Aula 4 - Modelos em Camadas, Segurança

Diego Passos

Universidade Federal Fluminense

Redes de Computadores

Material adaptado a partir dos slides originais de J.F Kurose and K.W. Ross.

Modelos em Camadas

“Camadas” de Protocolos

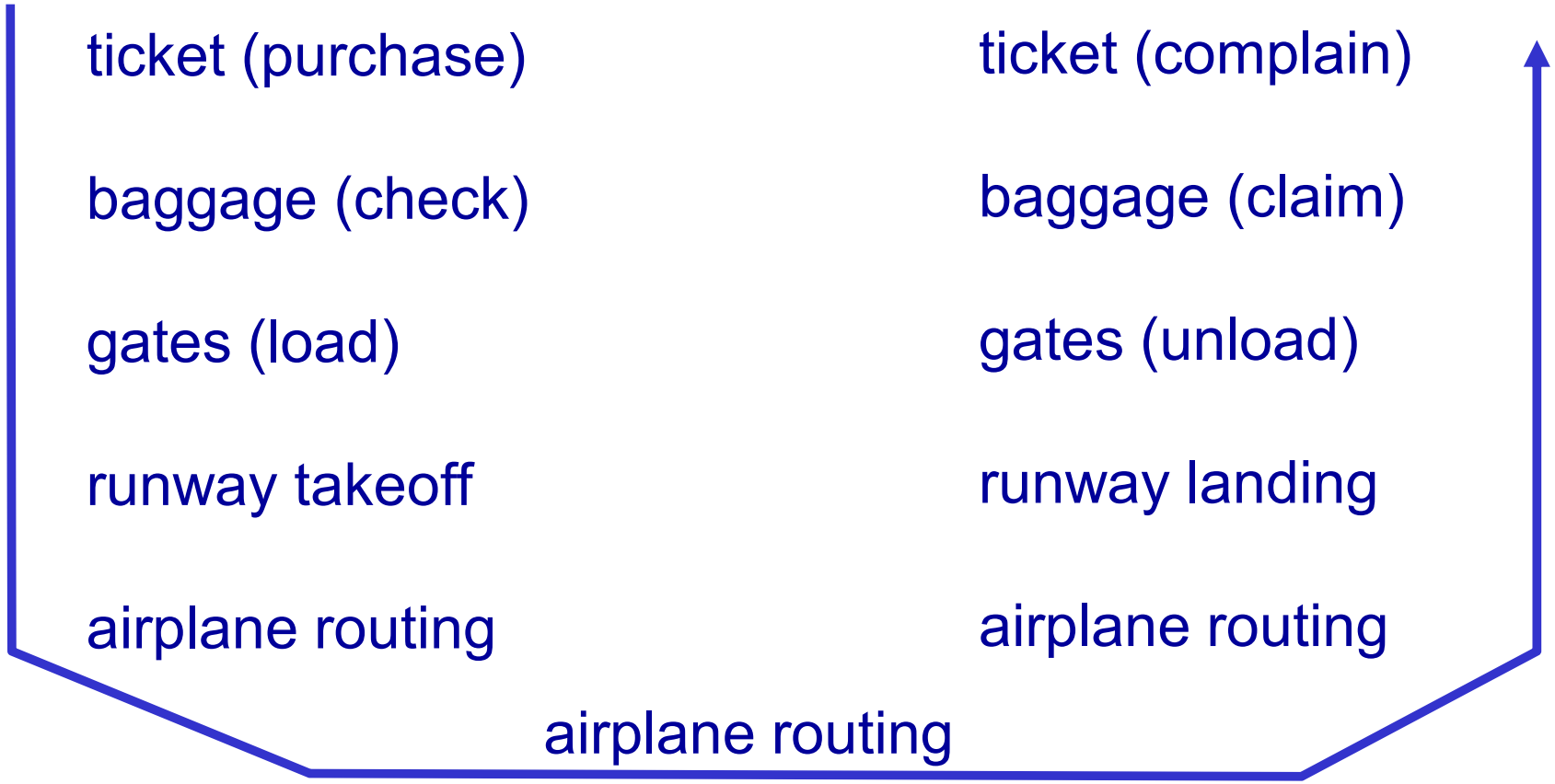
- **Redes são sistemas complexos, com várias “partes”.**
  - *Hosts*.
  - Roteadores.
  - Enlaces (de vários tipos).
  - Aplicações.
  - Protocolos.
  - *Hardware*, *software*.

Pergunta

Alguma chance de organizar a estrutura da rede?

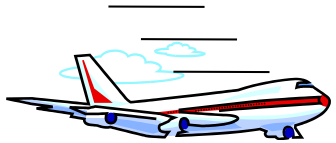
... ou ao menos nossa discussão sobre redes?

Analogia: Organização de uma Viagem Aérea (I)



- Uma série de passos envolvidos.

Organizando Funcionalidades da Cia. Aérea em Camadas



departure airport	intermediate air-traffic control centers		arrival airport	
ticket (purchase)			ticket (complain)	ticket
baggage (check)			baggage (claim	baggage
gates (load)			gates (unload)	gate
runway (takeoff)			runway (land)	takeoff/landing
airplane routing	airplane routing	airplane routing	airplane routing	airplane routing

- **Camadas:** cada camada implementa um serviço.
  - Através de ações internas da própria camada.
  - Dependendo de serviços providos pela camada abaixo.

Por Que uma Organização em Camadas?

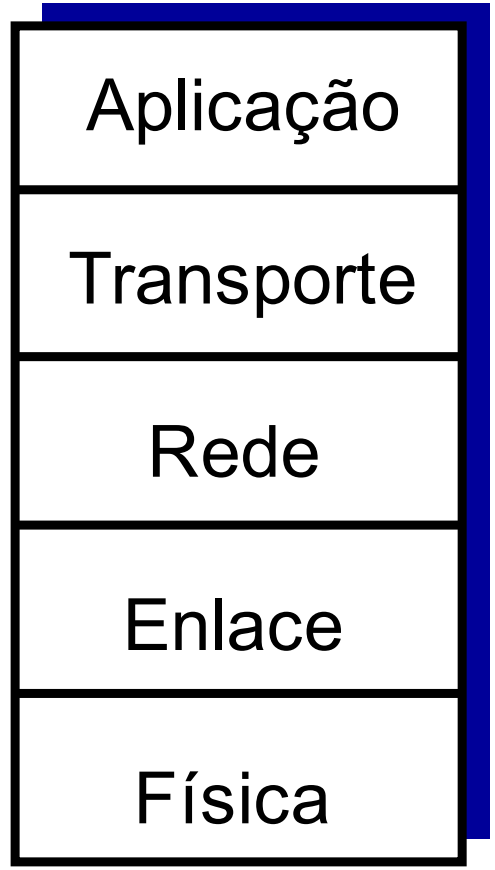
- Lidar com sistemas complexos:
  - Estrutura explícita permite identificar relações entre os pedaços do sistema.
    - **Modelo de referência** em camadas para discussão.
  - Modularização facilita a manutenção, atualização do sistema.
    - Alterar a implementação de uma camada é transparente para o resto do sistema.
    - *e.g.*, mudança no processo de embarque não afeta o resto do sistema da cia. aérea.
  - "Layering considered harmful"?

Pilha de Protocolos da Internet (I)

- Ou suíte de protocolos da Internet.
- Ou modelo TCP/IP.
- Define organização dos vários protocolos usados na Internet em camadas.
- Define **responsabilidades, serviços** de cada camada.
- Dividida em 4 ou 5 camadas, dependendo do autor.
  - Nomes das camadas também podem variar.
  - Nesta disciplina, **seguiremos o modelo do livro-texto**.

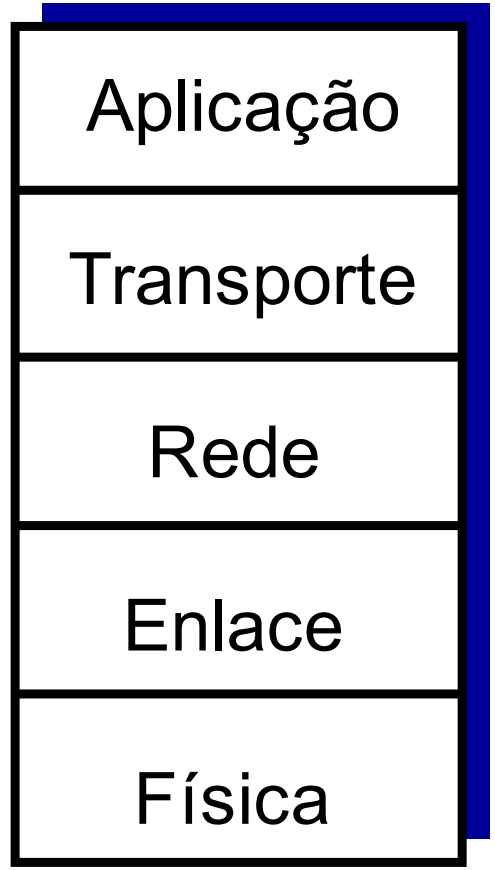
Pilha de Protocolos da Internet (II)

- **Aplicação:** suporte a aplicações de rede.
  - Definem formato, ordem, semântica das mensagens trocadas pelas aplicações.
  - Exemplo da web:
    - Cliente (*browser*) gera mensagem de requisição de conteúdo.
    - Servidor envia mensagem de resposta.
    - Cada mensagem tem seus campos específicos (próximo capítulo).
  - Exemplos de protocolos:
    - HTTP, FTP, SMTP, ...



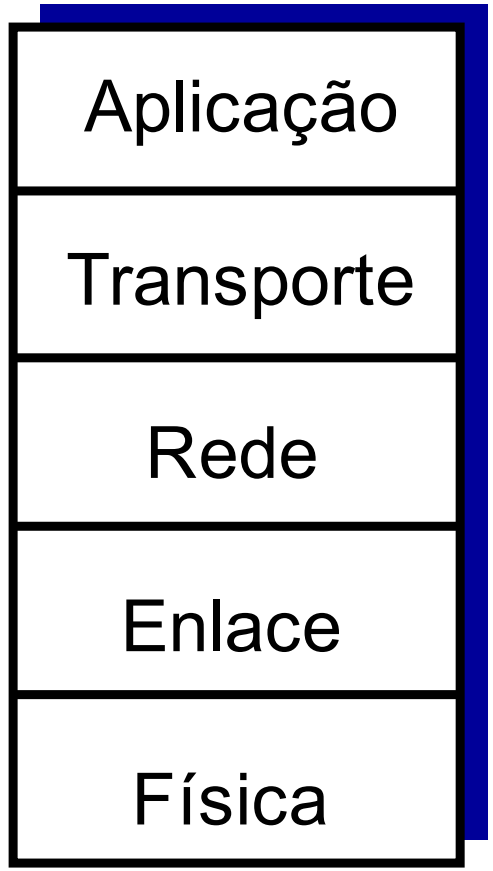
Pilha de Protocolos da Internet (III)

- **Transporte:** comunicação entre processos em computadores (potencialmente) diferentes.
  - Transfere dados de um processo para o outro.
    - Potencialmente, em computadores diferentes.
  - Dois exemplos clássicos de protocolos:
    - UDP e TCP.
  - Protocolos diferentes proveem **modelos de serviço diferentes**.
    - TCP provê garantias mais fortes.
  - **Responde a pergunta: para qual processo devemos enviar o conteúdo de um pacote que chegou a este *host*?**



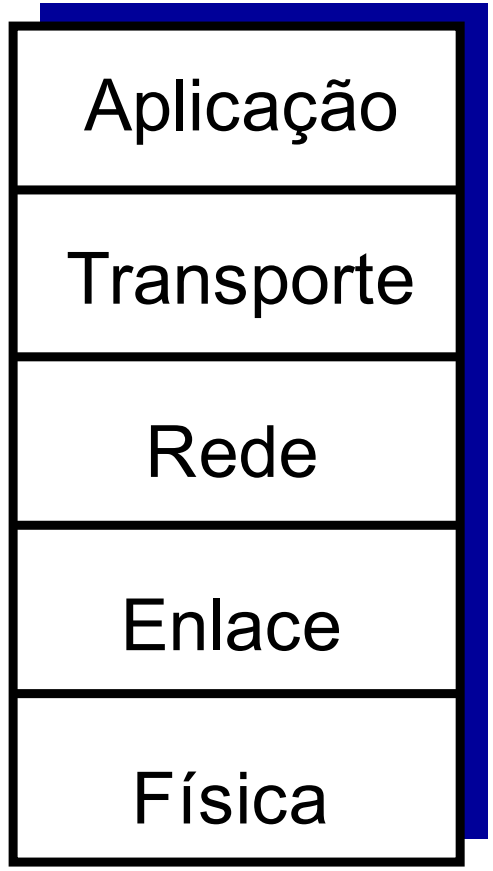
Pilha de Protocolos da Internet (IV)

- **Rede:** comunicação entre *hosts*.
  - Transfere dados de um *host* para outro.
  - Diferença (aparentemente) sutil em relação à camada de transporte.
    - Aquela comunicava processos específicos, diferenciando-os.
    - Esta comunica *hosts* indiscriminadamente.
  - Provê o serviço de roteamento dos pacotes.
    - Entre outros.
  - **Responde a pergunta: por qual caminho devemos enviar este pacote para que chegue ao *host* de destino?**



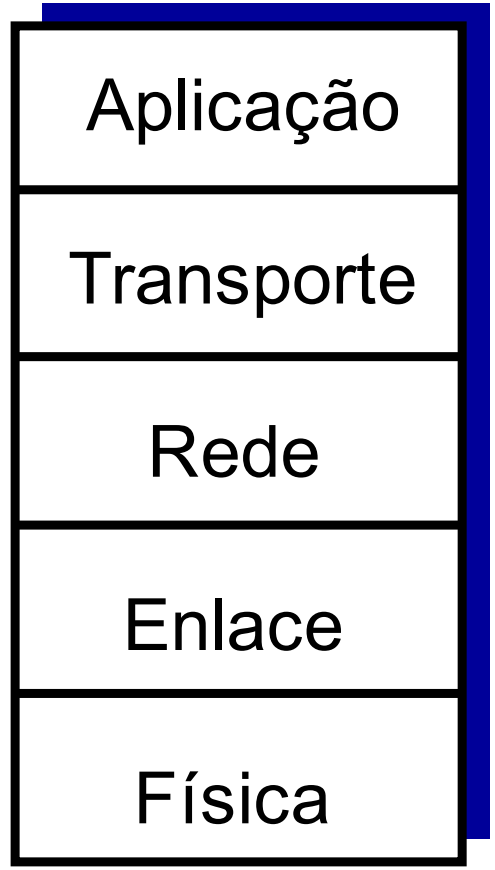
Pilha de Protocolos da Internet (V)

- **Enlace:** comunicação nós (*hosts*, comutadores) diretamente conectados por um enlace.
  - *i.e.*, nós "vizinhos".
  - Diferente da camada de rede, preocupação apenas com **próximo salto**.
    - Aspectos relacionados à transmissão do pacote pelo enlace.
  - Exemplo de serviço: integridade.
    - Em enlaces susceptíveis a falhas, verifica se houve bits errados na recepção pelo enlace.
  - **Responde a pergunta: como envio o pacote para o próximo dispositivo no caminho?**



Pilha de Protocolos da Internet (VI)

- **Física:** representação do pacote no meio físico de transmissão.
  - Traduz bits para sinais.
    - Pulsos elétricos, ondas acústicas, pulsos de luz, ...
  - Se preocupa com a forma mais eficiente de representação.
    - *e.g.*, como transmitir mais bits em menos tempo no canal?
    - *e.g.*, como minimizar os erros na transmissão?



Pilha de Protocolos: Uma Visão *Bottom-Up*

- Cada camada assume que camadas inferiores resolvem "uma parte do problema".
  - Sobre a solução existente, são adicionadas novas funcionalidades.
- Exemplo (simplificado):
  - Camada de enlace assume que sabemos enviar bits por um enlace.
    - Preocupa-se em verificar se bits chegaram corretos.
  - Camada de rede assume que sabemos enviar pacote entre nós diretamente conectados.
    - Preocupa-se em encontrar e usar caminhos de múltiplos saltos entre origem e destino.
  - Camada de transporte assume que sabemos enviar pacote entre origem e destino.
    - Preocupa-se em separar pacotes que chegam entre os vários processos do *host*.
  - Camada de aplicação assume que sabemos enviar pacotes entre processos em computadores diferentes.
    - Preocupa-se em gerar mensagens que permitam o funcionamento da **aplicação distribuída**.

Pilha de Protocolos: Uma Visão *Top-Down* (I)

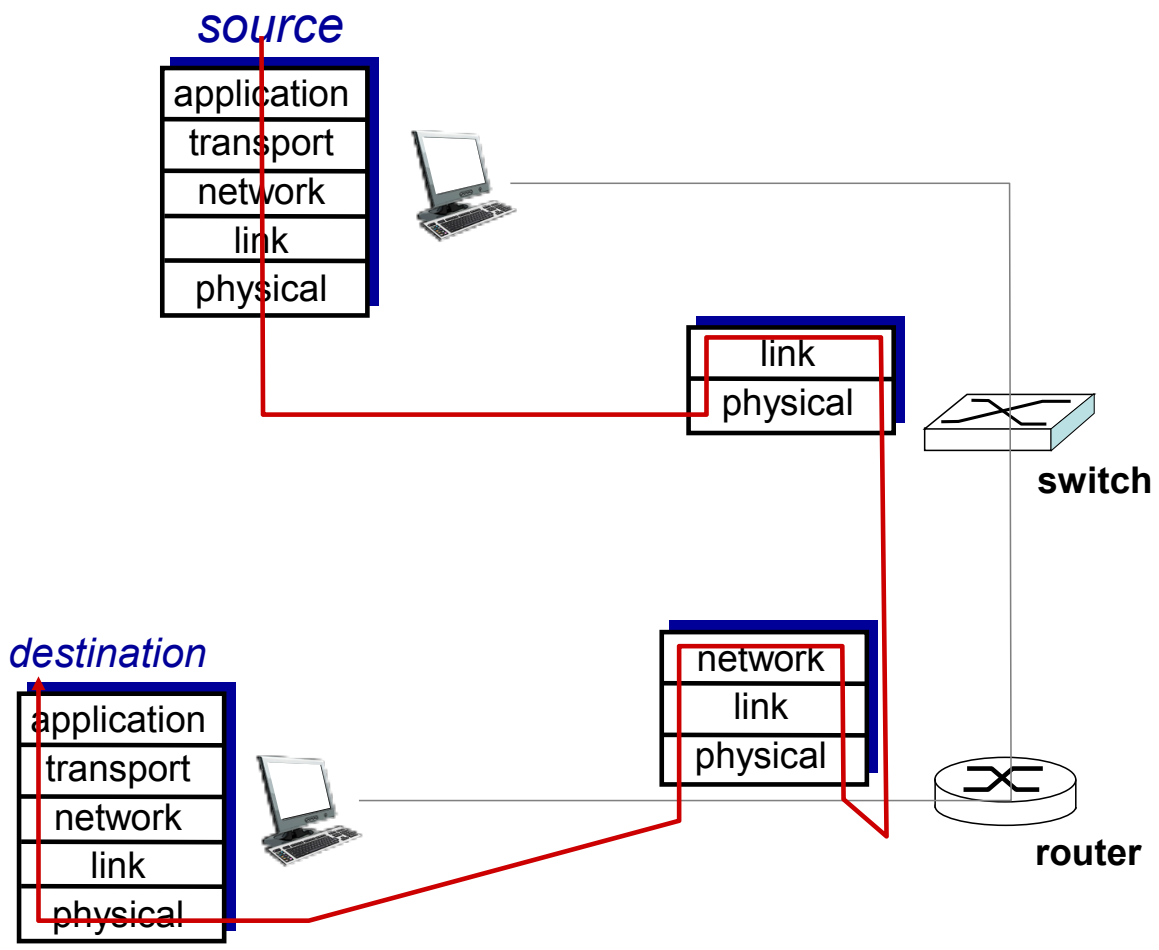
- Estratégia utilizada pelo livro-texto.
- Estudar as redes de computadores (Internet, em particular) percorrendo camadas de cima para baixo.
  - Aplicação – Capítulo 2.
  - Transporte – Capítulo 3.
  - Rede – Capítulo 4.
  - Enlace – Capítulo 5.
- No restante desta disciplina, estudaremos as várias camadas da pilha TCP/IP.

O Modelo de Referência ISO/OSI

- Modelo TCP/IP não é o único, absoluto.
- Uma alternativa: modelo OSI.
  - Sete camadas, ao invés de 5/4.
  - **Apresentação:** "traduz" formato dos dados entre a aplicação e a rede.
    - *e.g.*, criptografia, compressão, *endianess*.
  - **Sessão:** provê funcionalidades como sincronização, *checkpoints*, recuperação de dados.
- Como a Internet lida com a ausência destas camadas?
  - Funcionalidades implementadas na aplicação, **se necessárias**.
  - São necessárias?

Inteligência nas Bordas e Camadas

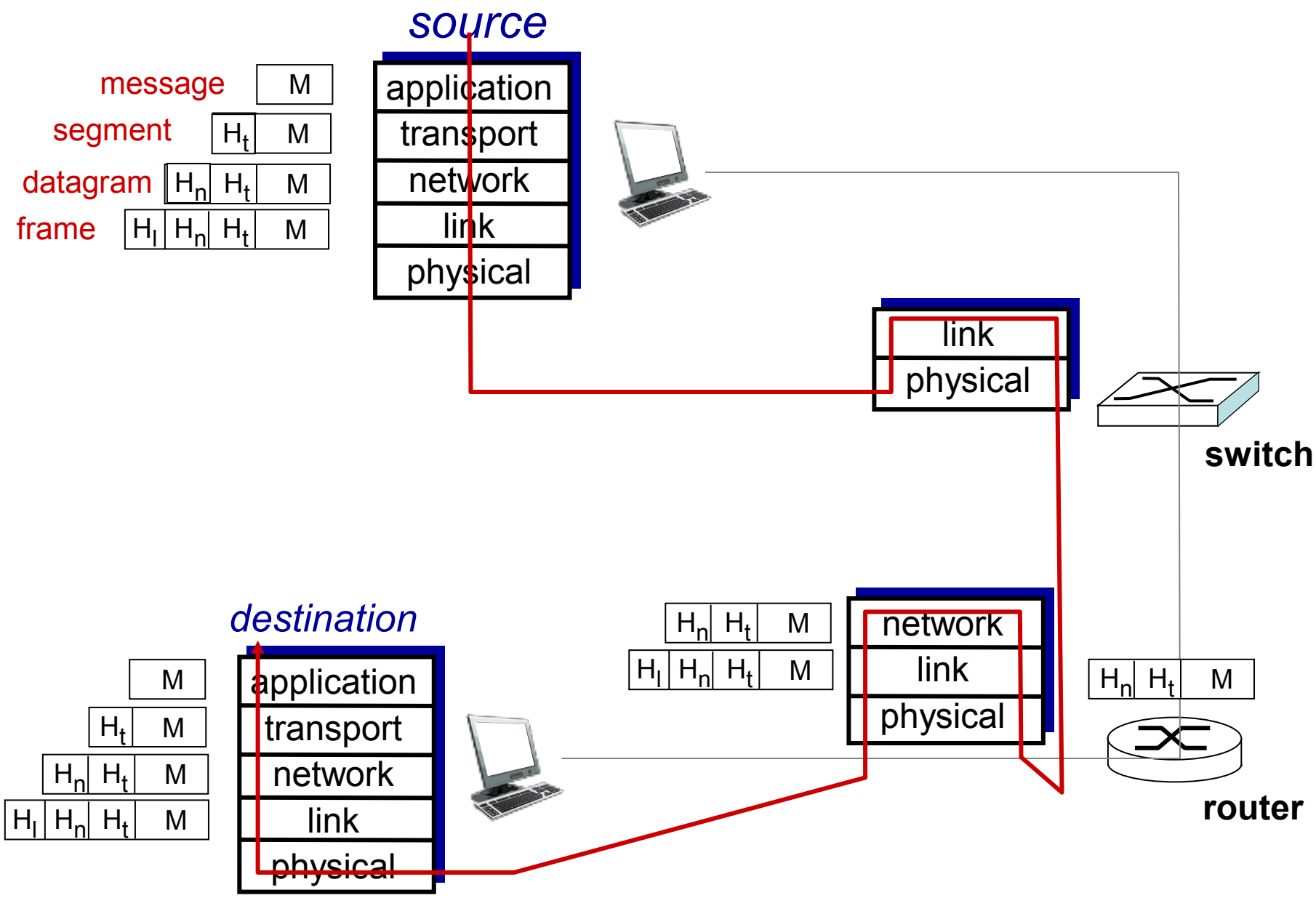
- Lembrando: na Internet, procura-se manter a inteligência nas bordas.
  - *i.e.*, na medida do possível, funcionalidades são mantidas nas bordas, e não no núcleo.
  - Argumento fim-a-fim.
- Isto se manifesta (idealmente) na organização em camadas.
  - *Hosts* implementam todas as camadas.
  - Comutadores implementam apenas as 2 ou 3 mais baixas.
    - *Switches* até a camada 2.
    - Roteadores até a camada 3.



Encapsulamento e Cabeçalhos (I)

- Pacotes são gerados (normalmente) na aplicação e descem pelas demais camadas.
- Cada nova camada pode precisar adicionar informações ao pacote para cumprir suas responsabilidades.
  - *e.g.*, camada de transporte adiciona um identificador ao pacote para que receptor saiba para qual processo este é destinado.
- Informações adicionais são colocadas em posições bem definidas do pacote.
  - Em **cabeçalhos**.
- Cada camada pode adicionar (e geralmente adiciona) seu cabeçalho à mensagem.
  - Com suas informações relevantes.

Encapsulamento e Cabeçalhos (II)



Segurança

Segurança em Redes

- **Campo que estuda**:
  - Como atacantes podem gerar problemas para a rede/computadores.
  - Como podemos nos defender destes ataques.
  - Como projetar a arquiteturas de redes imunes a ataques.
- Internet **não foi** originalmente pensada com (muita) segurança em mente.
  - Visão original: "grupo de usuários que confiam uns nos outros conectados a uma rede transparente".
  - Projetistas de protocolos da Internet estão sempre "correndo atrás".
  - Considerações de segurança aparecem em todas as camadas!

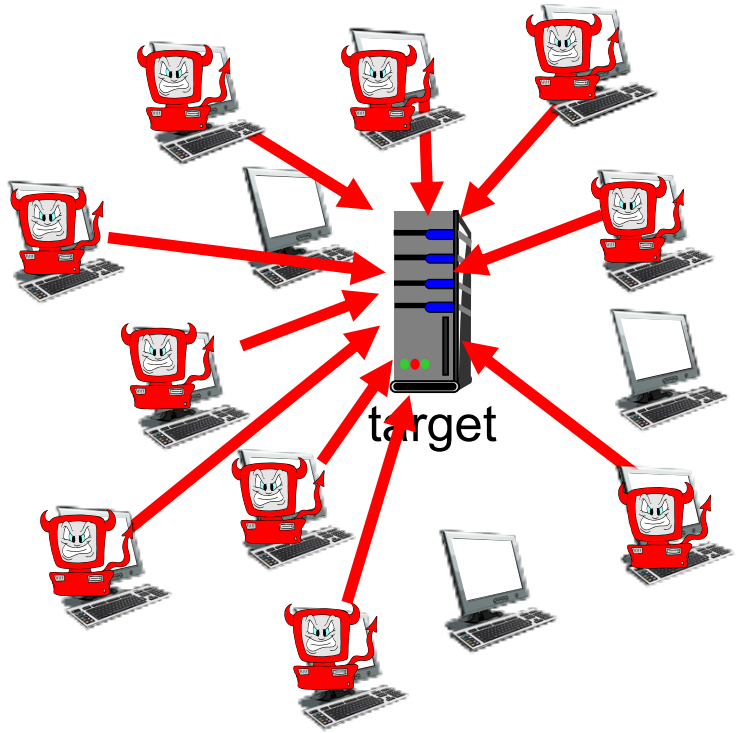
Atacantes: Inserção de *malware* nos *hosts* via Internet

- *Malware* pode infectar um *host* de algumas formas.
  - **Vírus:** *software* que se auto-replica através da recepção/execução de objetos pela rede (*e.g.*, anexo em e-mail).
  - **Worm:** *software* que se auto-replica através do recebimento/execução **passivos** (*e.g.*, automáticos) de um objeto.
- Um *malware* do tipo **spyware** pode gravar ações do usuário (*e.g.*, teclas pressionadas, páginas visitadas) e enviar para servidor do atacante.
- *Host* infectado pode ser controlado como parte de uma ***botnet***.

Ataques a Servidores, Infraestrutura de Rede

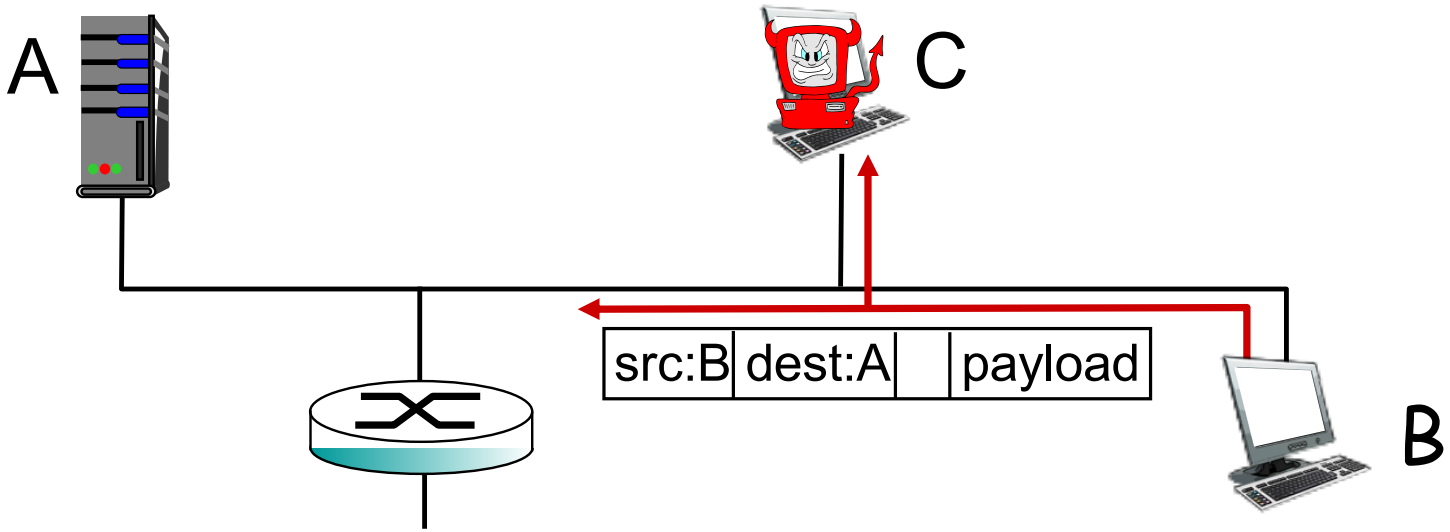
- **Ataque de Negação de Serviço:**
  - *Denial of Service* (DoS).
  - Atacante faz com que recurso (servidor, banda) fique indisponível para os usuários legítimos.
  - Normalmente, se basea na geração de tráfego artificial em grandes volumes, ocupando os recursos.

1. Selecionar o alvo.
2. Comprometer *hosts* pela rede (*i.e.*, criar uma *botnet*).
3. Enviar pacotes para o alvo a partir dos *hosts* comprometidos.
   - Mais de um *host* → DDoS.



Sniffing de Pacotes

- Normalmente, interfaces só passam para as camadas superiores quadros destinados ao próprio dispositivo.
- Mas, fisicamente, interface muitas vezes recebe quadros para outros nós.
  - *e.g.*, enlaces compartilhados.
- *Softwares* especiais podem capturar e exibir estes pacotes.
  - *Sniffers* de pacotes, como o Wireshark.



- Também utilizados para fins legítimos!

Histórico

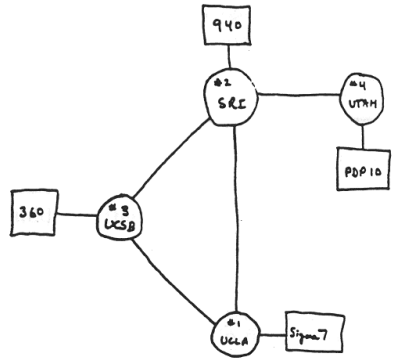
História da Internet (I)

1961 a 1972

Estabelecimento dos princípios da comutação de pacotes

- **1961:** Kleinrock mostra através de teoria das filas a efetividade da comutação de pacotes.
- **1964:** Comutação de pacotes é aplicada a redes militares.
- **1967:** Concepção da ARPAnet pela ARPA.
- **1969:** primeiro nó operacional da ARPAnet.

- **1972:**
  - Primeira demonstração pública da ARPAnet.
  - NCP (*Network Control Protocol*).
  - Primeiro programa de e-mail.
  - ARPAnet chega a 15 nós.



THE ARPA NETWORK

História da Internet (II)

1972 a 1980

Intercomunicação entre redes, redes novas e proprietárias

- **1970:** ALOHAnet no Havaii.
- **1974:** Cerf e Kahn definem arquitetura para intercomunicação de redes.
- **1976:** Ethernet é criado na Xerox PARC.
- **Final de 1970:** Arquiteturas proprietárias (DECnet, SNA, XNA).
- **Final de 1970:** Comutação de pacotes de comprimento fixo (precursor do ATM).
- **1979:** ARPAnet com 200 nós.

Princípios de intercomunicação de redes segundo Cerf e Kahn:

- Minimalismo, autonomia: evitar mudanças nas redes interconectadas.
- Modelo de serviço de **melhor esforço**.
- Roteadores ***stateless***.
- Controle descentralizado.

Definem a arquitetura da Internet atual

História da Internet (III)

1980 a 1990

Novos protocolos, proliferação de redes

- **1983:** Implantação do TCP/IP.
- **1982:** Protocolo de e-mail SMTP definido.
- **1983:** Protocolo DNS é definido para tradução de nomes.
- **1985:** Protocolo FTP é definido.
- Novas redes nacionais surgem nos EUA: Csnet, BITnet, NSFnet, Minitel.
- 100000 *hosts* conectados a confederação de redes.

História da Internet (IV)

1990 a 2005

Comercialização, a web, novas aplicações

- **Início de 1990:** ARPAnet é desativada.
- **1991:** NSF retira restrições de uso comercial da NSFnet.
- **Início de 1990:** Surgimento da Web.
  - Hipertexto.
  - HTML e HTTP: Berners-Lee.
  - 1994: Mosaic, mais tarde Netscape.
  - Fim da década 1990: comercialização da web.
- **Fim de 1990 a meados de 2000:**
  - Mais aplicações populares: mensagens instantâneas, transferência de arquivos via P2P.
  - Foco maior em segurança.
  - Estimativas de 50 milhões de *hosts*, mais de 100 milhões de usuários.
  - *Links* de *backbone* a Gb/s.

História da Internet (V)

2005 – presente

Expansão, aumento de escala, multimídia, dispositivos móveis.

- Aproximadamente 900 milhões de *hosts* (2012).
  - *Tablets*, *smartphones*, ...
  - Implantação agressiva de acesso banda larga.
  - Acesso à Internet sem fio se tornando ubíquo.
  - Surgimento das redes sociais.
    - Facebook: 1,65 bilhões de usuários (2016).
  - Servidores de conteúdo criam suas próprias redes.
    - "Evitam" Internet pública, entregam conteúdo de forma "instantânea": buscas, e-mail, vídeos.
  - Empresas, universidades, comércio eletrônico rodando seus serviços na "nuvem" (*e.g.*, EC2 da Amazon).