

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

MARCOS VINICIUS DA SILVA CARDOSO  
EDER MURILO DE MORAIS

**TRABALHO FINAL - FUNDAMENTOS EM SERVIDORES WEB**

**TRABALHO FINAL**  
**FUNDAMENTOS EM SERVIDORES WEB**  
**1º. semestre de 2024**

Neste documento abordaremos alguns protocolos da Internet: suas principais características, como funcionam, onde são utilizados e alguns exemplos de uso no Linux.

Quatro protocolos serão descritos, sendo estes: SSH (Secure Shell), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol) e FTP (File Transfer Protocol).

**Protocolo SSH**

Porta 22

Com a necessidade de acessar e administrar servidores de maneira remota e segura, surgiu o protocolo SSH (Secure Shell). Criado pelo engenheiro de software Tatu Ylönen, o protocolo SSH permite a conexão e comunicação entre cliente e servidor com informações criptografadas, tornando o processo seguro e impossibilitando que as informações compartilhadas sejam interceptadas.

O protocolo possui três camadas:

A **camada de transporte** cria uma conexão entre o cliente e o servidor e criptografa as informações transmitidas.

A **camada de autenticação** verifica a identidade do usuário que está tentando se conectar ao servidor, utilizando uma senha ou chave SSH.

E por fim, a **camada de sessão**. Essa é a camada responsável pela troca de informações, que permite que o usuário transfira arquivos e execute comandos.

Criptografia:

Criada através das **chaves SSH**. Cada dispositivo tem uma chave pública e uma chave privada. Durante a primeira conexão os dispositivos trocam suas chaves públicas. A chave pública é usada para criptografar os dados transmitidos, enquanto a chave privada serve para descriptografá-los.

Também existe o processo de autenticação, que pode ocorrer através de uma senha ou chave pública pré-compartilhada - o dispositivo remoto usa sua chave privada para assinar a chave pública do dispositivo local, e o dispositivo local verifica a assinatura usando a chave pública do dispositivo remoto.

**Protocolo DNS**

Porta 53

A sigla DNS significa Domain Name System, ou seja, Sistema de Nomes de Domínio. Para cada nome de domínio na Internet, existe um endereço de IP associado – o protocolo DNS registra essa informação.

Quando um usuário abre o navegador e digita o endereço URL referente ao domínio de um site, ele envia uma requisição na rede para encontrar o respectivo IP do servidor que o armazena.

Essa requisição é passada para o DNS, que identifica o endereço IP do domínio para que a conexão entre o cliente e o servidor possa acontecer.

### **Protocolo DHCP**

Porta 67 ou 68

É um protocolo de configuração que atribui dinamicamente: Endereço IP, máscara de Sub-rede, Gateway padrão e servidores DNS.

O DHCP é particularmente atrativo pela distribuição automática dessas configurações, o que economiza muito tempo de trabalho, principalmente considerando grandes redes de computadores que teriam que ser configuradas manualmente.

Como funciona:

É dividido em 4 etapas, que são: Discover, Offer, Request e Acknowledge.

Discover – Um cliente DHCP envia uma mensagem para o endereço de broadcast da rede (pois não tem um IP atribuído a ele) para encontrar servidores DHCP disponíveis.

Offer – Quando um servidor DHCP recebe a mensagem, ele responde com uma oferta (Offer) contendo uma proposta de configuração para o cliente.

Request – O cliente solicita o uso das configurações oferecidas pelo servidor.

Acknowledge – Nesta etapa ocorre a confirmação de que o cliente pode usar as configurações fornecidas pelo servidor.

### **Protocolo FTP**

Porta 21 ou 20

O protocolo de transferência de arquivos serve para que usuários possam realizar downloads e uploads de arquivos entre computadores.

Seu funcionamento é simples: O cliente FTP se conecta ao servidor FTP através de um IP ou domínio. O mesmo pode se conectar de forma “anônima” ou através de autenticação por senha. Feita a conexão, o usuário pode transferir arquivos utilizando comandos.