

Proteção de Email

Estrutura dos servidores de mail

- Estrutura dos servidores de mail
 - Normalmente o utilizador não fala diretamente com o recetor
 - Servidor de mail dedicado
 - (Message Transfer Agents: MTA)
 - A origem e o destino são chamados
 - Mail User Agents (MUA)
 - O email pode passar por vários MTAs

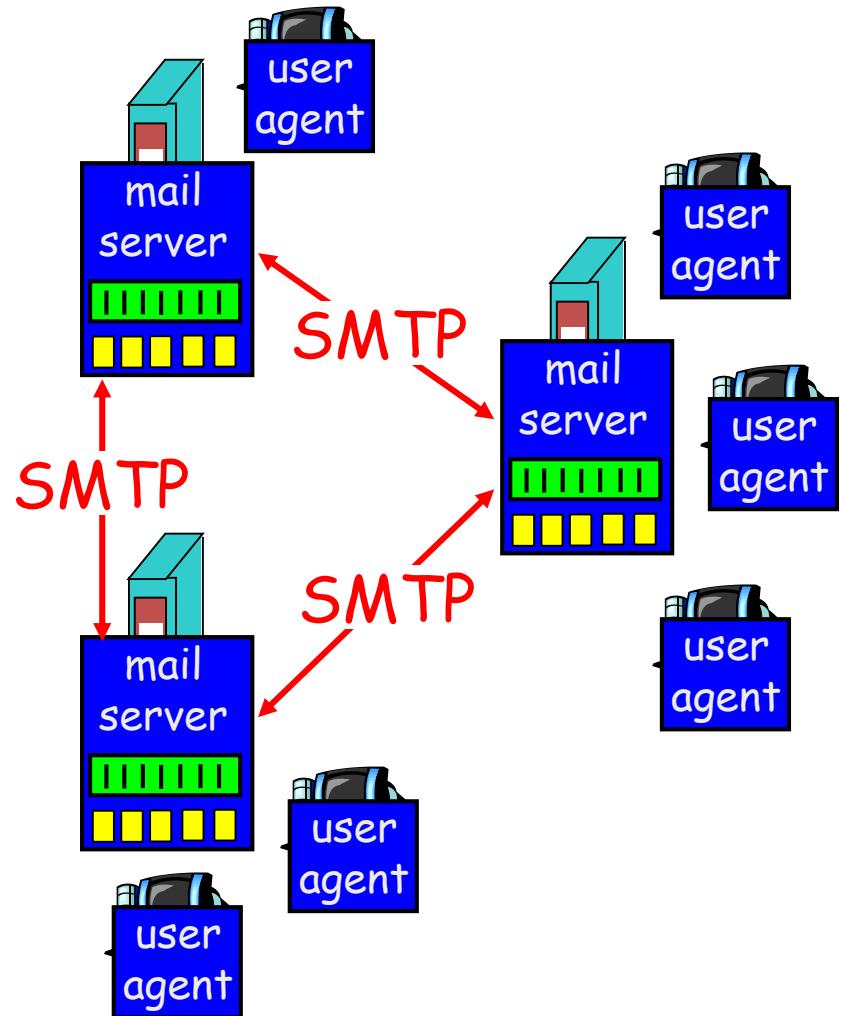
Envio de mail

Componentes:

- user agents
- mail servers
- simple mail transfer protocol: SMTP

User Agent

- “mail readers”
- Compor e ler mensagens de mail
- Ex.: Eudora, Outlook, elm
- Mensagens enviadas e recebidas são guardadas no servidor

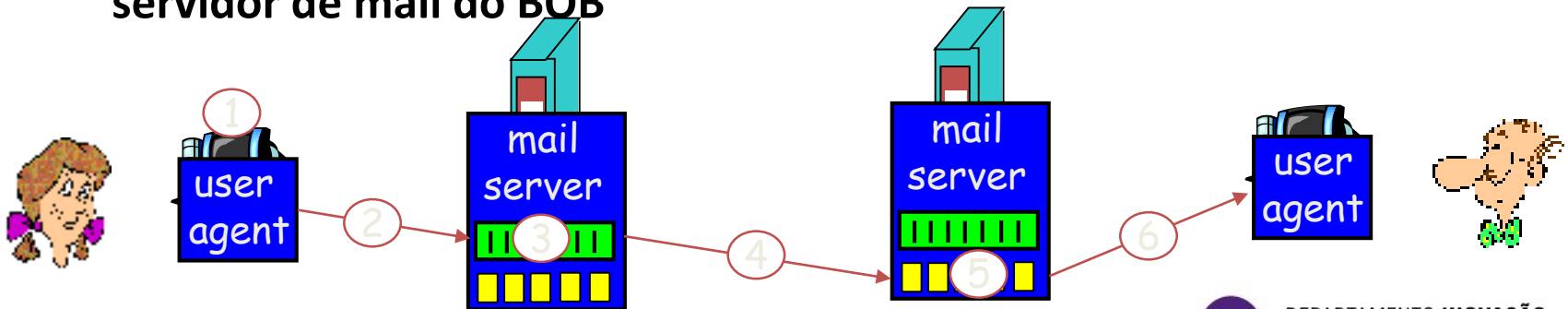


SMTP [RFC 5321]

- Utiliza o TCP para a transferência de mensagens de mail entre o cliente e o servidor, port 25/587
- Transferência direta: (troca de mensagens entre servidores)
- Transferência em três fases
 - handshaking (greeting)
 - Transferência de mensagens
 - Encerramento
- Interação comando/resposta
- Comandos: texto ASCII
- Resposta: código do estado e frase

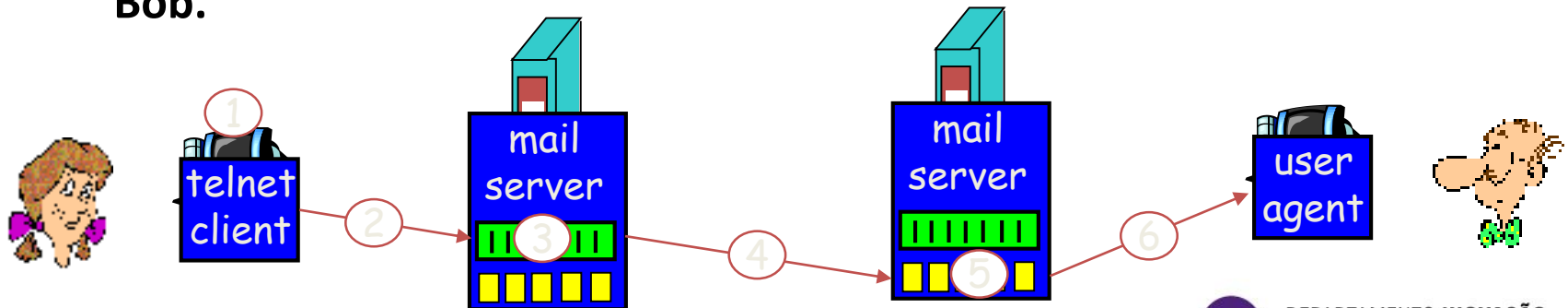
Envio de mensagem

- 1) Alice utiliza o UA para compor uma mensagem para bob@upt.pt
- 2) O UA da Alice envia a mensagem para o seu servidor de mail; que a coloca numa fila de mensagens
- 3) A parte do cliente do SMTP abre uma conexão com o servidor de mail do BOB
- 4) O cliente de SMTP envia a mensagem da Alice sobre a conexão TCP
- 5) O servidor de mail do Bob coloca a mensagem na mail box do Bob
- 6) O Bob utiliza o seu UA para ler a mensagem



Envio de mensagens

- 1) A Alice executa o cliente de telnet
- 2) O cliente de telnet da Alice abre uma conexão para um servidor de mail (Alice ou Bob) na porta 25
- 3) A Alice utiliza comandos de SMTP para codificar uma mensagem e enviar para o Bob.
- 4) O cliente de SMTP envia a mensagem da Alice para o servidor do Bob
- 5) O servidor de mail do Bob coloca a mensagem na mail box do Bob
- 6) O Bob lê a mensagem utilizando o UA



```
S: 220 smtp.example.com ESMTP Postfix          /* 220: service ready */
C: HELO relay.example.org                      /* identify urself */
S: 250 Hello relay.example.org, I am glad to meet you /* request ok */
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>          /* start mail input */
C: From: "Bob Example" <bob@example.org>
C: To: Alice Example <alice@example.com>
C: Date: Tue, 15 Jan 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye {The server closes the connection} /* close channel */
```

Listas de distribuição

- Listas de distribuição
 - Pode ser necessário enviar uma mensagem para um grupo de pessoas
 - Como mapear um endereço para uma lista de endereços:
 - Expandidas localmente
 - Expandidas remotamente

Expansão local

Vantagens da expansão local

É mais fácil prevenir loops de mail

É mais fácil de evitar o envio de múltiplas cópias para um utilizador

Expansão remota

- Vantagens da expansão remota
 - Pode enviar mensagens para listas de utilizadores que não conhece
 - Reduzir o tráfego enviado pelo dono da mensagem
 - Melhorar a eficiência: podem existir várias listas mantidas em vários servidores

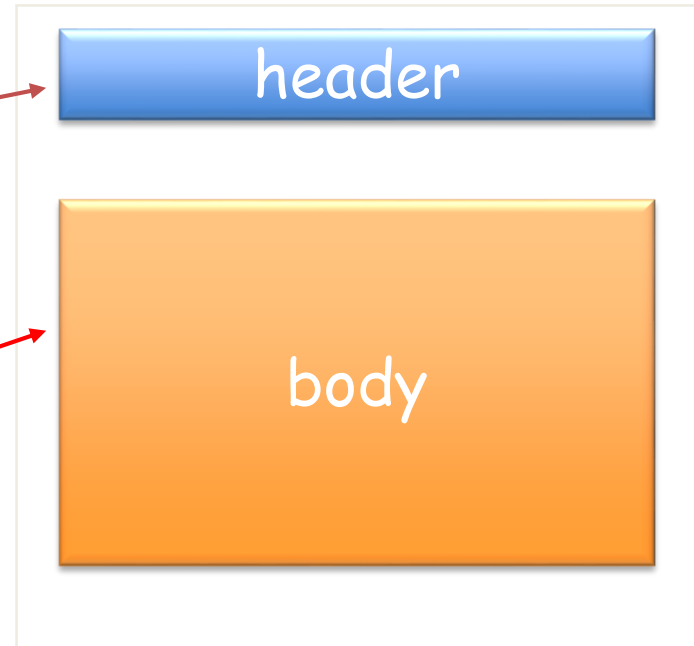
Formato das mensagens de mail

■ Linhas do cabeçalho

- To:
- From:
- Subject:

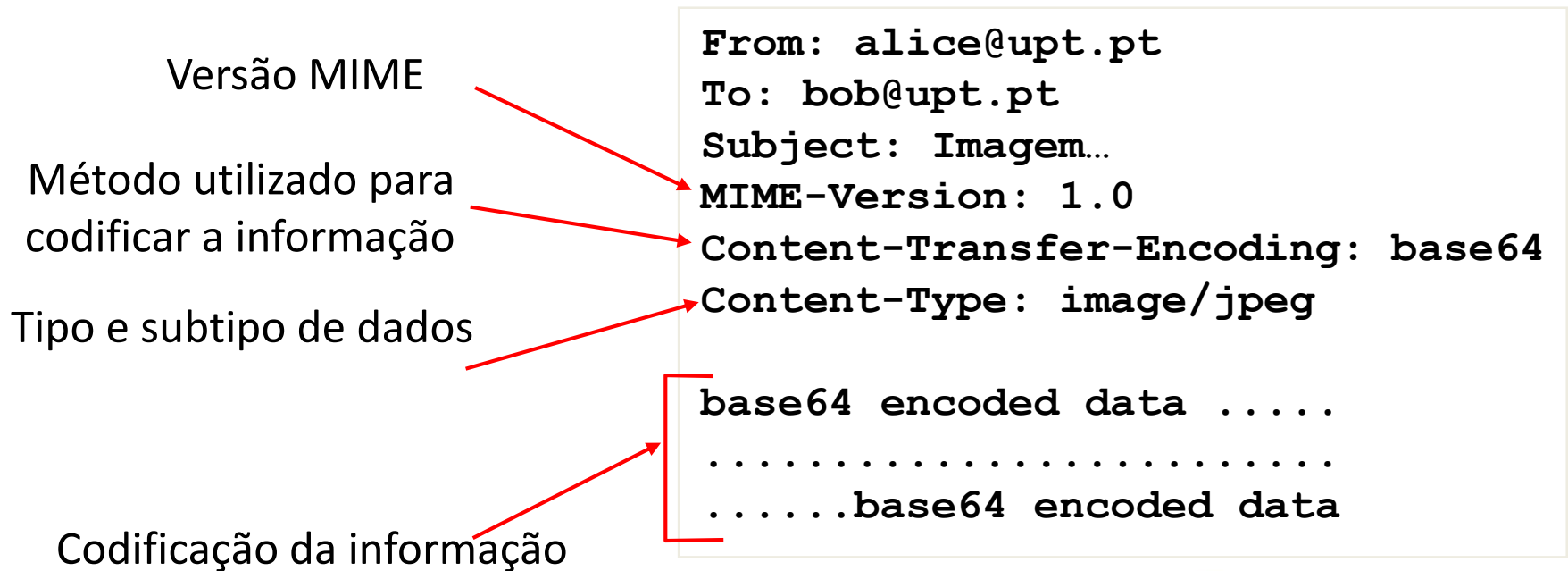
■ Corpo da mensagem

- Mensagem a enviar
(caracteres ASCII)

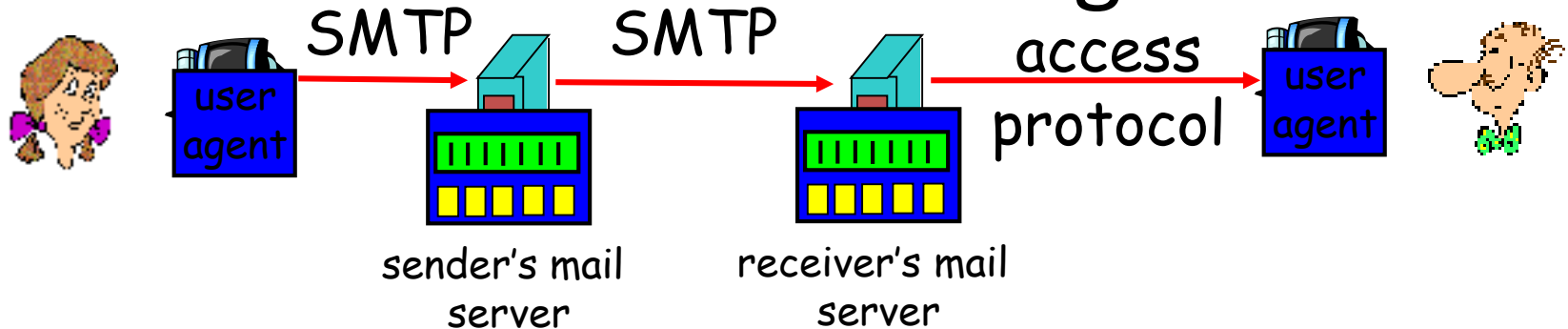


Extensões multimédia

- Linhas adicionais no cabeçalho da mensagem para declarar conteúdo MIME



Protocolos de recepção mensagens



- **SMTP:**
- **POP: Post Office Protocol [RFC 1939]**
- **IMAP: Internet Mail Access Protocol [RFC 1730][port 143]**

POP3 (port 110)

telnet alunos.upt.pt 110

Autorização

■ Comandos do cliente:

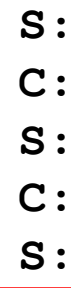
- user: qual o utilizador
- pass: password

■ Respostas do servidor

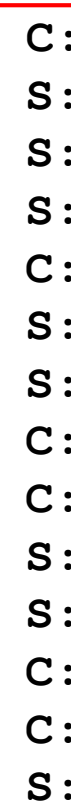
- +OK
- -ERR

Transação:

- list: lista os numeros das msgs
- retr: ler a mensagem numero
- dele: eliminar
- quit



```
S: +OK POP3 server ready
C: user alice
S: +OK
C: pass *****
S: +OK user successfully logged on
```



```
C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: <message 1 contents>
S: .
C: dele 1
C: retr 2
S: <message 2 contents>
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off
```

- IMAP: Internet Message Access Protocol
 - Suporta operações online e offline
 - Pode ficar uma cópia das mensagens no servidor
 - Suporte para autenticação encriptada
 - Informação sobre o estado da mensagem
 - Criação de diretórios na pasta do servidor
 - Pesquisa na lado do servidor

Segurança de mail

- Características do mail seguro
 - Privacidade
 - Autenticação
 - Integridade
 - Não repudição
 - Prova de entrega

- Confidencialidade
 - Várias fontes que podem violar a confidencialidade o mail: eavesdropper, administrador do serviço
 - Privacidade ponto a ponto
 - Não é eficiente utilizar chaves públicas para encriptar a informação
 - Vários utilizadores

Privacidade

- Privacidade com listas de distribuição
 - Expansão remota:
 - o emissor apenas precise de partilhar a chave com o servidor remoto
 - Expansão local:
 - Estabelecer uma chave com cada recetor da lista

Autenticação

- Autenticação do emissor
 - Assina a mensagem com a chave privada do emissor
 - Encripta a mensagem com um par de chaves
 - Autenticação do emissor em listas de distribuição
 - Utilização de assinaturas digitais
 - Se se utilizar a chave secreta o gestor de listas adiciona a sua informação da autenticação

Integridade

- Integridade de mensagens
 - A maior parte das vezes é integrada com a autenticação da origem

Não repudição

- Não repudição

- (Em Segurança da Informação, "não-repudição" se refere à incapacidade de um dos participantes de uma transação em mais tarde negar que tenha participado dela)
- Com chaves públicas
 - Assinatura digital
- Não repudição baseada na tecnologia da chave pública
- Não repudição com chaves secretas

Entrega

- Prova de submissão
 - O MTA que envia a mensagem disponibiliza um digest assinado do mail
- Prova de entrega
 - O recetor assina um recibo da mensagem

Ataques possíveis

Spoofing
(inacreditavelmente
simples)

Eavesdropping

Ataques aos protocolos de
acesso ao mail tais como
SMTP POP3, IMAP, etc.

Outros ataques, tais como
DoS

Análise de tráfego

Confiança no servidor de
mail

Ataques de mail

Utilização segura de mail

- Prevenir o spoofing
 - Assinatura digital com hash de um sentido
 - Timestamps.
- Prevenir o eavesdropping
 - Encriptação (camada do transporte ou da aplicação)
- Prevenir os ataques aos protocolos de mail
 - SSL (openSSL)
- Prevenir outros ataques : segurança geral de uma rede