Plan du cours

Services de Messagerie asynchrone sur Internet

(le courrier électronique)

Service de messagerie

But du service:

Permettre un échange de messages numériques en mode asynchrone

Service de messagerie

Supports et formes diverses:

Réseau local → intégré au SE (ex: Unix)

Internet → serveur smtp, pop, imap…

Téléphonie mobile → protocole sms sur GSM

(sms canal signalisation GSM contrairement aux MMS utilisant un canal utilisateur donc plus coûteux)

Service de messagerie

Historiquement Normes et protocoles diverses:

Messagerie propriétaire (Lotus Notes, Microsoft Exchange…

Convergence des standards Internet: smtp(s), pop(s), imap(s)…

Service de messagerie

Différents modes de connexion:

Temps réel (synchrone, connecté):

Messagerie instantanée, Chat, IRC…

Temps différé (asynchrone, déconnecté):

Mail, Liste de discussion …Forum, diffusion…

Le service de messagerie

Dans le cadre de ce cours nous étudierons les standards de messagerie Internet:

SMTP

POP

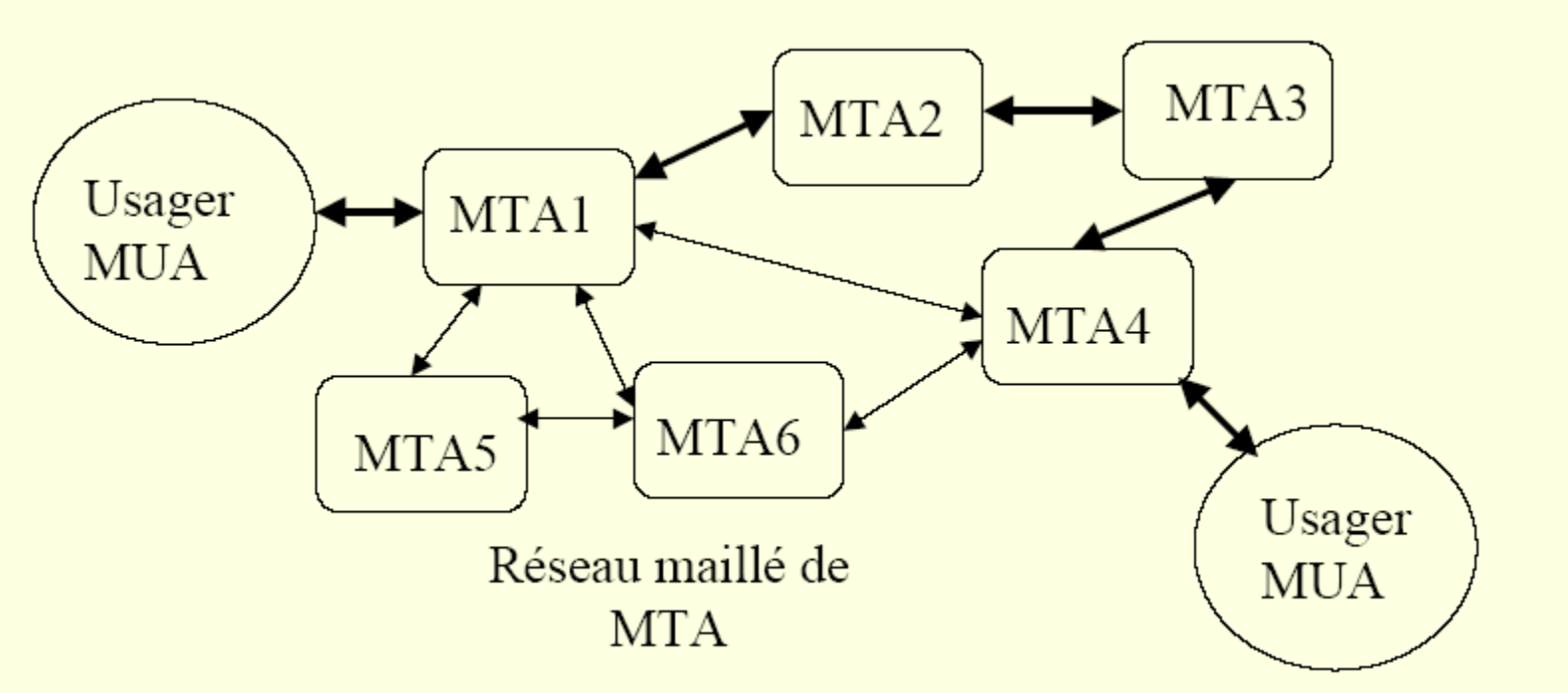
IMAP

… Les versions S sont généralement associées à un mécanisme de chiffrement supplémentaire (ex:TLS).

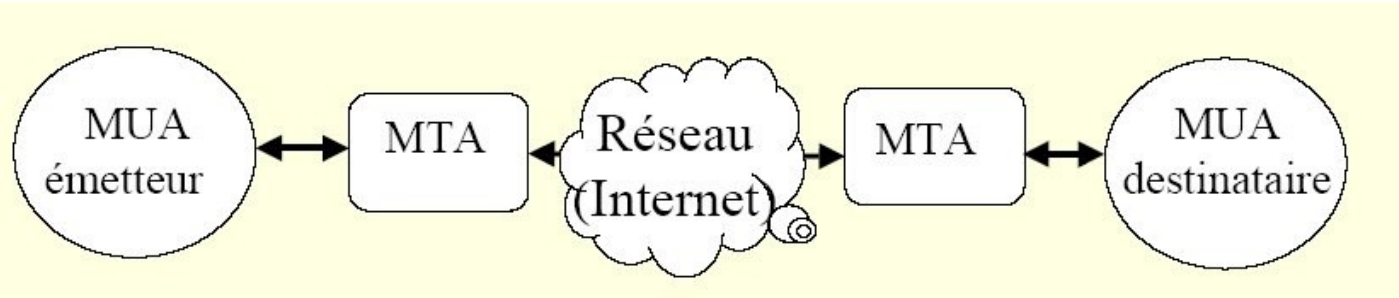
Le service de messagerie

Rappel sur les protocoles TCP/UDP IP (encapsulation protocolaire)

Le service de messagerie Internet : Échange des messages...

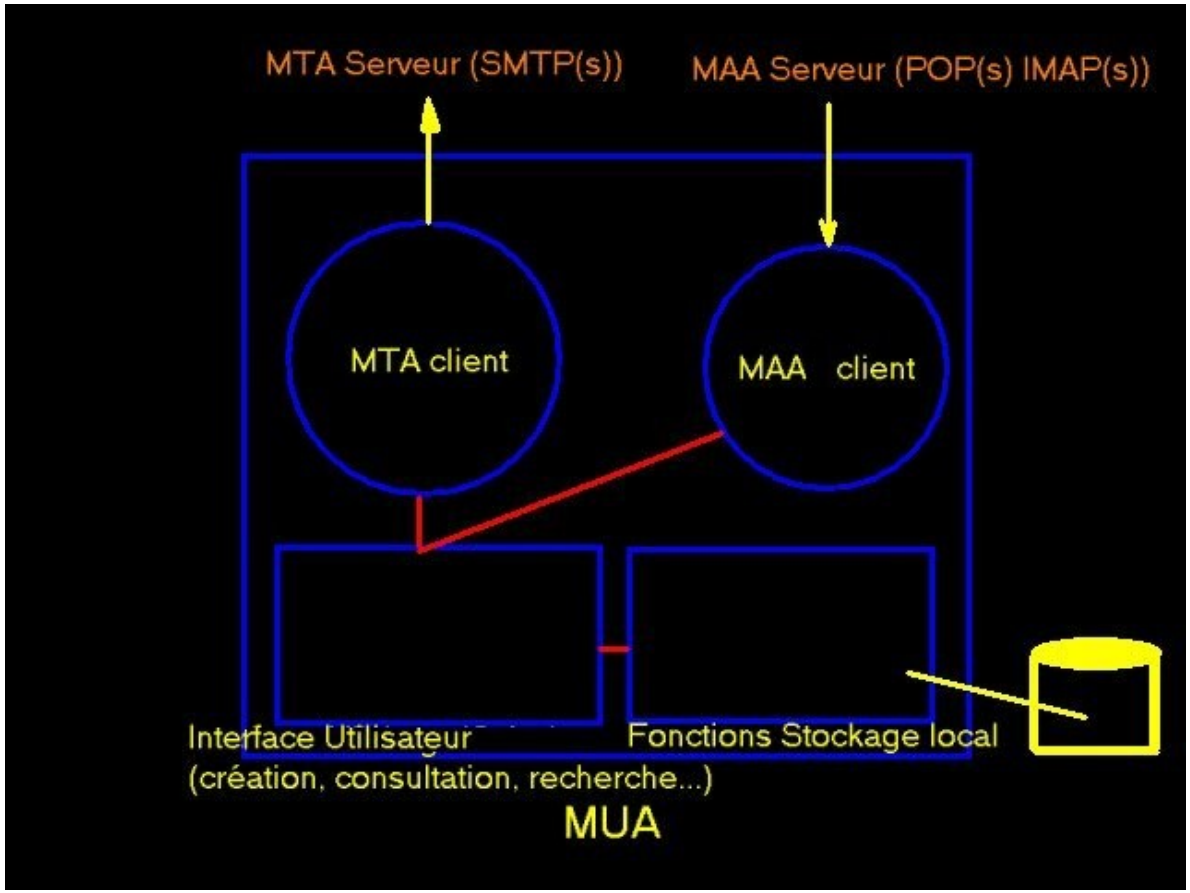


Le service de messagerie Internet
Vue externe du système

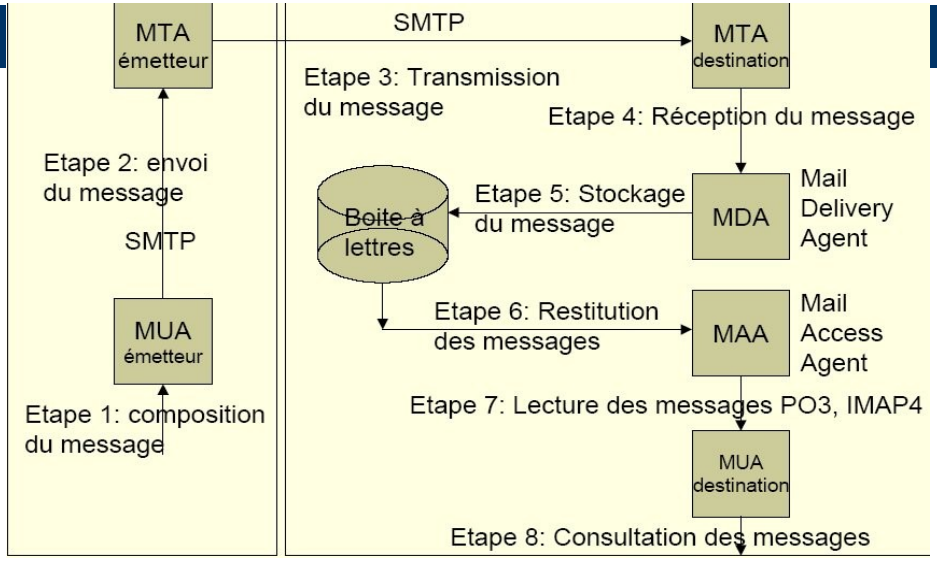


Le serveur de messagerie MTA **achemine directement un message** entre un émetteur et un destinataire. (Généralement via une Résolution DNS par rapport au MX du domaine destinataire) à travers Internet ou un intranet.

Le MUA


MTA Serveur (SMTP(s))
MAA Serveur (POP(s) IMAP(s))
MTA client
MAA client
Interface Utilisateur
(création, consultation, recherche...)
Fonctions Stockage local
MUA

Le service de messagerie Internet
Vue Interne du système



Le serveur de messagerie MTA **achemine directement un message** entre un émetteur et un destinataire. Des mécanismes locaux permettent le stockage et la lecture des messages. Le MDA varie en fonction de la méthode de stockage du message (Fichier, BDD, …). Le MDA est donc un agent chargé du stockage d'un message après sa réception par le MTA. Historiquement, sur les systèmes UNIX le MDA utilisait directement le fichier mail des comptes systèmes des utilisateurs pour déposer le courrier (pas de MAA particulier).

Le service de messagerie Internet
Vue externe du système

Deux notions essentielles:

1. Notion de **serveur** de messagerie (responsable d'un domaine et **commutateur** de courriers):

   -> agent de transfert de messages MTA (**'Mail Transfer Agent'**).

2. Notion de **client** de messagerie

   -> agent utilisateur de messagerie ou MUA (**'Mail User Agent'**).

3. Notions sous-jacentes : MDA (Mail Delivery Agent) stockage local des msg et MAA Mail Access Agent (serveur pour retirer les msg)

Le fonctionnement repose sur des mécanismes (protocoles) communs aux différentes entités.

(**ITU** : International Telecommunications Union http://www.itu.int/home/index-fr.html)

Le service de messagerie Internet

Etape 1: Un usager compose,avec l'aide de son client de messagerie un message (application (MUA), commande shell…)

Etape 2: Le message est transmis au MTA de l'usager (son serveur de messagerie via le protocole SMTP(s)). Le message peut passer par une succession de contrôles et de files d'attentes avant l'étape 3 (anti-virus, spams...).

Etape 3: Le message est transmis au serveur de messagerie du destinataire (après requête DNS sur champ MX du domaine).

Etape 4: Le MTA destinataire transmet le message à un agent MDA 'Mail Delivery Agent'. Le message peut passer par une succession de contrôles et de files d'attentes avant (anti-virus, spams...).

Le service de messagerie Internet

Etape 5: Le MDA stocke le courrier sur le système de stockage pour lequel il est conçu (fichier système, BDD...). C'est la configuration du MTA qui précise le MDA à utiliser (routage des messages).

Etape 6: Le destinataire dans le cadre d'un protocole de relève **POP** ou **IMAP** (généralement à travers son MUA) relève ses messages de sa boite à lettre via le **MAA ('Mail Access Agent (serveur) pop(s) imap(s)').** Sur les systèmes UNIX, il n'existait pas de MAA car le message était directement déposé dans le fichier mail du compte système de l'utilisateur UNIX par le MDA.

Etape 7: Les messages sont transmis au client de messagerie utilisateur (protocoles POP ou IMAP) relevé via son **Mail Access Agent (*Client)***. Il sont stockés dans des boites à lettre client (système de stockage de l'application ex : fichiers indexés…).

Etape 8: Le destinataire consulte ses messages en utilisant son interface cliente de messagerie (MUA). Le MUA est donc une interface pour créer, consulter ses messages et également un client MTA et un client MAA pour envoyer et retirer ses messages.

Le service de messagerie Internet

Les principaux protocoles de messagerie de l'Internet

Simple Mail Transfer Protocol (SMTP) (RFC 821)

Le protocole basé sur des messages de format textes qui définit les échanges entre serveurs de messagerie.

Extended Simple Mail Transfer Protocol (ESMTP) (RFC 1869)

Une évolution de SMTP qui définit des commandes supplémentaires.

Light Mail Transfer Protocol (LMTP)

Une Version Légère de SMTP pour l'échange rapide de msg entre 2 MTA sur un même réseau généralement (MTA Domaine vers MTA AV vers MTA Spams...)

Post Office Protocol (POP) : Un protocole de base de relève de courrier pour le dialogue entre un client de messagerie MUA et un serveur de messagerie dans sa partie MAA. (généralement pop3)

Internet Message Access Protocol (IMAP): Un autre protocole de relève qui offre des possibilités plus larges que POP (gestion des archives de courrier, limitation des volumes de données échangées …) (généralement imap 4)

Acronymes :

Le MUA (Mail User Agent) permet à l'utilisateur de composer, d'envoyer son mail (en utilisant le protocole smtp), de retirer son courrier (en utilisant le protocole pop ou imap). (MUA=MAA+MTA)

Le MAA (Mail Access Agent) va permettre au MUA d'accéder à sa boite à lettre. (serveur POP ou IMAP ex:qpopper (protocole POP3), courrier_imap (POP et IMAP), uw_Pop et uw_IMAP (université de Washington).

Le MTA (Mail Transfert Agent) va permettre au MUA d'envoyer ses mails. Il va également acheminer les messages vers les MTA destinataires. (serveur SMTP).

Le MDA (Mail Delevery Agent côté serveur) va permettre principalement l'enregistrement d'un message reçu localement ou via le réseau sur le système de messagerie (sur une arborescence de fichiers, dans une BDD…)

Adresses de messagerie

Les adresses utilisées dans l'Internet étaient initialement définies par la RFC 822, puis amendées par la RFC 1123. Par la suite, la RFC 2822 a rajeuni ces spécifications.

- Il n'y a pas de distinction entre minuscules et majuscules dans les adresses (sauf dans les commentaires ou les chaînes de caractères).

Quelques exemples concernant ces spécifications dans les diapos suivantes…

Adresses de messagerie

Adresses globales

Ces adresses sont qualifiées de globales car elles spécifient un site sans spécifier de chemin pour y arriver.

En cela, elles sont valides à n'importe quel point de l'Internet.

Exemple:

jdupond @ entreprise.fr
Il peut y avoir des espaces entre les différents constituants de l'adresse.

Adresses de messagerie

jdupond (Jean Dupond) @ entreprise.fr

La même adresse, mais avec un commentaire (entre parenthèses) insérée à n'importe quel point dans l'adresse.

Le commentaire est ignoré par l'agent de routage pour la prise de décision (mais il doit être laissé dans l'adresse).

Adresses de messagerie

"Jean Dupond"@entreprise.fr

La partie locale de l'adresse (entre guillemets) est considérée comme un seul mot. Le courrier est donc adressé à l'utilisateur
« Jean Dupond » dans le domaine entreprise.fr.

Adresses de messagerie

Jean Dupond <jdupond@entreprise.fr>

Dans ce cas, un commentaire (sans parenthèses) est ajouté à l'adresse.

Un programme privilégie ce qui est entre les caractères « < » et « > » et ignore tout le reste (mais laisse le commentaire).

Adresses de messagerie

"Jean Dupond" **<jdupond@entreprise.fr>**

Cette fois-ci, le commentaire est, au niveau syntaxique, un mot unique puisqu'il est placé entre guillemets. .

Adresses de messagerie

adresses littérales

jdupond @ [134.157.0.129]

La présence des crochets indique une adresse numérique, qui doit être prise telle quelle. Le courrier doit donc être envoyé à la machine d'adresse indiquée sans autre forme de traitement (en particulier, sans tenir compte des MX).

→ Les adresses littérales sont déconseillées. Le transfert peut fonctionner mais le message est refusé à l'arrivée.

Structure du message et de son enveloppe

Comme pour le courrier traditionnel, il existe des normes de construction pour l'enveloppe et le courrier lui-même.

Structure du message

Comment est construit un courrier postal traditionnel ?

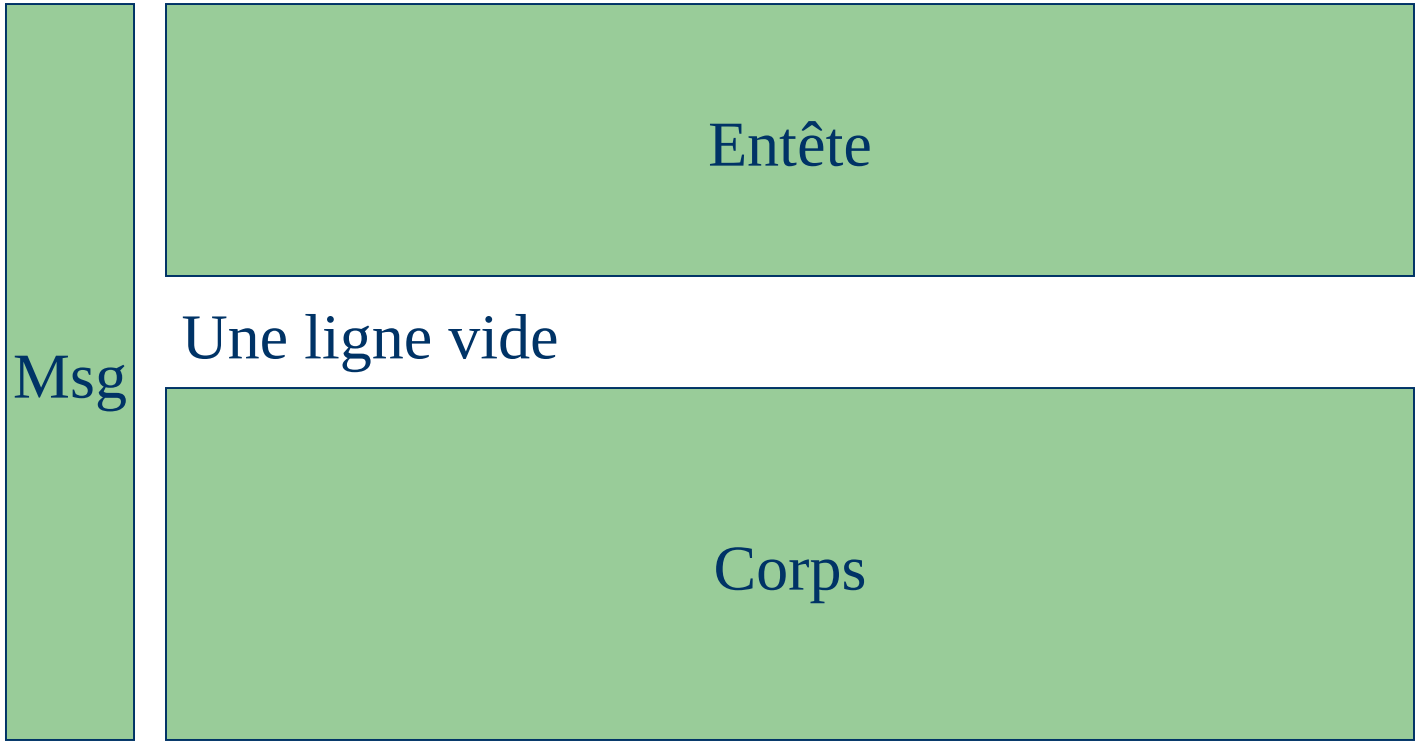
Le courrier numérique est calqué sur ce modèle...

- Une **enveloppe** avec ses informations
- Le **contenu** composé de l'entête et du corps du message.

Structure du message

1. Un entête (ou en-tête)
2. Un corps

Structure du message



Structure du message

Le corps est le contenu du message proprement dit. Il est séparé de l'en-tête par au moins une ligne vide.

Pendant longtemps, le contenu du corps n'était réglementé que par la RFC 2821 (lignes de 1000 caractères au maximum et caractères tronqués à 7 bits).

Le standard MIME définit dorénavant une structure pour le corps.

Structure du message

un en-tête

L'en-tête est une suite de champs, définis par la RFC 2822 placé avant le corps est séparé par au moins une ligne vide.

Structure du message

Chaque champ d'en-tête est constitué d'un mot-clef, du caractère « : », et des informations du champ. Si un champ est trop long, il peut continuer sur la ou les ligne(s) suivante(s). Dans ce cas, chaque ligne de continuation doit **commencer par un espace ou une tabulation**.

Les champs d'en-tête standardisés1.1

Les caractères suivants ont une signification particulière dans les champs:

Caractère	Signification
\	le caractère qui suit est spécial
« ……. »	pas d'interprétation à l'intérieur

Les champs d'en-tête standardisés1.1

Return-Path

Ajouté lors de la remise physique du message, c'est-à-dire lors du dépôt dans la boîte aux lettres finale par le dernier agent de transport, pour identifier le routage vers l'expéditeur ; **l'adresse qui est indiquée est celle de l'expéditeur réel « écrite » sur l'enveloppe** (l'émetteur réel, propriétaire d'une liste…);

Les champs d'en-tête standardisés1.1

Received

Ajouté par chaque agent de routage le long du chemin emprunté par le message pour signer et tracer ce chemin en cas de problème.

Comporte différentes informations.

Les champs d'en-tête standardisés1.1

Chaque agent apporte des informations complémentaires à RECEIVED:

from	site émetteur
by	site récepteur
via	chemin physique
with	protocole utilisé
id	identification du message pour le récepteur
for	forme initiale

Les champs d'en-tête standardisés1.1

Exemple:

Received: **from** sympa.ac-amiens.fr (sympa2.ac-amiens.fr [194.199.46.76]) **by** licorne.ac-amiens.fr (Netscape Messaging Server 4.15) **with** ESMTP id **IFLIAQ00.A0C**; Wed, 27 Apr 2005 10:01:38 +0200

Received: from smtp.ac-amiens.fr (localhost [127.0.0.1]) by smtp-out.ac-amiens.fr (Postfix) with ESMTP id AC8F018C108; Wed, 27 Apr 2005 09:42:49 +0200 (CEST)

...

Les champs d'en-tête standardisés1.1

From

Identité de l'expéditeur (la personne qui a souhaité que le message soit envoyé), placée par l'UA de l'émetteur. Attention à la confusion possible entre ce champ (avec caractère « : ») et la chaîne From placée dans les boîtes aux lettres par le programme de remise physique
pour séparer deux messages (utilisé par exemple par la commande Unix /bin/mail).
Ces deux chaînes sont proches, mais ont un sens différent (le premier est un champ d'en-tête, véhiculé avec le message, le deuxième est un délimiteur dans la boîte aux lettres du MUA) ;

Les champs d'en-tête standardisés1.1

Reply-To

Adresse de retour, placée par l'expéditeur, utilisée par le destinataire pour les réponses.

Si ce champ n'est pas spécifié, From est pris par défaut;

En cas d’utilisation du « *Répondre* » dans le MUA c’est vers cette adresse que l’on enverra le message de réponse.

Les champs d'en-tête standardisés1.1

Date

Date d'expédition, placée par l'UA de l'expéditeur :
jour de la semaine optionnel
quantième (2 chiffres)
mois (3 lettres)
année (4 chiffres)
heure
fuseau horaire
Exemple : Date: Fri, 23 Nov 2001 09:30:15 +0100

Les champs d'en-tête standardisés1.1

To

Destinataires principaux du message, spécifiés par l'expéditeur à l'aide de son UA ; (généralement utilisé par le répondre à Tous)

Exemple:

To: reseau@ac-amiens.fr, Claudine Less <claudine.less@ac-amiens.fr>, Christophe.vande@ac-amiens.fr

Les champs d'en-tête standardisés1.1

Cc (carbon copy)

Destinataires auxiliaires du message, spécifiés par l'expéditeur à l'aide de son UA

Les champs d'en-tête standardisés1.1

Bcc (blind carbon copy) Copie cachée

Destinataires auxiliaires, spécifiés par l'expéditeur à l'aide de son UA. Ce champ n'est pas transmis aux destinataires spécifiés par To et Cc

Les champs d'en-tête standardisés1.1

Message-Id

Identificateur unique du message, placé par le premier agent de routage, servant à référencer le message. Cet identificateur est souvent constitué d'une partie unique sur l'Internet (par exemple un nom de machine) et d'une partie unique sur la machine (par exemple une date et un identificateur de processus)

Les champs d'en-tête standardisés1.1

Encrypted

Indique que le message est chiffré et spécifie la méthode utilisée

Les champs d'en-tête standardisés1.1

X-???

Les champs commençant par X- ne sont pas définis et sont réservés pour les extensions non encore standardisées :

Exemple:

X-UIDL: 9657-1096958233
X-Mozilla-Status: 0001
X-Mozilla-Status2: 10000000

X-Virus-Scanned: amavisd-new at ac-amiens.fr
X-Antivirus: avast! (VPS 0516-7, 22/04/2005), Inbound message X-Antivirus-Status: Clean

Les Extensions MIME

MIME s'occupe du contenu du message (et rien d’autre!)

MIME étend la définition de ce que contient un courrier électronique. D'un simple texte unique à l'origine, on va pouvoir définir différents types de contenus et codages à l'intérieur d'un même message.

Les Extensions MIME

MIME étend le RFC 822 dans deux directions non traitées par le RFC original:

- gestion de différents types de données (typage + codage)
- gestion des messages plus complexes contenant plusieurs parties (le balisage est alors nécessaire)

Les Extensions MIME

Gestion de différents types de données

Le système de courrier défini dans les documents RFC 821 et 822 ne peut transmettre que des données ASCII (American Standard Code for Interchange) codés sur 7 bits. Cela suffit pour transmettre du texte uniquement composé avec le jeu de caractères ASCII US, mais il est impossible de gérer les autres langues qui ont un jeu de caractères plus varié ou de transférer des données binaires

Les Extensions MIME

Le RFC 822 ne fournit pas beaucoup de détails concernant la description du corps d'un message. Il se concentre sur les en-têtes. MIME va permettre de combler ce manque... Il faut annoncer l'utilisation de MIME dans l'entête du message par l'ensemble des balises :

MIME-version:
Content-type:
Content-transfer-encoding:

Les Extensions MIME

MIME résout ces manques en définissant des techniques d'encodage pour transmettre diverses formes de données et en définissant une structure pour le corps du message qui permet de typer les données transportées dans le message mais aussi de transporter plusieurs objets de différents types dans un même message.

Le **RFC 1521**, définit ces en-têtes.

MIME permet de structurer, de typer, de formater et de coder les informations contenues dans le corps du message.

Les Extensions MIME

Dans le cas simple d'un seul bloc contenu dans le message, on annonce directement la version MIME, le type MIME (image/jpeg par exemple), le codage des données du message.

Dans le cas d'un message formé de plusieurs « blocs » dans le corps du message (ex des fichiers joints), on annonce de nouveau pour chacun des blocs leurs types en reprenant les différentes informations précédentes en les séparant par une balise annoncée dans l'entête.

Les Extensions MIME

Cas simple de contenu :

Dans l'entête :

MIME-version:
Content-type:
Content-transfer-encoding:

Dans le corps :

Le contenu codé conformément aux données d'entêtes

Les Extensions MIME

Dans le cas de plusieurs contenus différents (fichiers attachés...), dans l'entête on annonce plus directement le type du contenu (texte, image...) mais que le message est composé de différentes parties en nommant une balise permettant de séparée ces différentes parties.

Dans l'entête :

MIME-version: 1.0

Content-type: **multipart/mixed**; **boundary="Valeur_de_la_Balise"**

Dans le corps :

On retrouve les différents contenus balisés et caractérisés par le format MIME

"Valeur_de_la_Balise"

Content-Type:

Content-Transfer-Encoding:

Le contenu.....

"Valeur_de_la_Balise"

Content-Type:

Content-Transfer-Encoding:

Le contenu.....

...

Les Extensions MIME

Dans l'entête on annonce la balise

Content-type: multipart/mixed; boundary=----------Balise

Dans le corps, on trouve les différents contenus séparés par la balise:

----------Balise

Content-Type: image/jpeg;
 name="postfix-synoptique.jpg"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="postfix-synoptique.jpg"

/9j/4AAQSkZJRgABAQEBLAEsAAD/2wBDAAEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEB
AQEBAQEBAQICAQECAQEBAgICAgICAgICAQICAgICAgICAgL/2wBDAQEBAQEBAQEBAQECAQEB...
L8vbo0cYqH1mlSbnNunCpGDc5Nx953+v4wxmLdehh3iqjoTpwbhzy5G+aWrjezfm1c+WqKKK
/wBcz4IKKKKKACiiigAooooA//9k=
----------Balise

Les Extensions MIME

Exemple simple :

To: pascal.vaniet@ac-amiens.fr
Message-id: <4991B348.5000007@laposte.net>
MIME-version: 1.0
Content-type: text/plain; charset=ISO-8859-1; format=flowed
Content-transfer-encoding: 7bit
X-Virus-Scanned: amavisd-new at ac-amiens.fr
X-Greylist: domain auto-whitelisted by SQLgrey-1.7.4
X-ME-UUID: 20090208170241194.2F6F17000085@mwinf8401.laposte.net
X-Antivirus: avast! (VPS 090207-0, 07/02/2009), Outbound message
X-Antivirus-Status: Clean
X-me-spamlevel: not-spam
X-me-spamrating: 40.000000
User-Agent: Thunderbird 2.0.0.4 (Windows/20070604)
Original-recipient: rfc822;pascal.vaniet@ac-amiens.fr

coucou,
tu vas bien ?

A+

Les Extensions MIME

Exemple plusieurs parties :

To: 'Pascal Vaniet' <pascal.vaniet@ac-amiens.fr>
Message-id: <002601c991ce$8998e900$a90310ac@w20030801882l>
MIME-version: 1.0
X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2900.3198
X-Mailer: Microsoft Office Outlook 11
Content-type: multipart/alternative; boundary="----=_NextPart_000_0027_01C991D6.EB5D5100"
Thread-index: AcmRzoiZ2FPMl0SKRZiUU16hnaBzjQ==
X-Virus-Scanned: amavisd-new at ac-amiens.fr
Original-recipient: rfc822;pascal.vaniet@ac-amiens.fr

This is a multi-part message in MIME format.

------=_NextPart_000_0027_01C991D6.EB5D5100
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Bonjour Pascal,
=20
M. Revelle me demande ou on en est pour le vpn ?
Christophe
------=_NextPart_000_0027_01C991D6.EB5D5100
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
<html xmlns:o=3D"urn:schemas-microsoft-com:office:office" =
xmlns:w=3D"urn:schemas-microsoft-com:office:word" =
xmlns=3D"http://www.w3.org/TR/REC-html40">
<head>
<meta http-equiv=3DContent-Type content=3D"text/html; =
charset=3Diso-8859-1">
</body>
</html>
------=_NextPart_000_0027_01C991D6.EB5D5100--

Les Extensions MIME

Autre exemple plusieurs parties :

Dans l'entête:

MIME-version: 1.0
Content-type: multipart/mixed; boundary="Boundary_(ID_wjCbSXnz0BIazBEaWifUIQ)"

********Dans l'entête le content-type identifie les propriétés de l'ensemble du corps du message**

Dans le corps:

********* Dans le corps on caractérise uniquement la partie balisée.**
This is a multi-part message in MIME format.

--Boundary_(ID_wjCbSXnz0BIazBEaWifUIQ)
Content-type: text/plain; charset=ISO-8859-1; format=flowed
Content-transfer-encoding: 8BIT

Voici les fichiers…

--Boundary_(ID_wjCbSXnz0BIazBEaWifUIQ)
Content-type: text/plain; name=logs-9-jours.txt
Content-transfer-encoding: 7BIT
Content-disposition: inline; filename=logs-9-jours.txt

Recherche adresse 213.188.129.183 dans access.log.1...
Recherche adresse 216.104.161.217 dans access.log.1...

--Boundary_(ID_wjCbSXnz0BIazBEaWifUIQ)
Content-type: image/jpeg; name=nikon1.jpg
Content-transfer-encoding: base64
Content-disposition: inline; filename=nikon1.jpg

/9j/4AAQSkZJRgABAQAAAQABAAD/4QBDRXhpZgAATU0AKgAAAAgAAQAPAAIAAAAhAAAAGgAA
…
AUUUUAf/2Q==

Les Extensions MIME: **Content-Type**

Content-Type définit le type des données incluses dans les messages.

Cet en-tête possède un champ « Subtype » qui permet de spécialiser la définition du type.

Bon nombre de sous-type ont été définis depuis la diffusion du RFC initial.

Les Extensions MIME: **Content-Type**

Quelques types et sous types (RFC 2045, 2046 et 2077):

text / plain, enriched, css, html…
Application / msexcel, pdf, rtf, x-csh…
Image / gif, jpeg…
Vidéo / mpeg, quicktime, x-msvideo, quicktime…
Audio / x-midi, x-wav, x-aiff...
Multipart (données composites)/ related, digest, encrypted…
Message / news, http…
…

Les Extensions MIME: **Content-Type**

Exemples:

text/plain
: pour les textes non formatés. Il faut noter qu'un courrier à l'ancienne mode (RFC 2822) est implicitement compris comme text/plain ;

text/enriched
: pour les textes comportant des directives de formatage.

Ces extensions peuvent être suivies par des paramètres.

→ voir RFC 2110

Les Extensions MIME: **Content-Type**

Exemple de paramètres:

Content-Type: text/plain; charset=ISO-8859-1; format=flowed

Le type particulier **Multipart**

- multipart

  Ce type est spécial, il spécifie qu'un message contient en réalité plusieurs sous-messages. Par exemple, un courrier peut contenir un texte, une image et un son. Le message a le type et le sous-type multipart/mixed. Le paramètre boundary= spécifie une chaîne de caractères dont le but est de séparer chaque sous-partie du message (définition d'une balise).

  Chaque sous-partie est composée d'une en-tête miniature spécifiant à nouveau un type et un sous-type MIME (text/plain, Image/ gif…)

Le type particulier **Multipart**

multipart/mixed :

les différents constituants sont indépendants et sont présentés par l'UA du destinataire dans l'ordre dans lequel ils sont placés dans le message ;

Le type particulier **Multipart**

multipart/alternative :

tous les constituants contiennent la même information, seule la présentation diffère. En fonction de ses capacités, l'UA du destinataire affiche le constituant « au mieux ». L'exemple typique est un texte envoyé en text/plain classique, en text/enriched avec des indications de formatage, et en application/postscript. L'utilisateur choisit la version la plus lisible pour lui (en fonction des options ou du matériel: texte normal s'il lit son courrier sur un Minitel (;-))), postscript s'il a un écran X11 avec un *previewer* PostScript, par exemple).

Le type particulier **Multipart**

multipart/digest :

Comparable à multipart/mixed, à ceci-près que chaque constituant est lui-même un courrier électronique.

multipart/parallel :

les différents constituants sont présentés simultanément à l'utilisateur. C'est typiquement le cas d'une image affichée en même temps que sa légende (un texte) et accompagnée d'un son.

Le type particulier **Multipart**

multipart/related :

les différents composants constituent un seul et même document, comme par exemple un texte HTML et des icônes associées.

(voir RFC 2112).

Le type particulier **Multipart**

Une partie d'un message multipart peut également être du type multipart. On obtient ainsi des messages qui peuvent être relativement complexes.

Exercice:

imaginer le mécanisme pour un contenu multipart mixed et pour chacun multipart alternative (entête et corps)

Les Extensions MIME: **Content-Transfer-Encoding**

L'en-tête Content-Transfer-Encoding identifie le type d'encodage utilisé pour transmettre les données.

Les Extensions MIME: **Content-Transfer-Encoding**

Codage	Informations sur	Codée sur	Transportable avec
`7bit`	7 bits	7 bits	SMTP
`quoted-printable`	8 bits	7 bits	SMTP
`base64`	8 bits	7 bits	SMTP
`8bit`	8 bits	8 bits	ESMTP/8bits
`binary`	8 bits	8 bits	ESMTP/binaire
x-token	N/A	N/A	N/A

Les Extensions MIME: **Content-Transfer-Encoding**

Exemple:

Content-Type: application/octet-stream; name=« test.wmv"
Content-Disposition: attachment; filename=« test.wmv"
Content-Transfer-Encoding: base64

MCaydY5mzxGm2QCqAGLObK4KAAAAAAAACAAAAAECQKTQ0gfj0hGX8ACgyV6oUOoAAAAAAAAABQAa
AEEAcwBwAGUAYwB0AFIAYQB0AGkAbwBYAAAAAwAEAAEAAAAaAEEAcwBwAGUAYwB0AFIAYQB0AGkA
bwBZAAAAAwAEAAEAAAAcAFcATQBGAFMARABLAFYAZQByAHMAaQBvAG4AAAAAABoAOQAuADAAMAAu
ADAAMAAuADMAMgA1ADAAAAAaAFcATQBGAFMARABLAE4AZQBlAGQAZQBkAAAAAAAWADAALgAwAC4A
MAAuADAAMAAwADAAAAAMAEkAcwBWAEIAUgAAAAIABAAAAAAAodyrjEepzxGO5ADADCBTZWgAAAAA
AAAAPkOhy5C9eUaCl+cjWcn4+r7oCgAAAAA8H9R9DMOxQHtAQAAAAAAAMCKvxMAAAAA8FqiEgAA
AAC4CwAAAAAAAIAAACkBQAApAUAANbUAgC1A79fLqnPEY7jAMAMIFNlEwcAAAAAAAR0tOruqnP
EY7mAMAMIFNlBgDlBgAAqUZDfODv/EuyKTk+3kFchSEAAAA

Les Extensions MIME: **Content-Transfer-Encoding**

quoted-printable:

> Ce codage consiste, en simplifiant quelque peu, à transformer les rares caractères accentués en une séquence équivalente n'utilisant que des caractères sur 7 bits ; cette transformation est faite en réécrivant un caractère en trois caractères : « = », puis les deux chiffres hexadécimaux du code du caractère

Exemple:

Content-Transfer-Encoding: quoted-printable

Voila une grande pens=E9e pleine de sagesse …

Les Extensions MIME: **Content-Transfer-Encoding**

base64:

Ce codage est comparable au codage uuencode traditionnel sous Unix (paquet sharutils ubuntu): il consiste à coder 3 octets dans 4, autrement dit découper 24 bits consécutifs (3 x 8) en 4 paquets de 6 bits, 6 bits suffisant pour représenter un caractère dans un alphabet commun à toutes les machines de la création. La taille maximale d'une ligne pour ce type de données est de 76 caractères. base64 permet de coder des fichiers binaires avec une surcharge (*overhead*) relativement faible par rapport au codage quoted-printable.

Les Extensions MIME: **Content-Transfer-Encoding**

Exemple base64:

Content-Type: text/plain; charset="iso-8859-1"

Content-Transfer-Encoding: base64

ICAgSmUgbmUgdm91cyBsZSBjb25zZWlsbGUgcGFzICBjYXIgdW4gbGluZXIgZXN0IGFzc2V6IGZy
YWdpbGUgZXN0IHVuZSBzaW1wbGUgYXNwZXJpdOkgbCdlbmRvbWFnZXJhaXQgcmFwaWRlbWVudC4N
Cl9fX19fX19fX19fX19fX19fX0FsYWluX19fX19fX19fX19fX19fX18N
Cg0KPlVuZSBkZXJuaehyZSBxdWVzdGlvbiBldCBqZSBuZSB2b3VzIGVtYup0ZSBwbHVzIC4uLiBw
cm9taXMhDQo+DQo+amUgcGVuc2UgbWV0dHJlIHVuIGxpbmVyIHBsdXT0dCBxdWUgZGUgY2FybGVy
…

Les Extensions MIME: **Content-Transfer-Encoding**

X-token

Cette extension permet aux développeurs de définir leur propre système d'encodage. Dans ce cas, le nom de la technique d'encodage doit être fourni avec une en-tête de la forme X-. De plus le lecteur de courrier doit avoir une référence à l'extension.

Exemple:

Content-Transfer-Encoding: x-mon-codage

Ou

Content-Transfer-Encoding: x-uuencode

Exercice

Déchiffrer le code source du message.

Enveloppe d’un message

Entre 2 MTA le message (entête + corps) est envoyé dans une enveloppe créée par le MTA émetteur. (Généralement commandes SMTP entre 2 MTA)

→ Pourquoi ?

Enveloppe d’un message

Si le champ To (de l’entête), était utilisé pour acheminer le message jusqu'à sa destination, cela poserait quelques problèmes:

Exemple :

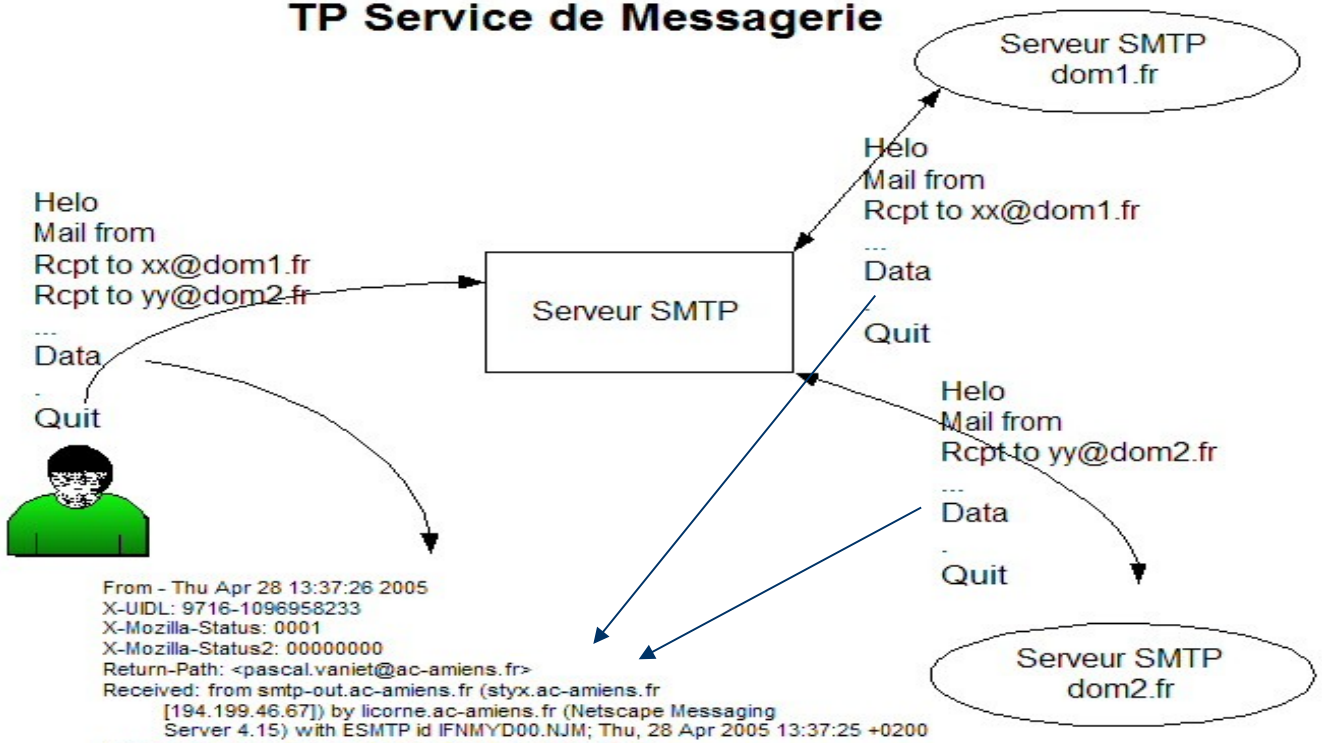
From: paul@unice.fr To: jdupond@entreprise.fr, jacques@urec.fr

Ce message est envoyé à partir du site unice.fr (From). Si le champ To est utilisé, le message est envoyé à entreprise.fr et à urec.fr. Qui vont à leur tour analyser les champs « to » est renvoyer vers entreprise.fr pour urec.fr et urec.fr pour entreprise.fr et ainsi de suite... Pour éviter ces boucles de courrier, comme pour le courrier postal on va utiliser une enveloppe par destinataire.

Enveloppe d’un message

Cette enveloppe est immatérielle : elle n'est pas stockée dans le message lorsqu'il est dans la boîte aux lettres. Elle est créée au cours de la phase de connexion entre MUA/MTA ou MTA/MTA à travers les commandes SMTP.

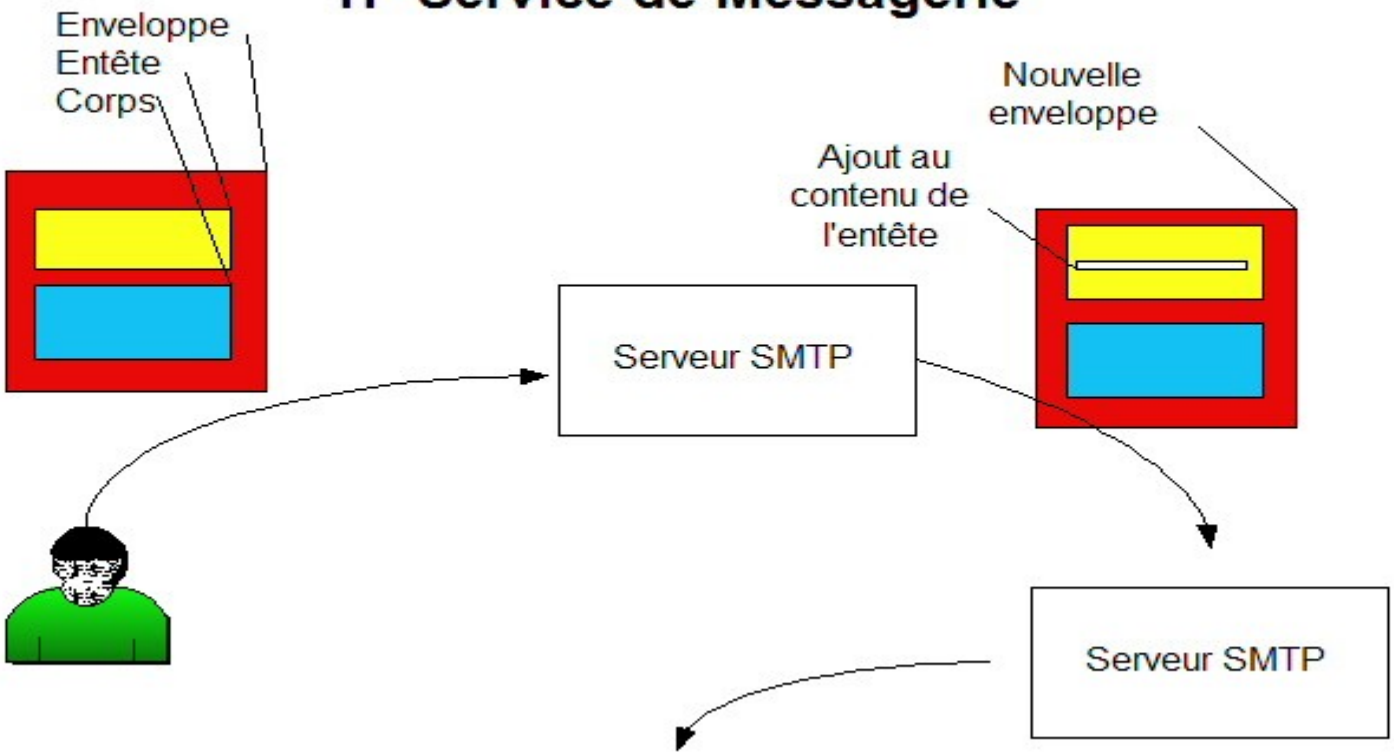
TP Service de Messagerie




```
From - Thu Apr 28 13:37:26 2005
X-UIDL: 9716-1096958233
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Return-Path: <pascal.vaniet@ac-amiens.fr>
Received: from smtp-out.ac-amiens.fr (styx.ac-amiens.fr
        [194.199.46.67]) by licorne.ac-amiens.fr (Netscape Messaging
        Server 4.15) with ESMTP id IFNMYD00.NJM; Thu, 28 Apr 2005 13:37:25 +0200
Received: from smtp.ac-amiens.fr (localhost [127.0.0.1])
             by smtp-out.ac-amiens.fr (Postfix) with ESMTP id 4A3E9182B53;
             Thu, 28 Apr 2005 13:37:25 +0200 (CEST)
Received: from localhost (localhost [127.0.0.1])
             by smtp.ac-amiens.fr (Postfix) with ESMTP id 2C90517C529;
             Thu, 28 Apr 2005 13:37:25 +0200 (CEST)
Received: from smtp.ac-amiens.fr ([127.0.0.1])
 by localhost (styx.ac-amiens.fr [127.0.0.1]) (amavisd-new, port 10024)
 with ESMTP id 22776-01; Thu, 28 Apr 2005 13:37:23 +0200 (CEST)
Received: from [127.0.0.1] (nat-pascal.ac-amiens.fr [194.199.47.19])
             by smtp.ac-amiens.fr (Postfix) with ESMTP id 53BB218E382;
             Thu, 28 Apr 2005 13:37:23 +0200 (CEST)
Message-ID: <4270CAF3.6070005@ac-amiens.fr>
Date: Thu, 28 Apr 2005 13:37:23 +0200
From: pascal vaniet <pascal.vaniet@ac-amiens.fr>
User-Agent: Mozilla Thunderbird 0.6 (Windows/20040502)
X-Accept-Language: fr, en
MIME-Version: 1.0
To: Pascal Vaniet <xx@domain1.fr>, yy@domain2.fr
Subject: test
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit


test
```

TP Service de Messagerie



Protocole SMTP

Simple Mail Transfert Protocol : protocole simple de transfert de courrier.

SMTP est un protocole de niveau application (comme http) qui va permettre l'échange des messages électroniques.

A l'origine elle est défini dans la RFC 821, puis amendé par certaines autres RFC donc la RFC 1123.

La version étendue est ESMTP, E pour Extended.(RFC 2821)

Protocole SMTP

Les implémentations de SMTP conformes à la RFC 821 initiale doivent avoir :

- Le messages sur 7 bits (tronqués explicitement à 7 bits)
- Le nom d'utilisateur < 64 caractères
- Le nom de domaine < 64 caractères
- Le nombre de destinataires < 100
- Les lignes < 1000 caractères

ESMTP apporte plus de fonctionnalités.

Protocole SMTP: les commandes principales

Commande	Syntaxe	Fonction
Hello	HELO <*machine émettrice*>	Identité SMTP
From	MAIL FROM: <*adresse provenance*>	Adresse expéditeur
Recipient	RCPT TO: <*adresse destination*>	Adresse destinataire
Data	DATA	Début du message
Reset	RSET	Annulation du message
Verify	VRFY<*chaîne*>	Vérification du nom de l'utilisateur
Expand	EXPN<*chaîne*>	Expansion liste de diffusion
Help	HELP[*chaîne*]	Demande d'aide en ligne
Quit	QUIT	Fin de session SMTP

Protocole ESMTP: les commandes principales

Mot clef	RFC	Extension
8BITMIME	1652	Accepte les données binaires 8 bits
CHUNKING	1830	Accepte les messages coupés en morceaux
CHECKPOINT	1845	Vérification et relance de la transaction si nécessaire
PIPELINING	1854	Accepte plusieurs commandes en un seul envoi
SIZE	1870	Donne la taille maximale autorisée des messages
DSN	1891	Fournit un acquittement de réception du message
ETRN	1985	Accepte les requêtes de traitement de file distants
ENHANCEDSTATUSCODES	2034	Fournit des codes d'erreurs améliorés

Les commandes SMTP / ESMTP

Liste complète (avec réf RFC) sur:

http://www.networksorcery.com/enp/protocol/smtp.htm

Protocole SMTP

Avec la commande EHLO le serveur renvoie les commandes ESMTP gérées par le serveur. Les commandes commençant par un X ne sont pas standardisées.

Exemple:

Connect host smtp.ac-amiens.fr

EHLO pvaniet

250-smtp.ac-amiens.fr

250-PIPELINING

250-SIZE 10240000

250-VRFY

250-ETRN

250 8BITMIME

Protocole SMTP

VRFY pvaniet@ac-amiens.fr

252 pvaniet@ac-amiens.fr

VRFY totor@ac-amiens.fr

550 <totor@ac-amiens.fr>: Recipient address rejected: User unknown in relay recipient table

Google: smtp reply code:
http://www.greenend.org.uk/rjk/2000/05/21/smtp-replies.html

SMTP Reply Codes

Différents types de réponses serveur
Code réponse (trois chiffres décimaux) et explication textuelle.
xyz <Texte explicatif> <CRLF>

1yz: Commande acceptée mais nécessite une demande d'action supplémentaire en reply (?!?)
(Ex Aucun…)
2yz: Requête satisfaite (action terminée)
(Ex 250 action completed)
3yz: Commande acceptée en attente d'infos complémentaires
(Ex Après une commande DATA « code 354 » en attente du contenu du message)
4xy: La commande à échouée temporairement
(Ex 452: Requested action not taken: insufficient system storage)
5yz: Réponse négative (commande échouée)

x0z: Syntaxe
x2z: Etat de la connexion
x5z: Etat du système de messagerie

SMTP Reply Codes

Code	Description
211	System status, or system help reply.
214	Help message.
220	*Domain* service ready. Ready to start TLS.
221	*Domain* service closing transmission channel.
250	OK, queuing for node *node* started. Requested mail action okay, completed.
251	OK, no messages waiting for node *node*. User not local, will forward to *forwardpath*.
252	OK, pending messages for node *node* started. Cannot VRFY user (e.g., info is not local), but will take message for this user and attempt delivery.

SMTP Reply Codes

253	OK, *messages* pending messages for node *node* started.
354	Start mail input; end with <CRLF>.<CRLF>.
355	Octet-offset is the transaction offset.
421	*Domain* service not available, closing transmission channel.
432	A password transition is needed.
450	Requested mail action not taken: mailbox unavailable. ATRN request refused.
451	Requested action aborted: local error in processing. Unable to process ATRN request now
452	Requested action not taken: insufficient system storage.

SMTP Reply Codes

453	You have no mail.
454	TLS not available due to temporary reason. Encryption required for requested authentication mechanism.
458	Unable to queue messages for node *node*.
459	Node *node* not allowed: *reason*.
500	Command not recognized: *command*. Syntax error.
501	Syntax error, no parameters allowed.
502	Command not implemented.
503	Bad sequence of commands.

SMTP Reply Codes

504	Command parameter not implemented.
521	*Machine* does not accept mail.
530	Must issue a STARTTLS command first. Encryption required for requested authentication mechanism.
534	Authentication mechanism is too weak.
538	Encryption required for requested authentication mechanism.
550	Requested action not taken: mailbox unavailable.
551	User not local; please try *forwardpath*.
552	Requested mail action aborted: exceeded storage allocation.
553	Requested action not taken: mailbox name not allowed.
554	Transaction failed.

SMTP sécurisé (TLS, SSL + Auth)

SMTP supporte aujourd'hui le chiffrement pendant le transfert du message et l'authentification pour la connexion.

SASL rfc 2222 et 4422, SMTP-AUTH rfc 2554

SASL:

Un mécanisme SASL est conçu comme une série de demandes d'accès et de réponses. Quelques uns des mécanismes actuellement définis sont :

"EXTERNAL", l'authentification est dérivée du contexte (par exemple pour les protocoles employant déjà IPsec ou TLS)
"ANONYMOUS, accès anonyme sans authentification.
"PLAIN", mot de passe en clair. (PLAIN rend obsolète le mécanisme LOGIN.)
"OTP", mécanisme de mot de passe à usage unique. (OTP rend obsolète le mécanisme SKEY.)
"SKEY", mécanisme de mot de passe à usage unique S/KEY.
"CRAM-MD5", mécanisme basé sur HMAC-MD5.
"DIGEST-MD5", mécanisme basé sur MD5 et compatible HTTP. (DIGEST-MD5 fournit une couche d'intégrité des données.)
"NTLM", mécanisme d'authentification pour réseau local NT.
"GSSAPI", pour l'authentification Kerberos V via GSSAPI. (GSSAPI fournit une couche d'intégrité des données.)

Un ensemble de mécanismes SASL est conçu de manière à pouvoir reconnaître n'importe quel mécanisme GSSAPI.

SMTP sécurisé (TLS, SSL + Auth)

Configuration pour l'université :

- IMAP (réception/consultation de mail) :
  serveur : imap.u-picardie.fr
  port : 143 (STARTTLS) ou 993 (SSL)
  mot de passe envoyé en clair dans le tunnel sécurisé (TLS ou SSL)

- SMTP (envoi de mail) :
  serveur : smtp.u-picardie.fr
  port : 587 (STARTTLS) ou 465 (SSL)
  mot de passe envoyé en clair dans le tunnel sécurisé (TLS ou SSL)

SMTP et DNS

Pour router les courriers, un serveur de messagerie se base sur les champs de type MX du serveur de noms du domaine de l'adresse destinataire.

Tout cela est définit par la RFC 974

Les champs de type MX permettent aussi d'indiquer des serveurs de secours.
Exemple:
Toto@domaine.fr
Dans le DNS de la zone domaine.fr:
IN MX 10 mailhost1.domaine.fr
IN MX 20 mailhost2.domaine.fr

SMTP et DNS

Exemple:

```
> set query=MX
> free.fr
Serveur :  etoile.in.ac-amiens.fr
Address:  172.30.177.253

Réponse ne faisant pas autorité :
free.fr MX preference = 40, mail exchanger = mx1-1.free.fr
free.fr MX preference = 10, mail exchanger = mx.free.fr
free.fr MX preference = 30, mail exchanger = mrelay1-2.free.fr
free.fr MX preference = 30, mail exchanger = mrelay2-1.free.fr
free.fr MX preference = 30, mail exchanger = mrelay2-2.free.fr

free.fr nameserver = freens1-a.free.fr
free.fr nameserver = freens1-1.free.fr
mx.free.fr       internet address = 212.27.42.18
mx.free.fr       internet address = 212.27.42.19
mx.free.fr       internet address = 212.27.42.20
mx.free.fr       internet address = 212.27.42.21
mx.free.fr       internet address = 212.27.42.22
mx.free.fr       internet address = 213.228.0.199
mrelay1-2.free.fr        internet address = 212.27.42.17
mrelay2-1.free.fr        internet address = 212.27.42.15
mrelay2-2.free.fr        internet address = 212.27.42.16
mx1-1.free.fr    internet address = 213.228.0.65
freens1-a.free.fr        internet address = 213.228.0.82
freens1-1.free.fr        internet address = 213.228.0.198
>
```

POP3 Post Office Protocol

Le protocole de relève le plus simple.

→ RFC 1939

L’inconvénient c’est qu’il ne gère pas les archives de courrier sur le serveur.

POP3 Post Office Protocol

Messages POP3 principaux:

" USER Fourniture du nom de la boite à lettre
" PASS Fourniture du mot de passe en clair
" APOP Fourniture cryptée du mot de passe
" STAT Nombre de messages dans la boite
" LIST Liste des messages présents
" RETR Transfert du message n
" DELE Marquage message pour la suppression
" LAST Numéro du dernier message consulté
" RSET Annulation des actions d’une session
" QUIT Fin de session.

IMAP4 Internet Message Access

→ RFC 2060

Protocole de relève plus complet.

- Gère les archives de courrier sur le serveur (primitives de création de dossiers et de transferts entre dossiers)
- Minimise les échanges de données sur le réseau.
- Le plus souvent utilisé en laissant les courriers dans la boite à lettre du serveur de messagerie.
- Un protocole adapté à la consultation à partir de plusieurs postes clients.

IMAP4 Internet Message Access

Messages IMAP4 principaux:

" AUTHENTICATE : Mécanisme d'authentification choisi.
" LOGIN : Usager mot de passe.
" LOGOUT : Fin de session IMAP.
" CREATE/DELETE/RENAME : Nom de boite à lettre.
" SELECT/EXAMINE : Nom de boite à lettre.
" LIST/LSUB/STATUS : Etat de la boite à lettre.
" EXPUNGE/CLOSE : Détruit les messages marqués (et ferme).
" SEARCH : Recherche de message sur différents critères.
" FETCH : Récupération des données concernant un courrier.
" COPY : Recopie d'un message d 'une boite à lettre dans une autre.
" CAPABILITY : Liste des fonctions implantées d'un serveur.
" NOOP : Opération vide.

Les principaux serveurs SMTP

Serveurs de messagerie **libres:**
(MTA Mail Transfert Agent):

- Sendmail (depuis 1980), Auteur principal Eric Allman,
  → problèmes de sécurité et de configuration (fichier sendmail.cf)
- Postfix (depuis 2001) Auteur principal Vietse Venema,
  → configuration plus simple.
- Exim (depuis 1995) Auteur Principal Philippe Hazel
- Qmail (depuis 1997) Auteur Dan Bernstein

Les principaux serveurs SMTP

Serveurs de messagerie **propriétaires:**

Logiciels de messagerie d'entreprise

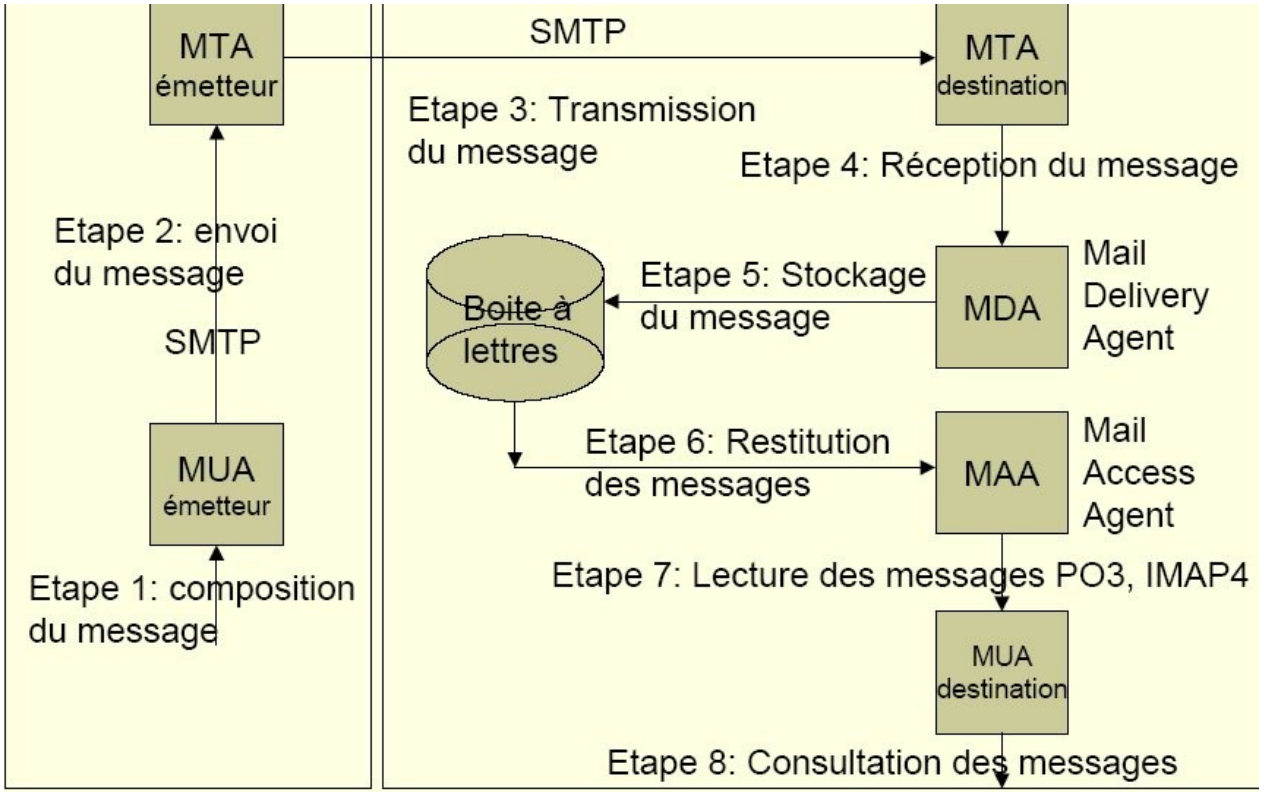
- **Exchange/Internet Information Service (Microsoft)**
- **Lotus Notes/Domino (IBM)**
- **IMAIL (Ipswitch)**
- **…**

Les principaux serveurs SMTP

Serveurs de messagerie:

http://en.wikipedia.org/wiki/Comparison_of_mail_servers

Le service de messagerie Internet
Vue Interne du système (plus en détail…)



Le SPAM

Le spamming, c'est le bombardement intempestif des newsgroups ou des boîtes aux lettres électroniques par des messages de toute sorte, publicitaires ou non.

Plus précisément, sont notamment considérés comme étant des actes de spamming, le fait d'écrire à un inconnu pour lui demander de venir visiter un site, d'inclure un individu dans une liste de diffusion sans son consentement, de diffuser sur un forum de discussion des messages sans rapport avec le thème de ce dernier.

Les différents synonymes (essentiellement d'origine québécoise) du spamming ou spam sont **courrier-rebut**, **pourriel** ou **polluriel**.

Le SPAM

SPAM est une marque de corned-beef (*Spiced Pork And Meat)*

On pourrait croire que l'explication s'arrête là : spam = truc dégueu…mais non: l'utilisation du terme Spam pour désigner des courriers électroniques abusifs est due aux Monty Python qui dans un de leurs sketchs, découvraient une carte où dans tous les plats il y avait du SPAM...

Le SPAM

Pourquoi le spamming est-il si répandu ?

Tout simplement parce que le spamming ne coûte presque rien !

L'achat de fichiers d'adresses ou de logiciels collecteurs d'e-mails se fait à un coût dérisoire (quelques dizaines d‘Euros). L'envoi des courriers électroniques ne coûte pas grand chose non plus (il suffit d'avoir une connexion Internet). Enfin, les retours sont nombreux : même avec un taux de clic faible, un envoi massif à plusieurs millions d'adresses génère quelques milliers de visites ! En clair, c'est tout bénéfice pour l'envoyeur.

Le SPAM

Identifier un SPAM:

Les résultats de l'opération "Boîte à spam", menée entre juillet et octobre 2002 par la CNIL, sont révélateurs. Sur 325 000 spams signalés par les internautes, 85 % étaient en langue anglaise et 55 % des messages en français étaient à caractère pornographique.

Le SPAM

Vous êtes spammé:

- **Votre fournisseur a cédé votre adresse e-mail**
- **Votre adresse a été générée au hasard**
- **Vous avez communiqué votre adresse à un site Web**
- **Vous avez publié votre adresse sur le Net**

Lutte anti-spam solutions

La première est d'installer un logiciel anti-spam sur chaque poste client. Cette option s'applique essentiellement aux petites structures, ou aux entreprises qui ne disposent pas de serveur de messagerie. Le coût n’est pas très élevé, mais les mises à jour doivent être effectuées sur tous les postes, ce qui implique une maintenance complexe

Lutte anti-spam solutions

On peut utiliser une passerelle spécialisée.

Il peut s’agir d’une "appliance", boîte noire qui regroupe le serveur physique, le serveur de messagerie et tous les outils antivirus et anti-spam nécessaires.

Une autre solution très utilisées par les entreprises consiste à passer par un serveur dédié contenant un anti-spam (open source ou pas), tel que SpamAssassin, IMSS (trend), Pyzor…

Lutte anti-spam solutions

Les technologies utilisées:

- Liste noire
- Liste blanche
- Filtre bayesien
- Analyse de texte
- Règles heuristiques
- Analyse sémantique
- Authentification

…

Lutte anti-spam solutions

Éditeur	Nom	Techniques de filtrage	Architecture	Prix
Aladdin	**eSafe Gateway**	Listes noires mises à jour tous les jours, filtres avec 17 mécanismes différents.	Architecture passerelle. Nécessite un serveur dédié Windows ou Virtual Appliance	3168 € HT pour 50 utilisateurs et 1 an de maintenance
Critical Path	**Critical Path**	Antispam de Brightmail (Symantec)	Solution hébergée	À partir de 0,35 € HT par utilisateur et par mois si plus de 1.000 utilisateurs
Goto Software	**Vade Retro**	Règles heuristiques, analyse sémantique, patterns HTML	Pour serveur de messagerie. Versions Windows, Linux, BSD et Solaris. Add-on pour Lotus Domino versions 5 et 6	290 € HT pour 25 utilisateurs et 1 an de mises à jour
Ipswitch	**Imail Server**	Filtrage par listes noires de domaines et d'URL. Plus de 20 filtres dont un filtrage bayésien, un système d'interrogation DNS inversée, ainsi que des filtres SMTP	Serveur de messagerie	- 730 € HT pour IMail Small Business (5 domaines de messagerie et 10 mailing lists, nombre d'utilisateurs illimité). - 1.570 € HT pour IMail Professionnel (nombre illimité de domaines, d'utilisateurs et de mailing lists)

Lutte anti-spam solutions

Claranet	**Clara MailBox**	Basé sur Spam Assassin	Architecture passerelle. Solution complète matérielle, logicielle et service	À partir de 590 € HT par mois
IronPort	**Serie C**	Antispam de Brightmail (Symantec)	Architecture passerelle. Solution complète matérielle et logicielle	10.000 € HT pour le C10 (250 utilisateurs) 25.000 à 30.000 € HT pour le C30 et 55.000 € HT pour le C60
Panda Software	**Platinium Internet Security**	Liste blanche. Filtres heuristiques	Logiciel pour poste client Windows	34 € HT ou 68 € HT avec 1 an de services
Symantec	**Norton Antispam**	Possibilité de filtrer les message en fonction de la langue. Filtre bayésien. Récupération du carnet d'adresses d'Outlook pour la liste blanche.	Logiciel pour poste client Windows	40 € HT par poste
Symantec	**AntiSpam pour SMTP**	Moteur heuristique. Listes noires multiples, listes blanches personnalisées. Blocage possible sur les noms et extension de fichiers	Passerelle logicielle	10,31 € HT par poste (50 à 99 postes)
Symantec	**Brightmail**	Signatures, filtre sur les en-têtes, filtre heuristique, listes noires.	Passerelle logicielle	40,69 € HT par an et par poste (50 à 99 postes)

Lutte anti-spam solutions

Trend Micro	**Spam Prevention Solution**	Filtre heuristique	Passerelle logicielle	22,57 € HT par poste (51 à 100 postes)
CipherTrust	**IronMail**	Techniques simultanées tels que les filtres bayésiens, filtres d'URL, listes noires et listes blanches	Architecture passerelle. Solution complète matérielle, logicielle et service	à partir de 9.990 € HT pour une centaine d'utilisateurs
Roaring Penguin	**CanIt**	Listes noires et listes blanches	Pour Unix, Linux avec SendMail. Code source fourni	6 € HT par an et par boîte aux lettre la première année.
Spam Assassin	**Spam Assassin**	Listes noires, filtres bayésiens, analyse du texte et des en-têtes.	Passerelle logicielle	Logiciel en open source. Utilisé dans de nombreuses applications commerciales Windows, Unix ou MacOS.
Webwasher	**Webwasher Anti Spam**	Listes blanches et noires, filtres bayésiens, analyse du texte et des en-têtes	Passerelle logicielle	23,20 € HT par utilisateur (50 postes). 20 € HT par utilisateur (100 postes) maintenance support et mise à jour compris.

Un hoax… (quoi ?)

Un hoax est une information fausse, périmée ou invérifiable propagée spontanément par les internautes. Les hoax peuvent concerner tout sujet susceptible de déclencher une émotion positive ou négative chez le lecteur : alerte virus, disparition d'enfant, promesse de bonheur, pétition, etc

Serveur MTA et code malveillant

Code malveillant: Virus, trojan, ver..

Pour généraliser « un code malveillant » est un programme (binaire, script, macro…) conçu pour être stocké sur votre ordinateur (mémoire, disque…), se multiplier, se répandre et finalement déclencher une action malveillante.

Serveur MTA et code malveillant

Le point d'entrée le plus fréquemment utilisé par les codes malveillants est le système de messagerie électronique. C'est pourquoi, pour être efficace, tout système de protection doit comprendre une protection active dédiée au serveur de messagerie électronique

Stopper les codes malveillants

1. Par un minimum de prévention (règles d'utilisation de l'internet et de la messagerie en particulier)

2. Par un logiciel installé sur le poste client

1. Par un logiciel installé sur les services d'échange de données (proxy web et ftp, **messagerie**, serveur de fichiers…)

2. Limiter l'accès aux infrastructures (physiquement, par le réseau→ firewall…)

3. Le tout (Bien entendu !)

Stopper les codes malveillants

Au niveau messagerie, c’est le MTA qui va analyser le flux échangé pour détecter les messages infectés (entête, corps, fichiers attachés).

Stopper les virus véhiculés par la messagerie

Exemple via les sources d'un message:

X-Antivirus: avast! (VPS 0517-1, 26/04/2005), Outbound message (1)
X-Antivirus-Status: Clean X-Virus-Scanned: amavisd-new (2)
X-Antivirus: avast! (VPS 0517-1, 26/04/2005), Inbound message (3)
X-Antivirus-Status: Clean (4)

Le message a été scanné par un anti-virus local en sortant du MUA avec avast (1), le MTA avec amavisd a scanné le message (2) et enfin le message a été de nouveau scanné par le MUA recepteur avec avast(3).

MTA anti-virus

Généralement, le MTA anti-virus se compose:

- Soit d'un moteur d'analyse et d'un fichier de signature,
- Soit d'un moteur heuristique.

Le fichier de signature ou de règles heuristiques évolue avec l'apparition des nouveaux virus. Les MAJ se font généralement automatiquement via le web.

MTA anti-virus

Méthode d’analyse:

- Expression régulière / champ d’entête, corps, pièces jointes…
- Méthodes heuristiques (comportement)

MTA anti-virus

- Trend Micro InterScan Viruswall
- McAfee Virus Scan
- Kaspersky AntiVirus
- F-PROT AntiVirus
- AmaViS / Clamav
- Bitdefende
- Sophos Sweep
- H+BEDV Central Command AntiVir

LE TD et LE TP:

TD: Découverte des protocoles SMTP, POP, IMAP
Première installation Postfix.
TP: Installation et Configuration Serveur SMTP, POP3
TP en fonction du temps restant: Anti-Spam, AntiVirus (solutions libres du type spamassassin, clamav)