

Segurança em Redes Privadas

Redes Geograficamente Distribuídas

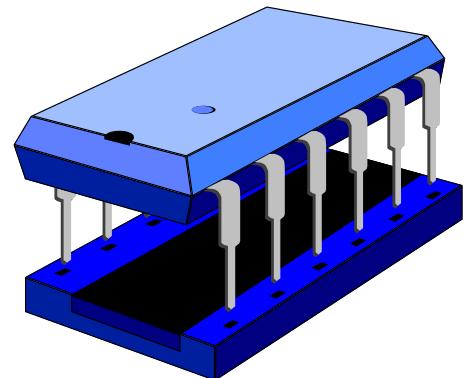


Segurança em Redes Privadas

Representação Física dos Dados

Primeira situação:

Dispositivos de armazenamento primário ou secundário, o que inclui a memória, unidades de disco rígido, unidades de disco óptico, unidades de fita, dentre outros componentes dos servidores e estações de trabalho.



Segunda situação:

Em trânsito pelo canal de comunicação, na forma de pacotes.

Segurança em Redes Privadas

Dados Transitando pela Rede

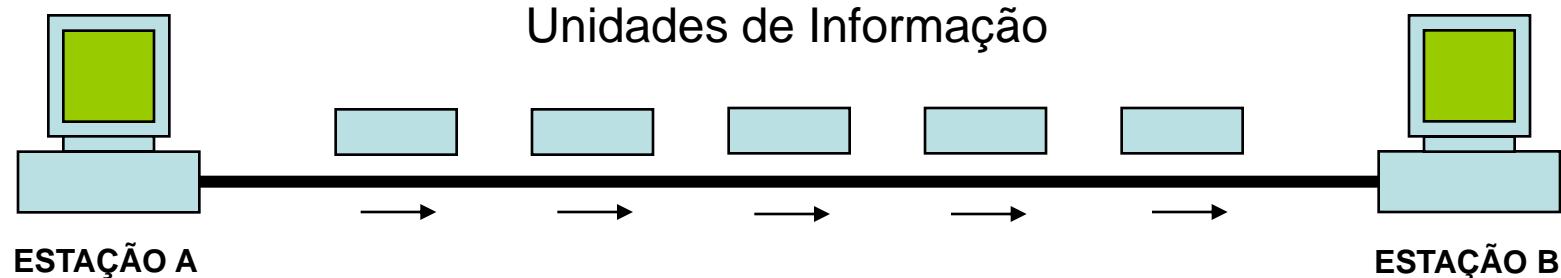
Pacotes de Rede (Encapsulamento)

Cabeçalho

Área de Dados

ID

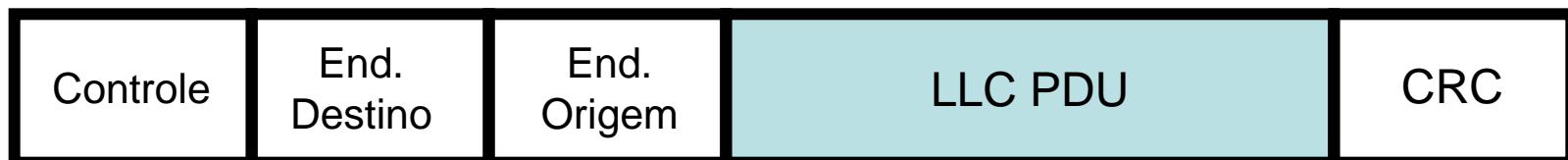
Dados do Usuário (Unidade)



Segurança em Redes Privadas

Pacote de Rede x Quadro Físico (IEEE 802.3)

Formato Genérico do Quadro Físico – MAC PDU
("Medium Access Control" – Controle de Acesso ao Meio Físico)



Formato Genérico da Unidade de Dados do LLC – LLC PDU
("Logical Link Control" – Controle de Enlace Lógico)



Observação: SAP ("Service Access Point" – Ponto de Acesso a Serviço)

Segurança em Redes Privadas

Invasão Passiva x Invasão Ativa

Na **Invasão Passiva** o agente monitora os dados de uma transmissão em andamento, sem emitir nenhum sinal eletrônico que possa revelar sua ação; este tipo de técnica é chamado de **SIGINT**.

Na **Invasão Ativa** o agente ataca a rede com o objetivo de violar os dados, muitas vezes criando um rastro que pode ser identificado pelos administradores do sistema que está sendo invadido; este tipo de técnica é chamado de **ELINT**.

Segurança em Redes Privadas

Técnicas de Invasão SIGINT Mais Usuais

**Sondagem de Pacotes de Rede
("Network Packet Sniffers")**

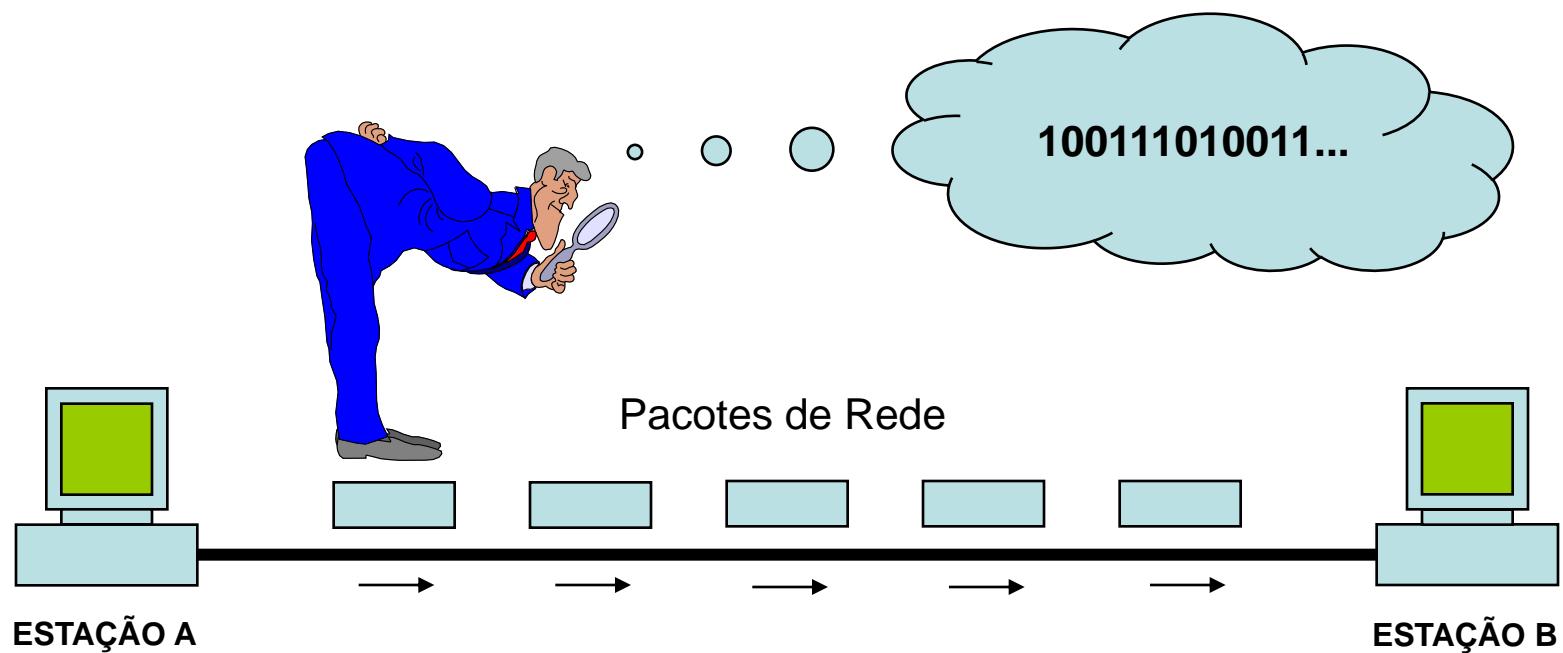
**Distribuição de Dados Sensíveis entre Fontes Externas
("Distribution of Sensitive Internal Information to External Sources")**

**Sondagem em Pontos de Interconexão Intermediários
("Man-in-the-Middle Attacks")**

Segurança em Redes Privadas

Sondagem de Pacotes de Rede ("Network Packet Sniffers")

O Farejador ("Sniffer") intercepta os pacotes de rede que são transmitidos através do canal, para analisar seu conteúdo

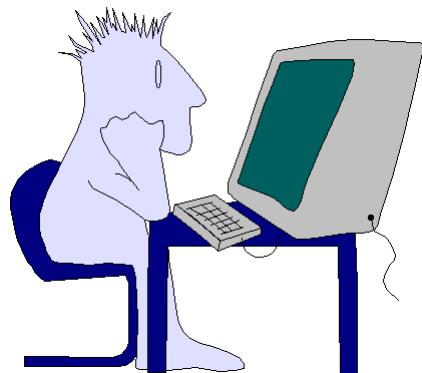


Segurança em Redes Privadas

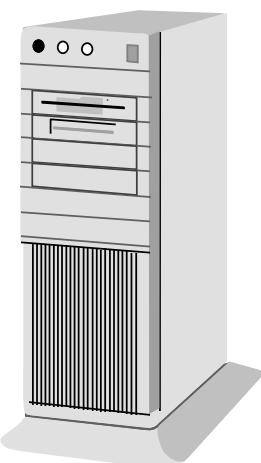
Distribuição de Dados Sensíveis entre Fontes Externas
("Distribution of Sensitive Internal Information to External Sources")

Uma boa política restringe de forma adequada o acesso à informação e os meios de transmiti-la dentro ou fora da rede privada, para evitar uma situação comprometedora

Usuário da Rede



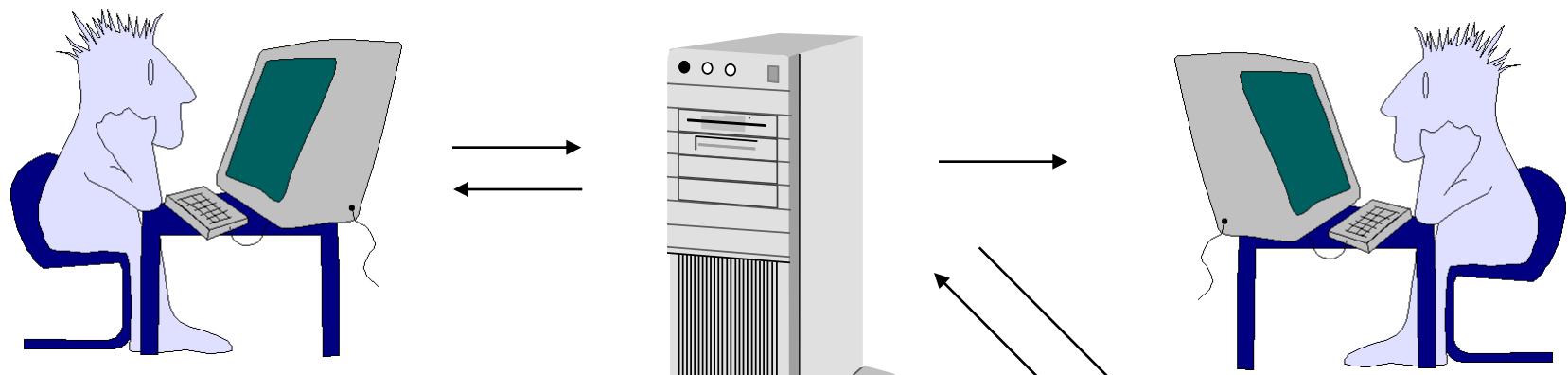
Pessoa não autorizada



Servidor FTP Externo

Segurança em Redes Privadas

Sondagem em Pontos de Interconexão Intermediários
("Man-in-the-Middle Attacks")



Para efetuar este tipo de ataque, o invasor deve atuar em um ponto intermediário entre o usuário que está acessando os recursos e a rede externa, como por exemplo o funcionário que trabalha no provedor de acesso à Internet

Segurança em Redes Privadas

Técnicas de Invasão ELINT Mais Usuais

Burla de Endereço IP (“IP Spoofing”)

Ataques sobre Senhas (“Password Attacks”)

Ataques a Nível de Aplicação (“Application Layer Attacks”)

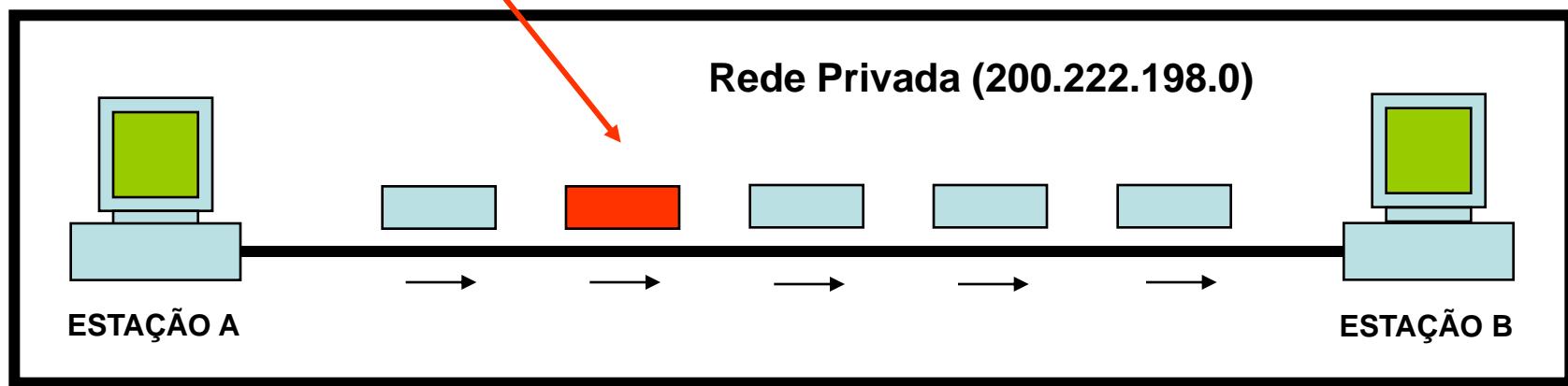
Negação de Serviço (“Denial-of-Service Attacks”)

Segurança em Redes Privadas

Burla de Endereço IP



O endereço IP de origem é substituído, nos pacotes de rede enviados pelo invasor, por um que esteja dentro da faixa de endereços alocados para a rede que está sendo violada

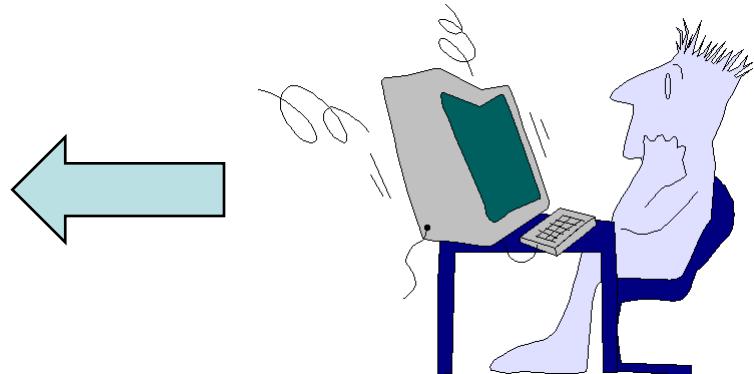


Segurança em Redes Privadas

Ataques sobre Senhas ("Password Attacks")

Neste tipo de ataque o invasor, valendo-se de programas específicos que operam a partir da técnica de tentativa-e-erro sucessivas vezes, procura identificar a senha e/ou o nome de usuário de pessoas com autorização para acessar os recursos da rede privada

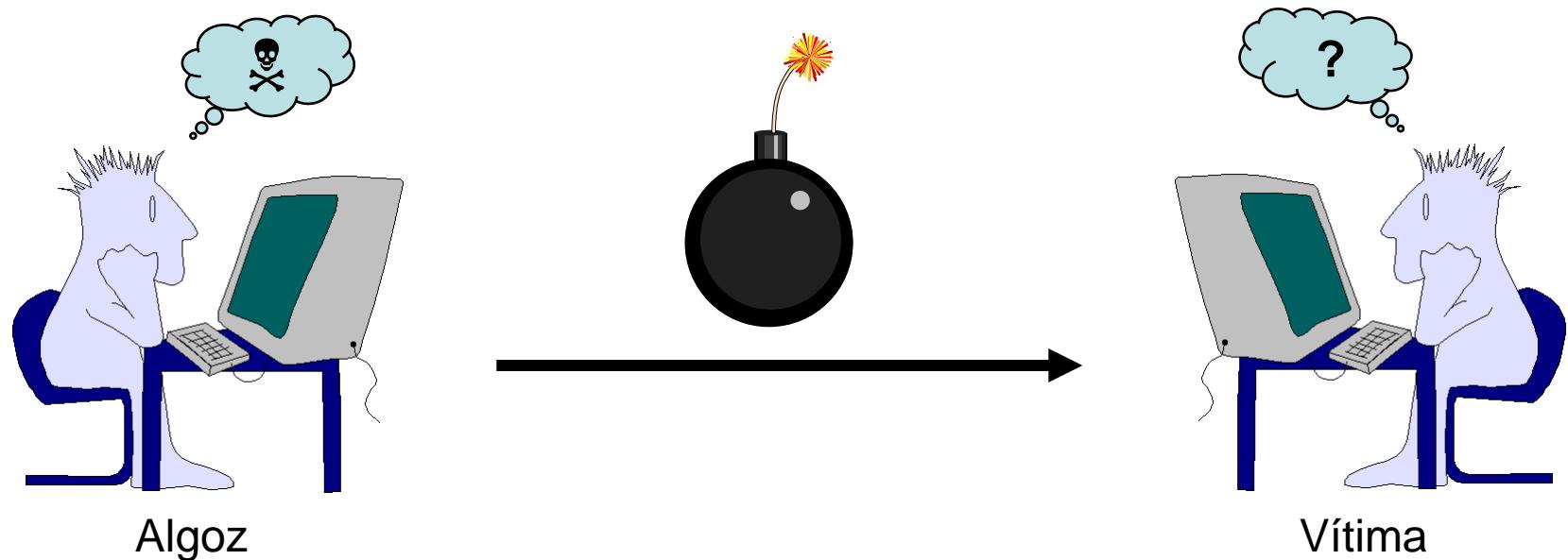
AABBAAYYOOOLMKJ
CJKDKLLSKLKLXCK
KCLXKCLZOSDOIOI
XLCKXLKCLKOOIOK



Segurança em Redes Privadas

Ataques a Nível de Aplicação ("Application Layer Attacks")

O invasor pode escrever programas maliciosos, como cavalos de tróia e vírus eletrônicos, com o objetivo de sabotar o sistema da vítima, ou ainda para obter dados confidenciais de forma ilícita



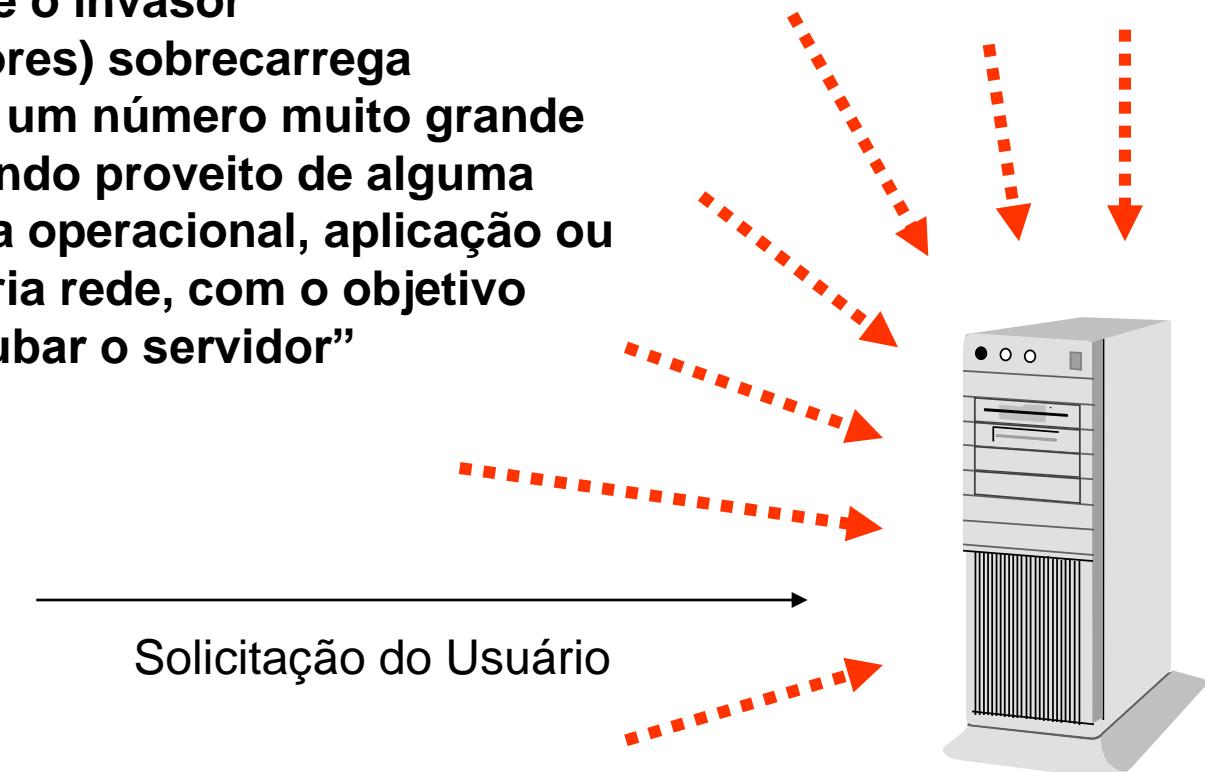
Segurança em Redes Privadas

Negação de serviço ("Denial-of-Service Attacks")

Neste tipo de ataque o invasor (ou grupo de invasores) sobrecarrega o sistema-alvo com um número muito grande de solicitações, tirando proveito de alguma restrição do sistema operacional, aplicação ou até mesmo da própria rede, com o objetivo específico de “derrubar o servidor”



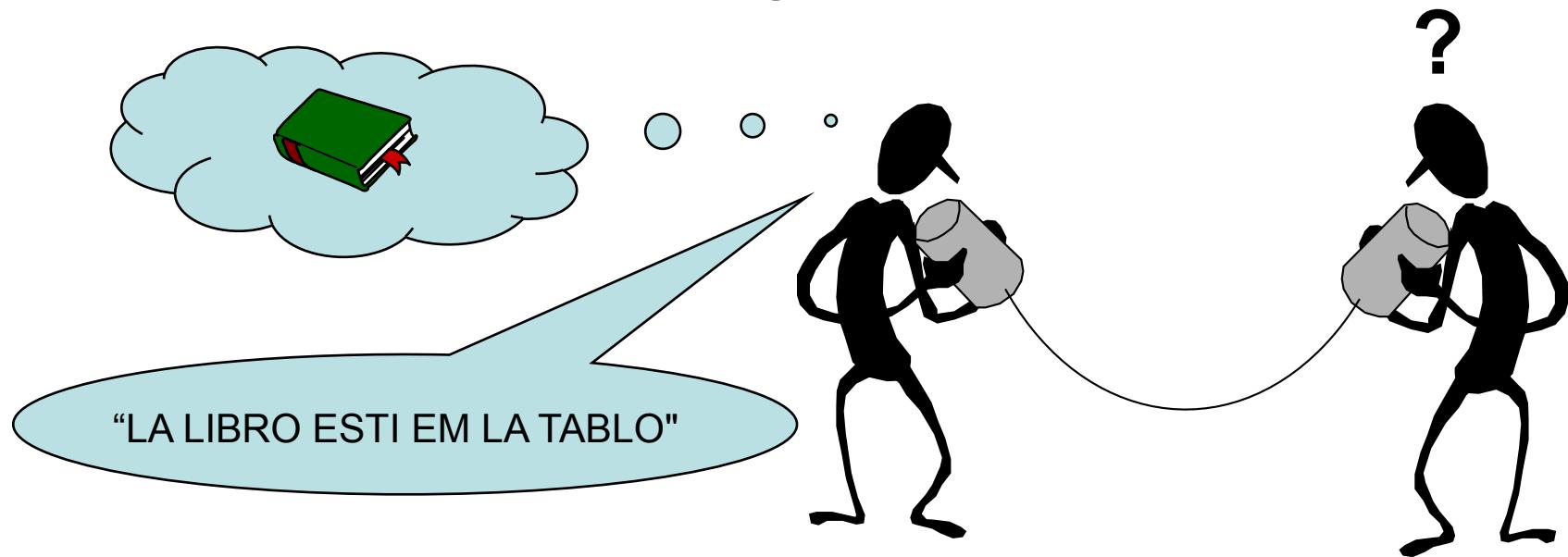
Solicitação do Usuário



Segurança em Redes Privadas

Sistema de Comunicação - Conceito

Um sistema de comunicação estabelece mecanismos para a troca de informações; entretanto, vale lembrar que o emissor e o receptor devem adotar o mesmo código (padrão), para que possam interpretar a mensagem de forma correta.



Segurança em Redes Privadas

Sistema de Comunicação - Elementos

São elementos genéricos de um sistema de comunicação:

- Emissor - Aquele que transmite a informação
- Mensagem - A própria informação, ou seja, uma coleção de dados
- Código - Padrão adotado para a correta interpretação da mensagem
- Canal - Meio físico para a transmissão da mensagem
- Receptor - Aquele que recebe a informação

Segurança em Redes Privadas

Sistema de Comunicação Redes de Computadores

Analogamente, podemos identificar os cinco elementos de comunicação em uma rede de computadores:

- Emissor - Estação de trabalho transmitindo os dados
- Mensagem - Padrão binário codificado pelo emissor
- Código - **Protocolo de comunicação** (estabelece as regras)
- Canal - Barramento e elementos intermediários de conexão
- Receptor - Estação de trabalho recebendo os dados

Segurança em Redes Privadas

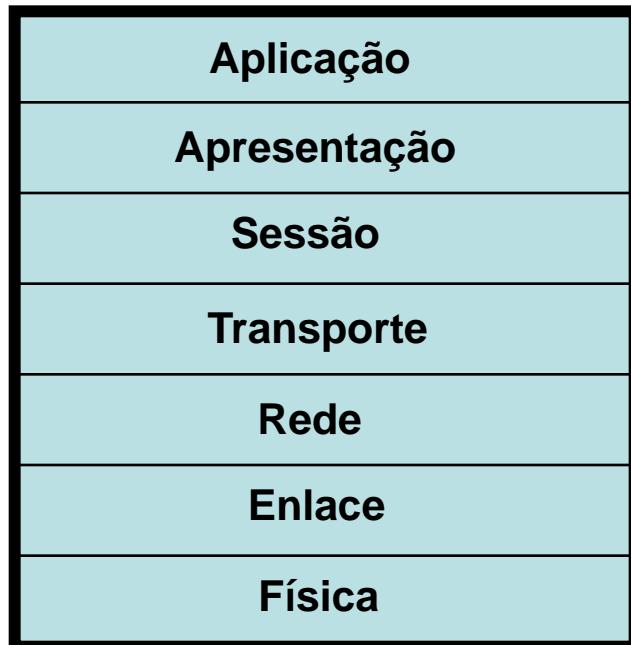
Sistema de Comunicação Protocolo de Comunicação

Pela definição, percebe-se que o protocolo é responsável pelas diretrizes básicas de comunicação, exercendo papel equivalente ao da língua para as pessoas; analogamente, como não é possível estabelecer um diálogo entre duas pessoas que não falam o mesmo idioma, também não é possível intercambiar dados entre computadores que utilizam protocolos diferentes. Logo, em uma mesma rede de computadores, todos os nós devem adotar o mesmo protocolo, isto é, empregar regras de comunicação equivalentes. O TCP/IP existe para permitir que não só os computadores (identificados pelo termo “hospedeiro”) de uma mesma rede possam comunicar-se, como também para tornar possível a comunicação inter-redes, ou seja, para viabilizar que computadores de redes distintas também consigam fazê-lo.

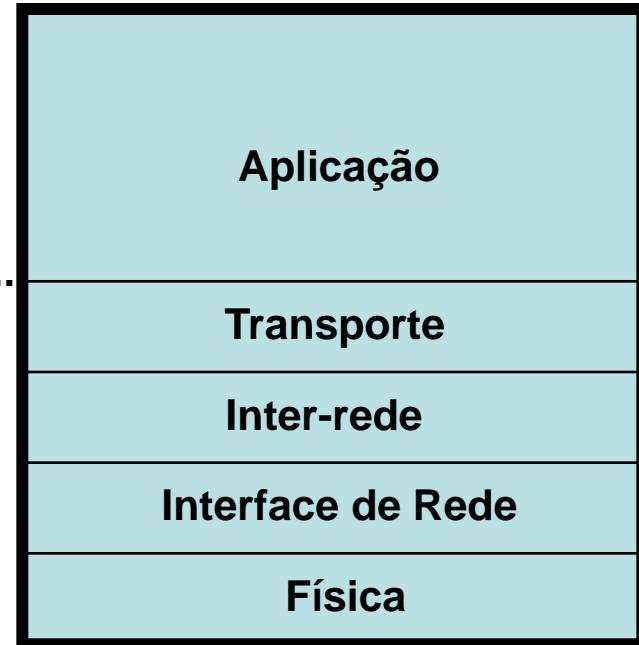
Segurança em Redes Privadas

Sistema de Comunicação
“Dividir para Conquistar”

Modelo ISO/OSI



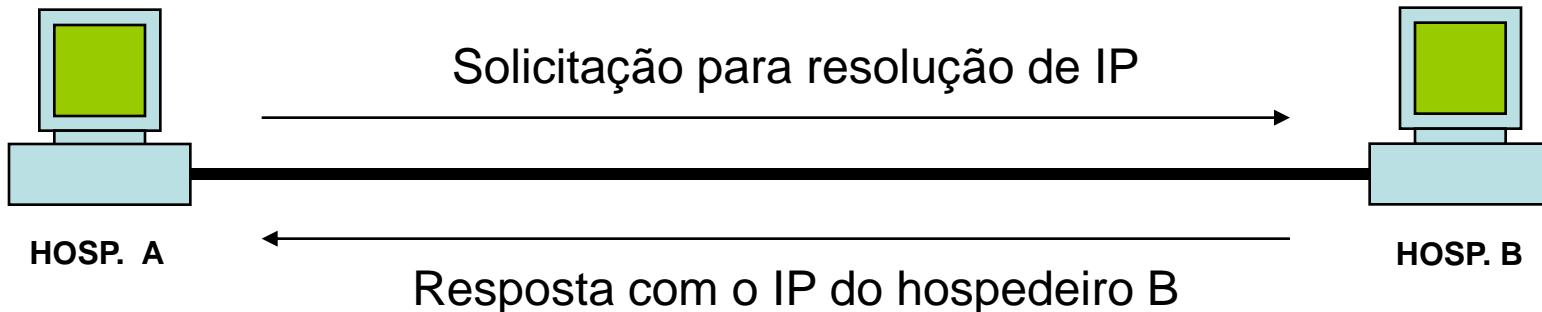
Modelo TCP/IP



Segurança em Redes Privadas

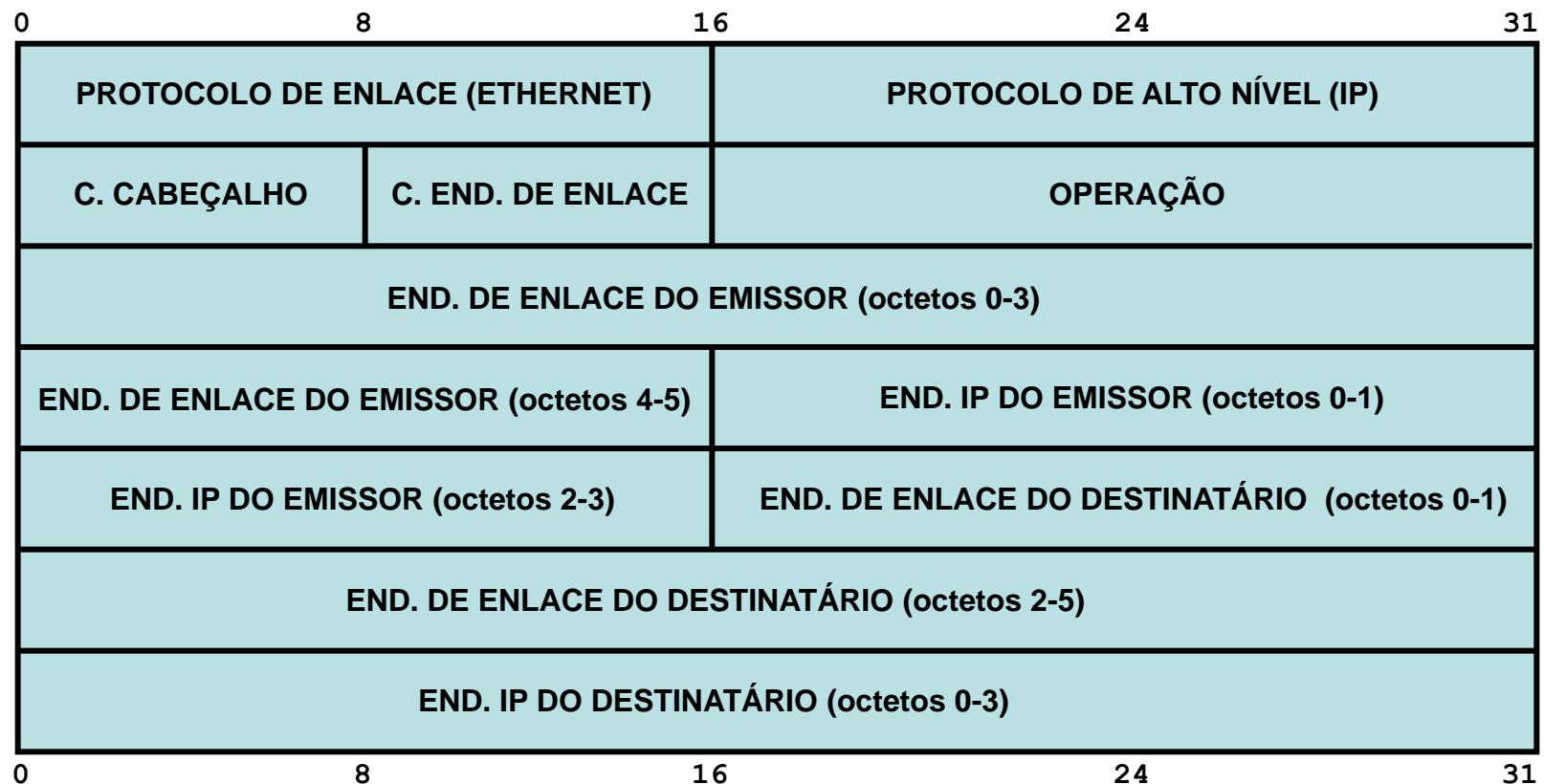
TCP/IP - Camada de Interface de Rede [nível 2]

Protocolos ARP e RARP
“Address Resolution Protocol”
(Protocolo para a Resolução de Endereços)
RARP - “Reverse Address Resolution Protocol”
Protocolo Reverso para a Resolução de Endereços



Segurança em Redes Privadas

TCP/IP - Formato dos Quadros ARP/RARP



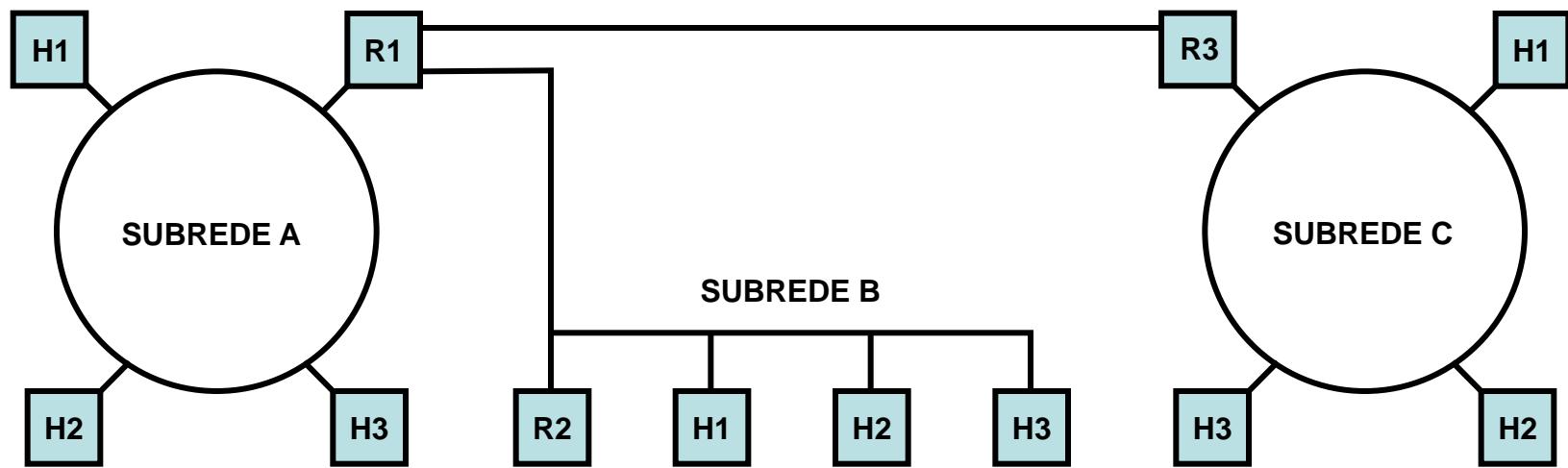
Segurança em Redes Privadas

TCP/IP - Camada de Inter-Rede [nível 3]

Protocolos IP e ICMP

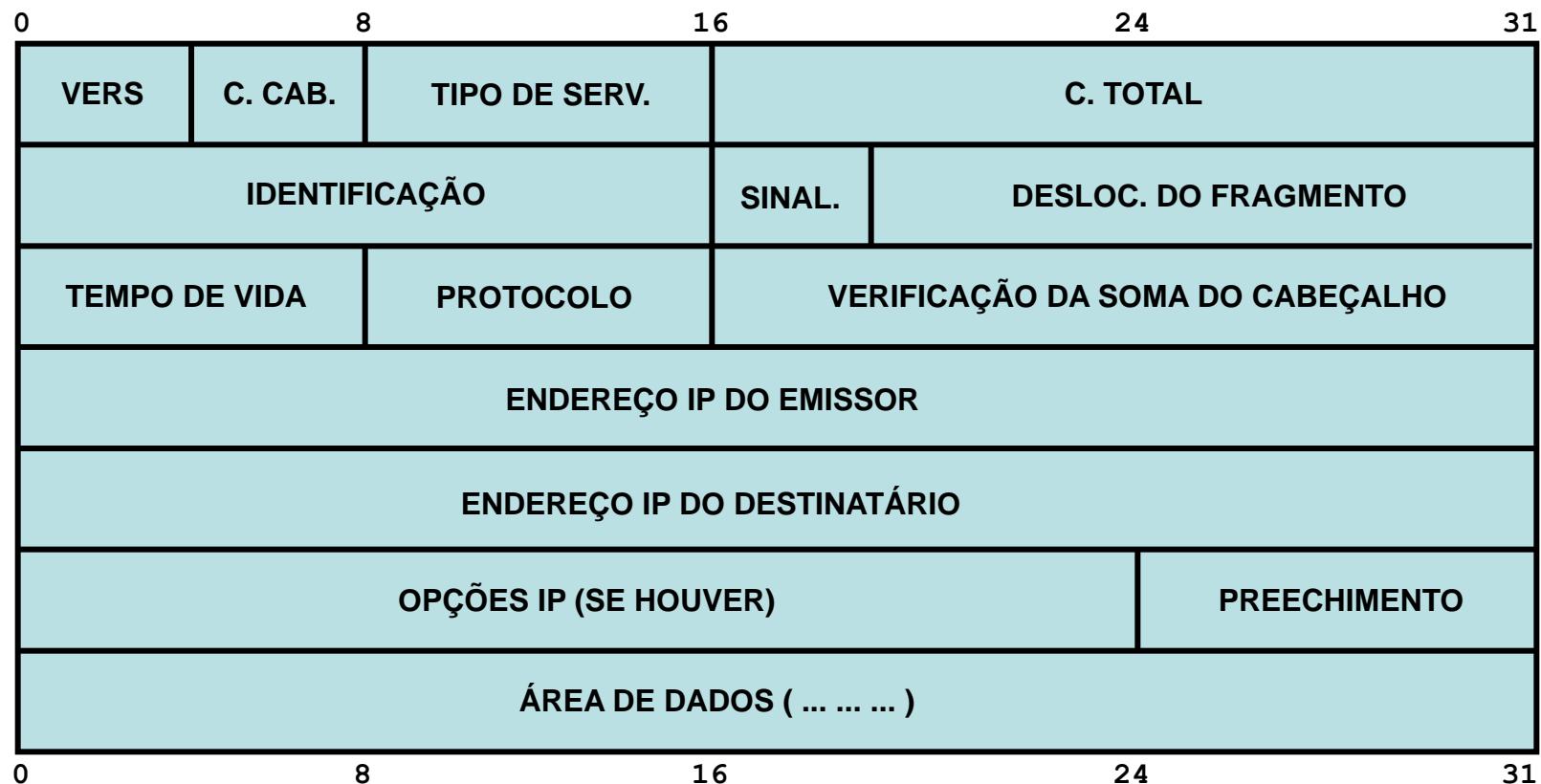
"Internet Protocol" (Protocolo de Inter-Rede)

Observação: O ICMP é parte da implementação do IP - Internet Control Message Protocol
(Protocolo Inter-Rede para Mensagens de Controle)



Segurança em Redes Privadas

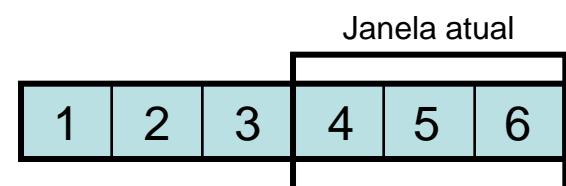
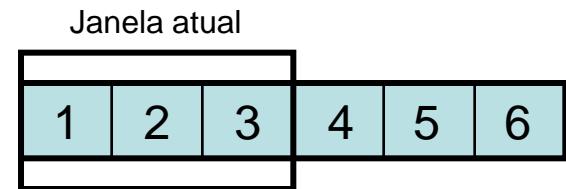
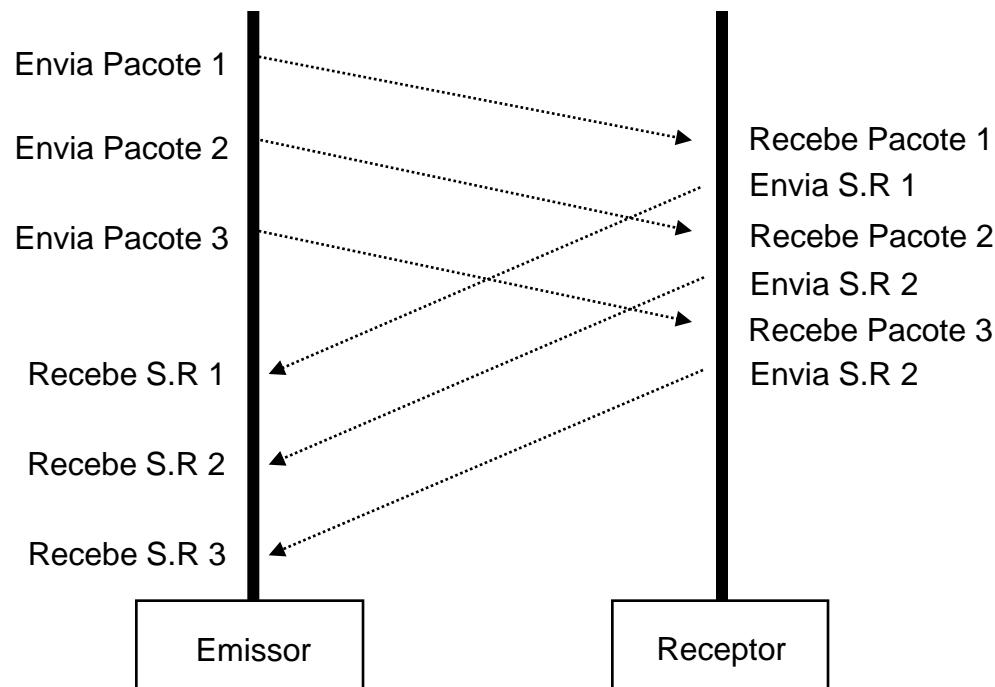
TCP/IP - Formato do Datagrama IP



Segurança em Redes Privadas

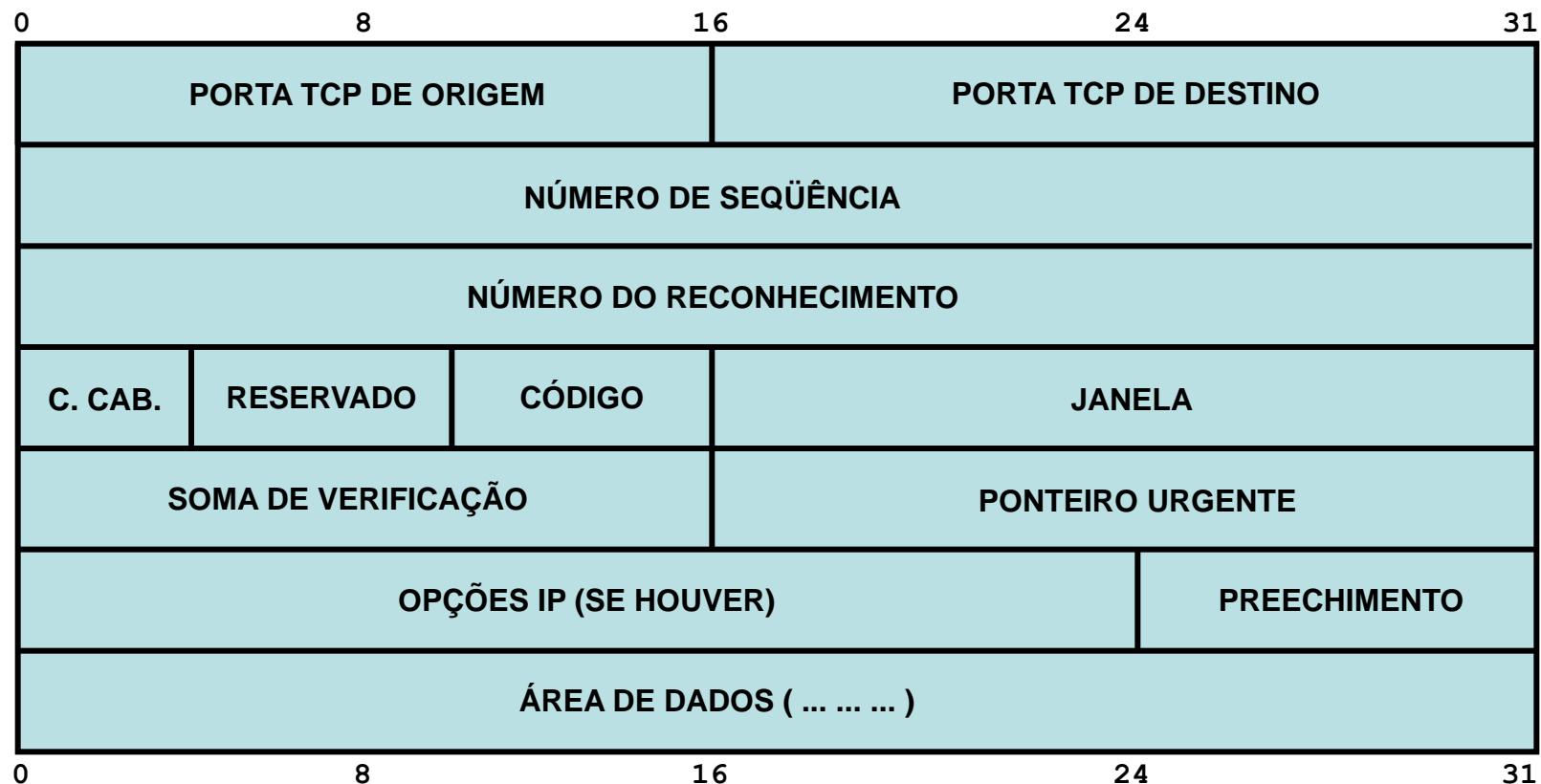
TCP/IP - Camada de Transporte [nível 4]

Protocolo de Janela Deslizante



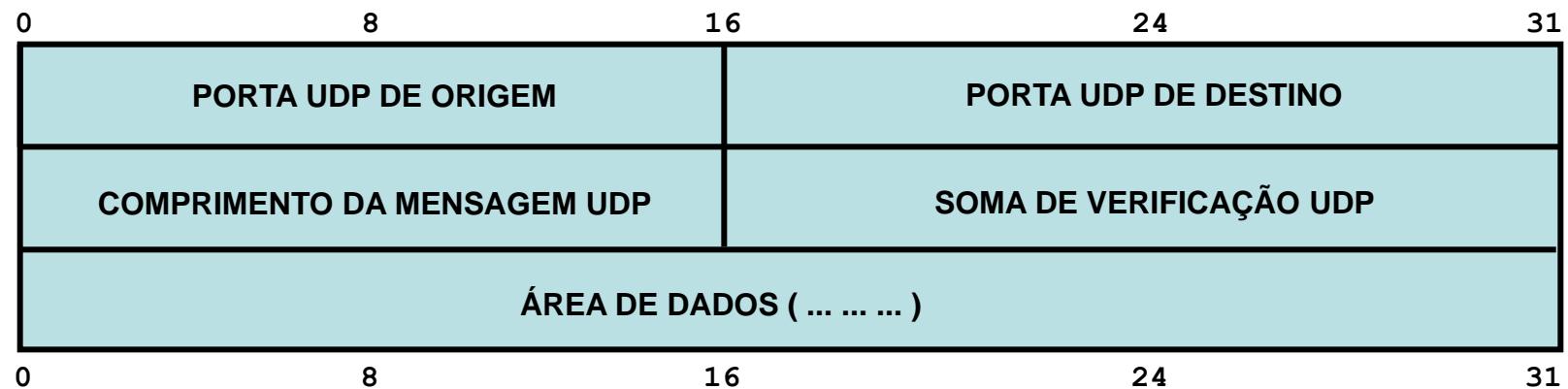
Segurança em Redes Privadas

TCP/IP - Formato do Datagrama TCP



Segurança em Redes Privadas

TCP/IP - Formato do Datagrama UDP



Segurança em Redes Privadas

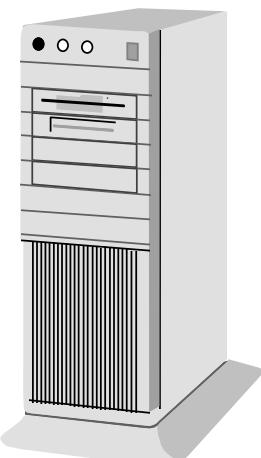
TCP/IP - Camada de Aplicação [nível 5]

A camada de Aplicação segue o modelo cliente-sevidor

Usuário remete a mensagem eletrônica usando o cliente SMTP



Servidor SMTP x Servidor POP



Usuário recebe a mensagem eletrônica usando o cliente POP



Segurança em Redes Privadas

TCP/IP - Exemplos de Aplicações (TCP/UDP)

Aplicações TCP conhecidas:

- porta 07 - ECHO
- porta 11 - USERS
- porta 13 - DAYTIME
- porta 20 - FTP DATA
- porta 21 - FTP
- porta 23 - TELNET
- porta 25 - SMTP
- porta 37 - TIME
- porta 42 - NAMESERVER
- porta 53 - DOMAIN

Aplicações UDP conhecidas:

- porta 07 - ECHO
- porta 11 - USERS
- porta 13 - DAYTIME
- porta 37 - TIME
- porta 42 - NAMESERVER
- porta 43 - NICNAME
- porta 53 - DOMAIN
- porta 67 - BOOTPS
- porta 68 - BOOTPC
- porta 69 - TFP

Segurança em Redes Privadas

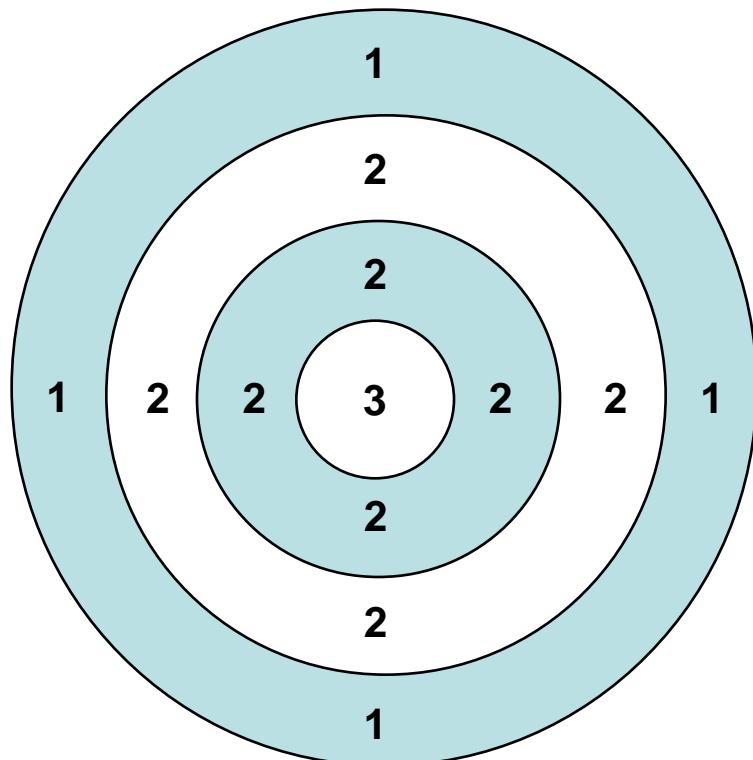
Sistemas de Parede Corta-Fogo (SPCF)

A comunicação entre o hospedeiro H1, da subrede A, e o hospedeiro H2, da subrede B, é intermediada pelo sistema de parede corta-fogo (os roteadores podem fazer parte da implementação)



Segurança em Redes Privadas

Sistemas de Parede Corta-Fogo Perímetros de Segurança



- (1) Perímetro de rede mais externo
- (2) Perímetros intermediários (n)
- (3) Perímetro de rede mais interno

INTERNET GLOBAL

Segurança em Redes Privadas

Sistemas de Parede Corta-Fogo

Designação dos Perímetros de Segurança

Segmentos do Perímetro de Segurança		
Posicionamento	Designação	Descrição
Perímetro de rede mais interno	Confiável	Aloca os recursos que demandam maior segurança
Perímetros intermediários	Confiável	Estabelece níveis internos de segurança
Perímetro de rede mais externo	Confiável (sob ataques)	Segmento entre o roteador mais externo e o sistema de parede corta-fogo
Redes externas identificadas	Não-confiável	Acesso restrito aos recursos internos para usuários autorizados
Redes externas não-identificadas	Desconhecida	O sistema não reconhece

Segurança em Redes Privadas

Sistemas de Parede Corta-Fogo

Tecnologias Existentes

Segurança x Performance

Duas questões principais devem ser analisadas ao se escolher uma estratégia de implementação a partir dos sistemas de parede corta-fogo existentes: **segurança e desempenho**. Um nível de segurança mais acentuado compromete o desempenho geral, visto que os pacotes trafegam até as camadas superiores da pilha de rede, onde serão inspecionados com mais critério. Logo, os sistemas de parede corta-fogo que atuam a nível de aplicação são considerados mais seguros do que as demais tecnologias; porém, em contrapartida, esta arquitetura é também a de operação mais lenta, efetuando um número de verificações bem superior.

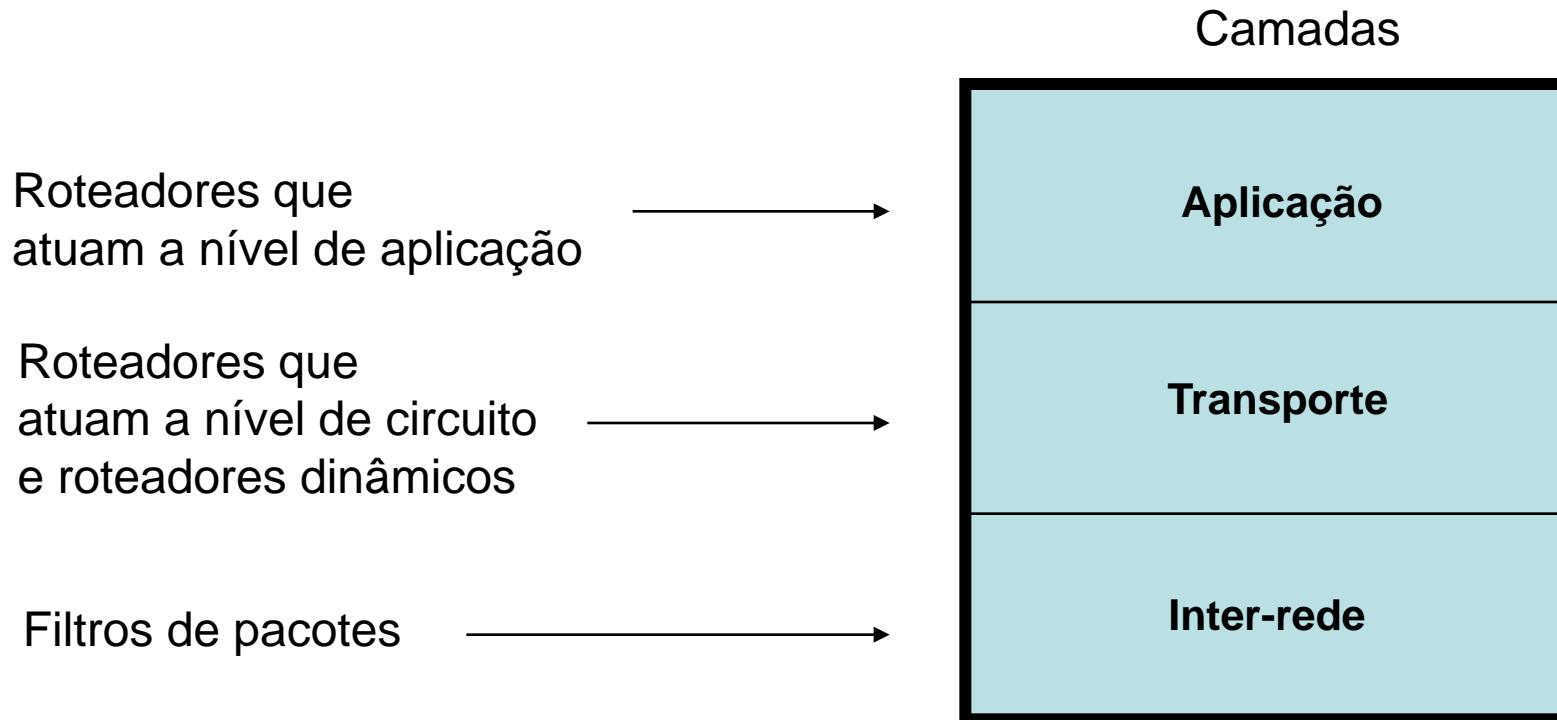
Segurança em Redes Privadas

Sistemas de Parede Corta-Fogo Tecnologias Existentes Mais Difundidas

- **Primeira Geração (1988) - Filtros de pacotes (roteadores)**
Jeff Mogul (Digital Equipments)
- **Segunda Geração (1989-1990) - SPCF que atuam a nível de circuito**
Dave Presotto e Howard Trickey (Laboratórios Bell - AT&T)
- **Terceira Geração (1990-1991) - SPCF que atuam a nível de aplicação**
Marcus Ranum (Digital Equipments)
Bill Cheswick (Laboratórios Bell - AT&T)
Gene Spafford (Universidade de Purdue)
- **Quarta Geração (1992) - SPCF dinâmicos**
Bob Braden e Annette DeSchon ...
(Instituto de Ciências da Informação da USC)
Bill Cheswick e Steve Bellovin (Laboratórios Bell - AT&T)

Segurança em Redes Privadas

Sistemas de Parede Corta-Fogo Tecnologias & Camadas Correspondentes



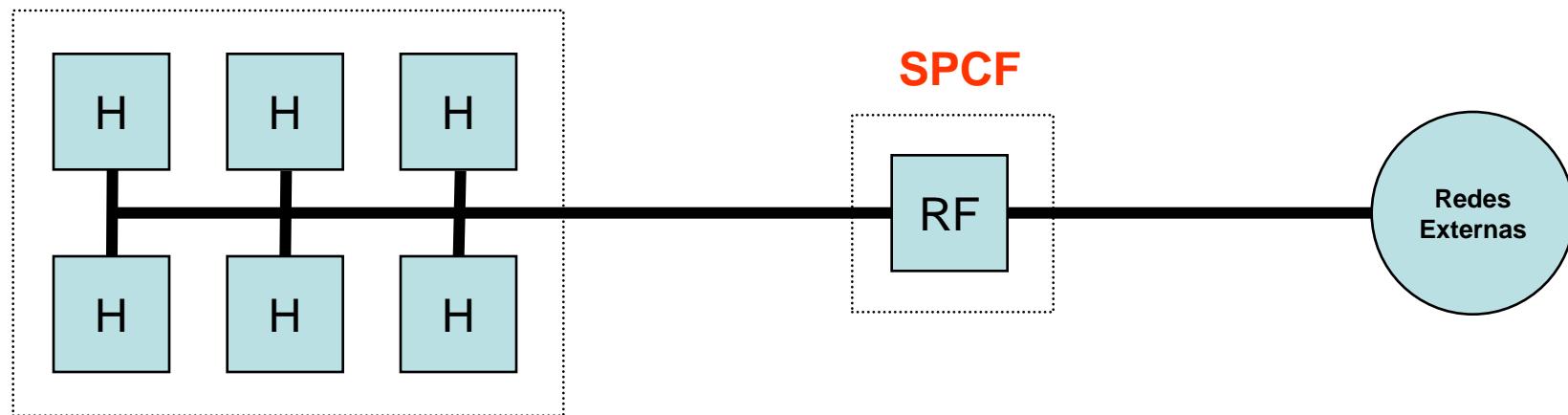
Segurança em Redes Privadas

Sistemas de Parede Corta-Fogo

Projetos (01)

Hospedeiro com Dupla-Conexão

(PI)



PI - Perímetro Interno || H - Hospedeiro || RF - Roteador Fiscalizador

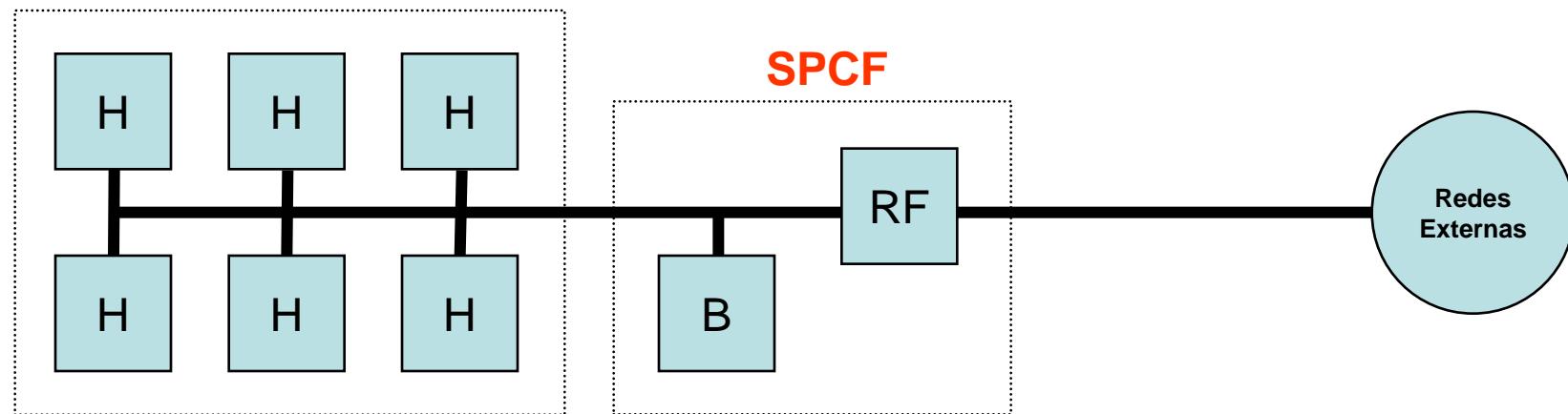
Segurança em Redes Privadas

Sistemas de Parede Corta-Fogo

Projetos (02)

Sistema Baseado em Bastião Protetor (Procurador)

(PI)



PI - Perímetro Interno || H - Hospedeiro || B - Bastião || RF - Roteador Fiscalizador

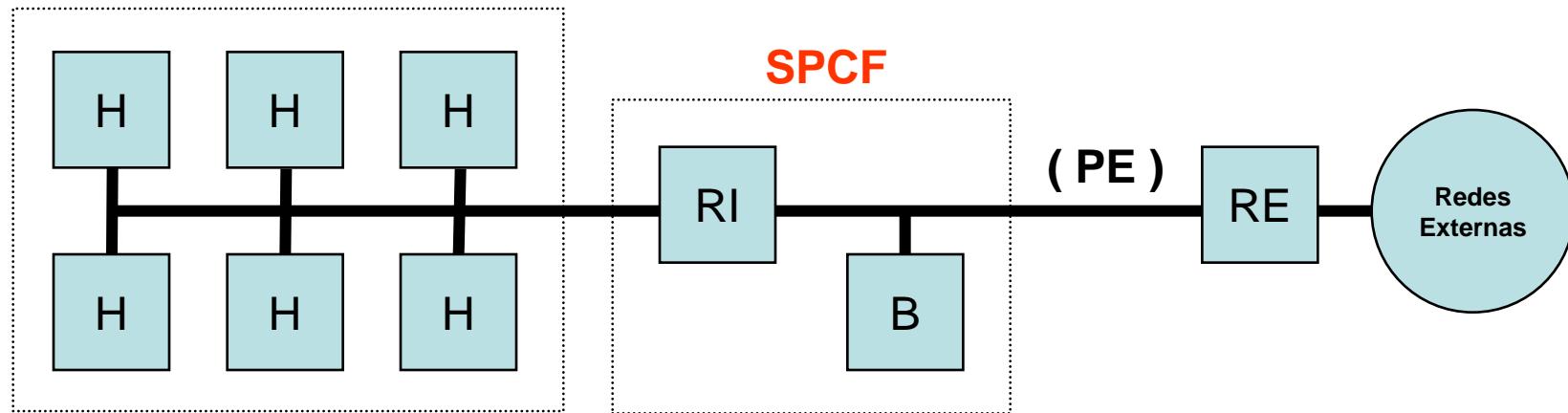
Segurança em Redes Privadas

Sistemas de Parede Corta-Fogo

Projetos (03)

Sub-Rede Protegida - Projeto Genérico

(PI)



PI - Perímetro Interno || H - Hospedeiro || RF - Roteador Fiscalizador || B - Bastião || PE - Perímetro Externo || RE - Roteador Externo

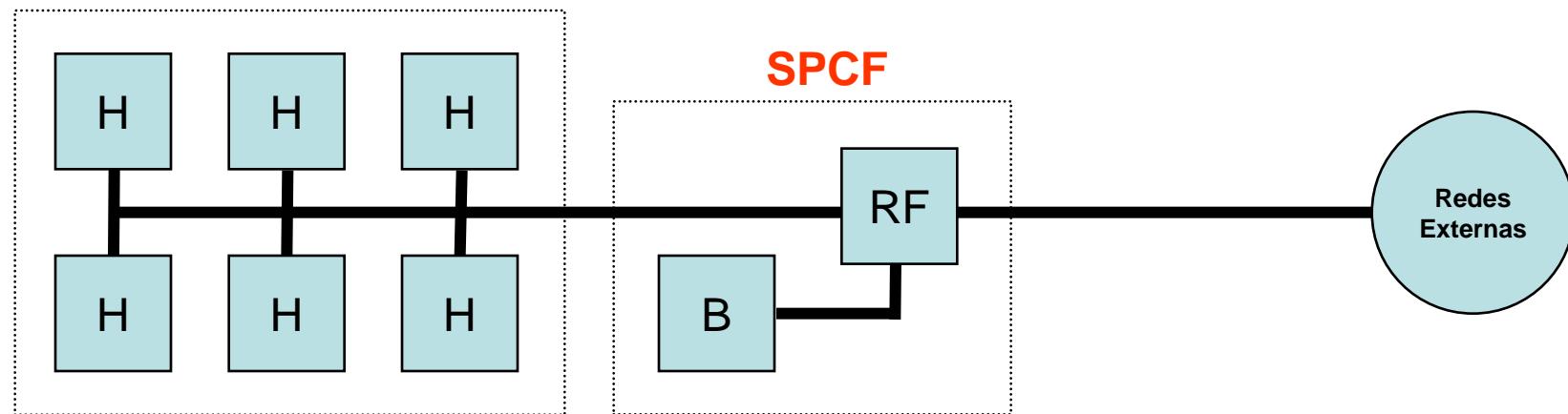
Segurança em Redes Privadas

Sistemas de Parede Corta-Fogo

Projetos (04)

Sub-Rede Protegida - Roteador Fiscalizador com Três Interfaces

(PI)



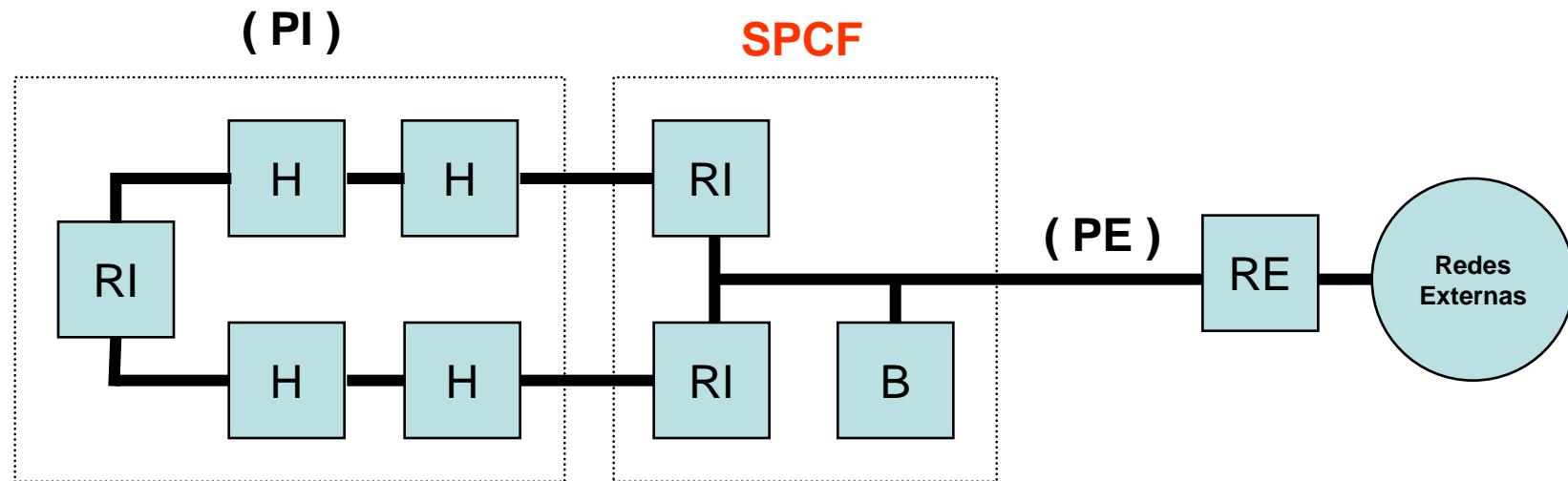
PI - Perímetro Interno || H - Hospedeiro || B - Bastião || RF - Roteador Fiscalizador

Segurança em Redes Privadas

Sistemas de Parede Corta-Fogo

Projetos (05)

Sub-Rede Protegida - Múltiplos Roteadores Internos (Maior Risco)



PI - Perímetro Interno || **H** - Hospedeiro || **RI** - Roteador Interno || **B** - Bastião || **RE** - Roteador Externo

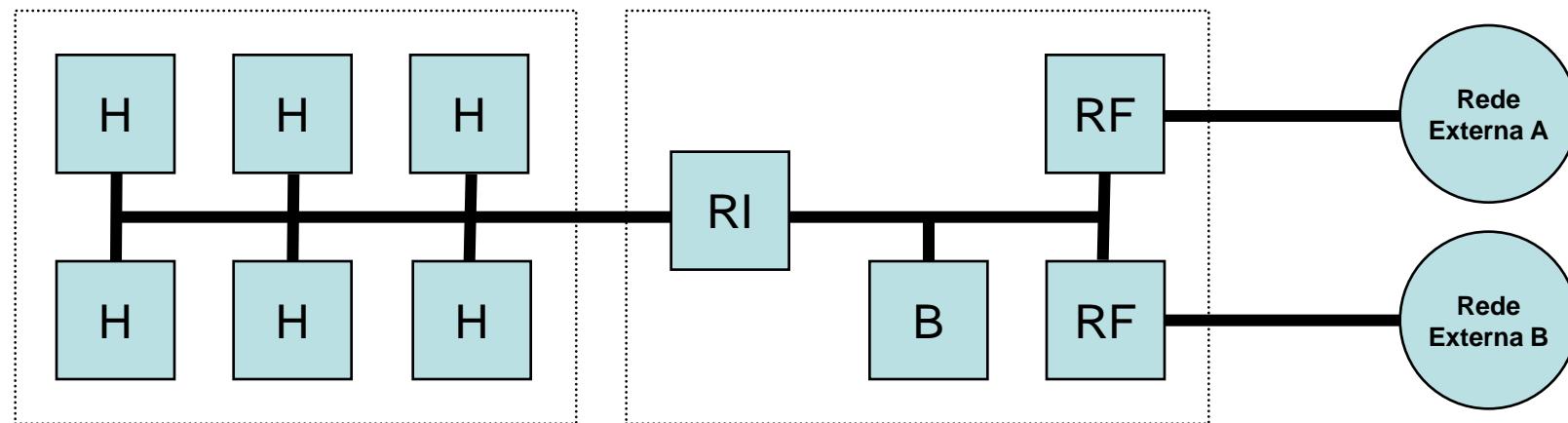
Segurança em Redes Privadas

Sistemas de Parede Corta-Fogo Projetos (06)

Sub-Rede Protegida - Múltiplos Roteadores Externos

(PI)

SPCF



PI - Perímetro Interno || **H** - Hospedeiro || **RI** - Roteador Interno || **B** - Bastião || **RF** - Roteador Fiscalizador

Segurança em Redes Privadas

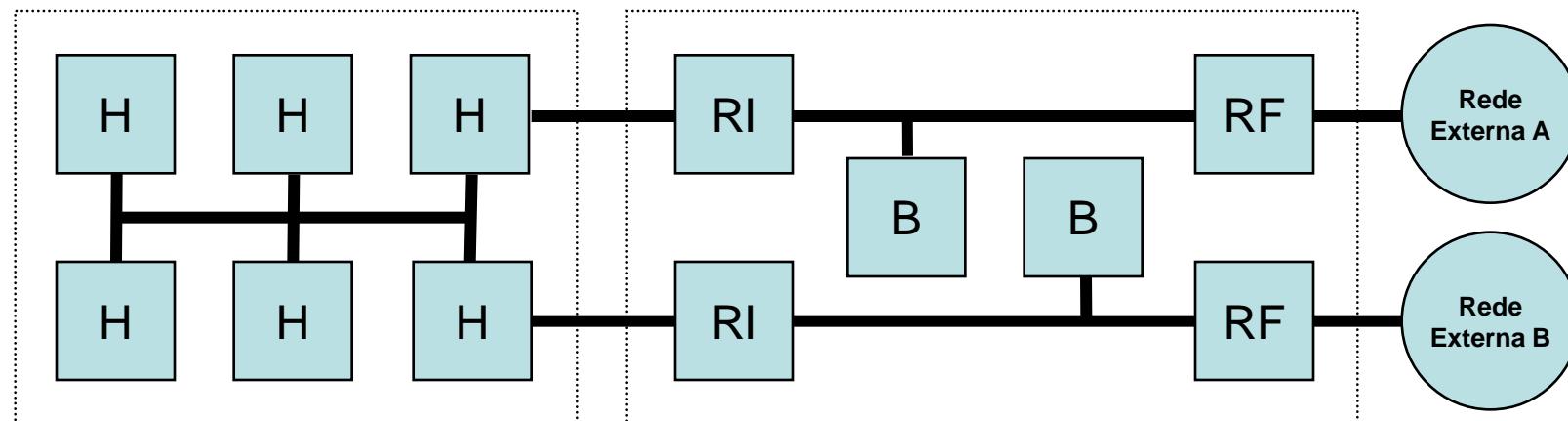
Sistemas de Parede Corta-Fogo

Projetos (07)

Sub-Rede Protegida - Múltiplas Redes Fronteiriças

(PI)

SPCF

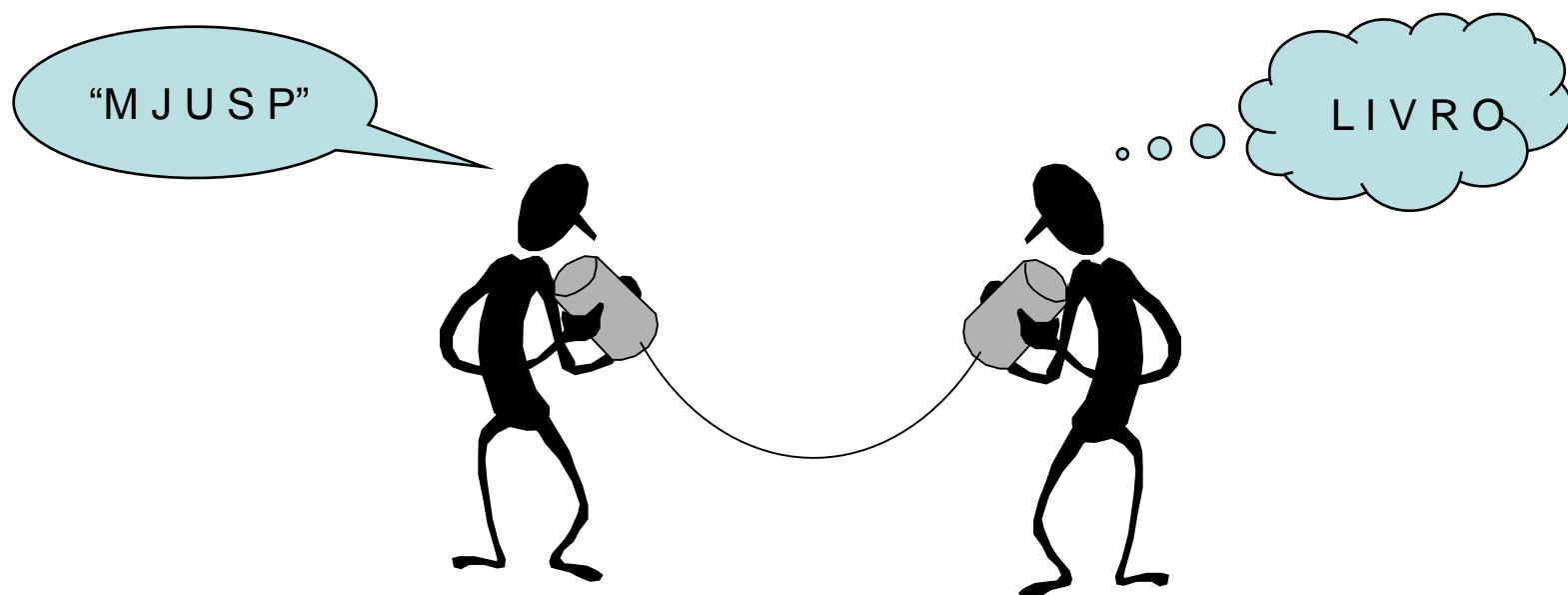


PI - Perímetro Interno || H - Hospedeiro || RI - Roteador Interno || B - Bastião || RF - Roteador Fiscalizador

Segurança em Redes Privadas

Criptografia

Criptografar é o processo de codificar uma mensagem, valendo-se de funções matemáticas



Segurança em Redes Privadas

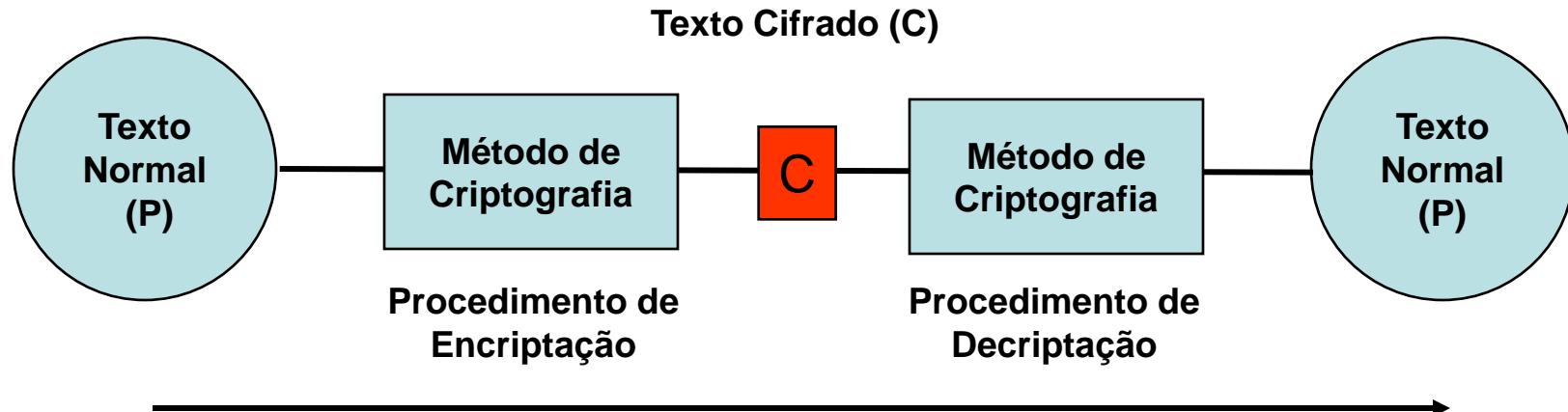
Criptografia - Etapas 01

A criptografia é constituída de duas etapas: **encriptar** é o processo de transformar os dados, dificultando sua interpretação; **decriptar** é o processo inverso, ou seja, converter os dados criptografados para a sua forma original, inteligível. Chaves - valores numéricos, expressos no sistema hexadecimal, que devem ser trocados entre os usuários envolvidos na comunicação - são empregadas durante a encriptação ou decriptação de uma mensagem; dependendo do método de criptografia empregado, a mesma chave pode ser usada nas duas etapas do processo, enquanto outros mecanismos utilizam chaves diferentes.

Segurança em Redes Privadas

Criptografia - Etapas 02

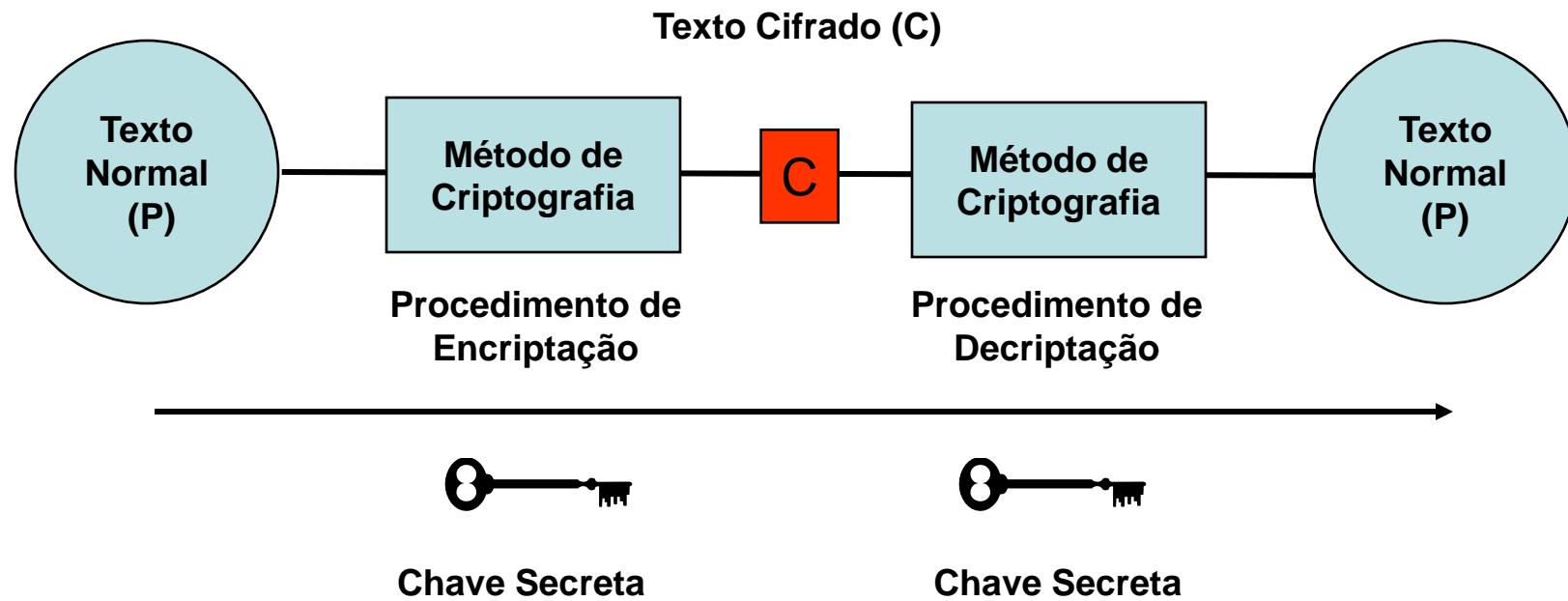
Etapas da Criptografia



Segurança em Redes Privadas

Criptografia Simétrica

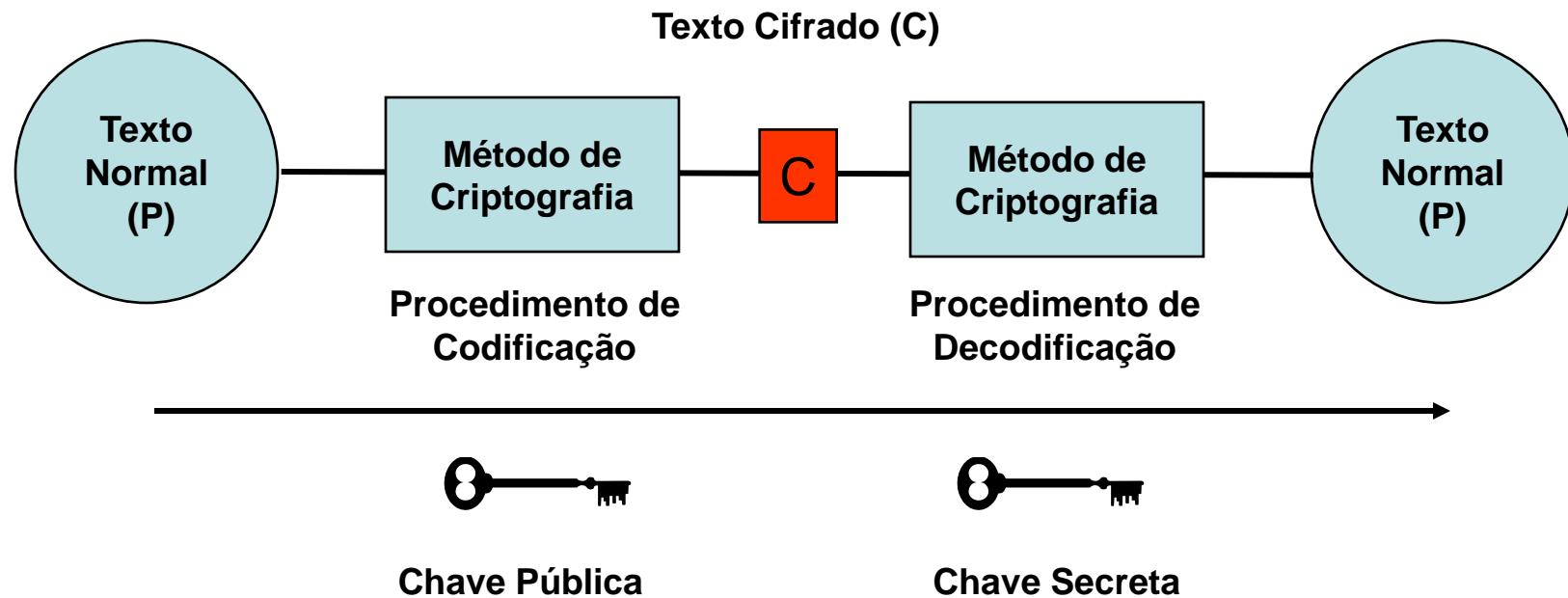
Esquema de Criptografia Utilizando uma Chave Secreta



Segurança em Redes Privadas

Criptografia Assimétrica

Esquema de Criptografia Utilizando duas Chaves



Segurança em Redes Privadas

Criptografia - Características Gerais

Confidencialidade

É quase impossível para um estranho que não possua a chave compreender a mensagem interceptada.

Integridade

É possível detectar adulterações nas mensagens.

Autenticação de Usuário

Através da autenticação é possível verificar se a pessoa que participa do processo de comunicação é, de fato, quem ela alega ser.

Segurança em Redes Privadas

Criptografia - Propriedades das Chaves

A chave pública e a chave privada definem operações criptográficas inversas entre si; entretanto, vale lembrar que é impraticável calcular a chave privada a partir da chave pública e vice-versa.

As chaves são números grandes, geralmente acima de 200 dígitos; é inviável memorizá-los e, por isso, devem mantidas em arquivos eletrônicos no computador.

A chave privada é protegida, cifrada a partir de criptografia simétrica e por uma frase-senha longa, com mais de 12 caracteres, por exemplo; o propósito é tornar a chave privada inutilizável caso o arquivo que a contenha esteja acessível.

Segurança em Redes Privadas

Criptografia - Técnicas Conhecidas

Rot 13

Crypt

DES

IDEA

RSA

PEM

PGP

RC2 e RC4

Segurança em Redes Privadas

Tipos de Cifragem de Blocos

Cifras de Substituição

ECB - “Electronic Code Book” (Modo do Livro de Códigos)

Máquinas de Cifragem

CBC - “Cipher Block Chaining” (Modo de Encadeamento de Blocos)

Cifras de Transposição

CFB - “Cipher Feedback” (Modo de Retroalimentação de Cifra)

Segurança em Redes Privadas

Criptografia - Tipos de Ataques

Ataque de Texto Cifrado (“Ciphertext-Only”)

Ataque de Texto Conhecido (“Known-Plaintext”)

Ataque Adaptativo do Texto Escolhido

Ataque do Texto Cifrado Escolhido (“Chosen-Ciphertext”)

Ataque de Chave Escolhida (“Chosen-Key”)

Segurança em Redes Privadas

Criptografia - Criptografia Assimétrica

CARACTERÍSTICAS

Confidencialidade

Um interceptador não é capaz de entender o que se passa no canal.

Autenticação

É possível provar que o remetente e o destinatário sejam, de fato, quem eles afirmam ser.

Segurança em Redes Privadas

Criptografia - Criptografia Assimétrica

CARACTERÍSTICAS

Não-Repudiação

O remetente não tem como negar que ele realmente é o autor da mensagem.

Integridade

Qualquer alteração em trânsito é detectada, o que resolve o problema da distribuição das chaves.

Segurança em Redes Privadas

Criptografia - Criptografia Simétrica

CARACTERÍSTICAS

Confiabilidade

É quase impossível para um estranho que não possua a chave compreender a mensagem interceptada.

Integridade

É possível detectar alterações nas mensagens.

Segurança em Redes Privadas

Criptografia - Criptografia Simétrica

DESVANTAGENS

O compartilhamento da chave deve ser feito no modo seguro, a revelação desta compromete todas as mensagens enviadas e torna o método inútil. A chave pode ser transmitida sem o conhecimento dos envolvidos.

Segurança em Redes Privadas

Criptografia

Método Simétrico x Método Assimétrico

Criptografia Simétrica (“Método Convencional”)

- Permitem repúdio
- Gerenciamento de chaves difícil
- Rápidas (da ordem de megabytes por segundo) em software

Criptografia Assimétrica (Baseada em Chave Pública)

- Da ordem de 1000 vezes mais lentas que a simétrica
- Gerenciamento de chaves muito mais fácil
- Novos serviços: autenticidade e não-repúdio

Segurança em Redes Privadas

Conclusão

