



Intégrez la flexibilité dans votre réseau

Philippe ROBERT

Orateur

Philippe ROBERT – p.robert@engitech.ch

MTCNA . MTCRE . MTCTCE . MTCUME

MTCWE . MTCINE . MTCIPv6E

certifié comme formateur MikroTik depuis 2013

(Microsoft – Vmware – Citrix certifications)

ENGITECH S.A. , Genève – Suisse

consulting, formation et distribution des produits MikroTik

gestion serveurs, datacenter, réseau wifi, voip

société certifiée MTCSA depuis 2018

Projects

- Support infra réseau:
ISP – WISP – VPN
- Installation
WIFI – VPN ...
- LTE



LTE

Wireless Antenna
LTE antenna

120 Mbps down
40 Mbps up

remplacement
de ligne ADSL

	Name	Type	MTU	Actual MTU	Tx	Rx
R	lte1	LTE	1500	1500	3.8 Mbps	127.2 Mbps

	Name	Type	MTU	Actual MTU	Tx	Rx
R	lte1	LTE	1500	1500	47.1 Mbps	1630.5 kbps



Actuellement RouterOS supporte les modem LTE cat. 4 (150 / 50 Mbps).

Dans les prochains mois, il supportera également les modems LTE cat. 6.

-> 300 / 50 à 600 / 100 Mbps

Matériel

Gamme complète ...

Cartes à intégrer (RBM11G, RB953GS, ...)

Routeur (hEX, CCR10xx, RB1100, ...)

Switch (CRS1xx, CRS2xx, CRS3xx, PoE, ...)

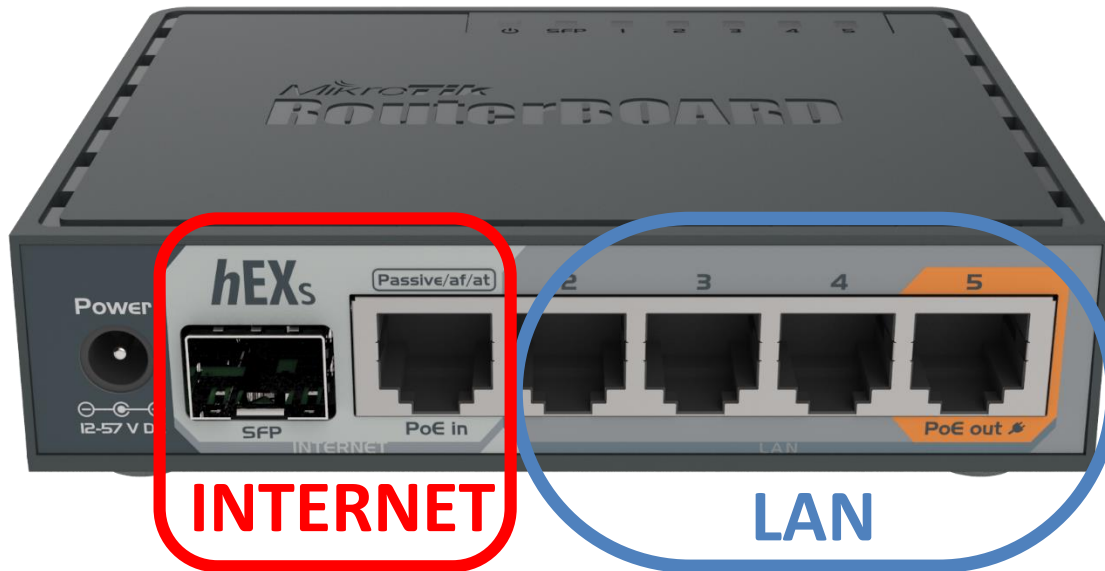
Avec antenne intégrée (SXT, LHG, WAP, ...)

et différentes fréquences: 2.4, 5, 60ghz, LTE ...

Powerline

Accessoires, SFP, ...

hEX S



- CPU puissant:
- 2x 880mhz MMIPS
 - Ram 256mb
 - Port SFP
 - Port USB
 - SD CARD
 - «Dude compatible»

Attribution des ports «internet», «lan» ?

Avec RouterOS, chaque port peut être reconfiguré

hEX S



12-57V !

PoE

Sortie PoE

Commutable!

Alimentation «flexible»
DC connecteur ou PoE ...

Les 2 simultanément !
Redondance d'alimentation possible
(5v différence préférable)

Pour:

- autre matériel MikroTik
- caméra, téléphone, bridge VDSL
- changement de voltage possible avec un splitter PoE (48v à 12v)

hEX S



SD CARD:

- Sauvegarde
- TFTP serveur
- FTP, SMB (sauvegarde d'autres périphériques)
- ...

Bouton «Reset»

- Remise aux paramètres d'usine
- Démarrage réseau

USB:

- Clef data
 - Woobm (management via wifi)
 - Liaison UPS, GPS, port série ...
 - Modem GSM (SMS..)
 - Modem 3G, 4G
- ou simplement comme alimentation
- caméra, routeur, AP, raspberry, ...

Bouton «Mode»

Exécution d'un script

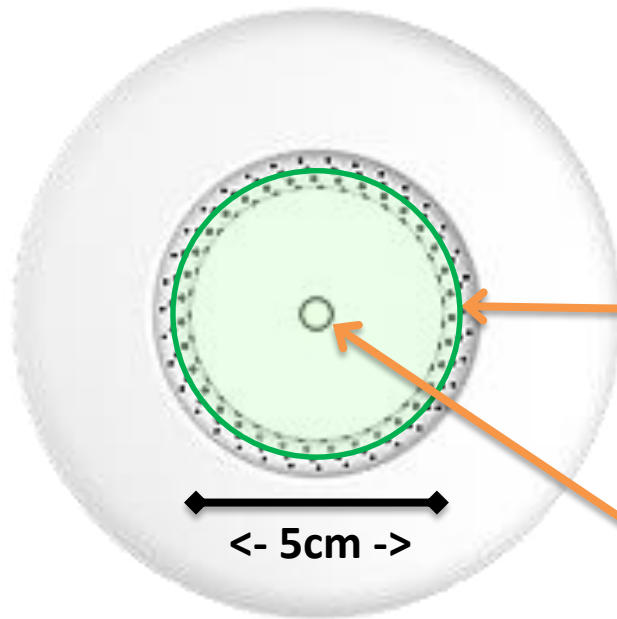
Mode Bouton

Présent sur:

RBcAPGi-5acD2nD (**cAP ac**)
RBwsAP5Hac2nD (wsAP ac lite)
RB750Gr3 (hEX)
RB760iGS (hEX S)
RB912R-2nD (LtAP mini, LtAP mini LTE/4G kit)
RBD52G-5HacD2HnD (hAP ac2)
RBLHGR (LHG LTE/4G kit)
RBSXTR (SXT LTE/4G kit)
CRS328-4C-20S-4S+RM
CRS328-24P-4S+RM

Mode Bouton

cAP AC -> The buzzer AP !



Le bouton occupe le centre de l'appareil et permet de donner facilement accès à une fonctionnalité.

Une Led peut aussi être paramétrée pour indiquer l'état de la commutation.

Mode Bouton

Exemple: on/off pour la partie wifi

Activation du "mode-button":

```
/system routerboard mode-button  
set enabled=yes on-event=wlan_on_off
```



Script:

```
:if ( [/int wlan get 0 disabled ] = true ) do={  
:interface wireless set numbers=0  
disabled=no;  
:interface wireless set numbers=1  
disabled=no;  
:system led set numbers=2 disabled=no  
type=on;  
} else={  
:interface wireless set numbers=0  
disabled=yes;  
:interface wireless set numbers=1  
disabled=yes;  
:system led set numbers=2 disabled=no  
type=off;  
}
```

Mode Bouton

ou toute autre utilisation

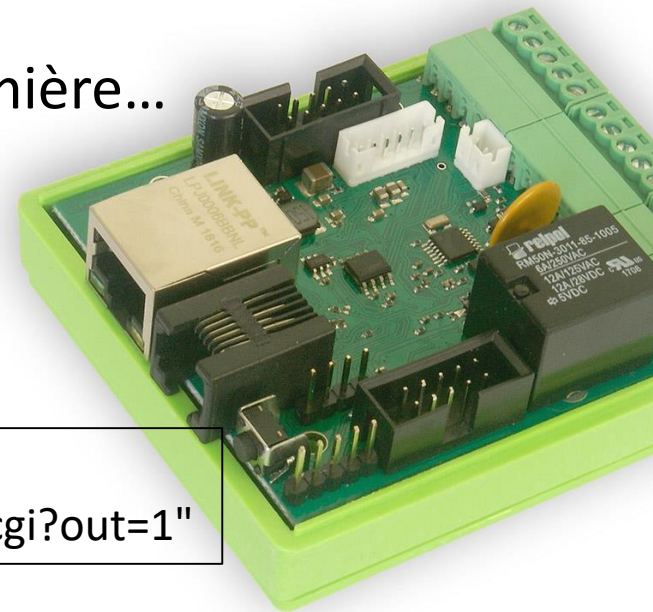
- N'importe quelle fonctionnalité de RouterOS
- Interaction avec d'autres appareils

Possibilité d'ouvrir une porte, allumer une lumière...

Tinycontrol, relais réseau commutable via url:

Script:

```
/tool fetch url="http://admin:admin@192.168.88.179/outs.cgi?out=1"
```



RouterOS

OS à multiples fonctionnalités
Bridge, firewall, wifi, VPN, Routage ...

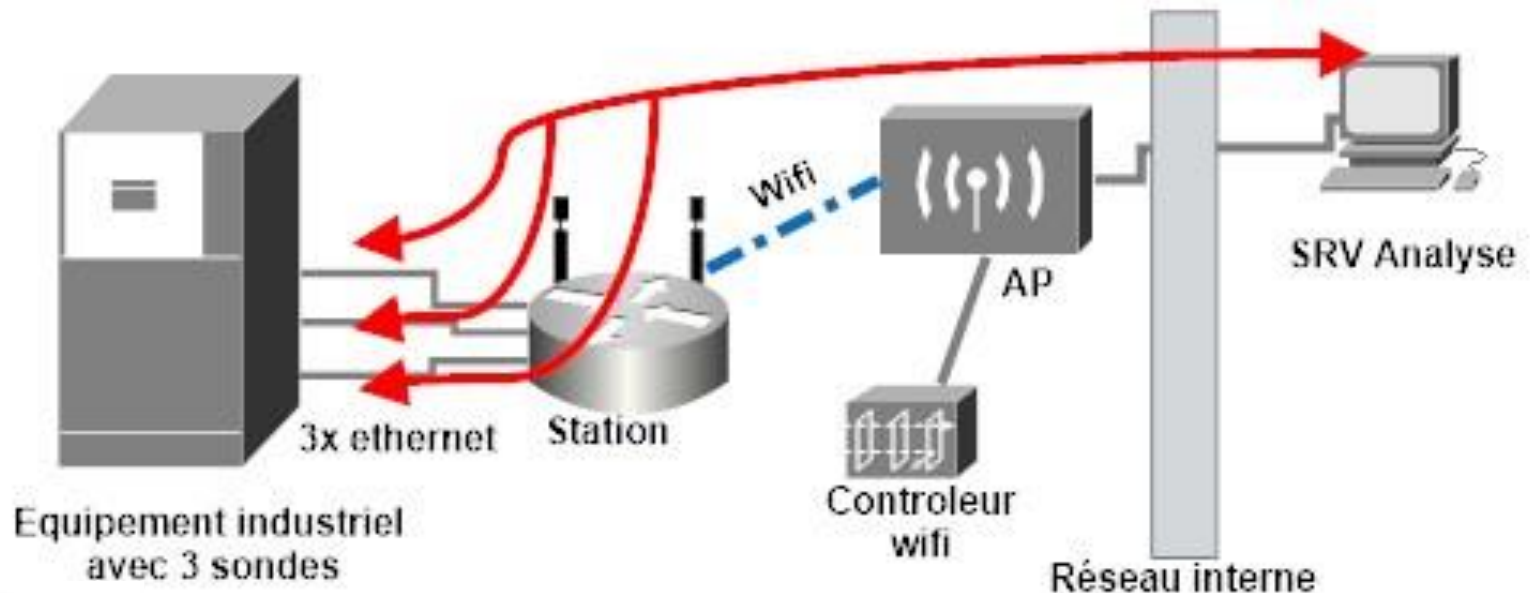
Même fonctionnalité sur tous les appareils MikroTik, l'utilisation peut dépendre des capacités du matériel

Permet de combiner ces différentes possibilités pour résoudre avec un appareil des cas de configuration complexe

Exemple de réalisation

Machines industrielles à relier au réseau de l'entreprise pour analyse des données.

- Ces machines ont une connectivité Ethernet
- Plusieurs sondes par machine, plusieurs connexions Ethernet nécessaires
- Obligation de connecter via wifi pour limiter les câblages



Exemple de réalisation

Problématique:

La société a investi «beaucoup» dans des APS d'une marque concurrente et une sécurisation des ces points d'accès a été configurée (WPA2 EAP, sécurité faite par une compagnie tierce et ne peut être modifiée).

Fait:

Plusieurs marques ont été testées comme client wifi (dont la marque des APs) mais le passage de plusieurs MAC ADDRESS ne fonctionne pas ou alors de manière aléatoire.

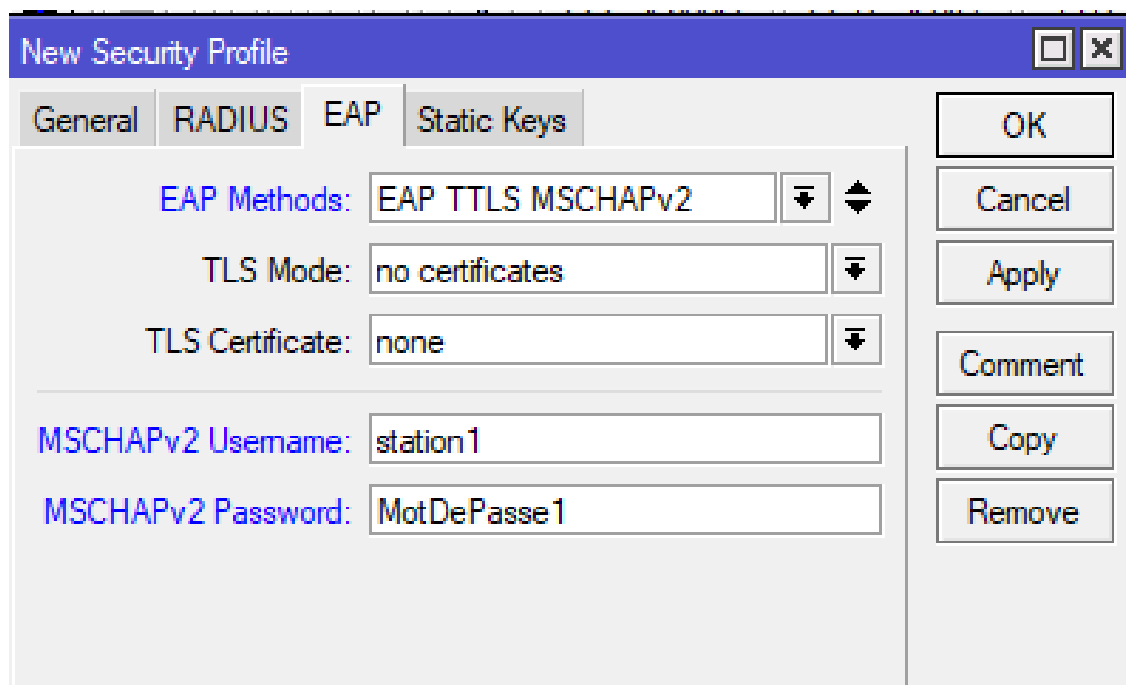
Situation

La sécurisation apportée sur les points d'accès wifi amène la complexité suivante:

- 1) L'authentification de la station doit se faire en sécurisation WPA2 EAP MSCHAP2
- 2) Le mode station wds ou le mode station pseudobridge ne fonctionne pas (Autres marques et MikroTik)
- 3) Plusieurs périphériques se trouvent derrière la station wifi (utilisation du mode pseudobridge clone pas suffisante)

Point 1

Le mode station avec WPA2 EAP est pris en charge:



Fonctionne parfaitement dans cette configuration.

Point 2 et 3

- Seul le mode «station fonctionne»
- Nécessité de relier les périphériques «Ethernet» via cette connexion wifi

Solution: (une des possibles...)

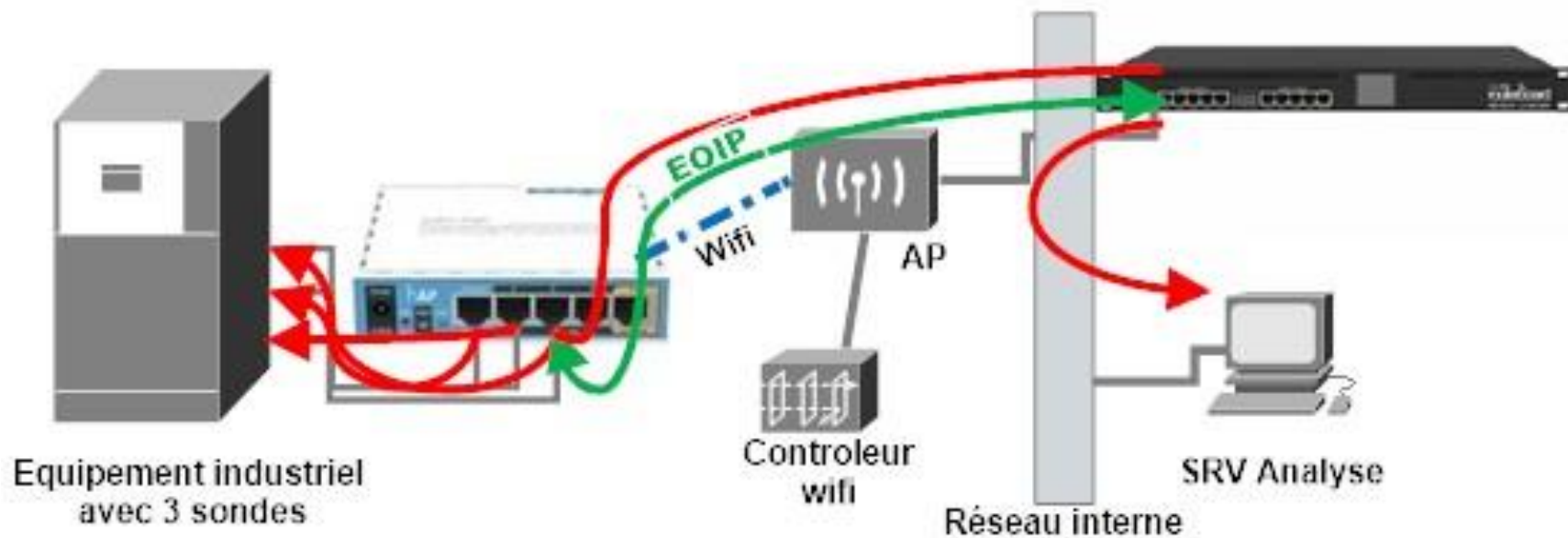
- Création d'un tunnel EOIP via le wifi (rajout d'un «serveur vpn»)
- Création d'un bridge – int. Ethernet et tunnel EOIP dans ce bridge

Choix du matériel:

Pour la partie cliente: **hAP ac lite** -> dual wifi, alimentation via 24v (voltage présent sur la machine industrielle)

Pour la partie serveur: **RB3011**, rackable suffisamment puissant pour la quantité de vpn (une centaine) nécessaire

Solution



La solution fonctionne

La solution fonctionne mais crée un SPOF.

En effet, si le serveur VPN n'est pas disponible, aucune liaison ne sera possible sur les sondes des machines industrielles.

Amélioration:

- ajout d'un second routeur VPN RB3011
- mettre l'adresse du serveur VPN en VRRP.
- recopier de façon automatique les tunnels VPN EOIP du 1^{er} routeur vers le 2^{ème} en cas de modification

V.R.R.P.

- «Virtual Router Redundancy Protocol» fournit une solution pour combiner un certain nombre de routeurs dans un groupe logique appelé «Virtual Router»
- Les routeurs faisant partie d'un même groupe se partagent une adresse IP que l'on va utiliser pour le VPN EOIP
- Rétablissement de la liaison en moins de 3 secondes

Configuration de V.R.R.P.

Ajouter une interface:

- interface associée (ether1)
- définir le VRID – id unique au groupe
- définir la priorité
 - -> 100 pour le maître (RB1)
 - -> 50 pour le backup (RB2)

Une fois que l'interface est créée, il faut lui assigner une adresse IP qui va être partagée entre les routeurs

RB1: 192.168.1.11/24

RB2: 192.168.1.12/24

VRRP ADRESSE: 192.168.1.254/32

Important : Toujours utiliser le subnet /32

The screenshot shows the configuration window for VRRP on interface ether1. The window has tabs for General, VRRP, Scripts, and Traffic. The VRRP tab is active. The configuration fields are as follows:

- Interface: ether1
- VRID: 1
- Priority: 100
- Interval: 1.00 s
- Preemption Mode
- Authentication: none (selected), simple, ah
- Password: (empty)
- Version: 3
- V3 Protocol: IPv4

At the bottom of the window, there are status indicators: enabled, running, slave, and master.

EOIP sur le second RB3011

Les tunnels peuvent être recopié du 1^{er} serveur vers le second.

Astuce:

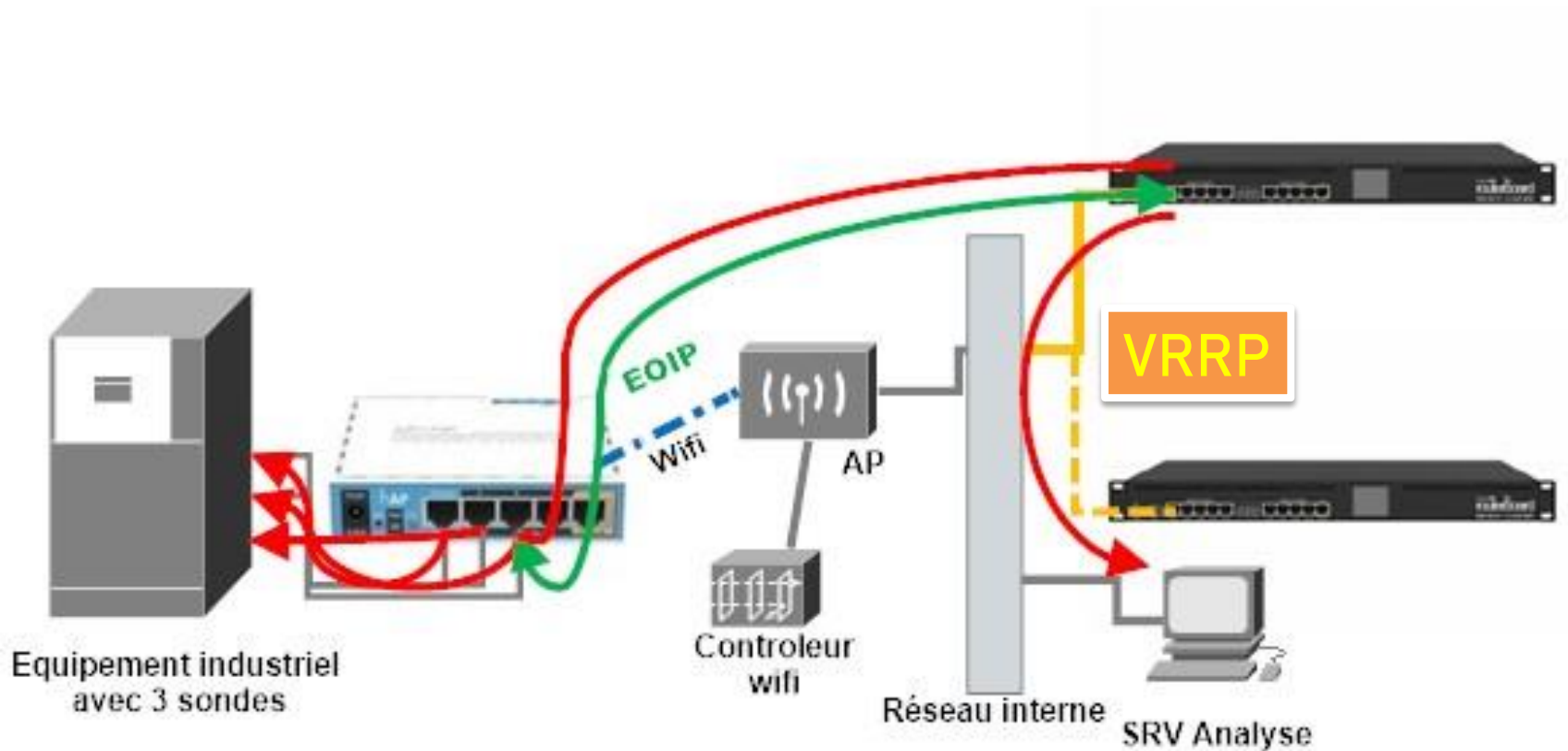
RouterOS ne va pas essayer de monter le tunnel EOIP si l'adresse LOCALE n'est pas active sur le routeur.

Donc, tant que le routeur est en mode «vrrp backup», l'adresse ne lui appartient pas et rien ne se passe.

EOIP

Local Address:	<input type="text" value="192.168.1.254"/>
Remote Address:	<input type="text" value="192.168.1.101"/>
Tunnel ID:	<input type="text" value="101"/>

Solution redondante



Conclusion

- Grâce au matériel MikroTik et aux possibilités de RouterOS, les possibilités de réalisations sont multiples, simples, efficaces et économiques.
- L'équipe MikroTik rajoute des fonctionnalités continuellement à RouterOS, ...

MERCI pour ces évolutions !

Philippe ROBERT - p.robert@engitech.ch