**Nível de Aplicação**

**Arquitetura Cliente-Servidor –** Processo onde uma aplicação inicia a interação com outra aplicação que sempre fica esperando.

**Arquitetura P2P –** Termo que refere-se a uma classe de sistemas e aplicações de uma maneira descentralizada para melhorar o desempenho. Altamente escaláveis mas difíceis de gerenciar.

**Arquitetura Híbrida –** Servidor intermedia informações enviadas pelos clientes.

**Comunicação entre Processos –** Dois processos se comunicam por meio de troca de mensagens (SOCKETS)

**Sockets –** Interface entre camada de aplicação e camada de transporte, tudo que vem de ou vai para um processo passa por ele

**Protocolos de Aplicação –** Definem tipo, sintaxe, semântica e as regras das mensagens.

**Socket UDP –** não confiável

**Socket TCP –** Confiável, garante entrega dos segmentos (stream=sequência de bytes transmitida)

**DHCP**

Simplificação de gestão do endereçamento e configuração

Gerencia automaticamente a atribuição das configurações TCP/IP das máquinas

Endereços dispensados em tempo finito

**Relay Agent –** Intermediário nas respostas ao cliente (re-encapsula)

**A table with black text

Description automatically generatedDNS**

Mapeia nomes simbólicos em endereços IP

Possui domínio raíz, cada nó ou domínio nessa hierarquia tem uma designação e pode conter sub-dominios, são agrupados em zonas

Podem ser divididos em Root Name Servers, Top Level Domain (TLD) ou servidores de autoridade (gerencia os nomes)

Serv. Raiz apontam para serv. TLD que apontam para serv. de autoridade

**Root Name Servers –** Respondem requisições sobre servidores de nomes do primeiro nível da árvore

**Definindo Domínio**

É preciso construir um arquivo de zona

As entradas nos arquivos são chamads de **Resource Records (RR)**

**RR –** SOA, NS, A, AAAA, CNAME, MX, PTR

**SOA (start-of-autority) –** Indica a utoridade para os dados deste domínio

**DNSSEC – Security extensions**

Protege contra ataques: **Falsificação de DNS/envenenamento de cache** (dados apontam para uma réplica do site original) , **tunulamento de DNS** (túnel que atravessam consultas e respostas de DNS), **ataque NXDOMAIN** (solicitando registros que não existem)

**Ferramento de Troubleshooting**

**Nslookup –** exibe informações fornecidas pelos servidores do nomes

**Mail exchangers, name servers**

**Whois –** Lista informações disponíveis sobre o registro de domínio

**Dig –** Permite consultar manualmente servidores DNS para obter informações sobre domínios

**NAT**

IPv4 limitado a quantidade máximo de hosts distintos

Reuso e economia de endereços IP, minimiza problema de segurança

Possui 3 fases:

**Address binding –** associação de endereços privados com públicos

**Address lookup and translation –** Pesquisa e tradução dos endereços dos pacotes de E/S

**Address unbinding –** endereço priv. não está mais associado a um endereço global

Características:

**Alocação transparente de endereços –** Liga endereços da rede privada com na rede global e vice-versa

**Roteamento transparente –** Traduz endereços do cabeçalho IP para que contenha end. Roteáveis do próprio NAT-router

**NAT Estático –** transparente, não economiza endereços e os hosts com endereços são traduzidos

**NAT Dinâmico –** controle baseado nas conexões

**IP Masquering ou NAPT –** Endereços IP representados por 1 único endereço público, máxima economia de endereços IP públicos, maior nível de segurança entre todas as técnicas

Endereço IP interno é substituído pelo IP público ou NAT router e núm. da porta TCP ou UDP é trocado por outro qualquer

**SMTP**

Orientado à conexão, enviar mensagens de correio eletrônico

Info de log na mensagem indicando o caminho percorrido

Utiliza o DNS para determinar o servidor de e-mail (Registro MX)

**POP**

Criado para recuperação de mensagens em sistemas de arquivos remotos

Estados:

**Autorização –** Identificação do usuário

**Transação –** Leitura das mensagens e indicação de deleção

**Atualização –** Libera recursos, atua sobre o sistema de arquivos e encerra conexão

Modos de operação:

**Download-and-delete –** usuário não pode reler o email em outro cliente

**Download-and-keep –** cópias das mensagens em clients diferentes

**IMAP**

**IMAP X POP 3 –** POP3 email sendo acessado somente de uma aplicação, IMAP permite acesso simultâneo por múltiplos clientes (acessa email em locais diferentes)

A close up of black text

Description automatically generated**HTTP**

Protocolo mais popular, interligam-se por hyperlinks, cliente/servidor

Utiliza TCP, porta 80

**Não persistente ( 0.9 E 1.0 ) –** 1 solicitação e 1 resposta

**Persistente ( 1.1 ) –** 1 solicitação e 1 resposta, depois solicitações e respostas adicionais

Tipos de mensagens:

**Solicitação –** Linha de requisição, cabeçalho e corpo

**Resposta –** Linha de status, cabeçalho e corpo

**GET Condicional –** Não enviar objeto se cliente já tem versão atual

**Proxy –** Atender pedido do cliente sem envolver servidor de origem

**URL –** Identifica o local e o host para acessar determinado recurso

**URN –** Nome do recurso que será acessado

**URI –** Identificador do recurso

**HTTPS –** Camada adicional de segurança que utiliza SSL, TLS ou QUIC

Ideia de criar um canal segura sobre rede insegura, criptografia bidirecional para cliente/servidor

Para construir, precisa criar um par de chaves (pública e privada), demanda muito processamento

Garante confidencialidade e integridade das requisições, apenas com TLS/SSL não é garantido.

**SNMP**

Modelo gerente/agente

Quatro componentes: elementos gerenciados (agente), estações de gerência (gerente), protocolos de gerência (SNMP) e informações de gerência (MIB)

Gerência de redes é uma aplicação que envolve trocas de dados entre os processos gerente e agente

**Gerente:**