

2 WAN · ROUTEROS 7

Failover & Load Balancing avec 2 WAN

Deux connexions Internet sur MikroTik : bascule automatique, partage de charge PCC, alertes et scripts prêts à coller

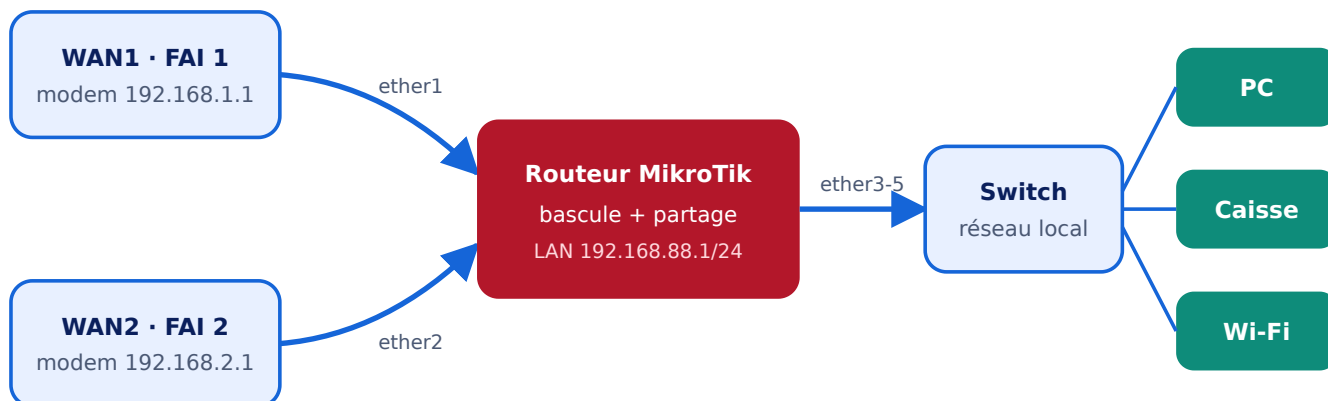
Professeur : Monsieur Stan · Tél. +228 91 53 84 61 · +228 96 18 64 01

Sommaire

1. Comprendre le failover et le load balancing
2. Le matériel et le plan d'adressage
3. Préparer le routeur
4. Failover simple : distance et check-gateway
5. Failover fiable : les routes récursives
6. Load balancing avec PCC
7. Connexions de débits différents
8. Forcer un appareil ou un service sur un WAN
9. Surveiller et être alerté
10. Tester et dépanner
11. Le script complet prêt à coller
12. Livrer au client
13. Exercices et test de connaissances

1 Comprendre le failover et le load balancing

Avec deux connexions Internet (par exemple fibre d'un fournisseur et 4G ou fibre d'un second fournisseur), un routeur MikroTik peut faire deux choses : basculer automatiquement sur la seconde connexion quand la première tombe (failover), et répartir le trafic sur les deux connexions quand elles marchent (load balancing). Les deux se combinent.



Si un fournisseur tombe, tout passe par l'autre. Quand les deux marchent, le trafic est réparti.

Plan type d'une installation 2 WAN

Pourquoi deux connexions ?

- Continuité : la caisse, le paiement Mobile Money et les appels ne s'arrêtent plus quand un fournisseur a une coupure.
- Débit : plusieurs utilisateurs profitent des deux connexions en même temps.
- Économie : une petite connexion de secours coûte moins cher qu'une journée de travail perdue.
- Indispensable pour : banques, cliniques, hôtels, cybercafés, hotspots, entreprises, écoles.

Les méthodes, de la plus simple à la plus complète

Méthode	Ce qu'elle fait	Niveau
Distance + check-gateway	Bascule si le modem ne répond plus	Débutant
Routes récursives	Bascule si Internet ne répond plus, même si le modem est allumé	Recommandé
ECMP	Répartition simple sur deux routes égales	Intermédiaire
PCC	Répartition maîtrisée par connexion + secours	Professionnel

Conseil

Une connexion d'un client (un téléchargement, un appel) passe toujours par UN seul WAN. Le load balancing répartit les connexions, il n'additionne pas le débit d'un seul téléchargement.

2 Le matériel et le plan d'adressage

N'importe quel MikroTik avec au moins 3 ports convient : hEX (RB750Gr3), hAP ac², RB4011 ou RB5009 pour les gros débits. Chaque modem arrive sur son propre port.

Élément	Port	Adresse
Modem fournisseur 1 (WAN1)	ether1	Routeur 192.168.1.2 · passerelle 192.168.1.1
Modem fournisseur 2 (WAN2)	ether2	Routeur 192.168.2.2 · passerelle 192.168.2.1
Réseau local (LAN)	ether3 à ether5	Routeur 192.168.88.1/24

Attention

Les deux modems ne doivent JAMAIS être dans le même réseau. Si les deux sont en 192.168.1.1, changez l'adresse LAN de l'un des modems (par exemple 192.168.2.1) dans sa page d'administration.

- Notez pour chaque fournisseur : type de connexion (IP fixe, DHCP ou PPPoE), débit réel, identifiants.
- Mesurez le débit de chaque connexion seule : il servira à répartir le trafic proportionnellement.
- Si possible, mettez les modems en mode bridge et laissez le MikroTik faire le routage.

3 Préparer le routeur

On part d'un routeur remis à zéro sans configuration par défaut (System → Reset Configuration → No Default Configuration). Connectez-vous avec Winbox par l'adresse MAC, puis collez ce script dans New Terminal.

```
/system identity set name="ROUTEUR-2WAN"
/user add name=stan group=full password="MotDePasseFort!"
/user disable admin
/interface bridge add name=bridge-lan
/interface bridge port
add bridge=bridge-lan interface=ether3
add bridge=bridge-lan interface=ether4
add bridge=bridge-lan interface=ether5
/interface list add name=WAN
/interface list add name=LAN
/interface list member
add list=WAN interface=ether1
add list=WAN interface=ether2
add list=LAN interface=bridge-lan
/ip address
add address=192.168.1.2/24 interface=ether1 comment="WAN1"
add address=192.168.2.2/24 interface=ether2 comment="WAN2"
add address=192.168.88.1/24 interface=bridge-lan comment="LAN"
/ip dns set servers=8.8.4.4,9.9.9.9 allow-remote-requests=yes
/ip pool add name=pool-lan ranges=192.168.88.10-192.168.88.250
/ip dhcp-server add name=dhcp-lan interface=bridge-lan address-pool=pool-lan lease-time=1d
/ip dhcp-server network add address=192.168.88.0/24 gateway=192.168.88.1 dns-server=192.168.88.1
/ip firewall nat
add chain=srcnat out-interface=ether1 action=masquerade comment="NAT WAN1"
add chain=srcnat out-interface=ether2 action=masquerade comment="NAT WAN2"
```

Conseil

Un NAT par WAN (out-interface) et non un seul NAT général : chaque connexion sort avec l'adresse du bon fournisseur.

Attention

Ajoutez aussi le pare-feu de base (bloquer les accès depuis la liste WAN). Le script « Pare-feu de base » est dans la plaquette de connaissance MikroTik du site.

4 Failover simple : distance et check-gateway

Deux routes par défaut : la plus petite distance gagne. check-gateway=ping envoie un ping à la passerelle toutes les 10 secondes ; si elle ne répond plus, la route est désactivée et la route de secours prend le relais.

```
/ip route
add dst-address=0.0.0.0/0 gateway=192.168.1.1 distance=1 check-gateway=ping comment="Principal WAN1"
add dst-address=0.0.0.0/0 gateway=192.168.2.1 distance=2 check-gateway=ping comment="Secours WAN2"
```

La limite de cette méthode

Le ping va seulement jusqu'au modem. Si la fibre est coupée chez le fournisseur mais que le modem reste allumé, le modem répond toujours et la bascule ne se fait pas. C'est le cas le plus fréquent en pratique : on utilise donc les routes récursives.

5 Failover fiable : les routes récursives

On fait vérifier une adresse sur Internet (8.8.8.8 pour WAN1, 1.1.1.1 pour WAN2) au lieu du modem. Chaque adresse de test est forcée à passer par son propre fournisseur. Si 8.8.8.8 ne répond plus par WAN1, c'est qu'Internet est réellement coupé sur WAN1, et la bascule se fait.

```
/ip route
# 1) Chaque adresse de test passe par son fournisseur
add dst-address=8.8.8.8/32 gateway=192.168.1.1 scope=10 comment="Test WAN1"
add dst-address=1.1.1.1/32 gateway=192.168.2.1 scope=10 comment="Test WAN2"
# 2) Interdire au test de passer par l'autre fournisseur
add dst-address=8.8.8.8/32 blackhole distance=20 comment="Test WAN1 jamais par WAN2"
add dst-address=1.1.1.1/32 blackhole distance=20 comment="Test WAN2 jamais par WAN1"
# 3) Routes par défaut récursives
add dst-address=0.0.0.0/0 gateway=8.8.8.8 target-scope=11 check-gateway=ping distance=1 comment="Principal WAN1"
add dst-address=0.0.0.0/0 gateway=1.1.1.1 target-scope=11 check-gateway=ping distance=2 comment="Secours WAN2"
```

Paramètre	Rôle
scope=10	La route de test est utilisable pour résoudre une autre route
target-scope=11	La route par défaut cherche sa passerelle (8.8.8.8) via la route de test
check-gateway=ping	Ping de 8.8.8.8 toutes les 10 s ; 2 échecs = route désactivée
distance	1 = principal, 2 = secours

Attention

N'utilisez pas 8.8.8.8 ou 1.1.1.1 comme serveur DNS du routeur : ces adresses ne passent que par un seul WAN. Prenez 8.8.4.4 et 9.9.9.9.

WAN en DHCP ou en PPPoE

Si un fournisseur donne l'adresse par DHCP, la passerelle peut changer. Le client DHCP met alors à jour la route de test automatiquement :

```
/ip dhcp-client add interface=ether1 add-default-route=no use-peer-dns=no script={
:if ($bound=1) do={
/ip route set [find comment="Test WAN1"] gateway="$gateway-address"
}
}
```

En PPPoE, la passerelle est simplement l'interface : remplacez gateway=192.168.1.1 par gateway=pppoe-out1 dans la route « Test WAN1 », et désactivez add-default-route sur le client PPPoE.

6 Load balancing avec PCC

PCC (Per Connection Classifier) répartit les nouvelles connexions entre les deux WAN selon un calcul sur les adresses. Une même connexion reste toujours sur le même WAN : les sites bancaires, WhatsApp et les jeux ne sont pas coupés.

Étape 1 : les tables de routage et les réseaux locaux

```
/routing table add name=to_WAN1 fib
/routing table add name=to_WAN2 fib
/ip firewall address-list
add list=RESEAUX_LOCAUX address=192.168.88.0/24
add list=RESEAUX_LOCAUX address=192.168.1.0/24
add list=RESEAUX_LOCAUX address=192.168.2.0/24
```

Étape 2 : le marquage (mangle)

```
/ip firewall mangle
# Le trafic vers les réseaux locaux n'est pas réparti
add chain=prerouting dst-address-list=RESEAUX_LOCAUX action=accept comment="Trafic local"
# Ce qui entre par un WAN repart par ce même WAN
add chain=prerouting in-interface=ether1 connection-mark=no-mark action=mark-connection new-connection-mark=WAN1_conn
add chain=prerouting in-interface=ether2 connection-mark=no-mark action=mark-connection new-connection-mark=WAN2_conn
# Répartition des nouvelles connexions du LAN : moitié / moitié
add chain=prerouting in-interface-list=LAN dst-address-type=!local connection-mark=no-mark per-connection-classifier=both-addresses:2/0 action=mark-connection new-connection-mark=WAN1_conn
add chain=prerouting in-interface-list=LAN dst-address-type=!local connection-mark=no-mark per-connection-classifier=both-addresses:2/1 action=mark-connection new-connection-mark=WAN2_conn
# Envoi de chaque connexion vers sa table
add chain=prerouting in-interface-list=LAN connection-mark=WAN1_conn action=mark-routing new-routing-mark=to_WAN1 passthrough=no
add chain=prerouting in-interface-list=LAN connection-mark=WAN2_conn action=mark-routing new-routing-mark=to_WAN2 passthrough=no
add chain=output connection-mark=WAN1_conn action=mark-routing new-routing-mark=to_WAN1 passthrough=no
add chain=output connection-mark=WAN2_conn action=mark-routing new-routing-mark=to_WAN2 passthrough=no
```

Étape 3 : les routes de chaque table, avec secours

```
/ip route
add dst-address=0.0.0.0/0 gateway=8.8.8.8@main target-scope=11 check-gateway=ping distance=1 routing-table=to_WAN1
add dst-address=0.0.0.0/0 gateway=1.1.1.1@main target-scope=11 check-gateway=ping distance=2 routing-table=to_WAN1
add dst-address=0.0.0.0/0 gateway=1.1.1.1@main target-scope=11 check-gateway=ping distance=1 routing-table=to_WAN2
add dst-address=0.0.0.0/0 gateway=8.8.8.8@main target-scope=11 check-gateway=ping distance=2 routing-table=to_WAN2
```

Chaque table a son WAN principal et l'autre WAN en secours : si WAN1 tombe, les connexions marquées to_WAN1 passent aussitôt par WAN2. Les routes de test du chapitre 5 doivent être en place (@main indique de chercher 8.8.8.8 dans la table principale).

Les variantes du classifieur

Classifieur	Effet	Conseil
src-address	Un PC reste toujours sur le même WAN	Le plus sûr pour les banques
both-addresses	Même PC + même site = même WAN	Bon équilibre (recommandé)
both-addresses-and-ports	Répartition la plus fine	Peut gêner certains sites sécurisés

Attention

Le FastTrack contourne le marquage. Désactivez-le avec : `/ip firewall filter disable [find action=fasttrack-connection]`

7 Connexions de débits différents

Si WAN1 fait 100 Mb/s et WAN2 50 Mb/s, on donne deux parts à WAN1 et une part à WAN2 en divisant en 3 au lieu de 2 :

```
/ip firewall mangle
remove [find per-connection-classifier~"both-addresses:2/"]
add chain=prerouting in-interface-list=LAN dst-address-type=!local connection-mark=no-mark per-connection-classifier=both-addresses:3/0 action=mark-connection new-connection-mark=WAN1_conn place-before=[find chain=prerouting new-routing-mark=to_WAN1]
add chain=prerouting in-interface-list=LAN dst-address-type=!local connection-mark=no-mark per-connection-classifier=both-addresses:3/1 action=mark-connection new-connection-mark=WAN1_conn place-before=[find chain=prerouting new-routing-mark=to_WAN1]
add chain=prerouting in-interface-list=LAN dst-address-type=!local connection-mark=no-mark per-connection-classifier=both-addresses:3/2 action=mark-connection new-connection-mark=WAN2_conn place-before=[find chain=prerouting new-routing-mark=to_WAN1]
```

Débits WAN1 / WAN2	Diviseur	Parts WAN1	Parts WAN2
Égaux	2	2/0	2/1
2 pour 1	3	3/0, 3/1	3/2
3 pour 1	4	4/0, 4/1, 4/2	4/3
3 pour 2	5	5/0, 5/1, 5/2	5/3, 5/4

Alternative rapide : ECMP

RouterOS 7 répartit aussi automatiquement le trafic entre deux routes de même distance (ECMP). C'est simple, mais moins maîtrisable que PCC :

```
/ip route
add dst-address=0.0.0.0/0 gateway=192.168.1.1 check-gateway=ping distance=1
add dst-address=0.0.0.0/0 gateway=192.168.2.1 check-gateway=ping distance=1
```

8 Forcer un appareil ou un service sur un WAN

Exemples : la caisse et le terminal de paiement toujours sur la fibre, les caméras sur la connexion secondaire, ou un serveur accessible depuis Internet par une IP fixe.

```
/ip firewall address-list
add list=FORCE_WAN1 address=192.168.88.20 comment="Caisse"
add list=FORCE_WAN2 address=192.168.88.50-192.168.88.60 comment="Cameras"
/ip firewall mangle
add chain=prerouting src-address-list=FORCE_WAN1 connection-mark=no-mark action=mark-connection new-connection-mark=WAN1_conn place-before=0
add chain=prerouting src-address-list=FORCE_WAN2 connection-mark=no-mark action=mark-connection new-connection-mark=WAN2_conn place-before=0
```

Ces règles placées en tête marquent la connexion avant le PCC ; la table de secours continue de fonctionner si le WAN choisi tombe.

Conseil

Pour le Hotspot : mettez les clients du hotspot sur la connexion la moins chère avec une liste FORCE_WAN2 sur le réseau 172.16.0.0/22.

9 Surveiller et être alerté

Netwatch surveille les adresses de test et écrit dans le journal à chaque panne ou rétablissement. Vous pouvez aussi recevoir un e-mail.

```
/tool netwatch
add host=8.8.8.8 type=icmp interval=10s comment="WAN1" down-script=":log warning \"WAN1 EN PANNE\"" up-script=":log info \"WAN1 RETABLI\""
add host=1.1.1.1 type=icmp interval=10s comment="WAN2" down-script=":log warning \"WAN2 EN PANNE\"" up-script=":log info \"WAN2 RETABLI\""
```

```
# Optionnel : alerte par e-mail (compte Gmail avec mot de passe d'application)
/tool e-mail set server=smtp.gmail.com port=587 tls=starttls from="votre.adresse@gmail.com" user="votre.adresse@gmail.com" password="motdepasse-application"
/tool netwatch set [find comment="WAN1"] down-script="/tool e-mail send to=\"votre.adresse@gmail.com\" subject=\"WAN1 en panne\" body=\"Bascule sur WAN2\""
```

- IP → Routes : la route active est marquée A ; une route en panne apparaît en bleu et sans A.
- Tools → Netwatch : état up ou down de chaque connexion.
- Interfaces → onglet Traffic : vérifiez que ether1 et ether2 transportent tous les deux du trafic.
- Log : historique des pannes et rétablissements.

10 Tester et dépanner

Les tests à faire avant de livrer

1. Débranchez le câble d'éther1 : Internet doit continuer après 10 à 20 secondes.
2. Rebranchez, puis débranchez la fibre côté modem 1 (le modem reste allumé) : la bascule doit aussi se faire.
3. Lancez plusieurs téléchargements depuis plusieurs PC : les deux interfaces WAN doivent avoir du trafic.
4. Ouvrez votre banque en ligne et WhatsApp Web : ils doivent rester connectés.

```
/ip route print where dst-address=0.0.0.0/0
/tool traceroute 8.8.8.8
/tool traceroute 1.1.1.1
/ip firewall connection print count-only where connection-mark=WAN1_conn
/ip firewall connection print count-only where connection-mark=WAN2_conn
```

Les pannes fréquentes

Problème	Cause probable	Solution
Pas de bascule quand la fibre est coupée	Failover simple sur la passerelle	Utiliser les routes récursives
Tout passe par un seul WAN	FastTrack actif ou règles mangle mal placées	Désactiver FastTrack, vérifier l'ordre
Site bancaire qui déconnecte	Classifieur avec les ports	Passer à both-addresses ou src-address
Le speedtest ne montre qu'un WAN	Normal : une connexion = un WAN	Tester avec plusieurs appareils
Impossible d'ouvrir la page d'un modem	Trafic local réparti	Ajouter son réseau à RESEAUX_LOCAUX
Les deux routes tombent	Adresses de test bloquées ou DNS	Changer d'adresse de test (9.9.9.9, 208.67.222.222)

11 Le script complet prêt à coller

Le script ci-dessous rassemble tout le cours : préparation, NAT, PCC moitié / moitié, routes récursives avec secours croisé et alertes. Adaptez les adresses des modems, puis collez-le dans New Terminal sur un routeur remis à zéro.

```

# ===== GLOB.IP.NET : 2 WAN, PARTAGE PCC + BASCULE AUTOMATIQUE (RouterOS 7) =====
# Adaptez : adresses des modems, ports, mots de passe. Faites une sauvegarde avant.
/system identity set name="ROUTEUR-2WAN"
/interface bridge add name=bridge-lan
/interface bridge port
add bridge=bridge-lan interface=ether3
add bridge=bridge-lan interface=ether4
add bridge=bridge-lan interface=ether5
/interface list add name=WAN
/interface list add name=LAN
/interface list member
add list=WAN interface=ether1
add list=WAN interface=ether2
add list=LAN interface=bridge-lan
/ip address
add address=192.168.1.2/24 interface=ether1 comment="WAN1"
add address=192.168.2.2/24 interface=ether2 comment="WAN2"
add address=192.168.88.1/24 interface=bridge-lan comment="LAN"
/ip dns set servers=8.8.4.4,9.9.9.9 allow-remote-requests=yes
/ip pool add name=pool-lan ranges=192.168.88.10-192.168.88.250
/ip dhcp-server add name=dhcp-lan interface=bridge-lan address-pool=pool-lan lease-time=1d
/ip dhcp-server network add address=192.168.88.0/24 gateway=192.168.88.1 dns-server=192.168.88.1
/ip firewall nat
add chain=srcnat out-interface=ether1 action=masquerade comment="NAT WAN1"
add chain=srcnat out-interface=ether2 action=masquerade comment="NAT WAN2"
# --- Tables de routage ---
/routing table add name=to_WAN1 fib
/routing table add name=to_WAN2 fib
# --- Réseaux locaux à ne pas répartir ---
/ip firewall address-list
add list=RESEAUX_LOCAUX address=192.168.88.0/24
add list=RESEAUX_LOCAUX address=192.168.1.0/24
add list=RESEAUX_LOCAUX address=192.168.2.0/24
# --- Marquage PCC ---
/ip firewall mangle
add chain=prerouting dst-address-list=RESEAUX_LOCAUX action=accept comment="Trafic local"
add chain=prerouting in-interface=ether1 connection-mark=no-mark action=mark-connection new-connection-mark=WAN1_conn
add chain=prerouting in-interface=ether2 connection-mark=no-mark action=mark-connection new-connection-mark=WAN2_conn
add chain=prerouting in-interface-list=LAN dst-address-type=!local connection-mark=no-mark per-connection-classifier=both-addresses:2/0 action=mark-connection new-connection-mark=WAN1_conn
add chain=prerouting in-interface-list=LAN dst-address-type=!local connection-mark=no-mark per-connection-classifier=both-addresses:2/1 action=mark-connection new-connection-mark=WAN2_conn
add chain=prerouting in-interface-list=LAN connection-mark=WAN1_conn action=mark-routing new-routing-mark=to_WAN1 passthrough=no
add chain=prerouting in-interface-list=LAN connection-mark=WAN2_conn action=mark-routing new-routing-mark=to_WAN2 passthrough=no
add chain=output connection-mark=WAN1_conn action=mark-routing new-routing-mark=to_WAN1 passthrough=no
add chain=output connection-mark=WAN2_conn action=mark-routing new-routing-mark=to_WAN2 passthrough=no
# --- Routes : test récursif dans la table principale ---
/ip route
add dst-address=8.8.8.8/32 gateway=192.168.1.1 scope=10 comment="Test WAN1"
add dst-address=1.1.1.1/32 gateway=192.168.2.1 scope=10 comment="Test WAN2"
add dst-address=8.8.8.8/32 blackhole distance=20 comment="Test WAN1 jamais par WAN2"
add dst-address=1.1.1.1/32 blackhole distance=20 comment="Test WAN2 jamais par WAN1"
add dst-address=0.0.0.0/0 gateway=8.8.8.8 target-scope=11 check-gateway=ping distance=1 comment="Principal WAN1"
add dst-address=0.0.0.0/0 gateway=1.1.1.1 target-scope=11 check-gateway=ping distance=2 comment="Secours WAN2"
# --- Routes des tables PCC, chacune avec secours sur l'autre WAN ---
add dst-address=0.0.0.0/0 gateway=8.8.8.8@main target-scope=11 check-gateway=ping distance=1 routing-table=to_WAN1
add dst-address=0.0.0.0/0 gateway=1.1.1.1@main target-scope=11 check-gateway=ping distance=2 routing-table=to_WAN1

```

```
add dst-address=0.0.0.0/0 gateway=1.1.1.1@main target-scope=11 check-gateway=ping distance=1 routing-table=to_WAN2
add dst-address=0.0.0.0/0 gateway=8.8.8.8@main target-scope=11 check-gateway=ping distance=2 routing-table=to_WAN2
# --- Le FastTrack contourne le marquage : on le désactive ---
/ip firewall filter disable [find action=fasttrack-connection]
# --- Alerte dans le journal quand un WAN tombe ---
/tool netwatch
add host=8.8.8.8 type=icmp interval=10s comment="WAN1" down-script=":log warning \"WAN1 EN PANNE\"" up-script=":log info \"WAN1 RETABLI\""
add host=1.1.1.1 type=icmp interval=10s comment="WAN2" down-script=":log warning \"WAN2 EN PANNE\"" up-script=":log info \"WAN2 RETABLI\""
```

Conseil

Faites ensuite File → Backup et gardez une copie du fichier .backup et de /export sur votre PC.

12 Livrer au client

- Étiquetez les câbles et les modems : WAN1, WAN2.
- Notez dans un document les identifiants des fournisseurs, l'adresse du routeur et votre compte administrateur.
- Montrez au client le voyant de chaque connexion et expliquez ce qui se passe en cas de panne.
- Proposez une visite de maintenance et la mise à jour de RouterOS tous les 3 à 6 mois.
- Gardez une sauvegarde de chaque client, datée et nommée.

Conseil

Besoin d'une installation double connexion clé en main ? GLOB.IP.NET installe et configure : +228 91 53 84 61.

13 Exercices et test

Exercices pratiques

1. Avec deux modems (ou un modem et un partage de connexion 4G), configurez les routes récursives du chapitre 5, puis débranchez la fibre du modem 1 en laissant le modem allumé : notez combien de secondes il faut pour que la bascule se fasse.
2. Mettez en place le PCC 2/1 pour deux connexions de 20 et 10 Mb/s, forcez la caisse (192.168.88.20) sur WAN1, puis vérifiez dans Interfaces que les deux WAN portent du trafic.

Test de connaissances

1. **Le modem du fournisseur 1 reste allumé mais la fibre est coupée. Quelle méthode détecte la panne ?**
a) Distance + check-gateway sur 192.168.1.1 · b) Routes récursives vers 8.8.8.8 · c) Un seul NAT masquerade · d) Le serveur DHCP
2. **Entre deux routes par défaut, laquelle est utilisée ?**
a) Celle avec la plus grande distance · b) Celle avec la plus petite distance · c) La plus récente · d) Les deux, toujours
3. **Que fait PCC ?**
a) Additionne le débit d'un seul téléchargement · b) Répartit les nouvelles connexions entre les WAN · c) Remplace le NAT · d) Bloque les sites
4. **WAN1 fait 100 Mb/s et WAN2 50 Mb/s. Quel réglage PCC ?**
a) 2/0 pour WAN1, 2/1 pour WAN2 · b) 3/0 et 3/1 pour WAN1, 3/2 pour WAN2 · c) 4/0 pour WAN1, le reste pour WAN2 · d) 1/0 pour les deux
5. **Pourquoi désactiver le FastTrack avec le PCC ?**
a) Il ralentit le routeur · b) Il contourne le marquage mangle · c) Il bloque le DHCP · d) Il désactive le NAT

Corrigé

1. b) Routes récursives vers 8.8.8.8 : Le ping vers le modem répond toujours ; seul un test vers Internet (route récursive) détecte la coupure.
2. b) Celle avec la plus petite distance : La plus petite distance gagne ; la seconde sert de secours.
3. b) Répartit les nouvelles connexions entre les WAN : PCC répartit les connexions ; une connexion reste sur un seul WAN.
4. b) 3/0 et 3/1 pour WAN1, 3/2 pour WAN2 : Diviseur 3 : deux parts pour WAN1, une part pour WAN2.
5. b) Il contourne le marquage mangle : Les paquets accélérés par FastTrack ne passent plus par les règles mangle.