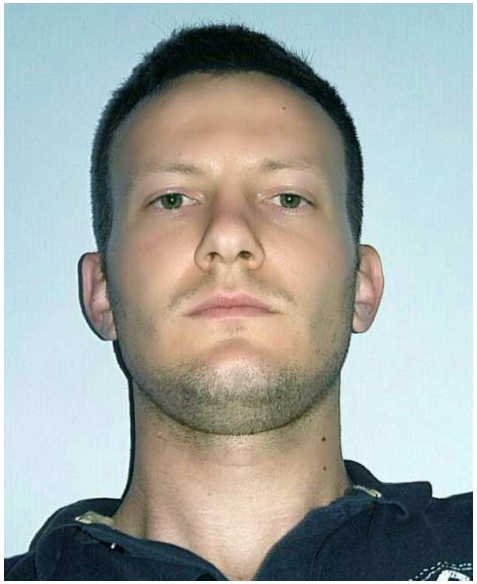
Redes de Computadores

Correio Eletrônico

ITnerante

Rafael Barão



- Mini – CV
  - Administrador de Redes do Poder Legislativo da cidade de Guarulhos-SP
  - Graduado em Ciência da Computação pela UNISO em 2010
  - Principais Aprovações:
    - PF 2013 – Perito Criminal Federal
    - SERPRO 2013 – Analista de Suporte
    - ANP 2012 – Analista Administrativo
    - CNJ 2012 – Analista Judiciário
    - CMG 2012 – Administrador de Redes
    - DERSA 2009 – Analista de Sistemas SR
    - CRF/SP 2009 – Analista de Sistemas
    - DATAPREV 2008 – Analista de TI (Banco de Dados)

ITnerante

Rafael Barão

- Contatos:

http://www.itnerante.com.br/profile/RafaelBarao

http://www.provasdeti.com.br/por-professor/rafael-barao.html

https://twitter.com/rafbarao

rafbarao@hotmail.com

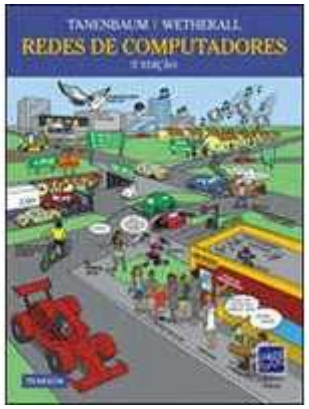
ITnerante

Escopo

- Abordar os assuntos mais recorrentes e com fortes tendências para concursos atuais
- Familiarizar o concursando com os tipos de questões mais frequentes.
- Abordar as metodologias de resolução de questões das principais bancas

ITnerante

Bibliografia



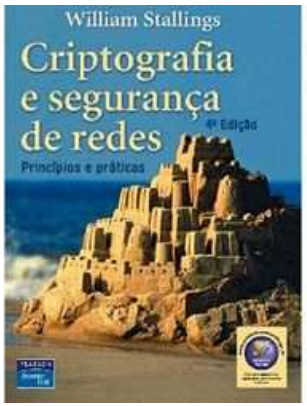
RFC
(Request for Comments)

cespeUnB

Fundação Carlos Chagas

ESAF

FUNDAÇÃO CESGRANRIO



cartilha.cert.br

ITnerante

Correio Eletrônico – Carga Horária

- **12 vídeo aulas (05h03m19s / 00h25m15s)**
  - Conceitos iniciais sobre correio eletrônico
  - Formatos de representação de mensagens
    - RFC 822, MIME
    - ASCII
    - Base64
  - Primeira bateria de questões de aprendizagem
  - Protocolos de transferência de mensagens
    - SMTP, ESMTP
    - POP3, IMAP
  - Segunda bateria de questões de aprendizagem
  - Terceira bateria de questões de aprendizagem
  - Segurança – Revisão e Embasamento
  - Criptografia em correio eletrônico
    - PGP, S/MIME, PEM
  - SPAM
    - Classificação e técnicas básicas de identificação
    - Tecnicas avançadas de identificação
  - Quarta bateria de questões de aprendizagem

ITnerante

Redes de Computadores

Correio Eletrônico

ITnerante

Características Iniciais

- Um dos principais serviços da internet
  - Propulsor da ARPANET
  - Utilizava FTP para transmissão de mensagens
- Sistema Assíncrono
  - Não há necessidade de sincronismo entre os pares comunicantes
- Ambiente Multiprotocolo
  - SMTP
  - POP
  - IMAP

ITnerante

Funções necessárias

- Composição
  - Criar mensagens e respostas
- Transferência
  - Deslocamento de uma mensagem entre o remetente e o destinatário
- Relatórios
  - Informações sobre o status da mensagem
- Exibição
  - Formato da mensagem
- Disposição
  - Manipulação da mensagem pelo destinatário

ITnerante

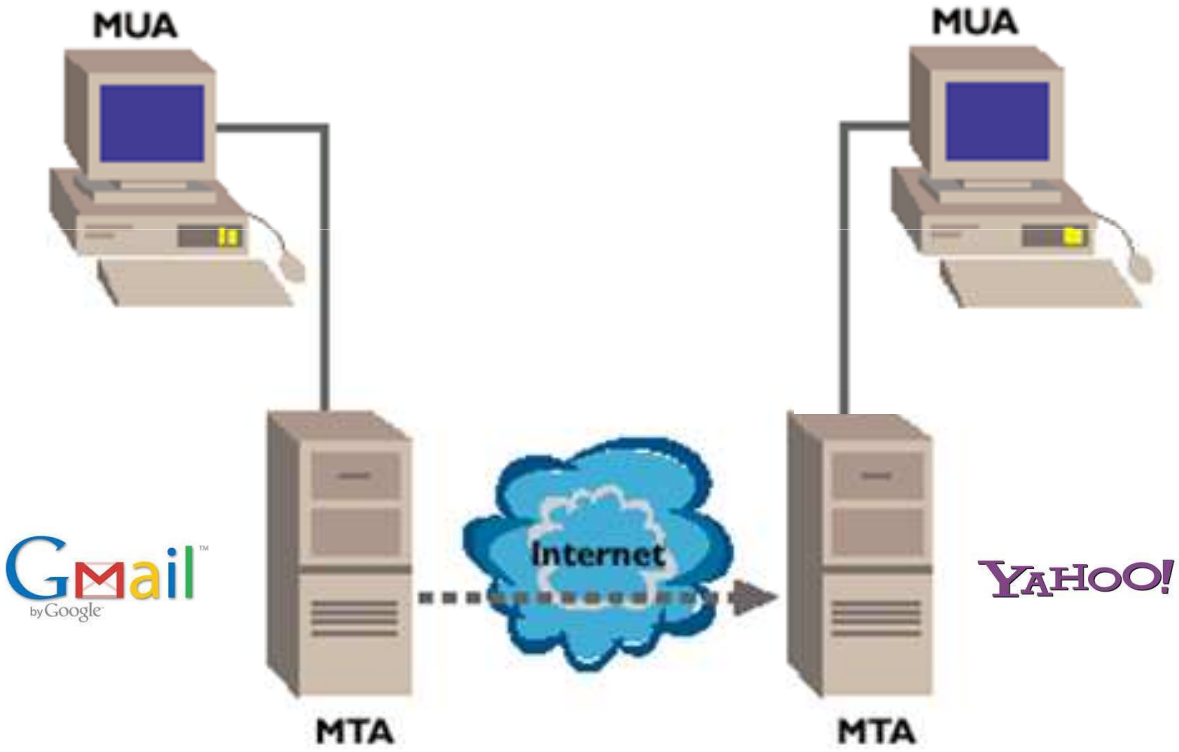
Personagens

- Agente do usuário / MUA
  - Software situado na máquina do cliente
  - Possibilita a leitura e envio de mensagens
- Agente de transferência de mensagens / MTA
  - Servidores de e-mail (deamon)
  - Deslocam as mensagens da origem até o destino
    - Cliente / Servidor
  - Não há interação direta do usuário

ITnerante

Personagens

- Funcionamento básico



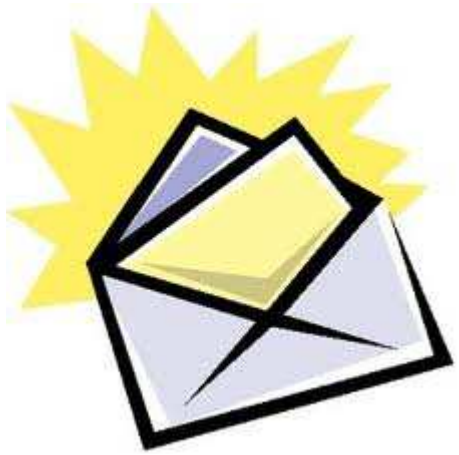
ITnerante

Recursos e Facilidades

- Entrega programada
- Prioridade de mensagem
- Informação de status
  - Notificação de entrega ou leitura
- Redirecionamento
  - Re-rotear mensagens recebidas
- Lista de distribuição / Lista de debate
  - Lista de e-mails agrupados em um único endereço
  - Diferente de endereçamento múltiplo

Composição da Mensagem

- Envelope
  - Informações necessárias para o transporte da mensagem
    - Endereço de destino
    - Prioridade
    - Nível de segurança
  - Utilizado pelo MTA para roteamento da mensagem
- Conteúdo
  - Cabeçalho
    - Infomações de controle para o MUA
  - Corpo
    - Destinatário



ITnerante

Formatos

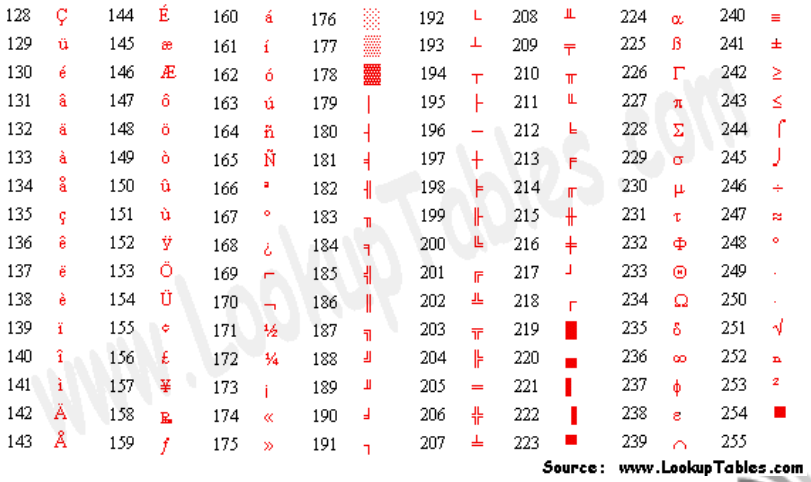
- X.400
  - ITU-T
  - Projeto muito complexo
  - Endereçamento
    - Similar ao formato X.500
      - X.509
      - LDAP
    - Exemplo
      - /C=BR/ST=SÃO PAULO/L=CAMPINAS/PA=AV. BRASIL/CN=JOÃO DA SILVA/

Formatos

- RFC 822
  - Padrão antigo
  - Contém campos que auxiliam na entrega a mensagem
  - Codificação em ASCII
    - 7 bits
    - 8 bits

Regular ASCII Chart (character codes 0 - 127)

000		(nul)	016	►	(dle)	032	sp	048	0	064	@	080	P	096	`	112	p
001	☺	(soh)	017	◄	(dc1)	033	!	049	1	065	A	081	Q	097	a	113	q
002	☻	(stx)	018	↕	(dc2)	034	"	050	2	066	B	082	R	098	b	114	r
003	♥	(etx)	019	‼	(dc3)	035	#	051	3	067	C	083	S	099	c	115	s
004	♦	(eot)	020	¶	(dc4)	036	$	052	4	068	D	084	T	100	d	116	t
005	♣	(enq)	021	§	(nak)	037	%	053	5	069	E	085	U	101	e	117	u
006	♠	(ack)	022	–	(syn)	038	&	054	6	070	F	086	V	102	f	118	v
007	•	(bel)	023	↨	(etb)	039	'	055	7	071	G	087	W	103	g	119	w
008	◘	(bs)	024	↑	(can)	040	(	056	8	072	H	088	X	104	h	120	x
009		(tab)	025	↓	(em)	041	)	057	9	073	I	089	Y	105	i	121	y
010		(lf)	026		(eof)	042	*	058	:	074	J	090	Z	106	j	122	z
011	♂	(vt)	027	←	(esc)	043	+	059	;	075	K	091	[	107	k	123	{
012	♀	(np)	028	∟	(fs)	044	,	060	<	076	L	092	\	108	l	124	|
013		(cr)	029	↔	(gs)	045	-	061	=	077	M	093	]	109	m	125	}
014	♫	(so)	030	▲	(rs)	046	.	062	>	078	N	094	^	110	n	126	~
015	☼	(si)	031	▼	(us)	047	/	063	?	079	O	095	_	111	o	127	⌂



Formatos

- RFC 822
  - Principais campos
    - To:
    - Cc:
    - Bcc:
    - From:
    - Date:
    - Message-Id:
    - Subject:
  - Endereçamento via DNS
    - endereco@dominio.com.br
  - Separa o cabeçalho da mensagem por meio de CRLF
  - Exemplo de mensagem:

```
From: joao@exemplo.com
To: roberto@exemplo.com
Cc: bruno@exemplo.com
Subject: Exemplo de mensagem

Esse é um exemplo de mensagem no formato RFC 822.
Reparem na linha em branco que separa o cabeçalho da mensagem.
```

Formatos

- MIME - Multipurpose Internet Mail Extensions
  - Inibir as limitações da RFC 822
    - Transmissão de dados não-ASCII
    - Possibilidade de anexar binários
    - Permitir o uso de caracteres especiais
  - Compatibilidade com a RFC 822
    - Mantém o formato antigo
    - Adiciona uma nova estrutura contendo novos campos

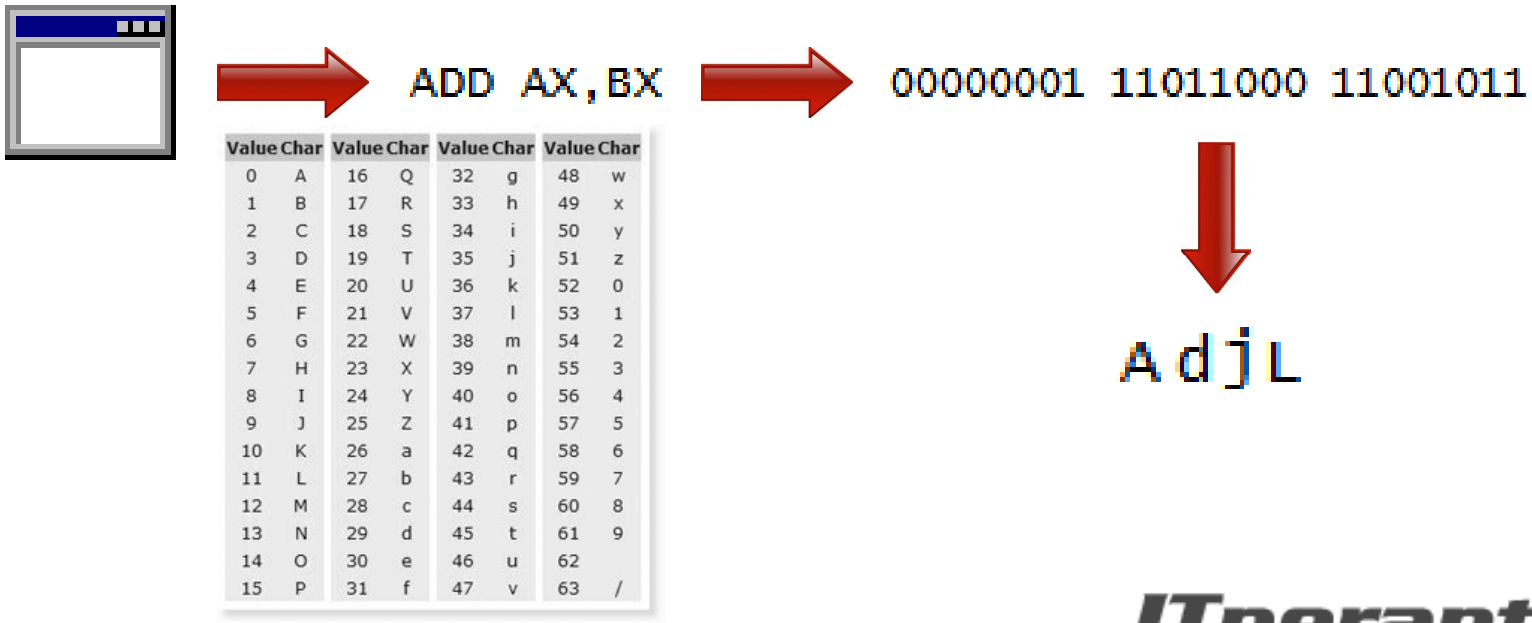
Formatos

- MIME - Multipurpose Internet Mail Extensions
  - Base64 / Radix64
    - Converte qualquer representação binária para texto
    - Grupos de 24 bits são divididos em unidades de 6 bits
    - Cada valor numérico representado pelo conjunto de 6 bits é convertido para um caractere alfanumérico

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	
15	P	31	f	47	v	63	/

Formatos

- MIME - Multipurpose Internet Mail Extensions
  - Base64 / Radix64
    - Processo de conversão
    - 3 bytes não ASCII são convertidos em 4 bytes ASCII



Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	
15	P	31	f	47	v	63	/

ITnerante

Formatos

- MIME - Multipurpose Internet Mail Extensions
  - 5 novos campos
    - **MIME-Version**:
    - **Content-Description**:
    - **Content-Id**:
      - Identificação exclusiva do conteúdo
    - **Content-Transfer-Encoding**:
      - Mensagens em texto ASCII
        - » 7 bits
        - » 8 bits
      - Mensagens com codificação binária
        - » Base64
      - Mensagens quase totalmente em ASCII
        - » quoted-printable
        - » Ex: Correio eletrônico -> Correio eletr=93nico

Formatos

- MIME - Multipurpose Internet Mail Extensions
  - 5 novos campos
    - **Content-Type**: Especifica a natureza do corpo da mensagem
      - Multipart
        - » Mixed
          - Permite uma mensagem conter múltiplos objetos de forma inependente
        - » Parallel
          - Inclusão de subpartes que devem ser executadas juntas
        - » Alternative
          - Mensagem simples contendo múltiplas representações dos mesmos dados
        - » Digest
          - Mensagem contendo um conjunto de outras mensagens

Formatos

- MIME - Multipurpose Internet Mail Extensions
  - 5 novos campos
    - **Content-Type**:
      - Text
        - » Plain
        - » Enriched
        - » HTML
        - » XML
      - Image
        - » GIF
        - » JPEG
      - Audio
      - Video
      - Application
        - » Octet-stream
        - » PostScript
      - Message
        - » RFC 822
        - » Partial
        - » External-body

ITnerante

Formatos

- MIME - Multipurpose Internet Mail Extensions
  - Exemplo de mensagem

```
Date: Fri, 20 Dec 2013 10:23:16 -0300 (EDT)
From: João Silva <joao@exemplo.com>
To: Pedro Almeida <pedro@exemplo.com>
Subject: Gráfico
Message-ID: <Pine.LNX.4.21.0005191019440.8452-101000@exemplo.com>
MIME-Version: 1.0
Content-Type: MULTIPART/MIXED; BOUNDARY="-1463757054-170444605-958746196=:8452"

Esse texto só será visualizado por um MUA que não possui suporte ao MIME

---1463757054-170444605-958746196=:8452
Content-Type: TEXT/ENRICHED;

Pedro, segue anexo o <bold> gráfico </bold> solicitado sobre o balanço mensal.

---1463757054-170444605-958746196=:8452
Content-Type: IMAGE/GIF; name="grafico.gif"
Content-Transfer-Encoding: BASE64
Content-ID: <Pine.LNX.4.21.0005191023160.8452@exemplo.com>
Content-Description: Gráfico do balanço

a/acUG5piNz/uXLzVJ2qm6dXz584S2WB1cJFi5cshZr539xVftnyFKUVTi2T
VjqvyhJLXb1m7TqoHPt6F/HW0g0bN63crGqVtWXrtu07BJihcsw71+zanRW8
Z89eq337RQ/Ip60xO3gIElX/LbikDm8T36KwbNmRo7O3zpHkPSZwHBqL//8f
lz1x2OOkyKJTi7aqbzutfUZI2gIuF8F2lr/D5dw2+fZdwpl8YVolI+CJ4/9/
joOyYed5QzMvhGqnm2V0WiClm///D0lfXHtJ6vLlK9w7rx7vQk5SQJbFtSms
1y9evXid7QZacgOxmSxktNzdtSwwU+J/VICaCPFIYU3XAJhIOtjf5sfyAAAA
JXRFWHRDb21tZW50AGNsaXAyZ2lmIHYuMC42IGJ5IFl2ZXMgUGlndWV0NnM7
vAAAAABJRU5ErkJggg==
---1463757054-170444605-958746196=:8452--
```

Questões de Aprendizagem

Ambiente e Formatos

ITnerante

TJ/RJ – FCC 2012 – Analista Judiciário – Analista de Sistemas

1. O serviço de correio eletrônico original da suite TCP-IP permitia somente caracteres de sete bits do conjunto ASCII. O crescimento e popularização da Internet estimularam a criação de mecanismos para contornar esta limitação, permitindo, entre outras coisas, a transmissão de som e imagem via correio eletrônico. Este é o caso do

A. Simple Mail Transfer Protocol (SMTP).
B. Multipurpose Internet Mail Extensions (MIME).
C. Post Office Protocol (POP).
D. Internet Message Access Protocol (IMAP).
E. Media Resource Control Protocol (MRCP).

Prefeitura de São Paulo – FCC 2012 – Auditor Fiscal Tributário – Tecnologia da Informação

2. O protocolo SMTP define o conceito de um Mail Transfer Agent (MTA) e de um Mail User Agent (MUA). Sobre estes agentes, é correto afirmar que

A. o protocolo usado na comunicação entre MUAs e MTAs é sempre o SMTP.

B. o protocolo usado na comunicação entre MUAs e MTAs é sempre o SMTP.

C. em um sistema de web mail o MTA é implementado por um servidor web.

D. em um sistema de web mail o MUA e o MTA devem residir no mesmo servidor com IP fixo.

E. não existem MUAs para dispositivos móveis, apenas para servidores com IP fixo.

3. Ferramentas clientes de correio eletrônico são capazes de exibir dados não-ASCII via mensagem padrão de correio eletrônico devido

A. à flag de sincronização.
B. ao HTML.
C. à MIME.
D. ao metadado.
E. à representação externa de dados (XDR).

4. O programa chamado MTA client é

A. Interface gráfica para compor o e-mail
B. Servidor para acesso à caixa postal
C. Cliente para acesso à caixa postal
D. Servidor para transferência do e-mail a outro servidor
E. Cliente para transferência do e-mail ao servidor

CRM/MG – FUMARC 2006 – Administrador de Rede

5. Analise as seguintes afirmativas sobre formato e codificação de mensagens de correio eletrônico:

I. Apesar do MIME especificar diversos formatos de dados, as mensagens de correio eletrônico são enviadas pelo SMTP no formato ASCII.

II. Na codificação MIME base64, cada grupo de 24 bits de dados são codificados por até 4 unidades de 6 bits como um caractere ASCII válido.

III. Para as mensagens textuais com poucos caracteres especiais, a codificação quoted-printable é mais eficiente que a codificação MIME.

A. I e II, apenas.

B. I e III, apenas.

C. II e III, apenas.

D. I, II e III.

EBC – CESPE 2011 – Analista de Empresa – Engenharia de Software

Com relação aos fundamentos de redes de computadores, julgue o item abaixo

6. Três importantes componentes do correio eletrônico são os agentes usuários, os servidores de email e o protocolo SMTP (Simple Mail Transfer Protocol).

TJ/RJ – FCC 2012 – Analista Judiciário – Analista de Sistemas

7. MIME é uma norma da Internet para o formato das mensagens De correio eletrônico que significa

A. Multipurpose Internet Mail Extensions.
B. Multiplex Internet Mail Extensions.
C. Multiple Internet Mail Extensions.
D. Multi Internet Mail Extensions.
E. Multidouble Internet Mail Extensions.

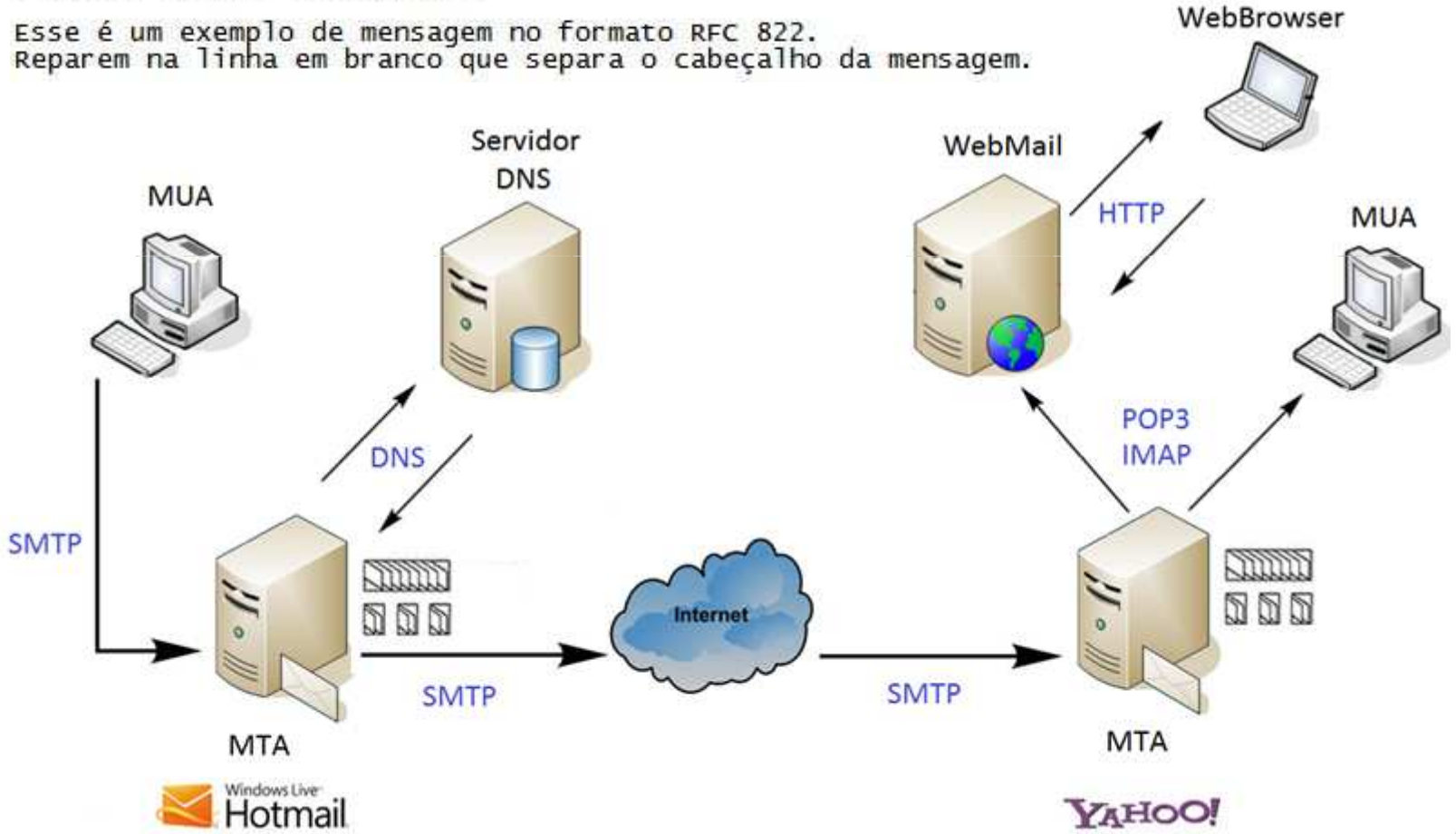
Gabarito

1. B
2. B
3. C
4. E
5. D
6. C
7. A

Protocolos

-
```
From: joao@hotmail.com
To: roberto@yahoo.com.br
Cc: bruno@yahoo.com.br
Subject: Exemplo de mensagem

Esse é um exemplo de mensagem no formato RFC 822.
Reparem na linha em branco que separa o cabeçalho da mensagem.
```



ITnerante

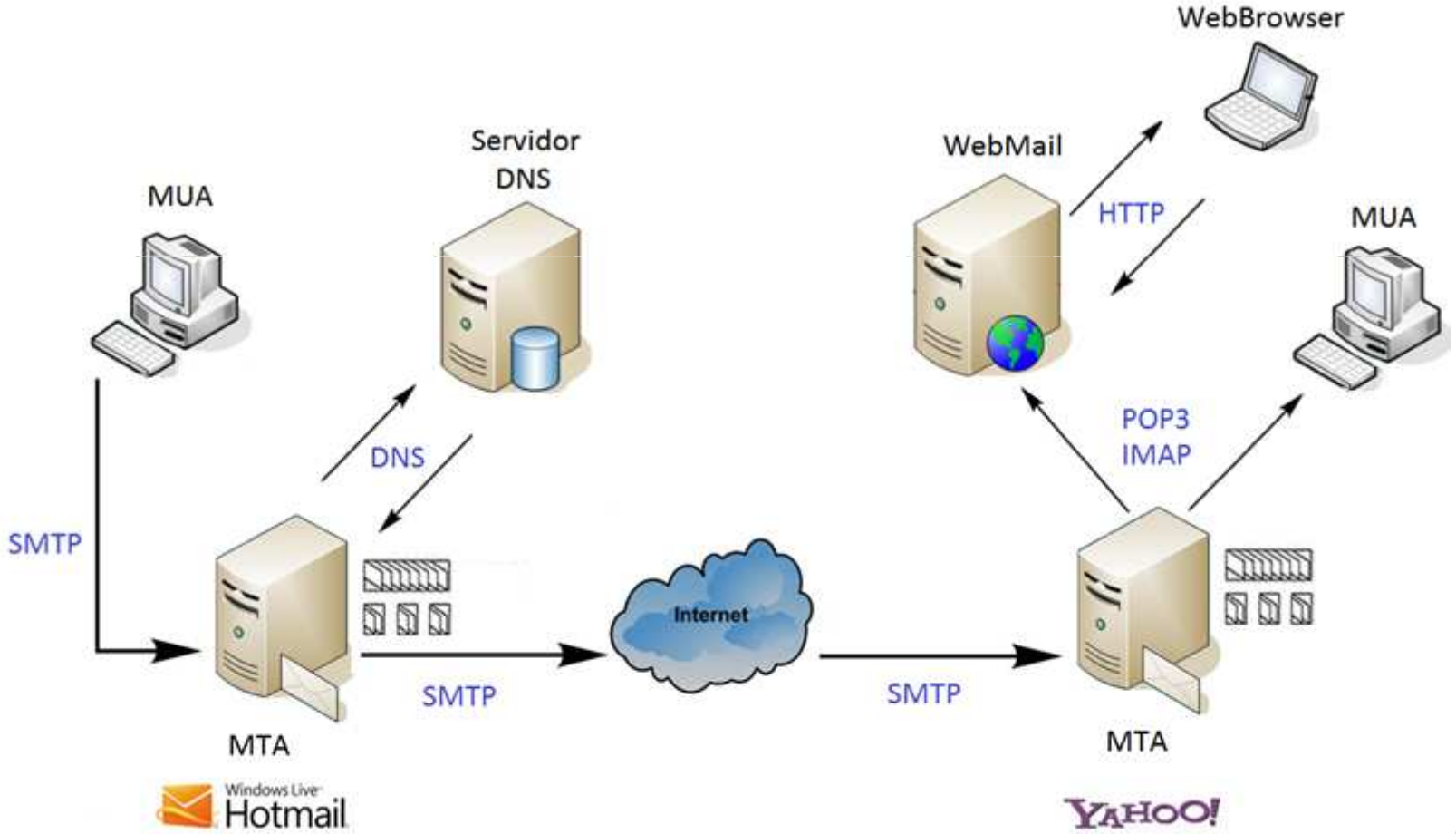
DNS

- Domain Name System
- Camada de aplicação
  - 53 - TCP/UDP
- Conexão TCP/UDP = End. IP + Porta
- Facilitar a descoberta do endereço IP
  - Nomes de domínio são mais mnemônicos para usuários e empresas
- Mapear nomes de domínios em registros de recursos
  - Principais tipos
    - A – Address
    - PTR - Pointer
    - NS - Name Server
    - MINFO - Mailbox Info
    - MX - Mail Exchange
      - Estabelece prioridade entre os servidores
    - TXT - Text
      - SPF - Sender Policy Framework

ITnerante

Protocolos

- Sistema de correio eletrônico



ITnerante

SMTP

- Simple Mail Transfer Protocol
- Camada de aplicação
  - 25/TCP
- Protocolo muito antigo
  - RFC 821
  - Comunicação por comandos
    - ASCII de 7 bits
    - Um comando por linha
- Store and Forward
  - Se o MTA destino estiver inativo, o MTA origem tenta novamente mais tarde
  - Cópia local só é excluída da fila de mensagens quando a cópia for aceita e armazenada pelo servidor destino

ITnerante

SMTP

- Atua como cliente e servidor
  - Relay
- Único protocolo de comunicação entre MTAs
- Conexões persistentes
  - Statefull
  - Envio de vários e-mail por conexão
  - Conexão TCP é encerrada com o comando QUIT
- Não se preocupa com o formato
  - Cabeçalho do envelope
  - Corpo da mensagem
- Não se preocupa com o armazenamento
  - Caixas de correio podem estar fisicamente armazenadas em outro servidor
- Mensagens de erro
  - Contêm um resumo do erro e o cabeçalho da mensagem causadora dos problemas

ITnerante

SMTP

- Exemplo de transferência

S: 220 smtp.yahoo.com
C: HELO smtp.yahoo.com
S: 250 Hello, I am glad to meet you
C: MAIL FROM:<joao@hotmail.com>
S: 250 Ok
C: RCPT TO:<roberto@yahoo.com.br>
S: 250 Ok
C: RCPT TO:<bruno@yahoo.com.br>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: joao@hotmail.com
To: roberto@yahoo.com.br
Cc: bruno@yahoo.com.br
Subject: Exemplo de mensagem

Esse é um exemplo de mensagem no formato RFC 822.
Reparem na linha em branco que separa o cabeçalho da mensagem.
.
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye

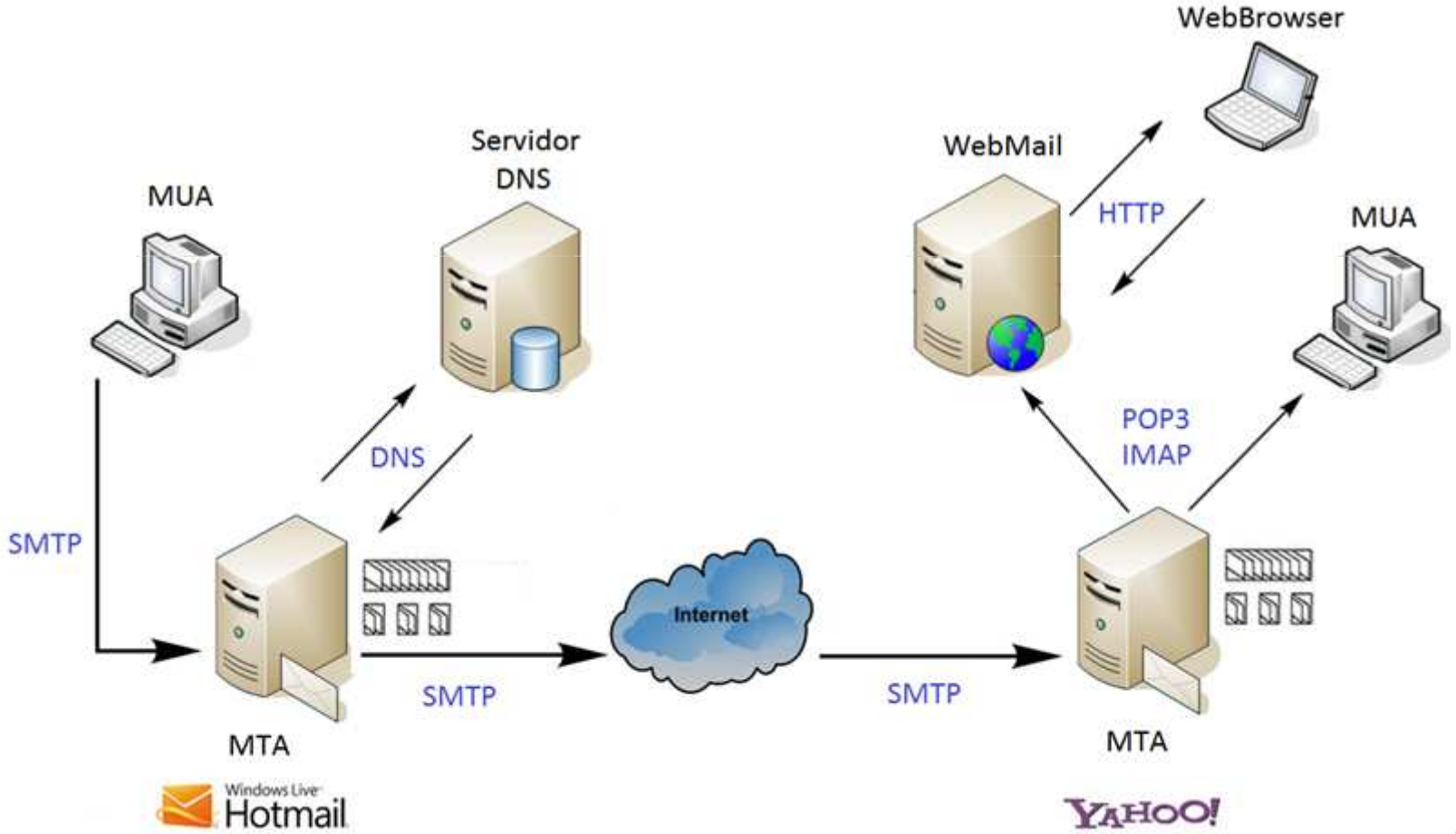
ESMTP

- Extended SMTP
- Contorna os problemas do SMTP padrão
  - Tamanho
  - Timeout
  - ASCII de 7 bits
- Principais melhorias
  - DSN - Delivery Status Notification
  - SIZE - Tamanho
  - AUTH – Autenticacao
- Verificação de compatibilidade
  - EHLO em vez de HELO

ITnerante

Protocolos

- Sistema de correio eletrônico



ITnerante

POP3

- Post Office Protocol Version 3
- RFC 1939
- Camada de aplicação
  - 110/TCP
- Protocolo Simples e Robusto
- Realiza o download da mensagem
  - Offline
  - A mensagem baixada é excluída do servidor
- Autenticação
  - Texto simples
  - Hash MD5 (APOP)
- Limitações
  - Apenas uma pasta (maildrop)
  - Não é possível ler parte da mensagem
  - Não há mecanismos de busca

ITnerante

POP3

- Estados
  - Autorização
    - Identificação e Autenticação através da combinação dos comandos:
      - USER e PASS
      - APOP (MD5)
  - Transação
    - Abertura do maildrop
    - Coleta da mensagem
      - Envio
      - Recebimento
      - Marcação para exclusão
    - Operação atômica
  - Atualização
    - Comando QUIT
    - Exclusão das mensagens marcadas
    - Fim da sessão POP e da conexão TCP

ITnerante

POP3

- Exemplo de recebimento

S: +OK POP3 yahoo.com.br server ready
C: USER roberto
S: +OK please send PASS command
C: PASS 12345
S: +OK roberto's maildrop has 2 messages (422 octets)
C: STAT
S: +OK 2 422
C: LIST
S: +OK 2 messages (422 octets)
S: 1 222
S: 2 200
S: .
C: RETR 1
S: +OK 222 octets
From: joao@hotmail.com
To: roberto@yahoo.com.br
Cc: bruno@yahoo.com.br
Subject: Exemplo de mensagem

Esse é um exemplo de mensagem no formato RFC 822.
Reparem na linha em branco que separa o cabeçalho da mensagem.
.
C: DELE 1
S: +OK
C: QUIT
S: +OK POP3 server disconnecting

IMAP

- Internet Message Access Protocol (versão 4)
- RFC 2060
- Camada de aplicação
  - 143/TCP
- Possui mais recursos, sendo mais complexo
- Surgiu da necessidade de acessar o e-mail a partir de várias máquinas
- Manipula a mensagem no servidor
  - Online
  - Mensagem ficam no servidor até que seja apagada pelo usuário
  - Permite o download de parte da mensagem
- Existem dezenas de comandos

ITnerante

IMAP

- Vantagens
  - Conexão permanente
  - Múltiplos clientes conectados a uma caixa
    - Compartilhamento em grupo
  - Informação de status da mensagem
  - Múltiplas pastas/caixas em uma mail box
  - Mecanismos de busca no servidor
- Desvantagens
  - Falha na conexão restringe o acesso ao email
  - Alto uso de recursos do servidor
  - Performance ruim em conexões lentas

ITnerante

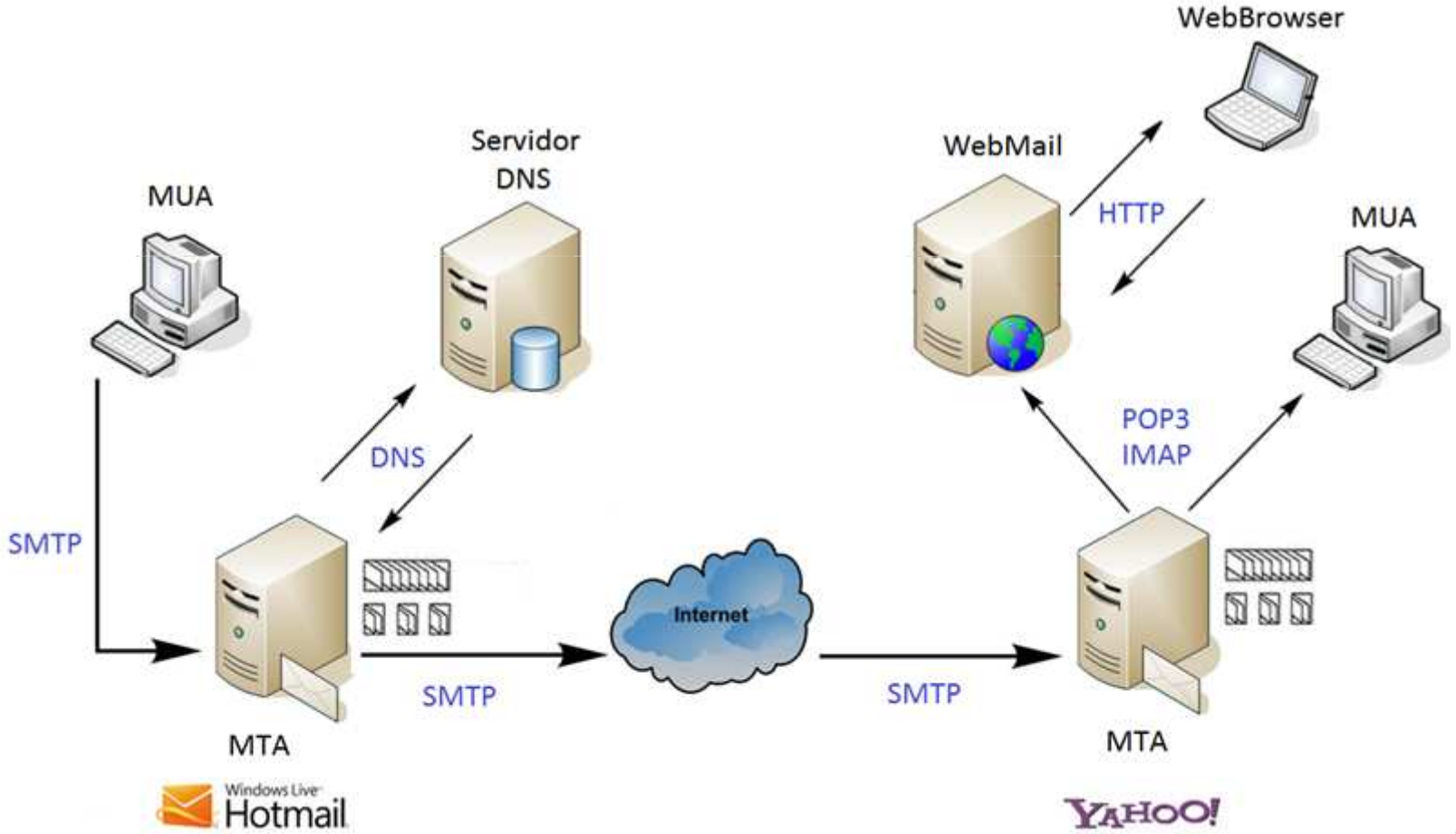
POP3 vs IMAP

Característica	P0P3	IMAP
Onde o protocolo é definido	RFC 1939	RFC 2060
Porta TCP usada	110	143
Onde o correio eletrônico é armazenado	PC do usuário	Servidor
Onde o correio eletrônico é lido	Off-line	On-line
Tempo de conexão exigido	Pequeno	Grande
Utilização de recursos do servidor	Mínima	Intensa
Várias caixas de correio	Não	Sim
Quem guarda cópias das caixas de correio	Usuário	ISP
Bom para usuários em trânsito	Não	Sim
Controle do usuário sobre o download	Pequeno	Grande
Downloads de mensagens parciais	Não	Sim
Implementação simples	Sim	Não

ITnerante

Protocolos

- Sistema de correio eletrônico



ITnerante

WebMail

- Utiliza HTTP entre o cliente e o servidor web
- Usa o navegador para ler e escrever e-mails
  - O servidor web faz papel de MUA
  - Não há necessidade de programas específicos
- Mensagens armazenadas no servidor do ISP
  - Utiliza, geralmente, IMAP entre o servidor web e o MTA
- Arquitetura em N camadas

ITnerante

Questões de Aprendizagem

Protocolos

ITnerante

Câmara dos Deputados – CESPE 2012 – Analista Legislativo – Engenharia Eletrônica Telecom (adaptada)

Julgue o próximo item, relativo à arquitetura TCP/IP e aos seus principais protocolos

1. O SMTP consiste em um protocolo muito utilizado pelos servidores de transporte de email modernos, apesar de possuir tecnologia bastante arcaica, surgida antes mesmo do protocolo HTTP.

MP/MA – FCC 2013 – Técnico Ministerial – Redes e Infraestrutura

2. Deseja-se implantar o serviço de e-mail corporativo em uma rede local de computadores (LAN) de uma empresa. O acesso dos usuários ao servidor deve ser feito de forma que não haja a necessidade de baixar os e-mails para o computador local para que sua leitura possa ser feita. O protocolo de acesso ao e-mail utilizado nessa implantação é o

A. FTP.
B. IMAP.
C. POP3.
D. DNS.
E. SNMP.

MP/MA – FCC 2013 – Analista Ministerial – Redes e Infraestrutura

3. Para que o protocolo SMTP funcione é necessário uma implementação mínima para todos os receptores. Essa implementação requer que alguns comandos estejam presentes. É INCORRETO dizer que dentre estes comandos esteja o comando

A. DATA.
B. HELO.
C. MAIL.
D. RCPT.
E. LOOP.

4.Sobre o Protocolo SMTP, considere:

I. Assim como no protocolo HTTP utilizado em páginas web, as sessões SMTP são stateless, ou seja, não é mantido o estado entre as sessões.

II. Os comandos e mensagens de dados, a não ser que sejam alteradas por uma extensão, são transmitidos em linhas. Linha é uma sequência de zero ou mais caracteres, terminada pela sequência de caracteres ASCII, CR e LF.

III. Os comandos e respostas possuem uma sintaxe livre e textual, porém todos os comandos devem começar com um código numérico de três dígitos e as repostas devem ser iniciados por um verbo no infinitivo.

Está correto o que se afirma **APENAS** em

A. I e II.

B. I e III.

C. II.

D. II e III.

E. III.

TRE/PE – FCC 2011 – Analista Judiciário – Análise de Sistemas

5.Considere:

I. No âmbito do SMTP, após estabelecer a conexão TCP com a porta 25, a máquina de transmissão opera como cliente e espera que a máquina de recepção, operando como servidor, dê início à comunicação.

II. No IMAP, é possível o compartilhamento de caixas postais entre usuários de um grupo de trabalho e as mensagens podem ser acessadas tanto por webmail quanto por uma aplicação cliente de correio eletrônico.

III. Após estabelecer uma conexão TCP com o agente de transferência de mensagens na porta 143, o protocolo POP3 passa por três estados em sequência, sendo um deles conhecido como Atualização, que tem como função a marcação das mensagens para exclusão da caixa de correio.

IV. Um URL pode ser dividido em três partes: o protocolo, o nome DNS da máquina em que a página está e, normalmente, um nome de arquivo na máquina onde ele reside.

É correto o que consta em I e II.

A. I e II, apenas.

B. III e IV, apenas.

C. I, II e IV, apenas.

D. II, III e IV, apenas.

E. I, II, III e IV.

6.Possibilita o envio de informações não-ASCII (exemplo imagens) em mensagens SMTP. Trata-se do padrão

A. RJ45.
B. MIME.
C. FDDI.
D. FTPS.
E. SMNP.

TRE/RN – FCC 2011 – Analista Judiciário – Análise de sistemas

7. No SMTP, o (I) endereço de e-mail da origem, (II) a data, (III) o assunto e (IV) a mensagem, são componentes, respectivamente, do

A. cabeçalho, do cabeçalho, do corpo e do corpo.
B. cabeçalho, do cabeçalho, do cabeçalho e do corpo.
C. cabeçalho, do corpo, do corpo e do corpo.
D. corpo, do cabeçalho, do cabeçalho e do corpo.
E. corpo, do cabeçalho, do corpo e do cabeçalho.

MEC – FGV 2009 – Gerente de Segurança

8. Em um protocolo para transferência de mensagens entre servidores e clientes, as mensagens são entregues a um servidor compartilhado, ideal para uso doméstico e para equipamentos sem conexão permanente à Internet. Nesse protocolo, os computadores pessoais se conectam periodicamente a este servidor e descarregam as mensagens para a máquina cliente. Esse protocolo é conhecido pela sigla:

A. PPP
B. POP
C. SMTP
D. QMAIL
E. BITNET

9. Em uma rede TCP/IP, o registro associado ao correio eletrônico em um serviço de nomes (DNS) é

A. A.
B. CNAME.
C. MX.
D. NS.
E. SOA.

10. Assinale a opção correta.

A. O protocolo POP3 provê meios para um usuário criar pastas remotas e designar mensagens a pastas.
B. O protocolo POP3 é definido no RFC 1939.
C. Em uma transação POP3, o controlador emite comandos e o servidor, uma demanda única para todos eles.
D. O protocolo POP3 é definido no RSC 1949.
E. O protocolo POP3 provê meios para um usuário criar janelas remotas e atribuir mensagens a pastas clientes.

ABIN – CESPE 2010 – Agente Téc. de Inteligência – Tecnologia da Informação (adaptada)

Julgue os próximos itens com relação a SMTP (simple mail transfer protocol).

11. O SMTP não especifica a maneira como o sistema de correio eletrônico transfere mensagens de uma máquina para outra.

12. Uma mensagem SMTP é composta de cabeçalho e corpo, que são separados por uma linha em branco.

ANP – CESPE 2013 – Analista Administrativo – Área V

Acerca de Internet, julgue o item abaixo.

13. Os webmails são páginas web utilizadas para a apresentação e a utilização dos protocolos envolvidos no envio e no recebimento de email. Uma das vantagens dos webmails é que o seu conteúdo pode ser acessado em qualquer lugar do mundo, autenticando-se em um navegador na World Wide Web.

ALE/SP – FCC 2010 – Agente Téc. Legislativo – Segurança de Redes

14. Com relação a correio eletrônico, o protocolo

A. SMTP permite que um cliente de e-mail obtenha as mensagens destinadas a um determinado endereço armazenadas em um servidor de e-mail.
B. POP3 permite que um cliente examine e apague mensagens armazenadas no servidor sem necessidade de transmiti-las integralmente ao cliente.
C. IMAP oferece toda a funcionalidade oferecida pelo protocolo POP3.
D. POP3 oferece toda a funcionalidade oferecida pelo protocolo IMAP.
E. IMAP só pode ser utilizado por intermédio de um navegador (webmail)

ALE/SP – FCC 2010 – Agente Téc. Legislativo – Segurança de Redes

15. De acordo com a atribuição da Internet Assigned Numbers Authority (IANA), os ports reservados para roteamento de mensagens via SMTP, transações via POP3 e transações via IMAP (todos "sem SSL") são, respectivamente,

A. 25, 110 e 143
B. 25, 587 e 110
C. 110, 25 e 143
D. 110, 143 e 587
E. 587, 110 e 143

Gabarito

1. C
2. B
3. E
4. C
5. C
6. B
7. B
8. B
9. C
10. B
11. E
12. C
13. C
14. C
15. A

Banco da Amazônia – CESPE 2010 – Redes e Telecomunicações

No que concerne aos serviços de Internet, julgue os itens.

16. O serviço de correio eletrônico é formado por três componentes principais: os agentes de usuário, usados para leitura das mensagens; os servidores de correio, que efetivamente enviam e recebem as mensagens; e o protocolo SMTP, usado apenas para a troca de mensagens entre servidores.

17. O SMTP é o principal protocolo de camada de aplicação do correio eletrônico, usando o serviço confiável de transferência de dados do TCP para troca de mensagens do servidor de correio do remetente para o do destinatário, segundo a arquitetura cliente-servidor.

18. Tanto o lado cliente como o lado servidor do SMTP funcionam em todos os servidores de correio eletrônico.

Casa da Moeda – CESGRANRIO 2009 – Analista – Suporte em TI

19. O servidor SMTP de uma empresa está temporariamente fora do ar, embora os acessos via POP e IMAP estejam no ar. Com base nessa situação, analise as afirmativas a seguir.

I - Os usuários estão impossibilitados de acessar suas caixas postais.

II - O IMAP é um protocolo que funciona como backup do SMTP.

III - Os usuários internos não podem enviar e-mails.

Está(ão) correta(s) APENAS a(s) afirmativa(s)

A. I.

B. II.

C. III.

D. I e II.

E. I e III.

UNIPAMPA – CESPE 2009 – Analista de TI – Redes e Suporte

A respeito dos serviços e protocolos da Internet, julgue os itens que se seguem.

20. O SMTP permite a troca de mensagens por meio do uso da estratégia store-and-forward.

21. O POP3 permite o envio de mensagens diretamente ao destinatário final.

MPE/RR – CESPE 2008 – Analista de Redes

No que se refere ao serviço de correio eletrônico em redes TCP/IP, julgue os itens subseqüentes.

22. O serviço de correio eletrônico é implementado pelo protocolo SMTP, cujos componentes são, tipicamente, o agente do usuário e o agente de transferência ou transporte, que implementa o servidor.

23. Em situações em que o usuário não acessa diretamente sua caixa de correio para leitura de mensagens, o acesso à caixa de correio é realizado por meio de um agente que transfere a caixa de correio do agente de transferência para a estação em que o usuário irá ler as mensagens localmente.

24. O SMTP utiliza a porta 25/TCP, enquanto a transferência da caixa de correio para a estação de usuário utiliza, normalmente, a porta 110/TCP ou 143/TCP.

25. Uma das opções de configuração do agente de transferência prevê seu uso como relay, mediando a conexão entre servidores, mas sem manter caixas de correio para os usuários.

26. O SMTP é um serviço que oferece confidencialidade e autenticidade na troca de mensagens.

27. Assinale a opção correta.

A. O POP3 começa quando o agente unitário fecha uma conexão TCP com o servidor múltiplo na porta 310.

B. Em uma transação POP3, o cliente analisa comandos e o provedor analisa dados.

C. O POP3 começa quando o agente de gestão abre uma conexão TCP com o servidor de execução na porta 100.

D. O POP3 começa quando o agente de usuário (o cliente abre uma conexão TCP com o servidor de correio (o servidor) na porta 110.

E. Em uma condição POP3, o cliente emite comandos entre servidores orientados a armazenamento.

BADESC – FGV 2010 – Analista de Sistemas – Suporte Técnico

28. Conforme a RFC 2060, o protocolo Internet Message Access Protocol - IMAP, cuja versão mais recente é IMAP4rev1, constitui um método de acesso às mensagens eletrônicas armazenadas em um servidor local ou remoto. Segundo a RFC 1733, uma das formas de se trabalhar com correio eletrônico remotamente, é aquela em que as mensagens e pastas ficam armazenadas no servidor, e o usuário as manipula remotamente por meio do programa cliente de correio eletrônico, com a possibilidade de criar, renomear, apagar e mover pastas, ativar marcações em mensagens e receber, seletivamente, partes de mensagens, dentre outras facilidades.

Esse modo de operação é denominado:

A. disconnected.
B. passivo.
C. offline.
D. online.
E. ativo.

CNJ – CESPE 2013 – Técnico Judiciário – Programação

A respeito de redes de computadores, julgue os itens subsequentes.

29. O serviço de webmail permite a um usuário acessar as mensagens em sua caixa postal no provedor, sem a necessidade de configurar o computador em uso com os nomes dos servidores de SMTP e POP.

30. Lista de discussão é uma ferramenta de comunicação limitada a uma intranet, ao passo que grupo de discussão é uma ferramenta gerenciável pela Internet que permite a um grupo de pessoas a troca de mensagens via email entre todos os membros do grupo.

31. No protocolo SMTP

A. a mensagem divide-se em duas partes: dados e instruções.
B. o formato dos endereços eletrônicos é nome do domínio@nome local.
C. o formato dos endereços eletrônicos é código de login@senha.nome local.
D. a transferência de mensagem é executada por um processo em background.
E. a mensagem divide-se em duas partes: dados alfanuméricos e dados numéricos.

Gabarito

16. E
17. C
18. C
19. C
20. C
21. E
22. C
23. C
24. C
25. C
26. E
27. D
28. D
29. C
30. E
31. D

ITnerante

Correio Eletrônico

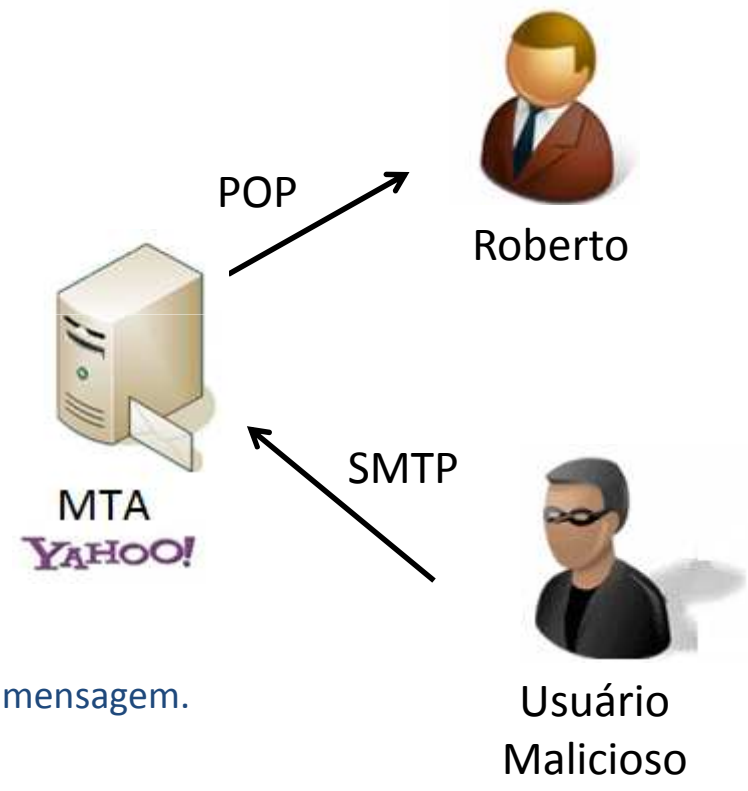
Segurança

Problemas de Segurança

- Integridade e Autenticidade

S: 220 smtp.yahoo.com
C: HELO smtp.yahoo.com
S: 250 Hello, I am glad to meet you
C: MAIL FROM:<hacker@blackhat.com>
S: 250 Ok
C: RCPT TO:<roberto@yahoo.com.br>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: joao@hotmail.com
To: roberto@yahoo.com.br
Subject: Exemplo de mensagem

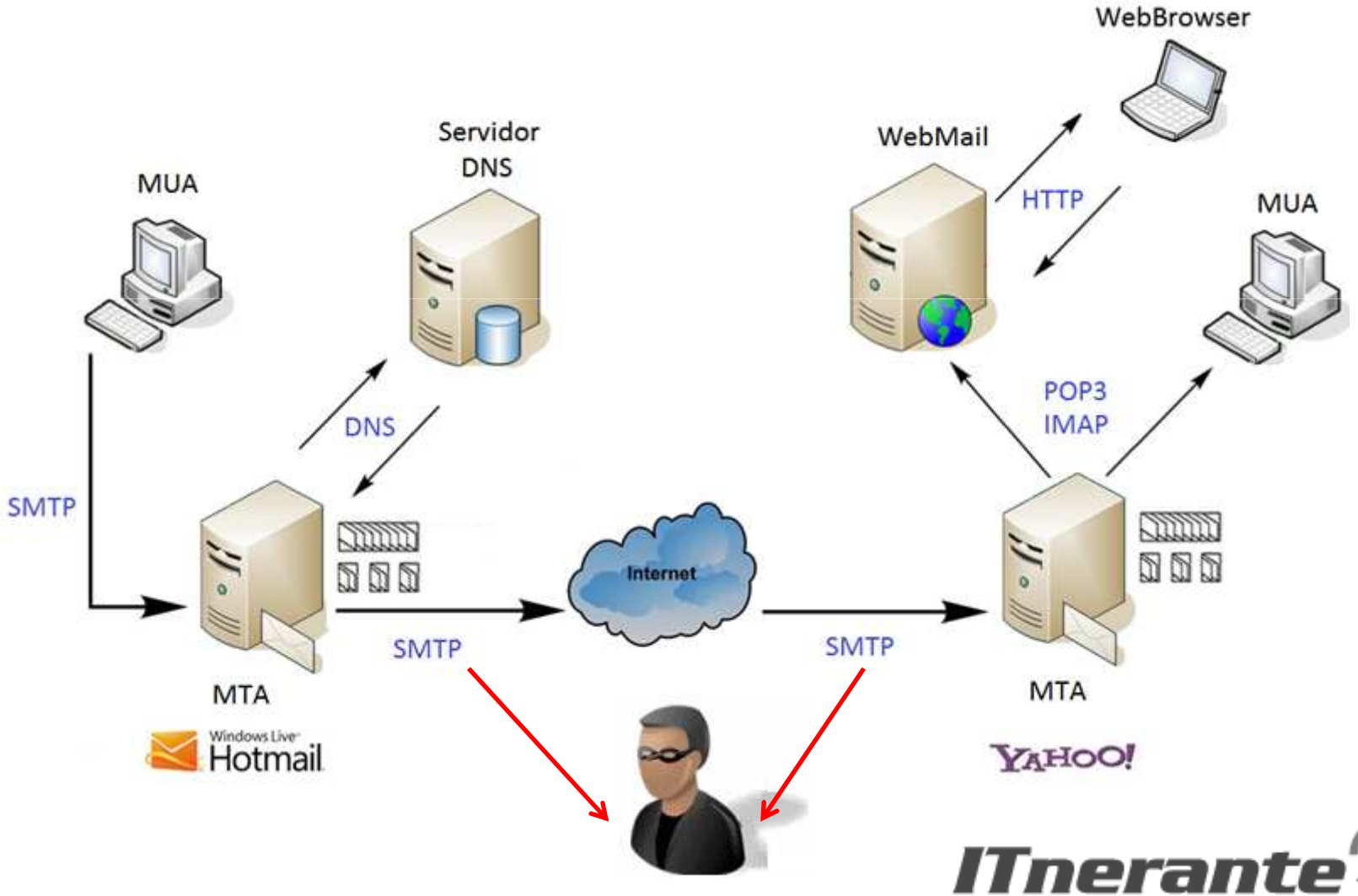
Esse é um exemplo de mensagem no formato RFC 822.
Reparem na linha em branco que separa o cabeçalho da mensagem.
.
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye



ITnerante

Problemas de Segurança

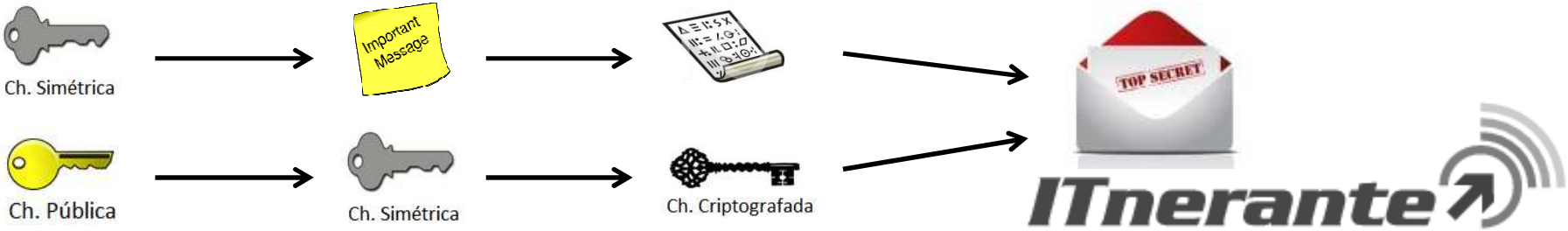
- Confidencialidade



ITnerante

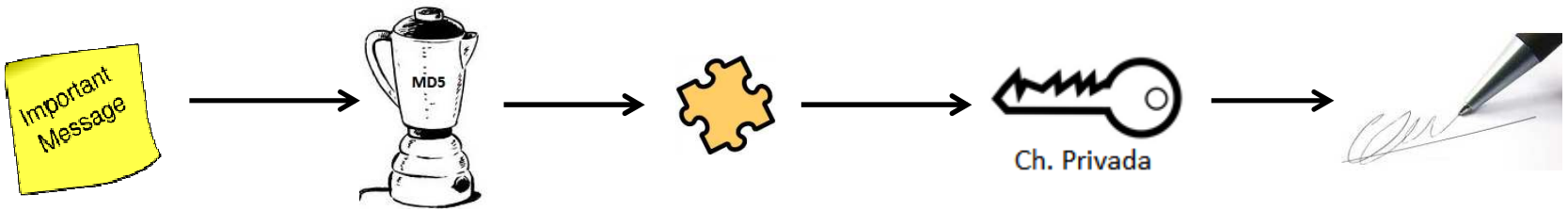
Criptografia

- Tipos
  - Chave Simétrica
    - Chaves de cifração e decifração iguais
    - Baixo custo computacional
    - DES, AES, RC4
  - Chave Assimétrica
    - Chaves de cifração e decifração diferentes
      - Chave pública
      - Chave privada
    - Alto custo computacional
    - RSA
- Envelopamento digital
  - Criptografia simétrica para cifração da mensagem
  - Criptografia assimétrica para cifração da chave simétrica



Criptografia

- Função de resumo (Hash)
  - Mesma entrada sempre gera a mesma saída
  - Unidirecional
  - Resumo fixo
  - MD5, SHA-1
- Assinatura digital
  - A mensagem é criptografada com a chave privada
  - Geralmente o hash é assinado
    - Economia de processamento



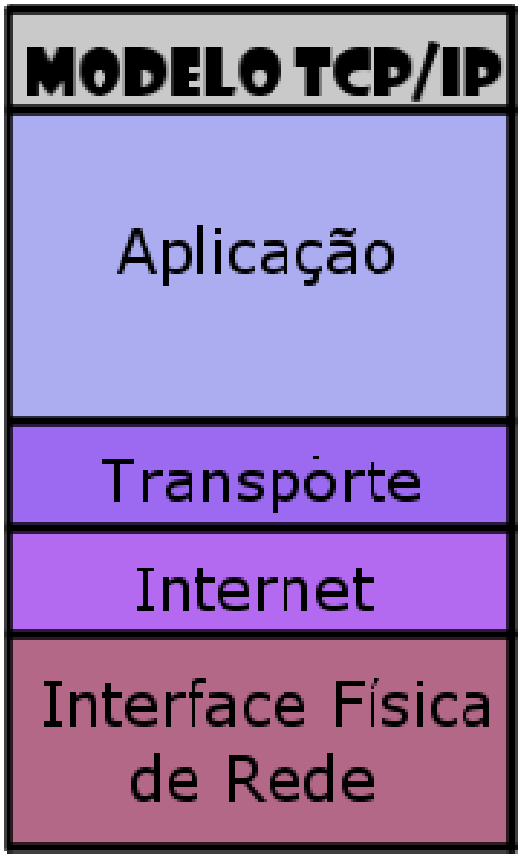
ITnerante

Certificados Digitais

- Garante a autenticidade de determinada pessoa ou organização
  - Autenticar a Chave Pública
- Relação de confiança hierárquica
  - Infraestrutura de Chaves Públicas (ICP)
  - Autoridade Certificadora
- Informações
  - Dados pessoais
  - Chave Pública
  - Validade
  - Assinatura da AC
- Padrão
  - X.509

ITnerante

Criptografia em Correio Eletrônico



- Camada de Transporte
  - SMTPS
    - 465/TCP
  - POP3S
    - 995/TCP
  - IMAPS
    - 993/TCP
  - HTTPS
    - 443/TCP
- Camada de Aplicação
  - PGP
    - Pretty Good Privacy
  - S/MIME
    - Secure MIME

ITnerante

PGP

- Pretty Good Privacy
- Mensagens eletrônicas pessoais
- Não oferece recursos de correio eletrônico
  - Criptografia e assinatura antes da transmissão
- Código fonte aberto e distribuído gratuitamente
- Utiliza algoritmos de criptografia existentes
  - RSA
  - CAST-128
  - SHA-1

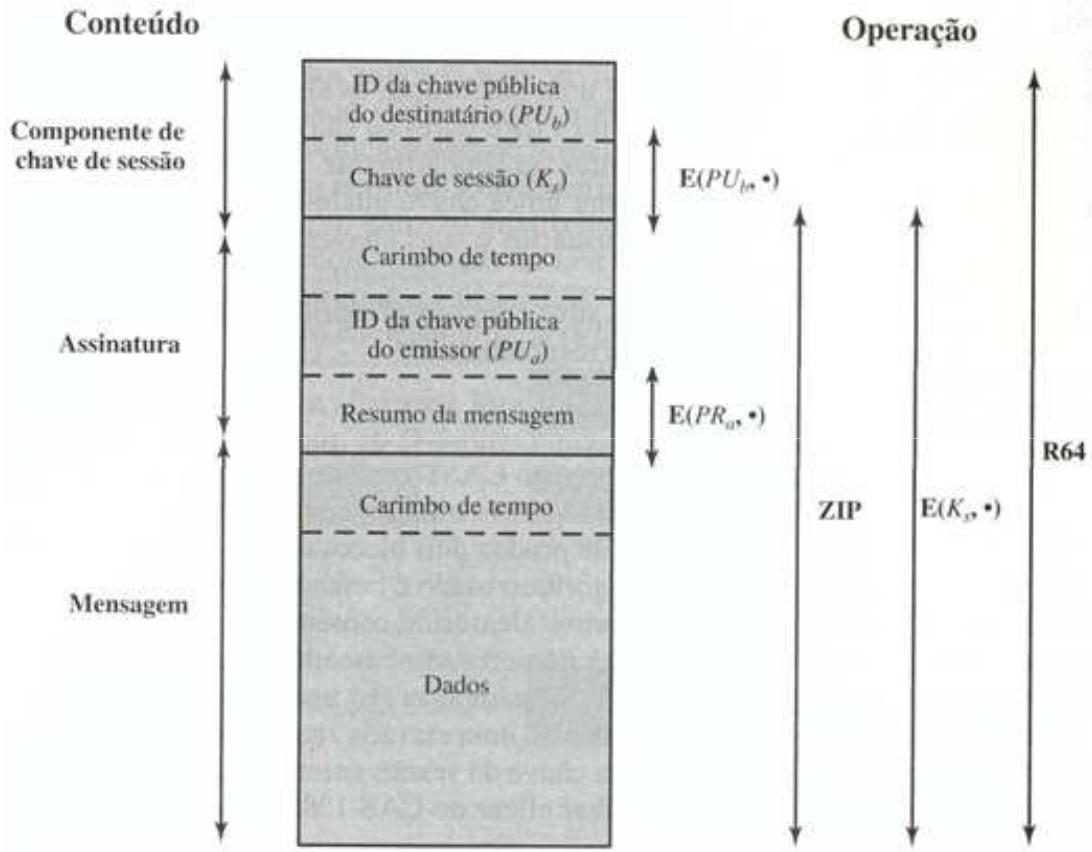
ITnerante

PGP

- Serviços
  - Assinatura Digital
    - Criptografia do hash com a chave privada
    - Assinaturas separadas
  - Criptografia
    - Codificação da mensagem com a chave simétrica
    - Uma chave simétrica por sessão
    - CAST-128, IDEA, 3DES
    - Modo CFB de 64 bits
  - Compressão
    - Reduz o tamanho da mensagem utilizando o algoritmo ZIP
  - Compatibilidade de e-mail
    - Codificação em Radix64
  - Segmentação
    - Fragmentação e remontagem de mensagens muito grandes

ITnerante

PGP



Notação:

$E(PU_b, \bullet)$	=	criptografia com a chave pública do usuário b
$E(PR_a, \bullet)$	=	criptografia com a chave privada do usuário a
$E(K_s, \bullet)$	=	criptografia com chave de sessão
ZIP	=	função de compressão Zip
R64	=	função de conversão radix 64

- Operação
  1. Hash e assinatura digital
  2. Compressão da mensagem
  3. Criptografia da mensagem comprimida com a chave de sessão
  4. Criptografia da chave de sessão com a chave pública do destinatário
  5. Conversão de toda mensagem em Radix64

ITnerante

PGP

- Gerenciamento de chaves
  - Não utiliza o padrão X.509
  - Cadeia de confiança não é hierárquica
  - Conceito transitivo de confiança
    - Não possui AC
  - Teia de Confiança
    - Web of Trust
    - Autenticidade é baseada na confiança depositada no usuário provedor da chave

ITnerante

PGP

- Armazenamento das chaves
  - Lista de chaves privadas
    - Armazena as chaves privadas do usuário
    - Informações
      - ID da chave
        - » 64 bits menos significativos
      - ID do usuário
        - » E-mail do proprietário da chave
      - Chave pública do usuário
      - Chave privada do usuário
        - » As chaves privadas são criptografadas utilizando como chave simétrica o hash de uma senha
          - KEK - Key Encription Key

PGP

- Armazenamento das chaves
  - Lista de chaves públicas
    - Armazena as chaves públicas dos contatos
    - Informações
      - ID da chave
      - ID do contato
      - Chave pública do contato
      - Confiança no proprietário
        - » Atribuído manualmente pelo usuário
        - » Poder do proprietário em assinar chaves públicas de outros contatos
      - Assinaturas
        - » Assinaturas que o proprietário da chave possui de outros contatos
      - Confiança nas assinaturas
        - » Nível de confiança no assinante para certificar a chave
      - Legitimidade da chave
        - » Campo calculado pelo PGP com base nos campos "Confiança no proprietário" e "Confiança nas assinaturas"

S/MIME

- Secure/Multipurpose Internet Mail Extension
- Mensagens eletrônicas corporativas
- Provê assinatura digital e encriptação de mensagens MIME
- Similar ao PGP
  - Utiliza o conceito de envelopamento digital
  - Criptografia da chave de sessão com a chave pública do destinatário
- Utiliza algoritmos de criptografia existentes
- Faz uso de certificados X.509 versão 3
  - Mas também admite Web of Trust

ITnerante

S/MIME

- Funções
  - Dados envelopados
    - Conteúdo somente criptografado
  - Dados assinados
    - Conteúdo somente assinado
    - Admite assinaturas de vários usuários
    - Codificação em Base64
  - Dados assinados às claras
    - Assina o conteúdo em um bloco separado da mensagem
    - Base64 somente na assinatura
    - Mantém a compatibilidade com a RFC 822
  - Dados assinados e envelopados

ITnerante

S/MIME

- Tipos de conteúdo S/MIME
  - Multipart
    - Signed
      - Mensagem assinada às claras em duas partes
  - Application
    - pkcs 7-signature
      - **signedData** -> Assinatura da mensagem às claras
    - pkcs 7-mime
      - **signedData** -> Assinatura da mensagem codificada
      - **envelopedData** -> Entidade S/MIME criptografada
      - **degenerated signedData** -> Contém apenas certificados digitais
      - **compressedData** -> Entidade S/MIME comprimida

S/MIME

- Exemplo de mensagem assinada às claras

```
MIME-Version: 1.0
Message-Id: <00103112005203.00349@amyemily.ig.com>
Date: Tue, 31 Oct 2000 12:00:52 -0600
From: User1
To: User2
Subject: Exemplo S/MIME
Content-Type: multipart/signed;
    micalg=SHA1;
    boundary="limite1";
    protocol="application/pkcs7-signature"

--limite1
Content-Type: text/plain
Esse é um exemplo de conteúdo assinado às claras.

--limite1
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

MIIDdwYJKoZIhvcNAQcCoIIDaDCCA2QCAQExCTAHBgUrDgMCGjALBgkqhkik
gMIIC3DCCApugAwIBAgICAMgwCQYHKoZIzjgEAzASMRAwDgYDVQQDEwdDYXJ
k5MDgxNzAxMTA0OVoXDTM5MTIzMTIzNTk1OVowEzERMA8GA1UEAxMIQWxpY2
IIBKWYHKoZIzjgEATCCAR4CgYEAgY3N7YPqCp45PsJIKKPkR5PdDteoDuxTx

--limite1--
```

S/MIME

- Exemplo de mensagem criptografada e assinada

```
MIME-Version: 1.0
Message-Id: <00103112005203.00349@amyemily.ig.com>
Date: Tue, 31 Oct 2000 12:00:52 -0600
From: User1
To: User2
Subject: Exemplo S/MIME
Content-Type: Multipart/Mixed; boundary="limite2";

--limite2
Content-Type: application/pkcs7-mime;
        smime-type=enveloped-data
        name=message.p7m;
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=message.p7m

MIIDmQYJKoZIhvcNAQcCoIIDijCCA4YCAQExCTAHBgUrDgMCGjAtBgkqhkiG9w0BBwGgIAQ
eDQpUaGlzIGlzIHNvbWUgc2FtcGxlIGNvbnRlbnQuoIIC4DCCAtwwggKboAMCAQICAgDIMA
kGByqGSM44BAMwEjEQMA4GA1UEAxMHQ2FybERTUzAeFw05OTA4MTcwMTEwNDlaFw0zOTEyM
zEyMzU5NTlaMBMxETAPBgNVBAMTCEFsaWNlRFNTMIIBtjCCASsGByqGSM44BAEwggEeAoGB
k0hmd1dRMSPUNbb+VRv/qJ8qIbPiR9PQeNW2PIu0WloErjhdbOBoA/6CN+GvIkq1MauCcNH
mCq7s/CTFHOEjgASeUjbMpx5g6A==

--limite2
Content-Type: application/pkcs7-mime;
        smime-type=signed-data;
        name=signature.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=signature.p7m

MIIBHgYJKoZIhvcNAQcDoIIBDzCCAQsCAQAxgcAwgb0CAQAwJjASMRAwDgYDVQQDEwdDYXJ
sUlNBAhBGNGvHgABWvBHTbi7NXXHQMA0GCSqGSIb3DQEBAQUABIGAC3EN5nGIiJi2lsGPcP
LrY4OxUk660cu1lXeCSFOSOpOJ7FuVyU=

--limite2--
```

ITnerante

PEM

- Privacy Enhanced Mail
- Envelopamento digital
  - Confidencialidade
  - Integridade
  - Autenticidade
- Utiliza certificados X.509
- Nunca foi utilizado
  - Entrou em colapso

ITnerante

SPAM

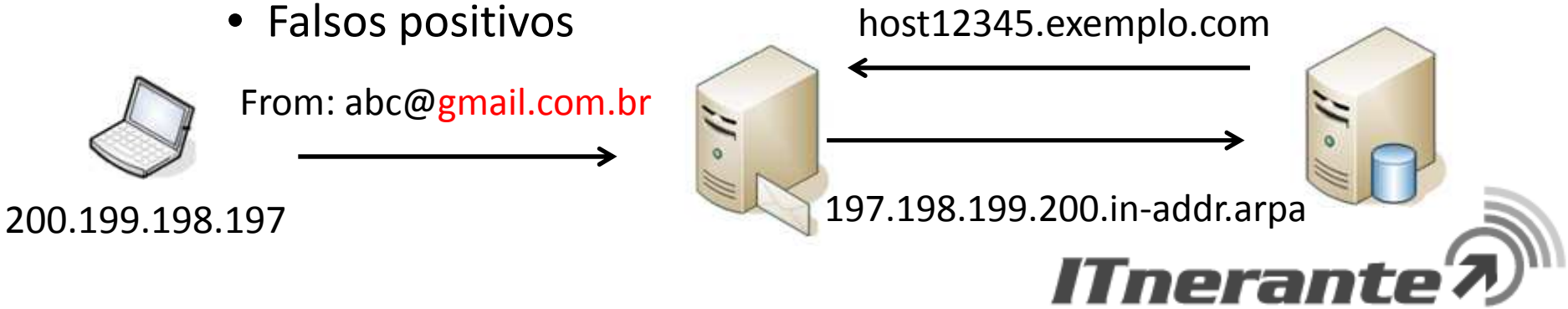
- Sending and Posting Advertisement in Mass
- E-mails não solicitados enviados a várias pessoas
  - UBE (Unsolicited Bulk E-mail)
- Geralmente associado a fins comerciais
- Alta distribuição de códigos maliciosos
- Spammers
  - Coletar endereços de e-mail
    - Ataques de dicionário
    - Códigos maliciosos
    - Harvesting
      - Varrer páginas Web, arquivos de listas de discussão, em busca de endereços de e-mail
  - Buscar meios de enviar spam
    - Relay aberto
    - Proxy aberto
    - SPAM Zombie

Classificação de SPAMs

- Harvesting
  - Chain Letters (correntes)
  - Hoax (boato)
    - Possui conteúdo alarmante ou falso
- Comerciais
  - Propagandas
    - UCE (Unsolicited Commercial E-mail)
  - Pornografia
- Fraudes
  - Scam (Golpe)
  - Phishing
- Outros
  - SPIM – Spam via Instant Messenge
  - SPIT - Spam via Internet Telephony
  - Spam via redes sociais

Técnicas Anti-SPAM

- Listas de Bloqueio
  - Bloqueia mensagens de servidores suspeitos
  - Utilizado por MUAs e por MTAs
    - Implementação simples
  - Não verifica conteúdo
    - Apenas endereços IP
  - Mantidas individualmente ou coletivamente
  - Checagem de informações DNS
    - Registro PTR
    - Falsos positivos



ITnerante

Técnicas Anti-SPAM

- Listas de Bloqueio
  - Blacklist (Lista Negra)
    - Fontes de spam
      - Endereços IP
      - Domínios
    - Listas de linhas discadas
      - Enumeram os domínios reversos de redes domésticas
    - Lista de relays e proxy abertos
      - MTAs mal configurados e navegação anônima
  - Blacklists conhecidas
    - SpamCop
    - CBL (Composite Blocking List)
    - SORBS (Spam and Open Relay Blocking System)
    - Spamhaus
    - Abusive Hosts Blocking List

ITnerante

Técnicas Anti-SPAM

- Listas de Bloqueio
  - Whitelist (Lista Branca)
    - Lista de exceções às regras de bloqueio por listas negras ou outros critérios
    - Não são submetidos às técnicas de bloqueio
- Greylisting
  - Método de filtragem de spams
  - Implantado no servidor de e-mails
  - Recusa temporariamente um e-mail e o recebe somente quando ele é reenviado
  - Servidores legítimos sempre reenviam as mensagens

ITnerante

Técnicas Anti-SPAM

- Regras de envio
  - Opt-in
    - Proibido mandar e-mails comerciais/spam
    - A menos que exista uma concordância prévia por parte do destinatário
  - Soft opt-in
    - Similar ao Opt-in
    - Existe uma relação comercial entre remetente e destinatário
    - Não é necessária a permissão explícita por parte do destinatário
  - Opt-out
    - Permitido mandar e-mails comerciais/spam
    - Deve haver um mecanismo de bloqueio das mensagens

ITnerante

Técnicas Anti-SPAM

- Filtros de Conteúdo
  - Reconhecimento de padrões que buscam identificar se o e-mail possui vírus ou spam
  - Análise do conteúdo da mensagem
    - Corpo
    - Anexos
  - Não verifica servidores
  - Alto custo de processamento
  - Falsos positivos

ITnerante

Técnicas Anti-SPAM

- Filtros de Conteúdo
  - Classificação
    - Antivírus
      - Necessidade de desmontar a mensagem
      - Descomprimir os anexos
      - Aplicado depois de outras técnicas
    - Bloqueio de anexos
      - Bloqueio de mensagens com determinados arquivos anexados
        - » .exe
        - » .scr
      - Cabeçalho MIME
        - » Content-Type:

ITnerante

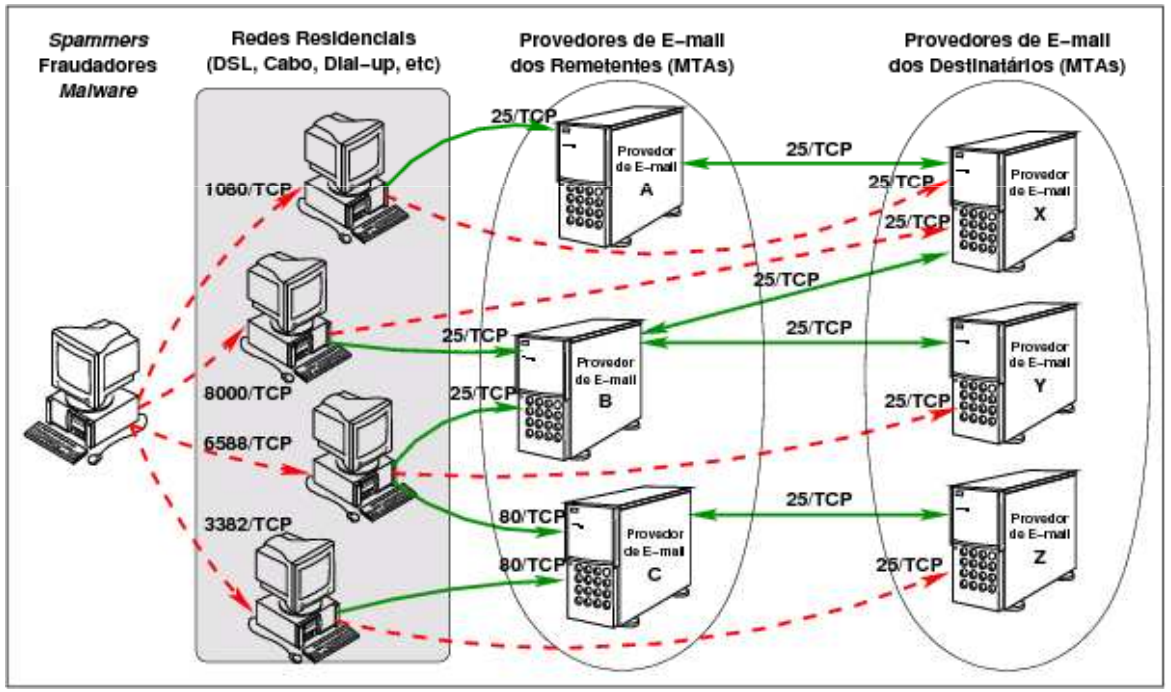
Técnicas Anti-SPAM

- Filtros de Conteúdo
  - Classificação
    - Filtro Bayesiano
      - Algoritmo de probabilidade baseado na Teorias de Bayes
      - Aprendizagem automática
        - » Treinamento inicial
        - » Criação de uma base de dados
        - » Avaliação da probabilidade de ser spam ou não
      - Foco no texto, não no anexo
      - Elevado consumo de CPU
      - Falsos positivos
        - » Quarentena

ITnerante

Técnicas Anti-SPAM

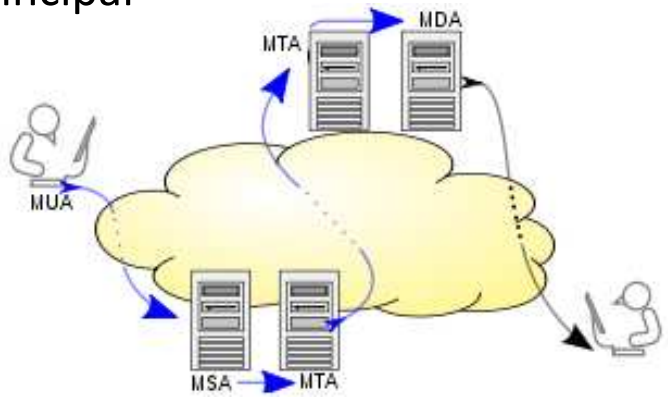
- Gerência da porta 25



ITnerante

Técnicas Anti-SPAM

- Gerência da porta 25
  - Separa as funcionalidades
    - Submissão da mensagem
    - Transporte de mensagens
  - Mail Submission Agent (MSA)
    - Software que atua como interface entre o MUA e MTA
    - Alteração da porta de 25 para 587
      - Porta 25 somente entre MTAs
  - Mail Delivery Agent (MDA)
    - Software responsável pela entrega dos e-mails nas caixas postais
    - Servidor principal



ITnerante

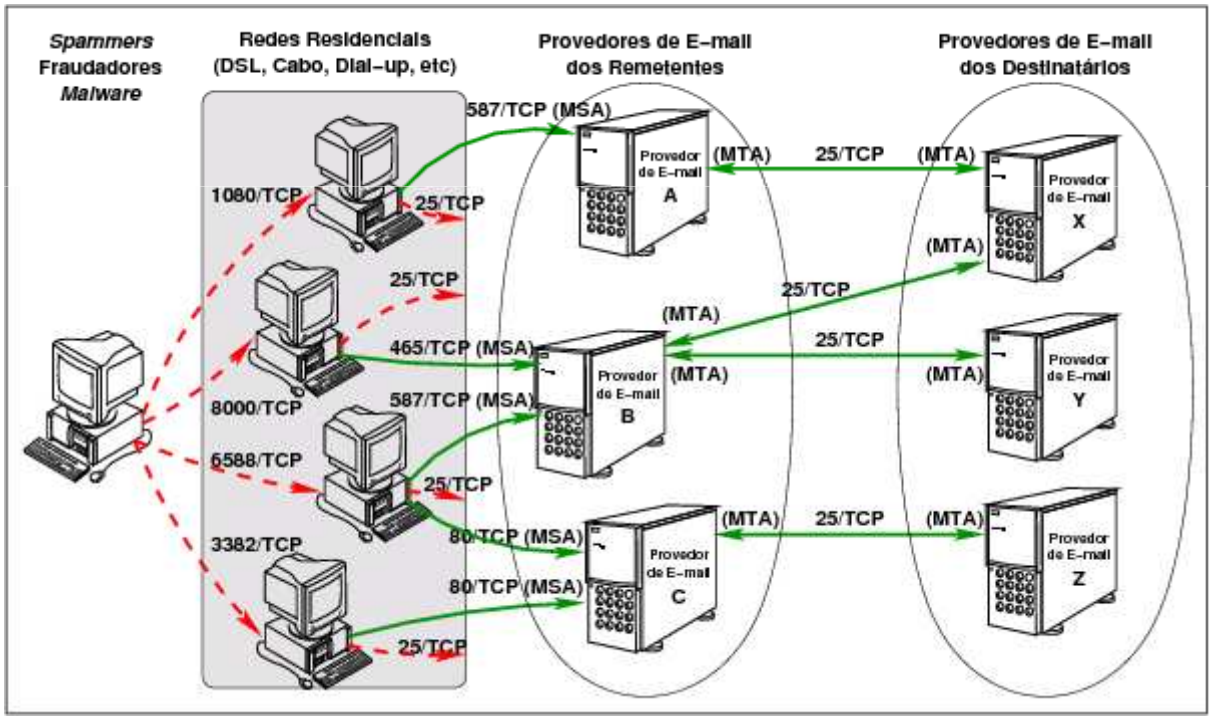
Técnicas Anti-SPAM

- Gerência da porta 25
  - Prática adotada no mundo inteiro
  - Autenticação obrigatória
  - Benefícios
    - Aplicar políticas diferentes para cada conexão
    - Concentra listas de bloqueio e filtros de conteúdo
    - Rastrear casos de abusos
    - Menor desperdício de banda
    - Melhorias futuras

ITnerante

Técnicas Anti-SPAM

- Gerência da porta 25



ITnerante

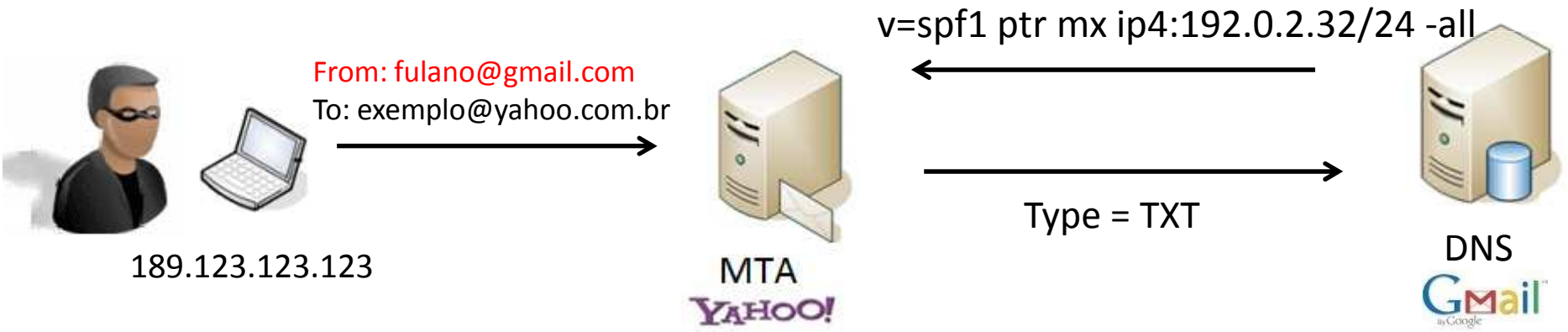
Técnicas Anti-SPAM

- SPF - Sender Policy Framework
  - Evita falsificação de endereço do remetente
    - Fake mail / Spoofing de e-mail
    - Fiscaliza o endereços IP do remetente
  - Utiliza o tipo de registro TXT do DNS
    - Sintaxe própria
  - Política SPF
    - Administrador de um domínio
      - Especifica os endereços das máquinas autorizadas a enviar mensagens
    - Administrador de um serviço de e-mail
      - Estabelece critérios de aceitação de mensagens em função da checagem das políticas SPF

ITnerante

Técnicas Anti-SPAM

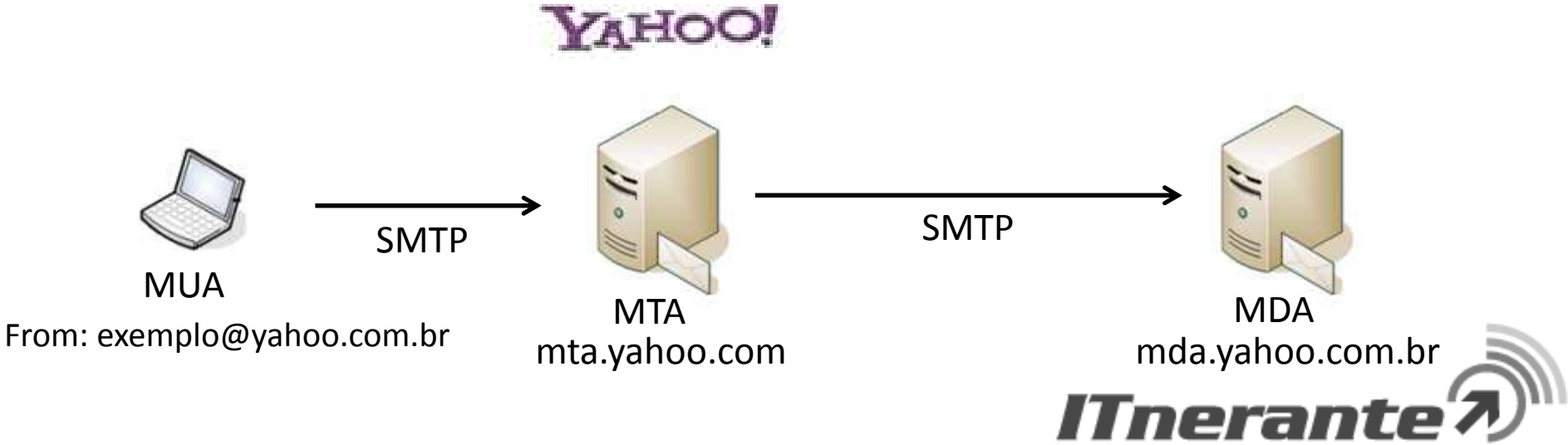
- SPF - Sender Policy Framework
  - Exemplo



ITnerante

Técnicas Anti-SPAM

- SPF - Sender Policy Framework
  - SRS - Sender Rewriting Scheme
    - Evita que MTAs que checam SPF rejeitem e-mails redirecionados
    - O relay reescreve o endereço do remetente no envelope e encapsula o endereço original
    - Contém uma assinatura e um *timestamp, permitindo o reconhecimento de sua validade*



ITnerante

Técnicas Anti-SPAM

- DKIM – Domain Keys Identified Mail
  - Utiliza autenticação por meio de chaves públicas
  - MTA assina cada mensagem com sua chave privada
    - Garante que a mensagem partiu de determinado MTA pertencente ao domínio da mensagem
  - Chave pública disponível via DNS
  - Verifica o conteúdo e cabeçalho da mensagem
    - SPF fiscaliza somente endereço IP

Questões de Aprendizagem

Segurança em Correio Eletrônico

PETROBRÁS – CESGRANRIO 2012 – Analista de Sistemas Júnior - Infraestrutura

1. São técnicas anti-spam aplicadas às mensagens de correios eletrônicos, EXCETO a técnica

A. Lista de bloqueio
B. Opt-in
C. Classificação de Conteúdo
D. Spam Zombies
E. Greylisting

UFPA – CEPS UFPA 2011 – Técnico em TI

2. Entre as inúmeras tecnologias de segurança inventadas para a internet, aquela representada por um sistema criptográfico que os aplicativos podem usar para criptografar os dados antes da transmissão é a tecnologia

A. SSH
B. PGP
C. SSL
D. IPsec
E. WEP

MPE/SE – FCC 2009 – Analista do MP – Análise de Sistemas

3. Um convite via e-mail, em nome de uma instituição governamental, para ser intermediário em uma transferência internacional de fundos de valor vultuoso, em que se oferece um ganho percentual do valor, porém se exige uma quantia antecipada para gastos com advogados, entre outros (ex. o golpe da Nigéria), de acordo com o cgi.br é classificado como

A. spyware.
B. hoax.
C. scam.
D. backdoor.
E. spam.

INMETRO – CESPE 2010 – Pesquisador – Metrologia em Informática (adaptada)

Julgue o item acerca de técnicas de criptografia.

4. A tecnologia pretty good privacy (PGP) compartilha vários conceitos e técnicas presentes na tecnologia de ICP, entre os quais, o conceito de web of trust, fundamentado na hierarquização da distribuição de chaves de criptografia assimétrica, o mesmo princípio da cadeia de certificados X.509 usadas nas ICPs.

5. Sobre regras de envio de mensagens por e-mail, considere:

I. Opt-out - é proibido mandar e-mails comerciais/spam, a menos que exista uma concordância prévia por parte do destinatário.

II. Opt-in - é permitido mandar e-mails comerciais/spam, mas deve-se prover um mecanismo para que o destinatário possa parar de receber as mensagens.

III. Soft opt-in - não é necessária a permissão explícita por parte do destinatário para receber e-mails do remetente porque já existe uma relação comercial.

É correto o que consta em

A. I, II e III.
B. I e II, apenas.
C. III, apenas.
D. II, apenas.
E. I, apenas.

TRF 1ª – FCC 2011 – Técnico Judiciário

6. O protocolo que permite que as mensagens de correio eletrônico trafeguem encriptadas e/ou assinadas digitalmente, para que e-mails não possam ser lidos ou adulterados por terceiros durante o seu trânsito entre a máquina do remetente e a do destinatário, é

A. SSL.
B. S/MIME.
C. Form Signing.
D. Authenticod.
E. Object Signing.

DPE/SP – FCC 2013 – Agente de Defensoria Pública – Administrador de Redes

7. É comum uma rede possuir dois (ou mais) servidores de correio eletrônico destinados à recepção de mensagens: um principal, responsável por entregar as mensagens para as caixas postais dos destinatários e outros secundários, que não fazem entrega de mensagens diretamente aos destinatários. Considerando que a Defensoria implementa este tipo de configuração como solução de correio eletrônico, assinale a afirmativa INCORRETA.

A. É importante verificar se o serviço de correio está se comportando como relay aberto. Uma maneira fácil de fazer isso é através de um comando **telnet** pela porta adequada, digitando os comandos do protocolo HTTP diretamente.

B. Caso o servidor principal fique impossibilitado de receber mensagens, os secundários as recebem e as enfileiram para retransmiti- las ao principal, quando este estiver restabelecido.

C. Todas as medidas **anti-spam** adotadas no servidor principal, como SPF, **greylisting** etc, devem, na medida do possível, ser implementadas no servidor secundário também, de modo que o spam seja barrado igualmente em qualquer um deles.

D. O servidor secundário deve saber para quais domínios ele pode fazer **relay**. Este servidor não deve ser configurado como "null relay client", para evitar que sua combinação com o servidor principal forme um **relay** aberto de segundo nível.

E. O servidor principal deve assumir que o servidor secundário é confiável e não fazer testes de SPF, nem colocar em **greylisting** mensagens que venham dele, pois, se ele foi corretamente configurado, essas verificações já foram feitas. Caso seja utilizado SPF, pode-se implementar SRS no servidor secundário.

CEHAP PB – CESPE 2009 – Analista de Sistemas (adaptada)

Com relação a criptografia, julgue o item a seguir.

8. O PGP (Pretty Good Privacy) é um software de criptografia para e-mail que pode, de acordo com a versão instalada, utilizar MD5 ou SHA para processar o resumo de mensagens; CAST, DES triplo ou IDEA para criptografar chaves simétricas; e RSA para criptografar chaves públicas.

TJ/RO – CESPE 2012 – Analista Judiciário

9. Um servidor de correio eletrônico utiliza diversos recursos, entre eles, um mecanismo de aprendizagem automática que coíbe mensagens indesejadas, denominado filtro de

A. conteúdo por peso de palavras.
B. antispam com a blacklist sorbs.
C. antispam com a blacklist spamhaus.
D. antispam com algoritmo Bayes.
E. antivírus por assinaturas.

10. A respeito de software PGP (Pretty Good Privacy), para fins de segurança em correio eletrônico, é correto afi rmar que

A. não utiliza o algoritmo SHA-1 (Secure Hash Algorithm) para o processamento de resumo de mensagem.

B. a compressão ZIP é aplicada após a assinatura e antes da encriptação de mensagens.

C. para compatibilidade de e-mails, usa-se o Radix-64, que mapeia cada grupo de 4 octetos para 3 caracteres ASC II.

D. a autenticação baseia-se nos algoritmos CAST-128 e RSA.

E. a confidencialidade de mensagens baseia-se, exclusivamente, em criptografi a assimétrica.

ELETROBRÁS – CESGRANRIO 2010 – Analista de Sistemas Infraestrutura

11. O presidente de uma empresa reclama com o diretor de TI a respeito do recebimento de muitos e-mails indesejados, principalmente sobre oferta de produtos não solicitados.

O diretor de TI pede uma solução à sua equipe que aponta ser necessário

A. bloquear o endereço IP remetente do e-mail no firewall externo ou roteador de borda.
B. bloquear o campo remetente (RFC 822) do e-mail no próprio servidor SMTP.
C. treinar uma rede neural com segmentos TCP para aprendizagem de classificação de SPAM.
D. utilizar filtros bayesianos como mecanismo de redução de e-mails indesejados.
E. eliminar os segmentos TCP que não sofreram confirmação de recebimento no roteador de borda.

TRF 3ª – FCC 2007 – Técnico Judiciário

12. Referem-se a sistemas de correio eletrônico seguro:

A. PGP (Pretty Good Privacy), PEM (Privacy Enhanced Mail) e S/MIME (Secure/MIME).
B. SSL (Secure Sockets Layer), PEM (Privacy Enhanced Mail) e S/MIME (Secure/MIME).
C. SSL (Secure Sockets Layer), Kerberos e PGP (Pretty Good Privacy).
D. Kerberos, S/MIME (Secure/MIME), SSL (Secure Sockets Layer).
E. PEM (Privacy Enhanced Mail), S/MIME (Secure/MIME) e Kerberos.

TRT 24ª – FCC 2011 – Técnico Judiciário

13. O usuário do computador recebe uma mensagem não solicitada, geralmente de conteúdo alarmista, a fim de assustá-lo e convencê-lo a continuar a corrente interminável de e-mails para gerar congestionamento na rede. Trata-se de um ataque denominado

A. Hoax.
B. Worms.
C. Trojans.
D. Spam.
E. Backdoors.

TRE/RJ – CESPE 2012 – Analista Judiciário – Análise de Sistemas (adaptada)

A respeito de correio eletrônico, julgue os item seguinte.

14. O termo spim é empregado para spams via instant messenge, ou seja, o envio de mensagens eletrônicas não solicitadas por meio dos aplicativos de troca de mensagens instantâneas como, por exemplo, o Microsoft Messenger e o ICQ.

CGU – ESAF 2012 – Analista de Finanças e Controle – Infraestrutura

15. Qual a diferença entre os protocolos SPF e DKIM?

A. O primeiro verifica o endereço IP do destinatário, enquanto o segundo verifica a estrutura do conteúdo do cabeçalho do e-mail.
B. O primeiro verifica o conteúdo do e-mail, enquanto o segundo verifica a sintaxe do conteúdo do e-mail.
C. O primeiro verifica o endereço IP do remetente, enquanto o segundo verifica a estrutura do conteúdo do e-mail.
D. O primeiro verifica a existência de palavras classificadas no e-mail, enquanto o segundo verifica a validade dos endereços de IP.
E. O primeiro verifica o conteúdo e o endereço IP do remetente, enquanto o segundo verifica a existência de palavras classificadas no e-mail.

Gabarito

1. D
2. B
3. C
4. E
5. C
6. B
7. A
8. C
9. D
10. B
11. D
12. A
13. A
14. C
15. C