
Redes de Computadores

(RCOMP – 2015/2016)



Correio eletrónico.
Protocolos SMTP, POP3 e IMAP.
Formato MIME

Correio eletrónico

O objetivo do correio eletrónico é o envio de mensagens *off-line* (não interativo) entre utilizadores. A única diferença relativamente a um sistema de correio tradicional é que as mensagens não são escritas em papel.

Num sistema de correio, o destinatário pode não estar presente no momento em que a mensagem chega (*off-line*). Consequentemente é necessário um local onde o *carteiro* possa colocar as mensagens até que o destinatário *apareça* para as recolher.

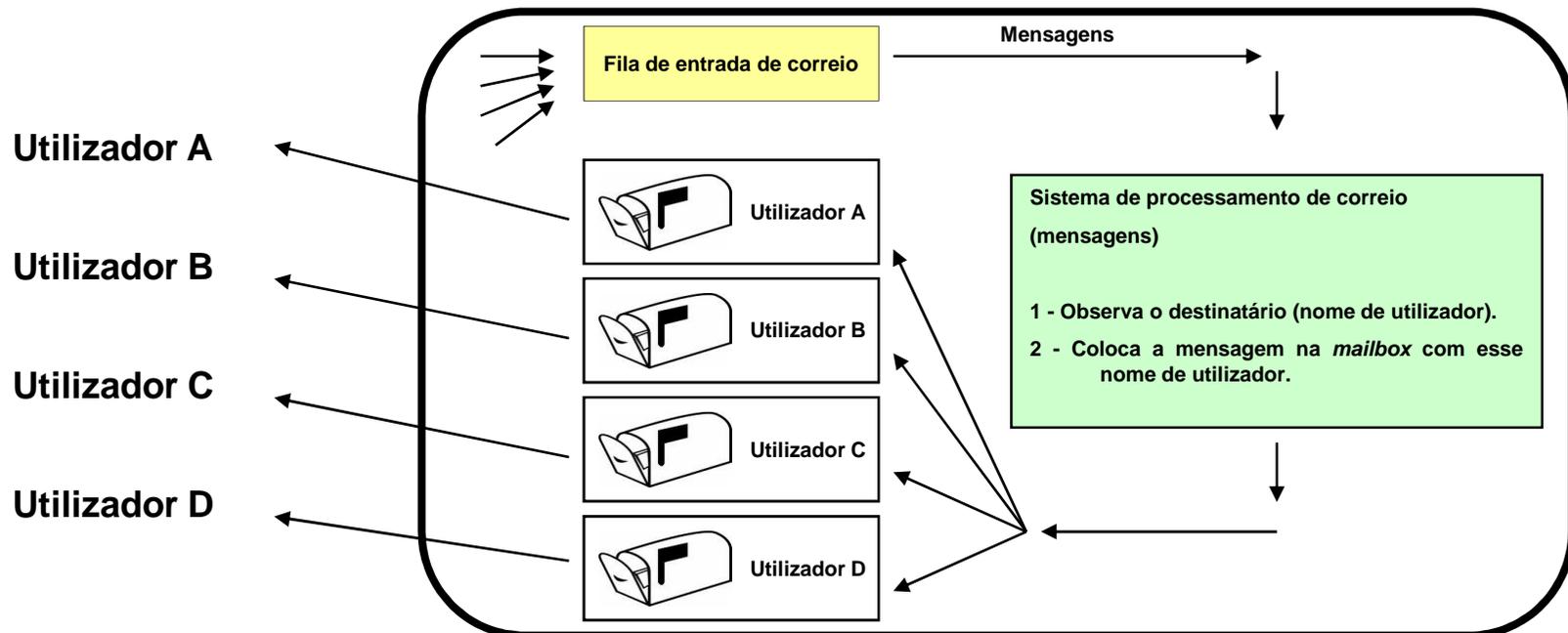
Cada destinatário possui um local de armazenamento de mensagens onde o sistema de correio deposita as mensagens que lhe são destinadas. Esse local de armazenamento é conhecido por caixa-do-correio (*mail-box*).



Caixas de correio – *mailboxes*



O sistema de correio eletrónico típico tem uma estrutura bastante simples:



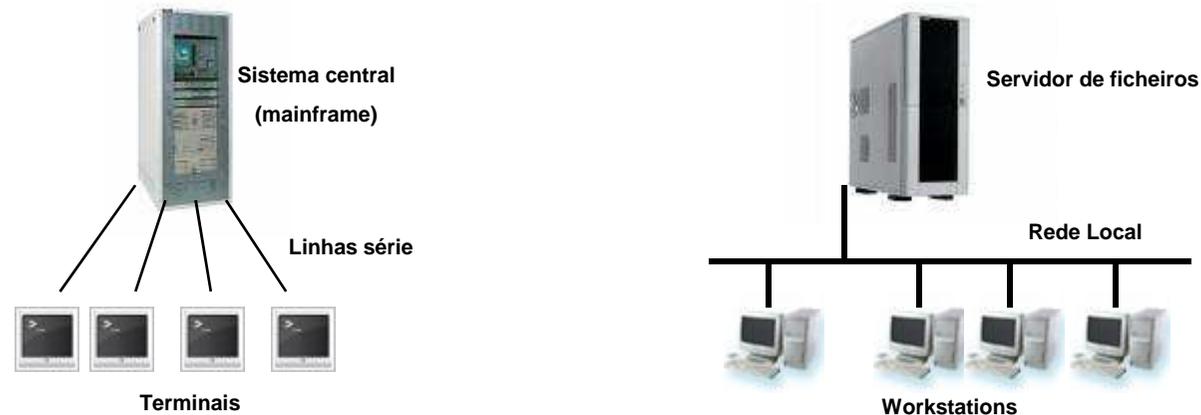
Cada mensagem tem um remetente e um destinatário que são nomes de utilizador. Cada utilizador possui uma *mailbox*, apenas o utilizador e o sistema podem aceder à *mailbox*.

O sistema pode ser implementado usando um sistema de ficheiros com permissões de utilizador.

Correio eletrónico baseado em sistema de ficheiros

Os sistemas de correio eletrónico desenvolveram-se usando simples sistemas de ficheiros partilhados. Tanto as *mailboxes* dos utilizadores como a fila de entrada de correio são objetos do sistema de ficheiros, ficheiros e/ou diretórios.

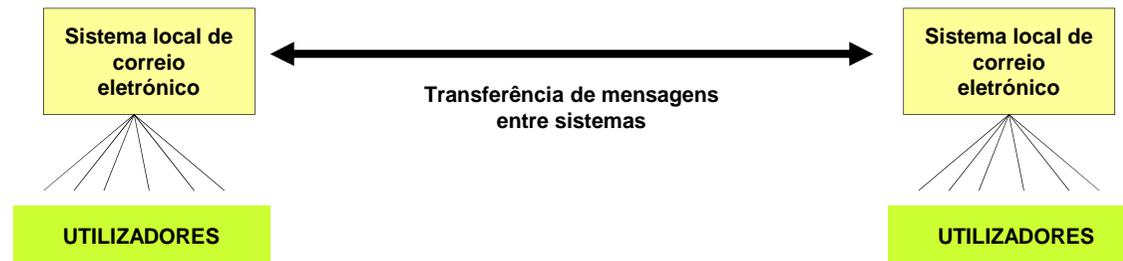
Um sistema deste tipo está totalmente contido num único servidor e não utiliza a rede diretamente.



Uma vez que o sistema está limitado a um único servidor/sistema, a identificação dos utilizadores faz-se recorrendo apenas ao nome do utilizador.

Correio eletrónico em rede

Com o progressivo desenvolvimento das redes de computadores, surgiu a necessidade de alargar o funcionamento dos sistemas de correio eletrónico existentes de tal modo que, utilizadores de sistemas centrais diferentes possam também comunicar uns com os outros.

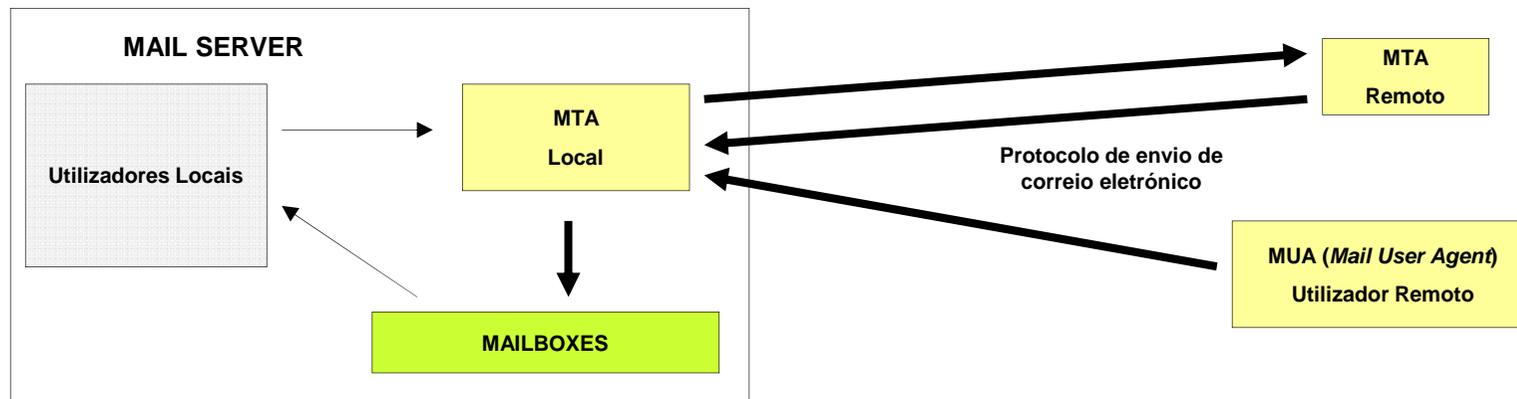


A comunicação entre sistemas centrais de correio recorre a uma infraestrutura de rede e será realizada segundo um protocolo de aplicação reconhecido pelos dois intervenientes.

A identificação dos utilizadores (remetente e destinatário) necessita agora de mais um elemento, a identificação do sistema de correio a que esse utilizador pertence, por exemplo: ***utilizador@sistema***

MTA – Mail Transport Agent

O sistema de processamento de correio residente em cada sistema passa a ter a capacidade de dialogar através da rede com outros sistemas e é designado de MTA (*Mail Transport Agent* ou *Message Transfer Agent*).



Os utilizadores locais continuam a usar diretamente o sistema de ficheiros para enviarem correio e lerem o correio das respetivas *mailboxes*.

O mesmo protocolo que é usado para envio de correio entre os MTA pode também ser usado para utilizadores remotos enviarem correio, através de software adequado designado de MUA (*Mail User Agent*).

SMTP – *Simple Mail Transfer Protocol*

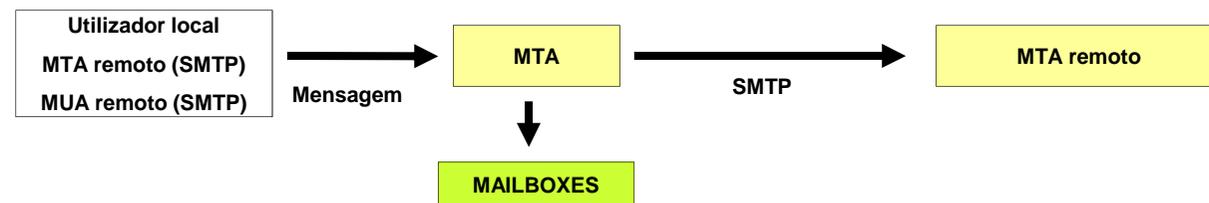
Na Internet, o protocolo de aplicação mais usado para transferir correio entre sistemas é o SMTP. A identificação dos utilizadores (*mailboxes*) usa a forma:

UTILIZADOR@NOME-DNS

NOME-DNS é o nome DNS qualificado do servidor de correio onde a *mailbox* desse utilizador se encontra.

Quando o MTA processa uma mensagem verifica se o *NOME-DNS* corresponde ao seu próprio nome, nessa caso procura a *mailbox* local correspondente ao *UTILIZADOR* e deposita lá a mensagem.

Se o *NOME-DNS* pertence a outro servidor, contacta esse servidor (resolvendo o nome DNS) e envia-lhe a mensagem usando o protocolo SMTP.



SMTP – Nome de domínio e registos MX

A identificação de *mailboxes* usa a forma **UTILIZADOR@NOME-DNS**. *NOME-DNS* identifica o servidor de correio, o endereço correspondente será contactado para efeitos de envio de correio.

Na prática torna-se mais cómodo identificar utilizadores em domínios DNS e não em servidores. Para conseguir isso pode-se recorrer ao domínio acima e criar um registo A que provoque a resolução do nome de domínio para o endereço do servidor de correio.

Atualmente o sistema DNS implementa registos apropriados para resolver este problema de uma forma mais eficiente, os registos MX (*Mail Exchanger*). Os registos MX associam diretamente o nome do domínio a um ou vários endereços dos servidores de correio desse domínio.

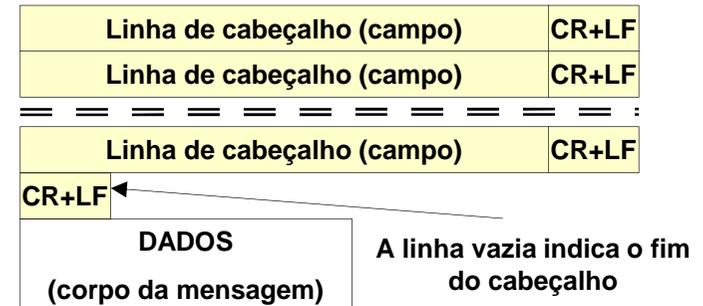
Os MTA atuais resolvem o nome do domínio pedindo o respetivo registo MX e não o registo A.

SMTP – Formato das mensagens

As mensagens de correio eletrónico são constituídas por um cabeçalho seguido do corpo da mensagem.

Cada linha de cabeçalho contém um identificador de campo e o respetivo valor, separado por “:”.

Os valores dos campos podem ocupar mais do que uma linha, nesse caso as linhas de continuação devem começar com um espaço em branco.



EXEMPLOS

```
From: Utilizador <user@dei.issep.ipp.pt>
Subject: Mensagem de Teste
Date: Wed, 21 May 2008 15:54:50 +0100
Reply-To: <user@ipp.pt>
To: <admin@dei.issep.ipp.pt>
Cc: <root@issep.ipp.pt>
Return-Path: <erros@dei.issep.ipp.pt>
Message-ID: <011701c8bb52$a1ca6f10$e55f4d30$@dei.issep.ipp.pt>
In-Reply-To: <8AB511FE5C834F8F8308E52E6437D5DB@ipp.pt>
```

SMTP – Protocolo

O SMTP usa uma ligação TCP para transferir a mensagem de correio eletrónico, para esse efeito os MTA aceitam ligações TCP no número de porto 25. Depois de estabelecida a ligação inicia-se um diálogo baseado em linhas de texto terminadas por CR+LF, seguindo um conjunto de comandos suportado (RFC 821). No exemplo seguinte o texto enviado pelo cliente encontra-se a **negrito**:

```
220 frodo.dei.isep.ipp.pt ESMTP Mailer DEINET-1.1; Wed, 21 May 2008 18:15:30 +0100
HELO frodo.dei.isep.ipp.pt
250 frodo.dei.isep.ipp.pt Hello pci14ppp.dei.isep.ipp.pt [193.136.62.213], pleased to meet you
MAIL FROM:<andre@dei.isep.ipp.pt>
250 2.1.0 <andre@dei.isep.ipp.pt>... Sender ok
RCPT TO:<asc@isep.ipp.pt>
250 2.1.5 <asc@isep.ipp.pt>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
From: "Andre Moreira" <andre@dei.isep.ipp.pt>
To: <asc@isep.ipp.pt>
Subject: Teste

Mensagem de teste
.
250 2.0.0 m4LHFUWx004991 Message accepted for delivery
QUIT
221 2.0.0 frodo.dei.isep.ipp.pt closing connection
```

ESMTP – *Extended SMTP / Enhanced SMTP*

O ESMTP (RFC 1869) possui um conjunto mais vasto de comandos do que o SMTP normal. Os clientes que desejam usar ESMTP em lugar de SMTP usam o comando *EHLO* em lugar do habitual comando *HELO*.

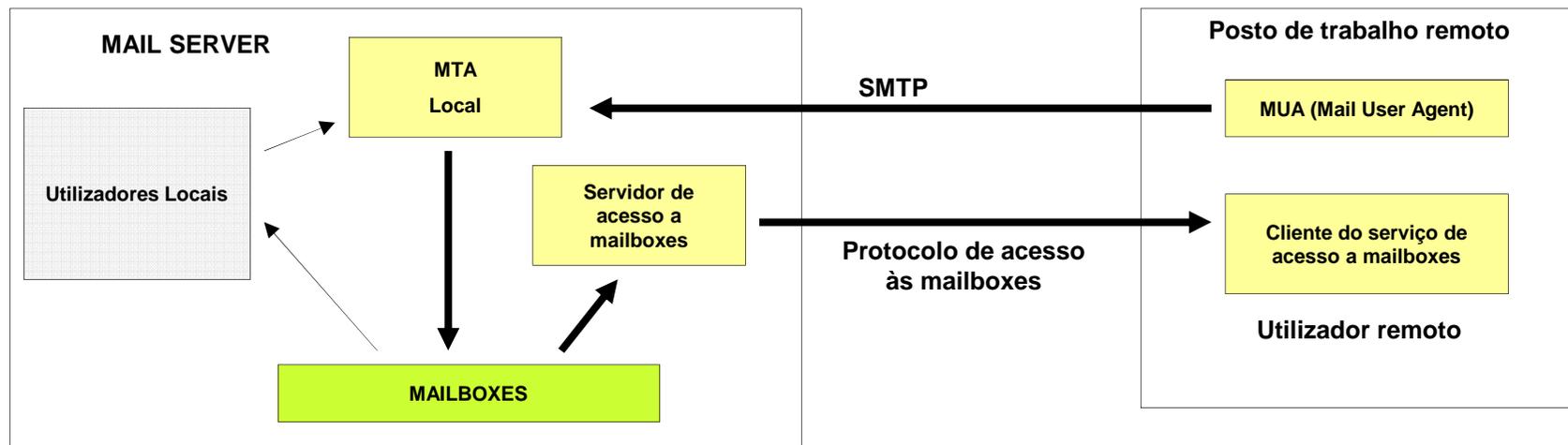
Se o servidor suporta ESMTP responde com um código de sucesso (250), caso contrário responde com um código de erro (5xx), nesse caso o cliente terá de enviar um *HELO* e limitar-se ao SMTP normal.

```
220 frodo.dei.issep.ipp.pt ESMTP Mailer DEINET-1.1; Wed, 21 May 2008 18:46:30 +0100
EHLO frodo.dei.issep.ipp.pt
250-frodo.dei.issep.ipp.pt Hello pci14ppp.dei.issep.ipp.pt [193.136.62.213], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE 33554432
250-DSN
250-ETRN
250-AUTH DIGEST-MD5
250-DELIVERBY
250 HELP
QUIT
```

A identificação das extensões suportadas pelo servidor é fornecida ao cliente juntamente com a resposta ao *EHLO*.

Correio eletrónico – Acesso remoto

Os utilizadores remotos de um sistema de correio podem recorrer ao protocolo SMTP para emitir mensagens, mas para poderem aceder às respetivas *mailboxes* torna-se necessário um protocolo adicional.



Atualmente os dois protocolos mais usados para acesso a *mailboxes* remotas são o IMAP4 e o POP3.

POP3 – *Post Office Protocol version 3*

O protocolo POP3 (RFC 1939) usa uma ligação TCP dirigida ao porto 110 do servidor, as mensagens trocadas entre o cliente e o servidor são comandos sob a forma de linhas de texto terminadas por CR+LF.

Depois de o cliente POP3 receber a frase de identificação do servidor deve autenticar-se, o exemplo seguinte apresenta a “negrito” as linhas enviadas pelo cliente:

```
+OK POP3 frodo.dei.isep.ipp.pt 2004.89mdk server ready
USER andre
+OK User name accepted, password please
PASS xxxxxxxx
+OK Mailbox open, 0 messages
STAT
+OK 0 0
LIST
+OK Mailbox scan listing follows
.
QUIT
+OK Sayonara
```

Além da autenticação baseada nos comandos USER/PASS, que só deve ser usada sobre ligações seguras (POP3S), também é suportada a autenticação tipo CHAP com o comando APOP.

IMAP4 – *Internet Message Access Protocol*

O protocolo POP3 é bastante limitado, normalmente serve apenas para obter o conteúdo da *mailbox* do utilizador e a ligação com o servidor é terminada após essa consulta integral.

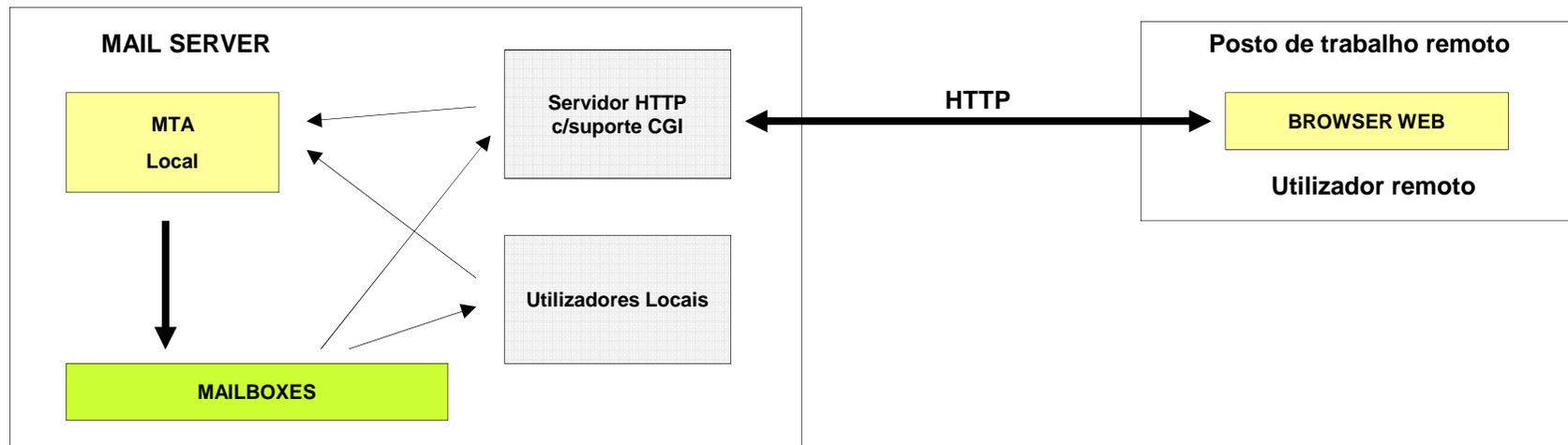
O protocolo IMAP4 (IMAP4rev1 - RFC 3501) é bastante mais interativo, também usa uma conexão TCP, neste caso para o porto 143, mas normalmente a ligação do cliente com o servidor mantém-se ativa constituindo uma sessão interativa.

Entre outras funcionalidades, o IMAP4 permite:

- Consulta da lista de mensagens disponíveis na *mailbox*.
- Leitura de uma mensagem específica, ou até uma parte de uma mensagem.
- Marcação de mensagens com estados (no servidor).
- Organização da *mailbox* em pastas (no servidor).
- Pesquisa de mensagens (no servidor).

WebMAIL

Muitas das vantagens equivalentes às do IMAP4 estão atualmente disponíveis usando sistemas conhecidos por *WebMail*. Trata-se de aplicações CGI que são executadas por um servidor HTTP residente na mesma máquina onde o sistema de correio está a funcionar.



Os CGI que constituem o *WebMail* interagem com o sistema de correio eletrónico do mesmo modo que os utilizadores locais. Deste modo eliminam todos os inconvenientes do acesso remoto sem necessidade de clientes especiais.

MIME - *Multipurpose Internet Mail Extensions*

O MIME é um formato de mensagens que permite ultrapassar as limitações das mensagens de texto simples. Embora tenha sido desenvolvido para o correio eletrónico é atualmente usado em muitos outros protocolos como por exemplo o HTTP.

Uma mensagem de correio eletrónico é identificada como estando em formato MIME através da presença do campo *MIME-Version* no cabeçalho, a versão atualmente em uso é a “1.0”.

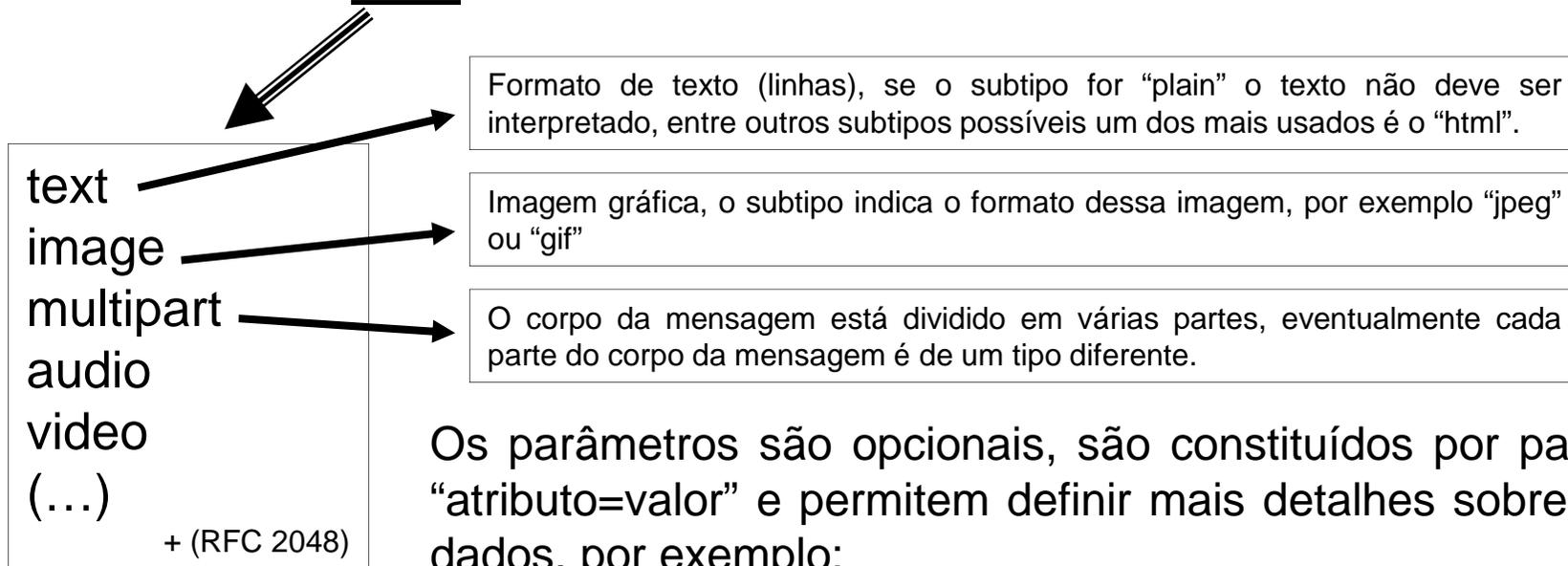
As mensagens em formato MIME possuem outras linhas de cabeçalho fundamentais para identificar quer o tipo de dados transportados no corpo (*Content-Type:*) quer a forma como esses dados estão representados (*Content-Transfer-Encoding:*).

No contexto do SMTP a mensagem é obrigatoriamente de texto, contudo esse texto pode ser usado para representar qualquer tipo de dados.

MIME – “Content-Type”

O campo de cabeçalho *Content-Type* fornece informação sobre o tipo de dados transportados no corpo da mensagem:

Content-Type: tipo/subtipo [; parâmetro [; parâmetro [...]]]



```
Content-Type: text/html; charset=us-ascii
```

O campo *Content-Type* é importante porque permite à aplicação de destino interpretar os dados para os apresentar corretamente ao utilizador.

MIME – “Content-Type: multipart”

O conteúdo *multipart* é bastante usado porque permite transportar numa única mensagem vários tipos de conteúdos diferentes em partes separadas. Exemplo:

```
MIME-Version: 1.0
Content-Type: multipart/mixed;
          boundary="-----_NextPart_000_038E_01C8BB64.2C534EC0"
Date: Wed, 21 May 2008 17:00:14 +0100

-----_NextPart_000_038E_01C8BB64.2C534EC0
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Bom dia, em anexo segue o ficheiro pedido.
Cumprimentos

-----_NextPart_000_038E_01C8BB64.2C534EC0
Content-Type: application/msword; name="documento.doc"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="documento.doc"

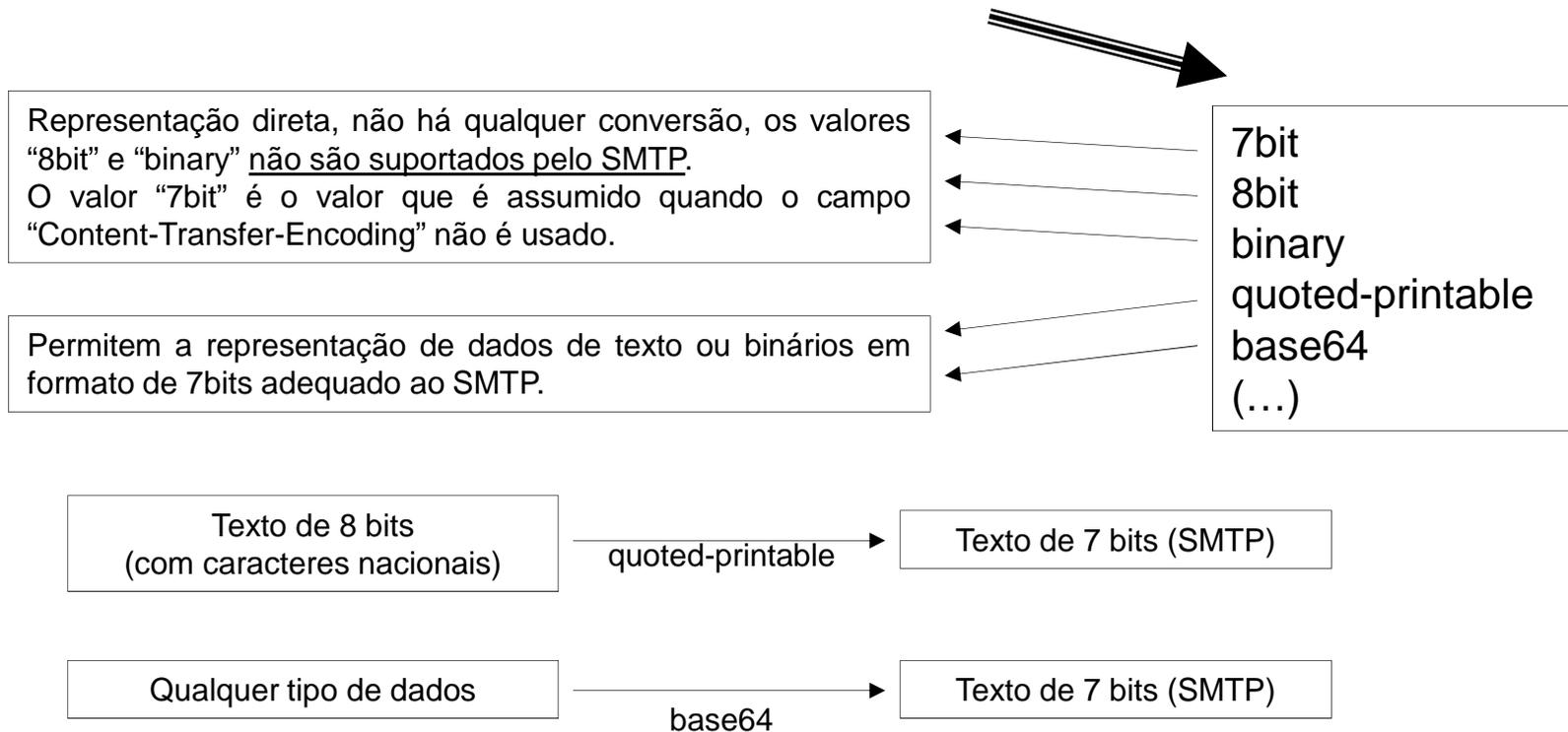
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAA==

-----_NextPart_000_038E_01C8BB64.2C534EC0--
```

MIME – “Content-Transfer-Encoding”

O SMTP apenas suporta texto simples com caracteres de 7 bits, todos os outros tipos de conteúdos tem de ser representados recorrendo apenas a este formato de texto simples.

Content-Transfer-Encoding: codificação



MIME – “Content-Transfer-Encoding: **quoted-printable**”

O objetivo da representação em formato “quoted-printable” é permitir a representação de qualquer tipo de texto em formato de 7 bits.

A codificação baseia-se, entre outros, nos seguintes princípios:

Qualquer caractere de 8 bits (octeto), com a exceção de CR/LF pode ser representado pela sequência “=XX”, onde XX representa o valor do octeto em notação hexadecimal.

Os caracteres com códigos ASCII 33 a 60 e 62 a 126 não necessitam de ser convertidos.

Os caracteres brancos (códigos ASCII 7 e 32) também não necessitam de ser convertidos, mas se ocorrerem no fim da linha, o final da linha terá de ser assinalado com o sinal “=”.

As linhas codificadas não podem ter mais do que 72 caracteres, o sinal “=” permite criar uma quebra de linha “soft”, apenas para efeitos de texto codificado.

MIME – “Content-Transfer-Encoding: **base64**”

A representação em formato *base64* pode ser usada para qualquer tipo de dados. A sua maior desvantagem é que os dados codificados ocupam cerca de 33% mais espaço do que os dados originais.

Foi escolhido um conjunto de 64 caracteres adequado: “ **A..Z a..z 0..9 + /** ”
Com 64 caracteres pode-se representar qualquer conjunto de 6 bits, $\log_2(64) = 6$.

Os octetos de entrada são agrupados em conjuntos de 3, cada 3 octetos (24 bits) vão produzir 4 caracteres no texto codificado. O texto codificado está limitado a linhas de 76 caracteres, mas na descodificação as mudanças de linha são ignoradas.

O sinal “=” é usado para indicar que o alinhamento do fim da mensagem não corresponde a 24 bits, nesse caso procede-se a um enchimento (*padding*) com bits 0, serão usados um ou dois sinais “=” conforme tenha sido necessário um enchimento de 8 ou 16 bits zero.