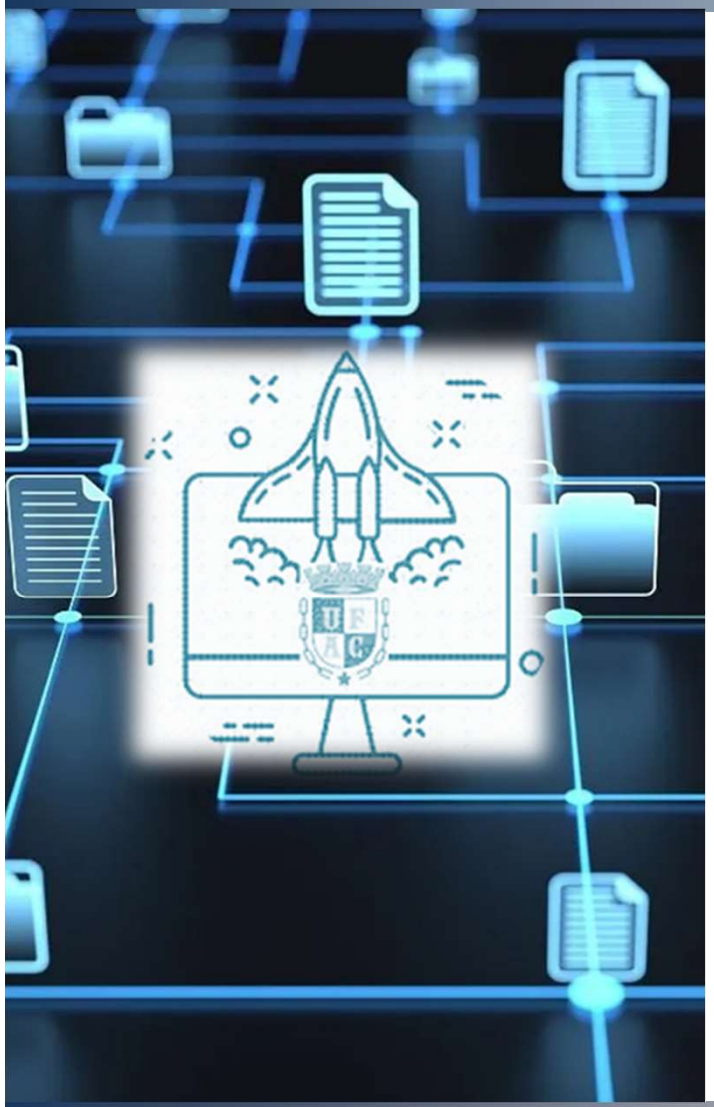
UFAC

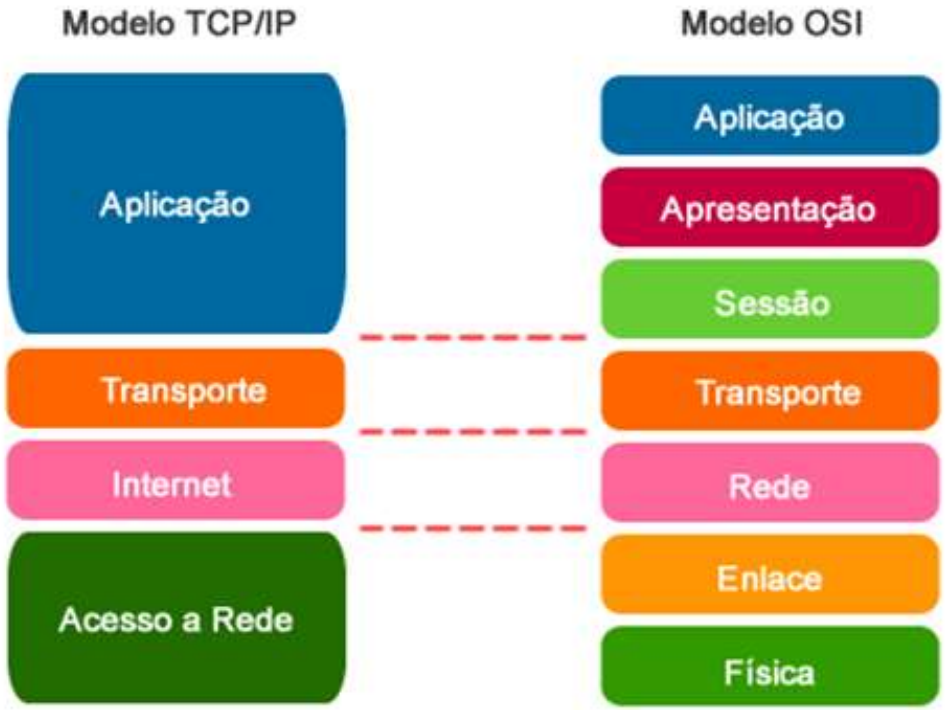


Redes de Computadores

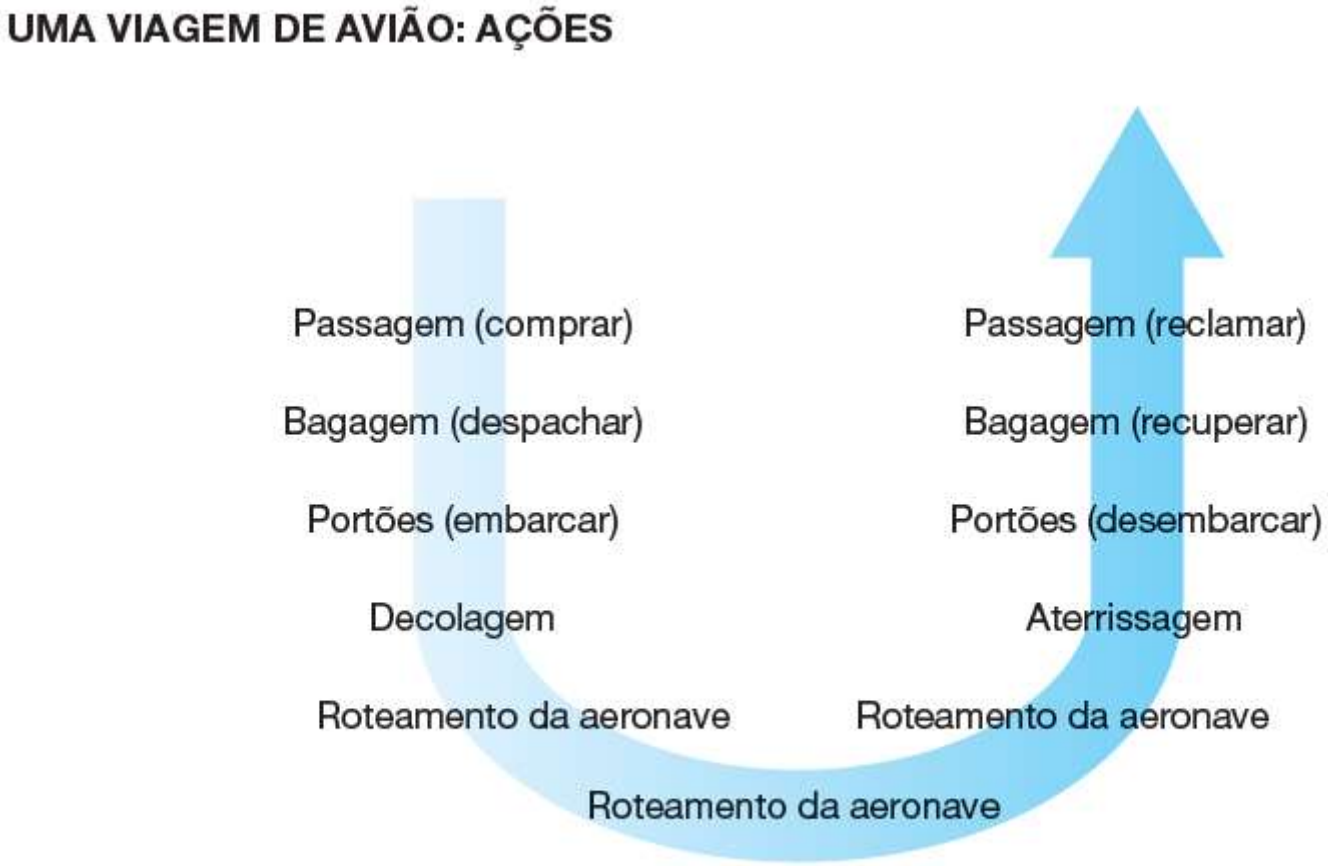
Prof. André Nasserala
andre.nasserala@ufac.br

Camadas de protocolo e seus modelos de serviço

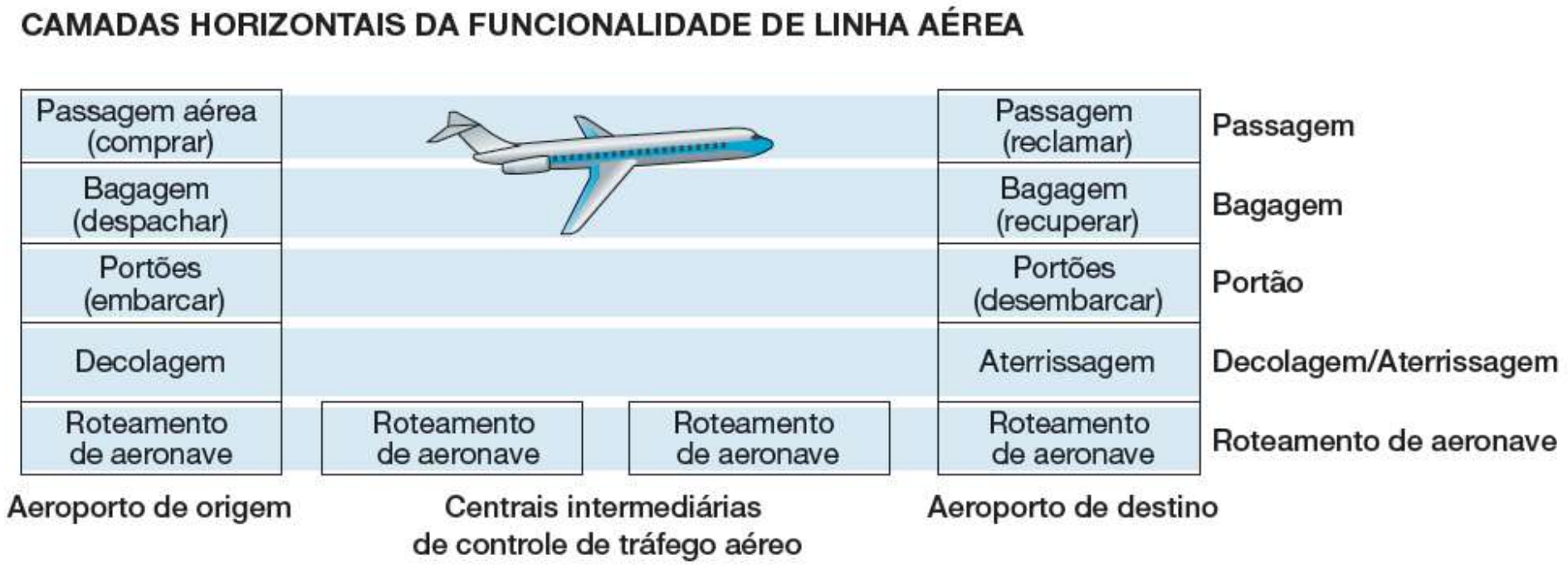
- Uma arquitetura de camadas nos permite discutir uma parcela específica e bem definida de um sistema grande e complexo.
- Essa simplificação tem considerável valor intrínseco, pois provê modularidade, tornando muito mais fácil modificar a execução do serviço prestado pela camada.
- Contanto que a camada forneça o mesmo serviço para a que está acima e use os mesmos serviços da que vem abaixo dela, o restante do sistema permanece inalterado quando a sua realização é modificada.



Camadas de protocolo e seus modelos de serviço



Camadas de protocolo e seus modelos de serviço



Camadas de protocolo

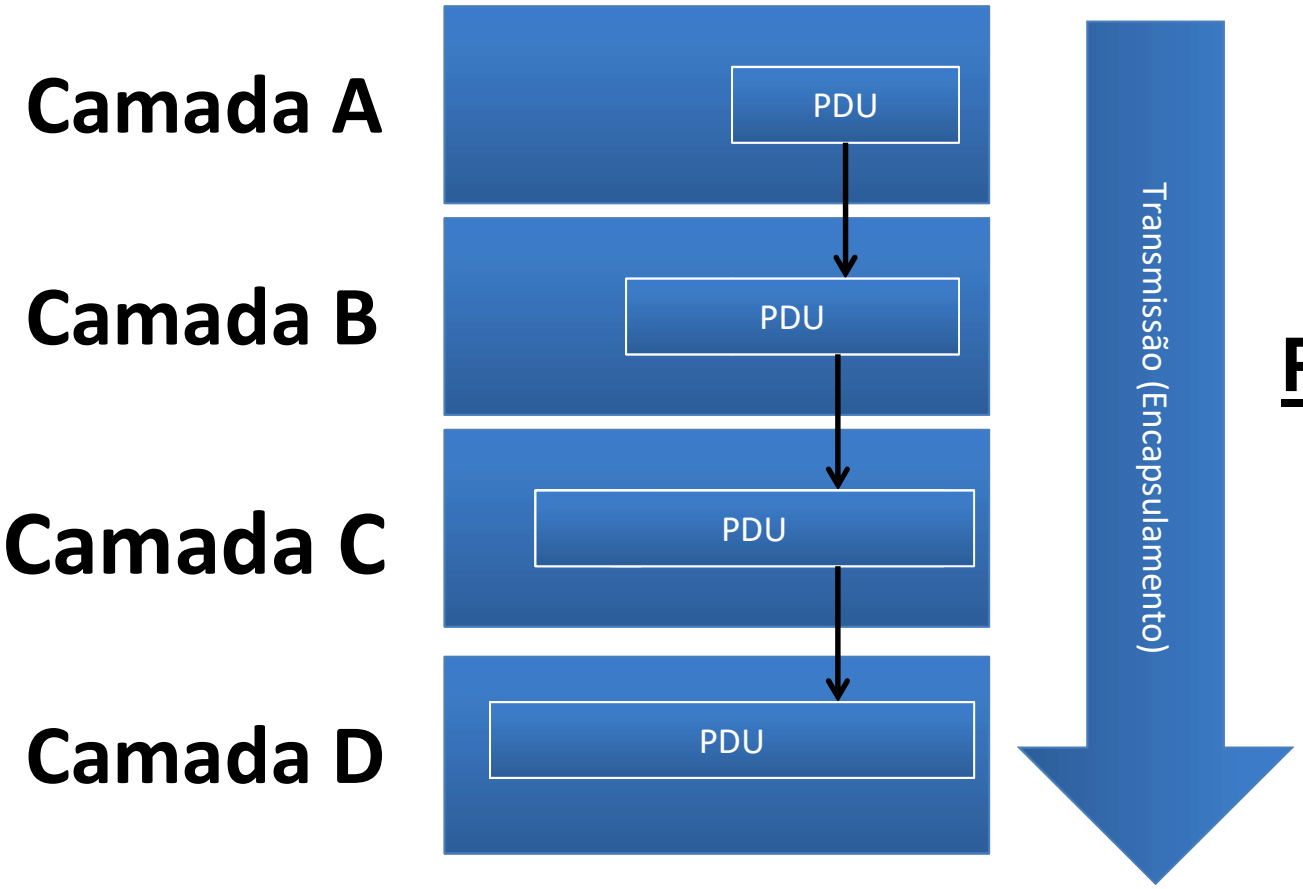
- As camadas de protocolo podem ser implementadas em software, hardware ou uma combinação de ambos.
- Localização:
- Camadas de aplicação e transporte: Geralmente em software nos sistemas finais (computadores, smartphones).
- Camadas física e de enlace de dados: Normalmente em hardware nas placas de rede (Ethernet, Wi-Fi).
- Camada de rede: Combinação de hardware e software.
- Distribuição: As funções de cada camada são distribuídas entre os diversos componentes da rede (sistemas finais, roteadores, switches).

Camadas de protocolo

- Ao receber dados para efetuar um serviço, a camada N necessita incluir um cabeçalho, no qual são registradas informações relativas à camada.
- A esse cabeçalho, damos o nome de Informação de Controle do Protocolo - **PCI** (Protocol Control Information).
- Aos dados recebidos pela camada N, damos o nome de Unidade de dados do Serviço - **SDU** (Service Data Unit).
- Ao conjunto formado por PCI + SDU damos o nome de Unidade de Dados do Protocolo - PDU (Protocol Data Unit). Portanto, **PDU = PCI + SDU.**

Camadas de protocolo

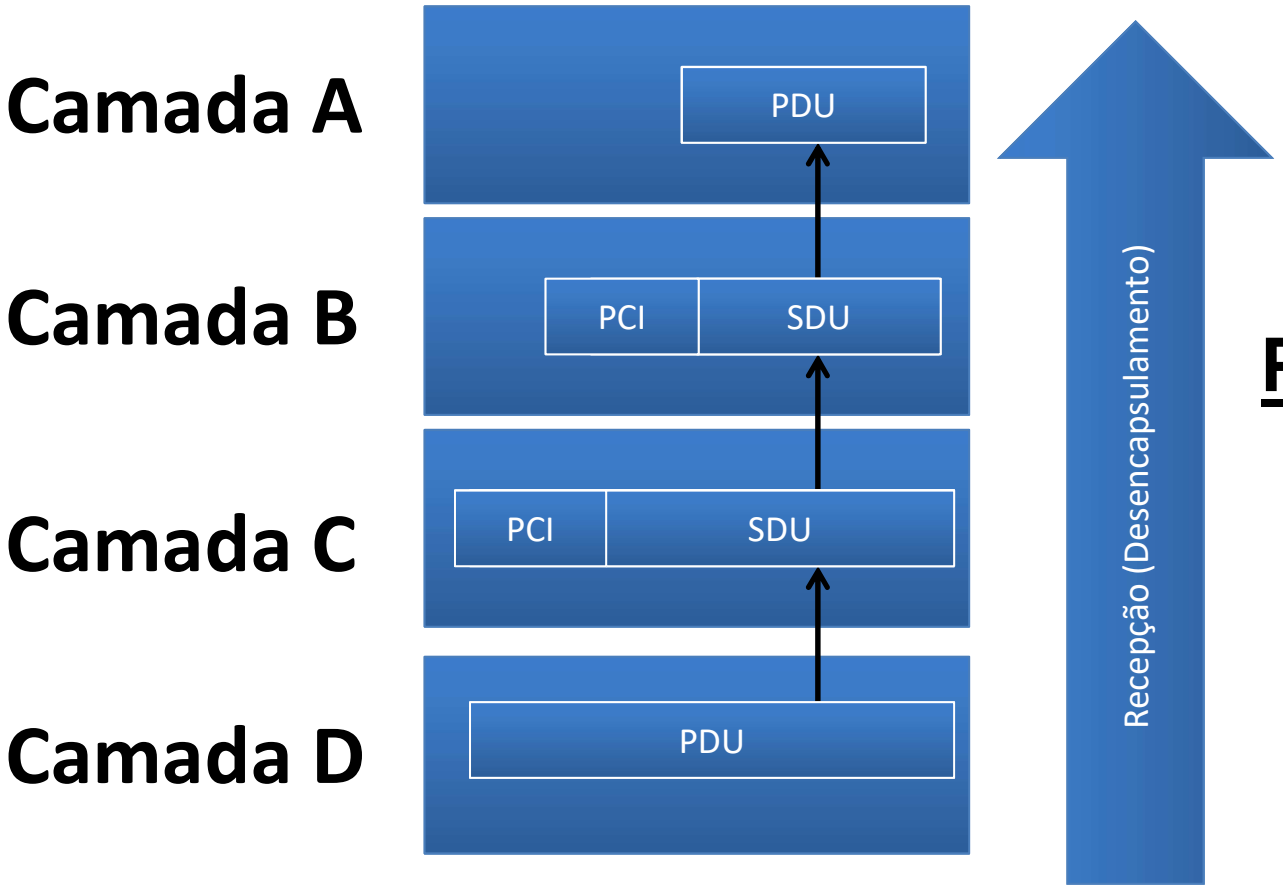
A troca de dados entre camadas



PDU = PCI + SDU

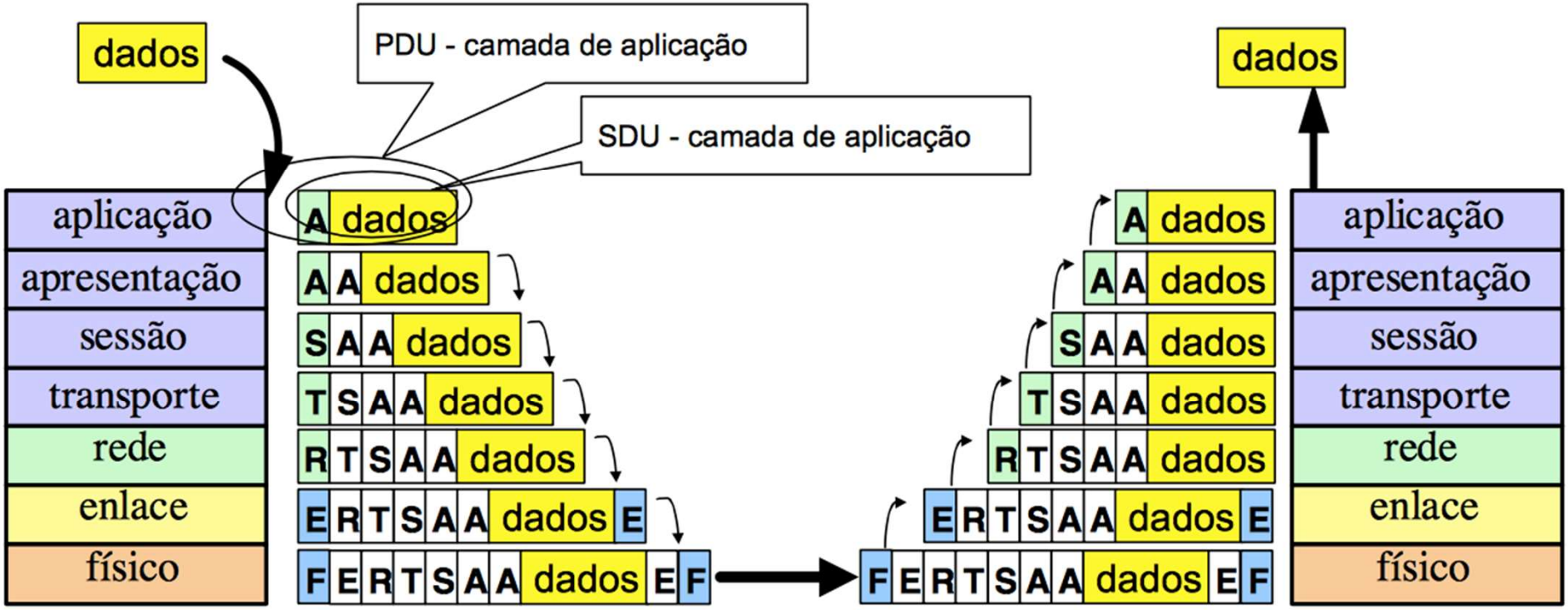
Camadas de protocolo

A troca de dados entre camadas



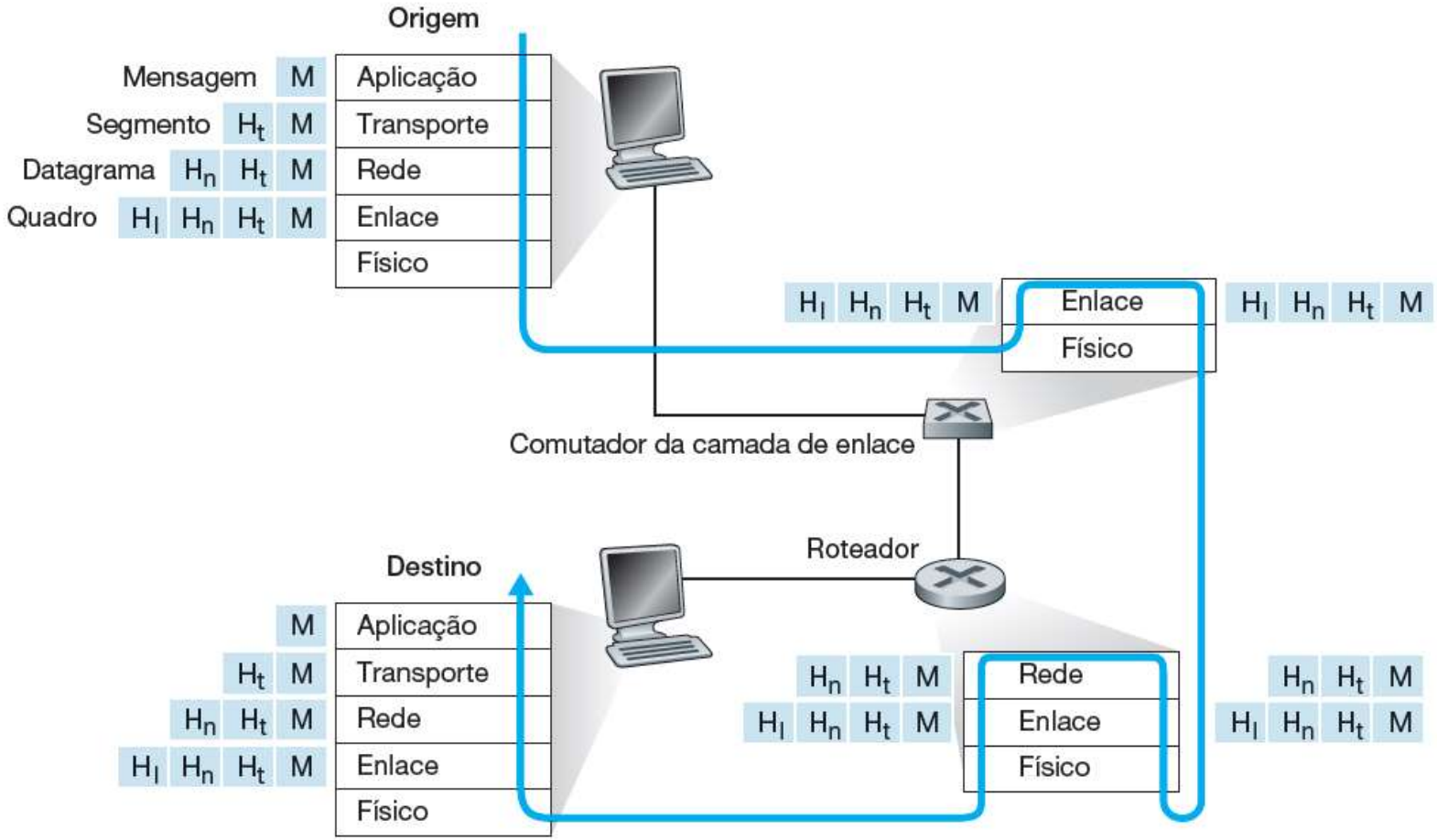
PDU = PCI + SDU

Camadas de protocolo



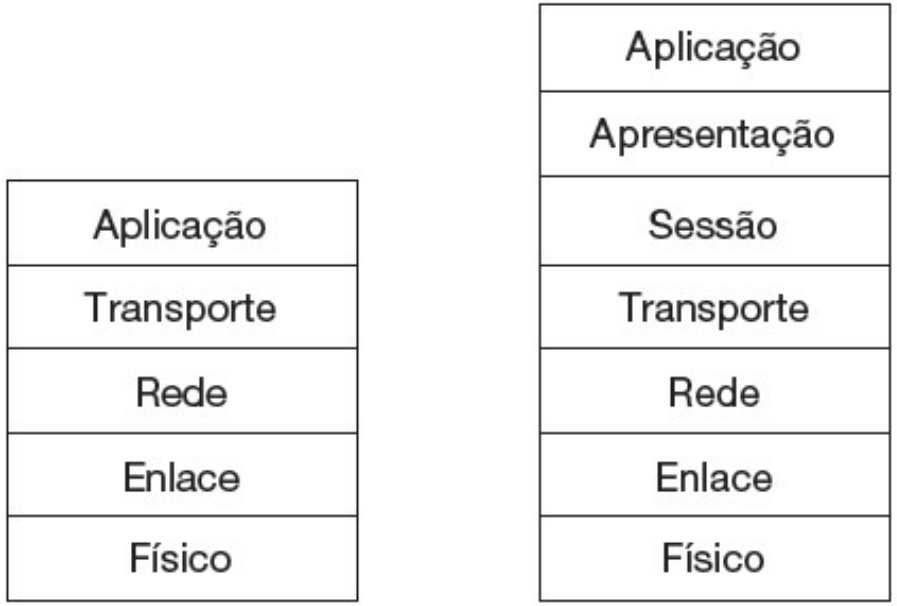
Camadas de protocolo

HOSPEDEIROS, ROTEADORES E COMUTADORES DE CAMADA DE ENLACE; CADA UM CONTÉM UM CONJUNTO DIFERENTE DE CAMADAS, REFLETINDO SUAS DIFERENÇAS EM FUNCIONALIDADE



Camadas de protocolo

A PILHA DE PROTOCOLOS DA INTERNET (A) E O MODELO DE REFERÊNCIA OSI (B)



a. Pilha de protocolos da Internet de cinco camadas

b. Modelo de referência ISO de sete camadas

Camada de Aplicação

- A camada de aplicação do modelo TCP/IP é a interface entre os aplicativos de usuário e a rede.
- É nessa camada que os protocolos de aplicação, como HTTP, FTP, SMTP e outros, interagem com os usuários ou outros aplicativos para fornecer serviços de rede.
- **Funções Principais:**
  - Interação com o usuário: Fornece uma interface para que os usuários possam acessar e utilizar os serviços de rede, como navegar na web, enviar e-mails ou transferir arquivos.
  - Definição de formatos de dados: Estabelece os formatos dos dados que serão trocados entre os aplicativos, garantindo que as informações sejam interpretadas corretamente.
  - Gerenciamento de sessões: Controla as sessões de comunicação entre os aplicativos, incluindo a criação, manutenção e término das conexões.
  - Sintaxe e semântica: Define a sintaxe (estrutura) e a semântica (significado) dos comandos e respostas trocados entre os aplicativos.

Camada de Aplicação

- **Protocolos de Aplicação Comuns:**
  - HTTP (Hypertext Transfer Protocol): Protocolo utilizado para a transferência de arquivos na Web, como páginas HTML, imagens e vídeos.
  - FTP (File Transfer Protocol): Protocolo utilizado para transferir arquivos entre computadores.
  - SMTP (Simple Mail Transfer Protocol): Protocolo utilizado para enviar e-mails.
  - POP3 (Post Office Protocol 3): Protocolo utilizado para receber e-mails.
  - SSH (Secure Shell): Protocolo seguro para acesso remoto a computadores.
  - DNS (Domain Name System): Sistema de nomes de domínio que traduz nomes amigáveis (como www.example.com) em endereços IP numéricos.

Camada de Aplicação

- **Como funciona:**

1. O aplicativo do usuário (por exemplo, um navegador web) envia uma solicitação para um servidor através da camada de aplicação.
2. A camada de aplicação formata a solicitação de acordo com o protocolo utilizado (HTTP, FTP, etc.) e a envia para a camada de transporte.
3. As camadas de transporte, rede e enlace encapsulam a solicitação e a encaminham até o destino.
4. O servidor recebe a solicitação, processa-a e envia uma resposta.
5. As camadas de rede, transporte e aplicação no servidor desencapsulam a resposta e a entregam ao aplicativo do servidor.
6. O aplicativo do servidor envia a resposta para o aplicativo do cliente.

Camada de Transporte

- A camada de transporte do modelo TCP/IP é responsável por fornecer serviços de comunicação confiáveis e eficientes entre os processos que rodam em hosts diferentes.
- Ela atua como uma ponte entre a camada de aplicação, que contém os protocolos utilizados pelos aplicativos, e a camada de rede, que cuida do roteamento dos pacotes pela internet.
- **Funções** Principais:
  - Gerenciamento de conexões: Estabelece, mantém e encerra conexões entre os processos.
  - Fragmentação e remontagem: Divide grandes mensagens em segmentos menores (fragmentação) para facilitar o envio pela rede e reune esses segmentos na ordem correta no destino (remontagem).
  - Controle de fluxo: Ajusta a taxa de envio de dados para evitar o congestionamento da rede.
  - Controle de erros: Detecta e corrige erros que possam ocorrer durante a transmissão dos dados.
  - Multiplexação: Permite que múltiplos processos compartilhem uma única conexão.

Camada de Transporte

- Protocolos de Transporte Comuns:
- **TCP (Transmission Control Protocol)**: É um protocolo orientado à conexão, confiável e orientado à byte.
- Garante a entrega ordenada e sem erros dos dados, além de controlar o fluxo e retransmitir pacotes perdidos.

- **UDP (User Datagram Protocol)**: É um protocolo sem conexão, não confiável e orientado a datagramas.
- Não garante a entrega dos dados, a ordem de chegada ou a ausência de erros, mas é mais leve e eficiente que o TCP.

Camada de Transporte

- **<u>Como funciona:</u>**

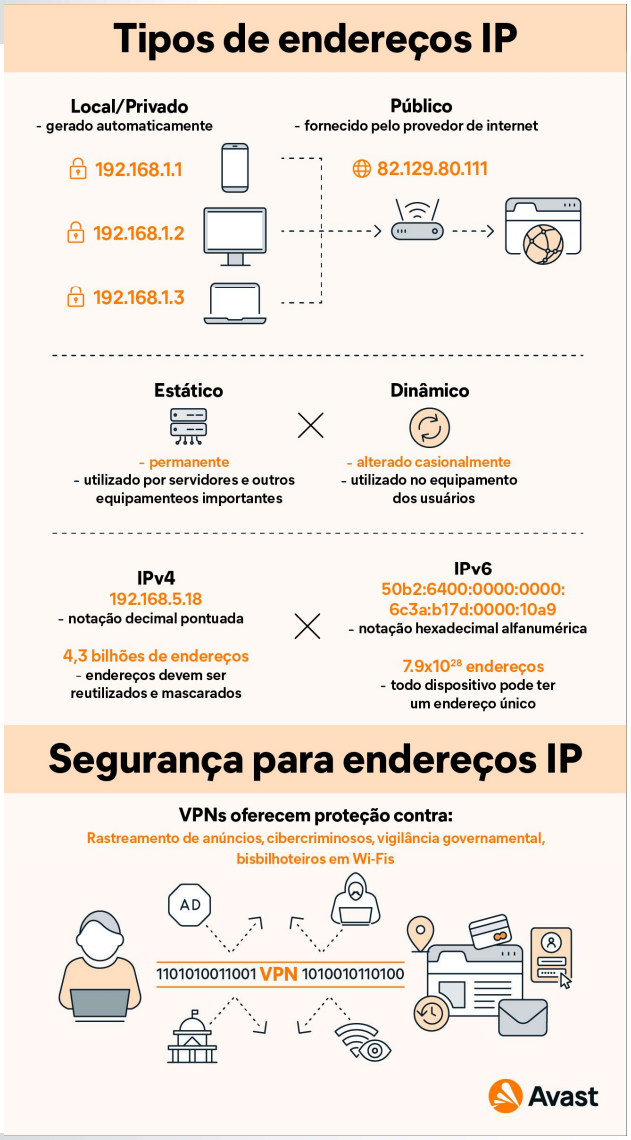
1. A camada de aplicação passa os dados para a camada de transporte.
2. A camada de transporte divide os dados em segmentos, adiciona informações de cabeçalho (como número de sequência, número de confirmação, etc.) e os entrega para a camada de rede.
3. A camada de rede encapsula os segmentos em pacotes e os encaminha pela rede.
4. A camada de transporte no host de destino recebe os pacotes, verifica a integridade dos dados e reúne os segmentos na ordem correta.
5. A camada de aplicação recebe os dados remontados e os entrega ao processo de destino.

Camada de Rede/Internet

- A camada de internet do modelo TCP/IP é responsável por rotear pacotes de dados de um host para outro em uma rede interconectada.
- Ela é a espinha dorsal da Internet, permitindo que dados sejam enviados entre redes distintas.
- **Funções Principais:**
  - Endereçamento: Cada dispositivo conectado à rede possui um endereço IP único que o identifica. A camada de internet utiliza esses endereços para determinar o caminho que um pacote deve seguir.
  - Roteamento: A camada de internet determina o melhor caminho para um pacote chegar ao seu destino, utilizando algoritmos de roteamento.
  - Fragmentação e remontagem: Divide pacotes grandes em fragmentos menores para que possam ser transmitidos por enlaces com tamanhos máximos de quadro diferentes e reune esses fragmentos no destino.

Camada de Rede/Internet

- **<u>Protocolo Principal:</u>**
- **IP** (***Internet Protocol***): É o protocolo principal da camada de internet.
- Ele encapsula os segmentos da camada de transporte em pacotes IP, adicionando informações de cabeçalho como o endereço IP do remetente e do destinatário.



Camada de Rede/Internet

- **Como funciona:**

1. A camada de transporte passa os segmentos para a camada de internet.
2. A camada de internet encapsula os segmentos em pacotes IP, adicionando o endereço IP do remetente e do destinatário.
3. Os roteadores examinam o endereço IP de destino de cada pacote e utilizam tabelas de roteamento para determinar o próximo salto para o pacote.
4. Os pacotes são encaminhados através de múltiplos roteadores até chegar ao destino.
5. A camada de internet no host de destino remove o cabeçalho IP e entrega o segmento para a camada de transporte.

Camadas de Enlace e Física

- As camadas de enlace e física (também conhecidas como camada de acesso ao meio) do modelo TCP/IP são as camadas mais próxima do hardware de rede.
- Elas são responsáveis por controlar o acesso físico ao meio de transmissão, como cabos de rede, sinais de rádio ou fibras ópticas.
- Essas camadas garantem que os dados sejam transmitidos de forma correta e eficiente entre os dispositivos conectados à rede.

Camadas de Enlace e Física

- **<u>Como funciona:</u>**

1. A camada de internet passa os segmentos para a camada de acesso ao meio.
2. A camada de acesso ao meio encapsula os segmentos em quadros, adicionando informações de cabeçalho e rodapé.
3. O dispositivo de rede (placa de rede, adaptador Wi-Fi) transmite o quadro pelo meio físico.
4. O dispositivo receptor recebe o quadro, verifica a integridade dos dados e passa os dados para a camada de transporte.

Modelo OSI

- Aplicação: Estabelecer comunicação entre os usuários e fornecer serviços básicos de comunicação.
- Apresentação: Realizar transformações nos dados antes de enviá-los a camada de aplicação. Entre essas transformações, poderíamos citar a criptografia e a compressão.
- Sessão: Fornecer a conexão entre dois processos.

Modelo OSI

- Transporte: Garantir que os dados cheguem ao seu destino, fornecendo uma comunicação fim a fim confiável, controlando o fluxo e a seqüência de pacotes.
- Rede: Rotear os pacotes da origem para o destino.
- Enlace Estabelecer a conexão entre dois dispositivos físicos compartilhando o mesmo meio físico. Detectar e corrigir erros que porventura venham a ocorrer no meio físico.
- Física: Transmitir a informação através do meio.

Redes sob ameaça

- Apesar de seus benefícios, a internet também é alvo de ataques por parte de indivíduos mal-intencionados que buscam causar danos a computadores, invadir privacidade e interromper serviços.
- A crescente complexidade e frequência de ataques cibernéticos exigem profissionais especializados para proteger redes e sistemas.
- É importante entender as vulnerabilidades das redes e os tipos de ataques mais comuns para desenvolver soluções eficazes.

A Ameaça do Malware na Internet

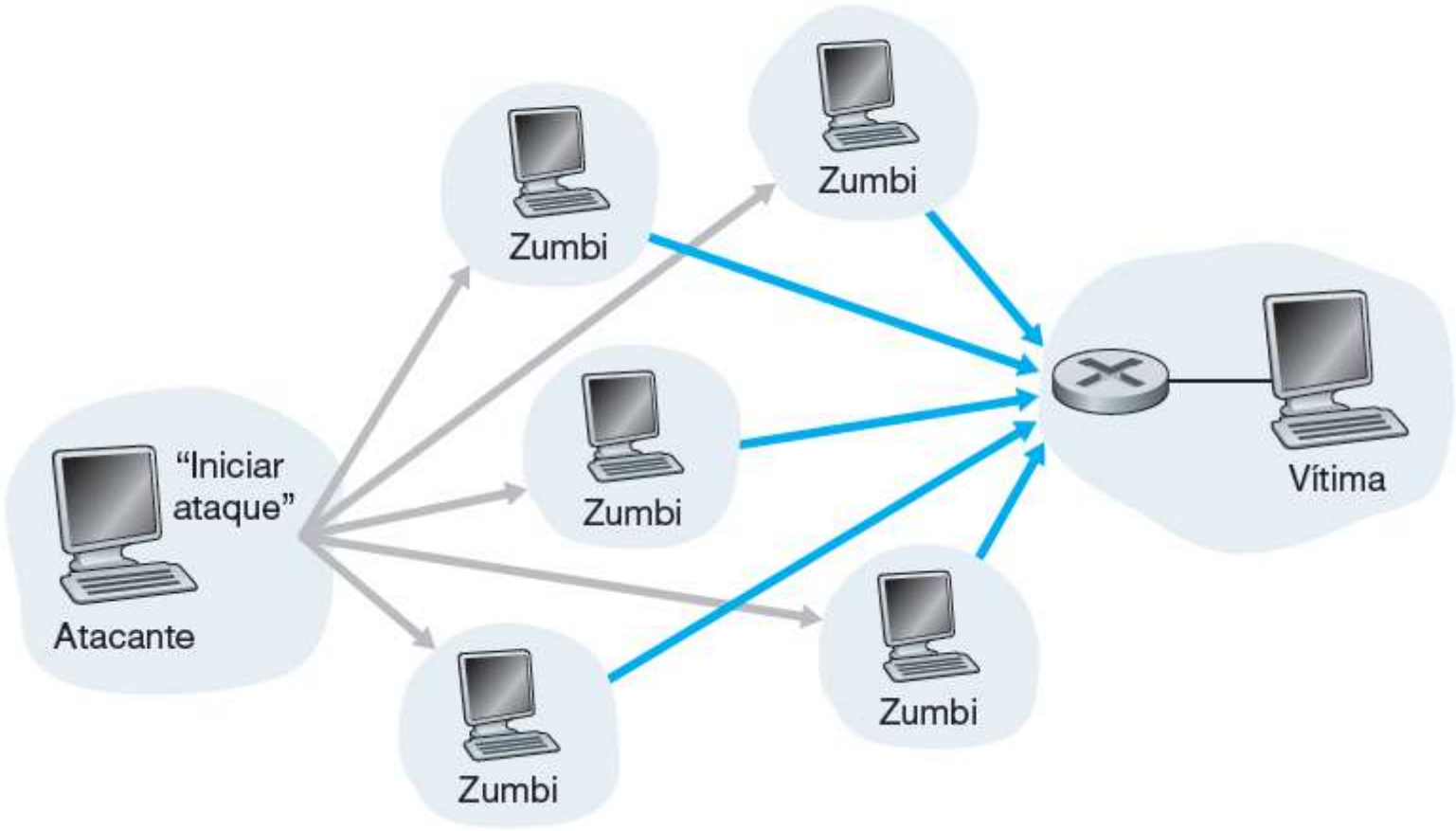
- Um Malware (software malicioso) pode coletar informações pessoais sensíveis, como senhas e dados financeiros.
- Vírus e outros tipos de malware podem apagar ou corromper arquivos importantes.
- Dispositivos infectados podem ser incorporados a botnets, redes de computadores controladas por criminosos para realizar ataques cibernéticos.
- Malware como vírus e worms podem se espalhar rapidamente pela internet, infectando novos dispositivos sem a necessidade de interação do usuário.

A Ameaça do Malware na Internet

- Vírus necessitam da interação do usuário para se propagar, geralmente através de anexos de e-mail ou downloads maliciosos.
- Worms são capazes de se autopropagar sem a necessidade de interação do usuário, explorando vulnerabilidades em softwares e sistemas.
- Os perigos do malware são diversos e em constante evolução.
- A cada dia, novos tipos de malware surgem, tornando a proteção de dispositivos cada vez mais desafiadora.

A Ameaça do Malware na Internet

UM ATAQUE DE RECUSA DE SERVIÇO DISTRIBUÍDO (DDoS)



Ataques de Negação de Serviço (DoS)

- Ataques de negação de serviço (DoS) visam tornar um recurso online (como um site ou servidor) indisponível para seus usuários legítimos.
- Ao inundar um sistema com tráfego excessivo ou explorando vulnerabilidades, o atacante impede que o serviço funcione normalmente.
- **Tipos de ataques DoS:**
- Ataque de vulnerabilidade: Explora falhas em softwares ou sistemas operacionais para comprometer o serviço.
- Inundação na largura de banda: Envia uma grande quantidade de tráfego para sobrecarregar a conexão do alvo.
- Inundação na conexão: Cria um grande número de conexões incompletas para esgotar os recursos do servidor.

Ataques de Negação de Serviço (DoS)

- **Ataques DDoS: Aumento da complexidade**
- Distribuição: Ao invés de um único atacante, os ataques DDoS utilizam múltiplas fontes para sobrecarregar o alvo, tornando a detecção e a defesa mais difíceis.
- Botnets: Redes de computadores infectados são frequentemente usadas para realizar ataques DDoS em grande escala.
- **Desafios para a defesa**:
- Detecção: É difícil distinguir entre tráfego legítimo e malicioso em um ataque DDoS.
- Prevenção: A proteção contra ataques DDoS exige uma combinação de medidas, como filtragem de pacotes, detecção de anomalias e mitigação de tráfego.

A Ameaça da Análise de Pacotes

- Análise de pacotes é a prática de interceptar e capturar o tráfego de dados que trafega em uma rede.
- Um atacante pode usar um software específico, chamado analisador de pacotes, para capturar e analisar esses dados.
- **Por que a análise de pacotes é um problema?**
- Informações sensíveis: Os pacotes capturados podem conter informações confidenciais como senhas, números de cartão de crédito e dados pessoais.
- Facilidade de acesso: A análise de pacotes pode ser realizada tanto em redes sem fio quanto com fio, tornando-a uma ameaça presente em diversos ambientes.
- Disponibilidade de ferramentas: Existem diversas ferramentas gratuitas e comerciais disponíveis para realizar a análise de pacotes.

A Ameaça da Análise de Pacotes

- **Consequências da análise de pacotes:**
- Violação de privacidade: A exposição de dados confidenciais pode levar a fraudes e outros crimes.
- Perda de informações confidenciais: Segredos comerciais e informações sensíveis podem ser expostas a concorrentes.
- Ataques cibernéticos: Os dados capturados podem ser utilizados para realizar ataques mais sofisticados.

- **Como se proteger?**
- Criptografia: A criptografia é a principal ferramenta para proteger a confidencialidade dos dados transmitidos em redes.
- Ela transforma os dados em um formato ilegível para quem não possui a chave de decodificação.

Bibliografia

- **Bibliografia Básica**
- - KUROSE, James F.; ROSS, Keith W. Redes de computadores e a Internet: uma abordagem top-down. 6a.ed. São Paulo: Pearson Addison Wesley, 2016.
- - TANENBAUM, Andrew S. Redes de Computadores. Rio de Janeiro: Campus, 6ª ed, 2021.
- - COMER, Douglas E. Redes de Computadores e Internet. 4. ed. Bookman, 2007.
- **Bibliografia Complementar**
- - STALLINGS, W. Redes e Sistemas de Comunicação de Dados, Rio de Janeiro: Elsevier. 5.Edicao, 2005.
- - TORRES, Gabriel. Redes de computadores. Rio de Janeiro: Nova Terra, 2010.