# A1. Principais Protocolos de Rede

M2.PROTOCOLOS E SEGURANÇA DE REDES

Prof. Esp. William C. Augustonelli (Billy)
william.augustonelli@docente.senai.sp – 1s2025

# Objetivo

- Capacitar os alunos a identificar, entender e aplicar os principais protocolos de rede em cenários reais e simulados
- Reconhecer suas funções e importância na comunicação entre dispositivos.

# Nossa aula de hoje...

- Introdução aos Protocolo de Rede
  - Atividade Prática 1 – Visualização de Tráfego de Pacotes no Packet Tracer
  - Atividade Prática 2 – Queda de DNS no Packet Tracer
- Principais Protocolos de Comunicação
  - Exemplos explicativos
  - Atividade Prática 3 – Simulando Protocolo FTP no Packet Tracer
- Laboratório 1 – Análise de Protocolos HTTP/ HTTPS com Wireshark
- Laboratório 2 – Análise de Protocolo DNS com Wireshark
- Laboratório 3 – Análise de Protocolo ICMP com Wireshark
- Laboratório 4 – Análise de Protocolo TCP e UDP com Wireshark
- Laboratório 5 – Packet Tracer com Serviços
- Segurança Básica e Protocolos

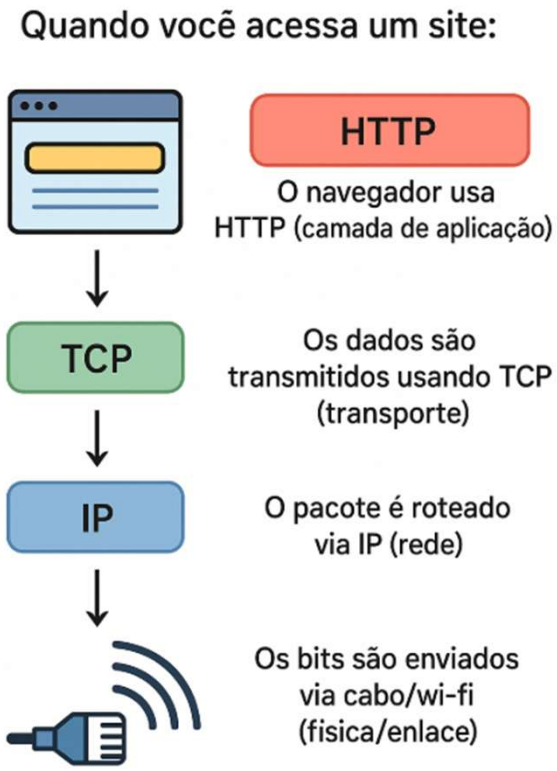
# Introdução aos Protocolos de Rede

- ***O que é um protocolo de rede?***
  - Um **protocolo de rede** é um **conjunto de regras e padrões** que definem como os dispositivos de uma rede devem **se comunicar entre si**.
  - Ele garante que a informação enviada de um computador seja compreendida corretamente pelo outro

- ***Por que os protocolos são importantes?***
  - ✓Garantem comunicação padronizada
  - ✓Permitem interoperabilidade entre diferentes fabricantes
  - ✓Facilitam a escalabilidade da internet e das redes privadas
  - ✓São essenciais para segurança, integridade e entrega de dados

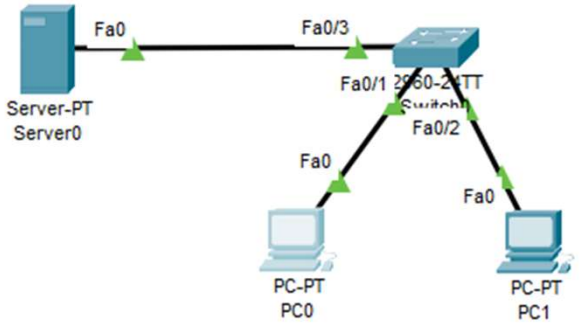
# Introdução aos Protocolos de Rede

- **Exemplo,** quando acessamos um site:
  1. O navegador utiliza HTTP (camada de aplicação)
  2. O dados são transmitidos usando TCP (camada de transporte)
  3. O pacote é roteado via IP (camada de rede)
  4. O bits são enviados via **cabo/ wi-fi** (camada física/ enlace)



# Atividade Prática 1 - Visualização de Tráfego de Pacotes no Packet Tracer

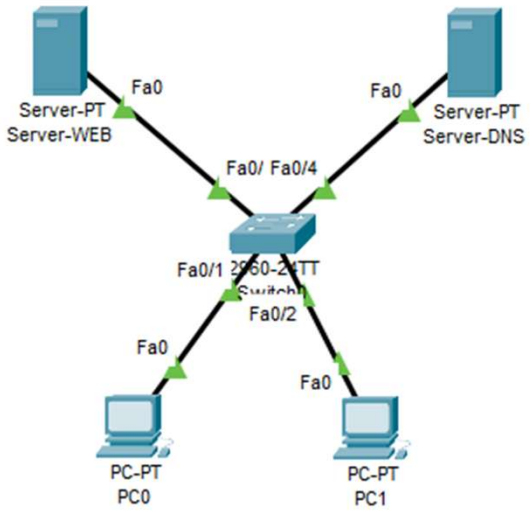
- **Cenário**
  - 2 PCs conectados a um Switch
  - Switch conectado a um Roteador
  - Um Servidor DNS, DHCP e HTTP habilitados
- **Agora vamos simular a entrega de pacotes**
  - **Simulação do DHCP**
  - **Simulação do DNS e HTTP/ HTTPS**




**Tire print dos resultados e salve!!!!**

# Atividade Prática 2 - Queda de DNS no Packet Tracer

- **Cenário**
  - 2 PCs conectados a um Switch
  - Switch conectado a um Roteador
  - Um Servidor DNS habilitado
  - Um Servidor DHCP habilitado
  - Um Servidor HTTP habilitado
- **Agora vamos simular a entrega de pacotes**
  - **Vamos simular a queda do DNS e ver como fica a entrega**




**Tire print dos resultados e salve!!!!**

# Principais Protocolos de Comunicação

- Protocolos de comunicação são regras padronizadas que **permitem a troca de dados entre dispositivos** de forma organizada, segura e eficiente.
- Cada protocolo tem um **propósito específico** e atua em uma ou mais **camadas** da rede (modelo OSI ou TCP/IP)

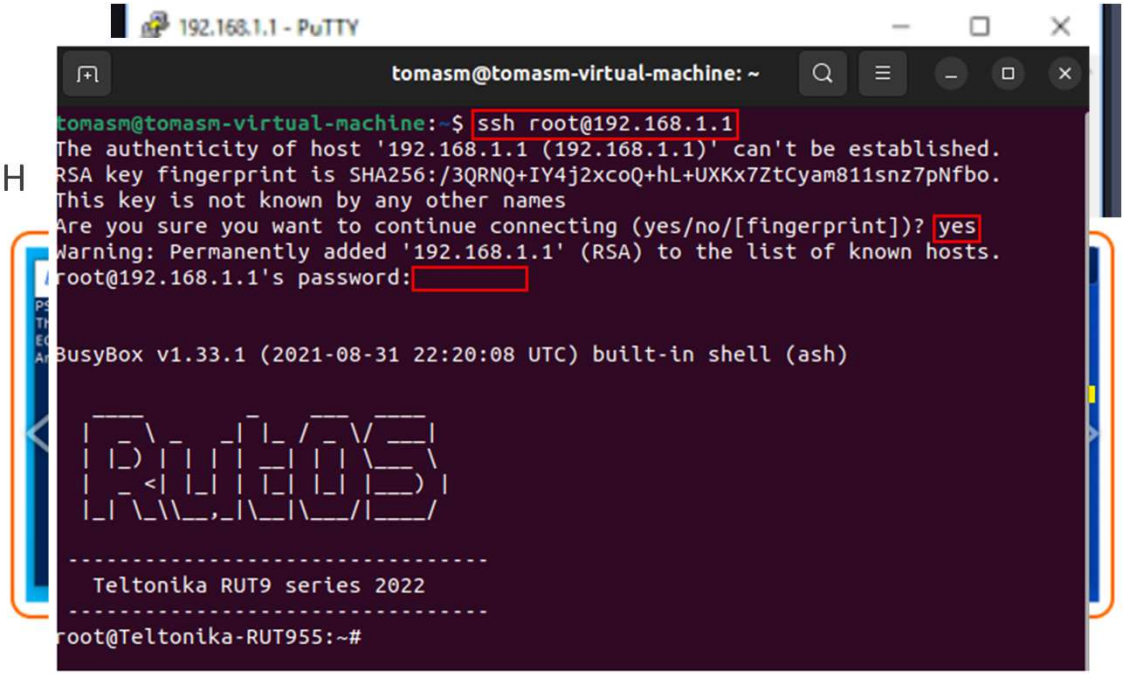
| Camada | Protocolo | Função |
|---|---|---|
| Aplicação | HTTP/HTTPS | Acesso a páginas web |
| Aplicação | DNS | Resolução de nomes |
| Aplicação | DHCP | Atribuição dinâmica de IP |
| Aplicação | FTP/SFTP | Transferência de arquivos |
| Aplicação | SMTP/POP3/IMAP | Envio/ Leitura de e-mails |
| Aplicação | SSH | Acesso remoto seguro |
| Transporte | TCP | Conexão confiável |
| Transporte | UDP | Conexão rápida |
| Rede | IP | Endereçamento e roteamento |
| Rede | ICMP | Diagnóstico (ex.: ping) |
| Enlace | ARP | Traduz IP em endereço MAC |

# Exemplos Explicativos

- HTTP vs HTTPS
  - HTTP → texto sem criptografia (porta 80)
  - HTTPS → criptografia com SSL/ TLS (porta 443)
- DNS
  - Converte nomes como www.google.com para IPs como 142.250.187.36
- DHCP
  - Atribui IP automaticamente ao dispositivo que se conectar à rede
  - Comando para renovar IP no Windows
    - Ipconfig /release
    - Ipconfig /renew

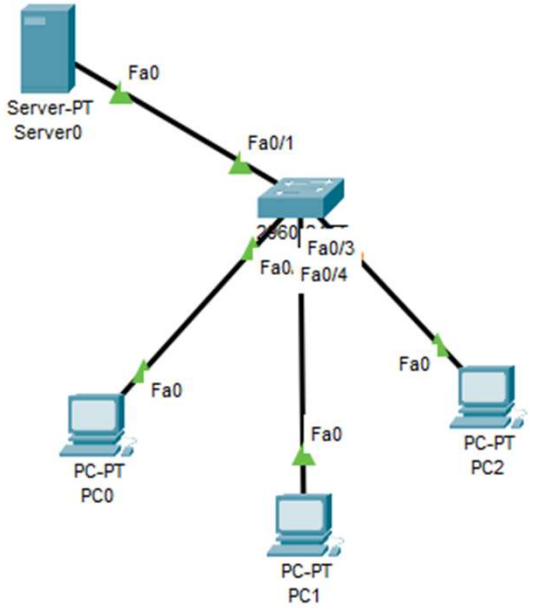
# Exemplos Explicativos

- FTP/ SFTP
  - FTP → porta 21, envia arquivos sem criptografia
  - SFTP → porta 22, envia arquivos baseado em SSH
- SSH
  - Acesso remoto via terminal
  - (Linux) ssh usuario@192.168.1.10
  - (PowerShell) ssh mint@laboratory.me -p 7777



# Atividade Prática 3 - Simulando o Protocolo FTP no Packet Tracer

- **Cenário**
  - Um servidor com DHCP, DNS, HTTP e FTP
  - 3 PCs
  - 1 Switch
- **Tarefas**
  1. Configurar o DHCP no servidor e verificar os IPs em PC0, PC1 e PC2
  2. Configurar o DNS e testar a resolução de nomes
  3. Acessar a página teste com navegador
  4. Acessar o FTP e baixar e enviar um arquivo (get e put)




**Tire print dos resultados e salve!!!!**

# Laboratório 1 – Análise de Protocolos HTTP/HTTPS com Wireshark

Relembrando...

- Wireshark é uma ferramenta gratuita de **captura e análise de pacotes de rede**.
- Ele permite ver **todo o tráfego que passa por uma interface de rede**, ajudando na detecção de problemas, análise de segurança e estudo de protocolos

1. Baixe o Wireshark e faça a instalação (caso não tenha no PC)
2. Abra e coloque para capturar pacotes
3. Acesse os sites: microsoft.com e http://httpforever.com
4. Volte ao Wireshark e pare a captura
5. Filtre por http analise os pacotes *request, response, headers*
6. Filte por tls ou ssl, analise os pacotes request, response, headers

**Tire print dos resultados e salve!!!!**

# Laboratório 2 – Análise de Protocolo DNS com Wireshark

1. Coloque o Wireshark para capturar pacotes
2. No prompt de comando, faça os seguintes comandos
   1. ipconfig /flushdns → limpa o cache de DNS
   2. nslookup www.uol.com.br
3. Volte no Wireshark e pare a captura
4. Filte por dns
5. Analise a requisição (*Query*) e resposta (*Response*), porta utilizada e tipo de registro solicitado

**Tire print dos resultados e salve!!!!**

# Laboratório 3 – Análise de Protocolo ICMP com Wireshark

1. Coloque o Wireshark para capturar pacotes
2. No prompt de comando, faça os seguintes comandos
    1. ping 8.8.8.8
3. Volte no Wireshark e pare a captura
4. Filte por icmp
5. Analise as mensagens *Echo Request* e *Echo Reply*, identificador e sequência

**Tire print dos resultados e salve!!!!**

# Laboratório 4 – Análise de Protocolo TCP e UDP com Wireshark

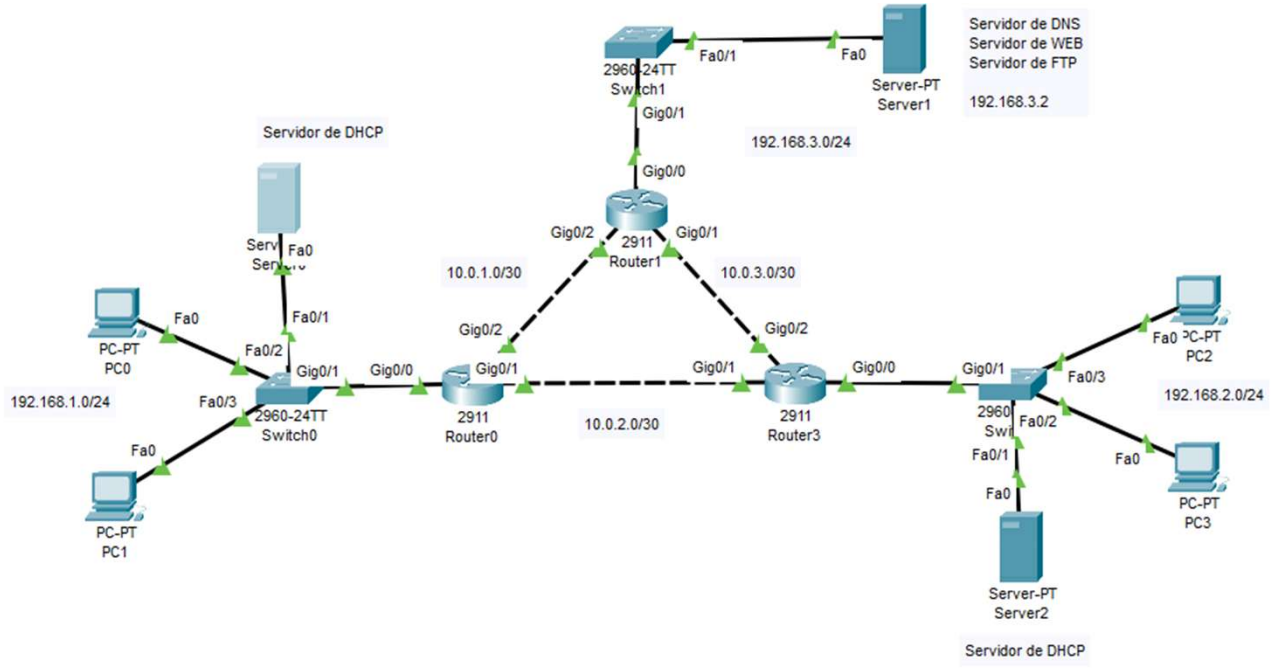
1. Coloque o Wireshark para capturar pacotes
2. No prompt de comando, faça os seguintes comandos
   1. telnet towel.blinkenlights.nl 23
   2. nslookup towel.blinkenlights.nl
3. Volte no Wireshark e pare a captura
4. Filtre por tcp, procure os pacotes enviados e recebidos para towel.blinkenlights.nl
5. Filtre por udp, procure os pacotes enviados e recebidos para towel.blinkenlights.nl

**Tire print dos resultados e salve!!!!**

# Laboratório 5 – Packet Tracer com Serviços

Montar um ambiente de rede no **Packet Tracer** que simule **serviços de rede reais**, como **DHCP, DNS, FTP e HTTP**, para observar e entender o funcionamento dos **principais protocolos de comunicação**, em um ambiente controlado

- **Parte 1 - Cenário de rede**
  - 1 roteador
  - 2 switches
  - 4 PCs
  - 2 Servidores com DHCP
  - 1 Servidor com DNS
  - 1 Servidor com HTTP e FTP



# Laboratório 5 – Packet Tracer com Serviços

- **Parte 2 – Teste de conectividade**

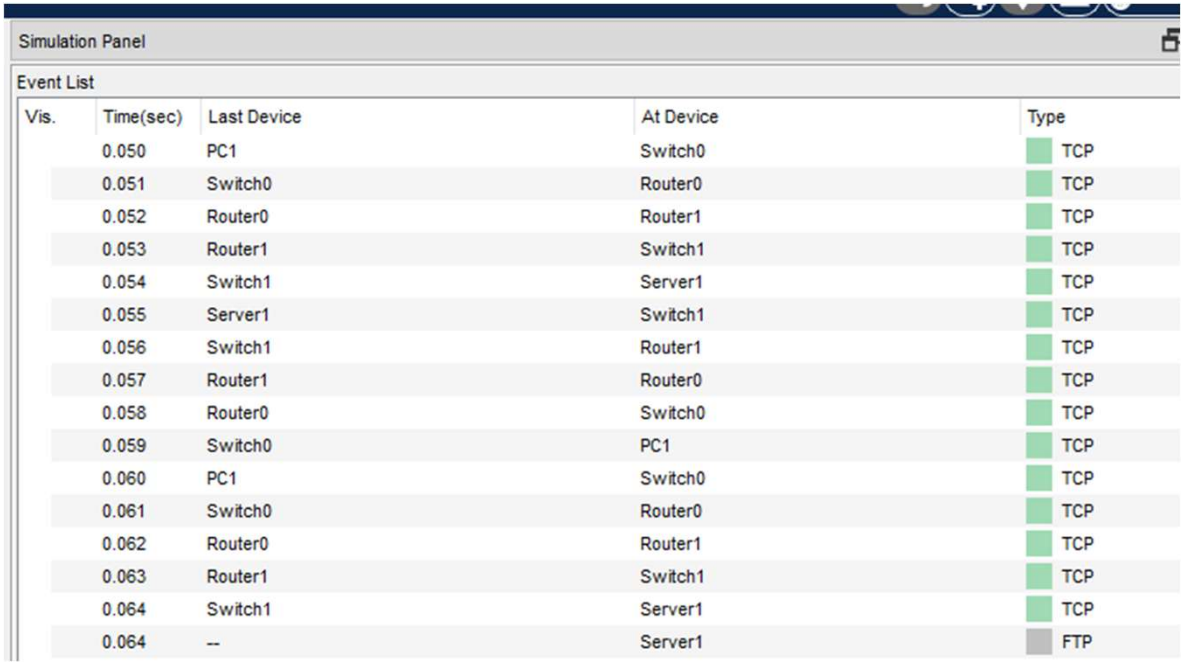
1. Verificação do DCHP
   - Conferir se os IPs foram atribuídos corretamente para cada rede
2. Teste de DNS e HTTP
   - Nos PCs acessar o site meusite.com
3. Teste de FTP
   - No PC > Desktop > Command Prompt
   - ftp ftp.local
   - Usuário cisco e senha cisco
   - dir

**Tire print dos resultados e salve!!!!**

# Laboratório 5 – Packet Tracer com  Serviços

➢ **Parte 3 – Modo de Simulação**

1. Troque o modo do Packet Tracer para **Simulation Mode**
2. Realize as seguintes ações
   1. Abrir o site meusite.com
   2. Executar o ftp ftp.local
3. Observar os protocolos envolvidos
   1. DNS
   2. TCP
   3. HTTP
   4. FTP
4. Clique em cada pacote para ver
   1. Origem/ destino
   2. Tipo de protocolo
   3. Camada do modelo OSI envolvido




| Vis. | Time(sec) | Last Device | At Device | Type |
|---|---|---|---|---|
| | 0.050 | PC1 | Switch0 | TCP |
| | 0.051 | Switch0 | Router0 | TCP |
| | 0.052 | Router0 | Router1 | TCP |
| | 0.053 | Router1 | Switch1 | TCP |
| | 0.054 | Switch1 | Server1 | TCP |
| | 0.055 | Server1 | Switch1 | TCP |
| | 0.056 | Switch1 | Router1 | TCP |
| | 0.057 | Router1 | Router0 | TCP |
| | 0.058 | Router0 | Switch0 | TCP |
| | 0.059 | Switch0 | PC1 | TCP |
| | 0.060 | PC1 | Switch0 | TCP |
| | 0.061 | Switch0 | Router0 | TCP |
| | 0.062 | Router0 | Router1 | TCP |
| | 0.063 | Router1 | Switch1 | TCP |
| | 0.064 | Switch1 | Server1 | TCP |
| | 0.064 | -- | Server1 | FTP |

**Tire print dos resultados e salve!!!!**

# Segurança Básica e Protocolos

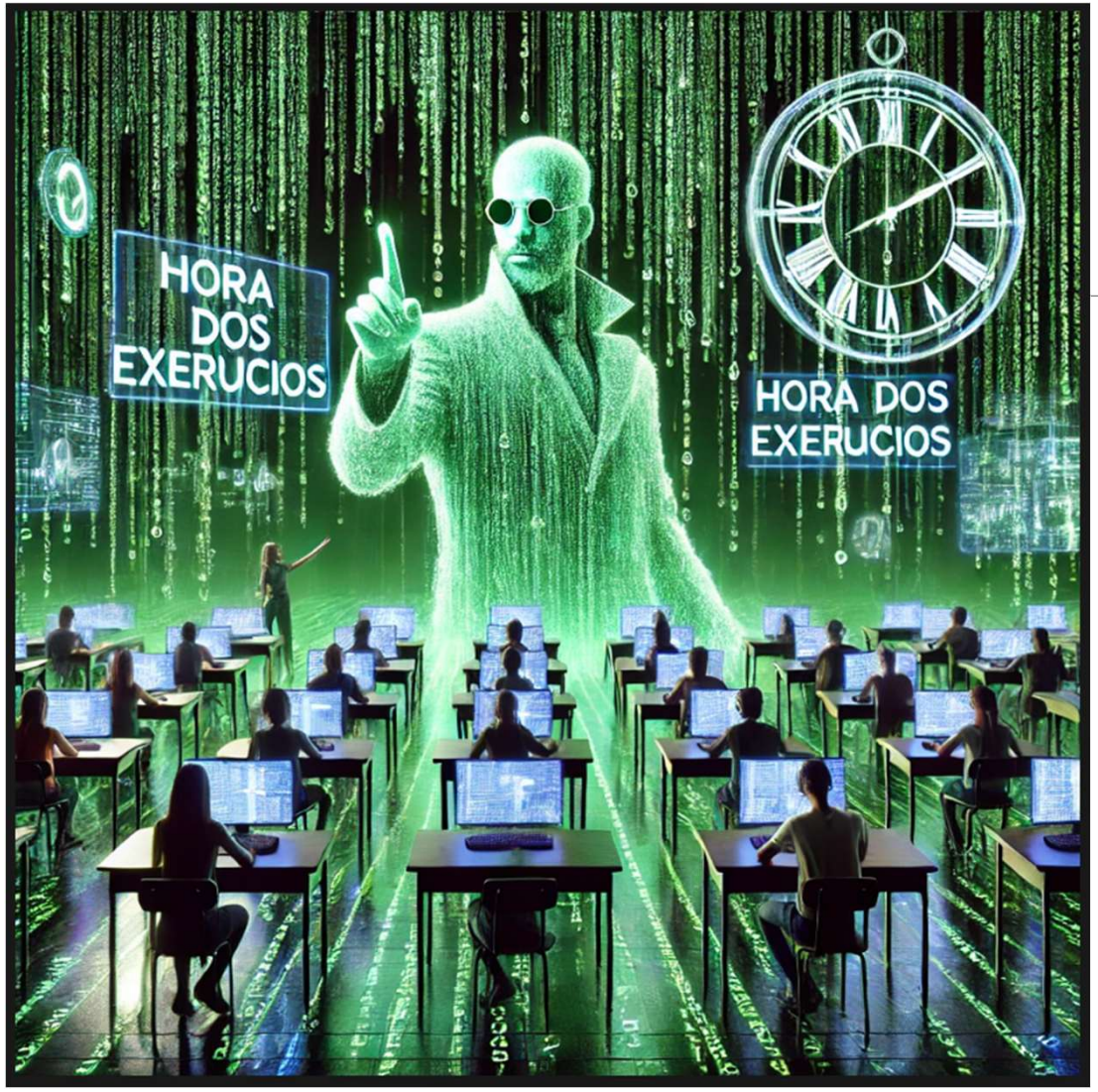
- ***O que é um protocolo seguro?***
  - Um protocolo seguro é aquele que **usa criptografia** e **mecanismos de autenticação** para proteger os dados transmitidos entre dispositivos

- **Propriedades de segurança desejáveis**
  - **Confidencialidade**: os dados não podem ser lidos por terceiros
  - **Integridade**: os dados não podem ser alterados sem detecção
  - **Autenticidade**: certeza da identidade do emissor

| Função | Inseguro | Seguro |
|---|---|---|
| Web | HTTP(80) | HTTPS(443) |
| Transferência | FTP(21) | SFTP(22) |
| Acesso Remoto | Telnet (23) | SSH (22) |

# Práticas de Segurança

- Nunca usar Telnet em redes públicas
- Preferir protocolos com S – HTTPS, SFTP, SSH
- Configurar firewall para bloquear portas inseguras
- Usar VPN para redes remotas
- Evitar salvar senhas em arquivos de texto




- Atividades no Classroom