Cours Courrier électronique

IUT1 dpt SRC L'Isle d'Abeau
Jean-François Berdjugin

Mail ou courrier électronique

Applications permettant d'envoyer et de recevoir du courrier électronique :

- Eléments de l'application
- Services rendus
- La structure des messages
- Le transfert des messages
- La confidentialité

Architecture et services

Deux types d'agents :

- **Les agents utilisateurs** : lecture, écriture du courrier.
- **Les agents de transfert** : transmission d'un message de sa source vers la destination.

Architecture et services

Services proposés :

- La composition
- Le transfert
- L'affichage
- La disposition

- Boîte au lettre
- Les listes de diffusion
- Courrier recommandé
- Chiffrement
- …

Architecture et services

Un courrier se compose :

- D'une enveloppe utilisée par l'agent de transfert
- D'une message lui-même subdivisé en
  - Une entête (header)
  - Un corps (body)

  utilisés par l'agent utilisateur

Enveloppe
MAIL From: origine RCPT To: destination
En-tête – Received: – Message-Id: – From: – Date: – Reply-To: – To: – Cc: copie – Bcc: copie secrète – Subject:
Corps

Agent utilisateur

- D'un point de vue utilisation l'agent utilisateur permet la composition, la réception, la réponse au message et la gestion des boîtes au lettres.

- Composition :
  - Utilisation d'un éditeur intégré ou non pour créer le contenu
  - Fourniture d'une adresse (trois standards)
    - RFC 2822 (ou nom DNS): utilisateur@machine.sousdomaine.domaine
    - X400 : C=CodePays; ADMD=400net; PRMD=switch; ORG=NomOrganisation; OU=Departement; S=Utilisateur
    - UUCP: Machine1!Machine2!...!Machine.Utilisateur (en voie d'abandon)

  Rem : mailing list ou liste de diffusion
  - mailing liste locale (plusieurs mail)
  - Mailing liste distante (un mail)

Agent utilisateur

- Réception
  - No du message
  - Drapeau (Flag)
    - L Lu
    - R Répondu
    - F fait suivre
  - Taille du message
  - Sujet

  Rem : personnalisation possible avec un profil utilisateur

No	Flag	Size	From	Subject
1	L	1024	Durand	test
2	LR	2048	Dupont	commu nication
3	LF	512	Jacques	jeux

Formats de message

A l'origine le mail était prévu pour transférer des messages en ASCII (American Standard Code for Information Interchange) un code sur 7 bits permettant de représenter 128 caractères.

=> Un format de base le RFC 822 qui a du évoluer pour répondre aux nouvelles exigences (multimédia, alphabets internationaux, idéogrammes).

RFC 822

Message :

- Une enveloppe
- Champs d'entête
- Ligne Blanche
- Message

L'agent utilisateur construit le message, le passe à l'agent de transfert qui utilise certains champs de l'entête pour construire l'enveloppe.

RFC 822: Champs d'entête liés au transfert de message

En-tête	Signification
To:	Adresse(s) électronique(s) destinataire(s) primaire(s)
Cc:	Adresse(s) électronique(s) destinataire(s) secondaire(s)
Bcc:	Adresse(s) électronique(s) destinataire(s) copie cachée
From:	Personne qui a crée le message
Received	Adresse électronique de l'émetteur
Received:	Ligne ajoutée par chaque agent de transfert le long de la route
Return-Path:	Utilisée pour identifier un chemin de retour vers l'émetteur

RFC 822: Champs d'entête liés a l'agent destinataire.

En-tête	Signification
Date:	Date et heure locale de l'envoi du message
Reply-To:	Adresse électronique ou envoyer les réponses
Message-Id:	Identifiant unique du message
In Reply-To:	Numéro du message auquel on répond
References:	Autres numéros de messages liés à celui-ci
Keywords:	Mots clefs
Subject:	Résumé

Limitation et évolution du format RFC 822

Le standard permet la création de nouvelles entêtes commençant par X-.

⇒ Un nouveau standard MIME(Multipurpose Ineternet Mail Extension) qui permet en structurant le corps du message et en définissant des règles de codage d'envoyer autre chose que du texte ASCII.

⇒ Compatibilité avec les agent de transfert, seuls les agents utilisateurs doivent évoluer.

MIME

En-tête	Signification
MIME-Version	Identification de la version de mime
Content-Description	Liste du contenu
Content-Id	Identificateur unique
Content-Transfert-Encoding	Façon dont le corps est emballé pour la transmission => **codage base 64 (blindage ASCII), Quoted printable** ou codage maison
Content-Type	Nature du message => Text (Plain, **Richtext**), Image, Audio, Vidéo, Application, **message**, **Multipart**

Codage base64

Idée faire tenir des octets (8 bits) dans 7 bits.

=>

- Prendre les octets 3 par 3 (24 bits)
- Découper les 24 bits en paquets de 6 bits (4 paquets)
- Convertir ces 6 bits en 7 bits.

Conclusion MIME

MIME permet donc :

- Des messages composés de plusieurs objets
- Plusieurs alphabets
- Des messages illimités
- Des fichiers binaires ou spécifiques à une application
- **Des messages multimédia** (audio, vidéo, image)
- **Du texte enrichi** (plusieurs polices de caractères, couleur...)
- Des liens

Transfert de message

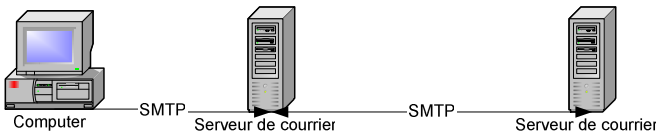
But faire passer le message d'un émetteur à un destinataire.

Du point de vue utilisateur le transfert de message est asymétrique : la réception et l'émission ne reposent pas sur le même protocole.

Message sortant : SMTP

Utilisation du protocole SMTP (Simple Mail Transfert Protocole) :

- Repose sur TCP => transfert fiable
- Utilise généralement le port 25
- Est un protocole ASCII



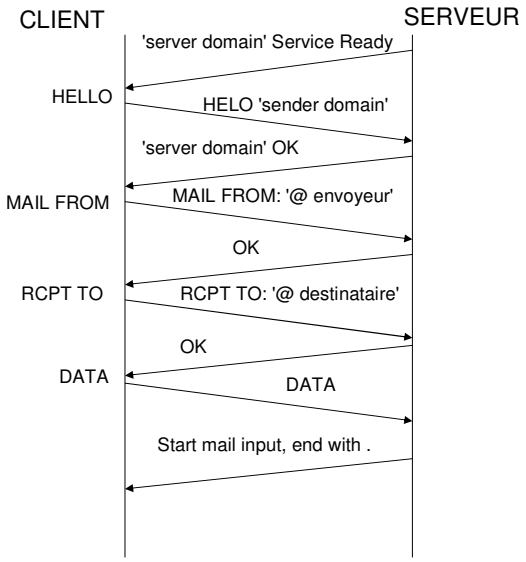
Commandes SMTP

Commande	Exemple	Description
HELO (désormais EHLO)	EHLO 193.56.47.125	Identification à l'aide de l'adresse IP ou du nom de domaine de l'ordinateur expéditeur
MAIL FROM:	MAIL FROM: expediteur@domaine.com	Identification de l'adresse de l'expéditeur
RCPT TO:	RCPT TO: destinataire@domaine.com	Identification de l'adresse du destinataire
DATA	DATA message	Corps du mail
QUIT	QUIT	Sortie du serveur SMTP
HELP	HELP	Liste des commandes SMTP supportées par le serveur

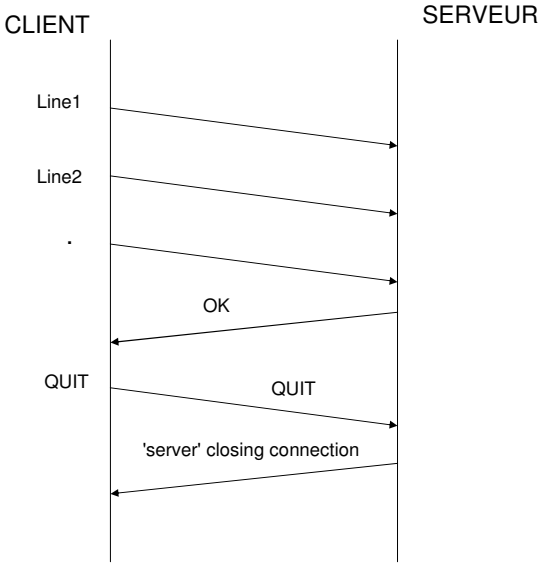
SMTP

Le client se connecte sur le port 25 du serveur avec le protocole TCP, puis :

- Le serveur envoie son identité et son état (disponible ou non).
- Si le serveur est prêt, le client envoie l'adresse de l'émetteur et du destinataire.
- Si le destinataire est géré par le serveur, le serveur donne son accord.
- Le client envoie le message
- Le serveur acquitte le message



SMTP

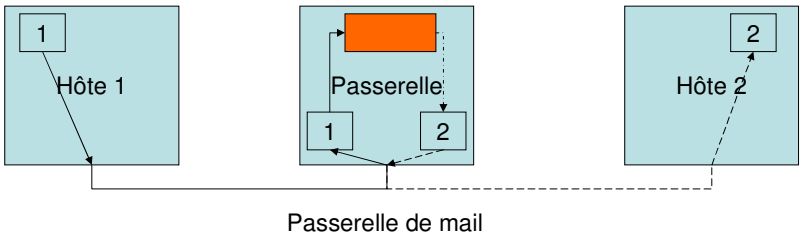


SMTP

S: **220** smtp.commentcamarche.net SMTP Ready
C: **EHLO** machine1.commentcamarche.net
S: **250** smtp.commentcamarche.net
C: **MAIL FROM:**<webmaster@commentcamarche.net>
S: **250** OK
C: **RCPT TO:**<meandus@meandus.net>
S: **250** OK
C: RCPT TO:<tittom@tittom.fr>
S: 550 No such user here
C: **DATA**
S: **354** Start mail input; end with <CRLF>.<CRLF>
C: Subject: Petit Bonjour
C: Salut Meandus, C: comment ca va?
C: C: A bientot !
C: <CRLF>**.**<CRLF>
S: **250** OK
C: **QUIT**
R: **221** smtp.commentcamarche.net closing transmission

Passerelles

Tous le monde n'est pas sur Internet,
Tous le monde ne parle pas RFC 822,
L'intranet peut être protégé par un firewall.
=>
Utilisation d'une passerelle.



Message entrant

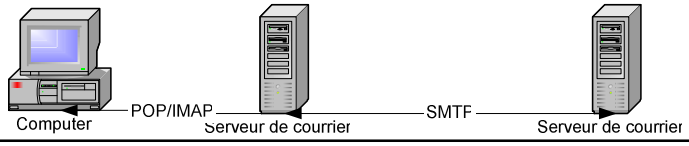
SMTP présuppose que l'ordinateur qui va recevoir le courrier est accessible en permanence. Ce qui n'est pas le cas de la plus part des machines.

=>

Aller chercher ses mails sur une machine serveur de courrier entrant.

=>

Utilisation du protocole POP, IMAP, DMSP



POP/IMAP/DMSP

POP : Post Office Protocol

Chargement local d'un courrier distant et accès par numéro d'arrivée.

IMAP :Interactive Mail Access Protocol

Référentiel commun et accès avec des attributs.

DMSP : Distributed Mail System Protocol

Courrier sur plusieurs machines avec synchronisation (à la connexion).

POP vs IMAP

POP
- Simple
- Fortement supporté

IMAP
- Accès simultanés
- Plusieurs boîte au lettres
- Tri suivant critères
- Existence de protocoles complémentaires destinés à la gestion des configurations utilisateurs (Internet Message SuPport).
- Accès aux données autres que le courrier électronique (News).

Commandes POP3	
Commande	**Description**
USER identifiant	Cette commande permet de s'authetifier. Elle doit être suivie du nom de l'utilisateur, c'est-à-dire une chaîne de caractères identifiant l'utilisateur sur le serveur. La commande USER doit précéder la commande *PASS*.
PASS mot_de_passe	La commande *PASS*, permet d'indiquer le mot de passe de l'utilisateur dont le nom a été spécifié lors d'une commande *USER* préalable.
STAT	Information sur les messages contenus sur le serveur
RETR	Numéro du message à récupérer
DELE	Numéro du message à supprimer
LIST [msg]	Numéro du message à afficher
NOOP	Permet de garder les connexion ouverte en cas d'inactivité
TOP <messageID> <n>	Commande affichant *n* lignes du message, dont le numéro est donné en argument. En cas du réponse positive du serveur, celui-ci renvoie les en-têtes du message, puis une ligne vierge et enfin les *n* premières lignes du message.
UIDL [msg]	Demande au serveur de renvoyer une ligne contenant des informations sur le message éventuellement donné en argument. Cette ligne contient une chaîne de caractères, appelée *listing d'identificateur unique*, permettant d'identifier de façon unique le message sur le serveur, indépendamment de la session. L'argument optionnel est un numéro correspondant à un message existant sur le serveur POP, c'est-à-dire un message non effacé).
QUIT	La commande *QUIT* demande la sortie du serveur POP3. Elle entraîne la suppression de tous les messages marqués comme effacés et renvoie l'état de cette action.

POP3

S: +OK mail.commentcamarche.net POP3 service
S: (Netscape Messaging Server 4.15 Patch 6 (built Mar 31 2001))
C: USER jeff
S: +OK Name is a valid mailbox
C: PASS mon_pass
S: +OK Maildrop ready
C: STAT S: +OK 2 0
C: TOP 1 5
S: Subject: Petit Bonjour
S: Salut Meandus,
S: comment ca va?
S:
S: A bientot !
C: QUIT
S: +OK

Confidentialité

Le courrier électronique souffre des problèmes suivants :

- Confidentialité (seul le destinataire doit pouvoir accéder à l'information)
- Authentification (certitude sur l'émetteur)
- Non Répudiation (certitude de la réception)

=>

- PGP (Pretty Good Privacy) Le standard de fait
- PEM (Privacy Enhanced Mail) Le standard internet

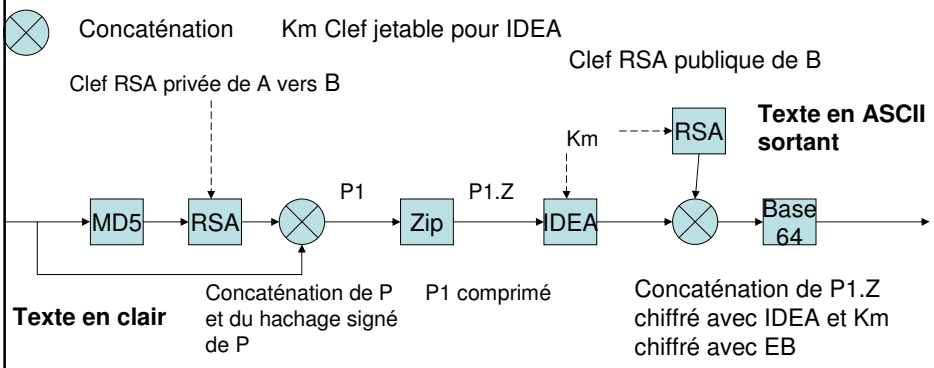
PGP

PGP est une boîte à outil permettant d'assurer l'authentification, le chiffrement, la non répudiation et la compression des messages

MD5 : permet d'obtenir l'empreinte d'un message (le hachage : un identifiant numérique).

RSA : est un algorithme de chiffrement à clef public

IDEA : est un algorithme de chiffrement à clef secrète



Fonctionnement de PGP avant envoi d'un message de A vers B

PGP

Un schéma bien compliqué pour le moment mais il convient de retenir :

- L'utilisation de clefs pour le chiffrement et le déchiffrement avec deux classes d'algorithmes ceux à clef secrète et ceux à clef public.
- Un mécanisme d'échange pour les clef publics
- L'utilisation d'une empreinte ou d'un hachage pour obtenir un identifiant numérique non unique mais dont il est très difficile d'écrire un message ayant le même identifiant.

Conclusion

- Service important
- Deux agents (utilisateur transfert)
- Message = enveloppe + en-tête + corps
- Deux protocole SMTP et POP(ou IMAP)
- Pas de confidentialité, d'authentification et de non répudiation prévue à l'origine