

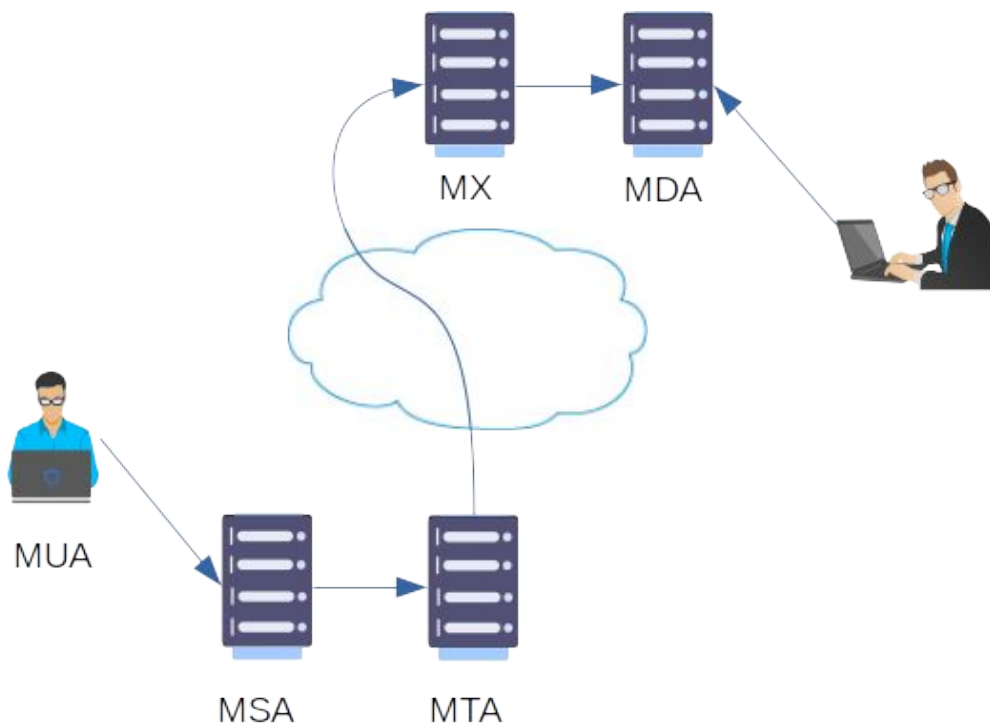


## SMTP: comment vos emails sont transportés

### Le parcours de l'email

**SMTP** (**S**imple **M**ail **T**ransport **P**rotocol) est un protocole de communication standard Internet pour la transmission d'emails. SMTP décrit comment vos emails sont envoyés depuis votre client de messagerie sur votre PC ou téléphone ou votre interface webmail jusqu'à leur destination.

Le parcours complet d'un email peut être représenté comme suit :



Quelques definitions:

- **MUA:** Mail User Agent: un client de messagerie comme Outlook, Thunderbird ou Gmail, que l'utilisateur utilise pour écrire et envoyer ses emails;
- **MSA:** Mail Submission Agent: la partie serveur de messagerie qui communique avec le MTA, généralement sur le port TCP 25 ou 587 en cas d'utilisation du chiffrement, et délivre le courrier au MTA;
- **MTA:** Mail Transfer Agent: la partie serveur de messagerie qui va déterminer où envoyer l'email vers le destinataire. Le MTA va chercher dans l'enregistrement DNS MX la partie domaine de l'adresse du destinataire pour trouver où envoyer l'email;
- **MX:** le MTA de destination;
- **MDA:** Mail Delivery Agent: le composant qui va stocker l'email reçu dans la boîte mail du destinataire.

Notez que plusieurs composants peuvent en fait partager le même serveur.

Toutes les transmissions entre les différents agents se font via le protocole SMTP. La récupération proprement dite de l'email par le destinataire se fait par d'autres moyens que nous expliquerons dans de prochains articles.

## Le langage de transmission des emails

### Définition

Comme son nom l'indique, SMTP est un **protocole**, c'est-à-dire un ensemble de commandes et de réponses standardisées entre les composants pour qu'ils puissent se comprendre.

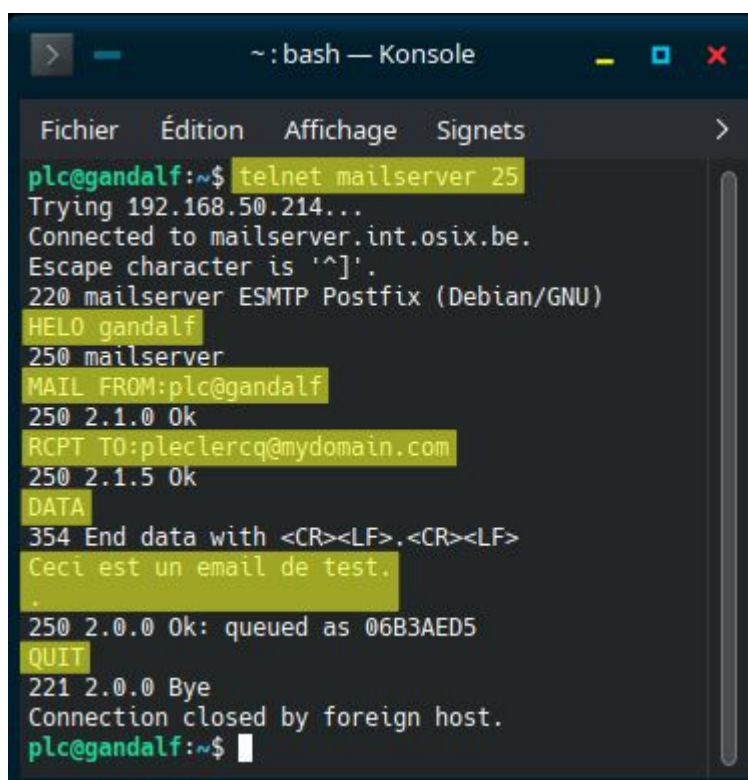
Vu du MUA (l'agent mail), ce protocole est vraiment très simple (comme encore une fois son nom l'indique).

Le protocole est basé sur 5 commandes principales :

- **HELO**: utilisé par le client pour s'identifier;
- **MAIL FROM**: utilisé par le client pour identifier l'expéditeur;
- **RCPT TO**: utilisé par le client pour identifier le destinataire;
- **DATA**: introduit le contenu réel de l'email. La fin des données est marquée par une ligne contenant uniquement un point simple (".");
- **QUIT**: ferme la conversation.

## Exemple

Dans l'exemple suivant, nous avons simplifié l'infrastructure au maximum. Nous avons une machine cliente (*gandalf*) qui envoie un mail à un utilisateur ayant un compte sur le serveur de messagerie du domaine *mydomain.com* lui-même (*mailserver*). Nous n'utiliserons pas de vrai client de messagerie; nous nous connecterons directement au port SMTP du serveur et saisirons les commandes SMTP manuellement.



```
> ~: bash — Konsole
Fichier  Édition  Affichage  Signets  >
plc@gandalf:~$ telnet mailserver 25
Trying 192.168.50.214...
Connected to mailserver.int.osix.be.
Escape character is '^]'.
220 mailserver ESMTP Postfix (Debian/GNU)
HELO gandalf
250 mailserver
MAIL FROM:plc@gandalf
250 2.1.0 Ok
RCPT TO:pleclercq@mydomain.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Ceci est un email de test.
.
250 2.0.0 Ok: queued as 06B3AED5
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
plc@gandalf:~$
```

Les lignes surlignées (HELO, MAIL FROM, RCPT TO, DATA, QUIT et les lignes entre "354..." et "250 2.0.0 OK...") sont tapées depuis le client. C'est exactement ce que votre client de messagerie habituel transmet lorsque vous envoyez un courrier électronique. Les réponses du serveur de messagerie commencent par 3 chiffres.

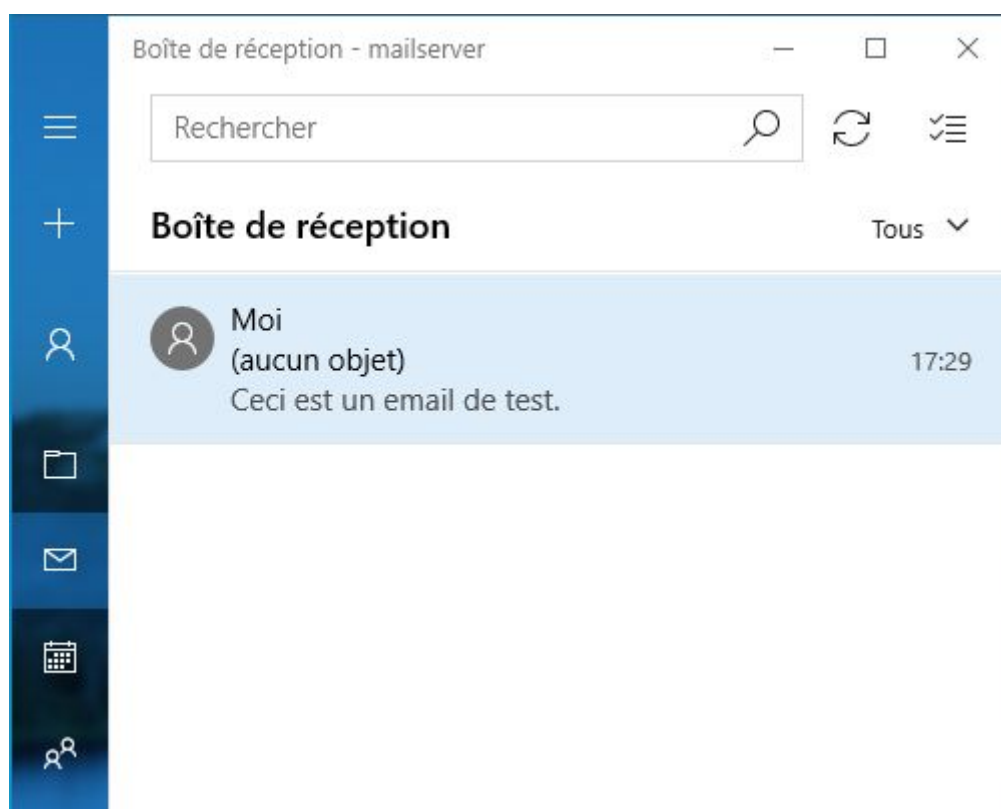
En utilisant un simple client de messagerie en ligne de commande sur le serveur *mailserver*, nous pouvons lire le contenu du courrier électronique suivant :

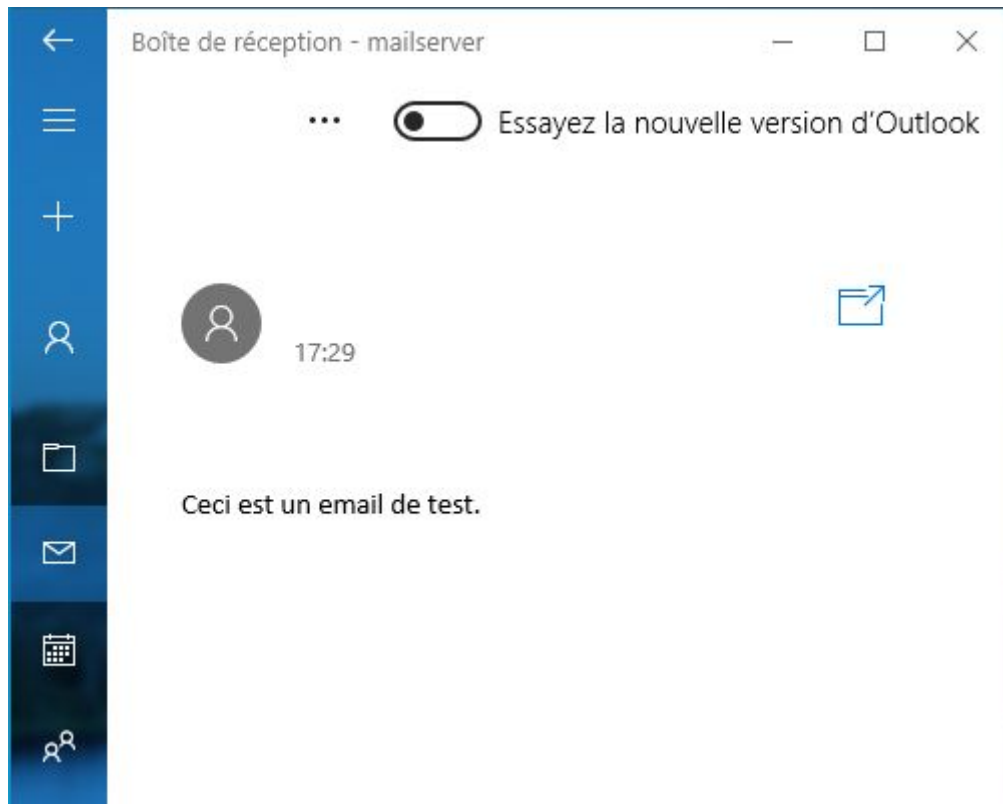
```
Return-Path: <plc@gandalf>
X-Original-To: pleclercq@mydomain.com
Delivered-To: pleclercq@mydomain.com
Received: from gandalf (unknown [192.168.50.31])
        by mailserver (Postfix) with SMTP id 4E3706EB
        for <pleclercq@mydomain.com>; Thu, 30 Jan 2025 19:53:06 +0100 (CET)

Ceci est un email de test.
```

Les données situées au-dessus du texte du contenu réel du courrier électronique sont appelées les en-têtes (*headers*) du courrier électronique. Elles donnent des détails techniques importants sur la source et le chemin de transmission du courrier électronique. Nous les analyserons dans un prochain article.

En utilisant un client de messagerie graphique (l'application courrier sous Windows), voici à quoi ressemble le mail reçu :





## Ajout de détails supplémentaires

Comme vous pouvez le voir ci-dessus, les clients de messagerie n'affichent pas beaucoup de détails et ne remplissent que les champs minimums de l'e-mail.

Plusieurs normes Internet définissent le contenu d'un e-mail. Notamment, les champs **From :** (De :), **To :** (À :) et **Subject :** (Sujet :) sont définis et sont utilisés par les clients de messagerie pour enrichir la description de l'email.

Voici un exemple d'email plus complet et de son apparence.

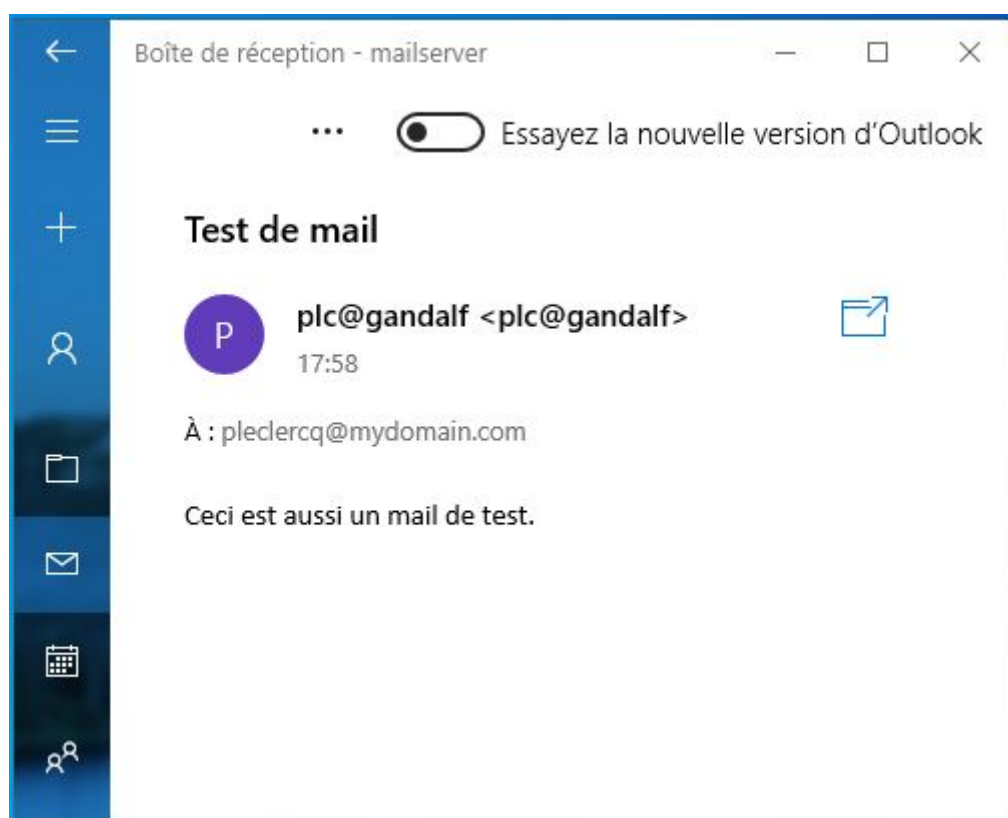
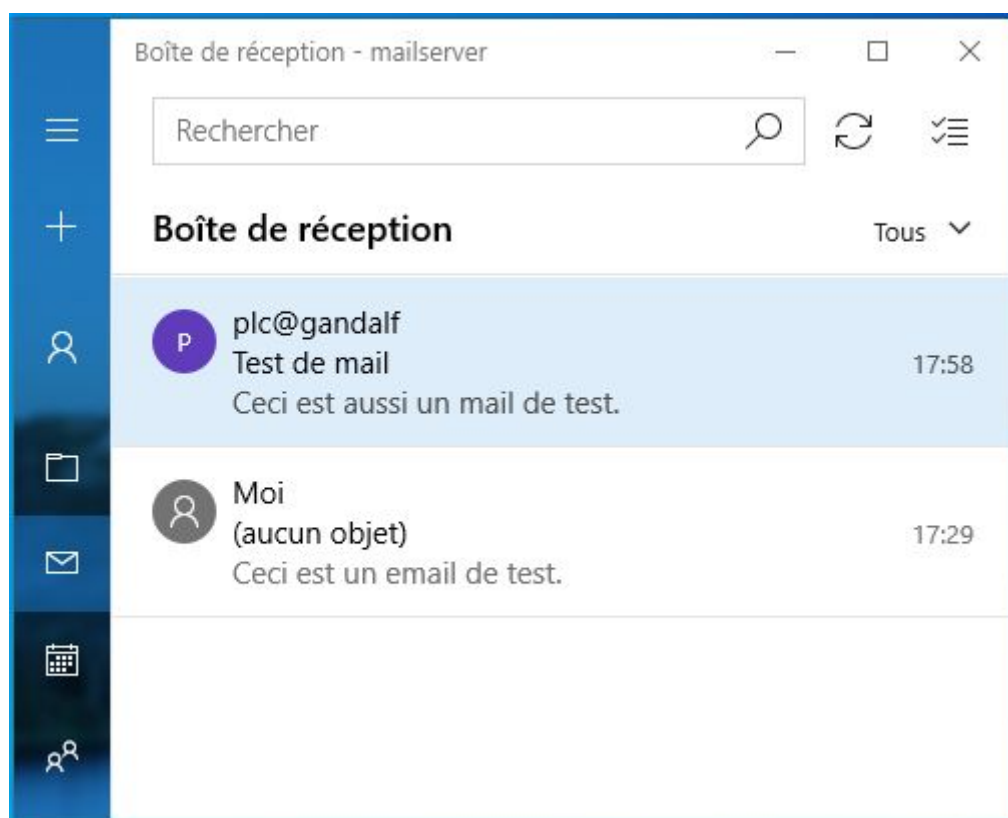
```
> ~: bash — Konsole
Fichier  Édition  Affichage  Signets
plc@gandalf:~$ telnet mailserver 25
Trying 192.168.50.214...
Connected to mailserver.int.osix.be.
Escape character is '^]'.
220 mailserver ESMTP Postfix (Debian/GNU)
HELO gandalf
250 mailserver
MAIL FROM:plc@gandalf
250 2.1.0 Ok
RCPT TO:pleclercq@mydomain.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: plc@gandalf
To: pleclercq@mydomain.com
Subject: Test de mail

Ceci est aussi un mail de test.
.
250 2.0.0 Ok: queued as D27D0ED5
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
plc@gandalf:~$
```

```
Return-Path: <plc@gandalf>
X-Original-To: pleclercq@mydomain.com
Delivered-To: pleclercq@mydomain.com
Received: from gandalf (unknown [192.168.50.31])
    by mailserver (Postfix) with SMTP id 1D74DED5
    for <pleclercq@mydomain.com>; Mon, 10 Feb 2025 17:43:11 +0100 (CET)
From: plc@gandalf
To: pleclercq@mydomain.com
Subject: Test de mail

Ceci est aussi un mail de test.
```





Vous pouvez désormais voir clairement le nom de l'expéditeur (*plc@gandalf*), le nom du destinataire (*pleclercq@mydomain.com*) et le sujet.

La plupart des clients de messagerie ajoutent ces champs lors de la transmission d'un email. Généralement, lorsque vous les configurez, ils vous demandent comment vous souhaitez que votre nom soit affiché ("Nom d'affichage" ou "Display name") pour remplir le

champ de données "De :" et ils copient le champ d'en-tête "RCPT T0" dans le champ de données "À :".

Dans un prochain article, nous verrons comment l'existence de ces champs de données et la façon dont ils sont affichés dans un agent de messagerie peuvent parfois être trompeuses et être utilisées par des attaquants pour confondre le destinataire.