R303 Messagerie

Laurent Billon

5 septembre 2023

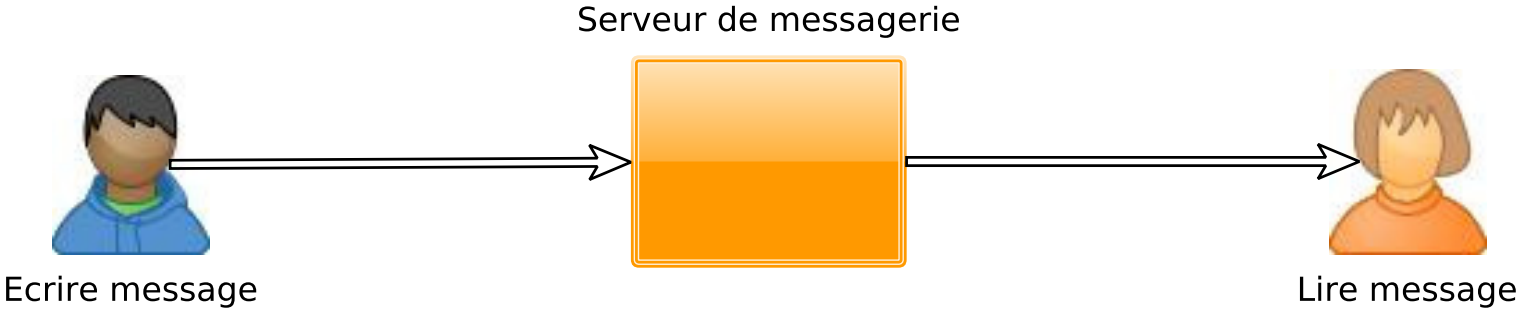
MESSAGERIE

La messagerie électronique est le principe d'envoi d'un courrier via la Poste.

1. Rédaction du message
2. Acheminement du message au destinataire
3. Lecture du message

Pour effectuer ces actions, il faut :

1. Adresse de messagerie pour l'expéditeur
2. Adresse de messagerie pour le destinataire
3. Logiciel pour la rédaction du message
4. Logiciels pour l'acheminement du message
5. Logiciel pour la lecture du message


Serveur de messagerie
Ecrire message
Lire message

Le système AUTODIN est un des premiers à utiliser le système de messagerie.
Le réseau ARPANET permit de faire avancer le projet de messagerie électronique.
En 1972 Ray Tomlinso proposa le afin de séparer le nom de l'utilisateur de la machine.

Les adresses de messagerie ont été définit la première fois dans la RFC 822

La derniere version est la RFC RFC 3696
Les adresses internet ne font pas de distinction minuscule et majuscule (sauf dans les commentaires et chaine de caractères).

- Adresse globales sont des adresses qui spécifient un site sans spécifier un chemin pour y arriver. Elles sont valides sur tout Internet
  - nomprenom@nom.tld : adresse standard
  - <nomprenom@nom.tld> : la présence de < et > indique une adresse exploitable facilement par un programme
  - nom prenom <nomprenom@nom.tld> : un commentaire est ajouter un programme privilégie ce qui est entre < et >
  - "nom prenom" <nomprenom@nom.tld> : le commentaire est vu comme un mot unique car entre "", peut être ajouter à tout type d'adresse internet

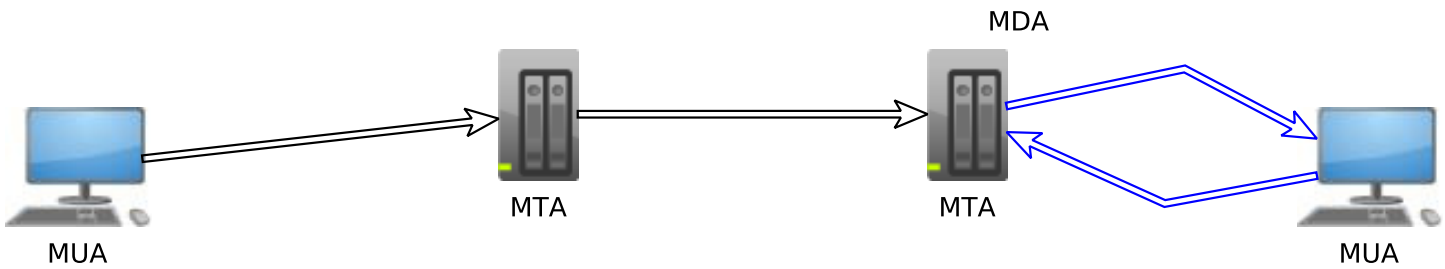
- adresse littéral : nomprenom @ [adresseip] : la présence des crochets indique une adresse numérique. Le message doit être envoyé tel quel, sans autre traitement ne pas tenir compte des MX. Ce type d'adresse est déconseillé.
- adresse vide : <> : Cette adresse, que peu de sites savent encore gérer correctement, est une adresse à laquelle, nous ne pouvons pas répondre. Lorsqu'un message d'erreur est généré, l'adresse de l'expéditeur du message d'erreur doit être initialisée à cette adresse. La plupart des sites utilisent aujourd'hui des noms comme Postmaster

Au départ le contenu était un message au format ASCII.
L'utilisation de l'UTF-8 se standardise.
Multipurpose **I**nternet **M**ail **E**xtension.
MIME est définit dans la RFC RFC 2045, la RFC RFC 2046, la RFC RFC 2047, la RFC RFC 2048.
Cela permet de joindre différents type de fichiers, il est déconseillé de joindre des fichiers en format propriétaire.

Pour chaque rôle, il existe au minimum un service

1. Logiciel pour la rédaction, lecture de courriel :
   - Client de messagerie lourd
   - Client de messagerie léger (web)
2. Envoi de message : SMTP
3. Réception de message : POP, IMAP

Les clients de messageries sont des **M**ail **U**ser **A**gent
Le client transmet au **M**ail **S**ubmission **A**gent qui va transmettre le message au premier message au premier **M**ail **T**ransfert **A**gent
Les services permettant l'acheminement des messages sont des **M**ail **T**ransfert **A**gent
Le MTA final délivre au **M**ail **D**elivery **A**gent le message qui sera transmis au client final.


MDA
MTA
MTA
MUA
MUA

Lors de l'envoi de message, il est possible :

- Faire une **C**opie **C**arbone
- Faire une **C**opie **C**arbone **I**nvisible
- Demander un accusé de réception
- Chiffrer le message

SMTP

Le Simple Mail Transfer Protocol est un protocole permettant le transfert de message électronique vers des serveurs de messagerie.
La première définition du SMTP est dans la RFC RFC 821 de 1982
La dernière en date est la RFC RFC 5321 de 2008.
Le SMTP utilise les ports :

- 25 en TCP
- 587 en TCP pour les connexions TLS.
- 465 en TCP pour les connexions SSL.

Le SMTP utilise des codes retour sur 3 chiffres. Le premier indique un statut global

- code 2 : demande exécutée sans erreur
- code 3 : demande en cours d'execution
- code 4 : erreur temporaire
- code 5 : demande non valide.

En 2006, il fut recommandé au FAI de bloquer le port 25.
Les FAI utilisent la connexion sur le port 587 avec authentification.

Installer un serveur SMTP sur Debian

```
#apt install postfix
```

POP

Le Post Office Protocol est un protocole permettant de récuperer des messages
La première définition du POP est dans la RFC RFC 937 de 1984
La dernière en date est la RFC RFC 1939 de 1996.
Le POP utilise les ports :

- 110 en TCP
- 995 en TCP pour les connexions SSL.

La dernière version est POP3, voici la liste des commandes :

- DELE numéromessage : efface le message spécifié
- LIST : donne une liste des messages ainsi que la taille de chaque message : un numéro suivi de la taille en octets ;
- RETR numéromessage : récupère le message indiqué ;
- STAT : indique le nombre de messages et la taille occupée par l'ensemble des messages ;
- TOP numéromessage nombrelignes : affiche les premières lignes du message.

- APOP : permet une authentification sécurisée (le mot de passe ne transite pas en clair) ;
- NOOP : ne rien faire, utile pour ne pas perdre la connexion et éviter un « délai d'attente dépassé » ;
- QUIT : quitter la session en cours ;
- RSET : réinitialise complètement la session ;
- UIDL : affiche (pour un seul ou pour tous les messages) un identifiant unique qui ne varie pas entre chaque session ;
- CAPA : affiche les informations du serveur.

Installer un serveur POP3 sur Debian

```
#apt install dovecot-pop3d
```

IMAP

Le **I**nteractive **M**essage **A**access **P**rotocol est un protocole permettant de récuperer des messages
La première définition de IMAP est dans la RFC RFC 3501 de 1986
La dernière en date est la RFC RFC 1939 de 1996.
IMAP utilise les ports :

- 220 en TCP pour IMAP3
- 143 en TCP pour IMAP2 et 4
- 143 en TCP pour les connexions TLS IMAP4
- 993 en TCP pour les connexions SSL

Installer un serveur IMAP sur Debian

```
#apt install dovecot-imapd
```

SECURITE

Le pourriel (SPAM) qui concerne les messages non-solicités, souvent ce sont de s messages publicitaire envoyés en masses.
Le premier pourriel fut envoyé le 3 mai 1978 par Gary Thuerk, marketeur. Il envoya son message à près de la totalité des utilisateurs d'ARPAnet vivant sur la côte ouest des États-Unis, soit environ 600 personnes.
En 2016 2,672 milliard de courriels échangés.
Le pourriel représente de 50 à 95% des messages selon le moment.
90% de ces pourriels est filtrés en amont.

La fraude (scam) est d'abuser de la crédulité des personnes afin d'obtenir de l'argent.
La plus connue est la fraude 419 (aussi appelée scam 419, ou arnaque nigériane) est une escroquerie répandue sur Internet. La dénomination 4-1-9 vient du numéro de l'article du code nigérian sanctionnant ce type de fraude.

Voici un exemple de courrier destiné à lancer une fraude 4-1-9 :

De : Fred Kone
Tel :***-********
Courriel :****@yahoo.com
Bonjour,
Je m'appelle Fred Kone je suis âgé de 26 ans et je vis en Côte d'Ivoire.

Malheureusement comme vous le savez mon pays traverse une période très difficile ce qui m'a contraint à fuir ma région d'habitation qui est Bouaké (dans le centre du pays). Mon père était un marchand de cacao très riche à Abidjan, la capitale économique de la Côte d'Ivoire.

Avant qu'il n'ait été grièvement blessé par les rebelles, urgemment conduit à l'hôpital il m'a fait savoir qu'il avait déposé 5 000 000 $ dans une mallette dans une société de sécurité basée à Abidjan.

A l'annonce de la mort de mon père je me suis précipité dans sa chambre dans le but de prendre tout ce qu'il avait comme document administratif, j'ai découvert le certificat de dépôt délivré par la compagnie de sécurité à mon père. Une fois arrivé à Abidjan j'ai essayé de vérifier la validité de ce document.

Le directeur de la société m'a confirmé l'existence de cette mallette dans leur établissement. De peur de perdre cet argent, je sollicite l'aide de quelqu'un afin de transférer ce seul bien que mon père m'a légué dans un pays étranger pour investir car la situation en Côte d'Ivoire est toujours incertaine.

Une fois le transfert effectué je me rendrai là-bas pour récupérer cet argent et y faire ma vie. Si vous êtes prêt à m'aider, envoyez-moi vite une réponse afin que l'on puisse trouver un conciliabule. Dans l'attente d'une suite favorable recevez mes salutations et que dieu vous bénisse.

PS : N'oubliez pas de me contacter directement à mon adresse privée :****@yahoo.com

La fraude 4-1-9 a été à l'origine de plusieurs morts violentes :

- En 1995, un Américain a ainsi été assassiné à Lagos, au Nigeria, après avoir tenté de récupérer son argent.
- En 2003, un Tchèque a tué par balle un diplomate nigérian qu'il prenait pour un responsable de l'escroquerie.
- En 2004, un Britannique s'est suicidé suite à une dépression provoquée par une escroquerie par scam.
- En 2004, un Grec, victime de scam, a été kidnappé à Durban en Afrique du Sud. Une rançon a été demandée mais n'a pas été payée. Il a été mutilé puis assassiné.

Les canulars (HOAX) se trouvent souvent sous la forme de courriel ou de simple lettre-chaîne. Dans ce dernier cas, Internet ne fait qu'amplifier un phénomène qui existait déjà à travers le courrier traditionnel.
À la différence des pourriels qui sont la plupart du temps envoyés de manière automatisée à une liste de destinataires, les canulars sont, eux, relayés manuellement par des personnes de bonne foi à qui on demande de renvoyer le message à toutes ses connaissances, ou à une adresse de courrier électronique bien précise.

Exemple : Cuire un œuf avec un portable : deux scientifiques russes auraient réussi à faire cuire un œuf placé entre deux téléphones cellulaires grâce à l'énergie émise par ceux-ci

La bombarderie (MAIL-BOMBING) Le mail-bombing est une technique d'attaque visant à saturer une boîte aux lettres électronique par l'envoi en masse de messages quelconques par un programme automatisé.
Cela se traduit concrètement par l'envoi d'une grande série de courriels à la même personne dans l'intention de bloquer sa boîte de messagerie (dont la capacité est généralement limitée chez le FAI / Hébergeur).

L'hameçonnage ou (PHISING), est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels :

- mot de passe
- numéro de carte de crédit
- date de naissance
- etc.

C'est une forme d'attaque informatique reposant sur l'ingénierie sociale (sécurité de l'information). L'hameçonnage peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques.