Répartition de charge sur plusieurs WANs via le mangle du pare-feu MikroTik

Philippe Escarbassière
Directeur Technique
Active+ Software, Groupe MHz Wireless

Qui sommes-nous ?

- **Active+ Software :**
  - Filiale de MHz Wireless
  - Éditeur de logiciel
  - Service+, ServiceMill, eMill, LC+, CloudSpot

- **MHz Wireless :**
  - Boutique en ligne, Master Distributor MikroTik
  - Spécialisé dans les réseaux sans fils
  - Expertise technique à disposition des clients
  - Distributeur du logiciel LC+
  - https://www.mhzshop.com

Problématiques rencontrées

- **Fourniture de solutions complètes :**
  - Matériel réseau filaire et sans fil
  - Mise en place d'une solution Hotspot LC+
  - Paramétrage complet du matériel

- **Problèmes :**
  - Fibre pas toujours disponible ou trop chère
  - Débits trop faibles pour satisfaire les clients

- **Solutions :**
  - Pont radio vers accès fibre quand possible
  - Multiplier les lignes ADSL / VDSL et répartir la charge...

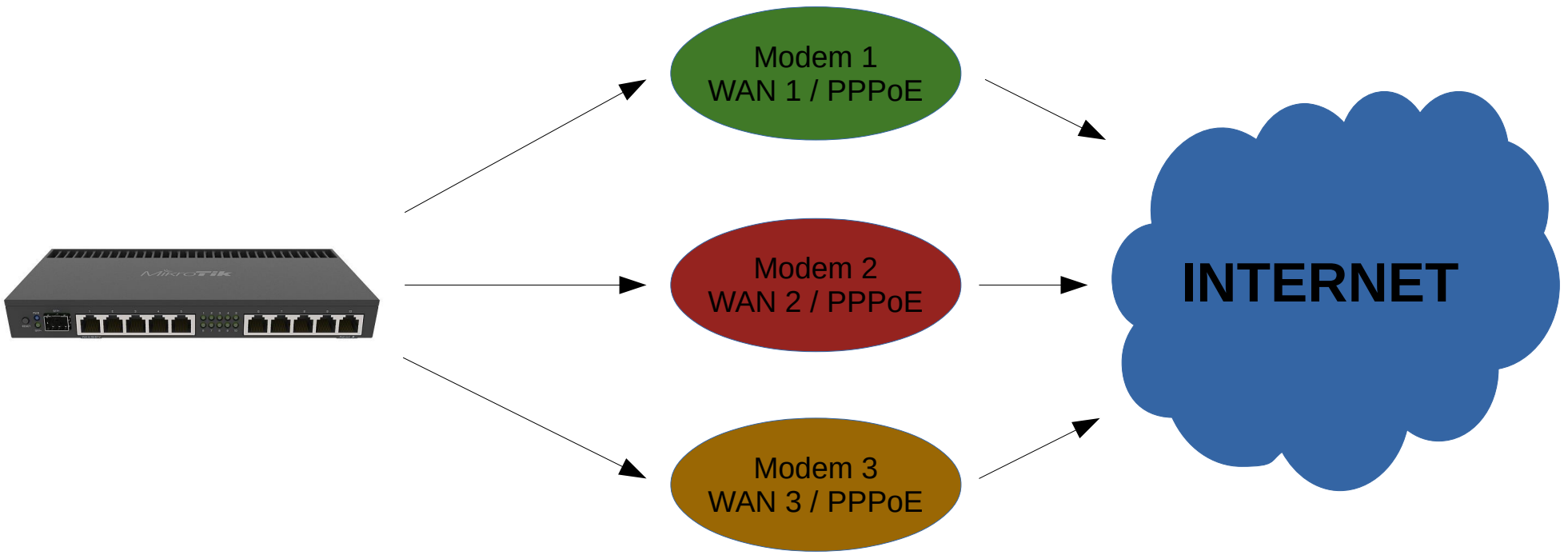
Exemple

- **Camping en campagne avec 3 lignes xDSL**

- **« BOX » opérateurs remplacées par des modems**
  - Évite une couche de NAT
  - Le routeur MikroTik reçoit les IPs publiques
  - Détection de panne plus facile pour redondance

- **WANs configurés en PPPoE**

Exemple


Modem 1
WAN 1 / PPPoE
Modem 2
WAN 2 / PPPoE
Modem 3
WAN 3 / PPPoE
INTERNET

Configuration des WANs

- **Création des connexions PPPoE :**

```
/interface pppoe-client
add disabled=no interface=ether1 name=pppoe-wan1 user=user1 \
    password=pass1
add disabled=no interface=ether2 name=pppoe-wan2 user=user2 \
    password=pass2
add disabled=no interface=ether3 name=pppoe-wan3 user=user3 \
    password=pass3
```

- **Ajout d'une adresse liste « RFC1918 » pour la NAT :**

```
/ip firewall address-list
add address=192.168.0.0/16 list=local
add address=172.16.0.0/12 list=local
add address=10.0.0.0/8 list=local
```

- **Une seule règle de NAT pour tous les WANs :**

```
/ip firewall nat add action=masquerade chain=srcnat \
    dst-address-list=!local src-address-list=local
```

Ajout des routes « normales »

- **Routes par défaut :**

```
/ip route add dst-address="0.0.0.0/0" gateway="pppoe-wan1" \
    check-gateway="ping";
/ip route add dst-address="0.0.0.0/0" gateway="pppoe-wan2" \
    check-gateway="ping";
/ip route add dst-address="0.0.0.0/0" gateway="pppoe-wan3" \
    check-gateway="ping";
```

- **Les paquets non « locaux » et non « marqués » sortiront par un de ces WANs**

- **Si une ligne xDSL tombe, sa passerelle devient injoignable et le routeur désactive la route associée**

Ajout des routes « marquées »

- **Routes par défaut « marquées » :**

```
/ip route add dst-address="0.0.0.0/0" gateway="pppoe-wan1" \
 check-gateway="ping" routing-mark="wan1";
/ip route add dst-address="0.0.0.0/0" gateway="pppoe-wan2" \
 check-gateway="ping" routing-mark="wan2";
/ip route add dst-address="0.0.0.0/0" gateway="pppoe-wan3" \
    check-gateway="ping" routing-mark="wan3";
```

- **Seuls les paquets ayant la marque correspondante sortiront par ces routes « marquées »**

- **Si une passerelle devient injoignable, la route « marquée » sera désactivée et les paquets sortiront par une des routes « normales »**

Répartition de la charge

- **En marquant les paquets pour qu'ils utilisent les 3 routes**

- **La chaîne « prerouting » du mangle est l'endroit idéal :**
  - La décision de routage n'est pas encore prise
  - Le marquage n'est pas possible ailleurs
  - Marquer le paquet ici changera donc sa route

- **Une règle par route de destination**

- **Chaque règle devra marquer environ 1/3 des paquets**

Mode de répartition

- **Aléatoire :**
  - Très bonne répartition mais...
  - Casse la plupart des protocoles

- **Basé sur les adresses sources (ou destinations) :**
  - Lourd à mettre en place, surtout si plusieurs LANs
  - Répartition absolument pas garantie

- **Per Connection Classifier :**
  - Ajouté à RouterOS v3.24 pour exactement ce cas
  - Réparti la charge de façon largement suffisante
  - Plusieurs modes permettent une plus ou moins grande stabilité de la route par machine

Mode de répartition

- **Points importants :**
  - Router les paquets du LAN vers le WAN uniquement
  - Inutile de continuer si le paquet est marqué
  - Fonctionne uniquement avec des « fractions »

```
/ip firewall mangle
add chain="prerouting" src-address-list="local" \
    dst-address-list="!local" per-connection-classifier=\
    "both-addresses:3/0" action="mark-routing" \
    new-routing-mark="wan1" passthrough="no";
add chain="prerouting" src-address-list="local" \
    dst-address-list="!local" per-connection-classifier=\
    "both-addresses:3/1" action="mark-routing" \
    new-routing-mark="wan2" passthrough="no";
add chain="prerouting" src-address-list="local" \
    dst-address-list="!local" per-connection-classifier=\
    "both-addresses:3/2" action="mark-routing" \
    new-routing-mark="wan3" passthrough="no";
```

Connexions entrantes

- **La répartition de charge fonctionne :**

9	mark routing	prerouting					local	!local	65.0 MiB	106 969
10	mark routing	prerouting					local	!local	82.6 MiB	103 069
11	mark routing	prerouting					local	!local	45.3 MiB	72 939

- **Mais l'accès distant au routeur (à sécuriser bien sûr) et les renvois de port ne fonctionnent pas toujours :**
  - Aléatoire en fonction de la source et de la destination
  - Le Per Connection Classifier change la route de retour

- **Solution :**
  - Marquer les connexions entrantes
  - Marquer les paquets sortants de ces connexions

Connexions entrantes

- **Marquer les connexions en fonction de l'interface entrante**
- **Les paquets réponses issus du routeur passent par la chaîne « output »**
- **Les paquets réponses provenant des renvois de port passent par la chaîne « prerouting »**
- **Les règles de marquages de paquets sortants doivent être placées avant celles de répartition de charge**

Connexions entrantes

- **Règles pour la première interface :**

```
/ip firewall mangle
add action="mark-connection" chain="prerouting" \
    connection-mark="no-mark" connection-state="new" \
    in-interface="pppoe-wan1" new-connection-mark="wan1" \
    passthrough="no";
add action="mark-routing" chain="prerouting" \
    connection-mark="wan1" in-interface="!pppoe-wan1" \
    new-routing-mark="wan1" passthrough="no";
add action="mark-routing" chain="output" connection-mark="wan1" \
    new-routing-mark="wan1" passthrough="no";
```

- **À répéter pour les deux autres interfaces...**

Sommaire

- **Questions ?**
- **Merci !**