# MikroTik RouterOS Formation

# MTCNA

7 – 9 décembre 2015, Genève

## Instructeur: Philippe ROBERT

MTCNA – Mikrotik Certified Network Associate

MTCRE – Mikrotik Certified Routing Engineer

MTCTCE – MikroTik Certified Traffic Control Engineer

MTCUME – MikroTik Certified User Manager Engineer

MTCWE – MikroTik Certified Wireless Engineer

MTCINE – MikroTik Certified Internetworking Engineer

MTCT – MikroTik Certified Trainer

Microsoft - MCSE – MCSA

VMWARE – VCP

*Contact: p.robert@engitech.ch - +41798529670*

## Horaires

- Horaires : 9h00 – 17h00
- Pauses : 10h30 et 15h00
- Repas : 12h30 -13h30



## Objectifs du cours

- Aperçu du logiciel RouterOS ainsi que des possibilités des Routerboard
- Exercices pratiques sur la configuration des routeurs MikroTik, ainsi que sur le management et le dépannage



## Contenu du cours

Module 1 – MikroTik RouterOS Introduction

Module 2 – MikroTik RouterOS Firewall

Module 3 – MikroTik RouterOS QoS

Module 4 – MikroTik RouterOS Network Management

Module 5 – MikroTik RouterOS Wireless

Module 6 – MikroTik RouterOS Bridging

Module 7 – MikroTik RouterOS Routing

Module 8 – MikroTik RouterOS Tunnels

## A propos de MikroTik

- Fabricant de matériel et aussi développeur logiciel
- Les produits de MikroTik sont aussi bien utilisés par des ISPs, des entreprises et des particuliers
- Les produits développés par MikroTik sont puissants, rapides et abordables



## MikroTik

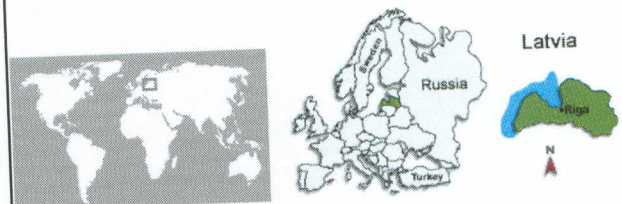
- 1995: Création de la société
- 1997: RouterOS software pour x86 (PC)
- 2002: RouterBOARD
- 2006: Premier MUM (MikroTik User Meeting)

# MikroTik sur la toile ?

- www.mikrotik.com
- www.routerboard.com
- mum.mikrotik.com
- wiki.mikrotik.com
- forum.mikrotik.com



# Où se trouve MikroTik ?




RIGA, Lettonie, Europe du nord, EU



# Présentez-vous

- Votre nom
- Votre compagnie
- Vos connaissances actuelles de RouterOS
- Votre expérience actuelle sur le réseau
- Quelles sont vos attentes pour ce cours

Retenez votre numéro X pour le cours : _____



# MikroTik RouterOS



# Qu'est-ce que RouterOS ?

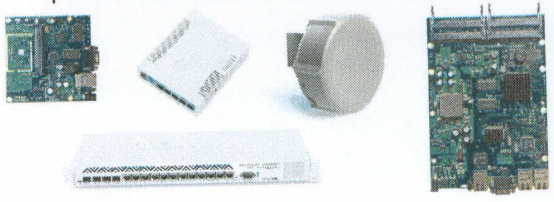
RouterOS est un système d'exploitation qui fonctionne sur plateforme x86 et Routerboard. Il fera fonctionner votre appareil comme:

- un routeur dédié
- un régulateur de bande-passante
- un analyseur de paquet (firewall)
- un appareil sans fil (ap, client,…) en 802.11a,b/g,n et protocoles Mikrotik

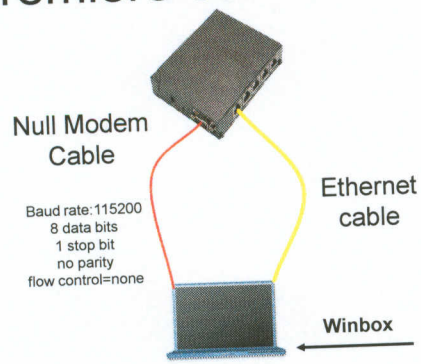


# RouterBOARD ?

- Matériel créé par MikroTik
- Une gamme étendue qui va du routeur personnel au concentrateur pour ISP



# Première connection



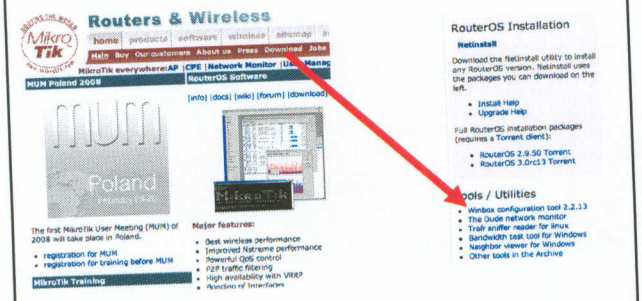

14

# Winbox

- L'application pour configurer RouterOS
- Il peut être téléchargé depuis le site www.mikrotik.com ou depuis la page web du routeur
- Il utilise les protocoles suivant pour se connecter: **TCP port 8291** ou **MAC-telnet**

15

# Télécharger Winbox

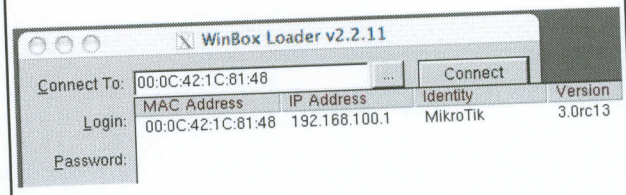



16

# Se connecter au routeur

LAB

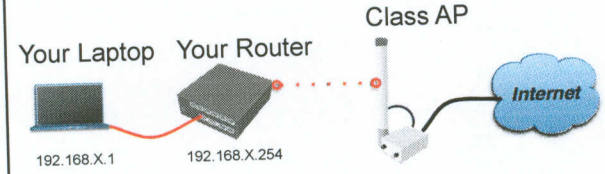
Cliquez sur le boutton [...] pour voir votre routeur




17

# Accéder à internet via le routeur

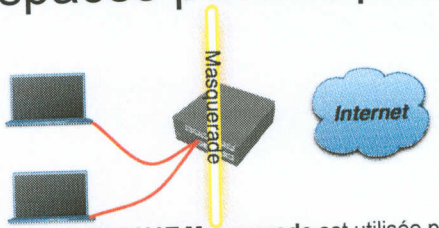
LAB




DHCP-Client sur la connection sans-fil
DNS serveur configuré sur le routeur

18

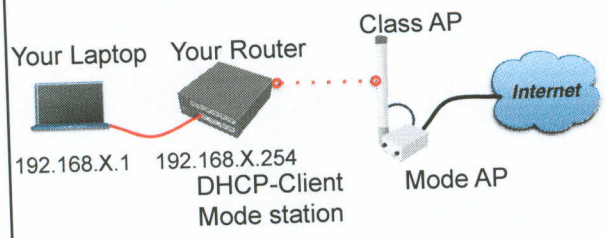
# Espaces privé et public




- **La fonctionnalité NAT Masquerade** est utilisée pour accéder à des réseaux publics depuis un réseau utilisant des adresses privées
- Les réseaux privés incluent les espaces suivants: 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255

19

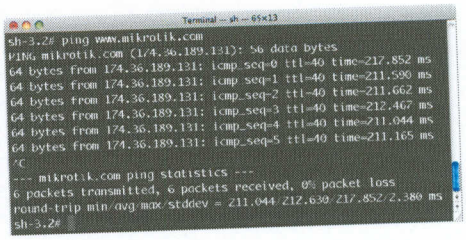
# Diagramme du réseau






# Vérifier la connectivité

Faire un Ping de www.mikrotik.com depuis votre laptop






# Erreurs possibles

- Le ping du routeur s'arrête au point d'accès
- Le routeur ne peut pas résoudre les noms
- Le laptop ne peut pas faire un ping au-delà du routeur
- Le laptop ne peut pas résoudre les noms
- Est-ce que la règle Nat Masquerade fonctionne?
- Est-ce que le laptop utilise le routeur comme passerelle par défaut et comme serveur DNS?

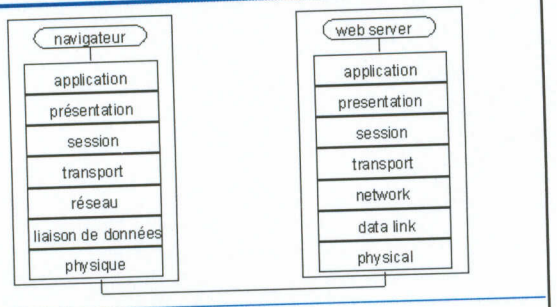


# Communication

- Le processus de communication est divisé en 7 couches
- La plus basse est la couche physique, la plus haute la couche applicative



## Les 7 couches du modèle OSI




# MAC address

- Il s'agit de l'adresse matérielle d'un appareil réseau – elle est unique
- Elle est utilisée pour la communication à l'intérieur d'un réseau
- Exemple: 00:0C:42:20:97:68

# IP

- Il s'agit de l'adresse logique d'un appareil réseau
- Elle est utilisée pour la communication entre réseaux
- Exemple: 159.148.60.20

26

# Sous-réseau

- Etendue d'adresses IP qui divise le réseau en segment
- Exemple: 255.255.255.0 ou /24

27

# Sous-réseau

- L'adresse du réseau est la première adresse du sous-réseau
- L'adresse de Broadcast est la dernière adresse du sous-réseau
- Elles sont réservées et ne peuvent pas être utilisées

Exemples:

adresse IP d'un appareil: 192.168.80.5/24

adresse du réseau: 192.168.80.0

adresse de Broadcast: 192.168.80.255

28

Calculation des sous-réseaux et des adresse disponibles.

**Outil sur internet:**

http://www.subnet-calculator.com/

**Outil windows:**

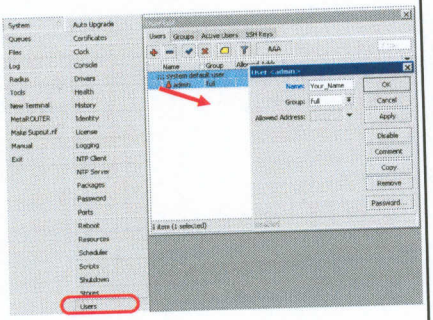
Advanced IP Address Calculator
http://www.radmin.fr/products/utilities.php

| CIDR | Subnet Mask | Available Hosts |
|---|---|---|
| /32 | 255.255.255.255 | |
| /30 | 255.255.255.252 | 4-2 |
| /29 | 255.255.255.248 | 8-2 |
| /28 | 255.255.255.240 | 16-2 |
| /27 | 255.255.255.224 | 32-2 |
| /26 | 255.255.255.192 | 64-2 |
| /25 | 255.255.255.128 | 128-2 |
| /24 | 255.255.255.0 | 256-2 |

29

# Gestion des utilisateurs du routeur

- Les accès au routeur peuvent être contrôlés
- Différents types d'utilisateurs peuvent être créés



30

LAB

# Gestion des utilisateurs

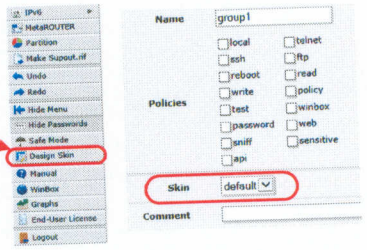
- Ajoutez un utilisateur avec les droits d'accès complet
- Soyez certains de vous rappeler de son nom et mot de passe
- Modifiez l'utilisateur admin en lecture seule
- Ouvrez une session sur le routeur avec le nouvel utilisateur

31

# Gestion des utilisateurs WEBFIG

"DESIGN SKIN"

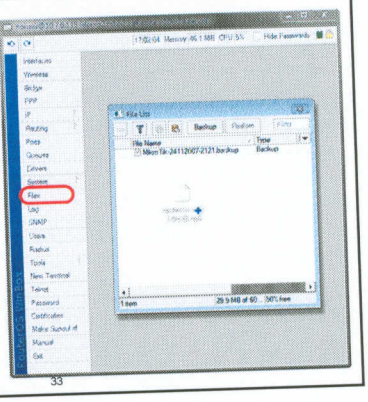
- Un interface specifique peut-être attribué à chaque utilisateur
- Mettre l'utilisateur dans le groupe et associé l'interface associée






# Mise à jour du Routeur

- Utilisez le package upgrade de RouterOS
- Glissez le fichier dans la fenêtre "Files"





LAB

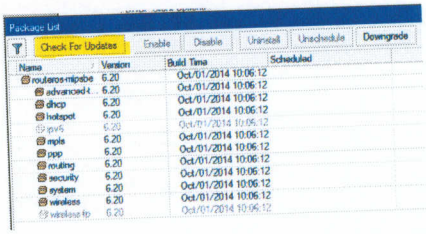
# Mise à jour du Routeur

- Téléchargez les paquets logiciels depuis ftp://192.168.200.254
- Transférez le paquet sur le routeur avec Winbox
- Redémarrez le routeur
- Les paquets logiciels les plus récents sont toujours disponibles sur www.mikrotik.com



# Maj(automatique) en V6

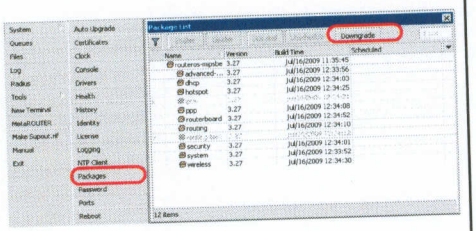
- System -> Packages -> Check for Updates






# Rétrograder le Routeur

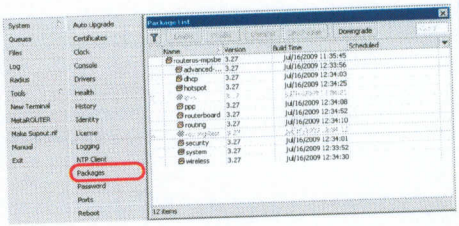
Si, pour une raison, vous devez revenir à une version précédente de RouterOS, il faut transférer le fichier RouterOS puis cliquer sur "Downgrade"






# Management des fonctionnalités

Les différentes fonctions de RouterOS sont activées par des paquets logiciels



# Information

| Name | Functions |
|---|---|
| advanced-tools | Email client, ping, netwatch |
| dhcp | DHCP Server and Client |
| hotspot | HotSpot Gateway |
| ntp | NTP server |
| ppp | PPP, PPTP, L2TP, PPPoE |
| routerboard | RouterBOARD specific functions |
| routing | RIP, OSPF, BGP |
| security | Secure Winbox, SSH, IPSec |
| wireless | Wireless 802.11a/b/g |
| user-manager | User-Manager management system |
| ipv6 | IPv6 |

Tous les paquets logiciels sont fait par MikroTik

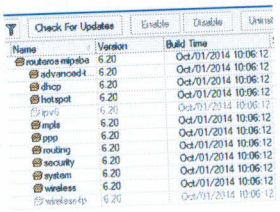
**Seul MikroTik** fait ces packages – il n'existe pas d'autres add-on ou drivers que l'on peut ajouter

Important:
le paquet system inclut le routage statique



# Information (2)

Paquets par défaut:




2 paquets wireless:

Seulement 1 des 2 peut-être activer à la fois

wireless-fp, nouvelles fonctionalités wireless:

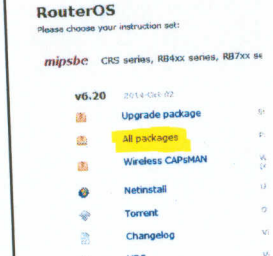
- Support 802.11ac
- Nécessaire pour Capsman

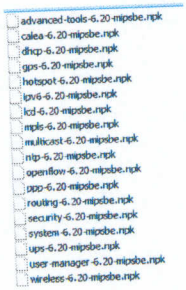


# Information (3)

Besoins d'autres paquets?

-> téléchargeable sur le site de MikroTik






LAB

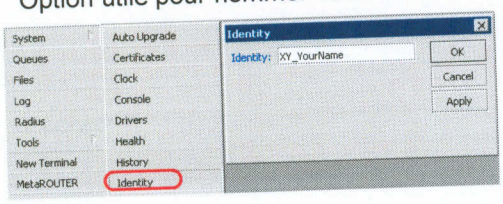
# RouterOS

- Désactivez le paquet wireless
- Redémarrez le routeur
- Vérifiez la liste des interfaces
- Réactivez le paquet wireless et redémarrez le routeur



# Router Identity

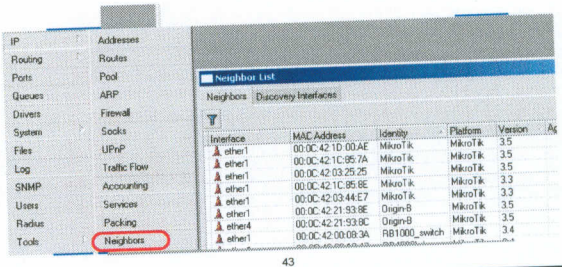
Option utile pour nommer votre routeur






# Routeur Identity

Cette information se retrouve à plusieurs endroits



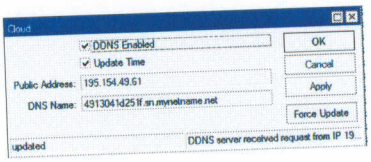
# Router Identity

LAB

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



# DDNS: IP -> CLOUD




- Client DDNS intégré à RouterOS
- Directement activable, permet de savoir l'ip adresse externe

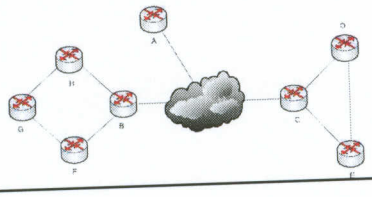


# ROMON

Router Management overlay Network

Nouvelle possibilité pour manager les routeurs (v.6.28)

**Permet de créer un ensemble de routeurs managés**

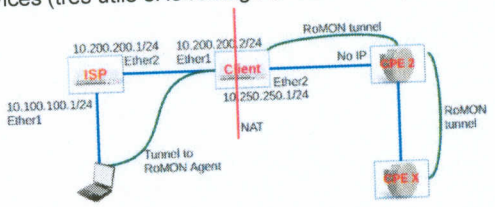



# ROMON

Utilise un protocole propriétaire de Mikrotik

Management par Ping, SSH et Winbox (version 3.x)

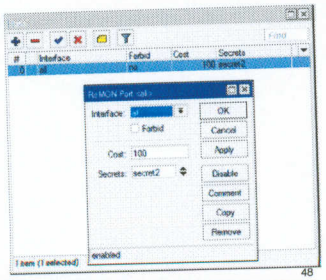
Uniquement besoin d'une connection layer 2 entre les devices (très utile si le routage IP est non disponible)

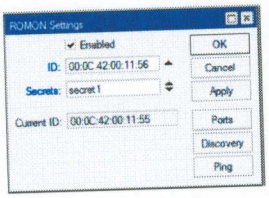





# ROMON

Tools -> ROMON pour l'activer



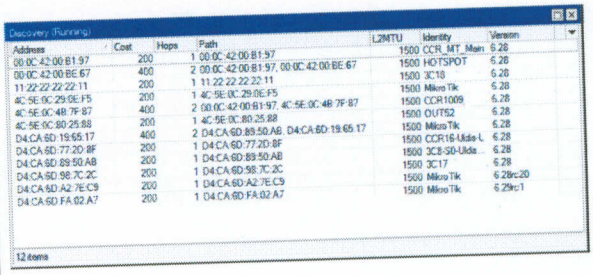




Permet de choisir sur quelle interface il fonctionne et une sécurité



# ROMON

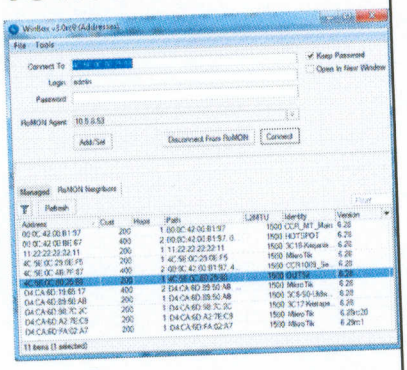
Discovery:



# ROMON

Depuis winbox:

1) Se connecter au routeur distant par RoMON
2) Choisir le routeur sur lequel on va se connecter via cette connection RoMON en précisant le mode de passe winbox du routeur de destination





# NTP

- Network Time Protocol, pour synchroniser l'heure
- RouterOS supporte les fonctionnalités NTP Client et NTP Serveur
- NTP Client est inclus dans le paquet system
- **NTP Serveur nécessite le paquet NTP**



# Pourquoi utiliser NTP ?

- Pour avoir l'heure correcte
- Pour toutes les cartes RouterBOARDs, aucun routeur fabriqué par MikroTik n'a de "pile" système
- Nécessaire pour avoir des logs lisibles, négociation ipsec, …

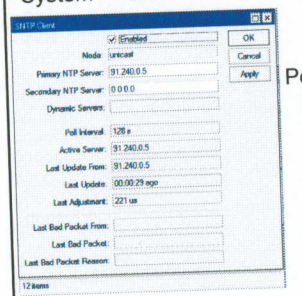


# SNTP Client

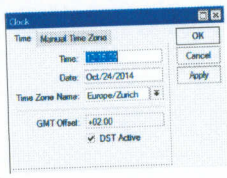
LAB

2 paramètres à configurer:

System -> SNTP Client:



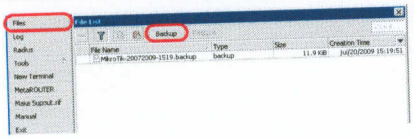
Pour modifier la "time zone", il faut le faire dans System -> clock





# Configuration des Backups

- Vous pouvez créer une sauvegarde et restaurer la configuration dans le menu "Files" de Winbox
- Les fichiers de Backup ne sont pas modifiables





# Configuration des Backups

- En plus, utilisez les commandes "export" et "import" en ligne de commande
- Les fichiers "export" sont modifiables
- Les mots de passe ne sont pas sauvés dans le fichier "export"

```
/export file=conf-august-2012
/ ip firewall filter export file=firewall-aug-2012
/ file print
/ import [Tab]
```

# Backup

LAB

- Créez les fichiers Backup et Export
- Transférez les fichiers sur votre laptop
- Ouvrez les fichiers dans un éditeur de texte



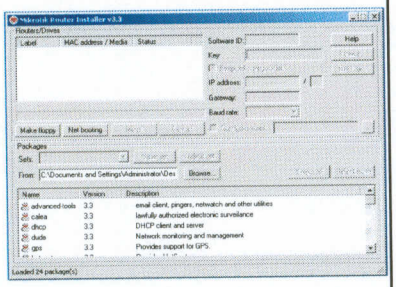
# Netinstall

- Netinstall est un programme qui permet d'installer et de réinstaller RouterOS
- Fonctionne uniquement sur Windows
- Une connection réseau directe au routeur est nécessaire
- Disponible sur le site www.mikrotik.com



# Netinstall

1. Net booting
2. Liste des routeurs
3. Keep old configuration
4. Packages
5. Install






# Netinstall
## (exercice facultatif)

LAB

- Téléchargez Netinstall depuis ftp://192.168.100.254
- Lancez Netinstall
- Activez le démarrage sur réseau (Net booting) en mettant comme adresse 192.168.x.13
- Utilisez un cable null modem et Putty pour se connecter
- Paramétrez le routeur pour qu'il démarre sur le réseau

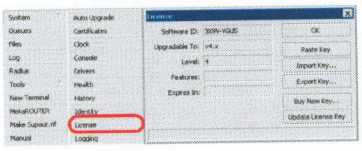


# RouterOS Licence

- Toutes les cartes RouterBOARDs sont livrées avec une licence
- Plusieurs niveaux de licence sont disponibles, il n'y a pas d'upgrade
- La licence installée peut être vue dans le menu system -> license
- Les licences pour X86 peuvent être achetées sur http://www.mikrotik.com ou chez les distributeurs



# Licence



# Licence

| Level number | 0 (Demo mode) | 1 (Free) | 3 (WISP CPE) | 4 (WISP) | 5 (WISP) | 6 (Controller) |
|---|---|---|---|---|---|---|
| Price | no key | registration required | volume only | $45 | $95 | $250 |
| Upgradable To | - | no upgrades | ROS v6.x | ROS v6.x | ROS v7.x | ROS v7.x |
| Initial Config Support | - | - | - | 15 days | 30 days | 30 days |
| Wireless AP | 24h trial | - | - | yes | yes | yes |
| Wireless Client and Bridge | 24h trial | - | yes | yes | yes | yes |
| RIP, OSPF, BGP protocols | 24h trial | - | yes(*) | yes | yes | yes |
| EoIP tunnels | 24h trial | 1 | unlimited | unlimited | unlimited | unlimited |
| PPPoE tunnels | 24h trial | 1 | 200 | 200 | 500 | unlimited |
| PPTP tunnels | 24h trial | 1 | 200 | 200 | 500 | unlimited |
| L2TP tunnels | 24h trial | 1 | 200 | 200 | 500 | unlimited |
| OVPN tunnels | 24h trial | 1 | 200 | 200 | unlimited | unlimited |
| VLAN interfaces | 24h trial | 1 | unlimited | unlimited | unlimited | unlimited |
| HotSpot active users | 24h trial | 1 | 1 | 200 | 500 | unlimited |
| RADIUS client | 24h trial | - | yes | yes | yes | yes |
| Queues | 24h trial | 1 | unlimited | unlimited | unlimited | unlimited |
| Web proxy | 24h trial | - | yes | yes | yes | yes |
| User manager active sessions | 24h trial | 1 | 10 | 20 | 50 | Unlimited |
| Number of KVM guests | none | 1 | Unlimited | Unlimited | Unlimited | Unlimited |



# Résumé



# Firewall



# Firewall

- Protège votre routeur et les clients d'accès non autorisés
- Pour réaliser cela, il faut créer des règles dans les sections "Firewall Filter" et "NAT"



# Firewall Filter

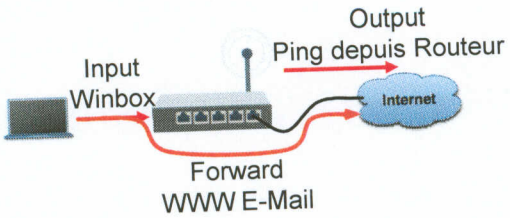
- Consiste en des règles définies par l'utilisateur et fonctionne sur le principe **IF-Then** (si l'objet de la règle est correct – alors -> action)
- Ces règles sont organisées en chaînes
- Il existe 2 sortes de chaînes: les chaînes prédéfinies et les chaînes créées par l'utilisateur



# Chaînes de filtrage

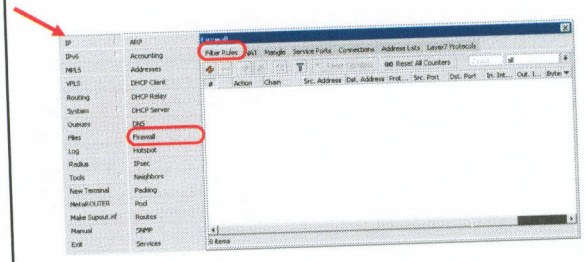
- Les règles peuvent être placées dans 3 chaînes par défaut
  - input (**paquets qui arrivent pour le routeur**)
  - output (**paquets générés par le routeur**)
  - forward (**paquets qui passent à travers le routeur**)

# Chaînes du Firewall






# Chaînes du Firewall






# Input

- Chaînes contenant des règles qui protègent le **routeur lui-même**
- L'ordre des règles est important



# Input Lab

LAB

- Modifiez l'adresse IP de votre laptop en 192.168.x.10
- Essayez de vous connecter -> le firewall fonctionne
- Vous pouvez toujours vous connecter au routeur par MAC-address
  Les règles définies dans "Firewall Filter" sont seulement pour le protocole IP
- Pouvez-vous atteindre internet ?



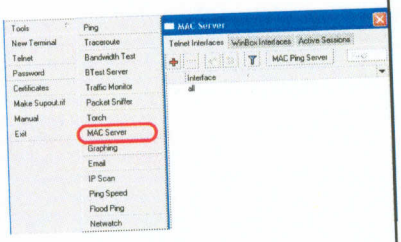
# Input

- L' accès à votre routeur est bloqué
- Internet ne fonctionne pas parce que les requêtes DNS sont aussi bloquées
- Modifiez la configuration pour que l'accès à internet fonctionne



# Input

- Vous pouvez désactiver l'accès par MAC-address dans le menu "Tools"
  **"MAC Server"**
- Modifiez l'adresse IP de votre laptop de nouveau en 192.168.X.1, et connectez-vous par IP



# Forward

- Chaînes contenant des règles qui contrôlent les paquets passant **à travers** le routeur
- Contrôle le trafic **vers et depuis les clients**



# Forward

LAB

- Créez des règles dans la chaîne Forward
- Essayez d'ouvrir www.mikrotik.com
- Essayez d'ouvrir http://192.168.X.254
- La page du routeur fonctionne car la règle créée est pour le trafic passant à travers le routeur



# Liste des ports connus

| Port | Protocol | Service |
|---|---|---|
| 80 | TCP | WWW, HTTP |
| 22 | TCP | SSH |
| 23 | TCP | Telnet |
| 53 | TCP/UDP | DNS |
| 21,20 | TCP | FTP |
| 8291 | TCP | Winbox |
| 123 | UDP | NTP |
| 443 | TCP | HTTPS, SSL |
| 5678 | UDP | MNDP |
| 8080 | TCP | MikroTik Proxy |
| 20561 | UDP | MAC-Winbox |
| /1 | ICMP | Pings |



# Liste d'adresses

- Il est possible de créer des groupes d'adresses et d'appliquer une règle firewall sur ces groupes
- Il est possible d'ajouter automatiquement des adresses dans un groupe et ensuite de bloquer ces adresses

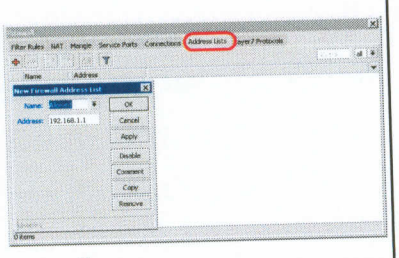


# Liste d'adresses

- Créez différentes listes

Dans une liste, il est possible d'ajouter:

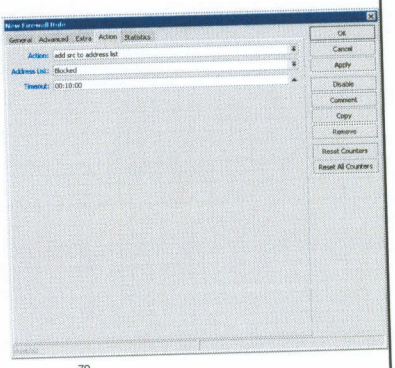
- Un sous-réseau (192.168.1.0/24)
- Une étendue d'adresse (192.168.1.10-192.168.1.20)
- Une seule IP (192.168.1.30)





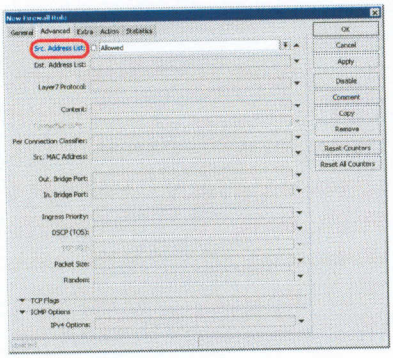

# Liste d'adresses

- Ajoutez une IP dans une liste d'adresses avec une règle de filtrage
- Spécifiez combien de temps elle doit rester dans ce groupe



# Firewall et listes d'adresses

- Possibilité de bloquer par source et destination





# Liste d'adresses

LAB

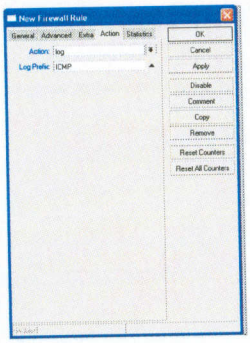
- Créez une liste d'adresses avec les IP autorisées
- Ajoutez une règle de Firewall pour autoriser ces adresses

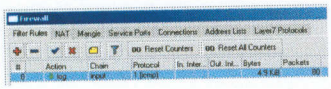


# Log du Firewall

LAB

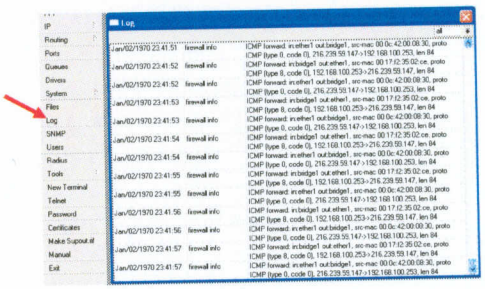
- Nous allons inscrire dans les logs les pings du client au routeur
- La règle de Log doit être ajoutée avant une autre action







# Log du Firewall





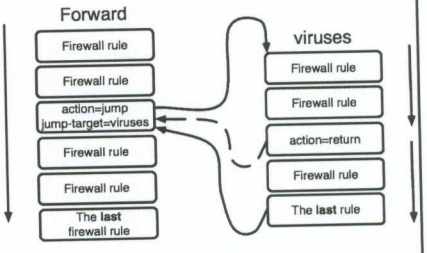
# Chaînes du Firewall

- A part les chaînes par défaut (input, forward, output), des chaînes personnalisées peuvent être créées
- Rend la structure des chaînes du firewall plus simple
- Diminue la charge CPU sur le routeur

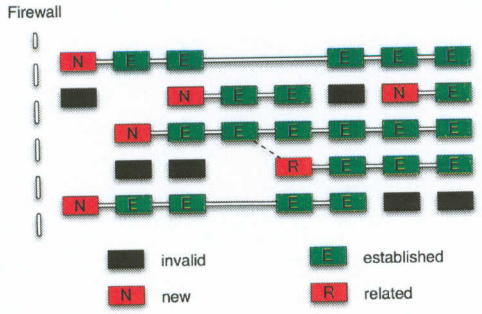


# Chaînes du Firewall en action

- Séquence des chaînes personnalisées du firewall
- Les chaînes personnalisées peuvent concerner des serveurs, des protocoles, etc.



# Connexions






# Etat des connexions

- Aviser, interdire les connexions invalides
- Le Firewall devrait traiter seulement les paquets IP des nouvelles connexions, il est recommandé d'exclure les autres états des règles du Firewall
- Les règles de filtrage possèdent la possibilité de vérifier l'état de la connexion pour cet usage



# Etat des connexions

LAB

- Ajoutez une règle pour interdire les paquets IP des connexions invalides
- Ajoutez une règle pour accepter les paquets IP des connexions établies
- Faites fonctionner le Firewall avec seulement des paquets IP de nouvelles connexions



# Résumé



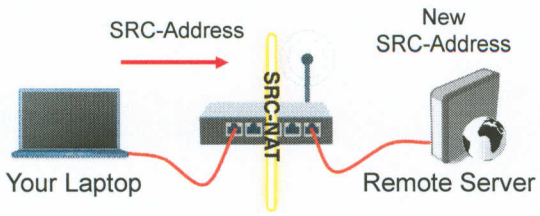
# Network Address Translation



# NAT

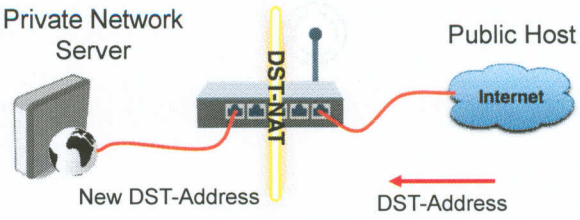
- Le routeur est capable de changer l'adresse **Source** ou celle de **Destination** des paquets IP passant à travers lui
- Ce procédé est nommé **src-nat** ou **dst-nat**

# SRC-NAT






# DST-NAT






# Chaînes NAT

- Pour réaliser ces scénarios, vous devez organiser vos règles NAT dans les chaînes appropriées: **dstnat** ou **srcnat**
- Les règles NAT fonctionnent selon le principe **IF-THEN** (comme les règles Firewall)

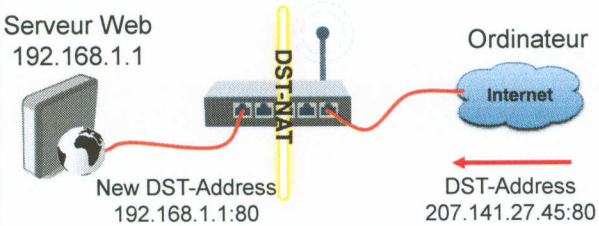


# DST-NAT

- DST-NAT modifie dans les paquets IP l'adresse de destination ainsi que le port
- Cette méthode peut être utilisée pour rediriger des utilisateurs d'internet vers un serveur de votre réseau privé



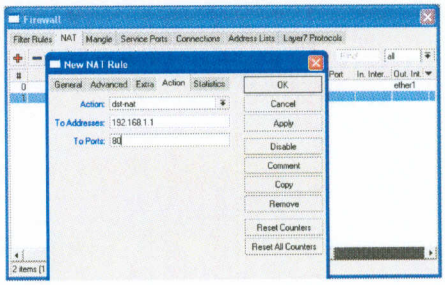
# Exemple DST-NAT






# Exemple DST-NAT

Création d'une règle pour rediriger le trafic vers le serveur WEB qui se trouve dans le réseau privé

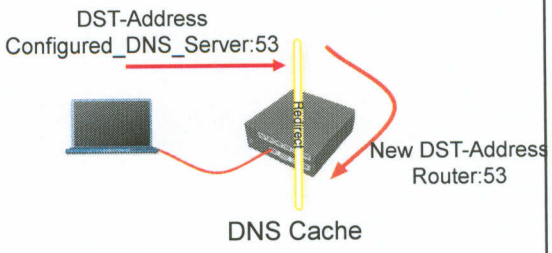


# Redirect

- Type spécial de DST-NAT
- Cette action redirige les paquets vers le routeur
- On peut utiliser cette fonctionnalité pour que le routeur soit un proxy pour certains services (DNS, HTTP)



# Exemple pour Redirect

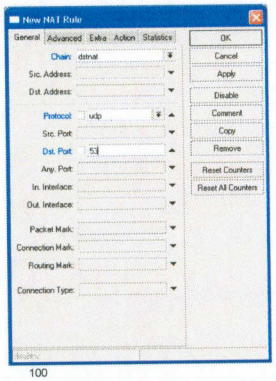





# Redirect

LAB

- Faites que les utilisateurs locaux utilisent le cache DNS du routeur
- Créez une règle pour le protocole **udp** et une autre pour **tcp**



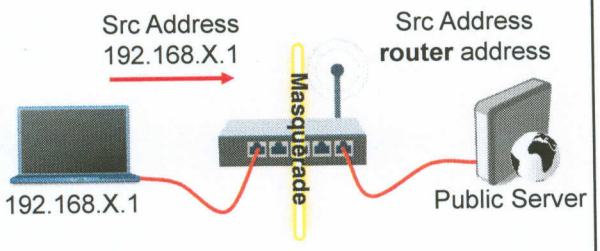



# SRC-NAT

- SRC-NAT modifie la source dans le paquet IP
- Vous pouvez l'utiliser pour connecter votre réseau privé à internet
- **Masquerade** est un type de SRC-NAT



# Masquerade

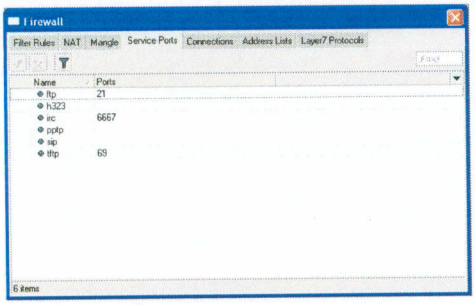





# Limitations de SRC-NAT

- La connexion vers des serveurs internes depuis l'extérieur n'est pas possible (besoin d'une règle DST-NAT)
- Certains protocoles nécessitent un service "NAT helpers" pour fonctionner correctement

# NAT Helpers






# Astuces pour Firewall

- Ajoutez des commentaires à vos règles
- Utilisez la fonction "Connection Tracking" et l'outil "Torch"

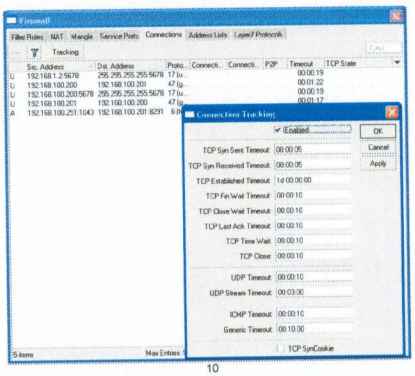


# Connection Tracking

- "Connection Tracking" gère les informations de toutes les connexions actives
- Cette fonctionnalité doit être active pour que le filtrage et le NAT du Firewall soient opérationnels

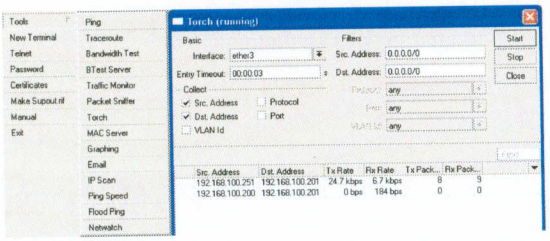


# Connection Tracking






# Torch




Rapport détaillé des connexions sur une interface



# Firewall Actions

- Accept
- Drop
- Reject
- Tarpit
- log
- add-src-to-address-list(dst)
- Jump, Return
- Passthrough

# Firewall Actions

- passthrough - ignore cette règle et passe à la suivante (utile pour des statistiques).
- reject – rejette le paquet et envoie un message "ICMP reject"
- tarpit – capture et maintient la connection TCP (reponds avec SYN/ACK à la connection entrante du paquet TCP SYN)
- accept - accepte le paquet. Le paquet n'est pas passé à la règle suivante du firewall.



# NAT Actions

- Accept
- DST-NAT/SRC-NAT
- Redirect
- Masquerade
- Netmap - creates a static 1:1 mapping of one set of IP addresses to another one. Often used to distribute public IP addresses to hosts on private networks
- Same - gives a particular client the same source/destination IP address from supplied range for each connection. This is most frequently used for services that expect the same client address for multiple connections from the same client



# Résumé



# Proxy



# Qu'est ce qu'un Proxy

- Il peut accélérer le browsing sur le WEB en cachant différentes informations
- Firewall HTTP

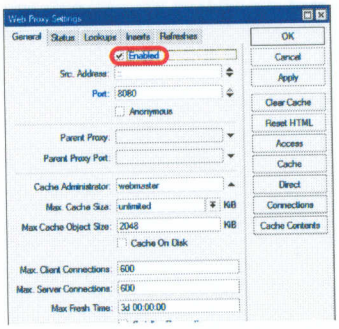


# Activer le Proxy

**IP -> Web Proxy**

L'option principale est **Enable (Activé)**

les autres paramètres sont optionnels



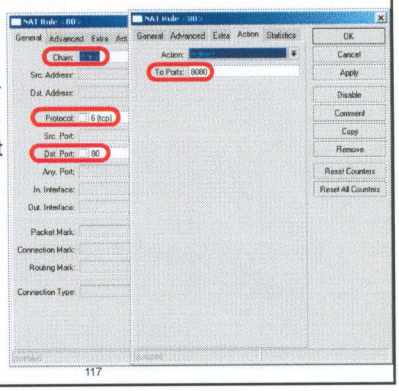
# Proxy en mode transparent

- L'utilisateur doit configurer son navigateur internet pour utiliser le serveur proxy
- En utilisant un mode transparent, cela permet de rediriger les utilisateurs vers le serveur proxy automatiquement



# Mode transparent

- Une règle DST-NAT est nécessaire pour le mode transparent
- Le trafic HTTP doit être redirigé sur le routeur





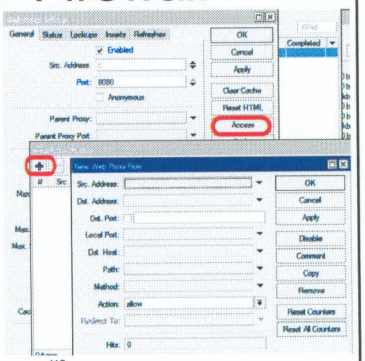
# HTTP Firewall

- Le serveur Proxy fonctionne aussi avec une access list. Elle permet de filtrer en fonction du nom DNS
- Vous pouvez rediriger vers des pages spécifiques



# HTTP Firewall

- Dst-Host = addresse de la page web (http://test.com)
- Path = tout ce qui est après http://test.com/**PATH**





# HTTP Firewall

LAB

- Créez une règle pour interdire l'accès à une page web spécifique
- Créez une règle pour rediriger depuis une page web non permise vers la page web de votre compagnie



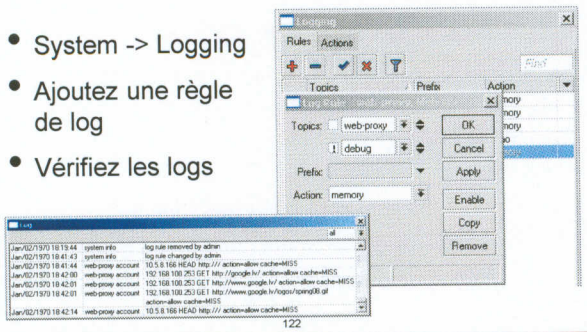
# Logs sur serveur Proxy

- Le serveur Proxy peut générer des fichiers de log des pages visitées par les utilisateurs
- Vérifiez que vous avez les ressources nécessaires pour gérer ces logs (c'est préferable de les stocker sur un support externe)

# Logs du serveur Proxy

LAB

- System -> Logging
- Ajoutez une règle de log
- Vérifiez les logs





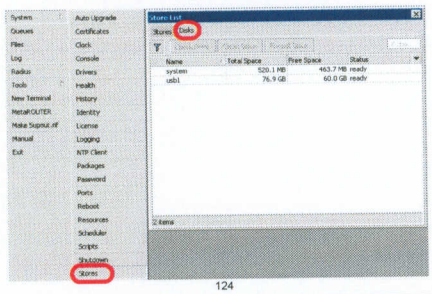

# Cache du Proxy

- Le cache du Proxy peut être stocké sur un support externe
- **Le service Store** de RouterOS gère tous les disques externes
- Le cache peut être enregistré sur un support IDE, SATA, USB, CF, MicroSD



# Service Store

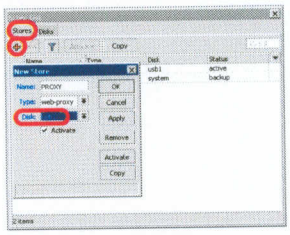
- Gère tous les disques externes
- Tous les disques nouvellement connectés doivent être formatés avant usage






# Ajoutez un stockage

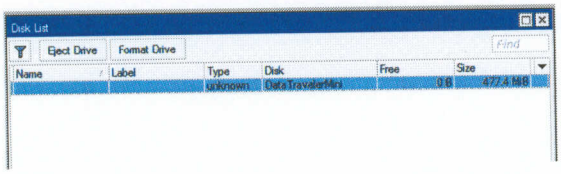
- Ajoutez un stockage pour sauver les données du proxy vers un disque externe
- Le service Store supporte les fonctionnalités proxy, user-manager, dude






# Nouveauté -> v.6.20

- System -> store n'existe plus
- Remplacé par System -> Disks

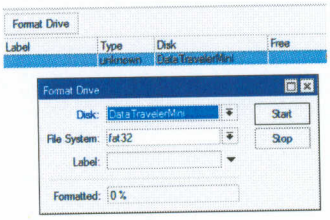



- Seulement les disks externes sont gérables



# Nouveauté -> v.6.20

- Possibilité d'utiliser du fat32 ou ext3




- Seulement les disks externes sont gérables
- Attention en cas de mise a jour

# Résumé



# Limitation de bande passante



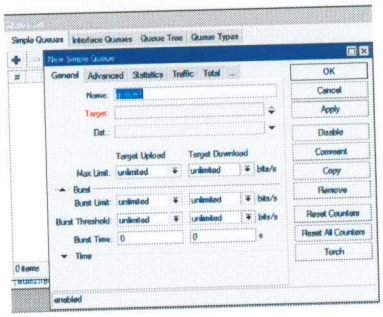
# Simple Queue

Il s'agit du moyen le plus simple pour limiter la bande passante pour:

- client download
- client upload
- client aggregate, download+upload



# Simple Queue






# Cible

- Vous **devez** utiliser une cible pour cette méthode:
  - **Une adresse IP**
  - **Un sous-réseau**
  - **Une interface**

L'ordre dans lequel sont entrées les files d'attente est important



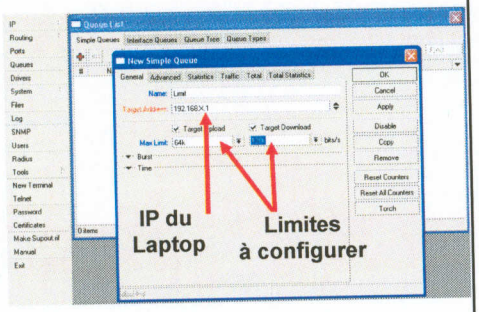
# Destination

- Adresse IP vers laquelle le trafic est dirigée
- L'interface par laquelle va passer les paquets en direction de la destination
- Pas obligatoire comme le champs "target"

# Simple Queue

LAB

- Créez une limitation pour votre laptop
- 64k Upload, 128k Download





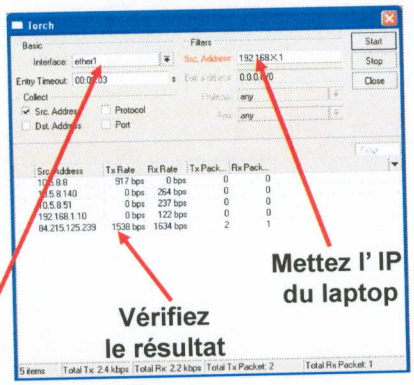

# Simple Queue

- Vérifiez les limites qui ont été mises
- L'outil Torch montre la vitesse de la bande passante



# Utiliser Torch

- Visualisez la vitesse actuelle

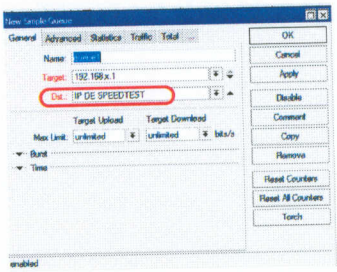





# Limitation pour un serveur spécifique

LAB

- Créons une limite pour speedtest
- L'adresse de destination est utilisée dans ce cas
- L'ordre des règles est important





# Limitation pour un serveur spécifique

LAB

- L'adresse de destination est utile pour mettre des accès illimités aux ressources du réseau local
- L'adresse cible et l'adresse de destination peuvent être échangées



# Couleur?

La couleur de la Queue montre l'utilisation de sa bande passante:

- Verte: 0-50%
- Jaune: 51-75%
- Rouge: 76-100%

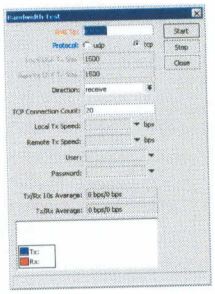
# Outil de mesure de la bande passante

- L'outil "Bandwidth test" peut être utilisé pour surveiller le débit vers un appareil distant
- Cela fonctionne entre 2 routeurs MikroTik, mais il existe aussi une version Windows de cet outil
- La version Windows est disponible sur le site www.MikroTik.com



# Test de bande passante

- Mettez l'adresse de destination (Test to)
- Sélectionnez le protocole
- TCP supporte plusieurs connexions
- Une authentification peut être nécessaire

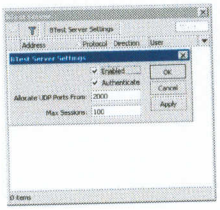




# Bandwidth Test

LAB

- La partie serveur doit être activée
- Il est préférable d'utiliser une authentification





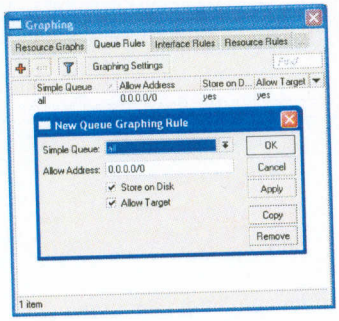
# Simple Queue Visualisation

- Il est possible d'avoir un **graphique** pour chaque "simple queue"
- Ces graphiques montrent la quantité de trafic qui est passée à travers la file d'attente



# Simple Queue Visualisation

Activons les graphiques pour les files d'attente

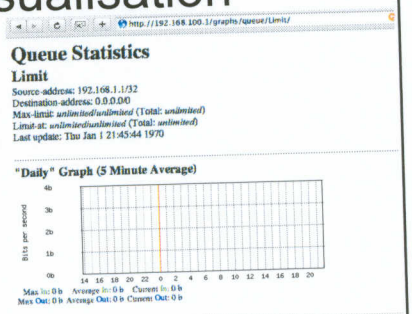





# Simple Queue Visualisation

LAB

- Pour voir les graphiques http://routeur_IP
- Vous pouvez donner l'accès à vos clients



# Gestion avancée de la bande passante



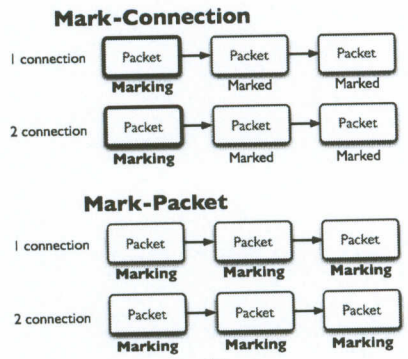
# Mangle

- Mangle est utilisé pour marquer les paquets IP
- Utilisé pour séparer différents types de trafic
- Ces "marques" ne sont actives qu'à l'intérieur du routeur
- Utilisé dans les files d'attente pour mettre des limitations différentes
- Mangle ne modifie pas la structure du paquet IP (à l'exception d'actions spécifiques DSCP, TTL)

(DSCP permet de passer le paquet IP avec une priorité aux autres routeurs)



# Mangle actions





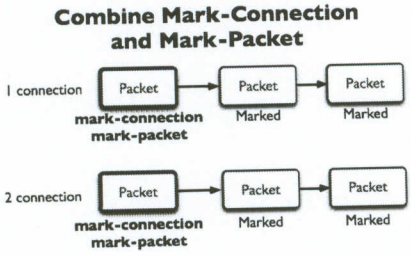

# Mangle actions

- **Mark-connection** utilise la base de suivi des connexions (connection tracking)
- L'information d'une nouvelle connexion est ajoutée à la table de suivi des connexions
- **Mark-packet** fonctionne directement avec les paquets
- Le routeur doit suivre chaque paquet pour appliquer la marque **Mark-packet**



# Optimal Mangle

- Les files d'attente ne fonctionnent qu'avec les marques sur les paquets

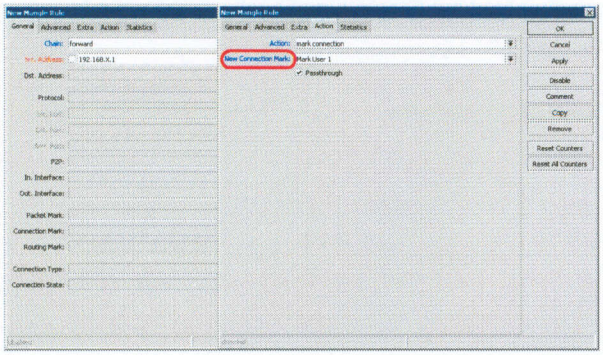





# Optimal Mangle

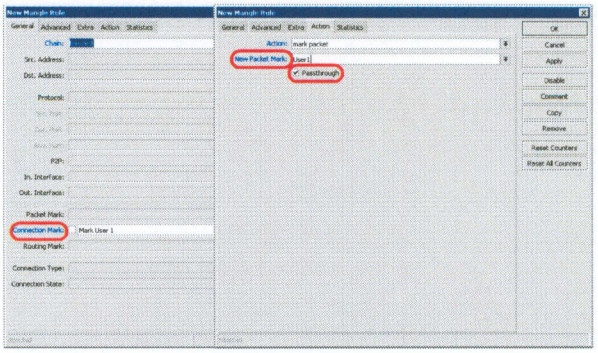
- Marquez les nouvelles connexions avec **mark-connection**
- Ajoutez une marque **mark-packet** pour toutes les connexions qui ont une marque **mark-connection**

# Mark Connection





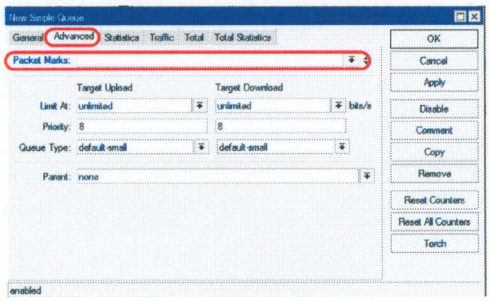
# Mark Packet





# Mark Packet

- Utilisation dans une simple queue:






# Mark Packet

Cette méthode permet donc de prioritiser certains traffics .... (voip, http..)

**Ou au contraire:**

De limiter tous les autres traffics (torrent ... ports non connus) à une faible bande passante



# Gestion avancée

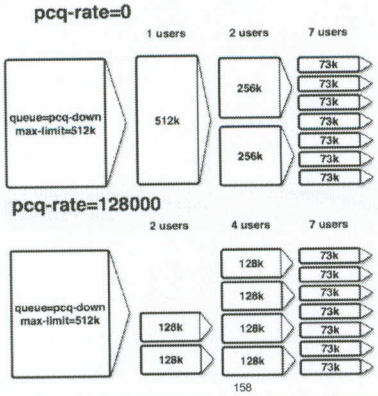
- Remplacer des centaines de files d'attente en une seule
- Mettre les mêmes limitations à tous les utilisateurs
- Equilibrer la bande passante disponible entre les utilisateurs



# PCQ

- PCQ est un type avancé de file d'attente
- PCQ utilise une classification pour diviser le trafic (from client point of view; src-address is upload, dst-address is download)

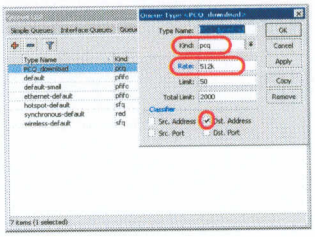
# PCQ






# PCQ, une limite pour tous

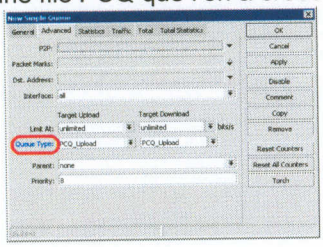
- PCQ permet de mettre une limite à tous les utilisateurs avec une seule file d'attente





# PCQ, une limite pour tous

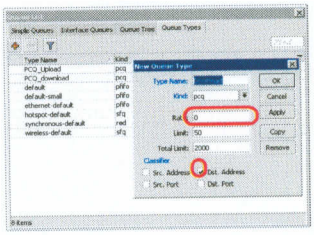
- Plusieurs files d'attente sont modifiées par une file PCQ que l'on a créée





# PCQ, égalise la bande passante

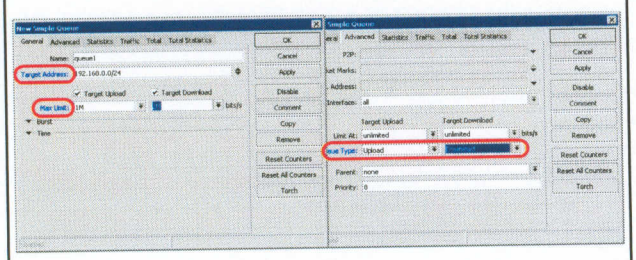
- Partage de façon égale la bande passante entre les clients





# PCQ, égalise la bande passante

1M upload/2M download partagé entre les utilisateurs





# PCQ

LAB

- Une queue PCQ va être créée sur le routeur principal

# Bursting

- Permettre aux utilisateurs, pendant un temps limité, d'avoir plus de bande passante que le paramêtre "max-limit" les y autorisent
- Utile dans certains cas pour avoir plus de vitesse pour certains traffics. Par exemple pour le HTTP, un utilisateur téléchargera rapidement la page et la lira pendant plusieurs secondes



# Bursting

**Burst-limit** : Vitesse maximum pendant que le burst est autorisé

**Burst-time** : Temps, en secondes, pendant lequel un échantilognage de vitesse est fait (pour calculer la vitesse moyenne). Ce n'est pas la durée de l'acceleration.

**Burst-threshold** : La valeur qui determine si un utilisateur peut bénéficier d'une acceleration ("burst")

**Average-rate** : Une moyenne de la vitesse de transfert calculée en 1/16th parts du "burst-time"

**Actual-rate** : Vitesse actuelle (en temps réel) des données



## Comment cela fonctionne:

L'accélération "Burst" est autorisée si le débit moyen est en dessous du "**burst-threshold**"

Le "Burst sera limité à la vitesse mise dans "**burst-limit**"

Le débit moyen est calculé par 16 valeurs de la vitesse réelle pendant le temps imparti ("Burst-time")

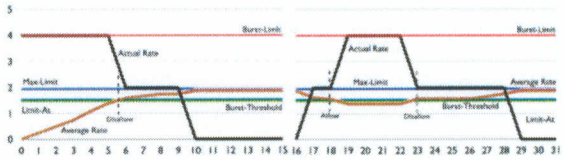
Si le temps est de 16 secondes -> 1 par seconde

Si le temps est de 8 secondes -> 1 toute les 0.5 seconde

Quand l'accélération commence, elle sera autorisée pendant un temps maximum défini en seconde:

**(burst-threshold x burst-time) / burst-limit**






Max-limit = 2 mb

Burst-time = 16 secondes

Burst-threshold = 1.5 mb

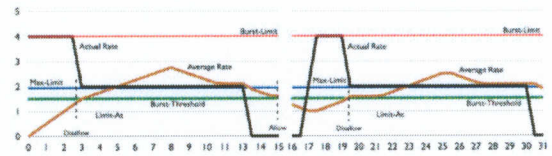
Burst-limit = 4 mb

**(burst-threshold x burst-time) / burst-limit**

**1.5 x 16 / 4**

**Accélération permise pour 6 secondes au maximum.**






Max-limit = 2 mb

Burst-time = 8 secondes

Burst-threshold = 1.5 mb

Burst-limit = 4 mb

**(burst-threshold x burst-time) / burst-limit**

**1.5 x 8 / 4**

**Accélération permise pour 3 secondes au maximum.**



# Résumé

# Wireless



# Communication sans-fil

- RouterOS supporte des modules radio permettant les communications sans-fil
- Ces modules fonctionnent en standard dans les bandes de fréquence 2.4GHz et 5GHz, mais on trouve aussi des modules dans d'autres bandes de fréquence (700mhz–900mhz–3.6ghz–6.4ghz–17ghz)
- Support complet des standards IEEE 802.11a, 802.11b, 802.11g, 802.11n et 801.11ac

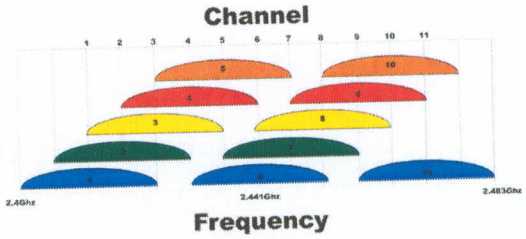


# Wireless Standards

- IEEE 802.11b – fréquences 2.4GHz, 11Mbps (débit réel: 8mpbs)
- IEEE 802.11g – fréquences 2.4GHz, 54Mbps (débit réel: 40mbps)
- IEEE 802.11a – fréquences 5GHz, 54Mbps (débit réel: 40mbps)
- IEEE 802.11n - fréquences 2.4GHz ou 5GHz, 300Mbps (débit réel: 220mbps)

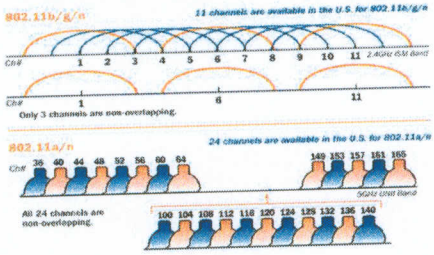


# 802.11 b/g channels




Il existe 11 canaux de 22mhz dans la bande de fréquence 2.4ghz.
Les canaux 1, 6 et 11 ne se chevauchent pas.
3 points d'accès peuvent occuper le même endroit sans interférences.

# Canaux 802.11a 5ghz




En 5ghz, 24 canaux de 10mhz: 12 canaux de 20MHZ ou encore 5 canaux de 40mhz ne se chevauchent pas.

# Fréquences admises

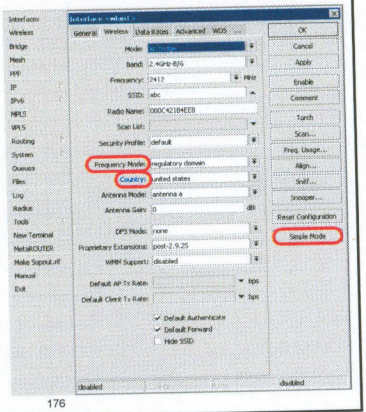
- Elles dépendent de la politique de régulation du pays
- En général, les cartes wifi peuvent supporter:

  2.4GHz: 2312 - 2499 MHz

  5GHz: 4920 - 6100 MHz

# Appliquer les limitations du pays

Paramètres à indiquer pour limiter la carte wifi






# RADIO Name

- Nous allons utiliser “RADIO Name” de la même façon que la fonction “router identity”
- Mettez comme “RADIO Name” **Nombre X + _ + votre nom**

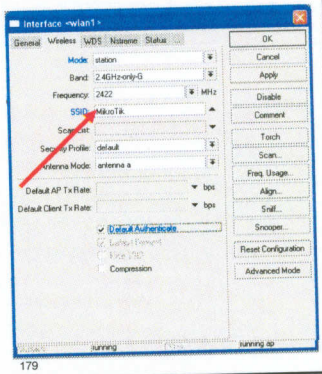


# Wireless Network




# Configuration en mode station

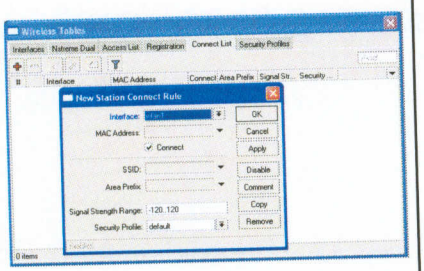
- Mettre l’interface en **mode station**
- Sélectionner la **bande**
- Mettre le **SSID**, l’identité du réseau wifi
- La fréquence n’est pas importante pour le client – utiliser scan






# Connect List

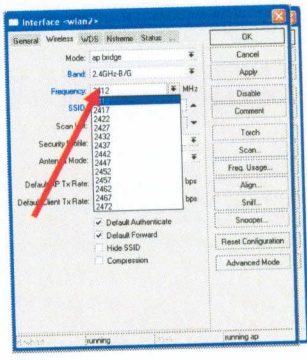
Ensemble de règles utilisées par le mode station pour sélectionner le point d’accès auquel il va se connecter





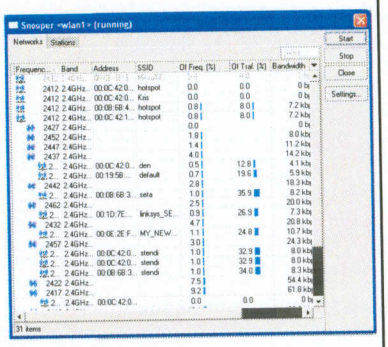

# Configuration en mode AP

- Paramétrez le routeur en **mode ap-bridge**
- Sélectionnez la **bande de fréquence (2.4 – 5)**
- Mettez le **SSID**, l’identité du réseau sans-fil
- Choisissez la **fréquence**



# Snooper – moniteur wifi

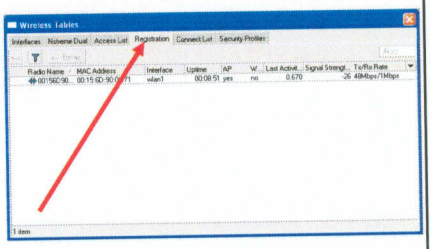
- L'outil **Snooper** permet de visualiser l'utilisation totale de la bande wifi
- L'**interface wifi est déconnectée** pendant ce scan



182

# Registration Table

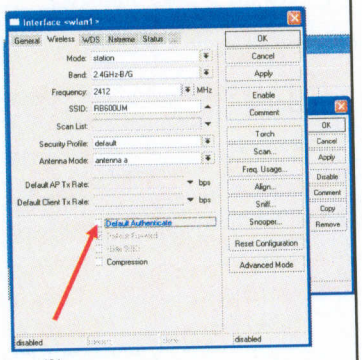
- Visualiser toutes les interfaces wifi qui sont connectées



183

# Sécurité sur les points d'accès

- **Access-list** est utilisé pour appliquer une sécurité basée sur les **adresses MAC**
- Si on désactive **l'authentification par défaut,** on utilisera uniquement les entrées de **l'Access-list**



184

# Default Authenticate

- **Oui,** les règles de l' Access-List sont vérifiées, le client pourra se connecter s'il n'y pas de règles d'interdiction
- **Non,** seules les règles de l' Access-List sont vérifiées

185

# Access-List

LAB

- Puisque vous avez le mode "station" configuré, nous allons procéder à l'exercice sur le routeur principal
- Désactivez la connection pour un client donné
- Autorisez uniquement la connexion pour des clients spécifiques

186

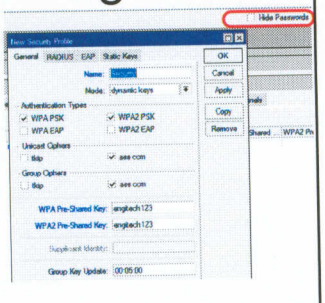
# Sécurité

- Nous allons activer le cryptage sur le réseau wifi
- Vous devez utiliser WPA ou WPA2 comme protocole de cryptage
- Tous les appareils sur le réseaux doivent avoir les mêmes options de sécurité

187

# Astuces de configuration

- Pour voir les Pre-Shared Key, cliquez sur "Hide Passwords"
- En utilisant cette option, il est possible de voir les autres informations cachées. Les seules variables qui restent cachées sont les mots de passe des utilisateurs du routeur

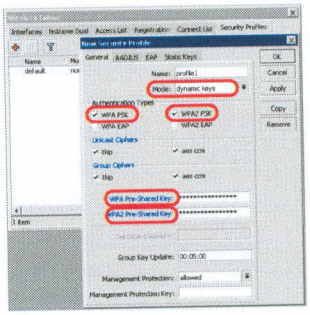





# Sécurité

LAB

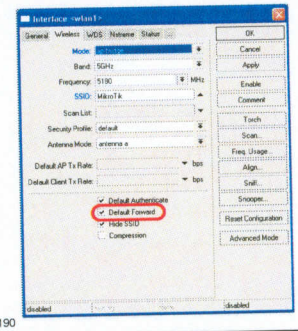
- Mettez un cryptage WPA pour le réseau wifi
- WPA Pre-Shared Key est **engitech123**





# Désactiver les connexions entre clients

**Default-Forward** est utilisé pour désactiver les communications entre clients connectés au même point d'accès





# Default Forward

- Les règles de l'Access-List ont une plus grande priorité
- Si la connexion entre les clients fonctionnent -> vérifiez l'Access-List



# 802.11N paramètres

- Data-rates
- HT chaines
- HT guard interval



# MikroTik protocoles

- Nstreme
- Nstreme Dual
- NV2 (TDMA)

# Nstreme

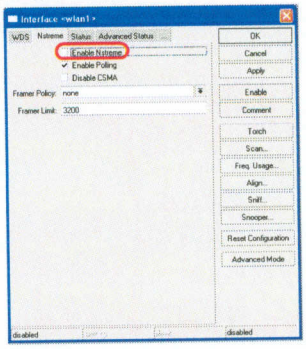
- Protocole propriétaire de MikroTik
- Améliore les liens sans-fil, surtout sur les liaisons de longue distance
- Pour l'utiliser sur votre réseau, activez ce protocole sur tous les appareils de ce réseau



# Nstreme

LAB

- Activez Nstreme sur votre routeur
- Vérifiez le statut de la connexion
- **Nstreme** doit être actif sur l'ensemble des routeurs






# NV2

Nouveau protocole basé sur la technologie TDMA (Time Division Multiple Access) - (Nstreme version 2).

TDMA is a channel access method for shared medium networks. It allows several users to share the same frequency channel by dividing the signal into different time slots. The users transmit in rapid succession, one after the other, each using his own time slot. This allows multiple stations to share the same transmission medium (e.g. radio frequency channel) while using only a part of its channel capacity.
Increased speed



# 40mhz en 2.4ghz

| Primary channel | 20 MHz | 40 MHz above | | | 40 MHz below | | |
|---|---|---|---|---|---|---|---|
| | Blocks | 2nd ch. | Center | Blocks | 2nd ch. | Center | Blocks |
| 1 | 1-3 | 5 | 3 | 1-7 | Not Available | | |
| 2 | 1-4 | 6 | 4 | 1-8 | Not Available | | |
| 3 | 1-5 | 7 | 5 | 1-9 | Not Available | | |
| 4 | 2-6 | 8 | 6 | 2-10 | Not Available | | |
| 5 | 3-7 | 9 | 7 | 3-11 | 1 | 3 | 1-7 |
| 6 | 4-8 | 10 | 8 | 4-12 | 2 | 4 | 1-8 |
| 7 | 5-9 | 11 | 9 | 5-13 | 3 | 5 | 1-9 |
| 8 | 6-10 | 12 | 10 | 6-13 | 4 | 6 | 2-10 |
| 9 | 7-11 | 13 | 11 | 7-13 | 5 | 7 | 3-11 |
| 10 | 8-12 | Not Available | | | 6 | 8 | 4-12 |
| 11 | 9-13 | Not Available | | | 7 | 9 | 5-13 |
| 12 | 10-13 | Not Available | | | 8 | 10 | 6-13 |
| 13 | 11-13 | Not Available | | | 9 | 11 | 7-13 |

Requiert une première bande de 20mhz ainsi qu'une 2ème bande qui est adjacente. La première bande est utilisée pour les clients qui ne sont pas capable de fonctionner en 40mhz. Quand la communication fonctionne en 40mhz, la fréquence centrale est le milieu des 2 bandes utilisées.



# HT guard interval

**Guard intervals** are used to ensure that distinct transmissions do not interfere with one another

The standard symbol guard interval used in 802.11 OFDM is 0.8 µs. To increase data rate, 802.11n added optional support for a 0.4 µs guard interval. This provides an 11% increase in data rate. The shorter guard interval results in a higher packet error rate when the delay spread of the channel exceed the guard interval and/or if timing synchronization between the transmitter and receiver is not precise.



# Vitesses MCS

| MCS index | Spatial streams | Modulation type | Coding rate | Data rate (Mbit/s) 20 MHz channel 800 ns GI | 20 MHz channel 400 ns GI | 40 MHz channel 800 ns GI | 40 MHz channel 400 ns GI |
|---|---|---|---|---|---|---|---|
| 0 | 1 | BPSK | 1/2 | 6.50 | 7.20 | 13.50 | 15.00 |
| 1 | 1 | QPSK | 1/2 | 13.00 | 14.40 | 27.00 | 30.00 |
| 2 | 1 | QPSK | 3/4 | 19.50 | 21.70 | 40.50 | 45.00 |
| 3 | 1 | 16-QAM | 1/2 | 26.00 | 28.90 | 54.00 | 60.00 |
| 4 | 1 | 16-QAM | 3/4 | 39.00 | 43.30 | 81.00 | 90.00 |
| 5 | 1 | 64-QAM | 2/3 | 52.00 | 57.80 | 108.00 | 120.00 |
| 6 | 1 | 64-QAM | 3/4 | 58.50 | 65.00 | 121.50 | 135.00 |
| 7 | 1 | 64-QAM | 5/6 | 65.00 | 72.20 | 135.00 | 150.00 |
| 8 | 2 | BPSK | 1/2 | 13.00 | 14.40 | 27.00 | 30.00 |
| 9 | 2 | QPSK | 1/2 | 26.00 | 28.90 | 54.00 | 60.00 |
| 10 | 2 | QPSK | 3/4 | 39.00 | 43.30 | 81.00 | 90.00 |
| 11 | 2 | 16-QAM | 1/2 | 52.00 | 57.80 | 108.00 | 120.00 |
| 12 | 2 | 16-QAM | 3/4 | 78.00 | 86.70 | 162.00 | 180.00 |
| 13 | 2 | 64-QAM | 2/3 | 104.00 | 115.60 | 216.00 | 240.00 |
| 14 | 2 | 64-QAM | 3/4 | 117.00 | 130.00 | 243.00 | 270.00 |
| 15 | 2 | 64-QAM | 5/6 | 130.00 | 144.40 | 270.00 | 300.00 |
| 16 | 3 | BPSK | 1/2 | 19.50 | 21.70 | 40.50 | 45.00 |
| 17 | 3 | QPSK | 1/2 | 39.00 | 43.30 | 81.00 | 90.00 |
| 18 | 3 | QPSK | 3/4 | 58.50 | 65.00 | 121.50 | 135.00 |
| 19 | 3 | 16-QAM | 1/2 | 78.00 | 86.70 | 162.00 | 180.00 |
| 20 | 3 | 16-QAM | 3/4 | 117.00 | 130.00 | 243.00 | 270.00 |
| 21 | 3 | 64-QAM | 2/3 | 156.00 | 173.30 | 324.00 | 360.00 |
| 22 | 3 | 64-QAM | 3/4 | 175.50 | 195.00 | 364.50 | 405.00 |
| 23 | 3 | 64-QAM | 5/6 | 195.00 | 216.70 | 405.00 | 450.00 |
| 24 | 4 | BPSK | 1/2 | 26.00 | 28.80 | 54.00 | 60.00 |
| 25 | 4 | QPSK | 1/2 | 52.00 | 57.60 | 108.00 | 120.00 |
| 26 | 4 | QPSK | 3/4 | 78.00 | 86.80 | 162.00 | 180.00 |
| 27 | 4 | 16-QAM | 1/2 | 104.00 | 115.60 | 216.00 | 240.00 |
| 28 | 4 | 16-QAM | 3/4 | 156.00 | 173.20 | 324.00 | 360.00 |
| 29 | 4 | 64-QAM | 2/3 | 208.00 | 231.20 | 432.00 | 480.00 |
| 30 | 4 | 64-QAM | 3/4 | 234.00 | 260.00 | 486.00 | 540.00 |
| 31 | 4 | 64-QAM | 5/6 | 260.00 | 288.80 | 540.00 | 600.00 |

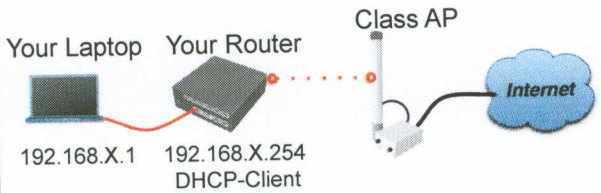
# Résumé

200

# Bridging

201

# Bridge Wireless Network

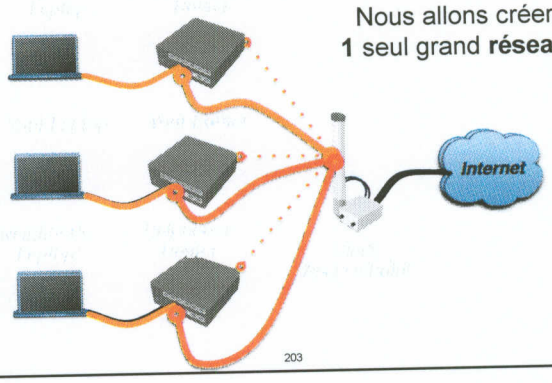



Remettre la configuration de notre cours

202

# Bridge Wireless Network

Nous allons créer
**1** seul grand **réseau**




203

# Bridge

- Nous allons réunir l'interface ethernet du réseau local avec l' interface sans-fil
- Un Bridge unifie différentes interfaces physiques en une seule interface logique
- Tous vos laptops seront dans le même réseau

204

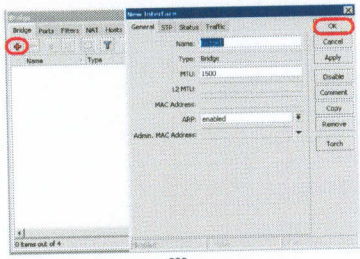
# Bridge

- Pour réunir ces interfaces , vous devez créer une interface bridge
- Ensuite, ajoutez les interfaces physiques à cette interface bridge

205

# Créer une interface Bridge

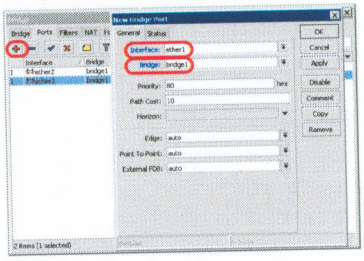
Une interface Bridge est configurée depuis le menu **/interface bridge**



206

# Ajouter un port Bridge

Les interfaces physiques sont ajoutées via l'onglet "ports"



207

# Bridge

- Il n'y a aucun problème pour réunir des interfaces ethernet dans un bridge
- Les clients Wifi (**mode=station**) ne supportent pas ce type d'association, cela est dû à une limitation du protocole 802.11

208

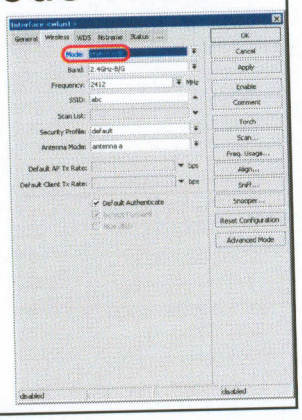
# Bridge Wifi clients

- **WDS** permet d'ajouter des clients wifi à une interface **bridge**
- WDS (Wireless Distribution System) permet la connection entre les points d'accès wifi

209

# Activer le mode WDS

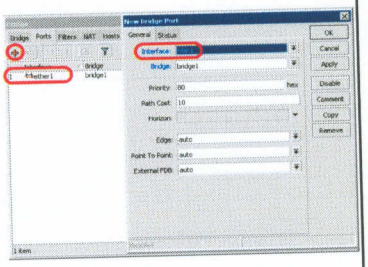
Station-wds est un mode client spécial avec le support de la fonctionnalité WDS



210

# Ajouter des ports au Bridge

- Ajoutez les interfaces public et local au bridge
- Ether1 (local), wlan1 (public)



211

# Access Point WDS

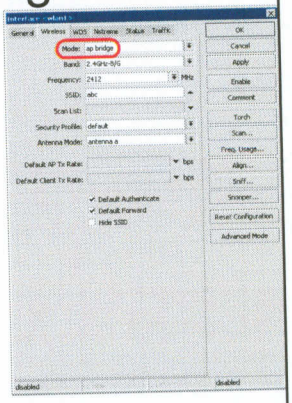
Plusieurs points vont être détaillés:

- Activez WDS sur l' AP-bridge, utilisez le mode=dynamic-mesh
- Les interfaces WDS sont créées au fur et à mesure
- Utilisez le bridge par défaut pour les interfaces WDS
- Ajoutez l'interface wifi au Bridge

212

# AP-bridge

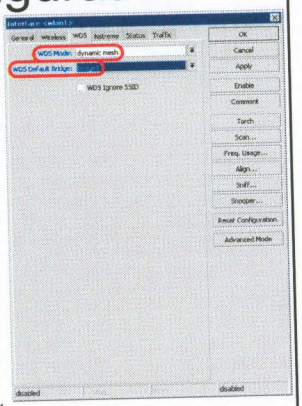
- Paramétrez le mode AP-bridge
- Ajoutez l'interface au **bridge**



213

# WDS configuration

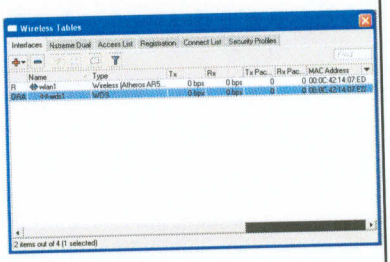
- Utilisez le mode WDS **dynamic-mesh**
- Les interfaces WDS sont créées dynamiquement
- Les autres points d'accès (AP) doivent aussi utiliser le mode **dynamic-mesh**



214

# WDS

- La liaison WDS est établie
- L'interface a été créée dynamiquement



215

# WDS

LAB

- Supprimez la règle NAT **masquerade**
- Supprimez le client **DHCP** sur l'interface wifi du routeur
- Utilisez le mode **station-wds** sur votre routeur
- Activez le DHCP client sur votre laptop
- Pouvez-vous faire un ping vers le laptop de votre voisin ?

216

# WDS

- Votre **routeur** est configuré comme un **Bridge Transparent** maintenant
- Vous devriez pouvoir faire un ping vers le routeur et le laptop de votre voisin
- Utilisez les bonnes adresses IP

217

## Restaurer la configuration

LAB

Pour restaurer la configuration:

- Remettez le mode wifi "Station"
- Ajoutez le client DHCP sur la bonne interface
- Ajoutez une règle de NAT masquerade
- Mettez une configuration réseau correcte sur votre laptop



## Résumé



## Routage



## Routes entre réseaux

- Nous avons remis la configuration
- Essayez de faire un ping vers le laptop de votre voisin
- L'adresse IP de votre voisin = 192.168.X.1
- Nous allons apprendre à créer des routes afin d'accéder au laptop de votre voisin



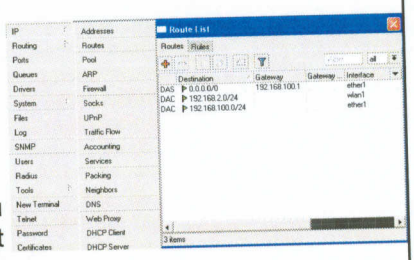
## Routes

- **Les règles de routage IP** définissent où les paquets doivent être envoyés
- Regardons dans Winbox, /ip routes, les règles définies actuellement



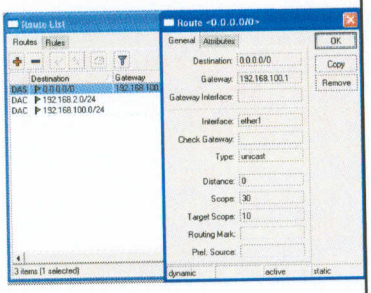
## Routes

- **Destination: réseaux** qui peuvent être joignables
- **Gateway:** passerelle réseau, l'adresse IP du routeur suivant pour atteindre la **destination**



# Passerelle par défaut

Default gateway: le routeur suivant où tout le trafic (**0.0.0.0**) est envoyé





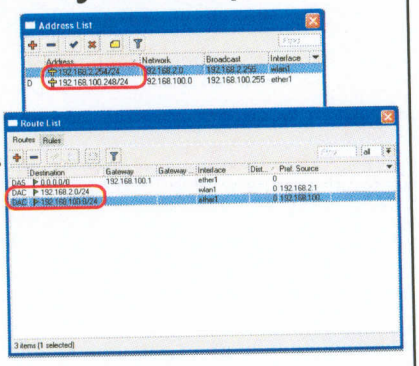

# Lab: Mettre la passerelle par défaut

- Actuellement, vous avez la passerelle par défaut reçue par le client DHCP
- Désactivez la réception de la passerelle par le client DHCP
- Ajoutez la passerelle par défaut manuellement



# Routes dynamiques

- Regardons les autres routes
- Les routes avec **DAC** sont ajoutées automatiquement
- **Les routes DAC** proviennent de la configuration des adresses IP






# Routes

- A - active
- D - dynamique
- C - connectée
- S - statique



# Routes statiques

- Notre but est de pouvoir faire un ping vers le laptop de votre voisin
- Nous allons utiliser des routes statiques pour y arriver



# Route statique

- Une route statique définit comment on peut atteindre une destination réseau spécifique
- **La passerelle par défaut** est aussi une route statique, elle envoie tout le trafic (destination 0.0.0.0) vers une destination – la passerelle

# Route statique

- Une route statique supplémentaire est nécessaire pour joindre le laptop de votre voisin
- La **passerelle** (le routeur principal) n'a pas d'information sur les différents réseaux privés que vous avez créés

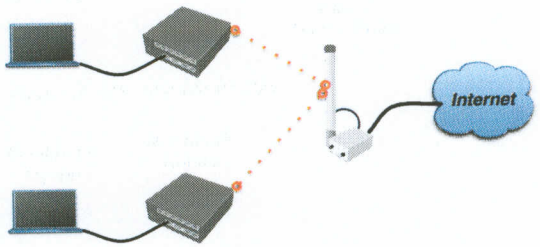


# Route vers le réseau voisin

- Souvenez-vous de la structure du réseau
- Neighbor's local network est 192.168.x.0/24
- Demandez à votre voisin l'adresse IP de son interface wifi



# Structure du réseau






LAB

# Route vers le réseau voisin

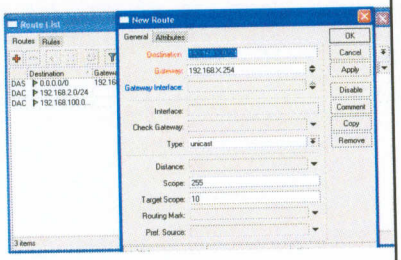
- Ajoutez une route
- Mettez comme **destination** le réseau local voisin
- Mettez comme passerelle l'adresse IP de la carte wifi du réseau voisin



LAB

# Route vers le réseau voisin

Essayez de faire un ping vers le laptop voisin






# Route active

Vous devriez pouvoir faire un ping vers le laptop voisin

# Routes dynamiques

- La même configuration est possible en utilisant des routes dynamiques
- Imaginez que vous ayez à ajouter des routes statiques pour tous les réseaux
- Au lieu de créer des centaines de routes, des protocoles de routage dynamiques peuvent être utilisés



# Routes dynamiques

- Facile à configurer, parfois difficile à gérer - dépanner
- Peut nécessiter des ressources CPU supplémentaires au niveau du routeur



# Routes dynamiques

- Nous allons utiliser OSPF
- OSPF est très rapide et optimal pour du routage dynamique
- Facile à configurer



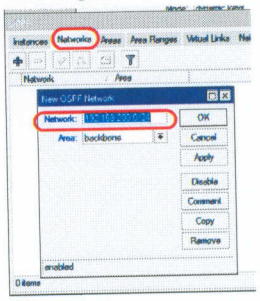
# OSPF configuration

Ajoutez les réseaux corrects dans la partie OSPF – Networks.

Les interfaces qui correspondent à ces réseaux vont automatiquement être actives.

Les interfaces OSPF s'annoncent sur le réseau et se connectent à leurs voisins.

Routing -> OSPF






# OSPF

LAB

- Vérifiez la table de routage
- Essayez de faire un ping vers les autres laptops
- Souvenez-vous qu'il faut des connaissances supplémentaires sur ce protocole avant d'implémenter OSPF sur un grand réseau



# Résumé

# Management du réseau local



# Accès au réseau local

- Le design d'un réseau est important
- Faites attention aux accès par les utilisateurs locaux
- Utilisez les fonctionnalités de RouterOS pour sécuriser les ressources du réseau



# ARP

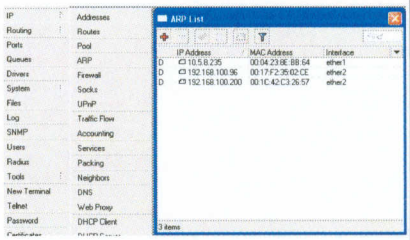
- Address Resolution Protocol
- ARP fait la liaison entre l'adresse IP du client et l'adresse MAC
- ARP fonctionne de manière dynamique, mais on peut aussi configurer manuellement des entrées



# ARP Table

ARP table:

adresse IP, adresse MAC et interface





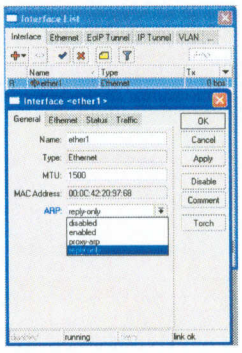

# Static ARP table

- Pour améliorer la sécurité du réseau, les entrées ARP peuvent être créées manuellement
- Les clients du routeur ne seront pas capables d'accéder à internet si leur adresse IP change



# Static ARP configuration

- Ajoutez une entrée statique dans la table ARP
- Paramétrez l'interface avec arp=reply-only pour désactiver la création dynamique d'entrée ARP
- Désactivez/activez l'interface ou redémarrez le routeur



# Static ARP

LAB

- Modifiez l'entrée ARP de votre laptop en statique
- Mettez arp=reply-only pour l'interface du réseau local
- Essayez de changer l'adresse IP de votre laptop
- Testez les accès vers internet



# Serveur DHCP

- Dynamic Host Configuration Protocol
- Est utilisé pour distribuer de façon automatique les adresses IP sur un réseau local
- Doit seulement être utilisé dans des réseaux sécurisés

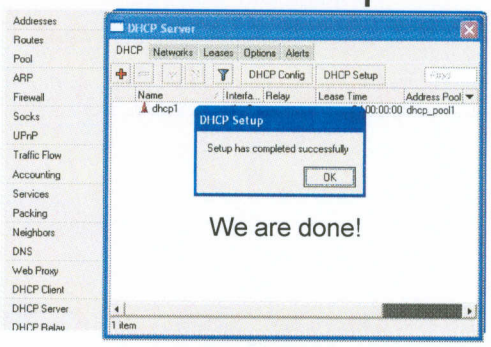


# Serveur DHCP

- Pour installer un serveur DHCP, vous devez avoir une adresse IP sur l'interface
- Utilisez la fonction "setup" pour activer le serveur DHCP
- Cette fonction vous demandera les informations nécessaires à la configuration du serveur DHCP



# DHCP Setup






# Important

- Pour configurer un serveur **DHCP** sur un **bridge**, il faut le faire sur l'interface du **bridge**
- DHCP serveur ne fonctionnera pas s'il est configuré sur un port du **bridge**



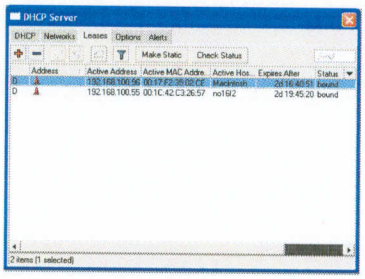
# Serveur DHCP

LAB

- Installez un serveur DHCP sur l'interface ethernet du routeur où est connecté votre laptop
- Modifiez votre laptop pour activer la configuration IP en DHCP
- Vérifiez la connectivité internet

# Serveur DHCP Information

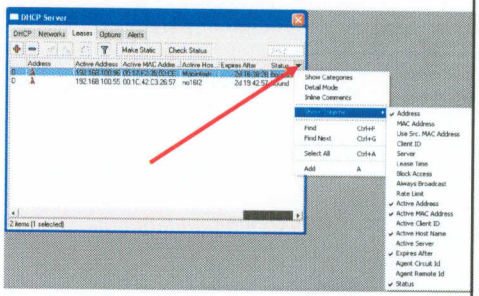
La colonne Leases (bail DHCP) fournit des informations sur les clients du serveur DHCP






# Astuce de configuration Winbox

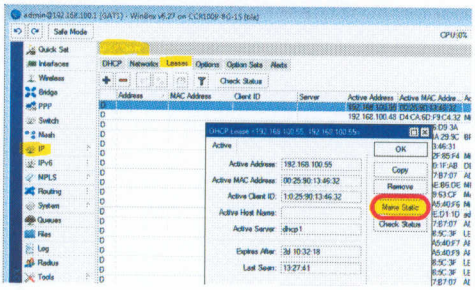
Affiche ou cache certaines colonnes dans Winbox






# Static Lease

- Nous pouvons changer le bail de dynamique en statique
- Le client recevra toujours la même adresse






# Static Lease

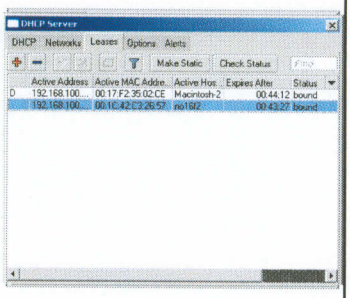
- Le serveur DHCP peut fonctionner sans baux dynamiques
- Les clients recevront seulement les adresses qui ont été préconfigurées



# Static Lease

LAB

- Modifiez le pool d'adresses pour être seulement statique
- Créez un bail statique






# HotSpot

# HotSpot

- Outil pour donner l'accès à internet
- HotSpot fournit l'authentification des clients avant de donner l'accès au réseau public
- Il permet aussi d'utiliser une base d'utilisateurs



# Pré-requis HotSpot

- Adresses IP correctes sur les interfaces entrante et sortante
- Un (ou plusieurs) serveur DNS configuré
- Au minimum un utilisateur HotSpot



# HotSpot Setup

- L'installation est similaire au serveur DHCP
- Il faut lancer le processus et répondre aux questions



# Important

- Les utilisateurs connectés à l'interface HotSpot seront déconnectés d'internet
- Le client devra être autorisé dans le système HotSpot pour avoir accès à internet



# Notes additionnelles

- La mise en place du HotSpot crée automatiquement une configuration dans le routeur:
  - **Un serveur DHCP** sur l'interface du Hotspot
  - **Un Pool** pour les clients du Hotspot
  - Des règles dynamiques dans le **Firewall** (Filter et NAT)



# HotSpot Help

- La page d'enregistrement du HotSpot s'affiche lorsque le client essaye d'accéder à une page web
- Pour sortir du HotSpot vous devez vous rendre à l'adresse http://router_IP ou http://HotSpot_DNS

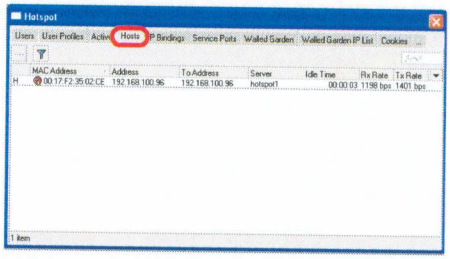
# HotSpot Setup

LAB

- Créez un HotSpot sur l'interface locale du routeur
- N'oubliez pas le nom d'utilisateur et le mot de passe, ou vous ne pourrez pas aller sur internet



# HotSpot -> Hosts

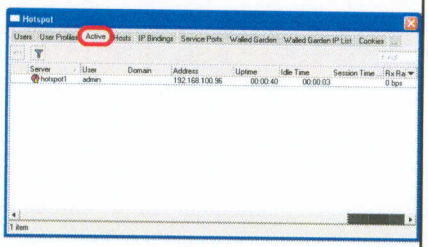



Information à propos des clients connectés au Hotspot



# HotSpot Active Table

Information sur les clients autorisés du Hotspot

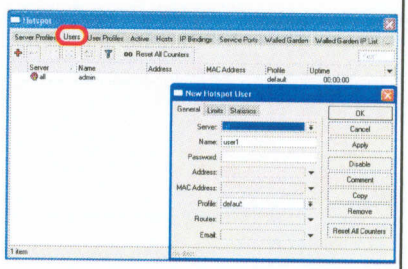





# User Management

- Ajouter
- Modifier
- Effacer

les utilisateurs du HotSpot





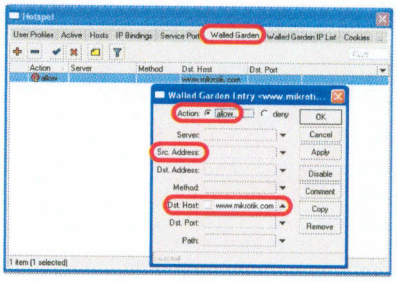

# HotSpot Walled-Garden

- Outil pour donner accès à des ressources spécifiques sans l'autorisation du Hotspot
- Walled-Garden pour HTTP et HTTPS
- Walled-Garden IP pour d'autres destinations (Telnet, SSH, Winbox, etc.)



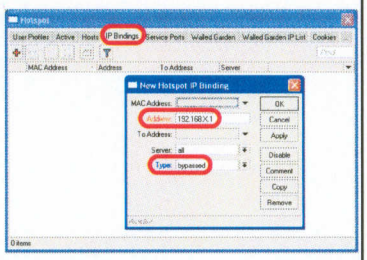
# Hotspot Walled-Garden

Permet l'accès à www.mikrotik.com



# Bypass Hotspot

- Permet à certains clients de passer à travers le HotSpot sans authentification
- Téléphones VoIP, imprimantes, superusers, …
- IP-bindings est utilisé pour cela





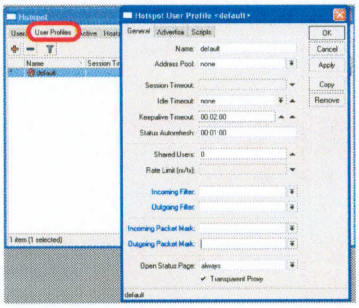

# Hotspot et bande passante

- Il est possible de mettre une limite automatique de bande passante pour tous les utilisateurs Hospot
- Une "Dynamic queue" est créée pour tous les utilisateurs du profil



# Hotspot User Profiles

User Profiles – ensemble de paramètres pour un groupe spécifique d'utilisateurs du Hotspot






# HotSpot

LAB

- Ajoutez un second utilisateur au Hotspot
- Permettez l'accès à www.mikrotik.com sans authentification Hotspot pour votre laptop
- Mettez une limite de bande passante de 1M/1M pour votre laptop



# Tunnels

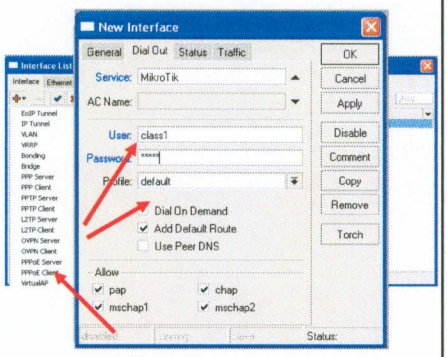


# PPPoE

- Point to Point Protocol over Ethernet est souvent utilisé pour contrôler les connexions desclients pour des réseaux DSL, modem cable et aussi des réseaux ethernet
- MikroTik RouterOS supporte PPPoE client et PPPoE server

# PPPoE Client Setup

- Ajoutez un client PPPoE
- Paramétrez l'**interface**
- Entrez le **nom d'utilisateur** et le **mot de passe**






# PPPoE Client

LAB

- Un serveur PPPoE va être créé sur le routeur principal
- Désactivez le client DHCP sur l'interface sortante de votre routeur
- Paramétrez un client PPPoE sur l'interface sortante
- Uilisez comme nom d'utilisateur **mtcna**, mot de passe **mtcna**



# PPPoE Client Setup

LAB

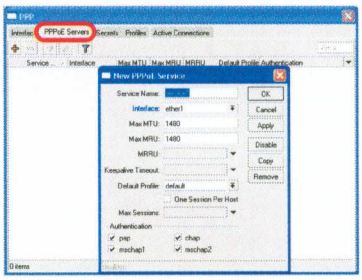
- Vérifier la connection PPP
- Désactivez le client PPPoE
- Activez le client DHCP pour restaurer l'ancienne configuration



# PPPoE Serveur Setup

LAB

- Selectionnez l'interface
- Selectionnez le profile

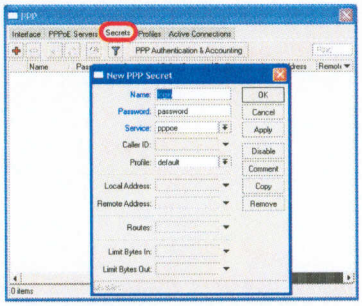





# PPP Secret

LAB

- Une database des clients des différents services
- Ajoutez un nom et un mot de passe
- Sélectionnez un service
- La configuration est prise depuis un "profile"



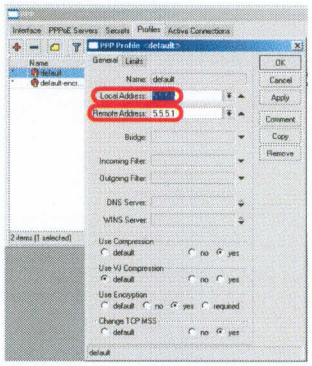



# PPP Profiles

- Ensemble des règles utilisées pour les clients PPP
- Moyen d'utiliser les mêmes paramètres de configuration pour différents clients

# PPP Profile

- **Local address** – adresse IP du serveur
- **Remote Address** – adresse IP du client






# PPPoE

- Important, le serveur PPPoE fonctionne sur une interface
- Une interface PPPoE peut être configurée sans adresse IP
- Pour des raisons de sécurité, il est préférable de configure l'interface PPPoE interface sans adresse IP

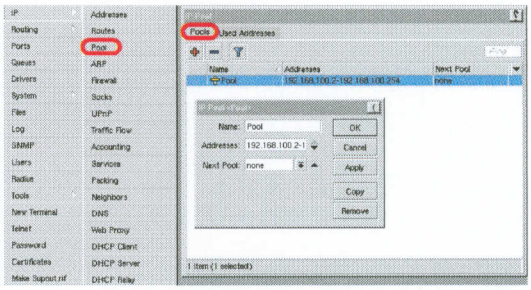


# Pools

- Un Pool définit un espace d'adresses IP pour les clients des services PPP, DHCP et HotSpot
- Nous allons utiliser un "pool", parce qu'il n'y aura plus qu'un seul client
- Les adresses sont prises dans le pool automatiquement

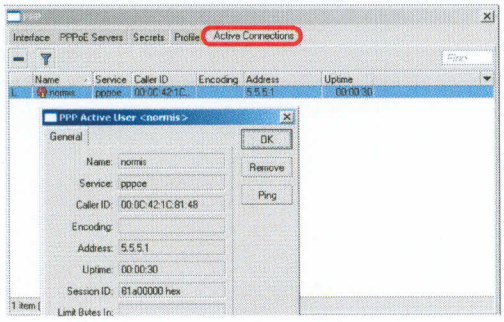


# Pool






# PPP Statut





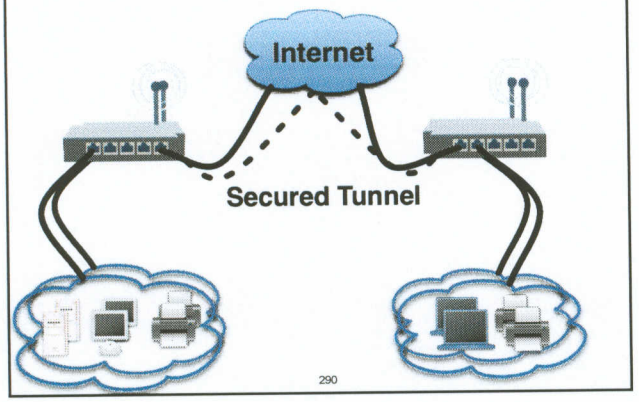

# PPTP

- Point to Point Tunnel Protocol permet de créer des tunnels encryptés
- MikroTik RouterOS inclut le support du client et du serveur PPTP

On peut l'utiliser pour:

- Sécuriser la liaison par internet entre des réseaux locaux
- Accéder à des ressources d'un réseau local depuis un client distant

# PPTP




290

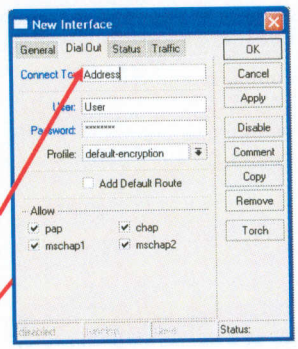
# Configuration PPTP

- La configuration PPTP est similaire à la configuration PPPoE
- La configuration L2TP est aussi similaire à celle des services PPTP et PPPoE

291

# Client PPTP

- Ajoutez une interface PPTP
- Entrez l'adresse IP du serveur PPTP
- Mettez l'utilisateur et le mot de passe




292

# PPTP Client

C'est suffisant pour la configuration du client PPTP

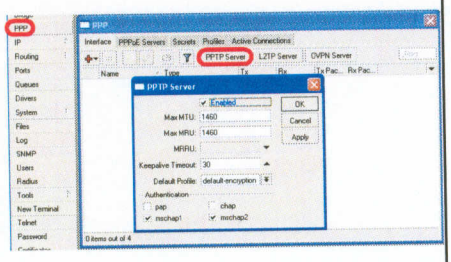
2 options:

- Utilisez l'option "Add Default Route" pour rediriger tout le traffic du routeur par le tunnel de la connexion PPTP
- Utilisez des routes statiques pour rediriger uniquement certaines connexions par le tunnel PPTP

293

# Serveur PPTP

- Le serveur PPTP peut assurer la connexion simultanée de plusieurs clients
- Activer ce service est aisé




294

# Clients du PPTP Server

- Les paramètres de connexion des clients PPTP sont enregistrés dans la section "ppp secret"
- Cette section "ppp secret" est utilisée pour les paramètres clients des connexions PPTP, L2TP et PPPoE
- ppp secret database est configurée sur le serveur

295

# Profile PPP

- Le même profil est utilisé pour les clients PPTP, PPPoE, L2TP and PPP



# PPTP

LAB

- Un serveur PPTP va être créé sur le routeur principal
- Configurez un client PPTP sur l'interface sortante
- Utilisez comme nom d'utilisateur **mtcna** et comme mot de passe **mtcna**
- Désactivez l'interface PPTP



# Résumé

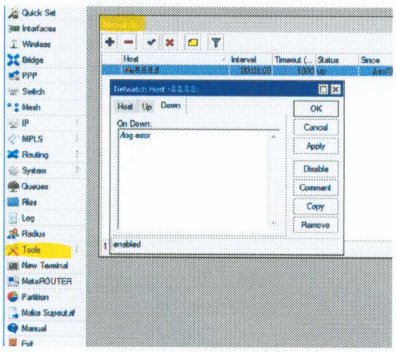


# Monitoring



# Netwatch

Outil intégré pour le monitoring de périphérique réseau






# Dude

- Network monitor program
- Automatic discovery of devices
- Draw and Layout map of your networks
- Services monitor and alerts
- It is **Free**

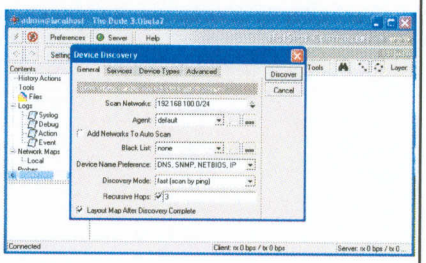
# Dude

- Dude consists of two parts:
  1. Dude server - the actual monitor program. It does not have a graphical interface. You can run Dude server even on RouterOS
  2. Dude client - connects to Dude server and shows all the information it receives



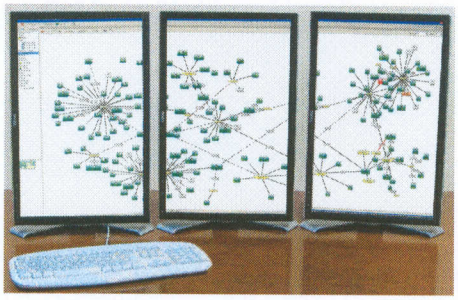
# Dude First Launch

- Discover option is offered for the first launch
- You can discover local network



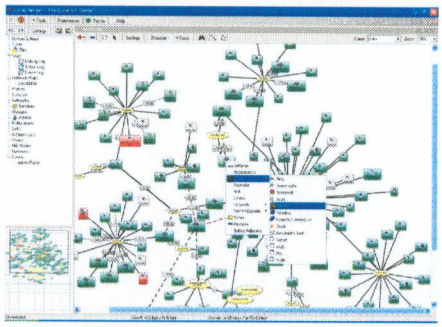



# Dude Usage





# Dude Usage





# Dépannage



# Mot de passe perdu?

- Sur certains routeurs, il existe un bouton reset (bouton, jumper ,…)
- Réinstallez le routeur (Netinstall)