

## Séquence 1 - Applications

Jean.Saquet@info.unicaen.fr, cmoreira@info.unicaen.fr

### 1 Configuration avancée d'un navigateur

On utilisera mozilla (disponible sous toutes les plate-formes), et la version réduite mozilla-firefox, comportant uniquement le navigateur, alors que la version complète comporte également un client mail (voir section suivante) et un composeur. Sous Mozilla, les menus de configuration sont accessibles dans "édition, préférences" (ou dans "mozilla, préférences" pour la version MacOSX).

Les menus de configuration varient entre les différentes versions de navigateur, mais les mêmes termes se retrouvent généralement. Il suffit donc de chercher un peu pour trouver les paramètres souhaités.

- Le proxy doit être programmé pour pouvoir sortir du domaine privé. Le nom est "proxy.info.unicaen.fr", le numéro de port est 3128. Configurez ce proxy pour les protocoles http et ftp.
- La page d'accueil peut être personnalisée. Mettez `http://www.info.unicaen.fr` ou autre à votre convenance. Il est également possible de démarrer avec une page vierge, ou la dernière page consultée, ou de choisir un fichier local.
- Les caractéristique d'affichage peuvent être modifiées (police de caractères, taille, couleurs des liens, ...) mais attention, ceci ne fonctionne que si la page n'impose pas elle-même ses propres polices et autres caractéristiques, ce qui est de plus en plus fréquent (voir les feuilles de style - unité A3).
- Le cache est une mémoire locale qui permet de mémoriser les pages récemment consultée, afin de ne pas aller les rechercher sur le serveur distant en cas de nouvelle demande de l'utilisateur. Le navigateur peut comparer les dates (de la page et de la copie locale) pour savoir s'il doit aller la rechercher. ceci peut se faire à chaque fois, ou une fois par session, ou jamais. On peut spécifier la taille allouée au cache, son emplacement, et on peut l'effacer.
- L'historique mémorise non pas le contenu, mais les url des pages consultées. On peut définir le nombre de jours mémorisés, vider l'historique.

⇒ *Configurez tous ces paramètres dans votre (vos) navigateur(s) préféré(s).*

### 2 Configuration d'un client mail

L'utilisation d'un client mail nécessite de connaître les paramètres de son compte de messagerie. Les informations qu'il est indispensable de renseigner sont :

- Le serveur smtp ou serveur d'envoi de mail (ou mail sortant).
- Le serveur pop ou imap (serveur de mail entrant) et sa nature (pop ou imap).
- Votre identifiant d'utilisateur et votre mot de passe.
- Votre adresse de courrier électronique.

Pour les étudiants et étudiantes de notre département, voir : `http://mail.etu.info.unicaen.fr/params/`. Pour votre compte personnel, ces paramètres vous sont fournis par l'organisme qui vous procure un compte de messagerie.

D'autres paramètres peuvent également être renseignés dans la configuration du client mail pour une meilleure utilisation, en particulier :

- Votre nom complet, votre société
- L’adresse à utiliser pour les réponses (pas nécessairement la même que celle du compte configuré).
- Dans le cas d’utilisation de serveur pop, le choix de laisser ou non une copie des messages sur le serveur, et si oui combien de temps.

D’autres paramètres concernent la manière de rédiger les messages, d’y attacher une signature, de filtrer les messages reçus, de relever son courrier automatiquement ou non, ...

⇒ *Découvrez, configurez tous ces paramètres dans le logiciel sylpheed sous Linux, avec Mozilla sous Linux, et chez vous avec votre mailer préféré.*

### 3 Webmail

Pour les étudiants et étudiantes de notre département, accessible par : <http://mail.etu.info.unicaen.fr>. Ne nécessite de connaître que vos identifiant et mot de passe, et l’utilisation d’un navigateur. Nécessite de rester connecté à l’Internet le temps de la consultation et de la rédaction des messages. Les possibilités sont celles du logiciel Webmail de votre fournisseur (peuvent varier selon ceux-ci).

L’utilisation de notre webmail est indispensable si vous désirez changer votre mot de passe de votre compte de messagerie universitaire.

### 4 Aliases et listes de diffusion

Certains clients mail travaillent avec un carnet d’adresse qui permet de saisir un nom abrégé (alias) au lieu de l’adresse électronique lorsque vous rédigez un mail. Le logiciel remplacera cet alias par l’adresse du destinataire.

Des listes de diffusion ont été créées pour désigner des groupes d’utilisateurs. Par exemple, celle de votre promotion : [m2-mi3@etu.info.unicaen.fr](mailto:m2-mi3@etu.info.unicaen.fr). Elles permettent d’envoyer un mail à plusieurs personnes (celles inscrites sur la liste). Attention toutefois à l’utilisation de celles-ci :

- Ne joignez pas de fichier à un tel envoi (qui serait d’ailleurs refusé dans la plupart des cas), ceci pour ne pas encombrer plusieurs boîtes avec ce fichier. Indiquez plutôt aux correspondants (à l’aide d’un message envoyé à la liste) que le fichier est disponible dans un sous-répertoire de votre `public.html`.
- Lorsque vous répondez à un message envoyé à une liste, il pourra, selon la configuration du serveur de listes, être envoyé lorsque vous utilisez le bouton ”répondre” de votre logiciel à TOUTE la liste, ce qui peut être ce que vous souhaitez, mais pas forcément. Faites donc attention, contrôlez le champ ”destinataire” de tout message que vous envoyez.

⇒ *Faites des essais d’envoi de message(s) à la liste correspondant à votre promotion. Ajoutez à votre carnet d’adresse un alias plus court pour désigner cette liste.*

### 5 Accès à distance

Historiquement, le protocole TELNET a été défini pour cela, mais est de moins en moins utilisé pour des raisons de sécurité. Nous utiliserons donc ssh pour des connexions sécurisées.

⇒ *Connectez-vous sur une autre machine au moyen de la commande : `ssh <nom de machine>`*

Vous pouvez choisir comme machine celle du voisin dans la salle de TP ; ou bien `sully.info.unicaen.fr`. Remarquez que :

- La première fois que vous vous connectez sur une machine, celle-ci vous envoie sa "clef publique" et il faut que vous lui fassiez confiance (on pourrait imaginer qu'un pirate essaie de se substituer à cette machine pour enregistrer votre mot de passe).
- La machine vous demande ensuite votre mot de passe, et vous le demandera lors d'une prochaine connexion (on rompt la communication par `exit`).

Hormis le premier échange de clef publique, toute la communication (y compris présentation du mot de passe) est chiffrée, ce qui assure une bonne sécurité. Il y a possibilité d'éviter d'avoir à taper son mot de passe à chaque connexion, à condition de s'enregistrer sur la machine distante de la manière suivante :

- Générez vos clefs au moyen de `ssh-keygen` :  
`ssh-keygen -t rsa`  
`ssh-keygen -t dsa`
- Des fichiers ont été créés dans votre répertoire (caché) `/<home>/.ssh`, en particulier `id_rsa.pub` et `id_dsa.pub`. Il s'agit de vos "clefs publiques".
- Créez, dans votre répertoire `.ssh`, le fichier `authorized_keys` en y copiant vos clefs publiques :  
`cat id_rsa.pub id_dsa.pub >authorized_keys`
- Retirez tout droit sur le fichier `authorized_keys` à tout autre que vous-même.
- Essayez à présent de vous connecter par `ssh` à une autre machine.

⇒ *Exécutez les opérations ci-dessus afin de pouvoir ultérieurement vous connecter d'une machine à une autre sans présentation du mot de passe.*

Note : la copie simple (ici par `cat`) des clefs dans le fichier `authorized_keys` fonctionne parce que vos répertoires (en particulier le `.ssh`) sont accessibles de toute machine du réseau du département d'informatique. Si vous désirez reproduire la manip. pour vous connecter sans présentation du mot de passe sur une machine réellement distante, il faudra copier ces fichiers dans le répertoire `.ssh` de votre "home directory" de la machine distante, ceci au moyen de `ftp` (pas conseillé) ou de `scp` ou `sftp`, cf. ci-dessous, "transferts sécurisés".

Il est possible de connaître, à chaque instant, les utilisateurs connectés à une machine au moyen de la commande "who".

⇒ *Exécutez la commande `who` lorsque d'autres utilisateurs que vous-même sont connectés à votre machine.*

⇒ *De chez vous, créez vos clefs `ssh` sur votre machine personnelle, et ajoutez les à votre fichier `authorized_keys` en vous connectant à `sully.info.unicaen.fr`.*

N.B. : Pour vous connecter par `ssh` à partir d'un compte qui n'a pas nécessairement le même identifiant que votre login à l'université, utilisez :

```
ssh <login>@<machine>
```

⇒ *Dans la salle de TP, simulez une connexion à partir d'un compte différent du vôtre en réalisant un `ssh` à partir d'un terminal ouvert par votre voisin ou voisine sur sa machine.*

## 6 Transferts sécurisés

Il est possible d'utiliser des transferts de fichiers ou des copies de fichiers en mode sécurisé (équivalents à `ssh`). Les commandes correspondantes sont `sftp` et `scp`.

⇒ *Exécutez les commandes "man `sftp`" et "man `scp`" pour connaître leurs possibilités. Essayez ces commandes entre deux machines (avec des identifiants différents entre fichiers source et destination, sinon ça*

*ne présente aucun intérêt dans la mesure où vous accédez à tous vos fichiers à partir de n'importe quelle machine du département).*

Pour transférer vos fichiers entre chez vous et votre compte universitaire, vous pouvez utiliser sftp.

*⇒ Utilisez une machine windows de la salle 138 pour vous connecter à votre compte universitaire en sftp ou scp au moyen de l'outil WinSCP3.*