

Aula 01: Introdução às Redes de Computadores

Definição de Redes de Computadores: Redes de computadores são definidas como um conjunto de computadores autônomos interconectados por uma tecnologia comum, permitindo o compartilhamento de recursos e a comunicação entre dispositivos.

Usos de Redes:

Comerciais: Compartilhamento de recursos como impressoras, desktops, e-commerce, confiabilidade, economia.

Domésticos: Troca de mensagens, redes sociais, entretenimento, conectividade (como redes ponto a ponto - P2P).

Modelos de Redes:

Cliente/Servidor: Um servidor central mantém as informações e os clientes fazem solicitações de dados por meio da rede. A comunicação é hierárquica, e o hardware do servidor é especializado.

Ponto a Ponto (P2P): Todos os dispositivos na rede têm a capacidade de agir como cliente e servidor simultaneamente, sem distinção entre eles.

Modelo Híbrido: Combina elementos de cliente/servidor e ponto a ponto, onde servidores em redes P2P mantêm seus clientes em um modelo hierárquico.

Tecnologias de Transmissão:

Broadcast: Todos os dispositivos competem pelo mesmo meio físico, o que pode gerar colisões de

dados.

Ponto a Ponto: A comunicação ocorre diretamente entre dois dispositivos, eliminando o risco de colisões.

Classificação das Redes:

LAN (Local Area Network): Redes locais, geralmente dentro de uma casa ou escritório.

WAN (Wide Area Network): Redes que cobrem grandes áreas geográficas, como a Internet.

PAN, MAN: Redes pessoais e metropolitanas, com diferentes alcances.

Questões Sociais: O impacto das redes de computadores em termos de segurança, privacidade, direitos autorais e a importância das leis para regular essas áreas.

Pergunta: Por que o broadcast gera colisão e o que é colisão? Resposta: O broadcast gera colisão porque todos os dispositivos conectados ao meio físico compartilham o mesmo canal de transmissão. Uma colisão ocorre quando dois dispositivos tentam transmitir dados ao mesmo tempo, causando uma sobreposição de sinais que corrompe as transmissões. Protocolos como CSMA/CD ajudam a detectar e corrigir essas colisões.

Pergunta: Por que o ponto a ponto funciona de maneira diferente do broadcast e evita colisão?

Resposta: A comunicação ponto a ponto funciona com um canal dedicado entre dois dispositivos, eliminando a competição de múltiplos emissores. Isso evita colisões, pois o meio físico é utilizado exclusivamente pelos dois dispositivos que estão se comunicando.

Pergunta: O que é o meio de comunicação? Resposta: O meio de comunicação é o canal físico ou lógico através do qual os dados são transmitidos. Pode ser um cabo de cobre, fibra óptica, ou ondas de rádio em redes sem fio.

Protocolos: Protocolos são um conjunto de regras que governam o formato e o significado das mensagens trocadas entre dispositivos em uma rede. Exemplos de protocolos incluem o DNS, que traduz nomes de domínio em endereços IP; o DHCP, que distribui endereços IP automaticamente; e o FTP, que permite a transferência de arquivos entre sistemas.

Hierarquia de Protocolos: A comunicação em rede é organizada em diferentes camadas, cada uma com responsabilidades específicas. A camada usa protocolos para implementar seus serviços e pode alterá-los sem mudar a visibilidade do serviço para outras camadas. Isso inclui desde a camada física, que transmite os bits através do meio, até a camada de aplicação, que lida com a interação direta com o usuário.

Pergunta: Serviços com e sem confirmação:

- a) Estabelecimento de conexão: Serviço com confirmação.
- b) Transmissão de dados: Pode ser com ou sem confirmação, dependendo do protocolo.
- c) Download de um arquivo: Serviço com confirmação.
- d) Ouvir rádio pela Internet: Serviço sem confirmação.
- e) Liberação de conexão: Serviço com confirmação.

Por que eles são com e sem confirmação? E o que significa ser um serviço com e sem confirmação?

Resposta:

Serviço com confirmação: Um serviço com confirmação é aquele em que o receptor envia uma mensagem de retorno (confirmação) ao transmissor para informar que os dados foram recebidos corretamente. Isso garante que o emissor saiba se a mensagem foi recebida e, caso não tenha sido, pode retransmitir os dados. Esse tipo de serviço é importante para a confiabilidade da comunicação.

Exemplo: Se você enviar um pacote de dados e o receptor não confirmar o recebimento, o serviço com confirmação solicitará que os dados sejam reenviados até que a confirmação seja recebida.

Serviço sem confirmação: Em um serviço sem confirmação, o transmissor envia os dados, mas não espera nem recebe uma confirmação de que o receptor os recebeu corretamente. Esse tipo de serviço é não confiável, pois não há garantia de que os dados chegaram, mas é mais rápido e eficiente em termos de recursos.

Exemplo: Se você estiver transmitindo um fluxo de vídeo ao vivo ou ouvindo rádio pela internet, a perda de alguns pacotes de dados não prejudica muito a experiência, então a confirmação não é necessária.

Por que os serviços listados são com e sem confirmação?

Estabelecimento de conexão (com confirmação): Quando duas máquinas desejam estabelecer uma conexão, é necessário garantir que ambas estejam prontas para se comunicar. O estabelecimento de conexão (ex.: no TCP) envolve uma troca de mensagens de confirmação (como o handshake de três vias) para garantir que a conexão foi iniciada com sucesso.

Transmissão de dados (com ou sem confirmação): A transmissão de dados pode ser feita de duas maneiras:

Com confirmação: Utilizando protocolos como o TCP, que garantem que cada segmento de dados enviado seja confirmado pelo receptor.

Sem confirmação: Utilizando o UDP, onde os dados são enviados sem garantir que o receptor os recebeu, usado em aplicações onde a velocidade é mais importante do que a confiabilidade (como em transmissões de vídeo ao vivo).

Download de um arquivo (com confirmação): Ao realizar um download, é essencial garantir que todos os pedaços do arquivo sejam recebidos corretamente. Nesse caso, o protocolo utilizado, como o TCP, solicita confirmações a cada etapa da transferência para garantir que o arquivo seja recebido integralmente e sem erros.

Ouvir rádio pela Internet (sem confirmação): Quando você ouve uma rádio pela internet ou assiste a uma transmissão ao vivo, os dados são enviados usando streaming sem confirmação (geralmente usando o UDP), pois é mais importante manter a fluidez do áudio/vídeo do que garantir que cada pacote de dados seja recebido. Se um pacote se perder, a transmissão continua sem interrupção, mesmo com uma pequena perda de qualidade.

Liberação de conexão (com confirmação): Assim como o estabelecimento de conexão, o encerramento (ou liberação) de uma conexão também requer confirmação para garantir que ambas as partes saibam que a comunicação foi encerrada corretamente. Isso evita situações em que uma máquina continue enviando dados sem que a outra esteja pronta para recebê-los.

Pergunta: DNS é um banco de dados hierárquico e distribuído (Resposta correta):

a) Banco de dados hierárquico - pode armazenar de forma distribuída quase qualquer tipo de dados, para praticamente qualquer finalidade.

Explique essa questão.

Resposta:

O DNS (Domain Name System) é frequentemente descrito como um banco de dados hierárquico e distribuído, pois ele organiza e distribui informações sobre nomes de domínio e seus endereços IP de uma forma que permite uma estrutura escalável e eficiente. Vamos entender o que isso significa:

Banco de Dados Hierárquico:

O DNS organiza as informações em uma hierarquia, semelhante a uma árvore, onde cada nível possui uma função específica e pode ser subdividido.

No topo dessa hierarquia estão os servidores raiz, que gerenciam os domínios de nível mais alto (Top Level Domains - TLDs), como ".com", ".org", ".br".

Abaixo dos TLDs estão os domínios de segundo nível, como google.com, example.org, que podem ser subdivididos em subdomínios (como mail.google.com).

Essa estrutura hierárquica permite que as consultas ao DNS sejam feitas de forma organizada, navegando pela árvore de domínios até encontrar o endereço correspondente.

Banco de Dados Distribuído:

O DNS não é um banco de dados centralizado. Em vez disso, ele é distribuído em milhões de servidores ao redor do mundo. Isso significa que cada servidor DNS armazena apenas uma parte da informação, geralmente relacionada ao seu domínio específico.

Isso aumenta a eficiência e a escalabilidade do sistema, pois evita sobrecargas e permite que a resolução de nomes ocorra de forma rápida e eficiente, sem depender de um único ponto de falha.

Armazenamento de Dados:

O DNS pode armazenar diferentes tipos de informações além de endereços IP, como registros MX (para e-mails), registros CNAME (para mapeamento de domínios), entre outros.

A natureza distribuída do DNS permite que ele seja usado para fins variados, como armazenamento de registros de segurança, além de funcionar como a base da infraestrutura de endereços da Internet.

Pergunta: Protocolo de e-mail responsável pela conversão de arquivos em formato ASCII:

c) MIME.

Explique essa também, pois acreditava ser o SMTP e estava errado.

Resposta:

O MIME (Multipurpose Internet Mail Extensions) é o protocolo de e-mail responsável por permitir a transmissão de diversos tipos de conteúdo em uma mensagem de e-mail, convertendo arquivos em um formato que pode ser transmitido através dos protocolos de e-mail, como o SMTP.

Por que MIME é usado?

Originalmente, os protocolos de e-mail, como o SMTP (Simple Mail Transfer Protocol), foram projetados para transmitir texto simples no formato ASCII. Isso funcionava bem quando as mensagens eram apenas texto, mas à medida que o uso da Internet cresceu, surgiu a necessidade de enviar outros tipos de dados, como:

Imagens

Vídeos

Documentos em outros formatos (PDF, Word, etc.)

O problema é que os e-mails deveriam ser transmitidos por redes que só suportavam texto ASCII. Como muitos desses arquivos contêm dados binários, eles precisavam ser convertidos para um formato de texto antes de serem enviados por SMTP. Aí entra o MIME.

O que é o MIME?

MIME é uma extensão dos formatos de e-mail que permite o envio de vários tipos de conteúdo, convertendo-os para um formato que pode ser transmitido via SMTP (que, por padrão, só trabalha com texto ASCII). Ele faz isso ao:

Codificar o conteúdo binário de um arquivo em ASCII.

Adicionar cabeçalhos especiais ao e-mail, indicando o tipo de conteúdo (imagem, vídeo, documento, etc.) e o formato de codificação utilizado.

Como o MIME funciona na prática?

Quando você envia um arquivo, como uma imagem ou PDF, via e-mail:

O MIME converte o arquivo binário para um formato que pode ser transmitido por SMTP (geralmente usando uma técnica chamada Base64, que transforma o arquivo binário em texto ASCII).

O e-mail recebe cabeçalhos MIME adicionais, que indicam ao destinatário como reconstruir e interpretar o conteúdo após o recebimento.

Quando o e-mail chega ao destinatário, o cliente de e-mail lê os cabeçalhos MIME, decodifica o conteúdo e apresenta o arquivo corretamente.

Diferença entre SMTP e MIME:

SMTP é o protocolo que envia e transfere os e-mails. Ele se encarrega de mover as mensagens de um servidor de e-mail para outro e garantir que a mensagem chegue ao seu destino. Porém, ele lida apenas com texto simples em formato ASCII.

MIME, por outro lado, estende as capacidades do e-mail para incluir conteúdo não-ASCII, como anexos (imagens, vídeos, PDFs) e permite o envio de mensagens em diferentes formatos, como HTML. Ele faz a codificação e conversão dos arquivos para que possam ser enviados por SMTP e outros protocolos.

Pergunta: Função que não pertence ao serviço DNS:

e) Distribuição de endereços IP de forma automática.

Por que ele não faz isso? Como o DNS opera?

Resposta:

O DNS (Domain Name System) não é responsável pela distribuição automática de endereços IP. O DNS tem como principal função a tradução de nomes de domínio (como www.exemplo.com) para endereços IP (como 192.168.1.1). Ele age como um "catálogo" que converte nomes que os humanos conseguem ler facilmente em endereços numéricos usados por computadores para comunicação.

Por que o DNS não faz a distribuição de IPs?

A distribuição automática de endereços IP é feita pelo protocolo DHCP (Dynamic Host

Configuration Protocol), que atribui dinamicamente endereços IP aos dispositivos conectados a uma rede. Quando um dispositivo (como um computador ou smartphone) se conecta à rede, o servidor DHCP atribui a ele um endereço IP temporário e outros detalhes, como a máscara de sub-rede e o gateway.

O DNS, por outro lado, apenas "resolve" (ou traduz) o nome de domínio em um endereço IP, mas não tem envolvimento com a distribuição de IPs para dispositivos.

Como o DNS opera?

O DNS funciona como um serviço de resolução de nomes que segue uma estrutura hierárquica e distribuída. O processo básico de funcionamento do DNS é o seguinte:

Consulta do DNS: Quando você digita um endereço como "www.exemplo.com" no navegador, seu computador (cliente DNS) faz uma consulta a um servidor DNS local (geralmente fornecido pelo seu provedor de Internet).

Resolução de Nomes:

Cache: Primeiro, o servidor DNS local verifica se já tem o endereço IP correspondente em seu cache. Se encontrar, retorna o IP sem precisar consultar outros servidores.

Servidores DNS Raiz: Se o servidor local não tiver o IP em cache, ele encaminha a solicitação para um dos servidores raiz (existem 13 servidores raiz no mundo, que são pontos principais de consulta no DNS).

TLD (Top-Level Domain): O servidor raiz redireciona a consulta para o servidor DNS que gerencia o domínio de topo (como ".com", ".org", ou ".br").

Servidor Autoritativo: Em seguida, o servidor de TLD redireciona a solicitação para o servidor DNS

autoritativo que possui os registros do domínio específico (como "exemplo.com").

Resposta: Finalmente, o servidor autoritativo retorna o endereço IP associado ao nome de domínio.

Entrega ao Usuário: O servidor DNS local envia o endereço IP ao computador solicitante, que então pode se conectar ao site usando o endereço IP fornecido.

Pergunta: Descreva o funcionamento de um serviço de e-mail:

Um cliente de e-mail envia uma mensagem para o servidor de envio (SMTP), que encaminha o e-mail para o servidor do destinatário, onde ele será armazenado até que o destinatário o recupere usando um cliente de e-mail e os protocolos POP ou IMAP.

Explique mais detalhadamente, me falando todos os conceitos relacionados ao e-mail, não conheço o que é POP IMAP.

Resposta:

O envio e recebimento de e-mails envolvem uma série de protocolos e servidores que garantem que a mensagem viaje corretamente do remetente até o destinatário. Vamos explorar o funcionamento do e-mail em detalhes:

1. SMTP (Simple Mail Transfer Protocol)

SMTP é o protocolo padrão usado para o envio de e-mails entre servidores de correio eletrônico. Ele é responsável por transferir o e-mail do cliente de envio (como Outlook, Thunderbird ou Gmail) para o servidor de correio de saída.

Funcionamento do SMTP:

O cliente de e-mail (como o Outlook ou Gmail) envia a mensagem para o servidor SMTP configurado pelo usuário.

O servidor SMTP, em seguida, consulta o DNS para encontrar o endereço IP do servidor de e-mail do destinatário.

O SMTP então transfere o e-mail para o servidor SMTP do destinatário, onde ele é armazenado até que o destinatário o recupere.

2. POP (Post Office Protocol) e IMAP (Internet Message Access Protocol)

Estes dois protocolos são usados para o recebimento de e-mails no cliente do usuário, mas operam de maneiras diferentes.

POP3 (Post Office Protocol - Versão 3)

O POP3 é um protocolo de e-mail que permite ao cliente (o software de e-mail do destinatário) baixar as mensagens do servidor para o seu dispositivo local.

Características do POP3:

Após o download, as mensagens são removidas do servidor (a menos que seja configurado de outra maneira).

É útil se o usuário deseja acessar o e-mail em apenas um dispositivo.

Vantagem: Economiza espaço no servidor, pois as mensagens são transferidas para o dispositivo do usuário.

Desvantagem: Não permite fácil sincronização entre múltiplos dispositivos (ou seja, se você ler um e-mail no celular, ele não aparecerá como lido no computador).

IMAP (Internet Message Access Protocol)

O IMAP é um protocolo que permite o acesso remoto às mensagens de e-mail, mantendo-as no

servidor e sincronizando-as em vários dispositivos.

Características do IMAP:

As mensagens permanecem no servidor, e os usuários podem acessá-las de vários dispositivos (por exemplo, telefone, computador e tablet).

Vantagem: A sincronização é automática; se um e-mail for lido ou excluído em um dispositivo, essa alteração será refletida em todos os dispositivos conectados.

Desvantagem: Requer mais armazenamento no servidor, pois os e-mails são mantidos lá em vez de serem baixados.

3. Funcionamento Geral do Serviço de E-mail:

Etapa 1: Envio de uma Mensagem

O usuário escreve um e-mail em um cliente de e-mail (ex.: Gmail, Outlook) e, ao clicar em "Enviar", o e-mail é transmitido para o servidor SMTP do remetente.

Etapa 2: Transferência via SMTP

O servidor SMTP do remetente encaminha o e-mail ao servidor SMTP do destinatário, fazendo uso do DNS para encontrar o caminho certo.

Se o endereço de e-mail de destino estiver no mesmo domínio, o servidor SMTP local já pode entregar o e-mail. Caso contrário, ele encaminha para outros servidores SMTP até chegar ao destino correto.

Etapa 3: Armazenamento no Servidor de Destino

O e-mail é armazenado no servidor de e-mail do destinatário até que o destinatário o baixe ou o acesse.

Etapa 4: Recebimento via POP ou IMAP

O destinatário abre o cliente de e-mail (como Gmail, Outlook ou Thunderbird), que faz a consulta ao servidor usando o protocolo POP3 ou IMAP.

Se for POP3, o e-mail é baixado para o dispositivo do destinatário e removido do servidor (a menos que seja configurado para manter uma cópia).

Se for IMAP, o e-mail é acessado diretamente no servidor e sincronizado entre todos os dispositivos conectados.