Managing QoS, Link Aggregation and redundancy with failover with Mikrotik

MUM Yaoundé – 26 janvier 2018

By Thierry KOUTANG
Senior Engineer / C.E.O INFOGENIE Technologies – Cameroun

MikroTik

A propos de moi

Thierry KOUTANG

- Ingénieur polytechnicien de Yaoundé
- Editeur & Infographe
- Développeur de plusieurs logiciels dont MaintaSoft, GestScol®, CFAPaye®, Caisse®, Callshop, Net-Manager, …
- Administrateur réseau (toutes les couches OSI)
- Expert VoIP, Bases de données, Linux

A propos de moi (2)

- Founder INFOGENIE Technologies
- Utilisateur de Mikrotik RouterOS depuis 1999
- Certifié Mikrotik MTCNA, MTCRE, MTCWE, IPV6
- 1er Trainer Mikrotik francophone
- Participation à près de 10 MUMs (Varsaw, Krakow, Wroclaw, Zagreb, Venise, Budapest, Milan, Prague, ...

A propos d'INFOGENIE

- ENTREPRISE CAMEROUNAISE DE SERVICES ET D'INGENIERIE INFORMATIQUE ET TELECOMS
- INTERNET SERVICE PROVIDER (**I.S.P/ F.A.I**)
- IP TELEPHONY SERVICES PROVIDER (**ITSP**)
- MEMBRE FONDATEUR DU POINT D'ECHANGE INTERNET DU CAMEROUN (**CAMIX**)
- FOURNISSEUR D'EQUIPEMENTS TELECOMS AUX OPERATEURS
- BUREAU D'ENREGISTREMENT DU .CM (**Registrar agréé ANTIC**)

A propos d'INFOGENIE (2)

- PARTENAIRE ET DISTRIBUTEUR AGREE **MIKROTIK**
- PREMIER CENTRE DE CERTIFICATION **MIKROTIK** EN Français AU MONDE
- EDITEUR DE LOGICIELS DE REFERENCE (**GestScol**, **CFAPaye**, ……)
- FOURNISSEUR DE **SOLUTIONS TECHNOLOGIQUES** (Entreprises, Administrations, Organisations et Particuliers)
- PRESENT DEPUIS **PLUS DE 15 ANS** SUR LE MARCHE

A propos d'INFOGENIE (3)

NOS SOLUTIONS CONCERNENT PLUS PRECISEMENT :

- Accès & Services Internet
- Matériels & Solutions Réseaux et Télécoms
- Communications Unifiées
- Vidéosurveillance & Télésurveillance
- Ingénierie Informatique (Intégration ERP, …)
- Biométrie et Contrôle d'accès
- GPS Tracking
- Formations & Certifications Mikrotik

Solutions disponibles en démonstration ici au MuM Yaoundé, ainsi que certains produits présentés par Normunds Rustanovics.

Problématique

Comment garantir un fonctionnement performant d'Internet avec un maximum de disponibilité dans un environnement complexe, qui prend en compte tant le comportement des utilisateurs que les difficultés avec les F.A.I

Constats

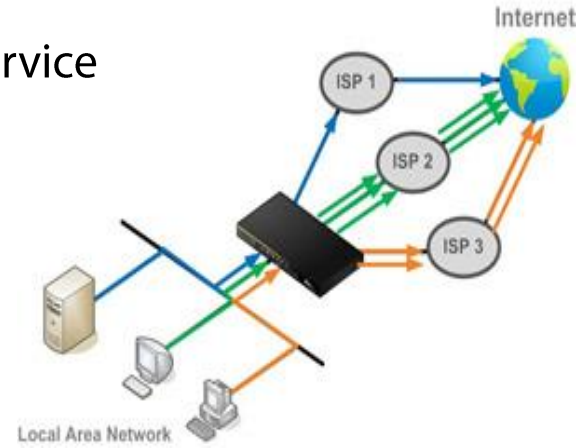
- Les besoins Internet des utilisateurs augmentent sans cesse
- L'accès se généralise, autrefois seuls quelques uns étaient connectés, maintenant c'est tout le monde
- Le développement du WiFi et des terminaux mobiles accentuent la pression sur la capacité
- Internet coûte cher, les budgets ne sont pas infinis, les contenus ne sont pas locaux
- Engorgement, plaintes des utilisateurs, instabilité des débits
- Comme on en dépend de plus en plus, on recourt à plusieurs liaisons (principale, backup, backup du backup, …)
- …. mais sans toujours avoir une bonne solution, ni d'automatisation dans la gestion de ce processus

Et pourtant ..

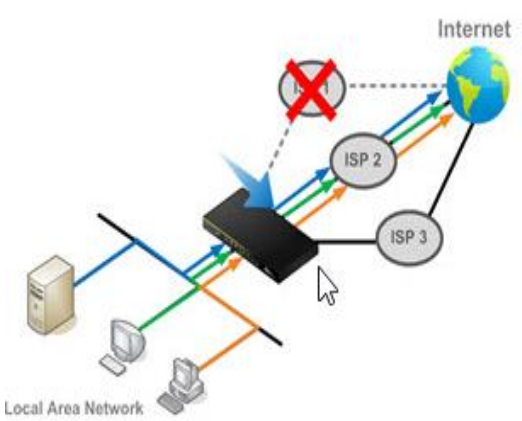
Tous ces problèmes peuvent être résolus avec un seul équipement!!!

Quality of Service

Backup



Link aggregation



Failover

Comprendre la QoS

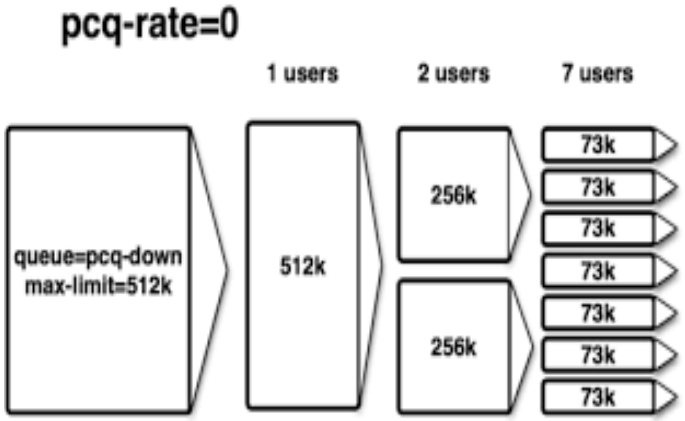
- La qualité de service n'est pas seulement limiter le débit, mais c'est surtout assurer la fluidité du trafic
- Certains trafics sont sensibles à la latence ou aux pertes de paquets (VoIP, vidéo interactive)
- D'autres sont utiles à la gestion du trafic et leur limitation agressive peut détériorer l'expérience utilisateur (DNS, ICMP)
- Pour d'autres trafics cela n'a pas une grande incidence (SMTP, Téléchargement HTTP/HTTPS, Peer to Peer)
- Dans RouterOS la QoS se fait à l'aide des « queues » (files d'attente)

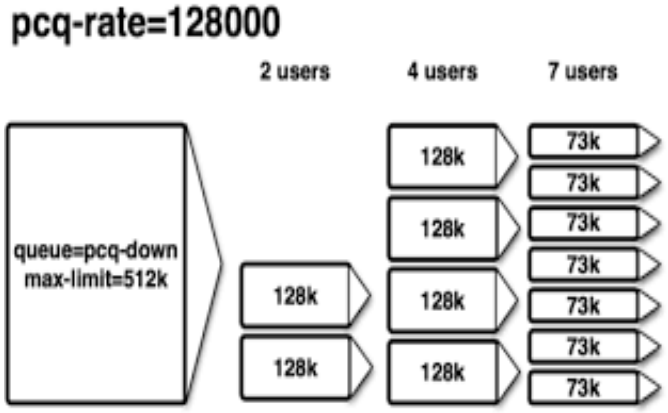
Comprendre la QoS (2)

- Les « queues » ont plusieurs paramètres parmi lesquels certains sont essentiels :
  - CIR (limit at)
  - MIR (max limit)
  - la Priorité
  - le type (algorithme de gestion), …
- Les queues ne s'appliquent qu'au trafic qui sort du routeur
- Vous n'avez aucun contrôle sur le trafic qui arrive à votre routeur, vous ne pouvez donc pas le limiter (surtout UDP)
- Le contrôle du débit de l'utilisateur se fait par conséquent à partir de l'interface du LAN pour son trafic RX et du WAN pour son trafic TX

Queues simples & Avancées

- Les queues simples permettent de limiter facilement le trafic vers une ou plusieurs adresses IP
- Les queues hiérarchiques permettent de gérer le trafic vers une ou plusieurs adresses IP avec d'autres algorithmes ou critères de répartition avancés
- PCQ (Per connection queue) est un type de queues avancées
- PCQ permet d'assigner un débit à un bloc d'adresse, en assurant une répartition grâce à des critères de classification qui peuvent garantir le débit montant ou descendant équitablement entre les utilisateurs





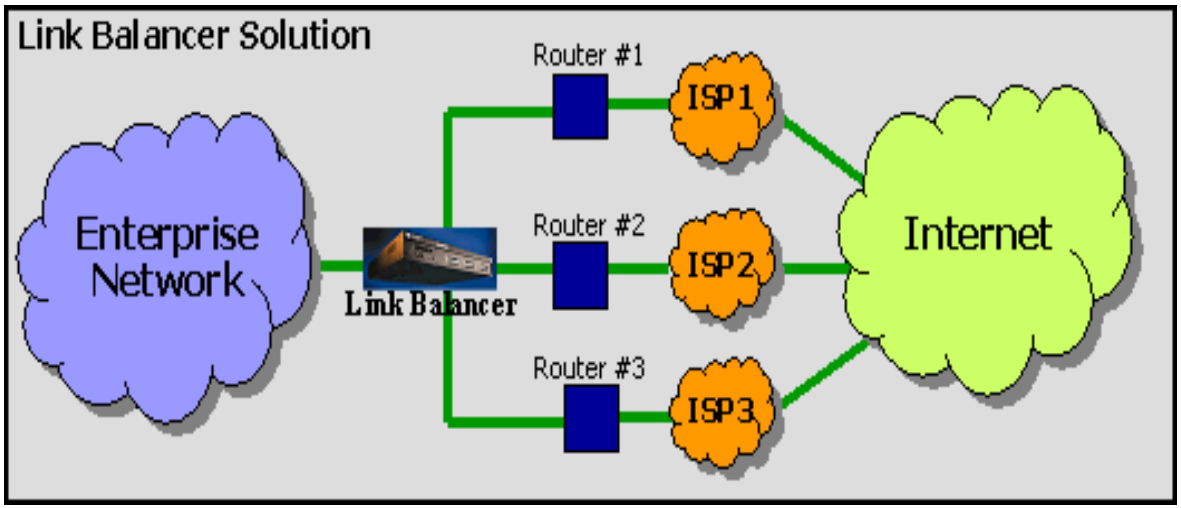
Implémentation de la QoS

- Commencer par implémenter des queues simples, les tester et monitorer (torch)
- Puis avancer vers les queues HTB notamment PCQ. La classification par adresse source pour le upload et par adresse de destination pour le download permet de garantir un équilibrage du débit entre les utilisateurs en upload comme en download, avec possibilités de limiter tout un groupe d'utilisateurs.
- Il est possible de classer les utilisateurs par débit : entre HAUT DEBIT, MOYEN DEBIT, BAS DEBIT, AUTRES
- Il est également possible combiner cette méthode avec le marquage des paquets pour donner la priorité aux petits flux par rapport au téléchargement lourds. Cette technique permet que les requêtes ICMP et DNS ne soient pas trop affectées en cas de congestion.

Les liaisons Backup

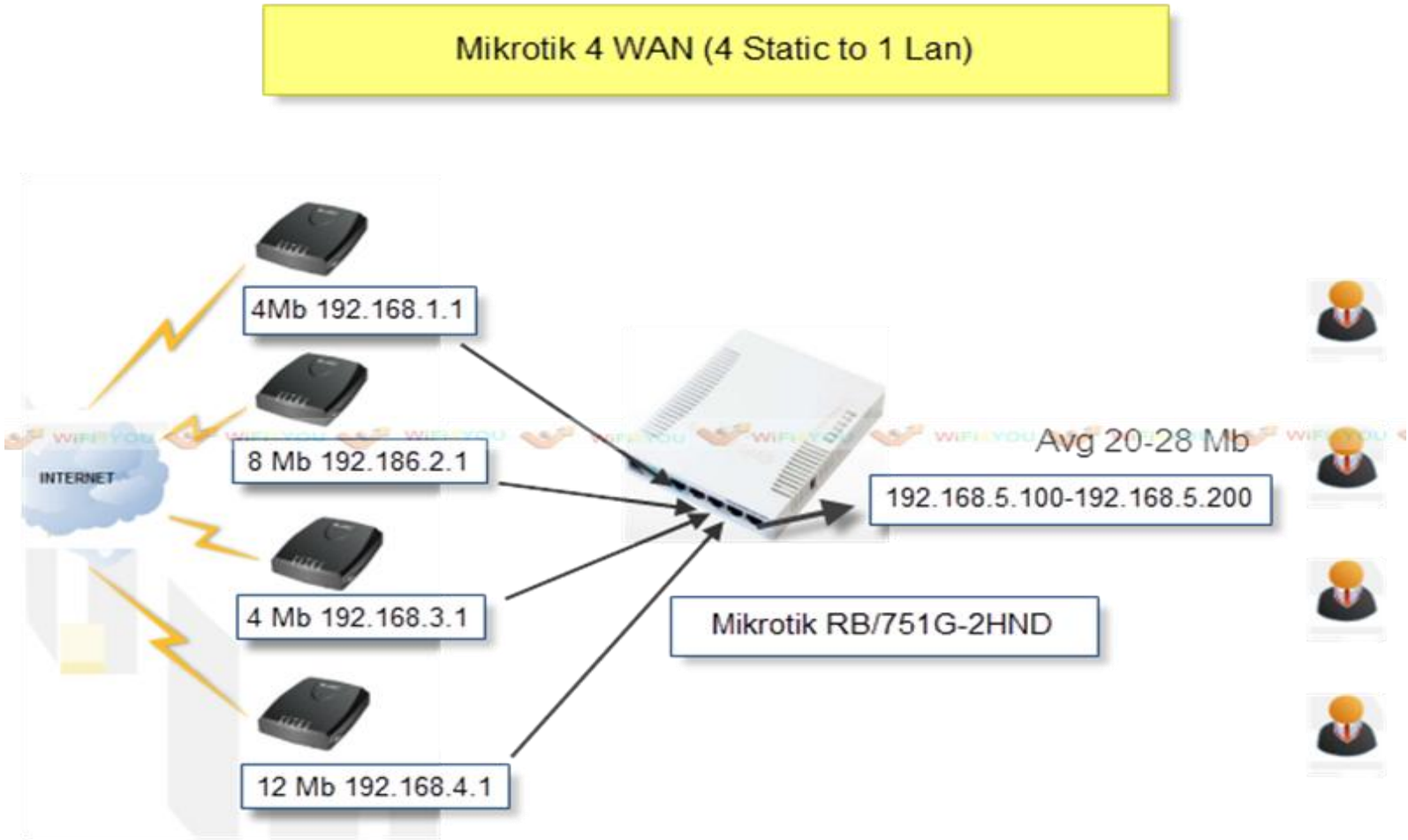
- Même si nous avons gérer la QoS, nous n'avons pas encore maximisé la continuité et la disponibilité de l'internet, d'où le recours aux liaisons backup.
- Certains font un basculement manuel (quand le lien principal est down, on appelle l'IT qui débranche à gauche pour brancher à droite) ou encore on change les paramètres IP. Ce n'est pas efficace.
- Certains payent une ou plusieurs connexions backup permanentes qu'ils n'utilisent presque jamais. Ce n'est pas économique
- Et pourtant il est possible d'agréger plusieurs liens WAN pour augmenter la capacité utilisée et augmenter sa sécurité, d'où l'**AGREGATION DE LIENS WAN**

Les liaisons Backup



- La majorité des Routerboard Mikrotik ont à partir de 3 interfaces Ethernet jusqu'à plusieurs interfaces SFP+.
- Chaque interface peut être connectée à un FAI différent avec des configurations différentes
- On peut même en connecter plus sur une même interface physique avec les VLAN …

Multiples liaisons WAN



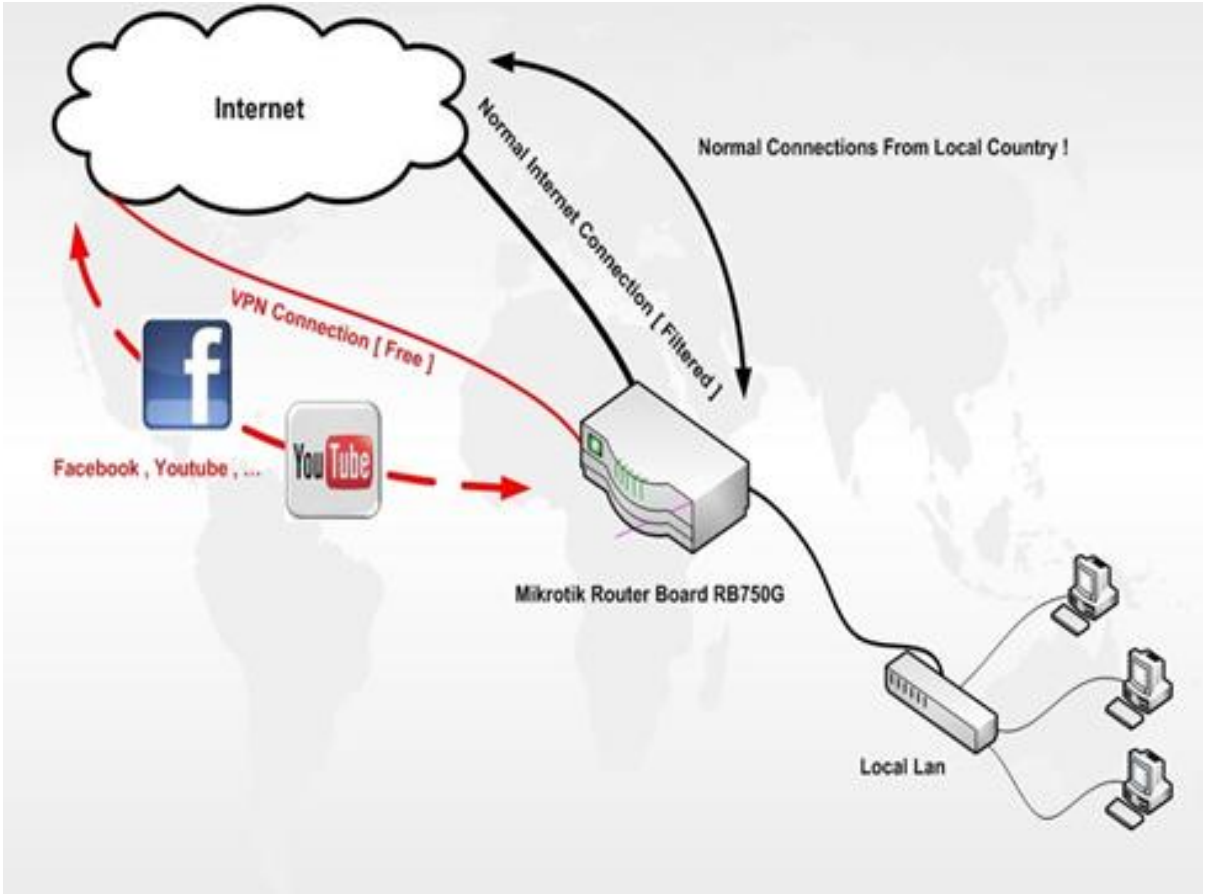
ECMP (Equal Cost Multi-Pathing)

- Un moyen simple d'utiliser l'agrégation des liens est ECMP
- L'ECMP (Equal-Cost Multi-Path) est un mécanisme d'acheminement des paquets le long de trajets multiples de coût égal dans le but d'obtenir un partage de charge de liaison presque équitable
- En pratique, il suffit pour une route d'avoir plusieurs passerelles de même poids, et le trafic se répartira sur les dites passerelles
- Il est possible de répéter une passerelle pour augmenter le volume de trafic à acheminer vers un FAI.

Policy Routing

- Un moyen un peu plus avancé d'utiliser l'agrégation de lien est de faire du « Policy Routing »
- Vous routez une partie du trafic sur le lien 1, et une autre partie sur le lien 2.
- Vous pouvez router les utilisateurs critiques sur le lien le plus stable et les terminaux mobiles et les autres utilisateurs sur le lien qui est moins stable
- Ou encore envoyer un type de trafic tels que Youtube ou Facebook sur un lien non filtré et le reste sur un lien filtré
- Vous pouvez marquer le trafic par différents critères et l'orienter vers des tables de routage différentes. Chaque table de routage peut avoir sa route par défaut (son FAI) et éventuellement ses propres routes statiques

Policy Routing (2)



- Ayant amélioré la qualité et exploité plusieurs liens, s'il y a une panne, le service ou certains utilisateurs seront toujours affectés. D'où le besoin de **redondance/ failover**

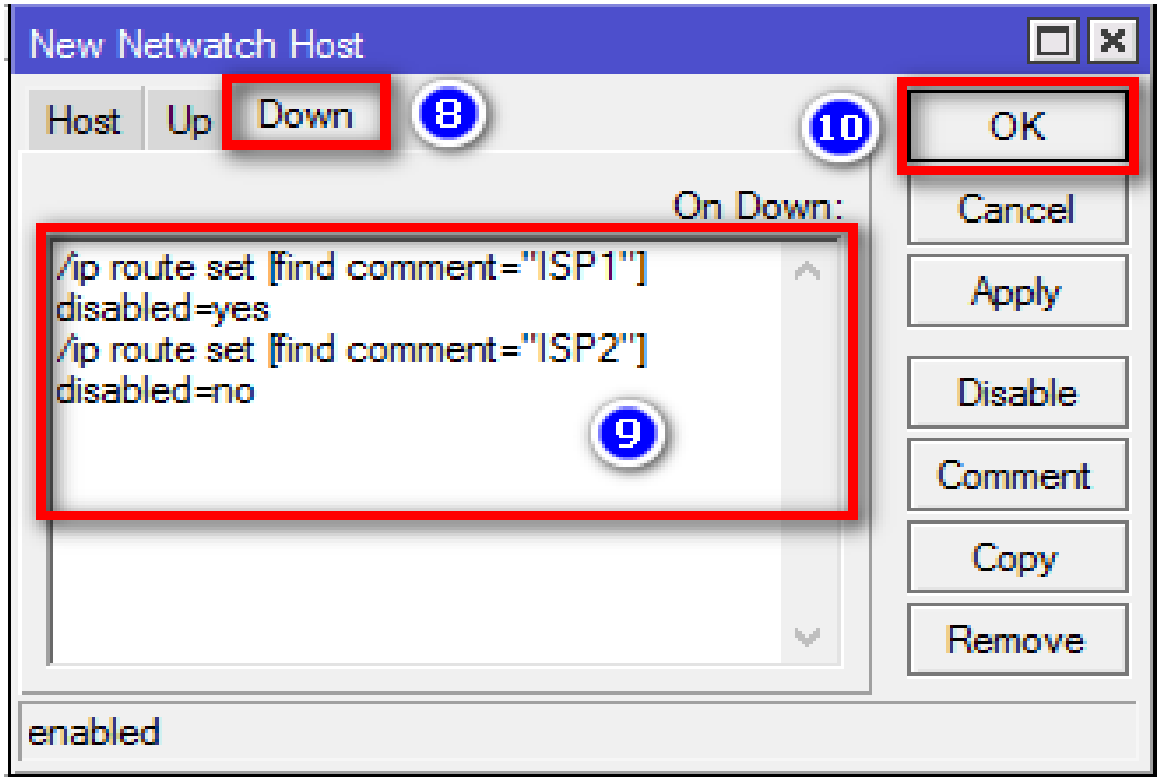
Failover

- Un moyen de mettre en œuvre le Fail Over est d'utiliser le poids des routes.
- On met la route principale avec une métrique faible et la route backup avec une métrique élevée. On rajoute la possibilité de pinguer la passerelle ou de vérifier la présence de son adresse Mac dans la table ARP
- Seulement, dans bien des cas ce , la passerelle de l'équipement de votre FAI passe, mais vous n'avez pas Internet. Faire un ping sur la passerelle, ou même avoir votre compte PPPoE enregistré ne vous avance pas beaucoup

Failover avec Netwatch

- Netwatch est une facilité Mikrotik qui vous permet de contrôler l'accessibilité à un hôte et d'exécuter des actions.
- Vous pouvez activer ou désactiver une route en fonction du PING vers l'hôte spécifié qui n'est pas dans votre réseau
- Ca marche bien. Seul problème, quand vous pinguer trop un hôte, il peut vous blacklister et ne plus répondre
- Autre problème, si vous le faites toutes les 10 minutes, vous aurez quand même en moyenne 5 minutes où vous n'aurez pas la connexion avant de basculer sur les routes fonctionnelles

Failover avec Netwatch (2)



Et vint les routes récursives …

- Pour améliorer la gestion du failover, nous pouvons faire appel aux routes récursives, supportées depuis quelques temps par Mikrotik.
- Les routes récursives sont traditionnellement associées au protocole BGP, en ce que la passerelle vers un réseau n'est pas forcément une interface physiquement connectée au routeur.
- Les paramètres SCOPE et TARGET SCOPE permettent de déterminer les routes candidates à l'examen pour la décision de routage et de fixer des passerelles non directement accessible via une interface « route récursive ».

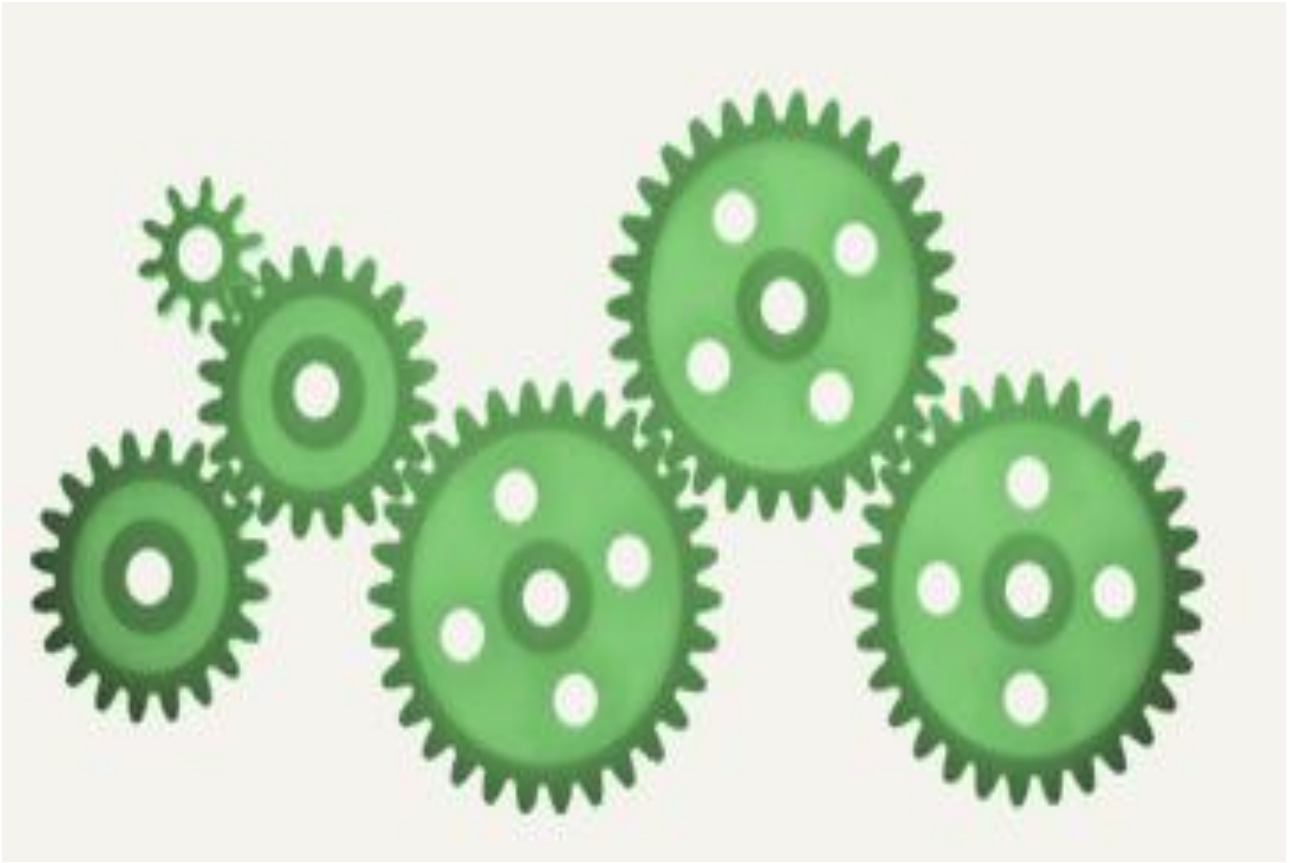
Routes récursives (2)

- Les routes récursives doivent être dans la table main, les passerelles peuvent servir dans les autres tables de routage
- Elles permettent de détecter un problème au-delà de la connexion directe avec le FAI
- En combinant avec le paramètre check-gateway, l'accessibilité de la route est vérifiée toutes les 10s et la route passe inactive dès qu'il y a 2 délais d'attente
- On peut en déduire un délai moyen de 10s avant basculement, pas sensible pour l'utilisateur

Routes récursives (2)

- Pour éviter le blacklisting, il est possible d'utiliser des adresses de serveurs DNS pour les tests (beaucoup sont en anycast)
- Ne pas utiliser les DNS de google (8.8.8.8, 8.8.4.4), trop populaires, vos utilisateurs pourraient en être affectés
- NATER le trafic qui peut changer d'opérateur à tout moment

CAS PRATIQUE



ATTENTION

Le banc d'essai ayant été réinitialisé après le MUM, certaines copies d'écran pourraient ne pas correspondre. Il avait été prévu de le remonter afin d'ajuster cette présentation. Les nombreuses contraintes n'ont pas permis de le faire, ce qui a retardé la présente publication. Prenant en compte la forte demande, il a été arrêté de publier la présentation telle qu'elle avant correction ultérieure éventuelle.

En cas de souci, contacter INFOGENIE Technologies à support@infogenie.cm

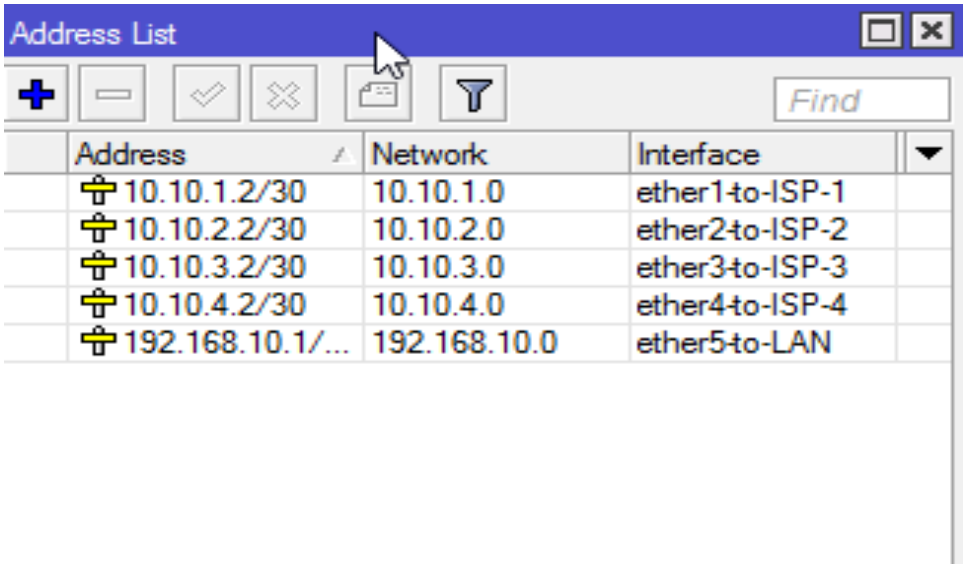
CAS PRATIQUE

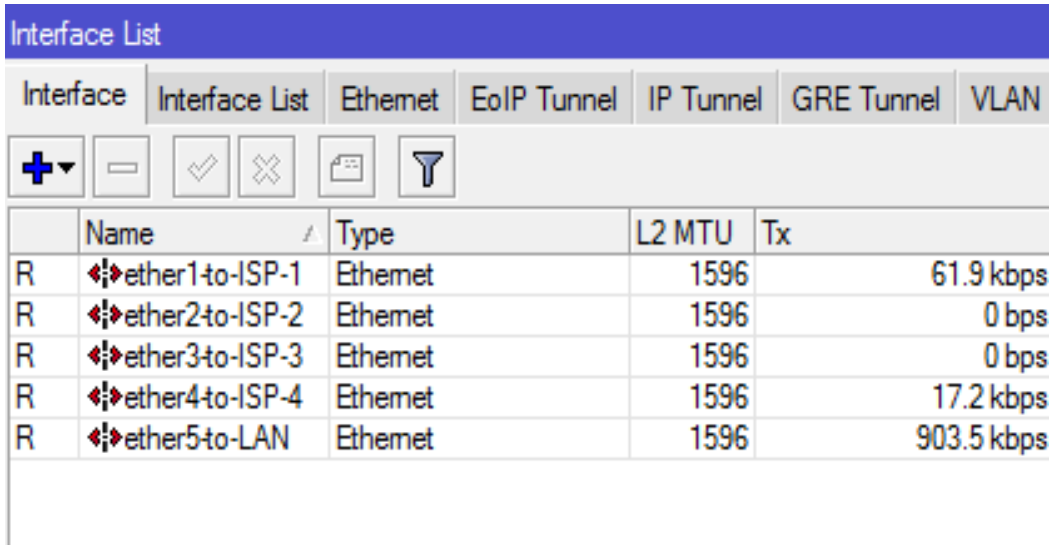
Client disposant de 4 connexions INTERNET :

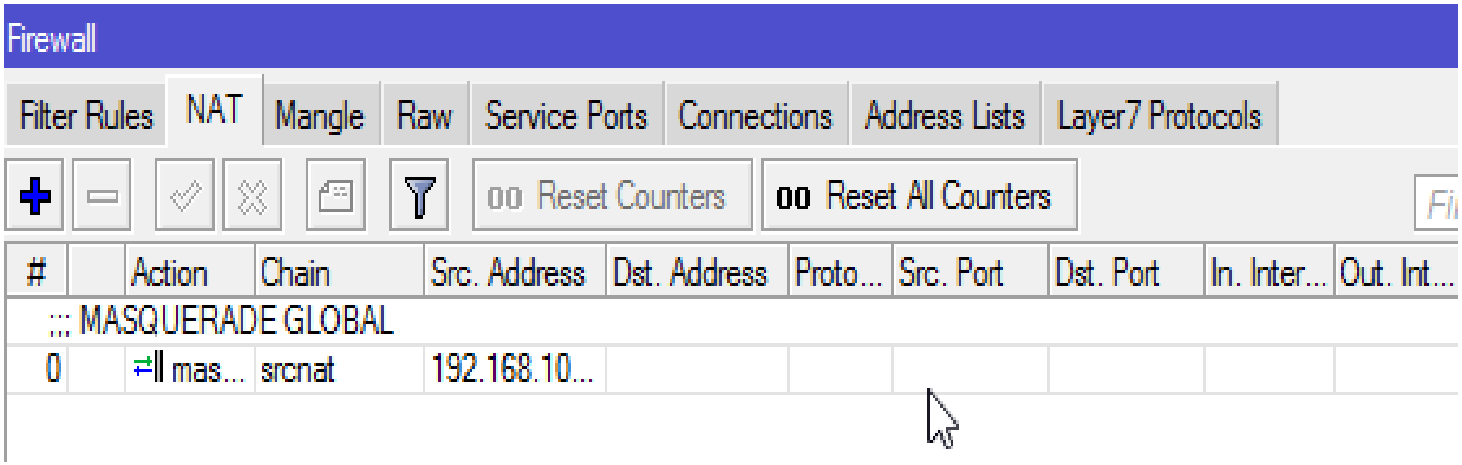
- 1 connexion dédiée 04Mbs chez INFOGENIE
- 1 connexion dédiée 02Mbs chez MTN
- 1 connexion partagée chez CAMTEL
- 1 connexion partagée mobile 3/4G

- Il fait du NAT sur ces adresses de réseau local (masquerade pour que ce soit automatique)

CAS PRATIQUE (2)







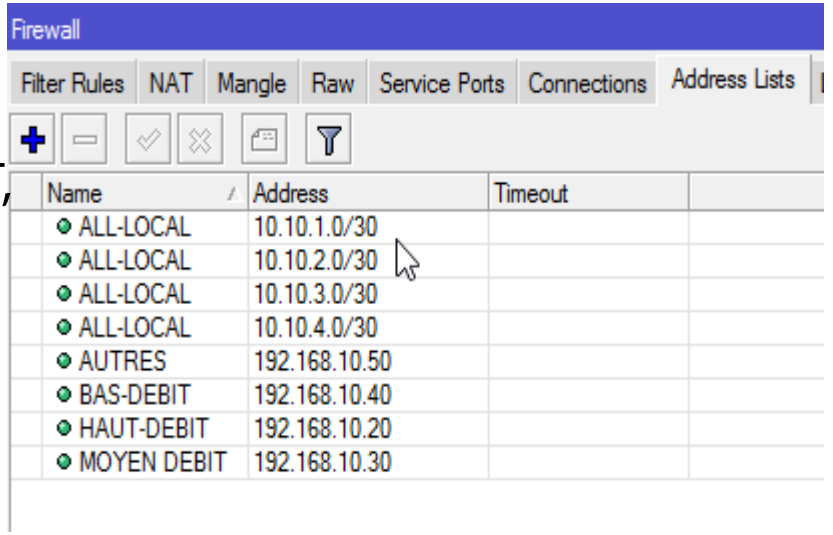
CAS PRATIQUE (3)

Nous voulons 04 niveaux de services :

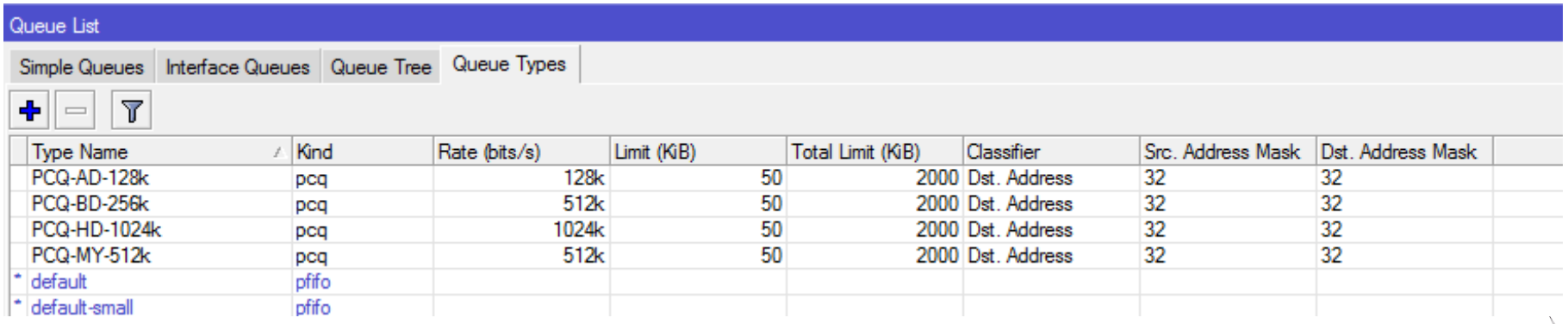
- Groupe HAUT DEBIT (sortie par liaison dédiée, priorité maximale, jusqu'à 1Mbs par utilisateur) associé à un PCQ dont le rate = 1024kbps
- Groupe MOYEN DEBIT associé à un PCQ dont le rate= 512kbps
- Groupe BAS DEBIT elle associé à un PCQ dont le rate est de =256kbps
- Groupe AUTRES associé à un PCQ dont le rate est de 128kbps
- Limite de 4Mbs pour les utilisateurs du groupe HAUT DEBIT avec possibilité de sortir par les liens 1, 2, 3 et 4
- Somme du débit des utilisateurs MOYEN DEBIT limitée à 2Mbs et possibilité de sortir par les liens 1, 2 et 3
- Somme du débit des utilisateurs BAS DEBIT limitée à 1Mbs et sortie par les liens 1 et 2
- Le groupe AUTRES est le groupe, sortie par le lien 2, pas de failover routé vers la connexion secondaire

CAS PRATIQUE (4)

- Création liste d'adresses
- Ajoute des règles de QoS pour améliorer la qualité. Débit max par groupe sous HAUT DEBIT, Débit max par utilisateur, exploitation de PCQ avec classiffier par @IP
- Ajout des adresses IP dans les adresses-list
- Mise en place du Policy Routing
- HAUT DEBIT vers Table MAIN, MOYEN DEBIT vers TABLE 2, BAS DEBIT VERS TABLE 3



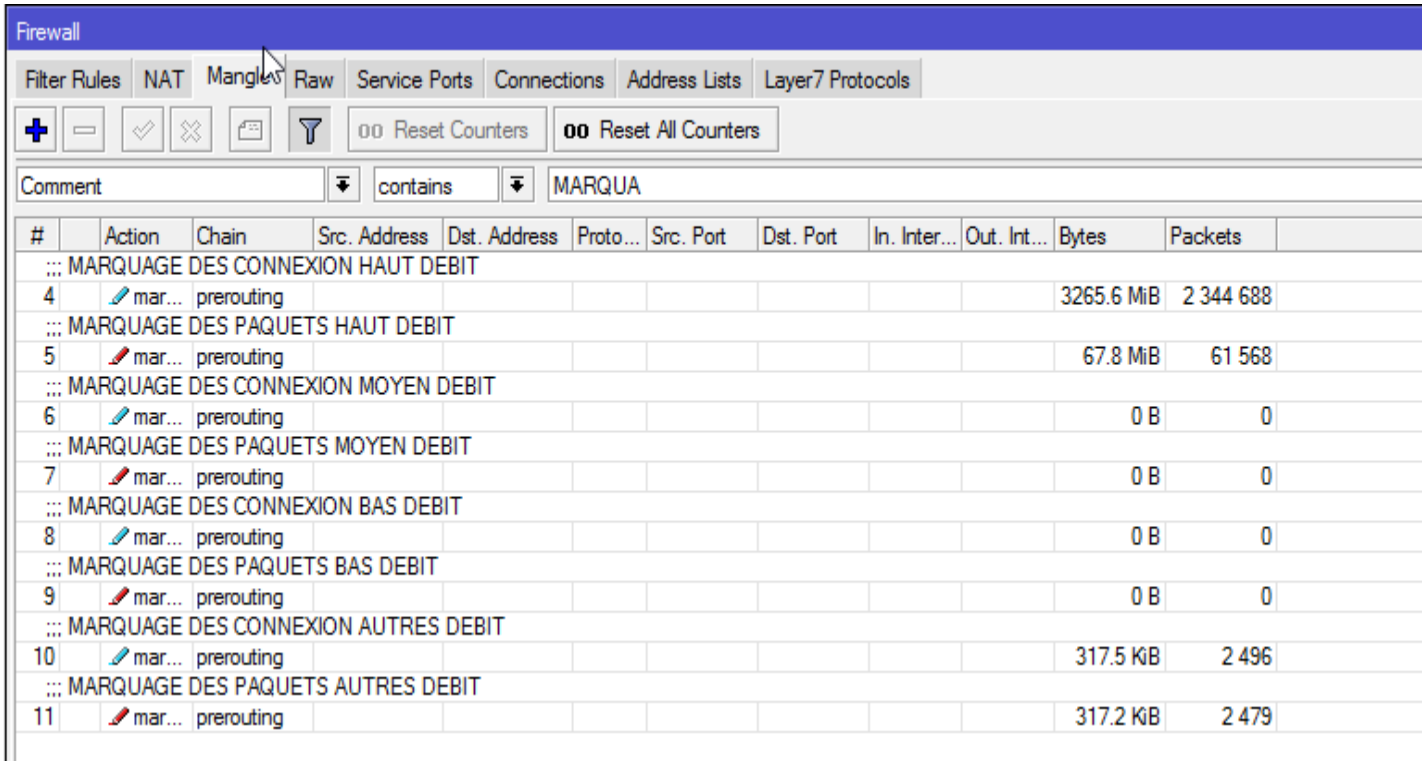
Name	Address	Timeout
ALL-LOCAL	10.10.1.0/30	
ALL-LOCAL	10.10.2.0/30	
ALL-LOCAL	10.10.3.0/30	
ALL-LOCAL	10.10.4.0/30	
AUTRES	192.168.10.50	
BAS-DEBIT	192.168.10.40	
HAUT-DEBIT	192.168.10.20	
MOYEN DEBIT	192.168.10.30	



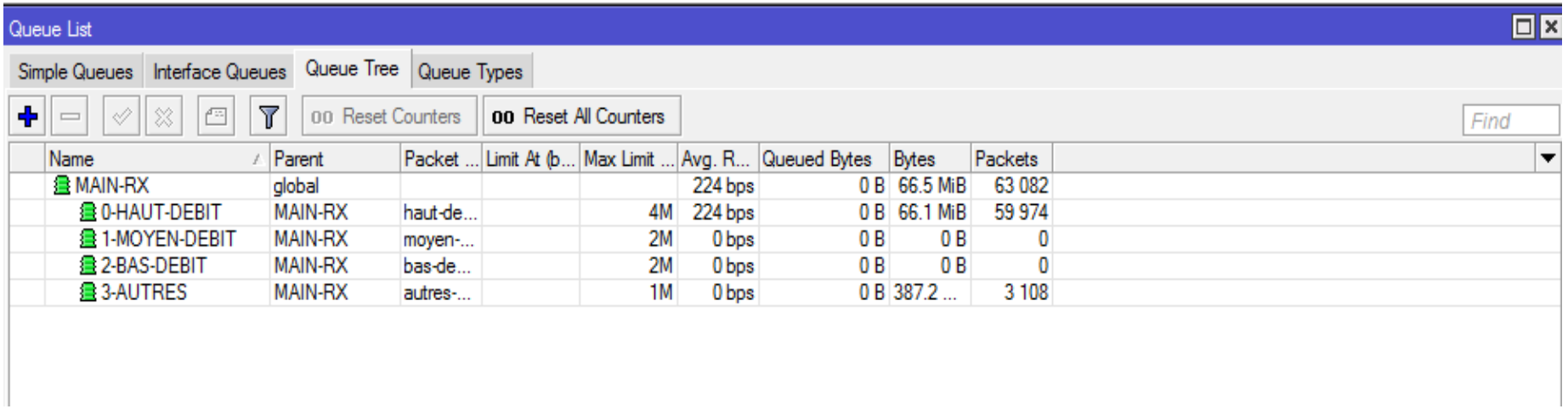
Type Name	Kind	Rate (bits/s)	Limit (KiB)	Total Limit (KiB)	Classifier	Src. Address Mask	Dst. Address Mask
PCQ-AD-128k	pcq	128k	50	2000	Dst. Address	32	32
PCQ-BD-256k	pcq	512k	50	2000	Dst. Address	32	32
PCQ-HD-1024k	pcq	1024k	50	2000	Dst. Address	32	32
PCQ-MY-512k	pcq	512k	50	2000	Dst. Address	32	32
* default	pfifo						
* default-small	pfifo						

CAS PRATIQUE (5)

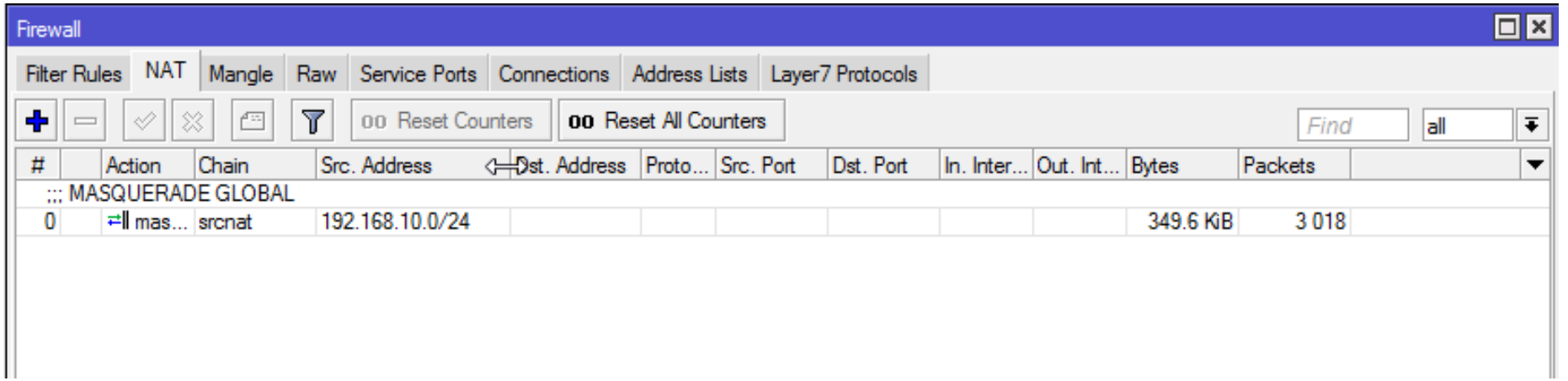
La mise en place de la Qos de fait en plusieurs étapes, elle commence par le marquage des connexions et de paquets par type d'utilisateurs



CAS PRATIQUE (6)



Name	Parent	Packet ...	Limit At (b...	Max Limit ...	Avg. R...	Queued Bytes	Bytes	Packets
MAIN-RX	global				224 bps	0 B	66.5 MiB	63 082
0-HAUT-DEBIT	MAIN-RX	haut-de...		4M	224 bps	0 B	66.1 MiB	59 974
1-MOYEN-DEBIT	MAIN-RX	moyen-...		2M	0 bps	0 B	0 B	0
2-BAS-DEBIT	MAIN-RX	bas-de...		2M	0 bps	0 B	0 B	0
3-AUTRES	MAIN-RX	autres-...		1M	0 bps	0 B	387.2 ...	3 108

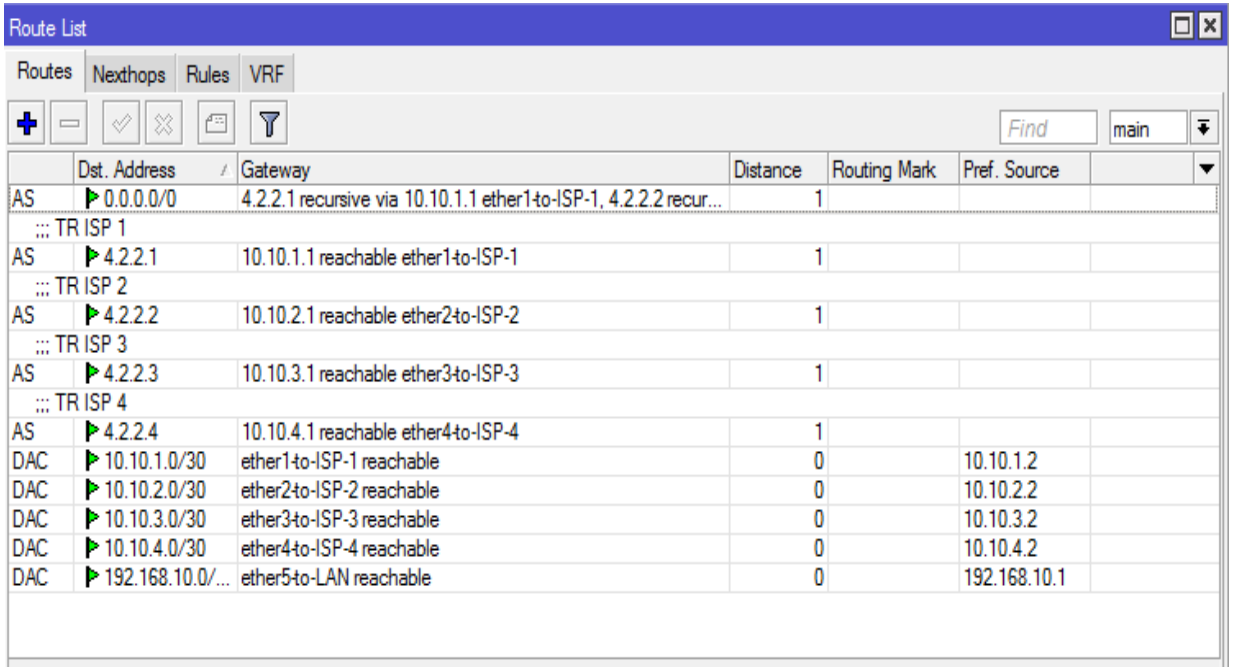


#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; MASQUERADE GLOBAL											
0	mas...	srcnat	192.168.10.0/24							349.6 KiB	3 018

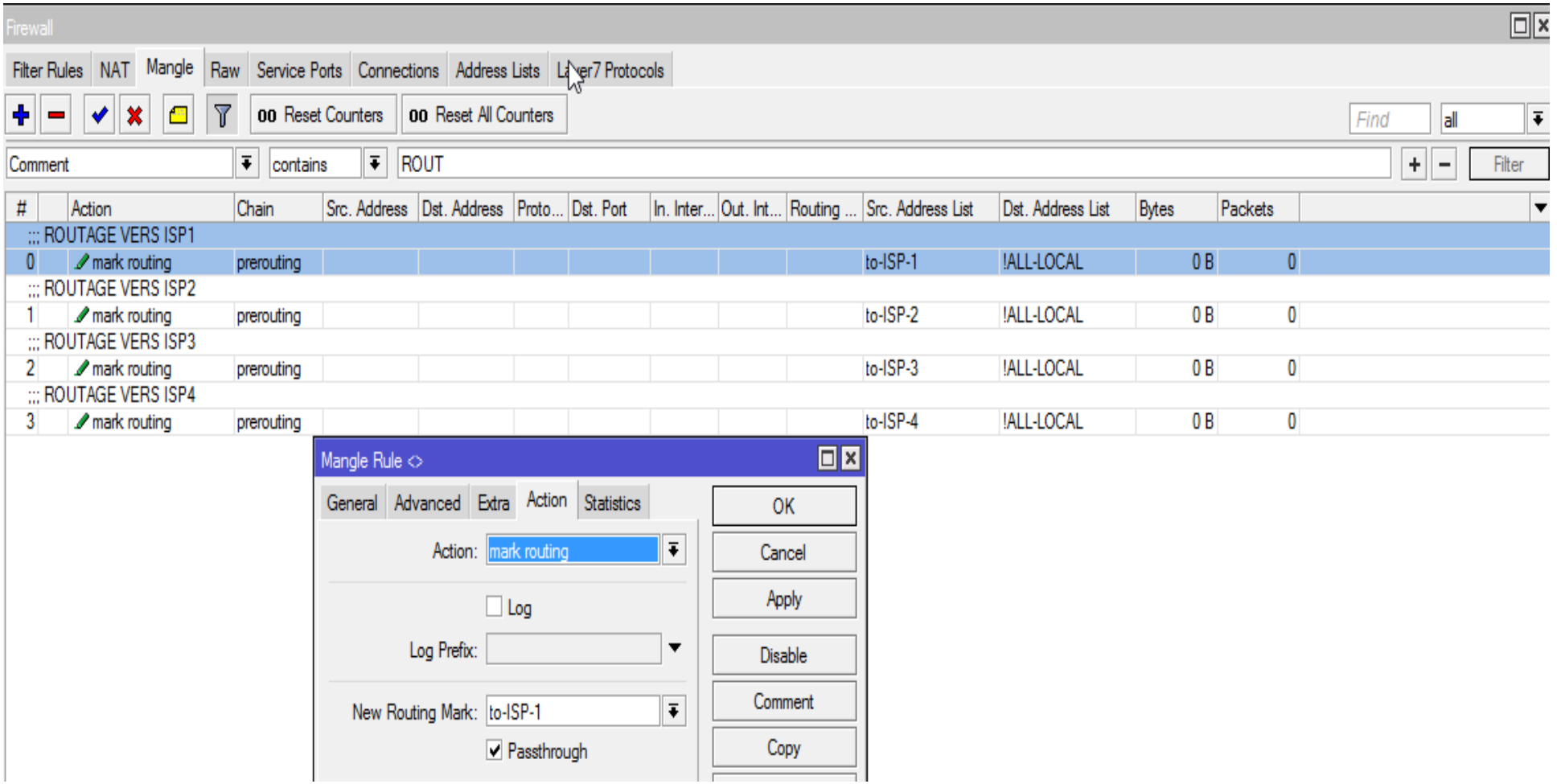
CAS PRATIQUE (7)

Mise en place de la QoS :

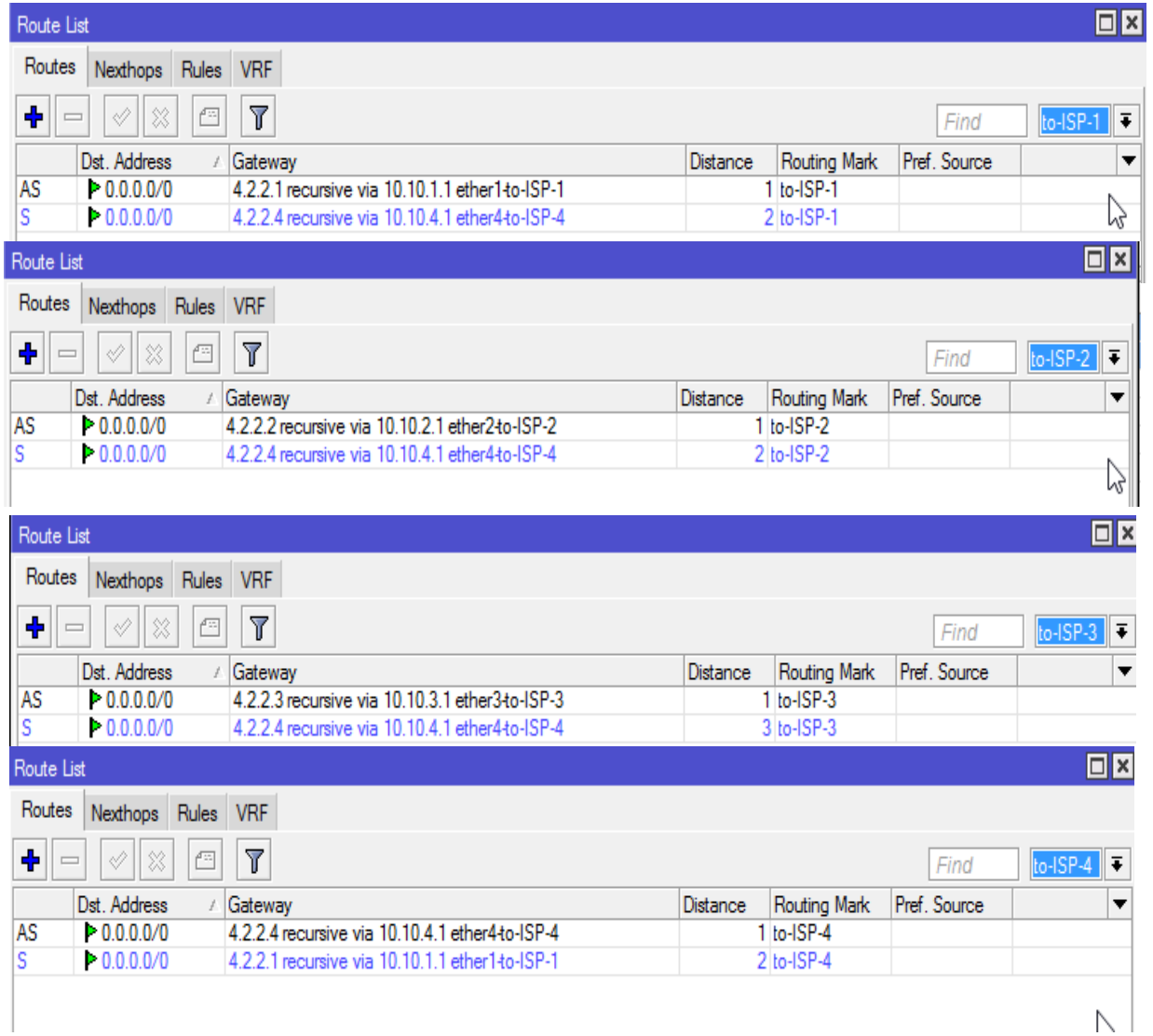
- marquer les différents trafics et à les envoyer dans les sous tables de tables de routage
- Ensuite configurer des routes de tests
- Ensuite configurer le routage récursif
- Enfin Activer le failover



CAS PRATIQUE (8)



CAS PRATIQUE (9)



Les FAIS sont les backup les uns des autres

CAS PRATIQUE (10)

Nous choisissons les hôtes de contrôle de chaque liaison que nous définissons dans la table main avec le scope 10 en nous assurant qu'ils sont PINGER pour garantir qu'Internet passe

- `add distance=10 gateway=4.2.2.2 check-gateway=ping comment="ROUTE RECURSIVE PRINCIPALE VIA ISP2"`
- `add distance=20 gateway=4.2.2.3 check-gateway=ping comment="ROUTE RECURSIVE SECONDAIRE VIA ISP1"`

Après nous n'avons plus qu'à définir les passerelles dans nos différentes tables de routage

- `/ip route`
- `add distance=10 gateway=4.2.2.2 comment="ROUTE RECURSIVE PRINCIPALE VIA CAMTEL-ADSL"`
- `add distance=20 gateway=4.2.2.3 comment="ROUTE RECURSIVE SECONDAIRE VIA INFOGENIE"`

Protocole de test

TEST QOS + AGREGATION

1. Mettre une @ IP dans un groupe et faire un bandwith test pour saturer et voir le throughput maximal
2. Faire un traceroute pour voir vers quel FAI il sort
3. Changer de plan de service à cette adresse et refaire un autre test de débit maximal.

TEST REDONDANCE/FAILOVER

1. On lance un ping continu à partir du LAN
2. Couper la liaison de sortie et noter le temps de basculement sur la seconde.
3. Remettre la liaison précédente, voir si le service est restauré automatiquement.

UNE TELLE CONFIGURATION VOUS DONNE 99,5% DE DISPONIBILITE

Brief summary
for ensglish speaking participants

QoS, Link Aggregation and redundancy with failover with Mikrotik


Je vous remercie