Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Hes·so

Téléinformatique – Ch. 15

Mail

Vincent Magnin
vincent.magnin@hefr.ch

Objectifs

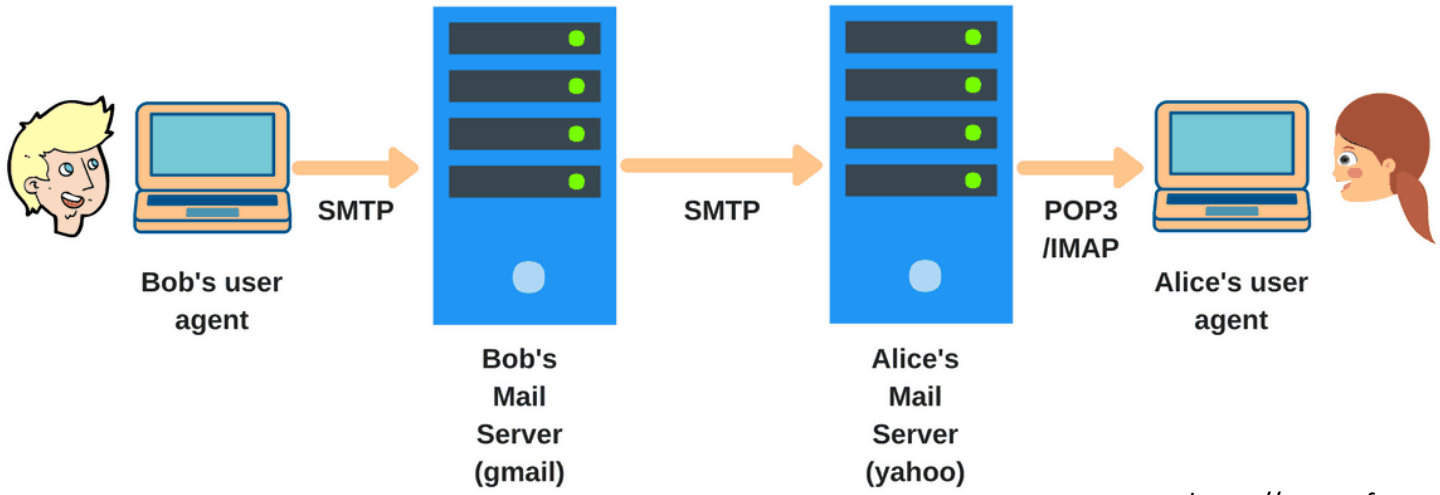
- Connaître les principaux protocoles mail.
- Connaître les commandes de SMTP et POP3.
- Connaître le processus d'acheminement des emails.

Généralités

L'email a considérablement changé notre manière de communiquer. C'est l'un des services les plus utilisés sur Internet.

Cette technologie utilise 3 protocoles principaux :

- SMTP pour les échanges de messages vers le serveur (envoi d'un email).
- POP3 et IMAP pour la récupération des messages sur les serveurs (réception)



https://www.afternerd.com/blog/smtp/

Protocole SMTP

Le protocole SMTP (Simple Mail Transfer Protocol) est le protocole standard pour l'envoi de courrier électronique. Il utilise le modèle C/S et est transporté sur le port 25/TCP.

Les commandes sont des lignes de textes terminées par un retour à la ligne.

Protocole SMTP (2)

Les commandes principales du protocole sont les suivantes :

- HELO ou EHLO : suivie du nom de domaine ou de l'utilisateur, sert à s'annoncer au serveur.
- MAIL FROM : sert à définir l'adresse de l'expéditeur.
- RCPT TO : sert à définir l'adresse du destinataire.
- DATA : suivie du corps du message, se termine par un retour à la ligne suivit d'un point, puis d'un retour à la ligne.
- QUIT : ferme la connexion.

Protocole SMTP (3)

Valide connexion client	S: 220 smtp.server.com Simple Mail Transfer Service Ready
Identification du client	C: HELO client.example.com S: 250 Hello client.example.com
Définition de l'expéditeur	C: MAIL FROM:<mail@samlogic.com> S: 250 OK
Définition du destinataire	C: RCPT TO:<john@mail.com> S: 250 OK
Transmission du message	C: DATA S: 354 Send message content; end with <CRLF>.<CRLF> C: *<The message data (body text, subject, e-mail header, attachments, etc) is sent>* C: .
Confirmation de réception	S: 250 OK, message accepted for delivery: queued as 12345
Terminer la session	C: QUIT S: 221 Bye

Protocole SMTP (4)

Comme pour différents protocoles (HTTP notamment), le protocole SMTP possède des codes de réponses qui sont transférées du serveur au client. On les appelle aussi des *status codes*.

Les principaux sont les suivants :

- 1xx : le serveur attend une confirmation.
- 2xx : la requête a été exécutée.
- 3xx : le serveur a besoin de plus d'informations.
- 4xx : une erreur temporaire est survenue.
- 5xx : le traitement de la requête n'est pas possible.

SMTP- Sécurité

Avant

Problème	Explication
Pas de chiffrement natif	Les commandes (`MAIL FROM`, `RCPT TO`, `DATA`) et le contenu du mail sont **envoyés en clair**, donc interceptables par un attaquant sur le réseau.
Pas d'authentification forte obligatoire	SMTP historique permettait d'envoyer un mail sans prouver qui tu es → ouverture aux **spoofing et relay spam**.
Pas de vérification de l'identité du destinataire	Le serveur SMTP accepte un mail pour n'importe quelle adresse, ce qui facilite le **spam**.
Pas de protection de l'intégrité	Rien n'empêche de modifier le contenu d'un mail en transit.

💬 En résumé : SMTP seul = **texte clair + aucune sécurité**, ce qui était acceptable dans les années 80 mais pas aujourd'hui.

Actuel

a) TLS (STARTTLS ou SMTPS)

- **Chiffre la connexion** entre client et serveur, ou serveur à serveur.
- Ports courants :
  - 587 → SMTP avec STARTTLS (recommandé pour envoi client → serveur)
  - 465 → SMTPS (SMTP implicite sécurisé)
- **Avantage :** le mot de passe et le contenu sont chiffrés en transit.

b) Authentification obligatoire

- `AUTH LOGIN` ou `AUTH PLAIN` → mot de passe envoyé dans la session chiffrée.
- OAuth2 → token d'accès à la place du mot de passe (Gmail, Outlook...).
- Évite le **spoofing depuis un client externe**.

c) Filtrage et validation côté serveur

- SPF, DKIM, DMARC → assurent que l'expéditeur est légitime.
- Permet de **réduire le spam et l'usurpation d'identité**.

Protocole POP3

Le protocole POP3 (Post Office Protocol version 3) permet de récupérer du courrier électronique sur un serveur. Il utilise le port 110/TCP.

Son fonctionnement est assez simple :

1. Connexion au serveur.
2. Téléchargement des mails en local.
3. Optionnellement, suppression de ces mails sur le serveur.
4. Déconnexion.

Protocole POP3 (2)

Les commandes principales du protocole sont les suivantes :

- USER : nom du compte.
- PASS : mot de passe (envoyé en clair ! Solution: POP3S)
- LIST : donne une liste des messages (un numéro) ainsi que leur taille (en octets).
- DELE <numéro message> : efface le message spécifié.
- RETR <numéro message> : récupère le message spécifié.
- STAT : indique le nombre de messages et la taille occupée par l'ensemble des messages.
- TOP <numéro message> <nombre de ligne> : affiche les premières lignes du message spécifié.

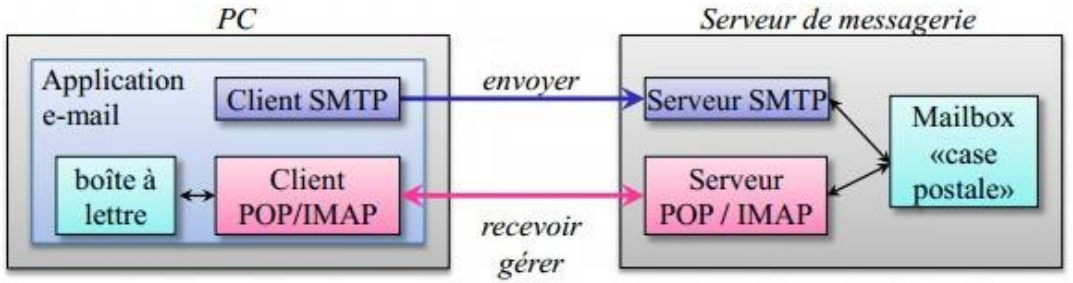
Protocole IMAP

Le protocole IMAP (Internet Message Access Protocol) utilise le port 143/TCP et possède plusieurs avantages par rapport à POP3.

Il y a notamment la notion de synchronisation : les emails restent sur le serveur IMAP et peuvent être gérés à distance par le client.

D'autres avantages existent, comme par exemple :

- La possibilité de permettre à plusieurs clients de gérer la même boîte mail simultanément (POP3 bloque la boîte mail pendant un accès).
- La possibilité d'envoyer des webmails.



Acheminement des emails

Pour transférer, envoyer et acheminer des emais, différentes entités existent :

Le MUA (Mail User Agent) :

- Représente le client de messagerie (Outlook, Thunderbird...).
- Permet la gestion de la boîte aux lettres.

Le MTA (Mail Transfert Agent) :

- Fonction d'un serveur mail chargé de l'envoi à d'autres MTA ou MDA.
- Analogie possible : bureau de poste.

Le MDA (Mail Delivery Agent) :

- Fonction d'un serveur mail chargé de délivrer le courrier aux MUA.
- Analogie : boîte aux lettres.

Références

- Ancien cours « Téléinformatique » (G. Waeber, S. Paccard, Q. Vaucher, N. Wirth).
- Ancien cours « Téléinformatique » (M. Roch-Neirey).