

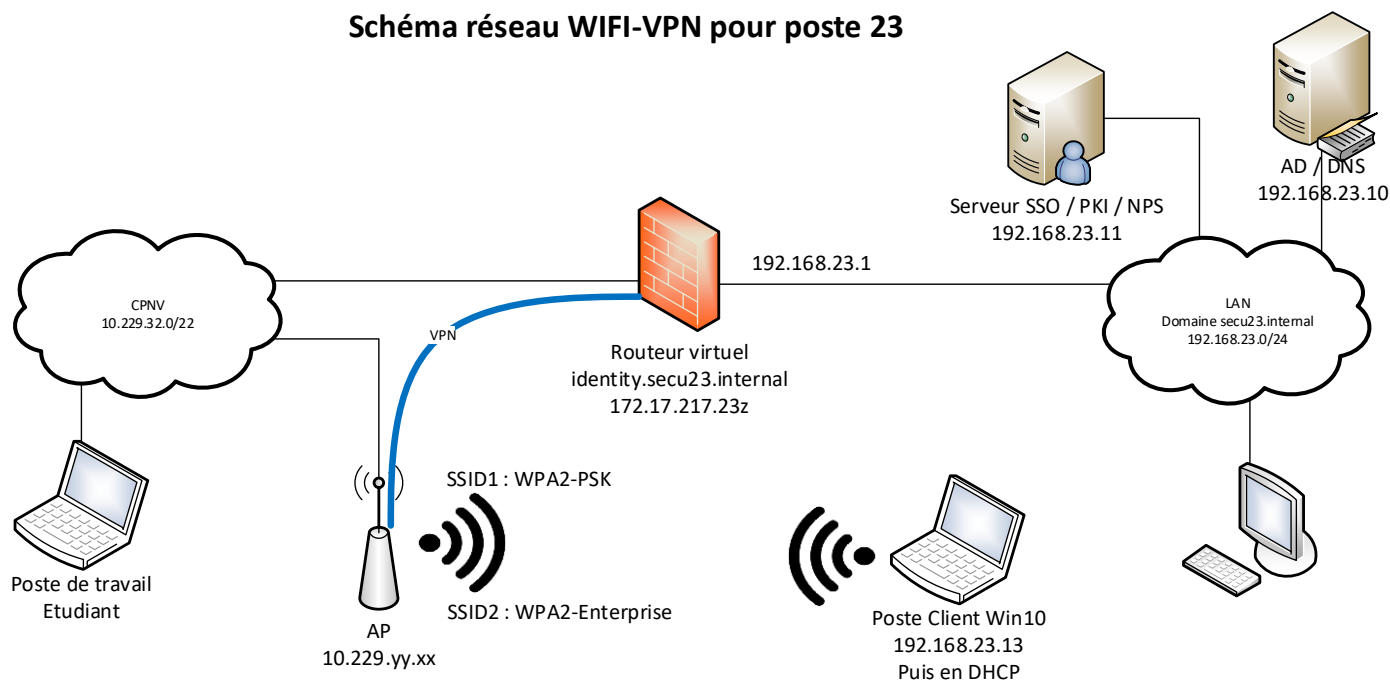
Configuration de l'AP Mikrotik

Table des matières

Configuration du routeur Mikrotik	1
Schéma explicatif	1
Connexion au routeur	2
Vérification DHCP	2
Configuration des Bridges	3
Configuration d'une IP attribuée au bridge	3
Configuration du SSID-PSK	4
Attribution des ports à leur bridge	5
Création du tunnel VPN	6
Test	6
Création d'un profil de sécurité Wifi pour le RADIUS, SSID WPA2-ENTERPRISE	7
Check du fonctionnement	9

Schéma explicatif

Schéma réseau WIFI-VPN pour poste 23



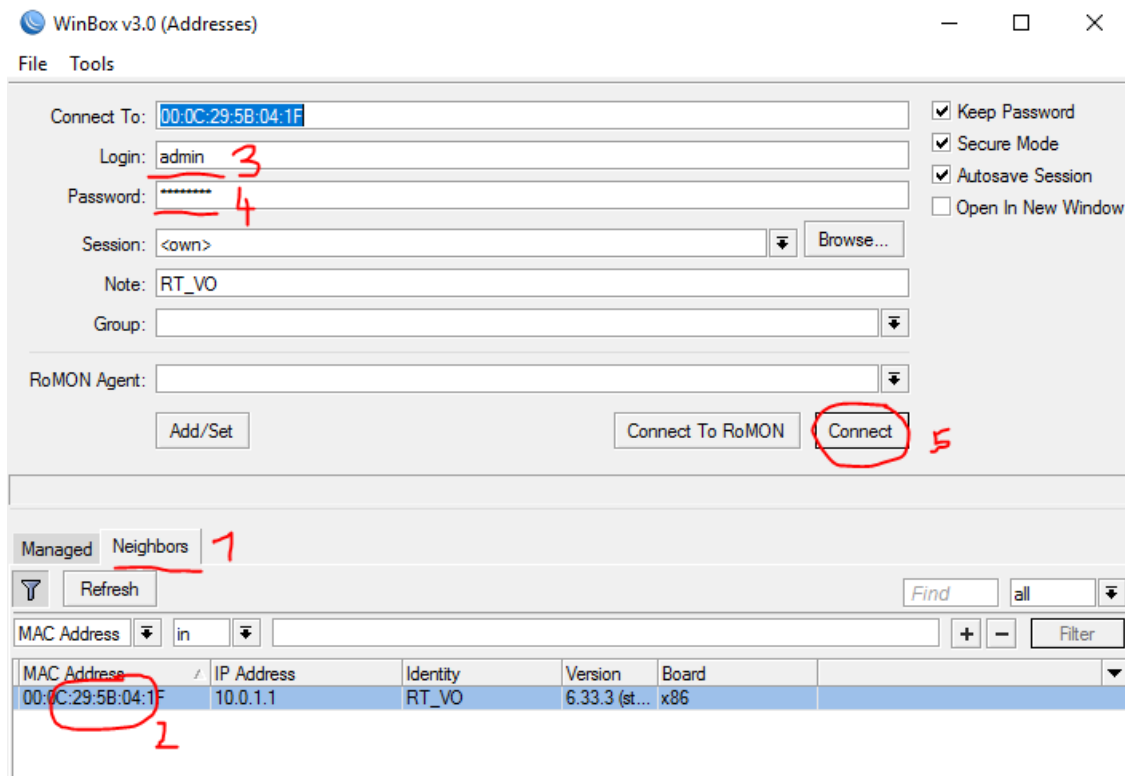
Connexion au routeur

Utiliser Winbox à télécharger sur www.mikrotik.com. Pas besoin de l'installer ce n'est qu'un exe.

A l'aide d'une machine Windows connecter un câble en direct sans passer par le réseau du CPNV.

Lancer Winbox

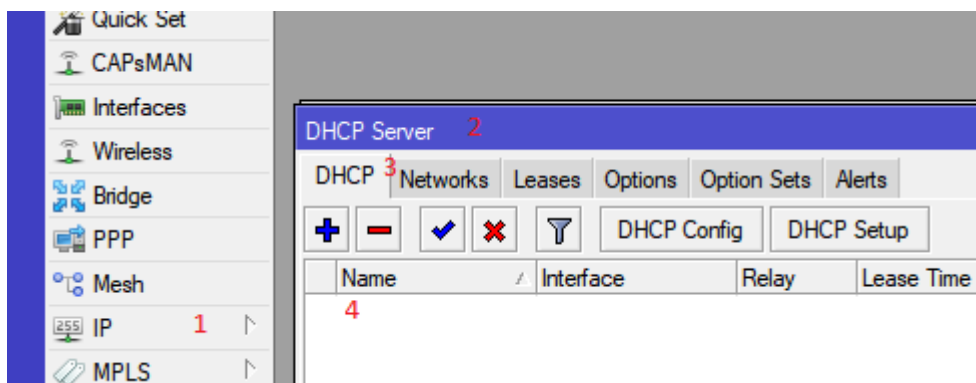
1. lancer la découverte
2. Cliquer sur la mac adresse de votre routeur
3. Mettre le login : généralement admin
4. Mettre le mot de passe : généralement rien (pas configuré)
5. Cliquer sur connect.



Vérification DHCP

Vérifier qu'il n'y ait pas de serveur DHCP qui puisse perturber le fonctionnement de l'école.

Menu IP -> DHCP Server -> Onglet DHCP -> vérifier qu'il n'y ait rien dans la liste du point 4.



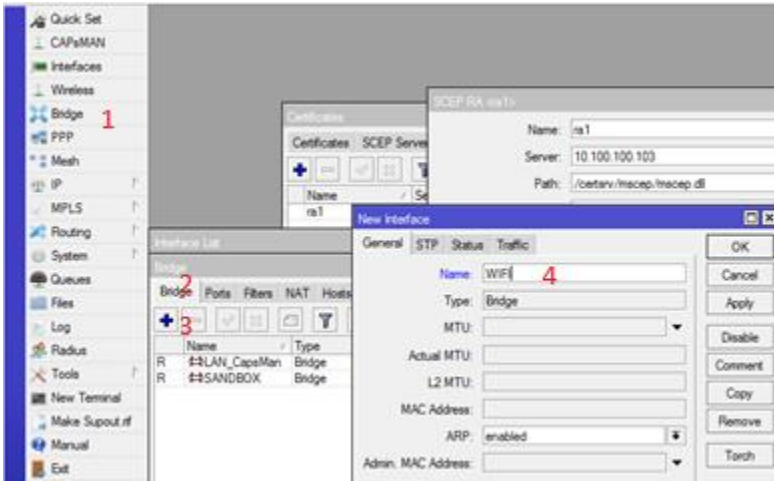
Configuration des Bridges

Pour les besoins du projet, nous devons créer deux Bridge

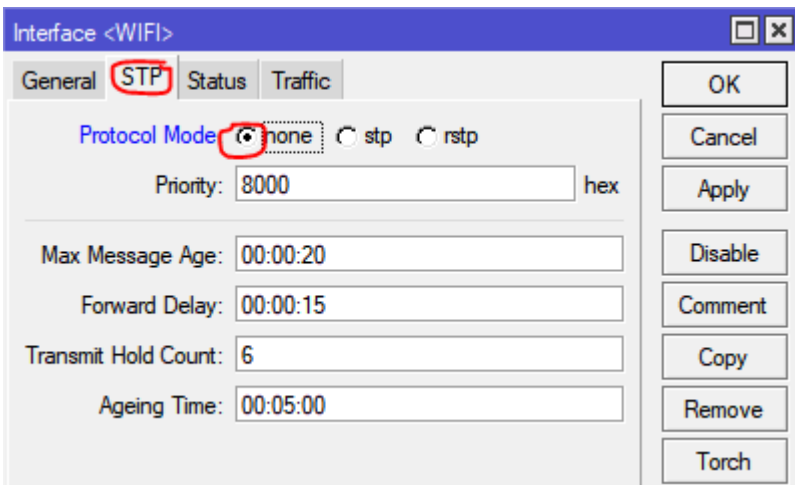
1. Bridge CPNV ou WAN
2. Bridge WIFI

Opération à exécuter

Menu Bridge, onglet Bridge, bouton Plus



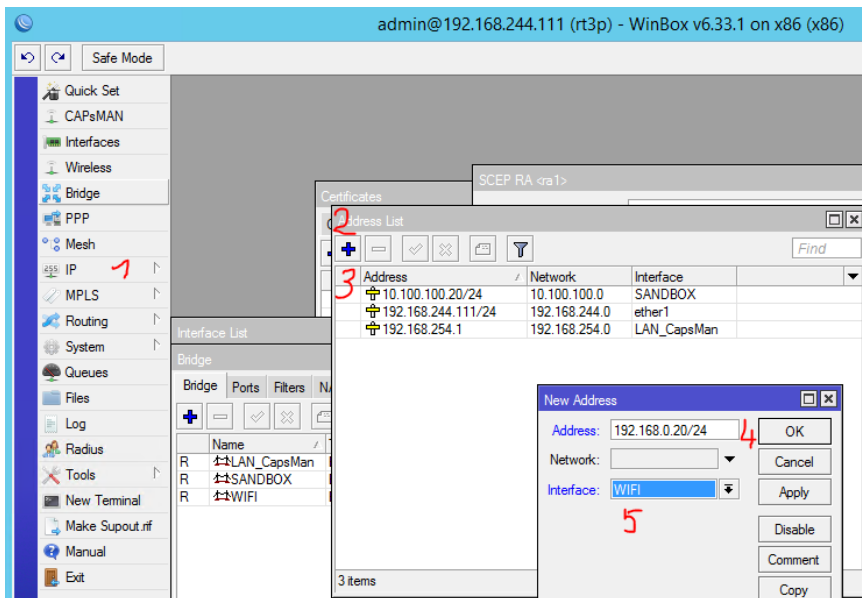
Attention ---- Désactiver le spanning-tree sur les bridges --- Sinon le port du switch du CPNV va tomber.



Configuration d'une IP attribuée au bridge

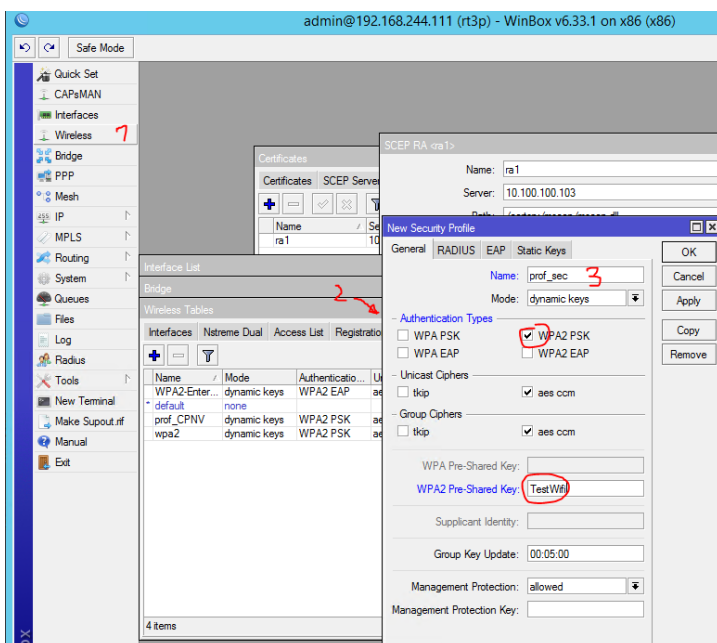
Pour le Bridge WIFI une ip de votre range LAN -> 192.168.x.20 (x est le numéro de votre PC Physique)

Pour le Bridge CPNV une ip de votre range CPNV -> 10.229.zz.xy (selon les plages d'adresse IP fixe attribuée à la classe)

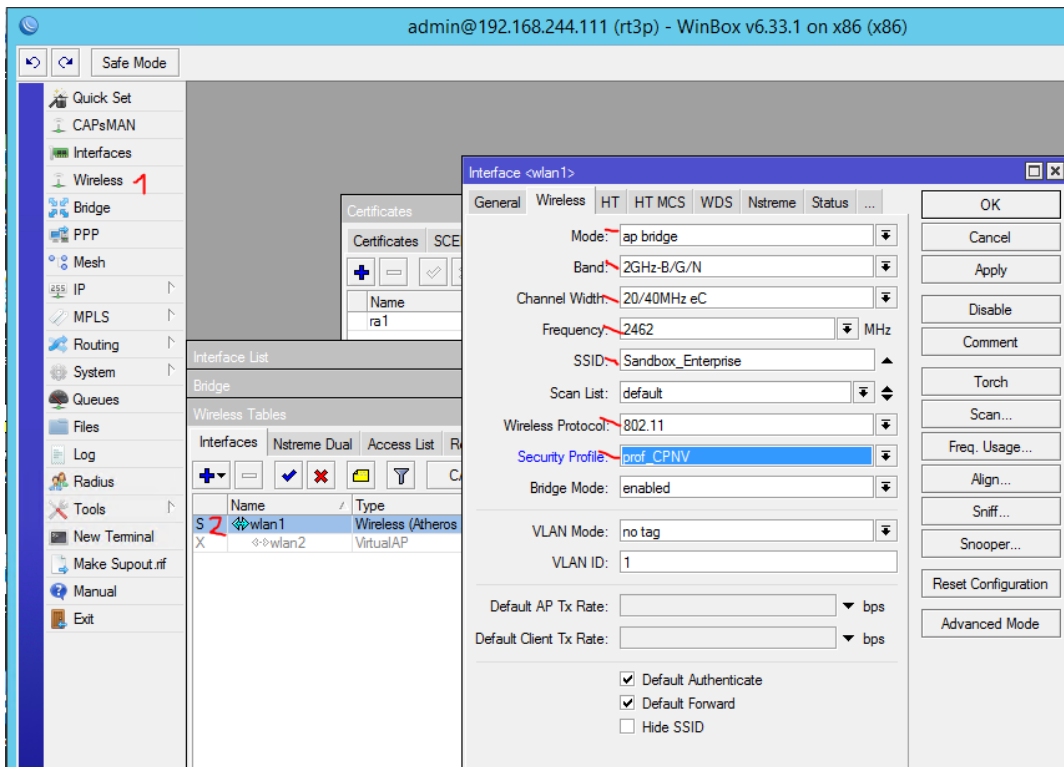


Configuration du SSID-PSK

Création d'un profil de sécurité pour faire un SSID en WPA2-PSK (avec un clé unique pour tout le monde)



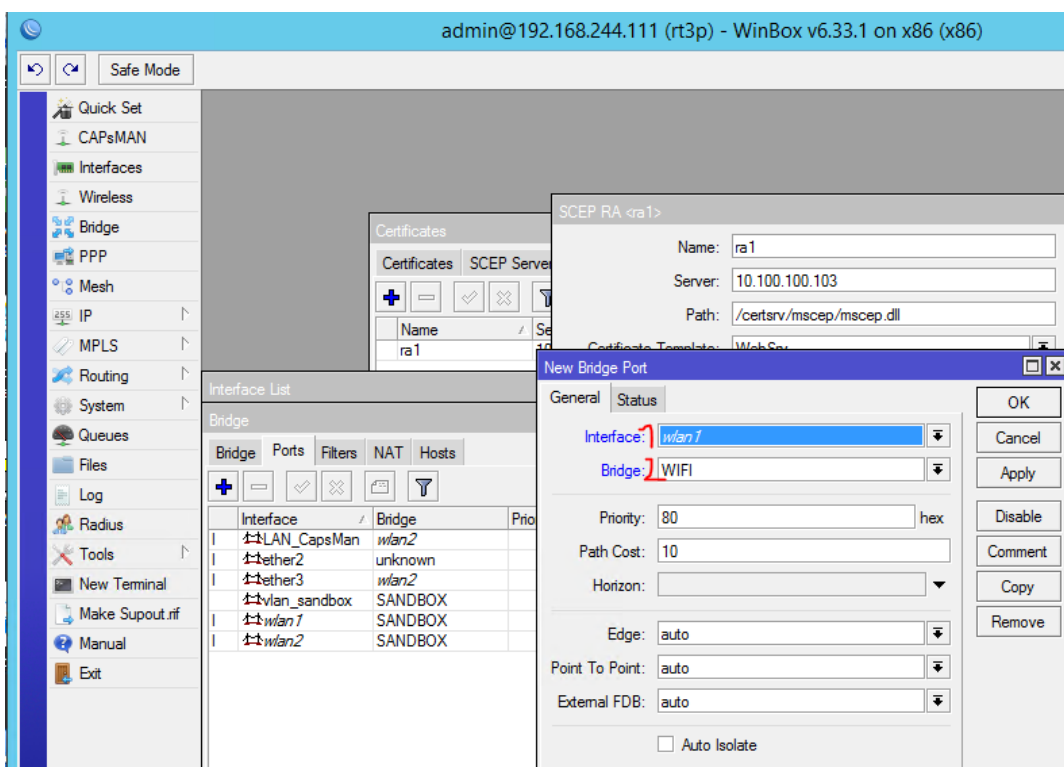
Configuration de la carte Wifi WLAN2 SSID et profil de sécurité



Attribution des ports à leur bridge

Connexion du wlan1 dans le bridge WIFI

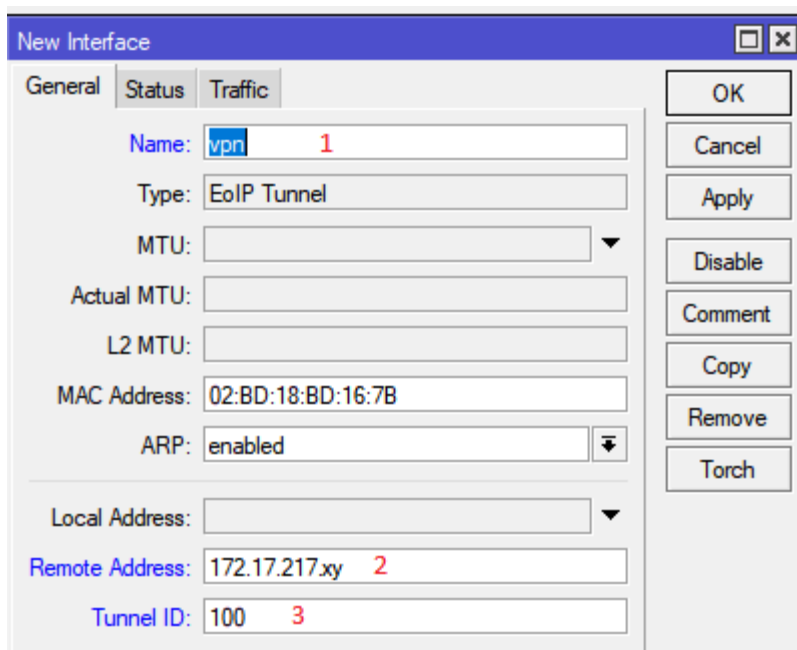
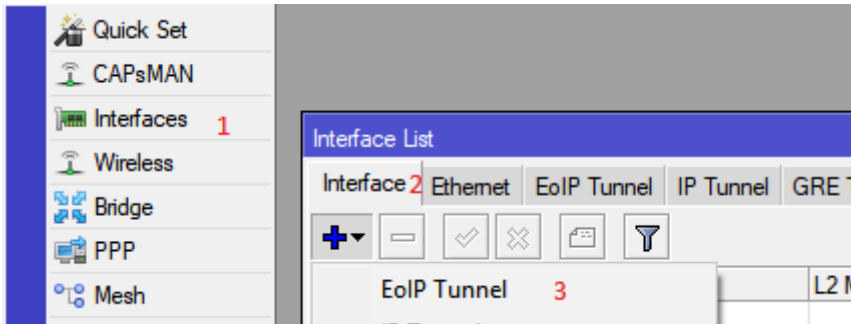
Connexion de la carte ether1 (ou celle sur lequel physiquement le routeur est connecté) dans le bridge CPNV



Création du tunnel VPN

Pour mettre en relation le LAN et le bridge WIFI nous devons établir un tunnel VPN de niveau 2 du protocole OSI (un approfondissement théorique sera donné plus tard), afin que les broadcasts puissent transiter à travers ce tunnel pour que les client Wifi puisse obtenir un IP du DHCP par exemple

Sur l'AP Création du tunnel en EoIP



Pour le point 2

- Sur l'AP mettre l'IP du routeur virtuel

Vous devez faire la même chose sur le routeur virtuel, mais en indiquant au point 2 l'adresse de l'AP

Puis le tunnel devrait monter automatiquement

Mettre l'interface eoip-vpn dans le Bridge WIFI et sur le routeur virtuel, vous devez mettre l'interface eoip-vpn dans le bridge LAN afin que le bridge Wifi de l'AP se retrouve en contact avec le bridge du LAN du routeur à travers le vpn.

Test

Depuis une machine du LAN secu-x.internal vous devriez pouvoir pinguer l'AP par son adresse IP 192.168.x.20 (IP du bridge WIFI) en passant par le tunnel vpn en toute transparence.

Création d'un profil de sécurité Wifi pour le RADIUS, SSID WPA2-ENTERPRISE

The screenshot shows the Mikrotik WinBox interface. On the left sidebar, the 'Radius' menu item is highlighted. The main window displays the 'New Radius Server' configuration dialog. The 'General' tab is selected. Under the 'Service' section, the 'ppp' checkbox is checked, and the 'wireless' checkbox is also checked. The 'Address' field is populated with '10.100.100.18', and the 'Secret' field contains 'Test123\$'. Other configuration options include 'Called ID', 'Domain', 'Authentication Port' (1812), 'Accounting Port' (1813), 'Timeout' (300 ms), 'Accounting Backup' (unchecked), 'Realm', and 'Src. Address'. The status at the bottom of the dialog is 'enabled'.

#	Service	Called ID	Domain	Address	Secret
1	ppp			10.100.100.18	Test123\$

Security Profile <WPA2-Enterprise>

General | **RADIUS** | EAP | Static Keys

Name:

Mode:

- Authentication Types

☐ WPA PSK ☐ WPA2 PSK

☐ WPA EAP ☒ WPA2 EAP

- Unicast Ciphers

☐ tkip ☒ aes ccm

- Group Ciphers

☐ tkip ☒ aes ccm

WPA Pre-Shared Key:

WPA2 Pre-Shared Key:

Supplicant Identity:

Group Key Update:

Management Protection:

Management Protection Key:

OK
Cancel
Apply
Copy
Remove

Security Profile <WPA2-Enterprise>

General | RADIUS | **EAP** | Static Keys

☐ MAC Authentication

☐ MAC Accounting

☒ EAP Accounting

Interim Update:

MAC Format:

MAC Mode:

MAC Caching Time:

OK
Cancel
Apply
Copy
Remove

Security Profile <WPA2-Enterprise>

General | **RADIUS** | EAP | Static Keys

EAP Methods:

TLS Mode:

TLS Certificate:

OK
Cancel
Apply
Copy
Remove

Check du fonctionnement

Radius Server <10.100.100.18>

General | **Status**

Pending:

Requests:

Accepts:

Rejects:

Resends:

Timeouts:

Bad Replies:

Last Request RTT:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Status