CENTRO UNIVERSITÁRIO DO PLANALTO CENTRAL APPARECIDO DOS SANTOS

CURSO DE GRADUAÇÃO EM ENGENHARIA DE SOFTWARE, BACHARELADO

Aprovado pelo Conselho Superior dia 07 de dezembro de 2018, Resolução nº 16/2018 de 10 de Dezembro de 2018

[Em vigor para os alunos que ingressaram a partir do 1° semestre letivo de 2019.1] 1,0

LISTA DE EXERCICIO – REVISÃO

Disciplina: Comunicação de Dados e Redes de Computadores
Alunos: **Guilherme Aires Gomes** **Igor Moreira de Souza** **João Henrique de Almeida Araújo** **Samuel Pinheiro Soares**

1. Defina redes WWAN e WPAN, indicando também o que segue para ambas:
   a. Comparação de dimensão;

   Ambas têm o prefixo *Wireless,* portanto, são sem fio. A WAN é uma sigla que significa *Wide Area Network*, abrangendo uma grande área, como por exemplo um país ou continente. A sigla PAN significa *Personal Area Network* e abrange uma área pequena, de 1 a 5 metros de proximidade do usuário.

   b. Análise de velocidade;

   WWAN - Utilizam tecnologias de comunicação como 4G, 5G, LTE, e redes de satélite. As velocidades podem variar dependendo da tecnologia usada. O 4G, por exemplo, pode oferecer velocidades de até 100 Mbps, enquanto o 5G pode ultrapassar 1 Gbps em condições ideais.

   WPAN - Utilizam formas de comunicação mais lentas. As principais tecnologias WPAN incluem Bluetooth, Zigbee, e UWB (Ultra-Wideband). A velocidade de transferência do Bluetooth, por exemplo, pode variar de 1 Mbps nas versões mais antigas a até 50 Mbps nas versões mais recentes como o Bluetooth 5.0.

   c. Principal utilização.

   WPAN - São geralmente utilizadas por dispositivos como smartphones, tablets, laptops e PCs em áreas urbanas e rurais.

   WLAN - São projetadas para conectar dispositivos pessoais, como smartphones, fones de ouvido, teclados, e outros periféricos dentro de uma área pequena, como uma sala.

2. Crie um quadro comparativo entre as redes LAN (Local Area Network), MAN (Metropolitan Area Network) e PAN (Personal Area Network), destacando as principais características, exemplos de uso e tecnologias utilizadas em cada tipo de rede. Explique também como essas redes se interconectam no dia a dia e os desafios de segurança associados a elas.

Tipos de redes	**Principais características**	**Exemplos de uso e tecnologias utilizadas**	**Desafios de segurança associados**
PAN	Rede pessoal que conecta dispositivos próximos a um indivíduos. Geralmente tem baixo custo, e estão embutidas em dispositivos pessoais.	Comunicação entre dispositivos como smartwatch, smartphone, e fones de ouvido. Ex: Bluetooth, NFC.	Vulnerável a interceptações, especialmente em Bluetooth e NFC.
LAN	Rede local que conecta dispositivos em uma área restrita, como um escritório ou casa. Possuem custo relativamente baixo, dependendo da escala e tecnologia.	Conexões de computadores em escritórios, escolas, ou residências. Ex: Wi-fi, Fibra ótica.	Alta segurança com firewalls, WPA2/WPA3, controle de acesso.
MAN	Rede que cobre uma cidade ou grande área metropolitana, conectando	Conexão de LANs de diferentes prédios, cidades inteligentes, redes de transporte	Desafios com interconexão segura de LANs e controle de acesso.

	múltiplas LANs.É mais cara devido ao uso de infraestrutura pública e privada para interconexão.	público. Ex: Ethernet.	

Como se interconectam no dia a dia:

PANs: Conectam dispositivos pessoais sem a necessidade de infraestrutura complexa. São utilizadas diariamente para comunicação rápida entre dispositivos portáteis, como conectar fones Bluetooth a um smartphone.

LANs: Conectam dispositivos dentro de uma casa, escritório ou escola, permitindo compartilhamento de recursos como arquivos, impressoras e acesso à internet. LANs podem se interconectar com outras LANs através da internet ou por meio de uma MAN.

MANs: Conectam diversas LANs em uma cidade ou campus, facilitando a comunicação entre locais separados geograficamente, como edifícios empresariais, universidades e governos. Muitas vezes, utilizam infraestrutura de terceiros, como ISPs.

3. Explique como as diferentes redes impactam o desempenho e a segurança de dispositivos IoT (Internet das Coisas). Considere exemplos práticos de aplicação dessas redes no gerenciamento de casas inteligentes, cidades conectadas e ambientes corporativos. Quais são os desafios de conectividade, latência e segurança específicos de cada tipo de rede quando se trata de IoT?
    a. **PAN:** Conectam dispositivos próximos, como wearables, lâmpadas e assistentes pessoais a um hub central. Em ambientes corporativos pode ser utilizada, por exemplo, para conectar periféricos a um computador. Redes PAN oferecem baixa latência devido a proximidade, e a conectividade será interrompida se os dispositivos saírem do alcance. PANs podem ser vulneráveis a interceptação e invasões, tornando necessárias medidas como criptografia, pareamento seguro e autenticação para proteger os dispositivos.
    b. **LAN:** Conectam dispositivos em um alcance maior que redes PAN. Amplamente utilizada através de Wi-Fi e cabos Ethernet em redes

domésticas e corporativas. No contexto de IoT pode ser utilizada para conectar câmeras de segurança, sistemas de controle de temperatura, fechaduras inteligentes e eletrodomésticos inteligentes. Oferecem baixa latência e alta estabilidade em uma infraestrutura bem configurada. A segurança em redes LAN pode ser comprometida por ataques como “man-in-the-middle” e DDoS. Criptografia de dados e segmentação de rede são essenciais para proteger dispositivos IoT nesse contexto.

c. **MAN:** Em cidades conectadas, MANs conectam várias LANs e proporcionam comunicação entre edifícios, bairros ou complexos industriais através de, principalmente, fibra ótica e redes móveis (4G/5G). Em cidades conectadas, MANs suportam infraestrutura urbana inteligente incluindo sistemas de controle de tráfego, iluminação pública, monitoramento ambiental e segurança. Oferecem alto desempenho através de uma alta capacidade de comunicação, lidando com um grande volume de dados. A latência é um pouco maior do que em redes LAN, a depender da distância e da infraestrutura. São alvos potenciais para ataques em larga escala. Para proteger dispositivos IoT em uma MAN, é necessário monitoramento contínuo, autenticação robusta e criptografia de ponta a ponta (E2EE).

d. **WAN:** Cobrem grandes áreas geográficas, como países e continentes, utilizando infraestrutura de redes móveis (4G/5G), links de fibra ótica e satélites. São essenciais para cidades conectadas e soluções corporativas globais, permitindo por exemplo, monitoramento de transporte público, sistemas de distribuição de energia e organização de cadeias logísticas. Oferecem cobertura abrangente e conectividade em qualquer lugar com acesso a infraestrutura de redes. No entanto, a latência é maior em comparação com redes MAN, podendo afetar aplicações que dependem de comunicação em tempo real. As WANs expõem dispositivos IoT à internet, tornando-os suscetíveis a diversos tipos de ataques. Uso de firewalls, VPNs e sistemas de detecção de intrusão é crucial para proteger dispositivos conectados a uma WAN.

4. Na arquitetura Cliente/Servidor, a importância não reside no fato de todas as máquinas serem do mesmo fabricante, mas sim na interoperabilidade e na adoção de padrões de comunicação. Essa importância é definida pela necessidade de que diferentes sistemas e dispositivos, independentemente de seus fabricantes, possam se comunicar e trocar informações de maneira eficiente. Com base nisso, responda quais são os principais protocolos e padrões que garantem a interoperabilidade em uma arquitetura Cliente/Servidor, e como

eles permitem que dispositivos e sistemas de diferentes fabricantes trabalhem juntos de forma eficaz?

Os principais protocolos são o **TCP** (Transmission Control Protocol) e o **UDP** (User Datagram Protocol). Eles são protocolos da camada de transporte do modelo OSI que fornecem métodos para a transmissão de dados. A arquitetura Cliente/Servidor cria uma separação clara entre quem faz a solicitação e quem atende a essa solicitação. Tanto o TCP quanto o UDP seguem os padrões definidos pela Internet Engineering Task Force (IETF). Esses padrões especificam como a comunicação deve ocorrer, independentemente dos dispositivos envolvidos. Fabricantes de diferentes sistemas podem implementar esses protocolos conforme as especificações, garantindo que seus dispositivos sejam capazes de se comunicar.

5. Explique a diferença entre Dados e Informação e como eles são transportados nas redes.

Dados são elementos não processados, brutos. Podem ser números, texto ou qualquer outro tipo de entrada/valor não analisado e interpretado. Informação é o resultado do processamento, organização e interpretação dos dados. Nas redes, o transporte de dados ocorre por meio de protocolos e tecnologias de comunicação.

6. Explique o modelo OSI (Open Systems Interconnection) e descreva as funções de cada uma das suas sete camadas. Como esse modelo auxilia na padronização da comunicação entre diferentes sistemas de rede e dispositivos, e quais são os principais protocolos associados a cada camada?

i. Camada física - Lida com a transmissão física de dados através dos meios de comunicação. Define características como taxa de dados e especificações de conectores. É responsável pela conversão dos bits em sinais que podem ser transmitidos por um meio físico. Os principais protocolos são RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11.

ii. Camada de Enlace - Proporciona comunicação confiável entre dois dispositivos conectados. Gerencia o acesso ao meio físico e trata erros de transmissão. Organiza os dados em quadros (frames) para serem transmitidos na rede. Os principais protocolos são Ethernet, 802.11, MAC/LLC, VALN, ATM,HDP, Fibre Channel, Frame Relay, HDLC, PPP, Q.921, Token Ring.

iii. Camada de Rede - Controla o roteamento dos pacotes de dados entre diferentes redes, decidindo o melhor caminho para os dados chegarem ao seu destino. É responsável pelo endereçamento lógico dos dispositivos na rede, comumente através de endereços IP. Os principais protocolos são IP, ARP, IPsec, IGMP, OSPF.
iv. Camada de Transporte - Garante a entrega dos dados, dividindo-os em segmentos para envio e reagrupando-os na chegada. Implementa controle de fluxo e detecção de erros, assegurando que os dados sejam entregues sem perdas, duplicações ou erros. Os principais protocolos são TCP, UDP, SCTP, SSL, TSL.
v. Camada de Sessão - Estabelece, gerencia e encerra sessões entre aplicações em diferentes dispositivos. Coordena a comunicação, permitindo que as aplicações transmitam dados bidirecionalmente e de forma sincronizada, garantindo que a conexão seja mantida enquanto a sessão estiver ativa. Os principais protocolos são o estabelecimento de sessão TCP, SIP, RTP.
vi. Camada de Apresentação - Atua como tradutora de dados, garantindo que a informação transmitida pela camada de aplicação de um sistema possa ser compreendida pela camada de aplicação de outra. Realiza conversão de formatos, criptografia, compressão e outros processos para garantir compatibilidade. Não possui protocolos específicos, mas é responsável por traduzir os mais diversos formatos de arquivo transmitidos pela rede como, por exemplo, HTML, DOC, JPEG, MP3, AVI entre outros.
vii. Camada de Aplicação - É a mais próxima do usuário final, fornecendo interfaces para aplicações acessarem os serviços da rede. Facilita a interação direta com aplicações de software, como navegadores web e clientes de e-mail. Os principais protocolos são HTTP/HTTPS, DNS, P2P, EMAIL/POP,SMTP, FTP.

7. Explique quando seria mais apropriado utilizar o protocolo TCP em vez de UDP e vice-versa, fornecendo exemplos de aplicações práticas para cada um. Quais são os trade-offs entre confiabilidade e velocidade ao escolher entre esses dois protocolos?

a. TCP: É mais apropriado quando é necessário a garantia da comunicação confiável e ordenada. Esse protocolo utiliza o 3-Way Handshake para estabelecer a conexão entre cliente e servidor, além disso, possui mecanismos de monitoramento dos estados da conexão e controle de

fluxo e congestionamento, garantindo a entrega dos pacotes. É ideal para transferência de dados críticos e configurações entre dispositivos.

b. **UDP:** É mais apropriado para uso em aplicações de tempo real, que necessitam de baixa latência. Não possui estabelecimento de conexão e garantia de entrega, sendo assim, não é confiável e pode haver perda de pacotes.

8. Explique quais são as desvantagens do uso de redes de computadores.
   - **Segurança**: Quando dispositivos estão interconectados, há um risco maior de ataques cibernéticos, como malwares, vírus, hackers e roubo de informações confidenciais. Manter a segurança em uma rede exige constante monitoramento, atualizações e práticas como o uso de firewalls, antivírus e criptografia.
   - **Custo de Implementação e Manutenção**: Criar e manter uma rede de computadores pode ser caro, especialmente em ambientes corporativos. Além do custo de hardware (roteadores, switches, cabos, servidores), é necessário investir em softwares de gerenciamento e segurança. A manutenção regular, como atualizações de software e substituição de equipamentos, também pode gerar despesas significativas.
   - **Dependência da Rede**: Em uma rede de computadores, a comunicação e o acesso a dados geralmente dependem da conectividade. Se a rede enfrentar problemas como falhas de hardware, interrupções de serviço ou ataques, as atividades dos usuários podem ser prejudicadas. Essa dependência pode causar atrasos ou paralisações nas operações.
   - **Complexidade de Gerenciamento**: Quanto maior e mais complexa for a rede, mais difícil será gerenciá-la. É necessário monitorar o tráfego, manter a segurança, configurar dispositivos e solucionar problemas. Isso pode exigir uma equipe especializada, aumentando a complexidade e os custos operacionais.
   - **Risco de Propagação de Problemas**: Em uma rede, problemas podem se espalhar rapidamente. Um dispositivo infectado por um vírus, por exemplo, pode contaminar outros dispositivos conectados. Além disso, falhas em um servidor ou roteador central podem impactar toda a rede, interrompendo o acesso a recursos e dados.
   - **Privacidade**: Em redes maiores, especialmente naquelas que conectam dispositivos em uma organização ou em espaços públicos, os dados dos usuários podem estar mais vulneráveis. Há um risco de vigilância e coleta de dados sem o consentimento dos usuários, o que pode impactar a privacidade e a confidencialidade das informações.

9. Qual a diferença entre uma conexão Ponto a Ponto e uma conexão Multiponto em redes de computadores, e em quais cenários cada uma seria mais adequada?

A ponto a ponto é uma conexão direta entre dois dispositivos, o que garante alta privacidade, segurança, custo baixo além de uma configuração mais simples. É adequada para cenários em que há a transmissão de dados críticos, ou para conectar dois dispositivos diretamente em uma rede local, como uma impressora a um computador, por exemplo.

A multiponto ou broadcast é uma conexão onde um único dispositivo se comunica com vários dispositivos simultaneamente através de uma rede compartilhada, tornando a rede mais escalável, mais complexa e mais cara. É adequada para redes LAN onde vários dispositivos se conectam a um roteador ou precisam se comunicar entre si. Também é adequada em casos de transmissão de dados para vários dispositivos, como em transmissões de TV ou em redes corporativas de larga escala.

10. Como os diferentes meios de transmissão (cabo metálico, fibra óptica, e wireless) impactam a velocidade e a qualidade da comunicação nas redes de computadores?

Cabos metálicos têm limitações quanto a velocidade de transmissão, além de uma atenuação do sinal em distâncias maiores. É suscetível a interferências eletromagnéticas e ruídos, resultando em perda de pacotes, retransmissões e consequentemente, redução da taxa de transferência de dados.

Fibra ótica oferece velocidades muito altas, podendo atingir dezenas e terabyte por segundo. Isso ocorre devido a capacidade de transmitir dados por meio de luz. É altamente resiliente a interferências eletromagnéticas, garantindo integridade dos dados. É um meio de comunicação de alta qualidade e baixa latência. Pode alcançar centenas de quilômetros sem a necessidade de amplificadores ou repetidores.

Redes wireless variam de velocidade dependendo da tecnologia utilizada, da proximidade ao ponto de acesso, congestionamento da rede e obstáculos físicos. É suscetível a interferências como barreiras físicas , outras redes e dispositivos e condições atmosféricas, podendo levar a variação da qualidade do sinal, alta latência e perda de pacotes.

11. Explique o funcionamento da comunicação no modo Simplex e dê um exemplo de aplicação prática em que esse tipo de enlace é utilizado.

O enlace simplex é unidirecional, significa que os dados trafegam somente do emissor para o receptor. Não há retorno de informação, reconhecimento ou possibilidade de resposta do receptor. Um exemplo de comunicação simplex é a transmissão de sinais de rádio.

12. Em que situações seria mais vantajoso utilizar uma comunicação do tipo Half-duplex em vez de Full-duplex, considerando o tráfego de dados e a eficiência?

O uso da comunicação *Half-duplex* é mais vantajoso do que *Full-duplex* em situações onde é necessário economizar recursos, minimizar interferências ou quando o tráfego de dados é intermitente e não exige uma transmissão simultânea nos dois sentidos. Algumas situações específicas incluem:

- Rádios comunicadores (walkie-talkies) alternado entre transmissão e recpção.

- Redes de sensores em aplicações de Internet das Coisas (IoT) em que os sensores enviam dados periodicamente para um servidor central e, ocasionalmente, recebem comandos de volta.

13. Como a distância física afeta o desempenho das linhas de comunicação em uma rede, e quais tecnologias são mais adequadas para transmissões de longas distâncias?

Distância física pode afetar o desempenho de uma rede através de:

1. **Atenuação do sinal:** À medida que um sinal se propaga ao longo de um meio físico (como cabos, por exemplo), ele perde força.
2. **Latência:** É o tempo que os dados levam para viajar de um ponto a outro, e aumenta com a distância física, se tornando perceptível em longas distâncias e prejudicando aplicações onde há necessidade de transmissão de dados em tempo real como chamadas de vídeo e jogos online.
3. **Interferência:** Em alguns tipos de rede podem ser afetados por interferência eletromagnética de outras fontes ou redes (cabos de energia, sinais de rádio, etc).

Para longas distâncias as tecnologias mais adequadas são: fibra ótica, satélites, micro-ondas terrestres, 4G/5G (médias distâncias).

14. O que é um Domain Name Service (DNS) e como ele funciona para a resolução do nome das máquinas que hospedam as páginas de interesse (páginas WEB).

É um sistema distribuído que traduz nomes de domínio (google.com) em endereços de IP. Esse processo de tradução é chamado de **resolução de nome** e têm essas etapas:

1. Solicitação de Resolução: Quando você digita um endereço web (URL) em seu navegador, como www.exemplo.com, o navegador envia uma consulta para o servidor DNS configurado no seu dispositivo (geralmente fornecido pelo seu provedor de internet ou roteador local).

2. Consulta ao Servidor DNS Local: O servidor DNS local (também conhecido como resolutor de DNS) verifica se ele já tem o endereço IP associado ao domínio armazenado em seu cache. Se tiver, ele responde imediatamente com o endereço IP, acelerando o processo.

3. Recursão: Se o endereço IP não estiver em cache, o resolutor DNS faz uma consulta recursiva, começando pelos servidores raiz (root servers). Esses servidores indicam os servidores de domínio de nível superior (TLD) correspondentes ao domínio solicitado. Por exemplo, para www.exemplo.com, os servidores raiz apontarão para os servidores .com.

4. Consulta aos Servidores TLD: Os servidores TLD (por exemplo, os servidores .com) são consultados em seguida e indicam os servidores de nomes autoritativos para o domínio solicitado (neste caso, exemplo.com).

5. Consulta ao Servidor Autoritativo: Finalmente, o servidor de nomes autoritativo para exemplo.com é consultado. Ele contém os registros específicos do domínio, incluindo o endereço IP associado a www.exemplo.com.

6. Retorno do Endereço IP: O servidor autoritativo responde com o endereço IP associado ao nome de domínio, e o resolutor de DNS local armazena essa informação em seu cache para futuras consultas.

7. Conexão ao Website: Com o endereço IP em mãos, o navegador pode se conectar ao servidor de destino para solicitar e carregar a página web.

15. Como a distinção entre bordas (edge) e núcleo (core) de uma rede influencia o desempenho e a eficiência da transmissão de dados, e quais são as principais funções de cada parte em uma infraestrutura de rede de grande escala?

A distinção da **borda (edge)** e **núcleo (core)** é fundamental para a arquitetura e desempenho na transmissão de dados. Cada qual apresenta uma função específica que influencia no desempenho da rede.

O **núcleo** tem como função o gerenciamento do tráfego de dados em grande escala e ademais, gerir que eles estão sendo entregues de modo eficiente entre os ramos do receptor, possuindo baixa latência e alta velocidade, sistema de confiabilidade e se interligando a grandes data centers.

Por final seu impacto no desempenho influencia no complexo de gerenciamento de grande volume de dados, obtendo baixas latências e sem congestionamento.

Já a **borda** é referente a parte de infraestrutura da rede, sendo o E/S, a conexão final dos dispositivos e a rede. Funcionando como uma interface de entrada e saída para os usuários/dispositivos e núcleos.

Sua função principal se encontra na conectividade de usuários, distribuição e adaptabilidade de tráfego, filtragem para segurança e edge computing.

Conectividade com usuários: A borda é o ponto onde os usuários e dispositivos se conectam à rede, sejam eles locais ou remotos. Aqui, ocorre a primeira interação com os dados que entram ou saem da rede.

Edge computing: Em infraestruturas modernas, a borda tem capacidade de processar dados localmente, invés de haver o processo de enviar para o núcleo e gerando mais estresse de processamento. Isso ocasiona em uma latência menor, e auxilia aplicações que precisam de respostas rápidas.

16. Explique o funcionamento do comutador de pacotes (packet switching) em redes de computadores e como ele difere do comutador de circuitos. Quais são as vantagens do comutador de pacotes para o tráfego de dados na internet e em que situações ele pode não ser a melhor escolha?

Packet Switching é um método de transmissão de dados, que quebra a informação inteira em blocos de dados (chamados pacotes) e envia-os na Internet. Os pacotes

funcionam de maneira independente e podem tomar diferentes rotas para chegar até o destino final (roteamento dinâmico), e são montados quando chegam no receptor.

Em suas vantagens, pode-se encontrar as seguintes conjunturas: Flexibilidade das conexões; escalabilidade para adaptação das redes de larga escala; Resiliência por haver haver a possibilidade dos pacotes tomarem diferentes rotas; Eficiência no uso das redes

As situações que implicam em que não pode ser a melhor escola a utilização de comutação de pacotes, seriam:

Aplicações que funcionam em tempo real, que exigem baixa latência e demanda de consistência, como chamadas e videochamadas. A variação de tempo (jitter) causará prejuízo no tempo para a qualidade dessa aplicação.

Redes de baixa tolerância a falhas, como as redes em que são utilizadas em controle industrial, onde deve haver sempre confiabilidade contínua e falta de atraso de Jitter.

A diferença entre de packet switching e comutador de circuitos está principalmente em como eles gerenciam o fluxo de dados através da rede. O comutador de circuitos é incluído um circuito dedicado antes da transmissão de dados, todo caminho é reservado e permanece fixo durante a comunicação, ele oferece maior previsibilidade, serve para comunicações contínuas e com baixa tolerancia de falhas, como chamadas e videochamadas.

17. Explique a diferença entre sinal analógico e sinal digital no contexto da transmissão de informações em redes de computadores. Quais são as vantagens e desvantagens de cada tipo de sinal, e em quais situações a conversão de sinais analógicos em digitais (e vice-versa) é necessária para garantir uma comunicação eficiente?

A diferença entre **analógico** e **digital** no contexto de redes de computadores reside na forma como eles representam os dados para transmiti-los.

O **sinal analógico** é um sinal elétrico continuo, que para representar um dado através de uma onda senoidal representando números quebrados. Através da mudança de comprimento de onda, amplitude e frequência é possível diferenciar dados e enviá-los para transmissão.

Vantagens:

Alta resolução: Por ser contínuo, um sinal analógico pode representar informações com uma precisão teórica infinita.**Facilidade de captação de fenômenos naturais**: Sinais como voz, temperatura ou luz são naturalmente analógicos.

Desvantagens:

Ruído e degradação: Os sinais analógicos são suscetíveis a ruídos e interferências durante a transmissão. Pequenas distorções podem resultar em perda de qualidade.

Dificuldade de processamento: Em sistemas de redes de computadores, sinais analógicos são mais difíceis de armazenar e processar eficientemente.

A princípio, o **sinal digital** é uma forma de transmissão sequencial, discreta e não contínua que utiliza sistema binário quando ocorre uma variação de tensão para definir um dado, podendo enviar tanto em pacotes de bits, ou Bytes.

Vantagens:

Imunidade ao ruído: Sinais digitais são mais resistentes ao ruído, uma vez que pequenas variações não afetam a interpretação dos valores binários (0 ou 1).

Processamento eficiente: Sinais digitais podem ser facilmente manipulados, processados e armazenados por dispositivos eletrônicos e computadores.

Compressão e correção de erros: Técnicas de compressão de dados e correção de erros são facilmente aplicáveis em sinais digitais

Desvantagens:

Perda de resolução: Ao converter sinais analógicos para digitais, algumas informações podem ser perdidas, especialmente se a taxa de amostragem (quantas vezes o sinal é medido por segundo) não for alta o suficiente.

Necessidade de conversão: Em sistemas que envolvem fenômenos analógicos (como voz ou som), é necessário converter esses sinais em digitais, o que requer hardware adicional e processamento

A necessidade de haver a conversão de sinal,é explicitamente necessária quando depende do modo em que o dispositivo funciona. A **conversão de sinais analógicos em digitais** é necessária sempre que fenômenos do mundo real, como som, vídeo ou dados de sensores, precisam ser processados e convertidos em digital para poder ser lido em binario. A **conversão digital para analógico** também é essencial para garantir que esses dados possam ser reproduzidos ou utilizados em dispositivos que interagem com o ambiente físico, como alto-falantes, monitores ou atuadores.

Uma pequena lista da transmissão que necessita de A/D (analógico em digital):

Gravação de áudio digital: Microfones capturam som em forma de sinal analógico, que precisa ser digitalizado para armazenamento em dispositivos como computadores, celulares ou gravadores.

Telefonia e VoIP: A voz humana é convertida de analógico para digital para ser transmitida via redes digitais, como a internet ou redes celulares.

Câmeras digitais: Câmeras capturam luz (sinal analógico) e convertem em dados digitais para gerar fotos ou vídeos.

Streaming de vídeo: Vídeos analógicos (capturados por câmeras) são convertidos para digital para transmissão por plataformas de streaming.

Telefonia celular: A voz captada por um microfone de celular é convertida para sinal digital antes de ser transmitida pelas torres de telefonia.

Rádio digital: Sinais de áudio são capturados em formato analógico e convertidos para digital para transmissão via rádio digital ou internet.

TV digital: Sinais de vídeo e áudio captados por câmeras e microfones em estúdios de televisão são convertidos para digital para transmissão via cabo, satélite ou internet.

Agora da conversão D/A:

Alto-falantes: Sistemas de áudio, como celulares, computadores e aparelhos de som, convertem sinais digitais em analógicos para que os alto-falantes possam reproduzir o som.

Fones de ouvido: O áudio digital, como músicas ou chamadas telefônicas, precisa ser convertido para analógico para ser ouvido pelos usuários.

Monitores e TVs: Dispositivos digitais como computadores, consoles de jogos e celulares convertem sinais digitais para analógicos para exibir imagens e vídeos em monitores ou televisores.

Projetores: Para exibir vídeos ou apresentações, os sinais digitais de um computador ou dispositivo de mídia são convertidos para analógicos, para serem projetados visualmente.

Telefonia fixa tradicional: Embora muitos sistemas de comunicação modernos sejam digitais, alguns sistemas de telefonia fixa ainda requerem a conversão de sinais digitais para analógicos para que a voz seja transmitida pelas linhas telefônicas tradicionais.

Chamadas de celular: Durante as chamadas de celular, a voz digitalizada é convertida de volta em sinais analógicos no alto-falante para que possa ser ouvida pela pessoa do outro lado.

Rádio AM/FM: Em rádios analógicos, o sinal digital (por exemplo, áudio digitalizado em estações de rádio) precisa ser convertido para analógico para ser transmitido e recebido pelos aparelhos de rádio.

Rádios de automóveis: Rádios que captam sinais de rádio digitais convertem os sinais de volta para analógico para serem ouvidos pelos usuários.

18. Defina o conceito de Redes de computadores e de sua importância no contexto atual da sociedade.

Redes de computadores são sistemas interconectados que facilitam a comunicação e o compartilhamento de recursos entre dispositivos como computadores, smartphones, servidores e outros aparelhos inteligentes. Essas redes podem variar em escala, desde redes locais menores (LANs) até redes globais, como a internet.

No mundo de hoje, as redes de computadores são fundamentais para quase todas as áreas da sociedade. Elas conectam pessoas, empresas e governos, permitindo a troca rápida de informações, a execução de serviços e a realização de tarefas à distância.

19. Explique os conceitos de multiplexação e demultiplexação em redes de comunicação.

A multiplexação é o processo de combinar vários fluxos de dados ou sinais em um único canal de comunicação. O objetivo é maximizar o uso de um recurso compartilhado.

FDM: cada fluxo de dados é transmitido em uma frequência diferente, dentro de um mesmo meio físico.

TDM: Os dados são transmitidos em "fatias" de tempo. Cada fluxo de dados tem um intervalo de tempo dedicado para enviar suas informações, alternando rapidamente entre eles.

WDM: Usado em redes de fibra óptica, é uma variação do FDM, onde diferentes sinais são transmitidos usando diferentes comprimentos de onda da luz.

A Demultiplexação é o processo inverso, onde o canal de comunicação compartilhado é dividido novamente em vários fluxos de dados individuais na ponta receptora. O demultiplexador recebe o fluxo multiplexado e separa os diferentes sinais ou dados, direcionando-os para seus respectivos destinos.

20. Dado o endereço IP em binário 11000000 10101000 00000010 00001100 e a máscara de sub-rede 11111111 11111111 11111111 00000000, converta ambos para o formato decimal. Qual é o endereço IP e a máscara de sub-rede resultantes? Quantos hosts podem ser endereçados nessa sub-rede?

192.168.2.12 / .255.255.255.0. É possível incluir 256 hosts, mas dois ficam exclusivos impossibilitando o alojamento de um host dinâmico, sendo esses dois exclusivos, um para identificação da sub-rede e o outro para broadcast.

BONS ESTUDOS!