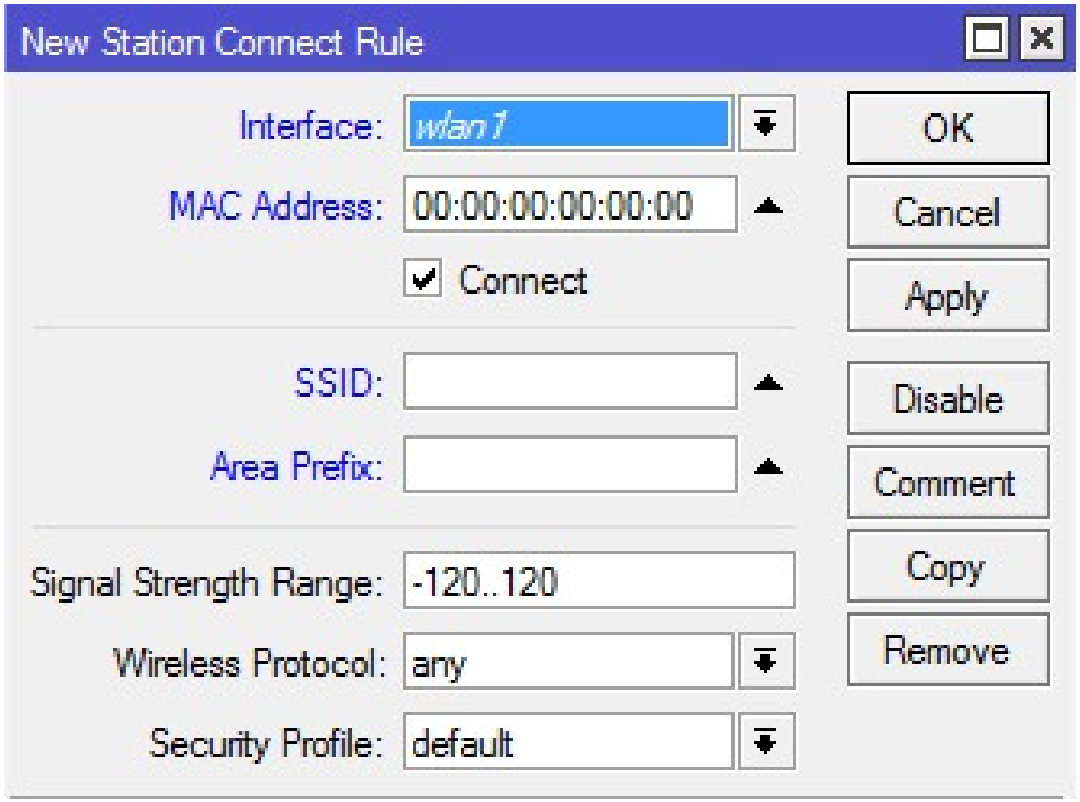


- private-algo (none, 40bit-wep, 104bit-wep, aes-ccm or tkip) : algoritma enkripsi WEP.
- private-key : kunci enkripsi WEP
- private-pre-shared-key : digunakan untuk metode kamanan WPA PSK.

Wireless Connect List

- Connect-list – digunakan untuk memberikan prioritas dan mengimplementasikan beberapa parameter keamanan pada sebuah wireless interface client yang akan terkoneksi pada sebuah AP.
- Hampir sama dengan access-list, Connect-list juga berbentuk kumpulan beberapa rule yang akan dibaca terurut dari atas ke bawah. Tetapi tidak seperti access-list, setiap rule connect-list hanya bisa diimplementasikan pada interface wireless yang spesifik.
- Klasifikasi filtering pada Rule connect-list bisa berupa MAC-address dari AP, signal strength dan beberapa parameter lain.

Connect List



connect (yes or no) :

yes – terkoneksi ke AP yang sesuai dengan rule.

no – tidak terkoneksi ke AP yang sesuai dengna rule

Connect List - Operation

- Rule Connect-list akan dibaca terurut dari atas ke bawah.
- Rule yang tidak aktif akan diabaikan.
- Jika ada beberapa rule connect-list yang memiliki klasifikasi yang sesuai (**mac-address,signal-strength**) maka rule yang digunakan adalah rule paling awal.
- Jika tidak terdapat rule yang cocok pada sebuah access point, maka kebijakan default yang akan digunakan (**default authentication**).

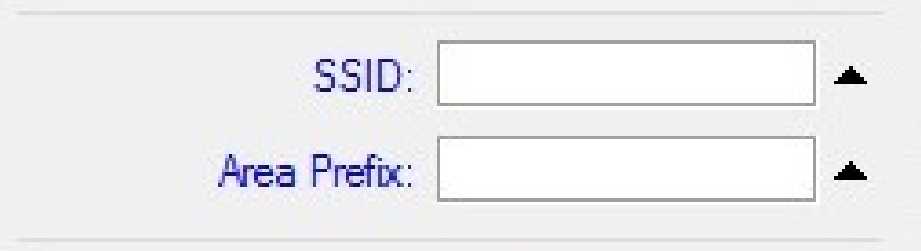
Connect List – Operation (2)

- Jika terdapat rule yang cocok pada sebuah access point dan terdapat parameter **connect=no** maka koneksi ke AP tersebut tidak akan dilakukan.
- Jika terdapat rule yang cocok pada sebuah access point dan terdapat parameter **connect=yes** maka koneksi ke AP tersebut akan dilakukan.
- Pada mode access point, rule connect list akan dipertimbangkan terlebih dahulu sebelum membuat link WDS ke perangkat AP lain. Jika tidak ada rule yang cocok pada connect-list maka interface akan menggunakan kebijakan default (**default authentication**) sebagai parameter penentu pembuatan link WDS.

Connect List – Mac address

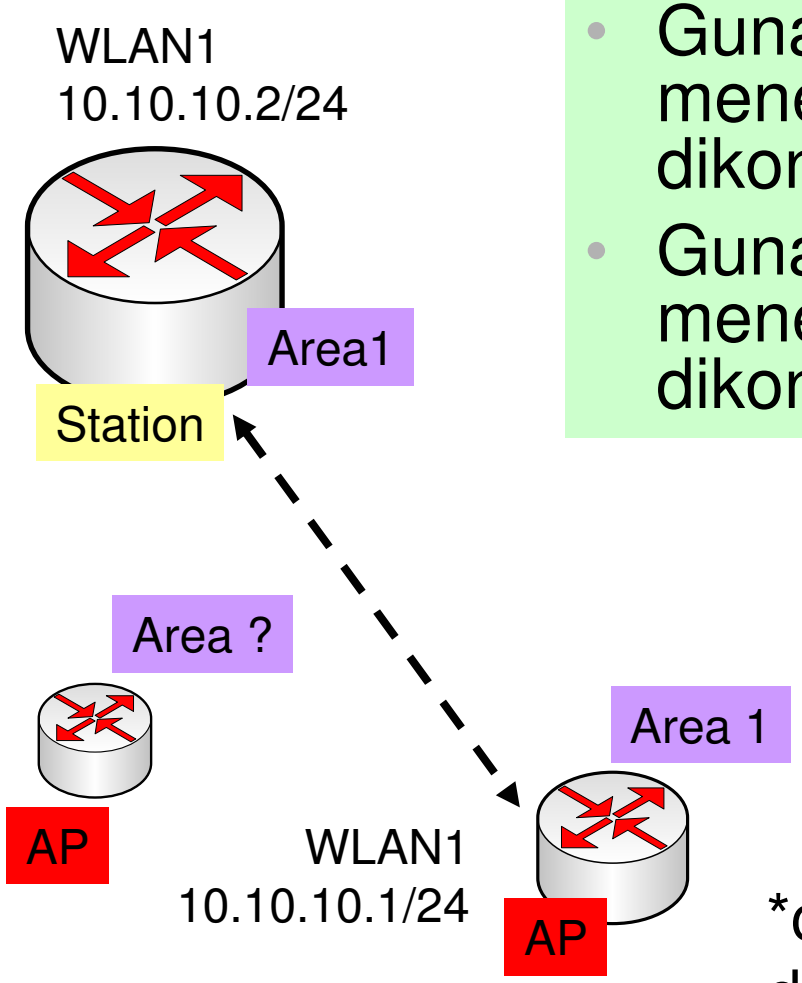
- **interface** – nama interface untuk rule yang akan dibuat, hanya bisa menggunakan satu interface untuk tiap rule.
- **mac-address** (default : 00:00:00:00:00:00) : untuk menentukan mac-address dari AP. Nilai default 00:00:00:00:00:00 berarti semua mac-address.

Connect List – SSID



- **area-prefix** (text) : parameter klasifikasi untuk menentukan nilai area dari sebuah AP. Hanya bisa digunakan di perangkat Mikrotik.
- **ssid** (text) : parameter klasifikasi untuk menetukan SSID dari AP yang ingin dikoneksikan, jika dikosongkan berarti semua ssid.
  - Parameter ini hanya berfungsi jika mode station diaktifkan di interface dan parameter ssid di interface tersebut kosong, atau jika pada mode Access Point dan parameter **wds-ignore-ssid=yes**

[LAB-3] Connect List AP Filter

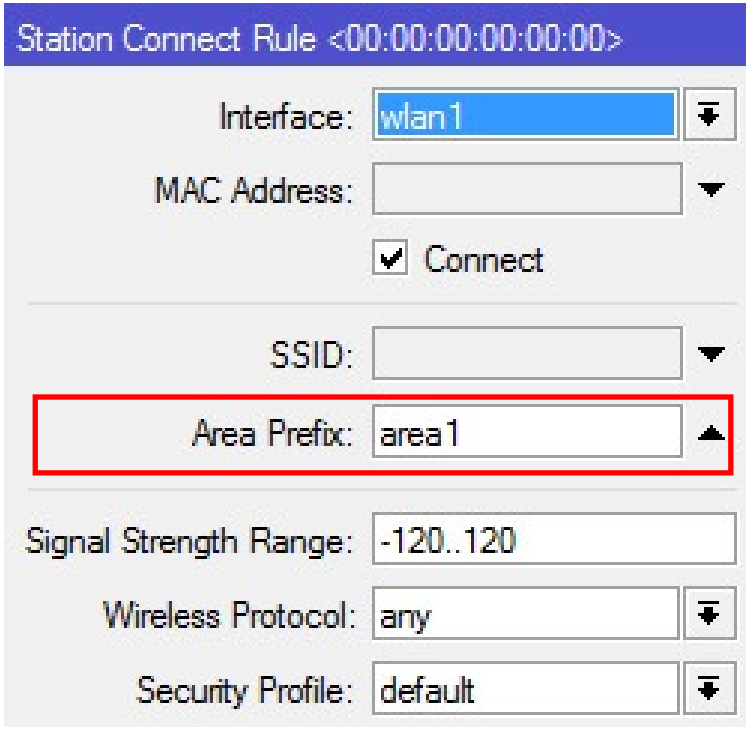


- Gunakan filter Mac-address untuk menetukan AP yang ingin dikoneksikan
- Gunakan filter area untuk menetukan AP mana yang ingin dikoneksikan

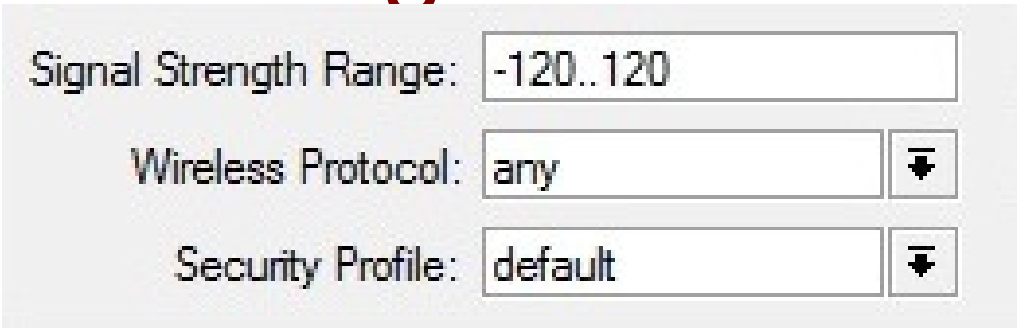
*coba koneksikan ke AP yang lain dengan area yang berbeda

Connect List – Area Filter

- Filter berikut akan memberikan perintah ke wireless client untuk terkoneksi ke AP manapun dengan ssid apapun yang masuk di “area1”

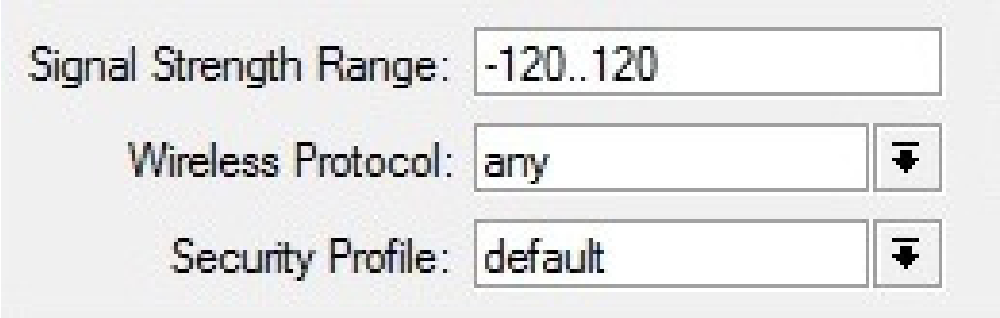


Connect List – Signal Filter



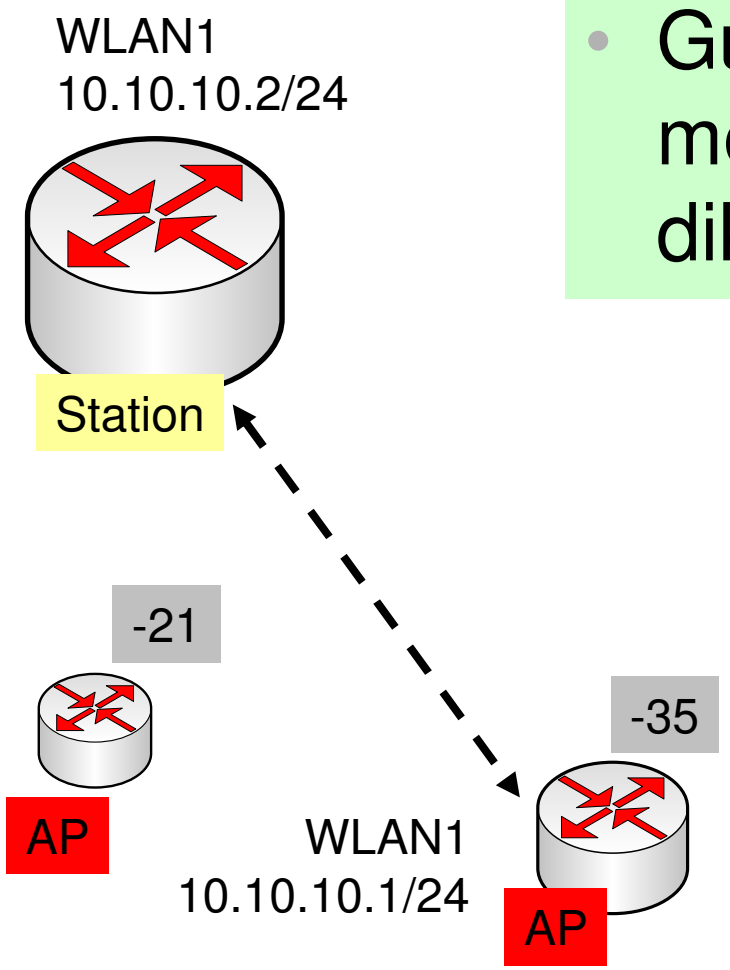
- **signal-range** (NUM..NUM – kedua parameter NUM adalah range antara -120..120; default : -120..120) : adalah paremeter untuk membatasi koneksi ke sebuah AP dengan kekuatan signal tertentu.
  - AP hanya bisa terkoneksi jika signal strength yang didapatkannya masuk dalam range yang sudah ditentukan. Jika signal mengalami perubahan dan tidak masuk dalam range maka koneksi ke AP akan diputus.

Connect List – Security Profile



- **security-profile** (nama security-profile, or none) : adalah nama security profile yang akan digunakan untuk terkoneksi ke sebuah AP. Jika nilai "**none**" digunakan mala kebijakan security yang digunakan adalah kebijakan keamanan yang terpasang di interface.
  - Untuk interface yang mengaktifkan mode AP tidak akan menggunakan parameter ini.

[LAB-4] Connect List Signal Filter

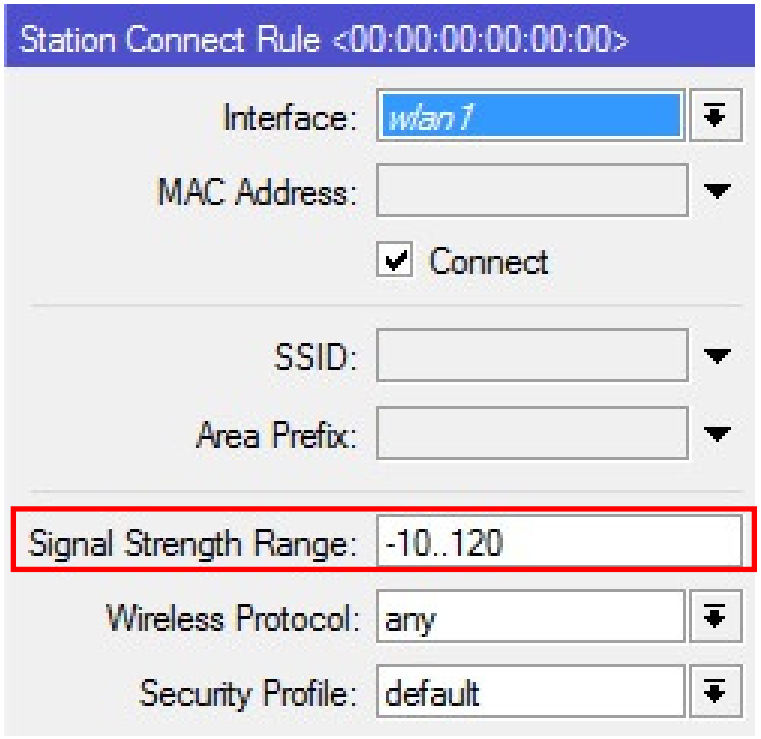


- Gunakan filter signal untuk menetukan AP yang ingin dikoneksikan

*ubah parameter tx-power untuk mempengaruhi signal

Signal Filter

- Rule berikut akan memerintahkan wireless interface yang :
- Menggunakan mode client
- Terkoneksi ke AP mana saja
- Dengan ssid apapun
- Tetapi hanya di AP yang memiliki signal strength minimal -10db



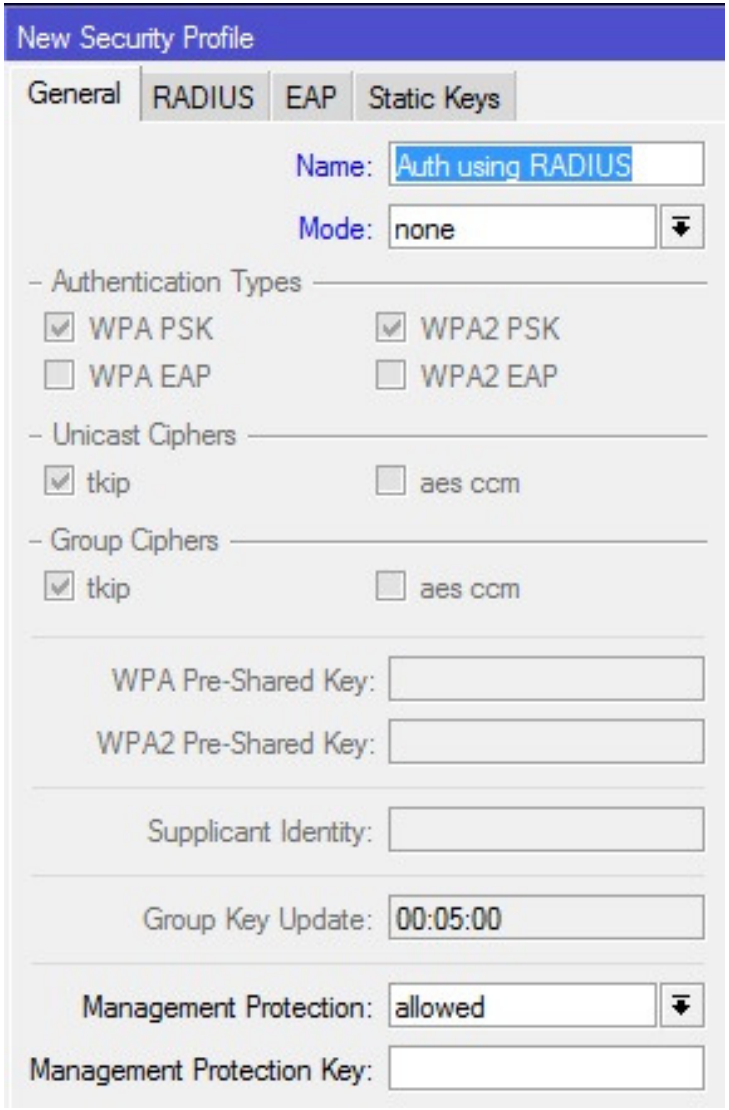
RADIUS MAC Authentication

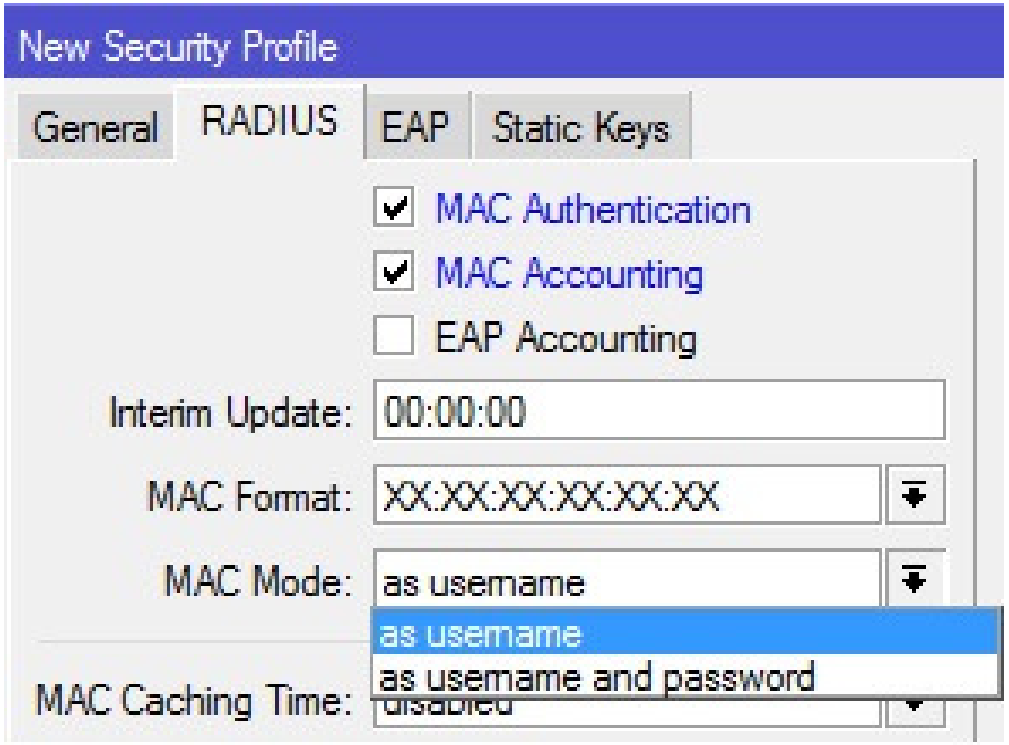
Wireless Mikrotik sudah support untuk melakukan autentikasi mac-address yang tersentralisasi dengan menggunakan bantuan RADIUS server. Termasuk fungsi accounting juga sudah bisa dilakukan untuk memonitor seberapa besar traffic dari client tersebut.

Sudah mampu juga untuk menggunakan fitur “Radius Incoming” yang mampu melakukan pemutusan akses client langsung dari Radius server.

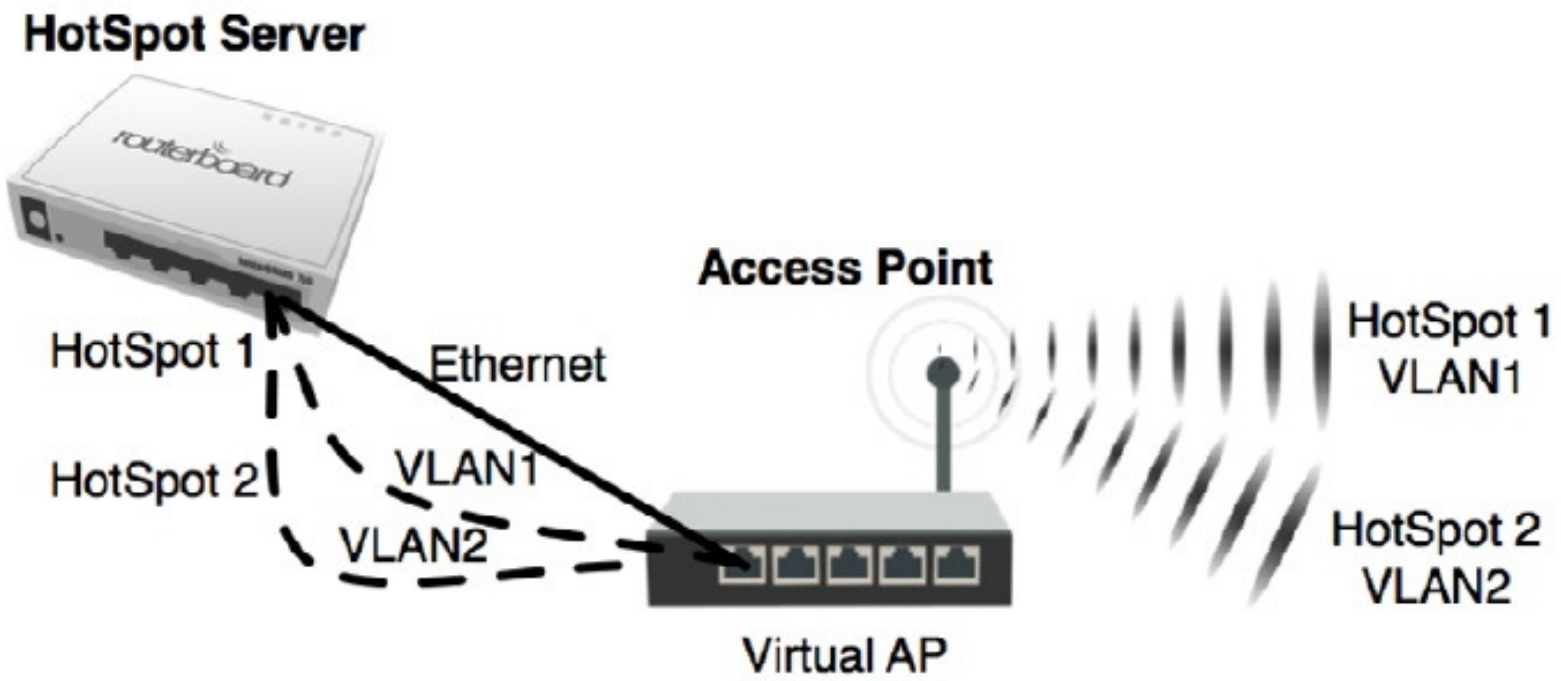
MAC mode – parameter mac-address akan menjadi username saja atau menjadi username dan password di Radius.

Radius Mac Authentication





VAP – Virtual Access Point



- "Virtual Access Point" adalah sebuah entitas logis yang diciptakan dari interface fisik Access Point (AP).
- Ketika sebuah AP secara fisik mendukung beberapa "Virtual AP", maka setiap AP Virtual menjadi sebuah AP virtual yang independen, meskipun hanya ada satu interface fisik.

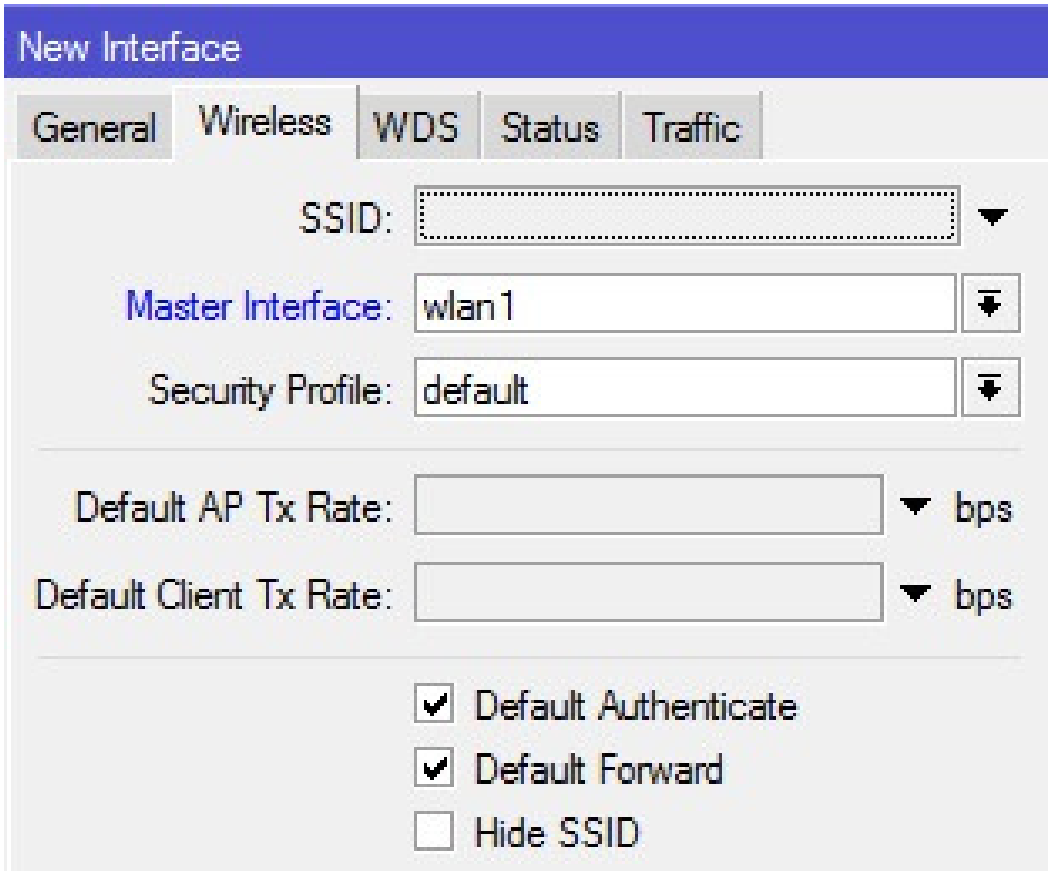
VAP Benefit

- Virtual AP memungkinkan penyedia jaringan untuk menawarkan beberapa layanan yang berbeda, serta memungkinkan untuk beberapa penyedia jaringan untuk berbagi infrastruktur fisik yang sama.
- Keuntungan menggunakan VAP meliputi:
  - **Channel Conservation** – karena adanya regulasi pada setiap negara dan standard komunikasi tertentu yang ada di area yang pentig (ex: bandara), maka penggunaan channel menjadi sangat terbatas. Dengan menggunakan VAP beberapa provider bisa berbagi infrastruktur tanpa melanggar regulasi yang ada.

VAP Benefit (2)

- **Capital expenditure reduction** – tuntutan service yang memadai untuk menunjang perkembangan ekonomi, menyebabkan perlunya efisiensi dalam mengembangkan infrastruktur. Dalam rangka memberikan hasil yang lebih baik pada biaya instalasi dan pemeliharaan infrastruktur nirkabel, adalah lebih hemat untuk membangun infrastruktur dan berbagi di antara beberapa penyedia, daripada untuk membangun infrastruktur yang tumpang tindih

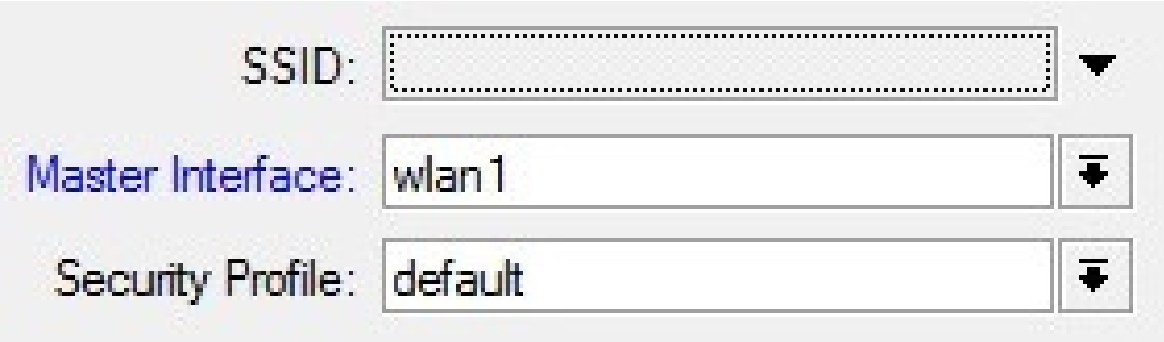
VAP Interface



Mikrotik VAP

- Virtual Access Point (VAP) interface digunakan untuk membuat sebuah AP Logis yang memiliki SSID dan Mac-address yang berbeda. Bisa disamakan seperti operasional VLAN tetapi menggunakan media Wireless.
- Secara teoritis mikrotik mampu untuk menciptakan 128 VAP di setiap interface fisiknya .
- RouterOS mikrotik support VAP pada wireless interface berchipset Atheros AR5212 sampai chipset terbaru saat ini.

VAP - Configuration



- **ssid** (default: MikroTik) – identitas dari wireless network yang akan terdistribusikan oleh VAP
- **master-interface** (name) – interface fisik yang akan digunakan oleh VAP
- **security-profile** (default: default) – security profile yang akan digunakan untuk memberikan parameter security pada jaringan wireless VAP.

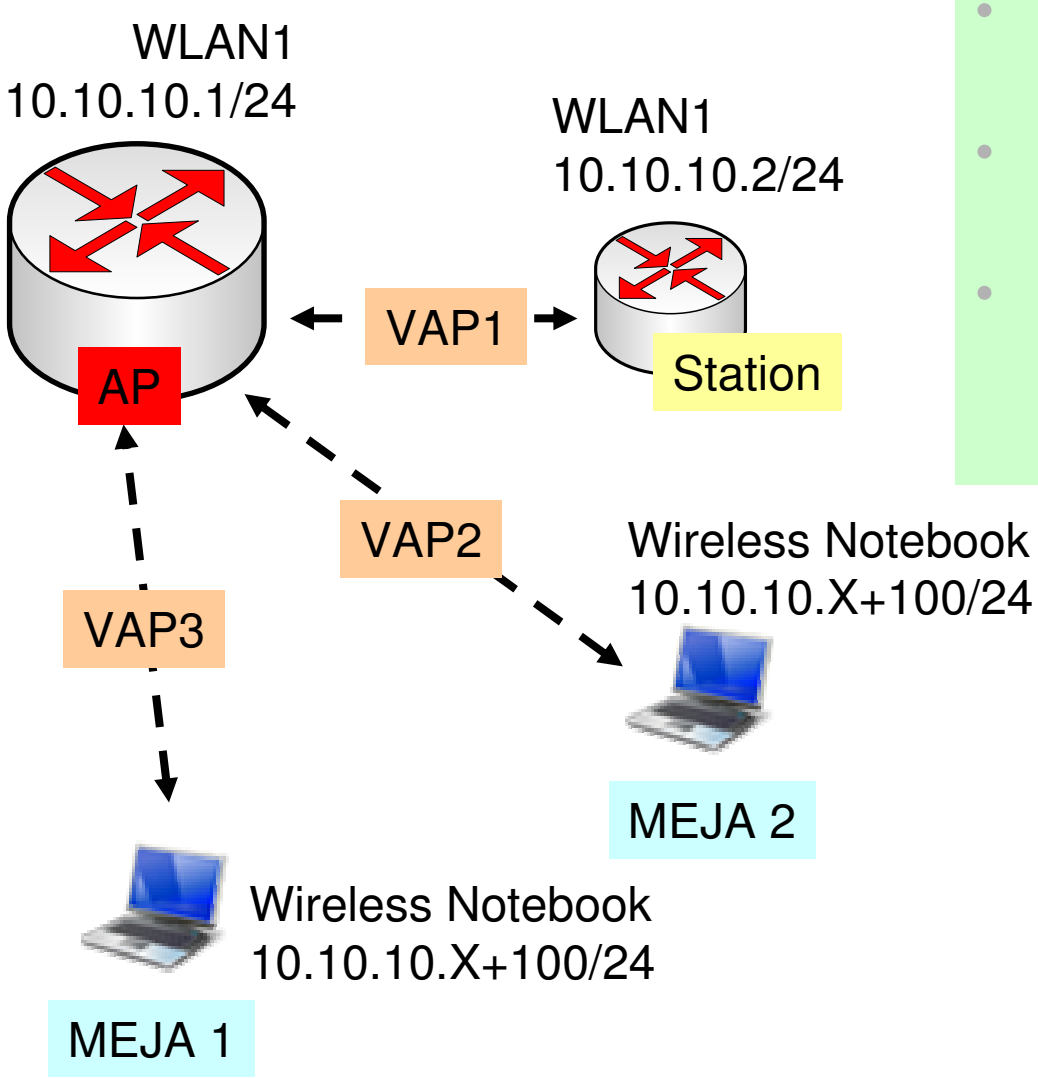
VAP - Limit

- **default-ap-tx-limit** (integer; default: 0) – adalah limit traffic rate untuk pengiriman data dari AP ke tiap client (bps).
  - 0 – berarti tanpa limit
- **default-client-tx-limit** (integer; default: 0) – adalah limit traffic rate untuk pengiriman data dari tiap client ke AP (bps). Hanya bekerja jika client sama-sama menggunakan mikrotik.
  - 0 – berarti tanpa limit

VAP - Authentication

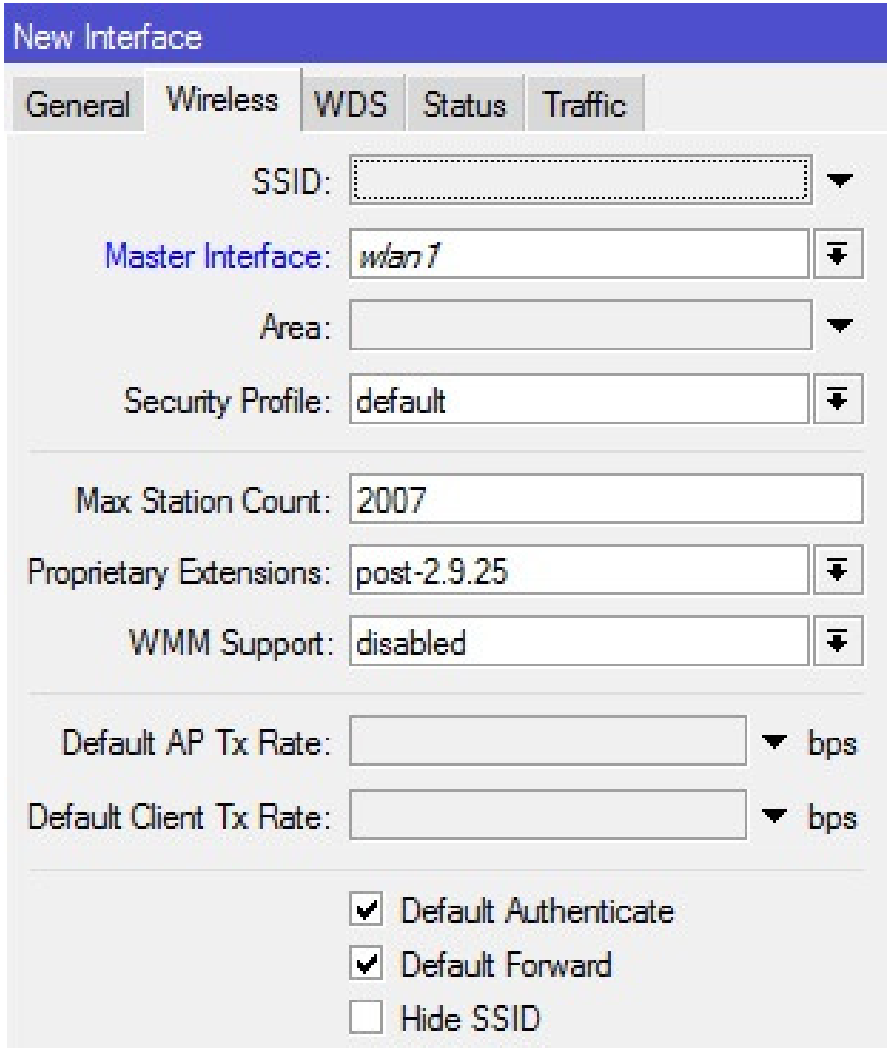
- **default-authentication** (default value: yes) :
  - Jika digunakan mode AP maka semua client yang tidak dibatasi di **access-list** akan diautentikasi dan bisa terkoneksi.
  - Jika digunakan di mode station maka wireless bisa terkoneksi ke AP manapun yang tidak dibatasi di **connect-list**.
- **default-forwarding** (default value: yes) :
  - Adalah parameter yang digunakan untuk forwarding traffic dari client ke client yang lain dalam AP yang sama. Bisa dibatasi lebih spesifik per clientnya di access-list.

[LAB-5] VAP Lab

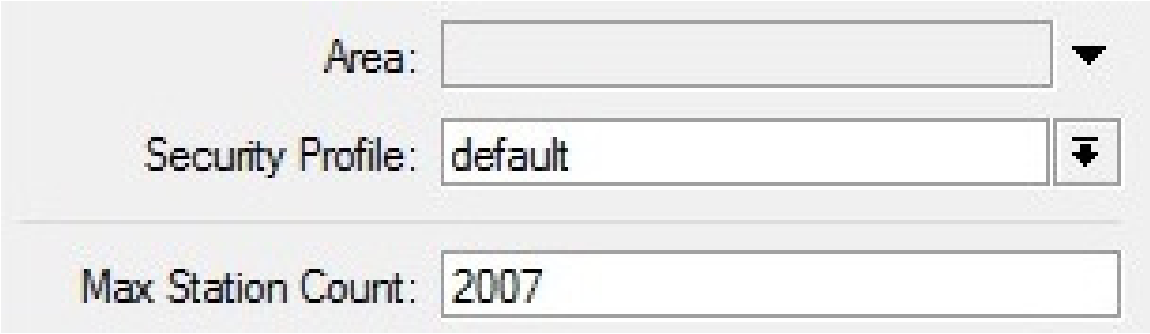


- Buat VAP dan SSID yang berbeda untuk tiap client.
- Tambah ip address untuk tiap VAP interface.
- Routing akan dilakukan untuk menghubungkan client dari setiap VAP.

VAP – Advanced Menu

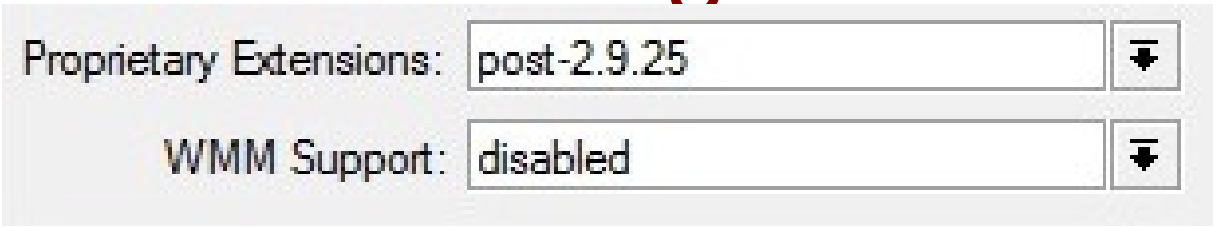


VAP – Advanced Config



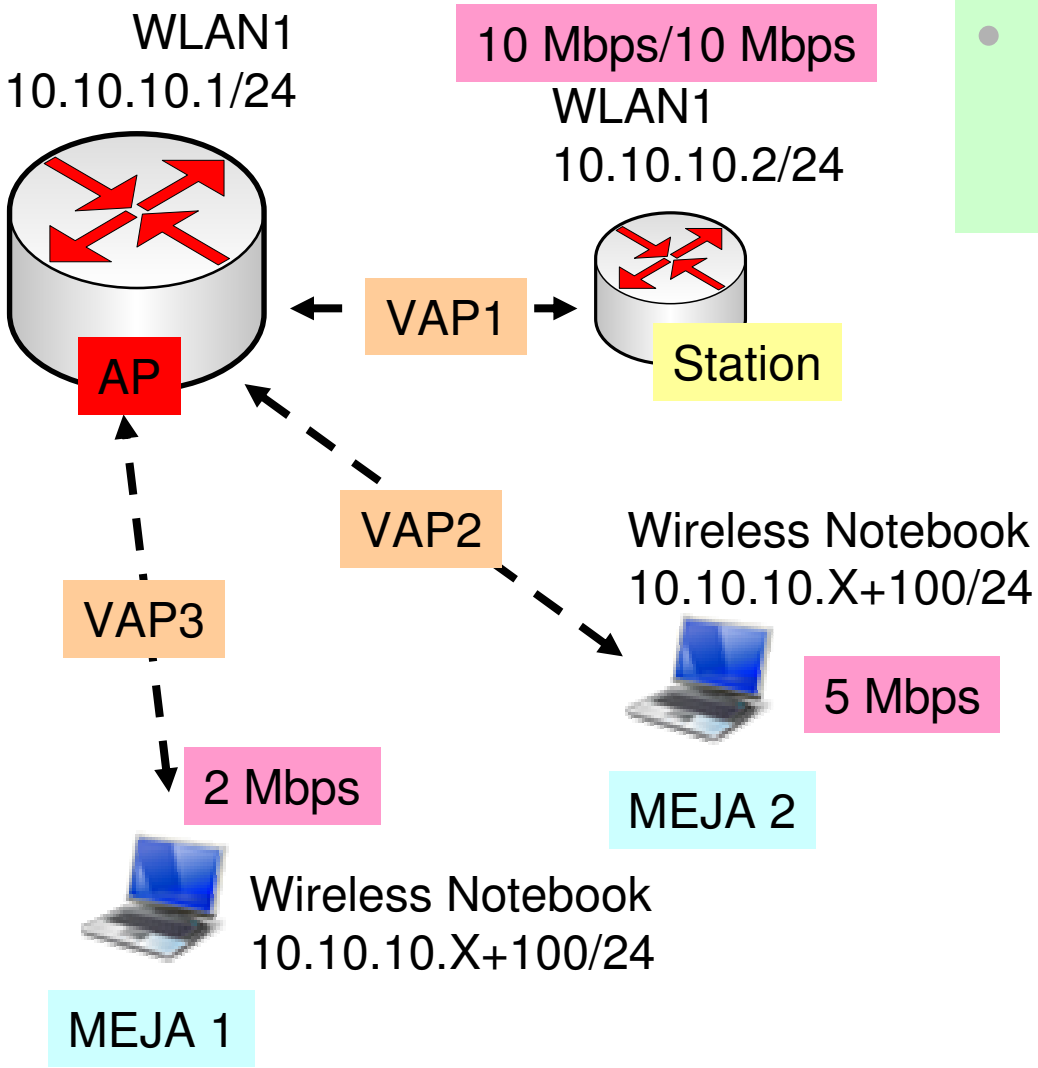
- **area** (default: **""**) – adalah parameter area yang digunakan untuk grouping dari VAP tersebut. Parameter ini juga akan berpengaruh di **connect-list** jika terdapat filter berdasarkan area.
- **max-station-count** (*integer*; default: **2007**) – jumlah client (secara teoritis) yang bisa terkoneksi ke VAP dalam waktu bersamaan.

VAP – Advanced Config



- **wmm-support** (disabled | enabled | required) – option untuk mengaktifkan WMM pada VAP.
- **proprietary-extensions** (default value: post-2.9.25) : RouterOS memiliki metode tertentu untuk melakukan management pengiriman frame data.
  - **pre-2.9.25** – Metode ini compatible dengan RouterOS versi baru tetapi tidak compatible dengan beberapa vendor client contohnya seperti vendor Centrino
  - **post-2.9.25** – Metode ini adalah metode standard yang comaptible dengan sebagian besar card yang beredar di pasaran dan juga card keluaran baru.

[LAB-6] VAP Limit Lab



- Limit traffic untuk tiap VAP