

INTERNET E REDE DE COMPUTADORES II

INTERNET / REDE DE COMPUTADORES II

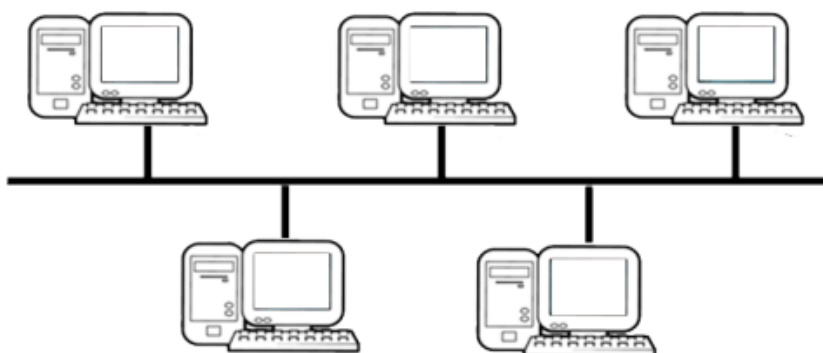
Os meios de transmissão não guiados diferem dos guiados principalmente pela ausência de um condutor físico, como um cabo. Nos meios não guiados, a transmissão de dados ocorre através de um meio físico distinto, o ar, que é utilizado como veículo para a propagação dos sinais. É importante destacar que não se deve confundir “meio físico” com “meio guiado”; o ar, embora não envolva cabos, ainda é um meio físico de transmissão.

MEIOS DE TRANSMISSÃO:

- Transmissão por rádio.
- Micro-ondas.
- Infravermelho.
- Transmissão por satélites.

Entre as tecnologias que utilizam meios não guiados, destacam-se a transmissão por rádio, micro-ondas, infravermelho e satélites. Nesses casos, não há cabos interligando os dispositivos; a transmissão se dá diretamente através do ar. Entretanto, é preciso considerar que esse tipo de transmissão está sujeito a interferências, como condições atmosféricas e obstáculos físicos, que podem afetar a qualidade do sinal.

TOPOLOGIA BARRAMENTO (LINEAR)



- Pode usar cabo coaxial ou cabo par trançado*;
- Pode ocorrer colisão (CSMA/CD);
- Rompimento cabo para a rede.

A topologia de barramento, também conhecida como linear, consiste em uma configuração na qual um único cabo é utilizado para conectar os computadores em uma rede. Nesse modelo, os computadores são conectados ao cabo, que serve como um meio de comunicação entre eles. Embora a disposição visual sugira que os computadores estejam organizados de forma linear, na prática, a disposição física pode variar.

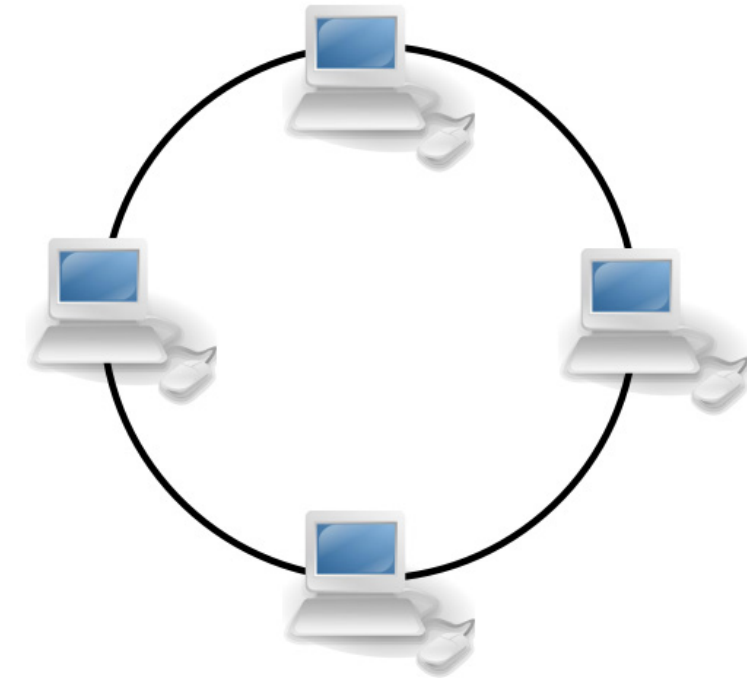
Para a interligação dos computadores, é possível utilizar cabos coaxiais ou, mais comumente, cabos de par trançado. Um dos desafios desse modelo de topologia é a possibilidade de colisões, que ocorrem quando dois ou mais computadores tentam transmitir dados simultaneamente, gerando conflitos na comunicação. Um exemplo seria uma situação em que, durante uma reunião, duas pessoas tentam falar ao mesmo tempo, interrompendo-se mutuamente até que uma decida ceder a vez à outra.

Para resolver esse problema de colisão, utiliza-se um algoritmo denominado CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Esse algoritmo atua gerando um intervalo de tempo aleatório, o que impede que os computadores tentem se comunicar simultaneamente, permitindo uma transmissão ordenada dos dados.

No algoritmo CSMA/CD, quando ocorre uma colisão, o sistema introduz um tempo de espera aleatório antes de permitir que os computadores tentem retransmitir os dados. Por exemplo, um computador pode ser instruído a esperar 10 segundos, enquanto outro aguarda um período adicional de tempo. Isso reduz a probabilidade de uma nova colisão, garantindo que a comunicação ocorra de forma ordenada. A informação sobre a colisão é então propagada para os outros computadores, permitindo que eles também ajustem suas transmissões.

No caso de colisões, somente um computador pode se comunicar por vez, uma vez que dois computadores tentando transmitir simultaneamente não serão capazes de se comunicar corretamente. Além disso, se ocorrer o rompimento do cabo principal da rede, a comunicação será interrompida, paralisando o funcionamento da rede.

TOPOLOGIA ANEL (TOKEN RING)



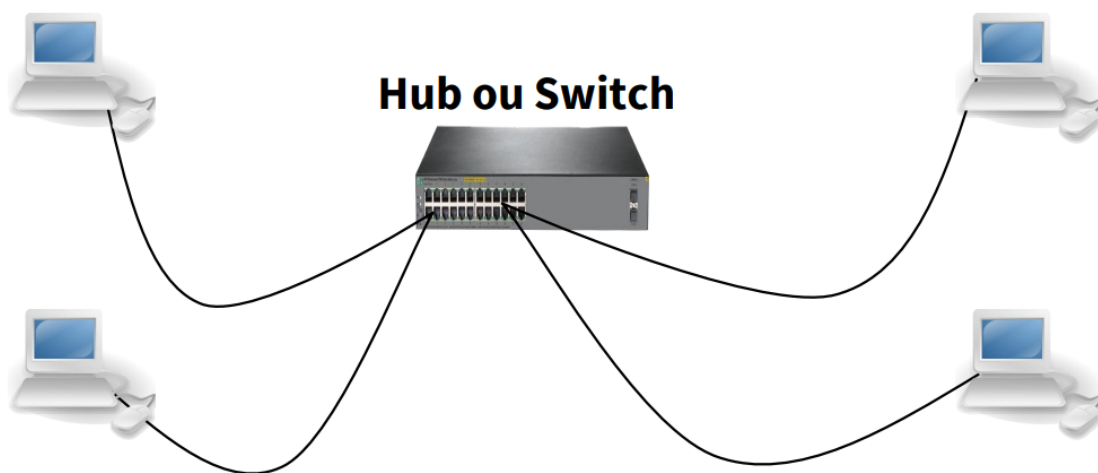
- Rompimento cabo para a rede;
- Para “falar” computador precisa do token;
- Praticamente imune a colisões.

Na topologia em anel, também conhecida como token ring, a comunicação é organizada de forma circular. Nesse modelo, um token, que pode ser comparado a um bastão, circula pela rede. Para que um computador transmita dados, ele precisa possuir o token. Caso o cabo se rompa, a rede também será paralisada, impedindo a comunicação entre os dispositivos. Embora existam variantes dessa topologia, como a configuração com cabo duplo, a versão mais comum, frequentemente abordada em provas, é aquela que não possui redundância no cabo.

Quando o computador precisa transmitir dados, aguarda a chegada do token, o qual circula pela rede. Após a chegada do token, o computador pode iniciar a comunicação. Esse processo torna a topologia em anel praticamente imune a colisões, uma vez que dois computadores não podem tentar se comunicar simultaneamente, a menos que possuam o token.

TOPOLOGIA ESTRELA HUB OU SWITCH

TOPOLOGIA ESTRELA



Atualmente, a topologia mais utilizada é a topologia estrela. Nessa configuração, a comunicação é centralizada por um concentrador, que pode ser um hub ou um switch. Esses dispositivos são responsáveis por concentrar as conexões entre os computadores na rede.

A principal vantagem da topologia estrela é que, em caso de falha no cabo de um computador, como o computador A, apenas esse computador será desconectado da rede, enquanto os demais continuarão funcionando normalmente. O funcionamento da rede não é interrompido, uma vez que não há dependência entre os computadores. Assim, a comunicação na rede continua sem problemas, mesmo quando ocorrem falhas localizadas. A seguir, abordam-se as principais diferenças entre um hub e um switch.

O hub, como concentrador, possui a característica de propagar informações para todas as portas simultaneamente. Esse dispositivo envia uma mensagem para todos os dispositivos conectados, independentemente de quem seja o destinatário. Por exemplo, em uma analogia, imagine um corredor com várias salas perpendiculares. Se uma pessoa em uma das pontas do corredor deseja comunicar algo a João, todos na proximidade ouvirão a mensagem, embora somente João seja o destinatário correto.

Essa característica do hub pode resultar em colisões, já que ele transmite as informações para todos os dispositivos na rede. Quando dois computadores tentam se comunicar ao mesmo tempo, pode ocorrer interferência, exigindo o uso de um algoritmo específico para resolver a colisão.

Em contrapartida, o switch é um dispositivo mais inteligente. Ao contrário do hub, que envia as mensagens para todos, o switch gerencia de forma individualizada as portas da rede. Ele transmite as informações apenas para o dispositivo correto, evitando colisões e garantindo a eficiência da comunicação. Esse gerenciamento eficaz das portas torna o switch imune a colisões, pois a transmissão de dados é direcionada exclusivamente ao receptor destinado.



5m

TOPOLOGIA SEM FIO (WIRELESS)



A topologia sem fio, também conhecida como wireless, tem a característica de propagar o sinal em todas as direções, embora a imagem apresentada possa sugerir um direcionamento específico. O sinal wireless se comporta de maneira similar às ondas geradas quando uma pedra é lançada em um lago, onde a água parada propaga-se em todas as direções. Contudo, deve-se destacar que o sinal está sujeito a interferências, principalmente de outras frequências semelhantes ou idênticas, como no caso de micro-ondas, telefones sem fio ou dispositivos domésticos que podem gerar ruído. Além disso, obstáculos físicos, como paredes, podem atenuar o sinal. Por exemplo, ao posicionar um roteador wireless em um cômodo, o sinal pode ser obstruído pela parede, diminuindo sua intensidade à medida que ultrapassa barreiras, até que desapareça completamente. Por essa razão, é fundamental escolher cuidadosamente a localização do roteador para garantir uma cobertura ideal.

TOPOLOGIA SEM FIO MALHA (MESH)



A topologia wireless também pode ser implementada em malha, ou seja, em uma configuração mesh, onde os dispositivos são interconectados de maneira independente entre si. Em uma rede mesh, como em uma residência, por exemplo, cada dispositivo pode se comunicar diretamente com os outros, sem depender de um único ponto central. Essa estrutura proporciona maior flexibilidade e resiliência à rede, especialmente em ambientes com obstáculos físicos, como paredes espessas, que podem dificultar a propagação do sinal em redes sem fio convencionais.

Ao posicionar um roteador wireless em um quarto, destinado aos equipamentos, o sinal não alcança adequadamente a sala, que está próxima. Para resolver essa questão, foi utilizado um dispositivo adicional que recebe o sinal fraco e o amplifica, similar à função de dois roteadores conectados. Esse equipamento aumenta a intensidade do sinal, permitindo uma cobertura mais eficiente.

Uma característica importante de uma rede mesh é que ela configura uma única rede. Ao transitar de um ambiente para outro, o dispositivo não precisa alternar de rede manualmente. O sistema identifica automaticamente o ponto de conexão com o sinal mais forte e realiza a troca sem a intervenção do usuário.

Anteriormente, as pessoas utilizavam repetidores wireless para amplificar o sinal, que, embora mantivesse o nome e a senha da rede, exigia a troca manual de rede ao transitar entre diferentes áreas. Alguns dispositivos modernos, como celulares, já conseguem realizar essa troca de forma automática. No entanto, em computadores, a troca manual ainda era necessária, o que, muitas vezes, se tornava um processo inconveniente. A rede mesh resolve esse problema, criando uma única rede integrada. Nessa configuração, os roteadores adicionais, chamados de nós, ampliam a cobertura, espelhando o sinal da rede principal.

Por exemplo, um colega, proprietário de uma residência maior, com dois andares e uma piscina, solicitou uma solução para expandir a rede sem fio em seu imóvel. A recomendação foi a implementação de uma rede mesh, que permitiria uma cobertura mais eficiente em todo o ambiente.

Para expandir uma rede, é recomendável utilizar no mínimo três ou quatro nós. O primeiro nó recebe o sinal na sala e transmite para o nó superior, que, por sua vez, se comunica com o nó inferior. Dessa forma, os nós estabelecem uma comunicação entre si. A adição ou remoção de nós é um processo simples, permitindo a fácil expansão ou redução da rede conforme necessário.

WIRELESS

Ao abordar as redes wireless, torna-se relevante compreender algumas terminologias a elas associadas.

- **WI-FI – IEEE 802.11:**

A rede Wi-Fi é regulamentada pelo padrão IEEE 802.11, cuja nomenclatura é amplamente empregada e comumente encontrada em exames.

O IEEE, Instituto de Engenheiros Eletricistas e Eletrônicos, é a organização responsável pela criação de normas e padrões para a internet. Existem outros institutos e normas que também regem aspectos da internet, mas o que deve ser lembrado no contexto do Wi-Fi é que o padrão 802.11 foi o primeiro a ser estabelecido para esse tipo de rede.

Grças a essa norma, por exemplo, ao adquirir um equipamento wireless, como um roteador AC, nos Estados Unidos e trazê-lo para o Brasil, ele poderá se conectar com os dispositivos compatíveis com a mesma tecnologia. A norma IEEE 802.11 garante a compatibilidade global entre os equipamentos, estabelecendo um padrão de comunicação universal para os dispositivos.

- **802.11a 54Mbps 5Ghz:**

O desenvolvimento do Wi-Fi trouxe melhorias ao longo do tempo, com avanços em suas versões. O padrão 802.11a, que ainda é mencionado em algumas provas, é uma versão antiga que já não é mais utilizada. Essa versão oferecia uma velocidade de 54 megabits por segundo, utilizando a frequência de 5 GHz. Vale ressaltar que o “b” minúsculo se refere a bits e não a bytes, o que é uma confusão comum.

Atualmente, as frequências mais comuns para equipamentos Wi-Fi são 2.4 GHz e 5 GHz. A frequência de 2.4 GHz é amplamente utilizada, principalmente devido ao seu alcance. Ela é eficaz para atravessar paredes, o que a torna útil em ambientes onde o sinal precisa percorrer longas distâncias. No entanto, essa frequência apresenta limitações em termos de velocidade e é mais suscetível a interferências de outros dispositivos, como micro-ondas e telefones sem fio, que também operam na mesma faixa. Essa interferência pode ser minimizada, muitas vezes, ajustando o canal de comunicação.



10m

Em contraste, a frequência de 5 GHz oferece maior resistência a interferências devido à diferença nas frequências utilizadas, o que a torna mais confiável. Embora o alcance dessa frequência seja inferior ao de 2.4 GHz, ela proporciona velocidades superiores, sendo mais adequada para aplicações que exigem maior desempenho na transmissão de dados.

Em ambientes com pouco espaço e alta demanda por velocidade, a melhor opção é a frequência de 5 GHz. No entanto, ao transitar de um cômodo para outro, a frequência de 2.4 GHz costuma ser mais eficaz devido ao seu alcance superior. Questões sobre essas escolhas de frequências frequentemente aparecem em provas, como, por exemplo, em situações em que um equipamento colocado no quarto apresenta um alcance limitado na sala. Nesse caso, a escolha mais apropriada seria a frequência de 2.4 GHz, devido à sua maior cobertura em ambientes mais amplos. Caso o ambiente necessite de mais velocidade, a frequência de 5 GHz é a opção recomendada.

- 802.11**b** 11Mb/s 2.4Ghz:
- 802.11**g** 54Mb/s 2.4Ghz:
- 802.11**n** 450Mb/s 2,4 GHz e 5 GHz – MIMO:
- 802.11**ac** 1300Mb/s 5Ghz:
- 802.11**ax** 10Gb/s 2,4 GHz, 5 GHz e 6 GHz:
- 802.11**be** 46Gb/s 2,4 GHz, 5 GHz e 6 GHz:

O padrão 802.11b, lançado posteriormente, oferece uma velocidade de 11 megabits por segundo e opera na frequência de 2.4 GHz. Já o 802.11g, que também utiliza a mesma frequência, voltou a atingir uma velocidade de 54 megabits por segundo. O padrão 802.11n, por sua vez, trouxe avanços significativos, alcançando 450 megabits por segundo e permitindo o uso simultâneo das frequências de 2.4 GHz e 5 GHz. O dispositivo escolhe automaticamente a rede a ser utilizada, dependendo da disponibilidade de cada frequência.

Além disso, o 802.11n introduziu a tecnologia MIMO (Múltiplas Entradas e Múltiplas Saídas), que possibilita a utilização de múltiplas antenas para envio e recebimento simultâneo de dados. Essa melhoria na capacidade de transmissão resultou em um aumento considerável na velocidade da rede, promovendo uma significativa evolução no desempenho da tecnologia.

O padrão 802.11ac, também conhecido como AC, proporcionou um aumento significativo na velocidade, alcançando 1300 megabits por segundo, utilizando principalmente a frequência de 5 GHz. Em seguida, o padrão 802.11ax, ou AX, atingiu a impressionante marca de 10 gigabits por segundo, representando uma transformação significativa na capacidade de transmissão de dados.

Para contextualizar essa evolução, é importante observar que para alcançar 1 gigabit, é necessário cerca de 1.000 megabits, o que evidencia o grande avanço nos padrões de rede sem fio. O 802.11ax opera nas frequências de 2.4, 5 e 6 GHz, sendo a introdução da frequência de 6 GHz um grande diferencial, proporcionando ainda mais eficiência, com características semelhantes às da frequência de 5 GHz.

Atualmente, o padrão 802.11be (BE) alcança velocidades de até 46 Gbps, também utilizando as frequências de 2.4, 5 e 6 GHz, com a frequência de 6 GHz oferecendo uma maior eficiência na transmissão de dados.

SEGURANÇA:

Protocolo	Segurança Atual	Criptografia
WEP	Obsoleto/Inseguro	RC4 (40/104 bits)
WPA	Obsoleto/Inseguro	TKIP
WPA2	Moderado	AES-CCMP
WPA3	Atual/Superior	AES + SAE + OWE

Em relação à segurança, os protocolos de criptografia começaram com o WEP, utilizado nos primeiros estágios do Wi-Fi. O objetivo principal desses protocolos de segurança é proteger os dados transmitidos pelo ar, uma vez que qualquer pessoa com o equipamento adequado pode interceptar as informações em trânsito. A implementação de criptografia visa proteger as senhas e dados durante a transmissão, garantindo a segurança da comunicação sem fio.

O aplicativo atualmente é considerado obsoleto e inseguro, devendo ser evitado. A criptografia utilizada nesse aplicativo é o algoritmo RC4, o qual não exige memorização para fins de avaliação, uma vez que é muito improvável que esse tema seja abordado em provas.

Posteriormente, foi desenvolvido o WPA, que também é atualmente considerado obsoleto e inseguro, utilizando o método de criptografia TKIP. Em seguida, surgiu o WPA2, que, embora ainda utilizado, é considerado moderadamente seguro. Esse protocolo não é obsoleto, mas apresenta algumas vulnerabilidades, dado que é uma evolução do WPA, que por sua vez, se baseava no WEP. O WPA2 trouxe melhorias substanciais ao utilizar o algoritmo de criptografia AES, que é muito mais seguro, e o CCMP.

O WPA3 é o protocolo mais recente e superior, empregando os algoritmos criptográficos AES, SAE e WE. Esses são os principais protocolos de segurança aplicados às redes Wi-Fi, e podem ser cobrados em avaliações sobre a tecnologia.



DIRETO DO CONCURSO

01. (COPESE/UFPI/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/2024) Sobre a tecnologia Wi-Fi, assinale a opção CORRETA:

- a) Wi-Fi utiliza o método de acesso CSMA/CD (Carrier Sense Multiple Access with Collision Detection) para gerenciar o tráfego na rede.
- b) Wi-Fi opera exclusivamente na faixa de frequência de 5 GHz.
- c) Wi-Fi permite a comunicação sem fio entre dispositivos usando padrões definidos pela IEEE, como 802.11a, 802.11b, 802.11g, 802.11n e 802.11ac.
- d) Wi-Fi exige uma conexão guiada entre os dispositivos e um ponto de acesso (AP).
- e) Wi-Fi não suporta criptografia para proteger os dados transmitidos.



- a) O método “CD” refere-se ao meio guiado, enquanto, no caso do Wi-Fi, utiliza-se o “CA” (Carrier Sense Multiple Access with Collision Avoidance), que tem como objetivo gerenciar o tráfego na rede, evitando colisões, o que é feito por meio de um algoritmo específico.
 - b) No que se refere à operação do Wi-Fi, ele opera exclusivamente na faixa de 5 GHz. Embora versões anteriores de Wi-Fi operem predominantemente em 5 GHz, as versões mais recentes são capazes de operar nas faixas de 2.4 GHz e 6 GHz também.
 - c) Em relação às versões de Wi-Fi, é correto afirmar que ele permite a comunicação sem fio entre dispositivos usando padrões definidos pela IEEE, como 802.11a, b, g, n e ac.
 - d) O Wi-Fi é caracterizado pela comunicação sem fio, utilizando uma conexão não guiada entre os dispositivos e o ponto de acesso (Access Point).
 - e) O Wi-Fi é capaz de suportar criptografia para proteger os dados transmitidos.
-

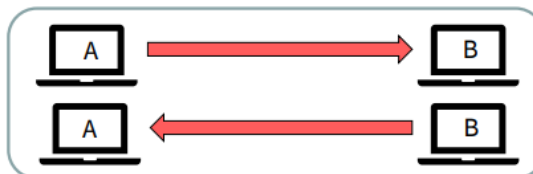
NOÇÕES BÁSICAS DE TRANSMISSÃO DE DADOS

Obs.: agora, abordando as noções básicas sobre transmissão de dados, é possível compreender os meios pelos quais essa transmissão pode ocorrer, seja por meios guiados ou não guiados. O foco, a seguir, é entender como se dá essa transmissão.

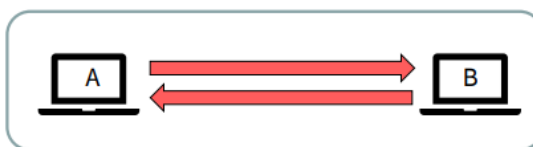
- **Simplex**



- **Half-duplex**



- **Full-duplex**



Uma forma de comunicação é a comunicação **simplex**, em que um dispositivo transmite e o outro apenas recebe, sem enviar dados de volta. Um exemplo clássico desse tipo de comunicação é a televisão convencional, na qual o espectador recebe a informação sem a capacidade de enviar nada de volta. Embora as Smart TVs modernas permitam interações como o envio de e-mails, o exemplo clássico remete à recepção de sinais, como no caso dos rádios AM ou FM, nos quais o ouvinte é passivo, recebendo a transmissão sem a possibilidade de enviar informações.

Na comunicação simplex, o dispositivo A transmite e o dispositivo B apenas recebe, sendo essa a única forma de interação. No entanto, em uma configuração diferente, o dispositivo B pode enviar e o A receber, o que caracteriza uma comunicação de fluxo unidirecional.

No modelo **half duplex**, a comunicação ocorre de forma bidirecional, mas de maneira alternada. Isso significa que o dispositivo A pode enviar informações em um momento e receber em outro, ocorrendo alternadamente, sem que ambos os dispositivos transmitam simultaneamente. Esse tipo de comunicação é análogo a uma conversa em que uma pessoa fala e a outra escuta, e depois de ouvir, a segunda pessoa fala enquanto a primeira escuta. A comunicação só acontece em um sentido de cada vez, o que pode ser visto como um modelo de interação saudável entre duas pessoas, onde um fala e o outro ouve.

Por fim, na comunicação **full duplex**, ambos os dispositivos podem enviar e receber informações simultaneamente. Esse modelo pode ser comparado a situações em que várias pessoas falam ao mesmo tempo, como no mercado de ações, onde todos negociam simultaneamente, apesar do aparente caos. Na comunicação full duplex, ambos os dispositivos conseguem interagir ao mesmo tempo, o que permite uma troca contínua de informações.

A principal diferença entre os modos de transmissão half duplex e full duplex reside na forma como os dispositivos podem se comunicar. No modo half duplex, os dispositivos podem transmitir e receber dados, mas não ao mesmo tempo; a comunicação ocorre alternadamente. Já no modo full duplex, os dispositivos conseguem transmitir e receber dados simultaneamente.



ATENÇÃO

Ao resolver questões sobre esses modos de transmissão, é importante evitar marcar excessivamente as alternativas, pois isso pode causar confusão ao transferir as respostas para o gabarito. Em casos de dúvidas, é recomendável lembrar as características principais de cada modo e refletir sobre elas ao ler as alternativas. O simples entendimento de que, no half duplex, a comunicação é alternada e, no full duplex, ela ocorre simultaneamente, facilita a escolha correta.

Além disso, ao analisar alternativas, pode ser útil fazer uma breve anotação para reforçar o entendimento das diferenças entre os modos, como, por exemplo, anotar “um de cada vez” para o half duplex e “ao mesmo tempo” para o full duplex. Essa prática ajuda a evitar erros na hora de responder.



DIRETO DO CONCURSO

02. (AVANÇA-SP/CÂMARA DE ITAPECERICA DA SERRA/2024) Dentre os modos de transmissão simplex, halfduplex e full-duplex, qual das alternativas descreve melhor a principal diferença existente entre os modos de half-duplex e fullduplex?

- a) Half-duplex permite transmitir e receber dados ao mesmo tempo, enquanto o fullduplex apenas envia dados.
- b) Half-duplex apenas pode enviar dados, enquanto o full-duplex permite a transmissão e a recepção de dados de modo alternado.
- c) Ambos os modos enviam e recebem dados, porém apenas o full-duplex o faz de modo simultâneo, enquanto half-duplex alterna entre os dois modos.
- d) Full-duplex atua como receptor do modo half-duplex.
- e) Full-duplex permite transmitir e receber dados ao mesmo tempo, enquanto halfduplex permite apenas receber dados para leitura.



- a) A alternativa descreve o modo “full-duplex”, que não existe; na verdade, refere-se ao modo simplex, que permite apenas o envio de dados.
- b) A definição trata-se da característica halfduplex.
- c) A alternativa descreve “fuduplex” como um modo que permite a transmissão e recepção alternada de dados, característica que, na realidade, corresponde ao modo half duplex.
- d) No modo full duplex, é possível enviar e receber dados simultaneamente, enquanto no modo half duplex, a comunicação ocorre alternadamente, ou seja, um dispositivo envia enquanto o outro recebe.
- e) A alternativa apresenta confusão conceitual ao afirmar que o full duplex atua como receptor no modo half duplex, sendo que o full duplex permite a transmissão e recepção simultânea de dados.

Obs.: uma sugestão é que, ao enfrentar questões sobre esses modos de transmissão, faça uma pausa e tente resolvê-las de forma independente, antes de revisar as alternativas.

A principal dificuldade no momento da prova é lembrar dos detalhes, que podem parecer simples, mas que, em um momento de tensão, podem ser interpretados de forma errada. Por isso, é fundamental revisar constantemente o conteúdo. Na hora da prova, o nervosismo pode dificultar a distinção entre situações que, se não forem compreendidas claramente, podem se tornar complexas. A dica, portanto, é tentar manter a calma durante a prova, pois quanto mais tenso o candidato estiver, mais difícil pode ser tomar decisões corretas.



DIRETO DO CONCURSO

03. (QUADRIX/CRT 1/ASSISTENTE ADMINISTRATIVO/2024) A topologia em estrela é considerada uma topologia pouco resistente a falhas, pois a interrupção de um único dispositivo é suficiente para interromper todo o funcionamento da rede, ou seja, afeta todos os outros dispositivos (nós)



25m

Na topologia em estrela, não há dependência direta entre os dispositivos.

04. (FURB/SAAE BLUMENAU/TÉCNICO EM INFORMÁTICA/2024) Sobre os tipos de rede, analise os itens a seguir: _____ é usado em uma área geográfica pequena, como um prédio. _____ cobre uma área geográfica maior do que _____, potencialmente uma cidade. _____ se estende por uma vasta área, como várias cidades ou até países. Assinale a alternativa que correta e respectivamente completa as lacunas nos excertos:

- a) WAN, MAN, WAN, LAN.
- b) LAN, MAN, LAN, WAN.
- c) LAN, WAN, LAN, SAN.
- d) PAN, SAN, PAN, WAN.
- e) PAN, MAN, SAN, WAN.



Quanto aos tipos de rede, é importante distinguir entre as diferentes escalas geográficas. A primeira rede cobre uma área geográfica pequena, como um prédio, o que caracteriza uma LAN (Local Area Network). A segunda rede cobre uma área maior, como uma cidade, caracterizando uma MAN (Metropolitan Area Network). Por fim, a terceira rede cobre uma área vasta, como várias cidades ou até mesmo países, caracterizando uma WAN (Wide Area Network). Assim, as redes podem ser diferenciadas pela extensão de sua cobertura geográfica: LAN para áreas pequenas, MAN para áreas urbanas e WAN para áreas extensas.

Essa questão foi bem estruturada, pois pode gerar dúvidas na hora da prova, especialmente em relação à comparação de áreas geográficas e à ordem de grandeza, algo que pode ser alterado para confundir o candidato, sem que haja problema na formulação da questão.

Com isso, mais um bloco de informações foi abordado. Embora ainda haja muito conteúdo a ser explorado, é importante manter a calma e a confiança, pois, com dedicação, será possível assimilar o material e obter um bom desempenho na prova. A confiança é fundamental nesse processo, e, com o esforço contínuo, o candidato estará preparado para a avaliação.

GABARITO

- | | |
|-------------|-------------|
| 1. c | 3. E |
| 2. c | 4. b |

Este material foi elaborado pela equipe pedagógica do Gran Concursos, de acordo com a aula preparada e ministrada pelo professor Jeferson Bogo Severino.

A presente gravação tem como objetivo auxiliar no acompanhamento e na revisão do conteúdo ministrado na videoaula. Não recomendamos a substituição do estudo em vídeo pela leitura exclusiva deste material.