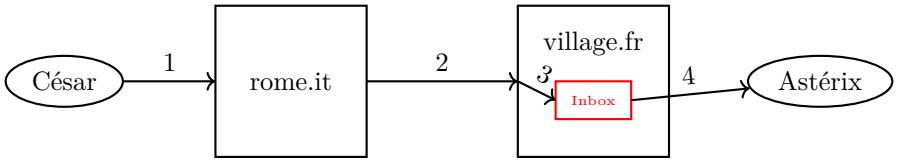
TP4 : Protocoles mail

1 Fonctionnement

Pour illustrer le fonctionnement des mails, on considère l'exemple suivant : l'utilisateur `Cesar` du serveur `rome.it` veut envoyer un message à l'utilisateur `Asterix` du serveur `village.fr`. La chaîne de transmission utilise plusieurs intermédiaires :

1. le MUA (Mail User Agent) de `Cesar` : il s'agit du client de messagerie de `Cesar`, qui crée le mail et l'envoie à `rome.it`.
2. un ou plusieurs MTA (Mail Transfer Agent) : il s'agit d'applications qui relayent le mail de serveur en serveur à partir de `rome.it` jusqu'à ce qu'il arrive à `village.fr`
3. le MDA (Mail Delivery Agent) : une application du serveur `village.fr` qui va déposer le courrier reçu dans un dossier spécifique (la boîte aux lettres d'`Asterix`).
4. le MUA d'`Asterix` : le client de messagerie d'`Asterix` qui va récupérer les mails reçus sur `village.fr`



La suite de ce TP est divisée en deux parties. Dans la première, on s'intéresse à ce qu'est un mail (en pratique) et au fonctionnement des protocoles mis en jeu :

— SMTP pour l'acheminement

— POP et IMAP pour la récupération de mails sur le serveur d'arrivée.

2 Contenu d'un mail

Un mail est un document texte constitué d'un *en-tête*, d'un *corps* et (éventuellement) d'une ou plusieurs pièces jointes.

Traditionnellement, votre application de messagerie favorite découpe ce fichier, affiche le corps du mail et extrait les informations utiles de l'en-tête. Il est possible d'obtenir le mail au format original ou au moins l'en-tête (par exemple « afficher l'orginal » sur gmail, ou « afficher les détails du message » sur le webmail de l'université).

Afficher l'original/l'en-tête de plusieurs de vos mails, puis inférer des réponses aux questions suivantes.

1. Quels champs permettent de connaître l'expéditeur/le destinataire ?
2. À quoi sert le champ `Return-Path` ?
3. Expliquer le contenu des champs `Received`.
4. Comment peut-on retrouver le temps d'acheminement du mail ?

Remarque : L'en-tête des mails est généré par l'utilisateur (ou plutôt son MUA), puis modifié par les MTA qui ajoutent petit à petit des informations. En particulier, rien n'oblige l'expéditeur à les remplir avec des informations valides. Un exemple flagrant est fourni par l'adresse de l'expéditeur : rien n'empêche [1] `Cesar` de remplir le champ `From` avec l'adresse `obelix@village.fr` !

5. Comment peut-on (espérer) détecter une telle usurpation ?

3 Acheminement

Le protocole SMTP (Simple Mail Transfer Protocol) sert à transférer des mails, comme son nom l'indique. Il fonctionne sur le principe client-serveur en mode connecté (sockets TCP). Le port traditionnellement utilisé est le port 25 (les variantes sécurisées utilisent 465 ou 587).

Une communication se base généralement sur le modèle suivant :

Client : `HELO` <ip-client>
Serveur : `250` <ip-serveur>
Client : `MAIL FROM:` <adresse-exp>
Serveur : `250` OK
Client : `RCPT TO:` <adresse-dest>
Serveur : `250` OK
Client : `DATA`
Serveur : `354`
Client : <en-tête>
Client : <corps>
Client : .
Serveur : `250` OK
Client : `QUIT`
Serveur : `221` Bye

```
HELO localhost
250 stadium.univ-lyon1.fr
MAIL FROM: cesar@rome.it
250 2.1.0 Ok
RCPT TO: asterix@village.fr
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Commande de menhirs

Ave Asterix,
[...]

.
250 2.0.0 Ok: queued as D6983EC0028
QUIT
221 2.0.0 Bye
```

Les réponses du serveur commencent (comme pour HTTP) par un nombre indiquant le type de réponse, suivi d'un message la détaillant. 2xx signifie que tout va bien, 354 est une réponse à DATA, et 4xx/5xx indiquent une erreur.

3.1 Installation

Dans la suite du TP, on veut pouvoir envoyer des mails à l'aide du protocole SMTP. Vous avez accès aux serveurs SMTP de l'université ou de vos boîtes mails personnelles. Cependant, il est probable qu'ils requièrent une authentification, ainsi qu'une connexion sécurisée afin de ne pas transmettre vos mots de passe en clair sur le réseau. On va donc commencer par installer un serveur SMTP sur vos machines (pensez à le désactiver à la fin du TP).

1. ... matériellement, par contre légalement c'est une autre histoire

— Sous Linux, un simple `sudo apt-get install postfix` règle la question (choisir « site internet »).

— Sous Windows, vous pouvez consulter `https://www.hmailserver.com/` pour installer et configurer le serveur.

3.2 Votre premier mail (au terminal)

En utilisant `telnet localhost 25` dans un terminal, communiquez avec votre serveur afin de vous envoyer un mail :

— Sur la même machine (à `<user>@localhost`)

— Sur votre adresse étudiante

— En changeant <ip-client> et/ou <adresse-exp>

Vérifiez que vous avez reçu ces mails (consultez la documentation pour savoir où sont stockés les mails reçus).

3.3 Scriptage

Écrire un programme qui prend en entrée une liste de noms et d'adresses mails et envoie à chaque adresse un mail personnalisé contenant « Bonjour <nom> ! ».

Remarque : Pour rester dans la légalité, n'utilisez que des adresses mail qui vous appartiennent pour les destinataires.

3.4 Failles

Expliquer comment une personne mal intentionnée (ayant accès au réseau) pourrait :

— Lire les mails reçus par un utilisateur donné

— Envoyer des mails en se faisant passer pour un autre utilisateur

4 Post Office Protocol

4.1 Fonctionnement

POP est un protocole de communication fonctionnant sur le modèle client-serveur, en mode connecté. Le port utilisé est traditionnellement 110. Il s'agit d'un protocole simple permettant de s'authentifier, récupérer son courrier et de gérer les erreurs.

Les commandes sont :

— USER <user>, PASS <password>

— STAT, LIST

— RETR, TOP

— DELE, RSET

— NOOP

— QUIT

Si ce n'est pas déjà fait, créez deux utilisateurs `Asterix` et `Cesar` dans hmailserver, et faites leur échanger quelques mails. Utilisez ensuite la commande `telnet localhost 110` pour tester le protocole POP et répondre aux questions suivantes.

1. Quels sont les deux types de réponses du serveur ? Quelle est leur syntaxe ?
2. Expliquer ce que renvoient les commandes STAT, LIST, et LIST <entier>.
3. La commande RETR prend un entier comme argument, tandis que TOP en prend deux. Tester et expliquer leur fonctionnement. Quelle utilité a la commande TOP <entier> 0 ?
4. Les commandes DELE et RSET gèrent la suppression de messages. Authentifiez vous, puis lancez (dans l'ordre) les commandes DELE 1, LIST, RSET, LIST. En déduire à quel moment le serveur supprime effectivement le message 1.
5. La commande NOOP ne fait rien. À quoi peut-elle donc servir ?

4.2 Scriptage

Écrire un programme chargé d'afficher sur la sortie standard tous les mails reçus par un utilisateur, et de les supprimer d'un serveur POP.

4.3 Avantages et inconvénients

6. Le protocole POP est-il sécurisé ?
7. Est-il possible d'utiliser le protocole POP pour récupérer ses mails sur plusieurs machines (ordinateur + smartphone, par exemple) ? Si oui, est-ce une bonne idée ?

En général, les MUA utilisant POP n'effectuent que les opérations suivantes :

— Ouverture de la connexion TCP

— Authentification

— Récupération de tous les mails

— (Effacement de tous les mails reçus du serveur)

En particulier, ceci génère un trafic important puisque tous les mails transitent sur le réseau même si on ne souhait accéder qu'à un seul. Ceci est à prendre en compte pour les connexions à faible débit (encore aujourd'hui !).