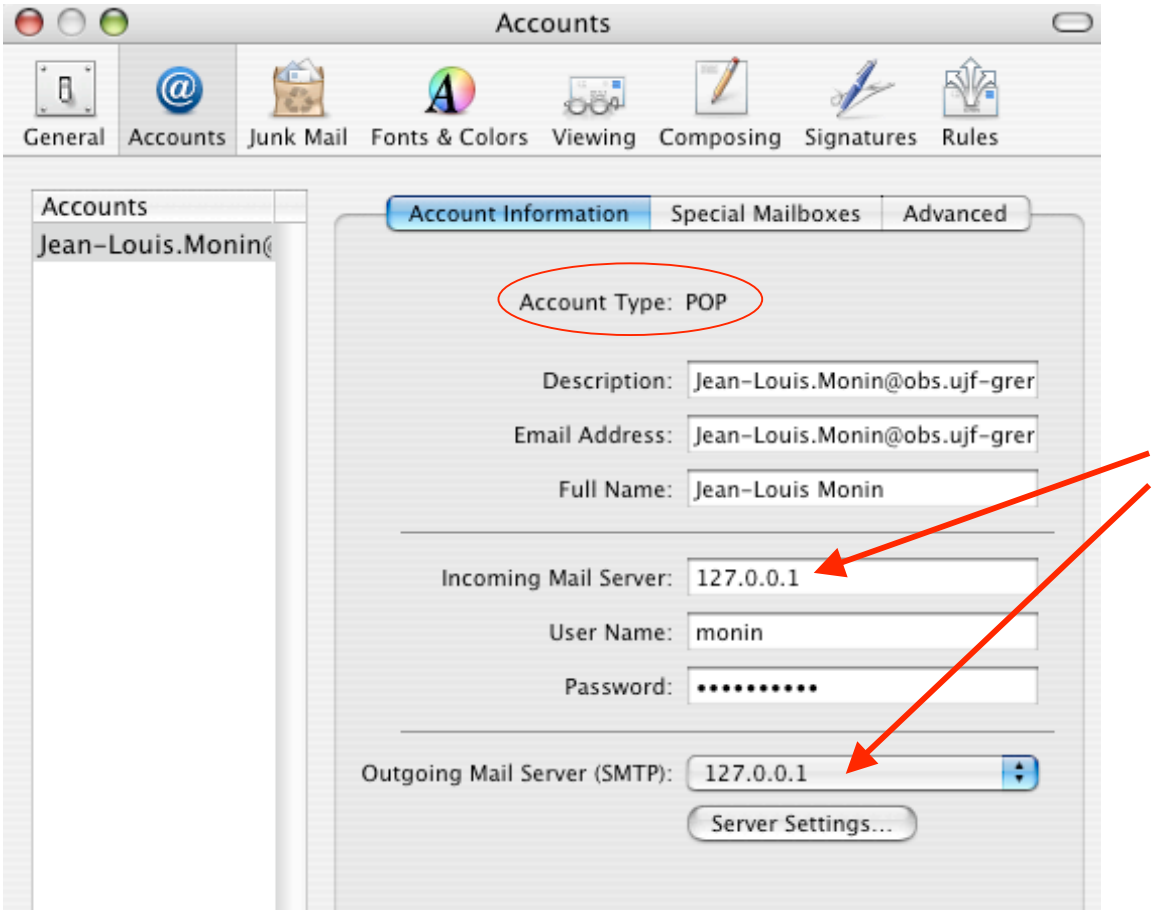
DOCS sur les Tunnels sous Mac OSX (et Mail)

Ce document donne une recette pour utiliser 'Mail', le programme de courrier apple, avec un tunnel connecté à une machine unix du labo.
Avantages : on peut lancer le tunnel de n'importe où (chez soi sous ADSL, à la guesthouse de l'ESO en DHCP, aux US, etc.), et on règle définitivement 'Mail' pour qu'il lise le courrier sur « 127.0.0.1 » (quezaco ? reportez-vous à ma doc précédente sur la question qui concernait les tunnels sous mac OS9, à l'époque des dinosaures, ou bien patientez, j'en reparle plus loin).
Inconvénients : on est obligé de lancer le tunnel en moyenne tous les jours, dès qu'on change de config réseau (ce genre de méthode concerne plutôt les possesseurs de portables qui changent de connexion réseau assez souvent, du labo au domicile).

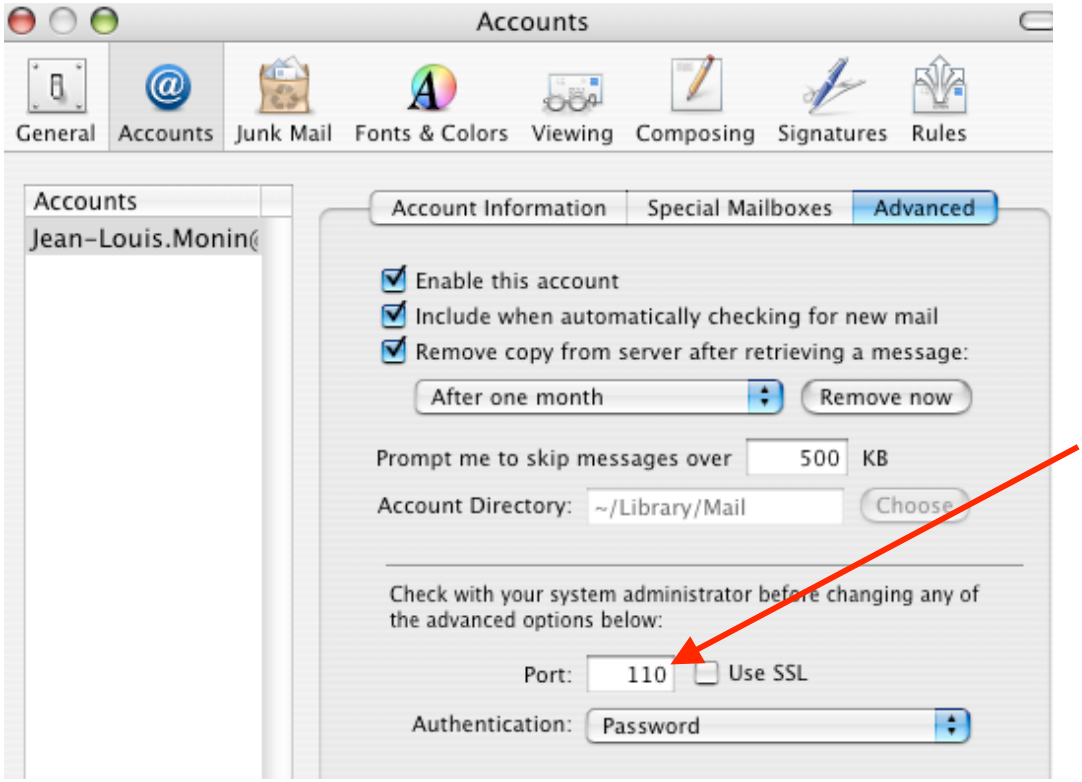
NB. Les réglages ont le look 'Mail 1.3.2 (v610/609)' sur mac OSX 10.3.2. Il se peut que les fenêtres de réglage de votre système soient un peu différentes, Je ne pense pas que ce soit bien grave.

Réglages de 'Mail'
Votre mailer doit être configuré pour lire les mails sur l'ordinateur sur lequel il tourne, c'est à dire sur le serveur d'adresse 127.0.0.1. C'est une convention que les ordinateurs s'appellent toujours eux-mêmes « 127.0.0.1 ». C'est ce qui rend le truc simple : vous n'avez plus à vous préoccuper de changer le serveur de mail, le SMTP, etc. ! Vous travaillez toujours avec 127.0.01. Voici le réglage :



Oui, j'utilise le mode « POP », on ne me fera pas changer d'idée, désolé. Si vous voulez utiliser IMAP, voyez d'autres gourous svp (mais a mon avis ca ne changera pas la philosophie de la méthode). Et tant qu'à faire, voyez ci-dessous le réglage de mon « Server Settings » (notez le port 25) :

J'ai aussi le réglage suivant dans l'onglet « advanced » (port 110) :



Je n'utilise donc pas SSL comme vous le voyez ; le mieux étant l'ennemi du bien, j'attends avec impatience qu'un autre explorateur l'essaye et me dise que ça marche bien pour le mettre en place.

Une fois que vous avez ce réglage effectué, il faut que vous ayez un tunnel actif, sinon 'Mail' appellera sa mère à chaque fois qu'il voudra lire le courrier car il ne se trouvera connecté à rien.

Mise en place du tunnel

Cette mise en place se fait au niveau système, c'est à dire par une commande sous terminal. Je vous passe les détails et je vous donne ci-dessous la commande magique que je tape, certes, 2 fois par jour.

Attention : **toute la phrase**, depuis « sudo » jusqu'à « 15000 » ***est sur la même ligne de commande***, ne faites pas attention à Word qui essaie de mettre en page ce document) :

```
sudo  ssh    -N    -f     -L110:195.220.79.11:110
-L25:195.220.79.11:25  -L143:195.220.79.11:143
monin@195.220.79.11  sleep 15000
```

Explication de texte :

• **sudo** : parce que les tunnels en deça de 1024 ne peuvent être créés que par un administrateur, vous avez donc besoin d'être « admin », et de connaître son mot de passe, pour créer les tunnels 25, 110, et 143 dont vous avez besoin.

• **ssh** : c'est le process tunnel itself

• **-N –f** : diverses option qui vont (très) bien, trust me.

• **-L<num> :195.220.79.11 :<num>** , où num = 110, 25, 143 : ça « connecte » les ports 110 (utilisé par POP pour rapatrier le courrier), 25 (utilisé par 'Mail' pour envoyer le courrier) et 143 (utilisé par IMAP pour rapatrier le courrier, quand je vous disais que ça aller marcher quand même !…)

• **monin@195.220.79.11** : c'est pour se lier au compte que vous possédez sur la machine dont l'adresse est 195.220.79.11, gagax1 au laog ici. Vous mettez votre identité de compte à la place de monin (vous ne pensiez pas lire mon courrier, non ?).

• **sleep 15000** : ca amène le tunnel à « s'effondrer » tout seul au bout de 15000 secondes, c'est à dire de l'ordre d'une demi-journée ; pas indispensable mais sécurité appréciable si on ne veut pas que votre machine reste jumelle de gagax1 trop longtemps.

Pour en savoir plus : taper « man ssh » sur votre clavier unix…

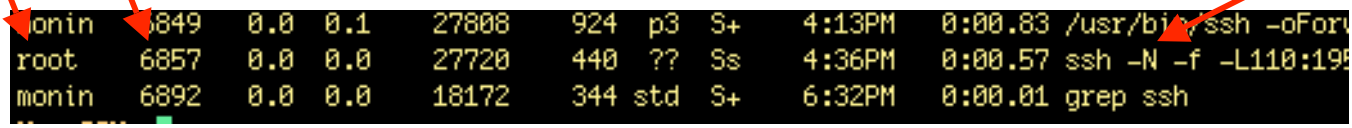
En pratique, j'ai un alias défini dans mon fichier .cshrc qui me permet de taper juste quelques lettres pour lancer le tunnel ; comme la commande implique « sudo « , le mac me demande mon mot de passe, puis, comme le tunnel se connecte à gagax1, c'est ensuite gagax1 qui me redemande mon mot de passe. Ensuite, c'est OK. 'Mail' fonctionne,

Que faire si j'ai déjà un tunnel mais qu'il ne marche plus ?

Ca vous arrivera si vous changez de configuration réseau. Par exemple vous mettez le portable en veille et vous rentrez chez vous où votre accès internet est géré différemment (en particulier, vous n'avez pas la même adresse, etc.). Le tunnel établi au laog ne peut plus marcher chez vous. Seule méthode connue de moi (dans l'ordre) :

1) vous réglez vos paramètres réseau pour être connecté correctement sur votre nouveau lieu de 'surf'

2) vous identifiez le numéro de process du tunnel déjà en place, en utilisant par exemple la commande : **`ps -aux | grep ssh.`**
Le système vous donne alors une suite d'informations assez absconses, qui ressemblent à ça :



Il y a bien un process appartenant à root (numéro **6857** dans l'exemple ci-dessus) qui concerne un tunnel (voir « ssh » vers la fin de la ligne).
3) vous « tuez » le process tunnel en cours par la commande : **`kill –9 6857.`**
Attention, dans cette commande le '-9' fait partie de la commande (c'est kill –9), et vous indiquerez bien sûr le numéro de process que vous aura renvoyé *votre* système.
4) vous relancez l'ordre de création de tunnel pour en avoir un adapté à votre nouveau lieu de travail.

et vous êtes reparti !!

NB1. Il arrive fréquemment que le process 'tunnel' s'effondre tout seul pendant l'intervalle qui sépare la déconnexion d'un lieu et la reconnexion au lieu suivant (et la définition des paramètres réseau adéquats). Dans ce cas, la commande « ps –aux … » ne vous montrera pas le tunnel en cours. Vous pouvez alors directement lancer le tunnel suivant.
NB2. Il arrive aussi que les tunnels aient la vie assez dure, en particulier ils peuvent résister un certain temps en apnée si votre machine ne fait pas d'accès réseau je suppose. Par exemple, de mon bureau à une salle de réunion ou de cours où je serais connecté de nouveau (sur la même adresse), ma machine se remet à lire le courrier comme si rien ne s'étais passé.
NB3. Si vous lancez un nouveau tunnel sans avoir tué le précédent, vous aurez un message d'erreur ressemblant à ça :

```
bind: Address already in use
channel_setup_fwd_listener: cannot listen to port: 110
bind: Address already in use
channel_setup_fwd_listener: cannot listen to port: 25
bind: Address already in use
channel_setup_fwd_listener: cannot listen to port: 143
Could not request local forwarding.
```

Vous n'avez plus alors qu'à tuer le nouveau tunnel pour laisser l'ancien respirer !

Good luck !