Envoi de message lorsque un autre serveur DHCP est détecté :

Pour envoyer un message par e-mail lorsqu'un autre serveur DHCP est trouvé il faut créer un script, en remplaçant adresse@email.com par les adresses e-mails auxquelles on veut les envoyer. L'adresse e-mail qu'il faut modifier dans « to » c'est l'adresse qui reçoit et dans « from » l'adresse qui l'envoie :

```
/system script add name=dhcp-alert source="/tool e-mail send
to=adresse@email.com subject=("Rogue DHCP Server Alert") body=("Rogue DHCP
Server detected on interface $interface, IP: $dhcpserver")
from=adresse@email.com
```

Pour envoyer des messages il faut configurer l'envoie avec le serveur SMTP c'est-à-dire l'adresse du serveur(address), le port(port), l'identifiant(user) et le mot de passe(password) du serveur SMTP :

```
/tool e-mail set address=adresse.serveur.smtp port=(n°du port)
from=adresse@email.com user=adresse@email.com password=(mot de passe serveur
SMTP)
```

On peut envoyer un mail de test pour vérifier si la configuration du serveur SMTP renseigné est bonne :

```
/tool e-mail send to=adresse@email.com from=adresse@email.com subject=Test
body=test
```

Il faut configurer l'alerte pour le serveur DHCP, par exemple pour l'interface ether4 :

```
/ip dhcp-server alert add interface=ether4 on-alert=dhcp-alert disabled=no
```

Il faut récupérer l'adresse MAC du DHCP que l'on connaît et le renseigner :

```
/ip dhcp-server alert set ether4 valid-server=00:00:00:00:00:00
```

DHCP snooping :

Le DHCP Snooping est une technique qui permet de configurer le switch pour **écouter le trafic DHCP** et arrêter tous les **paquets malveillants** non autorisés.

On peut créer ou utiliser le bridge existant pour rajouter le dhcp snooping :

```
/interface bridge set numbers=0 dhcp-snooping=yes
```

On peut rajouter l'option 82 que lorsque le dhcp snooping est activé. Celle-ci est implémentée sur un équipement de commutation, elle comprend l'ID de circuit, l'ID distant et l'ID fournisseur en sous-options. Ces sous-options sont des champs dans l'en-tête du paquet :

```
/interface bridge set [find where name="bridge"] add-dhcp-option82=yes
```

On peut créer ou utiliser le bridge existant pour rajouter le dhpc snooping. (bien vérifier les ports utilisés)

```
/interface bridge port set interface=ether2 bridge=bridge
```

Si un appareil envoi une requête il faut qu'elle atteigne le dhcp pour que celui-ci lui fournisse une adresse IP

```
/interface bridge port set interface=ether2 trusted=yes
```

DHCP snooping + Envoi de message lorsqu'un autre serveur DHCP est détecté avec 2 routeurs et 2 switchs :

On peut utiliser les deux ensemble. Si dans DHCP snooping, le port est mis en trusted=no, dans les logs il y aura seulement un avertissement.

Si le port est mis en trusted=yes, dans les logs il y aura un message d'erreur et un e-mail sera envoyé.

Lors de la configuration pour envoyer un message, si aucune adresse MAC n'est saisie pour valid-server, cela affichera un message d'erreur dans les logs et enverra un e-mail pour chaque nouveau DHCP détecté.

J'ai essayé de modifié le script pour qu'il envoie l'interface et son adresse IP car pour le moment il envoie seulement l'interface où le DHCP a été détecté, mais je n'y suis pas arrivé : soit le mail ne s'envoie pas, soit le corps du mail est vide.

Ce script est censé afficher dans le corps du mail la dernière modification faite en rapport avec l'interface ether4.

```
/tool e-mail send to=darkimoi14@gmail.com subject=("Rogue DHCP Server Alert")
body=([/execute {"/interface print detail where name=ether4" :foreach line in=[find] do={:put
$line} }])
```

Ce script doit créer une variable appelée $erreur pour récupérer dans les logs le dernier message d'erreur et l'afficher dans le mail.

```
:local erreur ""
:foreach logEntry in=[/log find where message~"error" limit=10] do={
  :set erreur ($erreur . [/log get $logEntry message] . "\n")
}
/tool e-mail send to=darkimoi14@gmail.com subject="Erreur détectée" body=$erreur
```

Mais au lieu de l'afficher directement dans le mail, il modifie le fichier erreur.txt et l'attache en pièce jointe dans le mail.

```
:foreach logEntry in=[/log find where message~"error" limit=10] do={
  :local logMessage [/log get $logEntry message]
  :put $logMessage
  :set erreur ($erreur . $logMessage . "\n")
}

:local fileName "erreur.txt"
:local filePath ("/" . $fileName)
/file print file=$fileName
:if ([:len [/file find where name=$fileName]] = 0) do={
  /file print file=$fileName
  /file set $fileName contents=""
```

```
}
/file set $fileName contents=($erreur . "\n")

/tool e-mail send to=darkimoi14@gmail.com subject="Erreur détectée" \
    file=$filePath
```

Créer des bridges et avoir accès à Internet :

Pour mettre en place deux bridges sur un routeur mikrotik il faut que ceux-ci aient accés à internet, Il faut que 2 ports soit sur un bridge avec un dhcp serveur à l'adresse 192.168.10.1 et les deux autres ports sur un autre bridge avec un dhcp serveur à l'adresse 192.168.25.254

J'ai donc commencé par supprimer les ports qui étaient assignés au bridge par défaut sauf le port ether2 connecté à l'ordinateur car je perdais la connection ssh.

J'ai crée deux nouveaux bridges :

```
/interface bridge add name=bridge10

/interface bridge add name=bridge25
```

J'ai ensuite assigné les bridges à des ports :

```
/interface bridge port add interface=ether3 bridge=bridge10

/interface bridge port add interface=ether4 bridge=bridge25

/interface bridge port add interface=ether5 bridge=bridge25
```

J'ai crée des adresses IP pour les bridges :

```
/ip address add address=192.168.10.1 interface=bridge10

/ip address add address=192.168.25.254 interface=bridge25
```

J'ai crée les plages IP pour les deux serveurs dhcp :

```
/ip pool add name=pool10 ranges=192.168.10.10-192.168.10.254

/ip pool add name=pool25 ranges=192.168.25.1-192.168.25.240
```

J'ai créer les serveurs dhcp :

```
/ip dhcp-server add name=server10 interface=bridge10 address-pool=pool10

/ip dhcp-server add name=server25 interface=bridge25 address-pool=pool25
```

J'ai ensuite configurer les réseaux pour les serveurs dhcp. J'ai pris comme exemple la configuration par défaut et je l'ai adapté pour avoir accès à internet :

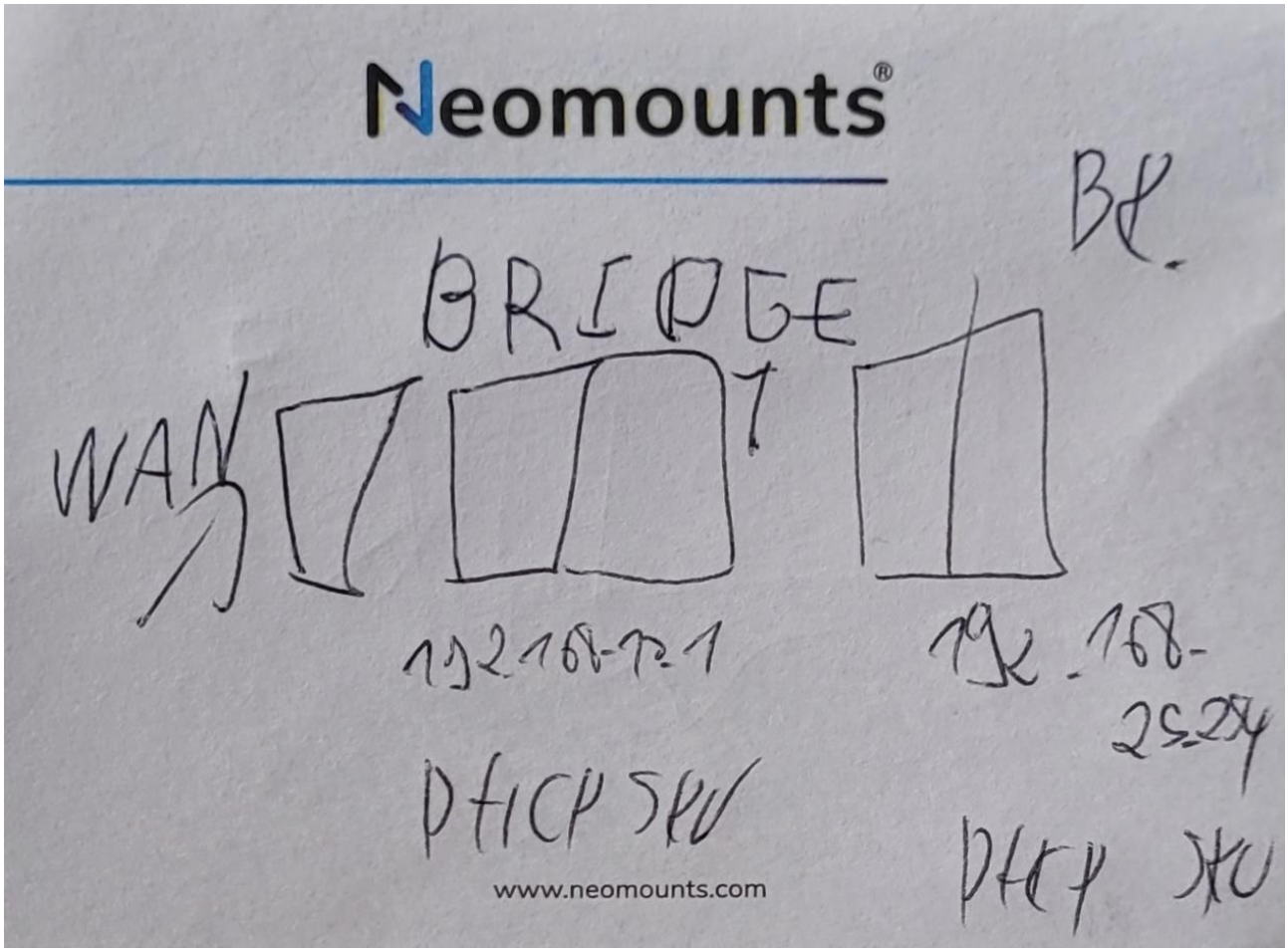
```
/ip dhcp-server network add address=192.168.10.0/24 gateway=192.168.10.1 dns-
server =192.168.10.1
```

/ip dhcp-server network add address=192.168.25.0/24 gateway=192.168.25.254 dns-server =192.168.25.254

Mais lorsque j'ai utilisé cette configuration je pouvais lancer un ping à l'adresse 8.8.8.8 mais je ne pouvais pas accéder à Internet. J'ai donc regardé le dhcp client (celui qui fourni par internet) et j'ai remplacé la passerelle des dhcp serveurs par celle utilisé par le dhcp client, mais là je ne pouvais plus faire de ping ni accéder à Internet. J'ai ensuite remis la passerelle du départ et j'ai mis le serveur dns de Pobrun et ça a marché.

/ip dhcp-server network edit number=0 gateway (en mettant 10.190.100.2)

/ip dhcp-server network edit number=1 gateway (en mettant 10.190.100.2)

/ip dhcp-server network edit number=0 dns-serveur (en mettant 10.188.2.68)

/ip dhcp-server network edit number=1 dns-serveur (en mettant 10.188.2.68)