Grenoble INP ENSIMAG

Chapitre AP_mel
Le courrier électronique (e-mail, courriel, mél)

Architecture
Protocoles SMTP, POP, IMAP
Codage MIME

APplications

Contenu du chapitre AP_mel

- Architecture
- SMTP *(Simple Mail Transfer Protocol):* acheminement du courrier
- Accès distant: POP, IMAP
- Format MIME *(Multipurpose Internet Mail Extensions)*
  - définit le type et le codage de l'information contenue dans le message

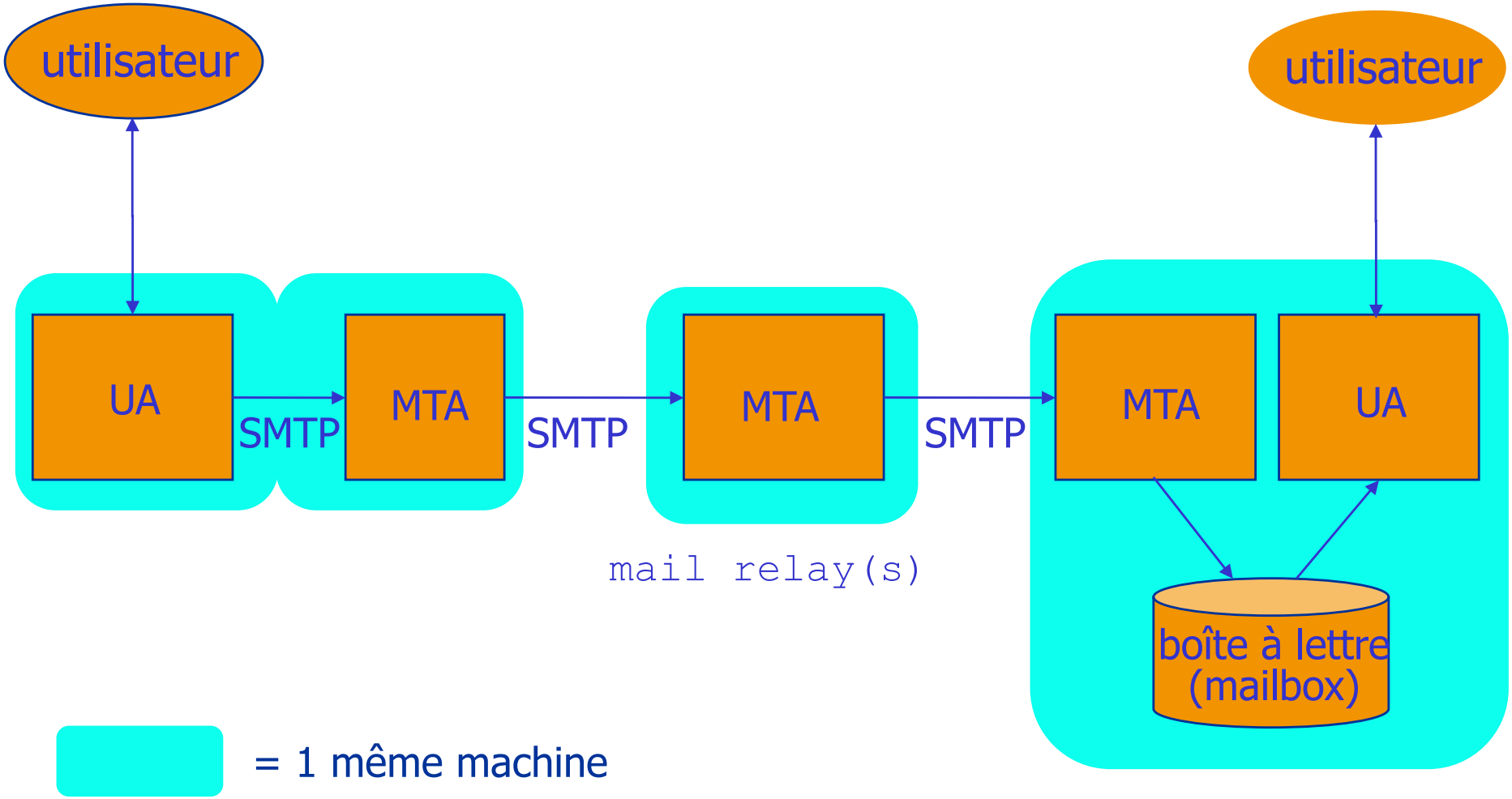
Architecture

- Le courrier électronique: fait intervenir 3 types de processus
  - agent utilisateur *(User Agent – UA ou MUA)* ~terminal, client – c' est l' IHM (interface utilisateur)
    mail, Thunderbird, Eudora, Outlook…
  - agent de transfert *(Mail Transfer Agent)* ~nœud intermédiaire
    sendmail, MS/Exchange
  - Gestionnaire de boîtes aux lettres (BAL) d'un domaine-zone
    Sendmail (historique), Dovecot, Postfix, Zimbra…

➔ Architecture + complexe que client-serveur

- Adresse - identifie un utilisateur
  - `user@domainName`
  - `domainName` est un nom de domaine (DNS)
    - virtuel (MX): par ex `roland.groz@imag.fr`
    - réel (A): par ex `grozr@ens.ensimag.fr`

Principe canonique (à l'origine)



Rôle des MTA

Asynchronisme, stockage intermédiaire, fiabilité, routage

- Si le MTA cible est en panne
  - le MTA en amont stocke le message et retransmet après un intervalle (30 minutes)
  - essaie 3-4 jours
- MTA permanents
  UA: peuvent être déconnectés (portables…)
- MTA peuvent centraliser le courrier en départ/arrivée pour une entreprise
  - Filtrage des virus, spams…

SMTP *(Simple Mail Transfer Protocol)*

- Protocole utilisé pour le transfert du courrier électronique (RFC 5321: ESMTP)
  - Entre MTA
  - De l'UA au MTA de rattachement pour l'envoi(*) du courrier
- Serveur : port 25 (465 pour smtps, version sécurisée)
- Mode connecté: le MTA amont ouvre une connexion par HELO (EHLO en ESMTP) pour s'identifier
  - cnx au niveau Application, au-dessus de la connexion TCP
- Ensuite il a accès à des commandes du serveur (i.e. PDU du protocole) permettant de définir expéditeur, destinataire et contenu du message.

(*) Et pour la réception par l'UA destinataire ?

Commandes SMTP

Envoi de message

```
HELO nom-de-site-client
MAIL FROM:<batman@batmobile.org>
RCPT TO:<superman@krypton.net>
DATA
ligne1
ligne2
ligne3
.
QUIT
```

NB: ligne1 ci-dessus, par exemple: `Subject: Sus a Joker !`

Autres commandes

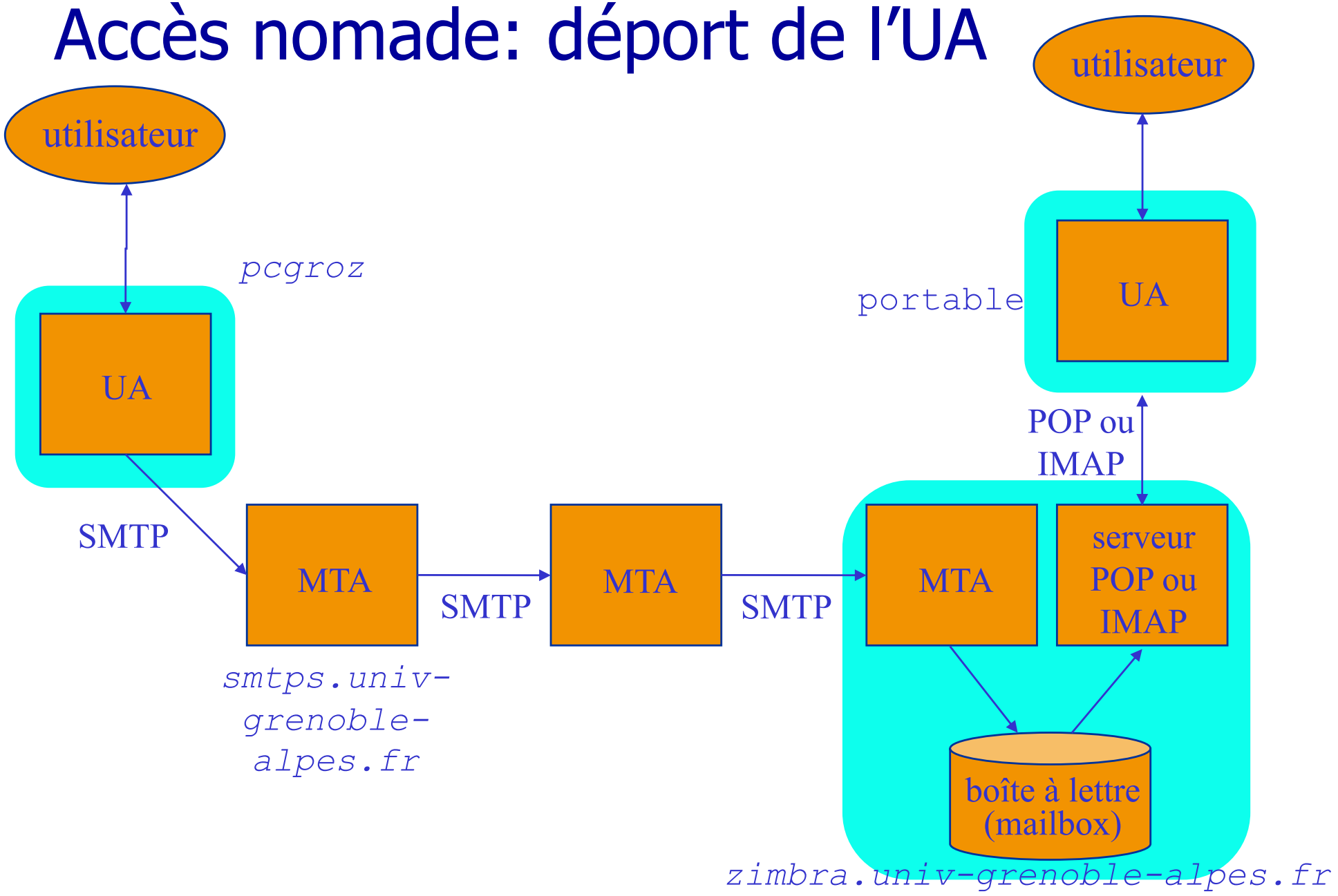
```
VRFY adresse
EXPN liste
HELP
RSET
```

Enveloppe, en-tête, contenu

- Enveloppe (commandes du protocole SMTP)
  - `MAIL From:`
  - `RCPT To:`
- En-tête (pour le UA et le lecteur humain)
  - `Received:`
  - `Message-Id:`
  - `From:`
  - `Date:`
  - `Reply-To:`
  - `To:`
  - `Cc: copie`
  - `Bcc: copie secrète`
  - `Subject:`
- Contenu: texte du message (ou fichiers inclus…)

Historiquement, SMTP ne transférait que de l'ASCII (besoin de codage de canal) – ESMTP transfère 8 bits

Accès nomade: déport de l'UA



Accès nomade

- POP *(Post-Office Protocol)* – *RFC 1939: POP3*
  - récupération de la boîte aux lettres distante
    les messages sont stockés par l'UA
  - MTA ne gère que la BAL de réception
  - Port serveur: 110 (995: pops)

Commandes: `USER, PASS, LIST, RETR, DELE, QUIT`

- IMAP *(Internet Mail Access Protocol)* – *RFC 9051*
  - utilisateur décide quels messages récupérer
    l'UA peut laisser le MTA stocker les messages
  - MTA gère BAL + dossiers archives (« folders »)
  - Port serveur: 143 (993: imaps)

Commandes POP

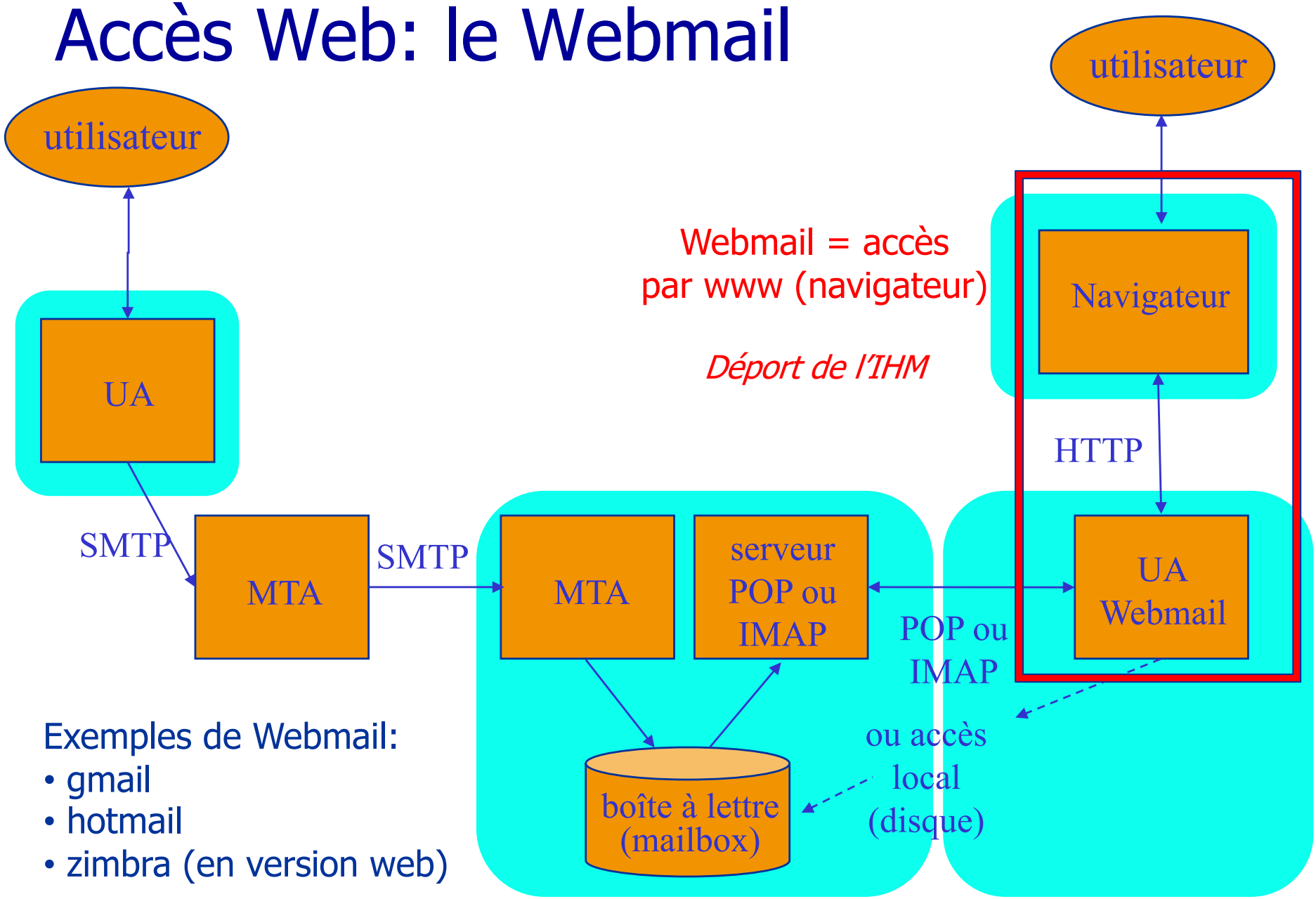

```
USER GROZ
+OK User name accepted, password please
PASS jesuiscaché
+OK Mailbox open, 3 messages
LIST
+OK Mailbox scan listing follows
1 1690
2 627
3 1541
.
RETR 2
+OK 627 octets
Received: (from groz@localhost)by ensibm.imag.fr for groz; …
Date: Mon, 23 Feb 2004 09:51:50 +0100
From: roland groz <groz@ensisun.imag.fr>
Message-Id: <200402230851.i1N8po070766@ensibm.imag.fr>
To: groz@ensibm.imag.fr
Subject: essai
…
.
QUIT
```

Commandes IMAP


```
a01 LOGIN groz jesuiscache
a01 OK Logged in.
a02 SELECT inbox
* FLAGS (\Answered \Flagged
  \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered
  \Flagged \Deleted \Seen \Draft
  \*)] Flags permitted.
* 3 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1290414471] UIDs
  valid
* OK [UIDNEXT 4] Predicted next
  UID
a03 STATUS inbox (messages)
* STATUS "inbox" (MESSAGES 3)
a04 STORE 2:3 flags \Deleted
* 2 FETCH (FLAGS (\Deleted))
a04 OK Store completed.
a05 EXPUNGE
* 2 EXPUNGE
a05 OK Expunge completed.
```

```
a06 FETCH 1:1 all
* 1 FETCH (FLAGS (\Seen)
   INTERNALDATE "02-Dec-2010
   08:37:49 +0100" RFC822.SIZE
   1930 ENVELOPE ("Thu, 2 Dec 2010
   08:37:43 +0100" "Essai"
   (("Roland Groz" NIL
   "Roland.Groz" "imag.fr"))
   (("Roland Groz" NIL
   "Roland.Groz" "imag.fr"))
   (("Roland Groz" NIL
   "Roland.Groz" "imag.fr")) ((NIL
   NIL "groz" "ensimag.imag.fr"))
   NIL NIL NIL "<E38C4FAB-C59F-
   4FDE-8A08-
   CB0C28B16D89@imag.fr>"))
a06 OK Fetch completed.
a07 CREATE bal_archive
a07 OK Create completed.
a08 COPY 1:1 bal_archive
a08 OK Copy completed.
a10 LOGOUT
* BYE Logging out
a10 OK Logout completed.
```

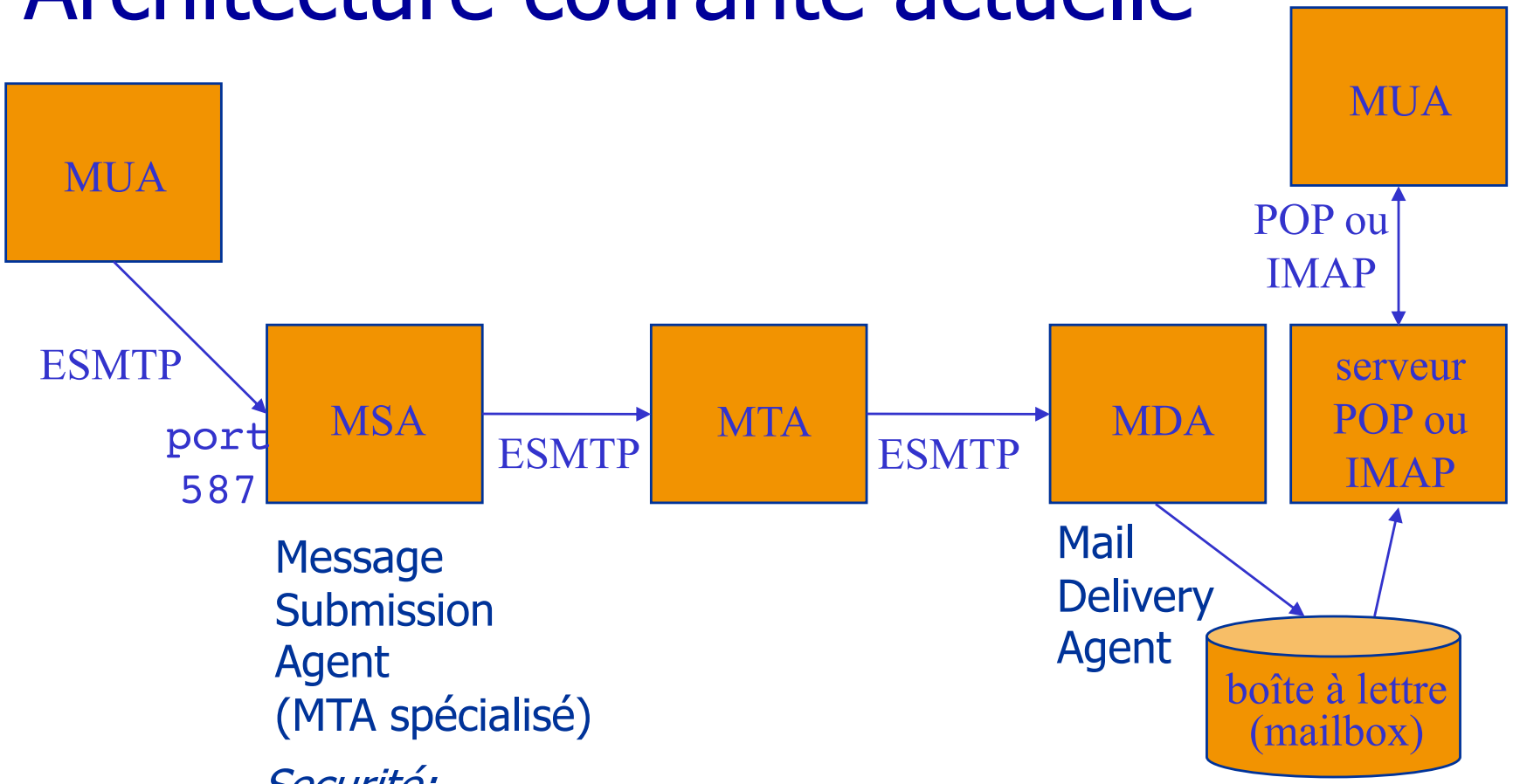
Accès Web: le Webmail



Exemples de Webmail:

- gmail
- hotmail
- zimbra (en version web)

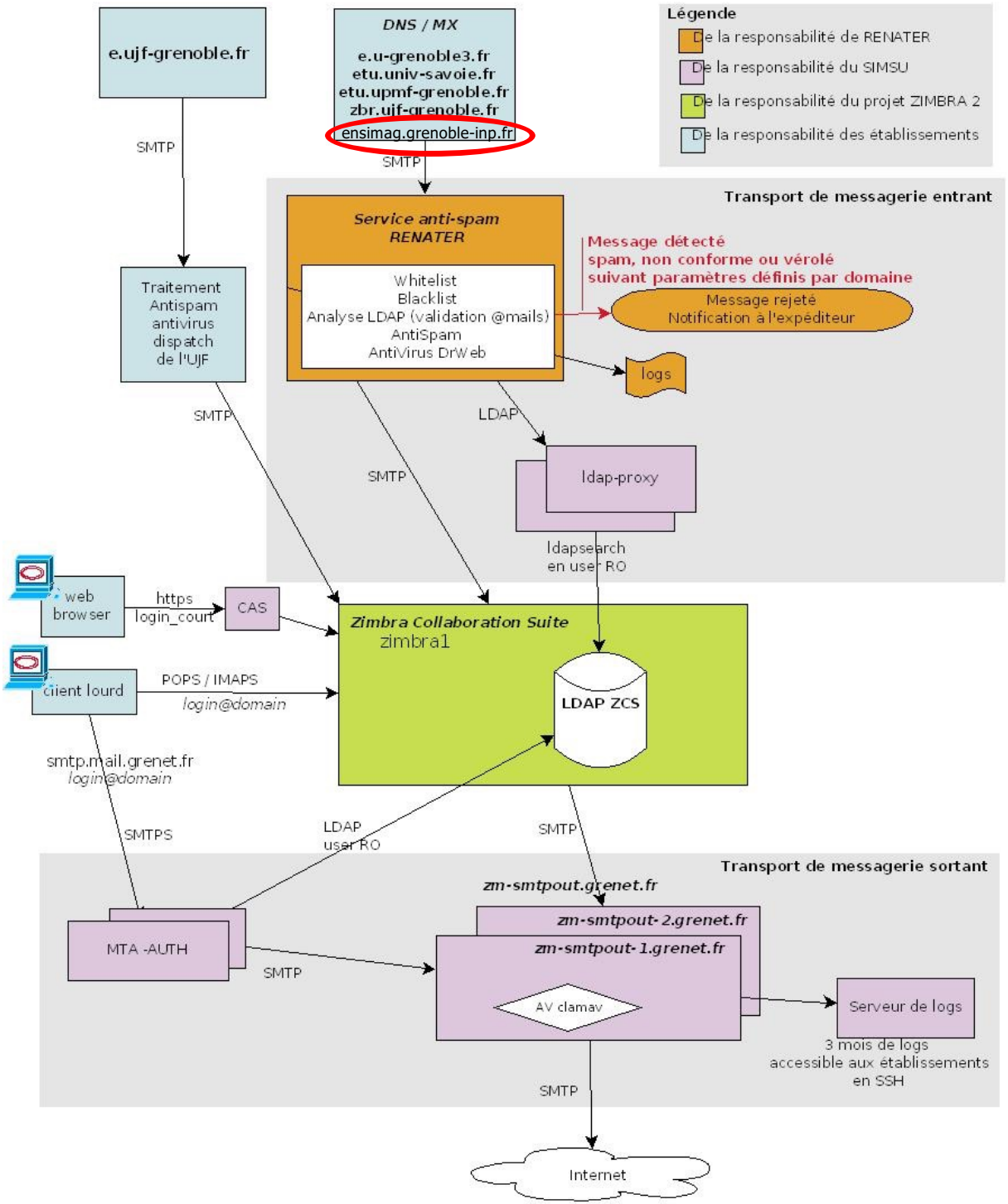
Architecture courante actuelle



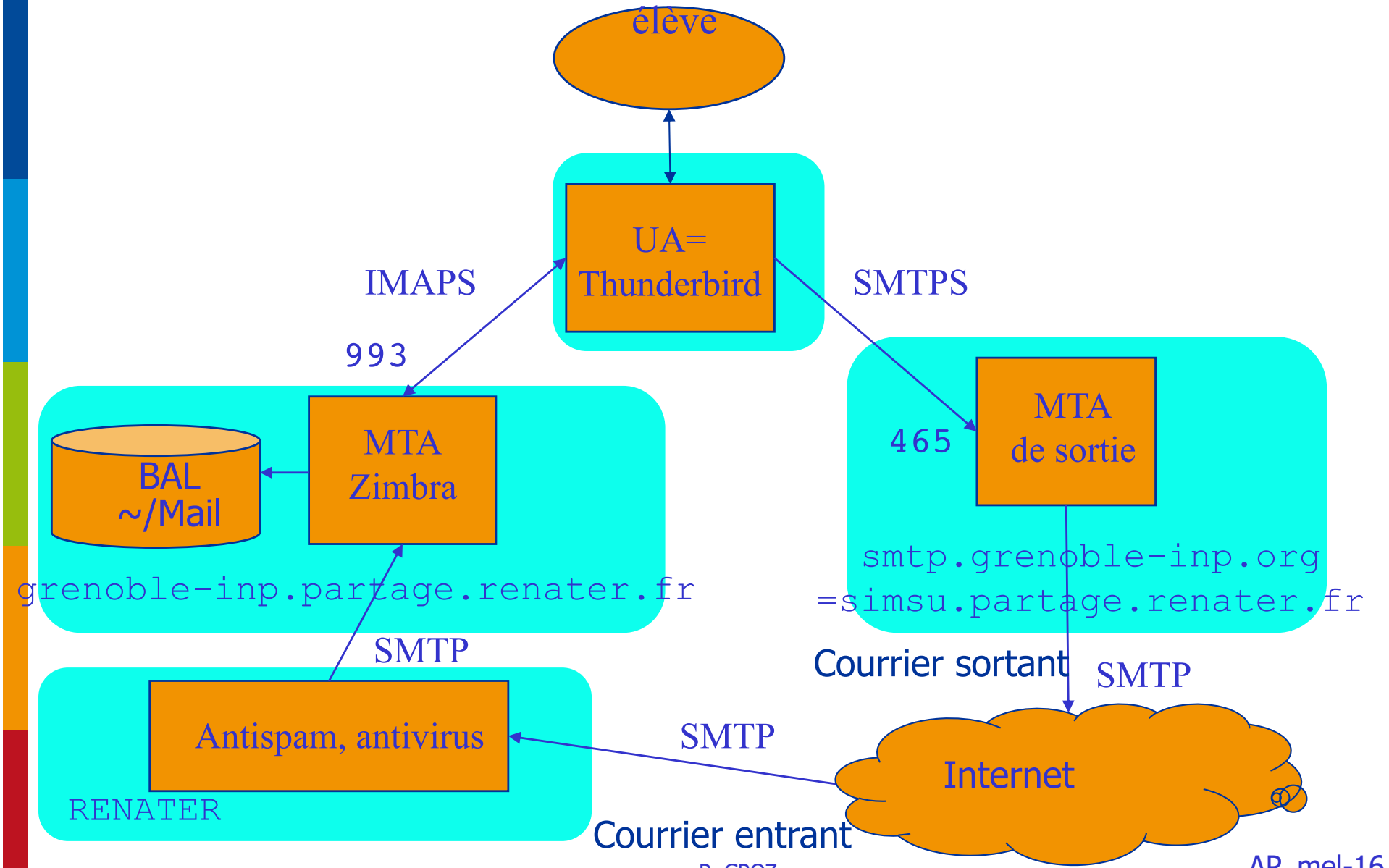
Securité:
Vérif. légitimité
(Sender Policy Framework)

Antispam,
Antivirus
Stockage des messages
et serveur POP/IMAP
(logiciels: dovecot, Zimbra, Postfix…)

Zimbra SIMSU
(jusqu'en oct 2016)



Architecture de messagerie Ensimag-Zimbra



MIME

- *Multipurpose Internet Mail Extensions*
  - Officiellement appelé « Media Types » (2005)
- Structuration et typage des contenus
- Résolution de plusieurs problèmes du courrier
  - texte avec accents
  - texte en alphabets autres que latins
  - messages contenants d'autres média (images, audio)
  - adaptation aux capacités de présentation de l'UA
- Utilisé aussi par WWW/HTTP (en-tête de la réponse)
- RFC: 2045 (base), 2046 (multipart, PJ), 2183 (Content-Disposition)

Extensions d'en-tête MIME

- `Mime-Version:`
- `Content-Type:`
  - `type/sous-type`

  description de la nature de données, et codage de source
- `Content-Transfer-Encoding:` codage de canal
  - `ASCII` (7-bits – pas de codage nécessaire)
  - `8bit` ou `binary` (suppose ESMTP sait transférer),
  - `quoted-printable`
  - `base64`
    - 24 bits $\rightarrow$ 4 $\times$ 6 bits codé en ASCII

Champs optionnels:

- `Content-ID:`
- `Content-Description:` descrip. « en clair » du contenu
- `Content-Disposition:` présentation par l'UA de PJ

Exemples de codage des textes

Texte	ISO-8859-1	UTF-8
Noël !	4e 6f eb 6c 20 21	4e 6f c3ab 6c 20 21
Nina написала:		4e 69 6e 61 20 d0bd d0b0 d0bf d0b8 d181 d0b0 d0bb d0b0 3a 20

C'est le codage "source": (pb1): numérisation en bit de lettres
Codage "canal" (pb2): comment faire passer des octets
sur un canal SMTP
qui ne sait transférer que de l'ASCII (codes <128: 00 à 7f)

Codage quoted-printable (QP)

- Convient pour du texte contenant quelques caractères non ASCII
- Codage en ASCII, seuls les caractères 8bits sont remplacés par: =Hex-code

Noël

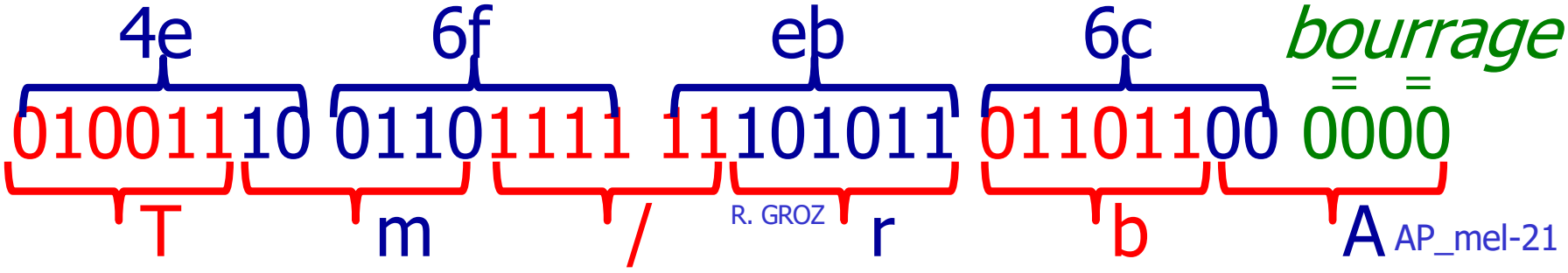
- Codage source ISO-8859-1: 4e 6f eb 6c
- Codage canal QP: N o =EB l

Codage base64 (codage de canal)

- Comment faire passer des codages « 8bits » par un canal (ex mél SMTP) qui ne transfère que « 7bits » ASCII ?
- 3 x 8 bits = 4 x 6 bits
  - 6 bits: 2^6 caractères; 26 min, 26 MAJ, 10 chiffres, + /

Binary	ASCII	Binary	ASCII	Binary	ASCII	Binary	ASCII
000000	A	010000	Q	100000	g	110000	w
000001	B	010001	R	100001	h	110001	x
000010	C	010010	S	100010	i	110010	y
000011	D	010011	T	100011	j	110011	z
000100	E	010100	U	100100	k	110100	0
000101	F	010101	V	100101	l	110101	1
000110	G	010110	W	100110	m	110110	2
000111	H	010111	X	100111	n	110111	3
001000	I	011000	Y	101000	o	111000	4
001001	J	011001	Z	101001	p	111001	5
001010	K	011010	a	101010	q	111010	6
001011	L	011011	b	101011	r	111011	7
001100	M	011100	c	101100	s	111100	8
001101	N	011101	d	101101	t	111101	9
001110	O	011110	e	101110	u	111110	+
001111	P	011111	f	101111	v	111111	/

- N o ë l → T m / r b A = =



```
---559023410-851401618-1086805356=:18859
Content-Type: TEXT/PLAIN; charset=ISO-8859-15
Content-Transfer-Encoding: QUOTED-PRINTABLE

Bonjour/soir
Vous trouverez en pi=E8ce jointe mon rapport de stage, au
   format PDF,
lisible =E0 l'=E9cran.
---559023410-851401618-1086805356=:18859
Content-Type: APPLICATION/PDF; name="rapport_master.pdf"
Content-Transfer-Encoding: BASE64

JVBERi0xLjIKJcfsj6IKMzkgMCBvYmoKPDwvTGVuZ3RoIDQwIDAgUi9GaWx0
ZXIgL0ZsYXRlRGVjb2RlPj4Kc3RyZWFtCnictVRLbtswEO1ap+AyXYjm/7N0
...
---------------02050703090401070807010З
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 8bit

Vous trouverez en pièce jointe mon rapport, lisible à l'écran.
```

Content-Type

```
text/plain
text/html
image/gif
image/jpeg
audio/basic
audio/mpeg
application/octet-stream
application/postcript
application/pdf
...
```

- Insertion de PJ

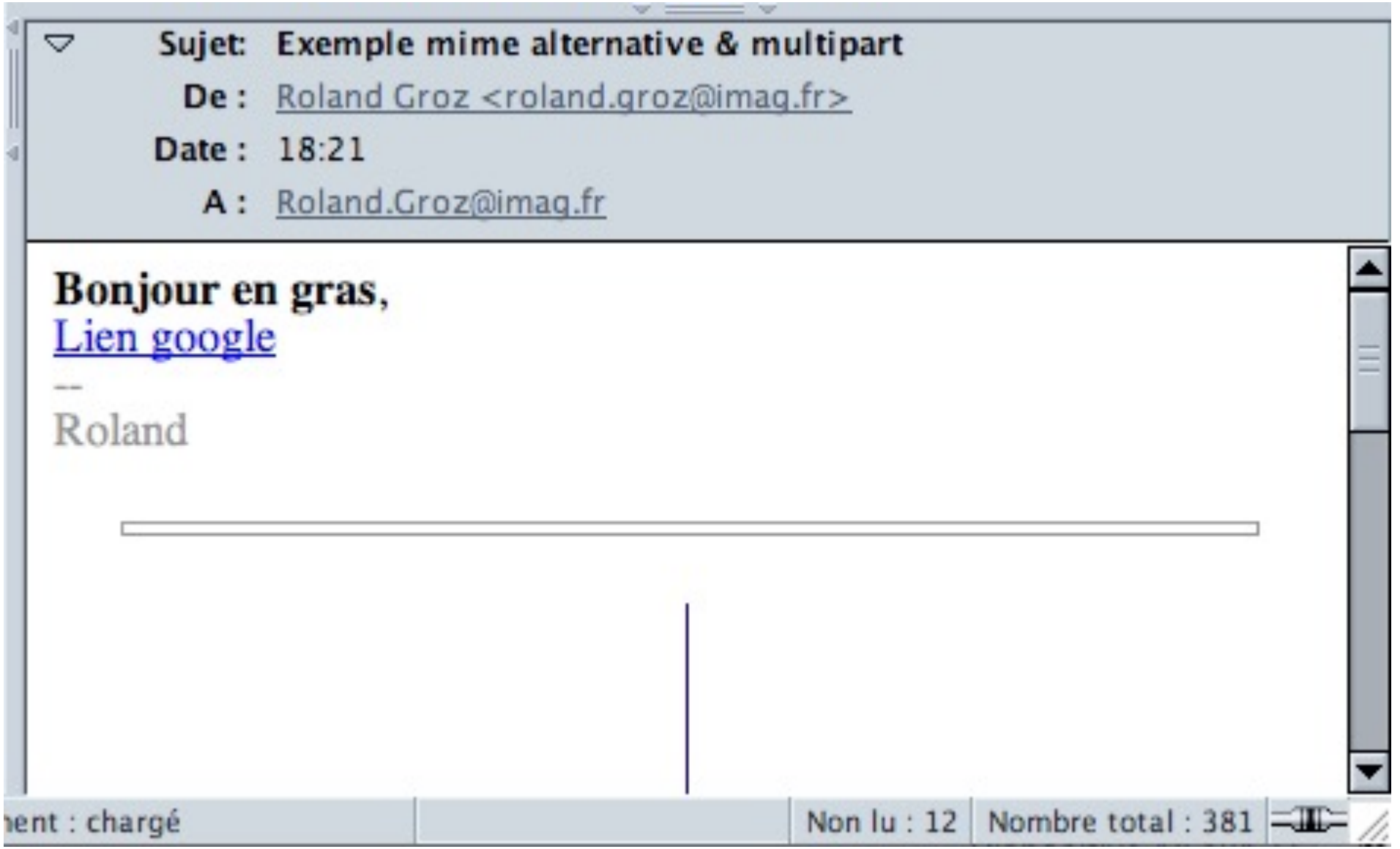
`multipart/mixed`

- Adaptation aux capacités de l'UA (par ex: text brut + HTML)

`multipart/alternative`

NB: HTML peut inclure des liens à des img etc.

Exemple de message multipart



```
Subject: Ex. mime alt+mixed
Content-Type: multipart/mixed;
 boundary="------------0820102"

This is a multi-part message in MIME format.
--------------0820102
Content-Type: multipart/alternative;
 boundary="------------0500906"

--------------0500906
Content-Type: text/plain; charset=us-ascii;
      format=flowed
Content-Transfer-Encoding: 7bit

  Bonjour en gras,
Lien google <http://google.fr>
--
Roland

--------------0500906
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01
       Transitional//EN">
<html>
<body>
    <b>Bonjour en gras</b>,<br>
  <a href="http://google.fr">Lien
       google</a><br>
  <div class="moz-signature">-- <br>
 Roland</div>
</body>
</html>

--------------0500906--

--------------0820102
Content-Type: image/gif; x-mac-type="0"; x-
       mac-creator="0";
 name="trait.gif"
Content-Transfer-Encoding: base64
Content-Disposition: inline;
 filename="trait.gif"

R0lGODlhAgCQAZH/AP///xgNiAAAAAAAACwAAAAAAgCQ
       AUACJgyMp8nrDZ+MdNqKr858+w5+
YkiOZomeasqubgu/ckzPdo3feh4WADs=
--------------0820102--
```

Bilan chapitre AP_mel: notions essentielles

- Architecture de la messagerie:
  - Cas nomade: protocoles POP et IMAP
  - Cas simple: notions de UA, MTA
- Comprendre le déroulement d'un protocole simple: SMTP
- Structure des messages
  - Enveloppes et en-têtes
  - Format MIME et codages

Google

APplications

S/MIME - Secure/Multipurpose Internet Mail Extension

- Sign and/or Encrypt messages
  - **Signed data** (digital signature)
    - encrypt message digest with private key of sender
    - content plus signature encoded using base64
    - reader without S/MIME cannot read the content
  - **Clear signed data** – only digital signature is encrypted
    - reader without S/MIME can read the content
  - **Enveloped data** – encrypted content
  - **Signed and enveloped data** – signed only and encrypted only, entities may be nested
- Uses X.509 certificates
  - each client must be configured with list of trusted keys (CA) used to verify incoming signatures

S/MIME signed-data