CRIPTOGRAFIA

- **Plano de Aulas:**
  - Modelo OSI;
  - Arquitetura TCP/IP;
  - Wireshark.

MODELO OSI

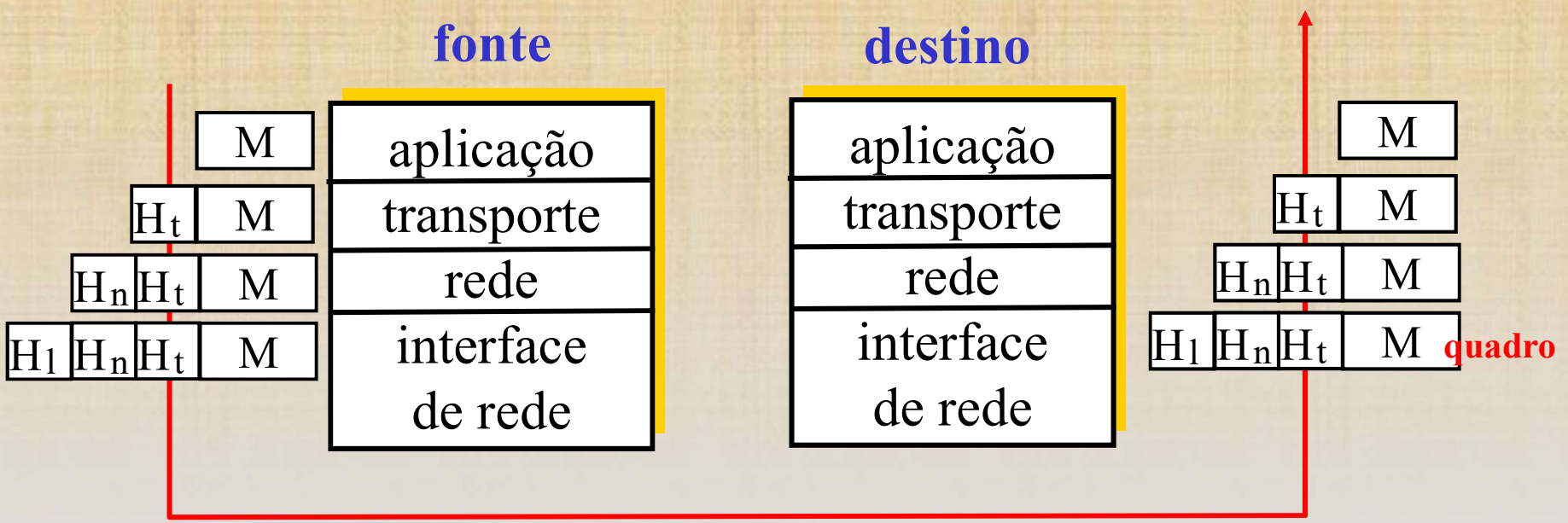
- Nas últimas décadas houve um aumento na quantidade de redes;
- Redes criadas com implementações diferentes de *hardware* e *software;*
- Como resultado, redes incompatíveis com diferentes especificações;
- Foi criado o ISO (*International Organization for Standardization*) para pesquisar sobre vários tipos de redes, abandonando os sistemas proprietários para utilizarem os sistemas abertos;
- Criação do modelo OSI (*Open Systems Interconnection*) pela ISO em 1984 para garantir interoperabilidade entre várias tecnologias de redes, criados por várias empresas de todo o mundo.

MODELO OSI

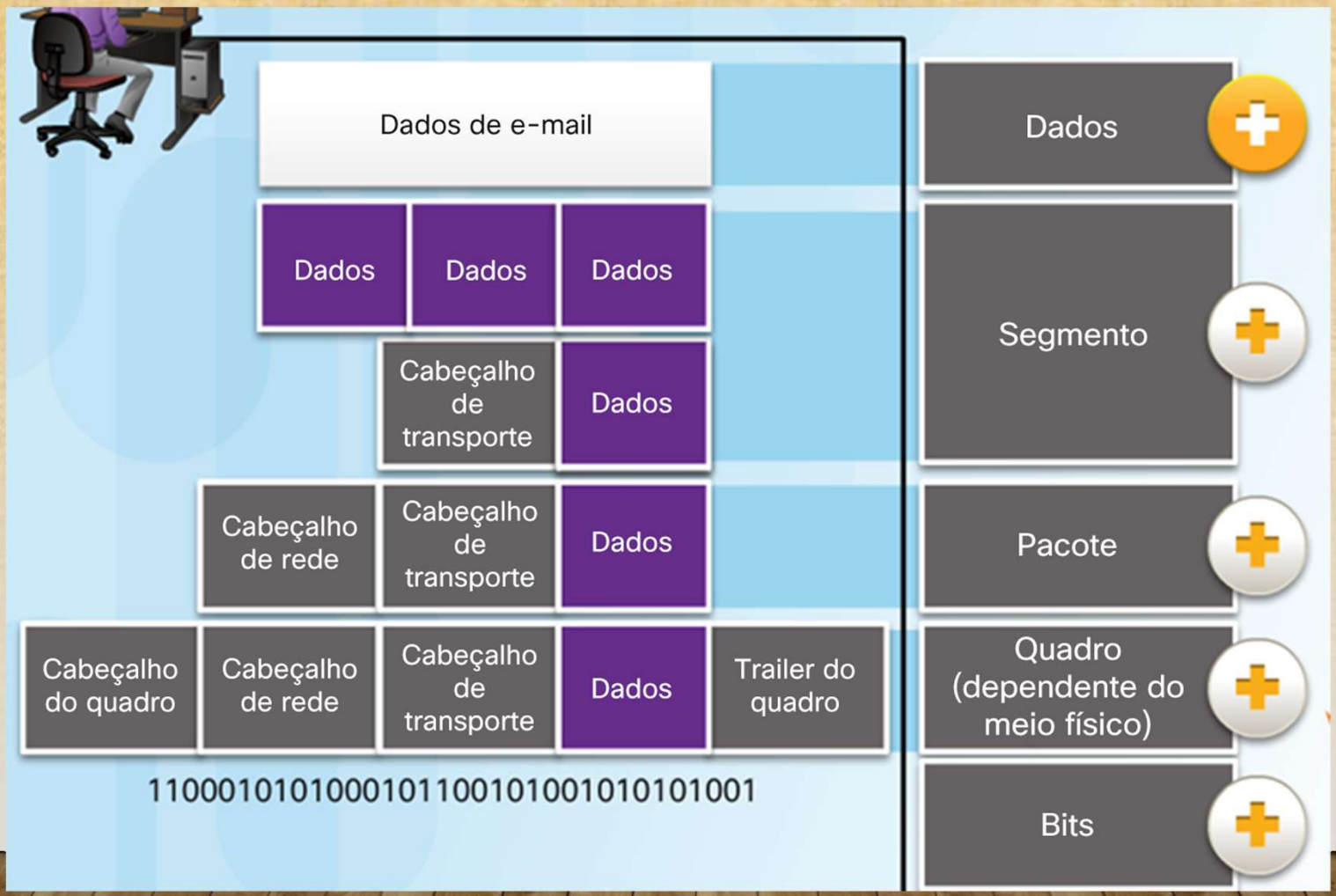
7.*Aplicação*	7.Aplicações do usuário (HTTP, SMTP), APIs, serviços de rede (DNS, DHCP)
6.Apresentação	6.Compressão, formatação e representação dos dados (ASCII, jpeg, criptografia)
5.*Sessão*	5.Sincronismo de diálogo, gerenciamento de sessão (sockets)
4.*Transporte*	4.Controle da QoS global, controle de fluxo, recuperação de erro, multiplexação
3.Rede	3.Endereçamento e roteamento
2.Enlace	2.Estabelecimento do enlace de dados, detecção de erros, delimitação de quadros
1.Física	1.Acesso ao meio de transmissão, interface física e elétrica, ativação da conexão.

ENCAPSULAMENTO DE DADOS

- Cada camada recebe dados de cima
- acrescenta um cabeçalho de informação para criar uma nova unidade de dados
- passa a nova unidade de dados para a camada abaixo



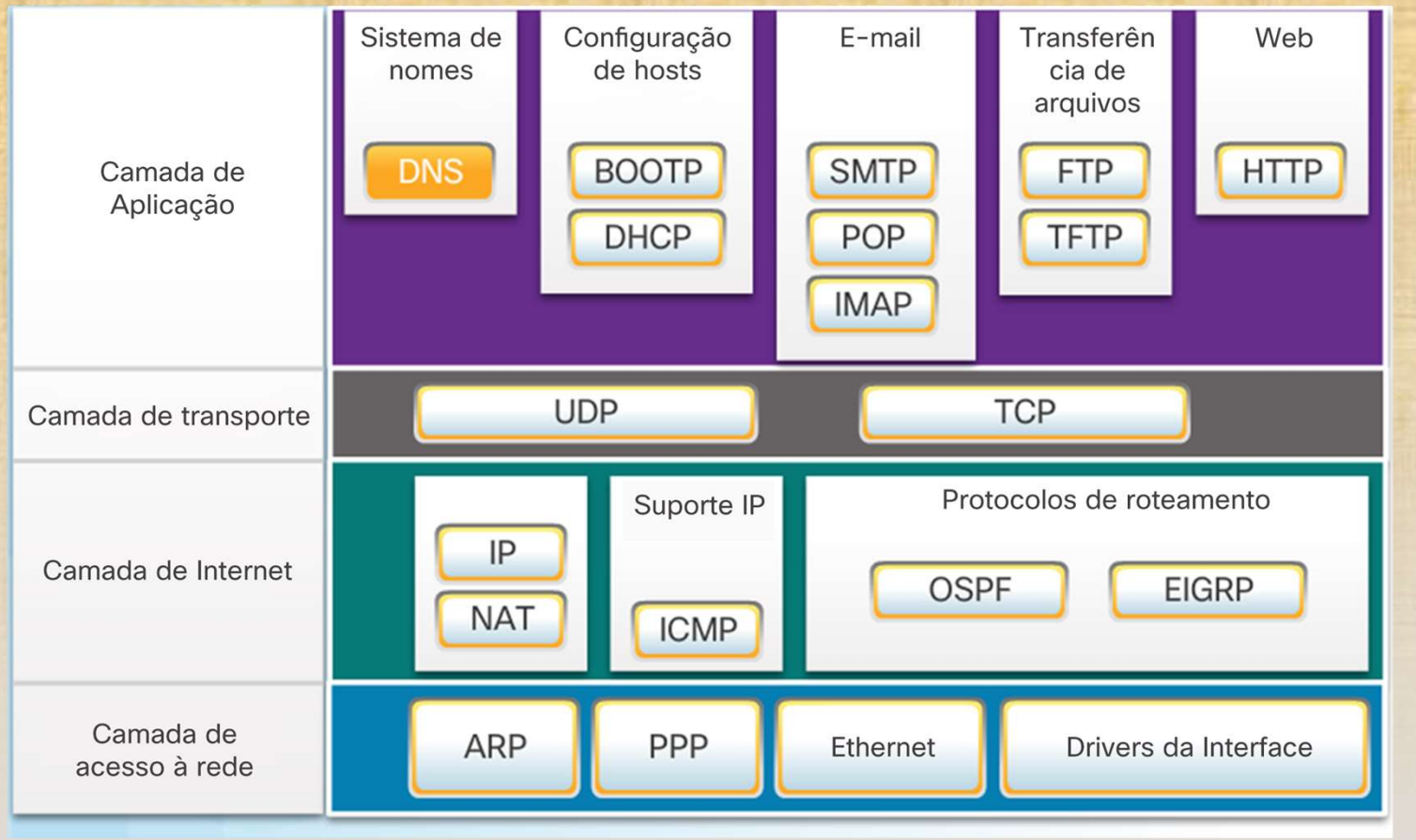
ENCAPSULAMENTO DE DADOS



ARQUITETURA TCP/IP

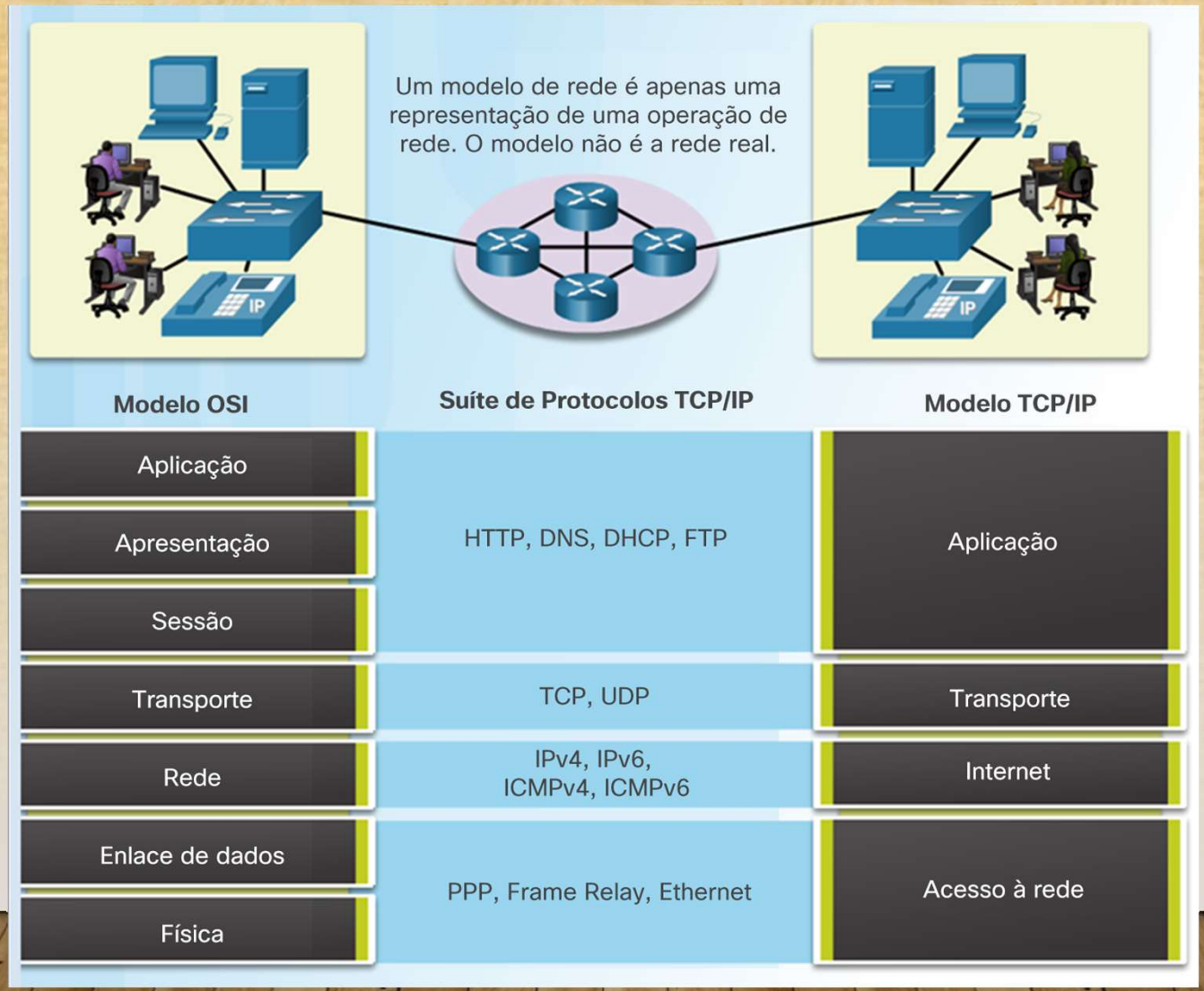
- O desenvolvimento do protocolo TCP/IP começou em 1969, com o projeto ARPANET, da Agência de Projetos de Pesquisas Avançadas do Departamento de Defesa dos Estados Unidos.
- O objetivo desse projeto foi desenvolver uma rede que interligasse os computadores do governo americano, de diferentes fabricantes e utilizando diferentes sistemas operacionais.
- Essa rede deveria ser descentralizada e mesmo que um dos computadores dessa rede fosse destruído por um eventual ataque militar, os demais continuariam a funcionar normalmente, graças a um mecanismo de rotas alternativas.
- Desses projetos surgiu o protocolo TCP/IP, que serviu de alicerce para a construção da rede que conhecemos como Internet.

ARQUITETURA TCP/IP



ARQUITETURA TCP/IP

MODELO DE CAMADAS



EXERCÍCIO

Núm. OSI	Nome da camada OSI	Núm. TCP/IP	Nome da camada TCP/IP	Unidade Encapsul.	Protocolos TCP/IP em cada camada TCP/IP	Utilitários TCP
7						
6						
5						
4						
3						
2						
1						

DEFINIÇÃO DO WIRESHARK

- **O que é o *Wireshark* e como funciona?**
  - É um analisador de protocolos de rede mais usado no mundo;
  - Captura pacotes na rede, decodifica esses pacotes em um formato de fácil interpretação e de modo interativo;
  - Usado para ambiente educacional e administradores de rede.

HISTÓRICO DO WIRESHARK

- **Em 1998 Gerald Combs necessitava de uma ferramenta para monitoramento de rede e desenvolveu o *Ethereal*;**
- **Primeira versão atualizada em julho de 1998 (v.0.2.0);**
- **Em Maio de 2006 passou a se chamar *Wireshark*, mantida por Gerald Combs, uma equipe de desenvolvimento e contribuidores.**

CARACTERÍSTICAS DO WIRESHARK

- **É distribuído sob licensa *open-source* GPL (*General Public License*);**
- **Captura em tempo real e análise *off-line;***
- **Multiplataforma (*Windows, Linux, OS X, Solaris, FreeBSD, NetBSD*, entre outras);**
- **Suporta mais de 750 protocolos (pilha TCP/IP, IEEE 802.11, *Bluetooth*, VOIP, USB);**
- **Reconhece (lê e escreve) diferentes formatos de captura (*tcpdump, libcap, NetMon, LanAnalyser*);**
- **Suporte a protocolos e sistemas seguros (IPSec, *Kerberos*, ssh, SSL/TLS, WEP, WPA/WPA2).**

APLICAÇÕES E CAPTURAS

- **Estudo de protocolos usado na pilha TCP/IP;**
- **Medidas e avaliação de desempenho;**
- **Vunerabilidades em protocolos de rede (http);**
- **Protocolos da camada de rede (ICMP – ping);**
- **Protocolos da camada de transporte (TCP e UDP);**
- **Protocolos seguros (SSL/TLS);**
- **Chamadas de VOIP.**