semana 9- aula 01
Protocolos e Camadas
Camada de Enlace: Controle de Acesso ao Meio e Detecção de Erros
Código da aula: [SIS]ANO1C2B2S9A1

Objetivos da Aula:

- ❖ Compreender o controle de acesso ao meio e a detecção de erros da camada de enlace com uso de hubs.
- ❖ Conhecer técnicas de computação e gerenciamento de dados para soluções em nuvem, parametrizando aplicações e dimensionando de acordo com as necessidades do negócio;
- ❖ Identificar e analisar problemas;

Exposição:

A Camada de Enlace (Data Link Layer), a segunda camada do Modelo OSI, tem como principal objetivo fornecer um meio confiável para a transferência de dados entre dois nós diretamente conectados em uma rede física. Ela atua como uma ponte entre a Camada Física (que lida com a transmissão bruta de bits) e a Camada de Rede (responsável pelo roteamento entre diferentes redes).

Pense na Camada de Enlace como o "carteiro local" da sua rede. Ela garante que a correspondência (seus dados) seja entregue de forma segura e eficiente entre vizinhos (dispositivos na mesma rede).

As principais funções da Camada de Enlace incluem:

- Enquadramento (Framing): Recebe os pacotes da Camada de Rede e os encapsula em unidades menores chamadas quadros (frames). Adiciona cabeçalhos e trailers aos dados, contendo informações de controle como endereços físicos (MAC), detecção de erros e controle de fluxo.
- Endereçamento Físico (MAC Addressing): Utiliza endereços MAC (Media Access Control) para identificar unicamente os dispositivos dentro da mesma rede local. Esses endereços são físicos, gravados na placa de interface de rede (NIC) de cada dispositivo.
- Controle de Acesso ao Meio (Media Access Control - MAC): Define as regras para que múltiplos dispositivos compartilhem o mesmo meio físico de transmissão (como um cabo Ethernet ou uma frequência Wi-Fi) sem que ocorram colisões e garantindo um acesso justo.
- Detecção e, em alguns casos, Correção de Erros: Implementa mecanismos para detectar erros que possam ocorrer durante a transmissão na Camada Física (ruídos, interferências). Alguns protocolos também possuem a capacidade de corrigir esses erros ou solicitar a retransmissão dos dados corrompidos.

- Controle de Fluxo: Regula a taxa de transmissão de dados entre dois nós para evitar que um transmissor rápido sobrecarregue um receptor mais lento, garantindo que os dados sejam processados de forma adequada.

Exemplos de protocolos e tecnologias da Camada de Enlace:

- **Ethernet (IEEE 802.3): O protocolo mais amplamente utilizado em redes locais (LANs) com fio. Define o formato dos quadros, o método de acesso ao meio (CSMA/CD em versões mais antigas, comutação em redes modernas) e as características físicas da conexão.**
- **Wi-Fi (IEEE 802.11): O padrão para redes locais sem fio (WLANs). Define o formato dos quadros, o método de acesso ao meio (CSMA/CA) e os mecanismos de segurança.**
- **PPP (Point-to-Point Protocol): Um protocolo usado para estabelecer conexões diretas (ponto a ponto) entre dois nós, como em conexões discadas, DSL ou conexões WAN seriais. Fornece autenticação, criptografia e compressão.**
- **HDLC (High-Level Data Link Control): Um protocolo de enlace de dados síncrono, orientado a bits, utilizado em redes WAN.**
- **Frame Relay: Uma tecnologia de comutação de pacotes utilizada em redes WAN, operando nas camadas física e de enlace.**
- **ATM (Asynchronous Transfer Mode): Outra tecnologia de comutação de pacotes para redes WAN, caracterizada por células de tamanho fixo.**

Em resumo, a Camada de Enlace é crucial para garantir uma comunicação confiável e organizada dentro de uma mesma rede física, preparando os dados para serem roteados para seus destinos finais pela Camada de Rede.

No contexto da Camada de Enlace do modelo OSI, a Detecção de Erros refere-se aos mecanismos implementados para identificar se os dados transmitidos através do meio físico foram alterados ou corrompidos durante o processo. Como a Camada Física é suscetível a ruídos, interferências e outros problemas que podem introduzir erros nos sinais elétricos, ópticos ou de rádio, a Camada de Enlace incorpora técnicas para verificar a integridade dos dados recebidos.

O objetivo principal da detecção de erros na Camada de Enlace é:

- Garantir a confiabilidade da comunicação local: Ao identificar quadros corrompidos, a camada pode descartá-los, evitando que dados errôneos sejam passados para as camadas superiores (especialmente a Camada de Rede).
- Solicitar retransmissão (em alguns casos): Alguns protocolos da Camada de Enlace, ao detectarem um erro, podem solicitar automaticamente a retransmissão do quadro corrompido pelo transmissor, garantindo a entrega correta dos dados.

Como a Detecção de Erros funciona na Camada de Enlace:

A detecção de erros geralmente envolve a adição de informações redundantes (bits extras) aos quadros de dados antes da transmissão. O dispositivo receptor realiza cálculos sobre os dados recebidos e as informações redundantes para verificar se houve alguma alteração. Se os cálculos não coincidirem, um erro é detectado.

Técnicas comuns de Detecção de Erros na Camada de Enlace:

- Bit de Paridade: Um bit adicional (paridade par ou ímpar) é adicionado a cada unidade de dados. O número total de bits '1' (incluindo o bit de paridade) deve ser par ou ímpar, dependendo do esquema de paridade utilizado. Se o receptor verificar uma paridade incorreta, um erro é detectado. É uma técnica simples, mas detecta apenas um número ímpar de erros.
- Checksum: Um valor numérico (checksum) é calculado com base nos dados transmitidos. Esse valor é incluído no quadro. O receptor realiza o mesmo cálculo nos dados recebidos e compara o resultado com o checksum recebido. Se os valores forem diferentes, um erro é detectado. O checksum é mais eficaz que o bit de paridade na detecção de múltiplos erros.
- CRC (Cyclic Redundancy Check): Uma técnica mais sofisticada e amplamente utilizada. Um polinômio gerador é usado para calcular um código de redundância cíclica (CRC) com base nos dados. Esse código é anexado ao quadro. O receptor realiza uma divisão polinomial nos dados recebidos usando o mesmo polinômio gerador. Se o resto da divisão for diferente de zero, um erro é detectado. O CRC é muito eficaz na detecção de uma grande variedade de erros, incluindo erros de burst (sequências de bits errados).

Exemplos no contexto dos protocolos da Camada de Enlace:

- Ethernet: Utiliza o CRC (normalmente CRC-32) para detecção de erros nos seus quadros.
- Wi-Fi: Também emprega o CRC para garantir a integridade dos dados transmitidos sem fio.
- HDLC e PPP: Podem utilizar o CRC como um dos seus mecanismos de detecção de erros.

É importante notar que a detecção de erros na Camada de Enlace não garante a ausência total de erros (principalmente em casos de múltiplos erros que se cancelam). No entanto, ela reduz significativamente a probabilidade de dados corrompidos serem passados para as camadas superiores, contribuindo para uma comunicação mais confiável dentro da rede local. A correção de erros, quando implementada na Camada de Enlace, geralmente envolve a retransmissão dos quadros detectados como errôneos.

semana 9- aula 02
Protocolos e Camadas
Camada de Enlace: Controle de Acesso ao Meio e Detecção de Erros
Código da aula: [SIS]ANO1C2B2S9A2

Objetivos da Aula:

- ❖ Compreender o controle de acesso ao meio e a detecção de erros da camada de enlace com uso de switches.
- ❖ Conhecer técnicas de computação e gerenciamento de dados para soluções em nuvem, parametrizando aplicações e dimensionando de acordo com as necessidades do negócio;
- ❖ Identificar e analisar problemas;

Exposição:

O Endereçamento MAC, também conhecido como endereçamento físico, é um identificador único de 48 bits (geralmente representado em formato hexadecimal) atribuído à placa de interface de rede (NIC) de um dispositivo. Ele opera na subcamada MAC (Media Access Control) da Camada de Enlace do Modelo OSI e tem como principal função identificar um dispositivo especificamente dentro de uma mesma rede local (LAN).

Pense no endereço MAC como o número de série gravado na sua placa de rede. Ele é único para cada interface de rede no mundo, teoricamente falando, pois é atribuído pelo fabricante do hardware.

As principais características do Endereçamento MAC são:

- Unicidade: Cada placa de rede fabricada deve ter um endereço MAC globalmente único. Isso evita conflitos de identificação dentro de uma rede local.
- Físico: O endereço MAC é gravado diretamente no hardware da placa de rede (na memória ROM ou outro tipo de memória não volátil) e, portanto, é considerado um endereço físico.
- Local: O endereçamento MAC é relevante apenas dentro do domínio de uma rede local. Roteadores utilizam endereços IP (da Camada de Rede) para encaminhar dados entre diferentes redes.
- Formato: Geralmente é representado por seis grupos de dois dígitos hexadecimais, separados por dois pontos, hífens ou sem separação (ex: `00:1A:2B:3C:4D:5E` ou `00-1A-2B-3C-4D-5E` ou `001A2B3C4D5E`).
- Estrutura: Os primeiros 24 bits do endereço MAC (conhecidos como OUI - Organizationally Unique Identifier) identificam o fabricante da placa de rede.

Os últimos 24 bits são atribuídos pelo fabricante para identificar unicamente a interface.

Em resumo, o Endereçamento MAC ou físico é a identidade de hardware de uma placa de rede, essencial para a comunicação e identificação de dispositivos dentro de uma rede local. Ele permite que switches e outros dispositivos da Camada de Enlace encaminhem corretamente os quadros de dados para o destino correto dentro do segmento de rede.

Em redes que utilizam switches, a detecção de erros ocorre principalmente no nível da Camada de Enlace, dentro do próprio switch, para garantir a integridade dos quadros que ele recebe e encaminha. Os switches implementam mecanismos de detecção de erros de forma semelhante a outros dispositivos da Camada de Enlace, focando em cada quadro individualmente.

Como a detecção de erros funciona em switches:

1. Recepção do Quadro: Quando um switch recebe um quadro em uma de suas portas, ele examina o quadro completo antes de tomar uma decisão sobre o seu encaminhamento (no modo de comutação "armazenar e encaminhar" - *store-and-forward*).

2. Verificação do Campo de Verificação de Sequência de Quadro (FCS - Frame Check Sequence): Cada quadro Ethernet (o protocolo mais comum em redes com switches) possui um campo chamado FCS no seu final (o *trailer* do quadro). Este campo contém um valor de CRC (Cyclic Redundancy Check).

3. Cálculo do CRC: O switch realiza o mesmo cálculo de CRC sobre os dados recebidos (os bytes do quadro entre os campos de endereço de destino e origem até o campo de dados) utilizando o mesmo polinômio gerador que o dispositivo transmissor utilizou para gerar o CRC original.

4. Comparação dos Valores de CRC: O valor de CRC calculado pelo switch é então comparado com o valor de CRC contido no campo FCS do quadro recebido.

5. Detecção de Erro:

    - Se os valores de CRC coincidirem: Isso indica que, muito provavelmente, os dados não foram corrompidos durante a transmissão entre o dispositivo de origem e o switch. O switch então prossegue com o processo de encaminhamento do quadro para a porta de destino apropriada.

    - Se os valores de CRC não coincidirem: Isso significa que um erro (ou múltiplos erros) ocorreu durante a transmissão. Nesse caso, o switch descarta o quadro defeituoso.

Importância da Detecção de Erros em Switches:

- Prevenção da Propagação de Dados Corrompidos: Ao descartar quadros com erros, os switches impedem que dados defeituosos se propaguem pela rede, evitando problemas de comunicação e inconsistências em outros dispositivos.
- Melhoria da Confiabilidade da Rede Local: A detecção de erros contribui para uma rede local mais confiável, garantindo que apenas dados íntegros sejam entregues aos dispositivos de destino.
- Diagnóstico de Problemas na Camada Física: Um alto número de quadros descartados devido a erros de CRC em uma porta específica de um switch pode indicar problemas na Camada Física, como cabos defeituosos, interferência eletromagnética ou problemas nas placas de rede dos dispositivos conectados a essa porta.

Observação: A maioria dos switches modernos opera no modo "armazenar e encaminhar" para garantir a integridade dos dados. Alguns switches mais antigos ou com configurações específicas podem operar em modo "corte direto" (*cut-through*), onde o encaminhamento do quadro começa antes que ele seja completamente recebido. Nesse modo, a detecção de erros pode ser limitada ou inexistente antes do início do encaminhamento, o que pode levar à propagação de quadros defeituosos. No entanto, o modo "armazenar e encaminhar" é o padrão para garantir a confiabilidade.

semana 9- aula 03
Protocolos e Camadas
Camada de Enlace: Controle de Acesso ao Meio e Detecção de Erros
Código da aula: [SIS]ANO1C2B2S9A3

Objetivos da Aula:

- Compreender as técnicas utilizadas na detecção de erros da camada de enlace.
- Conhecer técnicas de computação e gerenciamento de dados para soluções em nuvem, parametrizando aplicações e dimensionando de acordo com as necessidades do negócio;
- Identificar e analisar problemas;

Exposição:

Checksums são um tipo de técnica de detecção de erros utilizada em redes de computadores e armazenamento de dados para verificar a integridade dos dados transmitidos ou armazenados. Em essência, um checksum é um valor numérico calculado a partir de um bloco de dados. Esse valor é transmitido ou armazenado junto com os dados. O receptor (ou o sistema que lê os dados armazenados) realiza o mesmo cálculo sobre os dados recebidos/lidos e compara o resultado com o checksum recebido/armazenado.

Se os checksums coincidirem, é altamente provável que os dados não tenham sido alterados ou corrompidos durante a transmissão ou armazenamento.

Se os checksums não coincidirem, isso indica que houve uma alteração nos dados.

Como funciona o cálculo de um Checksum (de forma simplificada):

Existem diversas maneiras de calcular um checksum, mas uma das mais simples envolve os seguintes passos:

1. Dividir os dados: O bloco de dados é dividido em segmentos de tamanho fixo (por exemplo, bytes ou palavras de 16 bits).
2. Somar os segmentos: Esses segmentos são somados aritmeticamente.
3. Complemento de um (opcional): Em algumas implementações, o resultado da soma é complementado de um (todos os bits são invertidos).
4. O resultado é o Checksum: O valor final da soma (possivelmente complementado) é o checksum.

Exemplo Simplificado (usando bytes):

Suponha que os dados a serem transmitidos sejam os bytes: `0x45`, `0x6E`, `0x64`.

1. Soma: `0x45 + 0x6E + 0x64 = 0x157`

2. Truncamento (se necessário): Se o checksum for limitado a um byte, o overflow seria descartado, resultando em `0x57`.
3. Checksum: O checksum a ser transmitido junto com os dados seria `0x57`.

O receptor receberia os bytes `0x45`, `0x6E`, `0x64` e o checksum `0x57`. Ele realizaria a mesma soma (`0x45 + 0x6E + 0x64 = 0x157`) e, aplicando o mesmo truncamento (se necessário), obteria `0x57`. Como o checksum calculado coincide com o checksum recebido, assume-se que os dados foram transmitidos sem erros.

Características dos Checksums:

- Simples de implementar: Em geral, os algoritmos de checksum são relativamente fáceis de implementar em hardware e software.
- Rápido de calcular: O cálculo do checksum é geralmente rápido, adicionando pouca sobrecarga ao processo de transmissão ou armazenamento.
- Detecção de erros: São eficazes na detecção de muitos tipos de erros, especialmente erros aleatórios de um único bit e alguns erros de múltiplos bits.
- Limitações: Checksums mais simples podem não detectar todos os tipos de erros, especialmente se ocorrerem múltiplos erros que se "cancelam" na soma. Técnicas mais robustas como CRC (Cyclic Redundancy Check) oferecem uma maior capacidade de detecção de erros.

Onde os Checksums são utilizados:

- Protocolos de rede: Protocolos como TCP (na camada de transporte) e IP (na camada de rede) utilizam checksums para verificar a integridade dos seus cabeçalhos e, em alguns casos, dos dados.
- Armazenamento de dados: Alguns sistemas de arquivos e softwares de backup utilizam checksums para verificar se os arquivos foram corrompidos durante o armazenamento ou a transferência.
- Download de arquivos: Muitas vezes, ao baixar arquivos da internet, um checksum (geralmente em formatos como MD5 ou SHA) é fornecido para que o usuário possa verificar se o arquivo baixado está completo e não foi corrompido.

Em resumo, checksums são valores numéricos derivados de dados que servem como uma "assinatura" para verificar a integridade desses dados após a transmissão ou armazenamento. Eles oferecem uma maneira rápida e relativamente simples de detectar muitos tipos de erros, embora possam ter limitações em comparação com técnicas mais avançadas de detecção de erros.

Análise da diferenças entre Checksum e CRC

Eficiência na Detecção de Erros:

- Checksum: É um método simples que basicamente soma os valores dos dados transmitidos e usa o resultado (com algumas variações, como complemento de um) como um valor de verificação. Ele é eficiente para detectar erros simples, como a alteração de um único bit ou um pequeno número de bits adjacentes. No entanto, o checksum pode falhar em detectar erros mais complexos, como a troca de ordem de bits ou múltiplos erros que se cancelam na soma.

- CRC (Cyclic Redundancy Check): Utiliza a divisão polinomial em um campo finito para gerar um código de redundância. Essa abordagem torna o CRC significativamente mais eficiente na detecção de uma ampla gama de erros, incluindo erros únicos, múltiplos erros isolados, erros em burst (sequências de bits errados) e até mesmo alguns padrões de erros mais complexos. A eficiência do CRC depende do polinômio gerador escolhido; polinômios mais longos geralmente oferecem maior poder de detecção.

Complexidade de Implementação:

- Checksum: A implementação do checksum é relativamente simples. Envolve operações básicas de adição e, possivelmente, complementação. Isso torna o checksum fácil de entender e implementar em hardware e software, exigindo poucos recursos computacionais.

- CRC: A implementação do CRC é mais complexa. Envolve operações de divisão polinomial, que podem ser implementadas usando registradores de deslocamento com feedback XOR (LFSRs) em hardware ou por meio de algoritmos mais elaborados em software. Embora a lógica subjacente não seja excessivamente difícil, a implementação eficiente, especialmente em hardware de alta velocidade, requer um conhecimento mais aprofundado.

Velocidade de Processamento:

- Checksum: Devido à sua simplicidade, o cálculo do checksum é geralmente muito rápido. As operações de adição são rápidas e podem ser facilmente otimizadas. Isso torna o checksum adequado para aplicações onde a velocidade é crucial e a taxa de erro esperada é baixa.

- CRC: O processamento do CRC é mais lento que o checksum, especialmente quando implementado em software. As operações de divisão polinomial exigem mais ciclos de processamento. No entanto, implementações em hardware podem alcançar velocidades muito altas, tornando o CRC viável para aplicações de alta velocidade, como redes de comunicação. A velocidade do CRC depende do tamanho do polinômio gerador e da eficiência da implementação.

Aplicações Ideais:

- Checksum:
    - Aplicações com baixa probabilidade de erros: Onde erros complexos são raros e a velocidade é primordial.
    - Verificações rápidas e simples: Em cenários onde uma camada adicional de detecção de erros, mesmo que básica, é desejada com baixo overhead.
    - Alguns protocolos de rede mais antigos ou mais simples: Onde a complexidade era uma grande preocupação.
    - Verificação de integridade de arquivos pequenos: Onde a velocidade da verificação é mais importante que a robustez contra erros complexos.
- CRC:
    - Comunicação de dados: Amplamente utilizado em protocolos de rede (Ethernet, Wi-Fi), armazenamento de dados (HDDs, SSDs), compressão de dados (ZIP, RAR) e transmissão digital (DVD, Blu-ray) devido à sua alta capacidade de detecção de erros.
    - Aplicações onde a integridade dos dados é crucial: Onde a detecção de uma ampla gama de erros é fundamental para garantir a confiabilidade.
    - Sistemas com maior probabilidade de ruído ou interferência: Onde erros em burst são mais comuns.

semana 10- aula 01
Meios de transmissão
Meios de transmissão sem fio: Wi-Fi e Bluetooth
Código da aula: [SIS]ANO1C2B2S10A1

Objetivos da Aula:

- ❖ Demonstrar como os meios de transmissão não guiados são fundamentais dentro das redes de computadores.
- ❖ Compreender o que é e como funciona a rede sem fio.
- ❖ Conhecer técnicas de computação e gerenciamento de dados para soluções em nuvem, parametrizar aplicações e dimensiona-las de acordo com as necessidades do negócio.
- ❖ Resolver problemas técnicos computacionais.

Exposição:

Meios de transmissão sem fio referem-se às formas de comunicação que não utilizam cabos físicos para transmitir informações. Em vez disso, elas empregam ondas eletromagnéticas, como ondas de rádio, micro-ondas, infravermelho ou luz visível, para enviar dados através do ar ou do espaço.

Essas tecnologias permitem a comunicação entre dispositivos a distâncias variadas, proporcionando mobilidade e flexibilidade onde o uso de cabos seria impraticável ou indesejável.

Exemplos comuns de meios de transmissão sem fio:

- Wi-Fi: Amplamente utilizado para redes locais sem fio (WLAN - Wireless Local Area Network), o Wi-Fi permite que dispositivos como smartphones, laptops e smart TVs se conectem à internet ou se comuniquem entre si dentro de uma área limitada, como uma casa, escritório ou hotspot público. Ele opera geralmente nas frequências de 2.4 GHz e 5 GHz.
    - *Exemplo:* Conectar seu celular à rede Wi-Fi da sua casa para acessar a internet.
- Bluetooth: Tecnologia de curto alcance (WPAN - Wireless Personal Area Network) ideal para conectar dispositivos próximos, eliminando a necessidade de cabos para передачи de dados ou áudio.
    - *Exemplo:* Emparelhar fones de ouvido sem fio ao seu smartphone para ouvir música, conectar um mouse ou teclado sem fio a um computador.
- Redes Celulares (3G, 4G, 5G): Permitem a comunicação móvel em áreas geográficas amplas (WWAN - Wireless Wide Area Network) através de torres de celular. São essenciais para a comunicação por voz, acesso à internet

móvel e uma variedade de serviços em dispositivos portáteis.

    - *Exemplo:* Fazer uma chamada telefônica do seu celular, navegar na internet usando os dados móveis.
- Infravermelho: Utilizado para comunicação de curto alcance e geralmente requer uma linha de visão direta entre os dispositivos.

    - *Exemplo:* O controle remoto da sua televisão, que usa raios infravermelhos para mudar de canal ou ajustar o volume.
- Comunicação por Satélite: Permite a transmissão de dados e sinais por longas distâncias, cobrindo áreas extensas e até mesmo remotas onde outras infraestruturas de comunicação são limitadas.

    - *Exemplo:* Serviços de TV por satélite, comunicação via satélite para telefones em áreas isoladas, sistemas de GPS (Sistema de Posicionamento Global).
- NFC (Near Field Communication): Tecnologia de curtíssimo alcance que permite a comunicação entre dispositivos quando estão a poucos centímetros de distância.

    - *Exemplo:* Realizar pagamentos por aproximação com seu celular em terminais de pagamento, parear dispositivos Bluetooth rapidamente apenas encostando-os.
- RFID (Radio-Frequency Identification): Utiliza campos eletromagnéticos para identificar e rastrear automaticamente etiquetas anexadas a objetos.

    - *Exemplo:* Etiquetas de segurança em lojas, sistemas de controle de acesso, rastreamento de inventário em logística.

Em resumo, os meios de transmissão sem fio são a base da comunicação moderna sem a dependência de conexões físicas, permitindo a mobilidade, a conectividade em locais de difícil cabeamento e a criação de uma vasta gama de aplicações e serviços que fazem parte do nosso cotidiano.

semana 10- aula 02
Meios de transmissão
Meios de transmissão sem fio: Wi-Fi e Bluetooth
Código da aula: [SIS]ANO1C2B2S10A2

Objetivos da Aula:

- ❖ Demonstrar como os meios de transmissão não guiados são fundamentais dentro das redes de computadores.
- ❖ Compreender o que é e como funciona a rede sem fio.
- ❖ Conhecer técnicas de computação e gerenciamento de dados para soluções em nuvem, parametrizar aplicações e dimensiona-las de acordo com as necessidades do negócio.
- ❖ Resolver problemas técnicos computacionais.

Exposição:

Como Funciona a Rede Sem Fio Wi-Fi:

O Wi-Fi é uma tecnologia que permite a comunicação entre dispositivos sem a necessidade de cabos físicos, utilizando ondas de rádio para transmitir dados. Pense nisso como uma estação de rádio local que envia e recebe informações.

1. Componentes Principais:
    - Roteador Wi-Fi (ou Ponto de Acesso): Este é o coração da rede sem fio. Ele se conecta à internet (geralmente via um cabo Ethernet que vem de um modem) e atua como uma ponte entre a rede cabeada (internet) e a rede sem fio (seus dispositivos). O roteador contém antenas que transmitem e recebem sinais de rádio.
    - Dispositivos Cliente: São os aparelhos que você usa, como smartphones, laptops, tablets, smart TVs, consoles de videogame, etc., que possuem adaptadores Wi-Fi embutidos. Esses adaptadores são capazes de enviar e receber os sinais de rádio.
2. O Processo de Comunicação:
    - O roteador recebe dados da internet (por exemplo, uma página da web que você solicitou).
    - Ele converte esses dados em sinais de rádio.
    - Esses sinais de rádio são transmitidos pelo ar através das antenas do roteador, usando frequências específicas (mais comuns são 2.4 GHz e 5 GHz).
    - Seu dispositivo (com o adaptador Wi-Fi) "ouve" esses sinais de rádio.
    - O adaptador Wi-Fi no seu dispositivo recebe o sinal, o converte de volta em dados que o dispositivo pode entender e processar (exibindo a página da web).

- Quando você envia dados (como digitar um endereço de site), seu dispositivo converte esses dados em sinais de rádio e os envia de volta para o roteador.
- O roteador recebe esses sinais, os converte de volta em dados e os envia para a internet (ou para outro dispositivo na rede local).

3. Identificação da Rede:

    - SSID (Service Set Identifier): Cada rede Wi-Fi tem um nome único, chamado SSID (por exemplo, "MinhaCasaWifi", "RedeDoCafe"). Quando você procura redes Wi-Fi no seu dispositivo, vê uma lista de SSIDs disponíveis.
    - Senha (ou Chave de Segurança): Para evitar que qualquer pessoa se conecte à sua rede e acesse seus dados ou use sua internet, as redes Wi-Fi são geralmente protegidas por senha (usando protocolos de segurança como WPA2 ou WPA3). Seu dispositivo precisa da senha correta para se autenticar com o roteador e ter permissão para enviar e receber dados.

Como é Configurado um Roteador Wi-Fi:

A configuração de um roteador envolve acessar sua interface de gerenciamento e definir os parâmetros para a conexão com a internet e a criação da rede sem fio. O processo geral é o seguinte:

1. Conectar-se ao Roteador:

    - Primeiro, conecte um computador ou outro dispositivo ao roteador. Isso pode ser feito via cabo Ethernet (diretamente de uma porta LAN do roteador para a porta Ethernet do computador) ou, em alguns casos, conectando-se à rede Wi-Fi padrão do roteador (que geralmente vem sem senha ou com uma senha padrão impressa no aparelho).
    - Conecte a porta WAN (ou Internet) do roteador ao seu modem (onde vem o sinal da internet).
2. Acessar a Interface de Configuração:

    - Abra um navegador web (como Chrome, Firefox, Edge, etc.) no dispositivo conectado ao roteador.
    - Na barra de endereço do navegador, digite o endereço IP do roteador. Os endereços mais comuns são `192.168.1.1`, `192.168.0.1` ou `10.0.0.1`. Este endereço geralmente está impresso no roteador ou no manual.
    - Você será solicitado a inserir um nome de usuário e uma senha para acessar a interface. As credenciais padrão (geralmente `admin`/`admin`,

admin/password ou similares) também costumam estar no roteador ou no manual. É crucial alterar essas credenciais padrão por segurança!

3. Configurações Principais: Uma vez logado na interface, você encontrará várias opções, mas as mais importantes para a configuração inicial incluem:
    - Configuração de Internet (WAN Settings): Definir como o roteador se conecta ao seu provedor de internet. Na maioria dos casos, isso será feito automaticamente via DHCP, mas pode requerer configurar PPPoE (com nome de usuário e senha fornecidos pelo provedor) ou IP estático.
    - Configuração de Rede Sem Fio (Wireless Settings):
        - Nome da Rede (SSID): Defina o nome que você quer que sua rede Wi-Fi apareça para os dispositivos.
        - Tipo de Segurança/Criptografia: Escolha o método de segurança (WPA2-PSK ou WPA3 são os mais recomendados).
        - Senha da Rede Wi-Fi (Wireless Password/Passphrase): Crie uma senha forte para sua rede sem fio.
        - Frequência (2.4 GHz / 5 GHz): Alguns roteadores permitem configurar as redes de 2.4 GHz e 5 GHz separadamente, com nomes e senhas diferentes, ou unificadas.
        - Canal: Embora geralmente configurado automaticamente, em ambientes com muitas redes vizinhas, escolher um canal menos congestionado manualmente pode melhorar o desempenho.
    - Configurações de Rede Local (LAN Settings): Geralmente, a configuração padrão do DHCP (servidor que atribui IPs automaticamente aos seus dispositivos) já funciona bem, mas você pode ver ou alterar o endereço IP do próprio roteador na rede local (o gateway).
    - Alterar Senha de Acesso ao Roteador (Administration/Management): Essencial! Altere o nome de usuário e a senha padrão que você usou para acessar a interface de configuração.
4. Salvar e Reiniciar: Após fazer as alterações, salve as configurações. O roteador provavelmente reiniciará para que as novas configurações entrem em vigor.

Muitos roteadores modernos vêm com um "Assistente de Configuração Rápida" (Quick Setup Wizard) que simplifica esses passos iniciais, guiando o usuário através do processo de conexão com a internet e configuração básica do Wi-Fi.

semana 10- aula 03
Meios de transmissão
Meios de transmissão sem fio: Wi-Fi e Bluetooth
Código da aula: [SIS]ANO1C2B2S10A3

Objetivos da Aula:

- Compreender como funciona a rede sem fio Bluetooth.

Exposição:

Bluetooth é uma tecnologia de comunicação sem fio de curto alcance e baixo consumo de energia. Seu principal objetivo é permitir a troca de dados entre dispositivos próximos, substituindo a necessidade de cabos em muitas situações. É ideal para criar redes pessoais sem fio (WPAN - Wireless Personal Area Network).

Como Funciona:

1. Ondas de Rádio: O Bluetooth opera na banda de frequência de 2.4 GHz, que é uma faixa de frequência livre para uso global (Banda ISM - Industrial, Scientific and Medical). Ele utiliza uma técnica chamada "salto de frequência" (frequency hopping) para alternar rapidamente entre diferentes canais dentro dessa banda, o que ajuda a reduzir a interferência de outros dispositivos que operam na mesma frequência (como alguns fornos de micro-ondas e redes Wi-Fi mais antigas).

2. Pareamento (Pairing): Para que dois dispositivos Bluetooth se comuniquem pela primeira vez, eles precisam passar por um processo de pareamento. Neste processo, os dispositivos trocam informações e criam uma conexão segura e exclusiva. Geralmente, um dispositivo se torna o "Mestre" (Master) ou "Central" e o outro se torna o "Escravo" (Slave) ou "Periférico". Após o pareamento inicial, eles geralmente se reconhecem automaticamente em futuras conexões.

3. Piconet: Uma vez pareados e conectados, os dispositivos formam uma pequena rede ad-hoc chamada "piconet". Uma piconet típica consiste em um dispositivo mestre e até sete dispositivos escravos ativos. O mestre controla a comunicação dentro da piconet.

4. Troca de Dados: A comunicação dentro da piconet ocorre através dos sinais de rádio. Os dados são divididos em pacotes e enviados entre os dispositivos. O baixo consumo de energia é uma característica chave, tornando-o adequado para dispositivos alimentados por bateria.

Características Principais:

- Curto Alcance: O alcance típico varia de cerca de 10 metros (Classe 2, mais comum em celulares e PCs) a até 100 metros (Classe 1, para aplicações industriais ou de maior alcance).
- Baixo Consumo de Energia: Projetado para consumir pouca energia, o que é vital para dispositivos portáteis e vestíveis.
- Conexão Ponto a Ponto ou Ponto-Multiponto (Piconet): Permite a comunicação direta entre dois dispositivos ou entre um mestre e vários escravos.
- Baixo Custo: A tecnologia é relativamente barata de implementar em dispositivos.

Exemplos de Uso:

- Conectar fones de ouvido sem fio a um smartphone ou computador.
- Conectar teclados, mouses ou gamepads sem fio.
- Transferir arquivos (fotos, documentos) entre smartphones.
- Conectar o celular ao sistema de áudio de um carro.
- Conectar smartwatches e pulseiras fitness ao smartphone.
- Conectar dispositivos de Internet das Coisas (IoT) de baixo consumo.
- Usar alto-falantes sem fio.

Em resumo, o Bluetooth é uma tecnologia de comunicação sem fio otimizada para conexões de curto alcance entre dispositivos pessoais e periféricos, focando em praticidade e eficiência energética.

Link do vídeo: https://www.youtube.com/watch?v=xXzRKgZbKW8

semana 11 - aula 01

Protocolos e Camadas

Camada de Rede: Roteamento e Endereçamento IP

Código da aula: [SIS]ANO1C2B2S11A1

Objetivos da Aula:

- Compreender a Camada de rede do Modelo OSI e conhecer suas funções.
- Conhecer técnicas de computação e gerenciar dados para soluções em nuvem, parametrizar aplicações e dimensionar de acordo com as necessidades do negócio;
- Identificar e analisar problemas;
- Agir com curiosidade e criatividade na resolução de problemas técnicos.
- Recurso audiovisual para exibição de vídeos e imagens;
- Lápis e caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição:

Definição:

Esta aula aborda a Camada de Rede (Camada 3) do Modelo OSI (Open Systems Interconnection), que é responsável pelo roteamento de pacotes entre diferentes redes. Suas funções incluem o endereçamento lógico (IP), a determinação do melhor caminho para a entrega dos dados (roteamento) e a fragmentação/remontagem de pacotes, se necessário. Serão explorados os principais protocolos que operam nesta camada, como o IP (Internet Protocol), que é a base para a comunicação na internet.

Exemplos:

- **Endereçamento Lógico (IP):** Quando você digita um endereço de site no navegador, o sistema de nomes de domínio (DNS) o traduz para um endereço IP (e.g., `192.168.1.1` ou `2001:0db8::1`), que a camada de rede utiliza para direcionar o pacote.
- **Roteamento:** Um roteador, ao receber um pacote de dados, analisa o endereço IP de destino e, usando sua tabela de roteamento, decide qual a próxima "salto" (next hop) para que o pacote chegue ao seu destino final, passando por diversas redes até atingir o objetivo.
- **Fragmentação:** Se um pacote de dados é muito grande para ser transmitido por um determinado meio de rede, a camada de rede pode dividi-lo em pedaços menores (fragmentos) que são enviados individualmente e remontados no destino.

- **Protocolo IP:** O IP é o protocolo fundamental que permite que dados sejam enviados de uma origem para um destino através de várias redes interconectadas, como na internet.

slide 04

A **Camada de Rede**, ou Camada 3 do Modelo OSI, é o coração da comunicação entre diferentes redes e a base para a Internet como a conhecemos. Sua principal função é o roteamento, que é o processo de encontrar o melhor caminho para os pacotes de dados viajarem de uma origem a um destino, mesmo que estejam em redes geograficamente distantes e com tecnologias distintas. Para que isso seja possível, ela utiliza o conceito de endereçamento lógico, sendo o Protocolo da Internet (IP) o mais proeminente e universalmente utilizado. O IP permite que cada dispositivo conectado a uma rede global tenha um identificador único, tornando possível a entrega precisa dos dados.

Os **roteadores** são os dispositivos chave nesta camada. Eles funcionam como "guardas de trânsito", analisando os endereços IP de destino dos pacotes e, com base em suas tabelas de roteamento, encaminhando-os para a próxima etapa em direção ao seu objetivo. É graças a essa capacidade de roteamento que podemos enviar um e-mail para alguém do outro lado do mundo ou acessar um site hospedado em um servidor distante.

---

semana 11 - aula 02

Protocolos e Camadas

Camada de Rede: Endereçamento IP, ARP, ICMP e CIDR

Código da aula: [SIS]ANO1C2B2S11A2

Objetivos da Aula:

- Compreender a Camada de rede do Modelo OSI, o endereçamento IP e os protocolos associados.
- Conhecer técnicas de computação e gerenciar dados para soluções em nuvem, parametrizar aplicações e dimensionar de acordo com as necessidades do negócio;
- Identificar e analisar problemas;
- Agir com curiosidade e criatividade na resolução de problemas técnicos.
- Recurso audiovisual para exibição de vídeos e imagens;
- Lápis e caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição:

Definição:

Esta aula aprofunda o estudo do endereçamento IP, incluindo a compreensão do Protocolo de Resolução de Endereços (ARP - Address Resolution Protocol), que mapeia endereços IP lógicos para endereços MAC físicos. Também será abordado o Protocolo de Mensagens de Controle da Internet (ICMP - Internet Control Message Protocol), utilizado para enviar mensagens de erro e controle de rede. Por fim, será introduzido o CIDR (Classless Inter-Domain Routing), uma técnica eficiente de alocação de endereços IP e roteamento sem classes, que visa combater o esgotamento de endereços IPv4.

Exemplos:

- **Endereçamento IP:** Um computador em uma rede local com endereço IP `192.168.1.10` tentando se comunicar com um servidor em `192.168.1.50`.
- **ARP:** Quando o computador `192.168.1.10` precisa enviar dados para `192.168.1.50`, mas não sabe o endereço MAC do servidor, ele envia uma requisição ARP para descobrir essa informação, e o servidor responde com seu MAC.
- **ICMP:** O comando `ping` utiliza o ICMP para verificar a conectividade com um host. Se o host estiver inacessível, uma mensagem ICMP de "destino inacessível" pode ser gerada.
- **CIDR:** Em vez de usar classes de IP (A, B, C), o CIDR permite a alocação de blocos de endereços IP de tamanho variável, como `192.168.0.0/24`, o que otimiza o uso do espaço de endereçamento.

slide 04

Dando continuidade ao estudo da Camada de Rede, esta aula aprofunda a compreensão do **endereçamento IP** e introduz protocolos auxiliares que são cruciais para o seu funcionamento. O **ARP (Address Resolution Protocol)** é um desses pilares; ele é responsável por resolver o endereçamento lógico (IP) para o endereçamento físico (MAC) dentro de uma rede local. Imagine que o IP é o "nome" do seu vizinho, e o MAC é o "endereço da casa" dele. O ARP é quem faz essa tradução, permitindo que os dispositivos se encontrem na mesma rua.

Outro protocolo vital é o **ICMP (Internet Control Message Protocol)**. Este protocolo não transporta dados de aplicação, mas sim mensagens de controle e erro, essenciais para a saúde e diagnóstico da rede. Ferramentas como o `ping` e o `traceroute` dependem do ICMP para verificar a conectividade e identificar gargalos ou falhas na rota de comunicação. Conhecer o ICMP nos permite diagnosticar problemas de rede de forma eficaz.

Por fim, abordamos o **CIDR (Classless Inter-Domain Routing)**. Historicamente, os endereços IP eram divididos em classes (A, B, C), o que gerava um desperdício significativo de endereços. O CIDR revolucionou a forma como os blocos de endereços IP são alocados e roteados, permitindo uma distribuição mais flexível e eficiente. Ele se tornou fundamental para mitigar o **esgotamento dos endereços IPv4**, ao maximizar o uso do espaço de endereçamento disponível e prolongar a vida útil do IPv4 enquanto a transição para o IPv6 avança. A compreensão do CIDR é essencial para o gerenciamento eficaz de redes modernas e para a otimização do roteamento.

---

semana 11 - aula 03

Protocolos e Camadas

Camada de Rede: Roteamento e IPv6

Código da aula: [SIS]ANO1C2B2S11A3

Objetivos da Aula:

- Compreender a Camada de rede do Modelo OSI e o endereçamento IP, roteamento e IPv6.
- Conhecer técnicas de computação e gerenciar dados para soluções em nuvem, parametrizar aplicações e dimensionar de acordo com as necessidades do negócio;
- Identificar e analisar problemas;
- Agir com curiosidade e criatividade na resolução de problemas técnicos.
- Recurso audiovisual para exibição de vídeos e imagens;
- Lápis e caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição:

Definição:

Esta aula foca no processo de roteamento em redes de computadores, que envolve a escolha do melhor caminho para o envio de pacotes de dados. Serão explorados os conceitos e a necessidade da transição para o IPv6 (Internet Protocol version 6), a versão mais recente do protocolo IP. A aula detalha as características do IPv6, suas vantagens em relação ao IPv4, como o vasto espaço de endereçamento e melhorias de segurança, bem como os desafios de sua implementação.

Exemplos:

- **Roteamento:** Roteadores utilizam protocolos de roteamento (como OSPF ou BGP) para trocar informações sobre as rotas disponíveis e determinar o caminho mais eficiente para enviar pacotes de dados através da internet.
- **IPv6:** Um endereço IPv6 como `2001:0db8:85a3:0000:0000:8a2e:0370:7334`, que oferece um número exponencialmente maior de endereços em comparação com o IPv4.
- **Transição para IPv6:** Grandes provedores de internet e empresas, como Google e Facebook, já implementaram o IPv6 em suas infraestruturas para lidar com o crescimento da internet e o esgotamento de endereços IPv4.

slide 04

Nesta aula final da semana, aprofundamos o conceito de **roteamento** e aprofundamos na próxima geração do Protocolo da Internet: o **IPv6**. O roteamento é o processo pelo qual os roteadores determinam o melhor caminho para os pacotes de dados viajarem entre diferentes redes. Isso é realizado através de algoritmos complexos e tabelas de roteamento dinâmicas, que são constantemente atualizadas com informações sobre a topologia da rede e a disponibilidade das rotas. Compreender como o roteamento funciona é fundamental para projetar e solucionar problemas em redes complexas.

A necessidade do **IPv6** surge da iminente exaustão dos endereços IPv4. Com o crescimento exponencial de dispositivos conectados à internet (IoT, smartphones, etc.), o espaço de endereçamento de 32 bits do IPv4 tornou-se insuficiente. O IPv6, com seus **endereços de 128 bits**, oferece um número colossal de endereços únicos, virtualmente ilimitado para as necessidades futuras da internet. Essa expansão massiva de endereços é a principal vantagem do IPv6.

Além do vasto espaço de endereçamento, o IPv6 traz outras melhorias significativas. Ele foi projetado com maior **segurança** em mente, incorporando recursos como IPsec (IP Security) de forma nativa. Também simplifica o cabeçalho dos pacotes, o que pode levar a um **melhor desempenho** de roteamento e processamento de pacotes pelos roteadores. Embora a transição do IPv4 para o IPv6 apresente desafios de implementação e compatibilidade, ela é um passo inevitável e crucial para garantir a escalabilidade e a continuidade da Internet. As empresas e provedores de serviços de internet em todo o mundo estão gradualmente migrando para o IPv6 para preparar a rede para o futuro.