

# *Mail*



C. Gouinaud  
ISIMA  
2006-2007



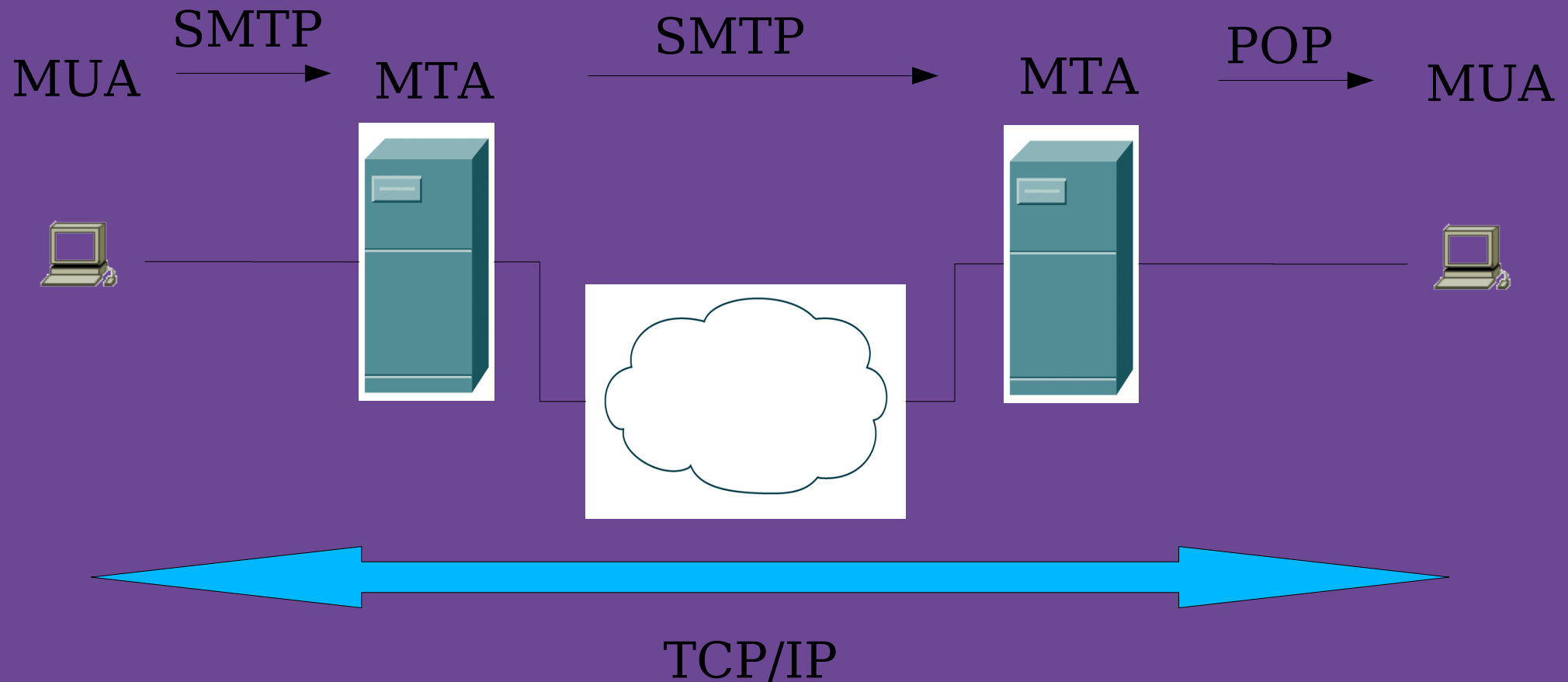
# Introduction

- Envoi entre clients via des serveurs
    - Nom de la forme : [gouinaud@isima.fr](mailto:gouinaud@isima.fr)
    - Corps du message libre
    - Un protocole d'envoi/un protocole de réception
  - Relayage entre serveurs
    - Relayage basé sur les noms
    - Pas de hiérarchie a priori
    - Pas de sécurité
    - Pas d'authentification
- 
-

# *Principe du transfert*

- MUA – mail user agent (pop imap)
  - Assure le relevé des mail
  - Assure l'envoi des mails
  - Assure certaines fonctions de filtrage
  - Outlook, thunderbird, imp, squirrelmail
- MTA – mail transfert agent
  - Assure l'envoi
  - Assure le relayage
  - Transmet au filtre

# *Schéma du transfert*



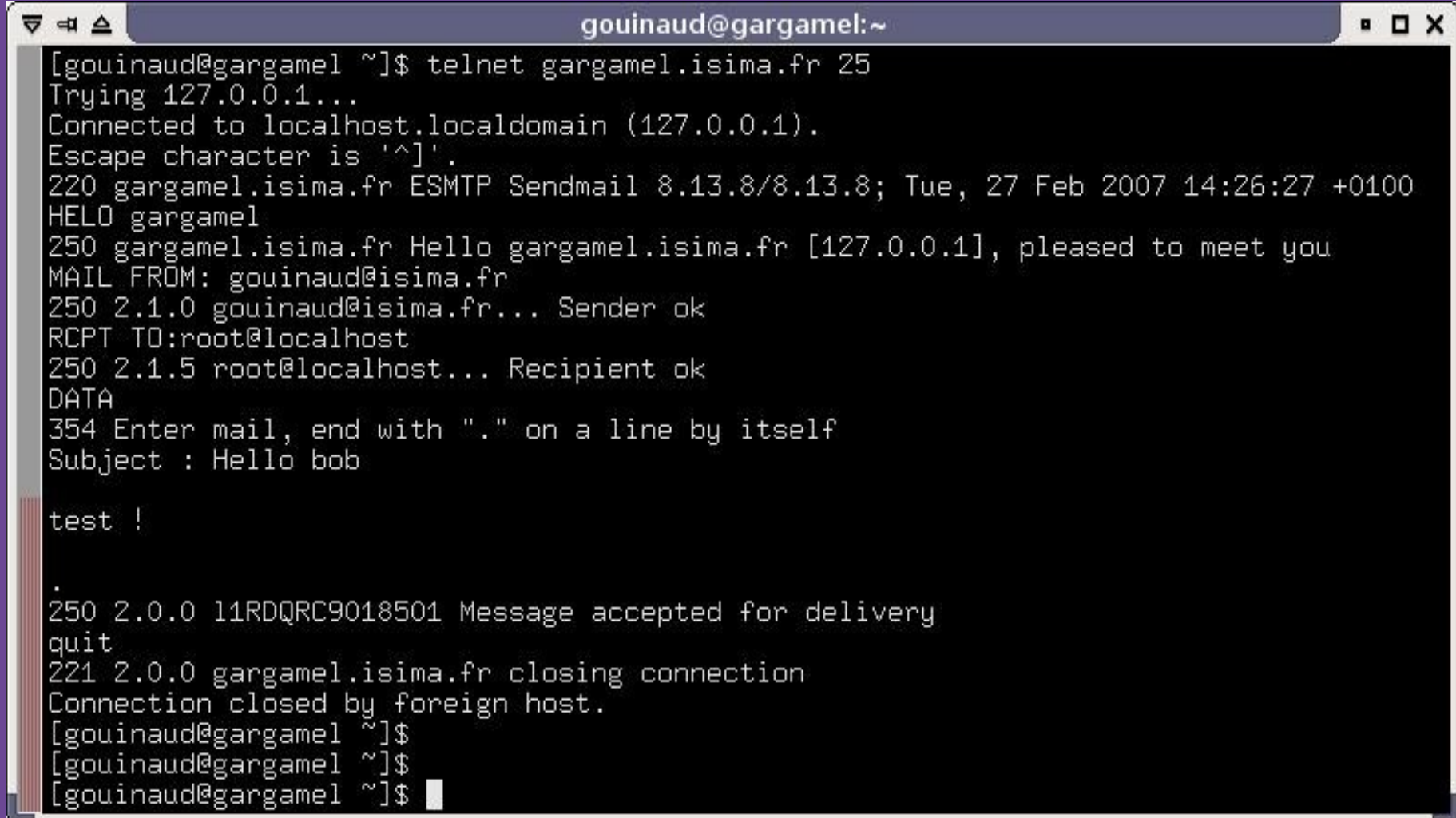
# *Protocole smtp*

- Protocole en mode texte
- Sur TCP/port 25
- Pas d'authentification forte
- Gestion de tentative d'envoi
- Numérotation des messages
- Support modeste du cryptage



# Exemple 1 : envoi manuel

On utilise telnet



```
gouinaud@gargamel:~  
[gouinaud@gargamel ~]$ telnet gargamel.isima.fr 25  
Trying 127.0.0.1...  
Connected to localhost.localdomain (127.0.0.1).  
Escape character is '^]'.  
220 gargamel.isima.fr ESMTP Sendmail 8.13.8/8.13.8; Tue, 27 Feb 2007 14:26:27 +0100  
HELO gargamel  
250 gargamel.isima.fr Hello gargamel.isima.fr [127.0.0.1], pleased to meet you  
MAIL FROM: gouinaud@isima.fr  
250 2.1.0 gouinaud@isima.fr... Sender ok  
RCPT TO:root@localhost  
250 2.1.5 root@localhost... Recipient ok  
DATA  
354 Enter mail, end with "." on a line by itself  
Subject : Hello bob  
  
test !  
  
.  
250 2.0.0 11RDQRC9018501 Message accepted for delivery  
quit  
221 2.0.0 gargamel.isima.fr closing connection  
Connection closed by foreign host.  
[gouinaud@gargamel ~]$  
[gouinaud@gargamel ~]$  
[gouinaud@gargamel ~]$
```

# *Format des messages*

- Enveloppe externe
  - Gérée par le MTA
  - Identification du mail
- Enveloppe interne
  - Date
  - Sujet
  - ....
- Corps du message
  - Text codage Mime

# *Enveloppe externe*

```
V8
T1172593995
K1172593996
N1
P120335
I253/0/19038430
MDeferred: Connection refused by garp.isima.fr.
Fbs
$_gargamel.isima.fr [127.0.0.1]
$rESMTP
$sgargamel.isima.fr
${daemon_flags}
${if_addr}127.0.0.1
S<root@gargamel.isima.fr>
MDeferred: Connection refused by garp.isima.fr.
rRFC822; gouinaud@garp.isima.fr
RPPFD:<gouinaud@garp.isima.fr>
```

- Serveur/relais
- destinataire
- Codage



# *Envelope interne*

```
RPFD: <gouinaud@garp.isima.fr>
H??Return-Path: <||g>
H??Received: from gargamel.isima.fr (gargamel.isima.fr [127.0.0.1])
    by gargamel.isima.fr (8.13.8/8.13.8) with ESMTP id 11RGXF1V025334
    for <gouinaud@garp.isima.fr>; Tue, 27 Feb 2007 17:33:15 +0100
H?x?Full-Name: root
H??Received: (from root@localhost)
    by gargamel.isima.fr (8.13.8/8.13.8/Submit) id 11RGWjsE025307
    for gouinaud@garp.isima.fr; Tue, 27 Feb 2007 17:32:45 +0100
H??Date: Tue, 27 Feb 2007 17:32:45 +0100
H??From: root <root@gargamel.isima.fr>
H??Message-Id: <200702271632.11RGWjsE025307@gargamel.isima.fr>
H??To: gouinaud@garp.isima.fr
H??Subject: etstt
.
```

- Trace
- Meta information (Subject, date)

# *Corps et codage Mime (RFC 822)*

- Message coupé en morceau
- Bornage indiqué dans l'enveloppe interne
- Codage multiple en format MIME
  - Fichier texte : text/plain
  - Fichier binaire : application/\*
  - Encodage en caractères (octets) : 8bits, base64

# Exemple de message :

```
V8
T1172653284
K1172653284
N1
P121104
I253/0/19038434
MDeferred: Connection refused by garp.isima.fr.
Fbs
$ _gargamel.isima.fr [127.0.0.1]
$rESMTP
$s[127.0.0.1]
${daemon_flags}
${if_addr}127.0.0.1
S<gouinaud@isima.fr>
MDeferred: Connection refused by garp.isima.fr.
rRFC822; gouinaud@garp.isima.fr
RPFd:<gouinaud@garp.isima.fr>
H?P?Return-Path: <g>
H??Received: from [127.0.0.1] (gargamel.isima.fr [127.0.0.1])
    by gargamel.isima.fr (8.13.8/8.13.8) with ESMTP id l1S91Oqo029501
    for <gouinaud@garp.isima.fr>; Wed, 28 Feb 2007 10:01:24 +0100
H??Message-ID: <45E544E3.9000909@isima.fr>
H??Date: Wed, 28 Feb 2007 10:01:23 +0100
H??From: Christophe Gouinaud <gouinaud@isima.fr>
H??User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7.2)
Netscape/7.2
H??X-Accept-Language: en, fr
H??MIME-Version: 1.0
H??To: gouinaud@garp.isima.fr
H??Subject: TEST COMPLET attachement
H??Content-Type: multipart/mixed;
    boundary="-----050309010606070901020201"
```

This is a multi-part message in MIME format.

```
-----050309010606070901020201
Content-Type: text/plain; charset=us-ascii;
format=flowed
Content-Transfer-Encoding: 7bit
```

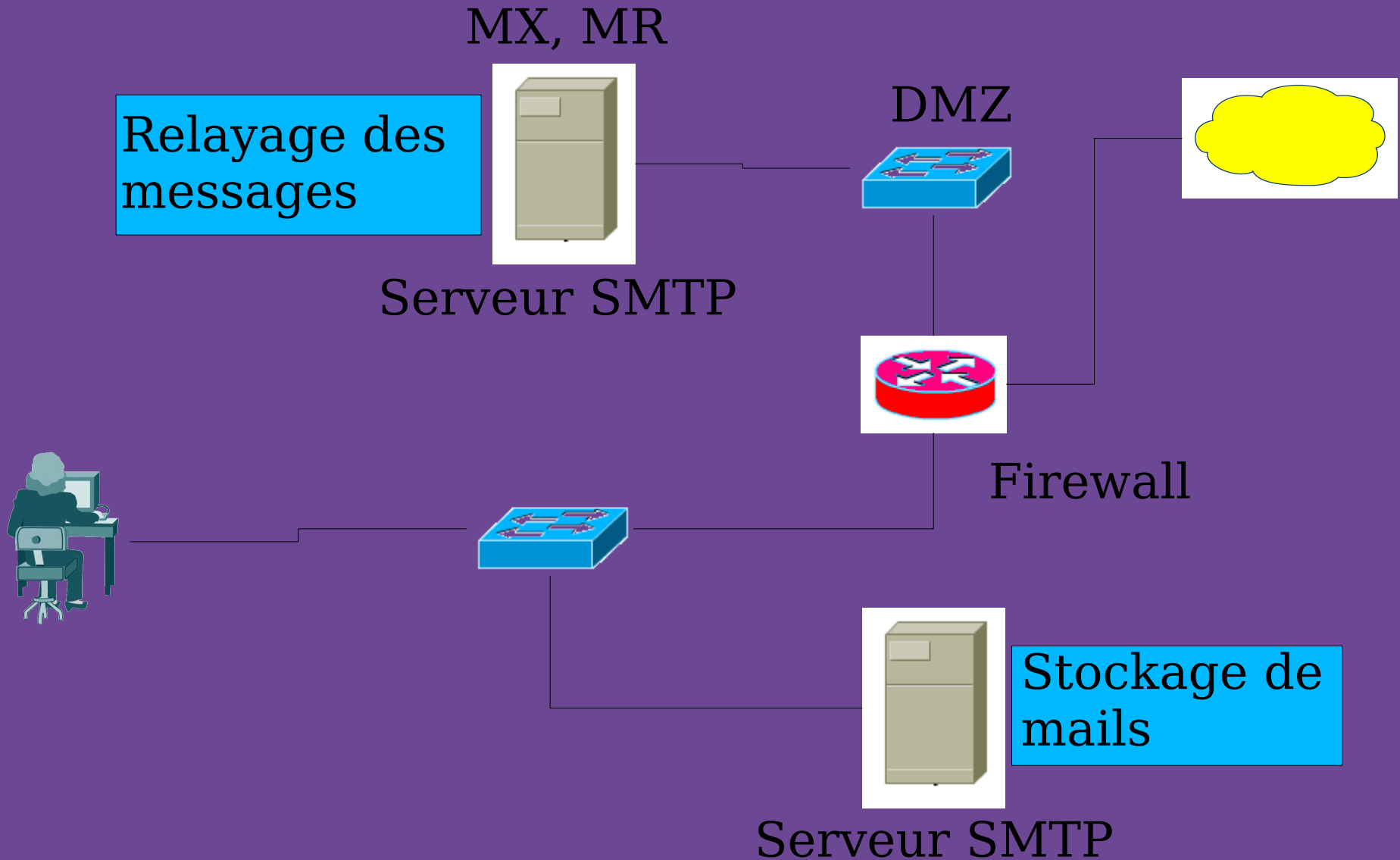
```
-----050309010606070901020201
Content-Type: application/msword;
    name="LISTtelephon.doc"
Content-Transfer-Encoding: base64
Content-Disposition: inline;
    filename="LISTtelephon.doc"
```

```
PGJyIC8+CjxiPl dhcm5pbmc8L2I+OiAgcmVhZGZpbGU
oaHR0cHM6Ly93d3cuaXNpbWEuZnIv
c29mdHMvTElTVHRlbGVwaG9uLmRvYy k6IGZhaWxlZ
CB0byBvcGVuIHN0cmVhbTogSFRUUCBy
ZXF1ZXN0IGZhaWxlZCEgSFRUUC8xLjEgNDA0IE5vd
CBGb3VuZA0KIGluIDxiPi92YXIvd3d3
L2h0bWwvaW50cmFuZXQvZG93bi5waHA8L2I+IG9uI
GxpbmUgPGI+OTI8L2I+PGJyIC8+Cg==
-----050309010606070901020201--
```

# *Routage des messages :*

- Mail exchanger – passerelle de réception
  - Reçoit les mails pour un domaine
  - Défini par des champs MX
  - Peut être multiple
- Mail relais
  - Envoit les mails pour un domaine
  - Doit tourner un MTA (sendmail,exim,qmail)
  - Cible des spammeurs

# Configuration typique



# *POP poste office protocole*

- Protocole simple
  - TCP port 110 – poppassd 106
  - Déplacement des mails en local
  - Authentification sur le système
  - Contrôlable par Tcpsd
  - Cryptage optionnel
  - Pas de gestion de boîtes déportées (sauvegarde ?)
- 
-

# *IMAP – Internet Mail Protcole*

- Protocole complexe
- TCP port 143/220/993
- Copie des mails en local facultative
- Authentification sur le système
- Contrôlable par Tcpsd
- Cryptage Optionnel
- Gestion de boîtes déportées (espace disque) !



# *Stockage du mail*

- Stockage pendant le transit
  - /var/spool/mqueue
  - Un fichier df
  - Un fichier qf
- Stockage final
  - Maildir – chaque mail dans un fichier séparé
  - Mh – deux fichiers par mail
  - Mbox – un fichier pour tous les mails



# Détail format mbox

Un mail

```
From root@gargamel.isima.fr Wed Feb 28 15:42:24 2007
Return-Path: <root@gargamel.isima.fr>
X-Spam-Checker-Version: SpamAssassin 3.1.7 (2006-10-05) on gargamel.isima.fr
X-Spam-Level:
X-Spam-Status: No, score=-4.4 required=5.0 tests=ALL_TRUSTED,BAYES_00
    autolearn=ham version=3.1.7
Received: from gargamel.isima.fr (gargamel.isima.fr [127.0.0.1])
    by gargamel.isima.fr (8.13.8/8.13.8) with ESMTP id l1SEgOwk010505;
    Wed, 28 Feb 2007 15:42:24 +0100
Received: (from root@localhost)
    by gargamel.isima.fr (8.13.8/8.13.8/Submit) id l1SEgOW7010504;
    Wed, 28 Feb 2007 15:42:24 +0100
Date: Wed, 28 Feb 2007 15:42:24 +0100
From: root <root@gargamel.isima.fr>
Message-Id: <200702281442.l1SEgOW7010504@gargamel.isima.fr>
To: gouinaud@gargamel.isima.fr
Subject: test 2
Cc: root@gargamel.isima.fr
```

encore Un

Un autre mail

```
From root@gargamel.isima.fr Wed Feb 28 15:42:24 2007
Return-Path: <root@gargamel.isima.fr>
X-Spam-Checker-Version: SpamAssassin 3.1.7 (2006-10-05) on gargamel.isima.fr
X-Spam-Level:
X-Spam-Status: No, score=-4.4 required=5.0 tests=ALL_TRUSTED,BAYES_00
    autolearn=ham version=3.1.7
Received: from gargamel.isima.fr (gargamel.isima.fr [127.0.0.1])
    by gargamel.isima.fr (8.13.8/8.13.8) with ESMTP id l1SEgOwk010505;
    Wed, 28 Feb 2007 15:42:24 +0100
Received: (from root@localhost)
    by gargamel.isima.fr (8.13.8/8.13.8/Submit) id l1SEgOW7010504;
    Wed, 28 Feb 2007 15:42:24 +0100
Date: Wed, 28 Feb 2007 15:42:24 +0100
From: root <root@gargamel.isima.fr>
Message-Id: <200702281443.l1SEgOW7010504@gargamel.isima.fr>
To: gouinaud@gargamel.isima.fr
Subject: test 3
Cc: root@gargamel.isima.fr
```

# *Partie pratique*

- Pop
- Imap
- Exim
- Postfix
- Sendmail
- Squirrel mail



*Sendmail*



# Installation

- A partir du code source [www.sendmail.org](http://www.sendmail.org)
- RedHat package rpm
  - Sendmail
  - Sendmail-cf
  - Sendmail-doc

```
rpm -i sendmail-8.13.1-2.i386.rpm  
rpm -i sendmail-cf-8.13.1-2.i386.rpm sendmail-doc-8.13.1-2.i386.rpm
```

# *Lancement/arrêt*

Prérequis : **DNS ou nommage !**

- Quand on envoie un mail

`/usr/lib/sendmail -f root root`

- Sous forme de daemon

- Démarrage (paramètres cachés -bd -q1h)

- `/etc/init.d/sendmail start`

- Arrêt

- `/etc/init.d/sendmail stop`

Ne pas oublier le `/etc/rcX.d/`

# Configuration

- Dans /etc/mail
  - sendmail.cf      configuration des fonctions
  - acces              configuration des filtres
  - domaintable    configuration des domaines
  - local-host-name   nom multiple
  - ....
- Se fabrique avec M4  
/usr/share/sendmail-cf/ sous RedHat.

# Création des configurations

- Utilisation de M4
- Ensemble de règles prédéfinies

```
OSTYPE(linux)dnl
FEATURE(redirect)dnl
FEATURE(`accept_unresolvable_domains')
MAILER(procmail)dnl
MAILER(smtp)dnl
FEATURE(`access_db')
FEATURE(`blacklist_recipient')
MASQUERADE_AS(isima.fr)
FEATURE(`promiscuous_relay')
FEATURE(`relay_entire_domain')
FEATURE(`relay_based_on_mx')
define(`MAIL_HUB',`smtp:sp.isima.fr')dnl
```

*Les définitions pour linux*

*Permet de définir un redirecteur*

*Accepte sans entre DNS (pratique en interne)*

*procmail pour smapassain, clamav*

*Fonction SMTP*

*Utilise le fichier /etc/access*

*Utiliser les balck liste*

*Réécrit tout les addresses locale en@ isima.fr*

*Relay ouvert :)*

*Relay tout le domaine*

*Gérer les mails locaux*

*Définition du relais*

- On compile : make CF=config
- On installe : make install-cf CF=config

# *Filtrage - Tri*

- Par table d'accès : /etc/access

Fichier IP,nom Action=RELAY,REJECT,OK

makemap hash access.db /etc/access

- Par programme externe
  - procmail
  - Spamassassin
  - Clamav

Cf : conf mail utilisateur

---

---



# *Postfix*

- Simple à mettre en oeuvre
- Filtrage complet
- Puissance limité
- Gestion uniquement local + smtp



# *Install et config Redhat*

- Package postfix

```
rpm -i postfix-2.1.5-4.2.RHEL4.i386.rpm
```

- Configuration dans /etc/postfix
  - main.cf fichier de config principale
  - Access fichier de filtrage
- Mettre un lien pour qu'il démarre
- Le système le lie à /usr/lib/sendmail



# *Exemple de config postfix*

Fichier main.cf :

```
Myhostname = gargamel.isima.fr
mydomain = isima.fr
myorigin = $mydomain
mynetworks = 192.168.102.0/24,
127.0.0.0/8
#inet_interfaces = 192.168.102.101
mydestination = sp.isima.fr,
localhost.$mydomain, $mydomain
```

Fichier access :

```
isima.fr RELAY
gargamel.isima.fr OK
chef@boulout.net REJECT
```

Fichier master.cf : pas toucher

---

---

## *Commandes pratiques :*

- Relecture de la config : postfix reload
  - Envoi des messages en attente : sendmail -q
  - Efface tous les messages en attente : postsuper -d aLL
  - Refaire la table access : postmap /etc/postfix/access
  - Arrêt/démarrage : /etc/init.d/postfix start | stop | restart
- 
-

# *Exim v4*

- Logiciel Libre GPL
- Orienté filtrage de mails
- Forte capacité de routage de mails
- Lent et complexe à configurer
- Plutôt utilisé sur la debian



# *Exim sur Redhat*

- Installation via rpm
- Configuration /etc/exim  
exim.conf au minimum :  
domainlist local\_domains = @isima.fr  
hostlist relay\_from\_hosts = 127.0.0.1 :  
192.168.102.0/24
- Gestion de la liste noire par acl dans le fichier de config.

# *Pop et Imap – Cyrus imapd*

- Installation (redhat)  
`rpm -i cyrus-imap.xxx.rpm`
- Configuration  
ajuster sendmail.cf façon cyrus-proto  
`/usr/share/sendmail/cf/`  
vérifier le lancement du saslauthd  
`/etc/init.d/saslauthd start`

# *Boîte mail cyrus*

- Créer un compte utilisateur (ou bien `saslpasswd2 -c`)
- Créer une boîte aux lettres CYRUS (impératif même pour root)  
# `cyrusadm -u cyrus localhost`  
> `cm user.root`  
> `cm user.duglu`
- Destruction des boîtes : détruire le répertoire `/var/spool/cyrus/user/duglu`



# *Cyrus Divers*

- Création de boîtes communes avec cyradm
- Configuration des clients classiques, en pop ou en imap
- Reconnaissance des boîtes automatique
- Filtrage des accès avec tcpd



# *Alias et liste*

- Alias  
Dans /etc/aliases  
castorj:riri,fifi,loulou  
toto::script
- Mailling list
  - Mailman
  - Sympa
  - Smartlist

# *Filtrage de spam et de virus*

- Clamav
- Spamassassin



# *Spamassassin*

- Installation via rpm
- Mise à jour : sa-update
- Apprentissage : sa-learn
- Activation :
  - Via sendmail.cf
  - Via procmail
- Mode client-serveur

# *Webmail – squirrelmail*

Client Email imap accessible via le WEB

- Installation apache2 SSL + PHP
- Recupérer la dernière version
- Dérouler et mettre les bons droits
- Configuration via le script



# Surveillance des logs

se trouve /var/log/maillog

- Utilisation de tail
- Utilisation de grep
- Utilisation de cut

```
Mar  4 09:19:33 elo sendmail[4416]: l248JX3n004416: from=root, size=307, class=0
, nrcpts=1, msgid=<200703040819.l248JX3n004416@elo.isima.fr>, relay=root@localho
st
```

```
Mar  4 09:19:34 elo sendmail[4417]: l248JXRg004417: from=<root@elo.isima.fr>, si
ze=557, class=0, nrcpts=1, msgid=<200703040819.l248JX3n004416@elo.isima.fr>, pro
to=ESMTP, daemon=MTA, relay=localhost.localdomain [127.0.0.1]
```

```
Mar  4 09:19:34 elo sendmail[4416]: l248JX3n004416: to=root, ctladdr=root (0/0),
delay=00:00:01, xdelay=00:00:01, mailer=relay, pri=30307, relay=[127.0.0.1] [12
7.0.0.1], dsn=2.0.0, stat=Sent (l248JXRg004417 Message accepted for delivery)
```

```
Mar  4 09:19:34 elo sendmail[4418]: l248JXRg004417: to=<root@elo.isima.fr>, ctla
ddr=<root@elo.isima.fr> (0/0), delay=00:00:00, xdelay=00:00:00, mailer=local, pr
i=30765, dsn=2.0.0, stat=Sent
```

# *Conclusion*

Mail linux redhat :

- Suite complète d'outils
- Performant
- Mal intégré avec Active Directory

