

# MESSAGERIE

Jean-Marc Pouchoulon Septembre 2022  
BUT R303

# Une vieille application de l'internet



- Mais elle fait toujours partie du socle des services internet.
- Elle n'a pas été pensée pour la sécurité mais pour la disponibilité

# c'est quoi un mel ?

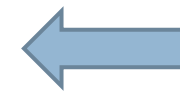
---

- En-Têtes
- Une ligne Blanche séparatrice
- Un corps.

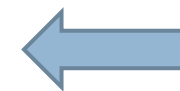
# Un mel:

```
Received: from smtp-racine.in.ac-montpellier.fr ([172.2 .170.1 4])
  by frontal-mes2.ac-montpellier.fr
  (Sun Java System Messaging Server 6.2-9.15 (built Dec 16 2008))
  with ESMTP id <OKTB00AQHJHOVY20@frontal-mes2.ac-montpellier.fr> for
  jean-marc.pouchoulon@ac-montpellier.fr; Wed, 18 Nov 2009 20:01:00 +0100 (CET)
Received: from v223antiv-1.in.ac-montpellier.fr
  (v223antiv-1.ac-montpellier.fr [192.16 .22 .27])
  by smtp-racine.in.ac-montpellier.fr (8.14.1/8.14.1)
  with ESMTP id nAIJ12As019963  for <jean-marc.pouchoulon@ac-montpellier.fr>;
  Wed, 18 Nov 2009 20:01:03 +0100
Received: from l172phy-01.in.ac-montpellier.fr
  (l172phy-01.in.ac-montpellier.fr [172.2 .1 . 8])
  by v223antiv-1.in.ac-montpellier.fr (8.13.8/8.13.8)
  with ESMTP id nAIJ0XTV023542  for <jean-marc.pouchoulon@ac-montpellier.fr>;
  Wed, 18 Nov 2009 20:00:33 +0100
Date: Wed, 18 Nov 2009 20:00:33 +0100
From: jean-marc.pouchoulon@ac-montpellier.fr
Subject: Alarm pb www.ac-montpellier.fr
To: jean-marc.pouchoulon@ac-montpellier.fr
Message-id: <200911181900.nAIJ0XTV023542@v223antiv-1.in.ac-montpellier.fr>
MIME-version: 1.0
Content-type: text/plain; charset=us-ascii
Content-transfer-encoding: 7bit
X-Anti-Virus: Kaspersky Anti-Virus for Sendmail with Milter API 5.6.20,
  bases: 20071122 #435115, check: 20091118 clean
X-Scanned-By: MIMEDefang 2.67 on 172.29.170.104

mechanize._response.httperror_seek_wrapper HTTP Error 503: Service Unavailable['http://www.ac-montpel
```



En-  
têtes



Ligne  
blanche



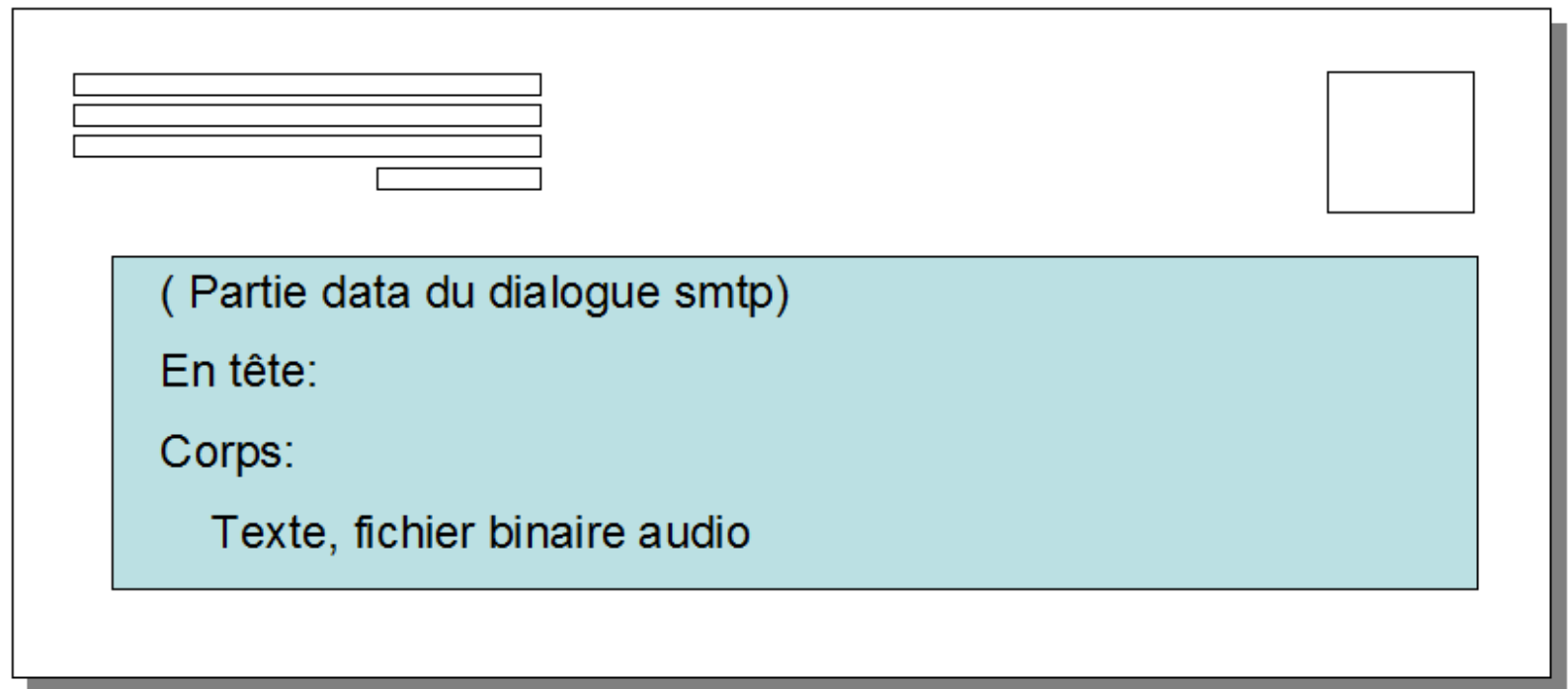
Corps du  
message

# Plusieurs domaines destinataires

- Dans un mel comment peux-t-on avoir plusieurs destinataires sur plusieurs domaines différents ?
- De plus Il faut que le destinataire des mels puisse voir tous les destinataires même si il est d'un autre domaine.
- Faut t il que le mel fasse la tournée des serveurs smtp ?

# Heureusement il y a l'enveloppe... smtp

Message = En-tête et corps dans une  
enveloppe !



# Dialogue smtp

- telnet antivirus 25...
- *220 mx1.ac-montpellier.fr ESMTP Sendmail 8.13.1/8.13.1; Sat, 11 Jun 2005 15:48:41 +0200*
- ehlo l1serv5
- *250-mx1.ac-montpellier.fr Hello l1serv5.in.ac-montpellier.fr [172.29.160.19], pleased to meet you*
  - 250-ENHANCEDSTATUSCODES*
  - 250-PIPELINING*
  - 250-8BITMIME*
  - 250-SIZE 7000000*
  - 250-DSN*
  - 250-ETRN*
  - 250-DELIVERBY*
  - 250 HELP*

# Dialogue smtp

**mail from:**<pouchou@ac-montpellier.fr>

> 250 2.1.0 <pouchou@ac-montpellier.fr>... Sender ok

**rcpt to:**<jean-marc.pouchoulon@ac-montpellier.fr>

250 2.1.5 <jean-marc.pouchoulon@ac-montpellier.fr>...  
Recipient ok

**data**

354 Enter mail, end with "." on a line by itself  
test.

.  
250 2.0.0 j5BDmftR020065 Message accepted for delivery

**quit**



# SMTP/ESMTP/MIME

- Smtip est prévu pour véhiculer uniquement les lignes de texte codées en ascii 7 bits.
- Message = En-Tête +Ligne Blanche +Corps.
- ESMTP est la norme, permet de travailler en 8 bits et d'utiliser le format MIME.
- MIME (RFC 2045) définit des techniques de codage pour le transport de données variées (audio , texte, vidéo).

# Routage des mels

- A la poste on tri le courrier mais comment aiguille-t-on un message ?
- Le ....

# Focus sur le en-têtes

**Return-Path:** <jean-marc.pouchoulon@ac-montpellier.fr>

**Received:** from mx1.ac-montpellier.fr ([192.168.61.213]) by svrs2.ac-montpellier.fr (Netscape Messaging Server 4.15) with ESMTP id IHX7WN00.11C for <jean-marc.pouchoulon@ac-montpellier.fr>; Sat, 11 Jun 2005 14:55:35 +0200

**Message-ID:** <42AADF28.2040401@ac-montpellier.fr> Date: Sat, 11 Jun 2005 14:55:04 +0200 From: "Pouchoulon Jean-Marc" <jean-marc.pouchoulon@ac-montpellier.fr>

**User-Agent:** Mozilla Thunderbird 0.9 (Windows/20041103)

**X-Accept-Language:** fr, en

MIME-Version: 1.0

**From:** jean-marc pouchoulon <jean-marc.pouchoulon@ac-montpellier.fr>

**To:** jean-marc pouchoulon <jean-marc.pouchoulon@ac-montpellier.fr>

**Subject:** Test d'envoi

**Content-Type:** multipart/mixed; boundary="-----070200080500000703030006"

**X-Greylist:** Sender DNS name whitelisted, not delayed by milter-greylist-1.6 (mx1.ac-montpellier.fr [192.168.61.213]); Sat, 11 Jun 2005 14:55:23 +0200 (CEST) X-Scanned-By: MIMEDefang 2.51 on 192.168.61.213

# Quelques définitions d'entêtes

- Return path = *adresse de l'expéditeur de l'enveloppe.*
- **Received** = *Rajouté par chaque mta traversé.*
- Message-id = *identifiant unique du message rajouté lors du premier routage.*
- To = *Destinaire.*
- **From** = *adresse de l'expéditeur.*
- X- *Champ non standardisé (ici antispam greylist)*
- Content-type : *Type/sous type [attribut = valeur] des données transportées. ( il existe 7 types fondamentaux : texte, image, audio, video, application, multipart (mixed,alternative,parrallèle, digest),message,report. )*
- Subject : *sujet*
- delivery-notifications-to: *le mua en le lisant demande le renvoi d'un accusé de réception à la lecture*

Il en existe bien d'autres ....

# Codes SMTP

- Success (2.X.X numeric codes)
- Persistent transient failure (4.X.X numeric codes)
- Permanent failures (5.X.X numeric codes)

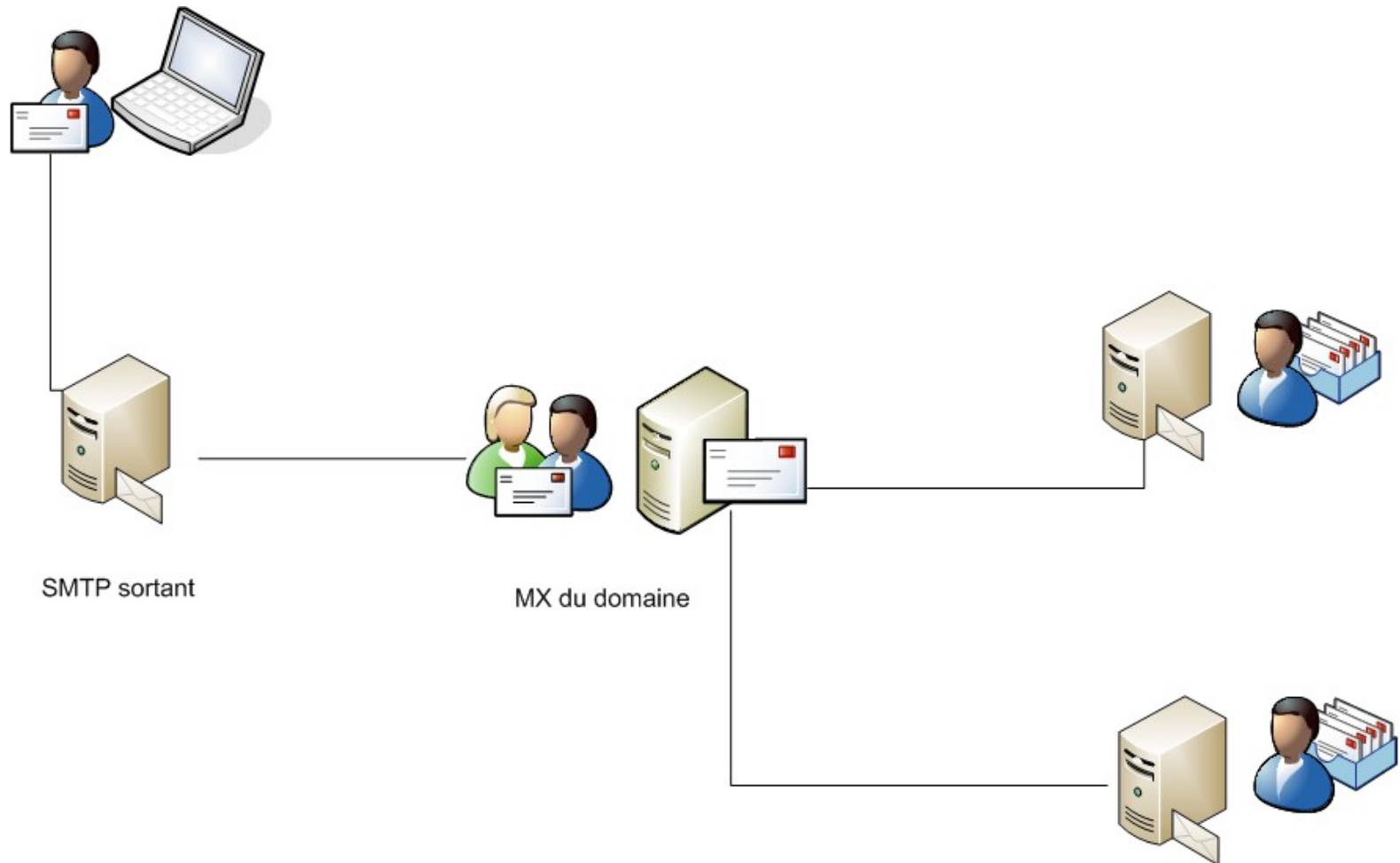
Une fois un mel accepté , c'est **votre responsabilité** de ne pas le perdre.

# Routage des Messages : Le MX

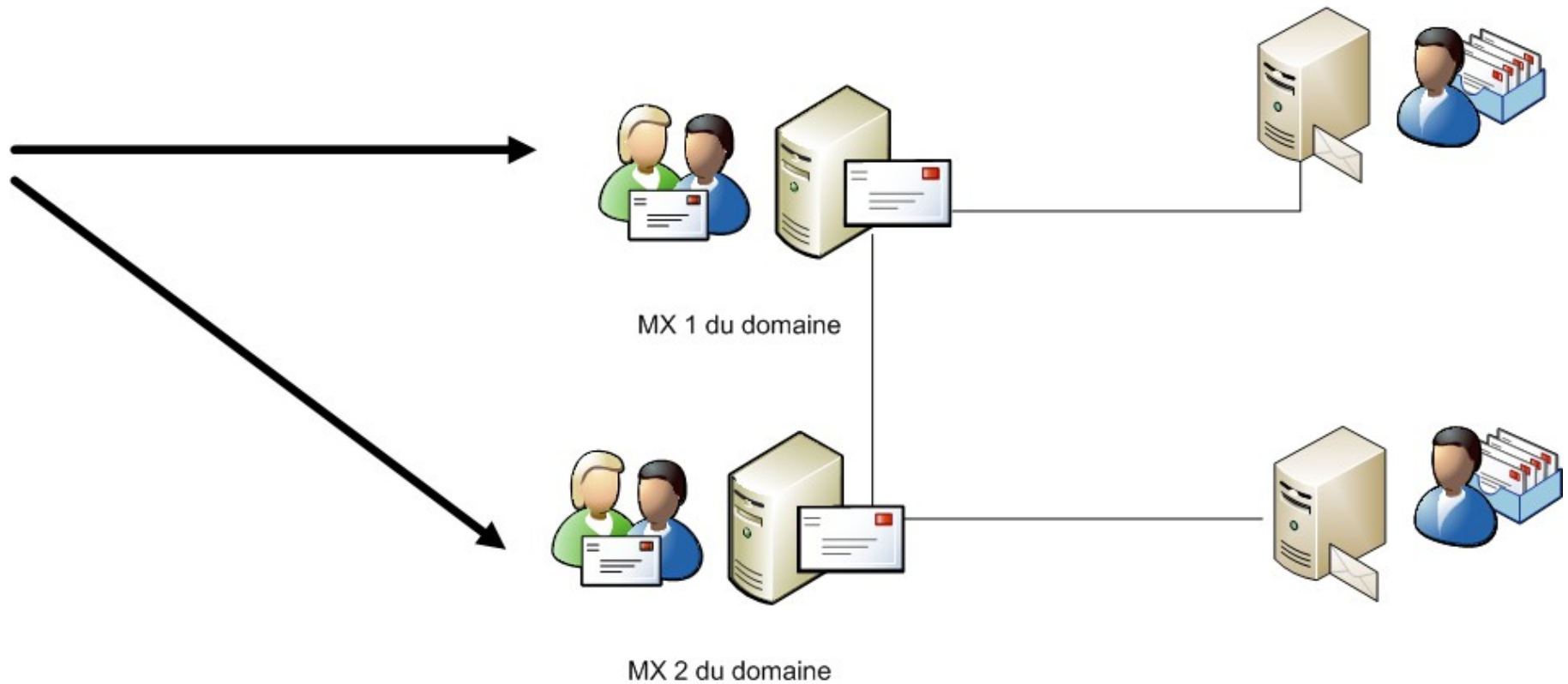
- Quand on demande l'envoi d'un mel au domaine ac-montpellier.fr , en fait le serveur de messagerie va demander au DNS de la zone ac-montpellier.fr quel est son (ses ) serveur(s) responsable(s) de la réception des mail

**MX = MAIL EXCHANGER**

# A quoi sert un MX ?

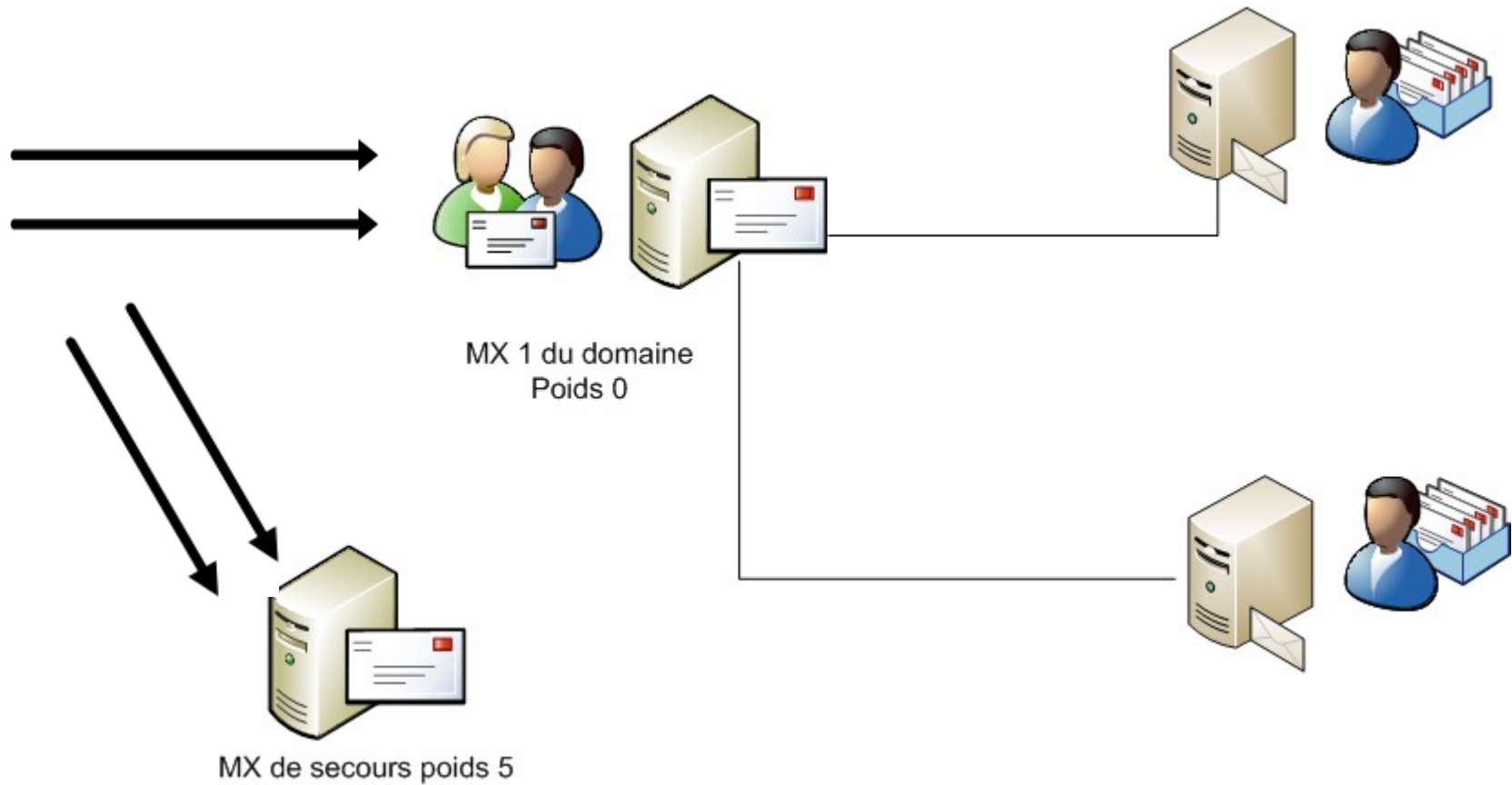


# A quoi sert un MX ?





# A quoi sert un MX ?



# Un MX sert donc à:

---



- Point d'accès unique d'un domaine ( Campus ou Entreprise)
- Equilibrage de charge
- Failover

# Exemple MX enregistrements DNS (Bind)

Host **www.ac-montpellier** a pour  
MX ces deux machines renater et  
proxecoles, proxecoles étant son mel  
exchanger préféré

<b>www.ac-montpellier.fr.</b>	<b>IN MX</b>	<b>4</b>
<b>renater.ac-montpellier.fr.</b>		
	<b>IN MX</b>	<b>0</b>
<b>proxecoles.ac-montpellier.fr.</b>		

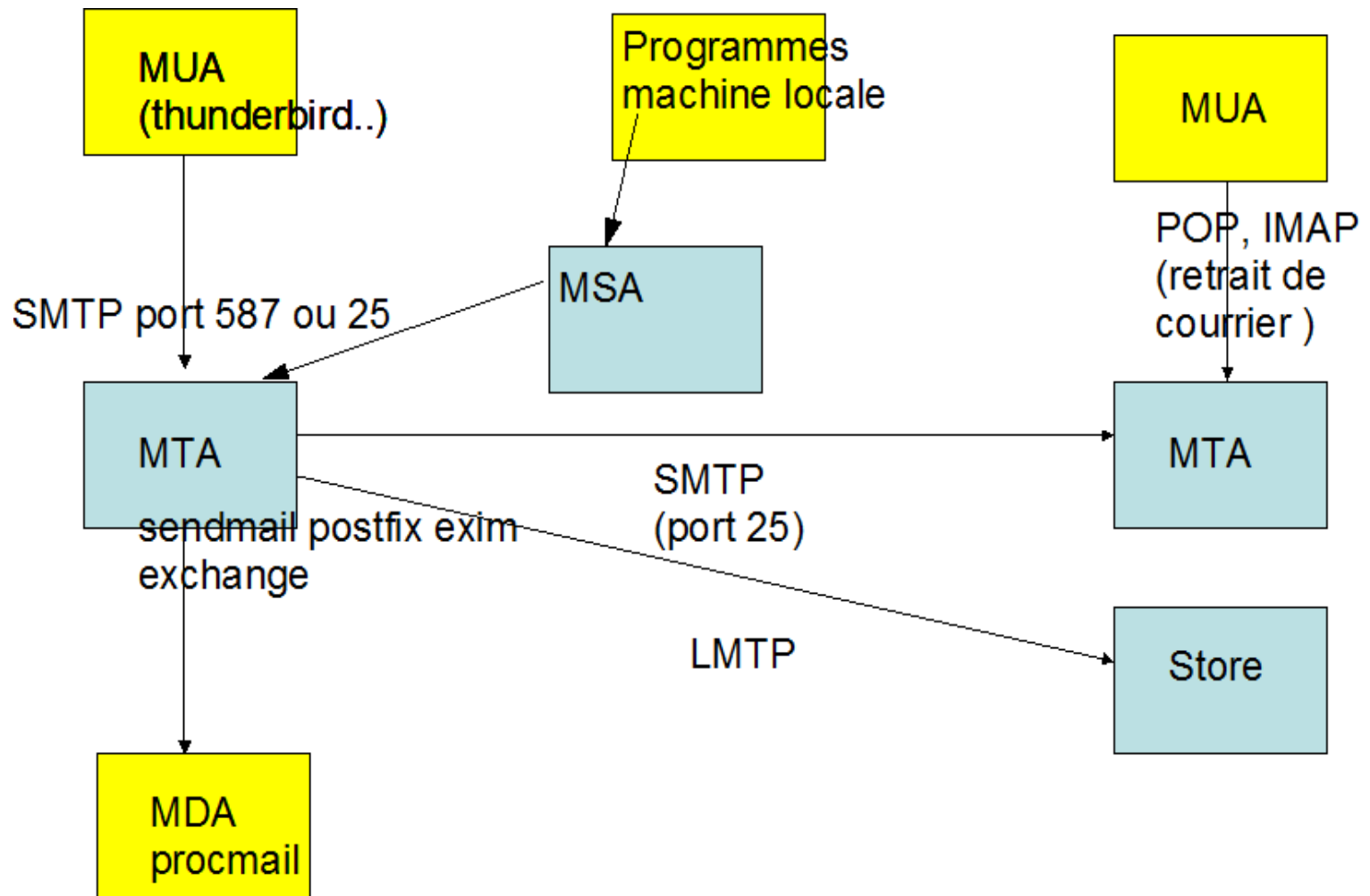
# Exemple MX enregistrements DNS (Bind)

 domain	 Poids	
ac-montpellier.fr. montpellier.fr.	IN MX 4	renater.ac-
ac-montpellier.fr. montpellier.fr.	IN MX 0	proxecoles.ac-
ac-montpellier.fr. montpellier.fr.	IN MX 0	proxecoles2.ac-
ac-montpellier.fr. montpellier.fr.	IN MX 3	renater4.ac-

# Un peu de vocabulaire technique

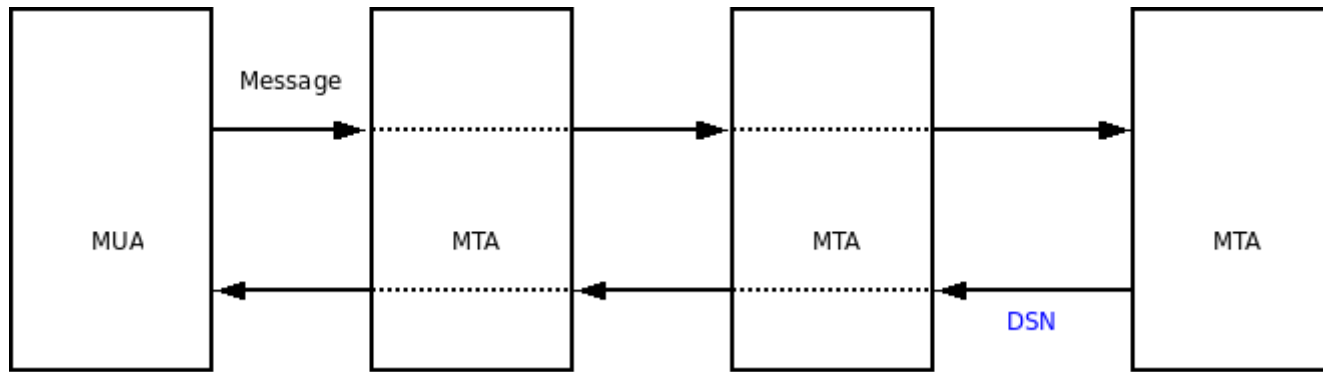
- **MTA** ( Mail Transfert Agent ). Transfert de message de serveur à serveur
- **MUA** ( Mail User Agent). Un client comme thunderbird, eudora...
- **MDA** ( Mail delivery Agent ) ex procmail
- **MSA** (Mail submission Agent rfc 2476, smtp sur le port 587).Il met les messages envoyés par un MUA au standard avant de les relayer. Authentification possible.

# Les acteurs de SMTP



# DSN

- Delivery Status Notification (Source trustedbird)



- Signature et chiffrement avec SMIME, trustedbird
- Mais...

# Un bounce

- The original message was received at Mon, 28 Dec 2009 14:45:08 +0100 from mta-2.ac-montpellier.fr [172.29.12.105] ----- The following addresses had permanent fatal errors -----  
<jeanmarc.pouchoulon2@gmail.com>  
(reason: 550-5.1.1 The email account that you tried to reach does not exist. Please try)  
----- Transcript of session follows ----- ... while talking to gmail-smtp-in.l.google.com.: >>>  
DATA



# Éléments clefs de la messagerie

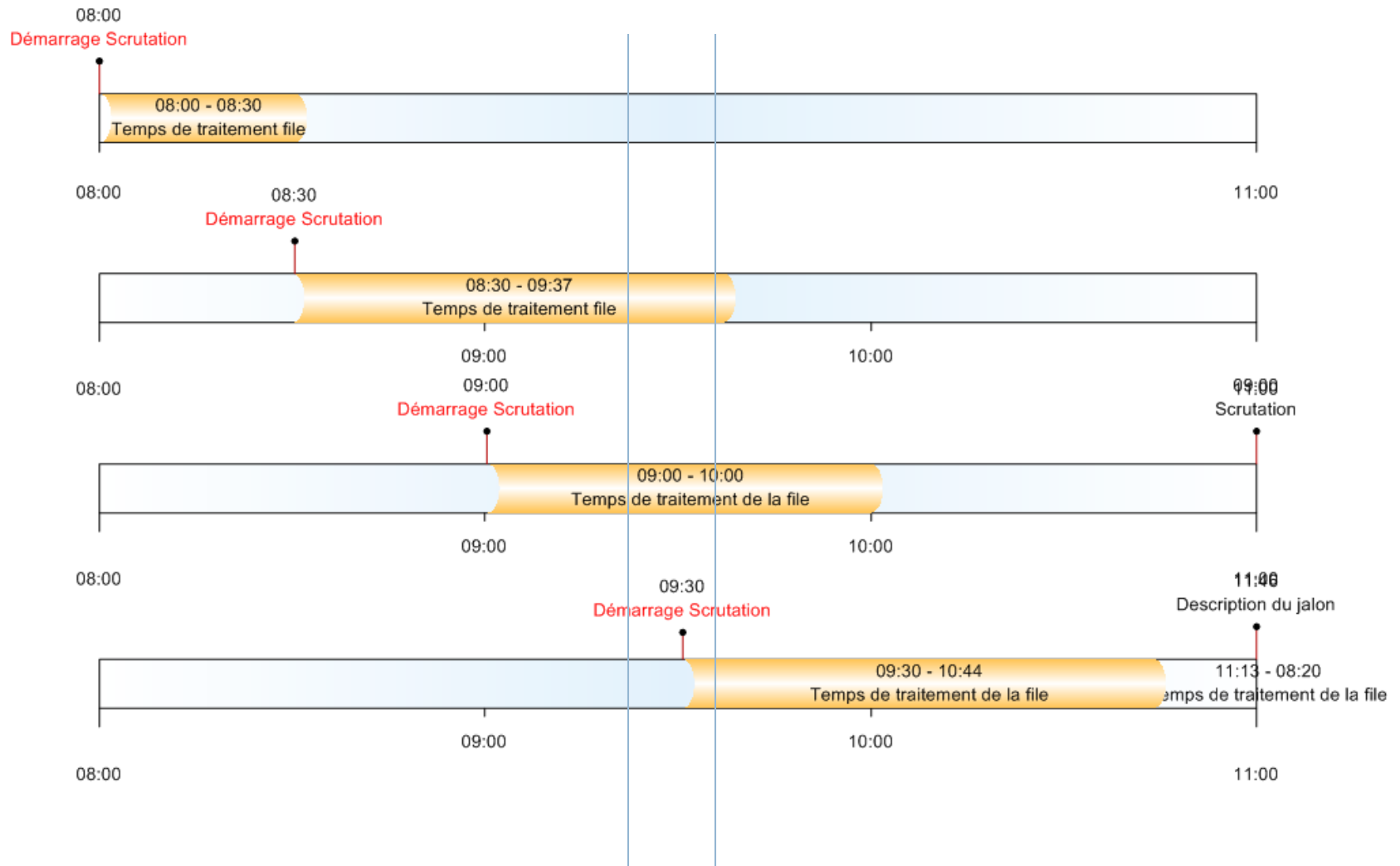
- Files d'attentes
- Annuaire LDAP
- Stockages

# Files d'attente

---

- Que se passe t il quand on envoie un message et que le serveur du destinataire n'est pas joignable ?

# File d'attente et temps de scrutation



# File d'attente

---

- Que faut t il donc faire pour correctement gérer les files d'attentes ?

# Réponses ...

- Séparation des disques systèmes
- Multiplication des files ( plusieurs vitesses)
- On peut les découper et les traiter ensuite.

Ne jamais travailler en mémoire.  
Pourquoi ?

# Annuaire LDAP

- ❑ Obligatoire pour gérer une seule base d'utilisateurs.
- ❑ Performances en lecture très importantes.
- ❑ On peut y stocker bien plus que ça ( route de messagerie, des alias...)
- ❑ Indissociable d'une messagerie moderne.
- ❑ Peut être remplacé/doublé par des fichiers de type BerkeleyDB.

# Stockage des messages

- Le stockage est réalisé sur des serveurs dédiés avec le protocole LMTP. ( = SMTP sur le LAN)
- Sur des messageries de tailles moyennes à importantes un espace dédié de stockage est indispensable.
- Le plus souvent il est réalisé sur un SAN , le serveur y accède via FC ou NFS ou ISCSI
- Il est difficile de sauvegarder une messagerie.

# Aliasing , Masquarading, Listes

- La gestion des alias est importante ( mieux vaut `jmp@ac-montpellier.fr` que `jean-marc.pouchoulon@ac-montpellier.fr` )
- Le Masquarading est utile ( machines avec des domaines internes non résolubles sur le web, fusion )
- Listes : en général on utilise un serveur dédié ( SYMPA par exemple ).



# Quelques MTA

- *Sendmail 8 ( le + ancien, le + documenté, le + paramétrable , le + complexe ?, le - sécurisé ? )*
- *Meta1 ex successeur de sendmail*
- *Postfix ( assez récent, architecture pensé au temps ou internet n'était déjà plus sur )*
- *D'autres libres Exim , Qmail ...*
- *Les payants : exchange , lotus , JES (sun)....*

# Le retrait du courrier

---

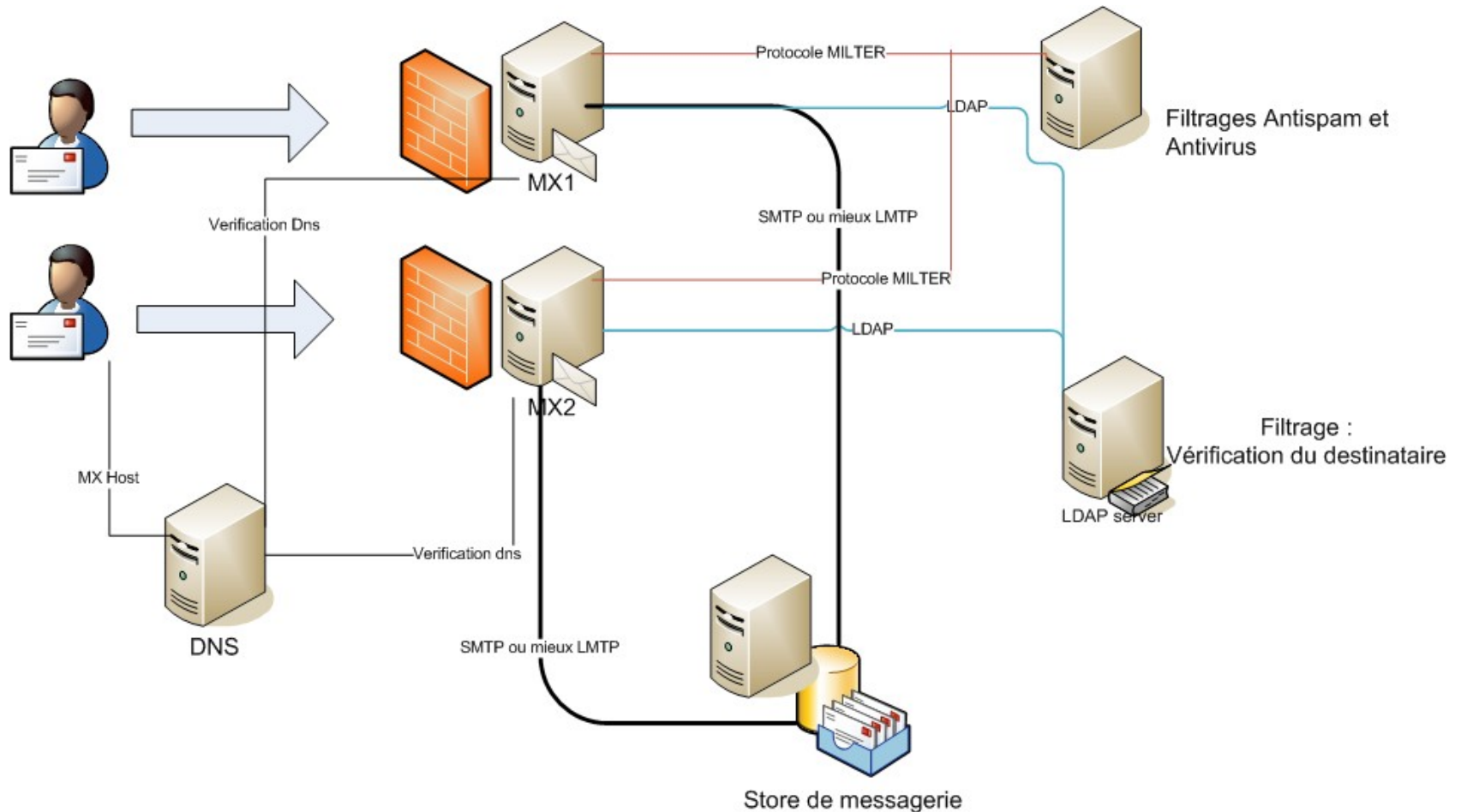
Une fois le courrier sur un Store il faut le retirer

- Soit protocole POP.
- Soit protocole IMAP.
  
- Différences entre les deux ?

# Serveurs de liste

- Les logiciels de messageries ne sont pas faits pour ça. ( gestion des droits , se passer de l'utilisateur système )
- Un logiciel français incontournable : Sympa
- Permet de gérer des listes , avec des backends d'utilisateurs et des scenarii.

# Une architecture de messagerie très simplifiée



# Part 2

---

## LUTTE ANTI-SPAM

# Définitions

- **SPAM (UCE – UBE)** : Envois massifs de courriers non sollicités (mauvaise bouffe )
- **opt-in**: L'envoi de messages est illégal sauf si l'utilisateur l'autorise expressément
- **opt-out**: L'envoi de messages est légal sauf si l'utilisateur ne le souhaite pas expressément.
- **Relais**: envoi d'un message d'un domaine a vers un domaine c en passant par un domaine b.

# Le constat sur les flux

- Un nombre de virus et de spams qui représentent  
jusqu'à 90 % du trafic mail.
- Le mel est égal à 7% du trafic internet dans mon environnement de travail. (avec greylist )
- Des risques et du temps perdu pour les utilisateurs.
- Une charge pour les serveurs de courriers non négligeable et la aussi un impact financier.

# SMTP est non sécurisé

- Aucune vérification du contenu issu de la commande DATA dans le dialogue SMTP et donc les en-têtes que vous voyez peuvent être fabriqués de toutes pièces.
- Donc l'expéditeur que votre client de messagerie fait apparaître peut être factice.



# A l'origine

- SMTP devait être tolérant au panne
- Il suffisait d'envoyer un mel à un serveur pour le voir acheminé. Au départ un serveur de mel était ouvert à tout envoi.
- Bien entendu ce n'est plus le cas aujourd'hui mais à vérifier ( sinon vous devenez une usine à blanchiment de mel )

# Modes de diffusion du SPAM

---

- Réseaux de Zombies.
  - Spammeurs Officiels.
  - Création/hacking de comptes.
  - Backscatering.
- ...

# Backscattering

- Usurpation de l'adresse expéditrice
- Envoie de mels vers des adresses n'existant pas ou injoignables et émissions de bounces vers l'expéditeur usurpé.

Donc il vaut mieux éviter de générer des bounces en:

- Vérifiant le destinataire au plus tôt ( Idap)
- Rejetant les virus sans bounces.
- Evitant les messages automatiques.( je suis en congé ...)

# Méthodes de lutte

- Respecter les RFC ( ehlo, résolution dns, attente de la bannière 220 = **tarpitting**).
- Contrôler les **débits**.
- Listes **noires** – bases de réputations (adresse ou domaine connues comme spammeurs), interrogation via le dns.
- Filtrages Bayésiens et statistiques.
- Utilisation de filtres « **Milters** » divers et variés.

# Méthodes de lutte (suite)

- **Scoring** (spamassassin qui va donner un score à un message en fonction de l'expéditeur, du contenu).
- **Empreintes de spam** ( checksum) + serveur (razor pyzor).
- **Dns et/ou crypto** ( DKIM -SPF ).
- **Listes Grises.** ( Greylist ).
- Boiboites ( Barracuda , Cisco Ironport , Vaderetro ....).
- White listing après confirmation par l'expéditeur (mailinblack).
- Vérification DNS.

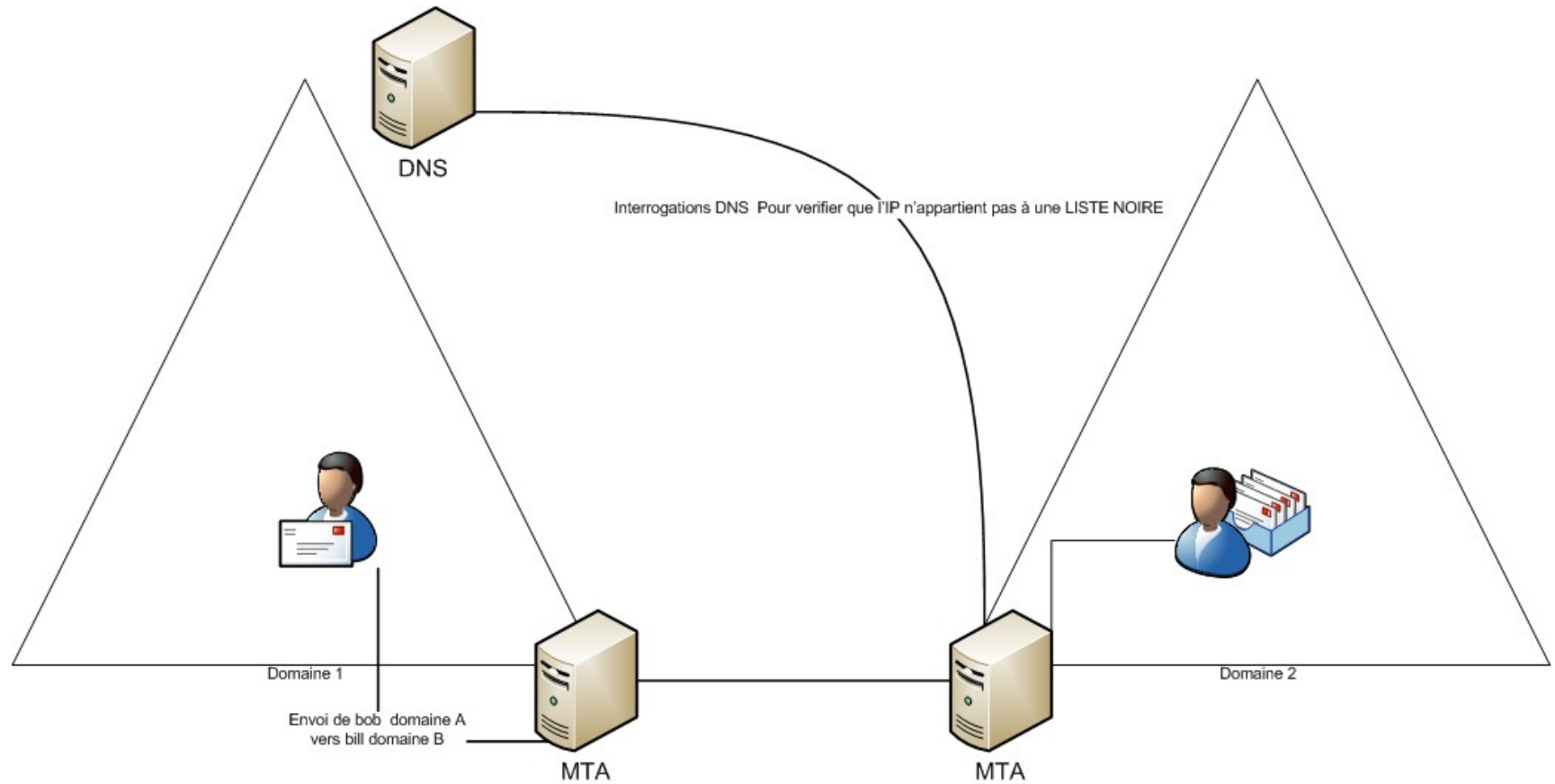
....

Combinaison de toutes ces méthodes.



# Zoom sur les méthodes de lutte

# Liste noire



# Listes Noires

## □ Principe :

Un mel arrive avec l'adresse a.b.c.d

On fait une requête reverse DNS vers un serveur de  
La liste noire que l'on veut utiliser ( par ex  
spamhaus)

d.c.b.a.sbl-xbl.spamhaus.org

Si c'est un spam une réponse dns comme 127.0.0.x  
Arrive indiquant que cet host est considéré comme  
un  
spammeur par la blacklist.



# Vérification de l'empreinte du mel

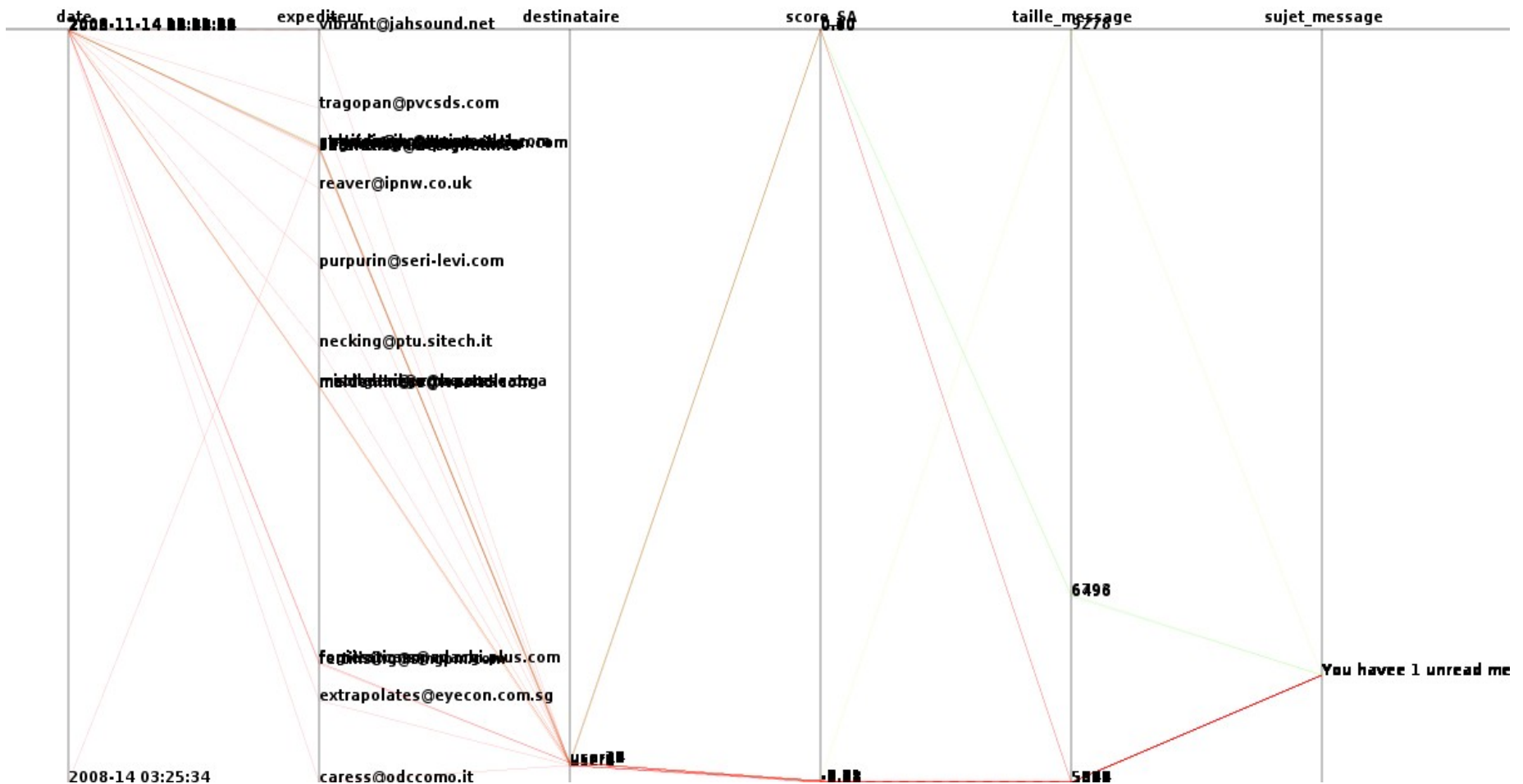
- Un mel arrive , une fonction de hashage le traite

Et une requête part vers un serveur pour vérifier que

Ce hashcode n'est pas connu comme celui d'un SPAM

Exemple : Pyzor, Razor

# Problème : un SPAM ca varie beaucoup!



# Milter un protocole pour le filtrage

- **API** permettant d'interfacer des filtres à chaque point du dialogue SMTP. Les filtres peuvent être écrits dans un langage quelconque ( C, Python, Perl...).
- Les filtres retournent (**callbacks**) à sendmail des ordres de continuer , rejeter , abandonner... les messages ou les connections.
- Postfix aussi supporte Milter

# Milters

**milter.org**

An interactive catalog of sendmail mail filters

[Login or Create an Account](#) ▶

[Catalog](#)

[Add](#)

[Developers](#)

[Lists](#)

[Search](#)

## Find a Milter

### Categories

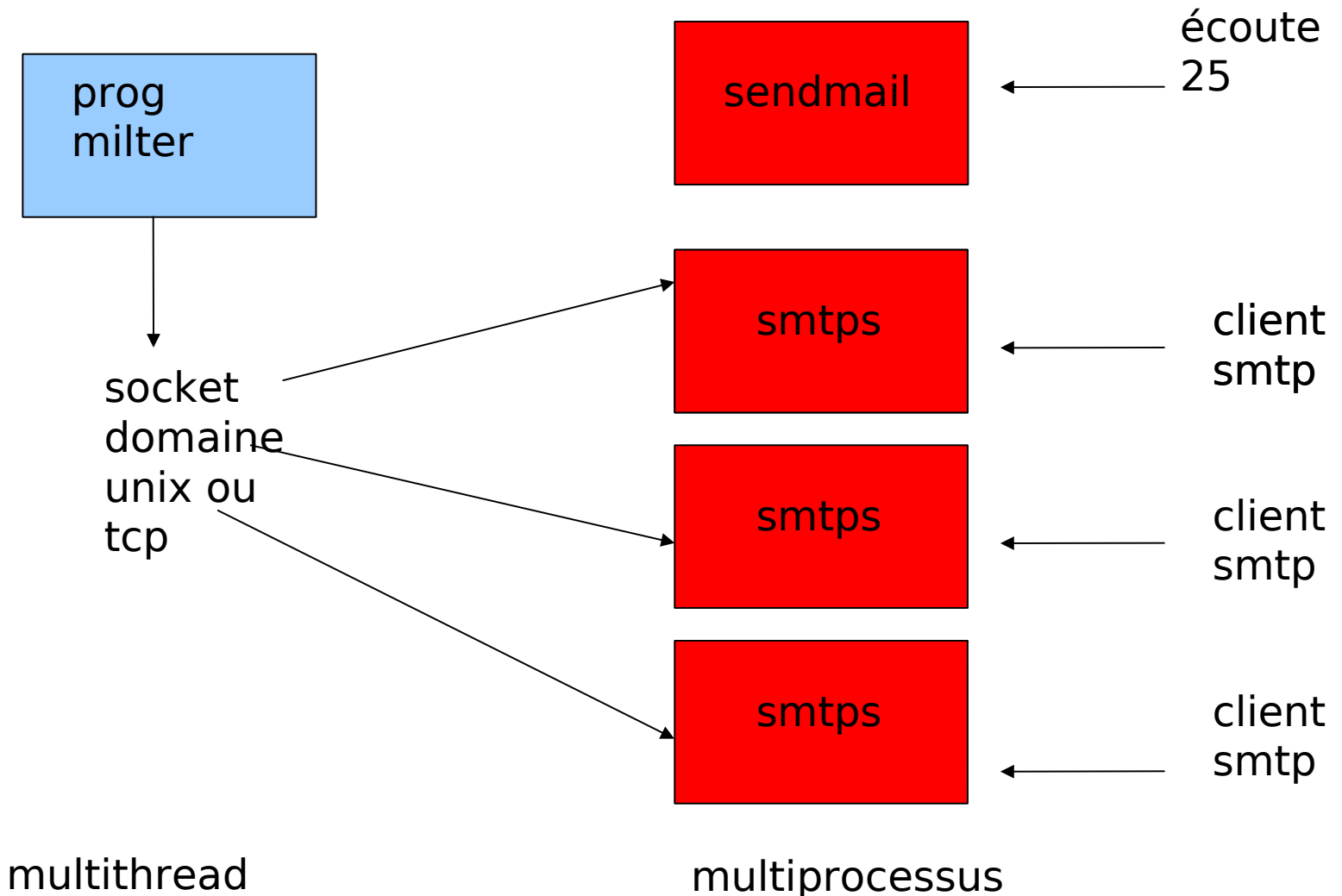
Select the categories it must be under:

- ☒ Anti-Spam
- ☐ Anti-Virus
- ☐ Archiving
- ☐ Content Mods
- ☐ Content Monitoring
- ☐ Developer
- ☐ Disclaimer
- ☐ Encryption
- ☒ Logging
- ☐ Other
- ☐ Security
- ☐ Signature/Verify
- ☐ Statistics
- ☐ Traffic Shaping

## Search Results: 7 Milters Found [\[perma link\]](#)

Name	Rating	Downloads	Updated	License
<a href="#">mailfromd</a>	★★★★★	2814	3 January 2010	<a href="#">Open Source: GPL</a>
<a href="#">MIMEDefang</a>	★★★★★	1076	3 January 2010	<a href="#">Open Source: GPL</a>
<a href="#">j-chkmail</a>	★★★★★	1991	3 January 2010	<a href="#">Open Source: GPL</a>
<a href="#">milter-callback</a>	★★★★★	271	1 January 2010	<a href="#">Open Source: GPL</a>
<a href="#">Spamilter</a>	★★★★★	358	1 January 2010	Open Source: BSD
<a href="#">milter-p0f</a>	★★★★★	246	2 January 2010	Other
<a href="#">milter-cli</a>	★★★★★	379	1 January 2010	Other

# Milter avec sendmail 8



# Le roi du scoring: Spamassassin

- **Spamassassin** est utilisé en version 3.2.5  
Produit sous licence apache.
- Il « **score** » le message en fonction de règles qui rajoutent ou enlèvent des points.
- Il est développé en PERL et à ce titre peut appeler d'autres modules PERL.

# Exemple de règles Spamassassin

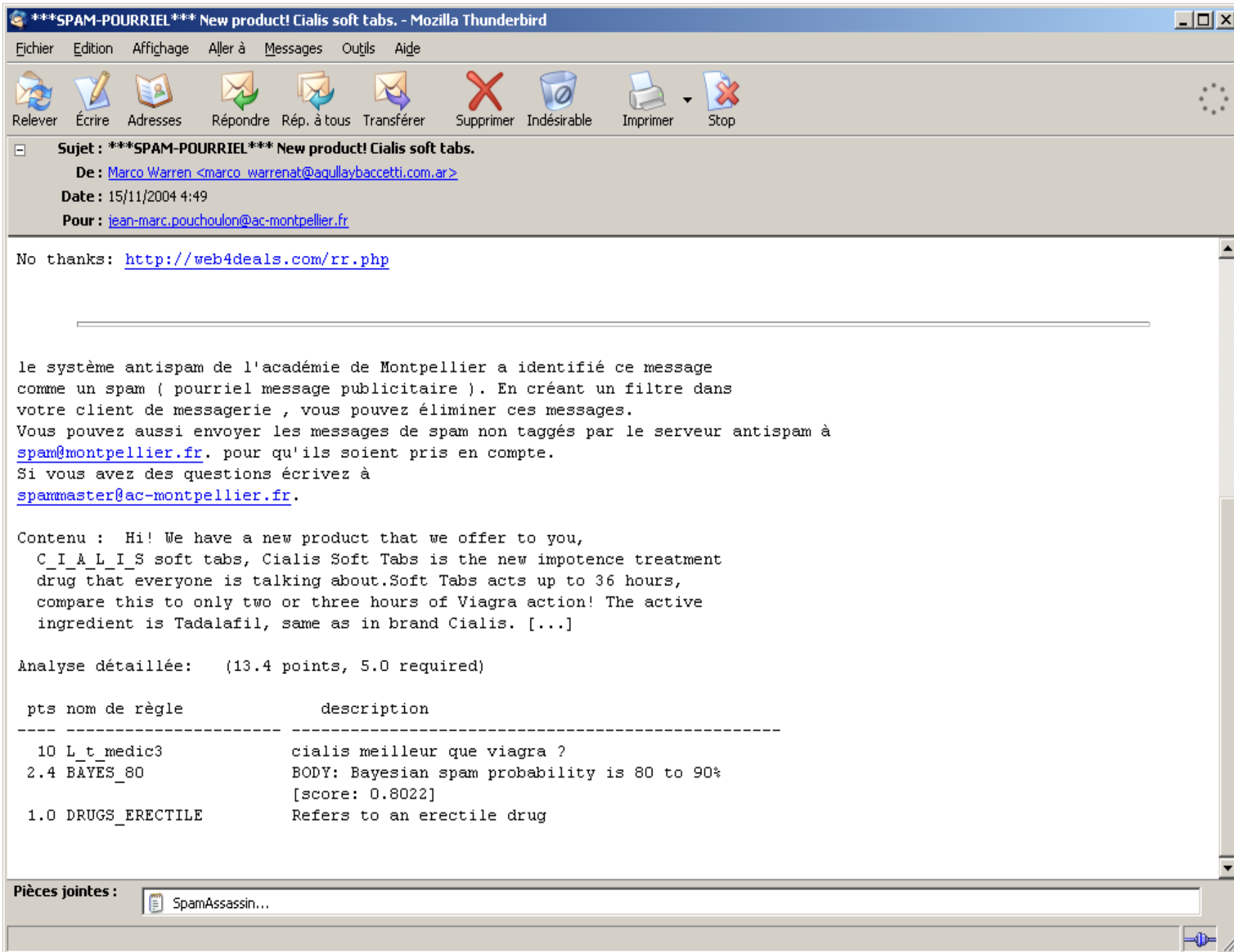
Regex sur le corps ou l'en-tête:

**header** L\_t\_medic1 Subject =~ /All your  
Prescripti\#on needs right here/i

**score** L\_t\_medic1 10.0

**describe** L\_t\_medic1

Un grand nombre de règles est fourni.





# Méthodes de lutte: SPF

Authentification d'un courrier via le dns ( cette machine est t-elle déclarée dans le dns comme pouvant envoyer du courrier dans le domaine expéditeur ?).

Exemple : **SPF** et ses dérivés

- Problème les spammeurs peuvent créer leurs propres enregistrements. Il faut donc que les listes noires soient très rapidement mise à jour
- le forwarding il faut réécrire les adresses des expéditeurs.

# SPF avec SA

Peu être utiliser comme un des critères de décisions :  
Permet à **SA** d'augmenter le score d'un message avec un domaine référencé et à Milter-Greylist de ne pas greylist l'envoi.

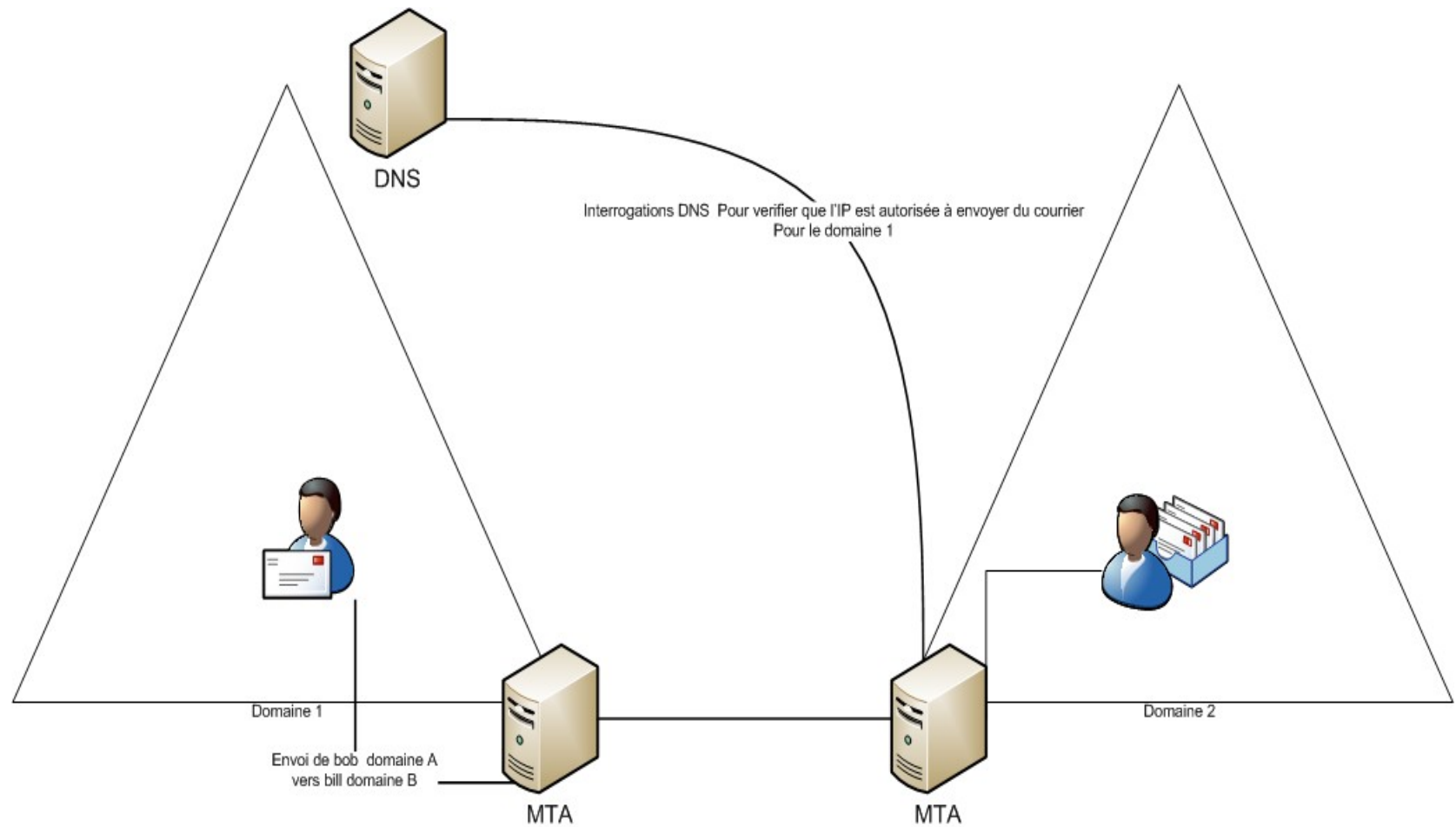
# SPF dans le DNS

; record antispam

```
ac-montpellier.fr. IN TXT "v=spf1 mx ptr -all"  
renater.ac-montpellier.fr. I TXT "v=spf1 a -all"  
renater3.ac-montpellier.fr. IN TXT "v=spf1 a -all"  
renater4.ac-montpellier.fr. IN TXT "v=spf1 a -all"
```

Ce qui indique que nous envoyons des messages depuis depuis nos MX.

# SPF

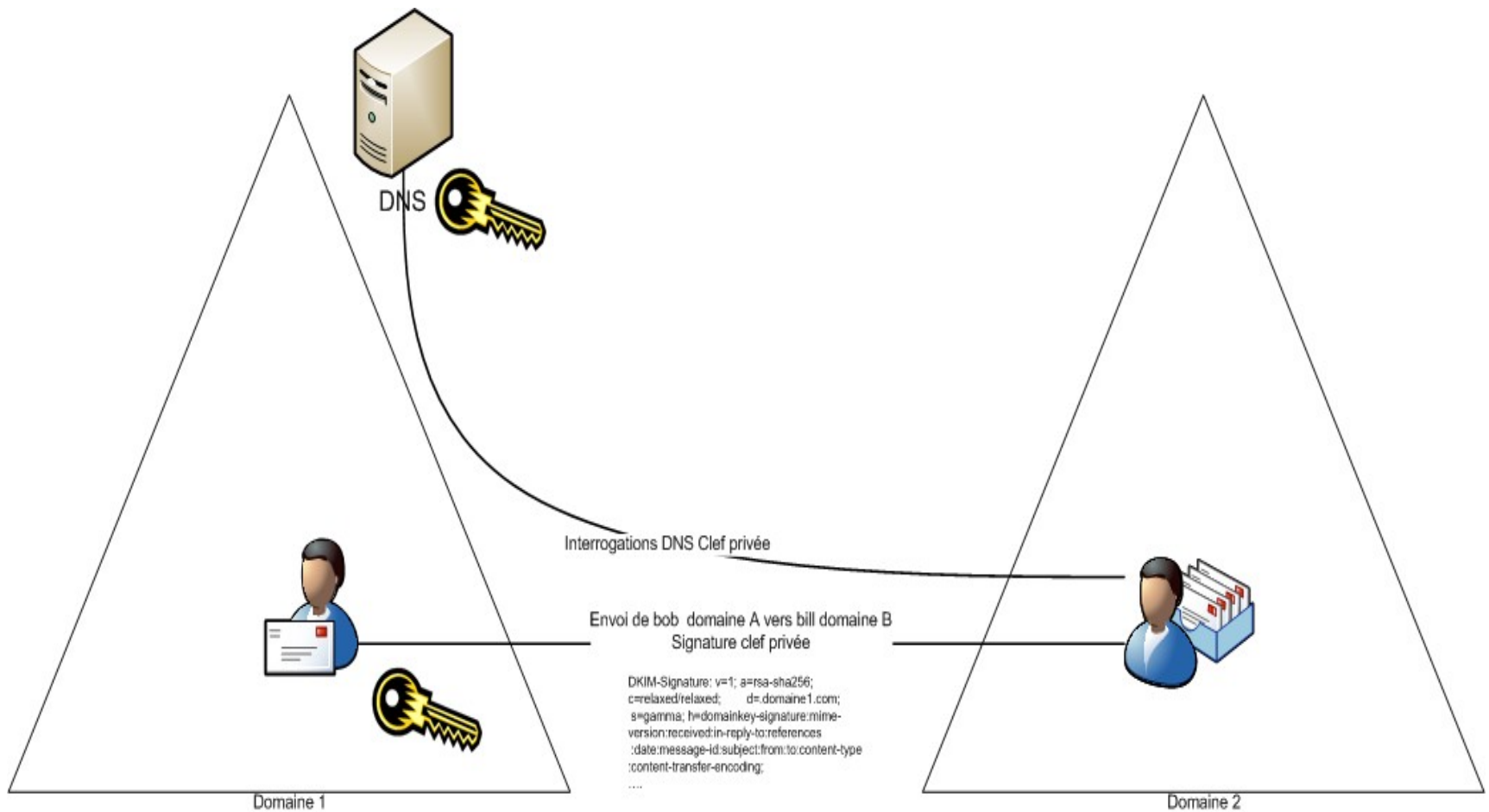


# DKIM

Signature des messages et des en-têtes ( en particulier from ) :

Au dns on dépose la clef publique , le mta signe avec la clef privée. La clef publique est stockées au dns et permet la vérification de la signature.

# DKIM



# DKIM

- Problèmes avec les listes de diffusion
- Les spammeurs ont été les premiers utilisateurs de DKIM
- Si on signe tout les messages , on peut signer aussi l'envoi de SPAM d'un Zombie appartenant à notre domaine

# GreyList.



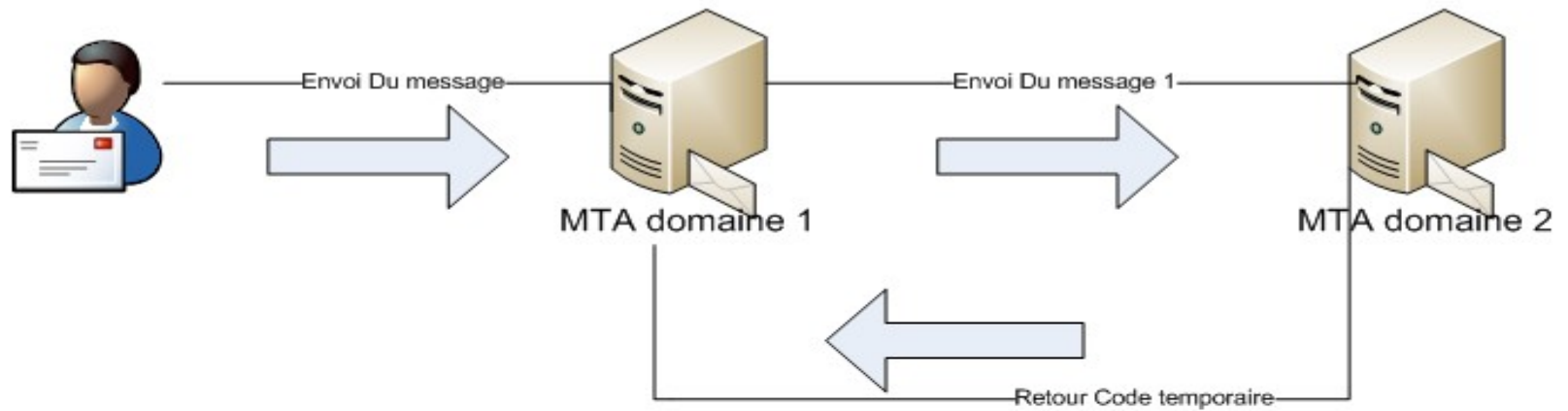
Le mécanisme :

- 1 Envoi du message par le serveur 1 , de l'utilisateur 1 vers l'utilisateur 2.
- 2 Refus du message avec un code indiquant un refus temporaire ( 4XX)
- 3 Ré-envoi du message par le serveur 1 et acceptation par le domaine de l'utilisateur 2

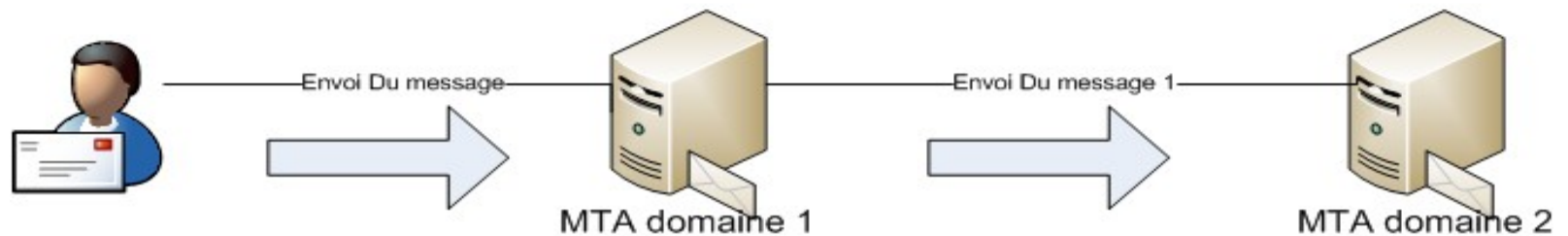


# Greylist

Première émission



Ré-émission et nouveau message



# milter-greylist: Mécanismes d'ajustements

- Seul le premier message est greylisté
- Problème des fermes de serveurs.
- Utilisation de white listing obligatoire, trop sensible pour les utilisateurs de retarder les messages.
- Importance de la fréquence de lecture des files d'attentes.

# Milter-greylist: Bilan

---

**Très efficace** pour le moment (depuis 5 ans ). Il a divisé par 10 le nombre de spams recus ! Il y a 0,003% des messages taggés par SA. Je suis passé personnellement de 300 SPAMS par semaine à 0.

# Le greylist différentiel avec milter-greylist

Faire une greylist différente en fonction:

**de l'adresse ip du MTA expéditeur:** On peut par exemple appliquer une pénalité de 12 heures pour les MTA dont l'IP est en liste noire.

**En fonction du pays expéditeur,** si le pays est connu pour abriter de nombreux spammeurs.

Pour le moment le greylist reste assez efficace sans cette dernière fonctionnalité.

# Origine des envois par pays sur une semaine avant greylist (Académie Montpellier)



United States : 20.44 %  
France : 9.97 %  
Germany : 7.36 %  
Poland : 5.24 %  
United Kingdom : 4.75 %  
Russian Federation : 3.70 %  
Korea, Republic of : 3.65 %  
China : 3.31 %  
Brazil : 2.68 %  
Spain : 2.51 %  
Italy : 2.44 %  
Israel : 2.16 %

# Origine des envois par pays après greylist

France : 79.31 %

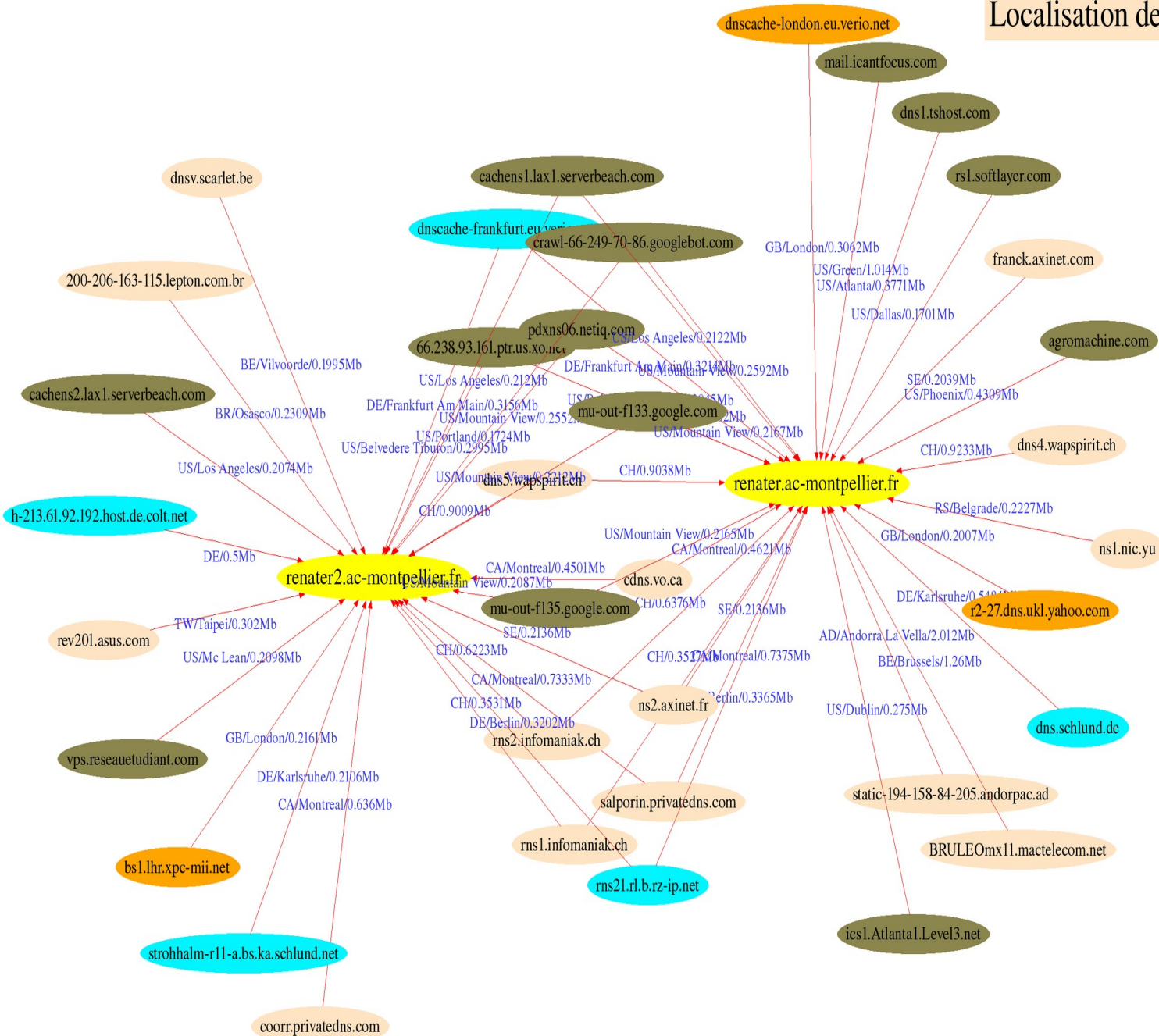
United States : 19.70 %

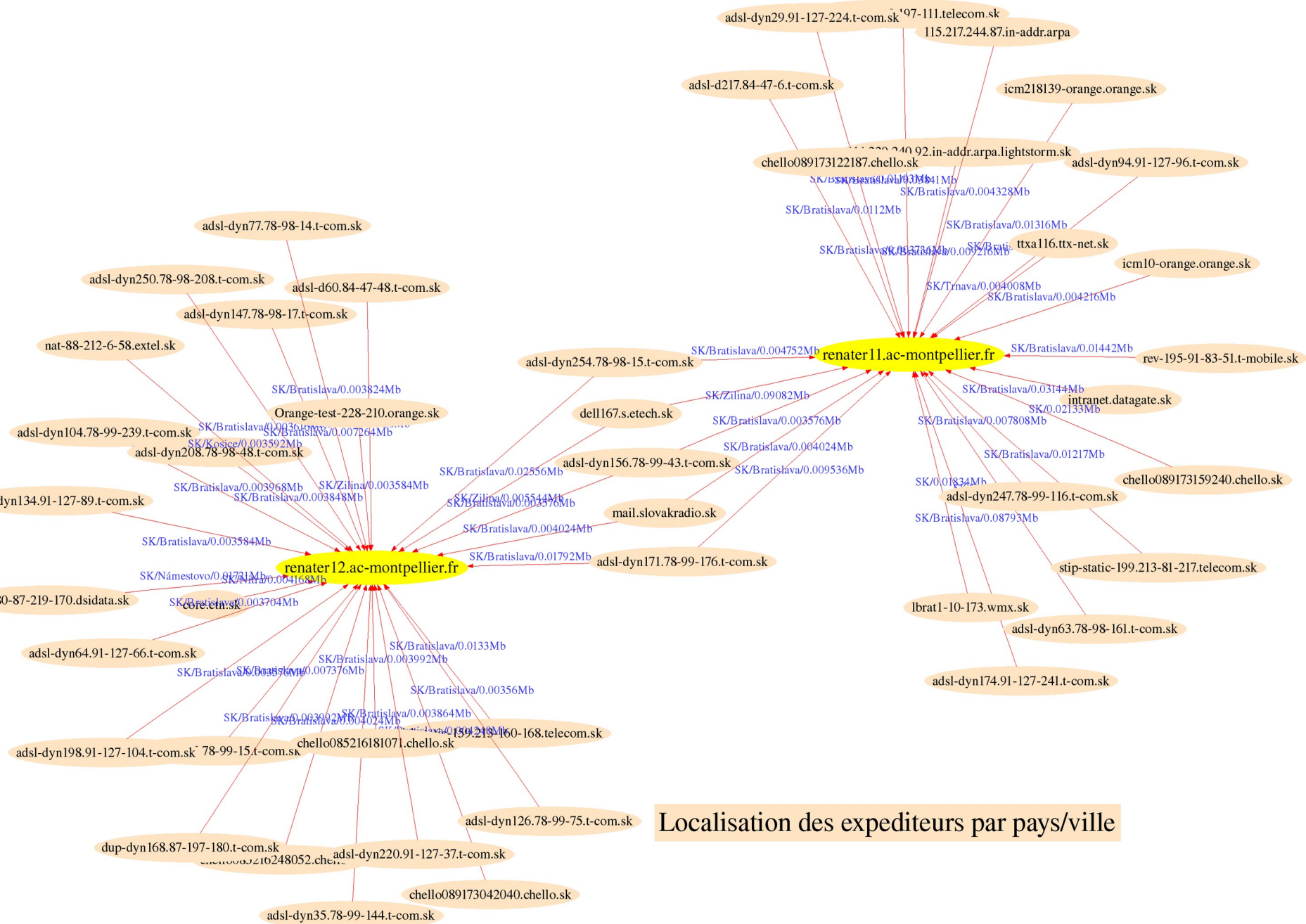
None : 0.49 %

Madagascar : 0.25 %

Andorra : 0.25 %

## Localisation des expéditeurs par pays/ville







# Limiter les flux: Un exemple avec le MTA sendmail

En version 8.13. sendmail contient des outils spécifiques pour l'antispam ( but ralentir les spammeurs pour tuer leur modèle économique )

- **ratecontrol** ( taux max de connexions par unité de temps )
- **conncontrol** (Nombre max de connexions par client smtp)
- **greetpause** ( temps d'affichage du message 220 de bienvenue)
- **Bad\_rcpt\_throttle** ( Permet de ralentir les attaques par dictionnaires ).

# Bloquer le SPAM avec le DNS: ex sendmail 8.14

- **Block\_bad\_helo** ( nom donné dans le ehlo/helo comme invalide ou appartenant à notre domaine ac-montpellier.fr ).
- **Badmx** ( verification de la presence d'un mx pour le domaine envoyeur )
- **Require\_rdns** (Vérification du reverse dns )

# Filtres Bayesiens

- La probabilité d'avoir le mot « viagra » dans un SPAM ou un HAM n'est pas la même. Il sera beaucoup plus fréquent dans un SPAM.
- Si on classifie les mels en SPAM et HAM on pourra en déduire cette probabilité.
- On arrive ensuite à scorer le message en fonction de son contenu.
- En réaction les spammeurs ont inventés les SPAMS images / pdf ...

# Lutte contre les SPAMs images et SPAM pdf avec des OCR.

TRADING ALERT!  
BREAKING NEWS ALERT ISSUED!!!

Trade Date: Friday, November 17, 2006  
Company: PRG Group Inc.  
Symbol: PRGJ  
Current Price: \$1.15  
3-Day Target: \$5  
Rating: 10/10  
Recommendation: STRONG BUY

## NEWS RELEASE:

Nov 16 2006, 1:02PM ATWEC Technologies Establishes a National Call Center. PRG Group Inc. will manage the call center and provide network services. Multinational PRG Group (PINKSHEETS: PRGJ) is publicly traded, and a total solutions provider of web-based applications, hosting services and network management. The company is partnered with IBM and Siebel ebusiness to provide its clients with the most up-to-date software, databases and networking tools.

When this Stock moves - WATCH OUT! Remember this is a STRONG BUY RECOMMENDATION ...

# Fuzzy OCR

- C'est un plugin perl de SPAM assassin qui va appeler des moteurs ocr.
- Il permet de retrouver des mots clefs dans les images.
- Une fois l'image scannée son empreinte est stockée dans une base de données my sql pour éviter de la rescanner.
- Les spammeurs tentent de contourner le filtre avec des images qui trompent les moteurs OCR.

# Bilan des méthodes

- **Greylist** est très efficace ( diminution par 10 du nombre de spams et de virus)mais pour combien de temps ?
- **Spf** est à utiliser en conjonction avec spamassassin ( diminue le score des messages) et greylist.
- Dkim est promu par la communauté actuellement.
- Le **mix** des méthodes est toujours nécessaires mais vaut mieux rejeter les messages en amont.



# Cryptographie avec la messagerie

# Authentication et Cryptage

---

- L'authentification des utilisateurs est indispensable pour les **Road Warriors** (Utilisateurs Itinérants )
- Elle permet d'autoriser le relay vers d'autres domaines sans utiliser de VPN.

Ne pas confondre authentification et cryptage.



# Authentication AUTH

## 3 « AUTH »:

- **Celui proposé par le serveur**

250-localhost.localdomain Hello root@localhost, pleased to meet you

250-ENHANCEDSTATUSCODES

250-PIPELINING

250-8BITMIME

250-SIZE

250-DSN

**250-AUTH GSSAPI DIGEST-MD5 CRAM-MD5**

avertit que le protocole AUTH est supporté.

- **AUTH méthode\_authentication** est la commande passée par le client pour l'authentification.

# Protocoles de sécurité

- **STARTTLS** RFC 2487 extension de service smtp pour du smtp sécurisé qui s'appuie sur TLS.
- **TLS** RFC 2246 protocole qui fournit des communications cryptées entre deux MTA.
- **AUTH** RFC 2254 extension du service SMTP pour l'authentification, qui définit le protocole AUTH qui sert à identifier les extrémités dans un échange de messageries électroniques.
- **SASL** RFC 2222 définit une méthode générale pour ajouter l'authentification à des protocoles orientés connexions tel que SMTP.

Sendmail intègre AUTH et STARTTLS mais dépend du système pour TLS et SASL.

# starttls

**Starttls** s'appuie sur TLS, basé sur SSL. TLS utilise la cryptographie à clefs publiques.

Sendmail propose l'extention starttls lors du dialogue smtp:

ehlo localhost

250-localhost.localdomain Hello root@localhost, pleased to meet you

250-ENHANCEDSTATUSCODES

250-PIPELINING

250-8BITMIME

250-SIZE

250-DSN

250-ETRN

250-AUTH GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN

250-STARTTLS

250-DELIVERBY

250 HELP

**STARTTLS**

220 2.0.0 **Ready to start TLS**

# starttls

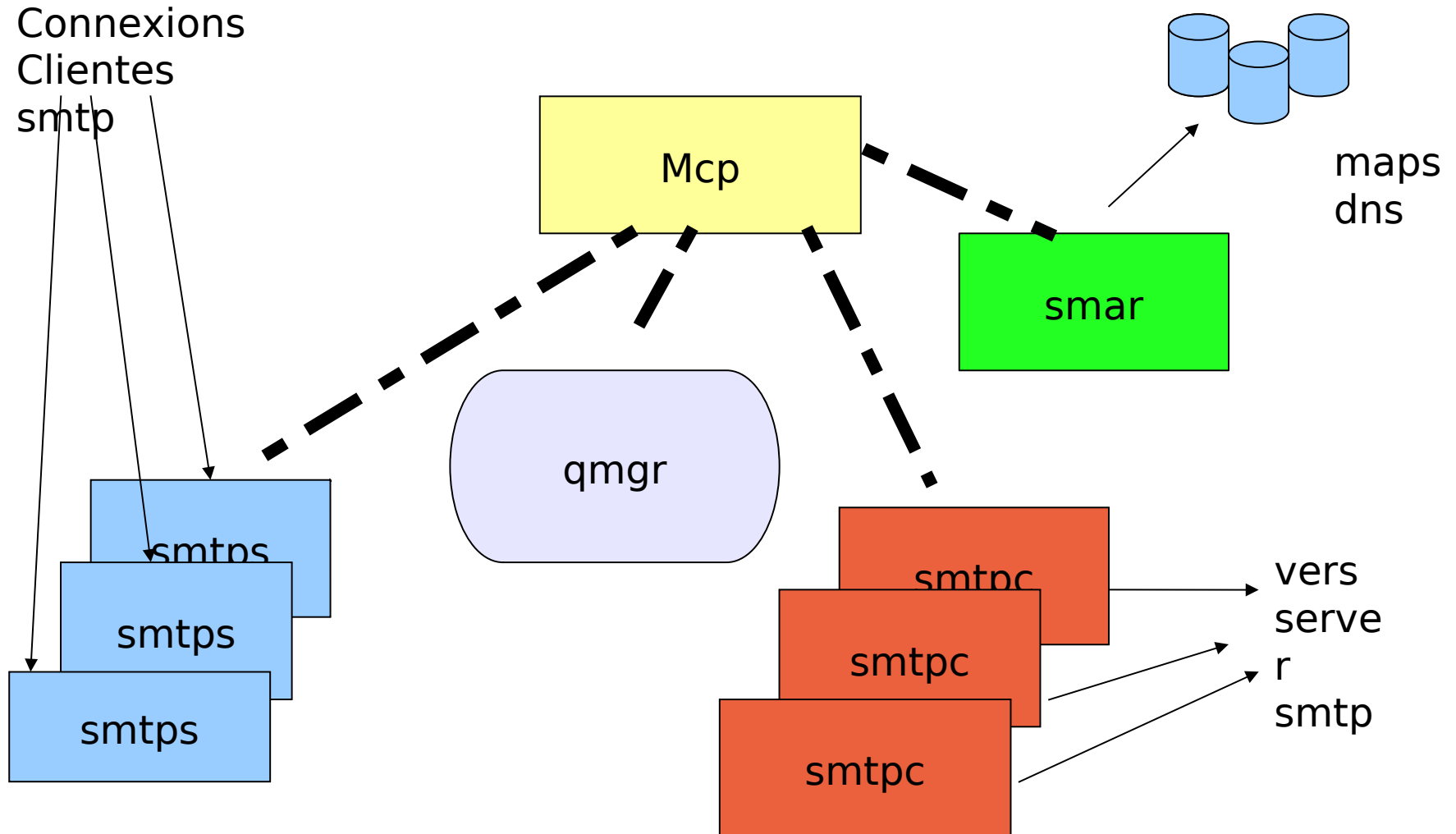
Starttls peut :

- **Verifier** l'identité du client ou du serveur lors de la transmission
- **Encrypter** la transmission des mails
- **Authentifier** un utilisateur pour autoriser le relais (comme AUTH)

# Spécialisation du MTA: ex meta 1

- Le processus de spécialisation est une caractéristique de l'informatique.
- Meta 1 est le plus récent des MTA et il est intéressant à étudier pour cela même son adoption est très restreinte

# Architecture meta1



# Modules meta1

- **MCP** (Master Control Program): C'est le chef d'orchestre, il démarre et relance les autres modules. Seul module fonctionnant sous root.
- **SMTPS** (smtp server) : Il réceptionne les message. Il peut avoir plusieurs instances (écoute sur différents ports, ip avec des fonctionnalités différentes ).
- **SMTPC** (smtp client) : Il distribue les messages aux autres serveurs smtp , lmtpt ou en local.
- **QMGR** (file d'attente manager ) : Il est chargé de la gestion de la file d'attente des messages en sortie, et en particulier de l'ordonnancement de leur traitement.
- **SMAR** (sendmail address resolver): il résout les adresses (alias + IP ) C'est aussi un cache.