Wireless Security

Certified Mikrotik Training Advance Wireless Class

Organized by: Citraweb Nusa Infomedia

(Mikrotik Certified Training Partner)

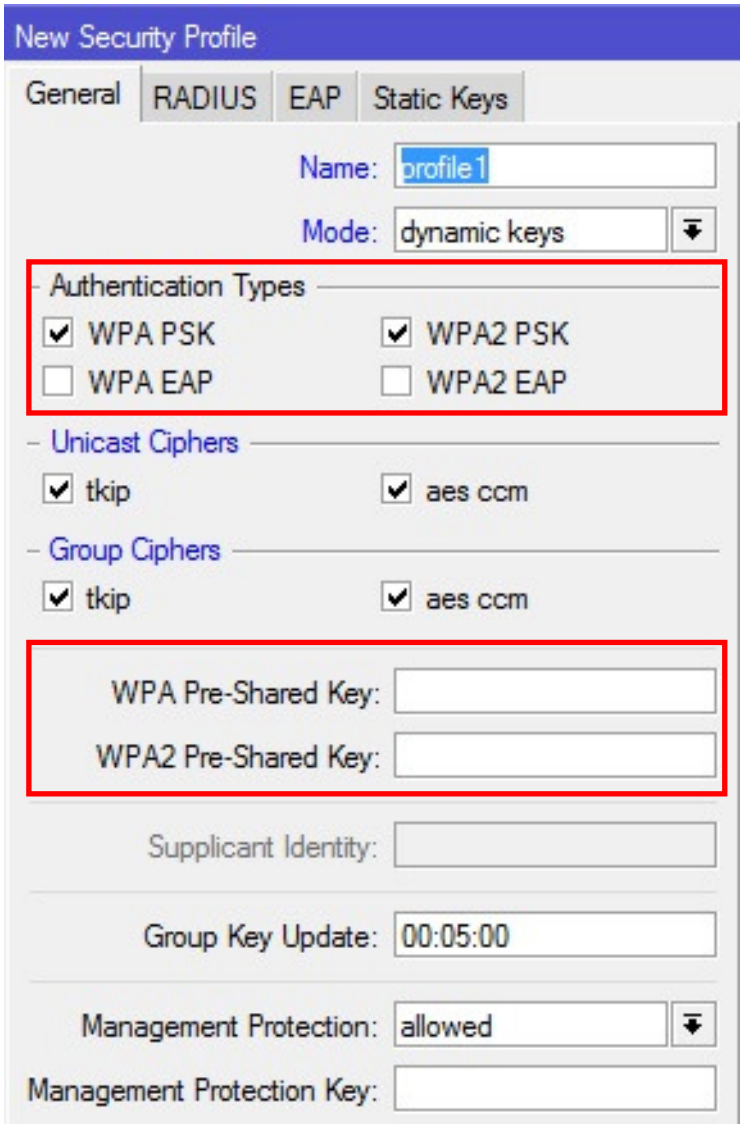
Training Outline

- Authentication
  - PSK Authentication
  - EAP Authentication
- Encryption
  - AES
  - TKIP
  - WEP
- EAP RADIUS & EAP-TLS Security
- Management Protection

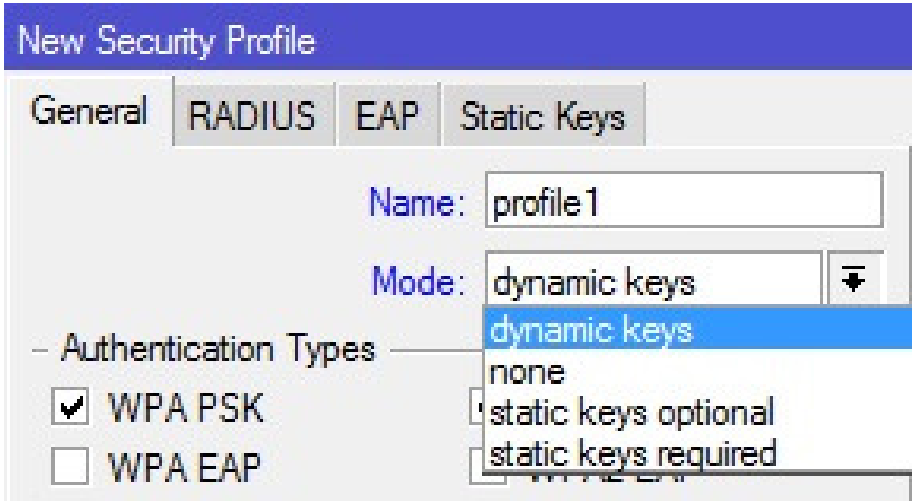
Security Principles

- **Authentication** – untuk memastikan bahwa komunikasi antar node (AP ke client dan sebaliknya) adalah benar-benar dari node perangkat yang memang terpercaya.
- **Data encryption :**
  - **Confidentiality** – untuk memastikan informasi data yang terjadi antar node memang hanya untuk node yang memang memiliki akses.
  - **Integrity** – untuk memastikan informasi data yang terjadi antar node benar-benar tidak terjadi pengubahan dari sumber atau node yang lain.

Security Profile



Security Profile - Mode



- **mode**
  - None
  - static-keys-optional
  - static-keys-required
  - dynamic-keys
- default value: none

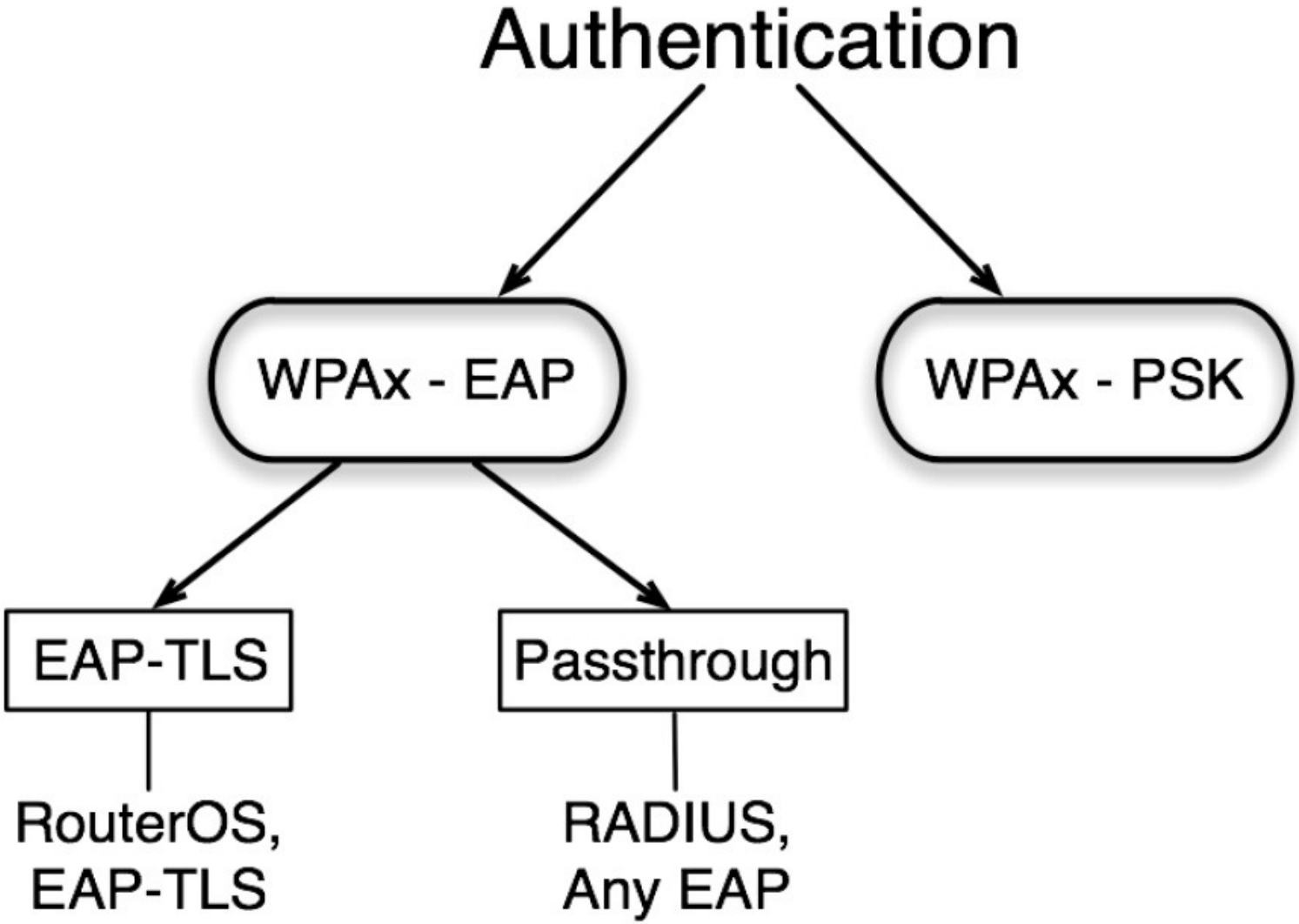
Security Profile - Mode

- **none** – enkripsi tidak dilakukan, jika terkoneksi ke frame yang terenkripsi maka komunikasi akan ditolak.
- **static-keys-required** – menggunakan metode enkripsi WEP, jika menggunakan metode ini maka komunikasi frame antar antar node yang tidak terenkripsi tidak dapat dilakukan atau ditolak.
  - Jika client (mode station) yang menggunakan mode keamanan **static-keys-required** tidak akan dapat terkoneksi ke AP yang menggunakan mode keamanan **static-keys-optional**.

Security Profile – Mode (2)

- **static-keys-optional** – menggunakan metode enkripsi WEP, tetapi juga mampu menerima serta mengirimkan frame data yang tidak terenkripsi.
  - Jika client (mode station) yang menggunakan mode keamanan **static-keys-optional** tidak akan dapat terkoneksi dengan AP yang menggunakan mode keamanan **static-keys-required**.
- **dynamic-keys** – menggunakan metode keamanan WPA.

Authentication Tree



PSK Authentication

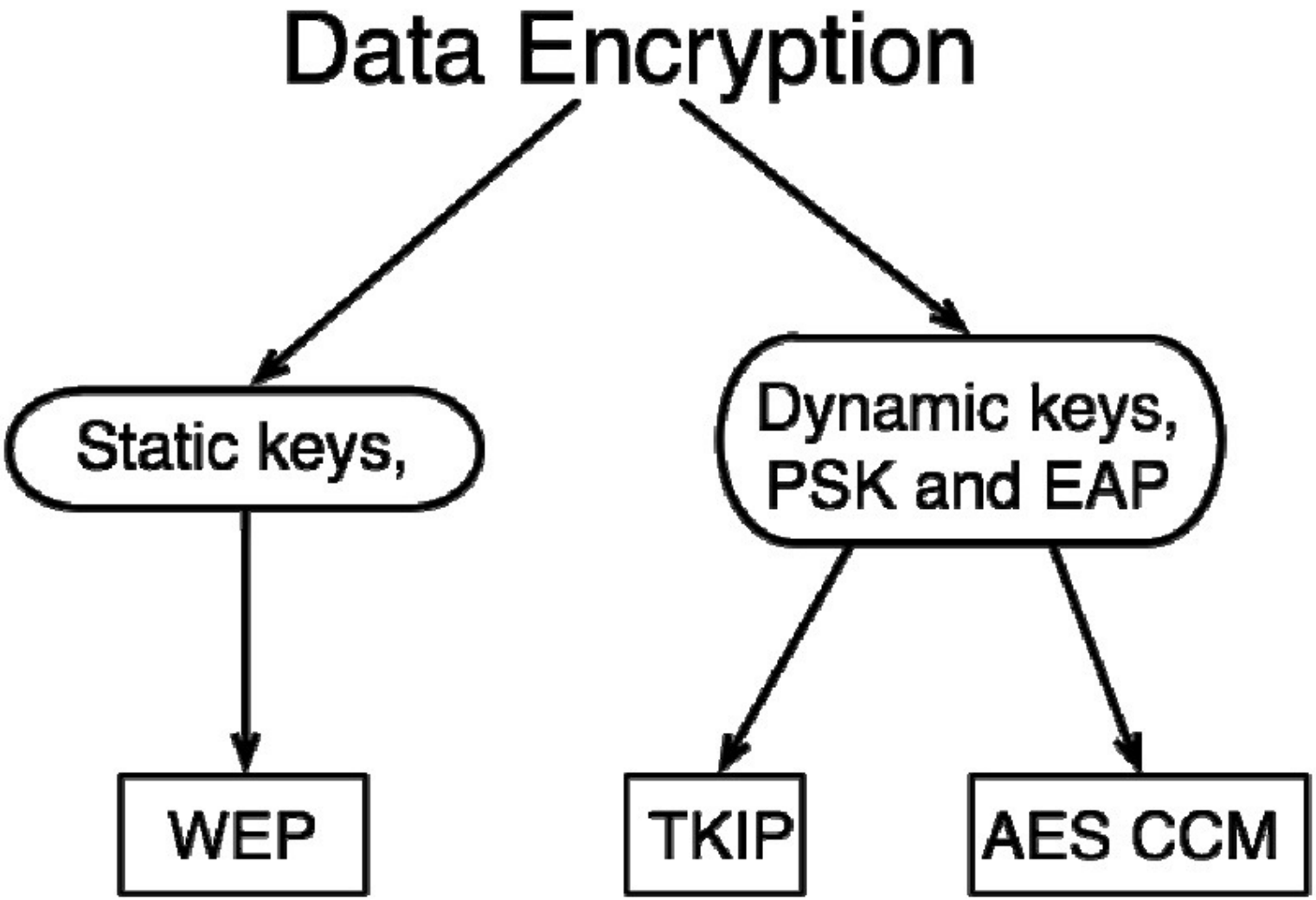
- **Pre-Shared Key** adalah sebuah mekanisme autentikasi yang menggunakan sebuah kata kunci yang sebelumnya sudah didistribusikan diantara kedua node (AP-Client).
- Metode ini Banyak digunakan di autentikasi komunikasi wireless.
- Pada sebuah security profile sangat memungkinakn untuk memasang beberapa metode autentikasi yang berbeda.
- Memungkinkan juga menggunakan "**PSK key**" yang berbeda untuk tiap node koneksi (client) dengan menggunakan **Access List**.

EAP Authentication

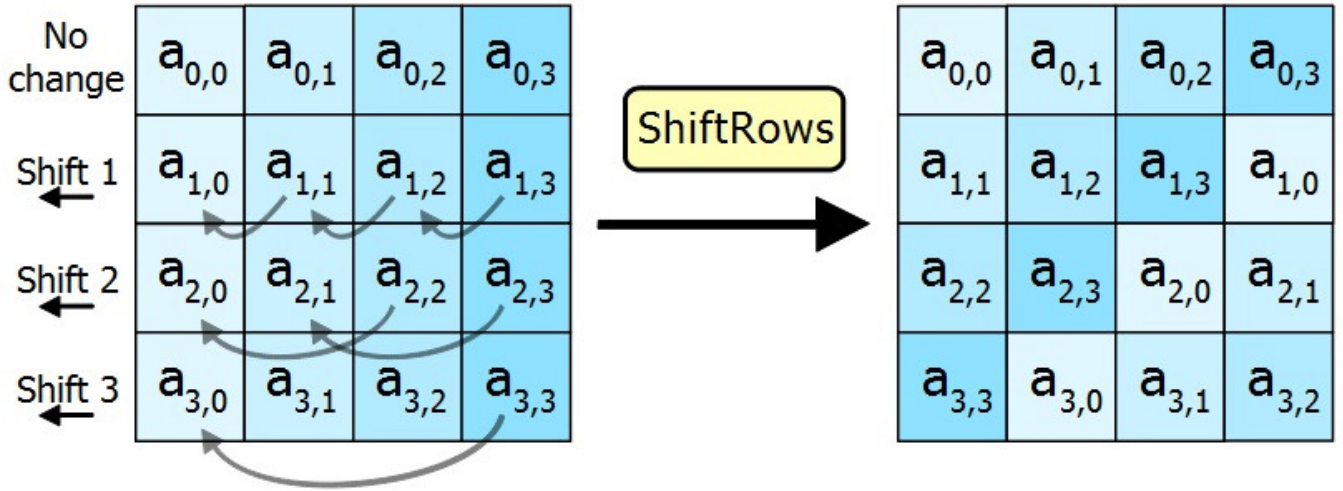
EAP – Extensible Authentication Protocol

- Memungkinkan administrator jaringan wireless untuk menggunakan metode autentikasi wireless yang beragam di RouterOS.
- Saat ini terdapat 40 macam metode autentikasi yang termasuk didalam golongan EAP.
- RouterOS support salah satunya yaitu **EAP-TLS**.
- RouterOS juga mampu menggunakan metode "**Passtrough**" yang akan meminta atau meneruskan metode autentikasi ke **RADIUS Server**.

Encryption

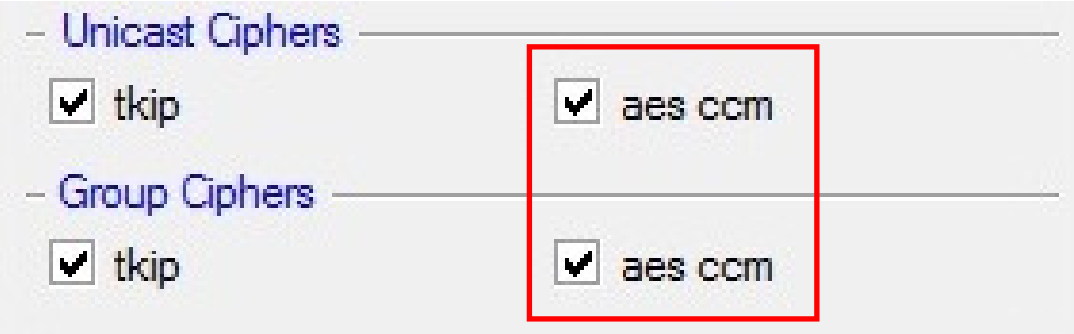

Data Encryption
Static keys,
Dynamic keys, PSK and EAP
WEP
TKIP
AES CCM

Encryption AES-CCM



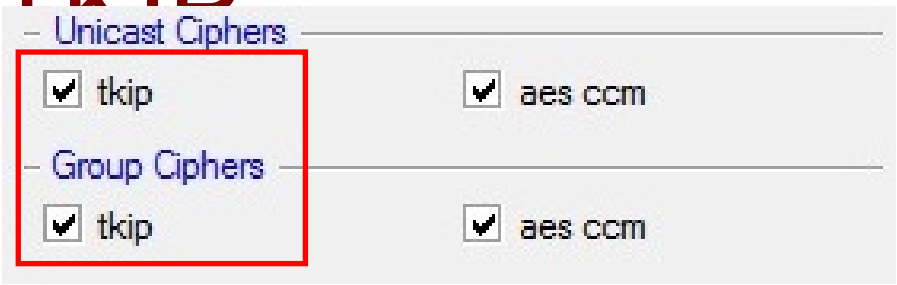
- **AES-CCM** – **AES** with **C**TR with **C**BC-**M**AC
- **AES** - Advanced Encryption Standard adalah sebuah metode enkripsi yang menggunakan blok pengkodean (Cipher) tetap yang besarnya 128bit. Untuk kunci (key) pengurainya bisa menggunakan 128,192 dan 256bit.
- **CTR** - Counter menghasilkan blok keystream dengan melakukan enkripsi secara berurutan nilai dari counter

AES-CCM (2)



- **CBC** - Cipher Block Chaining setiap blok kodetext akan dibandingkan dengan blok sebelumnya dengan menggunakan logika XOR. Dengan cara ini, setiap blok kodetext akan bergantung pada semua blok plaintext kunci.
- **MAC** - Message Authentication Code memungkinkan untuk mendeteksi adanya perubahan pada isi pesan.

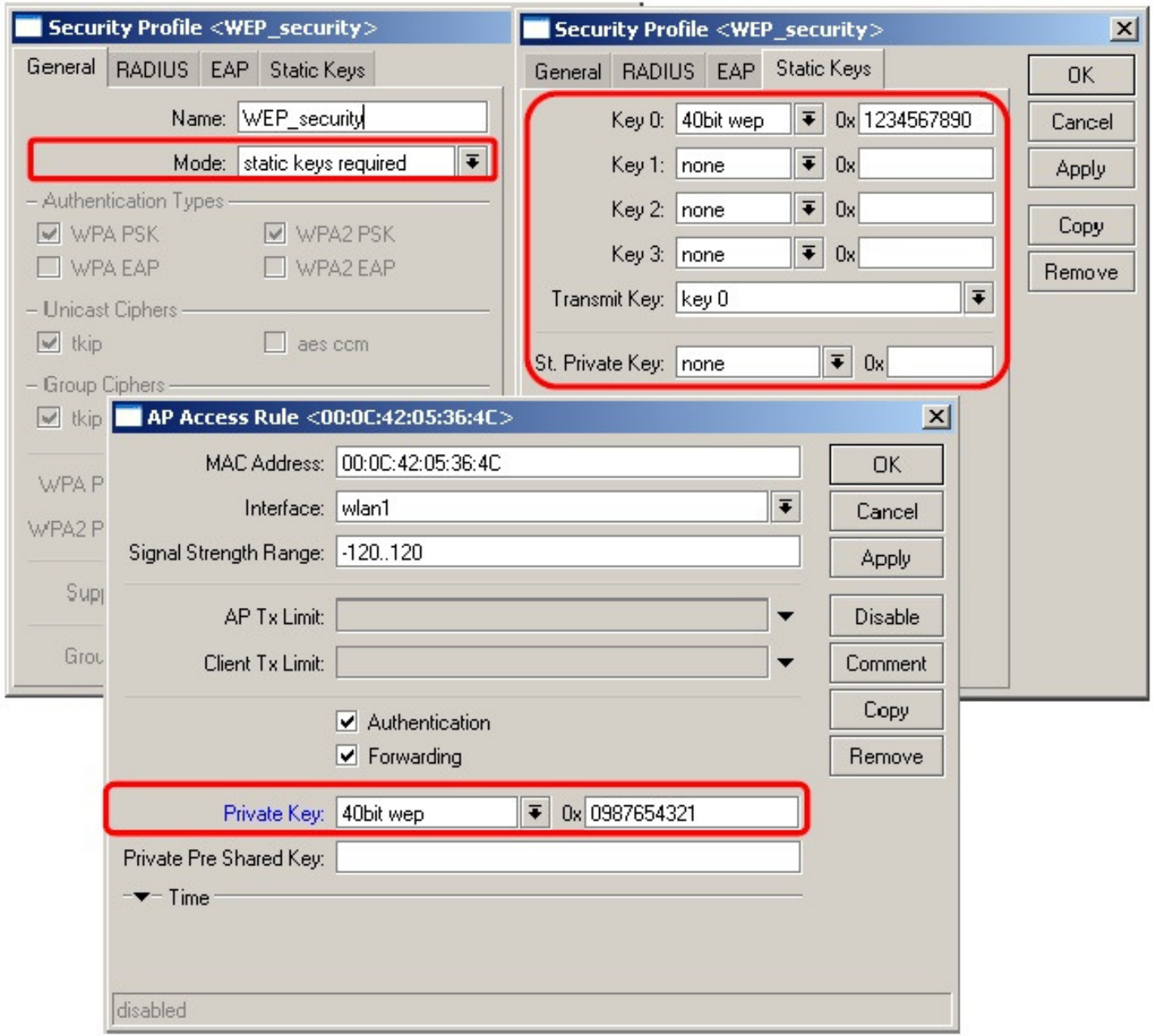
TKIP



- **TKIP** – Temporal Key Integrity Protocol adalah sebuah protocol keamanan yang khusus digunakan di jaringan Wireless 802.11.
- TKIP ini adalah sebuah penyempurnaan dari protocol terdahulu WEP berdasarkan Cipher stream RC4.
- Tidak seperti WEP, TKIP menghasilkan "**per-packet key mixing**", sebuah pesan yang ter-integrity yang memeriksa dan sebuah mekanisme "**re-keying**" sehingga pengalamatan menjadi isu pengamanan dengan WEP.
- Hal ini menambah kerumitan dari pen-dekodean kunci dengan menurunkan ketersediaan jumlah data kepada cracker, itu telah dienkripsi menggunakan suatu kunci khusus.

WEP

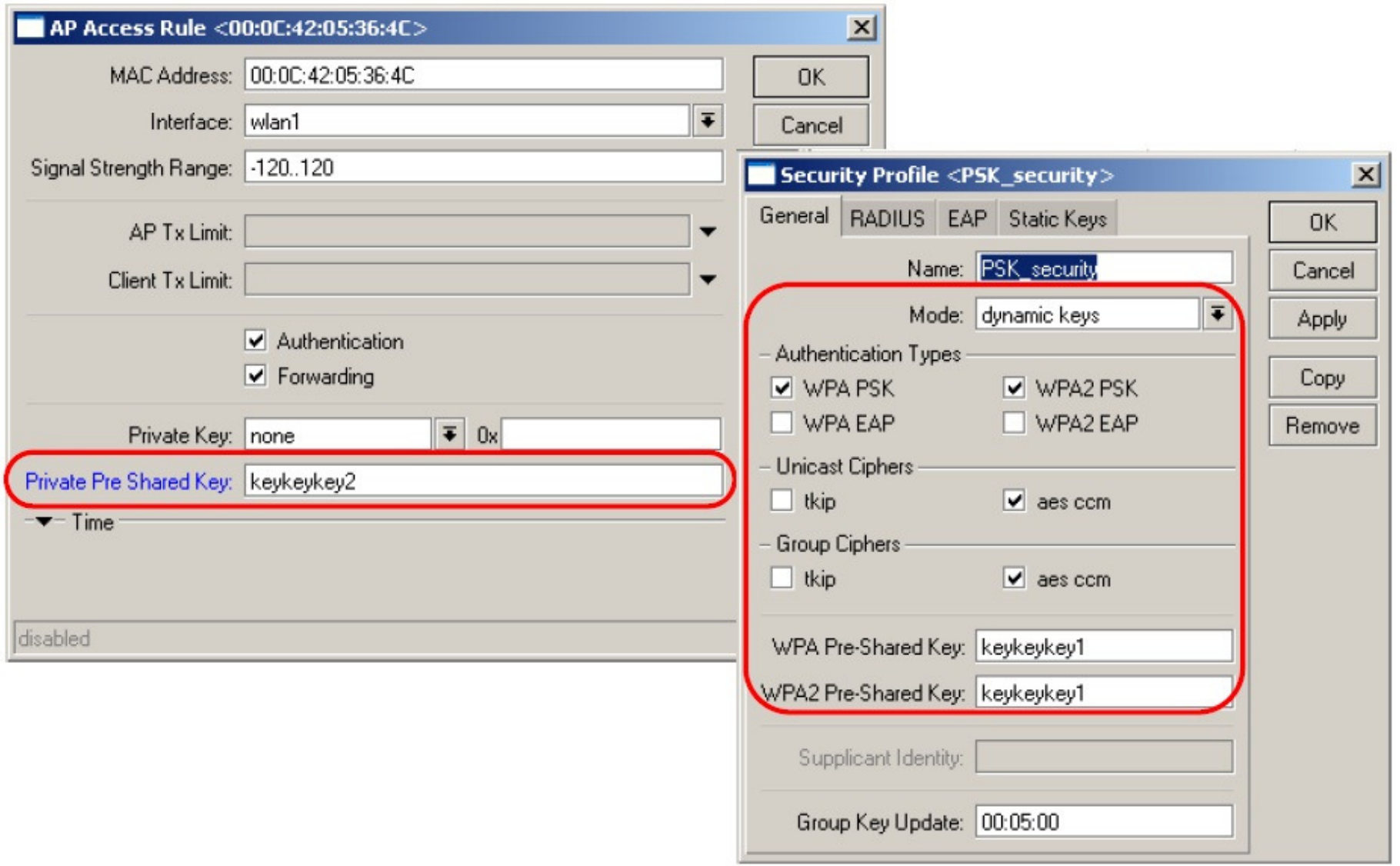
- **Wired Equivalent Privacy** adalah protocol security untuk wireless network terdahulu yang sudah mulai jarang digunakan.
- Selain sederhana tingkat keamanannya tidak terlalu kuat.
- Tidak memiliki proses Autentikasi.
- Tidak direkomendasikan lagi untuk menggunakan metode keamanan ini karena dirasa sangat rentan terhadap tool hacking yang berkembang saat ini.


Security Profile <WEP_security>
General
RADIUS
EAP
Static Keys
Name: WEP_security
Mode: static keys required
Authentication Types
WPA PSK
WPA2 PSK
WPA EAP
WPA2 EAP
Unicast Ciphers
tkip
aes ccm
Group Ciphers
tkip
Security Profile <WEP_security>
General
RADIUS
EAP
Static Keys
OK
Cancel
Apply
Copy
Remove
Key 0: 40bit wep 0x 1234567890
Key 1: none 0x
Key 2: none 0x
Key 3: none 0x
Transmit Key: key 0
St. Private Key: none 0x
AP Access Rule <00:0C:42:05:36:4C>
MAC Address: 00:0C:42:05:36:4C
Interface: wlan1
Signal Strength Range: -120..120
AP Tx Limit:
Client Tx Limit:
Authentication
Forwarding
Private Key: 40bit wep 0x 0987654321
Private Pre Shared Key:
Time
OK
Cancel
Apply
Disable
Comment
Copy
Remove
disabled

Pre-Shared Key (PSK)

- Untuk menggunakan autentikasi metode PSK :
  - Gunakan mode “**Dynamic Keys**”
  - Aktifkan pilihan “**WPAx-PSK**” pada parameter authentication type
  - Tentukan pengkodean yang digunakan untuk enkripsi Unicast and Group Ciphers (**AES CCM, TKIP**)
  - Tentukan **WPAx-Pre-Shared Key**

WPA-PSK


AP Access Rule <00:0C:42:05:36:4C>
MAC Address: 00:0C:42:05:36:4C
Interface: wlan1
Signal Strength Range: -120..120
AP Tx Limit:
Client Tx Limit:
Authentication
Forwarding
Private Key: none 0x
Private Pre Shared Key: keykeykey2
Time
disabled
OK
Cancel
Security Profile <PSK_security>
General RADIUS EAP Static Keys
Name: PSK_security
Mode: dynamic keys
Authentication Types
WPA PSK
WPA2 PSK
WPA EAP
WPA2 EAP
Unicast Ciphers
tkip
aes ccm
Group Ciphers
tkip
aes ccm
WPA Pre-Shared Key: keykeykey1
WPA2 Pre-Shared Key: keykeykey1
Supplicant Identity:
Group Key Update: 00:05:00
OK
Cancel
Apply
Copy
Remove

WPA Properties - Authentication Type

Hanya berfungsi jika security profile menggunakan **mode=dynamic-keys**.

- **authentication-types** – menentukan metode autentikasi yang akan digunakan. AP akan menawarkan metode autentikasi yang diguankan dan client akan terkoneksi ke AP menggunakan metode autentikasi yang disupport. Jika tidak ada satu pun metode yang ditawarkan cocok maka client tidak akan dapat terkoneksi.

WPA Properties – Unicast Ciphers

- **unicast-ciphers** – AP akan menawarkan semua ciphers yang digunakan, client akan mencoba terkoneksi menggunakan ciphers yang ada. Client dapat terkoneksi menggunakan minimal satu ciphers.
- salah satu ciphers akan digunakan untuk melakukan enkripsi frame komunikasi unicast yang terjadi antara AP-Client.

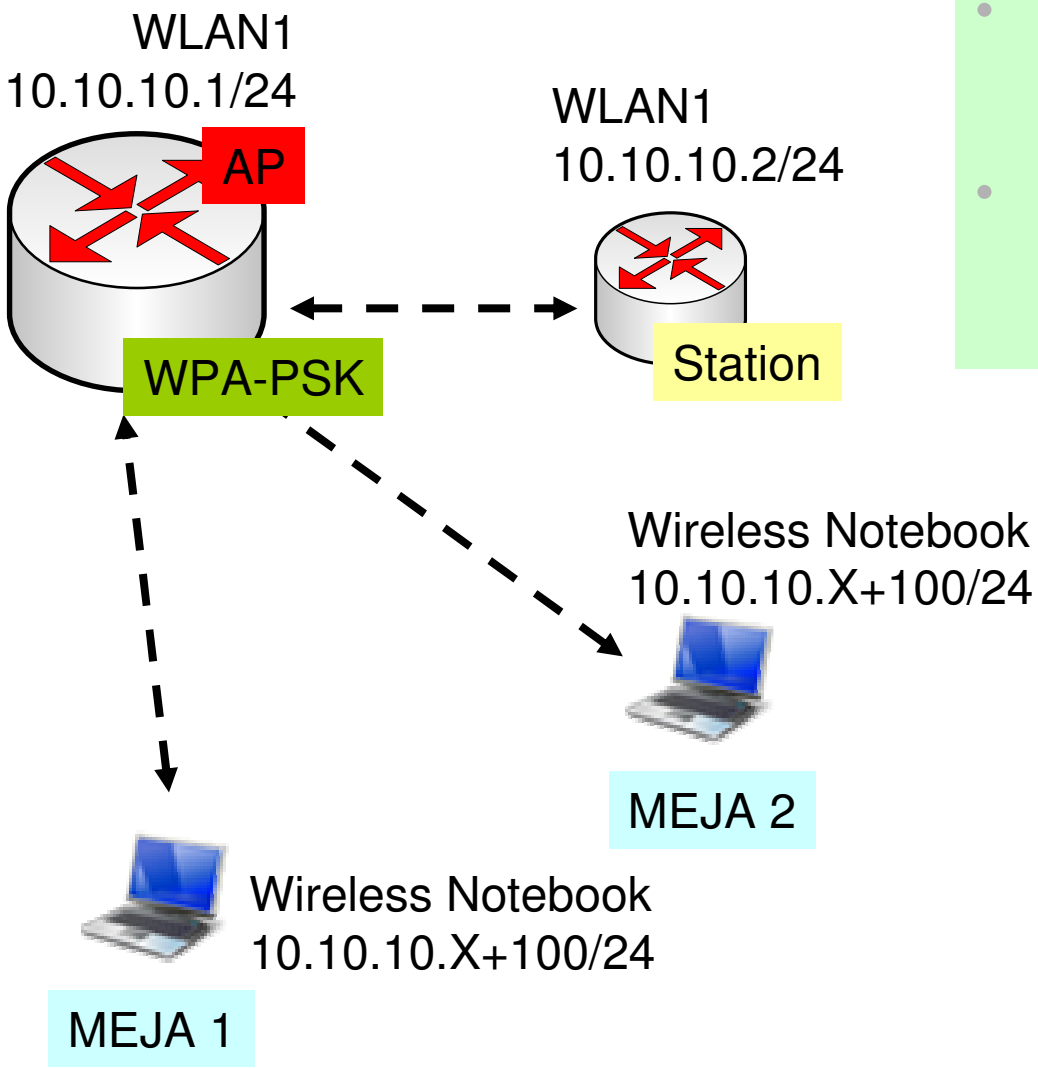
WPA properties – Group Ciphers

- **group-ciphers** – AP akan menawarkan semua ciphers yang digunakan, dan metode tersebut akan digunakan untuk melakukan enkripsi dari frame traffic broadcast dan multicast. Client dapat terkoneksi menggunakan minimal satu ciphers.
  - **tkip** – protocol enkripsi yang kompatibel dengan protocol WEP tetapi sudah menggunakan metode baru yang memperbaiki kekurangan WEP.
  - **aes-ccm** – protocol WPA yang lebih aman dibandingkan dengan WEP.

WPA properties – Group Key

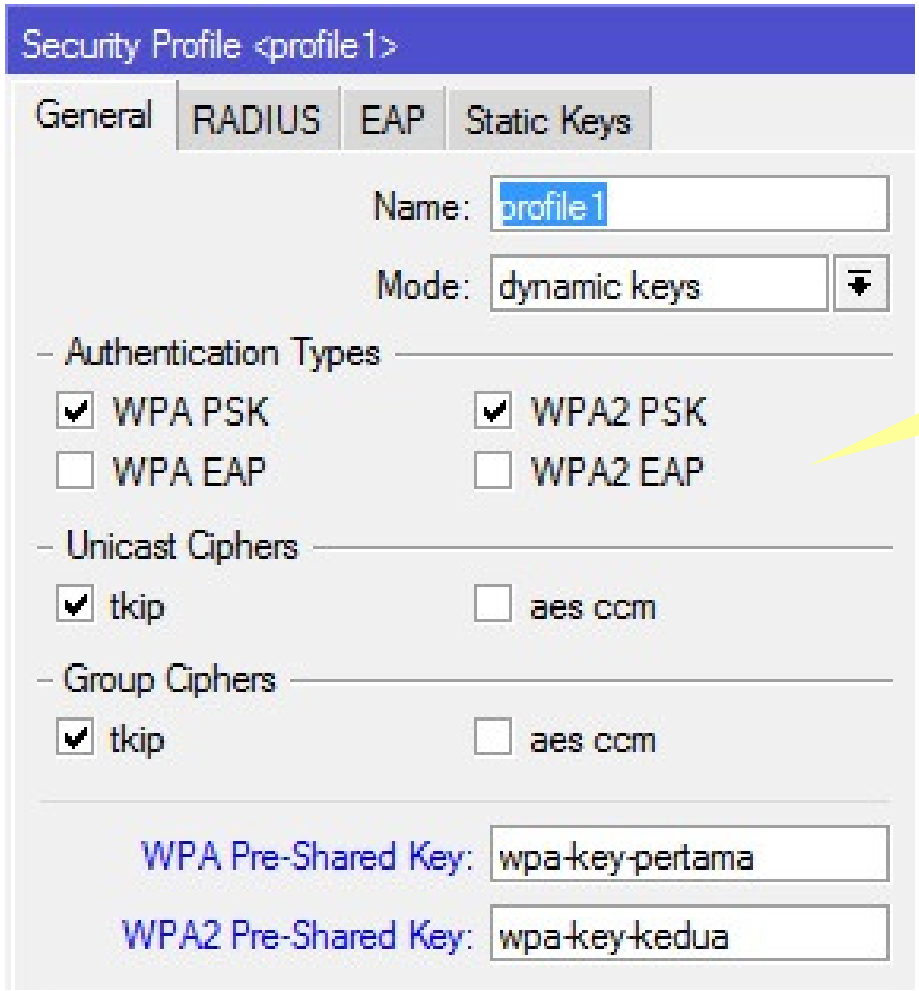
- **group-key-update** (time interval in the 30s..1h range; default value: 5m) : interval untuk melakukan pembaharuan group-key. Parameter ini tidak berpengaruh pada wireless yang menggunakan mode client.
- **wpa-pre-shared-key, wpa2-pre-shared-key** (text) : key yang digunakan untuk menggunakan autentikasi WPA di seluruh jaringan wireless yang terkoneksi. Nilai bisa berupa text.

[LAB-1] WPA Lab

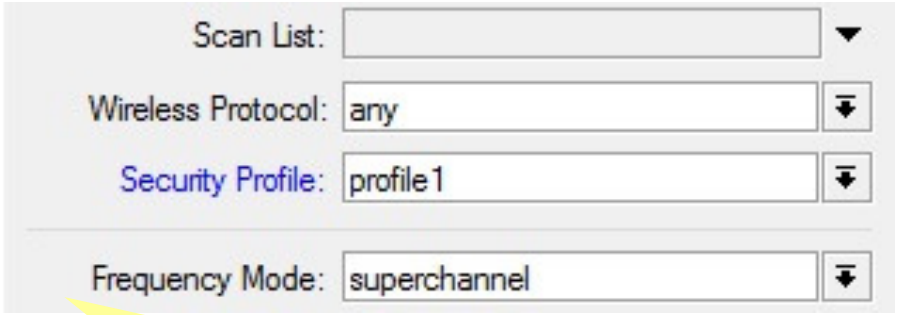


- Gunakan WPA-PSK untuk mengamankan jaringan wireless
- Security profile pada interface akan mempengaruhi semua client

Security Profile - Interface

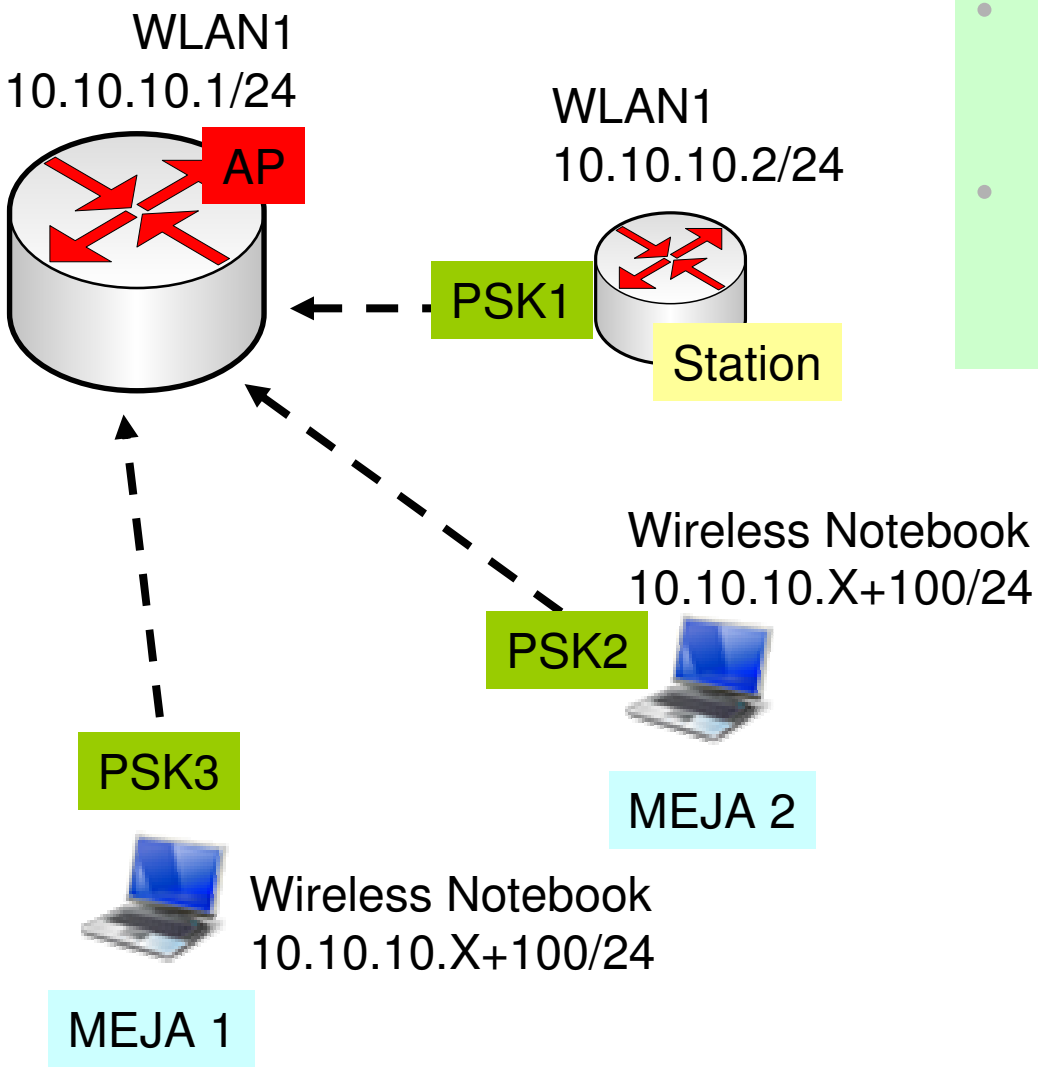


Konfigurasi Security Profile Yang menggunakan metode WPA-PSK



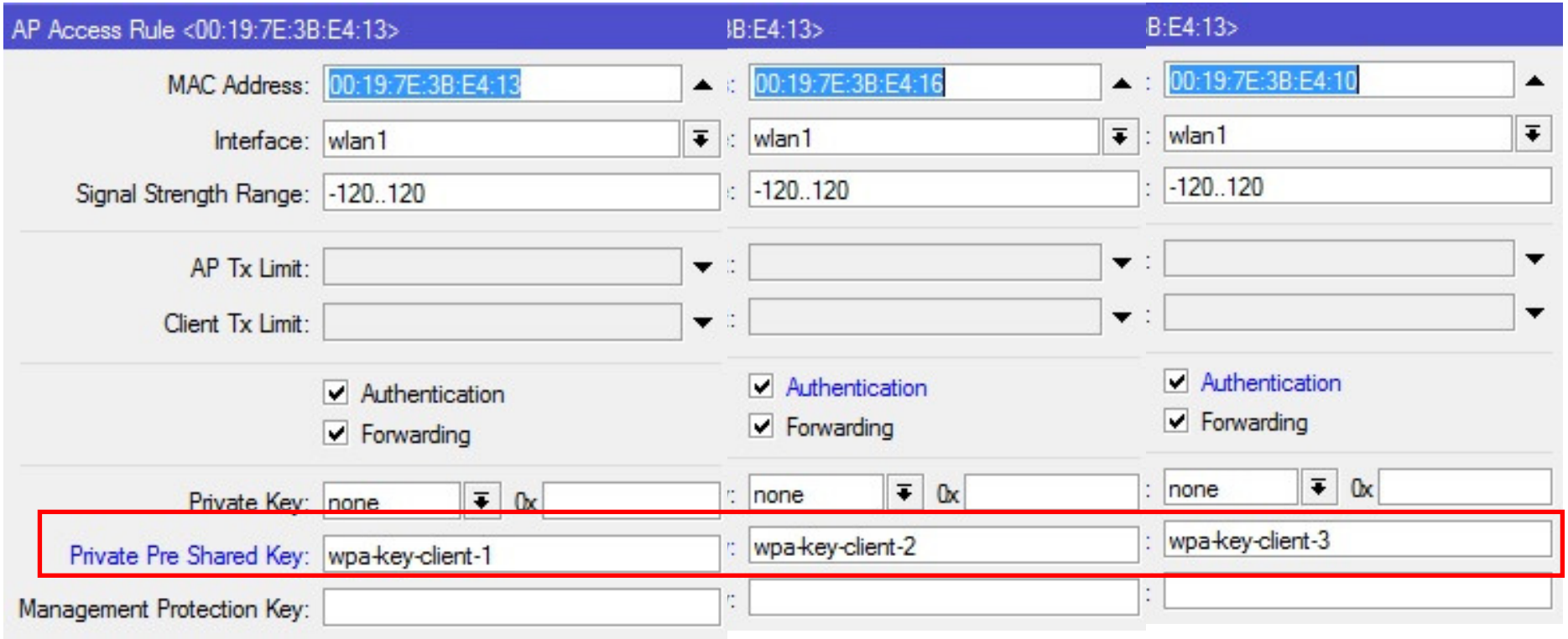
Security Profile yang baru diimplementasikan ke interface

[LAB-2] WPA Lab + Access List

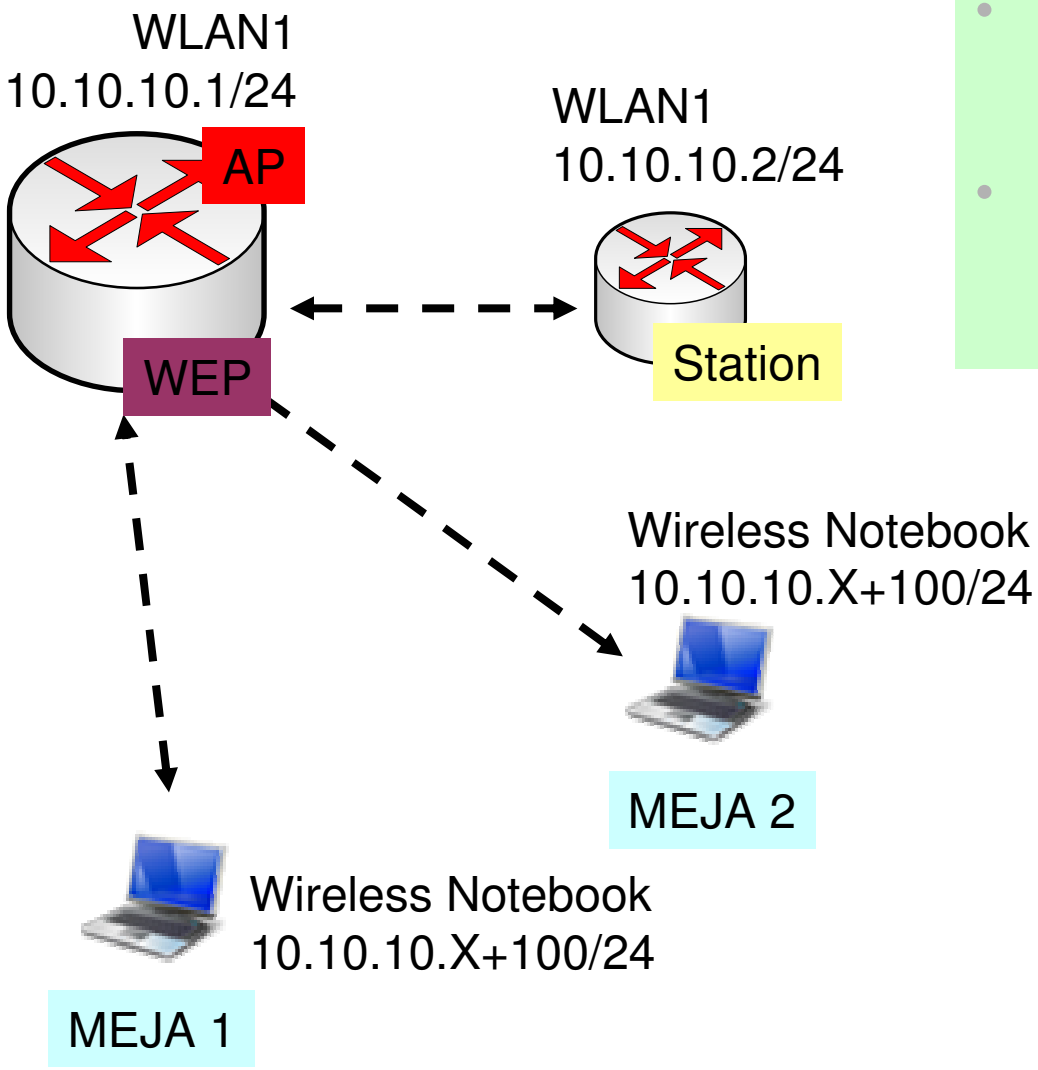


- Gunakan WPA-PSK untuk mengamankan jaringan wireless
- Gunakan access-list untuk menetukan pre-shared-key yang berbeda di tiap client

Access List – pre-shared-key

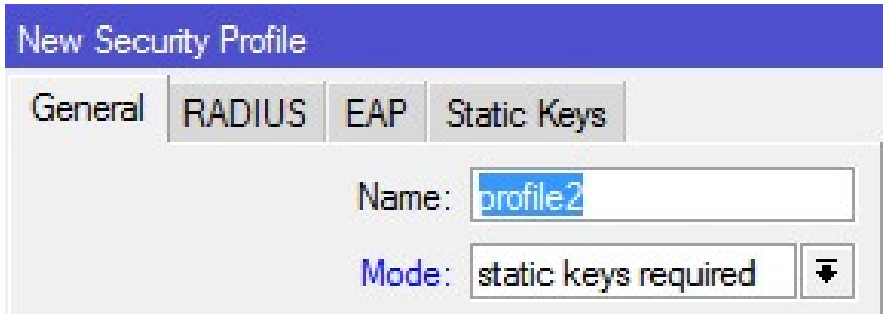


[LAB-3] WEP Lab

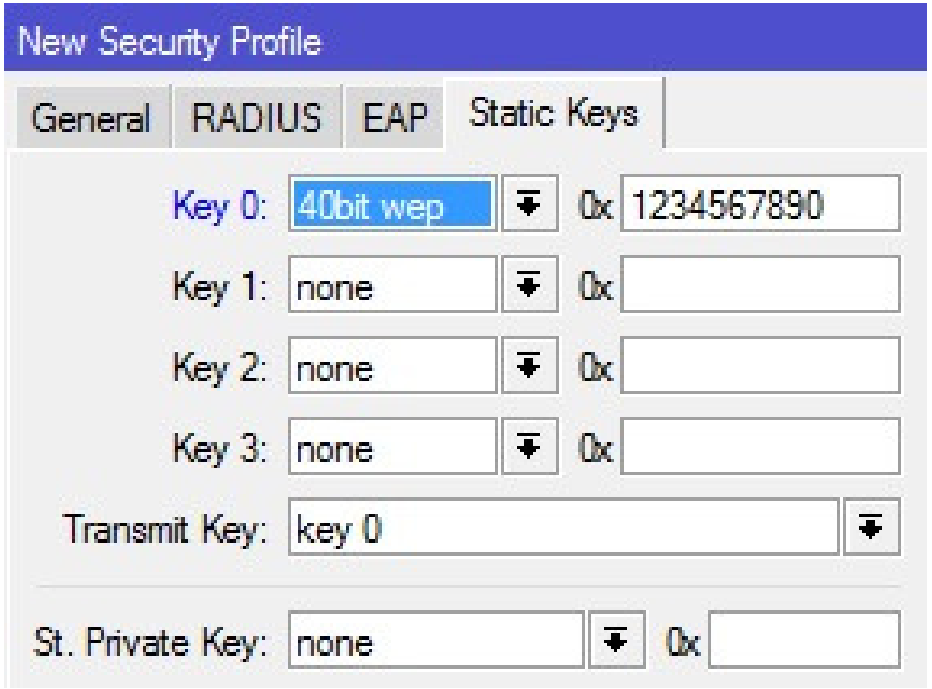


- Gunakan WEP untuk mengamankan jaringan wireless
- Security profile pada interface akan mempengaruhi semua client

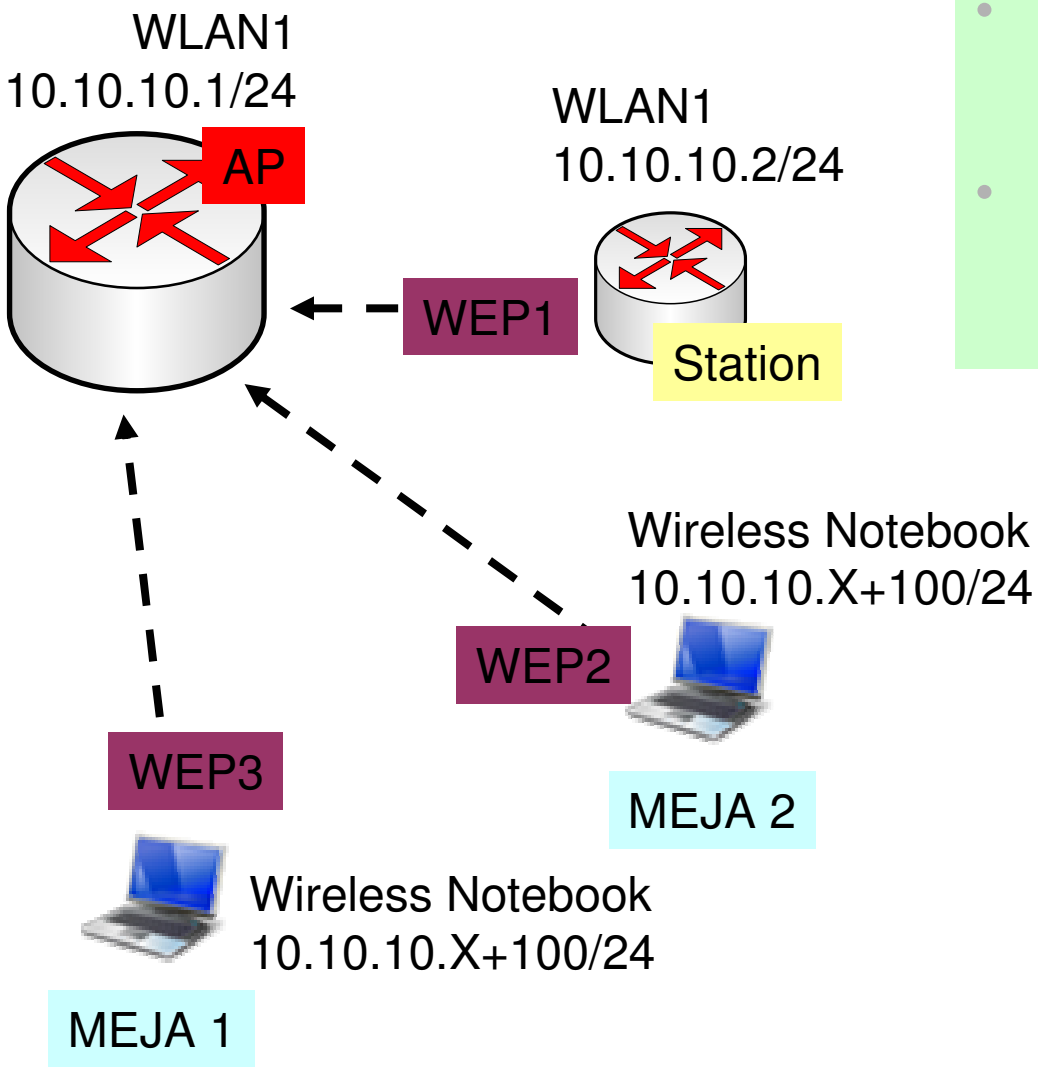
Security Profile - Interface



Security Profile baru yang Menggunakan metode Enkripsi WEP diterapkan Di interface.

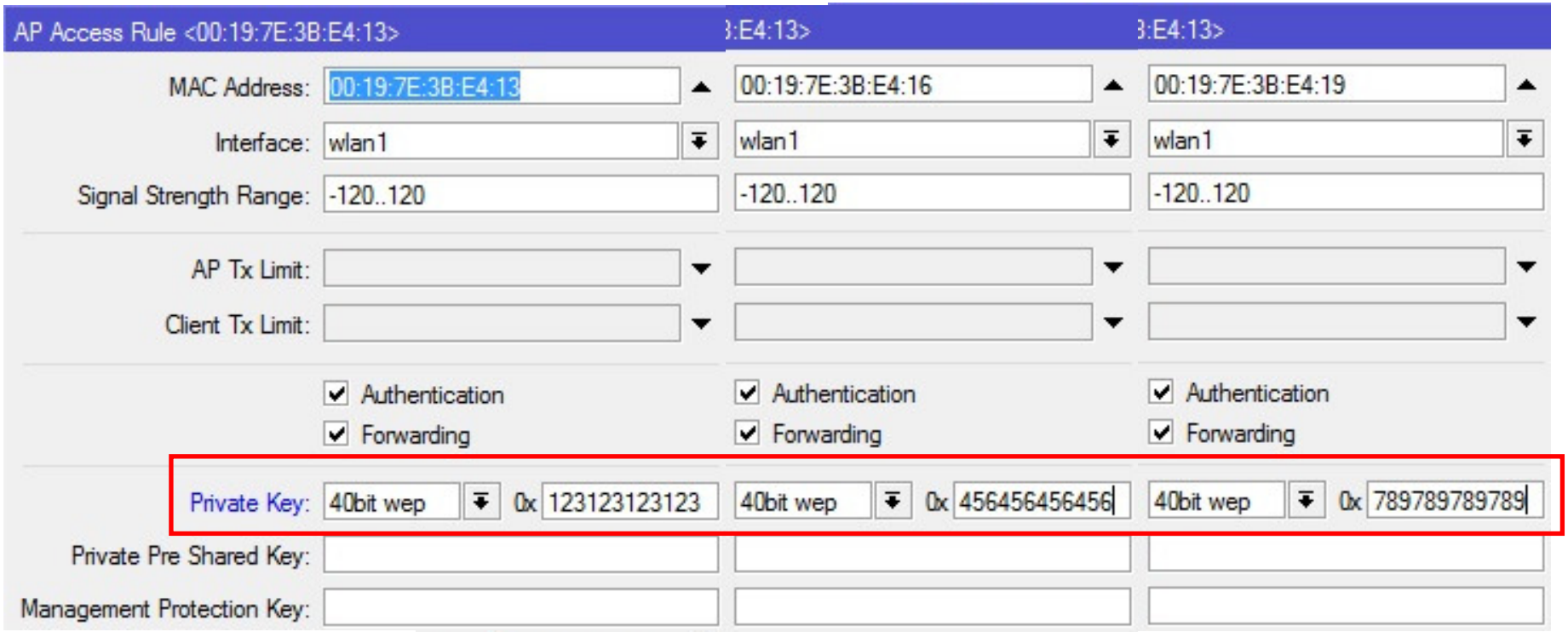


[LAB-4] WEP Lab + Access List



- Gunakan WEP untuk mengamankan jaringan wireless
- Gunakan access-list untuk menetukan WEP private-key yang berbeda di tiap client

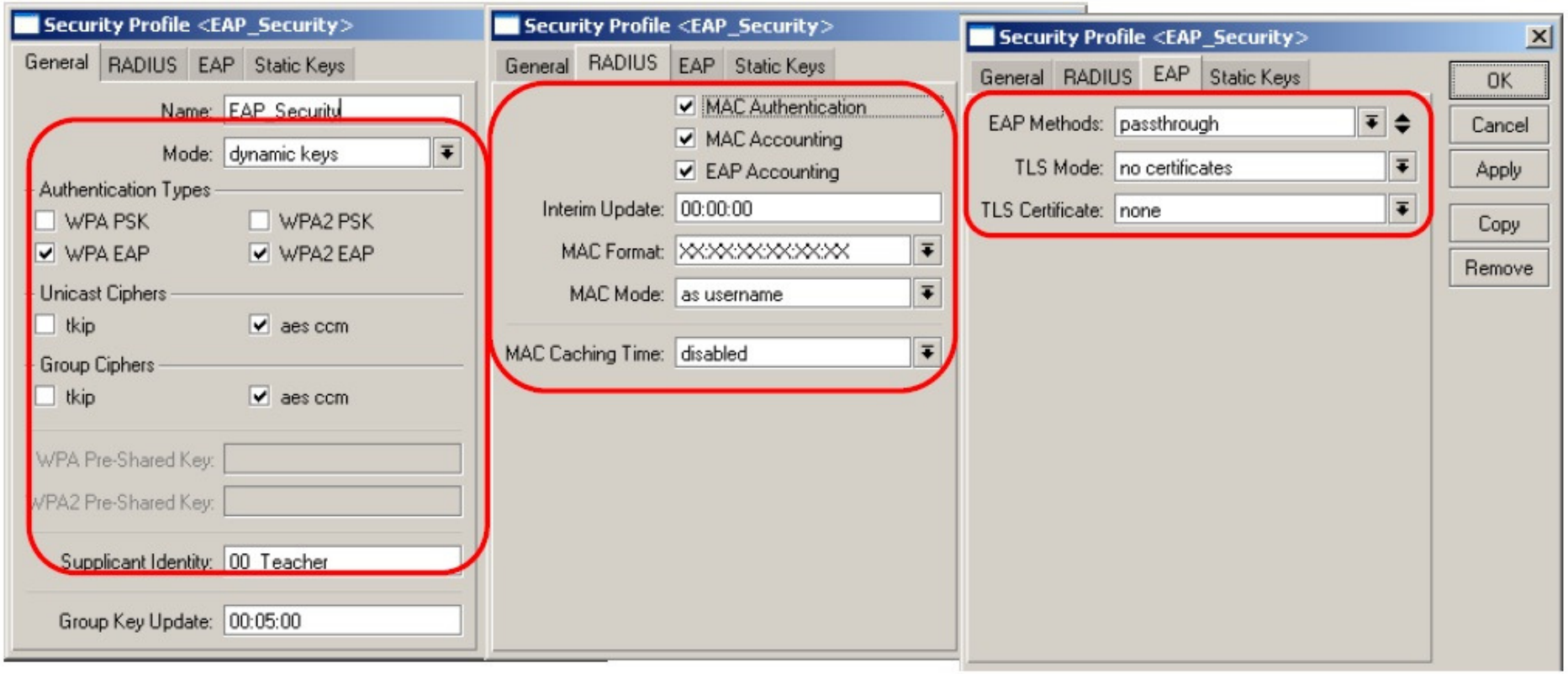
WEP with Access List



EAP - Passtrough

- Untuk mengaktifkan fitur keamanan autentikasi **EAP-Passthrough**:
  - Gunakan mode “**Dynamic Keys**”
  - Aktifkan type autentikasi “**WPAx-EAP**”
  - Aktifkan autentikasi menggunakan MAC-address
  - Pilih Metode EAP menggunakan metode “**Passthrough**”
  - Aktifkan Radius Cleint

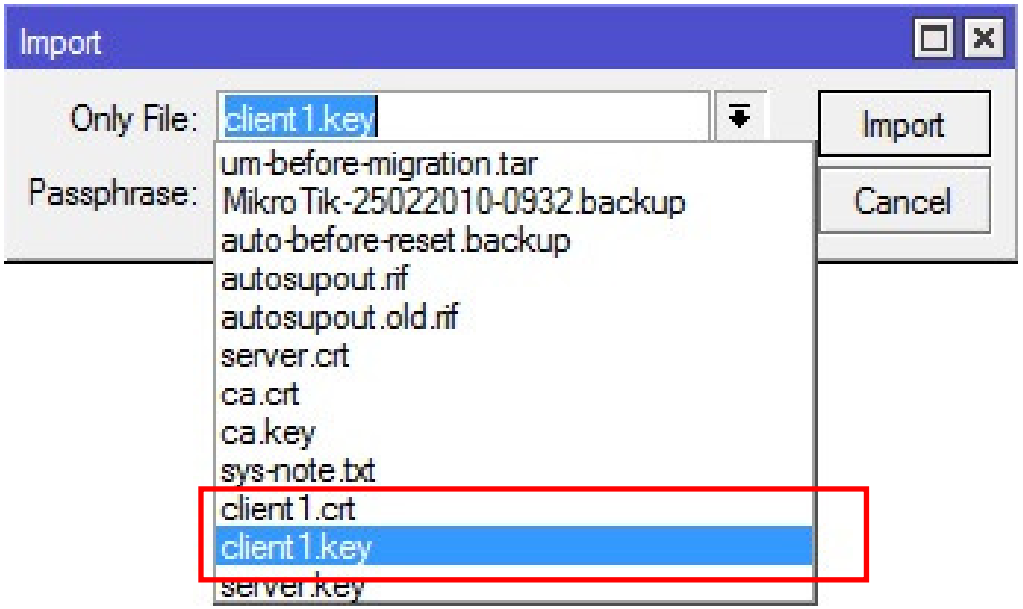
EAP – Passthrough RADIUS



EAP – TLS

- Untuk mengaktifkan autentikasi menggunakan metode **EAP-TLS**
  - Aktifkan type autentikasi “**WPAx-EAP**”
  - Gunakan opsi TLS jika ingin menggunakan Certificate
  - Import certificate SSL kemudian decript menggunakan key yang ada

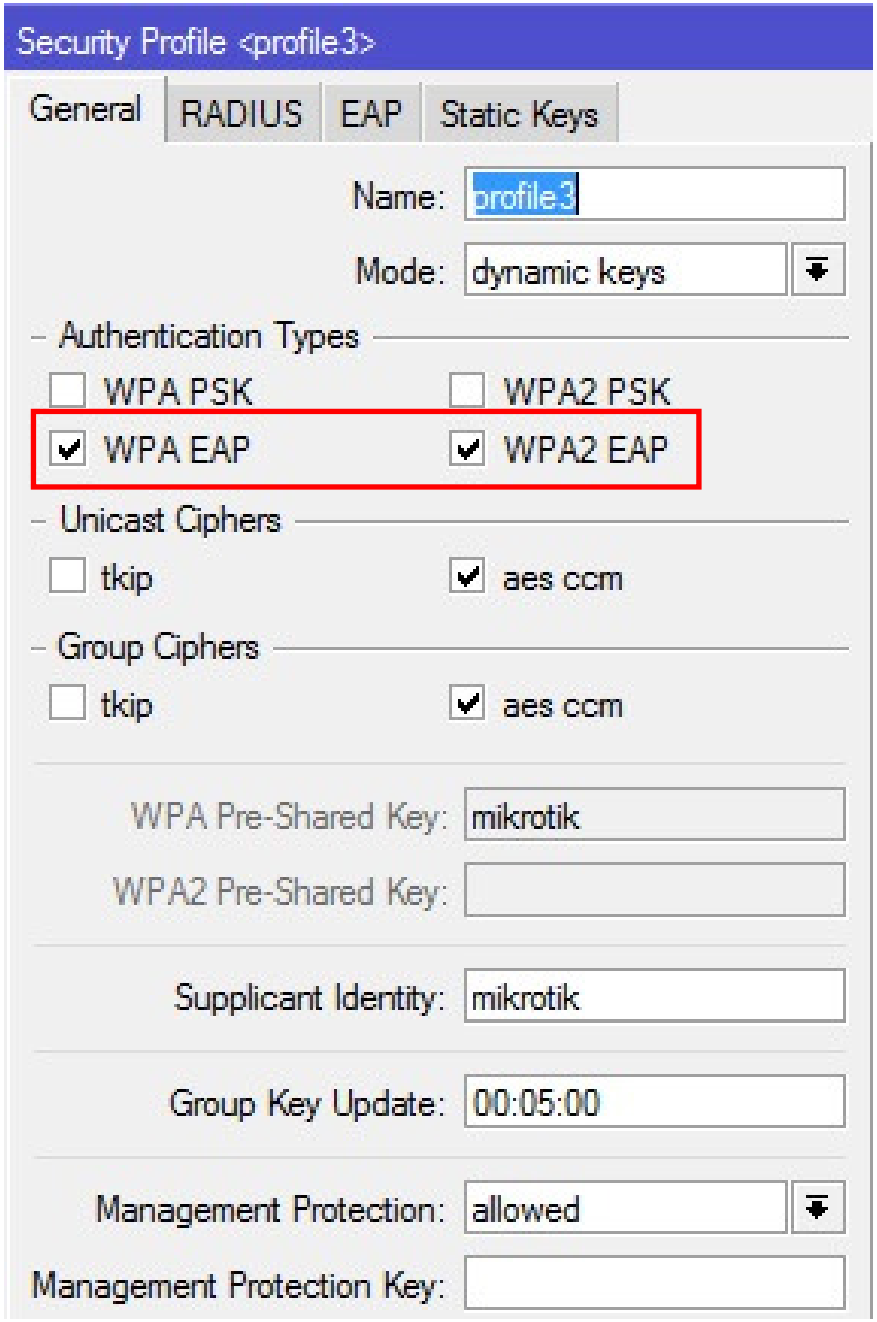
EAP-TLS – Import Certificate



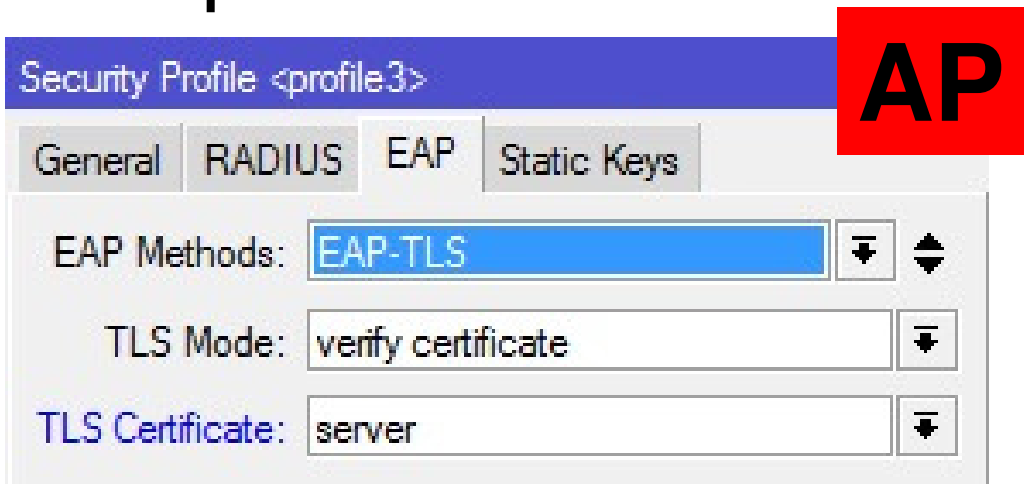
Sebelum menggunakan EAP-TLS
Import terlebih dahulu certificate SSL
Di kedua perangkat AP dan Client
Untuk diimplementasikan pada EAP-TLS.

WPA-

Dengan menggunakan
Autentication WPA-EAP
Maka akan traffic akan dibuatkan
Sesi enkripsi menggunakan
2048 bit anonymous
Diffie-Hellman key exchange



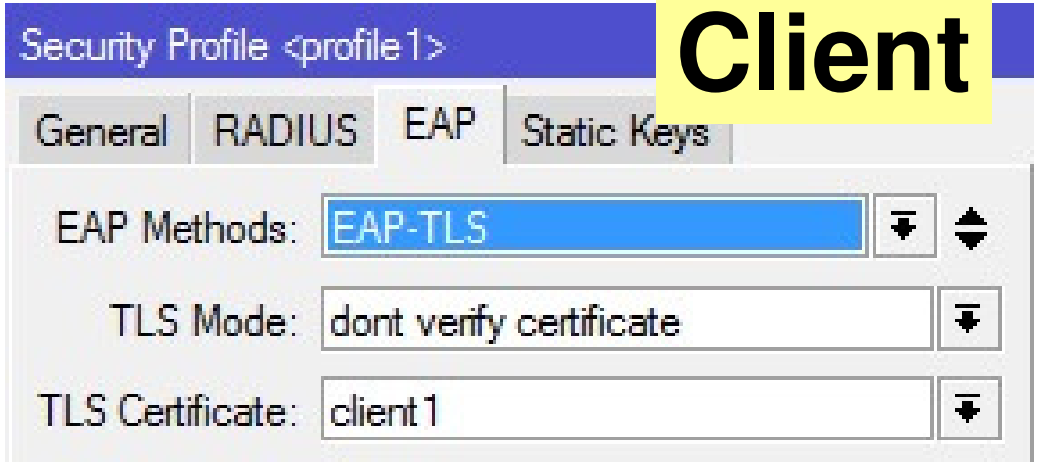
EAP-TLS -



AP

TLS mode: Verify certificate

Client harus menyediakan certificate



Client

Management Frame Protection

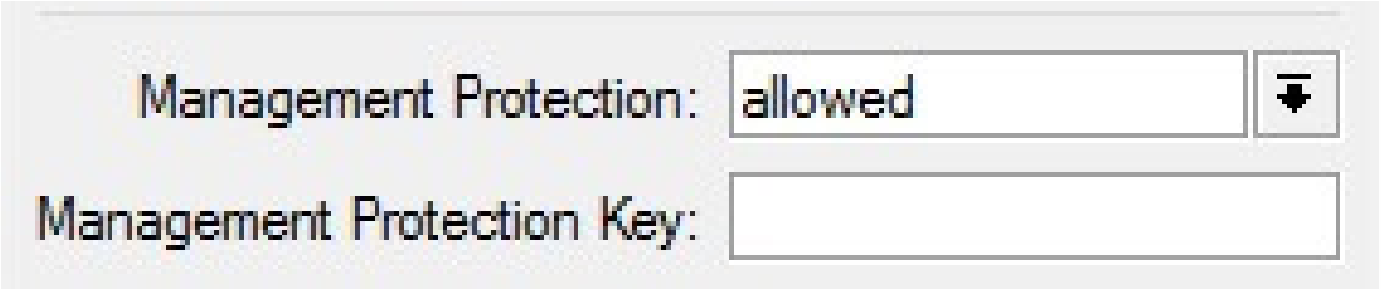
- RouterOS mengimplementasikan protocol keamanan khusus yang hanya bisa digunakan di sesama wirless mikrotik, yaitu algoritma **Management Frame Protection**.
- Perangkat wireless mikrotik mampu untuk memastikan bahwa asal frame yang diterima adalah dari node yang benar-benar terverifikasi dan bukan dari sumber yang lain yang bermaksud jahat.
- Mampu untuk mengatasi serangan deauthentication dan disassociation di perangkat wireless mikrotik.

Management Protection Settings

- Diimplementasikan dan dikonfigurasi di security profile
- **disabled** – tidak menggunakan management protection
- **allowed** – mengaktifkan management protection jika disupport oleh perangkat lawan.
  - Jika digunakan di AP – memperbolehkan perangkat client terkoneksi walaupun tidak support management protection.
  - Jika digunakan di Client – mampu terkoneksi ke AP yang support management protection atau ke AP yang tidak menggunakan protocol ini.

- **required** – hanya bisa terkoneksi ke perangkat lawan yang support management protection.
  - Jika digunakan di AP – hanya memperbolehkan client yang menggunakan management protection.
  - Jika digunakan di Client – hanya bisa terkoneksi ke AP yang menggunakan protocol ini.

management-protection-key



- Dikonfigurasi menggunakan parameter **management-protection-key.**
- Management Protection Key bisa ditentukan secara spesifik di Access-List atau bisa juga ditentukan menggunakan atribut di RADIUS.

management-protection-key