Arquitetura de Redes

Serviços de Rede

Prof.: Caio Malheiros

caio.duarte@sp.senai.br

Definição de Serviços de Redes

- **O que são Serviços de Redes?**

- Serviços de rede são funcionalidades que permitem a comunicação, o acesso e a transferência de dados entre dispositivos em uma rede.

- São essenciais para o funcionamento de sites, transferência de arquivos e acessos remotos.

Por que os Serviços de Redes são Importantes?

- **Facilitam a conectividade** entre dispositivos locais e globais
- **Permitem o acesso remoto** e a **transferência** de **arquivos**
- **Aumentam a segurança dos dad**os **durante** a **comunicação**

Tipos de Serviços de Redes

- **Tipos de Serviços de Redes**

- Diferentes serviços atendem a propósitos variados e são projetados para contextos específicos, como transferência de arquivos, navegação e acesso remoto.

Protocolo FTP - File Transfer Protocol

- **FTP (Protocolo de Transferência de Arquivos)**
- Usado para **transferir arquivos** entre dispositivos.
- Ideal para enviar e receber arquivos grandes.
- Funcionamento: cliente FTP se conecta a um servidor FTP para download/upload.

Protocolo FTP - File Transfer Protocol

- **Exemplo de utilização:**

  Hospedagem de Site em um servidor.

HTTP/HTTPS - Hypertext Transfer Protocol

- **HTTP (Hypertext Transfer Protocol)** é o protocolo básico para troca de informações na web.

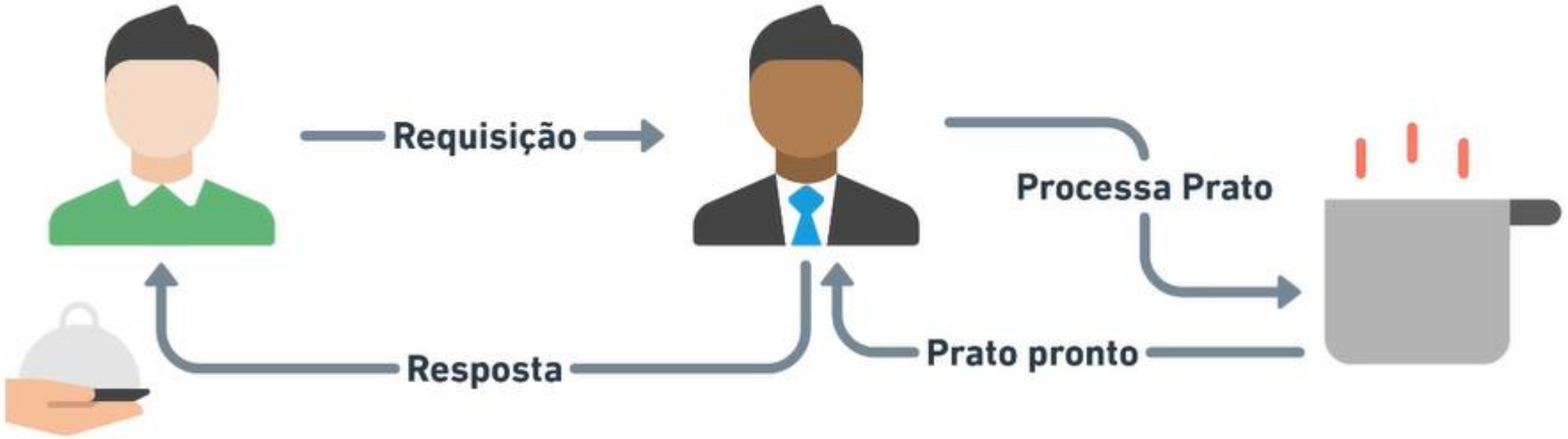
- Ele estabelece como os dados: (texto, imagens, vídeos) devem ser solicitados e entregues entre clientes (navegadores) e servidores web.

HTTP/HTTPS - Hypertext Transfer Protocol

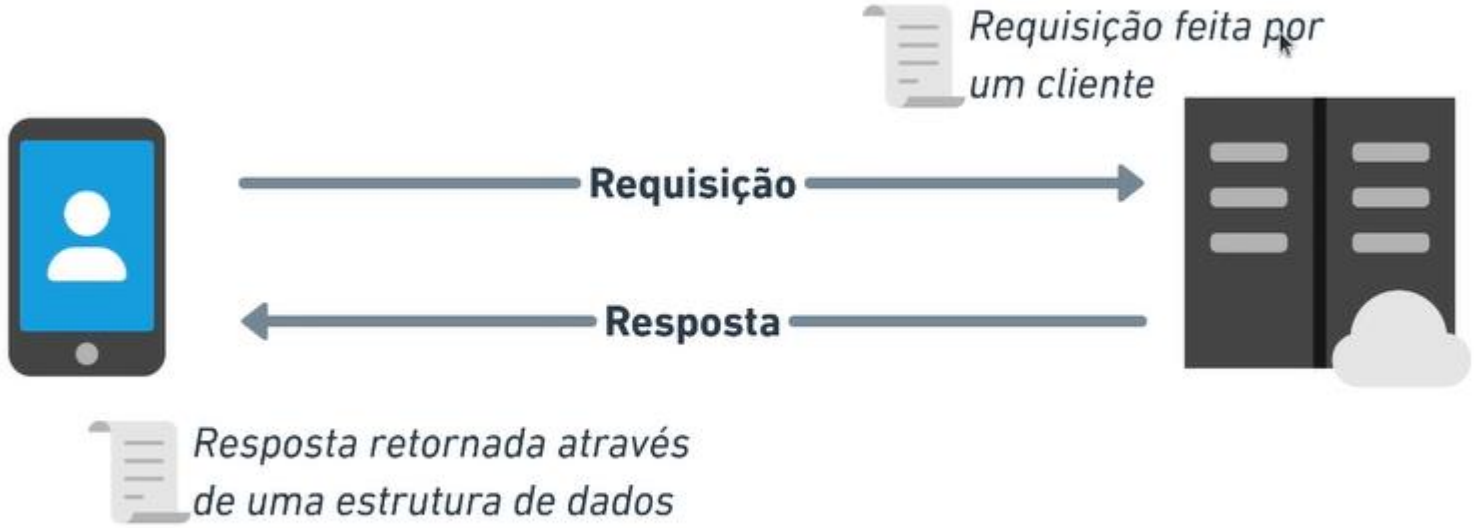
- **Como Funciona?**
- **Cliente-Servidor**: HTTP funciona em um modelo de cliente-servidor, onde o navegador (cliente) envia uma solicitação (request) e o servidor responde (response).

- **Conexão Stateless**: HTTP é um protocolo sem estado, ou seja, cada solicitação é independente. Isso significa que o servidor não mantém informações sobre a comunicação anterior.

HTTP/HTTPS – Como funciona?



HTTP/HTTPS – Como Funciona?



Tipos de Resposta – JSON vs XML


```json
{
  "cep": "18133-400",
  "logradouro": "Rua José Gomide de Castro",
  "complemento": "",
  "bairro": "Jardim Maria Trindade",
  "localidade": "São Roque",
  "uf": "SP",
  "ibge": "3550605",
  "gia": "6531",
  "ddd": "11",
  "siafi": "7113"
}
```


JSON


```xml
▼<xmlcep>
   <cep>18133-400</cep>
   <logradouro>Rua José Gomide de Castro</logradouro>
   <complemento/>
   <bairro>Jardim Maria Trindade</bairro>
   <localidade>São Roque</localidade>
   <uf>SP</uf>
   <ibge>3550605</ibge>
   <gia>6531</gia>
   <ddd>11</ddd>
   <siafi>7113</siafi>
 </xmlcep>
```


XML

https://viacep.com.br/

Métodos de Solicitação HTTP

- Métodos de Solicitação

- GET: Pede ao servidor para enviar um recurso (como uma página).
- POST: Envia dados para o servidor, geralmente usado em formulários.
- PUT: Atualiza um recurso existente.
- DELETE: Remove um recurso.

Estrutura de uma Requisição HTTP

- **URL**: Endereço da página ou recurso (ex: https://site.com/pagina).

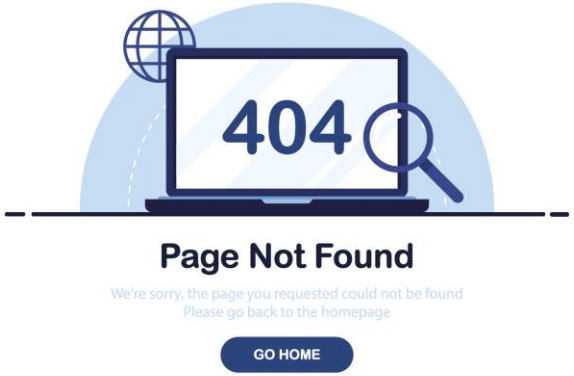
- **Cabeçalhos**: Contêm informações adicionais, como tipo de conteúdo, autorização, etc.

- **Corpo**: Pode conter **dados** adicionais (como em formulários POST).

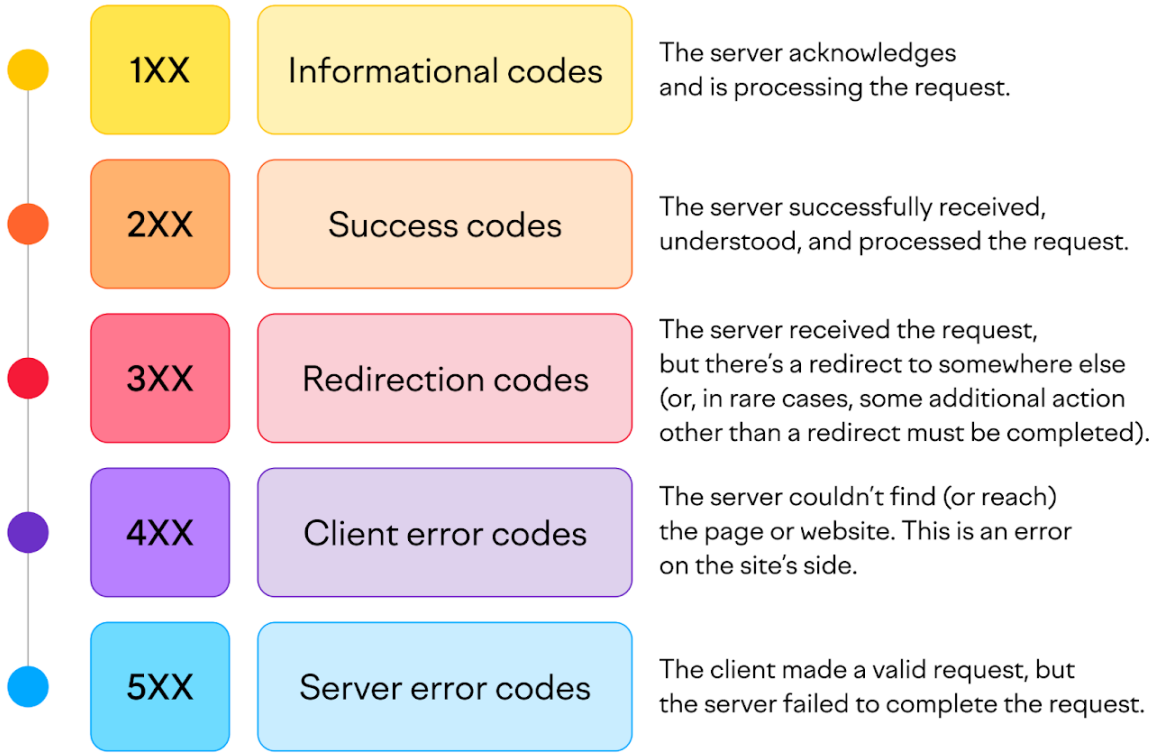
HTTP Status Codes

- **O que são HTTP Status Codes?**
- São códigos de resposta que indicam o status de uma solicitação HTTP.

- O servidor envia esses códigos para o navegador do cliente para informar se a solicitação foi bem-sucedida, se houve algum erro ou outra situação específica.



Principais Categorias de Status Codes:



Exemplos Comuns

- **200 OK:** Página carregada com sucesso.
- **404 Not Found:** Página não encontrada.
- **400 Bad Request**: Solicitação malformada; o servidor não consegue processar os dados enviados.
- **403 Forbidden**: Acesso negado.
- **500 Internal Server Error:** Erro interno do servidor.

Limitações do HTTP

- Uma das principais limitações do HTTP é a **falta de segurança**.

- Todo o tráfego HTTP é enviado em texto puro, o que significa que qualquer pessoa interceptando a comunicação pode ler as informações.

HTTPS: HTTP Seguro

- **HTTPS (Hypertext Transfer Protocol Secure)** é a versão segura do HTTP.

- Ele utiliza criptografia para garantir que a comunicação entre cliente e servidor seja privada e segura.

HTTPS: HTTP Seguro

- **Como Funciona?**

- **Camada de Segurança (SSL/TLS)**: HTTPS adiciona uma camada de criptografia usando SSL (Secure Sockets Layer) ou TLS (Transport Layer Security). Isso garante que as informações enviadas e recebidas estejam protegidas.

- **Certificado Digital**: Para usar HTTPS, o servidor precisa de um certificado digital emitido por uma Autoridade Certificadora (CA). Este certificado autentica a identidade do servidor e permite a troca de chaves para criptografia.

HTTPS: HTTP Seguro

- **Como Funciona?**

Benefícios do HTTPS

- **Confidencialidade**: Os dados são criptografados, protegendo contra interceptação.
- **Integridade**: HTTPS assegura que os dados não foram alterados durante o trânsito.
- **Autenticação**: O certificado digital confirma a identidade do servidor, protegendo contra sites falsos.

Passos de uma Conexão HTTPS

1. Cliente solicita uma conexão segura (HTTPS).
2. Servidor responde com um certificado digital.
3. Troca de chaves de criptografia entre o cliente e o servidor.
4. Dados são transmitidos de forma criptografada

Vantagens de Usar HTTPS

1. Proteção de Dados Sensíveis: Essencial para proteger informações de login, transações financeiras, dados pessoais.

2. SEO: Motores de busca, como o Google, priorizam sites com HTTPS.

3. Confiança do Usuário: Sites com HTTPS são identificados como seguros pelos navegadores, com um cadeado ao lado da URL.

RDP - Remote Desktop Protocol

- **RDP (Protocolo de Desktop Remoto)**
  - Usado para **acesso remoto** a outro computador, geralmente em uma rede corporativa.
  - **Permite que um usuário controle um dispositivo** remotamente como se estivesse fisicamente presente.
  - **Funcionamento**: conecta dispositivos usando uma sessão de RDP para transmitir tela e controles.

Dúvidas?
Ótimo dia para todos!