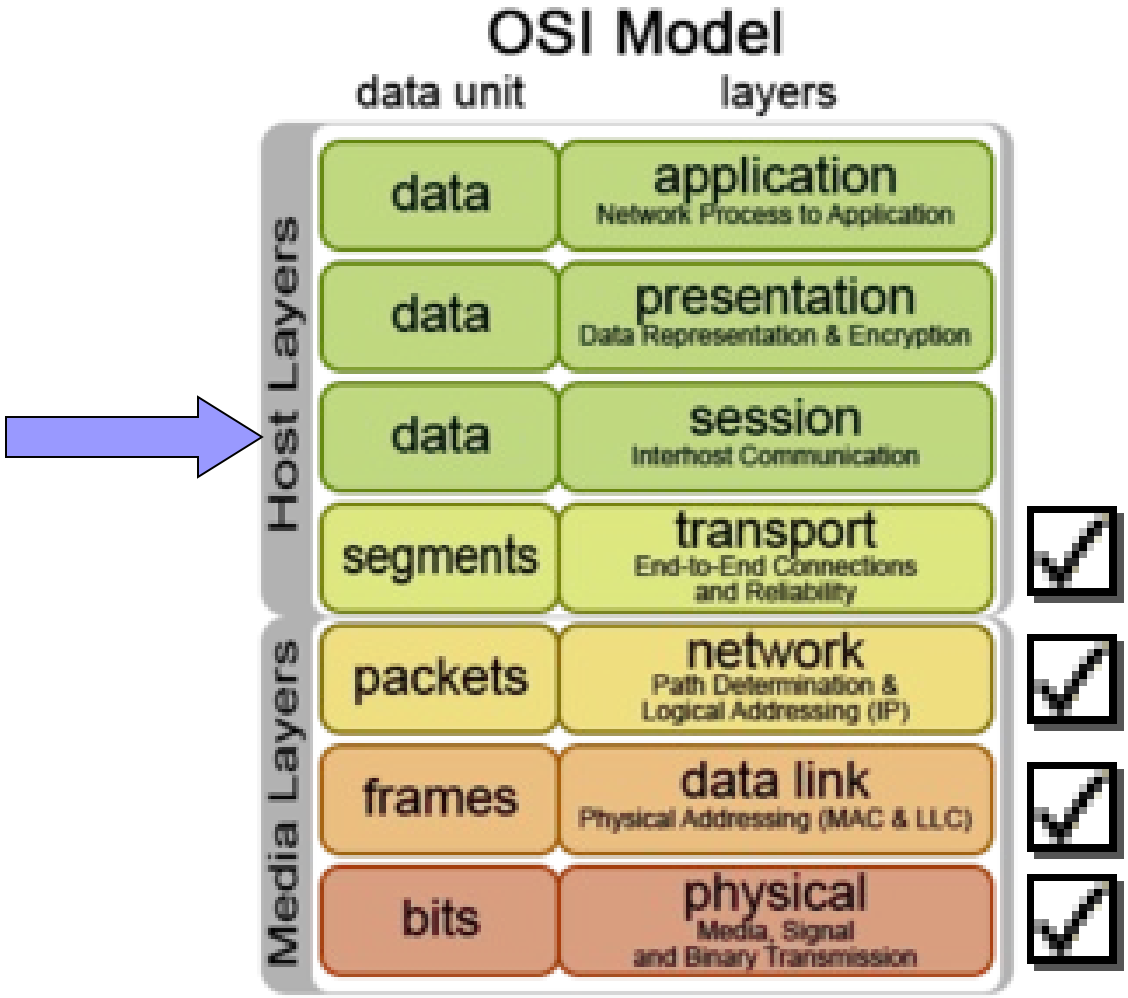
Redes de Computadores
Aula 4

Aleardo Manacero Jr.

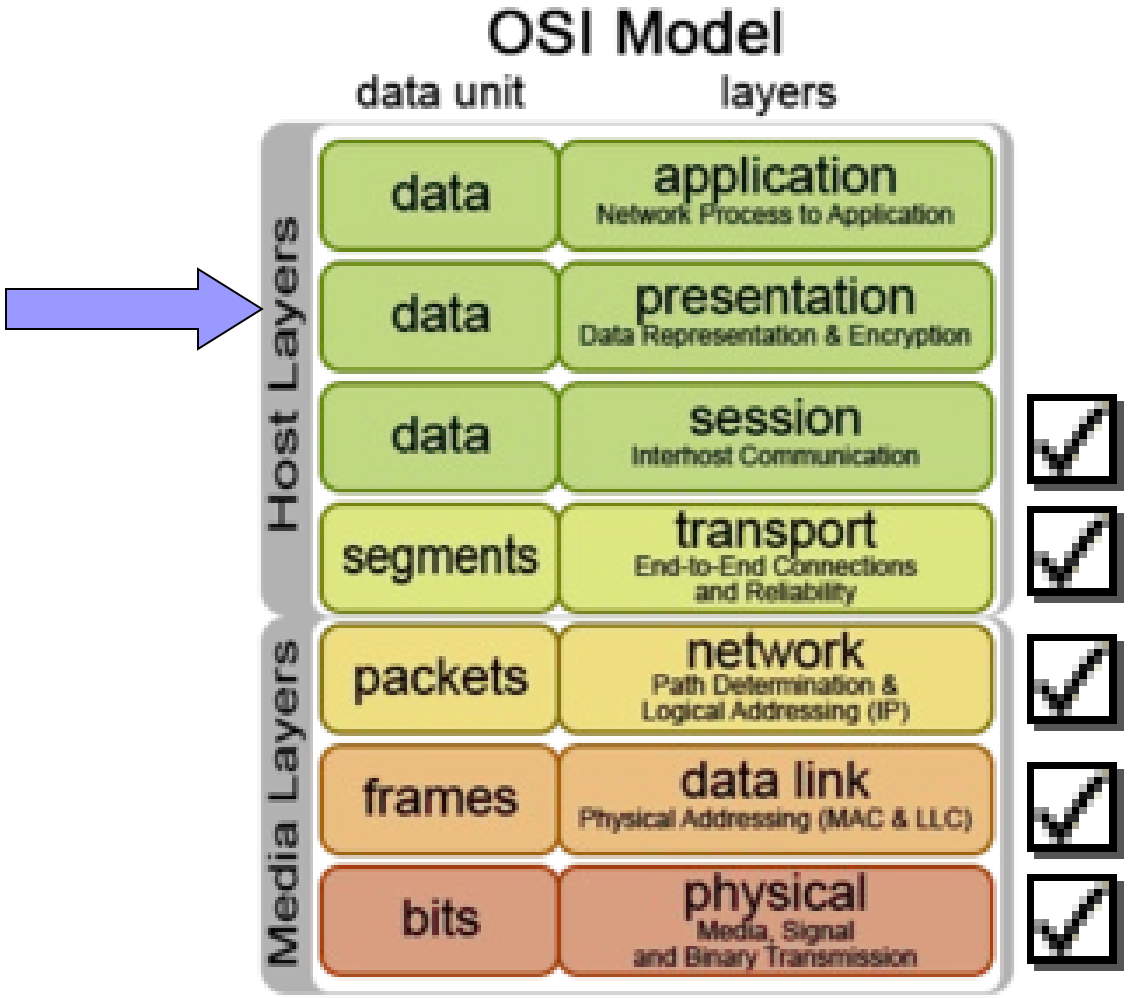
O protocolo RM-OSI



Camada de Sessão

- Supervisiona o diálogo entre os computadores envolvidos na conexão
- Cria pontos de sincronização para informações muito grandes
- Prepara a conexão antes do envio formal de dados

O protocolo RM-OSI



Camada de Apresentação

- Acordos sobre convenções e notações utilizadas
- Criptografia
- Compressão

Convenções

- Envolve aspectos como formato dos dados (*big-endian*, *low-endian*, ASCII, EBCDIC, etc.)

- Sintaxe dos comandos a serem utilizados (definição de uma linguagem comum, como a ASN.1 – Abstract Syntax Notation)

Criptografia

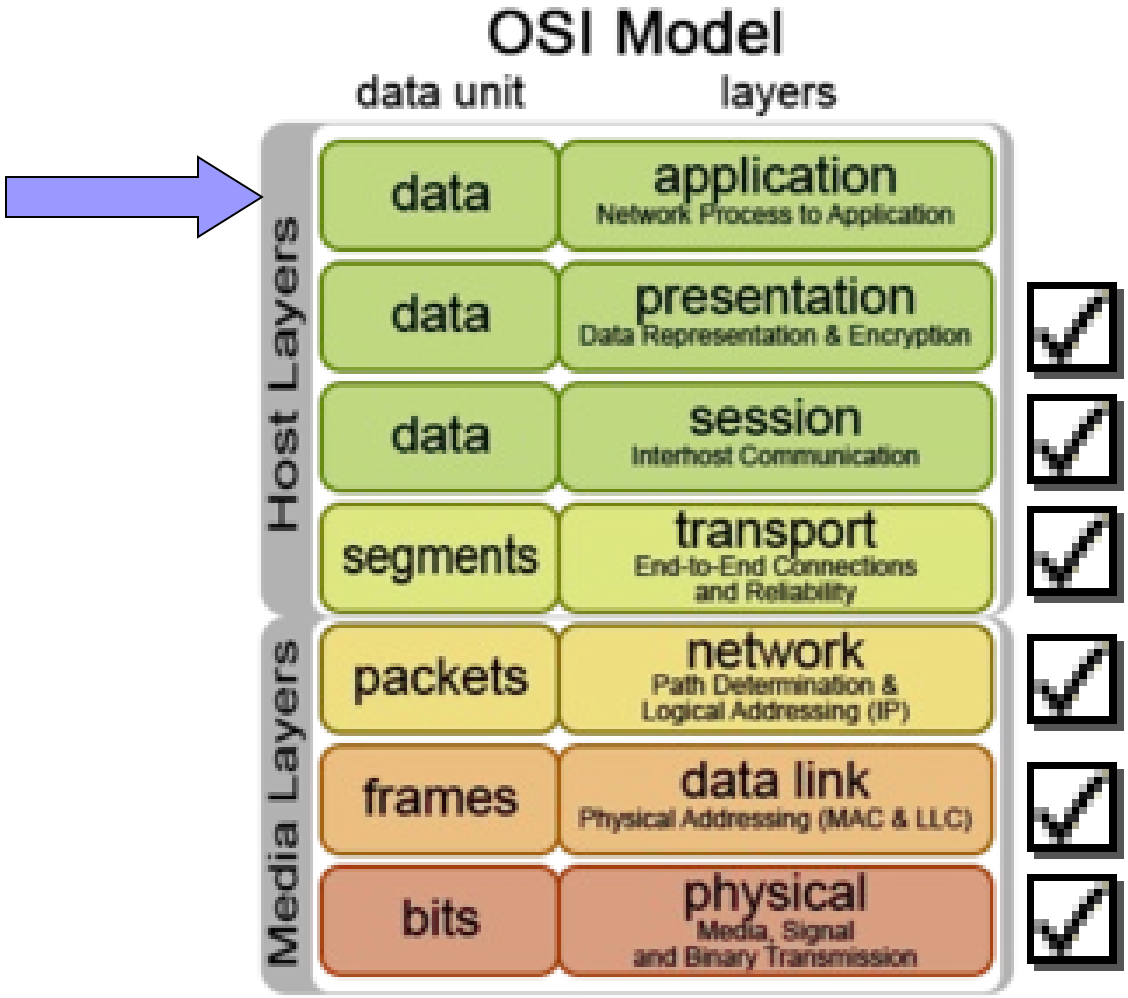
- Define formas de codificação das informações a serem transmitidas, de modo a diminuir o risco de serem lidas de modo ilícito
- Os métodos tradicionais de criptografia (DES, RSA) são usados aqui, quando necessários

Compressão

- Envolve a compactação das informações de forma a reduzir o consumo de banda passante

- Métodos como os de Huffman, Shannon-Fano e Liv-Zempel são utilizados para fazer a compressão

O protocolo RM-OSI



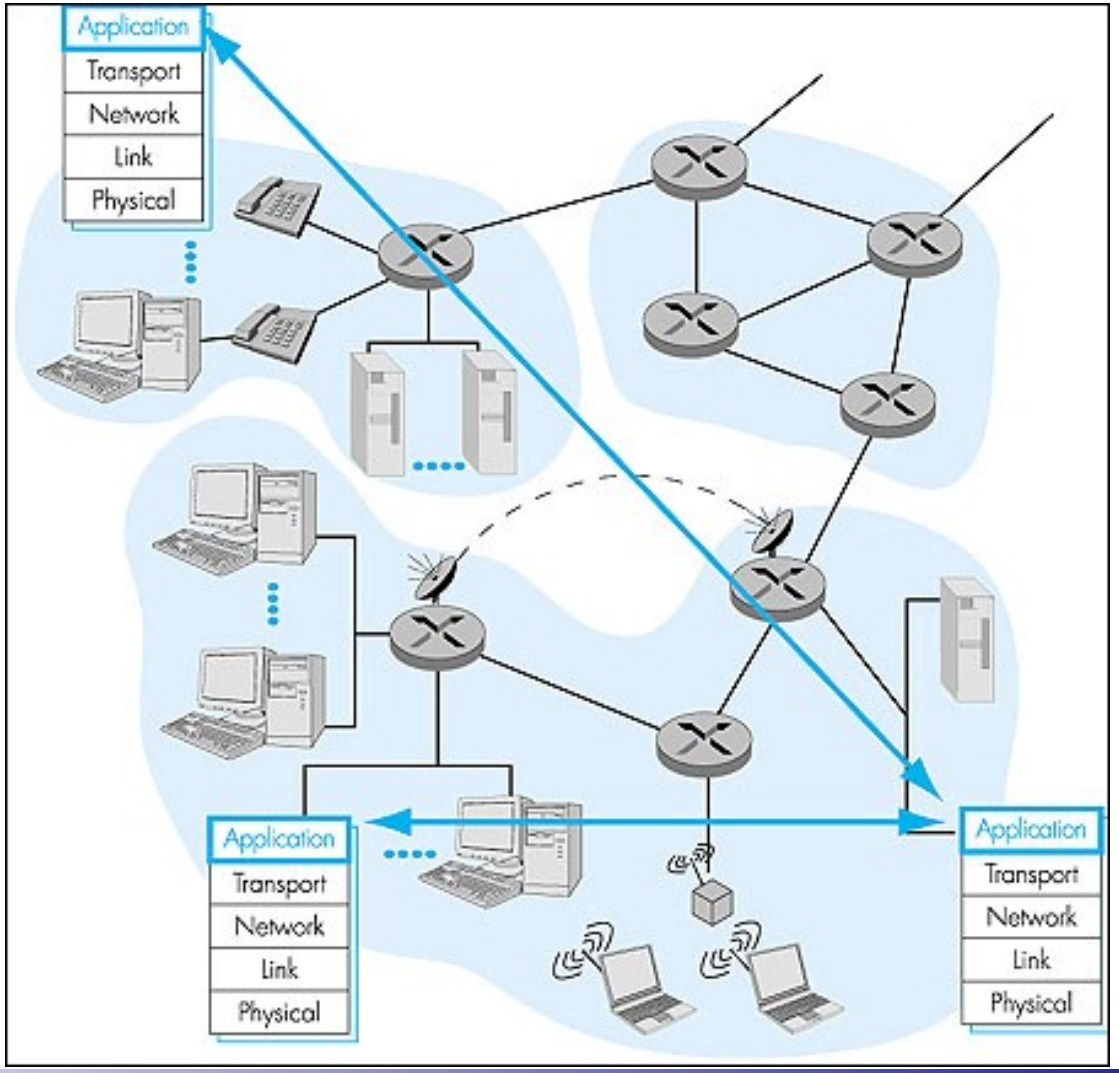
Camada de Aplicação

- Oferece serviços de rede para as aplicações em execução
- Modelo TCP/IP não contêm camadas de apresentação e sessão (incluídas nas camadas de aplicação e transporte)

Aplicações

- Uma aplicação é caracterizada por processos distribuídos em comunicação
- Executam nos sistemas finais trocando mensagens para implementar a aplicação, dependendo de um protocolo fim a fim subjacente para transferir as mensagens
- Exemplo de aplicações: WWW, transferência de arquivos, correio eletrônico, login remoto, etc

Aplicações


Application
Transport
Network
Link
Physical
Application
Transport
Network
Link
Physical
Application
Transport
Network
Link
Physical

Protocolo

- É uma parte da aplicação
- Define as mensagens que serão trocadas pelas aplicações e ações a serem tomadas a partir delas
- Utiliza de serviços providos nas camadas inferiores
- Processos em dois sistemas distintos comunicam-se trocando mensagens através da rede de computadores (processo emissor e processo receptor)

Protocolo

- Um protocolo da camada de aplicação define
  - Tipos de mensagens trocadas (pedido ou resposta)
  - Sintaxe dos campos das mensagens
  - Semântica dos campos das mensagens
  - Regras para determinar quando e como um processo emite ou responde mensagens

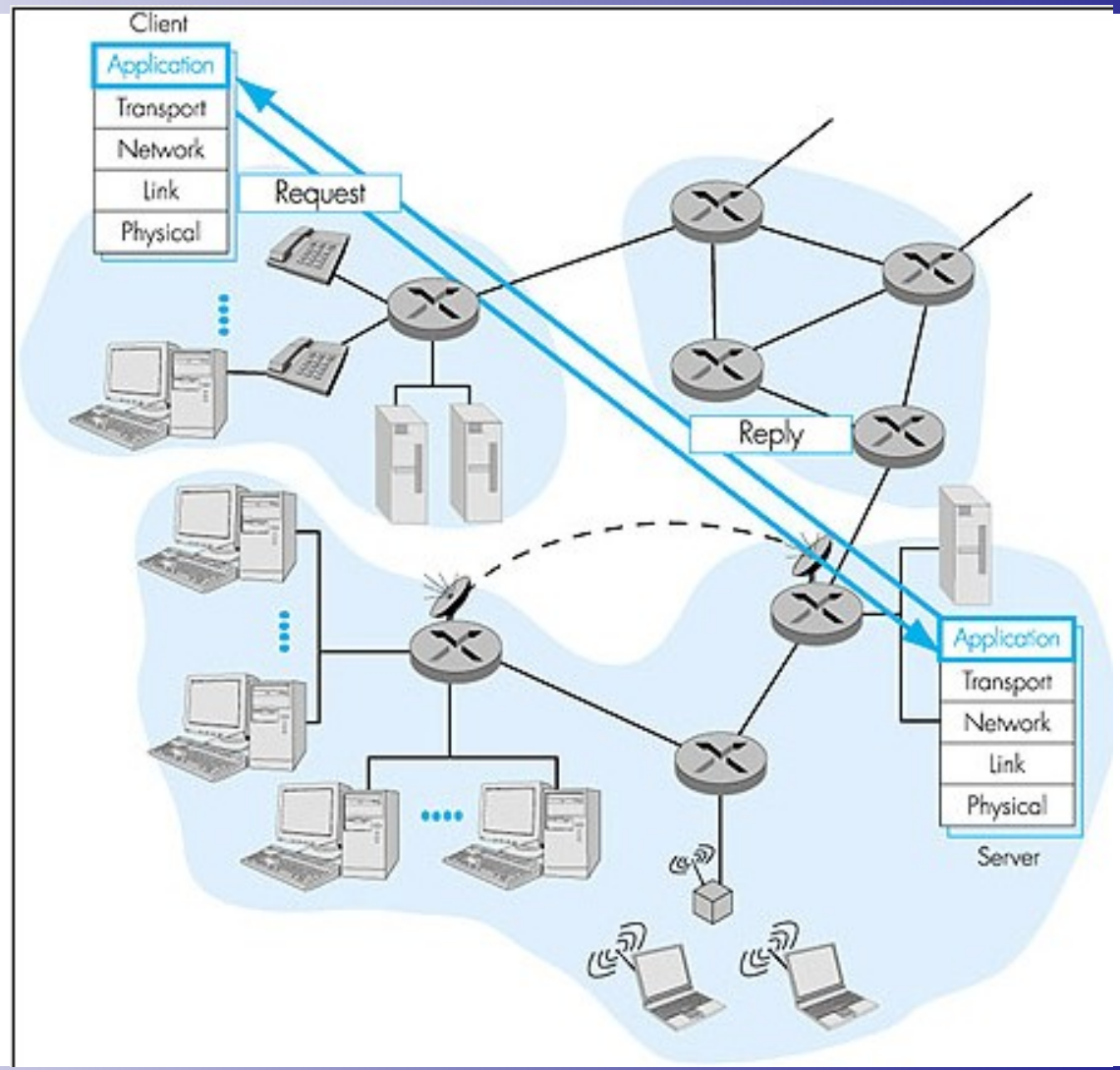
Agente de usuário

- Interface entre o usuário e a aplicação de rede
- Exemplo:
  - Correio eletrônico: Leitor/Compositor de mensagens (Eudora, Outlook, etc)
  - WWW: Browser (Internet Explorer, Netscape Navigator, etc)

Aplicações de rede

- As aplicações típicas de rede são compostas de duas partes:
  - Cliente (inicia o contato solicitando serviços de um servidor) Ex. WWW: cliente implementado no browser
  - Servidor (aguarda requisição e provê o serviço requisitado) Ex. Servidor WWW envia página solicitada

Aplicações de rede



Comunicação dos processos

- Como um processo identifica outro processo?
  - Endereço IP da máquina que executa o processo que quer se comunicar. Ex. 200.145.1.1:80
  - Número de porta que permite o receptor determinar para qual processo deve ser entregue a mensagem. Ex. Porta 80/TCP

Protocolo de transporte

- Qual protocolo de transporte as aplicações utilizam? Como é feita esta escolha para um projetista de aplicação?
  - Escolhe-se o protocolo que oferece serviços que atendam as necessidades da aplicação
- Métricas a serem consideradas na aplicação:
  - Perda de dados, temporização, largura de banda?

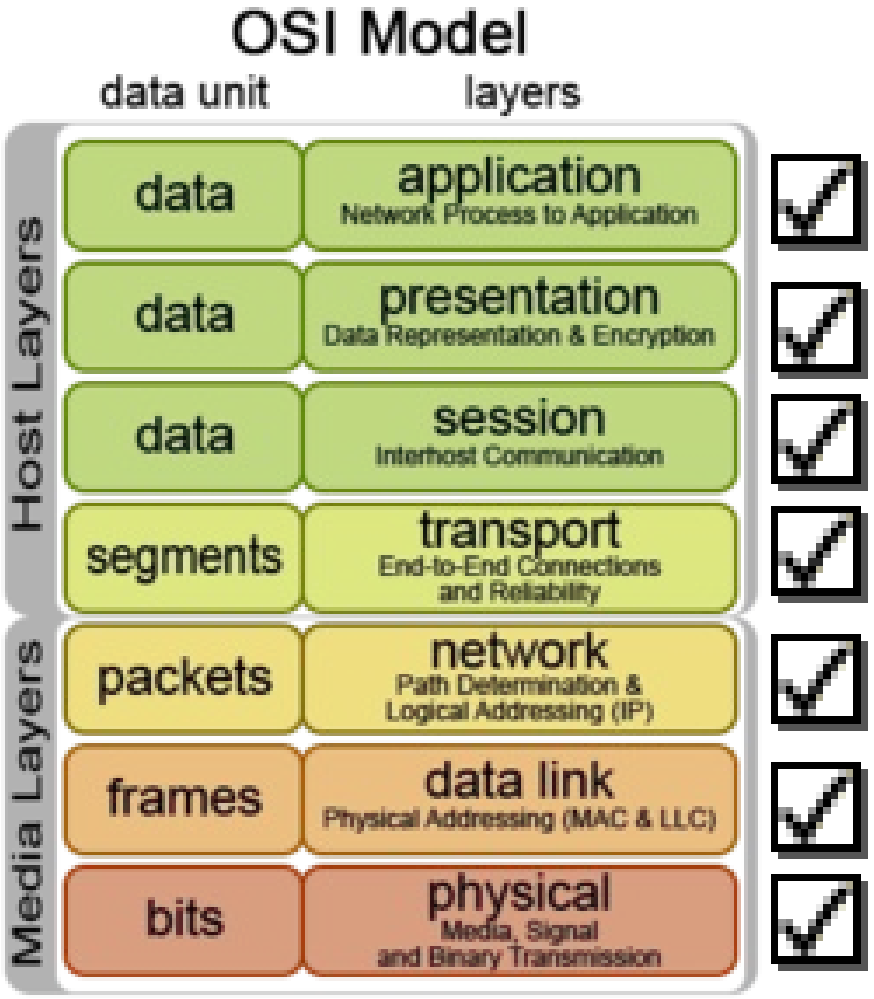
Métricas para cada aplicação

Application	Data loss	Bandwidth	Time sensitive
File transfer	No Loss	Elastic	No
E-mail	No Loss	Elastic	No
Web Documents	No Loss	Elastic (few Kbps)	No
Real-time Audio/Video	Loss-tolerant	Audio: Few Kbps - 1Mb Video: 10Kb - 5 Mb	Yes: 100s of Msec
Stored Audio/Video	Loss-tolerant	Same as Above	Yes: Few Seconds
Interactive games	Loss-tolerant	Few Kbps - 10Kb	Yes: 100s Msec
Financial Applications	No Loss	Elastic	Yes and No

Aplicações e seus protocolos

Applications	Application-layer Protocol	Underlying Transport Protocol
Electronic Mail	SMTP [RFC 821]	TCP
Remote Terminal Access	Telnet [RFC 854]	TCP
Web	HTTP [RFC 2068]	TCP
File Transfer	FTP [RFC 959]	TCP
Remote File Server	NFS [McKusik 1996]	UDP or TCP
Streaming Multimedia	Proprietary (for example, Real Networks)	UDP or TCP
Internet Telephony	Proprietary (for example, Vocaltec)	Typically UDP

O protocolo RM-OSI



Aplicações importantes

- Protocolos de acesso remoto
- Protocolos de correio
- Protocolos de troca de dados
- Protocolos de gerenciamento

Protocolos de acesso remoto

- Terminal virtual
- Execução remota
- DNS

Terminal Virtual

- Fornece remotamente a imagem de um terminal do equipamento ao qual se tem acesso
- Aplicações como xterm e vt100 representam exemplos de terminais virtuais

Execução remota

- Um dos pilares da criação da Internet
- Permite ao usuário fazer uso de equipamentos da rede, mesmo contato
- telnet e ssh são exemplos nessa categoria

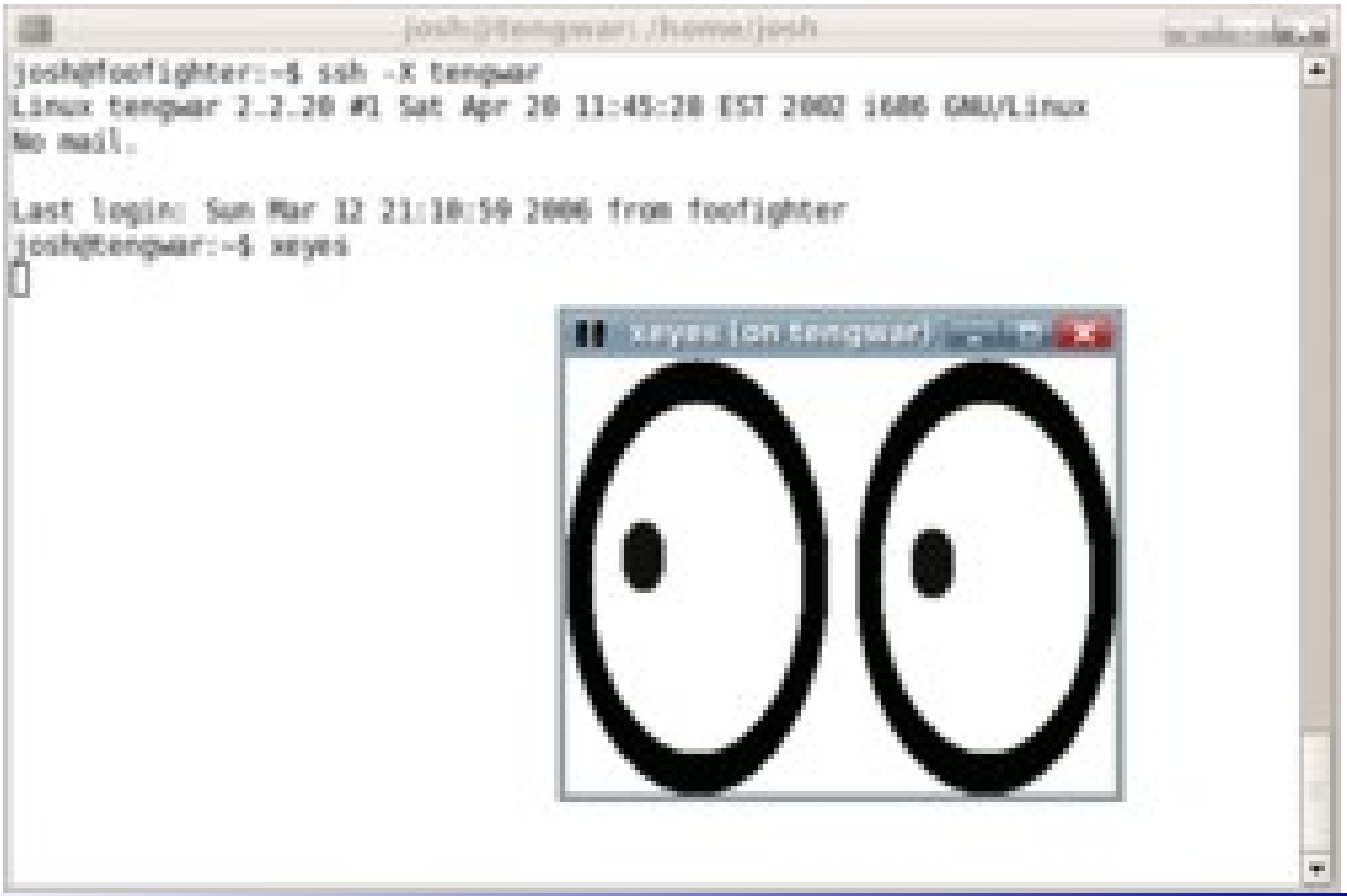
Telnet

- telnet foi uma das primeiras aplicações surgidas
- Apresenta problemas de segurança, em especial o fato de transmitir todas as informações na forma como são recebidas (sem criptografa-las), incluindo nomes e senhas de usuários

SSH

- Projetado em 1995 pelo finlandes Tatu Ylönen, o Secure Shell (SSH) é, na prática, um conjunto de aplicações
- Faz todas as transmissões usando criptografia
- Permite a autenticação do usuário e das máquinas envolvidas no processo

SSH


josh@foofighter:~$ ssh -X tengwar
Linux tengwar 2.2.20 #1 Sat Apr 20 11:45:28 EST 2002 i686 GNU/Linux
No mail.
Last login: Sun Mar 12 21:10:59 2006 from foofighter
josh@tengwar:~$ xeyes

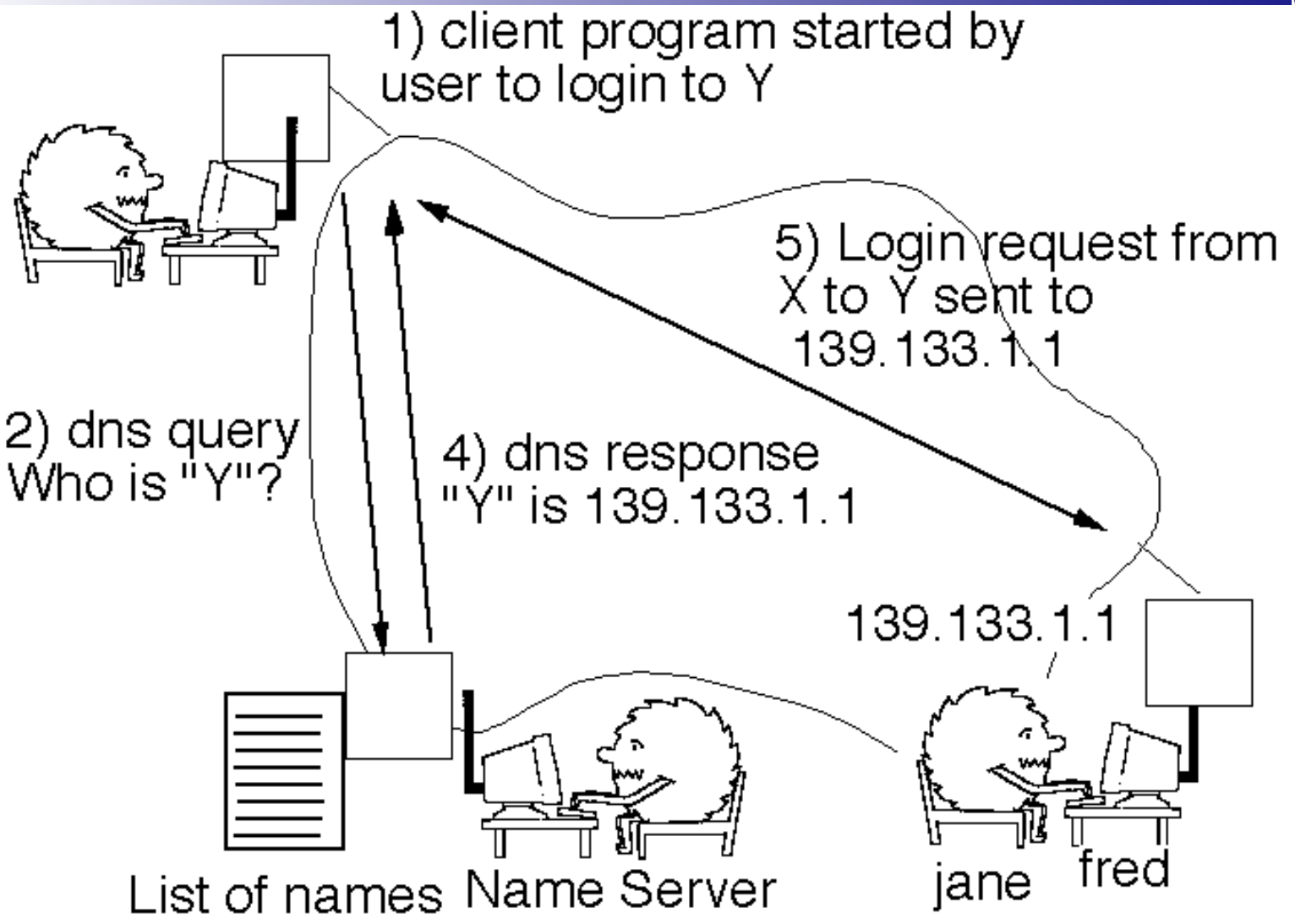
DNS

- Não é uma aplicação com o qual o usuário interage diretamente, e sim é uma função interna da Internet
- Tem a função de mapear endereços nomes em endereços IP. Porque fazer isso?
- Facilidade para os seres humanos, já que é mais fácil lembrar um nome do que vários números
- Para os dispositivos de rede ?, nomes são inviáveis porque podem ter comprimento variável e não são hierárquicos

DNS

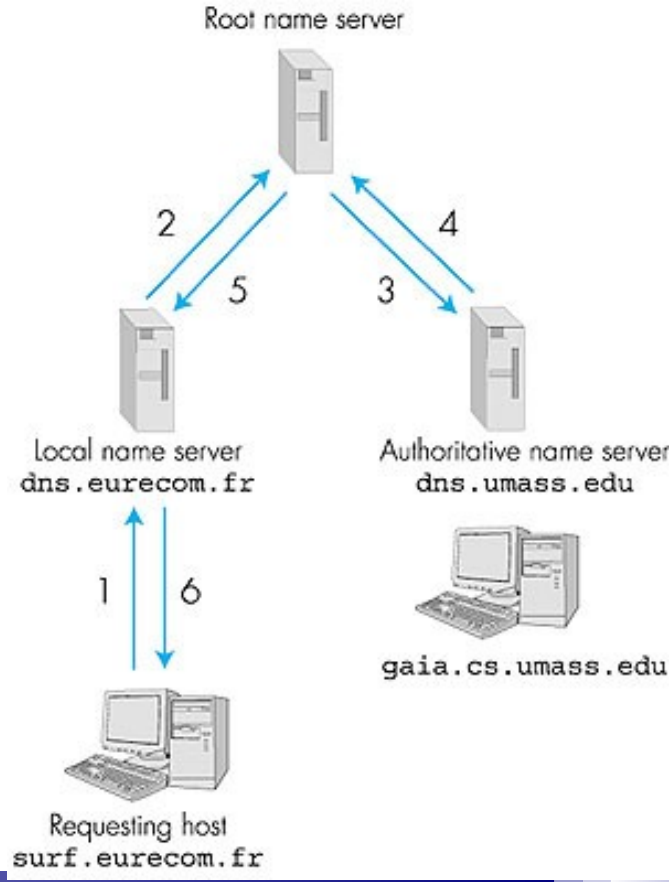
- Consiste de uma base de dados distribuída implementada em uma hierarquia de servidores de nomes
- Protocolo da camada de aplicação que permite a comunicação entre hosts e servidores de nome, de modo a fornecer o serviço de tradução.
- O DNS usa UDP/53
- Porque é distribuído e não centralizado?
  - Ponto único de falha, volume de tráfego, base de dados distante, dificuldade na manutenção

DNS


1) client program started by user to login to Y
5) Login request from X to Y sent to 139.133.1.1
2) dns query Who is "Y"?
4) dns response "Y" is 139.133.1.1
139.133.1.1
List of names
Name Server
jane
fred

DNS

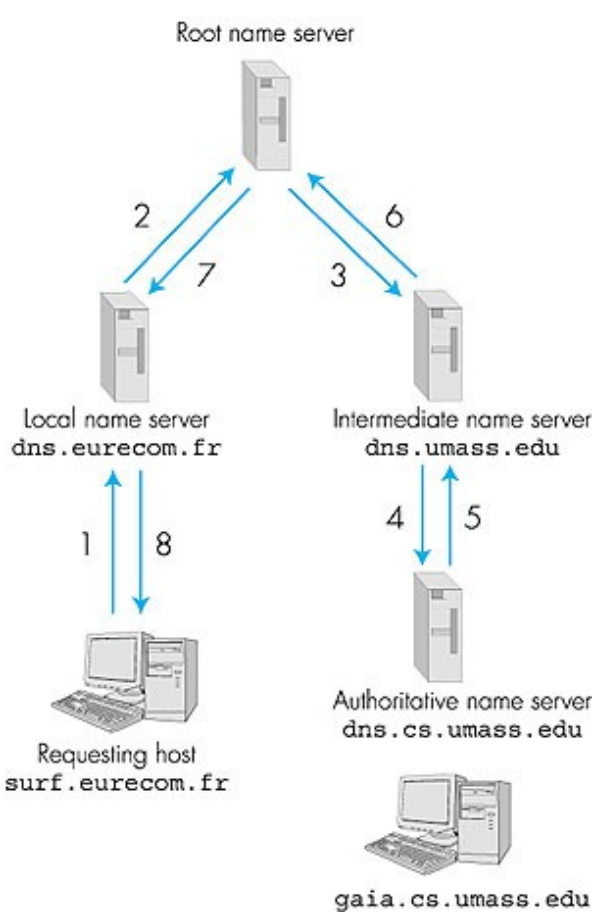
- Hierarquia dos servidores de nomes
  - Servidor de nome local
  - Servidor de nome raiz
  - Servidor de nome autoritativo
- Passos:
  - Host contacta servidor de nome local para um determinado nome X
  - Caso não tenha contata servidor raiz
  - Caso não tenha contata um servidor de nomes autoritativo para o nome X

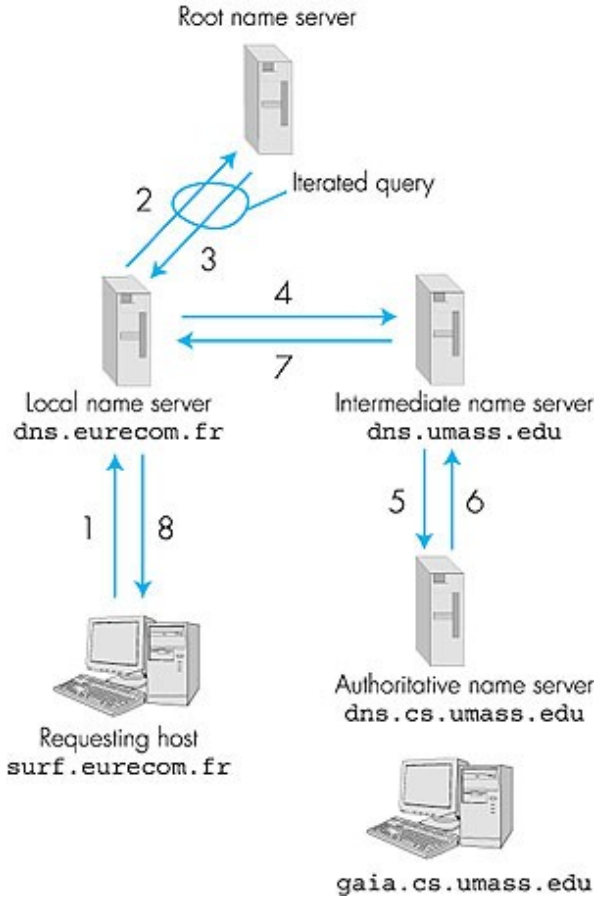


DNS

- Consultas podem ser recursivas ou iterativas
- Nas recursivas transfere a responsabilidade de resolução para o servidor de nomes contatado
- Nas iterativas o servidor responde ou indica o servidor de nomes a ser contatado
- Uso de cache e atualização de dados
  - Os servidores guardam o mapeamento em cache durante um determinado período (para futuras consultas)

DNS


Root name server
2
7
6
3
Local name server
dns.eurecom.fr
Intermediate name server
dns.umass.edu
1
8
4
5
Authoritative name server
dns.cs.umass.edu
Requesting host
surf.eurecom.fr
gaia.cs.umass.edu


Root name server
Iterated query
2
3
4
7
Local name server
dns.eurecom.fr
Intermediate name server
dns.umass.edu
1
8
5
6
Authoritative name server
dns.cs.umass.edu
Requesting host
surf.eurecom.fr
gaia.cs.umass.edu

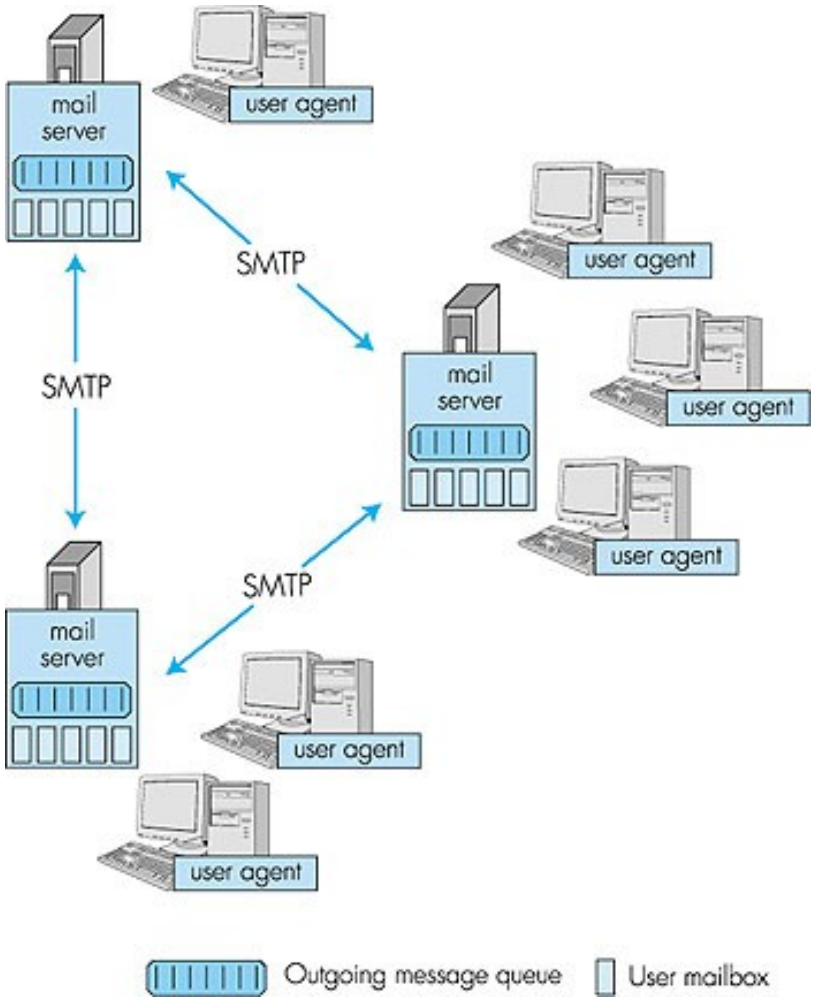
Protocolos de correio

- SMTP
- IMAP
- POP

Correio eletrônico

- Agente usuário: Mail User Agent (MUA)
  - Cliente de correio
  - Compor, editar, ler mensagens de correio
  - Ex. Eudora, Outlook
  - Mensagens de saída e entrada são armazenadas no servidor
- Agente de transporte: Mail Transport Agent (MTA)
  - Servidor de correio (contêm mensagens de chegada e de saída)
- Protocolo de correio
  - SMTP (Simple Mail Transfer Protocol), entre servidores para transferir mensagens de correio (papéis mútuos de cliente e servidor)

Correio eletrônico



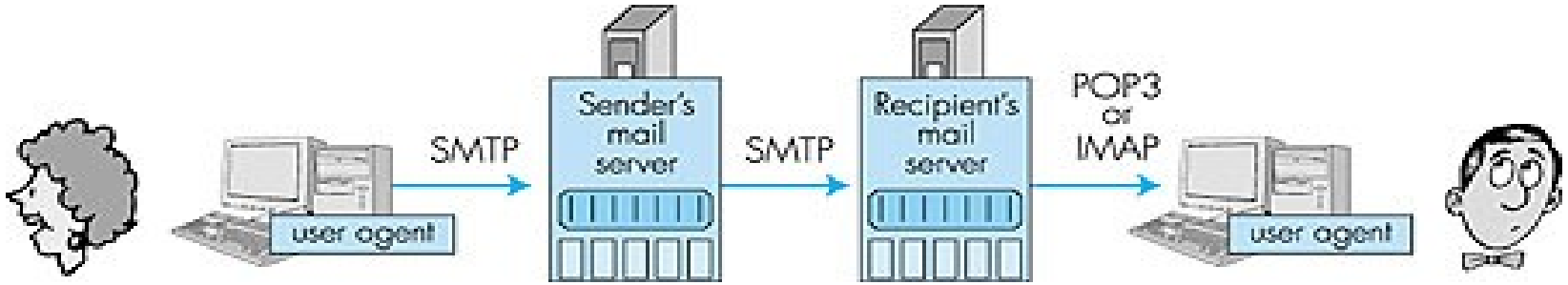
Correio eletrônico

- SMTP: usa TCP para transferência confiável na porta 25
- Mensagens em ASCII-7bits (cabeçalho e corpo)
- SMTP utiliza de conexões persistentes
- Mensagens contendo imagens, videos, audio, etc... precisam ser codificadas (MIME define isso, inserção de campos no cabeçalho para determinar tipo e codificação utilizada)

Correio eletrônico

- POP (Post Office Protocol)
  - Autorização, transação e atualização
- IMAP (Internet Mail Access Protocol)
  - Mais complexo em relação as opções
  - Pode manusear as mensagens armazenadas no servidor

- Através de HTTP pode-se acessar um servidor de correio. Ex. Hotmail, Yahoo, Gmail



Protocolos de troca de dados

- http
- ftp

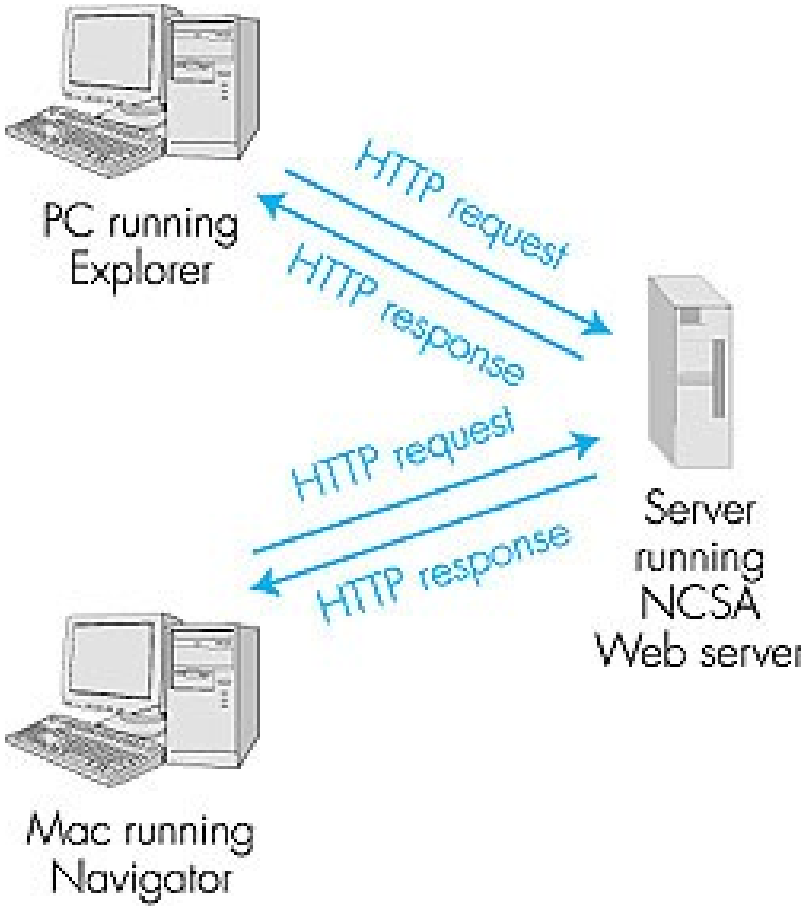
WWW (World Wide Web)

- Consiste de objetos e de uma URL (Universal Resource Locator)
- URL contêm nome do hospedeiro e o caminho pretendido
- Cliente para WWW (Internet Explorer, Netscape Navigator)
- Servidor para WWW (Apache, MS IIS)

WWW (World Wide Web)

- Protocolo: http (Hypertext Transfer Protocol)
- Cliente: Browser solicita objetos
- Servidor: Aguarda requisições e envia pedidos
- Usa serviço de transporte TCP
- Padrão de porta: 80
- Cliente inicia conexão, servidor aceita, ocorre troca de mensagens entre cliente e servidor e encerra a conexão.

WWW (World Wide Web)



WWW (World Wide Web)

- http é stateless (não armazena informações sobre pedidos anteriores do cliente)
- As conexões podem ser persistentes ou não persistentes
- Nas não persistentes cada objeto sofre dois RTT (Round Trip Time), um de estabelecimento da conexão e outro do pedido e envio. Geralmente utilizam de conexões TCP paralelas.

WWW (World Wide Web)

- Nas persistentes o cliente envia pedidos para todos objetos referenciados em um arquivo base (Ex. Html), portanto menos RTTs.
- O pedido pode ocorrer sem paralelismo ou com paralelismo
- O cliente-servidor mantêm a conexão aberta até a transferência de todos pedidos do cliente. Cada objeto sofre 1 RTT.

WWW (World Wide Web)

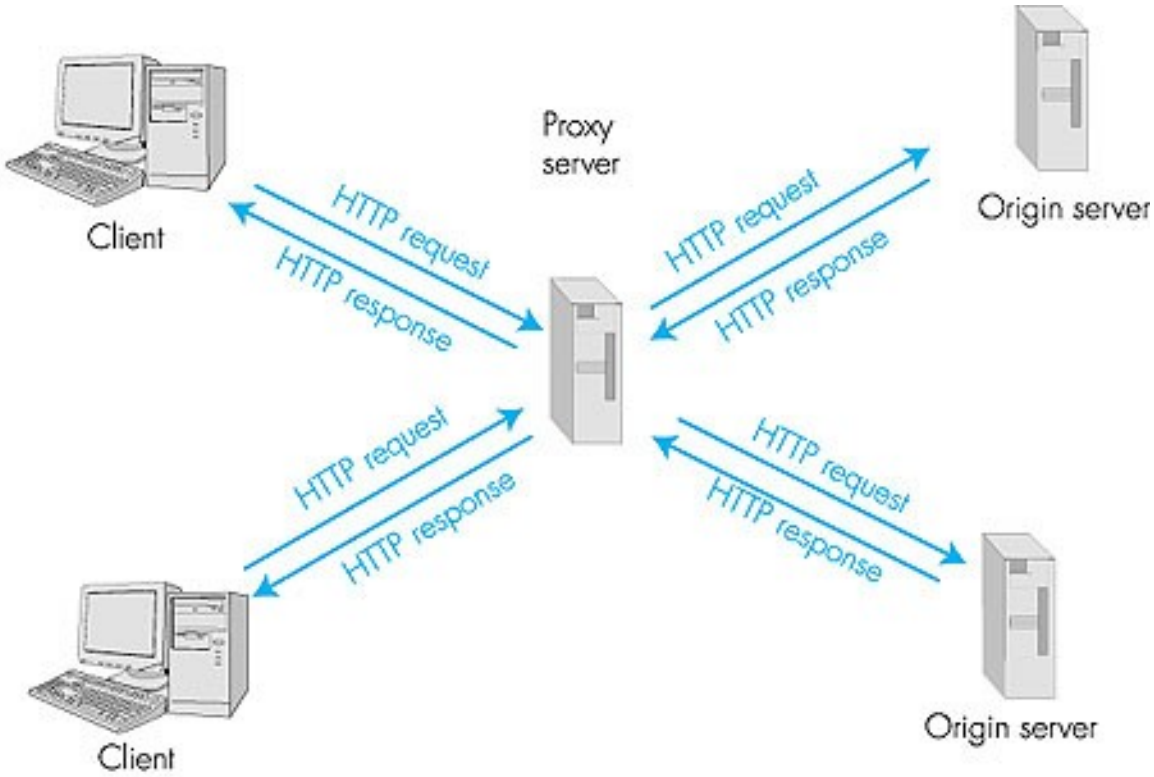
- Formas de autenticação do HTTP
- Objetivo: controlar o acesso ao servidor
  - Por autorização: Cliente solicita um objeto, e o servidor envia uma resposta com pedido de autorização (nome e senha)
  - Por cookies: Servidor envia um cookie ao cliente, e nos pedidos posteriores o cliente envia junto o cookie. Assim o servidor sabe quem é o cliente e suas preferências

WWW (World Wide Web)

- Uso de caching no cliente
  - Servidor não envia objeto ao o cliente, se este já possui a versão mais atual, só envia uma mensagem de resposta falando que o objeto não foi modificado. (cliente envia requisição com a data no cabeçalho)

- Uso de caching (proxy)
  - Atende o pedido do cliente sem envolver servidor de origem.
  - Porque usar proxy?
    - Tempo de resposta menor devido ao cache estar mais próximo do cliente

Proxy

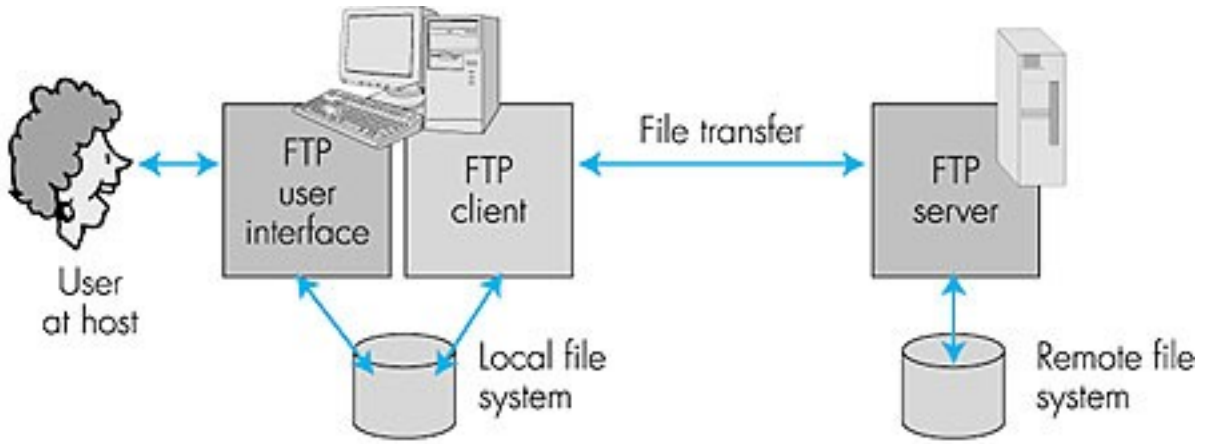

Proxy
server
Client
HTTP request
HTTP response
HTTP request
HTTP response
Origin server
HTTP request
HTTP response
HTTP request
HTTP response
Client
Origin server

Comparação SMTP com HTTP ?

- HTTP tem a função de adquirir objetos
- SMTP tem a função de enviar objetos
- Ambos tem interação de comando/resposta e códigos de status em ASCII
- No HTTP cada objeto é encapsulado em sua própria mensagem de resposta
- No SMTP múltiplos objetos são enviados na mensagem

Transferência de arquivos

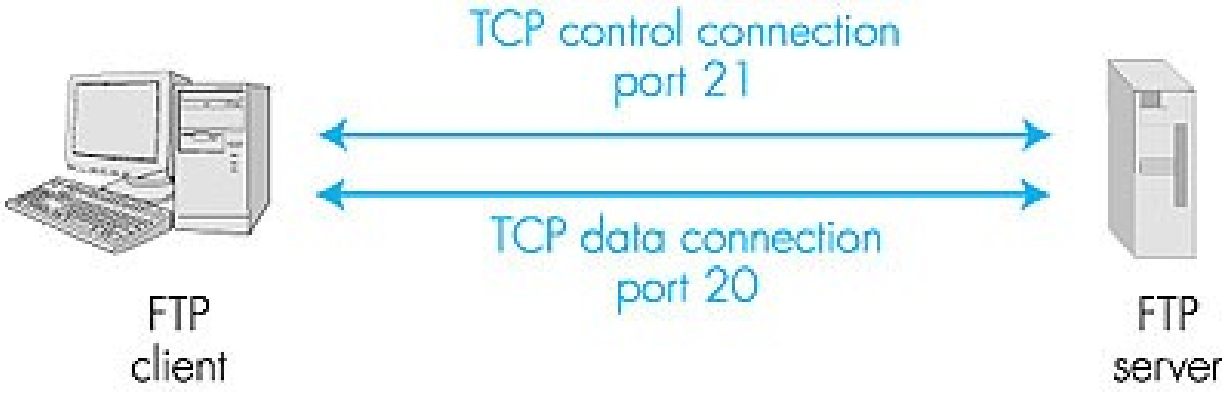
- Protocolo FTP: File Transfer Protocol
- Tranfere arquivos de/para servidor remoto
- Modelo cliente-servidor
- Porta servidor: 21/TCP



Transferência de arquivos

- São abertas duas conexões paralelas (controle na porta 21 e de dados na porta 20)

- Servidor mantêm informações de estado, como diretório corrente e autenticação.



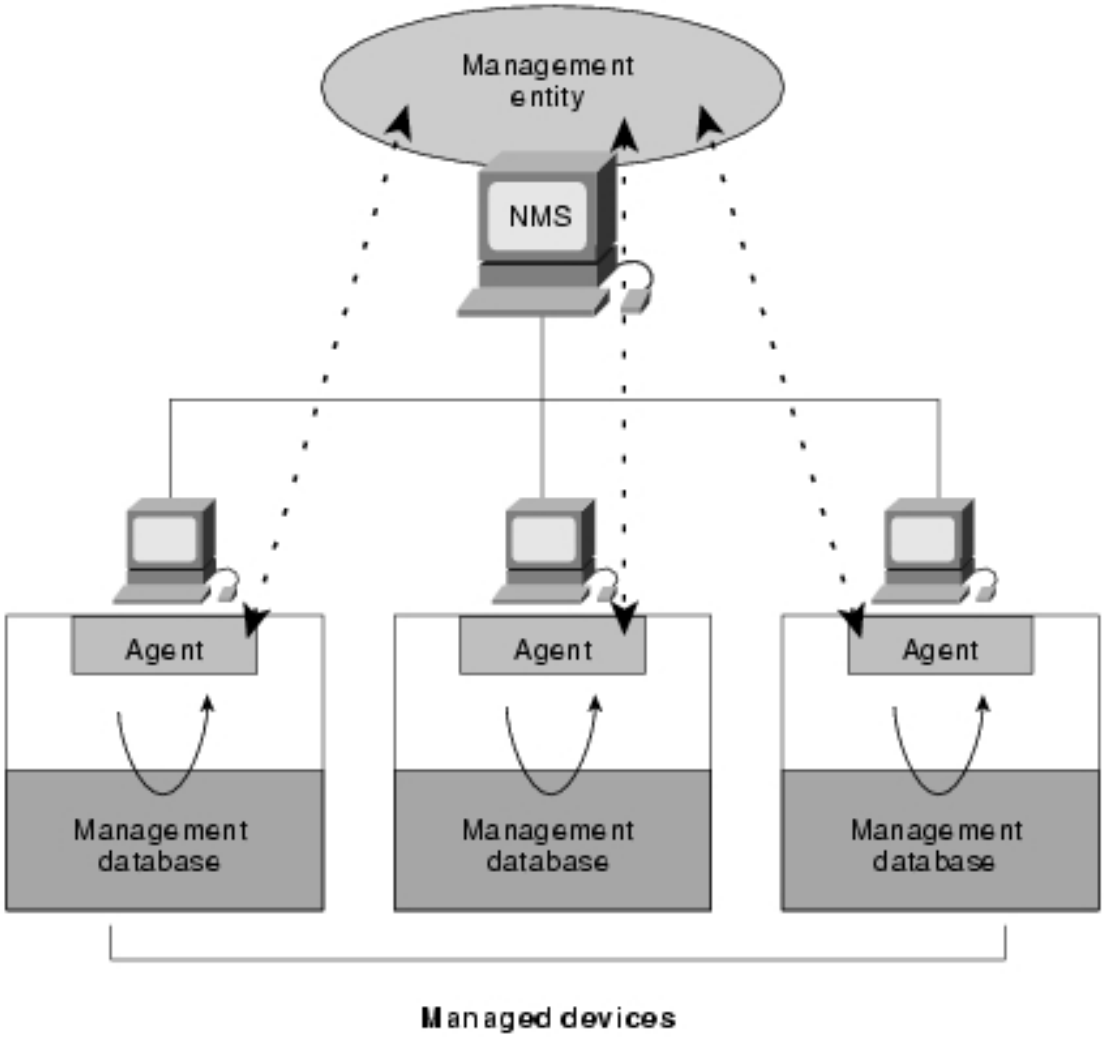
Protocolos de gerenciamento

- SNMP
- NFS
- NIS
- LDAP
- Segurança

SNMP

- Simple Network Management Protocol é um protocolo de gestão típica de redes TCP/IP
- Facilita o intercâmbio de informação entre os dispositivos de rede.
- Possibilita aos administradores de rede gerir o desempenho da rede, encontrar e resolver problemas de rede, e planejar o crescimento desta.

SNMP


Management entity
NMS
Agent
Agent
Agent
Management database
Management database
Management database
Managed devices

NFS

- É um sistema distribuído de arquivos criado pela Sun Microsystems
- Permite que usuários tenham, a partir de uma máquina qualquer, acessar arquivos distribuídos na rede como se fossem locais
- Tendência de desuso

NIS

- **Network Information Service,** é um protocolo para autenticação de usuários
- Criado pela Sun Microsystems como mecanismo de seu SO para o gerenciamento da estrutura de usuários e seus diretórios como um modelo cliente-servidor
- Tendência de desuso

LDAP

- **Lightweight Directory Access Protocol** é um protocolo para gerenciamento de estruturas de diretórios (incluíndo a autenticação e validação de acessos)
- Originou-se a partir do protocolo X-500, da ITU (International Telecommunication Union)

Comunicação segura

- Envolve sigilo, autenticação (máquina ou rede) e integridade da mensagem
  - Sujeito a quais tipos de ataques?
    - Sniffing (placa de rede em modo promíscuo), spoofing (falsificação IP), modificação
  - Autenticação
    - Procedimentos distintos (procedimentos simples envolvendo somente o acesso físico ao equipamento, ou mais complexos como timbre vocal, iris, impressão digital, DNA)

Comunicação segura

- Solução?
  - Através de criptografia
    - Permite o remetente disfarçar os dados de modo que um intruso não consiga obter informação com base nos dados interceptados.
    - Técnicas de codificação da mensagem são conhecidas, por isso tem um pedaço de informação secreta contida nas mensagens (as chaves)

Criptografia

- Dois tipos de chaves
  - Chaves simétricas (as chaves dos sistemas comunicantes são idênticas e secretas)
  - Chaves públicas (utiliza de um par de chaves, uma pública e outra privada)
- Chaves simétricas
  - Cifra de César (deslocamento no alfabeto por um índice k, e.g. (a letra a seria a letra d)), somente 25 valores possíveis de chaves

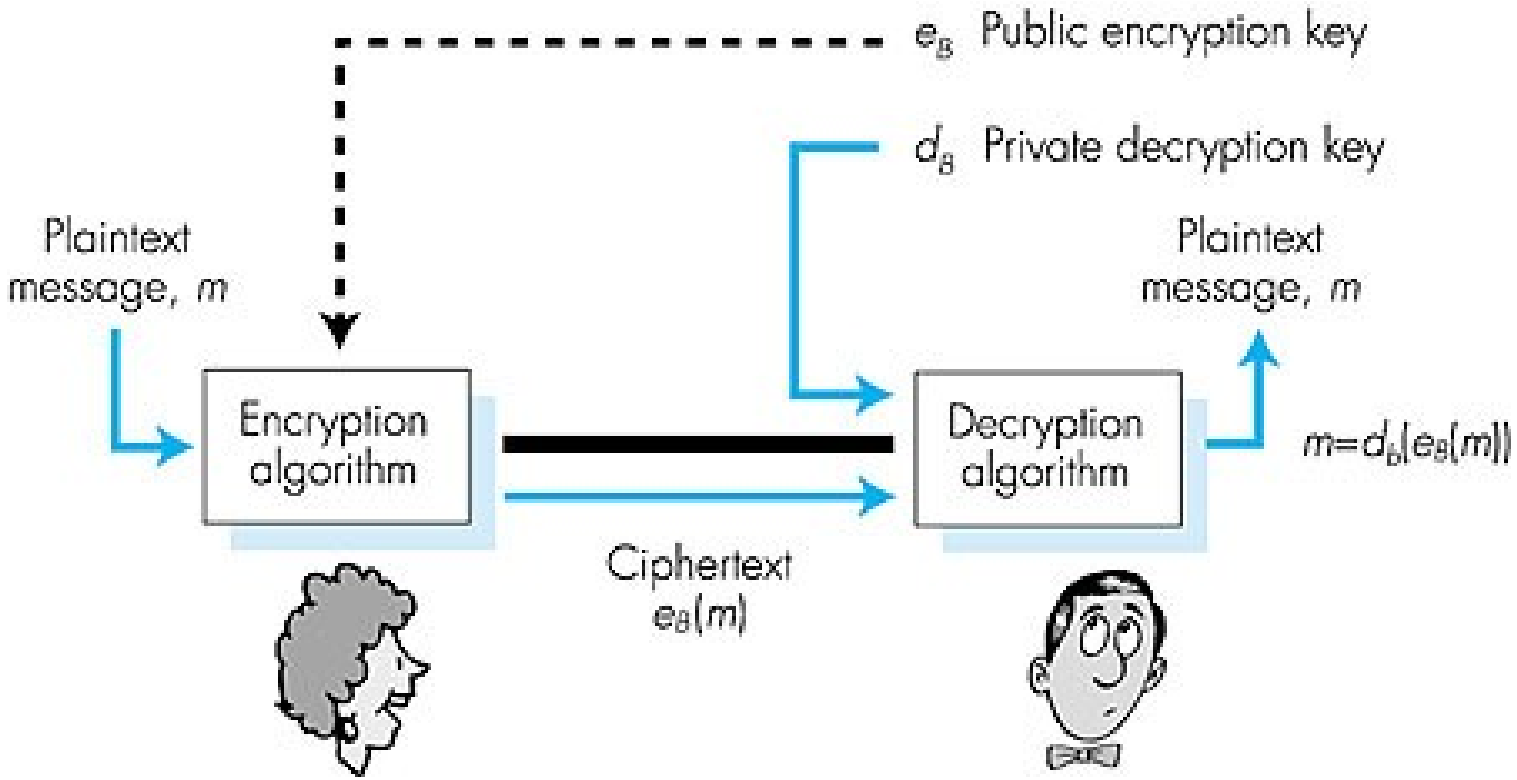
Criptografia

- Chaves simétricas
  - Cifra monoalfabética (qualquer letra pode ser substituída por qualquer outra)
  - Cifras polialfabéticas (Cifras de Vigenere), utilizam de múltiplas cifras monoalfabéticas
- Atualmente:
  - DES (Data Encryption Standard) e 3DES
  - Usa chave de 64 bits
  - 1997 (Uma equipe demorou quase 4 meses para quebrar uma mensagem, prêmio $ 10.000)
  - 1999 (menos de 22 horas em um computador que custa 250 mil dólares (“Deep Crack”)

Criptografia

- Chaves públicas (1976)
  - Dificuldade da chave simétrica?
    - Como entregar a chave com segurança
  - Utilizada não somente em criptografia, como autenticação e assinatura digital (será visto em slides posteriores)
  - Um dos algoritmos (RSA, nome dos autores)
  - Funcionamento?
  - Como autenticar o remetente da mensagem?
  - DES é 100x e entre 1000x a 10.000x mais rápido do que o RSA (software e hardware respectivamente)
  - Por isso na prática é usado em combinação com o DES (envio da chave DES através de criptografia RSA)

Criptografia por chaves públicas



Autenticação

- É o processo de provar a própria identidade, permitindo que o acesso lógico ao sistema seja habilitado para cada usuário.
- Baseada na posse (chave ou um cartão), conhecimento (um nome e uma senha), ou atributo (impressão digital, padrão de retina ou assinatura)

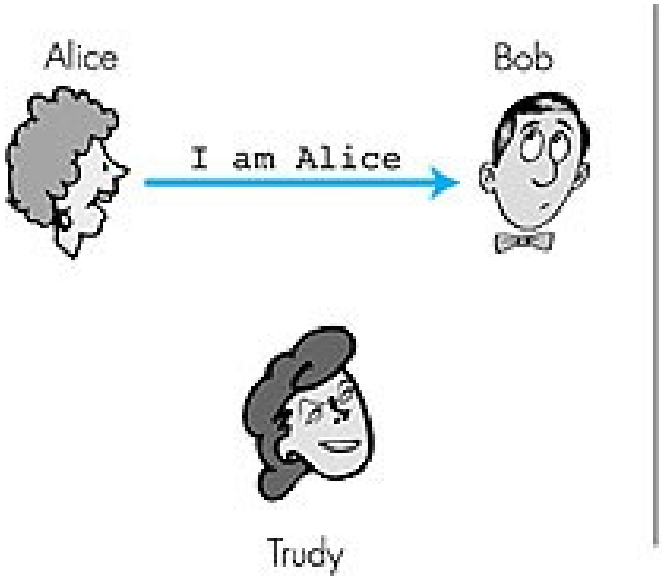
Autenticação

- Numa rede, as partes comunicantes não podem confiar em informações biométricas, a autenticação deve ser feita na base de mensagens e dados trocados como parte de um protocolo de autenticação
- O uso de senhas é extremamente comum, porque são fáceis de utilizar, porém tem vários problemas associados
  - Um outro usuário com a senha
    - Por descuido, por senhas fracas ou por força bruta
    - Por escuta da rede (sniffing), obtendo a senha

Autenticação

- Métodos preventivos:
  - O sistema pode gerar senhas (difícil para o usuário lembrar, ao contrário de senhas que o usuário cria que geralmente são fracas) ou alertar que a senha é fraca
  - Podem exigir troca de senha a cada período de tempo
  - Qual seria uma boa técnica para geração de senha?
- UNIX grava senhas criptografadas em um arquivo (força bruta poderia comparar estas senhas e descobrir alguma senha)

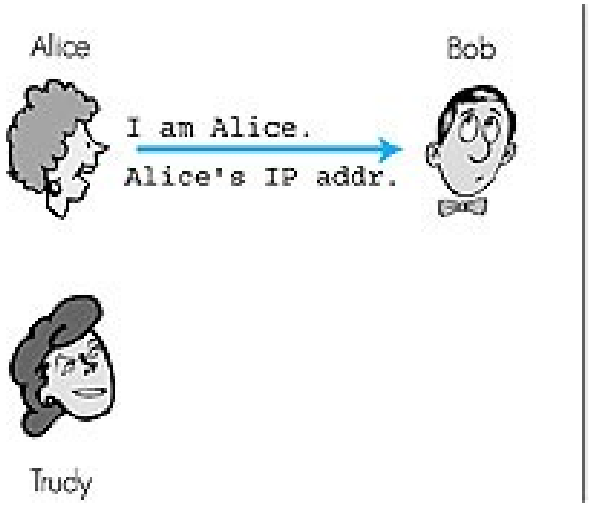
Autenticação de rede (Cenários)



Falha?

Trudy pode passar-se como se fosse a Alice

Autenticação de rede (Cenários)



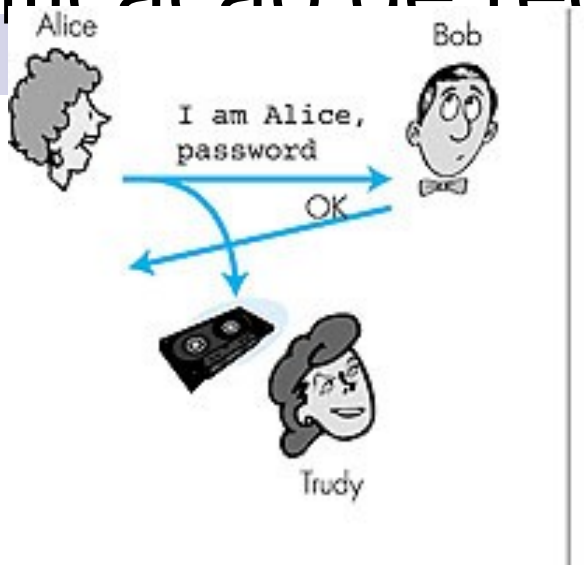
Falha?

Trudy poderia usar a técnica de spoofing para dizer que seu IP é igual o IP do computador de Alice

Solução?

Roteadores poderia verificar isso e não repassar IP falsificado

Autenticação de rede (Cenários)



Esquemas de autenticação (senha) são usados em HTTP, FTP e Telnet. Falha?

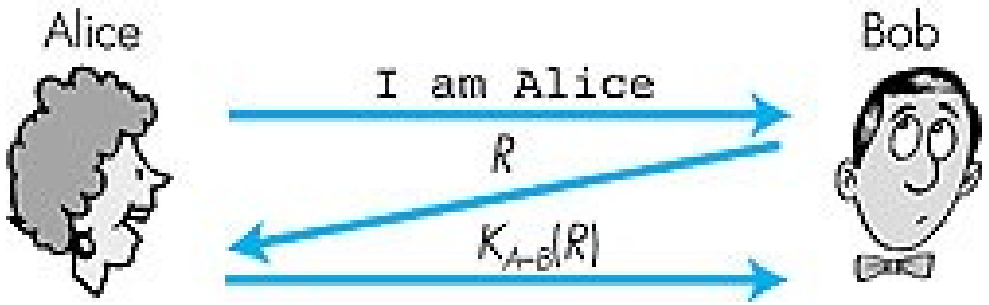
Trudy poderia usar a técnica de sniffing para capturar a senha de Alice

Solução?

Usar criptografia?

Não garante autenticação, porque Trudy poderia passar a senha criptografada e se passar por Alice

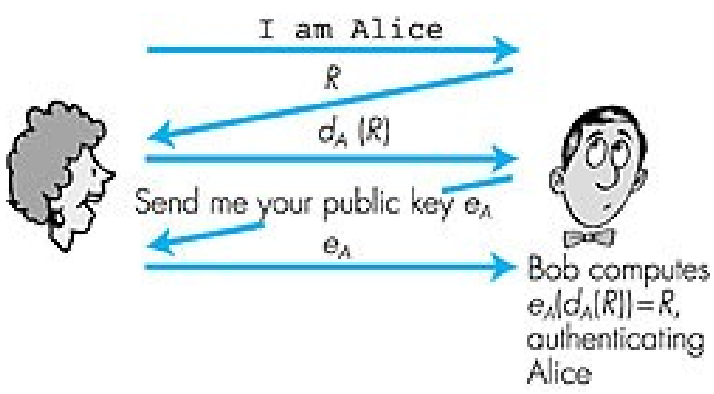
Autenticação de rede (Cenários)

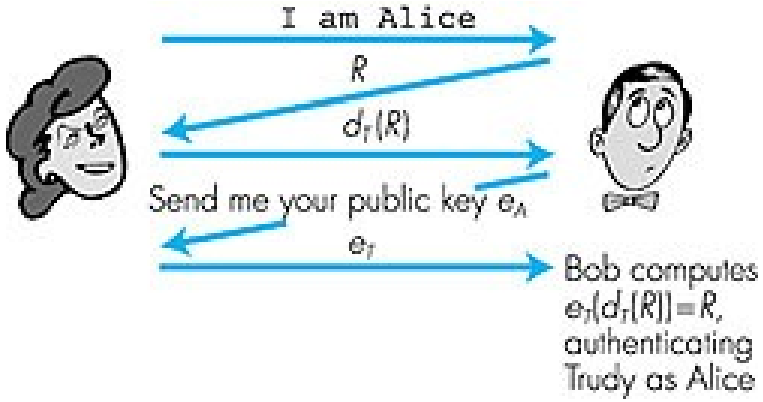


Bob envia um número (cada vez é diferente), Alice codifica este número R (chave simétrica) e envia a Bob, Bob decodifica e autentica a Alice usando a chave secreta

Não há cenário de falha

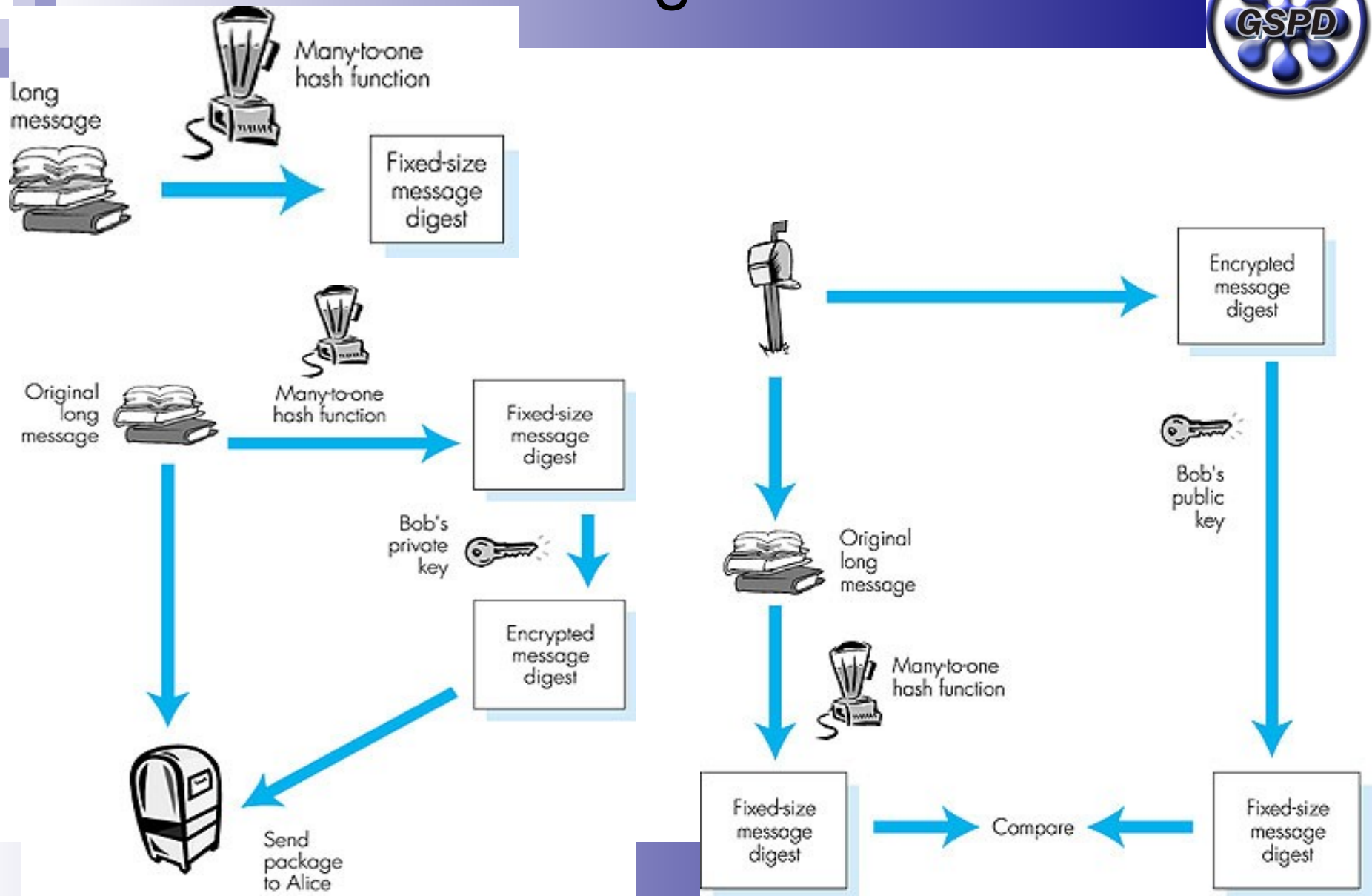
Autenticação de rede(Cenários)





E se fosse usar o esquema de chave pública?
R. Poderia ocorrer o caso de Trudy interceptar as mensagens que iam para Alice e se autenticar-se como se fosse Alice
Solução?
Distribuição segura das chaves públicas

Resumo de mensagem



Exemplo (E-mail seguro)

- Características para um e-mail seguro ?
  - Sigilo, autenticação do remetente, integridade da mensagem
- O que fazer para obter sigilo?
  - Para sigilo pode-se usar chaves simétricas (problema na distribuição), por isso uso de chaves públicas (ineficiência para mensagens longas)
  - Com isso uso de chave de sessão (criptografa uma chave simétrica com a chave pública)

Exemplo (E-mail seguro)

- O que fazer para autenticação do remetente e garantir a integridade da mensagem?
  - Assinaturas digitais e resumos de mensagem
  - Único problema é o fato de uma pessoa intervir na distribuição das chaves
- PGP
  - Em essência garante sigilo, autenticação do remetente e integridade da mensagem. Utiliza 3DES ou Idea para chaves simétricas, RSA para chaves públicas, MD5 ou SHA para resumos e oferece compressão de dados

Monitoramento de ameaças

- Deve analisar suspeitos padrões de atividade, por exemplo, tentativas mal sucedidas de autenticação (ataque por força bruta)
- Auditoria – gravar os horários, usuários e todos tipos de acesso aos objetos, útil para verificação e tomadas de melhores medidas de segurança
- Varrer o sistema periodicamente para encontrar buracos na segurança

Monitoramento de ameaças

- Verificar:
  - Senhas curtas ou fracas
  - Programas não autorizados em diretórios do sistema
  - Processo executando a muito tempo
  - Proteções impróprias de diretórios ou dados do sistema
  - Mudanças nos programas do sistema: monitorar valores de checksum

Firewall e IDS

- Firewall
  - Um firewall é colocado entre hosts confiáveis e hosts não confiáveis
  - Tem o papel de restringir o acesso a rede entre estes dois domínios de segurança

- Detecção de intrusos (IDS)
  - Tem o papel de detectar tentativas de intrusão
  - Métodos: através de auditoria e registros (logs)
  - Ex. Tripwire (verifica a alteração de arquivos e diretórios)
  - Monitoramento de chamadas de sistema