

---

## Semana 12 - Aula 1

Tópico Principal da Aula: Protocolos e Camadas - Camada de Transporte: Controle de Fluxo e Confiabilidade

**Subtítulo/Tema Específico:** Introdução à Camada de Transporte e suas Funções

**Código da aula:** [SIS]ANO1C2B2S12A1

### Objetivos da Aula:

- Compreender a camada de transporte do modelo OSI.
- Conhecer as funções da camada de transporte.

### Recursos Adicionais:

- Caderno para anotações;
- Recurso audiovisual para exibição de vídeos e imagens.

### Exposição do Conteúdo:

**Referência do Slide:** Slide 04 - Recapitulando

- **Definição:** Esta seção revisita conceitos da camada de rede (camada 3 do modelo OSI), especificamente sobre o IPv6 e a representação de endereços IP.
- **Aprofundamento/Complemento (se necessário):** A camada de rede é responsável pelo endereçamento e roteamento de pacotes entre redes. O IPv6, como mencionado, expande significativamente o número de endereços disponíveis em comparação com o IPv4, utilizando 128 bits, o que é crucial para o crescimento da internet e a proliferação de dispositivos conectados. A representação hexadecimal facilita a leitura e escrita desses longos endereços.
- **Exemplo Prático:** Ao acessar um site como "https://www.google.com/search?q=google.com", a camada de rede se encarrega de rotear os pacotes de dados do seu computador até o servidor do Google, utilizando o endereço IP (seja IPv4 ou IPv6) do servidor.

**Video:** <https://youtu.be/ykZpREKuELw?feature=shared>

#### Referência do Slide: Slide 05 - Camada de Transporte

- **Definição:** A camada de transporte, na arquitetura de redes, é a quarta camada do modelo OSI e a camada diretamente acima da camada de rede no modelo TCP/IP. Ela é responsável por fornecer comunicação lógica entre processos de aplicação que estão sendo executados em diferentes hosts. Isso significa que, do ponto de vista das aplicações, é como se houvesse uma conexão direta entre elas, independentemente da complexidade da rede subjacente.
- **Aprofundamento/Complemento (se necessário):** As principais responsabilidades da camada de transporte incluem a segmentação de dados da aplicação em unidades menores para transmissão (segmentos no TCP, datagramas no UDP), o controle de fluxo (para evitar que um remetente rápido sobrecarregue um receptor lento), o controle de erro (garantindo que todos os dados cheguem corretamente ao destino), e a multiplexação/demultiplexação (permitindo que múltiplas aplicações compartilhem a mesma conexão de rede).
- **Exemplo Prático:** Quando você assiste a um vídeo no YouTube e, ao mesmo tempo, navega em um site de notícias, a camada de transporte é a responsável por garantir que os dados do vídeo cheguem ao seu reprodutor de vídeo e os dados da página de notícias cheguem ao seu navegador, sem que haja confusão entre eles.

#### Referência do Slide: Slide 06 - Multiplexação e Demultiplexação

- **Definição:** Multiplexação é o processo pelo qual a camada de transporte em um host de origem combina dados de várias aplicações (processos) em um único fluxo de dados para ser transmitido pela rede. Demultiplexação é o processo inverso, onde a camada de transporte em um host de destino separa o fluxo de dados recebido e entrega os segmentos aos processos de aplicação corretos. Isso é feito através do uso de números de porta.
- **Aprofundamento/Complemento (se necessário):** Cada aplicação que deseja se comunicar pela rede é associada a um número de porta único. Quando um segmento chega ao host de destino, a camada de transporte examina o número da porta no cabeçalho do segmento para determinar qual processo de aplicação deve receber os dados. Isso permite que um único endereço IP (do host) seja compartilhado por várias aplicações simultaneamente.
- **Exemplo Prático:** Imagine um servidor web (porta 80/443) e um servidor de e-mail (porta 25/587) operando no mesmo computador com o mesmo endereço IP. Quando um pacote chega a esse IP, o número da porta no cabeçalho do pacote informa ao sistema operacional se ele deve ser entregue ao software do servidor web ou ao software do servidor de e-mail.

#### Referência do Slide: Slide 07 - Multiplexação e Demultiplexação: Porta

- **Definição:** Uma porta (port number) é um número de 16 bits que identifica um processo ou aplicação específica em um host que está enviando ou recebendo dados pela rede. As portas podem ser classificadas como "Portas Bem Conhecidas" (0-1023, atribuídas a serviços comuns como HTTP, FTP), "Portas Registradas" (1024-49151, para aplicações registradas por empresas ou desenvolvedores), e "Portas Dinâmicas/Privadas" (49152-65535, usadas por clientes para suas próprias comunicações efêmeras).
- **Aprofundamento/Complemento (se necessário):** Os números de porta, combinados com o endereço IP, formam um "socket", que é o ponto final de uma conexão de rede. A IANA (Internet Assigned Numbers Authority) é a organização responsável por manter o registro oficial de portas e os serviços associados a elas.
- **Exemplo Prático:** O serviço HTTP (navegação web) utiliza a porta 80 por padrão, e HTTPS (navegação web segura) utiliza a porta 443. Quando você digita "<http://www.exemplo.com>" no seu navegador, ele tenta se conectar ao servidor web na porta 80 (ou 443 para HTTPS) do endereço IP correspondente a "[www.exemplo.com](http://www.exemplo.com)".

#### Referência do Slide: Slide 08 - Multiplexação e Demultiplexação: Socket

- **Definição:** Um socket é uma interface de programação para comunicação em rede, que consiste na combinação de um endereço IP e um número de porta. Ele serve como um endpoint para a comunicação entre processos em diferentes hosts ou no mesmo host.
- **Aprofundamento/Complemento (se necessário):** Em termos de programação, um socket é um objeto que permite a um programa enviar e receber dados através de uma rede. Os sistemas operacionais fornecem APIs (Application Programming Interfaces) para que os programas possam criar e gerenciar sockets, abstraindo os detalhes de baixo nível da comunicação de rede.
- **Exemplo Prático:** Em um servidor, um socket pode ser configurado para "escutar" por conexões entrantes em uma porta específica. Quando um cliente tenta se conectar a essa porta, o servidor aceita a conexão e cria um novo socket para a comunicação com aquele cliente específico, permitindo que a comunicação ocorra.

---

## Semana 12 - Aula 2

Tópico Principal da Aula: Protocolos e Camadas - Camada de Transporte: Controle de Fluxo e Confiabilidade

**Subtítulo/Tema Específico:** Controle de Fluxo Parada e Espera (Stop-and-Wait) e Janela Deslizante (Sliding Window)

**Código da aula:** [SIS]ANO1C2B2S12A2

### Objetivos da Aula:

- Compreender o funcionamento do controle de fluxo e o protocolo TCP da Camada de Transporte.
- Conhecer o mecanismo de controle de fluxo parada e espera (stop and wait).
- Compreender o controle de fluxo de janela deslizante.

### Recursos Adicionais:

- Caderno para anotações;
- Recurso audiovisual para exibição de vídeos e imagens.

### Exposição do Conteúdo:

**Referência do Slide:** Slide 04 - Camada de transporte

- **Definição:** Relembra que a camada de transporte garante comunicações confiáveis, eficientes e ordenadas entre dispositivos em uma rede. Esta aula aprofundará o controle de fluxo e o protocolo TCP.
- **Aprofundamento/Complemento (se necessário):** A confiabilidade é um pilar da camada de transporte, especialmente com o TCP. Ela lida com a perda de pacotes, a duplicação e a entrega fora de ordem, garantindo que os dados cheguem ao destino exatamente como foram enviados. O controle de fluxo é um mecanismo crucial para evitar que o remetente sobrecarregue o receptor, garantindo que os dados sejam enviados a uma taxa que o receptor possa processar.
- **Exemplo Prático:** Imagine que você está baixando um arquivo grande. A camada de transporte, através do TCP, assegura que cada pedaço do arquivo chegue na ordem correta e que o download não seja interrompido por um envio de dados muito rápido que seu computador não consiga processar.

**Referência do Slide:** Slide 05 - Mecanismos de controle de fluxo

- **Definição:** Apresenta a necessidade de controle de fluxo em redes, onde a velocidade do remetente e do receptor pode variar. Os dois mecanismos principais discutidos são "Parada e Espera" e "Janela Deslizante".
- **Aprofundamento/Complemento (se necessário):** Sem controle de fluxo, um remetente rápido poderia enviar dados a uma taxa maior do que o receptor pode processar, resultando em perda de pacotes e retransmissões desnecessárias, diminuindo a eficiência da rede. O controle de fluxo visa otimizar a transferência de dados, adaptando-se às capacidades do receptor.
- **Exemplo Prático:** Pense em uma linha de produção. Se a primeira estação produz peças muito mais rápido do que a segunda estação pode montá-las, as peças se acumularão e algumas podem ser perdidas. O controle de fluxo seria como um mecanismo que sinaliza para a primeira estação diminuir a produção quando a segunda estação estiver sobrecarregada.

**Referência do Slide:** Slide 06 - Parada e espera

- **Definição:** No mecanismo "Parada e Espera" (Stop-and-Wait), o remetente envia um pacote de dados e, em seguida, aguarda um reconhecimento (ACK) do receptor antes de enviar o próximo pacote. Se o ACK não for recebido dentro de um determinado tempo limite, o remetente retransmite o pacote.
- **Aprofundamento/Complemento (se necessário):** Este é o mecanismo mais simples de controle de fluxo. Ele garante confiabilidade, mas é ineficiente em redes com alta latência ou longa distância, pois o remetente fica ocioso enquanto espera pelo ACK. O protocolo utiliza números de sequência para identificar os pacotes e evitar duplicações.
- **Exemplo Prático:** Imagine duas pessoas se comunicando por rádio em um local com muito eco. Uma pessoa fala uma frase, espera pela outra pessoa dizer "entendido" antes de falar a próxima frase. Se não ouvir "entendido", repete a frase.

**Referência do Slide:** Slide 07 - Janela deslizante

- **Definição:** O mecanismo "Janela Deslizante" (Sliding Window) permite que o remetente envie múltiplos pacotes sem esperar por um ACK para cada um, desde que o número de pacotes não reconhecidos esteja dentro de um tamanho de "janela" predefinido. O receptor envia ACKs cumulativos, indicando o próximo pacote esperado.
- **Aprofundamento/Complemento (se necessário):** Este método é muito mais eficiente que o "Parada e Espera" para redes com maior largura de banda ou latência. A "janela" é um buffer virtual que se move à medida que os dados são enviados e confirmados. Se houver perda de pacotes, o remetente pode retransmitir apenas os pacotes que não foram confirmados.

- **Exemplo Prático:** Pense em um caminhão entregando várias caixas para um depósito. Em vez de entregar uma caixa, esperar a confirmação do depósito e só então voltar para buscar a próxima, o caminhão pode levar um lote de 10 caixas. O depósito informa ao caminhão quais caixas já recebeu, e o caminhão continua entregando, ajustando a quantidade de caixas que pode enviar com base na capacidade do depósito.

#### Referência do Slide: Slide 08 - Protocolo TCP

- **Definição:** O Protocolo de Controle de Transmissão (TCP<sup>1</sup> - Transmission Control Protocol) é um dos principais protocolos da camada de transporte do modelo TCP/IP. É um protocolo orientado à conexão, confiável e que fornece controle de fluxo e controle de congestionamento.
- **Aprofundamento/Complemento (se necessário):** "Orientado à conexão" significa que o TCP estabelece uma conexão lógica (o "three-way handshake") entre o remetente e o receptor antes que a transmissão de dados comece, e encerra a conexão após a transmissão. A confiabilidade é alcançada através de números de sequência, ACKs, temporizadores e retransmissões. O controle de congestionamento evita que a rede seja sobrecarregada, ajustando a taxa de envio de dados com base nas condições da rede.
- **Exemplo Prático:** Ao realizar uma transação bancária online, o TCP garante que todos os dados da transação (seu login, valor, destinatário) cheguem ao servidor do banco de forma completa, na ordem correta e sem erros. Se houver um problema na rede, o TCP tentará retransmitir os dados até que sejam confirmados ou que a conexão falhe.

#### Referência do Slide: Slide 09 - Características do TCP

- **Definição:** As características essenciais do TCP incluem ser orientado à conexão (estabelecimento de sessão), ter controle de fluxo (gerenciar a taxa de envio de dados), controle de congestionamento (evitar a sobrecarga da rede), ser confiável (garantir a entrega de dados) e fornecer entrega em ordem (pacotes chegam na sequência correta).
- **Aprofundamento/Complemento (se necessário):** Cada uma dessas características contribui para a robustez do TCP. O estabelecimento de conexão (handshake) prepara os hosts para a comunicação. O controle de fluxo é implementado usando janelas deslizantes. O controle de congestionamento usa algoritmos complexos (como o slow start e congestion avoidance) para adaptar a taxa de envio. A confiabilidade é assegurada por mecanismos de retransmissão e verificação de integridade dos dados.
- **Exemplo Prático:** Um aplicativo de videoconferência pode usar TCP para enviar as informações de controle (como comandos de iniciar/parar a chamada), garantindo que esses comandos críticos sejam entregues

confiavelmente, mesmo que a transmissão de vídeo e áudio em tempo real possa usar um protocolo menos rigoroso (como UDP).

---

## Semana 12 - Aula 3

Tópico Principal da Aula: Protocolos e Camadas - Camada de Transporte: Controle de Fluxo e Confiabilidade

**Subtítulo/Tema Específico:** Protocolo UDP e Portas de Serviços

**Código da aula:** [SIS]ANO1C2B2S12A3

### Objetivos da Aula:

- Compreender o protocolo TCP e portas de serviços da camada de transporte.

### Recursos Adicionais:

- Caderno para anotações;
- Recurso audiovisual para exibição de vídeos e imagens.

### Exposição do Conteúdo:

#### Referência do Slide: Slide 04 - Recapitulando

- **Definição:** Esta seção relembra o que foi aprendido na aula anterior sobre o controle de fluxo e o protocolo TCP da camada de transporte, incluindo os mecanismos de parada e espera e janela deslizante.
- **Aprofundamento/Complemento (se necessário):** O controle de fluxo e o TCP são fundamentais para garantir a entrega confiável e ordenada de dados em redes complexas. A janela deslizante, em particular, otimiza o uso da largura de banda, permitindo que múltiplos segmentos sejam enviados sem esperar por um ACK para cada um, aumentando a eficiência da comunicação.
- **Exemplo Prático:** Ao enviar um e-mail com um anexo, o TCP se encarrega de dividir o anexo em segmentos, enviar esses segmentos e garantir que todos cheguem ao servidor de e-mail do destinatário na ordem correta e sem corrupção, retransmitindo qualquer segmento perdido.

#### Referência do Slide: Slide 05 - Camada de transporte

- **Definição:** Esta seção introduz o Protocolo de Datagramas de Usuário (UDP - User Datagram Protocol), contrastando-o com o TCP. O UDP é um protocolo da camada de transporte não orientado à conexão e não confiável, sendo mais rápido e leve que o TCP.



- **Aprofundamento/Complemento (se necessário):** Ao contrário do TCP, o UDP não estabelece uma conexão formal, não garante a entrega de pacotes, não controla o fluxo e não ordena os pacotes. Isso o torna ideal para aplicações onde a velocidade é mais crítica do que a confiabilidade total, e a perda ocasional de dados é aceitável.
- **Exemplo Prático:** Em uma transmissão de vídeo ao vivo, se alguns pacotes de dados de vídeo forem perdidos, a imagem pode ter pequenas falhas ou travamentos momentâneos, mas a transmissão continua em tempo real. Se o TCP fosse usado, a retransmissão de pacotes atrasaria a transmissão, tornando-a inviável para aplicações em tempo real.

#### **Referência do Slide:** Slide 06 - Características do UDP

- **Definição:** As principais características do UDP são: não orientado à conexão (não há estabelecimento de sessão), não confiável (não garante entrega), não oferece controle de fluxo, e é mais rápido e simples que o TCP.
- **Aprofundamento/Complemento (se necessário):** A simplicidade do UDP significa que ele tem menos sobrecarga de cabeçalho e não requer o gerenciamento de estados de conexão, o que resulta em menor latência. Sua natureza não confiável significa que a aplicação que o utiliza deve lidar com a perda, duplicação e reordenação de pacotes, se necessário.
- **Exemplo Prático:** Jogos online frequentemente utilizam UDP para o tráfego de dados de jogo (posição dos jogadores, disparos), pois um pequeno atraso para garantir a entrega de um pacote pode arruinar a experiência de jogo, enquanto a perda de um pacote ocasional é menos perceptível.

#### **Referência do Slide:** Slide 07 - Aplicações do UDP

- **Definição:** O UDP é frequentemente utilizado em aplicações que necessitam de baixa latência e onde a perda de pacotes é tolerável, como streaming de vídeo e áudio em tempo real, jogos online, DNS (Sistema de Nomes de Domínio) e VoIP (Voz sobre IP).
- **Aprofundamento/Complemento (se necessário):** Para o DNS, a natureza de requisição/resposta do UDP é ideal, pois uma única requisição e resposta podem ser processadas rapidamente. Se a resposta não chegar, a requisição pode ser retransmitida. Em VoIP, a voz humana é sensível a atrasos, então a prioridade é a entrega rápida, mesmo que alguns segmentos de áudio sejam perdidos.
- **Exemplo Prático:** Ao fazer uma chamada de voz pelo WhatsApp ou Skype, grande parte do tráfego de áudio é enviado via UDP para minimizar atrasos. A perda de alguns fragmentos de áudio pode resultar em uma breve interrupção na voz, mas a chamada continua fluida.

#### **Referência do Slide:** Slide 08 - TCP vs. UDP



- **Definição:** Este slide compara TCP e UDP, destacando suas diferenças principais: TCP é orientado à conexão, confiável, com controle de fluxo e congestionamento; UDP é não orientado à conexão, não confiável, e não possui esses controles, sendo mais rápido e leve.
- **Aprofundamento/Complemento (se necessário):** A escolha entre TCP e UDP depende dos requisitos da aplicação. Para aplicações que exigem alta integridade de dados (transferência de arquivos, e-mail), TCP é a escolha óbvia. Para aplicações que priorizam a velocidade e a tolerância a perdas (streaming, jogos), UDP é preferível.
- **Exemplo Prático:** Um navegador web usa TCP para carregar uma página (garantindo que todas as imagens, textos e scripts cheguem corretamente). Já um aplicativo que exibe feeds de notícias em tempo real, onde uma pequena atualização atrasada ou perdida não é crítica, pode usar UDP para atualizações rápidas.

**Referência do Slide:** Slide 09 - Portas de serviço

- **Definição:** As portas de serviço são números que identificam aplicações ou serviços específicos em um host. Elas permitem que o sistema operacional direcione o tráfego de rede para o processo correto. As portas são divididas em três categorias: Portas Bem Conhecidas (0-1023), Portas Registradas (1024-49151) e Portas Dinâmicas/Privadas (49152-65535).
- **Aprofundamento/Complemento (se necessário):** A IANA (Internet Assigned Numbers Authority) mantém a lista oficial de portas bem conhecidas e registradas. O uso de portas permite que vários serviços funcionem simultaneamente no mesmo servidor, utilizando o mesmo endereço IP, mas em portas diferentes.
- **Exemplo Prático:** O serviço FTP (File Transfer Protocol) utiliza as portas 20 (para controle) e 21 (para dados). Quando um cliente FTP se conecta a um servidor, ele tenta se comunicar nessas portas. Se um firewall está bloqueando essas portas, a comunicação FTP será impedida.

**Referência do Slide:** Slide 10 - Portas de serviço: TCP e UDP

- **Definição:** Ambos TCP e UDP utilizam números de porta para multiplexação e demultiplexação. Isso significa que, embora o número da porta possa ser o mesmo (ex: porta 53 para DNS), o contexto (TCP ou UDP) diferencia a comunicação. Por exemplo, DNS usa UDP para consultas rápidas e TCP para transferências de zona.
- **Aprofundamento/Complemento (se necessário):** É importante entender que um mesmo número de porta pode ser usado por um serviço TCP e um serviço UDP simultaneamente no mesmo host. O sistema operacional diferencia as conexões com base no protocolo (TCP ou UDP) e nos números de porta de origem e destino.

- **Exemplo Prático:** O serviço DNS (Domain Name System) utiliza a porta 53. Para consultas de nomes de domínio simples, ele geralmente usa UDP/53 devido à sua rapidez. No entanto, para transferências de zona DNS entre servidores (onde um servidor primário envia todo o seu banco de dados DNS para um servidor secundário), TCP/53 é usado para garantir a integridade e confiabilidade da transferência de dados.

---

Semana 13 - Aula 1

Tópico Principal da Aula: Topologia de Redes - Topologia em Malha e em Árvore

**Subtítulo/Tema Específico:** Introdução à Topologia em Malha

**Código da aula:** [SIS]ANO1C2B2S13A1

**Objetivos da Aula:**

- Compreender a topologia em malha e suas aplicações.

**Recursos Adicionais:**

- Caderno para anotações;
- Recurso audiovisual para a exibição de vídeos e imagens;
- Papel grande (para atividades práticas, se aplicável).

**Exposição do Conteúdo:**

**Referência do Slide:** Slide 04 - Vamos recapitular o que aprendemos sobre as topologias de rede

- **Definição:** Esta seção serve como uma revisão das topologias de rede previamente abordadas, como estrela, anel e barramento, e a importância de entender como os computadores estão interligados.
- **Aprofundamento/Complemento (se necessário):** Topologia de rede refere-se à arranjo físico ou lógico dos elementos de uma rede. Cada topologia tem suas próprias características, vantagens e desvantagens em termos de custo, desempenho, escalabilidade e resiliência a falhas. Relembrar as topologias básicas ajuda a contextualizar a topologia em malha.
- **Exemplo Prático:** A topologia em estrela, comum em redes domésticas e pequenas empresas, onde todos os dispositivos se conectam a um ponto central (como um roteador), facilita a detecção de problemas, mas o ponto central é um ponto único de falha. A topologia em barramento, mais antiga, onde todos os dispositivos compartilham um único cabo, é mais simples, mas a falha do cabo paralisa toda a rede.

#### Referência do Slide: Slide 05 - Topologia em malha

- **Definição:** A topologia em malha (ou *mesh topology*) é uma configuração de rede em que cada dispositivo está conectado com todos os outros dispositivos da rede, resultando em múltiplas rotas de comunicação.
- **Aprofundamento/Complemento (se necessário):** Existem dois tipos principais de topologia em malha: malha completa (full mesh), onde todos os nós estão conectados diretamente a todos os outros, e malha parcial (partial mesh), onde alguns nós estão conectados apenas aos nós com os quais mais se comunicam. A malha completa oferece o mais alto nível de redundância.
- **Exemplo Prático:** Imagine um grupo de amigos onde cada amigo tem uma linha de comunicação direta com todos os outros amigos. Se um amigo não puder se comunicar, os outros ainda podem falar entre si. Em uma rede, isso significa que se um cabo ou dispositivo falhar, o tráfego pode ser redirecionado por outras rotas.

#### Referência do Slide: Slide 06 - Topologia em malha: como funciona

- **Definição:** Na topologia em malha, os dados podem viajar de um dispositivo para outro através de múltiplos caminhos. Se um caminho falhar, o tráfego é automaticamente redirecionado para outro caminho disponível, garantindo alta redundância e tolerância a falhas.
- **Aprofundamento/Complemento (se necessário):** Para implementar uma topologia em malha, cada dispositivo precisa de várias interfaces de rede para se conectar aos outros dispositivos. Roteadores e switches inteligentes são frequentemente usados para gerenciar as rotas e garantir que o tráfego seja direcionado de forma eficiente. Protocolos de roteamento dinâmico são essenciais para que os nós descubram e utilizem os caminhos alternativos.
- **Exemplo Prático:** Em uma rede de câmeras de segurança de alta segurança em um banco, cada câmera e cada servidor de gravação podem estar conectados em uma topologia de malha. Se um cabo for cortado ou um servidor falhar, as imagens ainda podem ser gravadas e acessadas através de outros caminhos.

#### Referência do Slide: Slide 07 - Topologia em malha: vantagens

- **Definição:** As vantagens da topologia em malha incluem alta confiabilidade (devido à redundância de caminhos), maior tolerância a falhas (uma falha não derruba a rede inteira), melhor desempenho (múltiplos caminhos permitem balanceamento de carga) e segurança aprimorada (dificuldade de interceptação de dados).
- **Aprofundamento/Complemento (se necessário):** A redundância é a principal vantagem, pois garante que a rede permaneça operacional mesmo com a falha de vários links ou nós. O desempenho melhora porque o tráfego

pode ser distribuído por vários caminhos, evitando gargalos. A segurança é maior porque há muitos caminhos, dificultando para um invasor rastrear ou interromper todas as comunicações.

- **Exemplo Prático:** Redes de telecomunicações críticas, como as espinha dorsal da internet, frequentemente usam topologias em malha para garantir que o tráfego global não seja interrompido por falhas em um único ponto.

#### **Referência do Slide:** Slide 08 - Topologia em malha: desvantagens

- **Definição:** As desvantagens incluem o alto custo de implementação (muitos cabos e portas de interface), complexidade de gerenciamento (devido ao grande número de conexões) e escalabilidade limitada (adicionar novos dispositivos pode ser muito custoso e complexo).
- **Aprofundamento/Complemento (se necessário):** O número de conexões em uma malha completa cresce exponencialmente com o número de nós ( $N \times (N-1)/2$  conexões para  $N$  nós). Isso significa que, para redes muito grandes, a malha completa é impraticável. A complexidade de gerenciamento se manifesta na configuração de roteamento, manutenção de cabos e monitoramento de falhas.
- **Exemplo Prático:** Construir uma rede de malha completa para todos os computadores em um escritório grande seria proibitivamente caro, pois cada computador precisaria de várias placas de rede e seria necessário um emaranhado de cabos ligando todos a todos.

#### **Referência do Slide:** Slide 09 - Topologia em malha: aplicações

- **Definição:** A topologia em malha é usada em ambientes críticos onde a confiabilidade e a redundância são prioritárias, como redes de backbone da internet, redes de telecomunicações e infraestruturas de data centers.
- **Aprofundamento/Complemento (se necessário):** Além das aplicações listadas, a topologia em malha também é utilizada em redes sem fio (mesh networks) para estender a cobertura Wi-Fi e em ambientes industriais onde a disponibilidade contínua é fundamental para a operação de máquinas e processos.
- **Exemplo Prático:** Os sistemas de controle de tráfego aéreo, que exigem disponibilidade ininterrupta, podem usar topologias em malha para garantir que as informações sobre voos e aeronaves sejam sempre transmitidas, mesmo que haja falhas em equipamentos ou links de comunicação.

---

## Semana 13 - Aula 2

Tópico Principal da Aula: Topologia de Redes - Topologia em Malha e em Árvore

**Subtítulo/Tema Específico:** Topologia em Malha Sem Fio

**Código da aula:** [SIS]ANO1C2B2S13A2

### Objetivos da Aula:

- Compreender a topologia em malha sem fio e suas aplicações.

### Recursos Adicionais:

- Caderno para anotações;
- Recurso audiovisual para a exibição de vídeos e imagens;
- Papel grande (para atividades práticas, se aplicável).

### Exposição do Conteúdo:

**Referência do Slide:** Slide 04 - Vamos relembrar

- **Definição:** Esta seção recapitula o conceito de topologia em malha (ou *mesh topology*), onde cada dispositivo está conectado com todos os outros, e sua aplicação em ambientes críticos que exigem alta confiabilidade e redundância.
- **Aprofundamento/Complemento (se necessário):** A topologia em malha é intrinsecamente robusta devido à sua natureza de múltiplos caminhos. Isso contrasta com topologias mais simples, que podem ter pontos únicos de falha. A capacidade de autoconfiguração e auto-recuperação é um diferencial importante para redes de malha.
- **Exemplo Prático:** Em um campus universitário, se a rede principal falha, uma topologia em malha pode garantir que os serviços essenciais (como acesso à internet e sistemas acadêmicos) continuem operacionais através de caminhos alternativos.

**Referência do Slide:** Slide 05 - Topologia em malha sem fio

- **Definição:** A topologia em malha sem fio (wireless mesh network - WMN) segue princípios semelhantes aos da versão com fio, mas a comunicação entre os dispositivos ocorre sem cabos físicos, utilizando tecnologias sem fio como Wi-Fi. Dispositivos sem fio, como roteadores ou pontos de acesso, são interconectados para formar uma malha.
- **Aprofundamento/Complemento (se necessário):** Em uma WMN, os nós podem ser roteadores de malha que fornecem conectividade sem fio para dispositivos clientes, além de encaminharem o tráfego para outros roteadores

de malha. A ausência de cabos reduz a complexidade de implantação e o custo de infraestrutura física. As WMNs são frequentemente usadas em locais onde a cablagem é difícil ou impraticável.

- **Exemplo Prático:** Uma rede Wi-Fi em um grande evento ao ar livre, onde não é viável passar cabos por todo o local. Vários pontos de acesso sem fio podem ser configurados em uma malha, estendendo a cobertura e a capacidade da rede de forma flexível.

**Referência do Slide:** Slide 06 - Topologia em malha sem fio: como funciona

- **Definição:** Em uma WMN, cada nó (dispositivo sem fio) atua como um roteador, retransmitindo dados para outros nós da malha. Isso permite que a rede se estenda por uma área maior e forneça múltiplos caminhos para a comunicação, mantendo a redundância.
- **Aprofundamento/Complemento (se necessário):** Os nós em uma WMN são "inteligentes" e podem se comunicar dinamicamente entre si para encontrar os melhores caminhos para o tráfego de dados. Eles utilizam algoritmos de roteamento específicos para redes de malha sem fio, que consideram métricas como intensidade do sinal, latência e disponibilidade de largura de banda.
- **Exemplo Prático:** Em uma cidade inteligente, postes de luz equipados com roteadores de malha sem fio podem criar uma rede municipal que oferece Wi-Fi público e conecta sensores IoT (Internet das Coisas), como sensores de tráfego ou qualidade do ar, em toda a área.

**Referência do Slide:** Slide 07 - Topologia em malha sem fio: vantagens

- **Definição:** As vantagens da topologia em malha sem fio incluem flexibilidade (fácil implantação e reconfiguração), auto-organização (os nós podem se configurar e adaptar automaticamente), escalabilidade (fácil adicionar novos nós), alta confiabilidade (redundância sem fio) e cobertura estendida.
- **Aprofundamento/Complemento (se necessário):** A flexibilidade permite que a rede seja rapidamente expandida ou modificada conforme as necessidades, sem a necessidade de reconfiguração manual extensiva. A auto-organização e a auto-recuperação são cruciais, pois os nós podem detectar falhas e encontrar rotas alternativas sem intervenção humana.
- **Exemplo Prático:** Uma fazenda inteligente pode usar uma rede de malha sem fio para conectar sensores de solo e equipamentos de irrigação em uma vasta área, permitindo que os dados sejam coletados e enviados para um sistema central, mesmo em locais remotos.

**Referência do Slide:** Slide 08 - Topologia em malha sem fio: desvantagens

- **Definição:** As desvantagens incluem maior custo inicial (nós de malha mais caros), consumo de energia (nós ativos gastam mais bateria), potencial de

interferência (ambiente sem fio congestionado) e menor segurança (inerente à transmissão sem fio, embora criptografia ajude).

- **Aprofundamento/Complemento (se necessário):** O custo dos equipamentos pode ser mais alto porque os roteadores de malha são mais complexos do que os roteadores Wi-Fi comuns. O consumo de energia é um fator importante para nós alimentados por bateria. A interferência é um desafio comum em ambientes sem fio, e a segurança requer atenção extra, como o uso de criptografia forte (WPA3) e autenticação de dois fatores.
- **Exemplo Prático:** Em um hospital, embora a flexibilidade seja desejável, a interferência de equipamentos médicos e a necessidade de segurança robusta para dados de pacientes tornam a implantação de uma WMN um desafio que exige planejamento cuidadoso e mitigação de riscos.

**Referência do Slide:** Slide 09 - Topologia em malha sem fio: aplicações

- **Definição:** A topologia em malha sem fio é utilizada em ambientes como cidades inteligentes (para monitoramento e Wi-Fi público), redes corporativas (estender cobertura Wi-Fi), segurança pública (comunicações de emergência) e ambientes domésticos (sistemas Wi-Fi mesh).
- **Aprofundamento/Complemento (se necessário):** Além dessas aplicações, as WMNs também são usadas em ambientes industriais (IoT industrial), agricultura de precisão e até mesmo para comunicação em veículos autônomos. A capacidade de oferecer cobertura ubíqua e robusta é o principal atrativo.
- **Exemplo Prático:** Sistemas de Wi-Fi mesh para casa, como Google Nest Wifi ou TP-Link Deco, são um exemplo popular de WMN. Eles permitem que múltiplos roteadores funcionem juntos para fornecer uma cobertura Wi-Fi forte e consistente em toda a residência, eliminando pontos cegos.

---

Semana 13 - Aula 3

Tópico Principal da Aula: Topologia de Redes - Topologia em Malha e em Árvore

**Subtítulo/Tema Específico:** Topologia em Árvore

**Código da aula:** [SIS]ANO1C2B2S13A3

**Objetivos da Aula:**

- Compreender a topologia em árvore e suas aplicações.

**Recursos Adicionais:**

- Caderno para anotações;
- Recurso audiovisual para a exibição de vídeos e imagens;



- Papel grande (para atividades práticas, se aplicável).

## Exposição do Conteúdo:

### Referência do Slide: Slide 04 - Relembrando

- **Definição:** Esta seção serve como uma revisão rápida sobre a topologia em malha, tanto com fio quanto sem fio, e suas características de redundância e flexibilidade.
- **Aprofundamento/Complemento (se necessário):** A topologia em malha, em suas duas formas, é valorizada pela resiliência e capacidade de auto-recuperação. No entanto, é importante lembrar que a complexidade e o custo aumentam significativamente com o número de nós, especialmente na malha completa.
- **Exemplo Prático:** Em um cenário de recuperação de desastres, uma rede de malha sem fio pode ser rapidamente implantada para fornecer comunicação de emergência em áreas afetadas, onde a infraestrutura tradicional foi danificada.

### Referência do Slide: Slide 05 - Topologia em árvore

- **Definição:** A topologia em árvore (ou *tree topology*) é uma estrutura híbrida que combina as características da topologia em estrela e da topologia em barramento. Ela se organiza em uma hierarquia, com um nó central (raiz) e nós secundários que se ramificam a partir dele, formando uma estrutura semelhante a uma árvore.
- **Aprofundamento/Complemento (se necessário):** Na topologia em árvore, grupos de dispositivos são conectados a um hub ou switch secundário, que por sua vez se conecta a um hub ou switch de nível superior, e assim por diante, até um hub central. Isso permite que a rede seja segmentada em grupos lógicos, o que pode melhorar o gerenciamento e a contenção de problemas.
- **Exemplo Prático:** A estrutura de uma grande empresa com vários departamentos. Cada departamento pode ter sua própria rede em estrela (com um switch departamental), e esses switches departamentais se conectam a um switch central na sala de servidores principal da empresa, formando uma estrutura de árvore.

### Referência do Slide: Slide 06 - Topologia em árvore: como funciona

- **Definição:** A topologia em árvore utiliza um nó central que atua como o tronco da árvore, do qual se ramificam outros nós. Cada nó secundário pode, por sua vez, ter outros nós conectados a ele, criando uma hierarquia. Os dados fluem de e para o nó central através dos ramificações.

- **Aprofundamento/Complemento (se necessário):** A comunicação entre dois nós em ramos diferentes da árvore deve passar pelo nó pai comum ou, em última instância, pelo nó raiz. Isso pode introduzir um gargalo no nó raiz se o tráfego for muito intenso. No entanto, a segmentação da rede pode isolar problemas e limitar o domínio de broadcast.
- **Exemplo Prático:** A rede de uma escola com múltiplos laboratórios de informática. Cada laboratório tem um switch que conecta os computadores do laboratório (topologia estrela local). Todos esses switches de laboratório se conectam a um switch principal no prédio da administração, que serve como o tronco da árvore, conectando a internet.

**Referência do Slide:** Slide 07 - Topologia em árvore: vantagens

- **Definição:** As vantagens da topologia em árvore incluem a escalabilidade (fácil de expandir adicionando novos ramos), facilidade de gerenciamento e isolamento de falhas (um problema em um ramo não afeta toda a rede), e a capacidade de suportar múltiplos segmentos de rede.
- **Aprofundamento/Complemento (se necessário):** A escalabilidade é uma grande vantagem, pois novos segmentos (estrelas) podem ser adicionados sem afetar a estrutura existente. A hierarquia simplifica o gerenciamento, pois os administradores podem focar em segmentos específicos da rede. O isolamento de falhas significa que um problema em um switch de um ramo afetará apenas os dispositivos conectados a ele, não a rede inteira.
- **Exemplo Prático:** Em um shopping center, cada loja pode ter sua própria pequena rede, e todas essas redes se conectam a um backbone central. Se a rede de uma loja específica tiver um problema, isso não afetará as outras lojas nem o sistema de gerenciamento central do shopping.

**Referência do Slide:** Slide 08 - Topologia em árvore: desvantagens

- **Definição:** As desvantagens da topologia em árvore são a dependência do nó central (se o nó raiz falhar, toda a rede falha), o aumento do custo (mais cabeamento e hardware de rede do que topologias mais simples), e a complexidade na configuração inicial.
- **Aprofundamento/Complemento (se necessário):** O nó central é um ponto único de falha crítico, exigindo redundância se a alta disponibilidade for uma prioridade. O custo de cabeamento pode ser significativo em grandes redes, pois há uma necessidade de cabos para cada nível da hierarquia. A configuração inicial pode ser mais complexa do que em topologias simples, exigindo um planejamento cuidadoso da estrutura hierárquica.
- **Exemplo Prático:** Se o switch principal no centro de um campus universitário falhar, todos os laboratórios e escritórios conectados a ele perderão a conectividade com a internet e entre si, paralisando as operações.

**Referência do Slide:** Slide 09 - Topologia em árvore: aplicações

- **Definição:** A topologia em árvore é amplamente utilizada em redes de campus universitários, grandes empresas, redes de televisão a cabo e outras infraestruturas que requerem uma estrutura hierárquica e segmentação de rede.
  - **Aprofundamento/Complemento (se necessário):** Essa topologia é particularmente útil em ambientes onde o crescimento é esperado e a segmentação de rede é desejável para gerenciar o tráfego e a segurança. É uma escolha comum para redes locais (LANs) de médio a grande porte.
  - **Exemplo Prático:** Uma grande corporação com múltiplos andares ou prédios pode usar uma topologia em árvore. Cada andar ou prédio pode ter seu próprio switch ou hub, e esses switches se conectam a um switch de distribuição central, que por sua vez se conecta ao switch core da empresa.
-