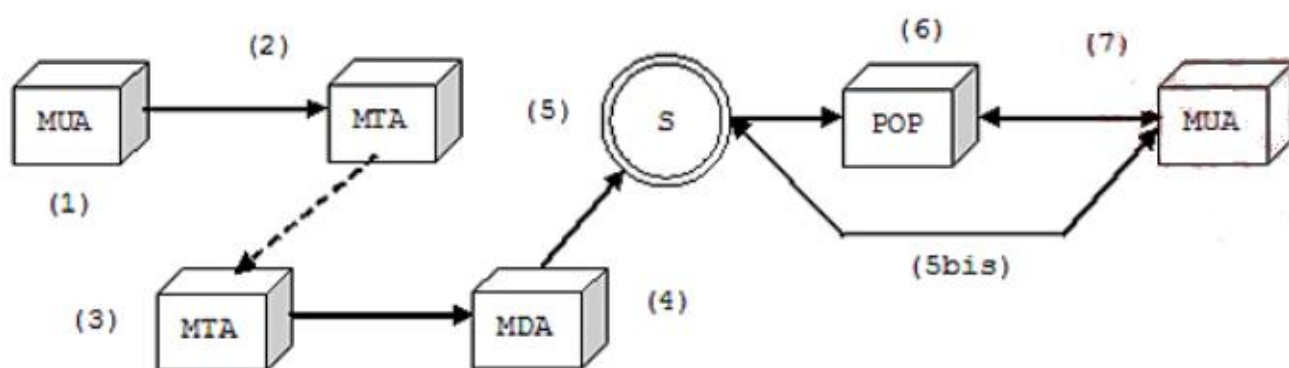
	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 5 Serveur de messagerie	Réseaux informatiques
BTS IRIS		TP

Un système de messagerie comporte nombre d'éléments en interaction les uns avec les autres, vous n'avez pas à choisir un logiciel mais plusieurs. La mise place de cet ensemble doit suivre une démarche rigoureuse sous peine de deux principaux avatars, une gestion difficile et un manque de sécurité avec l'intrusion de virus et du courrier non désiré.

La structure d'un système de messagerie

Le fonctionnement du courrier électronique respecte le modèle d'architecture client/serveur. Le système de messagerie compte plusieurs éléments :

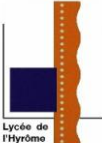


- Pour expédier un message (1), l'agent utilisateur (Mail User Agent ou MUA ; ex : mail le plus simple, mutt en mode console, Thunderbird en mode graphique) le compose d'abord, et l'envoie ensuite à un serveur de courrier exécutant un MTA.
- Le MTA (Mail Transfer Agent ; ex : sendmail, postfix, exim4) reçoit (2) par le protocole SMTP (on parlera donc de serveur SMTP) le message, détermine s'il doit le prendre ou non, ou le transmet à un autre MTA.
- Le MTA acceptant (3) le message le passe à un MDA (Mail Delivery Agent ; ex : procmail, postfix peut jouer le rôle) soit pour le stocker (4), soit pour le transmettre dans une base de données spécialisée.
- Le courrier est relevé par un MUA qui contacte un serveur POP/IMAP. Celui-ci relève le courrier (5) et le transmet au MUA (6).
- Si le stockage est local, la distribution l'est aussi (5 bis) directement par le MUA.

a. Composants du système de messagerie

Les protocoles :

- **SMTP** (Simple Mail Transfer Protocol) : port 25, permet le transfert d'un message entre un MUA et un MTA, ou entre deux MTA.

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 5 Serveur de messagerie	Réseaux informatiques
BTS IRIS		TP

- **POP** (Post Office Protocol) : port 110, récupère une boîte aux lettres en local afin de consulter les messages.
- **IMAP** (Internet Message Access Protocol) : port 143, fait la même chose que le protocole POP mais gère en plus directement les messages sur le serveur sans téléchargement.

Le format des adresses :

Les formats d'adresses sont nombreux, aussi il ne sera donné que deux exemples :

- **Adresses globales** : elles spécifient un site sans spécifier de chemin pour y arriver, en cela, elles sont valides à n'importe quel point d'Internet, exemple : jdupond@entreprise.fr.
- **Adresses littérales** : la présence des crochets indique une adresse numérique, qui doit être prise telle quelle, exemple : jdupond@[186.240.2.15].

Le format MIME (Multipurpose Internet Mail Extensions) :

Il s'agit d'une extension du système de courrier électronique existant : MIME s'occupe du contenu du message et non de son acheminement. MIME étend le contenu possible d'un message par :

- La gestion des types de données comme l'ajout d'autres langues ou la possibilité de transférer des données binaires.
- La gestion des messages plus complexes contenant plusieurs parties et la possibilité d'objets (images, audio, etc.).

b. Les problèmes du courrier électronique

Ils sont au nombre de deux : les virus car le courrier électronique est actuellement leur principale source de diffusion et le spam.

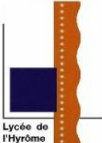
Le Spam :

Tout simplement un courrier non désiré envoyé à de multiples personnes, comme les prospectus qui inondent votre boîte aux lettres postale. Pour l'anecdote, le terme **spam** a deux origines possibles. Pour certains, il s'agit d'une marque américaine d'aliments bon marché de mauvaise qualité, alors que pour d'autres, il viendrait d'un sketch des Monty Python.

On peut classer les courriers non sollicités en plusieurs catégories :

- **UBE** (Unsolicited Bulk Email) : le classique courrier non désiré de masse.
- **UCE** (Unsolicited Commercial Email) : courriers purement commerciaux de démarchage éventuellement individuels.
- **MMF** (Make Money Fast) : chaînes de courriers (interdites en France et aux États-Unis entre autres) : comment devenir riche rapidement et sans effort, etc.

On peut ajouter les prétendues pétitions, les blagues à diffuser, les fausses nouvelles, etc., la liste est longue !

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 5 Serveur de messagerie	Réseaux informatiques
BTS IRIS		TP

Mise en place de base du serveur de messagerie

Vous utiliserez comme serveur SMTP (MTA) le logiciel libre Postfix à la place de Sendmail (ou Exim4) car il est simple à configurer, son niveau de sécurité est bon et il consomme moins de ressources système. Un serveur de messagerie complet se compose de plusieurs serveurs : le serveur de courrier entrant (SMTP) et celui sortant (POP et IMAP). Concrètement votre système de messagerie se composera de :

- L'UA (User Agent) chargé de poster et de lire le courrier (**Thunderbird** sur le client Lubuntu).
- Un MTA (Message Transfer Protocol) chargé de l'envoi et de la réception d'un message (**Postfix** sur SRVDMZ).
- Le MDA (Mail Delivery Agent) chargé de délivrer le message provenant du MTA dans une boîte aux lettres (**Procmail** sur SRVDMZ).
- Un serveur POP chargé de la récupération du courrier en local (**Dovecot-pop3d** sur SRVDMZ).

a. Postfix en tant que serveur local de messagerie

La première étape consiste à configurer un MTA sur le serveur SRVDMZ, ce qui correspond à une installation locale (pas de réseau). Dans ce type de configuration, les messages sont envoyés et reçus localement par les utilisateurs déclarés sur la machine (ici SRVDMZ).

Installez les paquetages de Postfix et de l'agent simple mail :

```
sudo aptitude install postfix postfix-doc mailutils procmail
```

Après le message d'information, choisissez pour l'instant Local uniquement. Validez le nom de courrier par défaut : srvmz.virtualux.fr. Le MTA Postfix démarre.

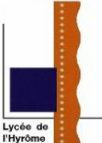
Première configuration :

Enlevez le commentaire de la première ligne concernant votre nom de serveur, vérifiez le nom du serveur pleinement qualifié dans le fichier /etc/postfix/main.cf et vérifiez la ligne indiquant à Postfix l'utilisation de procmail :

```
myorigin = /etc/mailname
myhostname = srvmz.virtualux.fr
mailbox_command = procmail -a "$EXTENSION"
```

Votre nom de courrier :

```
mydestination = srvmz.virtualux.fr,localhost.virtualux.fr,localhost
```

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 5 Serveur de messagerie	Réseaux informatiques
BTS IRIS		TP

La portée de l'écoute :

```
inet_interfaces = loopback-only
```

Premiers tests :

Relancez postfix :

```
sudo /etc/init.d/postfix restart
```

Regardez la bonne réactivité de Postfix en utilisant le protocole Telnet :

```
telnet localhost 25
```

Le serveur Postfix vous répond (quit pour sortir) :

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'
220 srvdmz.virtualux.fr ESMTP Postfix (Ubuntu)
```

Testez aussi la syntaxe du fichier /etc/postfix/main.cf par :

```
sudo /etc/init.d/postfix check
```

Cela peut sembler un luxe de précaution, mais la mise en place d'un serveur mail nécessite une méthodologie rigoureuse sous peine de chercher **très longtemps** l'erreur... Le résultat de la commande ne vous retourne rien en cas de bonne configuration. Après une modification du fichier /etc/postfix/main.cf, un simple /etc/init.d/postfix reload suffit (sauf si vous touchez à la directive inet_interfaces).

Le courrier du root :

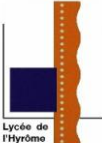
En règle générale, le courrier de l'utilisateur root est dirigé vers un autre compte : le vôtre ou celui indiqué à l'installation du serveur. Il vous permet de surveiller votre système sans devoir vous connecter avec tous les droits. Vous devez utiliser les alias dans le fichier /etc/aliases (dans notre cas l'utilisateur privilégié : eleve) :

Ajoutez l'alias du root dans le fichier /etc/aliases :

```
root: eleve
```

Faites prendre en compte cette modification par :

```
sudo newaliases
```

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 5 Serveur de messagerie	Réseaux informatiques
BTS IRIS		TP

Le scénario de test :

A partir de deux utilisateurs locaux avec mots de passe (toto et titi à créer), voici le scénario envisagé :

- Envoi en tant que eleve d'un message à toto et titi.
- Envoi en tant que toto d'un message à titi.
- Envoi en tant que toto d'un message à root, reçu en fait par eleve.

Vous allez utiliser comme MUA le programme mail et plusieurs consoles.

Pour envoyer un message :

- tapez **mail nom_utilisateur**,
- renseignez le sujet,
- ignorez les utilisateurs en copie en validant la ligne Cc sans la renseigner,
- puis tapez le message.
- Quittez l'édition du message et validez l'envoi du mail en tapant [Ctrl]**D**.

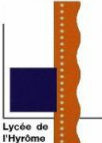
Notez que certaines versions anciennes de l'utilitaire mail exigeaient comme fin de message une ligne ne contenant que le caractère point.

Pour consulter un message :

- commande mail,
- puis t 1 pour lire le premier mail (etc.),
- d nmail pour détruire,
- ? pour voir l'aide,
- q pour quitter.

Avec le compte eleve, envoyez un message de test à titi et toto.

Connectez-vous en tant que toto, la commande simple mail vous indique un message reçu (un message vous le dit aussi lors de l'ouverture de session) :

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 5 Serveur de messagerie	Réseaux informatiques
BTS IRIS		TP

```

Ubuntu 12.04.1 LTS SRVDMZ tty2
SRVDMZ login: titi
Password:
Last login: Tue Sep 10 12:37:53 CEST 2013 on tty2
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

* Documentation:  https://help.ubuntu.com/

System information as of Mon Sep 16 10:44:08 CEST 2013

System load:  0.0                Processes:            73
Usage of /:   15.5% of 7.47GB    Users logged in:     1
Memory usage: 23%               IP address for eth0: 192.168.4.10
Swap usage:   0%

Graph this data and manage this system at https://landscape.canonical.com/

You have new mail.
titi@SRVDMZ:~$ mail
"/var/mail/titi": 1 message1 nouveau
>N  1 eleve                lun. sept. 16 10 13/406  test
?  _

```

Toujours en tant que toto, envoyez un message à titi et au root.
Connectez-vous en tant que titi : il doit recevoir deux messages.
Connectez-vous en tant que eleve, et vérifiez la présence du message de toto adressé au root.

Comme nous sommes dans le cadre d'une distribution locale, les courriers sont stockés dans le répertoire /var/mail/nom_utilisateur.

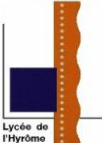
b. Postfix en serveur pour un domaine

Vous allez ajouter à votre serveur MTA la capacité d'un serveur POP. Pour cela, il faut le transformer en serveur pour un domaine. À partir du client, un utilisateur pourra consulter ses courriers de la machine SRVDMZ. Vous utiliserez comme serveur POP le logiciel **Dovecot**. La coopération entre Postfix et un serveur POP est simple : lorsque Postfix accepte la distribution d'un courrier, il le place dans l'espace de stockage. Ce dernier est utilisé ensuite par le serveur POP pour récupérer les courriers.

Installation du serveur POP

Installez les paquetages du service POP :

```
sudo apt-get install dovecot-pop3d
```

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 5 Serveur de messagerie	Réseaux informatiques
BTS IRIS		TP

Nous allons utiliser une politique d'authentification simple en « plain text », donc sans sécurité.
 Nous définirons également l'emplacement de la boîte aux lettres des utilisateurs pour leur première connexion.

Dans le fichier `/etc/dovecot/conf.d/10-auth.conf`, décommentez et modifiez la ligne :

```
disable_plaintext_auth = no.
```

Dans le fichier `/etc/dovecot/conf.d/10-mail.conf`, décommentez et modifiez les lignes :

```
mail_location = mbox:~/mail:INBOX=/var/mail/%u
mail_access_groups = mail.
```

Relancez le service Dovecot :

```
sudo /etc/init.d/dovecot restart
```

Vérifiez la bonne marche du serveur POP en local avec l'utilisateur toto (après la connexion, tapez user toto et pass passe_de_toto) :

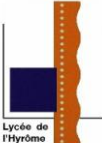
```
telnet localhost 110
```

Le serveur Dovecot vous répond :

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'
+OK Dovecot ready.
user toto
+OK
pass toto
+OK Logged in.
quit
```

Modifiez le fichier de configuration Postfix `/etc/postfix/main.cf` :

```
(...)
mydomain = virtualux.fr
myhostname = srvmz.$mydomain
(...)
mydestination = $myhostname,localhost.virtualux.fr,localhost,$mydomain
(...)
relayhost = $mydomain
relay_domains = $mydestination
mynetworks = 192.168.4.0/24 127.0.0.0/8
(...)
inet_interfaces = $myhostname, localhost
```

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 5 Serveur de messagerie	Réseaux informatiques
BTS IRIS		TP

Respectivement le domaine DNS, le serveur, le domaine de la délivrance du courrier et l'écoute de toutes interfaces du serveur. Comme on retrouve des variables dans la succession des directives, **faites attention à l'ordre** notamment pour \$mydomain.

Modification du DNS

Il faut indiquer à tout notre domaine la présence d'un serveur de messagerie et d'un serveur POP.

Modifiez votre fichier de zone DNS /var/cache/bind/db.virtualux.fr en y ajoutant **à la fin** la référence au serveur de messagerie et les alias pour les serveurs SMTP et POP :

```
@      IN      MX 10      srvdmz.virtualux.fr.
smtp   IN      CNAME    srvdmz
pop     IN      CNAME    srvdmz
```

Redémarrez les services DNS et Postfix :

```
sudo /etc/init.d/bind9 restart
sudo /etc/init.d/postfix restart
```

c. Vérifications sur le client Lubuntu

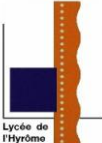
Vérifiez dans la console DOS la bonne connectivité DNS par ping pour pop.virtualux.fr et smtp.virtualux.fr.

Installez le paquet Thunderbird

Créez un compte mail avec **Thunderbird** pour les utilisateurs eleve et titi avec les serveurs pop.virtualux.fr pour le serveur de courrier entrant et smtp.virtualux.fr pour le serveur de courrier sortant.

N'hésitez pas à interrompre l'assistant de création de compte en cliquant sur le bouton **Configuration manuelle**. En effet, Thunderbird recherche dans sa base de données à quel hébergeur public il pourrait bien avoir affaire. Dans notre cas, il s'agit bien entendu d'un serveur inconnu de Thunderbird. Acceptez ensuite l'exception de sécurité de la part de Thunderbird qui n'apprécie pas qu'on se connecte à un serveur sans authentification sûre ni confidentialité. Dans la mesure où notre fonctionnement est strictement interne (serveurs et clients dans le même réseau privé et protégé), nous pouvons nous permettre cette légèreté.

Testez l'envoi et la réception de mail avec les différents comptes créés

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 5 Serveur de messagerie	Réseaux informatiques
BTS IRIS		TP

d. Exploiter au mieux les logs du système de messagerie

Un utilitaire (pflogsumm) écrit en Perl permet d'analyser en détail les logs d'un serveur de messagerie. Son fonctionnement est très simple, après installation du paquetage de même nom sur le serveur.

Lancez la commande `pflogsumm /var/log/mail.log | less` et appréciez le résultat...