# Prova 1

## Conteúdo de prova

- Estrutura físicas
- Topologias físicas diferenciar os tipos de redes (Barramento ,anel token ring ,estrela …HUB ,SWITCH ,arvore )
- Rede local LAN.
- Rede área pessoal PAN.
- Rede metropolitana MAN.
- Redes de longa distância WAN.
- Digital ,analógica (sentido da conexão half-duplex ,full-duplex …).
- Sincronismo (assíncrona , síncrona ).
- Endereçamento de mensagens (únicast ,broadcasting , multicast ).
- Arquitetura modelo cliente servidor (máquina cliente , processo cliente , solicitação …).
- Sistema não hierárquico sem clientes e servidores fixos.
- Classificação de processadores interconectados por escala
- Subrede
- Fluxos de pacotes do transmissor ao receptor (identificar tipo de conexão orientada ou não orientada …) .
- Circuito virtual.
- Primitivas de serviços.
- Modelo OSI (as 7 camadas).
- Modelo TCP/IP x OSI.
- Modelo TCP/IP.
- TCP e UDP.
- Ativos de redes : funcionalidades que cada dispositivo faz. (Moldem , HUB ,SWITCH ,roteadores , repetidor , pontes, gateway, backbone)

## Observações

Características

Desenhos arquiteturas ,desenhos de cada tipo de rede.

Saber qual as funções das camadas de cada modelo.

Questões tratadas em cada camada simplex ,Hallf duplex …

Principais funções de cada camada modelo OSI e TCP/IP.

Vantagens e desvantagens

Tipos de redes

Caminho do pacote

Diferença de mensagens enviadas com HUB ,SWITCH

# Revisão geral

## Estruturas físicas

Algumas estruturas fisicas incluem:

1. Rede de Área Local (LAN): É uma rede que cobre uma pequena área geográfica, como uma casa, escritório ou edifício. Geralmente é construída com cabos de cobre, como Ethernet, ou tecnologias sem fio, como Wi-Fi.
2. Rede de Área Metropolitana (MAN): É uma rede que cobre uma área geográfica maior do que uma LAN, geralmente uma cidade ou região metropolitana. Pode ser construída com cabos de fibra óptica ou sem fio.
3. Rede de Área Ampla (WAN): É uma rede que cobre uma área geográfica ainda maior, como um estado, país ou mesmo o mundo inteiro. Pode ser construída com cabos de fibra óptica, satélites ou outras tecnologias sem fio.
4. Topologia em Estrela: Nessa topologia, todos os dispositivos de rede são conectados a um ponto central, como um hub ou switch.
5. Topologia em Anel: Nessa topologia, os dispositivos de rede são conectados em uma forma circular, onde cada dispositivo é conectado ao seu vizinho, formando um anel.
6. Topologia em Malha: Nessa topologia, todos os dispositivos são conectados uns aos outros, criando várias rotas possíveis para o tráfego de dados.

## Topologias físicas diferenciar os tipos de redes

- Barramento: todos os dispositivos são conectados a um único cabo de comunicação. Nessa topologia, os dispositivos compartilham o mesmo canal de comunicação para enviar e receber dados. O cabo central atua como o "barramento" que conecta todos os dispositivos da rede. No entanto, a topologia de barramento também tem algumas desvantagens. Se o cabo central falhar, toda a rede pode ser afetada. Além disso, quanto mais dispositivos são adicionados à rede, menor é a largura de banda disponível para cada dispositivo, o que pode resultar em desempenho degradado ou problemas de congestionamento. Por esse motivo, a topologia de barramento é mais adequada para redes menores ou com um número limitado de dispositivos.

- Anel: A topologia em anel é um tipo de topologia de rede em que os dispositivos são conectados em uma estrutura circular fechada. Cada dispositivo é conectado a dois outros dispositivos adjacentes, formando um "anel" de dispositivos. Os dados são transmitidos de um dispositivo para o próximo, até que cheguem ao destino pretendido. Em uma rede em anel, os dados são transmitidos em uma única direção ao redor do anel. Quando um dispositivo envia dados, eles passam por todos os dispositivos no anel até chegar ao destino pretendido. Cada dispositivo na rede lê os dados, mas apenas o destinatário final os processa. A topologia em anel tem algumas vantagens, como alta confiabilidade e capacidade de fornecer desempenho uniforme em todas as áreas da rede. No entanto, ela também tem algumas desvantagens, como alta complexidade de

instalação e manutenção e falta de escalabilidade. Um exemplo de rede em anel é o Token Ring, que foi popular nos anos 80 e 90. Nesse sistema, os dados são transmitidos em um anel e os dispositivos só podem enviar dados quando recebem um "token" de um dispositivo adjacente. O token é passado ao redor do anel, permitindo que cada dispositivo envie dados em sua vez.

- Estrela: A topologia de rede em estrela é um tipo de topologia em que todos os dispositivos são conectados a um único ponto central, conhecido como "hub" ou "switch". Cada dispositivo é conectado diretamente ao hub/switch por meio de um cabo separado.

Nessa topologia, os dados são transmitidos do dispositivo de origem para o hub/switch, que então os encaminha para o dispositivo de destino apropriado. Isso significa que, em vez de compartilhar um único canal de comunicação como na topologia de barramento, cada dispositivo tem seu próprio canal dedicado de comunicação com o hub/switch.

A topologia em estrela é a mais comum em redes de computadores modernas, como as redes Ethernet. Ela oferece várias vantagens, incluindo:

- Facilidade de instalação e manutenção: Adicionar ou remover dispositivos da rede é fácil, pois cada dispositivo é conectado diretamente ao hub/switch.
- Confiabilidade: Se um cabo ou dispositivo falhar, apenas o dispositivo é afetado. Os outros dispositivos continuam a funcionar normalmente.
- Desempenho: Cada dispositivo tem seu próprio canal dedicado de comunicação com o hub/switch, o que significa que o tráfego de dados é mais rápido e menos propenso a congestionamentos.

No entanto, a topologia em estrela também tem algumas desvantagens, como a dependência do hub/switch. Se o hub/switch falhar, toda a rede pode ser afetada. Além disso, a topologia em estrela pode exigir mais cabos do que outras topologias, o que pode ser um problema em redes maiores.

- Arvore: A topologia em árvore é uma topologia de rede de computadores que combina as características da topologia em estrela e da topologia em barramento. Nessa topologia, vários hubs/switches são conectados em cascata para criar uma estrutura hierárquica em forma de árvore. Na topologia em árvore, os dispositivos finais (como computadores, impressoras e servidores) são conectados aos hubs/switches periféricos, que por sua vez são conectados a hubs/switches superiores. Essa estrutura hierárquica em camadas permite que os dados sejam transmitidos de forma eficiente entre os dispositivos finais e os servidores ou roteadores que conectam diferentes redes.

Os benefícios da topologia em árvore incluem:

- Escalabilidade: A topologia em árvore pode ser facilmente expandida para acomodar novos dispositivos e redes adicionais.

- Desempenho: Como os dados são transmitidos diretamente do dispositivo de origem ao destino, a topologia em árvore oferece um desempenho rápido e confiável.
- Confiabilidade: A topologia em árvore é menos propensa a falhas do que outras topologias, pois os dispositivos finais estão conectados diretamente aos hubs/switches periféricos e não dependem de um único cabo central como na topologia em barramento.

No entanto, a topologia em árvore também pode ter desvantagens, como a complexidade de instalação e manutenção e a dependência dos hubs/switches. Se um hub/switch falhar, todos os dispositivos conectados a ele serão afetados.

A topologia em árvore é comumente usada em redes de grande escala, como redes corporativas e de data centers, devido à sua capacidade de suportar um grande número de dispositivos e redes.

- Arquitetura Modelo Cliente - Servidor

O modelo cliente-servidor é um modelo de arquitetura de software em que um computador (o servidor) fornece serviços e recursos para outros computadores (os clientes) na rede. Esse modelo é amplamente utilizado em redes de computadores, sistemas de banco de dados, aplicativos da web e muitos outros sistemas de computador.

No modelo cliente-servidor, o servidor é responsável por gerenciar e fornecer os recursos solicitados pelos clientes, como arquivos, dados de banco de dados, páginas web, e-mail, etc. O cliente envia solicitações ao servidor e recebe as respostas correspondentes. O servidor é geralmente mais poderoso e possui mais recursos do que os clientes.

Os benefícios do modelo cliente-servidor incluem a capacidade de compartilhar recursos entre vários clientes, a capacidade de escalar para atender a demanda crescente de usuários e a flexibilidade para adicionar novos recursos e serviços conforme necessário. No entanto, esse modelo também pode apresentar desafios de segurança e gerenciamento de rede, especialmente em sistemas de grande escala.

# Sistema não hierárquicos - sem clientes e servidores fixos

Os sistemas não hierárquicos em redes de computadores são caracterizados pela ausência de uma estrutura hierárquica fixa ou centralizada. Em vez disso, os nós da rede

se comunicam de forma igualitária, compartilhando informações e recursos sem a necessidade de uma autoridade central ou de uma estrutura hierárquica rígida.

Esses sistemas são comumente encontrados em redes peer-to-peer (P2P), em que os computadores na rede são iguais em termos de poder de processamento e recursos, e cada computador é capaz de fornecer e acessar recursos compartilhados. O compartilhamento de recursos é realizado por meio de protocolos P2P, como BitTorrent e Gnutella.

Os sistemas não hierárquicos têm algumas vantagens em relação aos sistemas hierárquicos tradicionais, como:

- Escalabilidade: O sistema pode crescer facilmente à medida que mais nós são adicionados à rede, sem a necessidade de uma infraestrutura centralizada ou de uma hierarquia complexa.
- Flexibilidade: O sistema é flexível e adaptável às mudanças nas necessidades e nos requisitos dos usuários, sem a necessidade de uma autoridade central ou de uma estrutura hierárquica rígida.
- Resiliência: O sistema é resistente a falhas individuais, já que não há um único ponto de falha ou uma autoridade central.

No entanto, os sistemas não hierárquicos também podem ter algumas desvantagens, como:

- Gerenciamento de recursos: O gerenciamento de recursos compartilhados pode ser mais complexo, já que não há uma autoridade central para gerenciá-los.
- Segurança: A segurança pode ser um desafio, pois é necessário garantir que os nós da rede sejam confiáveis e autênticos.
- Eficiência: A eficiência pode ser reduzida, pois o tráfego de rede pode ser mais lento e menos otimizado do que em sistemas hierárquicos.

Os sistemas não hierárquicos são amplamente utilizados em aplicativos P2P, como compartilhamento de arquivos, jogos online e mensagens instantâneas. Esses sistemas oferecem uma alternativa flexível e escalável aos sistemas tradicionais de rede hierárquica.

# Rede local (LAN)

É uma rede de computadores que abrange uma área geográfica relativamente grande, como uma cidade ou uma região metropolitana. As redes MAN geralmente são projetadas para fornecer serviços de comunicação de alta velocidade entre organizações, prédios e departamentos em uma cidade ou região metropolitana.

As redes MAN são projetadas para operar em velocidades muito mais altas do que as redes LAN, com taxas de transmissão que variam de 100 Mbps a vários Gbps. As tecnologias comuns usadas em redes MAN incluem fibra óptica, Ethernet e SONET (Synchronous Optical Network).

# Rede metropolitana (MAN)

É uma rede de computadores que abrange uma área geográfica relativamente grande, como uma cidade ou uma região metropolitana. As redes MAN geralmente são projetadas para fornecer serviços de comunicação de alta velocidade entre organizações, prédios e departamentos em uma cidade ou região metropolitana.

As redes MAN são projetadas para operar em velocidades muito mais altas do que as redes LAN, com taxas de transmissão que variam de 100 Mbps a vários Gbps. As tecnologias comuns usadas em redes MAN incluem fibra óptica, Ethernet e SONET (Synchronous Optical Network).

# Rede de área pessoal (PAN)

É uma rede de computadores que conecta dispositivos pessoais em uma área geográfica muito pequena, como um metro ou menos. Essa rede é criada para que dispositivos, como smartphones, tablets, laptops e fones de ouvido, possam se comunicar e compartilhar informações sem fio.

As tecnologias comuns usadas em redes PAN incluem Bluetooth, NFC (Near Field Communication) e Zigbee. Essas tecnologias permitem que os dispositivos se comuniquem uns com os outros, compartilhando informações e recursos, como música, fotos, vídeos e arquivos.

As redes PAN são frequentemente usadas para conectar dispositivos pessoais, como fones de ouvido sem fio, relógios inteligentes e outros wearables, bem como para automação residencial. Por exemplo, um usuário pode controlar a iluminação, termostatos e outros dispositivos inteligentes em sua casa usando um aplicativo em seu smartphone, que se comunica com os dispositivos na rede PAN.

As redes PAN são frequentemente limitadas em termos de distância de comunicação, geralmente não excedendo um metro ou menos. Eles são muito úteis para conectar dispositivos pessoais próximos, como fones de ouvido sem fio a um smartphone, por exemplo.

As redes PAN também são usadas em áreas de negócios, como na indústria automotiva, onde os sensores em um carro se comunicam uns com os outros para permitir recursos como monitoramento de pneus e sistemas de navegação.

# Redes de longa distancia (WAN)

é uma rede de computadores que conecta dispositivos em diferentes áreas geográficas, como cidades, países e continentes. As redes WAN são usadas para conectar dispositivos em locais geograficamente dispersos, permitindo a comunicação e o compartilhamento de recursos entre esses dispositivos.

As tecnologias comuns usadas em redes WAN incluem linhas telefônicas, cabos submarinos, satélites e conexões sem fio, como Wi-Fi e celular. As redes WAN podem ser usadas para conectar empresas em diferentes locais, permitindo que os funcionários se comuniquem e trabalhem juntos, mesmo que estejam fisicamente distantes.

# Transmissão tipo analógico e digital

## Digital

Sinais regularmente na forma de pulsos elétricos que os computadores fazem internamente e a que fazem entre si em uma rede . Em curtas distancias.

## Analógica

Sinais irregulares . As interferencias não são tão danosas para longas distancias e por isso é muito usado para transmissão via linha telefonica como atraves do DSL . Na linha telefonica convencional é analogica.

Na transmissão analógica em redes de computadores, o sinal é transmitido em uma onda contínua que varia em amplitude e frequência. Isso é usado em aplicações como telefonia e transmissão de TV a cabo, onde a informação é transmitida como um sinal analógico. No entanto, a transmissão analógica é limitada pela qualidade do sinal, sendo mais suscetível a interferências e perda de qualidade com a distância. Por isso, é mais comum encontrar transmissões digitais em redes de computadores.

A transmissão digital é usada em redes de computadores para transmitir informações em sequências discretas de valores binários (0 e 1). Essas informações são transmitidas como pacotes de dados através de pulsos elétricos ou ópticos. A transmissão digital é mais confiável e eficiente do que a transmissão analógica, já que é menos suscetível a interferências e pode ser facilmente compactada para economizar espaço de armazenamento ou reduzir o tempo de transmissão. A transmissão digital também permite que várias informações sejam transmitidas simultaneamente, compartilhando a largura de banda disponível, o que é especialmente importante em redes de computadores.

Algumas das tecnologias de transmissão digital em redes de computadores incluem:

- Ethernet: uma tecnologia de rede local (LAN) que transmite dados digitalmente por meio de cabos de cobre ou fibras ópticas.
- Wi-Fi: uma tecnologia de rede sem fio que transmite dados digitalmente por meio de ondas de rádio.
- Bluetooth: uma tecnologia de comunicação sem fio de curto alcance que transmite dados digitalmente.
- Fibra óptica: uma tecnologia de transmissão de dados que usa cabos de fibras ópticas para transmitir informações digitalmente.

Em resumo, a transmissão digital é mais comum em redes de computadores, pois oferece maior confiabilidade e eficiência na transmissão de informações. No entanto, a transmissão analógica ainda é utilizada em algumas aplicações, como na transmissão de voz em telefonia, por exemplo.

# Simplex

O enlace é utilizado penas em um dos sentidos de transmissão. A transmissão simplex é um tipo de transmissão unidirecional onde a informação flui em apenas uma direção, do transmissor para o receptor, sem a possibilidade de haver comunicação no sentido inverso. Isso significa que, quando um dispositivo está transmitindo informações, ele não pode receber nenhuma informação de volta do dispositivo receptor.

# Half-duplex

O enlace é utilizado nos dois sentidos de transmissão, porém apenas um por vez. É a transmissão mais utilizada hoje em rede de computadores.

# Full-duplex

O enlace é utilizado nos dois possíveis sentidos de transmissão. Já existem transmissões Full Duplex emredes de computadores. Tecnicamente é mais rápida,o dobro da velocidade do half duplex, mas é necessário o dobro de fios tornando-a muito mais cara.

# Sincrona

Transmissão em que os dispositivos de origem e destino sincronizam seus relógios para garantir que os dados sejam transmitidos em intervalos regulares e predefinidos. Isso permite que a transmissão seja mais eficiente, uma vez que não há necessidade de transmitir informações adicionais para sincronizar os relógios em ambos os lados da conexão. O dispositivo de origem envia um sinal de sincronização para o dispositivo de destino no início da transmissão, e os dados são transmitidos em intervalos regulares definidos por esse sinal de sincronização. O dispositivo de destino usa o sinal de sincronização para alinhar seus relógios com o dispositivo de origem, permitindo que ele receba os dados em intervalos predefinidos e sem erros.

# Assincrona

transmissão em que os dados são transmitidos de forma independente, sem um sinal de sincronização contínuo entre os dispositivos de origem e destino. Nesse tipo de transmissão, cada caractere é transmitido com um sinal de start e um sinal de stop, que informam ao dispositivo receptor o início e o fim da transmissão de cada caractere. Os dispositivos de origem e destino não precisam estar sincronizados o tempo todo, o que torna esse tipo de transmissão mais flexível e adaptável a diferentes velocidades e condições de transmissão. No entanto, a transmissão assíncrona é mais lenta do que a transmissão síncrona, pois há um atraso entre a transmissão de cada caractere. A transmissão assíncrona é comumente usada em aplicações de baixa velocidade, como

em comunicações seriais, interfaces de comunicação entre computadores e periféricos, como teclados e mouses, e em redes de computadores em que a transmissão de dados é realizada em pacotes de tamanhos variáveis. Em resumo, a transmissão assíncrona é um tipo de transmissão em que os dados são transmitidos de forma independente, sem um sinal de sincronização contínuo entre os dispositivos de origem e destino, sendo mais flexível e adaptável a diferentes velocidades e condições de transmissão, mas mais lenta do que a transmissão síncrona. É comumente usada em aplicações de baixa velocidade, como em comunicações seriais, interfaces de comunicação entre computadores e periféricos, e em redes de computadores em que a transmissão de dados é realizada em pacotes de tamanhos variáveis.

# Endereçamento de mensagens

### Mensagem unicast

Quando a mensagem é destinada a um único e identificado destinatário.

### Mensagem broadcast

Quando a mensagem é destinada a todos os elementos. Neste caso é gerada uma única mensagem pelo emissor que é destinada a todos os elementos.

### Mensagem multicast

Quando a mensagem é destinada a um subconjunto selecionado de elementos. Neste caso é gerada uma única mensagem pelo emissor que é destinada aos elementos do grupo Multicast.

# Classificação de processadores interconectados por escala

Os processadores interconectados podem ser classificados em diferentes escalas, dependendo do número de processadores envolvidos e da complexidade da interconexão entre eles. As principais escalas são:

1. Multiprocessamento simétrico (SMP): é uma arquitetura de processamento em que vários processadores idênticos compartilham a mesma memória principal e dispositivos de entrada/saída. Os processadores podem executar tarefas independentes ou cooperar em uma única tarefa, com cada processador tendo acesso igual à memória e aos recursos do sistema. O SMP é usado em servidores de alta performance e estações de trabalho.
2. Cluster: é uma coleção de computadores independentes que trabalham juntos como um sistema único. Cada computador no cluster é chamado de nó e é conectado por uma rede de alta velocidade. O cluster pode ser usado para executar tarefas em paralelo, como análise de dados, simulações, renderização de imagens e computação científica.
3. Grid computing: é uma infraestrutura de computação distribuída que permite a coordenação de recursos de computação geograficamente distribuídos para

resolver problemas complexos em ciência, engenharia e negócios. Os recursos podem incluir computadores, armazenamento de dados, redes e instrumentos científicos. A rede de recursos é conectada por uma rede de alta velocidade e é gerenciada por um software de middleware.

4. Máquina paralela de memória compartilhada (MPP): é um sistema de computação paralela em que várias CPUs são conectadas a uma grande memória compartilhada, permitindo que todas as CPUs acessem a mesma memória em tempo real. Os sistemas MPP são usados para aplicações que exigem grande capacidade de processamento, como simulações de clima, física nuclear, engenharia e finanças.
5. Máquina paralela de memória distribuída (DMP): é um sistema de computação paralela em que várias CPUs são conectadas por uma rede de alta velocidade e cada CPU tem sua própria memória local. Os sistemas DMP são usados para aplicações que exigem grande capacidade de processamento distribuído, como análise de big data, processamento de imagens e transações financeiras.

Em resumo, os processadores interconectados podem ser classificados em diferentes escalas, como multiprocessamento simétrico (SMP), cluster, grid computing, máquina paralela de memória compartilhada (MPP) e máquina paralela de memória distribuída (DMP), dependendo do número de processadores envolvidos e da complexidade da interconexão entre eles. Cada escala é adequada para diferentes tipos de aplicações e exigências de processamento.

# Subrede

Uma sub-rede (ou subrede) é uma porção de uma rede IP (Internet Protocol) maior que é dividida em partes menores, permitindo que diferentes grupos de dispositivos sejam agrupados e gerenciados separadamente. Uma sub-rede é criada ao particionar uma rede IP em sub-redes menores usando uma máscara de sub-rede.

Uma máscara de sub-rede é uma sequência de bits que determina quais bits do endereço IP de um dispositivo pertencem à porção do host e quais bits pertencem à porção da rede. Ao aplicar uma máscara de sub-rede a um endereço IP, os bits de host são isolados, permitindo que os bits da rede sejam usados para identificar a sub-rede à qual o dispositivo pertence.

O uso de sub-redes ajuda a gerenciar grandes redes IP e a reduzir o tráfego de broadcast, já que os broadcasts são enviados apenas para dispositivos na mesma sub-rede. Além disso, permite que as políticas de segurança e as configurações de rede sejam aplicadas de forma granular a diferentes grupos de dispositivos.

Por exemplo, uma organização pode ter uma rede IP com o endereço 192.168.0.0/16. Se eles quiserem criar duas sub-redes, eles podem usar uma máscara de sub-rede de 255.255.128.0 (/17), que dividirá a rede em duas sub-redes de 192.168.0.0/17 e 192.168.128.0/17, permitindo que cada sub-rede tenha até 32.766 endereços IP disponíveis para dispositivos.

# Fluxos de pacotes do transmissor ao receptor

Em uma rede de computadores, os pacotes de dados são transmitidos do transmissor ao receptor através de um fluxo de pacotes que segue algumas etapas. Vamos considerar o exemplo de uma transmissão de dados de um computador A para um computador B em uma rede Ethernet:

1. A camada de aplicação do computador A gera os dados a serem transmitidos. Esses dados são divididos em pacotes pela camada de transporte.
2. A camada de transporte encapsula os dados em pacotes de transporte, adicionando um cabeçalho que contém informações sobre a origem, destino e outras informações relevantes.
3. Os pacotes de transporte são encapsulados na camada de rede, que adiciona um cabeçalho que contém informações sobre os endereços IP de origem e destino.
4. Os pacotes de rede são encapsulados na camada de enlace de dados, que adiciona um cabeçalho e um trailer que contêm informações sobre os endereços MAC de origem e destino.
5. O pacote é transmitido do computador A para o switch mais próximo.
6. O switch recebe o pacote e encaminha-o para o switch ou roteador mais próximo que está conectado ao computador B.
7. O pacote é entregue ao computador B.
8. O computador B recebe o pacote e remove os cabeçalhos adicionados pelas camadas de rede, transporte e enlace de dados.
9. O computador B recompõe os dados originais a partir dos pacotes de transporte.
10. A camada de aplicação do computador B recebe os dados e os processa conforme necessário.

Essas etapas formam um fluxo de pacotes que garante a transmissão bem-sucedida de dados de um computador A para um computador B em uma rede de computadores.

# Orientadas a conexão

Conexões orientadas a conexão são conexões que exigem um estabelecimento explícito antes que a comunicação possa começar. Isso significa que um protocolo de estabelecimento de conexão é usado antes que os dados possam ser trocados entre os dispositivos. Essas conexões geralmente são mais confiáveis, pois permitem que os dispositivos confirmem que estão prontos para a comunicação antes que a transmissão de dados comece. Exemplos de protocolos orientados a conexão incluem o TCP (Transmission Control Protocol) e o protocolo de controle de sessão do OSI (Open Systems Interconnection).

# Não orientadas a conexão

Conexões não orientadas a conexão, por outro lado, não exigem um estabelecimento explícito antes que a comunicação possa começar. Isso significa que os dados podem ser enviados imediatamente entre os dispositivos, sem a necessidade de estabelecer uma conexão primeiro. Essas conexões geralmente são menos confiáveis, pois não há confirmação de que os dispositivos estão prontos para a comunicação antes que a transmissão de dados comece. Exemplos de protocolos não orientados a conexão incluem o UDP (User Datagram Protocol) e o protocolo de datagrama do OSI.

# Circuito virtual

Um circuito virtual é um tipo de conexão de rede em que os dispositivos se comunicam como se estivessem conectados por um circuito dedicado. Isso é feito por meio da criação de um caminho virtual entre os dispositivos, que é definido por um conjunto de conexões lógicas que são estabelecidas antes da transmissão de dados.

Em um circuito virtual, cada dispositivo é identificado por um número de identificação exclusivo e o caminho virtual é estabelecido antes que os dados possam ser transmitidos. Uma vez que o caminho virtual é estabelecido, os dados são transmitidos ao longo desse caminho, e as conexões lógicas são mantidas para garantir que os dados sejam entregues corretamente.

Os circuitos virtuais são usados em muitas redes de computadores, incluindo as redes de telefonia, a Internet e as redes de área ampla. Eles são úteis para aplicações que exigem uma conexão confiável e previsível entre dispositivos, como videoconferência, jogos online e transmissão de mídia.

Uma das vantagens dos circuitos virtuais é a sua eficiência. Eles permitem que os dispositivos compartilhem os recursos de rede de forma mais eficiente, pois o caminho virtual é mantido durante toda a duração da conexão. Além disso, os circuitos virtuais podem garantir que os dados sejam entregues na ordem correta e sem erros, pois as conexões lógicas são mantidas ao longo do caminho virtual. No entanto, eles podem ser mais complexos e exigir mais recursos de rede do que outros tipos de conexão, como as conexões sem circuito virtual.

# Primitivas de serviços

Operações básicas que são oferecidas por um sistema de comunicação para permitir que os processos de aplicação acessem e controlem os serviços de comunicação disponíveis na rede. Essas primitivas podem ser usadas pelos processos de aplicação para enviar e receber mensagens, configurar conexões de rede, gerenciar erros de comunicação, entre outras funções.

As primitivas de serviço geralmente incluem as seguintes operações básicas:

1. Estabelecer conexão: usado para estabelecer uma conexão de comunicação entre dois processos de aplicação.
2. Liberar conexão: usado para encerrar uma conexão de comunicação estabelecida anteriormente.
3. Enviar mensagem: usado para enviar uma mensagem de um processo de aplicação para outro.
4. Receber mensagem: usado para receber uma mensagem enviada por um processo de aplicação.
5. Aceitar conexão: usado para aceitar uma solicitação de conexão recebida de um processo de aplicação.
6. Recusar conexão: usado para recusar uma solicitação de conexão recebida de um processo de aplicação.

7. Consultar status: usado para obter informações sobre o status atual da conexão de comunicação.
8. Gerenciar erros: usado para lidar com erros de comunicação, como erros de conexão, perda de dados ou falhas de rede.

As primitivas de serviço são uma parte importante da interface de programação de aplicativos (API) de muitos sistemas de comunicação, incluindo a Internet e as redes de área ampla. Eles fornecem uma maneira padronizada para que os processos de aplicação acessem e controlem os serviços de comunicação disponíveis na rede, independentemente da plataforma ou tecnologia de rede subjacente.

# Modelo OSI

funções de comunicação de rede e os protocolos de comunicação que devem ser seguidos em uma rede de computadores. Ele foi desenvolvido pela ISO (International Organization for Standardization) e é amplamente usado como um guia para o desenvolvimento de redes de computadores e protocolos de comunicação.

Composto por sete camadas , cada um com conjunto específico de funções de comunicação

1. Camada Física: esta camada define as especificações elétricas, mecânicas e físicas para o transporte de dados através do meio físico de comunicação, como cabos e conectores.
2. Camada de Enlace de Dados: esta camada gerencia a transmissão de dados entre dispositivos na mesma rede física, corrigindo erros de transmissão e controlando o fluxo de dados.
3. Camada de Rede: esta camada é responsável pela roteamento de pacotes de dados através de redes múltiplas, bem como pela determinação de caminhos de roteamento e endereçamento de dispositivos na rede.
4. Camada de Transporte: esta camada fornece serviços de transporte de dados fim a fim, dividindo os dados em pacotes menores, verificando a integridade dos dados e garantindo que os pacotes sejam entregues em ordem.
5. Camada de Sessão: esta camada estabelece e gerencia sessões de comunicação entre processos de aplicação em diferentes dispositivos, permitindo a sincronização e o controle do diálogo de comunicação.
6. Camada de Apresentação: esta camada realiza a conversão de dados em formatos reconhecíveis pelo receptor, como criptografia, compressão e conversão de caracteres.
7. Camada de Aplicação: esta camada fornece serviços de aplicação para os usuários finais, como e-mail, navegação na web e transferência de arquivos.

# Modelo TCP/IP x OSI

é um modelo de referência de comunicação de rede que descreve as funções de comunicação de rede e os protocolos de comunicação usados em redes de computadores. É o modelo de referência mais amplamente usado em redes de computadores e é usado como modelo de referência para a Internet.

O modelo TCP/IP é composto por quatro camadas, que são:

1. Camada de Interface de Rede: esta camada define as especificações elétricas, mecânicas e físicas para o transporte de dados através do meio físico de comunicação, como cabos de rede, fibra óptica ou ondas de rádio. Esta camada também inclui protocolos como Ethernet, Wi-Fi e Bluetooth.
2. Camada de Internet: esta camada é responsável pelo roteamento de pacotes de dados através de redes múltiplas, bem como pela determinação de caminhos de roteamento e endereçamento de dispositivos na rede. O protocolo IP (Internet Protocol) é o principal protocolo utilizado nesta camada.
3. Camada de Transporte: esta camada fornece serviços de transporte de dados fim a fim, dividindo os dados em pacotes menores, verificando a integridade dos dados e garantindo que os pacotes sejam entregues em ordem. Os protocolos mais conhecidos nesta camada são o TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol).
4. Camada de Aplicação: esta camada fornece serviços de aplicação para os usuários finais, como e-mail, navegação na web e transferência de arquivos. Alguns exemplos de protocolos nesta camada são o HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol) e SMTP (Simple Mail Transfer Protocol).

O modelo TCP/IP é mais simples que o modelo OSI (Open Systems Interconnection), comumente usado como outro modelo de referência para a comunicação de rede. No entanto, o modelo TCP/IP é mais prático e mais usado em redes de computadores do mundo real, pois foi criado especificamente para a Internet e é amplamente usado em dispositivos de rede, como roteadores, switches e modems.

### Comparação do modelos TCP/IP e OSI

Uma das principais diferenças entre os dois modelos é que o Modelo OSI é mais teórico e conceitual, enquanto o Modelo TCP/IP é mais prático e orientado para a implementação. Além disso, o Modelo TCP/IP é amplamente utilizado na internet, enquanto o Modelo OSI é mais utilizado em ambientes empresariais.

Em resumo, ambos os modelos são estruturas de referência importantes para a comunicação em redes de computadores, mas diferem em suas abordagens e em como as camadas são definidas. O Modelo OSI é mais abstrato e teórico, enquanto o Modelo TCP/IP é mais concreto e prático.

# Modelo TCP/IP

O modelo TCP/IP (Transmission Control Protocol/Internet Protocol) é um conjunto de protocolos de comunicação usados para conectar dispositivos em uma rede de computadores. O modelo TCP/IP consiste em quatro camadas, cada uma com uma função específica: Camada de Acesso à Rede: Essa camada é responsável pela transmissão de dados na rede física e é responsável pela conexão e desconexão de dispositivos na rede. Protocolos comuns nesta camada incluem Ethernet, Wi-Fi e Bluetooth. Camada Internet: Esta camada é responsável pela transmissão de pacotes de dados entre diferentes redes, utilizando o protocolo IP (Internet Protocol). A principal função desta camada é fornecer um caminho de comunicação entre dispositivos através de uma rede global. Camada de Transporte: Essa camada é responsável pela transmissão de dados de ponta a ponta pela rede, utilizando protocolos como TCP (Transmission Control Protocol) e UDP (User Datagram Protocol). O TCP fornece uma conexão confiável e orientada à conexão, enquanto o UDP é mais rápido, mas menos confiável. Camada de aplicativo: essa camada fornece serviços de rede para aplicativos que usam a rede, como e-mail, navegação na Web e transferência de arquivos. Os protocolos comuns nesta camada incluem HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol) e SMTP (Simple Mail Transfer Protocol). O modelo TCP/IP é o protocolo de comunicação mais utilizado na Internet e é compatível com uma ampla variedade de dispositivos e sistemas operacionais.

O modelo TCP/IP é um modelo de rede em camadas que descreve como os dados são transmitidos pela rede. Ele é composto por quatro camadas principais:

1. Camada de aplicação: Essa camada é a camada mais alta do modelo TCP/IP e é onde as aplicações de rede são executadas. As aplicações de rede incluem serviços como HTTP, FTP, SMTP, DNS e Telnet.
2. Camada de transporte: Essa camada é responsável por garantir que os dados sejam entregues corretamente e sem erros. Ela é composta por dois protocolos principais: o TCP (Protocolo de Controle de Transmissão) e o UDP (Protocolo de Datagrama de Usuário).
3. Camada de rede: Essa camada é responsável por rotear os dados através da rede. Ela utiliza endereços IP para encaminhar os pacotes de dados para o destino correto.
4. Camada de enlace: Essa camada é responsável por controlar o acesso ao meio físico da rede, garantindo que apenas um dispositivo possa transmitir dados de cada vez. Ela também é responsável por dividir os dados em quadros e adicionar informações de controle, como endereços MAC.

Cada camada do modelo TCP/IP tem uma função específica na transmissão de dados e trabalha em conjunto para garantir que os dados sejam transmitidos com segurança, eficiência e confiabilidade através da rede.

# TCP e UDP

TCP (Transmission Control Protocol) e UDP (User Datagram Protocol) são dois protocolos de transporte diferentes que operam na camada de transporte do modelo TCP/IP.

O TCP é um protocolo orientado à conexão que garante que todos os dados sejam entregues corretamente e em ordem, e fornece confiabilidade na transmissão de dados. O TCP segmenta os dados em pacotes menores e estabelece uma conexão com o destinatário antes de enviar os dados. Ele também possui mecanismos de controle de congestionamento e retransmissão de pacotes perdidos ou danificados.

Por outro lado, o UDP é um protocolo sem conexão que não garante a entrega dos dados ou sua ordem. Ele simplesmente envia os dados em pacotes chamados datagramas para o destinatário, sem estabelecer uma conexão prévia. O UDP é geralmente usado para aplicativos que requerem alta velocidade de transmissão e que podem tolerar alguma perda de dados, como transmissão de áudio e vídeo em tempo real.

Em resumo, o TCP é mais lento e confiável, enquanto o UDP é mais rápido, mas menos confiável. A escolha entre TCP e UDP depende do tipo de aplicação e dos requisitos de transmissão de dados necessários.

# Ativos de redes

Ativos de rede são dispositivos de hardware e software utilizados para conectar computadores, servidores e outros dispositivos em uma rede de computadores. Esses ativos de rede permitem que os dispositivos se comuniquem entre si e compartilhem recursos, como arquivos, impressoras e conexão com a Internet. Alguns exemplos de ativos de rede incluem:

1. Roteadores: Dispositivos usados para conectar várias redes e encaminhar o tráfego entre elas.
2. Switches: Dispositivos usados para conectar dispositivos em uma rede local (LAN) e encaminhar o tráfego entre eles.
3. Pontos de acesso sem fio (APs): Dispositivos usados para fornecer conectividade sem fio para dispositivos em uma rede.
4. Firewalls: Dispositivos usados para proteger uma rede contra ameaças externas, como hackers e malware.
5. Servidores: Dispositivos usados para fornecer serviços de rede, como hospedagem de sites, compartilhamento de arquivos e armazenamento em nuvem.

Esses são apenas alguns exemplos de ativos de rede, mas existem muitos outros tipos de dispositivos e tecnologias que são usados para construir e gerenciar redes de computadores.

### Caracteristicas destes ativos de rede

1. Switch: é um dispositivo que conecta vários dispositivos em uma rede local (LAN). Ele atua como um hub central, permitindo que os dispositivos se comuniquem uns com os outros. O switch é capaz de identificar o endereço MAC (Media Access Control) de cada dispositivo conectado a ele e, assim, enviar o tráfego de dados para o dispositivo correto.
2. Roteador: é um dispositivo que conecta duas ou mais redes, como a internet e a rede local. Ele é capaz de encaminhar o tráfego de dados entre as diferentes redes, usando um protocolo de roteamento, como o OSPF (Open Shortest Path First) ou o BGP (Border Gateway Protocol). O roteador também pode ser usado para filtrar o tráfego de dados e bloquear o acesso a determinados sites ou serviços.
3. Firewall: é um dispositivo que protege a rede contra ameaças externas, como ataques de hackers, vírus e malware. Ele faz isso monitorando o tráfego de entrada e saída da rede e filtrando o tráfego suspeito. O firewall pode ser configurado para bloquear o acesso a determinados sites ou serviços, e também pode ser usado para criar regras de segurança personalizadas.
4. Access point: é um dispositivo que permite que dispositivos sem fio se conectem a uma rede local. Ele cria uma rede sem fio (Wi-Fi) que os dispositivos podem acessar. O access point é geralmente conectado a um switch ou roteador para fornecer conectividade com fio à rede.
5. Servidor: é um computador ou dispositivo de armazenamento que fornece serviços para outros dispositivos em uma rede. O servidor pode ser usado para armazenar arquivos e compartilhá-los com outros dispositivos na rede, executar aplicativos e serviços, como email, banco de dados e web, e gerenciar contas de usuário e permissões.
6. Modem: é um dispositivo que converte o sinal digital de um computador ou dispositivo de rede em um sinal analógico que pode ser transmitido por uma linha telefônica, cabo coaxial ou fibra óptica. Ele também converte o sinal analógico recebido de volta para o sinal digital que pode ser processado pelo computador ou dispositivo de rede.
7. HUB: é um dispositivo que permite que vários dispositivos em uma rede compartilhem uma única conexão de rede. Ele funciona transmitindo os dados para todos os dispositivos conectados a ele, independentemente do endereço MAC. Como resultado, o tráfego de rede em um hub pode se tornar congestionado, tornando-o menos eficiente do que um switch.

Esses são apenas alguns dos principais ativos de rede. Cada um desempenha um papel importante na construção e manutenção de uma rede de computadores funcional.