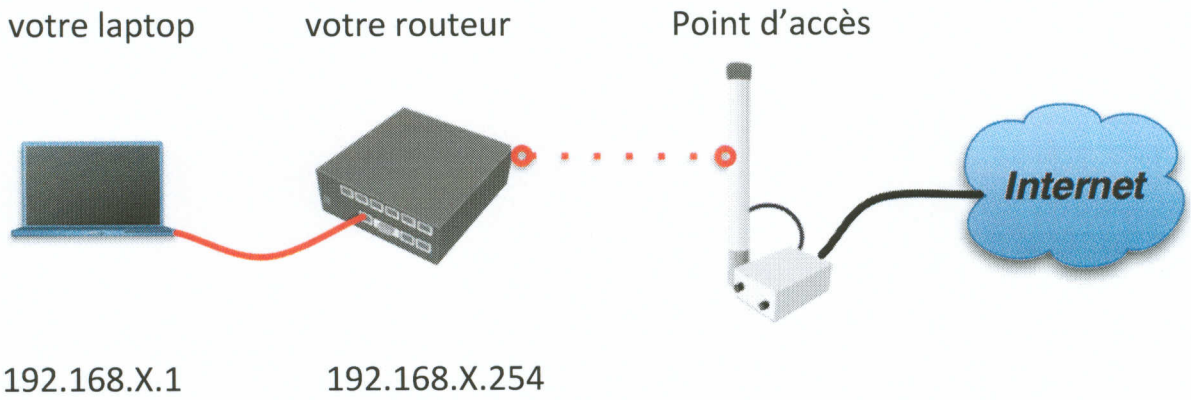
Module 1 – Introduction à MikroTik RouterOS

Dans cet exercice, vous allez apprendre comment accéder au routeur MikroTik et faire une configuration pour que le réseau local (derrière le routeur) puisse avoir une connectivité à internet. Après cela, vous apprendrez comment mettre à jour RouterOS. Les autres points de ce module sont la réinstallation de RouterOS, la sauvegarde et la restauration de la configuration du routeur ainsi que le management des utilisateurs.

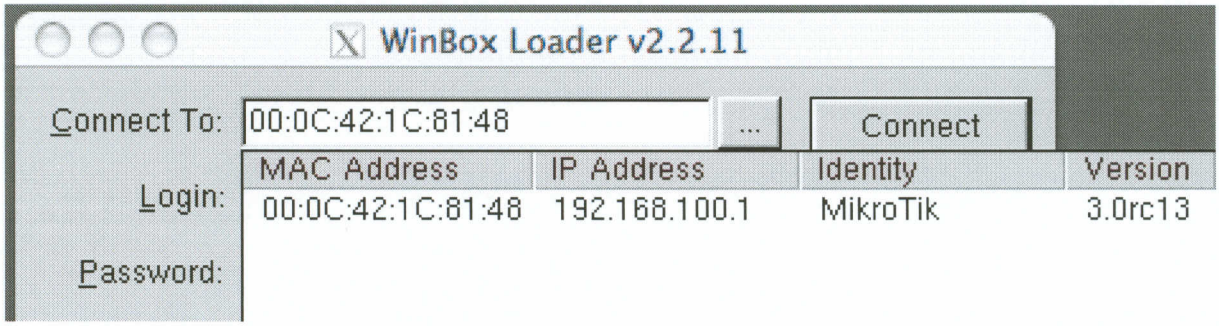


Vous avez un sous-réseau IP privé qui vous est dédié pour la classe :
192.168.X.0/24

Vous allez connecter votre réseau privé à internet par une connexion wifi sur votre routeur. Un serveur DHCP fonctionne sur le point d'accès de la classe. Votre routeur doit fournir le service DNS. Une configuration NAT est nécessaire sur le routeur pour assurer l'accessibilité à internet pour votre laptop.

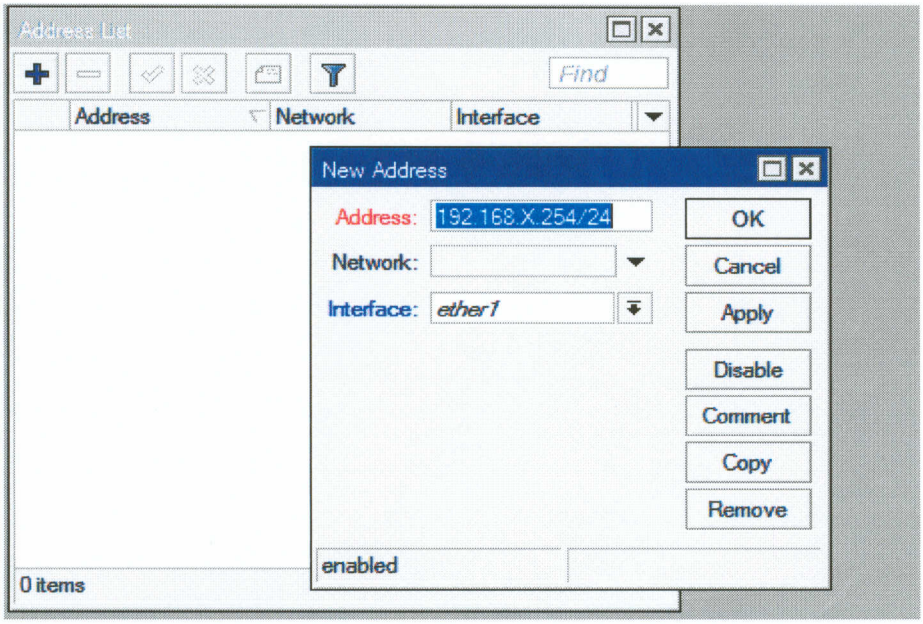
Exercice 1.1 – Accédez au routeur

1. Téléchargez Winbox depuis www.mikrotik.com
2. Cliquez sur le bouton [...] pour voir votre routeur, sélectionnez l'adresse MAC et ensuite cliquez sur « Connect ». L'utilisateur par défaut est admin sans mot-de-passe.
3. Cliquez sur « Remove configuration » si un message apparaît.

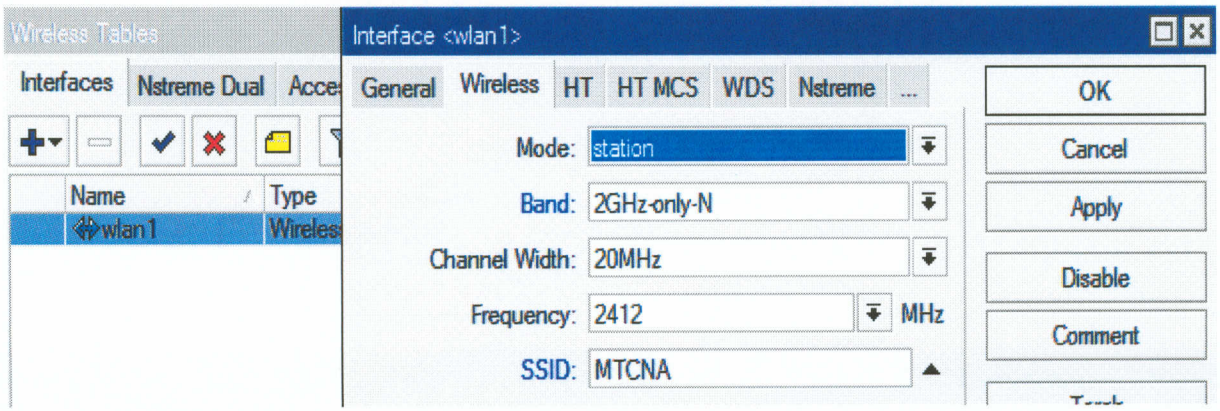


Exercice 1.2 – Configurez la connexion internet via le routeur

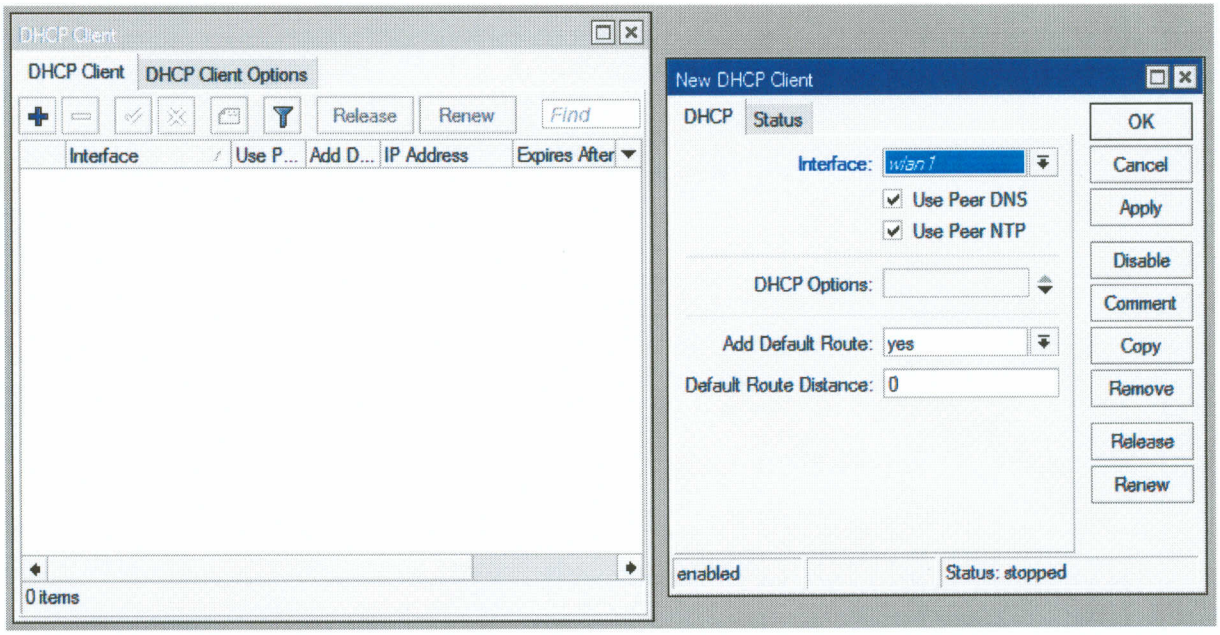
1. Désactivez les autres interfaces (wifi ou 3g) de votre laptop, ne gardez que la carte ethernet active.
2. Mettez comme adresse IP sur votre laptop 192.168.X.1.
3. Utilisez comme masque de sous-réseau 255.255.255.0.
4. Comme passerelle et serveur DNS, utilisez 192.168.X.254.
5. Connectez-vous au routeur par l'adresse MAC en utilisant Winbox.
6. Une fois connecté, allez dans IP -> Address et ajoutez 192.168.X.254 pour l'interface Ether1 de votre routeur.



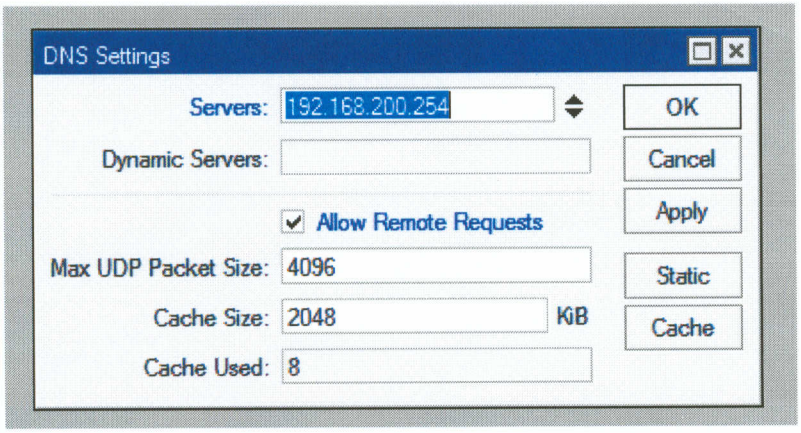
7. Fermez Winbox et reconnectez-vous cette fois en utilisant l'adresse IP (l'accès par l'adresse MAC doit seulement être utilisé quand l'accès par IP n'est pas possible).
8. Ouvrez Wireless dans le menu principal de Winbox. Sélectionnez et activez l'interface wlan1. Double cliquez sur wlan1 pour configurer l'interface wifi.



9. Mettez comme Wireless Mode le mode station, Band 2ghz only N et cliquez « Apply ».
10. Appuyez sur le bouton « Scan » pour trouver le réseau MTCNA.
11. Sélectionnez le réseau MTCNA et cliquez sur « Connect ».
12. Vérifiez l'enregistrement sur le réseau dans la partie « Registration ».
13. Installez un client DHCP sur l'interface wlan1 pour recevoir une adresse IP depuis le point d'accès.



14. Configurez le serveur DNS de votre routeur pour qu'il interroge le point d'accès (IP = 192.168.200.254).

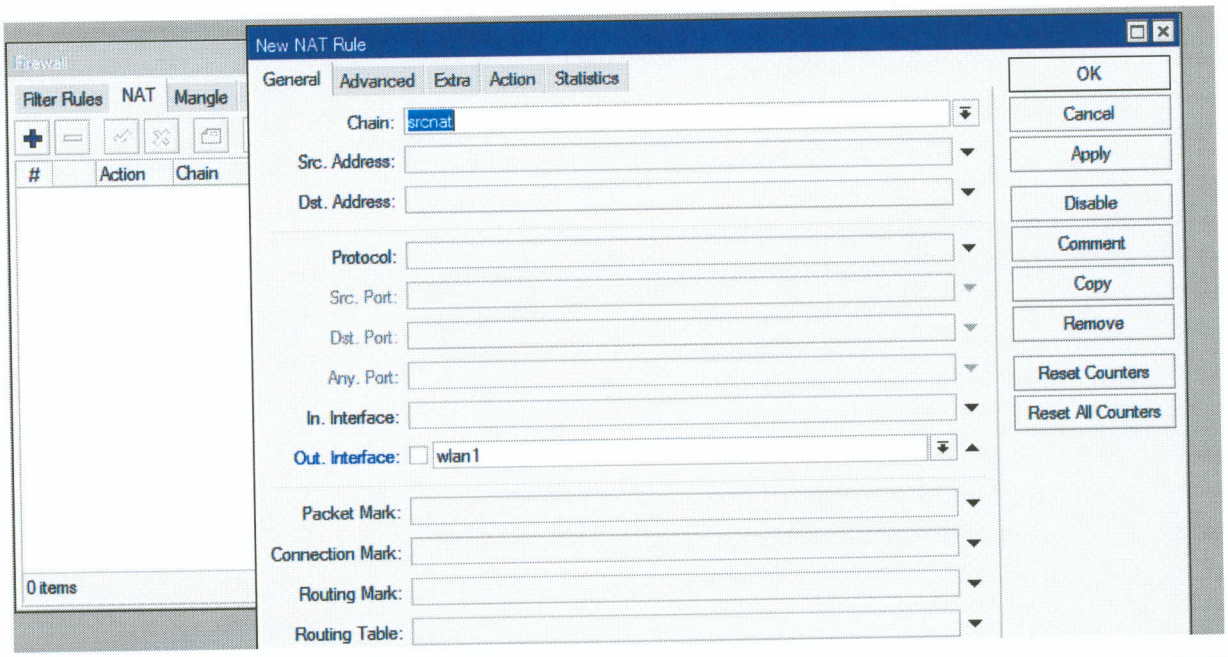


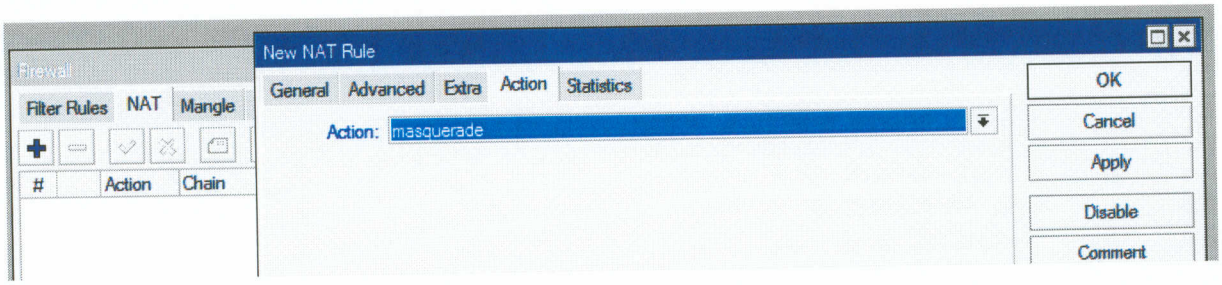
15. Configurez une translation d'adresse (NAT) pour que le réseau local derrière le routeur puisse accéder à internet :
Winbox menu : IP -> Firewall -> NAT.

Créez une nouvelle règle NAT avec les paramètres suivants :

- Chain = srcnat
- Output interface = wlan1.

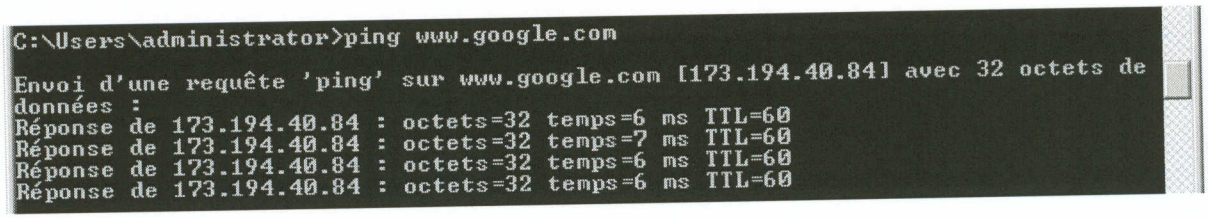
Et dans l'onglet « Action », mettez action=masquerade.





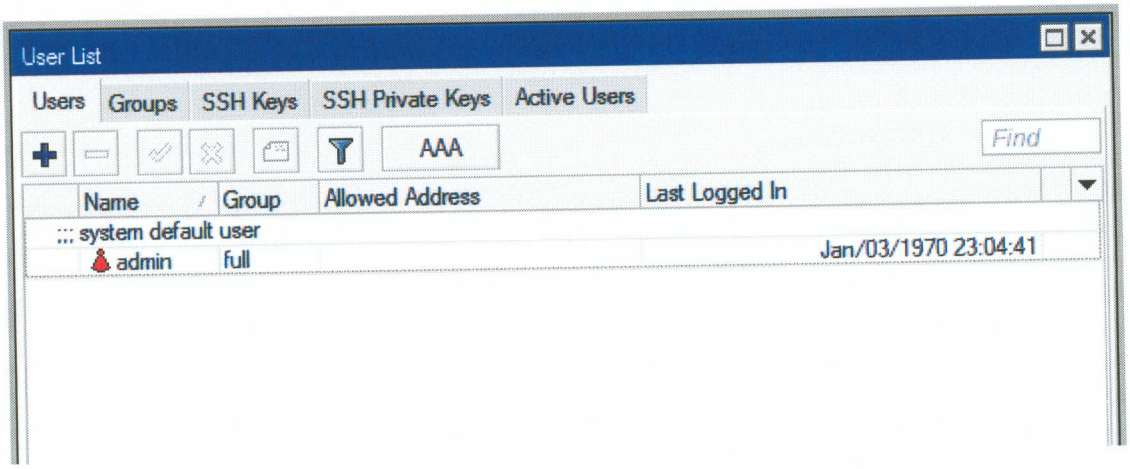
16. Pour finir, vérifiez que vous avez accès à internet depuis votre laptop.

Ping www.google.com



Exercice 1.3 – Gestion des utilisateurs du routeur

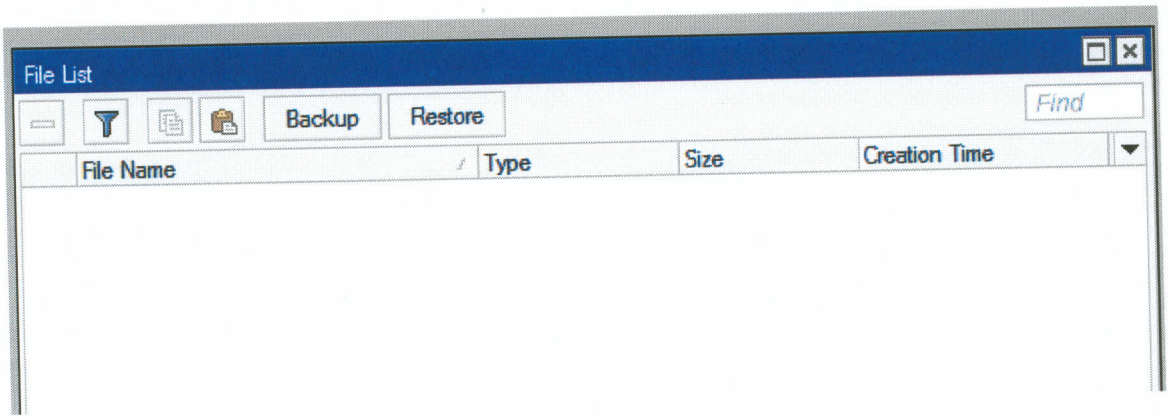
Allez dans Winbox -> Menu System -> Users.



1. Ajoutez un nouvel utilisateur au routeur avec comme droit « full access ».
2. Modifiez l'utilisateur « admin » en lecture seule.
3. Fermez Winbox et ouvrez une session avec le nouvel utilisateur créé.

Exercice 1.4 – Mise à jour de RouterOS

1. Vérifiez et téléchargez le dernier paquet de RouterOS depuis le site http://www.mikrotik.com/download.html
   Plusieurs versions sont présentes pour les différentes architectures CPU. Vous pouvez voir le modèle de processeur dans la barre titre de Winbox.
2. Transférez le fichier de Mise à jour vers votre routeur. Pour cela un simple glisser-déposer dans la fenêtre « files » de Winbox suffit.



3. Redémarrez le routeur depuis Winbox -> menu System -> Reboot.

Exercice 1.5 – Activation-désactivation des paquets de RouterOS

1. Désactivez le paquet wireless.
2. Redémarrez le routeur.
3. Vérifiez la liste des interfaces.
4. Réactivez le paquet wireless et redémarrez le routeur.

Exercice 1.6 – Nommez votre routeur

1. Mettez **votre chiffre + votre nom** comme routeur identity.
2. Activez l'interface wifi en tant que "Discovery interface".
3. Vérifiez que vous visualisez les autres routeurs dans la liste des "voisins".

> dyn dns

> romon > time > netinstall

Exercice 1.7 – Fichiers de backup et d'exportations

1. Allez dans Winbox -> Menu Files :
   pressez le bouton « Backup » -> un fichier est généré avec la sauvegarde de la configuration.
2. Transférez le fichier de sauvegarde sur votre laptop (glisser/déposer).
3. Dans Winbox – ouvrez une Console système.
4. En ligne de commande, tapez : /export file=mtcna1.
   Cela va générer le fichier d'exportation.
5. Transférez le fichier d'exportation sur votre laptop.
6. Avec un éditeur, ouvrez les 2 fichiers et comparez-les.

Exercice 1.8 – Netinstall (démonstration)

1. Téléchargez Netinstall sur le site de Mikrotik.
2. Mettez une adresse IP fixe sur votre laptop, activez le « Netbooting » et spécifiez l'adresse IP pour l'appareil distant (doit être dans le même sous-réseau que le laptop).
3. Connectez le routeur directement avec un câble ethernet (recommandé).
4. Connectez le router avec un câble série – lancez Putty.
5. Redémarrez le routeur – pressez une touche quand demandé.
6. Modifiez le routeur pour qu'il démarre sur le réseau.
7. Redémarrez le routeur – il doit apparaître dans Netinstall.
8. Sélectionnez le routeur, choisissez le paquet de RouterOS à installer.
9. Lancez l'installation – vérifiez l'état d'avancement.
10. Reconfigurez le routeur pour qu'il démarre en premier sur sa mémoire interne.

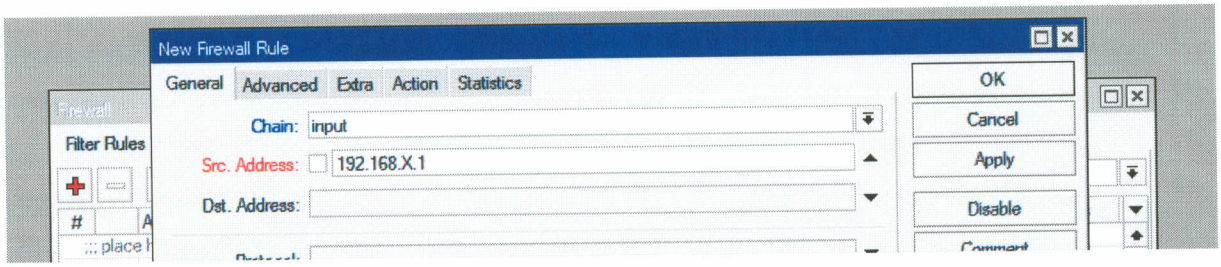
MODULE 2 – MikroTik RouterOS Firewall

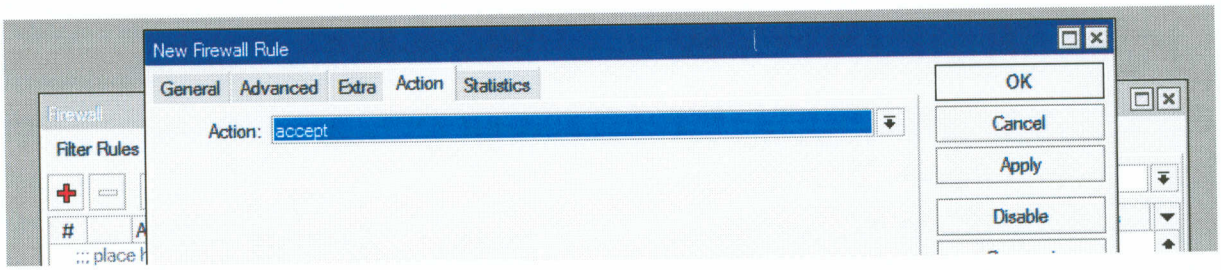
Les concepts du Firewall de RouterOS.

Exercice 2.1 – Protégez votre routeur – chaîne input

1. Ouvrez IP -> Firewall.

Créez une règle de filtrage pour autoriser les connections depuis votre laptop. Utilisez comme objet l'adresse IP source et comme action « accept ».





2. Créez une règle pour interdire tous les autres accès depuis votre réseau local. Utilisez comme objet l'adresse source du réseau 192.168.x.0/24 et comme action = discard.
3. Modifiez l'adresse de votre laptop en 192.168.X.10.
4. Essayez de vous connecter, le firewall fonctionne.
5. Vous pouvez vous connecter par adresse Mac uniquement.
6. Créez une règle additionnelle pour pouvoir vous connecter à internet – mettez cette règle en 1er (glisser-déplacer la nouvelle règle en haut de la liste).
7. Remettez l'adresse de votre laptop en 192.168.X.1 et reconnectez-vous en IP.

Exercice 2.2 – Protégez vos clients - chaîne forward

1. Créez une règle dans la chaîne forward qui bloque le protocole TCP port 80.
2. Essayez d'ouvrir depuis votre laptop le site www.mikrotik.com.
3. Essayez d'ouvrir http://192.168.X.254.
4. Ajoutez un commentaire à vos règles.

Exercice 2.3 – Liste d'adresse

1. Créez une liste d'adresse contenant les adresses 192.168.x.1 et 192.168.x.10.
2. Modifier la règle input (créé dans 2.1) pour autoriser le management du routeur depuis cette liste d'adresse.

Exercice 2.3.1 – Liste d'adresse – ajout automatique

1. Créez une règle dans la chaîne forward pour les paquets en direction de l'adresse 8.8.8.8 avec comme action d'ajouter la source dans une adresse liste - nommez cette liste « liste-88 »
2. Créez une règle d'interdiction (drop) dans la chaîne forward qui correspond aux paquets IP provenant de la liste d'adresse « liste-88 »
3. Ping 8.8.8.8 depuis votre laptop
4. Maintenant, essayez d'ouvrir une page sur internet
5. Désactivez ces 2 règles du firewall

Exercice 2.4 – Logs

1. Créez une règle pour créer les logs des pings de votre laptop vers le routeur (chaine input , protocole icmp , action=log)
2. Vérifiez les logs

Exercice 2.5 – Etat des connections

1. Désactivez les règles Firewall qui sont actuellement dans la chaîne input
2. Créez une règle dans la chaîne input pour interdire (drop) les paquets IP avec comme « état connexion invalide »
3. Créer une règle dans la chaîne input pour autoriser les paquets IP avec comme état « connexion établie »
4. Créer une règle dans la chaîne input pour interdire les paquets IP avec comme état « connexion nouvelle » et comme port et protocole le service Winbox. Mettez cette règle devant les autres règles.
5. Essayez d'ouvrir une seconde fenêtre Winbox (laissez la 1ère ouverte). Vous ne devriez pas pouvoir vous connecter – le firewall fonctionne.
6. Enlevez la règle d'interdiction créée au point 4.

Exercice 2.6 – Destination NAT et cache DNS

1. Changez le serveur DNS de votre laptop en 8.8.8.8. Vérifiez que les requètes DNS fonctionne depuis votre laptop.
2. Créez 2 règles (tcp et udp) dans la chaîne « dst-nat » du firewall pour rediriger le trafic DNS sur le routeur (action=redirect, port 53)
3. Ajoutez une entrée statique dans le cache DNS du routeur : www.yahoo.com , ip = 173.194.40.83
4. Maintenant ouvrez le site www.yahoo.com depuis votre laptop, quel site s'ouvre ?
5. Enlevez les règles du point 2 et l'entrée statique dans le DNS

Exercice 2.7 – Proxy

1. Activez le serveur Proxy de votre routeur sur le port 8080
2. Créez une règle dst-nat pour rediriger les requètes HTTP (tcp port80) vers le Proxy du routeur (tcp port 8080)(on créé un proxy transparent)
3. Créez une règle dans le Proxy pour interdire l'accès à www.cisco.com
4. Vérifiez que l'accès au site est interdit.
5. Créez une règle pour redirigez les pages non-permises vers le site www.mikrotik.com
6. Vérifiez la redirection.

Exercice 2.7.1 – logs du Proxy

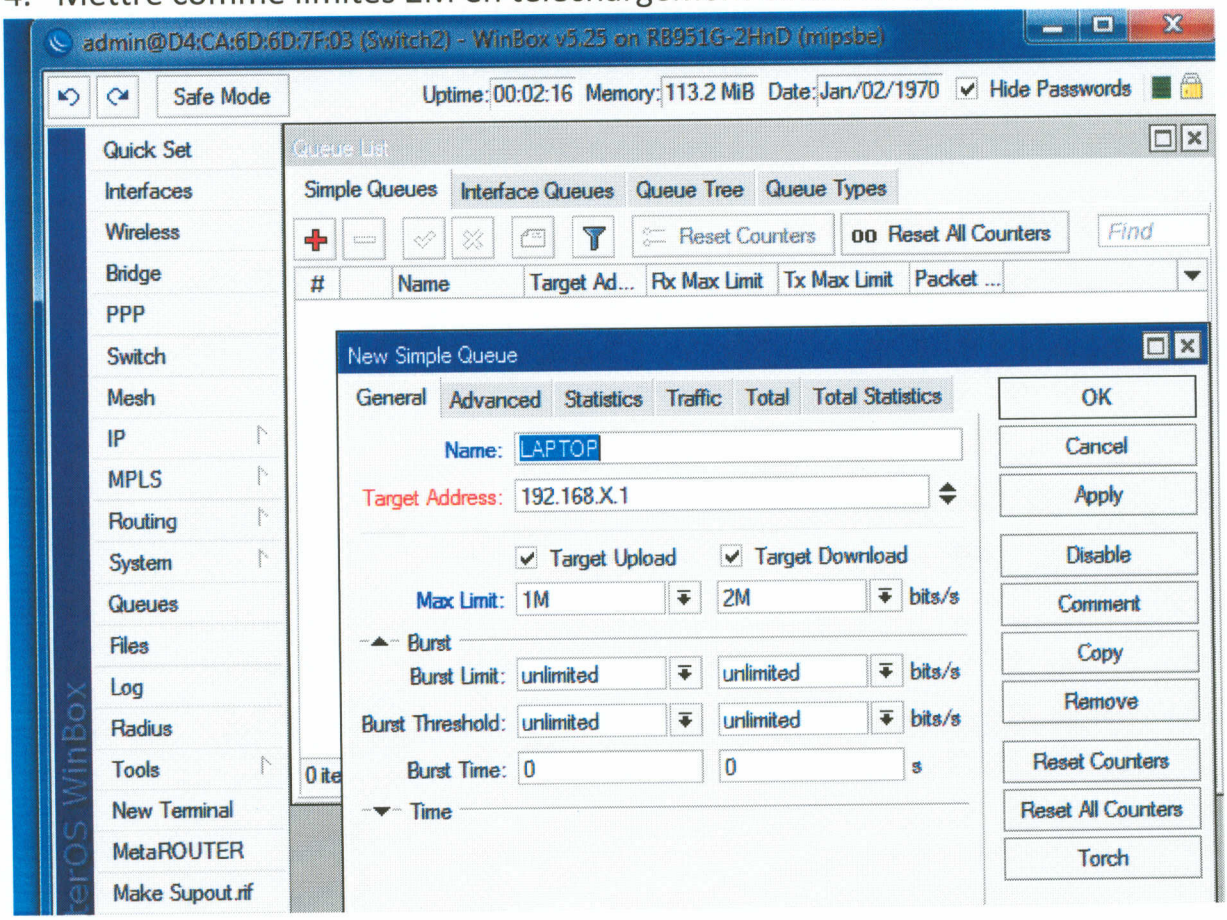
1. Allez dans System -> logging et ajoutez une règle pour créer des logs en mémoire
2. Naviguez sur internet depuis votre laptop et ensuite vérifiez les logs du routeur.
3. Inspectez l'onglet « Connections » du Proxy.
4. Désactivez le proxy et la règle dst-nat créez pour le proxy transparent.

Module 3 – Gestion de la bande passante dans RouterOS

Dans ces exercices, vous allez apprendre comment gérer la bande passante dans RouterOS.

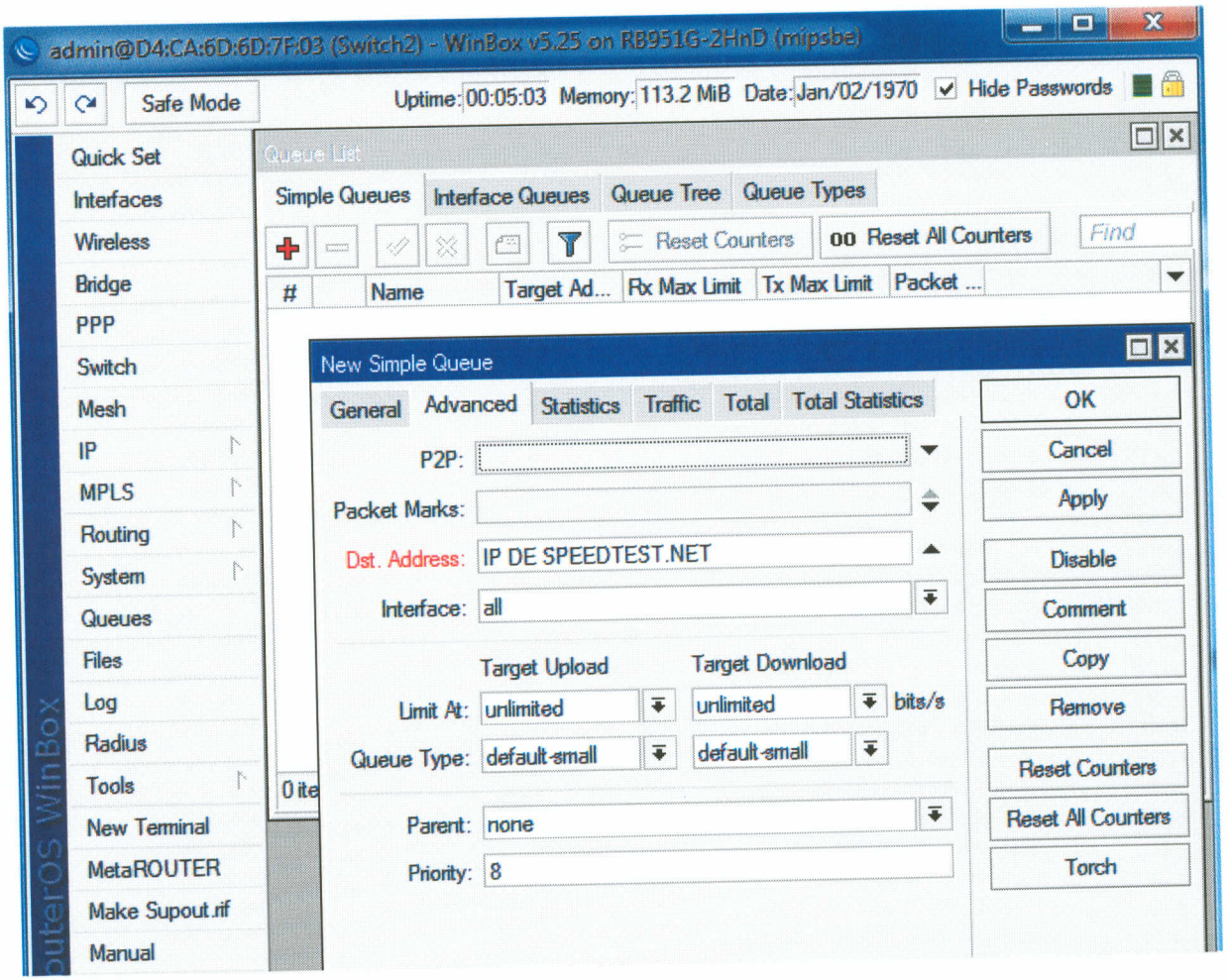
Exercice 3.1 – Simple Queue

1. Dans le menu principal, cliquez sur « Queue », puis dans l'onglet « Simple Queues » ajoutez une file d'attente
2. Nommez cette file d'attente LAPTOP
3. Utilisez comme Target-Address (adresse cible) l'IP de votre Laptop
4. Mettre comme limites 2M en téléchargement et 1M en envoi



5. Depuis le menu de Winbox -> tools -> torch et démarrez le sur « ether1 »
6. Sur votre laptop , accédez au site www.speedtest.net et vérifiez le résultat obtenu
7. Recommencez le test et vérifiez l'onglet « simple queue Traffic »

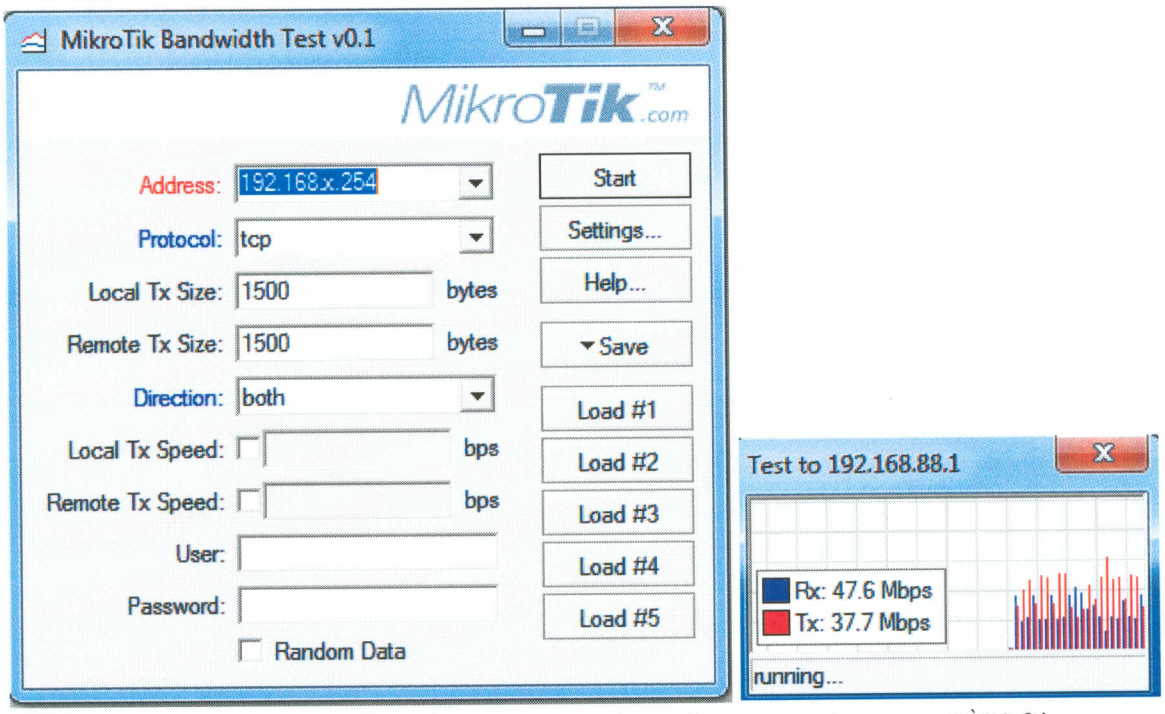
8. Depuis le menu principal de Winbox, ouvrir Tools-> Torch. Démmarrez Torch sur l'interface « ether1 » et répétez le test de vitesse sur speedtest.net . Repérez la connexion et notez l'adresse IP du serveur de speedtest .
9. Maintenant vous devez mettre à jour la file d'attente LAPTOP pour limiter le trafic uniquement vers le serveur de speedtest



10. Lancez une nouvelle fois le test de speedtest.net pour vérifiez que la bande passante est bien limitée
11. Lancez cette fois le test de speedtest.net sur un autre serveur et vérifiez qu'il n'y a pas de limitation de vitesse
12. Inversez dans la file d'attente LAPTOP les adresses IP dans Target-address et Dst-address. Lancez de nouveau le test de speedtest.net sur le 1er serveur. Les limitations doivent fonctionner, mais les vitesses de téléchargement et d'envoi doivent avoir changées
13. Réinversez les valeurs de Target-Address et de DST-Address

Exercice 3.2 – Bandwidth Test

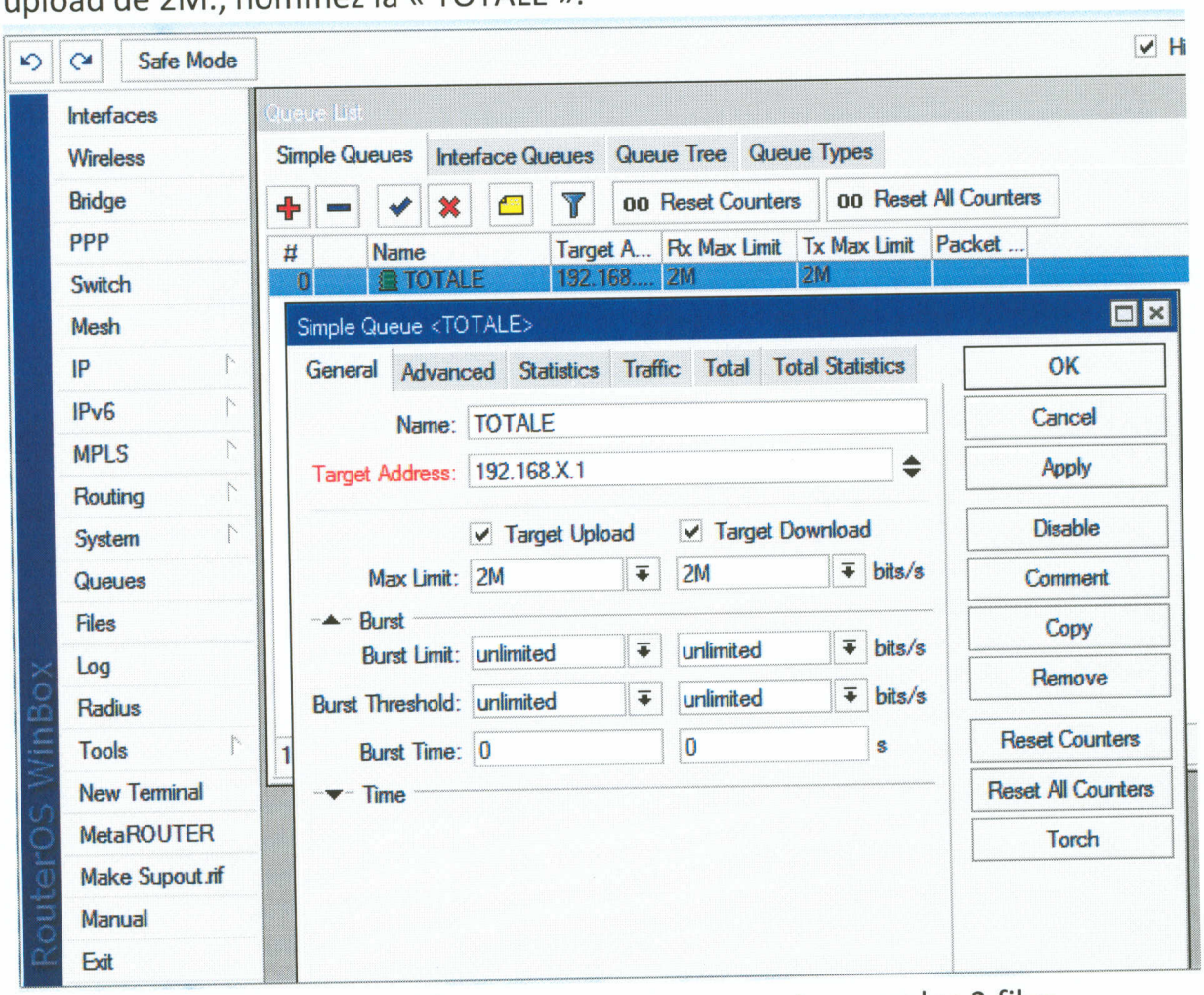
1. Téléchargez l'outil « bandwidth test » depuis le site www.mikrotik.com
2. Lancez un test en TCP vers votre routeur. « Bandwidtch server » est activé par défaut sur votre routeur, mais il requiert une authentification. Vérifiez la configuration du serveur dans Winbox (tools -> BTest Server) avant d'exécuter le test



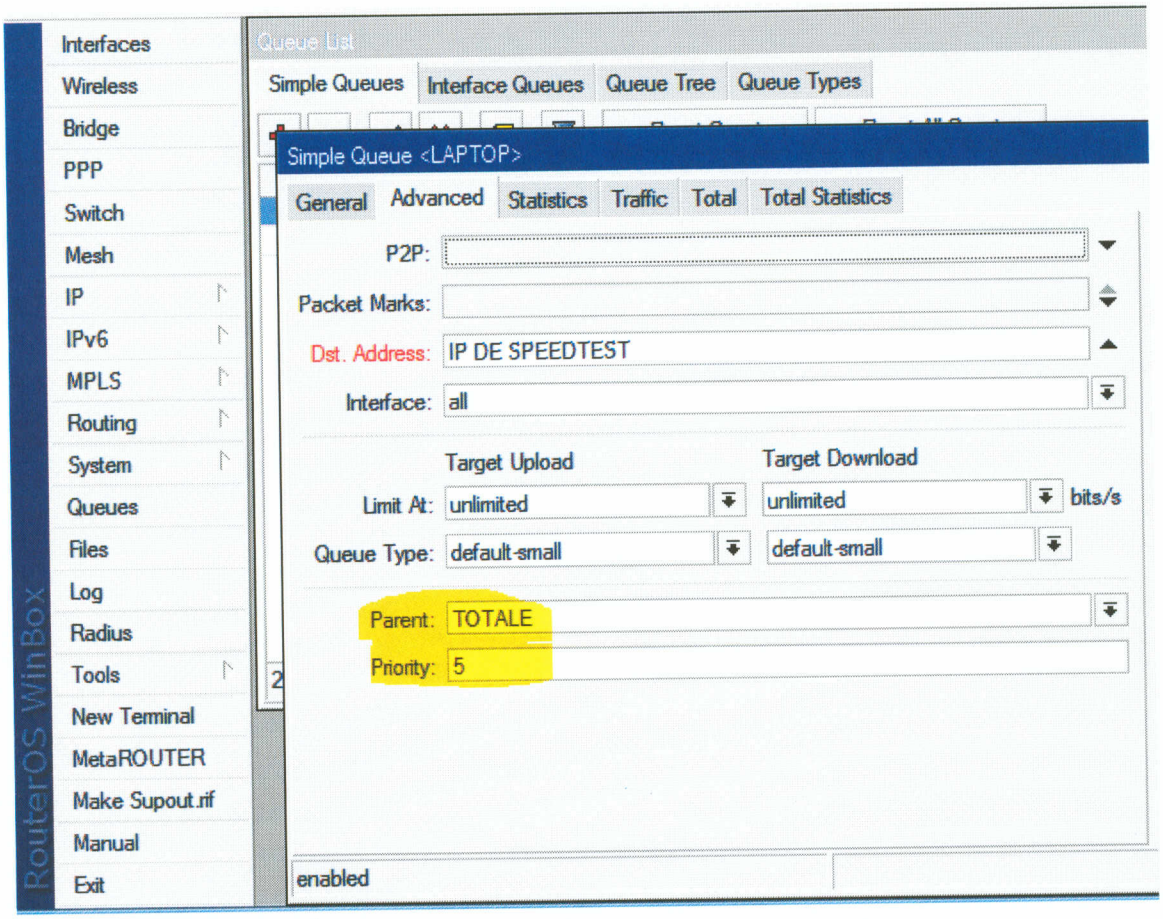
3. Pendant que le test de bande passante fonctionne, créez une 2ème file d'attente pour ce trafic et limitez votre laptop vers toutes les destinations. Appelez cette file d'attente LAPTOP2 et mettez comme limite 128k en téléchargement et 128k en envoi

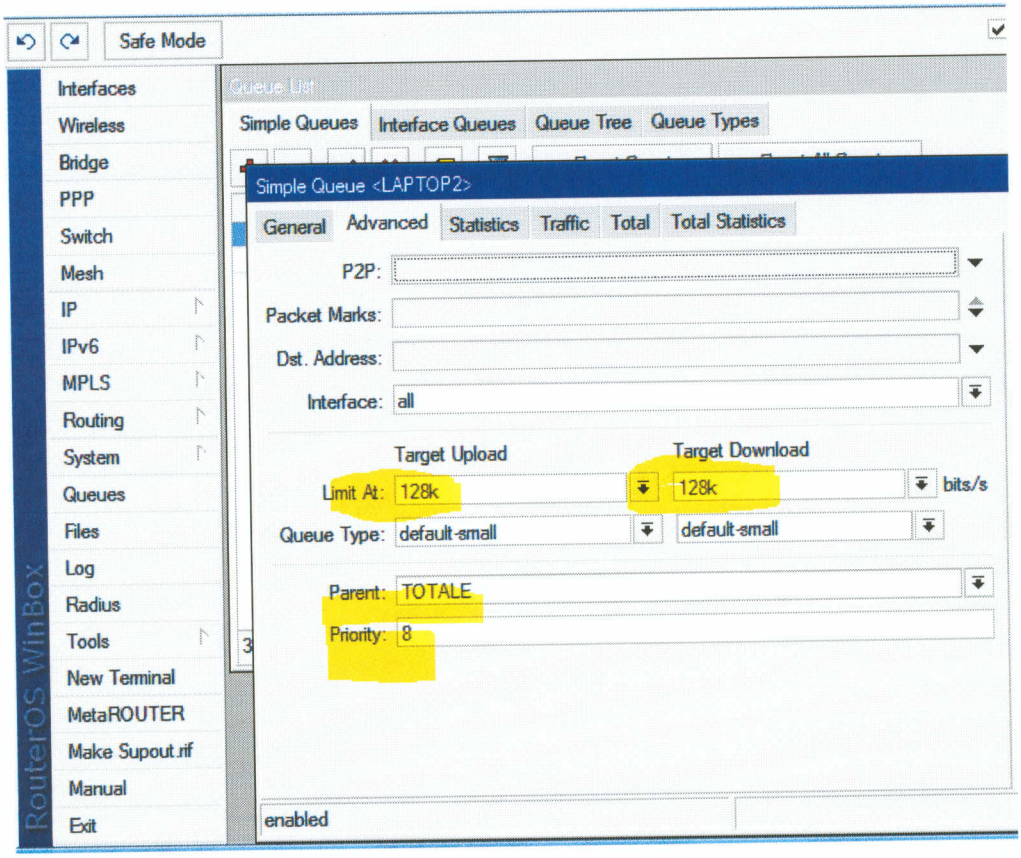
Exercice 3.3 – Priorité du trafic

1. Pour créer une gestion plus avancée de bande passante, il est possible de gérer des priorités. Créez une file d'attente avec comme download et upload de 2M., nommez la « TOTALE ».

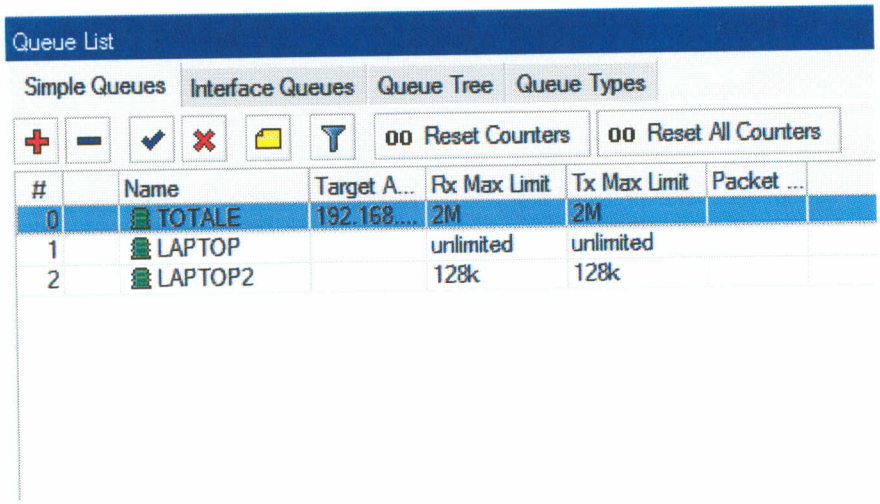


2. Mettez cette nouvelle File d'attente comme « parent » pour les 2 files d'attentes déjà créées (LAPTOP et LAPTOP2) – METTRE une priorité plus grande à la file d'attente LAPTOP (5 est plus grand que 8)


Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Make Supout.rif
Manual
Exit
RouterOS WinBox
Queue List
Simple Queues
Interface Queues
Queue Tree
Queue Types
Simple Queue <LAPTOP>
General
Advanced
Statistics
Traffic
Total
Total Statistics
P2P:
Packet Marks:
Dst. Address: IP DE SPEEDTEST
Interface: all
Target Upload
Target Download
Limit At: unlimited
unlimited
bits/s
Queue Type: default-small
default-small
Parent: TOTALE
Priority: 5
enabled


Safe Mode
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Make Supout.rif
Manual
Exit
RouterOS WinBox
Queue List
Simple Queues
Interface Queues
Queue Tree
Queue Types
Simple Queue <LAPTOP2>
General
Advanced
Statistics
Traffic
Total
Total Statistics
P2P:
Packet Marks:
Dst. Address:
Interface: all
Target Upload
Target Download
Limit At: 128k
128k
bits/s
Queue Type: default-small
default-small
Parent: TOTALE
Priority: 8
enabled

3. Maintenant vous devez avoir une structure de file d'attente :



4. Démarrer simultanément le test de speedtest et le test de bande passante du routeur.

Exercice 3.4 – Visualisation des files d'attente

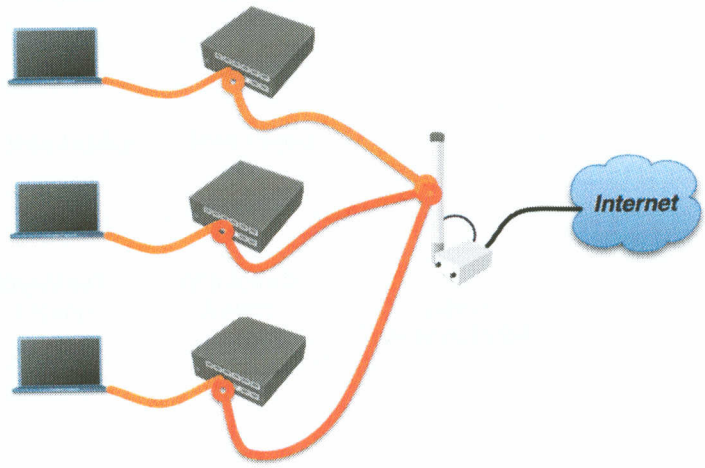
1. Ouvrez dans le menu de Winbox -> Tools -> Graphing
2. Ajoutez des règles pour générer les graphiques sur :
   a. Toutes les interfaces
   b. Toutes les files d'attente
   c. Toutes les ressources
3. Utilisez votre navigateur internet et vérifiez les graphiques sur : http://192.168.X.254/graphs/

Module 6 – Interface Bridge de RouterOS et WDS

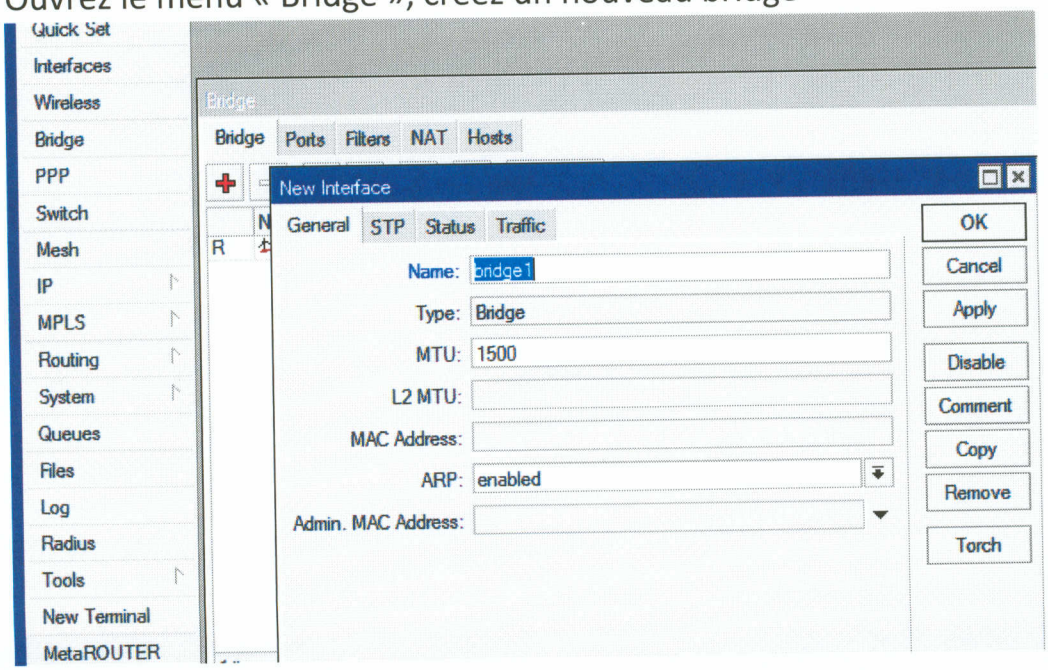
Dans ces exercices, vous allez les fonctionnalités Wireless WDS et Bridge.

Exercice 6.1 – Concept du Bridge

Nous allons créer un seul grand réseau avec le même domaine de broadcast

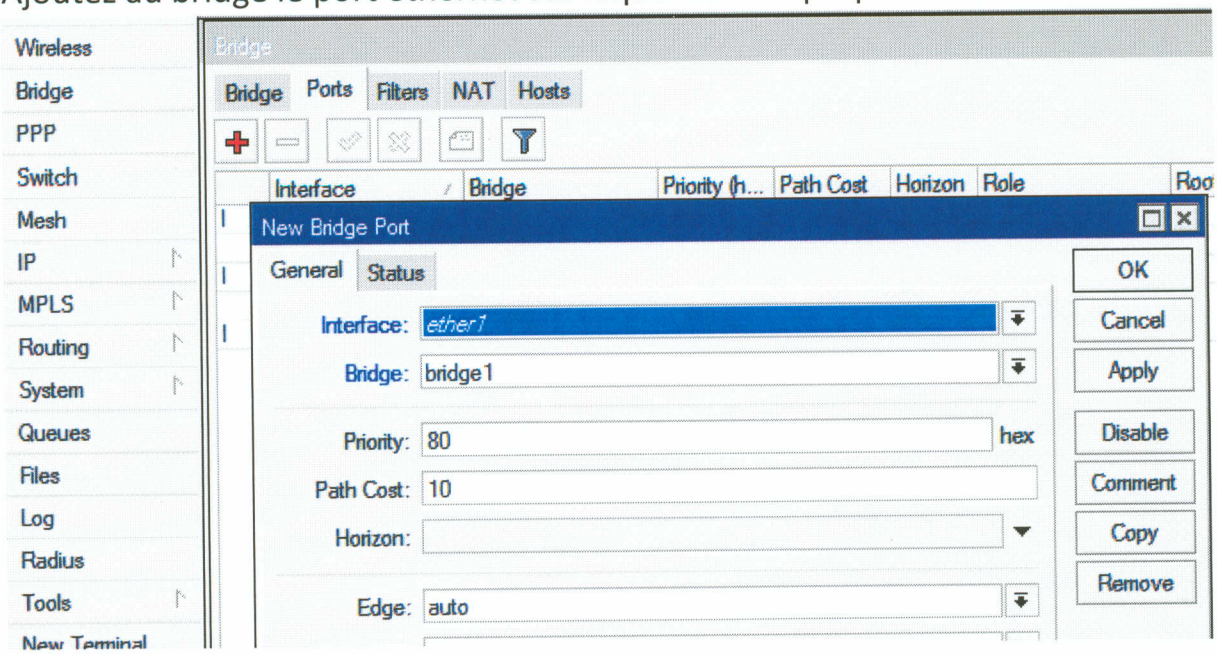


1. Supprimez l'adresse IP, le serveur DHCP et les règles de NAT de votre routeur. Activez le client DHCP sur votre laptop. Connectez-vous au routeur par MAC adresse
2. Ouvrez le menu « Bridge », créez un nouveau bridge

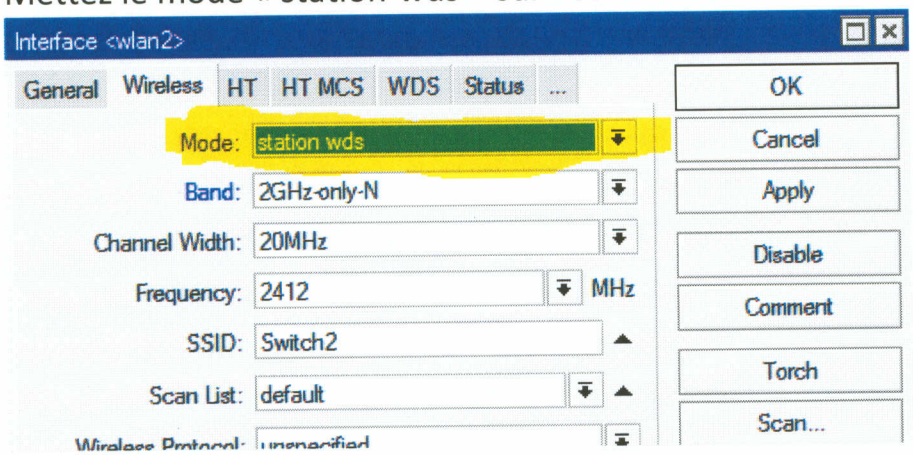


3.

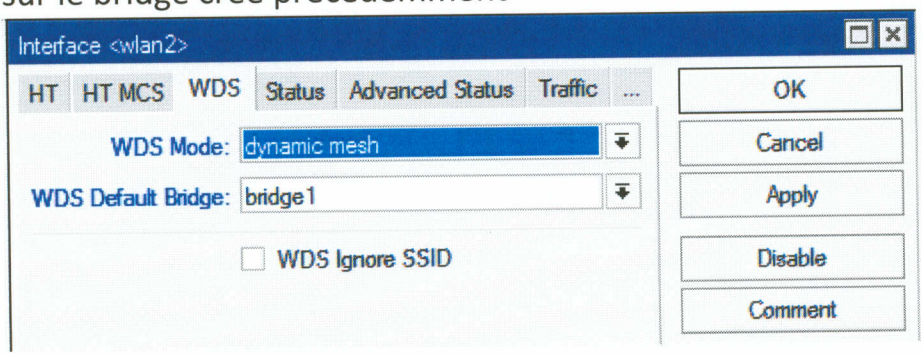
4. Ajoutez au bridge le port ethernet sur lequel votre laptop est connecté



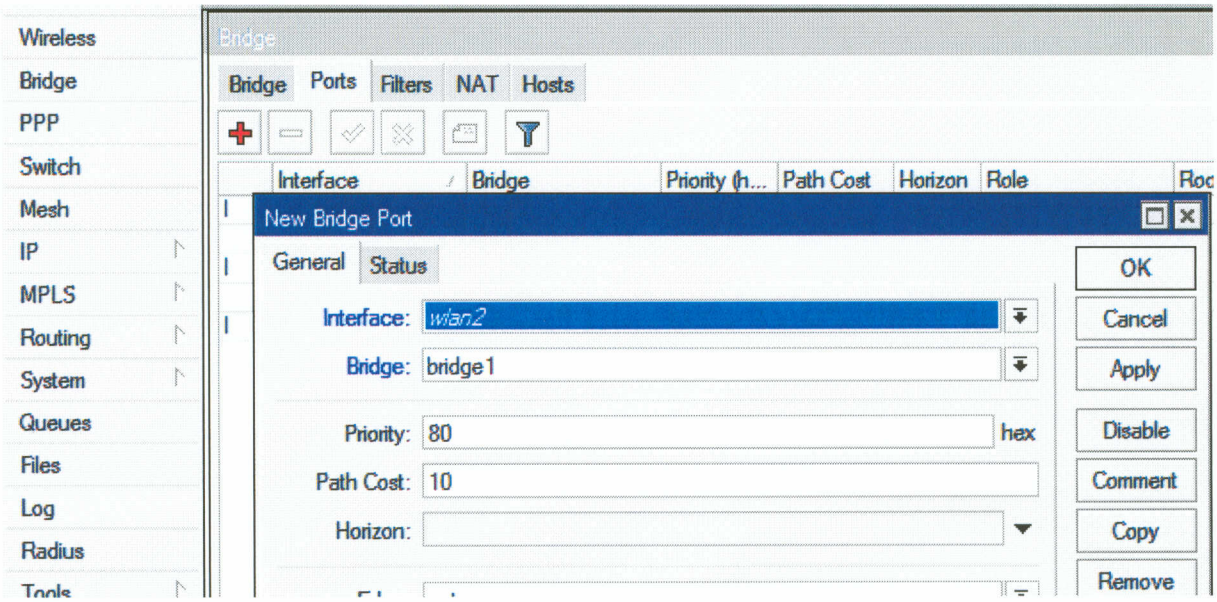
5. Mettez le mode « station-wds » sur votre carte wifi



6. Mettre le mode WDS en tant que « dynamic mesh » et WDS Default Bridge sur le bridge créé précédemment



7. Ajoutez l'interface wlan1 au bridge



8. Renouvelez le bail DHCP sur votre laptop, qu'elle adresse obtenez-vous ?
9. Essayez de faire un ping vers un laptop voisin

DHCP – PARAMETRAGES PERSONNALISES

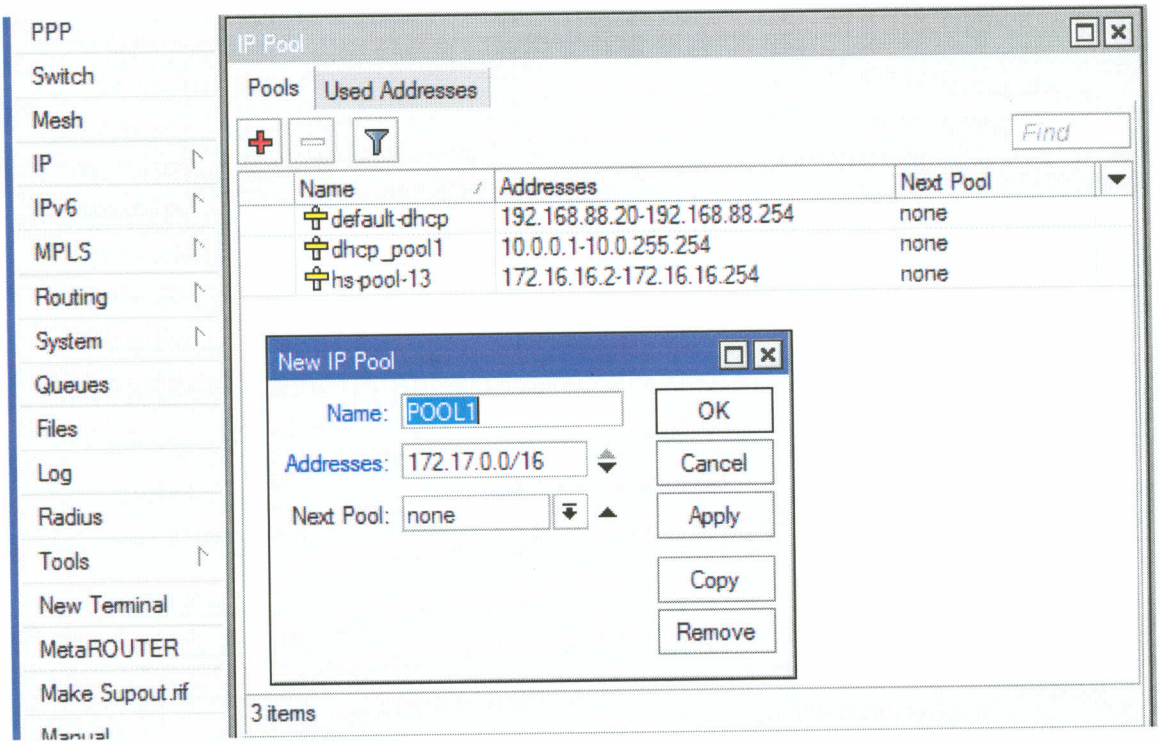
Dans cette configuration, nous allons mettre en place un serveur DHCP qui va distribuer des adresses IP aux clients avec comme spécificités :

- Subnet /32 distribué au client et firewall associé pour interdire la communication IP entre clients.
- Sécurisation du subnet pour autoriser uniquement les clients du serveur DHCP à discuter avec le routeur
- Définir l'adresse du serveur DHCP dans un subnet différent des clients.

Pour atteindre cette configuration, nous n'allons pas utiliser le « DHCP SETUP », mais créer les différents paramètres manuellement.

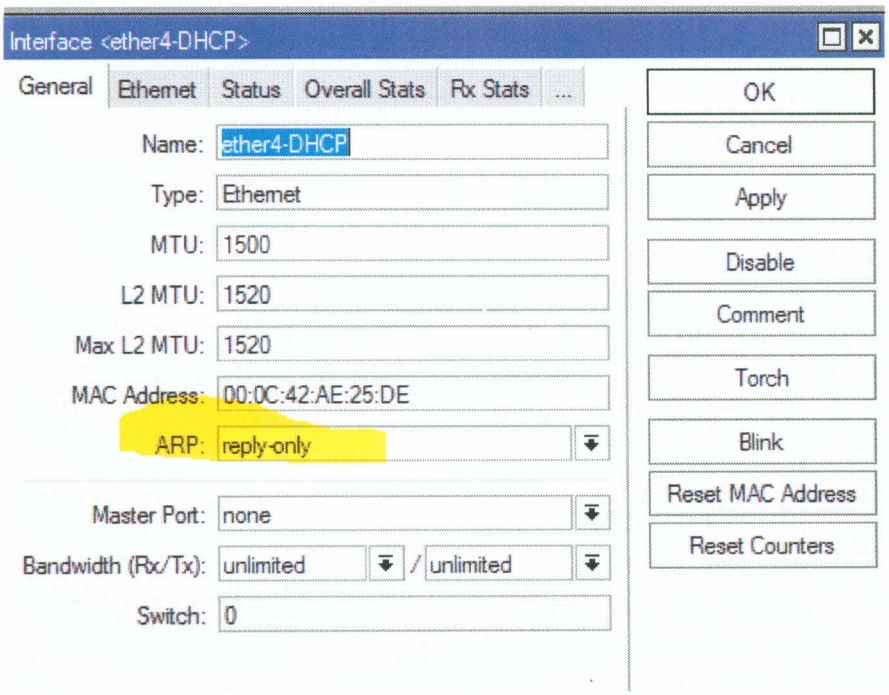
Etape 1 – création d'un pool IP pour les clients :

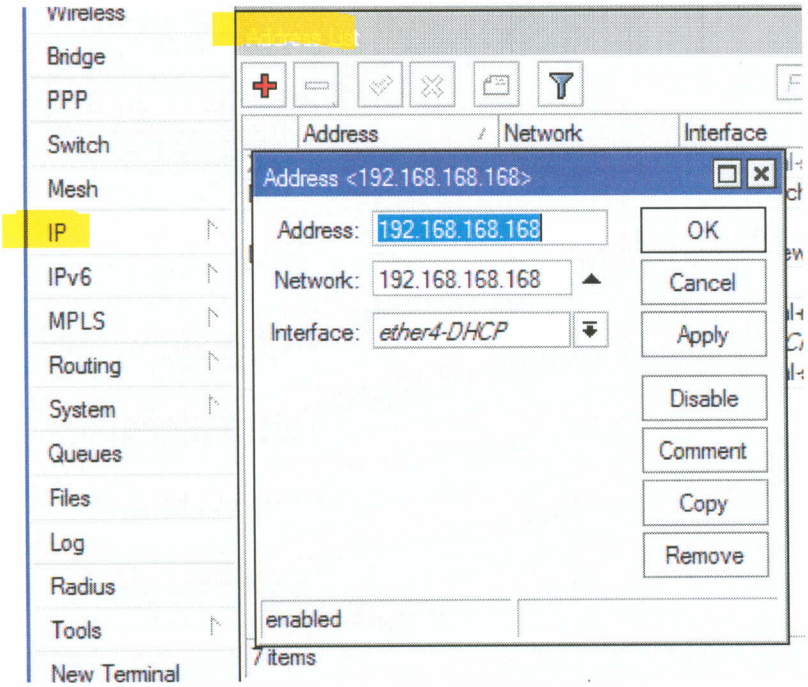
Adresses IP pour les clients de 172.17.0.1 à 172.17.255.254 :



Etape 2 – Assignation d'une adresse IP à l'interface :

Il faut assigner une adresse IP à l'interface sur laquelle va tourner le serveur DHCP. Dans cet exemple nous allons utiliser le port ethernet 4 (sur laquelle on va modifier le comportement ARP – ARP REPLY ONLY) et comme adresse IP : 192.168.168.168 (masque de sous-réseau /32)

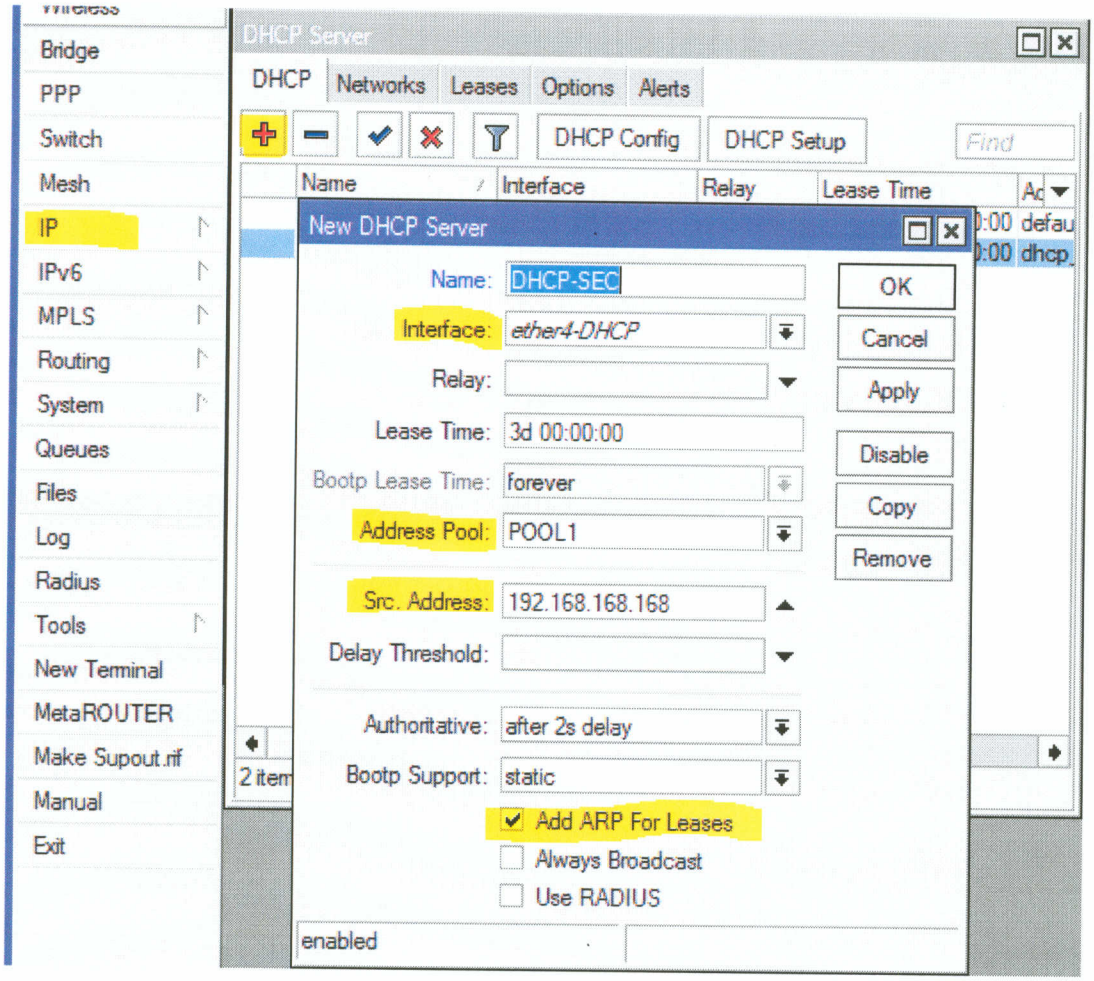




Etape 3 – Ajout du serveur DHCP :

Il faut maintenant créer manuellement un serveur DHCP :

- Interface sur laquelle va tourner le serveur
- Address Pool pour les clients
- Src. Address pour spécifier l'adresse du DHCP serveur qui doit être envoyée
- Add ARP for leases pour créer les associations MAC-ADDRESS – IP dans la table ARP du routeur

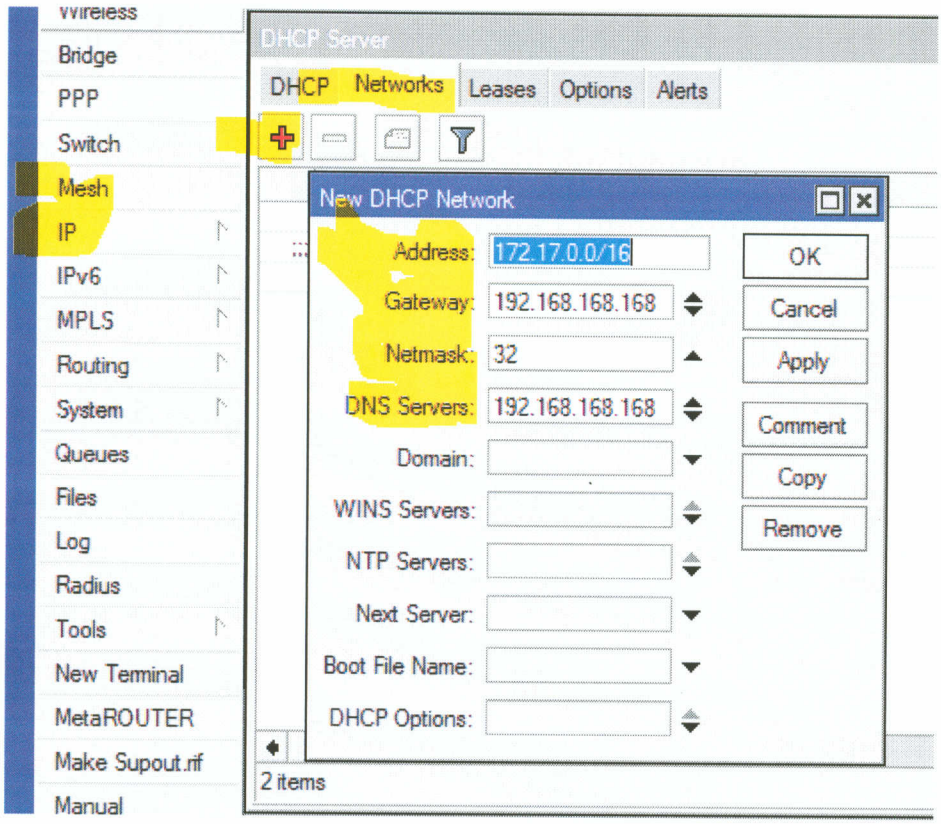


Etape 4 – Spécifier les paramètre clients :

Il faut maintenant spécifier les subnet et passerelle que les clients vont recevoir :

Dans DHCP Server -> Networks – ajoutez un nouveau Network pour préciser les différents paramètres que les clients du range 172.17.0.0/16 doivent recevoir :

- Champs Address (ip des clients)
- Passerelle (le routeur avec son adresse IP)
- Netmask, le subnet /32 pour obliger la communication directe avec la passerelle
- Le serveur DNS

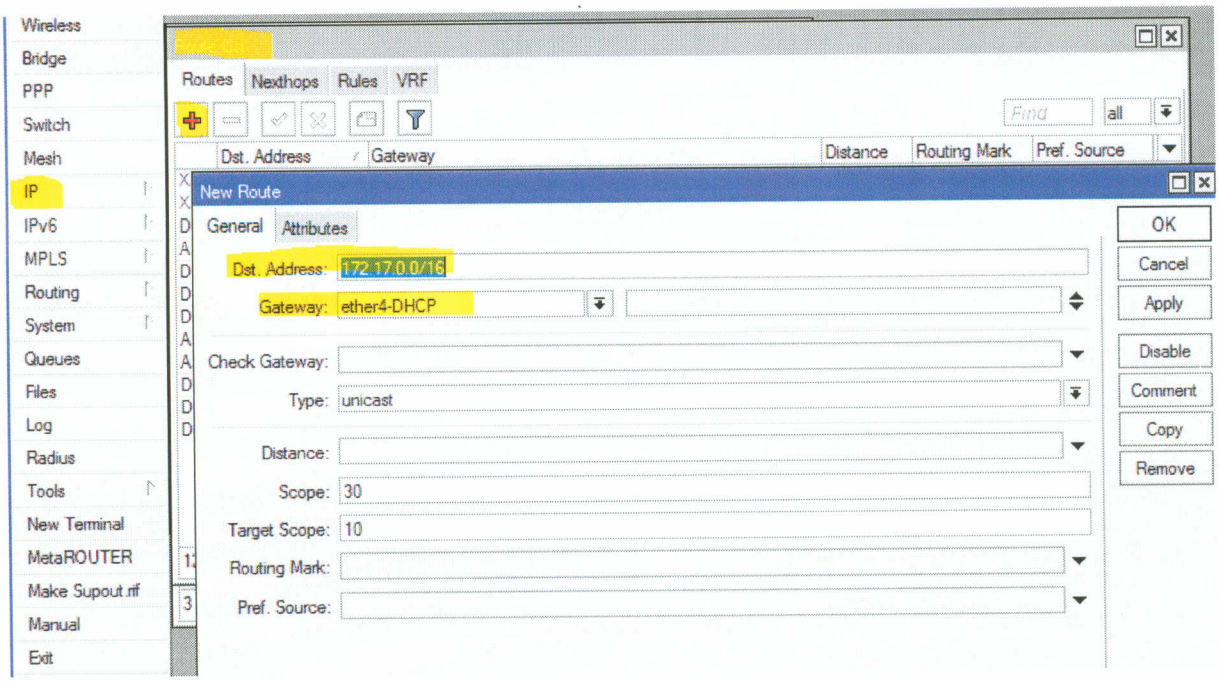


Etape 5 – FINALISATION :

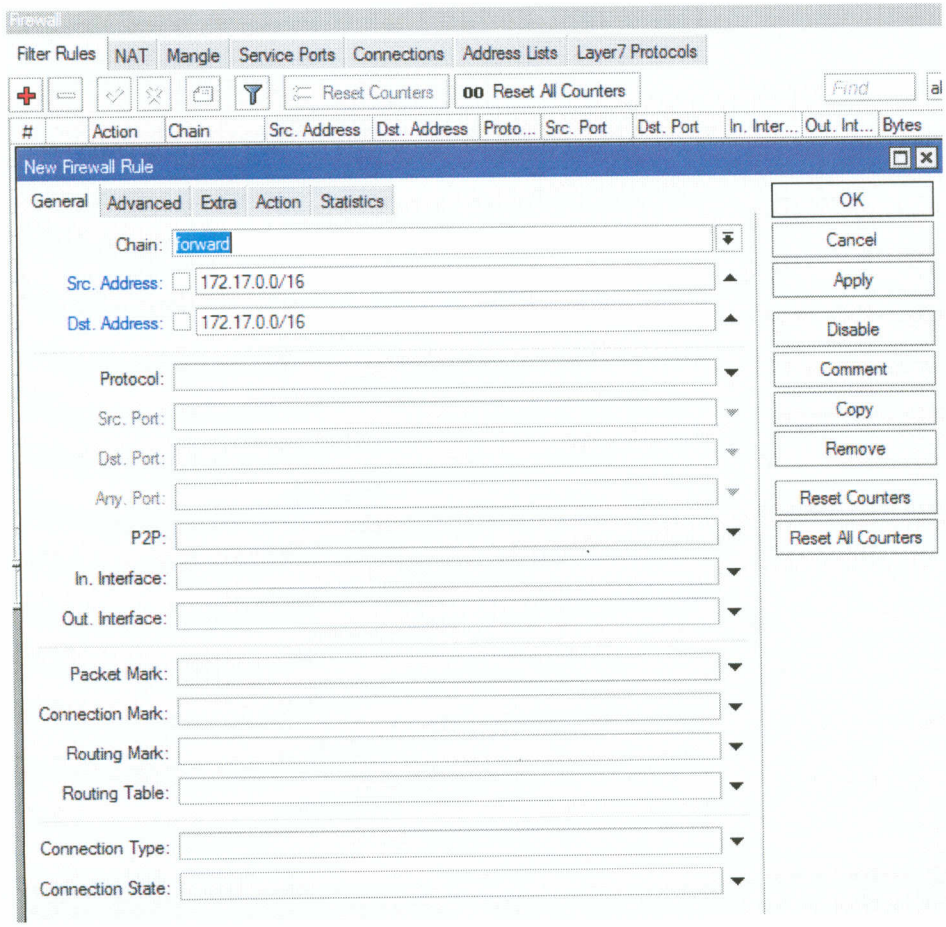
Il reste 2 choses à spécifier :

- Dire au routeur comment joindre le subnet 172.17.0.0/16 (actuellement il n'a pas de route pour joindre ce subnet, la seule route connectée à l'interface ethernet est pour le range 192.168.168.168/32.
- Empêcher la communication des clients en passant par la passerelle. (actuellement il n'y a pas de communication possible directement, mais comme RouterOS est un routeur, il va router les communications entre les clients si on ne l'interdit pas.

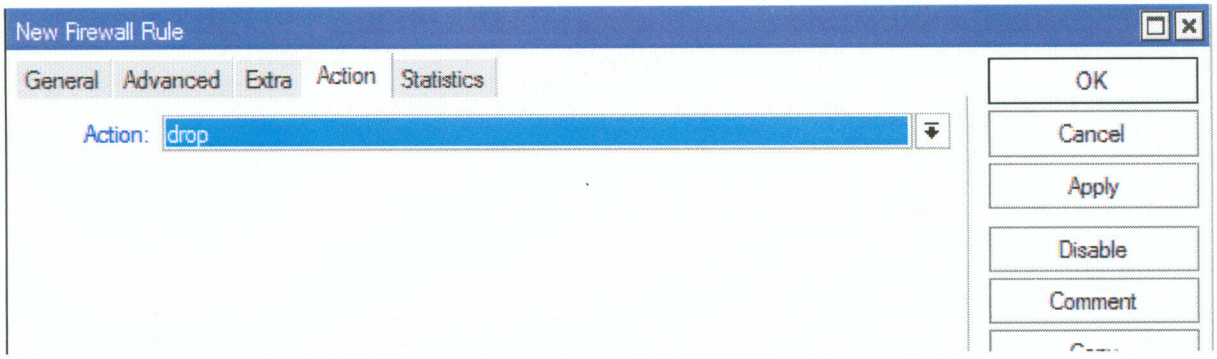
Création d'une route statique vers le subnet 172.17.0.0/16 en utilisant l'interface :



Création d'une règle firewall pour interdire le forward des paquets IP entre les différents clients :



Avec comme action « drop »



Etape 6 – TEST :

Avant de tester la connexion vers internet, vérifiez que vous avez une règle de NAT correcte pour le réseau 172.17.0.0/16

Si l'on connecte un client à l'interface :

```
C:\Users\FUJI>IPCONFIG

Configuration IP de Windows


Carte réseau sans fil Connexion réseau sans fil :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Ethernet Connexion au réseau local :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::7006:1d89:948d:26f
   Adresse IPv4. . . . . . . . . . . . . .: 172.17.255.255
   Masque de sous-réseau. . . . . . . . . : 255.255.255.255
   Passerelle par défaut. . . . . . . . . : 192.168.168.168

Carte Tunnel isatap.{52D68CDF-22D2-4925-91C4-4094033CF52A} :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Tunnel isatap.{7AAD6D3C-676E-4A59-B95B-B104A48B3202} :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Tunnel Teredo Tunneling Pseudo-Interface :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

C:\Users\FUJI>PING 8.8.8.8

Envoi d'une requête 'Ping'  8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=21 ms TTL=45
Réponse de 8.8.8.8 : octets=32 temps=21 ms TTL=45
Réponse de 8.8.8.8 : octets=32 temps=22 ms TTL=45
Réponse de 8.8.8.8 : octets=32 temps=20 ms TTL=45

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 20ms, Maximum = 22ms, Moyenne = 21ms

C:\Users\FUJI>
```

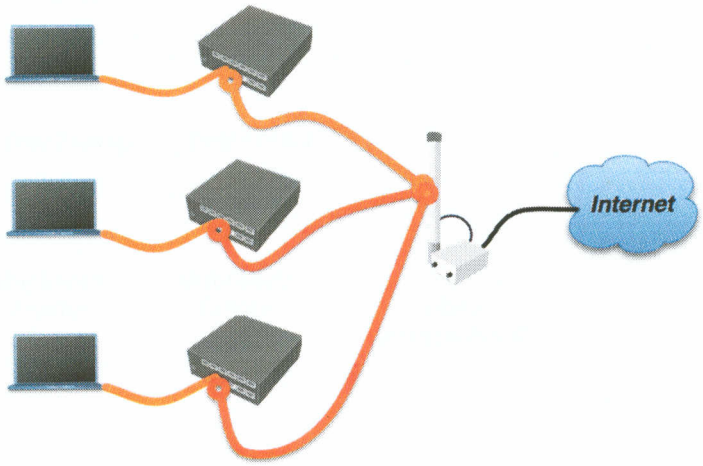
Donc cela fonctionne.

Module 8 – VPN et tunnels

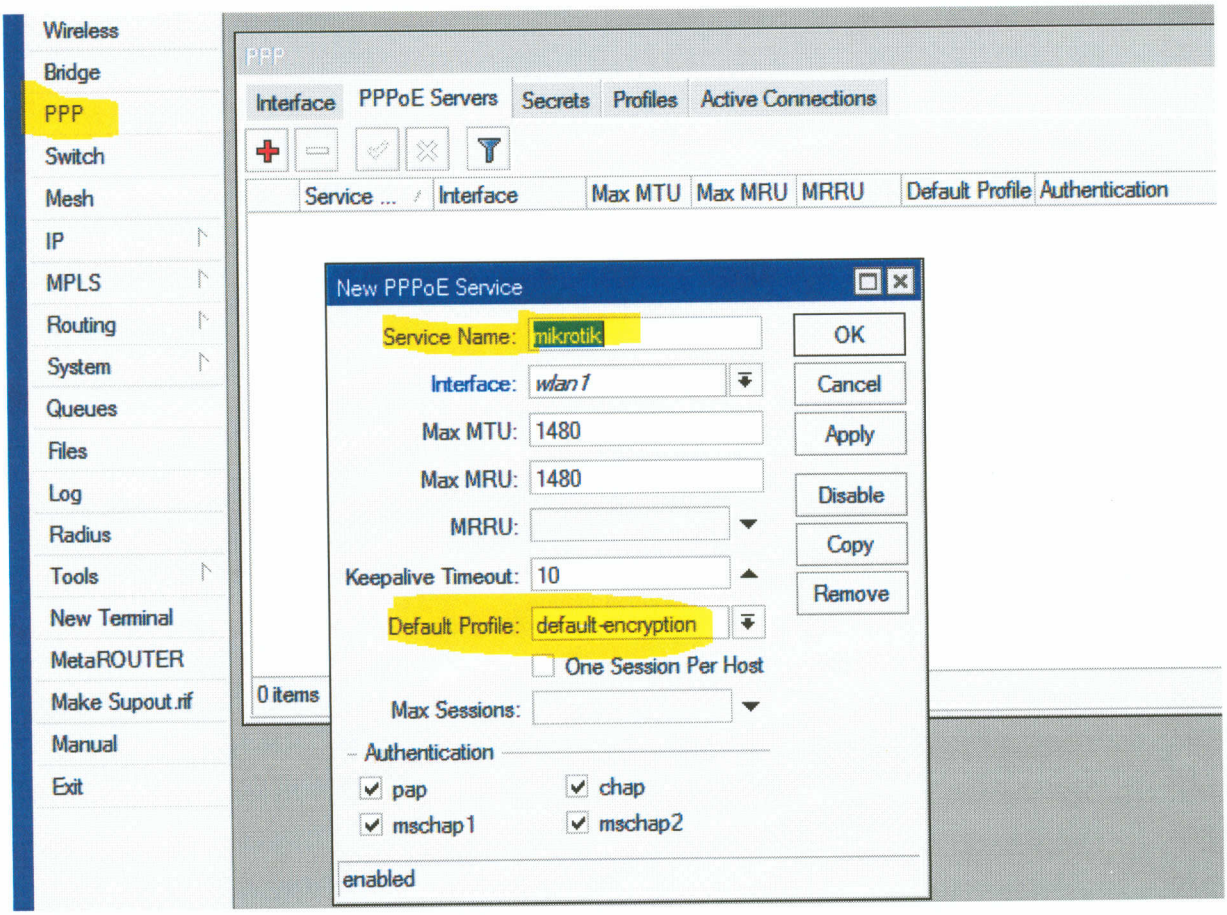
Dans ces exercices, nous allons installer les fonctionnalités PPPoE et PPTP.

Exercice 8.1 – PPPoE SERVEUR

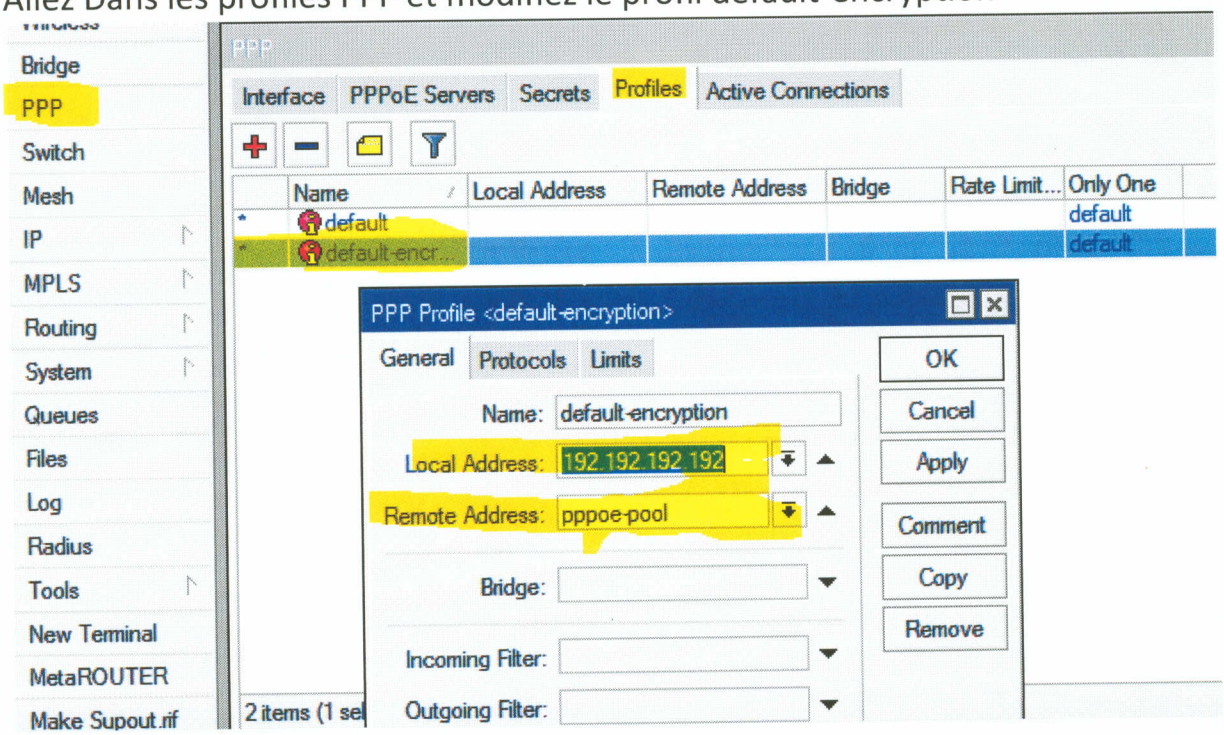
PPPoE serveur – (Démonstration sur routeur principal)



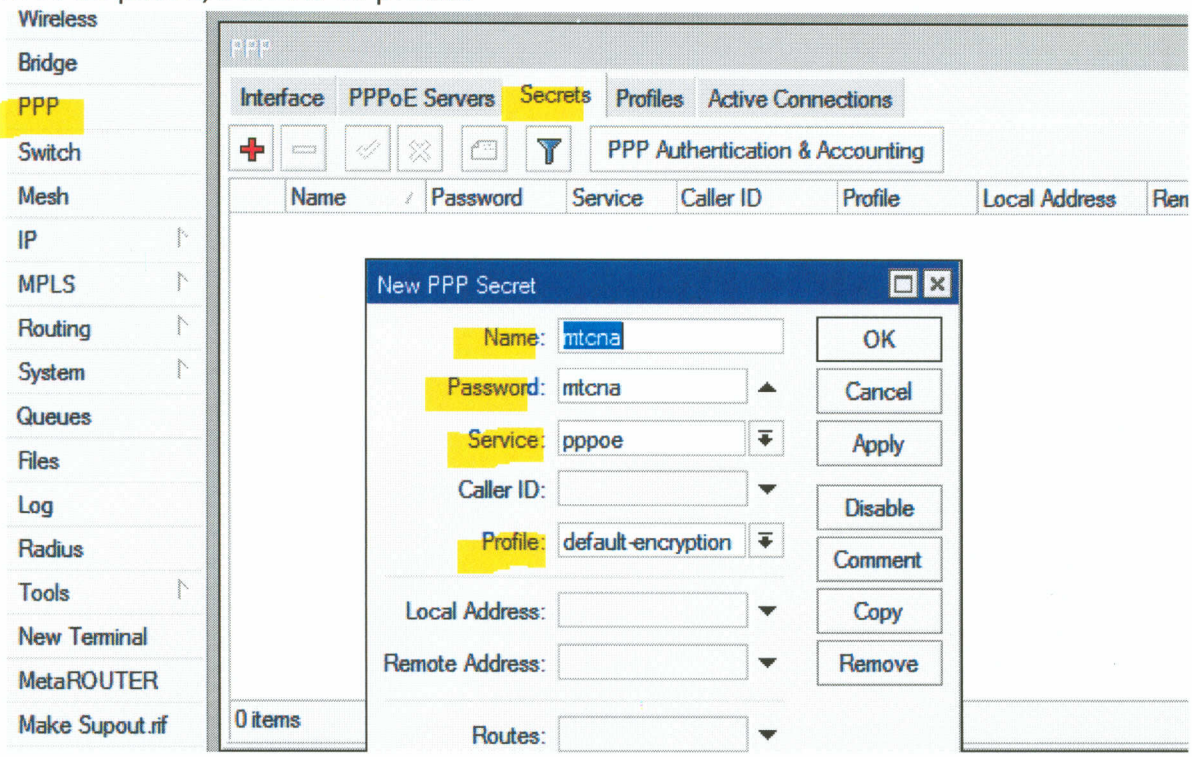
1. Supprimez l'adresse IP, et les services de l'interface sur laquelle le serveur PPPoE va être installé.
2. Ouvrez le menu « PPP », -> PPPoE Servers, et ajoutez un nouveau PPPoE service , Nous allons utilisez comme « Service name » = mikrotik.



3. Créez un pool IP pour les clients du service PPPoE (192.168.222.5-192.168.222.20)
4. Allez Dans les profiles PPP et modifiez le profil default-encryption



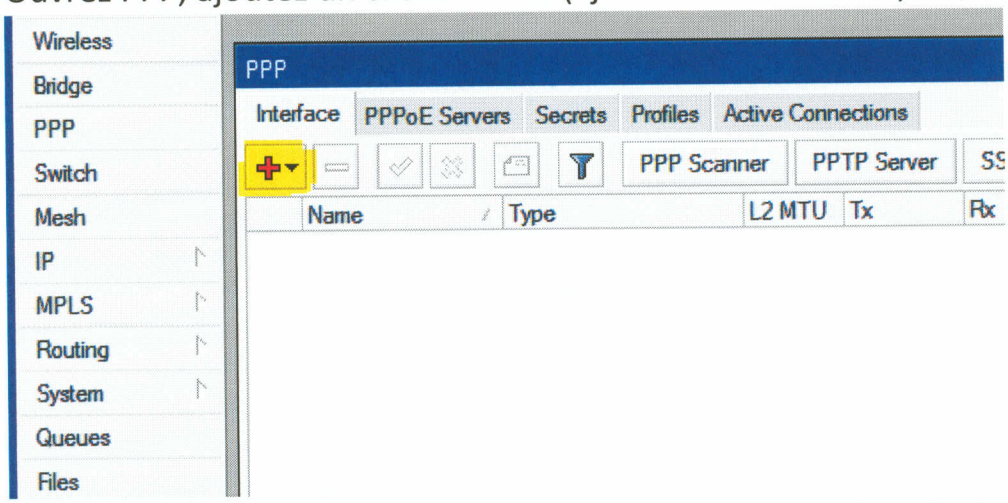
5. Ouvrez PPP -> Secrets, ajoutez un utlisateur et spécifiez le nom d'utilisateur, mot de passe, service et profile



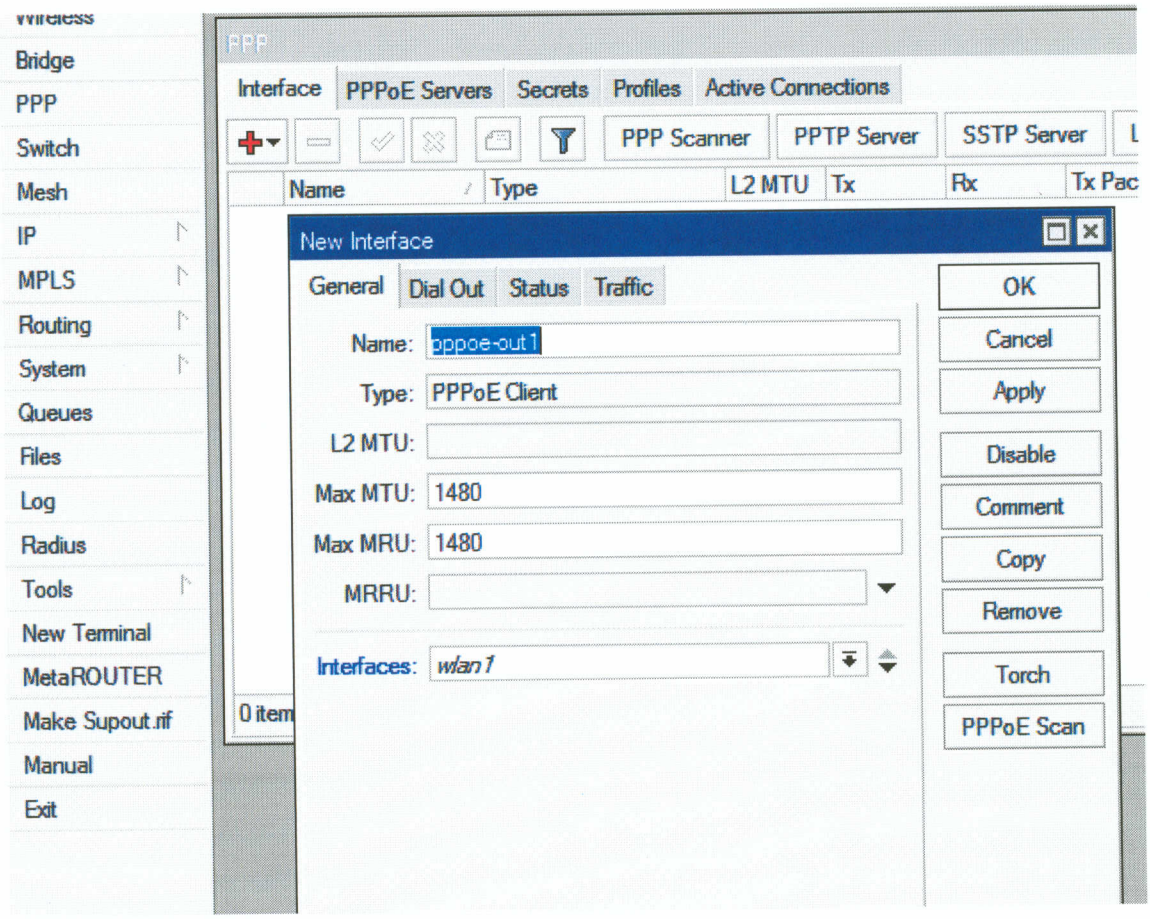
6. Ouvrir PPP, Active connections et attendre sur les connections des clients

Exercice 8.2 – PPPoE client

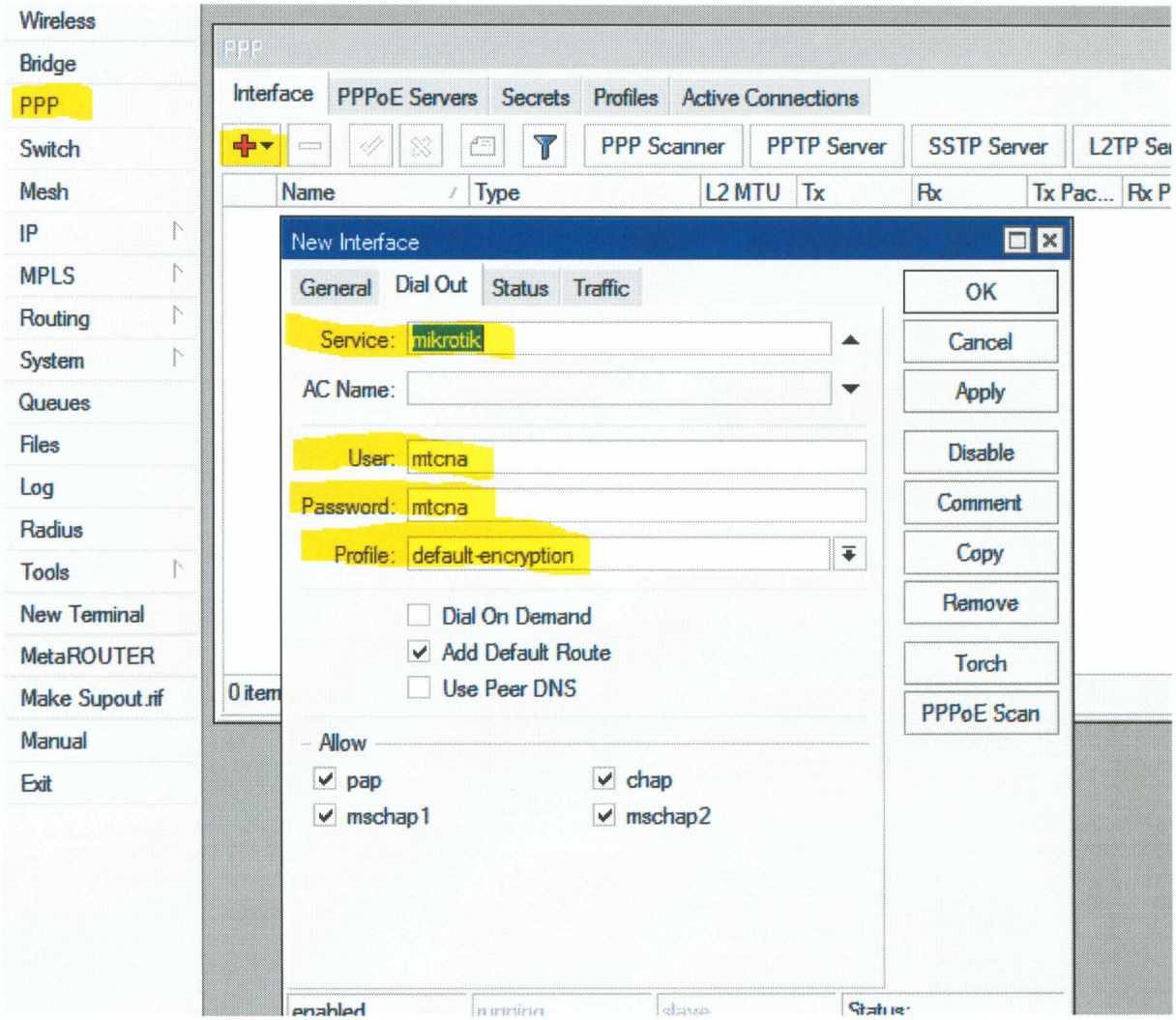
1. Désactiver l'adresse IP et le client DHCP sur l'interface WLAN1
2. Ouvrez PPP, ajoutez un client PPPoE (ajoutez une interface)



3. Vous avez à spécifiez l'interface su laquelle va tourner le PPPoE client



4. Il faut aussi mettre le service (mikrotik) l'utilisateur (mtcna) ainsi que le mot de passe (mtcna) et le bon profile



5. Vérifiez si vous obtenez une adresse IP
6. Vérifiez les routes et la connectivité internet