

# Le SMTP

[ [Accueil](#) ] [ [Les bases](#) ] [ [les Profondeurs](#) ] [ [Un SMTP "perso"](#) ] [ [Installation de Postfix](#) ]  
[ [Config avancée](#) ] [ [Conclusions](#) ]

---

**Ce chapitre a été remanié pour tenir compte des évolutions imposées par la lutte anti spam. Tout n'a pas été réécrit, ne vous étonnez donc pas d'éventuelles incohérences dans les dates et dans les versions de logiciel utilisés.**

## Simple Mail Transfert Protocol.

Un des protocoles les plus fondamentaux de l'Internet. Nous l'utilisons tous les jours et nous sommes loin d'en connaître toutes les finesses...

Lorsque j'ai décidé de construire cet exposé, je n'avais pas une idée exacte de la galère dans laquelle je me mettais. C'est exactement la même que celle dans laquelle vous allez vous mettre si vous poursuivez sa lecture... (On ne pourra pas dire que je soigne ma publicité).

Vous continuez? Je vous aurai prévenu ...

## Qu'allons nous voir au juste?

Ce site, comme le montre le plan un peu plus bas est assez volumineux. L'objectif initial était double:

- Détailler un peu ce qu'il se passe lorsqu'on envoie un message, comment l'information voyage et arrive chez le destinataire et comment s'y prendre pour que le destinataire dispose d'une information lisible. Tout le monde n'utilise pas les mêmes outils de messagerie, les mêmes systèmes d'exploitation, le but étant tout de même d'arriver à communiquer entre "mondes" différents.

Cette partie de l'exposé, je la voulais simple et relativement complète. J'ai vite constaté que c'était une gageure (*prononcer [gazyr] Action, projet, opinion si étrange, si difficile, qu'on dirait un pari impossible à tenir*).

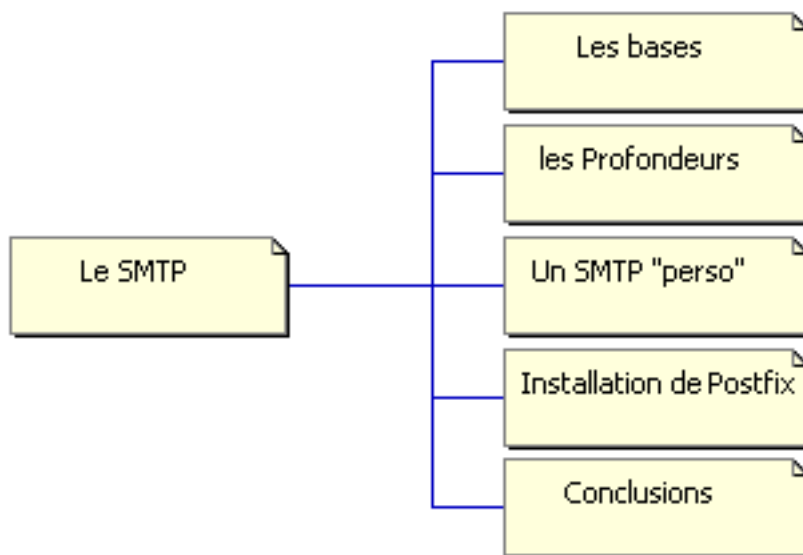
Cette partie là a donc explosé en deux morceaux:

- L'un qui reste simple et traite "en gros" du transport SMTP et en détail des divers moyens de coder un message pour qu'il puisse passer par les tuyaux de SMTP. Cette partie contient ce qui, à mon sens, devrait être connu de tout internaute responsable, parce que c'est le fondement d'une "tour de Babel" moderne. Autant vous dire que vous avez intérêt à lire au moins cette partie!
- L'autre morceau reprend en détail le transport SMTP, en s'appuyant sur une analyse de trames lors d'un envoi de message et sur une méthode d'envoi de message à la Robinson Crusoe, avec TELNET, pour manipuler soi-même les commandes reconnues par le protocole SMTP.

- Un autre volet intéressant consistait à montrer comment construire un système autonome qui permette de poster des messages sans avoir à utiliser le très célèbre smtp.wanadoo.fr. C'est une opération à priori très simple à réaliser, mais qui nécessite de connaître un minimum les outils que l'on emploie, si l'on ne veut pas courir le risque de jouer aux apprentis sorciers (je ne suis d'ailleurs pas complètement certain d'avoir entièrement évité l'écueil).

# Plan du site.

Comme d'habitude, un plan pour s'y retrouver...



---

[ [Accueil](#) ] [ [Les bases](#) ] [ [les Profondeurs](#) ] [ [Un SMTP "perso"](#) ] [ [Installation de Postfix](#) ]  
[ [Config avancée](#) ] [ [Conclusions](#) ]

---

# Les bases

[ [Accueil](#) ] [ [Les bases](#) ] [ [les Profondeurs](#) ] [ [Un SMTP "perso"](#) ] [ [Installation de Postfix](#) ] [ [Config avancée](#) ]  
[ [Conclusions](#) ]

Dans cette partie de l'exposé, nous allons voir en détail ce que tout internaute gagnerait à savoir, concernant la façon dont les e-mails voyagent, Quel est leur contenu exact, comment les informations sont codées...

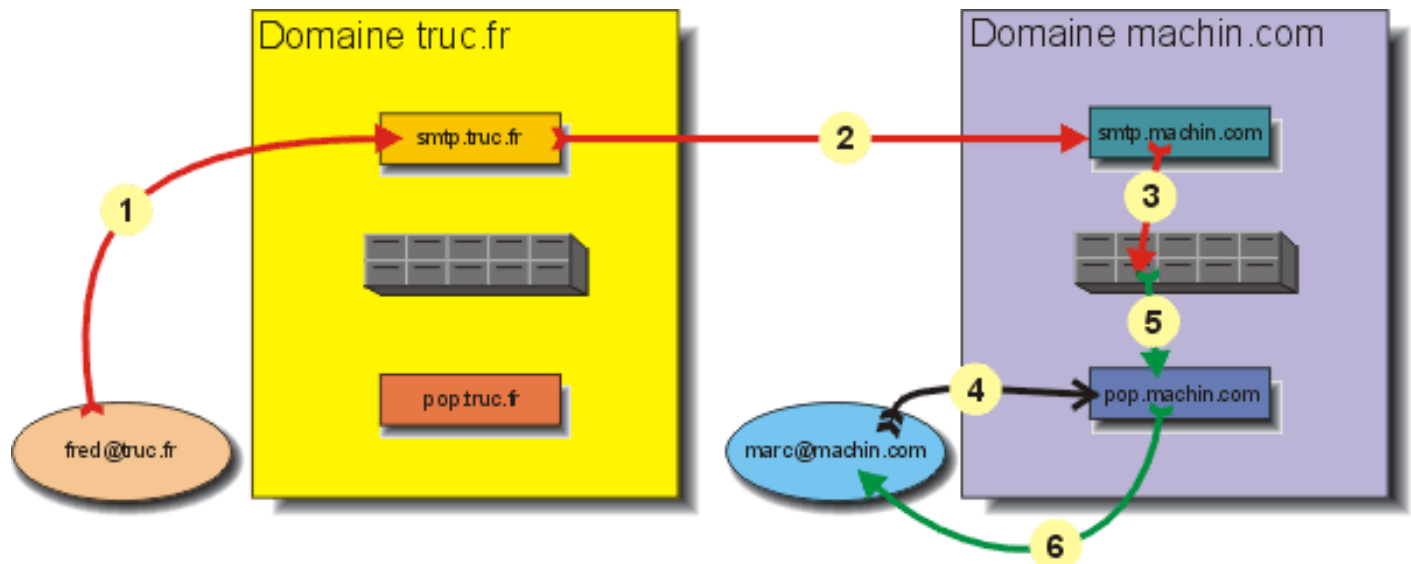
Cette partie est donc divisée en trois paragraphes:

- [La façon dont le message voyage, depuis l'émetteur jusqu'au destinataire.](#)
- [Une analyse détaillée de tout le contenu du message, y compris l'en-tête qui n'est pas visible par défaut dans les outils de messagerie courants.](#)
- [Une explication de la façon dont le contenu du message est codé pour pouvoir être transporté par SMTP.](#)

## Itinéraire d'un message électronique.

Supposons un cas simple (et cependant courant).

- Soit un utilisateur abonné chez "truc" et ayant pour adresse électronique: **fred@truc.fr**.
- Soit un autre utilisateur abonné chez "machin" et ayant pour adresse électronique **marc@machin.com**.
- truc dispose des serveurs:
  - smtp.truc.fr
  - pop.truc.fr
- machin dispose des serveurs:
  - smtp.machin.com
  - pop.machin.com
- Fred doit envoyer un message à marc.



1. Fred compose le message avec son outil de messagerie préféré, disons outlook express. Il a des avantages: Il est gratuit et il est fait par Microsoft.  
Une fois le message composé, Fred clique sur le bouton "envoyer". Comme il a correctement configuré son outil, le message est envoyé sur le serveur smtp.truc.fr ➡

2. Le serveur smtp.truc.fr reçoit le message, constate que le destinataire n'est pas dans son domaine. Il cherche alors un serveur de messagerie dans le domaine machin.com et le trouve. Il envoie le message à smtp.machin.com ➡
3. Le serveur smtp.machin.com reçoit le message, constate que le destinataire est bien dans son domaine. Il range alors le message dans la boîte aux lettres de Marc. Il y restera aussi longtemps qu'il le faudra, sans rien dire à personne. ➡
4. Un jour, Marc décide de regarder s'il n'a pas de messages. Il envoie donc une requête à son serveur pop.machin.com, au moyen de son outil de messagerie préféré, par exemple eudora. Il a des avantages: il en existe une version gratuite et il n'est pas fait par Microsoft. ➡
5. Le serveur pop consulte alors la boîte aux lettres de Marc, constate qu'il y a un message dedans. ➡
6. Il l'envoie alors à l'outil de messagerie de Marc qui, par défaut, demandera à pop.machin.com de le supprimer de la boîte aux lettres. Mais c'est un comportement par défaut, il est possible de demander à ne pas effacer les messages. Cette fonction est utile lorsque l'on désire consulter sa messagerie de divers endroits sans avoir à se renvoyer un message si on veut le relire ailleurs. ➡

POP3 est un protocole de relève de courrier. Sans pour l'instant entrer dans les détails, il en existe un autre appelé IMAP.

## Mécanismes mis en jeu.

### SMTP (Simple Message Transfert Protocol).

C'est le protocole applicatif qui permet de transporter les messages sur l'Internet. Il sait acheminer un message jusqu'à une boîte aux lettres, mais ne va pas plus loin.

Pour y arriver, il analyse dans un premier temps la partie de l'adresse située à droite du @ (à prononcer dans ce cas "at"), pour trouver le domaine du destinataire. Si ce domaine le concerne, il cherche alors la boîte aux lettres du destinataire en regardant la partie de l'adresse située à gauche du @. Si le domaine du destinataire ne le concerne pas, il va chercher le serveur SMTP qui gère ce domaine, au moyen des champs MX du DNS du domaine destinataire et transmet le message à ce serveur.

### POP3 (Post Office Protocol 3).

Ce protocole est exclusivement utilisé pour le dialogue entre le client de messagerie et la boîte aux lettres. Il ne fait pas de transport sur l'Internet, il permet juste à l'utilisateur de gérer son courrier. IMAP4 (Internet (ou Interactive ?) Mail (ou Message ?) Access Protocol version 4) en est une alternative.

### MUA, MTA, MDA et cetera.

Un peu de jargon:

- Le MUA (Mail User Agent), c'est le client de messagerie (Outlook Express, Eudora, Pegasus etc.).
- Le MTA (Mail Transfert Agent) est à prendre au sens plus large que le "serveur SMTP". Le courrier peut être acheminé d'un point à un autre par l'intermédiaire d'agents de transfert qui ne gèrent pas de boîtes aux lettres, mais savent relayer le courrier d'un point à un autre pour atteindre le serveur supportant les boîtes aux lettres. En effet, l'exemple vu plus haut est le plus simple que l'on puisse imaginer. Dans la pratique, le courrier peut transiter par plusieurs MTA. Nous le verrons plus loin.
- Le MDA (Mail Delivery Agent) est le service de remise du courrier dans les boîtes aux lettres des destinataires. Le MTA transmet au MDA les messages destinés aux clients du domaine.

## Récapitulons.

Lorsque l'on rédige un courrier et qu'on le poste, on le fait avec le MUA qui le transmet au MTA qu'on lui a signalé dans la configuration (pour nous, abonnés Wanadoo, c'est normalement smtp.wanadoo.fr). C'est [l'étape 1](#) du petit schéma.

De MTA en MTA, le message voyage jusque sur le MTA qui a en charge la messagerie du domaine du destinataire ([étape 2](#)). Il le passe alors (avec tous les autres messages entrant pour ce domaine) au MDA qui distribue ce courrier entrant dans les boîtes aux lettres concernées ([étape 3](#)).

Les [étapes 4, 5 et 6](#) concernent le serveur POP (ou IMAP)

---

## Dans les entrailles de l'e-mail.

D'abord, en français on ne dit pas "e-mail", ni "mail"; on dit "mèl" (je t'envoie un mèl, tu m'envoies un mèl, on s'envoie des mèls), on peut dire également "courriel". Mais, pour la bonne compréhension du texte, je continuerai à écrire "e-mail".

Lorsque vous recevez un e-mail, votre MUA (maintenant qu'on sait ce que c'est) vous montre:

- L'expéditeur.
- L'Objet (qu'il ne faut jamais oublier de remplir, c'est utile pour trier son courrier).
- Le texte (ou corps) du message.

Mais votre e-mail contient toute une partie "cachée" qui nous permet de savoir quel chemin cet e-mail a suivi pour arriver dans votre boîte aux lettres.

Cette partie, appelée l'en-tête, n'est pas "top secret", bien que non visible par défaut. Vous pouvez toujours la consulter avec votre MUA. Pour Outlook Express: Ouvrez le message, puis "Fichier/Détails/Source du message".

## Prenons un exemple:

```
Return-Path: <christian.caleca@wanadoo.fr>
Received: from alisier.w-n-doo.fr (smtp-rt-9.w-n-doo.fr [193.252.19.55])
        by mail.monaco.net (Pro-8.9.3/Pro-8.9.3) with ESMTTP id SAA07439
for <emel13@enprovence.com>; Thu, 11 May 2000 18:20:10 +0200
Received: from mahonia.w-n-doo.fr (193.252.19.58)
        by alisier.w-n-doo.fr; 11 May 2000 18:20:08 +0200
Received: from CHRIS (62.161.101.240)
        by mahonia.w-n-doo.fr; 11 May 2000 18:19:51 +0200
Message-ID: <000501bfbb64$afc796c0$0a00a8c0@maison.mrs>
From: "Christian CALECA" <christian.caleca@w-n-doo.fr>
To: <emel13@enprovence.com>
Subject: test itineraire
Date: Thu, 11 May 2000 18:19:24 +0200
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 8bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2919.6600
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6600
```

## Status:

Juste pour analyser l'en-tête

Toute la partie en gras constitue ce que l'on appelle l'en-tête, alors que la dernière ligne, le message lui-même, s'appelle le corps.

### Note :

Pour éviter de faire la partie trop belle aux robots renifleurs d'adresses e-mails, certains noms de domaines ont été volontairement dégradés.

## Détail de l'en-tête.

Tous les mots finis par ":" sont des champs qui ont une signification particulière, soit pour les MTA, soit pour les MUA. Nous allons détailler leur signification.

**Return-Path:** C'est l'adresse qui sera utilisée:

- Pour la réponse (la fonction répondre à l'expéditeur)
- Le renvoi du message s'il ne peut arriver au destinataire.

**Received:** Cette ligne est un peu particulière. Chaque MTA qui reçoit le message y inscrit le nom du MTA qui le lui a envoyé, ainsi que le sien. Il est ainsi possible de retracer complètement la route qu'a suivi le message de l'expéditeur jusqu'au destinataire.

**Message-ID:** C'est un identifiant unique du message. Il est attribué par le premier MTA qui reçoit le message (Protocole ESMTP: Extended SMTP).

**From:** C'est l'adresse de l'expéditeur. Elle est par défaut recopiée dans le "return path", sauf configuration différente du MUA de l'expéditeur.

**To:** C'est l'adresse du (ou des) destinataire(s)

**Subject:** L'objet du message

**Date:** La date d'émission écrite par le MUA de l'émetteur

**MIME-Version:** Version du mode de codage des données. Cette information a tellement d'importance que nous allons y consacrer toute une page.

**Content-Type:** Type de codage utilisé.

**charset=** Jeu de caractères utilisé.

**Content-Transfer-Encoding:** Codage sur 7 ou 8 bits.

**X-...** Tous les champs commençant par X ne sont pas des champs "officiels". Chaque MUA est libre d'en ajouter autant qu'il veut. Leur contenu n'est pas pris en compte par les MTA. Ainsi, il est illusoire de croire que le champ X-Priority ait une quelconque importance dans la vitesse de transport du message.

Cette liste de champs n'est pas complète. Il y en aurait pour trois pages à les énoncer tous...

## Utilité de l'en-tête.

L'en-tête contient donc toutes les informations nécessaires pour:

- Identifier l'auteur du message
- Identifier le destinataire
- Savoir à qui il faut répondre
- Retrouver le chemin suivi par le message
- Savoir comment a été codé ce message.

- Des informations "subsidiaries" (champs X...) qui ne sont pas utilisés par SMTP ni ESMTP, mais qui permettent de donner des informations qui peuvent être utiles, comme le MUA qui a généré le message.
- 

# Vertus et défauts de SMTP.

Ce protocole a la vertu d'être particulièrement "solide", mais il est un peu ancien et il lui manque quelques fonctionnalités qui seraient bien utiles aujourd'hui:

- La sécurisation de la transmission. Encore qu'une extension "STARTTLS" ait été créée dans ce but (voir à ce propos le site "[Sécurisation des courriers électroniques](#)")
- Les possibilités de transmettre autre chose que du texte brut.

Ces deux limites peuvent être contournées:

- En cryptant son message .
- En utilisant un artifice pour encoder tout type de document de telle manière que SMTP croie que c'est du texte. Etudier ce système ici nous mènerait trop loin. Si le sujet vous intéresse, consultez le chapitre sur [le codage des caractères](#).

Nous allons tout de même faire deux où trois observations utiles, pour comprendre mieux comment il faut configurer son MUA pour être lu correctement.

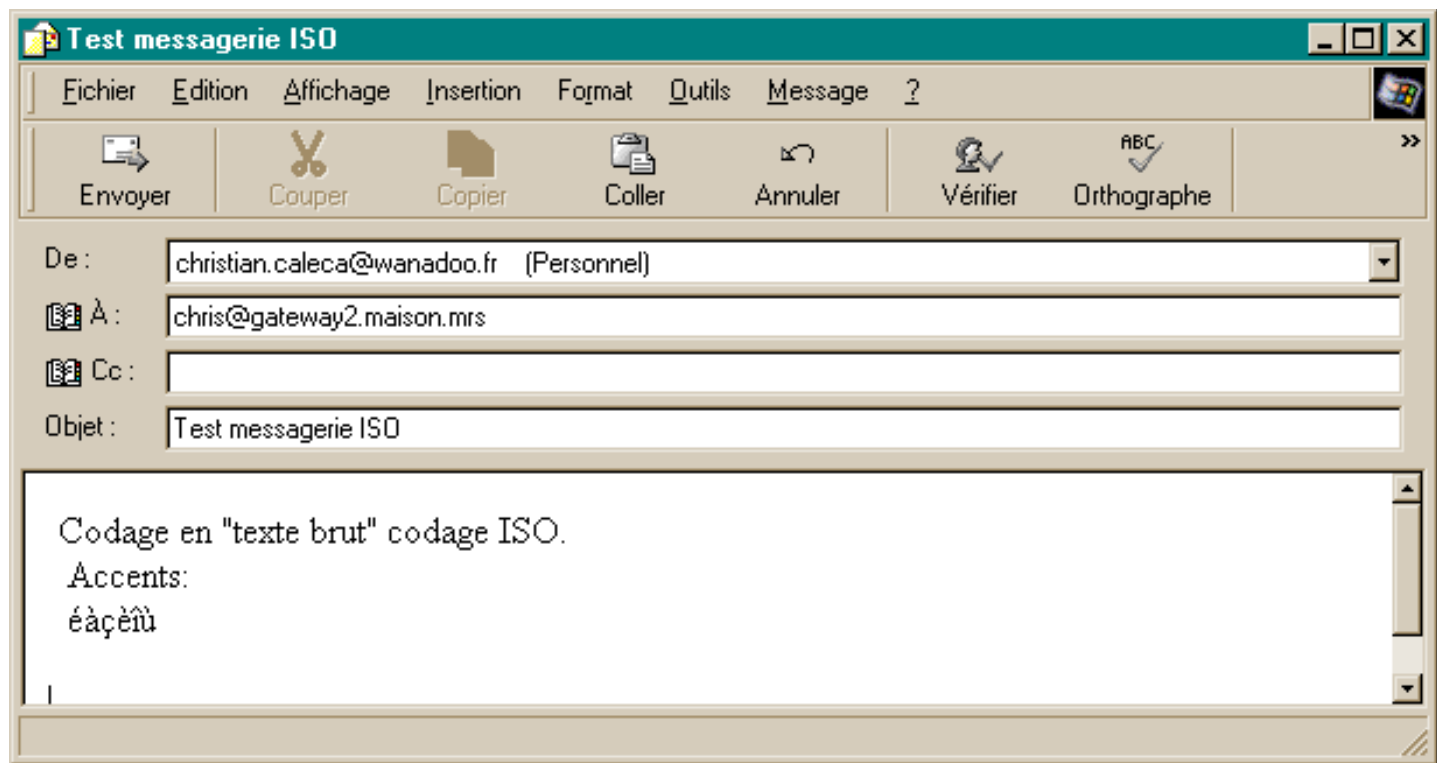
## Les divers codages utilisant MIME.

Bien que le codage des données soit traité plus en détail [ailleurs sur ce site](#), voyons tout de même rapidement quelques points importants.

Pour illustrer ceci, nous allons envoyer des messages avec Outlook Express et nous allons les lire avec un outil rustique sous Linux : l'outil "mail". Cet outil fonctionne en mode texte. plus rustique, vous n'aurez que Telnet.

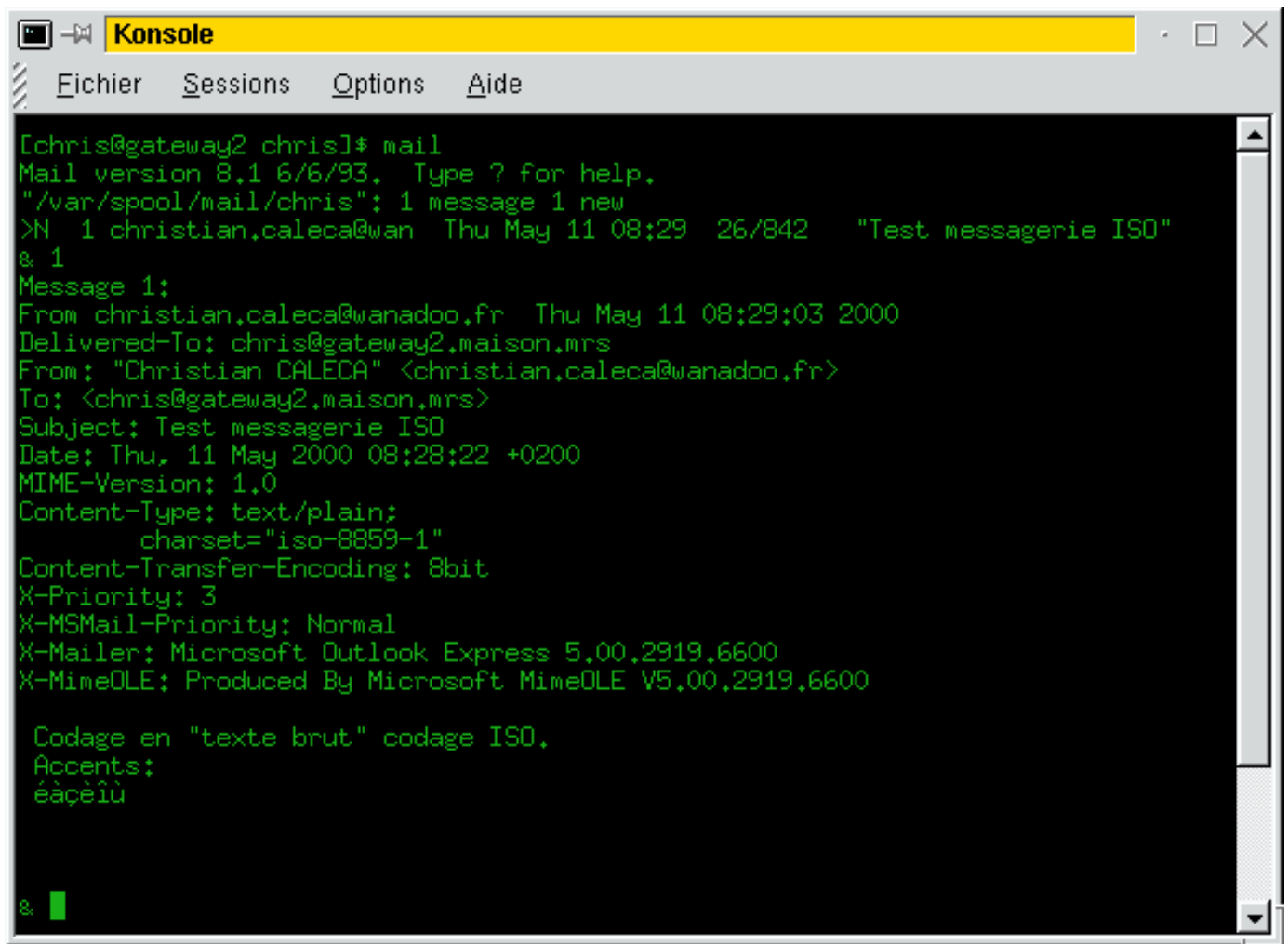
### Codage "Aucun" ou "plain/text".

C'est-à-dire pas de codage particulier pour le texte. On envoie ce message:



E l'on récupère ceci:





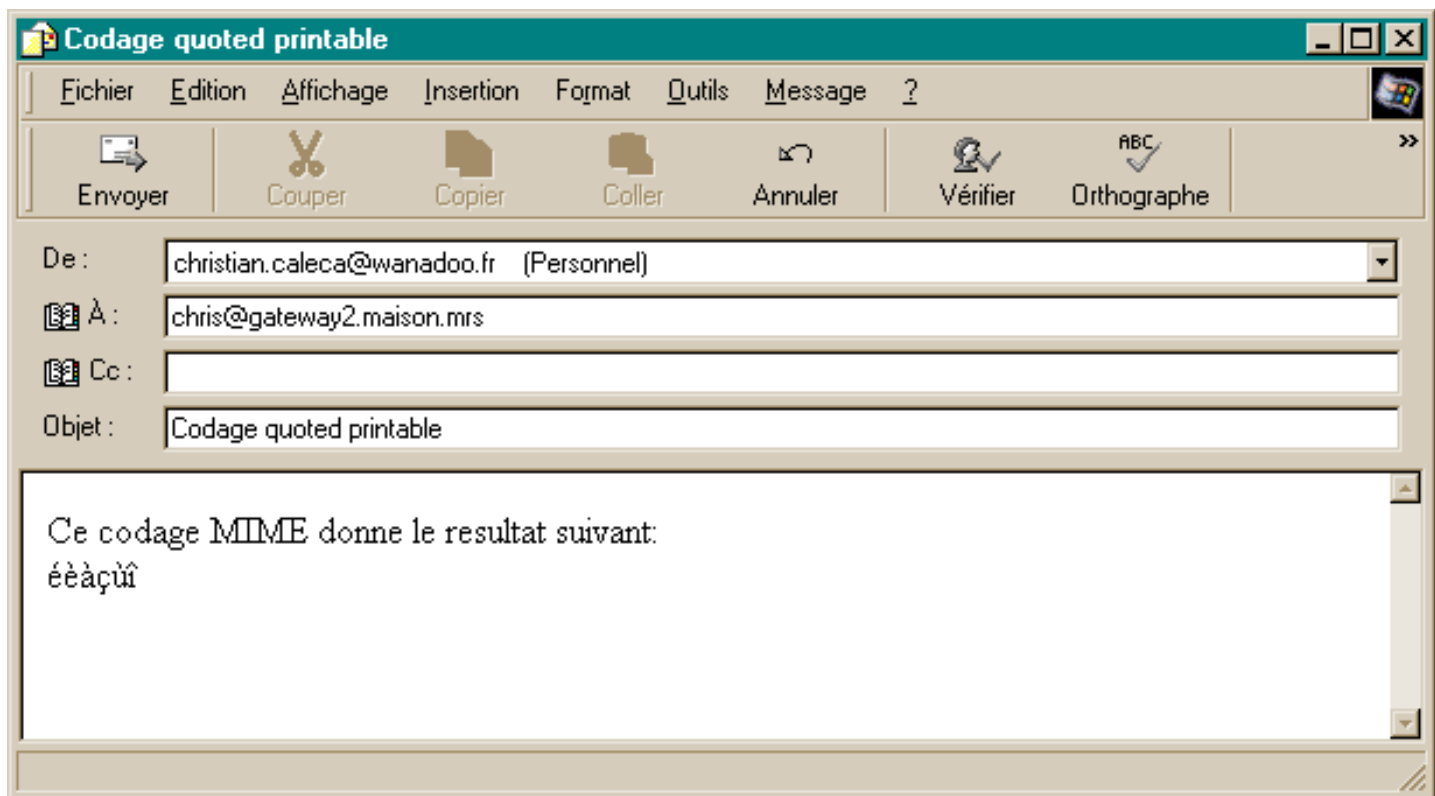
```
[chris@gateway2 chris]$ mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/chris": 1 message 1 new
>N 1 christian.caleca@wanadoo.fr Thu May 11 08:29 26/842 "Test messagerie ISO"
& 1
Message 1:
From: christian.caleca@wanadoo.fr Thu May 11 08:29:03 2000
Delivered-To: chris@gateway2.maison.mrs
From: "Christian CALECA" <christian.caleca@wanadoo.fr>
To: <chris@gateway2.maison.mrs>
Subject: Test messagerie ISO
Date: Thu, 11 May 2000 08:28:22 +0200
MIME-Version: 1.0
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 8bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2919.6600
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6600

Codage en "texte brut" codage ISO.
Accents:
éàçèîù
```

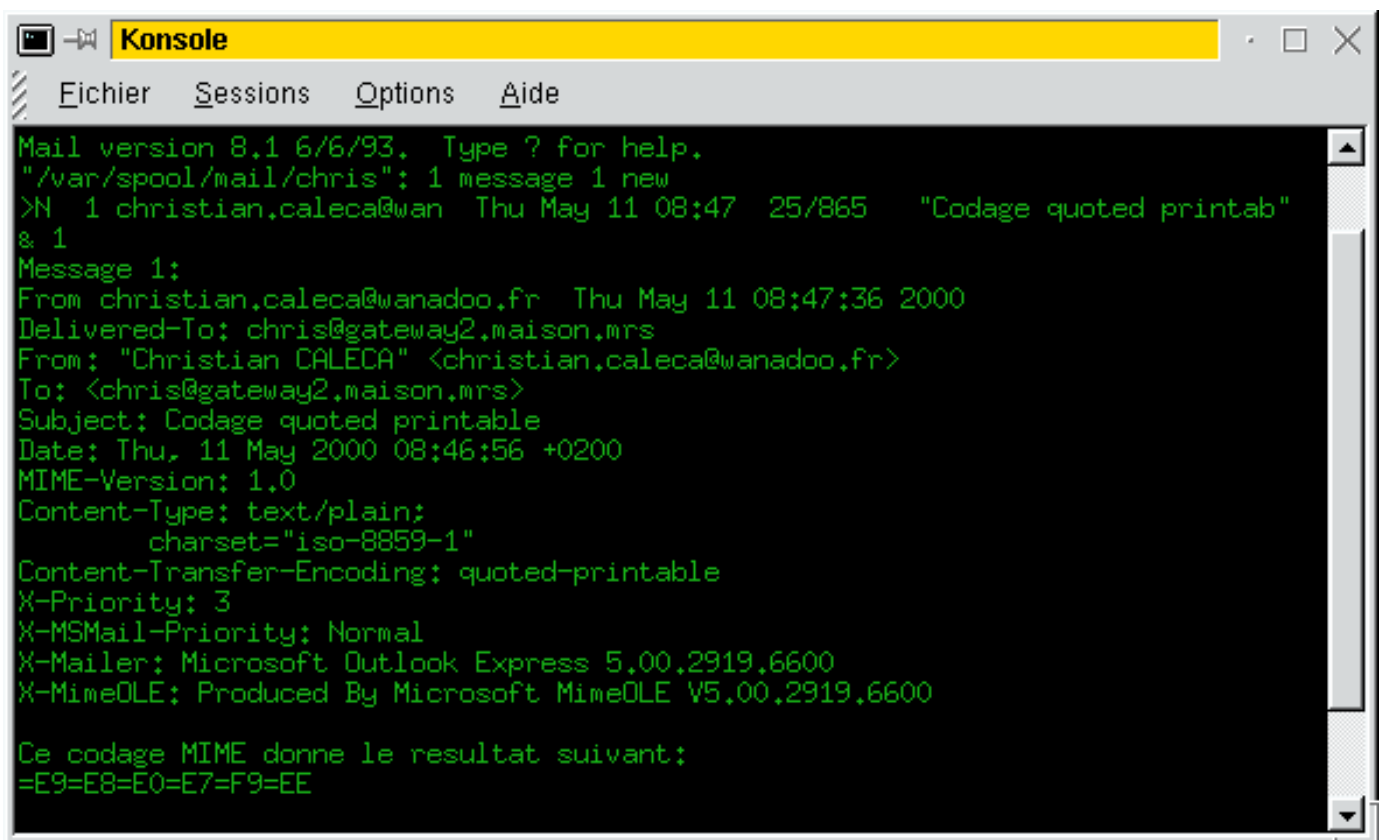
C'est correct. L'en-tête indique que le contenu est du texte de type "plain text" encodé sur 8 bits, avec un jeu de caractères "iso-8859-1". Comme vous pouvez le constater, le texte est parfaitement lisible. Il y a cependant un problème potentiel en voie de disparition: La plupart des MTA utilisent un protocole ESMTP qui gère l'ASCII sur 8 bits, mais il peut encore exister çà et là des vieux MTA qui mettront systématiquement le bit7 à 0. Le problème devrait aujourd'hui être rarissime. Dans ce cas, la seule solution est d'utiliser des caractères du code ASCII US, sans aucune lettre accentuée.

**Codage: "quoted printable".**

Outlook express propose ce mode en "texte brut". Essayons pour voir...



Ben c'est pas terrible; les lettres accentuées sont curieusement codées...

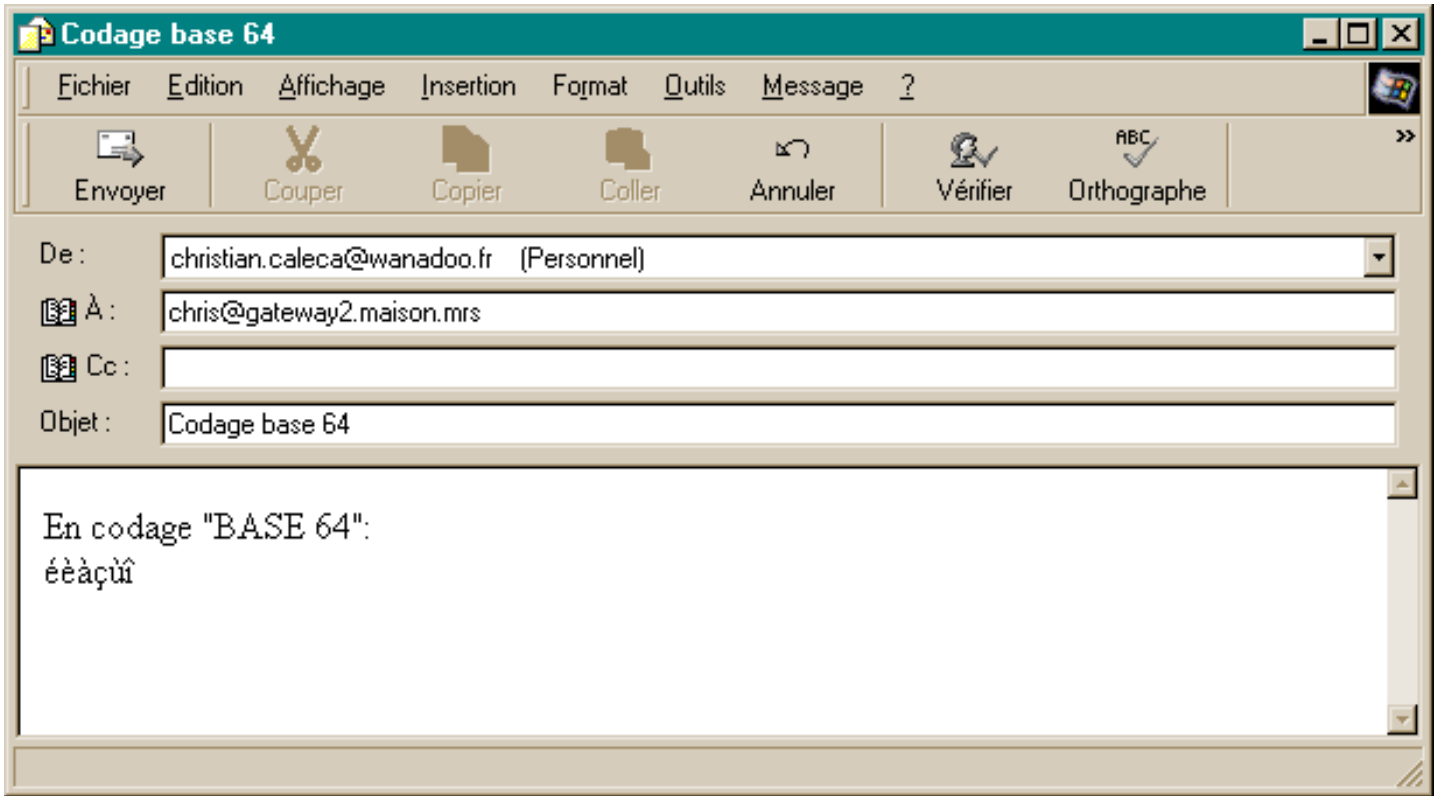


En fait, dans ce mode de codage, les caractères qui peuvent être codés sur 7 bits sont transmis normalement, ceux qui ne le peuvent pas (bit 7 à 1) sont remplacés par "=" et la valeur du code ASCII sur 8 bits exprimé en hexadécimal.

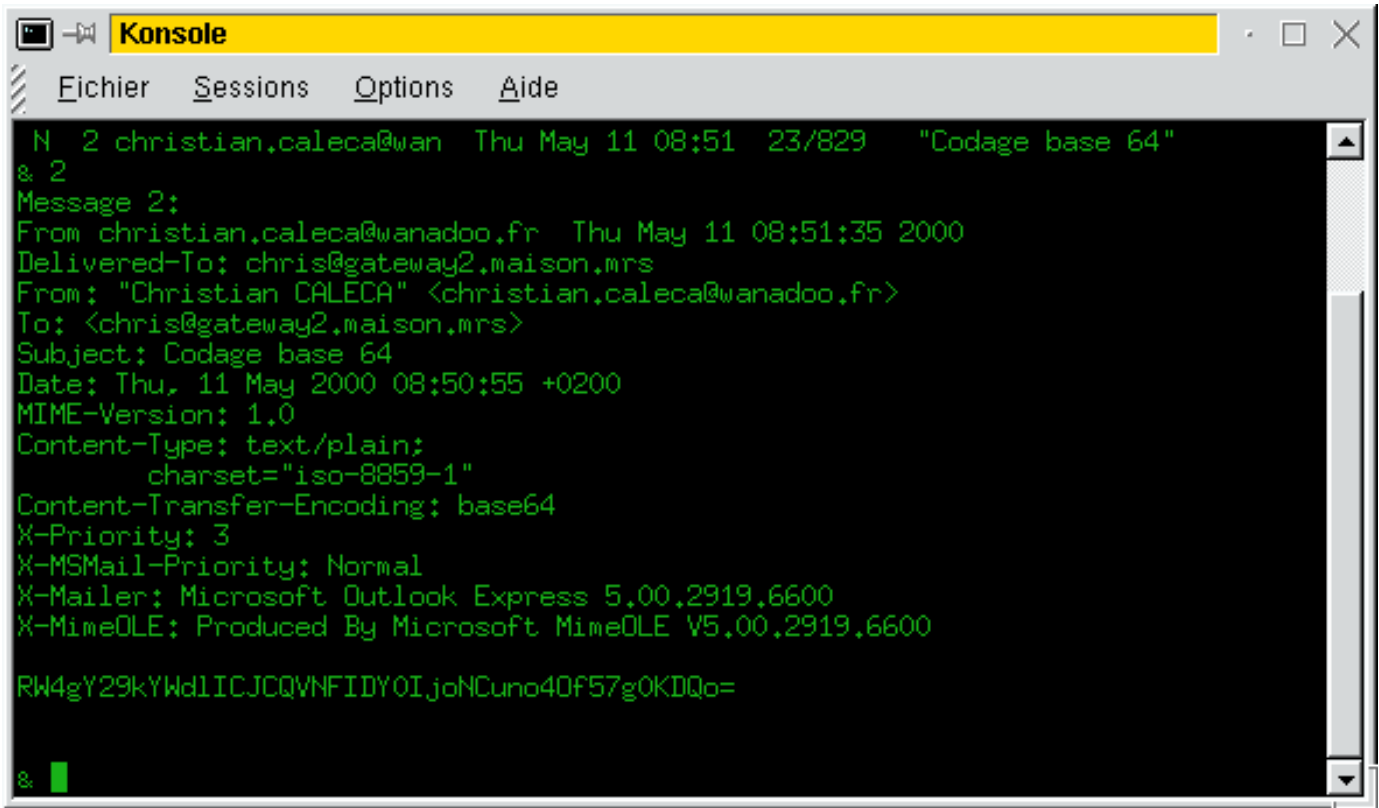
A ne pas utiliser donc, si le destinataire ne dispose pas d'outil sachant décoder ."quoted printable".

**Codage "base 64".**

Outlook Express propose également ce mode de codage, lorsque l'on choisit le "texte brut". On essaye...



C'est catastrophique. Mail ne sait pas du tout décoder le message...



Aucun caractère n'est lisible.

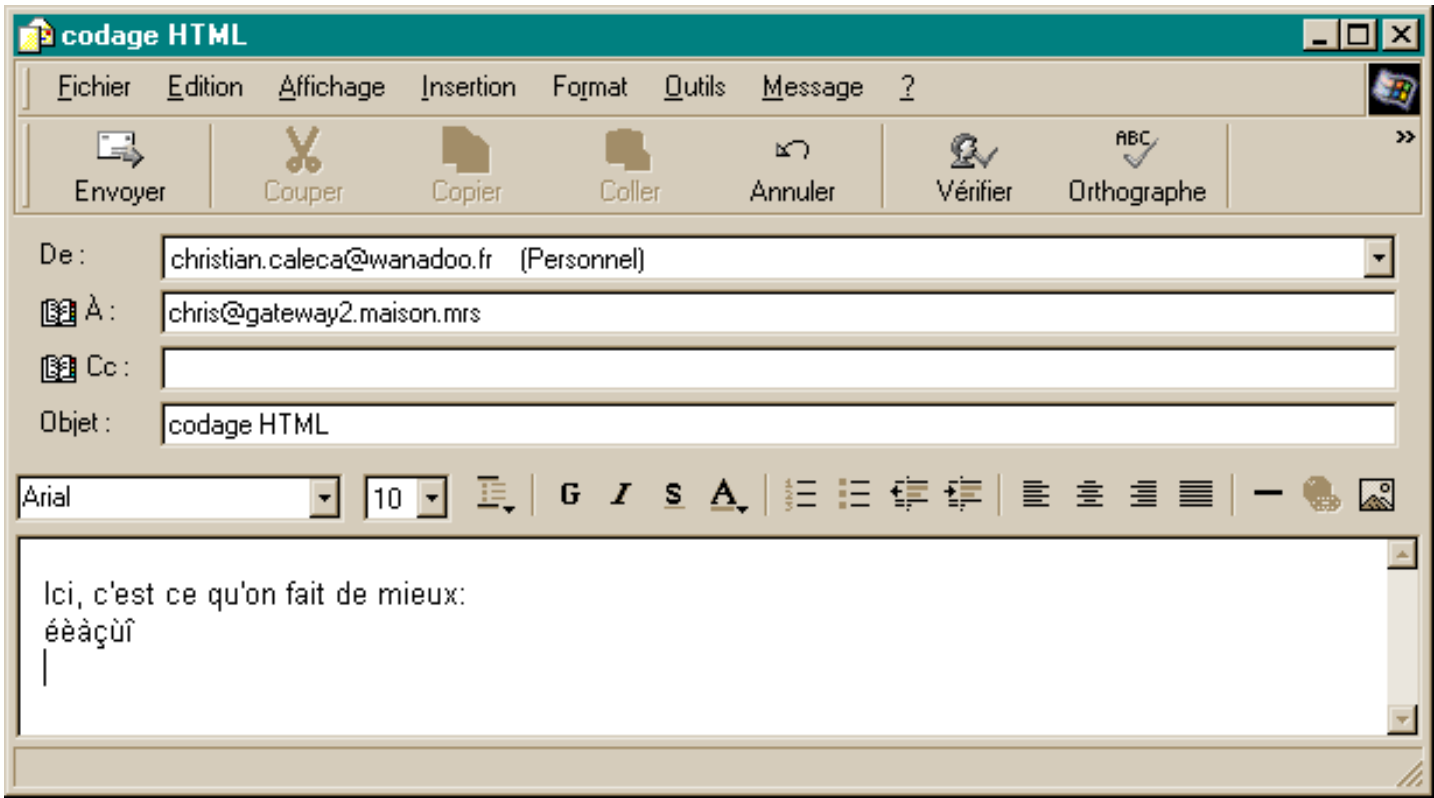
### Le codage HTML.

Enfin, le meilleur pour la fin, le message en HTML.

Je ne voudrais pas ici déclencher une polémique inextinguible sur ce sujet brûlant... Mais rappelons les faits.

Le texte pur, c'est bien, mais c'est de la génération de "edit", "notepad" et autres "vi". Autrement dit, aucun enrichissement possible du texte. Il peut pourtant être utile de rédiger ses messages avec quelques possibilités des traitements de texte, comme les notions de gras, italique, souligné, mise en surbrillance etc. D'où l'idée d'écrire ses messages en HTML qui sait faire tout ça.

Mais voyons ce que cela donne:



Ici, pas de copie d'écran, tellement le résultat est long:

- Ce qui est en gras constitue les morceaux de l'en-tête.
- Ce qui est surligné représente les spécificités du codage en HTML "multipart"
- Ce qui est en bleu, c'est l'explication de ce qu'il se passe. (Ca ne fait pas partie du message).

**From christian.caleca@w-n-doo.fr Thu May 11 09:00:46 2000**  
**Return-Path: <christian.caleca@w-n-doo.fr>**  
**Delivered-To: chris@gateway2.maison.mrs**  
**Received: from chris (chris.maison.mrs [192.168.0.10])**  
**by gateway2.maison.mrs (Postfix) with SMTP id DB2D51BAAF**  
**for <chris@gateway2.maison.mrs>; Thu, 11 May 2000 09:00:46 +0200 (CEST)**  
**Message-ID: <003501bfbb16\$8a226dd0\$0a00a8c0@maison.mrs>**  
**From: "Christian CALECA" <christian.caleca@w-n-doo.fr>**  
**To: <chris@gateway2.maison.mrs>**  
**Subject: codage HTML**  
**Date: Thu, 11 May 2000 09:00:06 +0200**  
**MIME-Version: 1.0**  
**Content-Type: multipart/alternative;**  
**L'extension MIME indique ici que le message va être codé en deux parties,**  
**de manière différente pour les deux parties...**  
**boundary="-----\_NextPart\_000\_0031\_01BFBB27.4D9A74F0"**  
**Avec une balise que l'on aura du mal à confondre**

avec le texte du message, quel qu'il soit.

X-Priority: 3

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook Express 5.00.2919.6600

X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6600

C'est un message de format MIME en plusieurs parties.

-----=\_NextPart\_000\_0031\_01BFBB27.4D9A74F0 Première balise

Content-Type: text/plain;

charset="iso-8859-1"

Content-Transfer-Encoding: 8bit

Ici, c'est ce qu'on fait de mieux:

éèàçùî

Cette première partie a été codée de façon basique,  
celle qui, normalement, doit fonctionner avec n'importe quel MUA, nous l'avons vu.

-----=\_NextPart\_000\_0031\_01BFBB27.4D9A74F0 Deuxième balise

Content-Type: text/html;

charset="iso-8859-1"

Content-Transfer-Encoding: quoted-printable Mais, ce n'est pas un bon choix...

Le "plain text" est à utiliser, même dans le codage HTML"

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">

<HTML><HEAD>

<META content=3D"text/html; charset=3Diso-8859-1" =

http-equiv=3DContent-Type>

<META content=3D"MSHTML 5.00.2919.6307" name=3DGENERATOR>

<STYLE></STYLE>

</HEAD>

<BODY bgColor=3D#ffffff>

<DIV><FONT face=3DArial size=3D2>Ici, c'est ce qu'on fait de =  
mieux:</FONT></DIV>

<DIV><FONT face=3DArial size=3D2>=E9=E8=E0=E7=F9=EE</FONT></DIV>

<DIV>&nbsp;</DIV></BODY></HTML>

Tout ceci est du jargon HTML. Simple ici, parce qu'il n'y a aucune fioriture!  
Ce paragraphe aurait été beaucoup plus long, si l'on avait mis des couleurs,  
Des tailles de polices différentes, et surtout un fond de papier.

-----=\_NextPart\_000\_0031\_01BFBB27.4D9A74F0-- Dernière balise.

Notez qu'Outlook Express, malgré tout le mal que l'on peut en dire ici où là, a la politesse de créer un paragraphe qui sera lisible par tout MUA.

Alors, pourquoi le HTML est-il proscrit par la netiquette?

- En tout premier lieu, hélas, un problème de sécurité. Un document HTML peut véhiculer des scripts malicieux ayant des comportements de virus.
- L'extrême longueur des messages générés, surtout si l'on s'amuse un peu trop avec les gadgets. Ce gonflement de la taille du message est souvent pénalisant:
  - Pour l'espace disque de celui qui conserve les messages qu'il reçoit.
  - La durée de chargement.
- La lisibilité aussi. La taille des polices étant fixée, un texte lisible sur un écran 800x600 deviendra très pénible à lire sur un 1280x1024!
- La plus élémentaire des politesses qui consiste à s'assurer que l'on ne dérange pas celui à qui l'on envoie ce message. Les dérangements les plus évidents étant:

- L'impossibilité pour le destinataire de lire correctement le message, n'étant pas outillé pour ça (mais là, à la rigueur, il peut peut-être faire l'effort d'utiliser des outils qui savent le faire, la politesse passe aussi par là...)
- Le temps de chargement des messages. C'est un argument qui me paraît plus convaincant. Si vous êtes en déplacement, que vous vous connectez avec un portable sur une ligne RTC de qualité douteuse, vous préférerez assurément que les messages soient le plus court possible.
- Certaines personnes reçoivent plusieurs dizaines de messages par jour. Même avec une bonne connexion, c'est mieux de faire court.
- Le dernier argument est une synthèse des autres, les boîtes aux lettres sont souvent limitées en taille par les fournisseurs d'accès. Plus les messages sont longs, moins on peut en mettre dedans. Les pièces jointes sont d'ailleurs aussi pénalisantes, mais elles sont parfois indispensables.

## Conclusions.

- Par défaut, postez en texte brut, "plain text" ou "aucun codage" avec Outlook Express.
- Ne postez en HTML qu'aux personnes qui vous l'ont permis, c'est plus poli.
- Ne postez en HTML que si c'est vraiment utile, (faire simplement "joli" n'est pas utile).

Voilà. Vous ne pourrez plus dire maintenant que vous ne saviez pas pourquoi il fallait faire attention au codage de vos messages :-)

# les Profondeurs

[ [Accueil](#) ] [ [Les bases](#) ] [ les Profondeurs ] [ [Un SMTP "perso"](#) ] [ [Installation de Postfix](#) ] [ [Config avancée](#) ] [ [Conclusions](#) ]

---

## Les mécanismes de SMTP.

Dans cette partie de l'exposé, nous allons regarder ce qu'il se passe dans les profondeurs du protocole SMTP.

### L'analyse de trames.

Comme d'habitude, rien ne vaut l'analyse des trames pour voir exactement ce qu'il se passe. Si l'on arrive à tout interpréter, on est certain de ne rien laisser passer du protocole. Ici, l'analyse est un peu longue, elle comporte deux parties:

- La recherche de l'adresse du MTA du destinataire (recherche DNS "classique")
- La transmission du message selon le protocole SMTP, qui s'appuie sur TCP. Les échanges sont un peu plus compliqués qu'en UDP, employé pour la résolution des noms.

### Envoyer un message "à la main".

Il existe un petit outil appelé "telnet" qui n'est rien d'autre qu'un terminal trivial en mode texte. Il est cependant possible de faire beaucoup de choses avec telnet, pas toujours très simplement, je vous l'accorde. Avec "telnet", il est possible de lire son courrier, d'en envoyer, de lire les news et bien d'autres choses encore.

Nous allons envoyer un message avec telnet, ce qui nous obligera à connaître toutes les commandes (du moins les plus importantes) du protocole SMTP.

---

## Espionnage d'un envoi.

Comme d'habitude, nous allons espionner l'envoi d'un e-mail avec notre "sniffer" préféré. Rien de tel pour bien comprendre comment les choses se passent.

### Enoncé du problème.

Depuis un poste du réseau privé, nous allons envoyer un message à l'adresse "*eme13@enprovence.com*" en employant notre serveur SMTP "gateway1.maison.mrs".

### Objectif de la manip.

Si nous arrivons à tracer toute la transaction, plus aucun détail du protocole SMTP ne nous échappera. Essayons pour voir.

Attention! C'est du TCP, ça va être long... (mais ça va être bon :-)

### Les trames récupérées.

- Ce qui est surligné en jaune est ce qui est le plus important.
- Ce qui est en bleu est un commentaire.

**Recherche de l'adresse du serveur SMTP du destinataire.**

Frame 3 (74 on wire, 74 captured)

...

Protocol: UDP (0x11)

Header checksum: 0x0a83 (correct)

Source: ca-ol-marseille-6-80.abo.w-n-doo.fr (62.161.101.80)

Destination: ns0.mrs.ftci.oleane.com (62.161.120.11) Notre DNS régional

#### User Datagram Protocol

Source port: 1038 (1038)

Destination port: domain (53)

Length: 40

Checksum: 0xb005

#### Domain Name System (query)

Transaction ID: 0xea25

Flags: 0x0100 (Standard query)

0... .. = Query

.000 0... .. = Standard query

.... ..0. .... = Message is not truncated

.... ...1 .... = Do query recursively

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

#### Queries

enprovence.com: type MX, class inet Notez la nature de la requête:

Name: enprovence.com

On demande un enregistrement de type MX

Type: Mail exchange

(Mail Exchanger)

Class: inet

La trame 3 constitue donc une requête DNS pour trouver un Mail Exchanger valide pour le domaine "enprovence.com"

Frame 4 (207 on wire, 207 captured)

...

Protocol: UDP (0x11)

Header checksum: 0x7fd6 (correct)

Source: ns0.mrs.ftci.oleane.com (62.161.120.11)

Destination: ca-ol-marseille-6-80.abo.w-n-doo.fr (62.161.101.80)

#### User Datagram Protocol

Source port: domain (53)

Destination port: 1038 (1038)

Length: 173

Checksum: 0xbffd

#### Domain Name System (response)

Transaction ID: 0xea25

Flags: 0x8180 (Standard query response, No error)

1... .. = Response

.000 0... .. = Standard query

.... ..0.. .... = Server isn't an authority for domain

.... ..0. .... = Message is not truncated

.... ...1 .... = Do query recursively

.... .... 1... .... = Server can do recursive queries

.... .... .... 0000 = No error

Questions: 1

Answer RRs: 2

Authority RRs: 2

Additional RRs: 3

Queries



enprovence.com: type MX, class inet  
Name: enprovence.com  
Type: Mail exchange  
Class: inet

**Answers** **La réponse de notre DNS concernant les MX**

**enprovence.com: type MX, class inet, preference 0, mx mail.monaco.net**  
Name: enprovence.com  
Type: Mail exchange  
Class: inet  
Time to live: 22 hours, 30 minutes, 40 seconds  
Data length: 19  
Preference: 0  
Mail exchange: mail.monaco.net

**enprovence.com: type MX, class inet, preference 1, mx dns2.monaco.net**  
Name: enprovence.com  
Type: Mail exchange  
Class: inet  
Time to live: 22 hours, 30 minutes, 40 seconds  
Data length: 9  
Preference: 1  
Mail exchange: dns2.monaco.net

**Notez qu'il y en a deux, avec des niveaux de préférence différents...**

**Notez également que les adresses IP n'ont pas été fournies...**

**Authoritative nameservers**

**enprovence.com: type NS, class inet, ns DNS1.monaco.net**  
Name: enprovence.com  
Type: Authoritative name server  
Class: inet  
Time to live: 14 hours, 39 minutes, 58 seconds  
Data length: 7  
Name server: DNS1.monaco.net

**enprovence.com: type NS, class inet, ns dns2.monaco.net**  
Name: enprovence.com  
Type: Authoritative name server  
Class: inet  
Time to live: 14 hours, 39 minutes, 58 seconds  
Data length: 2  
Name server: dns2.monaco.net

**Mais tout de même, la réponse intègre les noms des DNS impliqués dans l'affaire.**

**Additional records**

**mail.monaco.net: type A, class inet, addr 194.79.150.9**  
Name: mail.monaco.net  
Type: Host address  
Class: inet  
Time to live: 1 hour, 51 minutes, 41 seconds  
Data length: 4  
Addr: 194.79.150.9

**dns2.monaco.net: type A, class inet, addr 194.79.150.2**  
Name: dns2.monaco.net  
Type: Host address  
Class: inet  
Time to live: 13 hours, 11 minutes, 15 seconds  
Data length: 4  
Addr: 194.79.150.2

**DNS1.monaco.net: type A, class inet, addr 194.79.150.9**  
Name: DNS1.monaco.net

Type: Host address  
Class: inet  
Time to live: 14 hours, 9 minutes, 50 seconds  
Data length: 4  
Addr: 194.79.150.9

*Les "Additional records", tout le monde semble s'en moquer; pourtant, L'avenir va nous montrer qu'ils nous feraient gagner en efficacité... Nous avons ici toutes les IP nécessaires... Et pourtant... Notez également au passage la diversité des fonctions de l'hôte dns2.monaco.net Il est second MX et second NS*

Frame 5 (75 on wire, 75 captured)

...

Protocol: UDP (0x11)  
Header checksum: 0x0a81 (correct)  
**Source: ca-ol-marseille-6-80.abo.w-n-doo.fr (62.161.101.80)**  
**Destination: ns0.mrs.ftci.oleane.com (62.161.120.11)**

#### User Datagram Protocol

Source port: 1038 (1038)  
Destination port: domain (53)  
Length: 41  
Checksum: 0x3994

#### Domain Name System (query)

Transaction ID: 0xea26  
Flags: 0x0100 (Standard query)  
0... .. = Query  
.000 0... .. = Standard query  
.... ..0. .... = Message is not truncated  
.... ...1 .... = Do query recursively

Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0

#### Queries

**mail.monaco.net: type A, class inet**  
Name: mail.monaco.net  
Type: Host address  
Class: inet

*Et voilà, si le système avait tenu compte des "additional records". La question n'aurait pas été posée...*

Frame 6 (171 on wire, 171 captured)

...

Protocol: UDP (0x11)  
Header checksum: 0x7fed (correct)  
**Source: ns0.mrs.ftci.oleane.com (62.161.120.11)**  
**Destination: ca-ol-marseille-6-80.abo.w-n-doo.fr (62.161.101.80)**

#### User Datagram Protocol

Source port: domain (53)  
Destination port: 1038 (1038)  
Length: 137  
Checksum: 0xab21

#### Domain Name System (response)

Transaction ID: 0xea26  
Flags: 0x8180 (Standard query response, No error)  
1... .. = Response  
.000 0... .. = Standard query

```
.... .0.. .... = Server isn't an authority for domain
.... ..0. .... = Message is not truncated
.... ...1 .... = Do query recursively
.... .... 1... = Server can do recursive queries
.... .... .... 0000 = No error
```

Questions: 1

Answer RRs: 1

Authority RRs: 2

Additional RRs: 2

Queries

```
mail.monaco.net: type A, class inet
  Name: mail.monaco.net
  Type: Host address
  Class: inet
```

**Answers**

```
mail.monaco.net: type A, class inet, addr 194.79.150.9
```

...

**Authoritative nameservers** *Plus la liste des DNS ayant autorité*

```
MONACO.NET: type NS, class inet, ns DNS1.MONACO.NET
```

...

```
MONACO.NET: type NS, class inet, ns DNS2.MONACO.NET
```

...

Additional records

```
DNS1.MONACO.NET: type A, class inet, addr 194.79.150.9
```

...

```
DNS2.MONACO.NET: type A, class inet, addr 194.79.150.2
```

...

*Nous avons l'adresse de mail.monaco.net, mais nous la connaissons déjà...*

Frame 7 (75 on wire, 75 captured)

...

Protocol: UDP (0x11)

Header checksum: 0x0a80 (correct)

**Source:** ca-ol-marseille-6-80.abo.w-n-doo.fr (62.161.101.80)

**Destination:** ns0.mrs.ftci.oleane.com (62.161.120.11)

**User Datagram Protocol**

Source port: 1038 (1038)

Destination port: domain (53)

Length: 41

Checksum: 0x6692

**Domain Name System (query)**

Transaction ID: 0xea27

Flags: 0x0100 (Standard query)

```
0... .... = Query
```

```
.000 0... .... = Standard query
```

```
.... ..0. .... = Message is not truncated
```

```
.... ...1 .... = Do query recursively
```

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

**Queries**

```
dns2.monaco.net: type A, class inet
  Name: dns2.monaco.net
  Type: Host address
  Class: inet
```

*Encore une question futile...*

Frame 8 (166 on wire, 166 captured)

```
...
  Protocol: UDP (0x11)
  Header checksum: 0x7fec (correct)
  Source: ns0.mrs.ftci.oleane.com (62.161.120.11)
  Destination: ca-ol-marseille-6-80.abo.w-n-doo.fr (62.161.101.80)
User Datagram Protocol
  Source port: domain (53)
  Destination port: 1038 (1038)
  Length: 132
  Checksum: 0xd9dd
Domain Name System (response)
  Transaction ID: 0xea27
  Flags: 0x8180 (Standard query response, No error)
    1... .. = Response
    .000 0... .. = Standard query
    .... .0.. .. = Server isn't an authority for domain
    .... ..0. .... = Message is not truncated
    .... ...1 .... = Do query recursively
    .... .... 1... .. = Server can do recursive queries
    .... .... .... 0000 = No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 2
  Additional RRs: 2
  Queries
    dns2.monaco.net: type A, class inet
      Name: dns2.monaco.net
      Type: Host address
      Class: inet
  Answers
    dns2.monaco.net: type A, class inet, addr 194.79.150.2
```

```
...
  Authoritative nameservers
    MONACO.NET: type NS, class inet, ns DNS1.MONACO.NET
...
    MONACO.NET: type NS, class inet, ns dns2.monaco.net
...
  Additional records
    DNS1.MONACO.NET: type A, class inet, addr 194.79.150.9
...
    dns2.monaco.net: type A, class inet, addr 194.79.150.2
...
```

*Avec sa réponse pertinente, certes, mais qui ne nous apprend rien de nouveau*

A ce niveau, nous disposons:

- Des adresses des deux échangeurs de courrier pour le domaine "enprovence.com" (Dont nous avons appris au passage qu'il était hébergé à Monaco)
- Des adresses des serveurs de noms pour ce domaine.

Normalement, nous devrions attaquer le transfert du message, en commençant par le MX qui a la meilleure préférence. S'il ne répond pas, nous passerons à l'autre.

## La négociation SMTP.

Frame 9 (74 on wire, 74 captured)

...

Protocol: TCP (0x06) *Notez que l'on est maintenant en mode connecté...*

Header checksum: 0x28de (correct)

Source: ca-ol-marseille-6-80.abo.w-n-doo.fr (62.161.101.80)

Destination: dns1.monaco.net (194.79.150.9) *Ca ne vous choque pas?*

*On aurait pu s'attendre à ce que ce soit avec mail.monaco.net que le dialogue s'initie (c'est lui qui a la meilleure préférence)...*

*Mais regardez attentivement les adresses IP, et vous verrez que, surprise:*

*mail.monaco.net n'est autre que dns1.monaco.net*

Transmission Control Protocol, Src Port: 1027, Dst Port: smtp(25), Seq:2161513038,

Ack: 0

Source port: 1027 (1027)

Destination port: smtp (25)

Sequence number: 2161513038

Header length: 40 bytes

Flags: 0x0002 (SYN)

..0. .... = Urgent: Not set

...0 .... = Acknowledgment: Not set

.... 0... = Push: Not set

.... .0.. = Reset: Not set

.... ..1. = Syn: Set

.... ...0 = Fin: Not set

Window size: 32120

Checksum: 0x8248

Options: (20 bytes)

Maximum segment size: 1460 bytes

SACK permitted

Time stamp: tsval 5420137, tsecr 0

NOP

Window scale: 0 bytes

---

On va faire maintenant un petit bond en avant. L'analyse détaillée de ce qui suit s'apparente plus à une étude du protocole TCP, ce qui sort de notre sujet [et qui est traité ailleurs sur ce site](#). Toutefois, si vous voulez voir la suite, [le listing est disponible ici](#).

Juste pour constater que les e-mails circulent en clair sur le réseau et que n'importe quel "sniffer" peut les interpréter, je vous suggère d'aller directement voir la trame 45...

---

Frame 45 (706 on wire, 706 captured)

...

Protocol: TCP (0x06)

Header checksum: 0x2654 (correct)

Source: ca-ol-marseille-6-80.abo.w-n-doo.fr (62.161.101.80)

Destination: dns1.monaco.net (194.79.150.9)

Transmission Control Protocol, Src Port:1027, Dst Port:smtp(25, Seq:2161513153,

Ack:2324999158

Source port: 1027 (1027)

Destination port: smtp (25)

Sequence number: 2161513153

Acknowledgement number: 2324999158

Header length: 20 bytes

Flags: 0x0018 (PSH, ACK)

..0. .... = Urgent: Not set

...1 .... = Acknowledgment: Set

.... 1... = Push: Set

.... .0.. = Reset: Not set

.... ..0. = Syn: Not set

.... ...0 = Fin: Not set

Window size: 32120

Checksum: 0xfb10

Data (652 bytes)

0	00d0	7972	5c00	0020	af07	1a3d	0800	4500	..yr\... ..=..E.
10	02b4	15a6	4000	4006	2654	3ea1	6550	c24f	....@.@.&T>.eP.O
20	9609	0403	0019	80d6	12c1	8a94	abf6	5018	.....P.
30	7d78	fb10	0000	5265	6365	6976	6564	3a20	}x....Received:
40	6672	6f6d	2063	6872	6973	2028	6368	7269	from chris (chri
50	732e	6d61	6973	6f6e	2e6d	7273	205b	3139	s.maison.mrs [19
60	322e	3136	382e	302e	3130	5d29	0d0a	0962	2.168.0.10])...b
70	7920	6761	7465	7761	7931	2e6d	6169	736f	y gateway1.maiso
80	6e2e	6d72	7320	2850	6f73	7466	6978	2920	n.mrs (Postfix)
90	7769	7468	2053	4d54	5020	6964	2032	4131	with SMTP id 2A1
a0	3832	3130	3239	410d	0a09	666f	7220	3c65	821029A...for <e
b0	6d65	3133	4065	6e70	726f	7665	6e63	652e	mel3@enprovence.
c0	636f	6d3e	3b20	4d6f	6e2c	2032	3220	4d61	com>; Mon, 22 Ma
d0	7920	3230	3030	2032	303a	3238	3a30	3520	y 2000 20:28:05
e0	2b30	3230	3020	2843	4553	5429	0d0a	4d65	+0200 (CEST)..Me
f0	7373	6167	652d	4944	3a20	3c30	3035	3430	ssage-ID: <00540
100	3162	6663	3431	6224	3735	3132	6361	3330	1bfc41b\$7512ca30
110	2430	6130	3061	3863	3040	6d61	6973	6f6e	\$0a00a8c0@maison
120	2e6d	7273	3e0d	0a46	726f	6d3a	2022	4368	.mrs>..From: "Ch
130	7269	7374	6961	6e20	4341	4c45	4341	2220	ristian CALECA"
140	3c63	6872	6973	7469	616e	2e63	616c	6563	<christian.calec
150	6140	7761	6e61	646f	6f2e	6672	3e0d	0a54	a@w-n-doo.fr>..T
160	6f3a	203c	656d	6531	3340	656e	7072	6f76	o: <emel3@enprov
170	656e	6365	2e63	6f6d	3e0d	0a53	7562	6a65	ence.com>..Subje
180	6374	3a20	7465	7374	2053	4d54	500d	0a44	ct: test SMTP..D
190	6174	653a	204d	6f6e	2c20	3232	204d	6179	ate: Mon, 22 May
1a0	2032	3030	3020	3230	3a32	373a	3539	202b	2000 20:27:59 +
1b0	3032	3030	0d0a	4d49	4d45	2d56	6572	7369	0200..MIME-Versi
1c0	6f6e	3a20	312e	300d	0a43	6f6e	7465	6e74	on: 1.0..Content
1d0	2d54	7970	653a	2074	6578	742f	706c	6169	-Type: text/plai
1e0	6e3b	0d0a	0963	6861	7273	6574	3d22	6973	n;...charset="is
1f0	6f2d	3838	3539	2d31	220d	0a43	6f6e	7465	o-8859-1"..Conte
200	6e74	2d54	7261	6e73	6665	722d	456e	636f	nt-Transfer-Enco
210	6469	6e67	3a20	3762	6974	0d0a	582d	5072	ding: 7bit..X-Pr
220	696f	7269	7479	3a20	330d	0a58	2d4d	534d	iority: 3..X-MSM
230	6169	6c2d	5072	696f	7269	7479	3a20	4e6f	ail-Priority: No
240	726d	616c	0d0a	582d	4d61	696c	6572	3a20	rmal..X-Mailer:
250	4d69	6372	6f73	6f66	7420	4f75	746c	6f6f	Microsoft Outloo
260	6b20	4578	7072	6573	7320	352e	3030	2e32	k Express 5.00.2
270	3931	392e	3636	3030	0d0a	582d	4d69	6d65	919.6600..X-Mime
280	4f4c	453a	2050	726f	6475	6365	6420	4279	OLE: Produced By
290	204d	6963	726f	736f	6674	204d	696d	654f	Microsoft MimeO
2a0	4c45	2056	352e	3030	2e32	3931	392e	3636	LE V5.00.2919.66
2b0	3030	0d0a	0d0a	736e	6966	660d	0a0d	0a2e	00....sniff.....
2c0	0d0a								..

Et voilà... Sans précautions particulières, les messages circulent en clair sur le réseau au moment de leur émission vers leur(s) destinataire(s). Il vaut mieux le savoir. Nous verrons également dans le protocole POP3 que le message circule également en clair, avec en plus, le mot de passe du client, au moment de sa lecture.

Pour ceux qui ne sont pas encore rassasiés, [la fin de la connexion est disponible ici](#).

Pour finir, voici l'en-tête du message tel qu'il est déposé dans la Boîte aux lettres emel3@enprovence.com. Vous pouvez clairement y voir le chemin emprunté par le message. Comme chaque MTA complète l'en-tête en y insérant des lignes à son début, il faudra lire de bas en haut.

Return-Path: <christian.caleca@w-n-doo.fr>

\*\*\*

**2°/ Mon SMTP, côté Internet, envoie le message au SMTP du destinataire**

Received: from gateway1.maison.mrs  
(IDENT:postfix@ca-ol-marseille-6-80.abo.w-n-doo.fr [62.161.101.80])  
by mail.monaco.net (Pro-8.9.3/Pro-8.9.3) with ESMTP id UAA24841  
for <emel3@enprovence.com>; Mon, 22 May 2000 20:28:13 +0200

\*\*\*

**1°/ Mon poste de travail envoie le message sur mon SMTP, côté réseau ocal**

Received: from chris (chris.maison.mrs [192.168.0.10])  
by gateway1.maison.mrs (Postfix) with SMTP id 2A1821029A  
for <emel3@enprovence.com>; Mon, 22 May 2000 20:28:05 +0200 (CEST)

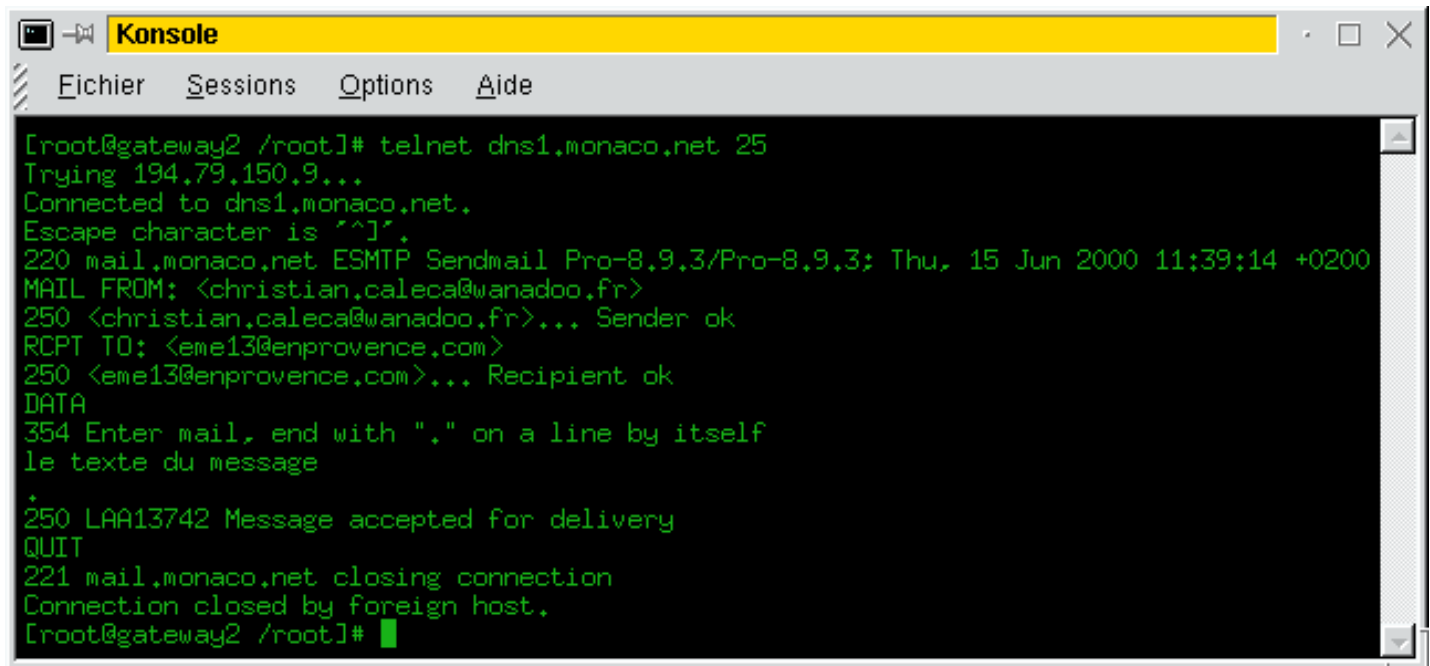
Message-ID: <005401bfc41b\$7512ca30\$0a00a8c0@maison.mrs>  
From: "Christian CALECA" <christian.caleca@w-n-doo.fr>  
To: <emel3@enprovence.com>  
Subject: test SMTP  
Date: Mon, 22 May 2000 20:27:59 +0200  
MIME-Version: 1.0  
Content-Type: text/plain;  
charset="iso-8859-1"  
Content-Transfer-Encoding: 7bit  
X-Priority: 3  
X-MSMail-Priority: Normal  
X-Mailer: Microsoft Outlook Express 5.00.2919.6600  
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6600  
Status:  
sniff

---

# Pour les plus démunis... Telnet.

## Envoi du message.

Pour ceux qui aiment bien comprendre, envoyons maintenant un message avec TELNET. La manip est faite à partir du poste Linux, parce que le client Telnet est tout de même plus efficace que celui fourni par windows, mais c'est possible aussi depuis un poste windows. Comme nous savons maintenant que le MX de enprovence.com n'est autre que dns1.monaco.net, nous allons nous adresser directement à lui.



```
[root@gateway2 /root]# telnet dns1.monaco.net 25
Trying 194.79.150.9...
Connected to dns1.monaco.net.
Escape character is '^]'.
220 mail.monaco.net ESMTP Sendmail Pro-8.9.3/Pro-8.9.3; Thu, 15 Jun 2000 11:39:14 +0200
MAIL FROM: <christian.caleca@wanadoo.fr>
250 <christian.caleca@wanadoo.fr>... Sender ok
RCPT TO: <eme13@enprovence.com>
250 <eme13@enprovence.com>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
le texte du message

250 LAA13742 Message accepted for delivery
QUIT
221 mail.monaco.net closing connection
Connection closed by foreign host.
[root@gateway2 /root]#
```

1. La ligne 1 démarre le client Telnet sur le serveur de messagerie dont on a trouvé le nom grâce au "sniff", sur le port 25 (port "officiel" d'écoute des MTA). On aurait pu le trouver également avec NSLOOKUP.
2. Les lignes 2, 3 et 4 indiquent que la connexion Telnet est correcte.
3. La ligne 5 (220 mail.monaco.net) est un message de bienvenue du serveur.
4. La ligne 6 (MAIL FROM) est la première commande que nous entrons. Elle donne l'adresse de l'émetteur du message. Suivant les règles de sécurité du MTA, cette adresse pourra ne pas être acceptée.
5. La ligne 7 (250 ...) indique que l'émetteur est accepté.
6. La ligne 8 (RCPT TO:) est la deuxième commande. Elle donne l'adresse du destinataire du message.
7. La ligne 9 (250...) Indique que le destinataire est accepté.
8. la ligne 10 (DATA) est encore une commande, elle indique que nous allons transmettre le message proprement dit.
9. La ligne 11 (354...) est une réponse indiquant comment il faut envoyer le texte du message.
10. La ligne 12 constitue le texte du message envoyé
11. La ligne 13 (.) indique le fin du message.
12. La ligne 14 (250...) Indique que le message est accepté.
13. La ligne 15 (QUIT) Est une commande pour indiquer au MTA que l'on a fini.
14. La ligne 16 (221) nous indique que le MTA a fermé la connexion.

## Analyse du résultat.

Voici le texte complet (En-tête comprise) du message tel que le destinataire le reçoit:

```
Return-Path: <christian.caleca@w-n-doo.fr>
C'est l'adresse de l'émetteur envoyée avec la commande MAIL FROM:
Received: from ca-ol-marseille-15-205.abo.w-n-doo.fr
      (IDENT:root@ca-ol-marseille-15-205.abo.w-n-doo.fr [213.56.62.205])
C'est la machine avec laquelle le message a été envoyé
by mail.monaco.net (Pro-8.9.3/Pro-8.9.3) with SMTP id TAA08106
for eme13@enprovence.com; Thu, 25 May 2000 19:43:56 +0200
C'est l'adresse du destinataire envoyée avec la commande RCPT TO:
Date: Thu, 25 May 2000 19:43:56 +0200
From: christian.caleca@w-n-doo.fr
Message-Id: <200005251743.TAA08106@mail.monaco.net>
```



X-Authentication-Warning: mail.monaco.net:

IDENT:root@ca-ol-marseille-15-205.abo.w-n-doo.fr [213.56.62.205]

didn't use HELO protocol

*Ici, c'est une info ajoutée par le MTA mail.monaco.net: Il prévient qu'il y a  
quelqu'un de grossier dans la chaîne  
d'envoi du message, il n'a pas utilisé le protocole HELO.*

Status:

le texte du message

## Quelques remarques.

- HELO, la commande manquante qui a généré le "X-Authentication-Warning", n'est pas nécessaire, mais il est préférable de l'utiliser. C'est de notre faute, nous aurions pu l'envoyer au début du dialogue. L'administrateur de mail.monaco.net aurait pu se vexer et rejeter le message.
- L'en-tête est très incomplète. A titre de comparaison, vous avez plus bas le même message envoyé "normalement" avec Outlook Express, par l'intermédiaire du MTA de wanadoo (smtp.wanadoo.fr). C'est tout simplement parce que tout ce qui n'est pas absolument nécessaire au transport du message est normalement inclus dans le texte du message. Nous aurions pu les introduire nous-même dans la petite manip vue plus haut. Certains MTA essayent plus ou moins de reconstruire les champs manquants, d'autres non.

## Conclusions.

Le processus d'envoi d'un e-mail par SMTP peut donc se découper en deux phases bien distinctes:

- Une recherche DNS sur les MX (Mail Exchanger) concernés par le domaine du destinataire (enprovence.com dans l'exemple).
- Un dialogue entre le MTA trouvé et le client, suivant le protocole SMTP pour transférer le message.
- Il n'est pas obligatoire que le message transite directement de votre serveur SMTP à celui du destinataire. Dans notre manipulation avec Telnet, nous avons contacté directement le MX du destinataire, lorsque nous envoyons le même message avec un MUA; le sera plus long, comme le montrent les exemples suivants:

- Envoyé par smtp.wanadoo.fr

Return-Path: <christian.caleca@w-n-doo.fr>

*Dernier MTA, celui qui gère la BAL du destinataire.*

Received: from camelia.wanadoo.fr (smtp-rt-10.wanadoo.fr [193.252.19.59])  
by mail.monaco.net (Pro-8.9.3/Pro-8.9.3) with ESMTP id OAA16616  
for <emel3@enprovence.com>; Sat, 27 May 2000 14:35:27 +0200

*Second MTA, toujours chez Wanadoo.*

*Le premier n'est donc qu'un agent de relais*

Received: from amyris.wanadoo.fr (193.252.19.150)  
by camelia.wanadoo.fr; 27 May 2000 14:08:11 +0200

*Premier MTA, celui sur lequel le MUA poste le message*

Received: from chris (62.161.101.80)  
by amyris.wanadoo.fr; 27 May 2000 14:07:57 +0200  
Message-ID: <00a001bfc7d4\$2cf01930\$0a00a8c0@maison.mrs>

From: "Christian CALECA" <christian.caleca@w-n-doo.fr>

To: <emel3@enprovence.com>

Subject:

Date: Sat, 27 May 2000 14:07:48 +0200

MIME-Version: 1.0  
Content-Type: text/plain;  
charset="iso-8859-1"  
Content-Transfer-Encoding: 7bit  
X-Priority: 3  
X-MSMail-Priority: Normal  
X-Mailer: Microsoft Outlook Express 5.00.2919.6600  
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6600  
Status: O

Le texte du message

Le chemin ici est le suivant:

- amyris.wanadoo.fr
- camelia.wanadoo.fr
- mail.monaco.net

Notez que n'apparaît pas smtp.wanadoo.fr

- Envoyé maintenant avec notre MTA personnel sur Gateway1:

Return-Path: <christian.caleca@w-n-doo.fr>

Received: from gateway1.maison.mrs

(IDENT:postfix@ca-ol-marseille-6-80.abo.wanadoo.fr [62.161.101.80])  
by mail.monaco.net (Pro-8.9.3/Pro-8.9.3) with ESMTP id PAA17676  
for <emel3@enprovence.com>; Sat, 27 May 2000 15:29:23 +0200

Received: from chris (chris.maison.mrs [192.168.0.10])

by gateway1.maison.mrs (Postfix) with SMTP id A38181105F  
for <emel3@enprovence.com>; Sat, 27 May 2000 15:29:15 +0200 (CEST)

Message-ID: <000901bfc7df\$884e4ad0\$0a00a8c0@maison.mrs>

From: "Christian CALECA" <christian.caleca@w-n-doo.fr>

To: <emel3@enprovence.com>

Subject:

Date: Sat, 27 May 2000 15:29:06 +0200

MIME-Version: 1.0

Content-Type: text/plain;

charset="iso-8859-1"

Content-Transfer-Encoding: 7bit

X-Priority: 3

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook Express 5.00.2919.6600

X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6600

Status: RO

Texte du message.

Le chemin ici est le suivant:

- gateway1.maison.mrs (notre MTA Postfix)
- mail.monaco.net

Ici, le message a directement été transmis depuis notre MTA vers celui du destinataire.

Ceci veut dire qu'il est parfaitement possible sur de grosses architectures, de créer des MTA qui ne font que relayer du courrier d'un point à un autre, sans gérer de destinataires.

---



# Un SMTP "perso"

[ [Accueil](#) ] [ [Les bases](#) ] [ [les Profondeurs](#) ] [ [Un SMTP "perso"](#) ] [ [Installation de Postfix](#) ] [ [Config avancée](#) ]  
[ [Conclusions](#) ]

---

## Que voulons-nous faire?

### Ce qui est utile.

Construire un serveur SMTP capable de relayer le courrier de nos postes locaux sans avoir à utiliser le serveur SMTP de notre fournisseur d'accès.

Notez cependant ceci :

Pour faire face à cette vérole de la messagerie que l'on appelle le "spam", de plus en plus de MTA destinataires n'acceptent plus de messages en provenance de MTA non connus. Dans le cadre d'un abonnement classique à un accès haut débit permanent, nous rencontrerons de plus en plus de problèmes de refus de la part des SMTP destinataires.

Quel intérêt alors, de monter son propre SMTP ?

- Vous pouvez disposer d'un nom de domaine officiel et repérable, auquel cas, votre MTA aura des chances de fonctionner, c'est le cas de bon nombre d'entreprises,
- Vous pouvez également utiliser votre MTA comme un relais vers le MTA de votre FAI. Les messages ne seront plus délivrés directement.  
Cette méthode ne vous affranchira pas des éventuelles pannes de MTA de votre FAI, mais vous n'aurez plus à attendre devant votre client de messagerie que le message veuille bien partir. Votre MTA s'arrangera avec celui de votre FAI pour transmettre les messages sitôt que ce sera possible, de façon transparente pour vous.
- Vous pouvez monter tout de même votre MTA en le configurant de la manière la plus propre possible et en essayant de contourner (proprement) les dispositifs de restriction. Il n'est bien entendu pas question de donner ici des méthodes frauduleuses.

### Ce qui est du luxe.

Au point où nous en sommes, autant réaliser un système de messagerie local. Je pourrai ainsi par exemple, envoyer un message à mes fils, situés dans leurs chambres respectives, quelques mètres plus loin :)

La seule chose que nous ne pourrons pas faire, c'est créer un système qui nous permette de recevoir du courrier directement sur notre domaine privé depuis l'Internet en se créant sa propre adresse de messagerie. Il nous manque peu de choses pour le faire, mais elles sont nécessaires:

- Un nom de domaine déposé.
- Une adresse IP fixe, c'est tout de même mieux, même si des solutions existent pour les adresses dynamiques.
- Un serveur DNS qui gère notre domaine et qui inscrive notre adresse IP en tant que MX (Mail eXchanger) pour notre domaine .

# De quoi avons-nous besoin?

De pas grand chose. Juste une machine sous Linux et même si elle est seule et directement connectée au Net, elle est parfaitement capable d'envoyer du courrier par elle-même, sans avoir à spécifier de serveur SMTP tiers. Il suffit qu'un MTA y soit installé, ce qui est la plupart du temps le cas si l'on choisit une option standard d'installation.

Les applications de ce type les plus connues sous Linux sont:

- Sendmail, le plus puissant, le plus ancien et le plus compliqué.
- Postfix, qui semble être un sérieux "challenger" (normalement installé par défaut avec la Mandrake 7.0 et suivantes)
- Qmail, dont on dit à peu près autant de bien que de mal
- Exim, qui est le MTA par défaut de l'illustre distribution Debian. C'est aussi un très bon MTA, affublé d'une documentation très riche, mais aussi très difficile à lire.

## Configuration utilisée ici.

Comme d'habitude, un petit réseau local de quelques hôtes sous Windows 98 ou supérieur, une passerelle Linux pour relier le tout à l'Internet. Cette passerelle, un P200 avec 128 Mo de RAM effectue le [masquage d'adresses](#) et sert également de [DNS](#) (Voir les chapitres consacrés à ce sujet).

## Comment nous y prendre?

- Nous allons dans un premier temps vérifier la présence du MTA Postfix et éventuellement l'installer, il est tout de même plus simple à manipuler que Sendmail.
- Nous allons ensuite nous intéresser un peu à l'anatomie de Postfix. Vous allez voir, ça fait un peu "usine à gaz", mais ce n'est pas si compliqué finalement.
- Enfin, nous allons configurer Postfix progressivement, pour essayer d'obtenir un fonctionnement fiable dans la majorité des cas.

## Notes de sécurité.

**Attention toutefois à ce que vous faites!**

**Sur une liaison permanente comme la notre, même avec une IP dynamique, il ne faut pas faire n'importe quoi.**

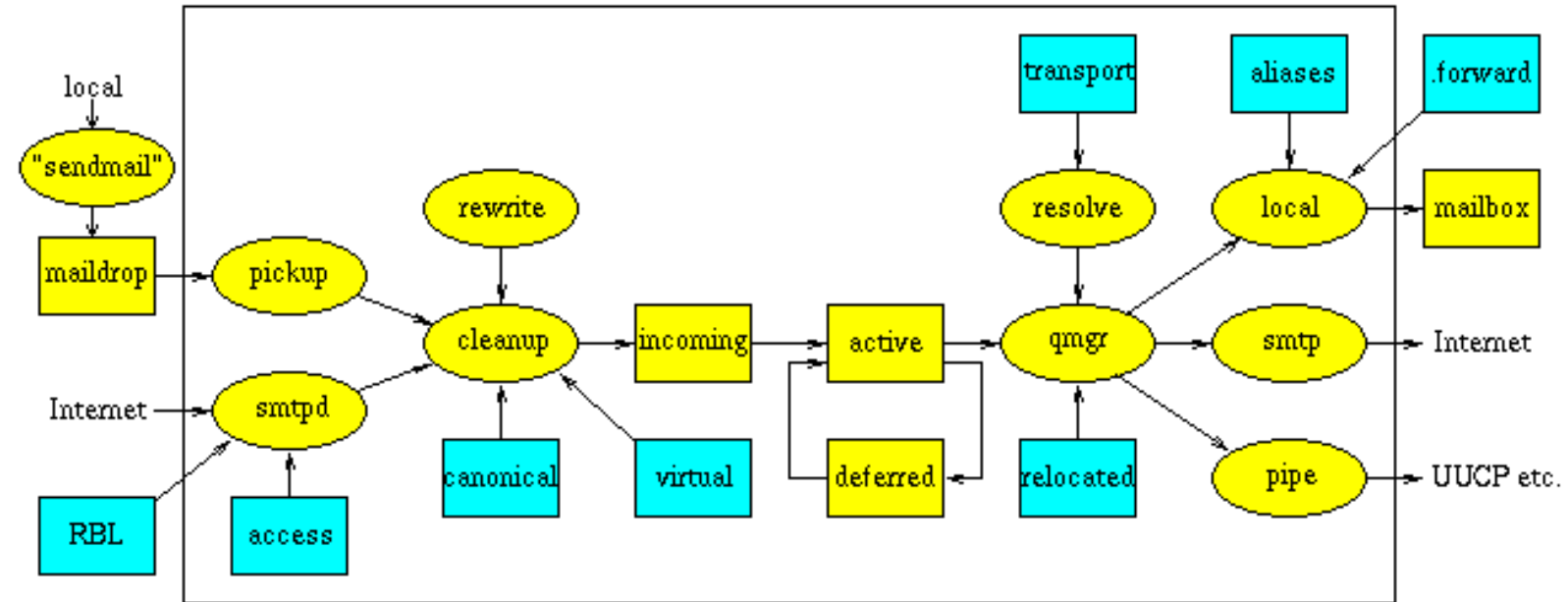
**Nous sommes en train de monter un serveur SMTP qui peut éventuellement servir de relais pour des utilisateurs mal intentionnés. Fréquentez un peu [fr.comp.mail](http://fr.comp.mail) pour voir ce qu'il peut se passer dans le petit monde des administrateurs de messagerie.**

**Il faut savoir que ces administrateurs sont confrontés aux problèmes créés par les "spammers" (sorte d'abrutis qui passent leur temps à inonder les boîtes aux lettres de messages inutiles, obscènes, voire vérolés). Normalement, pas mal de dispositions sont prises pour essayer de bloquer ces messages indésirables. Il est bon de ne jamais perdre de vue qu'il y a sur l'Internet des administrateurs professionnels**

qui se décarcassent pour que ça marche le mieux possible, et qu'il vaut mieux éviter de leur casser le travail.

# Anatomie de Postfix.

Postfix est un système de messagerie modulaire, contrairement à la plupart de ses concurrents. Vous avez ci-dessous le schéma fonctionnel dont nous allons essayer d'analyser grossièrement le fonctionnement. Tout ce qui suit peut être considéré comme une traduction libre de la documentation officielle du produit. Le site officiel de Postfix se trouve à l'adresse [www.postfix.org](http://www.postfix.org)

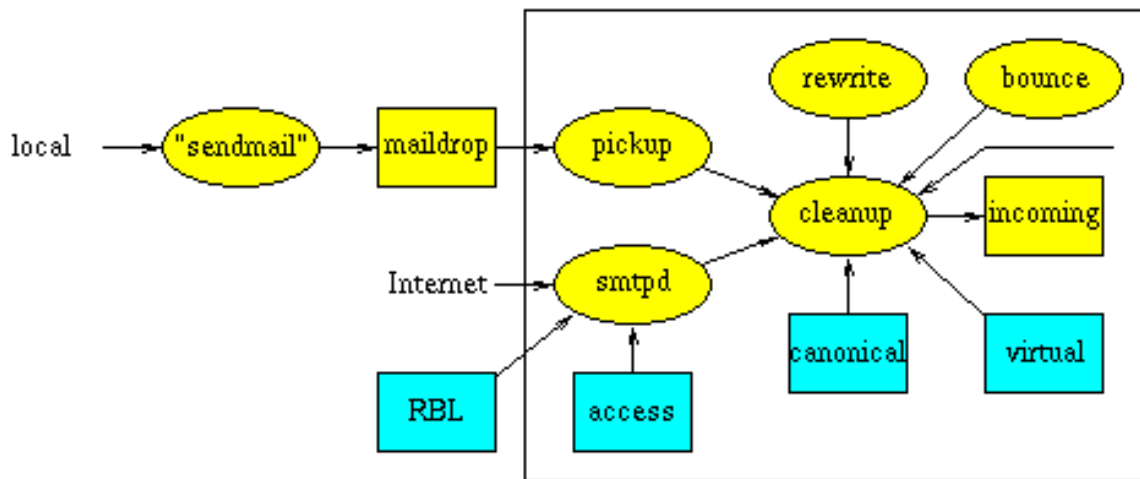


## Les files d'attente de Postfix.

Il y a cinq files d'attente pour les messages:

- "maildrop" qui reçoit les messages postés localement (depuis l'hôte lui-même).
- "incoming" qui reçoit aussi bien les messages postés localement que ceux qui arrivent du réseau (lorsque par exemple nous utilisons cet hôte comme serveur smtp pour notre réseau local). Les messages qui arrivent dans cette file ont déjà subi quelques traitements que nous détaillerons plus loin.
- "active" est la file qui contient les messages en cours d'envoi.
- "deferred" (différé), contient les messages qui, pour une raison ou une autre, n'ont pu être envoyés. Le protocole SMTP prévoit en effet de ne pas jeter systématiquement les messages qui n'ont pu être envoyés. Les messages classés dans "deferred" subiront plusieurs tentatives d'envoi en étant réinjectés dans "active".
- "mailbox" est la file d'attente des messages destinés aux utilisateurs locaux. nous verrons plus loin son utilité exacte.

# Réception d'un e-mail.



Lorsqu'un message arrive dans le système Postfix, quelle que soit son origine, son premier arrêt se fait dans "incoming". La figure ci contre montre les composants qui sont invoqués lors de l'arrivée d'un nouveau message.

## Origine du message.

### Le Message est posté localement.

Le programme Postfix "sendmail" (ne pas confondre avec le MTA concurrent) le dépose dans la file "maildrop" d'où il est retiré par le daemon "pickup". Ce daemon effectue quelques contrôles "sanitaires" dans le but de protéger le reste du système Postfix. Dans le but d'éviter des accidents, les permissions du répertoire contenant "maildrop" sont telles que tout le monde peut y écrire, mais aucun utilisateur ne peut en effacer le contenu.

### Le message vient du réseau.

Le serveur SMTP Postfix reçoit le message et effectue quelques contrôles "sanitaires", toujours dans le but de protéger le reste du système Postfix. Le serveur SMTP peut être configuré pour implémenter des contrôles UCE (Unsolicited Commercial Email) sur la base d'une liste noire locale où issue du réseau, de vérifications sur les DNS (domaine de l'expéditeur) où d'autres requêtes sur les informations concernant l'émetteur.

## Traitement du message.

### Le message n'est pas livrable.

Un e-mail est généré automatiquement par le système Postfix dans le but de renvoyer ce message à son expéditeur. Ce sont les daemons "bounce" (rebond) où "defer" (livraison) qui annoncent la mauvaise nouvelle.

Un e-mail est également généré automatiquement par le système Postfix dans le but de prévenir le responsable de la messagerie en cas de problème. Le système Postfix peut être configuré pour alerter

en cas de problème de protocole SMTP, de violation de règles de sécurité UCE etc. (Ce chemin est indiqué sur le graphique par la flèche sans label).

## Le message est livrable.

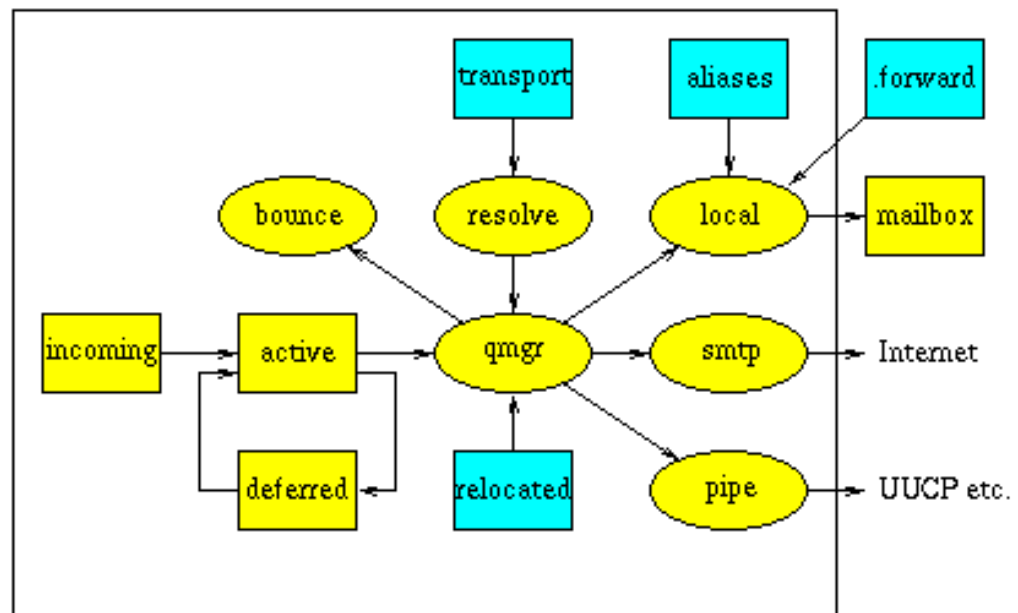
Le message est transmis par l'agent de livraison local soit par l'intermédiaire d'une entrée de la base de donnée des "alias" au niveau du système, soit par le fichier ".forward" au niveau de l'utilisateur. Nous reviendrons sur ces notions un peu complexes dans la configuration de Postfix.

Le daemon "cleanup" implémente le dernier traitement du message. Il ajoute le champ "**Form:**" et d'autres en-têtes dans le message, arrange les adresses de réponses dans le format "*user@fully.qualified.domain*" et optionnellement extrait les adresses des destinataires de l'en-tête. Le daemon "cleanup" insère le résultat dans une seule file d'attente: "incoming" et notifie le "queue manager" (qmgr sur le schéma complet) de l'arrivée d'un nouveau message. Le daemon "cleanup" peut être configuré pour transformer les adresses sur la base des tables de consultation "canonical" et "virtual". Nous verrons également cela dans la configuration de Postfix.

Sur la requête du daemon "cleanup", le daemon "trivial-rewrite" ré écrit les adresses dans le format standard "*user@fully.qualified.domain*".

## Livraison du message.

Chaque fois qu'un message est déposé dans la file d'attente "incoming", l'étape suivante consiste à le livrer. La figure ci contre montre les principaux composants de la fonction de livraison de Postfix.



Le gestionnaire de file d'attente est le cœur du système de messagerie Postfix. Il contacte les agents de livraison "local", "smtp" ou "pipe" (les anglophones ont un langage parfois amusant: Faire un "pipe" sur une "queue", ça peut prêter à confusion) et envoie une demande de livraison avec le chemin d'accès au fichier qui contient la file d'attente, l'adresse de l'expéditeur, le nom de l'hôte à qui il faut livrer si la destination n'est pas locale, et une où plusieurs adresses de destinataires.

Le gestionnaire maintient une file d'attente "deferred" séparée pour chaque message qui n'a pas pu être livré, de manière à ce qu'un compte-rendu de livraison trop volumineux ne vienne pas ralentir l'accès des autres files.

Le gestionnaire maintient une petite file d'attente "active" avec juste quelques messages prêts pour la livraison.



"active" agit comme une petite fenêtre sur les files d'attente "incoming" ou "deferred". Cette méthode évite au gestionnaire de faire des débordements de mémoire si le serveur est fortement chargé.

Optionnellement, le gestionnaire fait "rebondir" le message pour les destinataires qui sont référencés dans la table "relocated". Cette table contient des informations sur les utilisateurs qui ont changé d'adresse.

Sur la demande du gestionnaire de file d'attente, le daemon "trivial-rewrite" résout les destinations. Par défaut, il fait uniquement la distinction entre les destinations locales où distantes. Des informations de routage additionnelles peuvent être spécifiées dans la table "transport".

Sur la demande du gestionnaire de file d'attente, les daemons "bounce" et "defer" génèrent des rapports de non-livraison lorsqu'un message ne peut être acheminé, soit à cause d'une erreur non récupérable, soit parce que le destinataire n'est pas joignable pendant une durée trop longue.

L'agent local de la livraison sait gérer les boîtes aux lettres de type UNIX, les bases de données du type "alias" de sendmail (le MTA concurrent), les fichiers de type . forward de l'utilisateur. De multiples agents locaux de livraison peuvent être exécutés en parallèle, mais la livraison en parallèle au même utilisateur est habituellement limitée.

En même temps que l'agent de livraison "sendmail", l'agent de livraison "local" implémente l'interface utilisateur familière de sendmail (le MTA concurrent)

L'agent de la livraison locale a des possibilités pour utiliser d'autres moyens de livraison locale: vous pouvez le configurer pour livrer aux fichiers de boîte aux lettres dans les répertoires locaux d'utilisateur, et vous pouvez même le configurer pour déléguer la livraison de boîte aux lettres à une commande externe telle que le programme populaire "procmail".

Le client smtp recherche une liste d'échangeurs de courrier pour l'hôte de destination, trie la liste par préférence, et essaye chaque adresse alternativement jusqu'à ce qu'il trouve un serveur qui répond. Sur un système postfix chargé, vous verrez plusieurs processus de client de smtp fonctionner en parallèle.

Le "pipe" est l'interface de sortie vers d'autres transports de courrier (Le programme "sendmail" est l'interface d'entrée). Le système de courrier Postfix peut par exemple livrer du courrier par l'intermédiaire du protocole UUCP. Ce protocole vénérable est encore largement répandu. Par défaut, Postfix comprend des adresses de type "bang path" (Rassurez-vous, ici on parle de SMTP, pas de UUCP qui n'est plus de mise sur Internet, mais seulement dans des réseaux privés).

## Conclusion.

Si vous avez eu le courage de lire cette page jusqu'ici, vous êtes un brave. Si en plus, vous avez tout compris, alors vous êtes remarquable!

Pour résumer la situation, disons que Postfix sait faire les choses suivantes:

- Recevoir du courrier depuis le réseau. (Cette fonction nous intéresse).
- Recevoir du courrier depuis l'hôte local (Pourquoi ne pas s'en servir?)
- Acheminer du courrier dont la destination est ailleurs (C'est exactement ce que nous cherchons à faire).
- Acheminer du courrier localement. (Pourquoi pas?)
- Dans tout ce processus, Postfix est capable de modifier quelque peu les en-têtes de messages. Ca n'a pas beaucoup d'intérêt pour nous, sauf dans le cas où nous utiliserons l'hôte de Postfix pour expédier du courrier.

Il y a tout de même un détail qu'il ne faut pas laisser dans l'ombre: Postfix n'est pas un serveur POP ni IMAP. Même s'il sait livrer du courrier local, il ne sait pas gérer les boîtes aux lettres pour des clients distants. Si l'on veut

réaliser cette opération, il faudra ajouter un autre logiciel, ce que nous n'allons d'ailleurs pas nous priver de faire...

---

[ [Précédente](#) ] [ [Accueil](#) ] [ [Suivante](#) ]

---

# Installation de Postfix

[ [Accueil](#) ] [ [Les bases](#) ] [ [les Profondeurs](#) ] [ [Un SMTP "perso"](#) ] [ [Installation de Postfix](#) ] [ [Config avancée](#) ] [ [Conclusions](#) ]

---

## Configuration.

Nous l'avons dit, pour un petit réseau local, un P200 avec 128 Mo de RAM suffit très largement. Nous utilisons ici une Mandrake 9, qui normalement, installe Postfix par défaut. Postfix se trouve en paquets binaires pour toutes les grandes distributions Linux (RedHat, Debian, Mandrake...).

La machine en question s'appelle gw1.maison.mrs dans le réseau local. La commande :

```
hostname
```

affiche donc :

```
gw1.maison.mrs
```

## Vérifications.

Avant d'installer Postfix, il serait bon de vérifier si, par hasard, ce ne serait pas déjà fait, et il y a de fortes chances que ce soit fait. Pourquoi? Parce que le service de messagerie est un service "de base" chez UNIX. Il est fort probable que votre distribution Linux ait installé un MTA .

Le moyen le plus simple, c'est de vérifier la présence d'un service appelé "postfix" dans le répertoire "/etc/rc.d/init.d", et de vérifier que ce service est démarré dans le "runlevel" que vous utilisez (3 ou 5, suivant que vous démarrez en mode texte ou en mode graphique).

La commande (sous root):

```
/etc/init.d/postfix status
```

devrait donner un résultat explicite :

- -bash: /etc/init.d/postfix: No such file or directory  
# Probablement que Posfix n'est pas installé...
- master (pid xxxx) est en cours d'exécution...  
# Tout va bien , Postfix est installé et tourne.
- master est arrêté  
# Postfix est installé, mais ne tourne pas.

## Avant tout...

## Postfix doit tourner.

Avec la configuration par défaut, Postfix doit pouvoir tourner. Vérifiez que c'est le cas, comme vu plus haut.

## Les aliases.

Les aliases servent à rediriger les messages entrants pour un utilisateur vers un autre utilisateur. Le fichier /etc/postfix/aliases est là pour définir des sortes de redirections. En l'observant, vous constaterez qu'il existe beaucoup d'utilisateurs "fantômes", tous renvoyés vers "root".

Il faut savoir que Postfix n'a en principe pas le droit d'envoyer des messages à root. Vous avez, bien sûr, sur votre machine Linux, un compte d'utilisateur "normal" (pas root). C'est le moment de modifier le fichier des "aliases" pour rediriger "root" vers cet utilisateur. **Il faut le faire**, c'est impératif. Sur ma configuration, il existe un compte "chris" et la dernière ligne de /etc/postfix/aliases est de la forme :

```
root: chris
```

Faites la modification adaptée à votre utilisateur et relancez Postfix par un :

```
postfix reload
```

Dans la suite, nous appellerons ce compte : "user".

La fonction d'alias est plus largement détaillée plus loin dans cette page.

## Premier test : messagerie locale.

Il existe un fichier de logs très utile pour nous : /var/log/mail/info. Nous allons l'utiliser en permanence dans la suite.

Ouvrez une console sous root et faites :

```
tail -f /var/log/mail/info
```

Ceci vous permettra de suivre ce qu'il se passe plus facilement.

Nous allons, en restant complètement en local, envoyer un message à root, en étant l'utilisateur normal, celui que nous avons choisi comme alias de root, et que nous avons convenu d'appeler "user".

Ouvrez une deuxième console avec "user".

nous allons envoyer un message à "root" avec l'outil, spartiate, certes, mais installé par défaut dans Mandrake : "mail".

```
[chris@gw1 chris]$ mail root
Subject: test interne
coucou
.
Cc:
[chris@gw1 chris]$
```

Il n'est pas nécessaire d'indiquer l'adresse de "root". Sous entendu, c'est le root local. Nous entrons en mode interactif, mail demande d'abord le sujet du message. Ensuite il faut saisir le texte du message, en le terminant par une ligne qui ne contient qu'un point.

Mail demande alors d'éventuels destinataires en "carbon copy", nous laissons cette ligne vide. Un "return" et c'est fini.

Observons le journal dans la console root:

```
May 11 15:21:22
    gw1 postfix/nqmgr[4056]: 351BD800081:
    from=<chris@gw1.maison.mrs>, size=220, nrcpt=1 (queue active)
May 11 15:21:22
    gw1 postfix/local[4256]: 351BD800081:
    to=<chris@gw1.maison.mrs>, orig_to=<root>,
    relay=local, delay=0, status=sent ("|/usr/bin/procmail -Y -a $DOMAIN")
```

Tout semble bien s'être passé. Notez que le destinataire n'est pas root mais chris, le système d'alias a fonctionné correctement. Nous devons donc retrouver ce message dans notre boîte aux lettres (celle de chris) :

```
[chris@gw1 chris]$ mail
Mail version 8.1.1 6/6/93. Type ? for help.
"/var/spool/mail/chris": 2 messages 1 new
1 MAILER-DAEMON@gw1 Sat May 10 19:20 13/550 "DON'T DELETE THIS MESSAGE -- FOLDER
INTERNAL DATA"
```

```
>N 2 chris@gwl.maison Sun May 11 15:21 12/371 "test interne"
&
```

La commande "mail" toute seule permet de consulter ses messages. La partie surlignée indique un nouveau message. Nous tapons :

```
& t 2
Message 2:
From chris@gwl.maison.mrs Sun May 11 15:21:22 2003
X-Original-To: root
Delivered-To: postfix@gwl.maison.mrs
To: root@gwl.maison.mrs
Subject: test interne
Date: Sun, 11 May 2003 15:21:22 +0200 (CEST)
From: chris@gwl.maison.mrs (Christian Caléca)
```

coucou

&

Tout va bien, en local, ça fonctionne.

Quittons proprement mail en tapant juste un "x" ;

```
& q
Saved 1 message in mbox
Held 1 message in /var/spool/mail/chris
[chris@gwl chris]$
```

Bien. Essayons maintenant, en étant root d'envoyer un message à chris :

Je ne détaille pas trop, voici la séquence :

**## On passe en root pour envoyer...**

```
[chris@gwl chris]$ su root
Password:
[root@gwl chris]# mail chris
Subject: de root a chris
re coucou
.
```

Cc:  
**## On quitte root pour revenir en chris...**

```
[root@gwl chris]# exit
exit
[chris@gwl chris]$ mail
Mail version 8.1.1 6/6/93. Type ? for help.
"/var/spool/mail/chris": 2 messages 1 new
1 MAILER-DAEMON@gwl Sat May 10 19:20 13/550 "DON'T DELETE THIS MESSAGE -- FOLDER
INTERNAL DATA"
```

```
>N 2 root@gwl.maison. Sun May 11 15:42 12/374 "de root a chris"
& t 2
```

```
Message 2:
From root@gwl.maison.mrs Sun May 11 15:42:21 2003
X-Original-To: chris
Delivered-To: chris@gwl.maison.mrs
To: chris@gwl.maison.mrs
Subject: de root a chris
Date: Sun, 11 May 2003 15:42:21 +0200 (CEST)
From: root@gwl.maison.mrs (Christian Caleca) ### Voir remarque plus bas.
```

re coucou

```
& x  
[chris@gwl chris]$
```

Et dans le log, nous voyons :

```
May 11 15:42:21  
    gwl postfix/nqmgr[4056]: 63F3F800081:  
    from=<root@gwl.maison.mrs>, size=226, nrcpt=1 (queue active)  
May 11 15:42:21  
    gwl postfix/local[4333]: 63F3F800081:  
    to=<chris@gwl.maison.mrs>, orig_to=<chris>,  
    relay=local, delay=0, status=sent ("|/usr/bin/procmail -Y -a $DOMAIN")
```

Tout va toujours bien. Si root apparaît comme Christian Caleca, c'est que le fichier /etc/passwd a été modifié à la ligne "root" comme suit :

```
root:x:0:0:Christian Caleca:/root:/bin/bash
```

## Deuxième test : vers dehors.

Puisque tout se passe bien en local, essayons maintenant d'envoyer un message distant :

```
[chris@gwl chris]$ mail christian.caleca@free.fr  
Subject: test distant  
re re coucou  
.  
Cc:  
[chris@gwl chris]$
```

Je m'envoie un message dans ma boîte aux lettres chez Free. Voyons le journal :

```
May 11 16:06:23  
    gwl postfix/pickup[4746]: 61D3F800081: uid=501 from=<chris>  
May 11 16:06:23  
    gwl postfix/cleanup[4844]: 61D3F800081:  
message-id=<20030511140623.61D3F800081@gwl.maison.mrs>  
May 11 16:06:23  
    gwl postfix/nqmgr[4747]: 61D3F800081:  
    from=<chris@gwl.maison.mrs>, size=227, nrcpt=1 (queue active)  
May 11 16:06:57  
    gwl postfix/smtp[4846]: 61D3F800081:  
    to=<christian.caleca@free.fr>,  
    relay=mx.free.fr[213.228.0.13], delay=34,  
    status=bounced (host mx.free.fr[213.228.0.13]  
    said: 553 sorry, your envelope sender domain must exist (#5.7.1) (in reply to  
MAIL FROM command))  
May 11 16:06:57  
    gwl postfix/cleanup[4844]: 25CD28000BD:  
message-id=<20030511140657.25CD28000BD@gwl.maison.mrs>  
May 11 16:06:57  
    gwl postfix/nqmgr[4747]: 25CD28000BD: from=<>, size=2042, nrcpt=1 (queue active)  
May 11 16:06:57  
    gwl postfix/local[4849]: 25CD28000BD: to=<chris@gwl.maison.mrs>,  
    relay=local, delay=0, status=sent ("|/usr/bin/procmail -Y -a $DOMAIN")
```

Là, si j'ose ainsi m'exprimer, ça ne sent pas très bon... La zone surlignée indique l'erreur 553, explicitement indiquée par le

texte "le domaine de l'enveloppe de l'émetteur doit exister" et maison.mrs, c'est un domaine "en bois" qui n'est pas connu sur le Net.

Les lignes qui suivent dans le log semblent indiquer qu'un message a été envoyé en local à chris@gw1.maison.mrs. Allons voir ça.

```
[chris@gw1 chris]$ mail
Mail version 8.1.1 6/6/93. Type ? for help.
"/var/spool/mail/chris": 2 messages 1 new
1 MAILER-DAEMON@pchris Sat May 10 19:20 13/550 "DON'T DELETE THIS MESSAGE -- FOLDER
INTERNAL DATA"
>N 2 MAILER-DAEMON@pchris Sun May 11 16:06 63/2125 "Undelivered Mail Returned to
Sender"
& t 2
Message 2:
From MAILER-DAEMON Sun May 11 16:06:57 2003
X-Original-To: chris@gw1.maison.mrs
Delivered-To: chris@gw1.maison.mrs
Date: Sun, 11 May 2003 16:06:57 +0200 (CEST)
From: MAILER-DAEMON@gw1.maison.mrs (Mail Delivery System)
Subject: Undelivered Mail Returned to Sender
To: chris@gw1.maison.mrs
MIME-Version: 1.0
Content-Type: multipart/report; report-type=delivery-status;
boundary="61D3F800081.1052662017/gw1.maison.mrs"
```

This is a MIME-encapsulated message.

```
--61D3F800081.1052662017/gw1.maison.mrs
Content-Description: Notification
Content-Type: text/plain
```

This is the Postfix program at host gw1.maison.mrs.

I'm sorry to have to inform you that the message returned below could not be delivered to one or more destinations.

For further assistance, please send mail to <postmaster>

If you do so, please include this problem report. You can delete your own text from the message returned below.

The Postfix program

<christian.caleca@free.fr>: host mx.free.fr[213.228.0.13] said: 553 sorry, your envelope sender domain must exist (#5.7.1) (in reply to MAIL FROM command)

```
--61D3F800081.1052662017/gw1.maison.mrs
Content-Description: Delivery error report
Content-Type: message/delivery-status
```

```
Reporting-MTA: dns; gw1.maison.mrs
Arrival-Date: Sun, 11 May 2003 16:06:23 +0200 (CEST)
```

```
Final-Recipient: rfc822; christian.caleca@free.fr
Action: failed
```

Status: 5.0.0  
Diagnostic-Code: X-Postfix; host mx.free.fr[213.228.0.13] said: 553 sorry, your envelope sender domain must exist (#5.7.1) (in reply to MAIL FROM command)

--61D3F800081.1052662017/gw1.maison.mrs  
Content-Description: Undelivered Message  
Content-Type: message/rfc822

To: christian.caleca@free.fr  
Subject: test distant  
Message-Id: <20030511140623.61D3F800081@gw1.maison.mrs>  
Date: Sun, 11 May 2003 16:06:23 +0200 (CEST)  
From: chris@gw1.maison.mrs (Christian Caléca)

re re coucou

--61D3F800081.1052662017/gw1.maison.mrs--

&

Le "MAILER-DAEMON" renvoie un message à l'expéditeur, lui indiquant que son message a été refusé avec la raison de ce refus et la copie du message refusé. Ça n'a pas marché, mais ça l'a fait proprement.

## Première panne, premier remède.

Tout utilisateur d'une machine Linux, avec un MTA installé, dispose par le fait d'une adresse locale de la forme :  
utilisateur@nom.pleinement.qualifié.de.la.machine.

Dans notre cas, pour l'utilisateur "chris", ça donnera :  
chris@gw1.maison.mrs

Lorsque chris va utiliser "mail", ce dernier exploitera par défaut cette adresse comme étant celle de l'expéditeur. Ça ne pose aucun problème dans la messagerie locale, ça en pose naturellement un si chris envoie un message "à l'étranger" (chez free, dans l'exemple). En effet, l'adresse de l'émetteur n'a aucune validité sur le Net, puisque le domaine maison.mrs n'existe pas. Notez que l'on trouve encore quelques MTA extérieurs, qui ne font pas cette vérification.

Sauf si vous travaillez sur la machine qui héberge le MTA, avec un MUA (client de messagerie) aussi rudimentaire que "mail", ça ne gênera pas. En effet, un MUA plus évolué vous permettra de paramétrer une adresse d'auteur autre.

Il existe cependant un moyen de résoudre ce problème, si vous devez envoyer des messages depuis l'hôte du MTA. Il existe en effet une foule de bonnes raisons pour définir des scripts qui vous enverront des messages dans une boîte aux lettres distante...

## Changer l'adresse de l'expéditeur.

Il nous faut remplacer les adresses du genre "*root@gw1.maison.mrs*" par une vraie adresse comme "*christian.caleca@free.fr*". C'est tout à fait réalisable grâce à la fonction de réécriture d'adresse.

### Mode opératoire.

- Nous sommes "root" et nous créons avec un éditeur de texte quelconque, un fichier que nous allons appeler "sender\_canonical", dans lequel sur chaque ligne nous mettons:
  - Le nom d'utilisateur concerné (par exemple "root")
  - Un espace
  - L'adresse que l'on veut voir figurer (par exemple: christian.caleca@wanadoo.fr)
  - Répéter cette opération pour tous les utilisateurs de la machine Linux.



A la fin de l'opération, le fichier pourrait ressembler à ceci:

```
root      christian.caleca@free.fr #L'administrateur (moi)
chris     christian.caleca@free.fr # autre moi
```

N'oubliez pas d'éventuels utilisateurs "fantômes" comme "webmaster", "postmaster"... Tout utilisateur attaché à un service susceptible de vous envoyer des messages externes, si vous en avez besoin.

- Nous sauvons ce fichier dans le répertoire /etc/postfix

- Nous exécutons la commande

```
postmap /etc/postfix/sender_canonical
```

(Cette commande a pour effet de créer un fichier de base de données appelé sender\_canonical.db dans le même répertoire.

- **Nous effectuons une copie de sauvegarde du fichier /etc/postfix/main.cf que nous appellerons par exemple main.cf.0**

- Nous ouvrons avec notre éditeur de texte le fichier "/etc/postfix/main.cf" et nous ajoutons au paragraphe "ADDRESS REWRITING" la ligne (sans #):

```
sender_canonical_maps = hash:/etc/postfix/sender_canonical
```

- On enregistre et on exécute la commande:

```
postfix reload
```

- pour recharger le nouveau paramétrage

Et voilà. Maintenant, si j'envoie un message avec "mail" en tant que "root" ou "chris", le champ "From:" ne contiendra plus "*root@gwl.maison.mrs*", mais "*christian.caleca@free.fr*"

## Troisième test : depuis un poste client du LAN.

Ne faisons pas de "suspens" inutile, dans la configuration initiale de Postfix, il y a de fortes chances pour que ça ne fonctionne pas. Pour des raisons de sécurité, votre MTA est probablement configuré pour ne pas accepter de messages venant d'ailleurs que de "localhost"

## Modification minimale de la configuration.

- Vous allez dans /etc/postfix/main.cf qui est le fichier de configuration principal de Postfix.
- Cherchez dedans "inet\_interfaces", qui doit par défaut être égal à "localhost".
- Ne succombez pas, par simplicité, à l'envie de remplacer "localhost" par "all", ce qui potentiellement risquerait d'en faire un "open relay", mettez plutôt \$myhostname, localhost.
- Relancez Postfix par un /etc/init.d/postfix reload

Bien. Passons maintenant sur un poste du réseau privé. Nous allons utiliser Outlook Express.

Nous allons dans le menu Outils/Comptes, Onglet "courrier", puis un double click sur le compte par défaut...

Dans les propriétés de ce compte, pour le courrier sortant, remplacez votre

**Propriétés de Personnel** ? X

Général Serveurs Connexion Sécurité Avancé

Informations sur le serveur

Mon serveur de courrier entrant est un serveur **POP3**

Courrier entrant (POP3):

Courrier sortant (SMTP):

Serveur de courrier entrant

Nom du compte:

Mot de passe:

☒ Se souvenir du mot de passe

☐ Se connecter avec l'authentification par mot de passe sécurisé

Serveur de courrier sortant

☐ Mon serveur requiert une authentification

actuel serveur SMTP par:

- Le nom DNS de votre passerelle Linux si vous avez déjà configuré votre DNS personnel
- L'adresse IP de votre passerelle sur le réseau privé sinon.

C'est fait, il ne reste plus qu'à cliquer sur OK.

Nous nous envoyons à nous même un message bien senti du genre "Bonjour tout le monde"... Un tout petit instant d'attente et nous allons consulter notre boîte aux lettres:

```
Return-Path: <christian.caleca@free.fr>
Delivered-To: online.fr-christian.caleca@free.fr
Received: (qmail 8844 invoked from network); 21 May 2000 17:53:06 +0200
Received: from gw1.maison.mrs (62.161.101.80)
    by mrelay3-2.free.fr with SMTP; 21 May 2000 17:53:06 +0200
Received: from chris (pchris.maison.mrs [192.168.0.10])
    by gw1.maison.mrs (Postfix) with SMTP id 022A11029A
for <christian.caleca@free.fr>; Sun, 21 May 2000 17:52:56 +0200 (CEST)
Message-ID: <00a601bfc33c$9e749dc0$0a00a8c0@maison.mrs>
From: "Christian CALECA" <christian.caleca@free.fr>
To: <christian.caleca@free.fr>
Subject: Test Postfix
Date: Sun, 21 May 2000 17:52:50 +0200
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2919.6600
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6600
```

Bonjour tout le monde

Il y est!

Notez les lignes surlignées, votre SMTP fonctionne comme les vrais (d'ailleurs, c'en est un), il s'inscrit dans l'itinéraire suivi.

## Premier bilan.

Nous avons un MTA en état de marche, qui devrait pouvoir nous permettre de livrer directement notre courrier aux destinataires.

Malheureusement, à cause des problèmes de spam qui vont sans cesse croissants, Nous allons rapidement nous heurter à bon nombre de restrictions imposées par les administrateurs des SMTP des divers domaines destinataires.

Nous en avons déjà vu une, minimaliste, qui consiste à vérifier que le domaine de l'expéditeur est un domaine valide, Nous allons en voir dans la suite beaucoup d'autres.

---

## Configuration minimale de Postfix.

### Sécurités minimales.

Votre MTA est connecté à l'Internet de façon permanente. A priori, il sait faire tout ce qu'un MTA peut faire:

Il peut éventuellement servir de serveur SMTP à n'importe qui, il ne faut pas que cela puisse se faire. Nous l'avons déjà dit, les administrateurs de messageries prennent quelques précautions pour empêcher la propagation de certains messages indésirables, spams, messages contenant des virus, et autres perversités humaines. Il est facile de repérer un serveur SMTP à l'écoute sur le port 25 et d'essayer ensuite de s'en servir de relais; Vous risqueriez de vous retrouver "vecteur d'immondices".

De plus, si votre MTA sert "au peuple des spammers", votre FAI aura tôt fait de vous repérer et vous aurez alors probablement beaucoup d'ennuis...

La précaution élémentaire que nous avons prise plus haut, sur le paramètre "inet\_interfaces" constitue un strict minimum.

Dans un cas simple où votre MTA ne doit servir que dans les cas suivants :

- envoi de messages depuis votre domaine vers l'extérieur,
- envoi de messages locaux à destination d'utilisateurs de votre domaine (le même que celui de votre MTA), mais uniquement depuis le LAN (réseau local),

Vous pourrez toujours bloquer le port 25 en entrée sur l'interface côté Internet. De l'extérieur, on ne verra même plus que vous avez un SMTP.

Si vous disposez d'un domaine "officiel" sur le Net et que vous souhaitez exploiter votre MTA pour recevoir des messages depuis l'extérieur, ce sera un peu plus compliqué. Nous ne verrons pas en détail ici comment faire, disons juste que le paramètre "mydestination" vous permettra d'expliquer à Postfix qu'il ne doit accepter de messages venant de dehors qu'à la condition que ces messages lui soient destinés. Autrement dit, un message venant de dehors, à destination de @mondomaine.tld (si ce domaine est valide sur le Net), on acceptera. Mais un message entrant de dehors à destination de @nimportequelautre domaine.tld, on refusera de relayer.

Mais ce type de fonctionnement dépasse largement le cadre de cet exposé.

## Comment configurer Postfix.

Postfix se configure, nous l'avons vu, à partir d'un unique fichier: "main.cf" que l'on trouve normalement dans /etc/postfix/. Ce fichier est largement documenté, comme vous avez pu le constater.

Le gros problème que l'on rencontre, c'est la qualité de la documentation qui, visiblement, s'adresse uniquement à des spécialistes de la messagerie qui connaissent déjà bien "Sendmail", ce qui, du reste, est souvent le cas des documentations de

MTA. Celle d'exim est peut-être encore pire à ce niveau.

Si vous souhaitez remplacer "Root" par votre vrai nom dans l'identifiant de l'émetteur, il suffit de mettre à jour le fichier /etc/passwd. Chaque utilisateur peut y être référencé non seulement par son nom d'utilisateur, mais également par son vrai nom, c'est la partie soulignée dans l'exemple suivant:

```
root:x:0:0:L'Administrateur:/root:/bin/bash
```

Cette partie peut être vide ou contenir le nom d'utilisateur, ou encore le nom complet que vous voulez voir apparaître.

---

## Le luxe:

## Construire une messagerie privée.

Pourquoi ne pas profiter de Postfix pour réaliser une messagerie interne ? Cette messagerie permettrait à chaque utilisateur du réseau privé de disposer d'une boîte aux lettres personnelle en local. Au point où nous en sommes, c'est tellement simple à réaliser que ce serait bête de s'en priver. D'ailleurs, elle fonctionne déjà. A quoi ça sert ? Dans un réseau domestique, à pas grand chose, il faut bien le reconnaître. De plus, ces boîtes ne seront pas accessibles simplement depuis l'Internet, du fait de l'IP dynamique. En entreprise en revanche, ça peut présenter de nombreux intérêts, mais ça nous mènerait trop loin de les détailler ici:

- Avec l'aide de fetchmail, il est possible de gérer une BAL située chez votre FAI et disposant de plusieurs aliases (Plusieurs adresses de destinataires aboutissent à la même boîte aux lettres)
- Si votre FAI le permet, vous pouvez même gérer une file d'attente (une BAL dont l'adresse serait quelque chose comme \*@mondomaine.fr (compte "catch all"), boîte spéciale dans laquelle le MTA de votre FAI rangerait tout message dont la partie droite contient "mondomaine.fr") C'est vous qui gèrerez son contenu, en triant les adresses que vous jugerez valides, les classant dans vos BAL locales, et en rejetant celles qui ne le sont pas.

## Remarques préliminaires.

- Nous l'avons vu, par souci de sécurité, Postfix ne peut pas délivrer de messages à "root". Il ne faudra pas en être étonné. En revanche, il est possible de rediriger les messages pour "root" sur un autre utilisateur ("chris" par exemple). Ca a été fait dans le fichier des alias,
- Postfix n'a pas de fonctions POP ni IMAP, mais il sait ranger les messages locaux dans les files d'attentes de chaque utilisateur de la machine. Ce qui veut dire qu'il est possible de lire sa boîte aux lettres depuis l'hôte linux, mais pas depuis les autres postes du réseau. Nous arrangerons ça facilement.

## Mode opératoire.

Pour résoudre ces petits problèmes, nous devons donc:

- Rediriger les messages pour "root" dans la boîte de "chris".
- Installer un serveur POP (ou IMAP) pour pouvoir relever son courrier local depuis un autre poste.

## Rediriger les messages: La table des alias.

Il existe dans le répertoire /etc/postfix un fichier intitulé "aliases". Il a l'allure suivante:

```
# Basic system aliases -- these MUST be present.
MAILER-DAEMON: postmaster
postmaster: root

# General redirections for pseudo accounts.
bin: root
daemon: root
games: root
ingres: root
nobody: root
system: root
toor: root
uucp: root

# Well-known aliases.
manager: root
dumper: root
operator: root

# trap decode to catch security attacks
decode: root

# Person who should get root's mail
root: chris
```

Il s'agit d'une liste de noms d'utilisateurs qui n'ont pas de boîte aux lettres, mais qui peuvent recevoir des messages. Ces messages sont alors redirigés vers un autre utilisateur.

Dans le fichier d'origine, les noms de gauche sont des noms fictifs ou des noms de services. Ce sont des utilisateurs créés pour les besoins de service, ils ne correspondent pas à des utilisateurs "humains". Ils sont tous redirigés vers "root" .

Nous savons cependant que Postfix ne peut pas poster de messages à "root". Il faut donc rediriger "root" vers un autre utilisateur réel, ici "chris", sur la dernière ligne.

- Une fois ce fichier mis à jour, il faut exécuter la commande "postalias /etc/postfix/aliases" pour créer un fichier de base de données, comme on l'a déjà vu pour le "sender\_canonical".
- Dans le fichier /etc/postfix/main.cf, il faudra s'assurer qu'au paragraphe "ALIAS DATABASE" il existe une ligne: alias\_maps = hash:/etc/postfix/aliases (sans le # devant)
- Exécuter la commande "postfix reload"

## Le serveur POP3 (ou IMAP4).

Pour permettre la consultation de sa boîte aux lettres à distance, il suffit d'installer le daemon "IMAP" fourni dans les distributions Mandrake. Ce daemon va écouter sur le port 110 et répondra aux requêtes des MUA. Il faut vérifier que dans le fichier "/etc/inetd.conf" les lignes:

- pop-3 stream tcp nowait root /usr/sbin/tcpd ipop3d
- imap stream tcp nowait root /usr/bin/tcpd imapd

sont activées (pas de # devant). Si ce n'est pas le cas, il faut enlever ce #, enregistrer et relancer le daemon inetd (commande "killall -HUP inetd")

Si vous utilisez xinetd, ce qui est le cas des distributions Mandrake récentes, c'est un petit peu différent.

Le répertoire /etc/xinetd.d/ contient normalement deux fichiers :

- imap  
Assurez-vous que le paramètre "disable" = "no" si vous voulez utiliser imap,
- ipop3  
Normalement, pop3 est actif par défaut, à l'installation du paquetage.

## Vérification avec un client du réseau privé.

Nous allons sur un poste du réseau, dans notre MUA (ici Outlook Express) nous allons créer un nouveau compte de messagerie POP3 (Nous pourrions en profiter pour utiliser IMAP, mais ce n'est pas l'objet de ce chapitre. Les curieux peuvent essayer...).

**Propriétés de gateway2**

Général | Serveurs | Connexion | Sécurité | Avancé

Compte de courrier

Tapez le nom que vous voulez donner à ces serveurs.  
Par exemple : « Work » ou « Serveur de courrier Microsoft ».

gateway2

Informations utilisateur

Nom : Christian CALECA

Organisation :

Adresse d'email : chris@gateway2.maison.mrs

Adresse de réponse :

☒ Inclure ce compte lors de la réception ou de la synchronisation

OK Annuler Appliquer

Création du compte dans Outlook Express.

Notez l'adresse d'e-mail.

Le serveur POP est donc choisi comme étant la passerelle Linux (Si vous n'avez pas [de DNS pour votre réseau local](#), indiquez l'adresse IP de l'hôte dans le réseau privé, 192.168.0.253 chez moi).

Le nom d'utilisateur est connu sur l'hôte linux, le mot de passe est celui de "chris" sur la passerelle.

Autrement dit, le "login" correspond à celui de l'utilisateur "chris" sur l'hôte linux.

**Propriétés de gateway2** ? X

Général | Serveurs | Connexion | Sécurité | Avancé

Informations sur le serveur

Mon serveur de courrier entrant est un serveur **POP3**

Courrier entrant (POP3) : gateway2.maison.mrs

Courrier sortant (SMTP) : gateway2.maison.mrs

Serveur de courrier entrant

Nom du compte : chris

Mot de passe : xxxxxxx

☒ Se souvenir du mot de passe

☐ Se connecter avec l'authentification par mot de passe sécurisé

Serveur de courrier sortant

☐ Mon serveur requiert une authentification Paramètres...

OK Annuler Appliquer

**Test serveur POP** \_ □ X

Fichier Edition Affichage Insertion Format Outils Message >>

Envoyer Couper Copier Coller Annuler >>

De : chris@gateway2.maison.mrs (gateway2)

À : root@gateway2.maison.mrs

Cc :

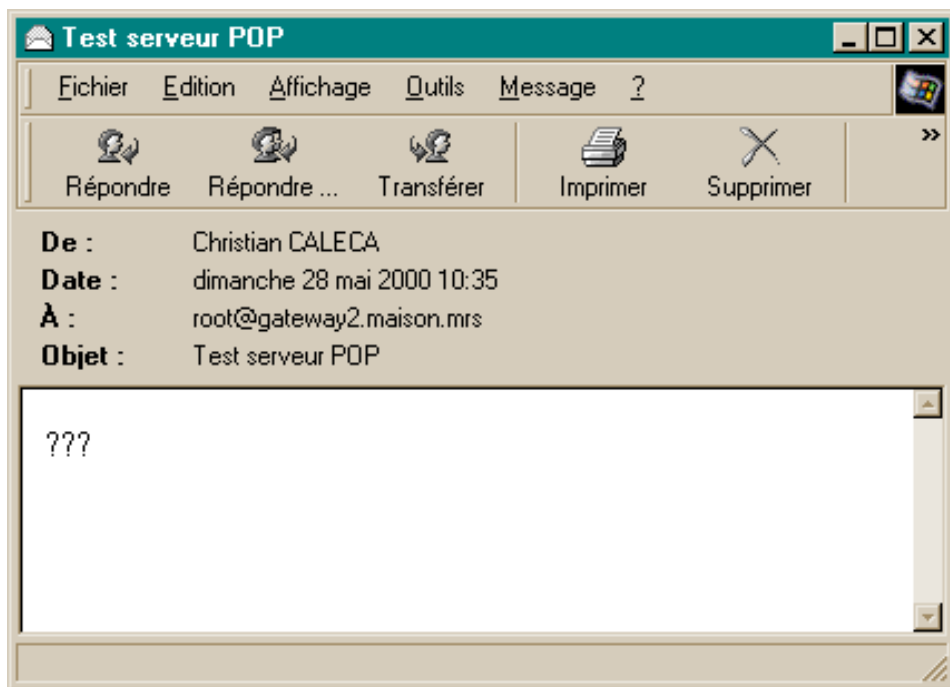
Cci :

Objet : Test serveur POP

???

On envoie un message à "root" en utilisant ce compte...

Notez les adresses de l'émetteur et du destinataire.



On va lire la boîte aux lettres de ce compte... Ça marche.

Rappelez-vous ce qui a été fait, nous avons créé un compte pour l'utilisateur "chris" sur gw2.maison.mrs, nous avons envoyé un message à "root", nous le récupérons, à distance, dans la boîte de "chris".

Le fonctionnement est donc bien celui souhaité.

Le contrat est rempli:

- Le serveur SMTP fonctionne sur la passerelle, aussi bien pour envoyer des messages à l'extérieur qu'à l'intérieur.
- L'adresse de l'émetteur est ré écrite avec un "vraie" adresse (fichier "sender-canonical").
- Les messages à destination de "root" sont déposés dans la boîte de "chris" (Fichier "aliases").
- Les boîtes aux lettres sont accessibles à distance par le protocole POP3 (installation du daemon "IMAP").

## Le luxe du luxe.

Ce serait bien si l'on pouvait, comme chez les vrais, envoyer un message interne à un utilisateur avec une adresse de la forme "chris@maison.mrs" à la place "chris@gateway2.maison.mrs"...

Mais Postfix est un VRAI MTA, c'est donc possible.

Un petit tour dans /etc/postfix/main.cf...

- Au paragraphe "INTERNET HOST AND DOMAIN NAMES":
  - Activer la ligne myhostname = <le nom de votre machine linux>
  - Activer la ligne mydomain=<le nom de votre domaine privé>
- Au paragraphe "RECEIVING MAIL":
  - Activer la ligne mydestination=\$myhostname, \$mydomain De cette manière Postfix comprendra aussi bien les adresses de la forme @gateway2.maison.mrs que @maison.mrs
- Relancer Postfix avec "postfix reload".

Ca doit fonctionner correctement.

Note :

Vous avez peut-être constaté que gw1 est devenu gateway2 au cours du temps ? Rien d'affolant à cela, cette machine est là pour faire des tests. C'est toujours une bonne idée de pouvoir faire des tests ailleurs que sur la machine dite "stabilisée".



# Config avancée

[ [Accueil](#) ] [ [Les bases](#) ] [ [les Profondeurs](#) ] [ [Un SMTP "perso"](#) ] [ [Installation de Postfix](#) ] [ [Config avancée](#) ]  
[ [Conclusions](#) ]

---

Vous l'aurez compris, cette possibilité de monter soi-même un SMTP, si elle rend des services évidents, présente malheureusement aussi quelques inconvénients.

Quoi de plus simple, en effet, que d'utiliser cette méthode pour envoyer du spam, sans passer par les éventuels contrôles de votre FAI ?

Bien entendu, l'humanité n'étant pas encore parfaite, ça n'a pas manqué de se produire, amenant les administrateurs de SMTP à prendre plus de précautions et à verrouiller de plus en plus leurs systèmes.

## Quelques restrictions imposées.

les administrateurs imposent donc de plus en plus de restrictions sur l'origine des messages qu'ils reçoivent. En voici quelques unes.

### Le domaine de l'expéditeur.

Celle là, nous l'avons déjà vue et nous avons vu comment la passer. Il suffit de s'arranger pour que l'adresse présente dans le champ de l'émetteur fasse référence à un domaine connu. Cette protection n'est hélas pas suffisante, puisque n'importe quelle fausse adresse, forgée sur un nom de domaine officiel, passera le contrôle. Ainsi, si vous envoyez des messages avec comme adresse d'émetteur : [iamaspamer@aol.com](mailto:iamaspamer@aol.com) , il y a des chances que ça passe.

### EHLO.

ESMTP propose la commande EHLO (ou HELO). Celui qui envoie le message en hélant un SMTP envoie cette commande avec comme argument son nom d'hôte.

Cette commande est une sorte de carte de visite. Dans un passé proche, cette présentation n'était pas forcément obligatoire. Elle le devient de plus en plus, et Il est possible de paramétrer un serveur SMTP :

- de manière à ce qu'il se contente de connaître le nom de l'émetteur, ce qui ne présente bien entendu pas un grand intérêt,
- de manière à faire une vérification DNS pour voir si ce nom est connu sur Internet, c'est déjà plus efficace, mais n'importe quel nom valable devrait faire l'affaire, il ne semble pas y avoir de vérification sur l'IP, du moins dans le cas de Postfix,
- de manière à vérifier que ce nom d'hôte correspond à un MX (Mail Exchanger) connu comme tel sur les DNS.

Comme il n'est bien entendu pas question ici de savoir si la chose est falsifiable ou non, nous dirons que cette barrière sera incontournable, sauf si nous disposons d'un nom de domaine et que nous avons fait référencer notre machine comme étant MX sur les DNS qui gèrent notre domaine. Mais ça voudra aussi dire que l'on devrait pouvoir recevoir des messages @notredomaine.tld. Il est possible de jouer sur les priorités, mais là n'est pas notre propos.

## Blacklists.

Comme tout ça ne suffit visiblement pas, les SMTP peuvent se référer à des listes noires. Ces listes contiennent des IPs qui ont été repérées comme étant émettrices de spams, ou plus largement, qui font partie de blocs d'IPs dans lesquels des spammeurs ont été détectés.

Vous voyez le problème, si vous avez droit à une IP dynamique, votre SMTP pourra tomber sur une IP blacklistée, parce qu'un spammeur aura utilisé cette IP avant vous.

Ca vous fera peut-être rire de savoir qu'à l'heure où je rédige ce paragraphe, les adresses IP utilisées par les clients Wanadoo Câble de Marseille (et peut-être aussi d'autres villes) sont toutes blacklistées ?

Et, bien entendu, ces protections sont cumulables.

Ainsi, toujours à l'heure où je rédige ces lignes, les destinataires @.univ-paris8.fr sont injoignables directement depuis un SMTP personnel.

## Contourner les interdits de certains FAI.

Du plus radical au plus compliqué, vous pourrez :

### Tout faire passer par le MTA de votre FAI.

La solution la plus simple consiste alors à tout envoyer sur le MTA de votre FAI. Lui, il est obligé de les accepter, c'est dans le contrat. C'est lui qui se chargera alors de transmettre aux destinataires.

Si vous désirez faire ceci, il suffit d'ouvrir main.cf, de rechercher le paramètre

**relayhost**

et de lui attribuer le nom du smtp de votre FAI. Par exemple :

**relayhost = smtp.wanadoo.fr**

Cette méthode est simple et définitive, mais introduit au moins une étape de plus et une source de panne supplémentaire. Son unique avantage est que les clients du réseau local dialoguent avec un MTA proche et rapide. En cas de lenteur du smtp de votre FAI, les clients ne seront pas perturbés, c'est votre MTA qui gèrera au mieux les faiblesses du MTA du FAI.

Le problème, c'est que tous vos messages sortants sont pénalisés par cette solution.

### Faire un tri sélectif, donc écologique.

Il est possible de travailler plus "finement" en délivrant directement les messages aux destinataires qui les acceptent et en passant par le smtp du FAI pour les autres.

Nous allons le faire, par exemple pour les domaines aol.com et aol.fr

- Créer un fichier texte /etc/postfix/transport\_maps
- écrire dedans les lignes suivantes :

```
aol.com smtp:smtp.wanadoo.fr
.aol.com smtp:smtp.wanadoo.fr
aol.fr smtp:smtp.wanadoo.fr
.aol.fr smtp:smtp.wanadoo.fr
```

Ceci veut dire en français que pour les messages à destination de domaines aol.com, aol.fr et leurs

sous domaines, nous utiliserons le protocole smtp pour transmettre ces messages à smtp.wanadoo.fr (bien entendu, c'est pour les abonnés Wanadoo. les autres doivent interpréter).

- Créer la base de données correspondante avec la commande :  
`postmap /etc/postfix/transport_maps`
- Modifier le fichier main.cf en y ajoutant la ligne suivante :  
`transport_maps = hash:/etc/postfix/transport_maps`
- Relancer postfix avec postfix reload

De cette manière, seuls les domaines qui posent problèmes seront acheminés via le MTA de votre FAI, tous les autres étant joints directement. C'est plus efficace, mais vous aurez probablement à modifier votre configuration suivant l'humeur des divers FAI.

## **Donner à votre machine un nom chrétien.**

Ce qui est bien sûr une façon de parler...

Vous serez probablement intéressé de savoir qu'à l'IP que votre FAI vous prête, est attaché un nom, souvent fort poétique d'ailleurs. Par exemple, actuellement je dispose de l'IP 80.8.163.152.

Si je fais une recherche DNS inverse, je trouve :

```
gw1:~# host 80.8.163.152
152.163.8.80.in-addr.arpa domain name pointer
ca-marseille-36-152.w80-8.abo.wanadoo.fr.
```

Joli non ?

Bien entendu, ce nom changera chaque fois que vous changerez d'IP...

Une possibilité serait alors de réaliser un script qui permettrait de changer le nom d'hôte de votre machine, chaque fois que l'IP change. C'est réalisable assez simplement, par exemple comme ceci :

Avec Mandrake, si vous utilisez PPPoE, allez dans le répertoire :

```
/etc/ppp/
```

et créez-y un script intitulé :

```
ip-up.local
```

de la forme suivante :

```
#!/bin/bash
# Ce script met à jour le nom d'hôte local à chaque changement d'IP
# et envoie un e-mail à une adresse extérieure, contenant :
# -- La nouvelle IP de la machine
# -- Son nouveau nom DNS
```

```
adresse="christian.caleca@free.fr"
sujet="gw1 : Nouvelle session PPPoE"
```

```
# la ligne suivante effectue la recherche inverse sur l'IP
# contenue dans le paramètre $4, et extrait le nom dans $monhote
monhote="`host $4 | awk '{print substr($NF,1,length($NF)-1)}'`"
# puis utilise la commande "hostname" pour mettre à jour le nom de la machine
```

```
/bin/hostname $monhote
/usr/sbin/postfix reload

# Le reste sert à envoyer l' e-mail
texte="$4 -- $monhote"
echo $texte | mail -s "$sujet" $adresse
```

### **Attention, en faisant ça, vous perturbez votre environnement, dont celui de Postfix !**

En effet, Postfix, comme beaucoup d'autres applications utilisent une fonction appelée "gethostname" pour connaître le nom d'hôte.

Dans le cas de Postfix, les valeurs de "myhostname" et aussi de "mydomain" seront affectées. C'est d'ailleurs bien le but de la manoeuvre, mais pensez alors à configurer "mydestination" autrement, si vous utilisez un service de messagerie locale.

Soyez donc prudent si vous voulez essayer cette méthode, et vérifiez bien qu'elle n'introduit pas de perturbations sur d'autres éventuels services.

Au final, vous pourriez avoir un fichier /etc/postfix/main.cf de la forme (débarassé de tous les commentaires, pour faire court):

```
command_directory = /usr/sbin
daemon_directory = /usr/lib/postfix
alias_maps = hash:/etc/postfix/aliases

mail_spool_directory = /var/spool/mail
mailbox_command = /usr/bin/procmail -Y -a $DOMAIN

smtpd_banner = ESMTP $mail_name
debug_peer_level = 2
debugger_command =
PATH=/usr/bin:/usr/X11R6/bin
xxgdb $daemon_directory/$process_name $process_id & sleep 5
delay_warning_time = 4
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
setgid_group = postdrop
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-1.1.11/samples
readme_directory = /usr/share/doc/postfix-1.1.11/README_FILES
alias_database = hash:/etc/postfix/aliases
transport_maps = hash:/etc/postfix/transport_maps
mydestination = gw1.maison.mrs, localhost.maison.mrs, maison.mrs
myorigin = gw1.maison.mrs
sender_canonical_maps = hash:/etc/postfix/sender-canonical
header_checks = regexp:/etc/postfix/header_checks
```

# Conclusions

[ [Accueil](#) ] [ [Les bases](#) ] [ [les Profondeurs](#) ] [ [Un SMTP "perso"](#) ] [ [Installation de Postfix](#) ]  
[ [Config avancée](#) ] [ [Conclusions](#) ]

---

Le domaine de la messagerie est fort complexe et je suis loin d'être suffisamment compétant en la matière pour avoir la prétention de tout dire sur le sujet.

Nous allons conclure cette partie par quelques remarques pêle-mêle.

- J'aurais aimé effectuer une ré écriture de l'adresse de l'émetteur pour les courriers extérieurs, mais pas pour les courriers intérieurs. Je n'ai pas trouvé de méthode (ce qui ne veut pas dire que ce soit impossible).
- J'aurais aimé que dans l'en-tête des messages envoyés à l'extérieur, l'étape de transport par mon MTA soit gommée:

```
Received: from chris (chris.maison.mrs [192.168.0.10])  
        by gw1.maison.mrs (Postfix) with SMTP id A38181105F
```

Grâce à l'aide d'un aimable lecteur, voici la solution, qui utilise les "expressions régulières". Je ne crois pas avoir vu ailleurs dans le monde une syntaxe plus obscure que celle des expressions régulières, mais leur obscurité n'a d'égal que leur puissance. Disons simplement pour ceux qui l'ignorent que les expressions régulières sont une sorte de filtre qui permet de dire si oui ou non une combinaison de caractères se trouve dans un texte donné. Ici, nous allons chercher toutes les lignes commençant par "Received:" et nous allons demander à Postfix de les supprimer.

Si vous voulez gommer de l'en-tête de vos messages sortants l'étape de votre MTA, il "suffit" donc de faire les choses suivantes :

- Créez un fichier texte nommé par exemple "header\_checks" dans le répertoire /etc/postfix/
- mettez-y dedans l'expression :  

```
/^Received:*/ IGNORE
```
- faites :  

```
postmap /etc/postfix/header_checks
```

  
pour construire la base de données
- ouvrez main.cf et dé commentez la ligne :  

```
header_checks = regexp:/etc/postfix/headers_checks
```
- relancez postfix par  

```
postfix reload
```

Et voilà. Les messages que vous enverrez depuis n'importe quel poste de votre réseau local sembleront tous provenir directement de votre passerelle.

Notez que cette "facilité" permet également d'autres choses :

- rejeter un message en fonction du contenu d'un en-tête, en donnant la directive REJECT

```
/^from: * chose@public\.com$/ REJECT
```

Rejettera tous les messages dont le champ from se terminera par chose@public.com

- inscrire dans les logs en fonction du contenu d'un en-tête, en donnant la directive WARN. Ceci recopie l'en-tête dans les logs, sans pour autant rejeter le message.

## Ce que l'on pourrait encore faire...

Bien des choses seraient encore possibles:

- Récupérer directement, à intervalles réguliers, son courrier sur ses divers comptes extérieurs et les classer dans des boîtes aux lettres créées sur la passerelle Linux, éventuellement en y appliquant des règles de filtrage fines. Ces options sont réalisables avec les fonctions "fetchmail" et "procmail". Si le cœur vous en dit...
- Rediriger automatiquement certains courriers vers d'autres destinations. (recipient\_canonical\_maps)
- Et bien d'autres choses encore.

Mais, encore une fois, le domaine de la messagerie est très vaste, c'est une spécialité à part entière. L'objectif initial est toutefois atteint: Nous voyons à peu près clairement comment les messages sont acheminés et savons maintenant envoyer nos messages sans les recours du SMTP de notre FAI, du moins si les destinataires ne sont pas trop stricts sur les origines des messages.

## Suite du dialogue.

Frame 12 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:12.5438

Time delta from previous packet: 0.074119 seconds

Frame Number: 12

Packet Length: 60 bytes

Capture Length: 60 bytes

Ethernet II

Destination: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Type: IP (0x0800)

Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 44

Identification: 0xf9a7

Flags: 0x00

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 57

Protocol: TCP (0x06)

Header checksum: 0x8bda (correct)

Source: dns1.monaco.net (194.79.150.9)

Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq: 2324998720, Ack: 2161513039

Source port: smtp (25)

Destination port: 1027 (1027)

Sequence number: 2324998720

Acknowledgement number: 2161513039

Header length: 24 bytes

Flags: 0x0012 (SYN, ACK)

..0. .... = Urgent: Not set

...1 .... = Acknowledgment: Set

.... 0... = Push: Not set

.... .0.. = Reset: Not set

.... ..1. = Syn: Set

.... ...0 = Fin: Not set

Window size: 32736

Checksum: 0x4fd5

Options: (4 bytes)

Maximum segment size: 1460 bytes

Frame 13 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:12.5440

Time delta from previous packet: 0.000276 seconds

Frame Number: 13

Packet Length: 60 bytes

Capture Length: 60 bytes

## Ethernet II

Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Source: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Type: IP (0x0800)

## Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 40

Identification: 0x1595

Flags: 0x04

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: TCP (0x06)

Header checksum: 0x28f1 (correct)

Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Destination: dns1.monaco.net (194.79.150.9)

Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq: 2161513039, Ack: 2324998721

Source port: 1027 (1027)

Destination port: smtp (25)

Sequence number: 2161513039

Acknowledgement number: 2324998721

Header length: 20 bytes

Flags: 0x0010 (ACK)

..0. .... = Urgent: Not set

...1 .... = Acknowledgment: Set

.... 0... = Push: Not set

.... .0.. = Reset: Not set

.... ..0. = Syn: Not set

.... ...0 = Fin: Not set

Window size: 32120

Checksum: 0x69fa

Frame 14 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:12.7006

Time delta from previous packet: 0.156549 seconds

Frame Number: 14

Packet Length: 60 bytes

Capture Length: 60 bytes

## Ethernet II

Destination: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Type: IP (0x0800)

## Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0



Total Length: 44  
Identification: 0xf9ae  
Flags: 0x00  
    .0.. = Don't fragment: Not set  
    ..0. = More fragments: Not set  
Fragment offset: 0  
Time to live: 57  
Protocol: TCP (0x06)  
Header checksum: 0x8bd3 (correct)  
Source: dns1.monaco.net (194.79.150.9)  
Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Transmission Control Protocol, Src Port: 20499 (20499), Dst Port: auth (113), Seq: 3617863760, Ack: 0

Source port: 20499 (20499)  
Destination port: auth (113)  
Sequence number: 3617863760  
Header length: 24 bytes  
Flags: 0x0002 (SYN)  
    ..0. .... = Urgent: Not set  
    ...0 .... = Acknowledgment: Not set  
    .... 0... = Push: Not set  
    .... .0.. = Reset: Not set  
    .... ..1. = Syn: Set  
    .... ...0 = Fin: Not set

Window size: 512  
Checksum: 0x3963  
Options: (4 bytes)  
    Maximum segment size: 1460 bytes

Frame 15 (60 on wire, 60 captured)  
Arrival Time: May 22, 2000 20:28:12.7008  
Time delta from previous packet: 0.000239 seconds  
Frame Number: 15  
Packet Length: 60 bytes  
Capture Length: 60 bytes

Ethernet II  
Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)  
Source: 00:20:af:07:1a:3d (3Com\_07:1a:3d)  
Type: IP (0x0800)

Internet Protocol  
Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default)  
    0000 00.. = Differentiated Services Codepoint: Default (0x00)  
    .... ..00 = Currently Unused: 0  
Total Length: 44  
Identification: 0x1596  
Flags: 0x04  
    .1.. = Don't fragment: Set  
    ..0. = More fragments: Not set  
Fragment offset: 0  
Time to live: 64  
Protocol: TCP (0x06)  
Header checksum: 0x28ec (correct)

Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)  
Destination: dns1.monaco.net (194.79.150.9)  
Transmission Control Protocol, Src Port: auth (113), Dst Port: 20499 (20499), Seq: 2168136768, Ack: 3617863761  
Source port: auth (113)  
Destination port: 20499 (20499)  
Sequence number: 2168136768  
Acknowledgement number: 3617863761  
Header length: 24 bytes  
Flags: 0x0012 (SYN, ACK)  
    ..0. .... = Urgent: Not set  
    ...1 .... = Acknowledgment: Set  
    .... 0... = Push: Not set  
    .... .0.. = Reset: Not set  
    .... ..1. = Syn: Set  
    .... ...0 = Fin: Not set  
Window size: 32120  
Checksum: 0x185e  
Options: (4 bytes)  
    Maximum segment size: 1460 bytes

Frame 16 (60 on wire, 60 captured)  
Arrival Time: May 22, 2000 20:28:12.7925  
Time delta from previous packet: 0.091623 seconds  
Frame Number: 16  
Packet Length: 60 bytes  
Capture Length: 60 bytes

Ethernet II  
Destination: 00:20:af:07:1a:3d (3Com\_07:1a:3d)  
Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)  
Type: IP (0x0800)

Internet Protocol  
Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default)  
    0000 00.. = Differentiated Services Codepoint: Default (0x00)  
    .... ..00 = Currently Unused: 0  
Total Length: 40  
Identification: 0xf9b1  
Flags: 0x04  
    .1.. = Don't fragment: Set  
    ..0. = More fragments: Not set  
Fragment offset: 0  
Time to live: 57  
Protocol: TCP (0x06)  
Header checksum: 0x4bd4 (correct)  
Source: dns1.monaco.net (194.79.150.9)  
Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Transmission Control Protocol, Src Port: 20499 (20499), Dst Port: auth (113), Seq: 3617863761, Ack: 2168136769  
Source port: 20499 (20499)  
Destination port: auth (113)  
Sequence number: 3617863761  
Acknowledgement number: 2168136769

Header length: 20 bytes  
Flags: 0x0010 (ACK)  
    ..0. .... = Urgent: Not set  
    ...1 .... = Acknowledgment: Set  
    .... 0... = Push: Not set  
    .... .0.. = Reset: Not set  
    .... ..0. = Syn: Not set  
    .... ...0 = Fin: Not set  
Window size: 32120  
Checksum: 0x301b

Frame 17 (63 on wire, 63 captured)  
Arrival Time: May 22, 2000 20:28:12.7939  
Time delta from previous packet: 0.001461 seconds  
Frame Number: 17  
Packet Length: 63 bytes  
Capture Length: 63 bytes

#### Ethernet II

Destination: 00:20:af:07:1a:3d (3Com\_07:1a:3d)  
Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)  
Type: IP (0x0800)

#### Internet Protocol

Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default)  
    0000 00.. = Differentiated Services Codepoint: Default (0x00)  
    .... ..00 = Currently Unused: 0  
Total Length: 49  
Identification: 0xf9b2  
Flags: 0x04  
    .1.. = Don't fragment: Set  
    ..0. = More fragments: Not set  
Fragment offset: 0  
Time to live: 57  
Protocol: TCP (0x06)  
Header checksum: 0x4bca (correct)  
Source: dns1.monaco.net (194.79.150.9)  
Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Transmission Control Protocol, Src Port: 20499 (20499), Dst Port: auth (113), Seq: 3617863761, Ack: 2168136769

Source port: 20499 (20499)  
Destination port: auth (113)  
Sequence number: 3617863761  
Acknowledgement number: 2168136769  
Header length: 20 bytes  
Flags: 0x0018 (PSH, ACK)  
    ..0. .... = Urgent: Not set  
    ...1 .... = Acknowledgment: Set  
    .... 1... = Push: Set  
    .... .0.. = Reset: Not set  
    .... ..0. = Syn: Not set  
    .... ...0 = Fin: Not set  
Window size: 32120  
Checksum: 0x6163

Data (9 bytes)

```
 0  0020 af07 1a3d 00d0 7972 5c00 0800 4500  . . . .=..yr\...E.
10 0031 f9b2 4000 3906 4bca c24f 9609 3ea1  .1...@.9.K..O...>.
20 6550 5013 0071 d7a4 3851 813b 2441 5018  ePP..q..8Q.;$AP.
30 7d78 6163 0000 3130 3237 2c32 350d 0a    }xac..1027,25..
```

Frame 18 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:12.7942  
Time delta from previous packet: 0.000253 seconds  
Frame Number: 18  
Packet Length: 60 bytes  
Capture Length: 60 bytes

Ethernet II

Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)  
Source: 00:20:af:07:1a:3d (3Com\_07:1a:3d)  
Type: IP (0x0800)

Internet Protocol

Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default)  
    0000 00.. = Differentiated Services Codepoint: Default (0x00)  
    .... ..00 = Currently Unused: 0  
Total Length: 40  
Identification: 0x1597  
Flags: 0x04  
    .1.. = Don't fragment: Set  
    ..0. = More fragments: Not set

Fragment offset: 0  
Time to live: 64  
Protocol: TCP (0x06)  
Header checksum: 0x28ef (correct)  
Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)  
Destination: dns1.monaco.net (194.79.150.9)

Transmission Control Protocol, Src Port: auth (113), Dst Port: 20499 (20499), Seq: 2168136769, Ack: 3617863770

Source port: auth (113)  
Destination port: 20499 (20499)  
Sequence number: 2168136769  
Acknowledgement number: 3617863770  
Header length: 20 bytes  
Flags: 0x0010 (ACK)  
    ..0. .... = Urgent: Not set  
    ...1 .... = Acknowledgment: Set  
    .... 0... = Push: Not set  
    .... .0.. = Reset: Not set  
    .... ..0. = Syn: Not set  
    .... ...0 = Fin: Not set  
Window size: 32120  
Checksum: 0x3012

Frame 19 (91 on wire, 91 captured)

Arrival Time: May 22, 2000 20:28:12.8189  
Time delta from previous packet: 0.024715 seconds  
Frame Number: 19  
Packet Length: 91 bytes

```

Capture Length: 91 bytes
Ethernet II
  Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)
  Source: 00:20:af:07:1a:3d (3Com_07:1a:3d)
  Type: IP (0x0800)
Internet Protocol
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
  Total Length: 77
  Identification: 0x1598
  Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
  Header checksum: 0x28c9 (correct)
  Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)
  Destination: dns1.monaco.net (194.79.150.9)
Transmission Control Protocol, Src Port: auth (113), Dst Port: 20499 (20499), Seq:
2168136769, Ack: 3617863770
  Source port: auth (113)
  Destination port: 20499 (20499)
  Sequence number: 2168136769
  Acknowledgement number: 3617863770
  Header length: 20 bytes
  Flags: 0x0018 (PSH, ACK)
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 1... = Push: Set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...0 = Fin: Not set
  Window size: 32120
  Checksum: 0x723c
Data (37 bytes)
  0  00d0 7972 5c00 0020 af07 1a3d 0800 4500  ..yr\... ..=..E.
 10  004d 1598 4000 4006 28c9 3ea1 6550 c24f  .M..@.@.(.>.eP.O
 20  9609 0071 5013 813b 2441 d7a4 385a 5018  ...qP...;A..8ZP.
 30  7d78 723c 0000 3130 3237 202c 2032 3520  }xr<..1027 , 25
 40  3a20 5553 4552 4944 203a 204f 5448 4552  : USERID : OTHER
 50  203a 706f 7374 6669 780d 0a          :postfix..
Frame 20 (60 on wire, 60 captured)
  Arrival Time: May 22, 2000 20:28:12.8193
  Time delta from previous packet: 0.000434 seconds
  Frame Number: 20
  Packet Length: 60 bytes
  Capture Length: 60 bytes
Ethernet II
  Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

```

Source: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Type: IP (0x0800)

#### Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 40

Identification: 0x1599

Flags: 0x04

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: TCP (0x06)

Header checksum: 0x28ed (correct)

Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Destination: dns1.monaco.net (194.79.150.9)

Transmission Control Protocol, Src Port: auth (113), Dst Port: 20499 (20499), Seq: 2168136806, Ack: 3617863770

Source port: auth (113)

Destination port: 20499 (20499)

Sequence number: 2168136806

Acknowledgement number: 3617863770

Header length: 20 bytes

Flags: 0x0011 (FIN, ACK)

..0. .... = Urgent: Not set

...1 .... = Acknowledgment: Set

.... 0... = Push: Not set

.... .0.. = Reset: Not set

.... ..0. = Syn: Not set

.... ...1 = Fin: Set

Window size: 32120

Checksum: 0x2fec

Frame 21 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:12.9009

Time delta from previous packet: 0.081595 seconds

Frame Number: 21

Packet Length: 60 bytes

Capture Length: 60 bytes

#### Ethernet II

Destination: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Type: IP (0x0800)

#### Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 40

Identification: 0xf9b6

Flags: 0x04

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 57

Protocol: TCP (0x06)

Header checksum: 0x4bcf (correct)

Source: dns1.monaco.net (194.79.150.9)

Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Transmission Control Protocol, Src Port: 20499 (20499), Dst Port: auth (113), Seq: 3617863770, Ack: 2168136807

Source port: 20499 (20499)

Destination port: auth (113)

Sequence number: 3617863770

Acknowledgement number: 2168136807

Header length: 20 bytes

Flags: 0x0010 (ACK)

..0. .... = Urgent: Not set

...1 .... = Acknowledgment: Set

.... 0... = Push: Not set

.... .0.. = Reset: Not set

.... ..0. = Syn: Not set

.... ...0 = Fin: Not set

Window size: 32120

Checksum: 0x2fec

Frame 22 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:12.9024

Time delta from previous packet: 0.001507 seconds

Frame Number: 22

Packet Length: 60 bytes

Capture Length: 60 bytes

Ethernet II

Destination: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Type: IP (0x0800)

Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 40

Identification: 0xf9b7

Flags: 0x00

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 57

Protocol: TCP (0x06)

Header checksum: 0x8bce (correct)

Source: dns1.monaco.net (194.79.150.9)

Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Transmission Control Protocol, Src Port: 20499 (20499), Dst Port: auth (113), Seq:

```
3617863770, Ack: 2168136807
  Source port: 20499 (20499)
  Destination port: auth (113)
  Sequence number: 3617863770
  Acknowledgement number: 2168136807
  Header length: 20 bytes
  Flags: 0x0011 (FIN, ACK)
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 0... = Push: Not set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...1 = Fin: Set
  Window size: 32120
  Checksum: 0x2feb

Frame 23 (60 on wire, 60 captured)
  Arrival Time: May 22, 2000 20:28:12.9026
  Time delta from previous packet: 0.000207 seconds
  Frame Number: 23
  Packet Length: 60 bytes
  Capture Length: 60 bytes

Ethernet II
  Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)
  Source: 00:20:af:07:1a:3d (3Com_07:1a:3d)
  Type: IP (0x0800)

Internet Protocol
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
  Total Length: 40
  Identification: 0x159b
  Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
  Header checksum: 0x28eb (correct)
  Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)
  Destination: dns1.monaco.net (194.79.150.9)

Transmission Control Protocol, Src Port: auth (113), Dst Port: 20499 (20499), Seq:
2168136807, Ack: 3617863771
  Source port: auth (113)
  Destination port: 20499 (20499)
  Sequence number: 2168136807
  Acknowledgement number: 3617863771
  Header length: 20 bytes
  Flags: 0x0010 (ACK)
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 0... = Push: Not set
```



.... .0.. = Reset: Not set  
.... ..0. = Syn: Not set  
.... ...0 = Fin: Not set

Window size: 32120

Checksum: 0x2feb

Frame 24 (143 on wire, 143 captured)

Arrival Time: May 22, 2000 20:28:12.9078

Time delta from previous packet: 0.005140 seconds

Frame Number: 24

Packet Length: 143 bytes

Capture Length: 143 bytes

Ethernet II

Destination: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Type: IP (0x0800)

Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 129

Identification: 0xf9b8

Flags: 0x04

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 57

Protocol: TCP (0x06)

Header checksum: 0x4b74 (correct)

Source: dns1.monaco.net (194.79.150.9)

Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq:  
2324998721, Ack: 2161513039

Source port: smtp (25)

Destination port: 1027 (1027)

Sequence number: 2324998721

Acknowledgement number: 2161513039

Header length: 20 bytes

Flags: 0x0018 (PSH, ACK)

..0. .... = Urgent: Not set

...1 .... = Acknowledgment: Set

.... 1... = Push: Set

.... .0.. = Reset: Not set

.... ..0. = Syn: Not set

.... ...0 = Fin: Not set

Window size: 32736

Checksum: 0x21a2

Data (89 bytes)

0	0020	af07	1a3d	00d0	7972	5c00	0800	4500	. ...=..yr\...E.
10	0081	f9b8	4000	3906	4b74	c24f	9609	3ea1	....@.9.Kt.O...>.
20	6550	0019	0403	8a94	aa41	80d6	124f	5018	eP.....A...OP.
30	7fe0	21a2	0000	3232	3020	6d61	696c	2e6d	..!...220 mail.m

```
40  6f6e 6163 6f2e 6e65 7420 4553 4d54 5020  onaco.net ESMTP
50  5365 6e64 6d61 696c 2050 726f 2d38 2e39  Sendmail Pro-8.9
60  2e33 2f50 726f 2d38 2e39 2e33 3b20 4d6f  .3/Pro-8.9.3; Mo
70  6e2c 2032 3220 4d61 7920 3230 3030 2032  n, 22 May 2000 2
80  303a 3238 3a31 3220 2b30 3230 300d 0a    0:28:12 +0200..
```

Frame 25 (60 on wire, 60 captured)

```
Arrival Time: May 22, 2000 20:28:12.9080
Time delta from previous packet: 0.000221 seconds
Frame Number: 25
Packet Length: 60 bytes
Capture Length: 60 bytes
```

Ethernet II

```
Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)
Source: 00:20:af:07:1a:3d (3Com_07:1a:3d)
Type: IP (0x0800)
```

Internet Protocol

```
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
Total Length: 40
Identification: 0x159c
Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0x28ea (correct)
Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)
Destination: dns1.monaco.net (194.79.150.9)
```

Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq: 2161513039, Ack: 2324998810

```
Source port: 1027 (1027)
Destination port: smtp (25)
Sequence number: 2161513039
Acknowledgement number: 2324998810
Header length: 20 bytes
Flags: 0x0010 (ACK)
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 0... = Push: Not set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...0 = Fin: Not set
Window size: 32120
Checksum: 0x69a1
```

Frame 26 (80 on wire, 80 captured)

```
Arrival Time: May 22, 2000 20:28:12.9089
Time delta from previous packet: 0.000924 seconds
Frame Number: 26
Packet Length: 80 bytes
```

```

Capture Length: 80 bytes
Ethernet II
  Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)
  Source: 00:20:af:07:1a:3d (3Com_07:1a:3d)
  Type: IP (0x0800)
Internet Protocol
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
  Total Length: 66
  Identification: 0x159d
  Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
  Header checksum: 0x28cf (correct)
  Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)
  Destination: dns1.monaco.net (194.79.150.9)
Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq:
2161513039, Ack: 2324998810
  Source port: 1027 (1027)
  Destination port: smtp (25)
  Sequence number: 2161513039
  Acknowledgement number: 2324998810
  Header length: 20 bytes
  Flags: 0x0018 (PSH, ACK)
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 1... = Push: Set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...0 = Fin: Not set
  Window size: 32120
  Checksum: 0x69bf
Data (26 bytes)
  0  00d0 7972 5c00 0020 af07 1a3d 0800 4500  ..yr\... ..=.E.
 10  0042 159d 4000 4006 28cf 3ea1 6550 c24f  .B..@.@.(.>.eP.O
 20  9609 0403 0019 80d6 124f 8a94 aa9a 5018  .....O....P.
 30  7d78 69bf 0000 4548 4c4f 2067 6174 6577  }xi...EHLO gatew
 40  6179 312e 6d61 6973 6f6e 2e6d 7273 0d0a  ayl.maison.mrs..

Frame 27 (260 on wire, 260 captured)
  Arrival Time: May 22, 2000 20:28:12.9956
  Time delta from previous packet: 0.086673 seconds
  Frame Number: 27
  Packet Length: 260 bytes
  Capture Length: 260 bytes
Ethernet II
  Destination: 00:20:af:07:1a:3d (3Com_07:1a:3d)
  Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

```

```

Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
Total Length: 246
Identification: 0xf9b9
Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
Fragment offset: 0
Time to live: 57
Protocol: TCP (0x06)
Header checksum: 0x4afe (correct)
Source: dns1.monaco.net (194.79.150.9)
Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)
Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq:
2324998810, Ack: 2161513065
Source port: smtp (25)
Destination port: 1027 (1027)
Sequence number: 2324998810
Acknowledgement number: 2161513065
Header length: 20 bytes
Flags: 0x0018 (PSH, ACK)
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 1... = Push: Set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...0 = Fin: Not set
Window size: 32736
Checksum: 0x3a89
Data (206 bytes)
  0  0020 af07 1a3d 00d0 7972 5c00 0800 4500  . . . .=..yr\...E.
 10 00f6 f9b9 4000 3906 4afe c24f 9609 3ea1  ....@.9.J..O...>.
 20 6550 0019 0403 8a94 aa9a 80d6 1269 5018  eP.....iP.
 30 7fe0 3a89 0000 3235 302d 6d61 696c 2e6d  ...250-mail.m
 40 6f6e 6163 6f2e 6e65 7420 4865 6c6c 6f20  onaco.net Hello
 50 4944 454e 543a 706f 7374 6669 7840 6361  IDENT:postfix@ca
 60 2d6f 6c2d 6d61 7273 6569 6c6c 652d 362d  -ol-marseille-6-
 70 3830 2e61 626f 2e77 616e 6164 6f6f 2e66  80.abo.wanadoo.f
 80 7220 5b36 322e 3136 312e 3130 312e 3830  r [62.161.101.80
 90 5d2c 2070 6c65 6173 6564 2074 6f20 6d65  ], pleased to me
 a0 6574 2079 6f75 0d0a 3235 302d 4558 504e  et you..250-EXPN
 b0 0d0a 3235 302d 5645 5242 0d0a 3235 302d  ..250-VERB..250-
 c0 3842 4954 4d49 4d45 0d0a 3235 302d 5349  8BITMIME..250-SI
 d0 5a45 2031 3030 3030 3030 300d 0a32 3530  ZE 10000000..250
 e0 2d44 534e 0d0a 3235 302d 4f4e 4558 0d0a  -DSN..250-ONEX..
 f0 3235 302d 5855 5352 0d0a 3235 3020 4845  250-XUSR..250 HE
100 4c50 0d0a                                     LP..

Frame 29 (60 on wire, 60 captured)

```

Arrival Time: May 22, 2000 20:28:13.0100  
Time delta from previous packet: 0.013472 seconds  
Frame Number: 29  
Packet Length: 60 bytes  
Capture Length: 60 bytes

Ethernet II

Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)  
Source: 00:20:af:07:1a:3d (3Com\_07:1a:3d)  
Type: IP (0x0800)

Internet Protocol

Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default)  
    0000 00.. = Differentiated Services Codepoint: Default (0x00)  
    .... ..00 = Currently Unused: 0  
Total Length: 40  
Identification: 0x159f  
Flags: 0x04  
    .1.. = Don't fragment: Set  
    ..0. = More fragments: Not set  
Fragment offset: 0  
Time to live: 64  
Protocol: TCP (0x06)  
Header checksum: 0x28e7 (correct)  
Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)  
Destination: dns1.monaco.net (194.79.150.9)

Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq: 2161513065, Ack: 2324999016

Source port: 1027 (1027)  
Destination port: smtp (25)  
Sequence number: 2161513065  
Acknowledgement number: 2324999016  
Header length: 20 bytes  
Flags: 0x0010 (ACK)  
    ..0. .... = Urgent: Not set  
    ...1 .... = Acknowledgment: Set  
    .... 0... = Push: Not set  
    .... .0.. = Reset: Not set  
    .... ..0. = Syn: Not set  
    .... ...0 = Fin: Not set  
Window size: 32120  
Checksum: 0x68b9

Frame 33 (104 on wire, 104 captured)

Arrival Time: May 22, 2000 20:28:13.0841  
Time delta from previous packet: 0.000619 seconds  
Frame Number: 33  
Packet Length: 104 bytes  
Capture Length: 104 bytes

Ethernet II

Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)  
Source: 00:20:af:07:1a:3d (3Com\_07:1a:3d)  
Type: IP (0x0800)

Internet Protocol

Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default)  
    0000 00.. = Differentiated Services Codepoint: Default (0x00)  
    .... ..00 = Currently Unused: 0

Total Length: 90

Identification: 0x15a1

Flags: 0x04

    .1.. = Don't fragment: Set

    ..0. = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: TCP (0x06)

Header checksum: 0x28b3 (correct)

Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Destination: dns1.monaco.net (194.79.150.9)

Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq:  
2161513065, Ack: 2324999016

Source port: 1027 (1027)

Destination port: smtp (25)

Sequence number: 2161513065

Acknowledgement number: 2324999016

Header length: 20 bytes

Flags: 0x0018 (PSH, ACK)

    ..0. .... = Urgent: Not set

    ...1 .... = Acknowledgment: Set

    .... 1... = Push: Set

    .... .0.. = Reset: Not set

    .... ..0. = Syn: Not set

    .... ...0 = Fin: Not set

Window size: 32120

Checksum: 0x4d92

Data (50 bytes)

0	00d0 7972 5c00 0020 af07 1a3d 0800 4500	..yr\... ..=..E.
10	005a 15a1 4000 4006 28b3 3ea1 6550 c24f	.Z...@.@.(.>.eP.O
20	9609 0403 0019 80d6 1269 8a94 ab68 5018	.....i...hP.
30	7d78 4d92 0000 4d41 494c 2046 524f 4d3a	}xM...MAIL FROM:
40	3c63 6872 6973 7469 616e 2e63 616c 6563	<christian.calec
50	6140 7761 6e61 646f 6f2e 6672 3e20 5349	a@wanadoo.fr> SI
60	5a45 3d36 3439 0d0a	ZE=649..

Frame 34 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:13.1545

Time delta from previous packet: 0.070380 seconds

Frame Number: 34

Packet Length: 60 bytes

Capture Length: 60 bytes

Ethernet II

Destination: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Type: IP (0x0800)

Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)  
0000 00.. = Differentiated Services Codepoint: Default (0x00)  
.... ..00 = Currently Unused: 0

Total Length: 40

Identification: 0xf9bd

Flags: 0x04

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 57

Protocol: TCP (0x06)

Header checksum: 0x4bc8 (correct)

Source: dns1.monaco.net (194.79.150.9)

Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq: 2324999016, Ack: 2161513115

Source port: smtp (25)

Destination port: 1027 (1027)

Sequence number: 2324999016

Acknowledgement number: 2161513115

Header length: 20 bytes

Flags: 0x0010 (ACK)

..0. .... = Urgent: Not set

...1 .... = Acknowledgment: Set

.... 0... = Push: Not set

.... .0.. = Reset: Not set

.... ..0. = Syn: Not set

.... ...0 = Fin: Not set

Window size: 32736

Checksum: 0x661f

Frame 35 (102 on wire, 102 captured)

Arrival Time: May 22, 2000 20:28:13.1567

Time delta from previous packet: 0.002275 seconds

Frame Number: 35

Packet Length: 102 bytes

Capture Length: 102 bytes

Ethernet II

Destination: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Type: IP (0x0800)

Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 88

Identification: 0xf9be

Flags: 0x04

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 57

```

Protocol: TCP (0x06)
Header checksum: 0x4b97 (correct)
Source: dns1.monaco.net (194.79.150.9)
Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)
Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq:
2324999016, Ack: 2161513115
Source port: smtp (25)
Destination port: 1027 (1027)
Sequence number: 2324999016
Acknowledgement number: 2161513115
Header length: 20 bytes
Flags: 0x0018 (PSH, ACK)
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 1... = Push: Set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...0 = Fin: Not set
Window size: 32736
Checksum: 0x6411
Data (48 bytes)
  0  0020 af07 1a3d 00d0 7972 5c00 0800 4500  . ...=..yr\...E.
 10  0058 f9be 4000 3906 4b97 c24f 9609 3ea1  .X...@.9.K..O...>.
 20  6550 0019 0403 8a94 ab68 80d6 129b 5018  eP.....h....P.
 30  7fe0 6411 0000 3235 3020 3c63 6872 6973  ..d...250 <chris
 40  7469 616e 2e63 616c 6563 6140 7761 6e61  tian.caleca@wana
 50  646f 6f2e 6672 3e2e 2e2e 2053 656e 6465  doo.fr>... Sende
 60  7220 6f6b 0d0a                                r ok..

Frame 36 (86 on wire, 86 captured)
Arrival Time: May 22, 2000 20:28:13.1572
Time delta from previous packet: 0.000500 seconds
Frame Number: 36
Packet Length: 86 bytes
Capture Length: 86 bytes
Ethernet II
Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)
Source: 00:20:af:07:1a:3d (3Com_07:1a:3d)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
Total Length: 72
Identification: 0x15a2
Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0x28c4 (correct)

```



```

Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)
Destination: dns1.monaco.net (194.79.150.9)
Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq:
2161513115, Ack: 2324999064
Source port: 1027 (1027)
Destination port: smtp (25)
Sequence number: 2161513115
Acknowledgement number: 2324999064
Header length: 20 bytes
Flags: 0x0018 (PSH, ACK)
    ..0. .... = Urgent: Not set
    .... 1... = Acknowledgment: Set
    .... 1... = Push: Set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...0 = Fin: Not set
Window size: 32120
Checksum: 0x3217
Data (32 bytes)
  0  00d0 7972 5c00 0020 af07 1a3d 0800 4500  ..yr\... ..=...E.
 10  0048 15a2 4000 4006 28c4 3ea1 6550 c24f  .H..@.@.(.>.eP.O
 20  9609 0403 0019 80d6 129b 8a94 ab98 5018  .....P.
 30  7d78 3217 0000 5243 5054 2054 4f3a 3c65  }x2...RCPT TO:<e
 40  6d65 3133 4065 6e70 726f 7665 6e63 652e  mel3@enprovence.
 50  636f 6d3e 0d0a                                com>..

Frame 38 (102 on wire, 102 captured)
Arrival Time: May 22, 2000 20:28:13.4835
Time delta from previous packet: 0.326307 seconds
Frame Number: 38
Packet Length: 102 bytes
Capture Length: 102 bytes
Ethernet II
Destination: 00:20:af:07:1a:3d (3Com_07:1a:3d)
Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
Total Length: 88
Identification: 0xf9c6
Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
Fragment offset: 0
Time to live: 57
Protocol: TCP (0x06)
Header checksum: 0x4b8f (correct)
Source: dns1.monaco.net (194.79.150.9)
Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)
Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq:

```

2324999016, Ack: 2161513115

Source port: smtp (25)

Destination port: 1027 (1027)

Sequence number: 2324999016

Acknowledgement number: 2161513115

Header length: 20 bytes

Flags: 0x0018 (PSH, ACK)

..0. .... = Urgent: Not set

...1 .... = Acknowledgment: Set

.... 1... = Push: Set

.... .0.. = Reset: Not set

.... ..0. = Syn: Not set

.... ...0 = Fin: Not set

Window size: 32736

Checksum: 0x6411

Data (48 bytes)

0	0020	af07	1a3d	00d0	7972	5c00	0800	4500	. ...=..yr\...E.
10	0058	f9c6	4000	3906	4b8f	c24f	9609	3ea1	.X...@.9.K..O...>.
20	6550	0019	0403	8a94	ab68	80d6	129b	5018	eP.....h....P.
30	7fe0	6411	0000	3235	3020	3c63	6872	6973	..d...250 <chris
40	7469	616e	2e63	616c	6563	6140	7761	6e61	tian.caleca@wana
50	646f	6f2e	6672	3e2e	2e2e	2053	656e	6465	doo.fr>... Sende
60	7220	6f6b	0d0a						r ok..

Frame 39 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:13.4837

Time delta from previous packet: 0.000203 seconds

Frame Number: 39

Packet Length: 60 bytes

Capture Length: 60 bytes

Ethernet II

Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Source: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Type: IP (0x0800)

Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 40

Identification: 0x15a3

Flags: 0x04

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: TCP (0x06)

Header checksum: 0x28e3 (correct)

Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Destination: dns1.monaco.net (194.79.150.9)

Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq: 2161513147, Ack: 2324999064

Source port: 1027 (1027)

Destination port: smtp (25)  
Sequence number: 2161513147  
Acknowledgement number: 2324999064  
Header length: 20 bytes  
Flags: 0x0010 (ACK)  
    ..0. .... = Urgent: Not set  
    ...1 .... = Acknowledgment: Set  
    .... 0... = Push: Not set  
    .... .0.. = Reset: Not set  
    .... ..0. = Syn: Not set  
    .... ...0 = Fin: Not set  
Window size: 32120  
Checksum: 0x6837

Frame 41 (86 on wire, 86 captured)  
Arrival Time: May 22, 2000 20:28:13.6500  
Time delta from previous packet: 0.166284 seconds  
Frame Number: 41  
Packet Length: 86 bytes  
Capture Length: 86 bytes

Ethernet II  
Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)  
Source: 00:20:af:07:1a:3d (3Com\_07:1a:3d)  
Type: IP (0x0800)

Internet Protocol  
Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default)  
    0000 00.. = Differentiated Services Codepoint: Default (0x00)  
    .... ..00 = Currently Unused: 0  
Total Length: 72  
Identification: 0x15a4  
Flags: 0x04  
    .1.. = Don't fragment: Set  
    ..0. = More fragments: Not set  
Fragment offset: 0  
Time to live: 64  
Protocol: TCP (0x06)  
Header checksum: 0x28c2 (correct)  
Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)  
Destination: dns1.monaco.net (194.79.150.9)

Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq:  
2161513115, Ack: 2324999064  
Source port: 1027 (1027)  
Destination port: smtp (25)  
Sequence number: 2161513115  
Acknowledgement number: 2324999064  
Header length: 20 bytes  
Flags: 0x0018 (PSH, ACK)  
    ..0. .... = Urgent: Not set  
    ...1 .... = Acknowledgment: Set  
    .... 1... = Push: Set  
    .... .0.. = Reset: Not set  
    .... ..0. = Syn: Not set

```

    .... ...0 = Fin: Not set
Window size: 32120
Checksum: 0x3217
Data (32 bytes)
  0  00d0 7972 5c00 0020 af07 1a3d 0800 4500  ..yr\... ...=...E.
 10  0048 15a4 4000 4006 28c2 3ea1 6550 c24f  .H..@.@.(.>.eP.O
 20  9609 0403 0019 80d6 129b 8a94 ab98 5018  .....P.
 30  7d78 3217 0000 5243 5054 2054 4f3a 3c65  }x2...RCPT TO:<e
 40  6d65 3133 4065 6e70 726f 7665 6e63 652e  mel3@enprovence.
 50  636f 6d3e 0d0a                                com>..

Frame 42 (98 on wire, 98 captured)
  Arrival Time: May 22, 2000 20:28:13.7612
  Time delta from previous packet: 0.111196 seconds
  Frame Number: 42
  Packet Length: 98 bytes
  Capture Length: 98 bytes

Ethernet II
  Destination: 00:20:af:07:1a:3d (3Com_07:1a:3d)
  Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)
  Type: IP (0x0800)

Internet Protocol
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
  Total Length: 84
  Identification: 0xf9cc
  Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 57
  Protocol: TCP (0x06)
  Header checksum: 0x4b8d (correct)
  Source: dns1.monaco.net (194.79.150.9)
  Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq:
2324999064, Ack: 2161513147
  Source port: smtp (25)
  Destination port: 1027 (1027)
  Sequence number: 2324999064
  Acknowledgement number: 2161513147
  Header length: 20 bytes
  Flags: 0x0018 (PSH, ACK)
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 1... = Push: Set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...0 = Fin: Not set
  Window size: 32736
  Checksum: 0x13d3

```

Data (44 bytes)

```
 0  0020 af07 1a3d 00d0 7972 5c00 0800 4500  . ...=..yr\...E.
10  0054 f9cc 4000 3906 4b8d c24f 9609 3ea1  .T...@.9.K..O...>.
20  6550 0019 0403 8a94 ab98 80d6 12bb 5018  eP.....P.
30  7fe0 13d3 0000 3235 3020 3c65 6d65 3133  .....250 <eme13
40  4065 6e70 726f 7665 6e63 652e 636f 6d3e  @enprovence.com>
50  2e2e 2e20 5265 6369 7069 656e 7420 6f6b  ... Recipient ok
60  0d0a                                     ..
```

Frame 43 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:13.7617  
Time delta from previous packet: 0.000470 seconds  
Frame Number: 43  
Packet Length: 60 bytes  
Capture Length: 60 bytes

Ethernet II

Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)  
Source: 00:20:af:07:1a:3d (3Com\_07:1a:3d)  
Type: IP (0x0800)

Internet Protocol

Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default)  
    0000 00.. = Differentiated Services Codepoint: Default (0x00)  
    .... ..00 = Currently Unused: 0  
Total Length: 46  
Identification: 0x15a5  
Flags: 0x04  
    .1.. = Don't fragment: Set  
    ..0. = More fragments: Not set  
Fragment offset: 0  
Time to live: 64  
Protocol: TCP (0x06)  
Header checksum: 0x28db (correct)  
Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)  
Destination: dns1.monaco.net (194.79.150.9)

Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq: 2161513147, Ack: 2324999108

Source port: 1027 (1027)  
Destination port: smtp (25)  
Sequence number: 2161513147  
Acknowledgement number: 2324999108  
Header length: 20 bytes  
Flags: 0x0018 (PSH, ACK)  
    ..0. .... = Urgent: Not set  
    ...1 .... = Acknowledgment: Set  
    .... 1... = Push: Set  
    .... .0.. = Reset: Not set  
    .... ..0. = Syn: Not set  
    .... ...0 = Fin: Not set  
Window size: 32120  
Checksum: 0xc270

Data (6 bytes)

```
 0  00d0 7972 5c00 0020 af07 1a3d 0800 4500  ..yr\.. ...=..E.
```

```

10  002e 15a5 4000 4006 28db 3ea1 6550 c24f  ....@.@.(.>.eP.O
20  9609 0403 0019 80d6 12bb 8a94 abc4 5018  ....P.
30  7d78 c270 0000 4441 5441 0d0a          }x.p..DATA..

```

Frame 44 (104 on wire, 104 captured)

```

Arrival Time: May 22, 2000 20:28:13.8553
Time delta from previous packet: 0.093591 seconds
Frame Number: 44
Packet Length: 104 bytes
Capture Length: 104 bytes

```

Ethernet II

```

Destination: 00:20:af:07:1a:3d (3Com_07:1a:3d)
Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)
Type: IP (0x0800)

```

Internet Protocol

```

Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
Total Length: 90
Identification: 0xf9d0
Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
Fragment offset: 0
Time to live: 57
Protocol: TCP (0x06)
Header checksum: 0x4b83 (correct)
Source: dns1.monaco.net (194.79.150.9)
Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

```

Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq: 2324999108, Ack: 2161513153

```

Source port: smtp (25)
Destination port: 1027 (1027)
Sequence number: 2324999108
Acknowledgement number: 2161513153
Header length: 20 bytes
Flags: 0x0018 (PSH, ACK)
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 1... = Push: Set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...0 = Fin: Not set
Window size: 32736
Checksum: 0x113b

```

Data (50 bytes)

```

0   0020 af07 1a3d 00d0 7972 5c00 0800 4500  . ...=..yr\...E.
10  005a f9d0 4000 3906 4b83 c24f 9609 3ea1  .Z...@.9.K..O...>.
20  6550 0019 0403 8a94 abc4 80d6 12c1 5018  eP.....P.
30  7fe0 113b 0000 3335 3420 456e 7465 7220  ...;..354 Enter
40  6d61 696c 2c20 656e 6420 7769 7468 2022  mail, end with "
50  2e22 206f 6e20 6120 6c69 6e65 2062 7920  ." on a line by

```

60 6974 7365 6c66 0d0a

itself..

## Suite du dialogue...

Frame 46 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:13.9536

Time delta from previous packet: 0.096518 seconds

Frame Number: 46

Packet Length: 60 bytes

Capture Length: 60 bytes

Ethernet II

Destination: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Type: IP (0x0800)

Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 40

Identification: 0xf9d2

Flags: 0x04

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 57

Protocol: TCP (0x06)

Header checksum: 0x4bb3 (correct)

Source: dns1.monaco.net (194.79.150.9)

Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq: 2324999158, Ack: 2161513805

Source port: smtp (25)

Destination port: 1027 (1027)

Sequence number: 2324999158

Acknowledgement number: 2161513805

Header length: 20 bytes

Flags: 0x0010 (ACK)

..0. .... = Urgent: Not set

...1 .... = Acknowledgment: Set

.... 0... = Push: Not set

.... .0.. = Reset: Not set

.... ..0. = Syn: Not set

.... ...0 = Fin: Not set

Window size: 32736

Checksum: 0x62df

Frame 47 (98 on wire, 98 captured)

Arrival Time: May 22, 2000 20:28:13.9721

Time delta from previous packet: 0.018529 seconds

Frame Number: 47

Packet Length: 98 bytes

Capture Length: 98 bytes

Ethernet II

Destination: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Type: IP (0x0800)

Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 84

Identification: 0xf9d3

Flags: 0x04

.1.. = Don't fragment: Set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 57

Protocol: TCP (0x06)

Header checksum: 0x4b86 (correct)

Source: dns1.monaco.net (194.79.150.9)

Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq: 2324999158, Ack: 2161513805

Source port: smtp (25)

Destination port: 1027 (1027)

Sequence number: 2324999158

Acknowledgement number: 2161513805

Header length: 20 bytes

Flags: 0x0018 (PSH, ACK)

..0. .... = Urgent: Not set

...1 .... = Acknowledgment: Set

.... 1... = Push: Set

.... .0.. = Reset: Not set

.... ..0. = Syn: Not set

.... ...0 = Fin: Not set

Window size: 32736

Checksum: 0x3fef

Data (44 bytes)

0	0020	af07	1a3d	00d0	7972	5c00	0800	4500	. . . .=..yr\...E.
10	0054	f9d3	4000	3906	4b86	c24f	9609	3ea1	.T..@.9.K..O...>.
20	6550	0019	0403	8a94	abf6	80d6	154d	5018	eP.....MP.
30	7fe0	3fef	0000	3235	3020	5541	4132	3438	..?...250 UAA248
40	3431	204d	6573	7361	6765	2061	6363	6570	41 Message accep
50	7465	6420	666f	7220	6465	6c69	7665	7279	ted for delivery
60	0d0a								..

Frame 48 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:13.9750

Time delta from previous packet: 0.002943 seconds

Frame Number: 48

Packet Length: 60 bytes

Capture Length: 60 bytes

Ethernet II

Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Source: 00:20:af:07:1a:3d (3Com\_07:1a:3d)



```

Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
Total Length: 46
Identification: 0x15a7
Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0x28d9 (correct)
Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)
Destination: dns1.monaco.net (194.79.150.9)
Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq:
2161513805, Ack: 2324999202
Source port: 1027 (1027)
Destination port: smtp (25)
Sequence number: 2161513805
Acknowledgement number: 2324999202
Header length: 20 bytes
Flags: 0x0018 (PSH, ACK)
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 1... = Push: Set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...0 = Fin: Not set
Window size: 32120
Checksum: 0xbd59
Data (6 bytes)
  0  00d0 7972 5c00 0020 af07 1a3d 0800 4500  ..yr\... ..=...E.
 10  002e 15a7 4000 4006 28d9 3ea1 6550 c24f  ....@.@.(.>.eP.O
 20  9609 0403 0019 80d6 154d 8a94 ac22 5018  .....M..."P.
 30  7d78 bd59 0000 5155 4954 0d0a          }x.Y..QUIT..
Frame 49 (60 on wire, 60 captured)
Arrival Time: May 22, 2000 20:28:13.9751
Time delta from previous packet: 0.000091 seconds
Frame Number: 49
Packet Length: 60 bytes
Capture Length: 60 bytes
Ethernet II
Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)
Source: 00:20:af:07:1a:3d (3Com_07:1a:3d)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)

```

```

    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
Total Length: 40
Identification: 0x15a8
Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0x28de (correct)
Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)
Destination: dns1.monaco.net (194.79.150.9)
Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq:
2161513811, Ack: 2324999202
Source port: 1027 (1027)
Destination port: smtp (25)
Sequence number: 2161513811
Acknowledgement number: 2324999202
Header length: 20 bytes
Flags: 0x0011 (FIN, ACK)
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 0... = Push: Not set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...1 = Fin: Set
Window size: 32120
Checksum: 0x6514
Frame 50 (60 on wire, 60 captured)
Arrival Time: May 22, 2000 20:28:14.0380
Time delta from previous packet: 0.062912 seconds
Frame Number: 50
Packet Length: 60 bytes
Capture Length: 60 bytes
Ethernet II
Destination: 00:20:af:07:1a:3d (3Com_07:1a:3d)
Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
Total Length: 40
Identification: 0xf9d4
Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
Fragment offset: 0
Time to live: 57
Protocol: TCP (0x06)

```

```
Header checksum: 0x4bb1 (correct)
Source: dns1.monaco.net (194.79.150.9)
Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)
Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq:
2324999202, Ack: 2161513812
Source port: smtp (25)
Destination port: 1027 (1027)
Sequence number: 2324999202
Acknowledgement number: 2161513812
Header length: 20 bytes
Flags: 0x0010 (ACK)
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 0... = Push: Not set
    .... .0.. = Reset: Not set
    .... ..0. = Syn: Not set
    .... ...0 = Fin: Not set
Window size: 32729
Checksum: 0x62b3

Frame 51 (94 on wire, 94 captured)
Arrival Time: May 22, 2000 20:28:14.0402
Time delta from previous packet: 0.002152 seconds
Frame Number: 51
Packet Length: 94 bytes
Capture Length: 94 bytes

Ethernet II
Destination: 00:20:af:07:1a:3d (3Com_07:1a:3d)
Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)
Type: IP (0x0800)

Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
Total Length: 80
Identification: 0xf9d5
Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
Fragment offset: 0
Time to live: 57
Protocol: TCP (0x06)
Header checksum: 0x4b88 (correct)
Source: dns1.monaco.net (194.79.150.9)
Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)
Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq:
2324999202, Ack: 2161513812
Source port: smtp (25)
Destination port: 1027 (1027)
Sequence number: 2324999202
Acknowledgement number: 2161513812
Header length: 20 bytes
```

Flags: 0x0018 (PSH, ACK)  
..0. .... = Urgent: Not set  
...1 .... = Acknowledgment: Set  
.... 1... = Push: Set  
.... .0.. = Reset: Not set  
.... ..0. = Syn: Not set  
.... ...0 = Fin: Not set

Window size: 32736

Checksum: 0x0bd7

Data (40 bytes)

0	0020	af07	1a3d	00d0	7972	5c00	0800	4500	. ...=..yr\...E.
10	0050	f9d5	4000	3906	4b88	c24f	9609	3ea1	.P...@.9.K..O...>.
20	6550	0019	0403	8a94	ac22	80d6	1554	5018	eP....."....TP.
30	7fe0	0bd7	0000	3232	3120	6d61	696c	2e6d	.....221 mail.m
40	6f6e	6163	6f2e	6e65	7420	636c	6f73	696e	onaco.net closin
50	6720	636f	6e6e	6563	7469	6f6e	0d0a		g connection..

Frame 52 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:14.0404

Time delta from previous packet: 0.000239 seconds

Frame Number: 52

Packet Length: 60 bytes

Capture Length: 60 bytes

Ethernet II

Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Source: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Type: IP (0x0800)

Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 40

Identification: 0x15a9

Flags: 0x00

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 255

Protocol: TCP (0x06)

Header checksum: 0xa9dc (correct)

Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Destination: dns1.monaco.net (194.79.150.9)

Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq: 2161513812, Ack: 0

Source port: 1027 (1027)

Destination port: smtp (25)

Sequence number: 2161513812

Header length: 20 bytes

Flags: 0x0004 (RST)

..0. .... = Urgent: Not set

...0 .... = Acknowledgment: Not set

.... 0... = Push: Not set

.... .1.. = Reset: Set  
.... ..0. = Syn: Not set  
.... ...0 = Fin: Not set

Window size: 0

Checksum: 0x1950

Frame 53 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:14.0465

Time delta from previous packet: 0.006020 seconds

Frame Number: 53

Packet Length: 60 bytes

Capture Length: 60 bytes

Ethernet II

Destination: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Source: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Type: IP (0x0800)

Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 40

Identification: 0xf9d6

Flags: 0x00

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 57

Protocol: TCP (0x06)

Header checksum: 0x8baf (correct)

Source: dns1.monaco.net (194.79.150.9)

Destination: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Transmission Control Protocol, Src Port: smtp (25), Dst Port: 1027 (1027), Seq:  
2324999242, Ack: 2161513812

Source port: smtp (25)

Destination port: 1027 (1027)

Sequence number: 2324999242

Acknowledgement number: 2161513812

Header length: 20 bytes

Flags: 0x0011 (FIN, ACK)

..0. .... = Urgent: Not set

...1 .... = Acknowledgment: Set

.... 0... = Push: Not set

.... .0.. = Reset: Not set

.... ..0. = Syn: Not set

.... ...1 = Fin: Set

Window size: 32736

Checksum: 0x6283

Frame 54 (60 on wire, 60 captured)

Arrival Time: May 22, 2000 20:28:14.0467

Time delta from previous packet: 0.000212 seconds

Frame Number: 54

Packet Length: 60 bytes

Capture Length: 60 bytes

Ethernet II

Destination: 00:d0:79:72:5c:00 (00:d0:79:72:5c:00)

Source: 00:20:af:07:1a:3d (3Com\_07:1a:3d)

Type: IP (0x0800)

Internet Protocol

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..00 = Currently Unused: 0

Total Length: 40

Identification: 0x15aa

Flags: 0x00

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 255

Protocol: TCP (0x06)

Header checksum: 0xa9db (correct)

Source: ca-ol-marseille-6-80.abo.wanadoo.fr (62.161.101.80)

Destination: dns1.monaco.net (194.79.150.9)

Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: smtp (25), Seq: 2161513812, Ack: 0

Source port: 1027 (1027)

Destination port: smtp (25)

Sequence number: 2161513812

Header length: 20 bytes

Flags: 0x0004 (RST)

..0. .... = Urgent: Not set

...0 .... = Acknowledgment: Not set

.... 0... = Push: Not set

.... .1.. = Reset: Set

.... ..0. = Syn: Not set

.... ...0 = Fin: Not set

Window size: 0

Checksum: 0x1950