



REDES DE COMPUTADORES

EDMAR ALVES SENNE

ACESSE AQUI ESTE
MATERIAL DIGITAL!

EXPEDIENTE

Coordenador(a) de Conteúdo

Edmar Alves Senne

Projeto Gráfico e Capa

Arthur Cantareli Silva

Editoração

Alan Diego Hordinha

Design Educacional

Rossana Costa Giani

Revisão Textual

Elaine Machado

Ilustração

André Azevedo, Bruno Pardinho e

Eduardo Aparecido Alves

Fotos

Shutterstock e Envato

FICHA CATALOGRÁFICA

N964 Núcleo de Educação a Distância. **SENNE**, Edmar Alves.

Redes de Computadores / Edmar Alves Senne. - Florianópolis,
SC: Arqué, 2025.

264 p.

ISBN papel 978-65-279-1066-4

ISBN digital 978-65-279-1065-7

1. Redes 2. Computadores 3. EaD. I. Título.

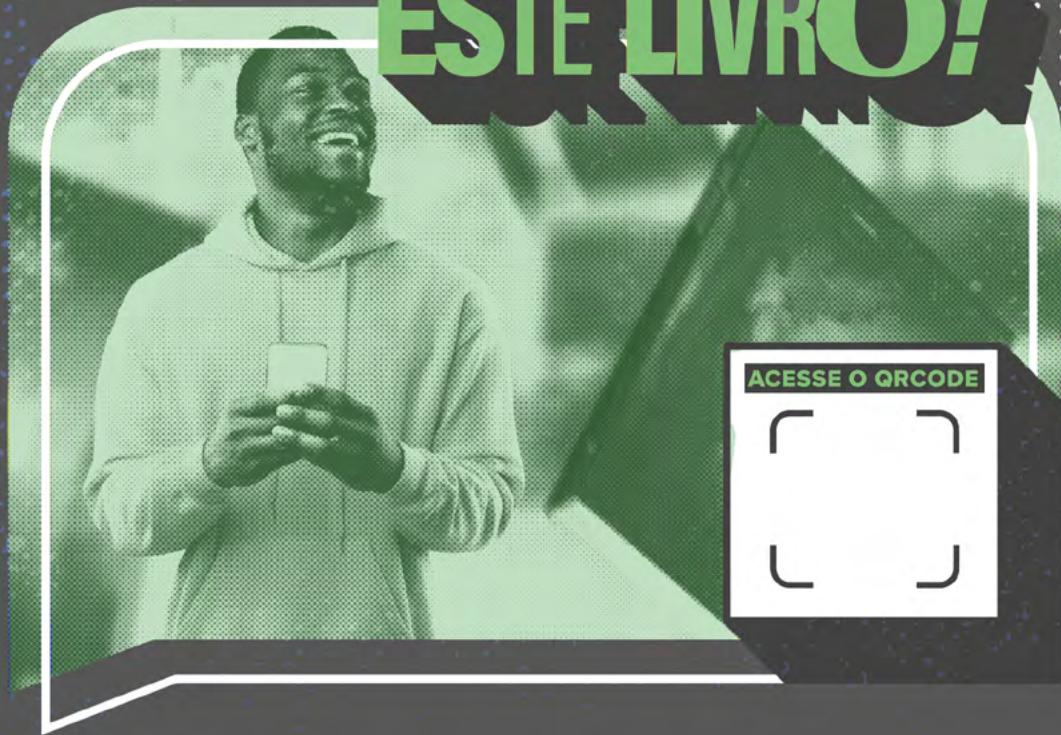
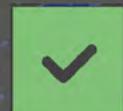
CDD - 004.62

Bibliotecária: Leila Regina do Nascimento - CRB- 9/1722.

Ficha catalográfica elaborada de acordo com os dados fornecidos pelo(a) autor(a).

Impresso por:

AVALIE ESTE LIVRO!



ACESSE O QR CODE



CRIAR MOMENTOS DE APRENDIZAGENS
INESQUECÍVEIS É O NOSSO OBJETIVO E POR ISSO,
GOSTARIAMOS DE SABER COMO FOI SUA EXPERIÊNCIA.

Conta para nós! leva *menos de 2 minutos*. Vamos lá?!

DIGITE O CÓDIGO

02511835

Aa

RESPOnda A
PESQUISA

... ?

... Aa



RECURSOS DE IMERSÃO



PENSANDO JUNTOS

Este item corresponde a uma proposta de reflexão que pode ser apresentada por meio de uma frase, um trecho breve ou uma pergunta.



APROFUNDANDO

Utilizado para temas, assuntos ou conceitos avançados, levando ao aprofundamento do que está sendo trabalhado naquele momento do texto.



EU INDICO

Utilizado para agregar um conteúdo externo.



ZOOM NO CONHECIMENTO

Utilizado para desmistificar pontos que possam gerar confusão sobre o tema. Após o texto trazer a explicação, essa interlocução pode trazer pontos adicionais que contribuam para que o estudante não fique com dúvidas sobre o tema.

PRODUTOS AUDIOVISUAIS

Os elementos abaixo possuem recursos audiovisuais. Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.



PLAY NO CONHECIMENTO

Professores especialistas e convidados, ampliando as discussões sobre os temas por meio de fantásticos podcasts.



EM FOCO

Utilizado para aprofundar o conhecimento em conteúdos relevantes utilizando uma linguagem audiovisual.



INDICAÇÃO DE FILME

Uma dose extra de conhecimento é sempre bem-vinda. Aqui você terá indicações de filmes que se conectam com o tema do conteúdo.

FILME



INDICAÇÃO DE LIVRO

Uma dose extra de conhecimento é sempre bem-vinda. Aqui você terá indicações de livros que agregarão muito na sua vida profissional.

LIVRO



CAMINHOS DE APRENDIZAGEM

7

UNIDADE 1

FUNDAMENTOS DE REDES DE COMPUTADORES	8
--	---

37

UNIDADE 2

PROTOCOLOS E COMUNICAÇÃO EM REDES	38
---	----

TOPOLOGIAS E MEIOS DE TRANSMISSÃO	56
---	----

95

UNIDADE 3

MODELOS DE REFERÊNCIA E ARQUITETURAS DE REDE	96
--	----

SEGURANÇA EM REDES	128
------------------------------	-----

157

UNIDADE 4

REDES SEM FIO E MOBILIDADE	158
--------------------------------------	-----

ADMINISTRAÇÃO E GERENCIAMENTO DE REDES	182
--	-----

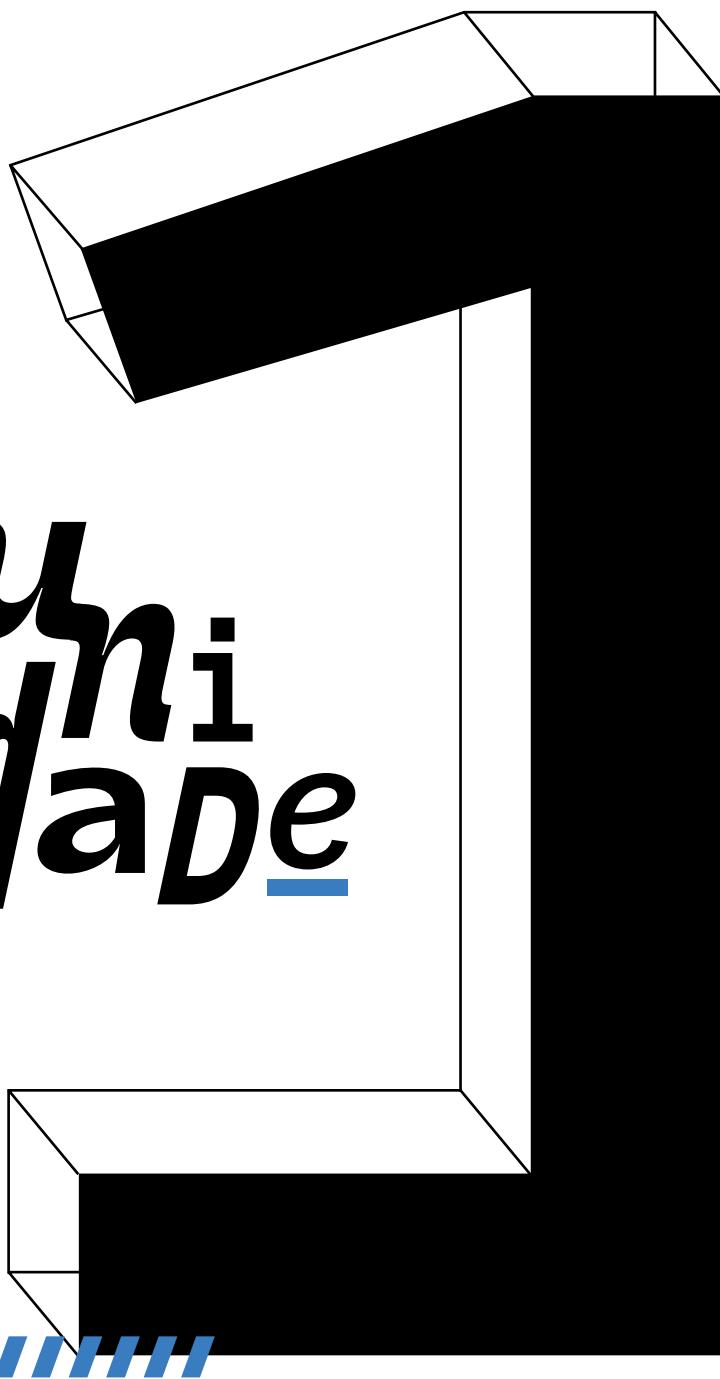
203

UNIDADE 5

REDES EM NUVEM E VIRTUALIZAÇÃO	204
--	-----

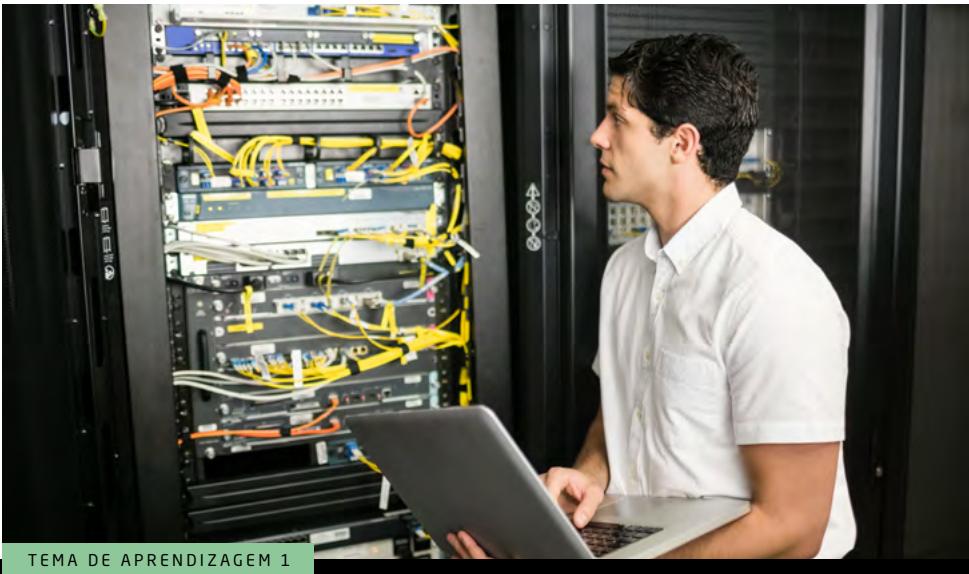
TÓPICOS AVANÇADOS EM REDES	240
--------------------------------------	-----





*uni
dade*

The graphic design features a large, bold, black sans-serif typeface for the word "uni". Below it, the word "dade" is written in a similar font, with the letter "d" being the most prominent. A horizontal blue line underlines the "d" of "dade". The background is white, and the letters are partially obscured by several black geometric shapes. These shapes include a large trapezoidal block above the "uni" and a tall rectangular block to the right of the "dade" that has a vertical white stripe. At the bottom, there's a smaller trapezoidal shape and a series of blue diagonal stripes.



TEMA DE APRENDIZAGEM 1

FUNDAMENTOS DE REDES DE COMPUTADORES

MINHAS METAS

- Compreender os conceitos básicos de Redes de Computadores.
- Analisar a evolução das Redes de Computadores.
- Reconhecer a importância das Redes na Engenharia de Software.
- Explorar diferentes Arquiteturas de Redes e Seus Componentes.
- Classificar e diferenciar tipos de Redes de Computadores (LAN, WAN, MAN).
- Abordar tendências emergentes em Redes de Computadores.
- Aplicar conhecimentos de Redes para resolver problemas práticos.

INICIE SUA JORNADA

Estudante, imagine você em um dia típico como um profissional moderno: você verifica e-mails no smartphone enquanto toma café da manhã, participa de uma reunião virtual com colegas de diferentes partes do mundo, acessa documentos armazenados na nuvem e colabora em tempo real em projetos com outras pessoas. Se tudo isso simplesmente parasse de funcionar, como você completaria suas tarefas? Esse cenário destaca a importância das redes de computadores.

É importante entendermos que em qualquer campo da tecnologia da informação podemos otimizar seu desempenho. Esse conhecimento não apenas permite que você construa sistemas mais eficientes e seguros, mas também abre portas para inovações que podem transformar indústrias inteiras. A habilidade de projetar e gerenciar redes eficazes é uma competência essencial que diferencia profissionais no mercado de trabalho, tornando-os mais valiosos e indispensáveis.

A experimentação em ambientes controlados, como laboratórios de redes, permite que você, estudante, coloque em prática os conceitos aprendidos, simule problemas reais e teste suas soluções. Configurar roteadores, *Switches* e pontos de acesso, criar e administrar redes locais (LANs) e explorar tecnologias emergentes como a Internet das Coisas (IoT) são atividades práticas que enriquecem o aprendizado. Essa experimentação prepara você para enfrentar desafios no mundo real, desenvolvendo habilidades técnicas e resolução de problemas.

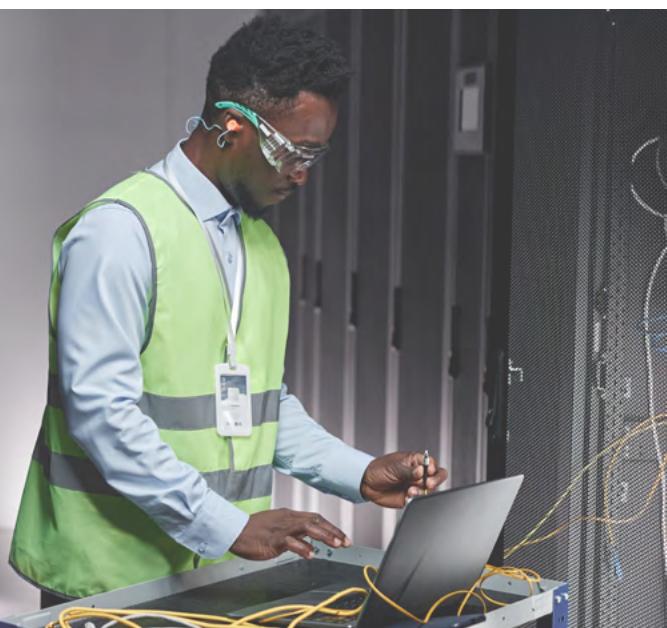
Ao final do processo de aprendizagem, é importante você refletir sobre o que foi aprendido e como isso se aplica ao desenvolvimento profissional. Como entender os fundamentos de redes de computadores, que impactam diretamente a eficiência e segurança das operações empresariais? Que papel você, como futuro profissional, pode desempenhar na inovação e melhoria contínua dessas redes? Refletir sobre essas questões não só reforça o conhecimento adquirido, mas também ajuda a definir um propósito e direção na sua carreira. A compreensão das redes de computadores não é apenas um requisito técnico, mas uma chave para a construção de um futuro mais conectado e eficiente.

**PLAY NO CONHECIMENTO**

Você está curioso sobre o que faz um profissional de redes de computadores? Quer saber mais sobre os desafios e as oportunidades dessa carreira em constante evolução? Então, não perca o nosso podcast! Exploraremos o papel essencial desses especialistas na manutenção e segurança das infraestruturas digitais que suportam nossa sociedade. Inicie agora sua jornada rumo ao sucesso profissional nas redes de computadores! **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

VAMOS RECORDAR?

Para garantir que você, estudante, tenha uma compreensão sólida dos conceitos fundamentais antes de se aprofundar nos detalhes das redes de computadores, é essencial resgatar alguns conteúdos-base e prévios ao assunto. Um artigo da Amazon que introduz os fundamentos das redes, incluindo os principais tipos de redes (LAN, WAN, MAN) e os componentes utilizados. <https://cutt.ly/7eFB614l>

DESENVOLVA SEU POTENCIAL

INTRODUÇÃO AOS FUNDAMENTOS DE REDES DE COMPUTADORES

Redes de computadores são fundamentais para a comunicação moderna, permitindo a troca de dados entre dispositivos como computadores, servidores, smartphones e outros equipamentos conectados.

Segundo Tanenbaum e Wetherall (2011, p. 6), “as redes de computadores são a espinha dorsal da infraestrutura de TI de qualquer organização”. Uma rede de computadores é um conjunto de dispositivos interconectados que compartilham recursos e dados. As redes variam em tamanho e complexidade, desde redes locais em um escritório até a vasta rede global conhecida como Internet.

Objetivos das redes de computadores

As redes de computadores têm como principais objetivos permitir o compartilhamento de recursos, como arquivos e impressoras, aumentar a confiabilidade por meio de redundância, facilitar a comunicação e colaboração entre usuários, e garantir acessibilidade e mobilidade ao prover acesso remoto a recursos e informações.

- **Compartilhamento de Recursos:** permitir que dispositivos compartilhem recursos como impressoras, arquivos e internet.
- **Confiabilidade e Redundância:** aumentar a confiabilidade dos sistemas por meio de redundância.
- **Comunicação e Colaboração:** facilitar a comunicação entre usuários por meio de e-mails, mensagens instantâneas e videoconferências.
- **Acessibilidade e Mobilidade:** prover acesso remoto a recursos e informações.

Evolução das redes de computadores

A evolução das redes de computadores pode ser dividida em várias fases, cada uma marcada por inovações tecnológicas e mudanças no uso.

ANOS 1960: INÍCIO

A origem das redes de computadores está nas necessidades militares e acadêmicas. A Arpanet (*Advanced Research Projects Agency Network*), precursora da Internet, foi desenvolvida nos EUA pela Arpa (*Advanced Research Projects Agency*) como um projeto para criar uma rede descentralizada de comunicação que pudesse sobreviver a falhas parciais.

ANOS 1970: EXPANSÃO E PADRONIZAÇÃO

Durante os anos 1970, o conceito de protocolos de rede começou a tomar forma. O desenvolvimento do TCP/IP (*Transmission Control Protocol/Internet Protocol*) foi um marco importante, permitindo a comunicação entre redes heterogêneas.

ANOS 1980: COMERCIALIZAÇÃO

Os anos 1980 presenciam o início da comercialização das redes de computadores. As *LANs* (*Local Area Networks*) começaram a ser amplamente utilizadas em empresas, e o *Ethernet* se tornou o padrão predominante para redes locais.

ANOS 1990: A INTERNET

A década de 1990 foi marcada pela explosão da Internet. O desenvolvimento da *World Wide Web*, juntamente com navegadores web como o *Mosaic* e o *Netscape*, tornou a Internet acessível ao público em geral, revolucionando a comunicação e o acesso à informação.

ANOS 2000: REDES SEM FIO E MOBILIDADE

A introdução das redes sem fio (Wi-Fi) e o aumento da popularidade dos dispositivos móveis transformaram a forma como as pessoas acessam e utilizam redes de computadores. A mobilidade e a conectividade contínua se tornaram características essenciais.

ANOS 2010 E ALÉM: IOT, 5G E COMPUTAÇÃO EM NUVEM

As redes de computadores continuaram a evoluir com a introdução da Internet das Coisas (IoT), que conecta uma variedade de dispositivos à Internet, e a implantação de redes 5G, oferecendo velocidades mais altas e menor latência. A computação em nuvem também se tornou um componente crucial, permitindo o armazenamento e processamento de dados em data centers remotos.



EU INDICO

Para explorarmos e nos aprofundarmos sobre o que é redes de computadores e como ela funciona, acompanhe o artigo O que são redes de computadores? Acesse em: <https://aws.amazon.com/pt/what-is/computer-networking/>

As redes de computadores desempenham um papel fundamental na engenharia de software. Elas não só facilitam a colaboração entre desenvolvedores distribuídos geograficamente, mas também suportam a implementação e a operação de aplicativos distribuídos e serviços baseados na nuvem.

- **Desenvolvimento Colaborativo:** ferramentas de controle de versão como *Git*, serviços de hospedagem de repositórios como *GitHub* e plataformas de integração contínua permitem que equipes de desenvolvimento colaborem de maneira eficiente, independentemente de sua localização geográfica.
- **Aplicativos Distribuídos:** aplicativos modernos, muitas vezes, são distribuídos com componentes rodando em diferentes servidores e se comunicando por meio da rede. Microsserviços, por exemplo, são arquiteturas em que serviços independentes se comunicam via APIs de rede.
- **Serviços em Nuvem:** a computação em nuvem permite que desenvolvedores hospedem e escalem seus aplicativos sem a necessidade de gerenciar infraestrutura física. Serviços como AWS, Google Cloud e Azure oferecem uma ampla gama de serviços de rede que facilitam o desenvolvimento e a implantação de software.

- **Arquitetura de Rede e Componentes:** a arquitetura de rede se refere ao layout lógico e físico dos componentes de rede e sua interconexão. A arquitetura pode variar dependendo do tamanho e do propósito da rede.
- **Topologias de Rede:** as topologias de rede descrevem a disposição dos dispositivos e a forma como eles estão interconectados em uma rede de computadores. Cada topologia possui características distintas que influenciam o desempenho, a escalabilidade e a manutenção da rede.

A seguir, algumas das principais topologias:

TOPOLOGIA EM ESTRELA

Pense que todos os dispositivos, como computadores e impressoras, estão conectados a um ponto central, tipo um Switch ou roteador. Esse ponto central gerencia todo o tráfego de dados, como se fosse uma 'central de comando'. Se o ponto central falhar, toda a rede para de funcionar.

TOPOLOGIA EM ANEL

Cada dispositivo está ligado a dois outros, formando um círculo ou anel. Os dados passam de um dispositivo para o outro até chegar ao destino, como se estivessem dando voltas nesse anel. Se um dispositivo falhar, toda a rede pode ser afetada, mas existe a possibilidade de usar uma conexão de backup para evitar isso.

TOPOLOGIA EM BARRAMENTO

Todos os dispositivos compartilham o mesmo caminho de comunicação, como se estivessem todos ouvindo a mesma conversa em uma única sala. Cada dispositivo se conecta a esse barramento e pode enviar ou receber dados através dele. Se o cabo principal do barramento falhar, a rede toda para de funcionar.

TOPOLOGIA EM MALHA

Imagine uma rede em que cada dispositivo está ligado a vários outros. Isso cria múltiplos caminhos para os dados, tornando a rede muito robusta. Se um caminho falhar, os dados podem pegar outro caminho. É mais complexa e cara, mas oferece alta confiabilidade.

Cada topologia tem suas próprias vantagens e desvantagens, e a escolha da topologia adequada depende das necessidades específicas da rede, como o tamanho, o orçamento, a importância da redundância e a facilidade de manutenção.



Componentes de rede

Os componentes de rede são os dispositivos e equipamentos essenciais que permitem a comunicação e o compartilhamento de recursos entre dispositivos em uma rede de computadores.

Cada componente desempenha um papel específico na construção, operação e gerenciamento da rede. Aqui estão os principais componentes de rede: roteador (router), *Switch*, *hub*, modem, *Access Point* (ponto de acesso), *Firewall*, repetidor, *bridge* (ponte), *Gateway*, cabo de rede e *NIC* (*network interface card*).

- **Roteador (Router):** Pense nele como um diretor de tráfego que conecta redes diferentes e direciona os pacotes de dados entre elas. Imagine que ele ajuda a sua rede local (aquele que você tem em casa) a se conectar com a Internet, muitos roteadores oferecem extras como *Firewall* e VPN para proteger e melhorar sua conexão.
- **Switch:** o *Switch* é como um organizador dentro da sua rede local. Ele conecta vários dispositivos, como computadores e impressoras, e se certifica de que os dados vão diretamente para o dispositivo correto, sem

causar colisões. Isso significa que ele melhora a eficiência da sua rede, garantindo que todos possam trabalhar mais rápido.

- **Hub:** chegamos no *hub*, ele é um pouco mais simples, também pode conectar vários dispositivos em uma rede local, mas, ao contrário do *Switch*, envia os dados para todos os dispositivos conectados, mesmo que só um deles precise dessa informação. Isso pode gerar um pouco de confusão e tornar a rede menos eficiente.
- **Modem:** o modem é um dispositivo fundamental para conectar sua rede local à Internet. Ele transforma os sinais digitais do seu computador em sinais analógicos que podem ser transmitidos através de linhas telefônicas ou cabos, e vice-versa. Sem ele, a sua rede não teria como acessar a Internet.
- **Access Point (Ponto de Acesso):** ao se tratar de redes sem fio, o *Access Point* (ou ponto de acesso) permite que dispositivos como laptops e smartphones se conectem à sua rede local via Wi-Fi. Ele expande a cobertura da sua rede sem fio, tornando possível o acesso em mais áreas da sua casa ou escritório.
- **Firewall:** tratando-se de segurança, o *Firewall* é essencial. Ele é como um guarda que monitora e controla o tráfego de dados que entra e sai da sua rede, protegendo-a contra invasões e ataques cibernéticos.
- **Repetidor:** se você está enfrentando problemas de sinal em partes da sua casa, um repetidor pode ajudar. Ele pega o sinal de dados e o amplifica, estendendo o alcance da rede para áreas mais distantes ou onde o sinal está fraco.
- **Bridge (Ponte):** uma *bridge* (ou ponte) é usada para conectar duas redes ou segmentos de rede, permitindo que funcionem como uma única rede integrada. Isso ajuda a melhorar o desempenho da rede ao filtrar o tráfego e reduzir colisões.
- **Gateway:** Já o *Gateway* atua como um tradutor entre redes que utilizam protocolos diferentes. Ele é o ponto de entrada ou saída para dados que precisam ser convertidos para se comunicarem com outras redes.

- **Cabo de Rede:** os cabos de rede são as vias por onde os dados viajam dentro da rede. Eles vêm em diferentes tipos, como cabos *Ethernet*, fibra óptica e coaxiais, cada um com suas próprias características e usos específicos.
- **NIC (*Network Interface Card*):** chegamos à placa que conecta o seu computador à rede, seja através de um cabo ou de Wi-Fi. Sem ela, seu computador não conseguiria se comunicar com outros dispositivos na rede.

Cada um desses componentes desempenha um papel crucial na construção e manutenção de redes de computadores, garantindo que os dados sejam transmitidos de forma eficiente, segura e confiável entre os dispositivos.

CLASSIFICAÇÃO DE REDES DE COMPUTADORES

As redes de computadores podem ser classificadas com base na sua escala e área geográfica coberta.

LAN (*Local Area Network*)

LAN ou Rede de Área Local, refere-se a uma rede que cobre uma área geográfica limitada, como uma casa, escritório, escola ou edifício. Essas redes são geralmente pequenas em escala, confinadas a uma única localização, e conectam dispositivos como computadores, impressoras, roteadores e *Switches*.

As LANs utilizam várias **tecnologias** para transmitir dados. As duas mais comuns são *Ethernet* e Wi-Fi:

- **Ethernet:** utiliza cabos físicos para conectar dispositivos, proporcionando alta velocidade de transmissão de dados e confiabilidade. É frequentemente usada em ambientes empresariais, para os quais a estabilidade e a velocidade são cruciais.
- **Wi-Fi:** permite conexões sem fio entre dispositivos, oferecendo flexibilidade e mobilidade. É amplamente usada em residências, escritórios e espaços públicos.

As LANs têm suas **vantagens** tais como:

ALTA VELOCIDADE

As LANs podem oferecer altas taxas de transferência de dados, normalmente na faixa de gigabits por segundo (Gbps).

BAIXO CUSTO

A configuração e a manutenção de uma LAN são geralmente mais baratas comparadas a redes que cobrem áreas maiores.

FÁCIL MANUTENÇÃO

Devido ao seu alcance limitado e ao uso de tecnologias padronizadas, as LANs são mais fáceis de configurar, gerenciar e solucionar problemas.

MAN (*Metropolitan Area Network*)

MAN, ou Rede de Área Metropolitana, cobre uma área geográfica maior que uma LAN, mas menor que uma WAN. Geralmente, uma MAN abrange uma cidade, campus universitário ou uma grande área metropolitana, conectando várias LANs dentro dessa área.

As MANs utilizam **tecnologias** que podem cobrir distâncias maiores e conectar diferentes locais dentro de uma cidade ou área metropolitana.

- **Ethernet Metropolitana:** uma extensão da tecnologia *Ethernet* usada em LANs, adaptada para distâncias maiores. É comum em ambientes urbanos conectar diferentes edifícios ou instalações.
- **WiMAX (*Worldwide Interoperability for Microwave Access*):** uma tecnologia sem fio que oferece acesso de banda larga a longas distâncias. É usada para fornecer conectividade em áreas metropolitanas e rurais onde a instalação de cabos não é viável.

As MANs tem suas **vantagens** tais como:

- **Cobertura Ampla:** capaz de conectar várias LANs dentro de uma grande área geográfica, proporcionando comunicação eficiente entre locais dispersos.
- **Alta Capacidade:** pode suportar muitos dispositivos e tráfego de dados intensivo, sendo ideal para grandes organizações e instituições.
- **Flexibilidade:** permite a interconexão de redes diferentes ao usar várias tecnologias e infraestruturas.

WAN (*Wide Area Network*)

WAN, ou Rede de Área Ampla, cobre grandes áreas geográficas, como cidades, países ou até continentes. É usada para conectar várias LANs e MANs, permitindo que dispositivos em locais distantes se comuniquem.



A Internet é o exemplo mais conhecido de uma WAN. Outras WANs incluem redes corporativas que conectam várias filiais em diferentes partes do mundo. WANs utilizam diversas **tecnologias** avançadas para transmitir dados a longas distâncias:

- **MPLS (Multiprotocol Label Switching)**: uma técnica de roteamento eficiente que encaminha dados usando rótulos. É usada para criar conexões privadas de alta velocidade entre diferentes locais.
- **Frame Relay**: uma tecnologia de transmissão de dados que facilita a comunicação entre redes locais em diferentes locais geográficos, utilizando uma rede de comutação de pacotes.
- **ATM (Asynchronous Transfer Mode)**: uma tecnologia que transmite dados em células de tamanho fixo, ideal para suportar voz, vídeo e dados em uma rede de alta velocidade.

As WANs tem suas **vantagens** tais como:

CONECTIVIDADE GLOBAL

Permite a interconexão de redes em diferentes partes do mundo, facilitando a comunicação e a colaboração global.

ESCALABILIDADE

Pode acomodar muitos dispositivos e um volume substancial de tráfego de dados.

RESILIÊNCIA

WANs são projetadas para serem robustas e confiáveis, com várias camadas de redundância para garantir a continuidade dos serviços.

Os diferentes tipos de redes de computadores, LAN, MAN e WAN, atendem a diferentes necessidades de conectividade, desde a comunicação em pequenos ambientes locais até a interconexão de redes em escala global. Compreender as características, tecnologias e vantagens de cada tipo de rede é crucial para o planejamento e implementação eficaz de infraestruturas de rede que atendam às demandas específicas de diferentes organizações e ambientes.

TENDÊNCIAS EMERGENTES

As redes de computadores continuam a evoluir com novas tecnologias que prometem transformar a conectividade e o processamento de dados. A transição para tecnologias emergentes, como 6G, *Edge Computing* e *Quantum Networking*, transformará a forma como os dados são processados e transmitidos.



EU INDICO

Ao analisarmos as inovações tecnológicas, é fundamental considerar sua estruturação no mercado, mas também podemos imaginar seu impacto para os profissionais de TI? Acompanhe o artigo a seguir para refletirmos sobre você, futuro profissional. <https://www.profissionaisti.com.br/inovacoes-tecnologicas-e-seu-impacto-para-profissionais-de-ti/>

Agora vamos explorar três tecnologias emergentes, o 6G que promete revolucionar a conectividade móvel, *Edge Computing* melhorando a eficiência no processamento de dados e *Quantum Networking* para uma infraestrutura de comunicação global mais segura e eficiente.

6G - O que é?

O **6G** (sexta geração de tecnologia de redes móveis) é a próxima etapa na evolução das redes celulares, projetada para suceder o 5G. Embora ainda esteja em fase de pesquisa e desenvolvimento, o 6G promete trazer avanços significativos em termos de velocidade, conectividade, latência e novas aplicações que poderão transformar diversas indústrias.

Acompanhe, a seguir, algumas das características do 6G que incluem velocidades de dados extremamente rápidas, densidade dos dispositivos conectados para suportar a Internet das Coisas (IoT). Conheça as **principais características do 6G**:

- **Velocidades de Dados Ultrarrápidas**

- O 6G está sendo projetado para oferecer velocidades de transmissão de dados de até 100 vezes maiores do que o 5G. Isso significa que as velocidades podem atingir até 1 Tbps (terabit por segundo) em condições ideais.
- Com essa capacidade, será possível baixar filmes em alta definição ou grandes volumes de dados em segundos.

- **Latência Ultra Baixa**

- A latência no 6G deverá ser extremamente baixa, na ordem de microssegundos (μ s), em comparação com milissegundos (ms) no 5G. Isso é crucial para aplicações que exigem respostas em tempo real, como veículos autônomos, cirurgias robóticas e jogos imersivos.

- **Conectividade**

- O 6G permitirá a conexão de uma quantidade massiva de dispositivos simultaneamente, suportando de maneira eficiente a Internet das Coisas (IoT) em larga escala.
- A conectividade se estenderá a áreas remotas, ambientes subterrâneos e até mesmo ambientes espaciais, criando uma rede verdadeiramente global.

- **Inteligência Artificial (IA) Integrada**

- A rede 6G será altamente inteligente, utilizando IA e *machine learning* para otimizar a alocação de recursos, melhorar a qualidade do serviço e prever falhas de rede antes que ocorram.
- A IA também permitirá a criação de redes autônomas que podem se auto-organizar e ajustar automaticamente sua configuração com base nas condições da rede.

- **Convergência de Redes**

- O 6G poderá integrar diferentes tipos de redes, incluindo redes móveis, Wi-Fi, satélites e até redes ópticas, proporcionando uma experiência de conectividade contínua.
- Isso significa que os dispositivos poderão alternar entre diferentes tipos de conexão sem interrupções.

Os **benefícios do 6G** incluem velocidades de conexão muito mais rápidas, permitindo transferências de dados quase instantâneas e suporte a aplicações avançadas como realidade aumentada e virtual imersivas.

■ Experiências Imersivas

- O 6G vai possibilitar novas formas de interação com a realidade aumentada (AR), realidade virtual (VR) e realidade estendida (XR), permitindo experiências mais imersivas e interativas.
- A comunicação holográfica, em que os usuários podem ver e interagir com hologramas de pessoas em tempo real, se tornará uma realidade.

■ Comunicação Instantânea e de Alta Fidelidade

- Aplicações como telepresença, em que indivíduos podem sentir como se estivessem presentes em um local distante, se tornarão muito mais realistas e envolventes, graças à alta velocidade e baixa latência do 6G.

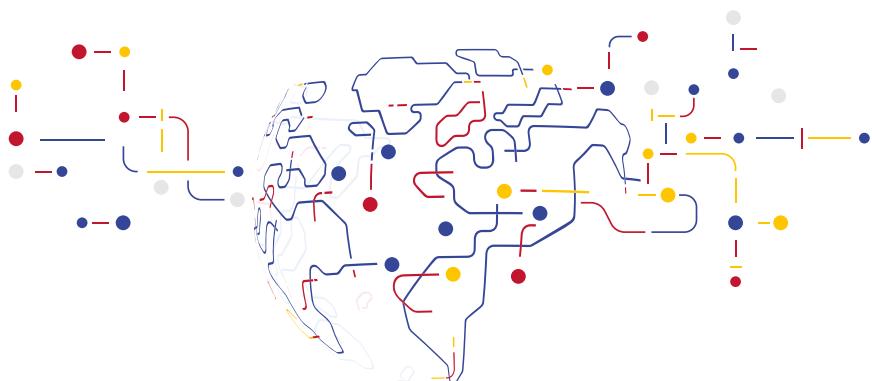
■ IoT Massivo

- Com a capacidade de suportar trilhões de dispositivos conectados, o 6G será o alicerce para cidades inteligentes, fábricas automatizadas e agricultura de precisão.
- Sensores e dispositivos IoT poderão operar com uma eficiência muito maior, coletando e transmitindo dados em tempo real.

■ Sustentabilidade

- O 6G está sendo projetado com a sustentabilidade em mente. Redes mais eficientes energeticamente, combinadas com dispositivos mais inteligentes, ajudarão a reduzir o consumo de energia e a pegada de carbono das operações de rede.

Os **desafios do 6G** incluem a necessidade de desenvolver novas infraestruturas para suportar as altíssimas frequências usadas, que exigem mais antenas e maior densidade de redes.



INFRAESTRUTURA E CUSTOS

A implantação do 6G exigirá uma infraestrutura completamente nova, o que representa um desafio técnico e financeiro significativo. Novas antenas, torres e tecnologias de *backend* precisarão ser desenvolvidas e instaladas.

REGULAMENTAÇÃO E PADRONIZAÇÃO

Antes que o 6G possa ser amplamente adotado, será necessário que os órgãos reguladores em todo o mundo estabeleçam padrões globais para a tecnologia. A harmonização das frequências e a regulamentação do espectro são questões críticas.

SEGURANÇA E PRIVACIDADE

À medida que o 6G se expande para novos tipos de aplicações e dispositivos, a segurança e a privacidade dos dados se tornam uma preocupação maior. Tecnologias robustas de criptografia e protocolos de segurança serão essenciais para proteger a rede contra ameaças cibernéticas.

DESENVOLVIMENTO TECNOLÓGICO

A tecnologia para suportar 6G, como semicondutores mais avançados e novas formas de comunicação de rádio, ainda está em desenvolvimento. O sucesso do 6G depende de avanços significativos nessas áreas.

Conheceremos, agora, um pouco mais as aplicações futuras do 6G:

- **Cidades Inteligentes e Sustentáveis:** o 6G permitirá a criação de cidades verdadeiramente inteligentes, em que sistemas de transporte, energia, saúde e segurança serão interconectados e gerenciados em tempo real para maximizar a eficiência e a sustentabilidade.
- **Saúde Remota e Cirurgia Robótica:** a combinação de alta velocidade e latência ultrabaixa permitirá que os médicos realizem cirurgias remotamente com precisão extrema, abrindo novas possibilidades para a telemedicina.

- **Exploração Espacial e Comunicação Interplanetária:** com a expansão da exploração espacial, o 6G pode fornecer a infraestrutura necessária para a comunicação de alta velocidade entre a Terra e as missões espaciais ou até mesmo entre planetas.
- **Indústria 4.0 e Automação:** fábricas automatizadas se beneficiarão da capacidade do 6G de conectar e coordenar máquinas, robôs e sistemas de forma eficiente e em tempo real, promovendo um aumento significativo na produtividade.

O que é *Edge Computing*?

É uma arquitetura de TI distribuída que traz o poder de processamento e armazenamento de dados para mais perto dos dispositivos e fontes de dados. Em vez de enviar todos os dados para um data center centralizado ou para a nuvem para serem processados, o *Edge Computing* permite que os dados sejam processados mais próximos do local onde são gerados.

Como funciona o *Edge Computing*? No *Edge Computing*, dispositivos como sensores, câmeras, ou qualquer dispositivo IoT (Internet das Coisas), coletam dados e os processam em servidores locais ou dispositivos chamados ‘*Edge Nodes*’. Esses dispositivos realizam parte do processamento necessário antes de enviar os dados relevantes para um data center centralizado ou para a nuvem. Isso reduz a quantidade de dados que precisa ser enviada, diminuindo o tempo de resposta e a largura de banda necessária.

Conheça as vantagens do *Edge Computing*:

- **Redução da Latência:** ao processar dados mais próximos da fonte, o *Edge Computing* diminui a latência, ou seja, o tempo que leva para os dados percorrerem entre o dispositivo e o servidor. Isso é crucial para aplicações que exigem respostas em tempo real, como veículos autônomos ou cirurgias robóticas.
- **Economia de Largura de Banda:** ao processar e filtrar dados localmente, menos informações precisam ser enviadas pela rede, economizando largura de banda. Isso é especialmente importante em ambientes em que a largura de banda é limitada ou cara.
- **Melhor Resiliência e Segurança:** como parte dos dados são processados localmente, a rede pode continuar funcionando mesmo que a co-

nexão com a nuvem seja interrompida. Além disso, ao processar dados sensíveis localmente, a segurança é aumentada, pois menos dados são transmitidos pela rede.

Agora, os desafios do *Edge Computing*:

- **Gerenciamento e Manutenção:** com a descentralização do processamento, o gerenciamento de dispositivos e sistemas no *Edge* pode ser mais complexo. É necessário monitorar, atualizar e manter uma maior quantidade de dispositivos distribuídos.
- **Segurança:** embora a segurança seja uma vantagem, também é um desafio. Dispositivos no *Edge* são mais vulneráveis a ataques físicos e cibernéticos, e a proteção desses dispositivos é crítica.
- **Interoperabilidade:** a variedade de dispositivos e tecnologias envolvidas no *Edge Computing* pode criar problemas de compatibilidade e interoperabilidade, especialmente em ambientes complexos.

E para encerrar o assunto *Edge Computing*, aqui estão algumas aplicações:

- **Veículos Autônomos:** carros autônomos precisam processar grandes quantidades de dados em tempo real para tomar decisões instantâneas. *Edge Computing* permite que o processamento aconteça no veículo, reduzindo a latência e melhorando a segurança.
- **Cidades Inteligentes:** em cidades inteligentes, sensores e câmeras espalhados por toda a cidade coletam dados para otimizar o tráfego, monitorar a qualidade do ar e gerenciar a iluminação pública. O *Edge Computing* permite que esses dados sejam processados localmente, melhorando a eficiência.
- **IoT Industrial:** em fábricas e instalações industriais, o *Edge Computing* é usado para monitorar e controlar equipamentos em tempo real, detectando falhas e otimizando processos sem a necessidade de enviar dados para a nuvem.
- **Realidade Aumentada e Virtual:** aplicações de AR e VR exigem processamento de dados extremamente rápido para fornecer experiências imersivas e interativas. O *Edge Computing* ajuda a reduzir a latência e melhorar a qualidade dessas experiências.



Quantum Networking

Quantum Networking é uma área emergente da tecnologia que se baseia nos princípios da mecânica quântica para transmitir e processar informações de maneiras que vão além das capacidades das redes clássicas. Ela representa um avanço significativo em relação às redes tradicionais, com potencial para revolucionar campos como criptografia, computação distribuída e comunicações ultrasseguras.

Conheça os **fundamentos** da *Quantum Networking*:

- ***Qubits e Informação Quântica:*** em redes quânticas, a unidade básica de informação é o *qubit* (bit quântico), que, ao contrário de um bit clássico, pode existir em uma superposição de estados (0 e 1 ao mesmo tempo). Isso permite que as redes quânticas processem informações de maneira mais eficiente do que as redes tradicionais.
- ***Entanglement (Emaranhamento Quântico):*** um dos fenômenos fundamentais explorados em redes quânticas é o emaranhamento quântico, em que dois ou mais *qubits* se tornam correlacionados de tal forma que o estado de um *qubit* está intrinsecamente ligado ao estado do outro,

independentemente da distância entre eles. Essa propriedade é crucial para a comunicação quântica, pois permite o teletransporte quântico de estados de *qubits* e é essencial para protocolos de criptografia quântica, como a distribuição de chaves quânticas (QKD).

- **Quantum Key Distribution (QKD):** a QKD é uma aplicação prática de redes quânticas, que utiliza os princípios da mecânica quântica para criar um sistema de comunicação extremamente seguro. Qualquer tentativa de interceptar a chave quântica altera o estado quântico da informação, alertando as partes envolvidas sobre a tentativa de espionagem. Isso torna a QKD uma ferramenta poderosa para proteger dados sensíveis.
- **Quantum Repeaters:** um dos desafios na construção de redes quânticas de longa distância é a atenuação e a perda de sinal. Para superar isso, os repetidores quânticos são desenvolvidos para estender a distância de comunicação. Eles funcionam armazenando e retransmitindo *qubits*, utilizando *entanglement* para preservar a informação quântica ao longo da rede.
- **Quantum Internet:** a visão de uma ‘*Quantum Internet*’ é uma rede global de comunicação que conecta dispositivos quânticos (como computadores quânticos) por meio de canais quânticos seguros. Esse conceito ainda está em desenvolvimento, mas tem o potencial de transformar a maneira como informações sensíveis são transmitidas e como os computadores quânticos trabalham em conjunto.

Aqui estão algumas possibilidades de aplicações:

- **Criptografia Inquebrável:** as redes quânticas podem oferecer segurança sem precedentes por meio de criptografia quântica, protegendo comunicações contra ataques cibernéticos, incluindo aqueles que utilizam computadores quânticos.
- **Computação Distribuída:** em uma rede quântica, diferentes computadores quânticos poderiam trabalhar em conjunto para resolver problemas complexos de maneira colaborativa, compartilhando estados quânticos e processando dados em paralelo de formas que seriam impossíveis para computadores clássicos.
- **Metrologia e Sensoriamento Quântico:** redes quânticas poderiam melhorar a precisão de sistemas de sensoriamento e medição, como relógios atômicos distribuídos ou interferômetros quânticos, permitindo medições extremamente precisas em grande escala.

Saiba quais **os desafios e o futuro** da *Quantum Networking*: o desenvolvimento de redes quânticas ainda enfrenta **desafios significativos**, como a manutenção do *entanglement* em longas distâncias, a minimização de erros de transmissão quântica e a construção de infraestrutura física para suportar essas redes. Contudo, os progressos em tecnologias de repetidores quânticos, detecção de *fotons* únicos e controle preciso de *qubits* indicam que esses desafios podem ser superados nos próximos anos.

As redes de computadores são fundamentais para a sociedade moderna contemporânea facilitando assim a comunicação, o compartilhamento de recursos e a execução de aplicativos distribuídos. Desde suas origens nos anos 1960 até as tendências emergentes de hoje, como 6G e *Edge Computing*, as redes continuam a evoluir e expandir suas capacidades, suportando uma variedade cada vez maior de aplicações e serviços.

Como Sinclair (2018, p. 18) afirma, “à medida que a internet estender seu alcance a objetos físicos e se tornar também a Internet das Coisas, não só a Internet das Pessoas, ela reconfigurará todos os setores que estiverem no percurso”.

Compreender os fundamentos das redes de computadores é essencial para qualquer profissional de tecnologia, pois essas redes são a base sobre a qual muitos outros sistemas e aplicativos são construídos.

Esse conhecimento permite projetar, implementar e manter redes de forma eficiente e segura, além de facilitar a inovação e a adaptação às novas tecnologias.

EM FOCO

Estudante, para expandir seus conhecimentos sobre o assunto abordado, assista a aula que preparamos especialmente para você. Acreditamos que essa aula complementará e aprofundará ainda mais o seu entendimento sobre o tema. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

NOVOS DESAFIOS

A compreensão dos fundamentos das redes de computadores é uma habilidade crucial que transcende a teoria e se manifesta diretamente nas demandas do mercado de trabalho contemporâneo. Ao longo desta jornada, exploramos desde a introdução e evolução das redes de computadores até a importância das redes na engenharia de software, suas arquiteturas e componentes, e as classificações e tendências emergentes. Este conhecimento não apenas fundamenta a base técnica necessária, mas também ilumina as conexões práticas que você, estudante, deve fazer para se tornar um profissional competente e inovador.

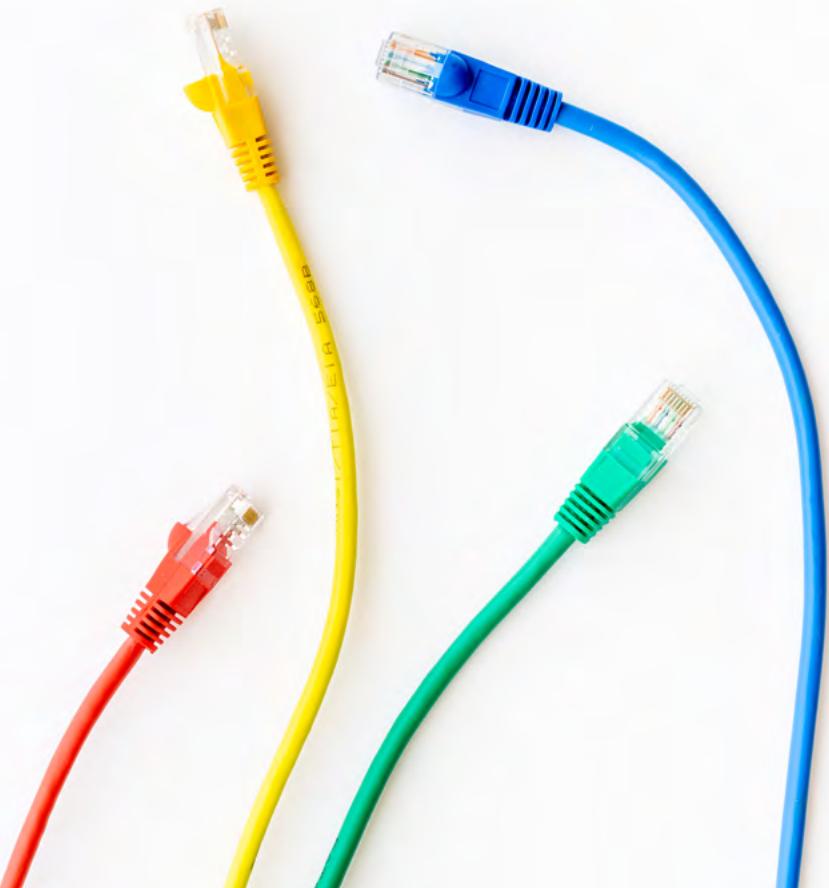
As redes de computadores formam o cerne da infraestrutura digital global. Profissionais que dominam essa área são indispensáveis em empresas de tecnologia, provedores de serviços de internet, grandes corporações e startups. No ambiente profissional, a teoria aprendida em sala de aula se traduz em habilidades práticas essenciais: configurar e manter redes LAN e WAN, implementar segurança de rede, gerenciar tráfego de dados e resolver problemas de conectividade. O conhecimento em arquiteturas de rede, como topologias de estrela e malha, bem como a familiaridade com componentes de rede como roteadores e *Switches*, prepara os estudantes para desenhar e otimizar infraestruturas de rede complexas.

As tendências emergentes, como 6G, *Edge Computing* e *Quantum Networking*, representam o futuro da conectividade. Profissionais capacitados serão aqueles que, além de entender dessas tecnologias, também podem aplicá-las para resolver problemas reais e criar soluções inovadoras. Por exemplo, a implementação de *Edge Computing* pode reduzir significativamente a latência em aplicações críticas, como em veículos autônomos e cidades inteligentes, oferecendo uma vantagem competitiva no mercado.

O mercado de trabalho valoriza profissionais que possuem conhecimento teórico e demonstram habilidade prática e adaptabilidade a novas tecnologias. A prática em ambientes de laboratório e a experiência com ferramentas de simulação e configuração de rede são vitais. Projetos práticos, estágios e certificações específicas, como as oferecidas pela Cisco e CompTIA, podem abrir portas e proporcionar uma vantagem no competitivo mercado de trabalho.

A habilidade de solucionar problemas de rede de maneira eficiente e a capacidade de inovar com novas tecnologias são altamente valorizadas no mercado de trabalho. Profissionais que conseguem integrar segurança cibernética em suas práticas de rede, garantindo a proteção de dados e a continuidade dos serviços, são especialmente procurados. A conexão entre teoria e prática no estudo das redes de computadores **prepara você, estudante, para um mercado de trabalho dinâmico e em constante evolução.**

Com uma base sólida de conhecimento e habilidades práticas, os futuros profissionais estarão prontos para enfrentar desafios, implementar soluções inovadoras e se destacar em suas carreiras. Aprofundar-se nos fundamentos e acompanhar as tendências emergentes permitirá que contribuam de maneira significativa para o avanço da tecnologia e para a construção de um mundo cada vez mais conectado e eficiente.



VAMOS PRATICAR

- Redes de computadores são essenciais para a comunicação moderna, permitindo a troca de dados entre dispositivos como computadores, servidores, smartphones e outros equipamentos conectados. Segundo Tanenbaum e Wetherall (2011), "às redes de computadores são a espinha dorsal da infraestrutura de TI de qualquer organização". Elas variam em tamanho e complexidade, desde redes locais em escritórios até a vasta rede global conhecida como Internet (Tanenbaum; Wetherall, 2011).

Com base no texto apresentado, identifique a afirmativa correta sobre os objetivos das redes de computadores:

- O objetivo de 'Compartilhamento de Recursos' refere-se a garantir que os sistemas continuem operando mesmo após a falha de um componente.
- O objetivo de 'Confiabilidade e Redundância' está relacionado a permitir que dispositivos compartilhem recursos como impressoras e arquivos.
- O objetivo de 'Comunicação e Colaboração' visa facilitar a comunicação entre usuários por meio de e-mails, mensagens instantâneas e videoconferências.

Assinale a alternativa correta:

- I, apenas.
 - III, apenas.
 - I e II, apenas.
 - II e III, apenas.
 - I, II e III.
- Uma LAN (*Local Area Network*) é uma rede que cobre uma área geográfica limitada, como uma casa, escritório, escola ou edifício, conectando dispositivos como computadores, impressoras, roteadores e *Switches*. As LANs utilizam principalmente tecnologias *Ethernet* e *Wi-Fi*. *Ethernet* utiliza cabos físicos para alta velocidade e confiabilidade, sendo comum em ambientes empresariais. *Wi-Fi* permite conexão sem fio, proporcionando flexibilidade e mobilidade, amplamente usada em residências e escritórios. As vantagens das LANs incluem alta velocidade de transferência de dados, baixo custo de configuração e manutenção, e facilidade de gerenciamento devido ao seu alcance limitado e uso de tecnologias padronizadas (Tanenbaum; Wetherall, 2011).

Com base no texto sobre LAN (*Local Area Network*), identifique a alternativa que descreve corretamente uma das principais vantagens da utilização de redes LAN.

VAMOS PRATICAR

- a) As LANs oferecem conectividade global e são ideais para redes que cobrem grandes áreas geográficas, como países e continentes.
 - b) A manutenção de uma LAN é complexa e cara devido ao uso de tecnologias especializadas e a necessidade de cobrir grandes distâncias.
 - c) As LANs utilizam tecnologias exclusivamente sem fio, como WiMAX, para fornecer flexibilidade e mobilidade em áreas metropolitanas.
 - d) Uma das principais vantagens das LANs é a alta velocidade de transmissão de dados, que pode alcançar gigabits por segundo (Gbps).
 - e) As LANs dependem exclusivamente de conexões via satélite para transmitir dados, proporcionando alta confiabilidade e baixa latência.
3. Os componentes de rede desempenham papéis cruciais na operação de redes de computadores. Entre os principais componentes estão o roteador, o *Switch* e o *hub*. Cada um desses dispositivos tem funções e características distintas que impactam a eficiência e a performance da rede (Stallings, 2013).

Com base nas informações apresentadas, avalie as asserções a seguir e a relação proposta entre elas:

I - O roteador é responsável por conectar redes diferentes e encaminhar pacotes de dados entre elas, além de poder oferecer funções adicionais como *Firewall* e *VPN*.

PORQUE

II - O *Switch* opera em uma rede local (LAN) direcionando pacotes de dados especificamente para o dispositivo de destino, o que reduz colisões e melhora a eficiência da rede em comparação com o *hub*.

A respeito dessas asserções, assinale a alternativa correta:

- a) As asserções I e II são verdadeiras, e a II é uma justificativa correta da I.
- b) As asserções I e II são verdadeiras, mas a II não é uma justificativa correta da I.
- c) A asserção I é uma proposição verdadeira e a II é uma proposição falsa.
- d) A asserção I é uma proposição falsa e a II é uma proposição verdadeira.
- e) As asserções I e II são falsas.

REFERÊNCIAS

- STALLINGS, W. **Computer networking with Internet protocols and technology.** São Paulo: Pearson, 2013.
- SINCLAIR, B. **IoT:** como usar a internet das coisas para alavancar seus negócios. Belo Horizonte: Autêntica Business, 2018.
- TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores.** 5. ed. São Paulo: Pearson Universidades, 2011.

CONFIRA SUAS RESPOSTAS

1. Alternativa B.

A afirmativa III é a correta porque descreve precisamente o objetivo de 'Comunicação e Colaboração' das redes de computadores. Esse objetivo é voltado para melhorar a interação entre os usuários, proporcionando meios eficientes de comunicação, como e-mails, mensagens instantâneas e videoconferências. As outras afirmativas estão incorretas porque: A afirmativa I descreve erroneamente o objetivo de 'Compartilhamento de Recursos', que, na verdade, é permitir que dispositivos compartilhem recursos, e não garantir a operação contínua após falhas.

A afirmativa II descreve erroneamente o objetivo de 'Confiabilidade e Redundância', que é aumentar a confiabilidade do sistema por meio de redundância, e não compartilhar recursos.

2. Alternativa D.

A alternativa d) está correta porque uma das vantagens destacadas no texto sobre LANs é a alta velocidade de transmissão de dados, com taxas que podem alcançar gigabits por segundo (Gbps). As demais alternativas não correspondem às informações fornecidas no texto. Alternativas a) e e) se referem a redes de maior escala, como WANs, enquanto as alternativas b) e c) contêm informações incorretas sobre a complexidade de manutenção e tecnologias utilizadas.

3. Alternativa A.

A asserção I é verdadeira, pois o roteador conecta diferentes redes e pode fornecer funções adicionais como *Firewall* e VPN.

A asserção II é verdadeira, pois o *Switch* efetivamente reduz colisões e melhora a eficiência da rede ao direcionar pacotes especificamente para o dispositivo de destino, em contraste com o *hub* que retransmite pacotes para todos os dispositivos. A segunda asserção justifica a primeira, demonstrando a eficiência do roteador em comparação com outros dispositivos como o *hub*.







PROTOCOLOS E COMUNICAÇÃO EM REDES

MINHAS METAS

- Compreender os conceitos básicos de protocolos de comunicação.
- Diferenciar modelos de comunicação cliente-servidor e Peer-to-Peer.
- Explicar os princípios de comutação de pacotes e comutação de circuitos.
- Aplicar conceitos de endereçamento IP e DNS.
- Analisar e comparar protocolos de transporte (TCP e UDP).
- Demonstrar conhecimento prático de protocolos de aplicação (HTTP, FTP, SMTP).
- Integrar conhecimentos para resolver problemas de redes.

INICIE SUA JORNADA

No mundo interconectado de hoje, o conhecimento sobre redes de computadores e seus protocolos de comunicação é essencial para qualquer profissional de tecnologia. Mas por que isso é tão importante?

Imagine uma empresa global que depende de uma comunicação rápida e segura entre seus escritórios espalhados pelo mundo. O que aconteceria se um simples erro de configuração de rede interrompesse a comunicação entre esses escritórios? Ou se uma falha de segurança comprometesse informações confidenciais?

Essas situações mostram a complexidade e os desafios enfrentados na gestão de redes, evidenciando a importância de dominar conceitos como endereçamento IP, comutação de pacotes e protocolos de transporte. Identificar e compreender esses problemas é o primeiro passo para solucioná-los. Compreender como as redes de comunicação funcionam não é apenas um exercício teórico, mas uma habilidade que se traduz diretamente no mundo real.



PLAY NO CONHECIMENTO

Você já ouviu falar do Modelo OSI, mas não sabe ao certo como ele funciona? No episódio desta semana, exploraremos as sete camadas que organizam a comunicação em redes de computadores. Descubra como os dados viajam da sua máquina até o destino, passando por conceitos essenciais como camadas de transporte, rede, sessão, e muito mais! Se você quer entender melhor o que acontece por trás dos bastidores quando envia uma mensagem ou acessa um site, não perca este episódio. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

A aprendizagem realmente ganha vida quando você coloca a mão na massa. Por exemplo, quando você está configurando redes ou aplicando protocolos como o TCP/IP, todos aqueles conceitos teóricos que você aprendeu começam a fazer sentido de verdade. Você começa a enxergar como tudo funciona na prática. Isso ajuda a fixar a teoria e proporciona habilidades essenciais, como identificar problemas, configurar equipamentos e encontrar soluções eficazes. Quando você pratica o que aprende, isso se transforma em algo que poderá ser utilizado no seu trabalho!

Além de praticar, é muito importante refletir sobre o que você aprendeu. Isso significa refletir sobre como as redes afetam o dia a dia de uma empresa, como aquilo que você viu na teoria se aplicou na prática e o que você fez para resolver os desafios que apareceram. Essa reflexão contribui para consolidar o aprendizado e estimula a pensar em maneiras de aprimorar suas ações. Assim, você evolui constantemente, porque sempre vai ter algo novo para aprender e melhorar.

Como a experimentação prática e a reflexão crítica podem impactar positivamente o aprendizado de redes de computadores e contribuir para o seu desenvolvimento como um profissional de redes?

VAMOS RECORDAR?

Que tal relembrarmos como a comunicação acontece na internet? Para isso, indico um artigo muito interessante abordando e explicando esse protocolo de comunicação. Acesse em: <https://rockcontent.com/br/blog/http>

DESENVOLVA SEU POTENCIAL

PROTOCOLO DE COMUNICAÇÃO: FUNDAMENTOS E APLICAÇÕES

Segundo Kurose e Ross (2021, p. 213), “os protocolos de comunicação são de extrema importância para a Internet moderna, permitindo que dispositivos em todo o mundo se conectem e compartilhem informações de maneira eficiente e segura”.

Eles definem um conjunto de regras que governam a troca de dados entre diferentes sistemas, garantindo que a comunicação seja compreendida por todos os participantes, independentemente das diferenças nos equipamentos ou plataformas utilizadas. Sem esses protocolos, a comunicação digital como a conhecemos hoje seria impossível, pois cada dispositivo falaria sua própria ‘linguagem’, sem a garantia de que os dados enviados seriam interpretados corretamente pelo destinatário.



INDICAÇÃO DE FILME

Jogo da Imitação

Esse é um filme ambientado em 1939, que retrata a vida do matemático britânico Alan Turing, interpretado por Benedict Cumberbatch, e seu papel fundamental na decodificação das mensagens nazistas durante a Segunda Guerra Mundial. Turing, então aluno da Universidade de Cambridge, é recrutado pela recém-criada agência de inteligência britânica, MI6, para trabalhar na quebra dos códigos nazistas, em especial o enigma 'Enigma', considerado impossível de ser decifrado. Ao lado de sua equipe, que inclui Joan Clarke, Turing dedica-se a analisar as mensagens cifradas e constrói uma máquina inovadora para decodificá-las. Sua conquista não só mudou o curso da guerra, como o transformou em um herói.

Refletindo sobre a história: o filme apresenta uma reflexão sobre a justiça e o legado de Turing na história da computação.



A importância dos protocolos de comunicação pode ser vista como na indicação do filme, em que Turing desenvolveu e implementou um método de comunicação que transformou para sempre a forma como nos comunicamos atualmente.

PROTOCOLOS DE COMUNICAÇÃO

Protocolos de comunicação são conjuntos de regras que permitem a transmissão de dados entre diferentes sistemas em uma rede. Eles estabelecem como os dados devem ser formatados, transmitidos, recebidos e processados. A importância dos protocolos de comunicação reside na padronização que eles proporcionam, garantindo que diferentes dispositivos possam se comunicar de forma coerente, independentemente de suas diferenças de hardware ou software (Tanenbaum; Wetherall, 2011).

Sem protocolos, cada dispositivo precisaria usar seu próprio método de comunicação, resultando em uma fragmentação que tornaria a interoperabilidade quase impossível.

Sem protocolos, cada dispositivo precisaria usar seu próprio método

Os protocolos de comunicação operam em diferentes camadas, sendo os mais conhecidos o Modelo OSI (*Open Systems Interconnection*) e o Modelo TCP/IP. O Modelo OSI divide a comunicação de rede em sete camadas: Física, Enlace de Dados, Rede, Transporte, Sessão, Apresentação e Aplicação. Cada camada tem funções específicas e se comunica apenas com a camada diretamente acima ou abaixo dela (Benedetti; Anderson, 2010).

Já o Modelo TCP/IP, que é a base da Internet, possui quatro camadas: Link, Internet, Transporte e Aplicação. Essa divisão em camadas facilita o desenvolvimento e a implementação de protocolos, permitindo que cada camada se concentre em um aspecto específico da comunicação (Kurose; Ross, 2021).

Existem vários protocolos de comunicação que desempenham funções específicas dentro de uma rede.

ZOOM NO CONHECIMENTO

O **HTTP (HyperText Transfer Protocol)**, por exemplo, é o protocolo principal usado para a transferência de páginas web. O **FTP (File Transfer Protocol)** é utilizado para a transferência de arquivos entre um cliente e um servidor. Já o **SMTP (Simple Mail Transfer Protocol)** é o protocolo padrão para o envio de e-mails na Internet. O **DNS (Domain Name System)** é responsável por traduzir nomes de domínio legíveis por humanos em endereços IP, permitindo que usuários acessem sites usando nomes fáceis de lembrar (Tanenbaum; Wetherall, 2011).

Cada um desses protocolos desempenha um papel crucial no funcionamento da Internet e de outras redes.



COMUNICAÇÃO CLIENTE-SERVIDOR E PEER-TO-PEER

O **modelo Cliente-Servidor** é um dos mais comuns em redes de computadores. Nesse modelo, o **cliente** é a entidade que solicita um serviço, enquanto o **servidor** é a entidade que fornece esse serviço.

Por exemplo, quando você acessa um site, seu navegador atua como o cliente, solicitando dados ao servidor web, que então responde com às páginas solicitadas. Esse modelo é amplamente utilizado devido à sua eficiência e escalabilidade. Ele permite uma centralização de recursos e dados, facilitando a manutenção e o gerenciamento. No entanto, uma desvantagem é que, se o servidor falhar, todos os clientes dependentes dele também serão afetados.

No **modelo Peer-to-Peer (P2P)**, todos os participantes (ou nós) na rede têm capacidades equivalentes e podem atuar tanto como clientes quanto como servidores. Um exemplo clássico desse modelo é representado pelos protocolos de compartilhamento de arquivos, como os usados em *torrents*, nele os usuários compartilham pedaços de arquivos uns com os outros sem a necessidade de um servidor central. O modelo P2P oferece maior resistência a falhas, já que a rede não depende de um único ponto de falha. No entanto, ele pode ser mais difícil de gerenciar e menos seguro, pois cada nó precisa confiar nos outros para o compartilhamento de dados.

A principal diferença entre os modelos Cliente-Servidor e *Peer-to-Peer* é a forma como os recursos são distribuídos e acessados:

ZOOM NO CONHECIMENTO

No modelo **Cliente-Servidor**, o servidor centraliza os recursos e os distribui conforme a necessidade, enquanto no modelo **Peer-to-Peer**, os recursos são distribuídos entre todos os nós. O modelo Cliente-Servidor é mais adequado para aplicações em que a centralização e o controle são cruciais, como em bancos de dados corporativos. Já o modelo **P2P** é ideal para aplicações que exigem alta disponibilidade e escalabilidade, como redes de compartilhamento de arquivos e algumas redes sociais descentralizadas (Benedetti; Anderson, 2010).

COMUTAÇÃO DE PACOTES E COMUTAÇÃO DE CIRCUITOS

A **comutação de circuitos** é uma técnica de comunicação em que um caminho dedicado é estabelecido entre duas partes antes que a comunicação real comece. Esse caminho permanece ativo durante toda a sessão de comunicação. É amplamente utilizado em redes telefônicas tradicionais, em que uma linha dedicada é reservada para a duração de uma chamada.

A principal vantagem da comutação de circuitos é a garantia de largura de banda e qualidade de serviço, uma vez que o caminho dedicado não é compartilhado com outros usuários. No entanto, é uma abordagem menos eficiente para redes modernas, em que a largura de banda disponível precisa ser utilizada de forma dinâmica e compartilhada entre muitos usuários.

Na **comutação de pacotes**, os dados são divididos em pequenos pacotes, enviados independentemente uns dos outros pela rede. Cada pacote pode seguir um caminho diferente e, ao chegar ao destino, os pacotes são reordenados para reconstruir a mensagem original. Essa técnica é a base da Internet moderna, pois permite uma utilização muito mais eficiente da largura de banda disponível, além de maior resistência a falhas na rede. A comutação de pacotes é amplamente utilizada em redes IP, nelas a flexibilidade e a eficiência são fundamentais. Uma desvantagem potencial é a possibilidade de variação na latência, já que os pacotes podem chegar ao destino em momentos diferentes.

A comutação de circuitos oferece consistência e previsibilidade, sendo ideal para aplicações em que a qualidade de serviço é crítica, como chamadas de voz de alta qualidade. No entanto, ela desperdiça recursos quando o circuito não está em uso. A comutação de pacotes, por outro lado, é altamente eficiente, utilizando os recursos de rede de maneira mais dinâmica, mas pode sofrer com a variação de latência e possíveis atrasos.

Para a maioria das aplicações de Internet, a comutação de pacotes é a escolha preferida, enquanto a comutação de circuitos ainda é utilizada em algumas aplicações especializadas (Dorsey, on-line, [20-?]).

ENDEREÇAMENTO IP, DNS, DHCP, ARP E IPV6

O **endereçamento IP** é o sistema pelo qual dispositivos em uma rede são identificados de maneira única. Cada dispositivo recebe um endereço IP que funciona como seu identificador na rede. O sistema de endereçamento IP é dividido em duas versões principais: **IPv4** e **IPv6**. O **IPv4** utiliza um formato de 32 bits, permitindo cerca de 4,3 bilhões de endereços únicos (Milaré, 2022).

No entanto, com o crescimento exponencial da Internet, esses endereços começaram a se esgotar, levando ao desenvolvimento do **IPv6**, que utiliza um formato de 128 bits, proporcionando um número quase ilimitado de endereços. A transição para o IPv6 está em andamento, mas ainda enfrenta desafios de adoção em algumas regiões e infraestruturas.

O **DNS** é um sistema crucial para a navegação na Internet, pois traduz nomes de domínio legíveis por humanos, como www.exemplo.com, em endereços IP que os computadores utilizam para identificar servidores na rede.

De acordo com Kurose e Ross (2021, p. 213), “sem o DNS, os usuários precisam memorizar longas sequências de números (endereços IP) para acessar sites”. O DNS funciona como uma espécie de ‘agenda telefônica’ da Internet, em que os nomes são mapeados para seus respectivos números. Isso facilita a usabilidade da web e melhora a eficiência da comunicação entre dispositivos.



O **DHCP** é um protocolo de rede que automatiza a atribuição de endereços IP a dispositivos em uma rede. Quando um dispositivo se conecta à rede, o DHCP atribui a ele um endereço IP disponível, garantindo que não haja conflitos de endereços na rede. Isso simplifica a gestão da rede, especialmente em grandes redes corporativas, nas quais a atribuição manual de endereços IP seria impraticável. Além de endereços IP, o DHCP também pode fornecer outras informações importantes, como a máscara de sub-rede e os servidores DNS a serem usados.

O **ARP** é um protocolo usado para mapear endereços IP para endereços MAC (*Media Access Control*), usados para identificar dispositivos na camada de enlace. Quando um dispositivo deseja comunicar-se com outro na mesma rede, ele usa o ARP para descobrir o endereço MAC correspondente ao endereço IP de destino. Esse processo é fundamental para a operação das redes Ethernet, pois permite que os dados sejam entregues ao dispositivo correto em uma rede local.

O **IPv6** foi desenvolvido para resolver os problemas de esgotamento de endereços IP que afetam o IPv4. Com um espaço de endereçamento muito maior, o IPv6, além de oferecer mais endereços, traz melhorias em termos de segurança e eficiência. Ele inclui recursos como autoconfiguração, em que dispositivos podem gerar seus próprios endereços IP sem a necessidade de um servidor DHCP, e suporte nativo a IPsec (*Internet Protocol Security*), que é um conjunto de protocolos para garantir a comunicação segura sobre uma rede IP. A transição para o IPv6 é uma necessidade crescente à medida que o número de dispositivos conectados à Internet continua a crescer.

PROTÓCOLOS DE TRANSPORTE (TCP, UDP)

O **TCP** é um protocolo de transporte confiável, orientado à conexão, que garante que os dados enviados cheguem ao destino corretamente e na ordem correta. Ele estabelece uma conexão entre o emissor e o receptor antes que a transmissão de dados ocorra e utiliza um sistema de confirmação para garantir que cada pacote foi recebido. Caso um pacote seja perdido ou corrompido, o TCP o retransmite. Devido a essas características, o TCP é ideal para aplicações nas quais a integridade dos dados é crítica, como transferência de arquivos, navegação web, e envio de e-mails.

O **UDP** é um protocolo de transporte que, ao contrário do TCP, não fornece garantias de entrega. Ele envia pacotes de dados, chamados de datagramas, sem verificar se eles chegaram ao destino. Isso torna o UDP mais rápido e eficiente, mas menos confiável. Ele é amplamente utilizado em aplicações em que a velocidade é mais importante que a confiabilidade, como em transmissões de vídeo ao vivo, jogos on-line, e VoIP (*Voice over IP*). Como o UDP não precisa estabelecer uma conexão antes de enviar dados, ele também é mais adequado para transmissões que exigem baixa latência.

A escolha entre TCP e UDP depende do tipo de aplicação e das necessidades específicas de comunicação. O TCP é preferível em situações em que a precisão dos dados é crucial, mesmo que a transmissão seja um pouco mais lenta, como em serviços de e-mail ou sites de comércio eletrônico. Por outro lado, o UDP é ideal para aplicações nas quais a velocidade é crítica e a perda ocasional de pacotes não prejudica a qualidade geral, como em streaming de mídia e jogos on-line. Cada protocolo tem seu lugar no ecossistema de rede, complementando-se em diferentes cenários.

**Cada protocolo
tem seu lugar no
ecossistema de rede**

PROTÓCOLOS DE APLICAÇÃO (HTTP, FTP, SMTP)

O **HTTP** é o protocolo fundamental para a navegação na web. Ele define como as mensagens são formatadas e transmitidas e como os servidores e navegadores devem responder aos vários comandos. Quando você acessa um site, seu navegador envia uma solicitação HTTP ao servidor web, que responde com o conteúdo solicitado. O HTTP evoluiu ao longo do tempo, com as versões **HTTP/2** e **HTTP/3** trazendo melhorias significativas em termos de eficiência e segurança, como multiplexação de conexões e suporte a TLS (*Transport Layer Security*) (Benedetti; Anderson, 2010).

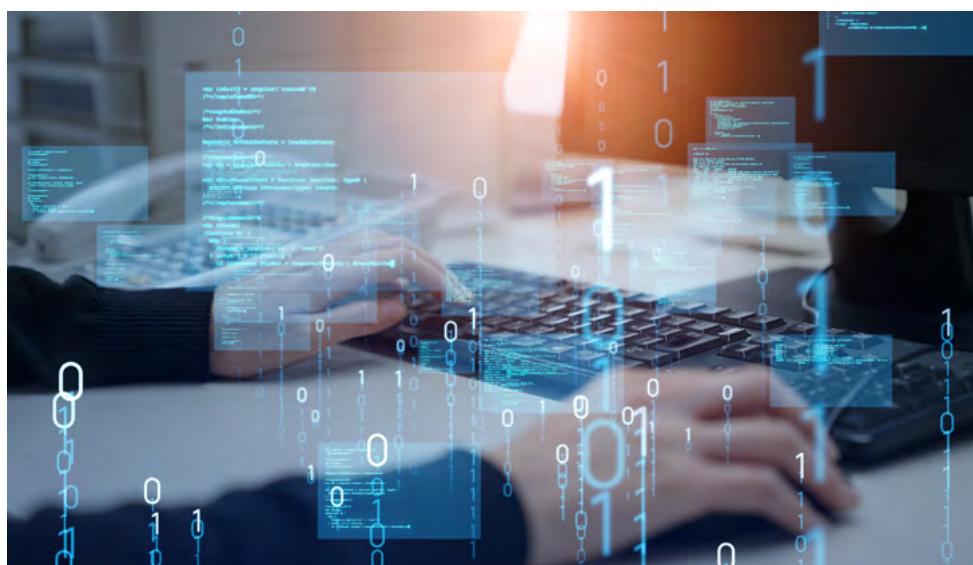
O **FTP** é um protocolo utilizado para a transferência de arquivos entre um cliente e um servidor. Ele permite que os usuários enviem e recebam arquivos, além de navegar pelos diretórios de um servidor remoto. Embora menos utilizado para o upload de sites modernos, o FTP ainda é amplamente usado em ambientes corporativos e para a transferência de grandes quantidades de dados.

No entanto, por padrão, o FTP não é seguro, pois os dados, incluindo as credenciais de login, são transmitidos em texto simples. Isso levou ao desenvolvimento de alternativas mais seguras, como o **SFTP** (*Secure File Transfer Protocol*).

O **SMTP** é o protocolo padrão para o envio de e-mails na Internet. Ele define como as mensagens de e-mail são enviadas de um cliente de e-mail para um servidor de e-mail e de um servidor para outro até que a mensagem chegue ao seu destino final. O SMTP é simples e eficiente, mas também tem limitações, como a falta de suporte nativo para transmissão segura de mensagens, o que foi abordado com o uso de criptografia por meio de **TLS** (*Transport Layer Security*). O SMTP continua sendo a base do sistema de e-mail global, apesar de outras tecnologias auxiliarem na gestão e entrega de e-mails.

Importância dos protocolos na comunicação moderna

Os **protocolos de comunicação** continuam a ser a base da conectividade moderna, garantindo que dados possam ser compartilhados de forma eficiente, segura e confiável entre dispositivos em todo o mundo. À medida que a tecnologia avança e a Internet das Coisas (IoT) e outras inovações expandem ainda mais o número de dispositivos conectados, a importância desses protocolos só tende a crescer (Sinclair, 2018).



Eles não apenas permitem a operação contínua e confiável das redes atuais, mas também facilitam a inovação, permitindo o desenvolvimento de novos serviços e aplicações que tornam a comunicação digital mais acessível e poderosa.

Esse documento abordou os principais protocolos de comunicação que sustentam a Internet e outras redes de computadores. Discutimos a importância dos protocolos na padronização e facilitação da comunicação digital, explorando em detalhes os modelos de comunicação Cliente-Servidor e *Peer-to-Peer*, os mecanismos de comutação de pacotes e circuitos, e o endereçamento IP, incluindo a transição para IPv6. Também examinamos os protocolos de transporte TCP e UDP, comparando suas características e aplicações, e revisamos os principais protocolos de aplicação, como HTTP, FTP e SMTP, que são fundamentais para a operação da Internet (Kurose; Ross, 2021).

 **EM FOCO**

Estudante, acreditamos que essa aula complementará e aprofundará ainda mais o seu entendimento sobre o tema. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

NOVOS DESAFIOS

A experimentação prática desempenha um papel fundamental no aprendizado de redes de computadores, pois permite que você, estudante, aplique protocolos como TCP/IP e enfrente problemas de conectividade em um ambiente real. Ao trabalhar diretamente com a configuração de redes e a resolução de problemas, você colocará em ação os conceitos teóricos que aprendeu, o que reforça seu entendimento e desenvolve habilidades práticas importantes, como o diagnóstico e a implementação de soluções eficazes.

A reflexão sobre essas experiências práticas é essencial para consolidar o aprendizado. Ao analisar como as redes impactam o cotidiano de uma organização e como os conceitos se aplicam em situações reais, são identificados os desafios enfrentados e as soluções que funcionaram. Essa reflexão crítica ajuda a melhorar

o conhecimento adquirido, permitindo que você, estudante, reconheça áreas de aprimoramento e estabeleça metas para seu desenvolvimento profissional contínuo. Dessa forma, a combinação de experimentação e reflexão cria um ciclo de aprendizado constante e o prepara para enfrentar desafios no mercado de trabalho.

À medida que avançamos no estudo dos protocolos de comunicação e na compreensão dos diferentes modelos de rede, fica claro que esses conhecimentos são a base para uma carreira de sucesso no campo da tecnologia da informação. A interconexão entre teoria e prática é crucial para o desenvolvimento profissional, pois o mercado de trabalho atual e futuro exige não apenas uma compreensão teórica dos conceitos, mas também a capacidade de os aplicar de forma criativa e eficaz.

No cenário atual, tecnologias como cibersegurança, computação em nuvem e Internet das Coisas (IoT) estão em constante expansão. Cada uma dessas áreas depende fortemente dos protocolos de comunicação que estudamos, como HTTP, FTP, TCP/IP, e DNS, para operar com eficiência e segurança. Profissionais que dominam esses protocolos e entendem as nuances dos diferentes modelos de comunicação, como cliente-servidor e *Peer-to-Peer*, estão mais bem equipados para lidar com os desafios dessas tecnologias emergentes.

Por exemplo, em **cibersegurança**, a compreensão detalhada dos protocolos de rede é essencial para proteger sistemas contra ameaças. Saber como um ataque pode explorar vulnerabilidades em protocolos de comunicação permite que o profissional desenvolva medidas de defesa mais robustas. Da mesma for-



ma, na computação em nuvem, a eficiência e a segurança da comunicação entre servidores e clientes são fundamentais para garantir a integridade dos dados e a qualidade dos serviços oferecidos.

A **Internet das Coisas** (IoT) que conecta dispositivos diversos em uma rede, depende de uma comunicação eficaz e segura. A familiaridade com endereçamento IP, DHCP, e a transição para IPv6 é vital para gerenciar a crescente quantidade de dispositivos conectados e garantir que eles possam se comunicar sem problemas em uma rede global.

As empresas buscam profissionais entendam os fundamentos e que possuam a habilidade de aplicar esses conhecimentos em cenários complexos e em constante evolução. O domínio dos conteúdos abordados oferece ao futuro profissional uma vantagem competitiva, permitindo que contribua significativamente para o desenvolvimento de soluções tecnológicas inovadoras. Essa capacidade de transformar teoria em prática é o que distingue um bom profissional em tecnologia da informação e é fundamental para a criação de soluções que atendam às demandas de um mercado cada vez mais digital e interconectado.

Portanto, ao dominar esses conceitos, você, estudante, se prepara para os desafios do ambiente profissional atual, se posicionando como protagonista na criação e implementação de tecnologias que moldam o futuro. A interconexão entre teoria e prática, aliada à capacidade de adaptação e inovação, será a chave para o sucesso em sua carreira e para o avanço da indústria tecnológica como um todo.



VAMOS PRATICAR

1. O modelo Cliente-Servidor e o modelo *Peer-to-Peer* (P2P) são dois paradigmas fundamentais em redes de computadores. No modelo Cliente-Servidor, há uma clara distinção entre os clientes que solicitam serviços e os servidores que os fornecem, como em servidores web. Esse modelo centraliza os recursos, facilitando o gerenciamento, mas cria um ponto único de falha. No modelo P2P, todos os participantes da rede podem atuar como clientes e servidores simultaneamente, compartilhando recursos entre si, o que aumenta a resistência a falhas, mas pode dificultar o gerenciamento e diminuir a segurança (Benedetti; Anderson, 2010).

Com base no texto, analise as seguintes afirmações sobre os modelos Cliente-Servidor e *Peer-to-Peer* (P2P):

- I - O modelo Cliente-Servidor centraliza os recursos, facilitando o gerenciamento, mas cria um ponto único de falha.
- II - O modelo P2P é mais resistente a falhas porque não depende de um único servidor central.
- III - No modelo P2P, todos nós temos a mesma capacidade e função, o que simplifica a segurança e o gerenciamento.

É correto o que se afirma em:

- a) I, apenas.
- b) III, apenas.
- c) I e II, apenas.
- d) II e III, apenas.
- e) I, II e III.

2. O Modelo OSI (*Open Systems Interconnection*) é uma referência fundamental para a comunicação em redes de computadores, dividido em sete camadas: Física, Enlace de Dados, Rede, Transporte, Sessão, Apresentação e Aplicação. Cada camada tem uma função específica, interagindo com as camadas diretamente acima e abaixo. A camada de Transporte, por exemplo, é responsável por garantir a entrega confiável de dados entre dispositivos, enquanto a camada de Rede gerencia o endereçamento e roteamento dos pacotes de dados. Esse modelo facilita a padronização e o desenvolvimento de protocolos de comunicação (Kurose; Ross, 2021).

Com base no texto, analise as seguintes afirmações sobre o Modelo OSI:

VAMOS PRATICAR

- I - A camada de Rede do Modelo OSI é responsável pelo roteamento dos pacotes de dados entre diferentes redes.
- II - A camada de Sessão é responsável por gerenciar o roteamento de pacotes de dados.
- III - A camada de Transporte lida com o endereçamento físico dos dispositivos na rede.
- IV - A camada de apresentação do Modelo OSI é responsável pelo roteamento de pacotes.

É correto o que se afirma em:

- a) I, apenas.
 - b) II e IV, apenas.
 - c) III e IV, apenas.
 - d) I, II e III, apenas.
 - e) I, II, III e IV.
3. O DNS é um sistema essencial na Internet que mapeia nomes de domínio para endereços IP, permitindo que os usuários accessem sites por meio de nomes legíveis em vez de números complexos. Além de traduzir nomes de domínio em endereços IP, o DNS também facilita a distribuição do tráfego da web, melhorando a eficiência e a velocidade da navegação. Sem o DNS, a usabilidade da Internet seria significativamente reduzida, pois os usuários precisariam memorizar longas sequências numéricas para acessar sites (Tanenbaum; Wetherall, 2011).

Com base no texto, analise as seguintes afirmações sobre o DNS:

- I - O DNS mapeia nomes de domínio para endereços IP, facilitando o acesso aos sites.
- II - O DNS é responsável por atribuir endereços IP aos dispositivos em uma rede.
- III - O DNS contribui para a eficiência da navegação na Internet ao distribuir o tráfego de maneira eficaz.
- IV - Sem o DNS, os usuários precisam memorizar sequências numéricas para acessar sites.

É correto o que se afirma em:

- a) I e IV, apenas.
- b) II e III, apenas.
- c) III e IV, apenas.
- d) I, II e III, apenas.
- e) II, III e IV, apenas.

REFERÊNCIAS

BENEDETTI, R.; ANDERSON, AL. **Use a cabeça! Redes de computadores**. Rio de Janeiro: Alta Books, 2010.

DORSEY, R. **Diferença entre comutação de circuitos e comutação de pacotes**. [20-?]. Disponível em: https://por.asayamind.com/diferenca-entre-comutacao-de-circuitos-e-comutacao-de-pacotes#goog_rewarded. Acesso em: 18 set. 2024.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet**: Uma Abordagem Top-Down. São Paulo: Pearson, 2021.

MILARÉ, L. IPv4 e IPv6: as diferenças e semelhanças entre os protocolos. **Blog hostgator**, 14 fev. 2022. Disponível em: <https://www.hostgator.com.br/blog/ipv4-ipv6-diferencias-semelhancas-protocolos/>. Acesso em: 18 set. 2024.

SINCLAIR, B. **IoT**: Como usar a internet das coisas para alavancar seus negócios. Belo Horizonte: Autêntica Business, 2018.

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores**. São Paulo: Pearson, 2011.

CONFIRA SUAS RESPOSTAS

1. Alternativa C.

A afirmação I está correta, pois o modelo Cliente-Servidor realmente centraliza os recursos, facilitando o gerenciamento, mas criando um ponto único de falha. A afirmação II está correta, pois no modelo P2P, a ausência de um servidor central aumenta a resistência a falhas. A afirmação III está incorreta porque o modelo P2P, embora resistente a falhas, não simplifica a segurança e o gerenciamento; na verdade, ele pode complicá-los.

2. Alternativa A.

A afirmação I está correta, pois a camada de Rede do Modelo OSI é, de fato, responsável pelo roteamento dos pacotes de dados entre redes. A afirmação II está incorreta, pois a camada de Sessão gerencia as conexões entre aplicativos, não o roteamento. A afirmação III está incorreta, pois o endereçamento físico é tratado pela camada de Enlace de Dados, não pela de Transporte. A afirmação IV está incorreta, pois a camada de apresentação é responsável pela tradução de dados, não pelo roteamento.

3. Alternativa A.

O DNS é responsável por mapear nomes de domínio para endereços IP (afirmação I) e, sem ele, os usuários teriam que memorizar sequências numéricas (afirmação IV). A afirmação II está incorreta, pois a atribuição de endereços IP é responsabilidade do DHCP, não do DNS. A afirmação III está parcialmente correta, mas é insuficiente sem o contexto completo, e a eficiência de navegação também depende de outros fatores além da distribuição de tráfego.



TOPOLOGIAS E MEIOS DE TRANSMISSÃO

MINHAS METAS

- Compreender as diferentes topologias de rede.
- Analisar as vantagens e desvantagens das topologias de rede.
- Identificar os tipos de meios de transmissão.
- Entender a relação entre meios de transmissão e a performance da rede.
- Refletir sobre topologia e o meio de transmissão adequados para diferentes cenários.
- Aplicar conceitos de redundância e segurança em topologias de rede.
- Interpretar diagramas e esquemas de rede.

INICIE SUA JORNADA

Estudante, neste tema de aprendizagem, discutiremos algo que está presente em quase tudo o que fazemos no mundo moderno: as redes de computadores. Você já parou para pensar em como, ao acessar a internet ou ao enviar um e-mail no trabalho, tudo isso acontece? As redes estão por trás de cada interação digital, e entender como elas operam se tornou uma habilidade essencial, especialmente para quem trabalha com TI.

Agora, imagine o seguinte: como os dados viajam do seu dispositivo até o servidor da sua empresa ou o site que você está acessando? E mais importante, como isso acontece de maneira eficiente e segura? Essas perguntas são fundamentais no estudo das topologias de rede e dos meios de transmissão.

Pense, por exemplo, em uma empresa moderna. Como garantir que a comunicação entre setores, ou até entre filiais, seja rápida e confiável? E o que acontece se houver uma falha nessa comunicação? Compreender o básico de redes, como as diferentes topologias (estrela, anel, barramento, malha) e os meios de transmissão (fibra óptica, cabos coaxiais, wireless), ajuda a prevenir problemas e a manter tudo funcionando sem interrupções.



PLAY NO CONHECIMENTO

Você já se perguntou como funcionam os mapas que organizam e conectam toda a sua rede de computadores? Vamos mergulhar no mundo dos diagramas e esquemas de redes, de maneira prática e descomplicada, como esses diagramas podem ajudar a visualizar, planejar e solucionar problemas nas redes de qualquer tamanho. Conecte-se conosco e aprenda a dominar a arte dos mapas das redes de computadores! **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

Sabe o que é interessante? Estudar redes de comunicação não é só entender um monte de conceitos técnicos complicados. É, na verdade, enxergar as ‘conexões invisíveis’ que permitem que diversos setores da economia e da vida cotidiana

operem com eficiência. Quando você explora essas topologias e tecnologias, começa a perceber como as decisões sobre a arquitetura de uma rede afetam diretamente fatores como desempenho, segurança e escalabilidade de um sistema.

Mas, claro, só estudar a teoria não é suficiente, certo? A prática é fundamental. Configurar redes reais, mexer com cabos, roteadores, *switches*, e aplicar tecnologias, como a fibra óptica, é o que transforma o seu aprendizado dos livros em habilidades práticas. Isso prepara você, estudante, para o mercado de trabalho, porque você já simulará problemas reais e implementará soluções.

Agora, pense comigo: além de colocar a mão na massa, refletir sobre o que você está fazendo também é essencial. Ao analisar como as redes funcionam no dia a dia de uma empresa e como cada conceito ajuda a resolver um problema, você consegue melhorar suas decisões. Isso cria um ciclo de aprendizado contínuo, e esse ciclo prepara-o cada vez mais para os desafios que vão aparecer no futuro.

VAMOS RECORDAR?

Estudante, é importante entender a utilização dos equipamentos para a criação de redes de computadores de maneira eficiente. Para isso, acompanhe um conteúdo excelente por meio do link a seguir. <https://www.youtube.com/watch?v=u2LeXYo7vrE>

DESENVOLVA SEU POTENCIAL

TOPOLOGIAS E MEIOS DE TRANSMISSÃO EM REDES DE COMPUTADORES

Estudante, segundo Benedetti e Anderson (2010, p. 30), “as redes de computadores são estruturas complexas que conectam dispositivos e facilitam a troca de dados”. Compreender a forma como essas redes são organizadas e os meios pelos

quais as informações são transmitidas é fundamental para qualquer profissional ou estudante da área de tecnologia da informação. Neste tema de aprendizagem, abordaremos as principais topologias de redes e os meios de transmissão utilizados, oferecendo uma visão detalhada e prática do funcionamento das redes.

Compreender as diferentes topologias de rede

As topologias de rede definem a forma como os dispositivos (nós) são interconectados. Existem várias topologias utilizadas em diferentes tipos de redes, cada uma com características únicas. Vamos conhecer!

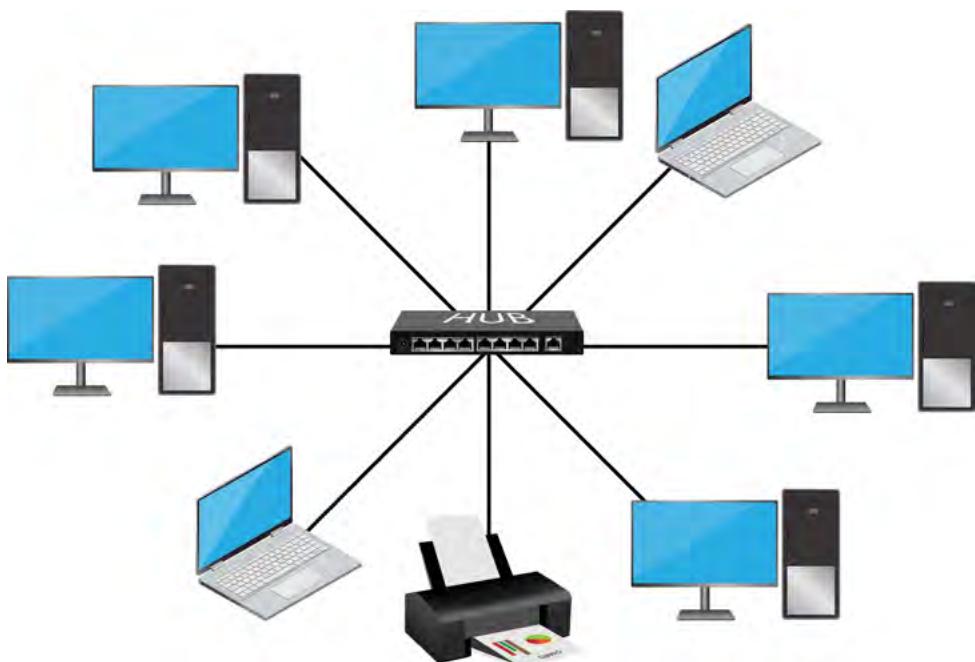


Figura 1 - Topologia Estrela

Descrição da Imagem: é uma ilustração com cinco computadores, dois notebooks e uma impressora, formando uma estrela com um em cada ponta, representando a topologia estrela. Fim da descrição.

TOPOLOGIA ESTRELA

Agora, discutiremos uma das topologias de rede mais comuns e práticas: a Topologia Estrela. Imagina o seguinte cenário: todos os dispositivos (computadores, impressoras etc.) de uma rede estão conectados a um ponto central – geralmente um *switch*, *hub* ou roteador. É como se cada dispositivo fosse um braço de uma estrela, e o ponto central fosse o núcleo. Toda a comunicação entre os dispositivos passa por esse centro, que organiza e direciona os dados para o destinatário correto.

Você já deve ter visto isso em muitos lugares, especialmente em escritórios e escolas, em que cada computador ou impressora está conectado a um único ponto central. A topologia estrela traz várias vantagens e desvantagens, vejamos algumas delas, segundo Barreto, Zanin e Saraiva (2018, on-line):

FACILIDADE DE GERENCIAMENTO

Se você precisar adicionar ou remover um dispositivo, é bem simples e não afeta o funcionamento dos outros.

ISOLAMENTO DE FALHAS

Se um cabo ou um dispositivo da rede der problema, apenas aquele pedaço da rede é afetado, enquanto o restante continua funcionando normalmente.

DEPENDÊNCIA DO PONTO CENTRAL

Se o *switch* ou roteador, que é o coração da rede, parar de funcionar, toda a rede fica inoperante.

CUSTO DE CABOS

Como cada dispositivo precisa de uma conexão direta com o ponto central, pode ser necessário usar bastante cabo, especialmente em ambientes maiores.

Escritórios e escolas frequentemente utilizam redes em estrela, em que vários computadores e impressoras estão conectados a um único *switch*, que organiza a comunicação. Perceba, estudante, fiz a construção da simulação da Topologia Estrela enquanto discorríamos sobre topologia.

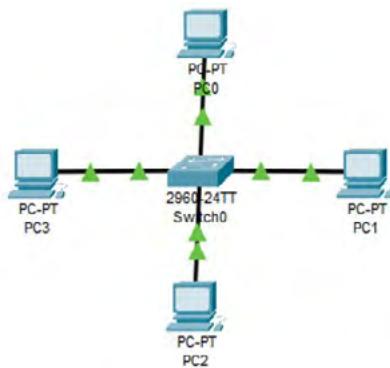


Figura 2 - Topologia Estrela

Descrição da Imagem: a figura apresenta a construção da topologia estrela, com quatro computadores conectados a um switch central. Fim da descrição.

Para exemplificar, veja mais uma imagem com a tela do *Cisco Packet Tracer*.

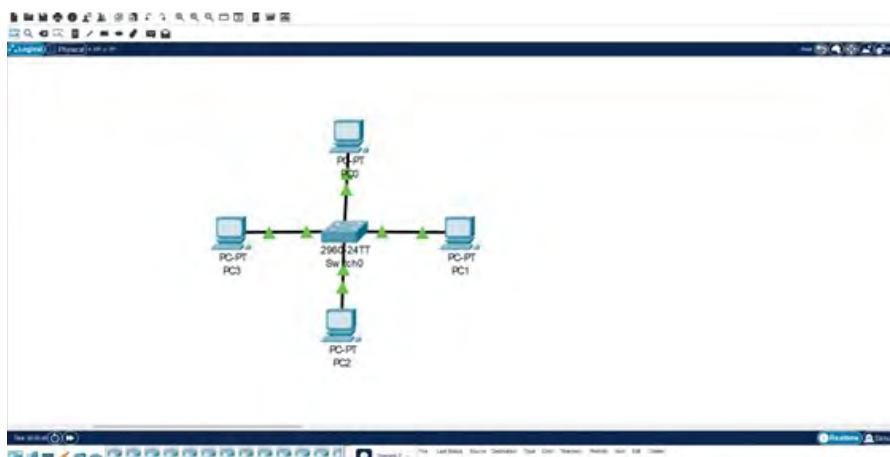


Figura 3 – Print da tela inteira (*Cisco Packet Tracer*)

Descrição da Imagem: a figura apresenta um print da tela do Cisco Packet Tracer com a topologia estrela. Fim da descrição.

Se você quiser aprofundar ainda mais seu conhecimento, um ótimo livro para começar é o *Redes de Computadores*, de Andrew Tanenbaum.



INDICAÇÃO DE LIVRO

Rede de Computadores

Essa obra é considerada a 'bíblia' das redes de computadores. Nela, Tanenbaum, Feamster e Wetherall explicam o funcionamento das redes de forma abrangente, começando pela camada física e avançando até as aplicações. Os capítulos apresentam conceitos-chave, ilustrados com exemplos de redes reais, incluindo a Internet, redes sem fio, LANs sem fio, banda larga sem fio e Bluetooth. É uma leitura clássica e vai ajudar você a entender não só as topologias, mas o funcionamento completo das redes.



Topologia anel

Nessa topologia, os dispositivos são conectados em série, formando um círculo fechado. Parece simples, não é? Os dados circulam de um dispositivo para o outro, passando por todos até chegar ao destino. Essa comunicação pode ser em uma única **direção (unidirecional)** ou em ambas as **direções (bidirecional)**, dependendo da configuração.

Agora, pensando nas vantagens, uma delas é a facilidade de identificar falhas. Como os dados têm um caminho específico para seguir, se algo der errado, fica mais fácil descobrir onde está o problema. Há uma igualdade de distribuição de largura de banda, ou seja, todos os dispositivos têm o mesmo acesso ao meio de transmissão, evitando que um único nó domine o tráfego.

Por outro lado, nem tudo é perfeito. Um ponto fraco dessa topologia é a vulnerabilidade a falhas. Se um único dispositivo ou cabo der problema, pode afetar toda a rede e interromper a comunicação. Outra desvantagem é que expandir a rede pode ser um pouco complicado. Adicionar novos dispositivos pode exigir parar tudo para ajustar a configuração.

Imagina uma roda gigante, em que os assentos são os dispositivos da rede e as conexões entre eles são os cabos. Na topologia em anel, tudo está interligado formando um círculo. Os dados não têm liberdade para pular direto para o destino. Eles seguem uma rota bem definida, passando por cada dispositivo (ou nó) até chegar ao destinatário. Isso pode acontecer em uma única direção (unidirecional) ou nas duas (bidirecional), dependendo da configuração da rede.

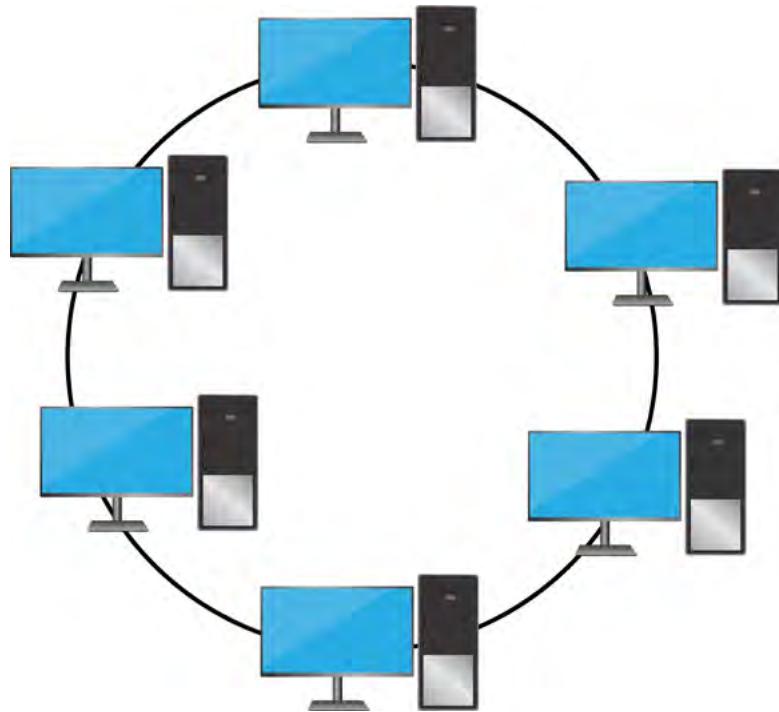


Figura 4 – Topologia Anel

Descrição da Imagem: a figura apresenta uma topologia anel. É uma ilustração de seis computadores em formato de anel. Fim da descrição.

Uma das grandes vantagens do anel é que ele facilita muito a identificação de falhas. Como os dados percorrem um trajeto fixo, qualquer interrupção no fluxo é fácil de localizar. Se um dispositivo parar de funcionar, sabemos exatamente onde está o problema, e isso ajuda na manutenção. Existe uma igualdade na distribuição de largura de banda. Como todos os dispositivos estão na fila, ninguém monopoliza o tráfego, garantindo que todos tenham o mesmo acesso.

Contudo, a topologia em anel também tem suas desvantagens. Por exemplo, ela é muito mais vulnerável a falhas do que outras topologias. Se um único dispositivo ou cabo falhar, todo o sistema pode parar. O caminho circular que facilita a detecção de falhas também significa que a rede pode ficar completamente inoperante com um único problema. Outro ponto negativo é a dificuldade de expansão. Para adicionar novos dispositivos, você precisa interromper o funcionamento da rede, o que pode não ser prático em ambientes que exigem alta disponibilidade.

APROFUNDANDO

Um exemplo de Rede *Token Ring*, que foi desenvolvida na época de 1980 e 1990 pela IBM, é que eram amplamente utilizadas em ambientes industriais, seguindo exatamente esse modelo de anel. Isso fazia sentido, mas com a chegada da *Ethernet* e suas vantagens (como maior flexibilidade e robustez), o uso de topologias em anel foi diminuindo significativamente.

Topologia barramento

Na topologia de barramento, todos os dispositivos da rede estão conectados a um único cabo de comunicação, esse cabo é o meio de transporte dos dados, e só um dispositivo por vez pode enviar informações, enquanto os outros aguardam sua vez.

Ela brilha em termos de custo reduzido. Como todos os dispositivos compartilham o mesmo cabo, você economiza em cabeamento. Sua simplicidade torna essa topologia uma escolha prática para redes pequenas. A configuração inicial é fácil e rápida, sem muita complicações, o que a tornava ideal para ambientes menores, como laboratórios de informática em escolas ou pequenas empresas.

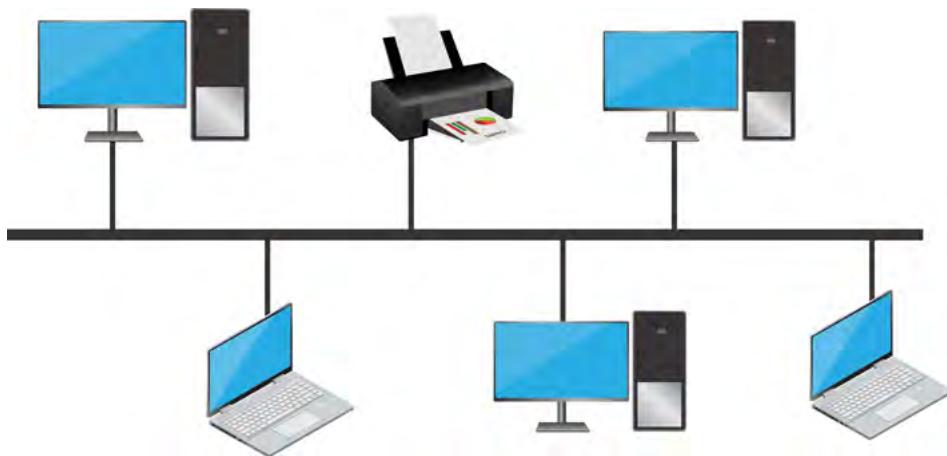


Figura 5 - Topologia Barramento

Descrição da Imagem: É uma ilustração com dois computadores e uma impressora na parte de cima e dois notebooks e um computador na parte de baixo da linha em forma de barramento, representando a topologia barramento. Fim da descrição.

A topologia de barramento tem suas limitações, como todos compartilham o mesmo cabo, o risco de colisões de dados é alto. Se dois dispositivos tentarem enviar dados ao mesmo tempo, haverá uma colisão, e isso prejudica o desempenho da rede.

Para contornar essa situação e lidar com as colisões, as redes com barramento utilizavam métodos como CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). Entretanto, o problema persistia. Outro ponto é a falta de escalabilidade. Se você quiser adicionar mais dispositivos à rede, vai notar que o desempenho diminui, pois o barramento acaba ficando congestionado.

Podemos citar como exemplo prático de redes de barramento os laboratórios de informática antigos, em que diversos computadores compartilham um único cabo *Ethernet*. Todos usavam o mesmo meio de transmissão, o que facilitava a instalação e manutenção. Todavia, com o tempo, esse modelo foi substituído por soluções mais robustas e escaláveis, como a topologia em estrela.

Topologia malha



PENSANDO JUNTOS

Você já pensou em como seria viver em um mundo onde cada pessoa pudesse se comunicar diretamente com qualquer outra, sem depender de intermediários?

Agora, imagine essa ideia aplicada a redes de computadores, e você terá uma noção do que é a topologia de malha. Nesse modelo, todos os dispositivos da rede estão conectados uns aos outros, criando um verdadeiro emaranhado de conexões – algo quase poético se pararmos para pensar.

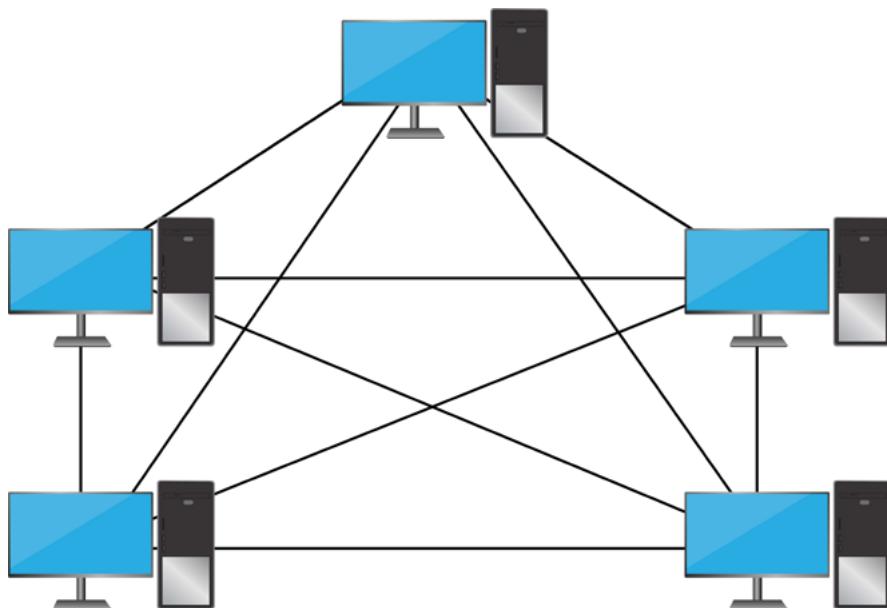


Figura 6 - Topologia Malha

Descrição da Imagem: É uma ilustração com cinco computadores em forma de malha, representando a topologia malha. Fim da descrição.

O maior trunfo da topologia de malha é a redundância. Se um caminho falha, não há pânico. O dado simplesmente escolhe outro caminho disponível, garantindo que ele chegue ao destino sem interrupções. Isso é essencial em sistemas em que falhas não são uma opção. Data centers, por exemplo, dependem muito desse tipo de configuração. Afinal, se um componente falha e o sistema inteiro cair, o prejuízo seria astronômico.

Para ver a redundância em ação, você pode desconectar um cabo e observar como o restante da rede continua funcionando sem interrupções (graças ao fato de que existem múltiplos caminhos de comunicação).

Outro ponto forte dessa topologia é a distribuição do tráfego. Imagine uma estrada com várias vias alternativas. Em vez de todos os carros seguirem pela mesma rota e ficarem presos em congestionamentos, eles podem se dividir por diferentes caminhos, acelerando o fluxo geral. A topologia de malha faz exatamente isso com os dados, mantendo a rede fluida e eficiente.

No entanto, claro, não dá para ignorar os desafios. Embora a ideia de cada nó esteja conectada a todos os outros pareça fantástica em termos de confiabilidade, essa rede de conexões diretas pode ser caríssima e muito complexa de gerenciar, especialmente em grandes redes. É como tentar organizar uma teia gigantesca – quanto mais dispositivos, mais complicada a estrutura.



PENSANDO JUNTOS

Então, em que essa topologia é mais aplicada? Lugares nos quais falhar não é uma opção. Pense em infraestruturas críticas e data centers. Nesses ambientes, a malha garante que, mesmo com um componente fora do ar, o sistema continue funcionando. Isso pode fazer toda a diferença.

Topologia híbrida

Imagine o seguinte cenário: você está montando uma rede para uma grande empresa ou universidade. Algumas áreas da instituição precisam de uma rede rápida e eficiente para muitos dispositivos, enquanto outras precisam de segurança e redundância. Como você faria para que tudo funcionasse de maneira integrada? É aí que entra a topologia híbrida.

A topologia híbrida é como misturar o melhor de dois (ou mais) mundos. Ela combina diferentes tipos de topologias, em estrela, anel, malha ou barramento, para criar uma solução sob medida para atender às necessidades de uma rede específica.

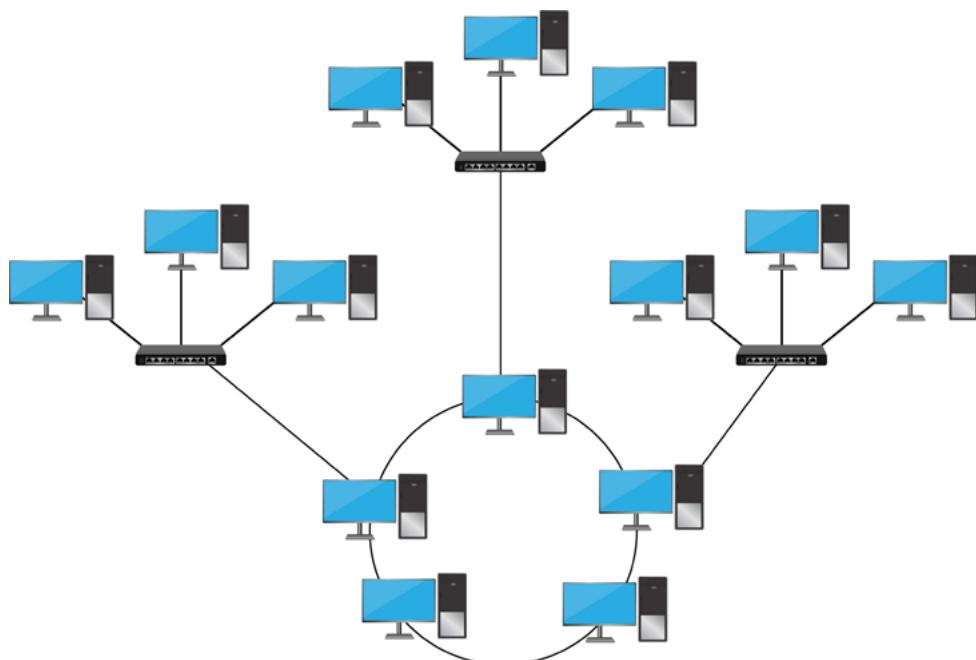


Figura 7 - Topologia Híbrida

Descrição da Imagem: É uma ilustração, representando a topologia híbrida, com 14 computadores que compõem quatro grupos. Desses quatro grupos, apenas um grupo tem cinco computadores. Os três grupos de três computadores estão interligados no grupo com cinco computadores em forma de malha. Fim da descrição.

Pense numa universidade, por exemplo. Cada departamento pode estar organizado em uma topologia em estrela, em que todos os computadores estão conectados a um *switch* central. Mas, e se a universidade também quiser garantir uma conexão redundante e confiável entre os departamentos? Nesse caso, os *switches* desses departamentos poderiam ser interconectados em uma topologia em malha, criando um sistema robusto e eficiente que garante que, se um caminho falhar, outro caminho estará disponível para o tráfego de dados.

A flexibilidade é o grande trunfo da topologia híbrida. Ao misturar diferentes topologias, podemos ajustar a estrutura da rede exatamente conforme as necessidades de cada setor ou departamento. Se uma precisa de velocidade, usamos estrela, se outro precisa de mais segurança e redundância, incorporamos elementos de malha.

Por outro lado, essa flexibilidade tem um custo: a complexidade. Como estamos lidando com múltiplas topologias, o gerenciamento e a manutenção da rede podem se tornar mais difíceis. Às vezes, é como tentar ajustar várias peças diferentes de um quebra-cabeça para funcionar perfeitamente juntas. Problemas de compatibilidade entre as diferentes topologias podem surgir, exigindo soluções técnicas mais avançadas.

A flexibilidade é o grande trunfo da topologia híbrida

IDENTIFICAR OS TIPOS DE MEIOS DE TRANSMISSÃO

Os meios de transmissão são os canais pelos quais os dados trafegam. Eles podem ser divididos em meios guiados, nos quais os sinais percorrem por meio de cabos físicos, e meios não guiados, como transmissões via ondas de rádio. Conheça a seguir os tipos de meio de transmissão: fibra óptica, cabo coaxial, 5G/6G.

Fibra óptica

A fibra óptica é uma tecnologia essencial para redes de alta velocidade e longa distância, que vem substituindo progressivamente os cabos de cobre tradicionais. Esse meio de comunicação tem capacidade de transmitir grandes quantidades de dados a velocidades muito altas e com baixa perda de sinal, o que o torna ideal para conexões de internet, redes empresariais e infraestruturas de telecomunicações.



APROFUNDANDO

A **fibra óptica** é composta por fios extremamente finos, de vidro ou plástico, que conduzem pulsos de luz de uma ponta à outra. Esses pulsos são interpretados como dados digitais, permitindo a comunicação entre dispositivos a grandes distâncias sem perda significativa de qualidade.

Cada fibra possui três camadas principais, a importância de entendê-las também nos faz mais assertivos em relação à escolha de utilização da fibra óptica.

- **Camada Núcleo:** é a parte central da fibra, por onde passa a luz. É feita de vidro ou plástico de alta pureza para minimizar a dispersão e a perda do sinal.
- **Camada Revestimento:** envolve o núcleo e tem um índice de refração mais baixo, o que ajuda a manter a luz confinada no núcleo, refletindo-a de volta em vez de deixá-la escapar.
- **Camada Casco protetor:** uma camada externa que protege a fibra contra danos físicos (Barreto; Zanin; Saraiva, 2018).

Os tipos de Fibra Óptica também são conceitos importantes que nos ajudam no momento da escolha da fibra para o planejamento e implementação da rede.

ZOOM NO CONHECIMENTO

Monomodo tem um núcleo menor e é projetado para transmissão de dados a longas distâncias com uma única onda de luz. Ideal para infraestrutura de *backbone* de internet e telecomunicações.

Multimodo possui um núcleo mais largo e permite múltiplos modos de transmissão de luz. É ideal para distâncias menores, como redes locais (LANs) em prédios e campus corporativos.

Vejamos as Vantagens da Fibra Óptica:

- **Alta Largura de Banda:** a fibra óptica pode suportar uma largura de banda significativamente maior que os cabos de cobre. Isso significa que mais dados podem ser transmitidos ao mesmo tempo.
- **Baixa Perda de Dados:** o sinal em uma fibra óptica pode viajar distâncias muito maiores sem a necessidade de amplificação, devido à baixa perda de sinal.
- **Imunidade a Interferências Eletromagnéticas:** como a fibra óptica usa luz em vez de eletricidade, ela não é suscetível a interferências eletromagnéticas (EMI), o que melhora a confiabilidade do sinal (Barreto; Zanin; Saraiva, 2018).

Os custos associados à instalação de fibra óptica podem ser altos, principalmente se comparados a cabos de cobre, mas apresentam um melhor custo-benefício a longo prazo. Vamos detalhar esses custos em duas categorias principais, segundo Kurose e Ross (2021):

MATERIAIS

O cabo de fibra óptica é mais caro que o cabo de cobre, devido ao processo de fabricação mais sofisticado e ao uso de materiais de alta pureza.

EQUIPAMENTOS

Para instalar e emendar fibra óptica são necessários equipamentos especializados, como máquinas de fusão de fibra e ferramentas para polimento de conectores.

INFRAESTRUTURA

Em áreas onde a infraestrutura já está estabelecida, a instalação pode ser mais simples. No entanto, em locais onde será necessário cavar, instalar dutos e conduítes, os custos podem ser muito altos.

Agora podemos conhecer, em manutenção e equipamentos de rede, os seguintes aspectos: a fibra óptica exige manutenção mínima devido à sua durabilidade, mas os equipamentos para transmissão de sinal (como *switches* e roteadores compatíveis com fibra) podem ser caros, afirma Kurose e Ross (2021).

Conversores de mídia são comuns em redes que precisam de integração entre fibra e cobre, o que gera um custo adicional, além da necessidade de técnicos especializados. Uma das aplicações é em redes metropolitanas, um exemplo prático nas quais a fibra óptica é aplicada para conectar diferentes regiões de uma cidade. Empresas e provedores de internet geralmente usam fibras monomodo para criar redes de *backbone*, capazes de transportar dados por vários quilômetros sem perda de qualidade (Kurose; Ross, 2021).

Também temos as aplicações em *data centers*, a fibra óptica é essencial para transferências rápidas de dados entre servidores e armazenamentos.

 ZOOM NO CONHECIMENTO

A fibra **multimodo** é comumente utilizada para distâncias menores dentro de instalações, enquanto a fibra **monomodo** é empregada em distâncias maiores para conexões interdatacenters.

Embora a fibra óptica seja uma tecnologia avançada, ainda existem desafios técnicos para serem implementadas, de acordo com Maia (2013, on-line), por exemplo:

- **Sensibilidade à curvatura:** a curvatura excessiva de uma fibra óptica pode causar perda de sinal, por isso é fundamental respeitar o raio de curvatura recomendado pelo fabricante durante a instalação.
- **Temperatura e Clima:** em ambientes externos, a fibra precisa de revestimentos que a protejam de variações de temperatura e umidade, elevando o custo em áreas com condições ambientais extremas.

Cabo coaxial

O cabo coaxial é um meio de transmissão de dados amplamente utilizado para transportar sinais de televisão, internet e redes locais em pequenas distâncias. Desenvolvido para resistir a interferências externas e proporcionar uma comunicação estável, ele foi muito utilizado em redes de computadores e telecomunicações antes da popularização da fibra óptica.



A estrutura do cabo coaxial é composta por várias camadas que contribuem para sua capacidade de transmissão e resistência a interferências externas (Maia, 2013).

CONDUTOR CENTRAL

É geralmente um fio de cobre ou alumínio, que conduz o sinal principal. Esse condutor pode ser sólido ou trançado, dependendo da aplicação.

ISOLANTE DIELÉTRICO

Envolve o condutor central e serve para manter o sinal dentro do cabo, reduzindo a perda de sinal. Esse material é feito de plástico ou polímeros especiais.

BLINDAGEM

Consiste em uma malha metálica, ou uma combinação de malha e fita de alumínio, que protege contra interferências eletromagnéticas (EMI) e interferência de radiofrequência (RFI).

REVESTIMENTO EXTERNO (CAPA)

É uma camada de PVC ou outro material plástico que protege o cabo de danos físicos e desgastes.

Essa construção em camadas ajuda o cabo coaxial a manter a qualidade do sinal e a minimizar a interferência, sendo, por isso, uma escolha sólida para transmissão de dados, especialmente em ambientes com altos níveis de ruído eletromagnético. Existem vários tipos de cabo coaxial, cada um adequado para diferentes aplicações e distâncias, segundo Maia (2013). Os principais tipos incluem:

- **RG-6:** usado principalmente em instalações de TV a cabo e redes domésticas. Possui boa resistência a interferências e é adequado para distâncias médias.

- **RG-59:** também usado em sistemas de TV, mas com menor capacidade de alcance e resistência. É adequado para distâncias curtas.
- **RG-11:** usado em longas distâncias, como em infraestrutura de telecomunicações. Sua construção mais robusta permite menor perda de sinal ao longo de extensões maiores.

Conforme Kurose e Ross (2021), esses diferentes modelos de cabo coaxial oferecem opções para diversos tipos de instalação e exigências de desempenho, o cabo coaxial é utilizado em várias áreas, principalmente em:

- **Televisão a Cabo:** a maior parte dos sistemas de TV a cabo utiliza coaxial RG-6 para transportar sinais de áudio e vídeo de maneira estável e com baixa interferência.
- **Internet Banda Larga:** redes de internet a cabo usam coaxial em combinação com fibra óptica para levar o sinal até as residências. Em muitos casos, o sinal de internet é transmitido pela mesma infraestrutura da TV a cabo.
- **Sistemas de CFTV:** em circuitos fechados de televisão (CFTV), o coaxial é utilizado para transportar vídeo de câmeras até o sistema de monitoramento.
- **Antenas e Satélites:** o cabo coaxial também é essencial para ligar antenas e sistemas de satélite aos receptores, aproveitando-se de sua blindagem contra interferências externas.

Comparado a outros tipos de cabos, o coaxial apresenta algumas características únicas, além de algumas vantagens com relação à fibra:

MAIOR RESISTÊNCIA A INTERFERÊNCIAS

Devido à blindagem, o cabo coaxial é mais resistente a interferências eletromagnéticas do que os cabos de par trançado.

CUSTO-BENEFÍCIO

É mais barato que a fibra óptica e pode ser uma solução econômica para redes locais e distâncias curtas.

PROTEÇÃO CONTRA INTERFERÊNCIAS

A blindagem reduz ruídos externos, garantindo a qualidade do sinal.

LIMITAÇÕES DE DISTÂNCIA E VELOCIDADE

Não é indicado para transmissões de alta velocidade e distâncias muito longas. Nesses casos, a fibra óptica é mais eficiente.

RIGIDEZ

O cabo coaxial é menos flexível que o par trançado, o que pode dificultar a instalação em áreas de difícil acesso.

5G/6G

Estudante, agora, trataremos sobre o 5G e o futuro 6G. O 5G, como você deve saber, é a quinta geração das redes móveis e chegou com uma promessa ambiciosa: oferecer velocidades muito mais altas do que as que temos no 4G. E não para por aí, o 6G, que ainda está em fase de desenvolvimento, deve ir além, trazendo avanços impressionantes em termos de velocidade, conectividade e uma latência incrivelmente baixa.

Primeiro, temos a **alta velocidade**. O 5G oferece velocidades muito maiores do que o 4G, o que é perfeito para tarefas que exigem grande largura de banda, como streaming de vídeos em alta definição ou download de arquivos pesados. Depois, vem a **baixa latência**, que é essencial para aplicações que precisam de respostas rápidas, quase instantâneas. Pense em veículos autônomos, por exemplo, ou dispositivos IoT (Internet das Coisas), que dependem de uma comunicação rápida e precisa.

A implantação do 5G enfrenta obstáculos como a infraestrutura limitada. Instalar torres 5G não é algo barato ou rápido, especialmente em áreas rurais onde a cobertura tende a ser mais demorada. Outro ponto é a penetração limitada das ondas de alta frequência, que, apesar de permitirem altas velocidades, têm dificuldade para atravessar paredes e outros obstáculos.

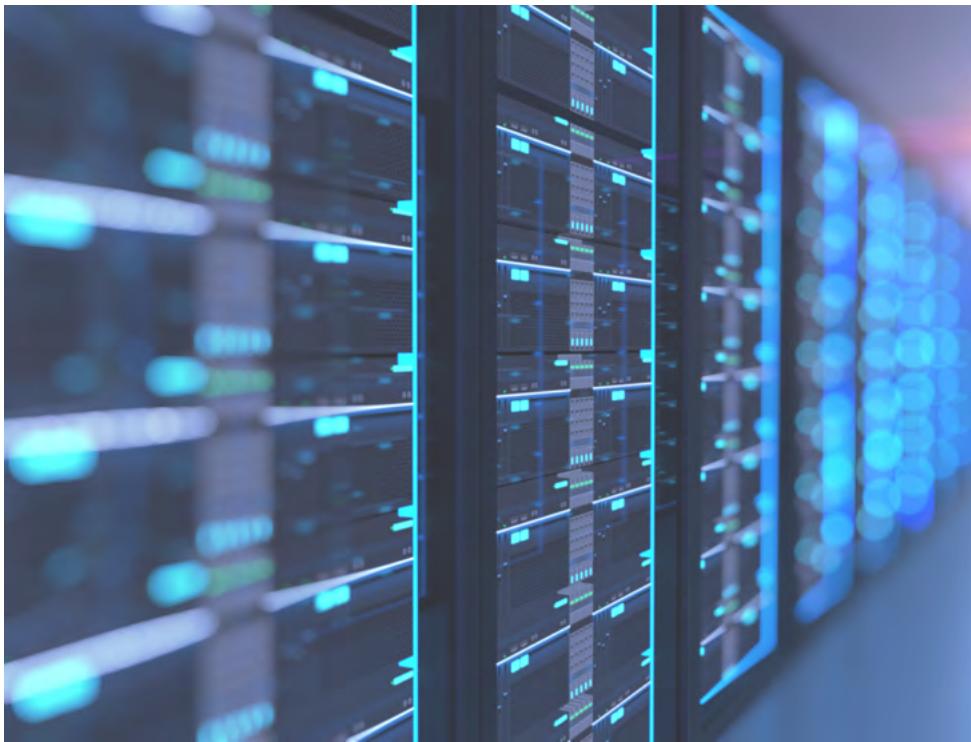
Nas áreas urbanas, as redes 5G são usadas para suportar a crescente demanda por conectividade móvel, assim como para dar suporte a tecnologias emergentes, como a IoT. Esses avanços estão transformando a forma como interagimos com a tecnologia em nosso cotidiano.

O custo do cabo coaxial é relativamente baixo em comparação a outras tecnologias de transmissão. Isso se aplica tanto ao preço do cabo quanto aos conectores e equipamentos necessários para a instalação. Esse fator, aliado à durabilidade, torna o coaxial uma opção atraente para aplicações em que o custo-benefício é prioritário.

No entanto, em cenários que demandam alta velocidade e larga largura de banda, o investimento em fibra óptica se torna mais viável, ainda que seja mais caro. Em redes domésticas e pequenas instalações comerciais, onde o orçamento é um fator importante, o coaxial ainda representa uma solução econômica e eficaz.

EQUIPAMENTOS DE REDE (SWITCHES, ROTEADORES, HUBS)

Segundo Sinclair (2018, p. 18), “os equipamentos de rede são essenciais para a operação de qualquer rede, seja para direcionar o tráfego de dados ou conectar dispositivos”. Na sequência, conversaremos um pouco sobre os diferentes dispositivos que formam a base das redes locais e como eles trabalham juntos para facilitar a comunicação. A seguir, os tipos de equipamento de rede:



Switches

Você já parou para pensar como os dados trafegam eficientemente entre diferentes dispositivos em uma rede? É exatamente nesse momento que os *switches* entram em cena!

Um *switch* é um dispositivo de rede que opera na Camada de Enlace do modelo OSI, responsável por conectar vários dispositivos dentro de uma mesma rede local (LAN). Ao contrário dos *hubs*, que transmitem dados para todos os dispositivos, o *switch* têm a capacidade de filtrar e encaminhar pacotes de dados somente para o dispositivo de destino.

Quando um dispositivo, digamos um computador, envia um quadro *Ethernet* para outro, o *switch* analisa o endereço MAC de origem e destino. Vamos supor que temos um *switch* com três dispositivos conectados: Computador A, Computador B e Computador C. Se o Computador A enviar dados para o Computador B, o *switch* realiza o seguinte tráfego:

O *switch* recebe o quadro na porta correspondente ao computador A, ele realiza a leitura do endereço MAC de destino (referente ao do computador B) e consulta sua tabela de endereços MAC para verificar onde o computador B está conectado, após a verificação ele encaminha a informação para a porta em que o computador B está conectado.

Isso é muito mais eficiente do que um *hub*, a comunicação fica mais rápida e as colisões são minimizadas! “O uso de *switches* reduz o tráfego desnecessário e melhora o desempenho da rede” (Tanenbaum; Wetherall, 2011, p. 54).

Existem diferentes tipos de *switches*, cada um com suas características. Vamos falar de dois tipos comuns (Kurose; Ross, 2021, on-line):

ZOOM NO CONHECIMENTO

Switches não gerenciados: são simples e prontos para usar. Eles não oferecem configurações avançadas. Um exemplo é um switch usado em uma pequena rede doméstica.

Switches gerenciados: esses switches oferecem uma variedade de recursos de gerenciamento, como VLANs (redes locais virtuais), QoS (qualidade de serviço) e monitoramento de tráfego. Eles são usados em ambientes corporativos onde é necessário maior controle e segurança.

Você consegue pensar em um cenário em que um *switch* gerenciado poderia ser mais benéfico do que um não gerenciado? Para entender melhor, você pode realizar um teste, se você tiver acesso a um *switch* gerenciado, tente configurar uma VLAN:

- Identifique os dispositivos conectados ao *switch*;
- Acesse a interface de gerenciamento do *switch* (normalmente através de um navegador);
- Crie uma VLAN e atribua dispositivos a ela;
- Teste a comunicação entre os dispositivos na mesma VLAN e fora dela (Benedetti; Anderson, 2010).

Você perceberá como a separação de tráfego pode otimizar o desempenho! Vamos refletir sobre a importância dos *switches* na sua futura carreira em TI. Como você acha que o entendimento profundo de *switches* pode impactar suas habilidades em redes? Pense em uma situação em que você precise diagnosticar um problema de rede. Saber como os *switches* funcionam será fundamental para resolver questões de conectividade e desempenho.



VOCÊ SABE RESPONDER?

O que acontece em uma rede quando muitas transmissões ocorrem ao mesmo tempo em um *hub*? Como os *switches* evitam esse problema?

Os *switches* são essenciais para a eficiência das redes modernas. Eles não apenas melhoraram o desempenho da rede, mas também proporcionam recursos avançados que ajudam na gestão e segurança dos dados. Agora que você tem uma base sólida sobre *switches*, pode começar a explorar mais as suas aplicações e configurações.

Roteadores

Um roteador é um dispositivo que conecta diferentes redes e é responsável por direcionar pacotes de dados entre essas redes. Ele opera na Camada de Rede do modelo OSI, utilizando endereços IP para encaminhar os dados de forma eficiente.

Quando um pacote de dados chega a um roteador, ele analisa o endereço de destino e determina a melhor rota para enviá-lo, semelhante a um GPS que calcula o melhor caminho para um destino.

Considere uma situação em que você tem dois escritórios de uma empresa em diferentes locais, conectados à internet. Se um computador no Escritório A quer se comunicar com um computador no Escritório B, o roteador no Escritório A analisa o endereço IP do computador de destino e envia os dados pela rota mais eficiente. Se necessário, o roteador pode até encaminhar o tráfego através de vários roteadores até que os dados cheguem ao seu destino.



Conforme Benedetti e Anderson (2010), os roteadores são mais sofisticados que os *hubs*, pois:

- Podem gerenciar o tráfego de dados, minimizando colisões e aumentando a eficiência;
- Podem conectar redes diferentes, como redes locais (LAN) a redes mais amplas (WAN), incluindo a internet;

Os roteadores desempenham um papel vital em redes modernas, possibilitando a comunicação entre diferentes redes de forma eficiente e segura. Compreender como funcionam é essencial para qualquer profissional de TI.

Hubs

Um *Hub* é um dispositivo que conecta vários dispositivos dentro de uma rede local. Sua principal função é receber dados de um dispositivo e transmiti-los para todos os outros conectados, sem considerar quem é o destinatário. Quando um dispositivo envia dados para o *hub*, ele transmite essas informações para todas as portas conectadas a ele. Isso significa que todos os dispositivos conectados recebem a mesma mensagem, mesmo que não sejam o destinatário. Como o *hub* envia os dados para todos os dispositivos, isso pode causar conflitos e colisões, diminuindo a eficiência da rede.



Suponha que você tenha um *hub* com quatro dispositivos: Computador A, Computador B, Computador C e Computador D. Se o Computador A enviar um quadro de dados para o Computador B, o *hub* enviará esse quadro para todos os outros computadores também. Essa abordagem resulta em congestionamento de rede e diminuição da largura de banda disponível. Os *hubs* foram importantes no desenvolvimento das redes locais, mas suas limitações os tornaram obsoletos em muitos cenários. Com o avanço da tecnologia, os *hubs* foram superados por dispositivos mais sofisticados.

TOPOLOGIA PARA DIFERENTES CENÁRIOS

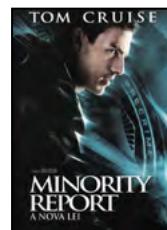
A seleção da topologia e do meio de transmissão depende das necessidades da rede. Uma rede corporativa pode optar por uma topologia em estrela com cabos de cobre para conectar computadores de mesa e fibra óptica para interconectar departamentos, garantindo alta velocidade e redundância. Já uma rede doméstica pode utilizar Wi-Fi para a conveniência da mobilidade, mesmo que isso signifique uma redução na velocidade máxima em comparação com uma conexão com fio.



INDICAÇÃO DE FILME

Minority Report – A Nova Lei

O contexto do filme se passa no ano de 2054, e há um sistema que permite que crimes sejam previstos com precisão, o que faz a taxa de assassinatos cair para zero. O problema começa quando o detetive John Anderton, um dos principais agentes do combate ao crime, descobre que foi previsto um assassino que ele mesmo cometerá, colocando em dúvida sua reputação e a confiabilidade do sistema.



CONCEITOS DE REDUNDÂNCIA E SEGURANÇA EM TOPOLOGIAS

Segundo Tanenbaum e Wetherall (2011, p. 168), “a redundância em redes garante que, caso uma parte falhe, outra rota esteja disponível para o tráfego de dados.”

A topologia em malha, por exemplo, é altamente redundante, pois oferece múltiplos caminhos para os dados viajarem. Relacionando a indicação anterior do filme em termos de segurança, a escolha da topologia também desempenha um papel importante. Redes com uma única falha central, como a topologia em estrela, exigem um controle rigoroso de segurança no ponto central, enquanto em topologias distribuídas, como a malha, o monitoramento de segurança precisa ser mais abrangente.

INTERPRETAR DIAGRAMAS E ESQUEMAS DE REDE

VOCÊ SABE RESPONDER?

Você já se perguntou por que essa habilidade é tão essencial para quem trabalha com redes?

Bom, pense nos diagramas como mapas da sua rede. Eles mostram a topologia, ou seja, como os dispositivos estão dispostos, quais meios de transmissão são usados e como tudo isso se conecta, tanto fisicamente quanto logicamente (Lacerda, 2022).

Imagine, se você entender bem esse mapa, poderá identificar rapidamente o localização do erro quando houver um problema. Fica muito mais fácil propor melhorias ou realizar novas implementações.

O diagrama mostra a localização física dos dispositivos de rede, como roteadores, *switches*, servidores, estações de trabalho e cabos. Ele é utilizado para entender a disposição física e facilitar o processo de manutenção e expansão da rede.

Por exemplo, um **diagrama físico** pode incluir um mapa dos andares de um prédio, com pontos de rede, rack de servidores e outros equipamentos em suas localizações reais. O **diagrama lógico** apresenta a estrutura de comunicação e conexão entre os dispositivos, sem levar em conta a disposição física. Nele, são mostradas as sub-redes, VLANs (*Virtual Local Area Networks*), roteadores, *gateways* e outros elementos lógicos. Esse tipo de diagrama é fundamental para visualizar o fluxo de dados, as rotas e as relações entre diferentes sub-redes, simplificando a resolução de problemas e a configuração.

Para criar uma documentação de rede clara e completa, cada diagrama deve conter elementos específicos e detalhamentos técnicos. Cada dispositivo de rede (ex.: *switch*, roteador, firewall) deve ser identificado no diagrama com um nome, IP e outras informações essenciais, como o modelo e as interfaces de rede utilizadas. A documentação também deve detalhar as interfaces conectadas, como portas *Ethernet*, *uplinks* e conexões de fibra óptica:

Dispositivo: *Switch Cisco Catalyst 2960*

IP: 192.168.1.1

Interfaces

- GigabitEthernet0/1 (Conectado ao Roteador Principal)

- GigabitEthernet0/2 (Conectado ao Servidor)

As sub-redes devem ser representadas com seus endereços IP e máscaras de sub-rede. No diagrama lógico, por exemplo, é comum mostrar as divisões de sub-redes para segmentação de tráfego e segurança:

Sub-rede A (Rede Interna)

Endereço: 192.168.10.0/24

Máscara de Sub-rede: 255.255.255.0

Gateway: 192.168.10.1

A topologia é o padrão de interconexão entre dispositivos. Na documentação é necessário incluir a topologia utilizada (como estrela, malha ou árvore) e detalhes sobre o roteamento, especificando quais dispositivos roteiam para quais redes.

A documentação de um esquema de rede também deve incluir as configurações de segurança, como firewalls, VLANs e ACLs (listas de controle de acesso) configuradas. Isso ajuda a entender as políticas de segurança implementadas e como o tráfego é filtrado ou segmentado.

VLAN 10: Rede de Vendas (192.168.20.0/24)

VLAN 20: Rede de Suporte (192.168.30.0/24)

VLAN 30: Rede Administrativa (192.168.40.0/24)

ACL: Permitir tráfego entre VLAN 10 e VLAN 30 apenas na porta 80 (HTTP)

Utilizar ferramentas de diagramação, como *Visio*, *Lucidchart* ou *Diagram Designer*, pode auxiliar na criação de diagramas organizados e precisos. Segundo Lacerda (2022) essas ferramentas oferecem ícones padrão para representar *switches*, roteadores e outros dispositivos, facilitando a leitura e a interpretação do esquema. A documentação completa pode incluir anexos, como:

- Capturas de configuração de dispositivos principais.
- Planilhas com endereçamento IP e mapeamento de portas.
- Observações sobre limitações de banda ou recomendações de expansão.

Aliás, de acordo com Kurose e Ross (2021, p. 137), “entender as topologias de rede, os meios de transmissão e os equipamentos é essencial para realmente compreender o funcionamento e a otimização das redes modernas.” Então, quanto mais você se familiarizar com esses diagramas e essas conexões, mais preparado estará para lidar com qualquer situação no mundo das redes.

A aplicação desses conceitos em redes virtuais (VLANs), além da implementação de QoS e SD-WAN, ajuda a garantir que redes corporativas e domésticas possam atender às demandas crescentes de conectividade, segurança e desempenho.

A integração entre essas tecnologias permite que redes sejam projetadas e gerenciadas de maneira eficiente, garantindo qualidade e robustez para os usuários finais.

EM FOCO

Estudante, para expandir seus conhecimentos sobre o assunto abordado, gostaríamos de lhe indicar a aula que preparamos especialmente para você. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

NOVOS DESAFIOS

À medida que avançamos em uma era cada vez mais digital, o papel do profissional de redes de computadores se torna ainda mais crítico e complexo. A conectividade global não só está em expansão, como também é cada vez mais sofisticada. As inovações tecnológicas, como o surgimento das redes 5G

e a evolução para o 6G, a crescente demanda por redes definidas por software (SD-WAN), e a necessidade de gerenciar a Qualidade de Serviço (QoS) para aplicações que exigem alta performance, como streaming e videoconferências, exigem profissionais que dominem tanto os conceitos básicos quanto às tecnologias emergentes.

Como discutimos ao longo deste tema, entender as topologias de rede e os meios de transmissão é fundamental para qualquer profissional que deseja atuar no campo de redes. Esses conhecimentos formam a base sobre a qual novas tecnologias serão construídas. Saber como configurar uma topologia em estrela ou escolher entre fibra óptica e wireless são habilidades que transcendem o conhecimento técnico; elas preparam o profissional para tomar decisões estratégicas que podem impactar diretamente o desempenho e a segurança das operações em uma organização.

A experimentação prática, explorada durante este curso, não é apenas uma etapa do aprendizado, mas uma experiência que simula os desafios do mercado de trabalho. **O futuro profissional de redes precisará aplicar essas habilidades diariamente** ao configurar redes virtuais (VLANs), gerenciar o tráfego de dados, otimizar o uso de *switches* e roteadores, e garantir que a conectividade seja eficiente, escalável e segura. Cada escolha, desde o tipo de topologia até o meio de transmissão utilizado, tem impacto direto na qualidade dos serviços prestados.

A capacidade de reflexão crítica sobre as práticas e experimentações realizadas será o diferencial para os futuros profissionais de destaque. No cenário atual, em que as infraestruturas de redes estão constantemente sendo desafiadas por novas demandas tecnológicas, como a Internet das Coisas (IoT) e a computação em nuvem, é crucial que os profissionais sejam adaptáveis e estejam sempre prontos para aprender e se atualizar. A reflexão sobre suas experiências anteriores permitirá que identifiquem áreas de melhoria e inovação, posicionando-os como agentes estratégicos na transformação digital de empresas e organizações.

O futuro do profissional de redes de computadores está intimamente ligado à sua capacidade de lidar com desafios cada vez mais complexos e de se adaptar a um mundo em rápida evolução. Ao dominar os conceitos abordados aqui, ele estará preparado para acompanhar essas mudanças e liderar as inovações que transformarão o futuro das redes e da conectividade global.

VAMOS PRATICAR

1. Na topologia em anel, os dispositivos são conectados em série, formando um círculo por onde os dados circulam até chegarem ao destinatário. Esse modelo oferece uma distribuição equilibrada de largura de banda entre os nós e facilita a identificação de falhas, porém é vulnerável, pois a falha de um dispositivo pode paralisar a rede. Sua expansão é complexa, o que limitou sua popularidade frente a tecnologias mais modernas, como o *Ethernet* (Kurose, 2021).

Com base na descrição da topologia em anel, analise as afirmativas a seguir:

- I - A topologia em anel garante uma distribuição igual de largura de banda entre os dispositivos conectados.
- II - A falha de um dispositivo em uma rede em anel pode interromper a comunicação de toda a rede.
- III - A expansão da topologia em anel pode ser difícil e interromper o funcionamento da rede.

É correto o que se afirma em:

- a) I, apenas.
- b) III, apenas.
- c) I e II, apenas.
- d) II e III, apenas.
- e) I, II e III.

2. Na topologia de barramento, todos os dispositivos estão conectados a um único cabo de comunicação, chamado barramento. Apenas um dispositivo pode transmitir dados por vez, o que pode levar a colisões de dados. Essa topologia é simples e de baixo custo, mas enfrenta problemas de escalabilidade e desempenho à medida que mais dispositivos são conectados (Kurose, 2021).

Com base na topologia de barramento, qual das alternativas a seguir descreve corretamente suas características?

VAMOS PRATICAR

- a) A topologia de barramento é escalável e evita colisões de dados, pois cada dispositivo tem um canal dedicado de transmissão.
 - b) Um dos maiores benefícios da topologia de barramento é que múltiplos dispositivos podem transmitir dados simultaneamente sem interferências.
 - c) A topologia de barramento tem um custo reduzido de cabeamento, mas pode enfrentar colisões de dados quando vários dispositivos tentam se comunicar ao mesmo tempo.
 - d) A principal vantagem da topologia de barramento é sua capacidade de suportar um grande número de dispositivos sem comprometer o desempenho.
 - e) A topologia de barramento é a mais comum nas redes modernas por sua eficiência e capacidade de evitar falhas de comunicação.
3. Os equipamentos de rede, como *switches*, roteadores e *hubs*, são fundamentais para o funcionamento de qualquer rede. Os *switches* conectam dispositivos em uma rede local (LAN) e encaminham dados apenas para o destinatário correto, oferecendo melhor controle do tráfego. Já os roteadores conectam diferentes redes, como uma rede doméstica à Internet, direcionando pacotes de dados de forma eficiente. *Hubs*, por sua vez, são dispositivos simples que transmitem dados para todos os dispositivos conectados, mas são menos eficientes que os *switches* e estão se tornando obsoletos (Kurose, 2021).

Com base nas informações apresentadas, avalie as asserções a seguir e a relação proposta entre elas:

I - Os *switches* oferecem melhor controle sobre o tráfego da rede, enviando dados apenas para o dispositivo de destino correto.

PORQUE

II - Os *hubs* são dispositivos que transmitem dados recebidos para todos os dispositivos conectados, o que os torna menos eficientes em comparação aos *switches*.

A respeito dessas asserções, assinale a alternativa correta:

- a) As asserções I e II são verdadeiras, e a II é uma justificativa correta da I.
- b) As asserções I e II são verdadeiras, mas a II não é uma justificativa correta da I.
- c) A asserção I é uma proposição verdadeira e a II é uma proposição falsa.
- d) A asserção I é uma proposição falsa e a II é uma proposição verdadeira.
- e) As asserções I e II são falsas.

REFERÊNCIAS

- BENEDETTI, R.; ANDERSON, AL. **Use a cabeça! Redes de computadores**. Rio de Janeiro: Alta Books, 2010.
- KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet**: uma abordagem top-down. São Paulo: Pearson, 2021.
- TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores**. São Paulo: Pearson, 2011.
- SINCLAIR, B. **IoT**: como usar a internet das coisas para alavancar seus negócios. Belo Horizonte: Autêntica Business, 2018.
- BARRETO, J. dos S.; ZANIN, A.; SARAIVA, M. de O. **Fundamentos de redes de computadores**. Porto Alegre: SAGAH, 2018. *E-book*.
- LACERDA, P. S. Pádua de et al. **Projeto de redes de computadores**. Porto Alegre: SAGAH, 2022. *E-book*.
- MAIA, L. P. **Arquitetura de redes de computadores**, 2. ed. Rio de Janeiro: LTC, 2013. *E-book*.

CONFIRA SUAS RESPOSTAS

1. Alternativa E.

Na topologia em anel, a largura de banda é distribuída igualmente entre os dispositivos, a falha de um único dispositivo pode interromper a comunicação da rede, e a expansão da rede pode ser complexa, exigindo uma parada temporária.

2. Alternativa C.

Essa alternativa reflete com precisão os desafios da topologia de barramento: custo baixo, simplicidade, mas também problemas com colisões de dados e limitações em redes maiores. As demais alternativas estão incorretas, pois apresentam características que não condizem com a topologia de barramento, como escalabilidade e múltiplos canais de transmissão.

3. Alternativa A.

A asserção I é verdadeira, pois os *switches* realmente encaminham dados apenas para o destinatário, otimizando o tráfego da rede. A asserção II também é verdadeira, pois os *hubs*, por transmitirem dados para todos os dispositivos, tornam-se menos eficientes e, por isso, seu uso diminui em favor dos *switches* em redes contemporâneas.

MEU ESPAÇO



unidade





TEMA DE APRENDIZAGEM 4

MODELOS DE REFERÊNCIA E ARQUITETURAS DE REDE

MINHAS METAS

- Compreender os modelos de referência de redes.
- Conhecer a prática de conceitos de redes.
- Entender de arquiteturas de redes modernas.
- Explorar tecnologias de *Edge Computing* e *Cloud Computing*.
- Desenvolver de habilidades para solução de problemas em redes.
- Preparar para desafios do mercado de trabalho.
- Refletir sobre inovações em redes.

INICIE SUA JORNADA

No processo de desenvolvimento profissional daqueles que se preparam para atuar na área de redes de computadores, é essencial compreender os principais modelos de referência e as arquiteturas que fundamentam o funcionamento das redes modernas. A seguir, exploraremos quatro tópicos importantes que promovem uma identificação prática com o tema.

No cenário atual, a crescente demanda por conectividade e o avanço acelerado das tecnologias de comunicação criam desafios para a implementação e gestão de redes eficientes. Com a migração para a computação em nuvem e a disseminação de dispositivos IoT, como garantir a segurança, a baixa latência e a escalabilidade? Como os modelos de referência tradicionais, como o OSI e o TCP/IP, se ajustam a essas novas demandas? Essas questões provocam uma reflexão sobre a capacidade das arquiteturas de rede modernas em atender a esses requisitos.

Para dar significado a esses desafios, é necessário revisitar os modelos de referência clássicos, como o OSI e o TCP/IP, que continuam sendo pilares fundamentais para a compreensão da estrutura e do comportamento das redes. No entanto, arquiteturas mais recentes, como Redes Definidas por Software (SDN) e NFV (Virtualização de Funções de Rede), têm revolucionado a forma como redes são gerenciadas, proporcionando maior flexibilidade e automação, adequando-se às demandas atuais por redes mais dinâmicas e responsivas.

Criam desafios para a implementação e gestão de redes eficientes



PLAY NO CONHECIMENTO

Você já ouviu falar da Internet das Coisas e as redes modernas? Quer entender como essas tecnologias estão transformando o mundo ao seu redor e o que isso significa para o futuro? Vamos explorar como dispositivos inteligentes se conectam e como as redes 5G, Wi-Fi 6 e outras inovações estão revolucionando nossas casas, cidades e indústrias. Descubra os desafios, as oportunidades e o futuro dessa tecnologia! **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

Em sua jornada profissional, surgirão as oportunidades de experimentar essas tecnologias de maneira prática. Simulações de redes SDN, configurações de ambientes de *Edge Computing* e integração com serviços de *Cloud Computing* são exemplos de atividades que permitem explorar esses conceitos no mundo real. Tais experimentos possibilitam vivenciar os benefícios de uma rede flexível e programável, além de perceber a importância da computação distribuída em borda para o processamento de dados mais próximo do usuário final.

A reflexão sobre o papel das novas arquiteturas de rede no contexto de transformação digital é crucial. O uso de *Edge Computing* e *fog computing*, aliados à computação em nuvem, oferece soluções para lidar com o processamento e a transmissão de grandes volumes de dados em tempo real, essencial para setores como saúde, manufatura e automação. A capacidade de interligar esses conceitos com os fundamentos dos modelos de referência clássicos reforça o papel estratégico que essas tecnologias desempenham no desenvolvimento de soluções robustas e escaláveis para o futuro.

Com esses pontos em mente, o estudante pode começar a vislumbrar o impacto das redes modernas e de suas arquiteturas na prática profissional, compreendendo a importância de uma base teórica sólida aliada à inovação tecnológica.

VAMOS RECORDAR?

Endereçamento IP, nós utilizamos todos os dias, toda vez que nos conectamos na internet, ou seja, hoje em dia é a todo momento. Por isso, vamos relembrar esse tópico tão importante para nosso tema e assim compreendermos a sua função. Acesse o link: https://www.youtube.com/watch?v=q65kHlvtWxg&list=PLHz_AreHm4dkd4lr9GoUp-W-YaHYdTDuP&index=9

DESENVOLVA SEU POTENCIAL

COMPREENDER OS MODELOS DE REFERÊNCIA DE REDES

Segundo Forouzan e Mosharraf (2012, p. 87), “o **Modelo OSI** (*Open Systems Interconnection*) e o **Modelo TCP/IP** (*Transmission Control Protocol/Internet Protocol*) são pilares fundamentais para a compreensão da estrutura das redes de computadores.”

Ambos descrevem a comunicação de dados em camadas, em que cada camada desempenha uma função específica no processo de transmissão e recepção de dados. A seguir, serão apresentados os Modelos OSI e o Modelo TCP/IP.

MODELO OSI (*OPEN SYSTEMS INTERCONNECTION*)

O **Modelo OSI** é uma referência teórica que descreve como os dados são transmitidos e recebidos em uma rede. Ele é composto por **sete camadas**, e cada uma desempenha uma função específica (Benedetti; Anderson, 2010) e se comunica com as camadas acima e abaixo.



A seguir, na Figura 1, podemos conhecer as Camadas do OSI, com exemplos práticos:



Figura 1 - Camadas do OSI

Descrição da Imagem: a figura apresenta um infográfico de uma pirâmide invertida das camadas do OSI. De baixo para cima, temos a primeira camada: Física, a segunda camada: Enlace de Dados, a terceira camada: Rede, a quarta camada: Transporte, a quinta camada: Sessão, a sexta camada: Apresentação e a sétima e última camada: Aplicação. Fim da descrição.

Camada 1: física

Essa camada lida com a **transmissão física dos dados**, convertendo os bits em sinais elétricos ou ópticos. É a camada que interage diretamente com o hardware da rede, como cabos, *switches*, *hubs* e outros dispositivos.

Imagine que você está conectando seu computador a um roteador usando um cabo *Ethernet*. A camada física garante que os sinais elétricos que representam os dados possam viajar pelo cabo até o roteador, que depois os direciona para outro destino. Quando você conecta um cabo de rede, ou o técnico de internet instala fibra óptica na sua casa, tudo isso faz parte da camada física. Nesse nível, estamos falando de elementos como tensão elétrica, fibras ópticas e radiofrequência no caso de redes sem fio (Wi-Fi).

Quer tentar uma prática? Teste a qualidade de uma conexão *Ethernet* e verifique os status dos LEDs em um *switch* de rede, que indicam se há ou não uma boa conexão física.

Camada 2: enlace de dados

A camada de enlace de dados é responsável por garantir uma comunicação livre de erros entre dois dispositivos diretamente conectados, criando o que chamamos de quadros de dados. Ela também lida com o controle de acesso ao meio de transmissão e o endereçamento físico (usando endereços MAC). Vejamos a divisão da camada enlace:

ZOOM NO CONHECIMENTO

Subcamada MAC: controla o acesso dos dispositivos na rede ao meio físico, identificando cada dispositivo por um endereço MAC único.

Subcamada LLC: Lida com a multiplexação de protocolos, permitindo que vários protocolos utilizem a mesma conexão física.

Segundo Torres (2016, p. 54), “em uma rede LAN, quando um *switch* precisa encaminhar dados para um dispositivo específico, ele usa o endereço MAC do dispositivo para garantir que a mensagem seja enviada para o destinatário correto.” Se houver erros na transmissão, como colisões de dados, a camada de enlace corrige esses problemas localmente.

Você provavelmente já ouviu falar no protocolo **Ethernet** ou no **Wi-Fi**, certo? Ambos operam na camada de enlace. Quando você está conectado a uma rede sem fio, a camada de enlace é a responsável por organizar e garantir que os dados sejam transmitidos corretamente entre o seu computador e o ponto de acesso (o famoso *Access Point*).

Camada 3: rede

A camada de rede se ocupa do roteamento e endereçamento lógico, com o **protocolo IP** sendo o mais conhecido. Ela garante que os pacotes de dados possam viajar entre diferentes redes, decidindo qual é o melhor caminho para chegarem ao destino final.

Quando você acessa um site fora do seu país, por exemplo, os dados precisam ser roteados por várias redes até chegar ao servidor daquele site. A camada de rede utiliza o IP (endereçamento lógico) para identificar a origem e o destino dos pacotes e determinar o caminho mais eficiente. Observe um exemplo prático na Figura 2:

```
C:\Users\edmar>tracert www.google.com

Rastreando a rota para www.google.com
[2800:3f0:4001:834::2004] com no máximo 30 saltos:

 1 21 ms 2 ms 1 ms 2804:14d:902b::3ef
 2 101 ms 10 ms 9 ms 2804:14d:902b::1
 3 13 ms 17 ms 12 ms 2804:14d:9000:189:5:2:139:5
 4 13 ms 17 ms * 2804:a8:2:c2::791
 5 * * * Esgotado o tempo limite do pedido.
 6 * * * Esgotado o tempo limite do pedido.
 7 10 ms * * 2001:4860:1:1::294
 8 8 ms 10 ms 8 ms 2800:3f0:8064::1
```

```
9 12 ms 10 ms 24 ms 2001:4860:0:1::56e8
10 10 ms 11 ms 24 ms 2001:4860:0:1::2201
11 8 ms 11 ms 8 ms 2800:3f0:4001:834::2004
Rastreamento concluído.
```

Figura 2 - Exemplo tracert / Fonte: o autor.

Descrição da Imagem: a figura apresenta uma tela *prompt* de comando do windows exibindo o rastreamento dos pacotes após o comando *tracert*. Fim da descrição..

Abra o terminal <www.google.com> e digite o comando **tracert** (no Windows) ou **traceroute** (no Linux/Mac). Isso vai mostrar o caminho que os pacotes de dados percorrem da sua máquina até o servidor do Google, passando por vários roteadores no meio do caminho. Eles podem ver quantos “*hops*” (saltos) são necessários para que os dados cheguem ao destino, e como a camada de rede faz o roteamento.

Camada 4: transporte

A camada de transporte garante a entrega confiável dos dados entre os dispositivos. Aqui, temos dois protocolos principais: o **TCP** (que oferece uma entrega confiável, com verificação de erros) e o **UDP** (um protocolo mais rápido, mas que não garante a entrega de todos os pacotes).

Vamos conhecer os principais protocolos:

- **TCP (*Transmission Control Protocol*)**: garante a entrega confiável dos dados, retransmitindo pacotes perdidos e organizando-os na ordem correta.
- **UDP (*User Datagram Protocol*)**: oferece um serviço mais simples, sem garantia de entrega, mas com baixa latência, adequado para aplicações em que a velocidade é mais importante que a confiabilidade.



EU INDICO

Faça uma simulação de perda de pacotes para demonstrar a diferença entre TCP e UDP. Uma ideia seria usar ferramentas como **iperf** para simular uma transmissão de dados com TCP e UDP e ver como cada protocolo reage a uma rede com alta latência ou perda de pacotes. Podemos ver como o TCP garante que os dados sejam retransmitidos, enquanto o UDP simplesmente ignora as perdas para manter a fluidez. Acompanhe, por meio do link a seguir, um passo a passo para realizar essa simulação. <https://www.dell.com/support/kbdoc/pt-br/000139427/como-testar-a-largura-de-banda-da-rede-dispon%C3%ADvel-usando-o-iperf>



ZOOM NO CONHECIMENTO

O **protocolo TCP** é utilizado ao enviar um arquivo por e-mail ou ao acessar uma página web. Ele garante que todos os pacotes de dados sejam entregues corretamente e reorganizados na ordem correta. Já o **protocolo UDP** pode ser usado em transmissões ao vivo de vídeo ou áudio, em que alguns pacotes perdidos são aceitáveis desde que a transmissão ocorra em tempo real.

Camada 5: sessão

A camada de sessão gerencia e controla as conexões (sessões) entre dispositivos. Ela garante que as sessões sejam estabelecidas, mantidas durante a transferência de dados e encerradas corretamente.

Quando você se conecta a um servidor de banco de dados, a camada de sessão garante que a comunicação seja estabelecida. Se houver uma interrupção, essa camada pode restabelecer a conexão ou encerrar a sessão corretamente, garantindo a integridade da comunicação.



APROFUNDANDO

No caso de sistemas como o *Remote Desktop Protocol (RDP)*, que permite acesso remoto a outros computadores, a camada de sessão garante que sua sessão seja mantida aberta mesmo se houver pequenos problemas de conexão. Uma forma de você praticar isso seria criar sessões remotas (via RDP ou SSH) e analisar como o sistema reage a quedas temporárias de conexão.

Imagine que você está participando de uma videoconferência. A camada de sessão gerencia essa conexão, garantindo que, se a rede cair por um momento, a comunicação possa ser retomada quando a conexão for restabelecida, sem precisar reiniciar toda a chamada.

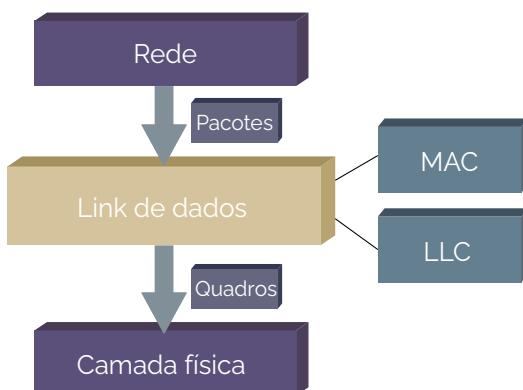


Figura 3 - Camada sessão

Descrição da Imagem: é um modelo de subcamadas de link de dados, um fluxograma com sete retângulos, sendo três grandes, dois médios e dois pequenos. De cima para baixo temos o primeiro retângulo escrito: rede, com uma seta para o segundo retângulo escrito; link de dados, com uma seta para o terceiro retângulo escrito: física. Entre 'rede' e 'física' há dois retângulos pequenos escritos: pacotes e quadros. O retângulo de link de dados é interligado por dois retângulos escritos MAC e LLC. Fim da descrição.



INDICAÇÃO DE FILME

A era dos dados (documentário)

Essa série documental traz informações relacionadas a como os dados se tornaram um recurso valioso e como são coletados, armazenados e usados em nossa sociedade atual. Os episódios exploram o impacto da mineração de dados, da inteligência artificial e do aprendizado de máquina em áreas como política, economia, privacidade e segurança, além de levantar preocupações sobre vigilância e controle.



Considerando a indicação do documentário *A era dos dados*, podemos relacioná-la à camada sessão do modelo OSI, responsável por estabelecer e gerenciar as conexões entre as aplicações.

Camada 6: apresentação

A camada de apresentação é responsável por traduzir os dados entre o formato que o aplicativo entende e o formato utilizado na rede. Ela também lida com a criptografia e a compressão dos dados. Quando você acessa um site seguro usando **HTTPS**, os dados são criptografados na camada de apresentação, ou quando você abre um arquivo de vídeo compactado, essa camada lida com a descompressão, garantindo que o arquivo possa ser reproduzido corretamente.

Para entendermos esse conceito podemos baixar e analisar um certificado SSL de um site usando o navegador, mostrando como a criptografia funciona na camada de apresentação. Podemos usar programas como o Gzip para comprimir e descomprimir arquivos, observando a interação entre essa camada e as aplicações.

Camada 7: aplicação

A camada de aplicação é a interface que os usuários veem. Ela interage diretamente com os aplicativos de rede que usamos diariamente, como navegadores web, clientes de e-mail, e serviços de mensagens.

 ZOOM NO CONHECIMENTO

O protocolo HTTP, usado para navegação na web, é um exemplo clássico da camada de aplicação. Ao digitar o endereço de um site no navegador, o HTTP transmite a solicitação ao servidor web, que responde enviando a página desejada. Outro exemplo é o protocolo SMTP, que permite o envio de e-mails.

Como vimos, o Modelo OSI divide a comunicação em sete camadas, e cada uma desempenha um papel fundamental para garantir que a comunicação funcione de ponta a ponta. Desde a transmissão física dos dados até a interação final do usuário, cada camada é interdependente, garantindo que a troca de informações aconteça de forma organizada, segura e eficiente.



MODELO TCP/IP

O **Modelo TCP/IP** é mais prático e usado amplamente para a interconexão de redes, especialmente na Internet. Ao contrário do modelo OSI, ele possui apenas **quatro camadas**, que agrupam funções de forma mais simplificada.

Camada 1: enlace

Consideremos a Camada de Enlace como a base da comunicação em redes. Sabe quando você envia uma mensagem de texto pelo seu smartphone, e ela chega rapidinho ao destinatário? Essa camada está por trás de tudo, garantindo que os dados sejam transmitidos de um dispositivo para outro, seja por um cabo *Ethernet*, seja por Wi-Fi. Ela cuida do ‘como’ os bits de dados se movem de uma máquina para a outra.

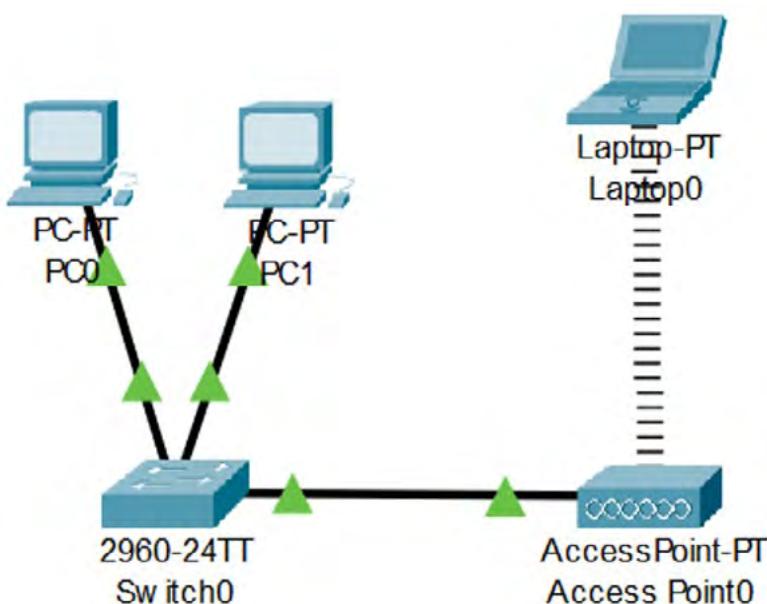


Figura 4 - Visão geral da rede / Fonte: o autor.

Descrição da Imagem: a figura apresenta a visão geral de uma rede com dois computadores conectados a um switch, e um laptop conectado ao access point. Fim da descrição.

A função principal da Camada de Enlace é garantir que os dados que trafegam entre dois dispositivos em uma mesma rede cheguem corretamente. Para isso, ela precisa lidar com alguns desafios, como detectar e corrigir erros de transmissão. Imagine um trem de bits correndo nos trilhos, e a Camada de Enlace é quem garante que o trem chegue intacto ao destino, sem perder vagões (ou bits) no caminho.

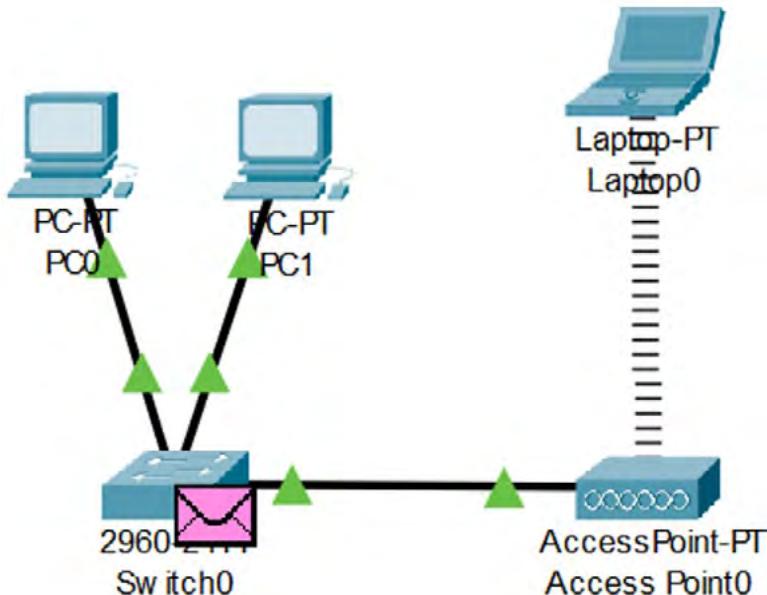


Figura 5 - Dados trafegando / Fonte: o autor.

Descrição da Imagem: a figura apresenta os dados enviando e trafegando de um computador ao switch, sendo enviado ao access point e redirecionado ao laptop. Fim da descrição.

Um exemplo clássico dessa camada em ação é o **protocolo Ethernet**. Quando você conecta seu computador à internet por um cabo, é a *Ethernet* que está cuidando de todo o processo de envio e recepção de dados, transformando-os em sinais elétricos que viajam pelos fios. Já quando você usa Wi-Fi, a lógica é similar, mas, em vez de sinais elétricos, a comunicação ocorre por meio de ondas de rádio.

Se a Camada de Enlace falhar, toda a comunicação entre os dispositivos conectados à rede local pode ser prejudicada. Pense nos erros de transmissão como um ruído no telefone. Se houver interferência demais, a mensagem não será entendida corretamente. É aqui que entra a detecção e a correção de erros dessa camada. Protocolos como o CSMA/CD no *Ethernet*, por exemplo, evitam colisões, assegurando que dois dispositivos ou mais não enviem dados ao mesmo tempo na rede e, caso ocorra um conflito, eles ajustem o envio para tentar novamente.

A Camada de Enlace é fundamental para a comunicação local em qualquer rede. Ela é o alicerce sobre o qual as camadas superiores, como a Camada de Rede (que lida com o roteamento de pacotes), se apoiam. Sem ela, a comunicação entre dispositivos na mesma rede seria caótica.

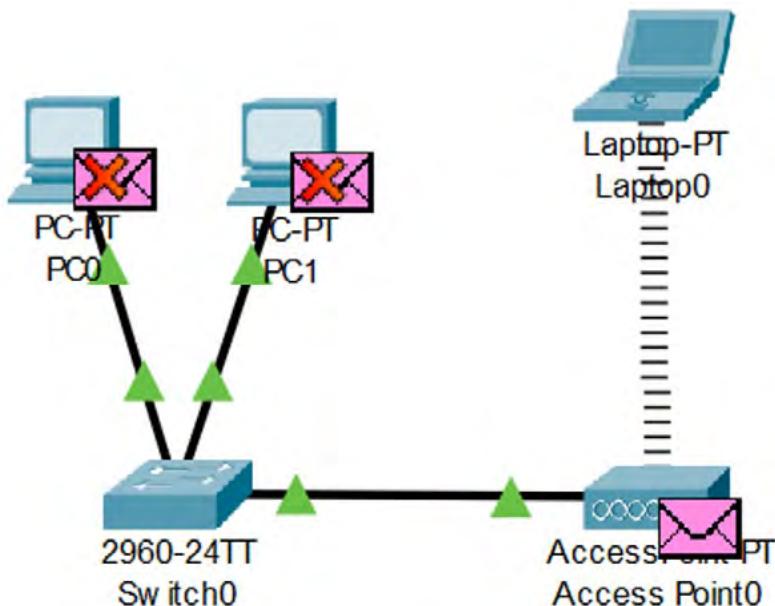


Figura 6 - Entrega dos dados / Fonte: o autor.

Descrição da Imagem: a figura apresenta a entrega dos dados. São dois pacotes de dados que falharam ao chegarem no destino, sendo enviados do switch aos computadores. Fim da descrição.

Então, toda vez que sua internet parece mais lenta, ou quando um arquivo não chega corretamente ao destino, pode haver algo relacionado à Camada de Enlace. E é por isso que estudar seus protocolos, como *Ethernet* e *Wi-Fi*, é essencial para quem quer se aprofundar no mundo das redes.

Camada 2: internet

Agora que chegamos à Camada de Internet, falaremos da sua principal função: endereçamento lógico e roteamento de pacotes de dados. Mas o que isso signi-

fica na prática? Imagine que os dados são como cartas que precisam chegar ao destino correto. Aqui, essa camada é o carteiro inteligente que decide o melhor caminho para entregar essas cartas, mesmo que o destinatário esteja em outro bairro, cidade ou até mesmo país!

A Chave para o Roteamento é o Protocolo IP. O protagonista dessa camada é o IP (Internet Protocol). Esse protocolo é responsável por atribuir um endereço IP a cada dispositivo conectado à rede. Pense no endereço IP como o CEP digital que identifica de maneira única computadores, smartphones e até impressoras na rede. Sem esse número, seria impossível enviar dados de um ponto ao outro com segurança.

Endereços IP são formados por sequências numéricas (no formato IPv4, algo como 192.168.0.1") ou alfanuméricas (no caso do IPv6). Esses números identificam onde seu dispositivo está na grande teia da Internet.

O Que acontece quando você acessa um site? Faremos agora uma pequena jornada. Quando você digita www.google.com no navegador, a seguinte sequência de eventos acontece:

- Seu computador envia uma solicitação (um pacote de dados) pedindo para acessar o site.
- O protocolo IP entra em ação, atribuindo ao seu computador um endereço de origem (seu endereço IP) e ao servidor do Google um endereço de destino (o IP do servidor).
- Esses pacotes são então roteados por vários dispositivos, como roteadores, até alcançarem o servidor correto.
- Uma vez que o servidor responde, ele faz o caminho inverso: os pacotes retornam para seu computador por meio do roteamento IP.



APROFUNDANDO

Agora, o que é o **roteamento**? Imagine que a Internet é como uma série de estradas conectando diferentes cidades (as redes). O roteador é como uma central de transporte que decide qual é a melhor 'estrada' para seus pacotes que seguem até o destino. Esses roteadores trocam informações constantemente para garantir que seus dados cheguem o mais rápido possível, desviando até de 'estradas congestionadas' (rotas lentas ou sobrecarregadas).

Se você já configurou uma rede Wi-Fi em casa, talvez tenha visto números como ‘192.168.1.1’ no seu roteador. Isso é um endereço IP privado, utilizado apenas dentro da sua rede doméstica. Seu roteador usa esse IP para se comunicar com os dispositivos da sua casa. Quando você acessa a Internet, o roteador atribui um endereço IP público (fornecido pelo provedor de Internet) para que você possa se comunicar com redes externas. Aqui, os pacotes são roteados para fora, passando pelos provedores e chegando ao destino final.

Agora pense em um roteador corporativo que precisa gerenciar centenas ou até milhares de endereços IP em uma empresa. Ele deve garantir que cada dispositivo, seja um computador no departamento de vendas ou um servidor em TI, tenha um IP único e que os pacotes de dados sejam enviados corretamente, sem que haja conflitos de endereços.

Além do IP, temos outros protocolos que trabalham em conjunto para garantir que os dados cheguem ao destino correto, são os **Protocolos Auxiliares**:

ZOOM NO CONHECIMENTO

ICMP (*Internet Control Message Protocol*): ele é o responsável por ferramentas como o ping. O ping serve para testar se um dispositivo está acessível na rede. Se você pingar o IP de um servidor e ele responder, isso significa que a rota está funcionando.

ARP (*Address Resolution Protocol*): traduz endereços IP para endereços MAC (endereços físicos das placas de rede), possibilitando que os dados cheguem ao destino correto dentro de uma rede local.

A Camada de Internet é o núcleo da comunicação global. Sem o IP, não haveria como as máquinas se identificarem, e sem o roteamento, os dados ficariam perdidos, sem saber para onde ir. Ao entender como essa camada funciona, os alunos se capacitam a resolver problemas como conflitos de IP, além de otimizar o roteamento em redes corporativas e pessoais.

**A Camada de Internet
é o núcleo da
comunicação global**

Camada 3: transporte

Imagine que você está enviando um pacote muito importante pelo correio. Quer garantir que ele chegue ao destino, completo e sem erros, certo? A Camada de Transporte em uma rede funciona exatamente assim: ela garante a entrega de dados de ponta a ponta, controlando se os pacotes chegam no destino, em ordem e sem falhas. Vamos conhecer os dois protocolos principais dessa camada – TCP e UDP – e entender como cada um lida com essa responsabilidade de maneira diferente.

TCP (*Transmission Control Protocol*) se refere à prioridade para a confiabilidade. O TCP é aquele mensageiro super cuidadoso. Ele garante que cada parte da informação (ou pacotes, no mundo digital) chegue completa e na sequência correta ao destino. O mais interessante sobre o TCP é a sua confiabilidade.

Pense em uma situação em que você está baixando um documento importante, como uma proposta de trabalho ou um software. O TCP age dividindo o arquivo em pequenos pedaços, chamados de pacotes, e realiza três ações principais:

CONFIRMA A ENTREGA

Para cada pacote enviado, ele espera uma confirmação (ACK) do destinatário dizendo: 'Sim, recebi!'. Caso essa confirmação não chegue, o TCP retransmite o pacote.

ORGANIZA OS PACOTES

Quando os pacotes chegam, o TCP reordena tudo antes de entregar o conteúdo para a aplicação. Isso significa que mesmo que os pacotes cheguem fora de ordem, o usuário recebe o arquivo final de forma correta.

GARANTE INTEGRIDADE

Se algum pacote se corromper ou se perder no caminho, o TCP detecta e envia novamente a parte que deu errado.

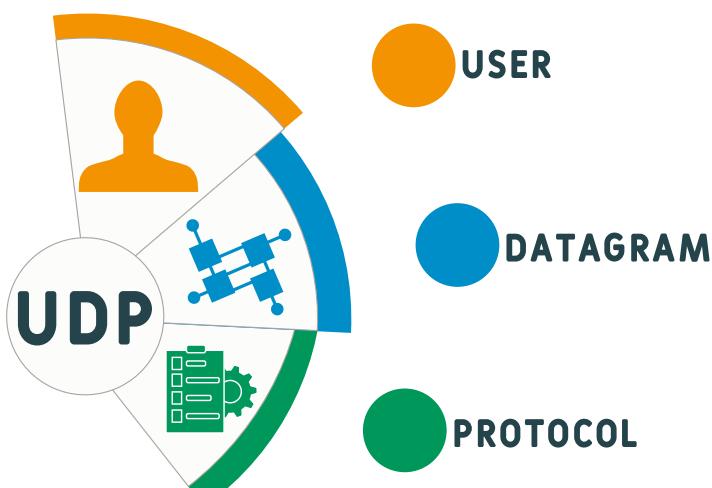
Quanto ao **Download de um arquivo**, imagine que você está baixando um grande arquivo de vídeo de um site. O TCP vai dividir esse vídeo em vários pacotes e enviar um a um. Se qualquer um desses pacotes se perder ou chegar corrompido, ele vai transmitir novamente até que todos cheguem ao destino em perfeita ordem.

O download só é finalizado quando todos os pacotes chegam, garantindo que o vídeo possa ser reproduzido sem falhas. Esse é o exemplo clássico de como o TCP é utilizado para garantir que cada byte de informação chegue corretamente.

UDP (User Datagram Protocol), aqui a pressa é prioridade. Agora, nem sempre você precisa de tanta confiabilidade. Às vezes, a velocidade é mais importante que a precisão total. Imagine uma chamada de vídeo ou uma partida de jogo on-line – você quer que a comunicação seja rápida, mesmo que uma pequena parte dos dados não chegue. É aqui que entra o UDP.

Ao contrário do TCP, o UDP:

- **Não verifica a entrega:** ele envia pacotes e não espera uma confirmação de recebimento. Isso o torna muito mais rápido.
- **Não reorganize os pacotes:** se os pacotes chegarem fora de ordem ou alguns perderem, ele não se preocupa em ordená-los. Isso pode resultar em pequenas falhas visuais ou sonoras, mas a velocidade da comunicação é mantida.
- **Entrega sem garantias:** em uma transmissão ao vivo, por exemplo, perder alguns pacotes não compromete tanto a experiência quanto atrasá-la.



A Camada 3 é o transporte que se refere ao centro da comunicação confiável (ou veloz) em redes modernas. Entender o TCP e o UDP permite aos profissionais de TI tomar decisões informadas sobre como projetar e otimizar a comunicação de dados. No final, o segredo é saber quando priorizar a confiabilidade (TCP) e quando a rapidez (UDP) deve ser o foco. Em um mundo cada vez mais conectado, esse conhecimento prático faz toda a diferença na construção de redes eficientes e funcionais.

Camada 4: aplicação

Agora chegamos à camada mais próxima de nós, usuários: a Camada de Aplicação. É aqui que a ‘mágica’ acontece, em que nós, seres humanos, interagimos diretamente com a rede por intermédio de programas e serviços. Essa camada não lida com pacotes de dados, endereços IP, ou roteamento, mas sim com a experiência que temos ao navegar na web, enviar e-mails, transferir arquivos, entre outros. Mas o que isso significa na prática? Vamos descobrir!

A Função da Camada de Aplicação é o ponto em que a rede encontra o usuário.

A principal função da Camada 4 é fazer a “ponte” entre os serviços da rede e os programas que usamos. Quando você entra em um site, envia um e-mail ou baixa um arquivo, o que realmente está acontecendo por trás dessas ações é que os protocolos dessa camada estão se comunicando com servidores, garantindo que os dados sejam entregues de uma maneira que possamos entender e utilizar. E quais são esses protocolos?

Vamos explorar três dos mais conhecidos:

HTTP/HTTPS (HYPERTEXT TRANSFER PROTOCOL / SECURE HTTP)

O protocolo usado para navegação web.

SMTP (SIMPLE MAIL TRANSFER PROTOCOL)

O protocolo que gerencia o envio de e-mails.

FTP (FILE TRANSFER PROTOCOL)

Usado para transferir arquivos entre computadores.

■ Exemplo 1: HTTP/HTTPS – Navegação na Web.

Imagine que você quer acessar o site da sua universidade. Você abre o navegador, digita o URL e aperta ‘Enter’. O que acontece a seguir?

- **Você digita a URL (por exemplo, www.universidade.com):** neste momento, o seu navegador inicia uma comunicação utilizando o HTTP (ou HTTPS, se o site for seguro). Esse protocolo faz uma solicitação ao servidor em que o site está hospedado, pedindo para ‘ver’ o conteúdo.
- **O servidor responde:** o servidor envia de volta os arquivos que formam a página, incluindo textos, imagens, vídeos e mais.
- **O navegador exibe o conteúdo:** o navegador interpreta esses arquivos e monta o site que você vê na tela. Nesse processo, o protocolo HTTP (ou HTTPS) foi o responsável pela troca de dados entre o seu computador e o servidor.

Quanto à Segurança do HTTPS, refletamos: você já reparou que alguns sites mostram um cadeado no navegador? Isso significa que eles estão usando o HTTPS, que é o HTTP combinado com uma camada de segurança chamada SSL/TLS. Ele garante que os dados trocados entre você e o site sejam criptografados, ou seja, seguros contra interceptação. Esse protocolo é essencial em sites de compras on-line, bancos e qualquer outro lugar em que informações sensíveis são trocadas.

■ Exemplo 2: SMTP – Envio de E-mails.

Agora, veremos como funciona o SMTP mediante uma situação do cotidiano: o envio de um e-mail.

- **Você escreve um e-mail:** imagine que você está enviando uma mensagem para um colega de trabalho. Depois de digitar o conteúdo e clicar

em Enviar, inicia o protocolo SMTP, o qual trabalha para garantir que a mensagem seja entregue ao destinatário.

- **O e-mail é enviado para o servidor SMTP:** o e-mail primeiro passa pelo servidor SMTP do seu provedor (como Gmail ou Outlook), que verifica o endereço de e-mail do destinatário e tenta encontrar o caminho mais rápido e eficiente para entregar a mensagem.
- **Entrega ao servidor de destino:** o servidor SMTP do remetente se comunica com o servidor do destinatário (o provedor de e-mail de quem vai receber), e se tudo estiver funcionando corretamente, o e-mail é entregue na caixa de entrada.

O Papel do SMTP e a Entrega de E-mails é primordial, pois garante que os e-mails sejam entregues da maneira mais eficiente possível, mas ele também depende de outros protocolos, como o POP3 ou IMAP, que são responsáveis por baixar ou sincronizar os e-mails no dispositivo do destinatário. Esses protocolos complementares fazem parte da camada de aplicação, garantindo uma comunicação eficiente entre servidores e dispositivos.

- **Exemplo 3: FTP – Transferência de Arquivos.**

Por último, apresentamos o FTP, um protocolo clássico usado para transferir arquivos entre dispositivos. Imagine que você está trabalhando em um projeto colaborativo e precisa enviar um arquivo grande para um servidor a fim de que outros membros da equipe possam acessá-lo.

- **Você usa um cliente FTP:** existem programas específicos (clientes FTP) que permitem que você selecione um arquivo e envie para um servidor remoto.
- **O FTP se conecta ao servidor:** o cliente FTP se conecta ao servidor de destino usando o protocolo FTP, e assim a conexão é estabelecida, você pode começar a enviar o arquivo.
- **Envio e recebimento de arquivos:** o FTP facilita a troca de arquivos grandes, permitindo não apenas enviar, mas também baixar arquivos do servidor. Empresas que trabalham com grandes volumes de dados, como agências de design ou desenvolvimento de software, muitas vezes, utilizam esse protocolo.

- **Exemplo Prático: usando o FTP para Transferência de Arquivos.**

Imagine que você faz parte de uma equipe de design e precisa compartilhar arquivos pesados, como vídeos ou imagens em alta resolução, com os colegas. O objetivo é enviar esses arquivos para um servidor central em que todos os membros possam acessá-los e baixá-los quando precisarem.

Passo a passo de como isso funciona:

- **Escolha de um Cliente FTP:** para começar, você escolhe um programa cliente FTP, como o **FileZilla**, uma ferramenta popular e gratuita. Esse cliente FTP permite que você se conecte a servidores remotos e envie ou receba arquivos facilmente.
- **Conexão ao Servidor:** ao abrir o FileZilla, você precisará fornecer algumas informações:
- **Endereço do servidor FTP:** esse endereço é geralmente fornecido pelo administrador do servidor e pode se parecer com **ftp.exemplo.com**.
- **Nome de usuário e senha:** para garantir a segurança dos dados, o acesso geralmente é protegido por um login.
- **Porta de conexão:** normalmente, o FTP usa a porta 21 para estabelecer conexões.
- **Navegação e Seleção de Arquivos:** assim que a conexão for estabelecida, você verá duas partes na interface do FileZilla: uma representa os arquivos do seu computador (à esquerda) e a outra representa os arquivos no servidor remoto (à direita). Agora, você pode navegar nas pastas locais, selecionar os arquivos que deseja compartilhar e arrastá-los para a seção do servidor.
- **Transferência de Arquivos:** ao arrastar e soltar o arquivo, o FTP inicia o processo de transferência. Dependendo do tamanho dos arquivos e da velocidade de conexão, isso pode demorar alguns minutos. O cliente FTP mostrará o progresso para cada arquivo transferido.
- **Acesso dos Colegas aos Arquivos:** uma vez no servidor, seus colegas de equipe também poderão usar o FileZilla (ou outro cliente FTP) para acessar o servidor, visualizar e baixar esses arquivos. Isso facilita o trabalho colaborativo, especialmente com arquivos grandes que seriam difíceis de enviar por e-mail.

- **Baixar Arquivos do Servidor:** além de enviar, você também pode baixar arquivos do servidor para o seu computador. É útil caso algum colega faça alterações em um projeto compartilhado e envie a versão atualizada para o servidor.

Um ponto importante sobre **FTP e Segurança** é que ele, por padrão, não criptografa os dados enviados. Isso significa que se você estiver enviando informações sensíveis, o FTP pode não ser a melhor escolha. Felizmente, existem variações mais seguras, como o SFTP (*Secure File Transfer Protocol*) que usa criptografia para proteger os dados.

O modelo TCP/IP é mais simples e direto, agrupando algumas funções do modelo OSI. Ele foi criado especificamente para suportar a interconexão de redes, especialmente na Internet, e é amplamente adotado em redes modernas. Segundo Comer (2016, p. 87), “a importância de revisitar esses modelos está no fato de que, mesmo com o surgimento de novas tecnologias e arquiteturas, eles ainda são utilizados como referência no ensino e na prática de redes.” Eles fornecem uma base sólida para entender as interações entre diferentes dispositivos e protocolos, seja em redes locais ou na Internet global.



ENTENDER DE ARQUITETURAS DE REDE MODERNAS

As **arquiteturas de redes** evoluíram significativamente, e com isso surgiram novas arquiteturas que buscam resolver desafios contemporâneos, como a crescente demanda por alta velocidade, flexibilidade e segurança.

Mais duas das tecnologias-chave que revolucionaram essas arquiteturas são as Redes Definidas por Software (SDN) e a *Network Functions Virtualization* (NFV). Ambas trabalham para melhorar a eficiência e a flexibilidade, mas têm diferentes funções (Kurose; Ross, 2021). Observemos o Quadro 1.

REDES DEFINIDAS POR SOFTWARE (SDN)	<i>NETWORK FUNCTIONS VIRTUALIZATION (NFV)</i>
<p>Função: SDN é uma abordagem moderna para redes em que o controle da rede (decisões de roteamento e políticas) é separado da infraestrutura física (<i>switches</i> e roteadores). O SDN permite que a rede seja programada centralmente, facilitando o gerenciamento e a automação.</p>	<p>Função: NFV separa as funções de rede (como <i>firewalls</i>, roteadores e平衡adores de carga) do hardware específico, permitindo que essas funções sejam executadas em servidores genéricos e virtualizados.</p>
<p>Exemplo: em um ambiente de data center, um controlador SDN pode alterar dinamicamente a rota de pacotes para balancear a carga entre diferentes servidores sem a necessidade de modificar fisicamente a rede.</p>	<p>Exemplo: um <i>firewall</i> que antes era um dispositivo físico agora pode ser um software que roda em uma máquina virtual, facilitando sua implantação e escalabilidade.</p>

Quadro 1 - Diferenças entre SDN x NFV / Fonte: o autor.

EXPLORAR TECNOLOGIAS DE **EDGE COMPUTING** E **FOG COMPUTING**

Com o crescimento da **Internet das Coisas (IoT)** e a necessidade de processamento em tempo real, surgem novos paradigmas como **Edge Computing** e **Fog computing**. Ambos focam em trazer o processamento de dados para mais perto da fonte, reduzindo a latência e o consumo de largura de banda. Observe o Quadro 2.

EDGE COMPUTING	FOG COMPUTING
<p>Função: o <i>Edge Computing</i> move o processamento de dados para mais próximo da fonte de geração de dados (como sensores IoT), ao invés de enviar todos os dados para servidores na nuvem.</p>	<p>Função: uma extensão do <i>Edge Computing</i>, o <i>Fog computing</i> distribui o processamento, armazenamento e redes entre a borda (<i>edge</i>) e a nuvem, criando uma infraestrutura descentralizada.</p>
<p>Exemplo: em uma fábrica, sensores de máquinas podem processar dados localmente para detectar falhas em tempo real, sem precisar depender da latência da nuvem.</p>	<p>Exemplo: em uma rede de energia inteligente, dispositivos de <i>fog computing</i> podem tomar decisões locais sobre o uso de energia, ao mesmo tempo que se comunicam com a nuvem para otimizar a eficiência global.</p>

Quadro 2 - Diferenças entre *Edge Computing* e *Fog computing* / Fonte: o autor.

COMPUTAÇÃO EM BORDA (EDGE COMPUTING) E CLOUD COMPUTING

A Computação em Nuvem (*Cloud Computing*) continua a ser uma peça-chave para o armazenamento e processamento de grandes volumes de dados. No entanto, a crescente demanda por processamento local trouxe a computação de borda como complemento.



 ZOOM NO CONHECIMENTO

Edge Computing: foca no processamento local dos dados para reduzir a latência e minimizar a dependência da nuvem.

Cloud Computing: oferece armazenamento e processamento centralizados na nuvem, escaláveis e acessíveis de qualquer lugar, mas com maior latência em comparação ao Edge.

Exemplo: em carros autônomos, o *Edge Computing* processa informações críticas, como a detecção de obstáculos, diretamente no veículo, enquanto a *Cloud Computing* armazena e processa grandes volumes de dados sobre rotas e padrões de tráfego para análises posteriores.

O avanço das arquiteturas de rede modernas e o uso de tecnologias como SDN, NFV, *Edge Computing* e *Cloud Computing* têm transformado o modo como as redes são planejadas e operadas. Esses conceitos não apenas facilitam o gerenciamento e a expansão das redes, mas também oferecem soluções inovadoras para os desafios atuais, como a latência, a escalabilidade e a eficiência de processamento. Segundo Kurose e Ross (2021, p. 125), “ao compreender essas tecnologias e saber aplicá-las, os profissionais de redes estarão prontos para enfrentar os desafios de um mundo cada vez mais conectado e demandante de respostas rápidas.”

Essa afirmação reforça o papel essencial que o conhecimento sólido sobre redes desempenha no cenário atual. Não basta apenas conhecer a teoria; é preciso estar preparado para colocar esse conhecimento em prática de forma estratégica e eficiente, adaptando-se às constantes inovações tecnológicas.

Portanto, à medida que o mercado exige cada vez mais soluções ágeis e robustas, o profissional de TI que dominar essas ferramentas será capaz de projetar e manter infraestruturas que atendam às crescentes demandas de conectividade e segurança. Dessa forma, estar atualizado com as tecnologias emergentes, como SDN, *Cloud Computing* e *Edge Computing*, se torna não apenas uma vantagem competitiva, mas uma necessidade para sobreviver e prosperar em um ambiente digital em rápida transformação.

**É preciso estar preparado
para colocar esse
conhecimento em prática**

 **EM FOCO**

Estudante, acreditamos que essa aula complementará e aprofundará ainda mais o seu entendimento sobre o tema. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

NOVOS DESAFIOS

Agora refletiremos um pouco sobre o que exploramos até aqui sobre redes, começando pelos modelos OSI e TCP/IP. O modelo OSI é um mapa teórico para entender o fluxo de dados em camadas, enquanto o TCP/IP é um modelo prático e amplamente usado. Além disso, aborda inovações como Redes Definidas por Software (SDN), Virtualização de Funções de Rede (NFV), *Edge Computing* e *Cloud Computing*. Essas tecnologias modernas tornam as redes mais ágeis e flexíveis, permitindo que grandes empresas automatizem a gestão de redes, reduzindo custos e aumentando a velocidade de resposta às novas demandas.

Profissionais de redes enfrentam o desafio de gerenciar infraestruturas complexas, exigindo rapidez, segurança e adaptabilidade. Entender modelos como OSI e TCP/IP é essencial para diagnosticar problemas e melhorar o desempenho. Com o avanço de tecnologias como *Edge* e *Cloud Computing* e a expansão da Internet das Coisas (IoT), dominar esses conceitos se torna um diferencial, especialmente com o 5G e o aumento de dispositivos conectados.

Então, se você está pensando em ingressar ou já está trilhando seu caminho no mundo das redes, tenha em mente que o conhecimento adquirido prepara os profissionais para resolver problemas e inovar, sendo valioso tanto em grandes corporações quanto em startups no contexto da transformação digital. Com as mudanças que estão por vir, como o 5G e a expansão do IoT, esse conhecimento será ainda mais valioso.

Profissionais de redes enfrentam o desafio de gerenciar infraestruturas

VAMOS PRATICAR

1. O Modelo OSI (*Open Systems Interconnection*) é uma estrutura teórica que define como os dados são transmitidos e recebidos em redes de computadores, dividindo o processo em sete camadas, cada uma com funções específicas (Benedetti; Anderson, 2010).

Com base no funcionamento da Camada Física do modelo OSI, qual das seguintes alternativas não descreve corretamente o papel dessa camada?

- a) A Camada Física lida com a transmissão de bits através de meios físicos, como cabos de cobre ou fibras ópticas.
 - b) A Camada Física trata da definição das características elétricas e mecânicas dos meios de transmissão.
 - c) A Camada Física é responsável pelo roteamento dos pacotes de dados entre diferentes redes.
 - d) Em uma rede *Ethernet*, a Camada Física transmite sinais elétricos ou de luz ao longo do meio de comunicação.
 - e) A Camada Física garante a transmissão correta de bits, independentemente do meio físico utilizado.
-
2. Redes Definidas por Software (SDN) e *Network Functions Virtualization* (NFV) são duas abordagens inovadoras que mudaram a maneira como as redes são gerenciadas. SDN separa o controle da rede da infraestrutura física, permitindo que o controle seja programado de forma centralizada. NFV, por outro lado, desvincula as funções de rede do hardware específico, permitindo que sejam executadas em servidores virtualizados, oferecendo mais flexibilidade e escalabilidade (Kurose; Ross, 2021).

Considere as seguintes afirmativas sobre SDN e NFV:

- I - NFV permite que as funções de rede sejam executadas exclusivamente em hardware dedicado para maior desempenho.
- II - NFV elimina a necessidade de hardware específico, virtualizando funções de rede como firewalls e roteadores.
- III - No SDN, o controle de rede é centralizado e separado da infraestrutura física.
- IV - SDN facilita a automação e o gerenciamento dinâmico da rede.

VAMOS PRATICAR

É correto o que se afirma em:

- a) I, apenas.
 - b) II e IV, apenas.
 - c) III e IV, apenas.
 - d) I e III, apenas.
 - e) I, II, III e IV.
3. Com o aumento do uso de Internet das Coisas (IoT), paradigmas como *Edge Computing* e *Fog computing* têm sido desenvolvidos para trazer o processamento de dados para mais próximo da origem, diminuindo a latência e o consumo de largura de banda. O *Edge Computing* processa dados localmente, na borda da rede, enquanto o *Fog computing* é uma extensão do edge, distribuindo o processamento entre a borda e a nuvem, criando uma infraestrutura mais descentralizada e eficiente (Kurose; Ross, 2021).

Sobre os paradigmas Edge Computing e Fog computing, considere as seguintes afirmativas:

- I - *Edge Computing* processa dados na borda da rede, próximo da fonte de geração, sem depender da nuvem.
- II - *Fog computing* distribui o processamento entre a borda da rede e a nuvem, criando uma estrutura híbrida.
- III - *Fog computing* pode melhorar a eficiência de redes IoT ao permitir decisões locais e otimizar recursos globais.
- IV - *Edge Computing* é uma tecnologia dependente de processamento centralizado na nuvem.

É correto o que se afirma em:

- a) I e IV, apenas.
- b) II e III, apenas.
- c) III e IV, apenas.
- d) I, II e III, apenas.
- e) II, III e IV, apenas.

REFERÊNCIAS

BENEDETTI, R.; ANDERSON, AL. **Use a cabeça!** Redes de computadores. Rio de Janeiro: Rio de Janeiro: Alta Books. 2010.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet:** uma abordagem top-down. Londres: Pearson. 2021.

FOROUZAN, B. A.; MOSHARRAF, F. **Redes de computadores:** uma abordagem top-down. Porto Alegre: AMGH. 2012.

COMER, D. E. **Redes de computadores e internet.** Porto Alegre: Bookman. 2016.

TORRES, G. **Redes de computadores.** Rio de Janeiro: Nova terra. 2016.

CONFIRA SUAS RESPOSTAS

1. Alternativa C.

A Camada Física cuida apenas da transmissão de bits (0s e 1s) através do meio de comunicação, sem qualquer envolvimento no roteamento ou no controle do fluxo de pacotes. Ela se ocupa de características elétricas e mecânicas do meio de transmissão, garantindo que os bits sejam enviados de maneira correta entre dispositivos.

2. Alternativa C.

A afirmativa III está correta, pois o controle da rede no SDN é, de fato, centralizado e separado da infraestrutura física.

A afirmativa IV está correta, já que o SDN facilita o gerenciamento e automação dinâmica da rede, permitindo mudanças rápidas e eficientes.

3. Alternativa D.

A afirmativa I está correta, pois o *Edge Computing* processa dados localmente, próximo da fonte de geração, como em sensores IoT.

A afirmativa II está correta, já que o *Fog computing* distribui o processamento entre a borda da rede e a nuvem, criando uma infraestrutura híbrida e descentralizada.

A afirmativa III está correta, pois o *Fog computing* permite decisões locais e pode melhorar a eficiência de redes IoT, otimizando o uso de recursos globais.

A afirmativa IV está incorreta, pois o *Edge Computing* é caracterizado pela independência da nuvem, ao contrário do processamento centralizado.



TEMA DE APRENDIZAGEM 5

SEGURANÇA EM REDES

MINHAS METAS

- Compreender os Princípios de Segurança em Redes.
- Explorar Criptografia e Autenticação Avançada.
- Implementar *Firewalls*, IDS/IPS e Segurança de Endpoint.
- Desenvolver e aplicar Políticas de Segurança de Rede.
- Avaliar a segurança em Redes Sem Fio.
- Entender e utilizar *Threat Intelligence* (Inteligência de Ameaças).
- Aplicar *Machine Learning* em Segurança de Redes.

INICIE SUA JORNADA

Vamos conversar sobre um tema que tem ganhado cada vez mais relevância: **a segurança em redes**. No cenário atual, em que as tecnologias avançam a passos largos e a digitalização permeia todos os processos, garantir a segurança se tornou uma prioridade não só para as grandes corporações, mas também para as pequenas empresas.

VOCÊ SABE RESPONDER?

Você já parou para pensar nos ataques cibernéticos que ocorrem diariamente?

Vazamentos de dados, *ransomware* e invasões de sistemas são só algumas das ameaças que todos enfrentamos. No entanto, você pode se perguntar: em um ambiente em que a troca de informações é constante e tão valiosa, como podemos assegurar que essas transações sejam seguras? E o que está realmente em jogo quando dados pessoais ou corporativos são expostos a ataques? Essas são questões cruciais que nós, profissionais de TI, devemos enfrentar para proteger nossos ativos digitais.

A segurança em redes vai muito além de um mero aspecto técnico. É, na verdade, uma responsabilidade profissional fundamental. Profissionais de TI, sejam desenvolvedores, administradores de rede ou analistas de segurança, precisam reconhecer que os princípios de segurança não são apenas teóricos.

Eles são práticas indispensáveis que nos protegem contra perdas financeiras, danos à reputação e violações de privacidade. Por isso, dominar temas como criptografia, autenticação avançada, políticas de segurança e a implementação de *firewalls*, IDS/IPS é essencial. Isso permite que você, como futuro profissional, atue de forma estratégica, contribuindo para a criação de um ambiente digital seguro e resiliente.

**A segurança em redes
vai muito além de um
mero aspecto técnico**

**PLAY NO CONHECIMENTO**

Vamos explorar o que é **Cibersegurança**, o que é **Segurança da Informação**, como essas áreas estão conectadas, os desafios enfrentados atualmente, e o que podemos fazer para garantir que nossas informações permaneçam seguras na era digital. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

O que podemos fazer na prática? Durante este curso, você terá a oportunidade de vivenciar a aplicação de diversas ferramentas de segurança de rede, como **firewalls** e sistemas de prevenção de intrusões. Poderá simular ambientes de rede e testar a eficácia de técnicas de criptografia e autenticação em diferentes cenários. Essas experiências práticas são fundamentais! Elas ajudam a solidificar os conceitos e mostram como essas tecnologias se aplicam diretamente ao seu futuro ambiente de trabalho.

A segurança em redes está em constante evolução. Novas ameaças surgem e as tecnologias avançam a cada dia. Por isso, a reflexão sobre os impactos das políticas de segurança, o uso de inteligência de ameaças (*Threat Intelligence*) e até mesmo a aplicação de *Machine Learning* para a detecção de ataques deve ser contínua. Como futuros profissionais de TI, é essencial que você pense criticamente em como equilibrar segurança com usabilidade e como contribuir para um ambiente digital mais seguro.

Por fim, lembre-se: a reflexão sobre os impactos éticos e legais de suas decisões na área de segurança é fundamental. Isso garantirá que você atue de maneira responsável e proativa no mercado. Está preparado para essa jornada? Vamos juntos explorar o fascinante mundo da segurança em redes!

VAMOS RECORDAR?

Um dos pontos importantes na Segurança em Redes hoje é a utilização do *Machine Learning*. Portanto, é interessante explorarmos e entendermos um pouco esse fundamento, acompanhe o link a seguir. <https://www.youtube.com/watch?v=oPrOA2JK6GQ>

DESENVOLVA SEU POTENCIAL

INTRODUÇÃO AOS PRINCÍPIOS DE SEGURANÇA EM REDES

Estudante, a segurança em redes, especialmente em ambientes digitais e corporativos, é fundamentada em três princípios centrais conhecidos como a Tríade CIA: Confidencialidade, Integridade e Disponibilidade (Barreto; Zanin; Saraiva, 2018). Observe a seguir esses princípios na Figura 1:



Figura 1 - Tripé da Segurança / Fonte: Barreto et al. (2018, on-line).

Descrição da Imagem: a figura apresenta um triângulo maior dividido em três outros que representam o tripé da segurança: Confidencialidade, Integridade e Disponibilidade. No centro do triângulo maior há um triângulo invertido escrito: Tripé da segurança, ligado aos outros três triângulos. Fim da descrição..

Esses pilares não apenas guiam a criação de políticas de segurança, mas também são a base de qualquer arquitetura de segurança cibernética robusta (Barreto; Zanin; Saraiva, on-line). Vamos explorar em profundidade cada um desses elementos, sua aplicação prática, ameaças associadas e as contramedidas adequadas.

A **confidencialidade** é o princípio que garante que a informação sensível só seja acessada por aqueles que têm permissão adequada. Isso significa que indivíduos não autorizados não podem visualizar, copiar ou interceptar dados. A confidencialidade é crítica para proteger informações privadas, financeiras, de saúde e outras classificadas como sensíveis.

CRIPTOGRAFIA

Uma das principais técnicas usadas para garantir a confidencialidade. A criptografia transforma dados em um formato ilegível para qualquer pessoa que não possua a chave correta. Exemplos de criptografia incluem AES (*Advanced Encryption Standard*) e RSA (*Rivest–Shamir–Adleman*).

CONTROLE DE ACESSO

Mecanismos de autenticação multifator (MFA) e gerenciamento de identidade e acesso (IAM) garantem que apenas usuários autorizados possam acessar recursos específicos.

SEGURANÇA DE TRANSPORTE

Protocolos como TLS/SSL são usados para proteger a confidencialidade dos dados em trânsito, como em sites HTTPS (Barreto; Zanin; Saraiva, 2018).

Confira algumas ameaças à tríade de segurança e confidencialidade

Exploraremos, agora, alguns dos desafios que enfrentamos na segurança da informação. Os ataques de interceptação são alguns dos mais preocupantes. Imagine que atacantes tentam interceptar dados em trânsito utilizando técnicas como o

man-in-the-middle (MITM). Nesse tipo de ataque, a comunicação entre duas partes é capturada e, possivelmente, alterada sem que elas percebam.

Mas não para por aí. O acesso não autorizado é outro grande problema. Usuários mal-intencionados, que podem ser tanto hackers quanto *insiders*, exploram vulnerabilidades para acessar informações que deveriam estar protegidas. É comum que ataques de engenharia social, como o *phishing*, sejam utilizados para contornar os controles de acesso, fazendo com que pessoas revelem dados sensíveis.

Temos o **malware**. Ferramentas maliciosas como *keyloggers* e *spyware* podem ser instaladas em sistemas para capturar informações confidenciais, como senhas ou números de cartões de crédito.

Agora, discutiremos a **integridade**. Este é um princípio fundamental que assegura que os dados permaneçam consistentes, precisos e confiáveis durante todo o seu ciclo de vida. Isso significa que os dados não podem ser alterados de forma não autorizada, seja acidentalmente ou intencionalmente, enquanto estão em trânsito ou em repouso.



A integridade também abrange a proteção do sistema e dos arquivos. Como isso se aplica na prática? Observemos alguns exemplos, segundo Barreto, Zanin e Saraiva (2018, on-line):

- **Assinaturas Digitais:** elas garantem que um documento ou mensagem não tenha sido alterado desde sua criação. Utilizam algoritmos de *hash* e criptografia assimétrica para verificar a autenticidade e a integridade dos dados.
- **Hashes Criptográficos:** algoritmos como o SHA-256 geram uma impressão digital única para cada arquivo ou mensagem. Se os dados forem alterados, o *hash* resultante mudará, sinalizando uma violação de integridade.
- **Controle de Versão e Backups:** manter várias versões de um arquivo ou sistema, além de realizar backups regulares, ajuda a garantir que, em caso de modificação não autorizada, seja possível restaurar a versão original.

Entretanto, existem **ameaças** à integridade que não podemos ignorar:

- **Ataques de Modificação de Dados:** atacantes podem tentar alterar registros, como transações financeiras ou dados de clientes, para obter vantagens ou causar danos. Isso pode acontecer em ataques de SQL injection ou na manipulação de pacotes durante a transmissão de dados.
- **Malware:** programas maliciosos como *ransomware* podem corromper ou modificar arquivos críticos de um sistema.
- **Erros Humanos:** alterações acidentais nos dados, feitas por administradores de sistemas ou usuários finais, também podem comprometer a integridade (Barreto; Zanin; Saraiva, 2018).

Então, quais medidas de controle podemos implementar para **proteger** a integridade dos dados? Aqui estão algumas sugestões:

- **Verificações de Integridade:** implementar verificações de integridade de arquivos e sistemas críticos pode ajudar a detectar alterações não autorizadas.
- **Monitoramento e Log:** usar mecanismos de autenticação e log para rastrear quem fez mudanças nos sistemas ou dados.

- **Detecção de Intrusões:** adotar ferramentas como IDS/IPS para monitorar o tráfego de rede e alertar sobre tentativas de adulteração de dados.
- **Backups e Auditoria:** realizar backups periódicos e manter registros de auditoria detalhados para garantir que qualquer alteração possa ser revertida ou rastreada (Barreto; Zanin; Saraiva, 2018).

Por fim, abordaremos a **disponibilidade**. Este princípio assegura que sistemas, serviços e dados estejam acessíveis para usuários autorizados sempre que necessário. Isso envolve a capacidade de resistir a falhas, ataques ou outros eventos que possam interromper o funcionamento normal de uma rede ou sistema.

Como garantimos a disponibilidade na prática?

- **Sistemas Redundantes:** usar arquiteturas de alta disponibilidade (HA) com redundância, como servidores espelho e *clusters de failover*, assegura que o serviço continue funcionando mesmo se um servidor falhar.
- **Balanceamento de Carga:** distribuir a carga de trabalho entre vários servidores garante que o sistema não fique sobrecarregado.
- **Backups e Planos de Recuperação de Desastres:** manter backups regulares e ter um plano de recuperação robusto permite restaurar rapidamente o sistema após uma falha ou ataque (Souza *et al.* 2021).

É importante estarmos cientes das ameaças à disponibilidade:

- **Ataques DoS/DDoS:** esses ataques sobrecarregam um sistema ou serviço, impedindo que usuários legítimos acessem recursos da rede.
- **Falhas de Hardware/Software:** erros em componentes físicos ou falhas em atualizações de software podem causar a indisponibilidade de sistemas críticos.
- **Desastres Naturais ou Falhas Elétricas:** catástrofes como inundações, incêndios ou falhas de energia podem interromper significativamente a disponibilidade de serviços (Souza *et al.*, 2021).

Vamos explorar juntos as melhores práticas e estratégias para garantir a segurança, integridade e disponibilidade dos nossos sistemas!

**EU INDICO**

É muito importante entendermos cada vez mais a Tríade CIA. Para isso, eu trouxe um artigo muito bacana. Acesse em: <https://blog.bughunt.com.br/triade-cia/>

A **Tríade CIA** é fundamental para a criação de redes seguras e eficazes, abordando as principais necessidades de confidencialidade, integridade e disponibilidade dos dados e sistemas. Cada um desses princípios é vulnerável a ameaças específicas, e a implementação de contramedidas adequadas, como criptografia, monitoramento de integridade e redundância, é essencial para mitigar riscos e proteger ativos em rede.

A segurança eficaz em redes depende de uma abordagem holística que integre esses princípios de forma coesa e alinhada às necessidades organizacionais.

A criptografia e a autenticação avançada são elementos críticos para garantir a segurança das comunicações, dos dados e das transações no ambiente digital. Segundo Torres (2016, p. 148), “eles servem como a linha de defesa contra acessos não autorizados, interceptação de dados e ataques cibernéticos”.

A segurança eficaz em redes depende de uma abordagem holística



CRIPTOGRAFIA

A **criptografia** envolve a transformação de dados legíveis em um formato ininteligível (texto cifrado), que só pode ser revertido ao seu estado original (texto claro) por quem possuir a chave correta. Esse processo protege a confidencialidade e a integridade das informações.

Segundo Stallings (2014, p. 43):



A criptografia é amplamente utilizada para proteger dados em trânsito e em repouso em uma variedade de sistemas, desde a comunicação entre dispositivos até o armazenamento de dados confidenciais.

Afinal o que é criptografia? Quando falamos de criptografia digital, não estamos mais falando de texto, estamos falando de números. Então ‘criptografar’ algo com uma chave pública, ‘descriptografar’ algo com a chave privada são apenas operações matemáticas que realizamos com uma chave.

```
function criptografar (mensagem, expoente, modulo) {  
    return (mensagem ** expoente) % modulo  
}
```

Figura 2 - Função Criptografia / Fonte: o autor.

Descrição da Imagem: a figura apresenta um exemplo de criptografia em linguagem Javascript: function criptografar (mensagem, expoente, modulo) { return (mensagem ** expoente) % modulo }. Fim da descrição.

Existem dois principais tipos de criptografia: simétrica e assimétrica. Cada um possui características e aplicações específicas na proteção de informações. Vejamos:

Criptografia simétrica

Na **criptografia simétrica**, a mesma chave é usada tanto para cifrar quanto para decifrar os dados. Esse método é eficiente em termos de desempenho, mas

apresenta desafios em relação à segurança da chave, pois a chave precisa ser compartilhada entre as partes que se comunicam.

Segundo a IBM ([202-?]) conheça as criptografias simétricas:

AES (ADVANCED ENCRYPTION STANDARD)

O AES é amplamente utilizado em criptografia simétrica devido à sua segurança e eficiência. Ele pode operar em tamanhos de chave de 128, 192 e 256 bits, oferecendo um bom equilíbrio entre segurança e desempenho.

DES (DATA ENCRYPTION STANDARD) E 3DES

Embora o DES tenha sido um dos primeiros algoritmos simétricos amplamente usados, ele foi substituído pelo 3DES e, eventualmente, pelo AES devido à vulnerabilidade de força bruta.

DESEMPENHO RÁPIDO

A criptografia simétrica é mais rápida em comparação com a assimétrica, o que a torna ideal para cenários em que grandes volumes de dados precisam ser cifrados rapidamente.

SIMPlicidade

Por utilizar apenas uma chave, o processo de criptografia e decriptação é relativamente simples.

DISTRIBUIÇÃO DE CHAVES

A segurança da chave é um ponto crítico, pois ambas as partes precisam compartilhar a chave secreta de maneira segura. Se a chave for interceptada, todo o sistema estará comprometido.

Criptografia assimétrica

A **criptografia assimétrica** usa um par de chaves: uma chave pública para cifrar e uma chave privada para decifrar os dados. Esse método elimina a necessidade de compartilhamento seguro de chaves, pois a chave pública pode ser distribuída abertamente, enquanto a chave privada permanece em segredo com o destinatário.

A seguir, observe alguns do Algoritmos, segundo Infortrend ([202-?]) e IBM (2024):

- **RSA (*Rivest-Shamir-Adleman*)**: um dos algoritmos assimétricos mais usados, o RSA permite que dados sejam cifrados com uma chave pública e só possam ser decifrados com a chave privada correspondente. É amplamente utilizado em protocolos de segurança da internet, como o SSL/TLS.
- **ECDSA (*Elliptic Curve Digital Signature Algorithm*)**: baseado em criptografia de curva elíptica, o ECDSA é mais eficiente que o RSA, especialmente com chaves menores, oferecendo segurança comparável com menos consumo de recursos

Vejamos algumas vantagens:

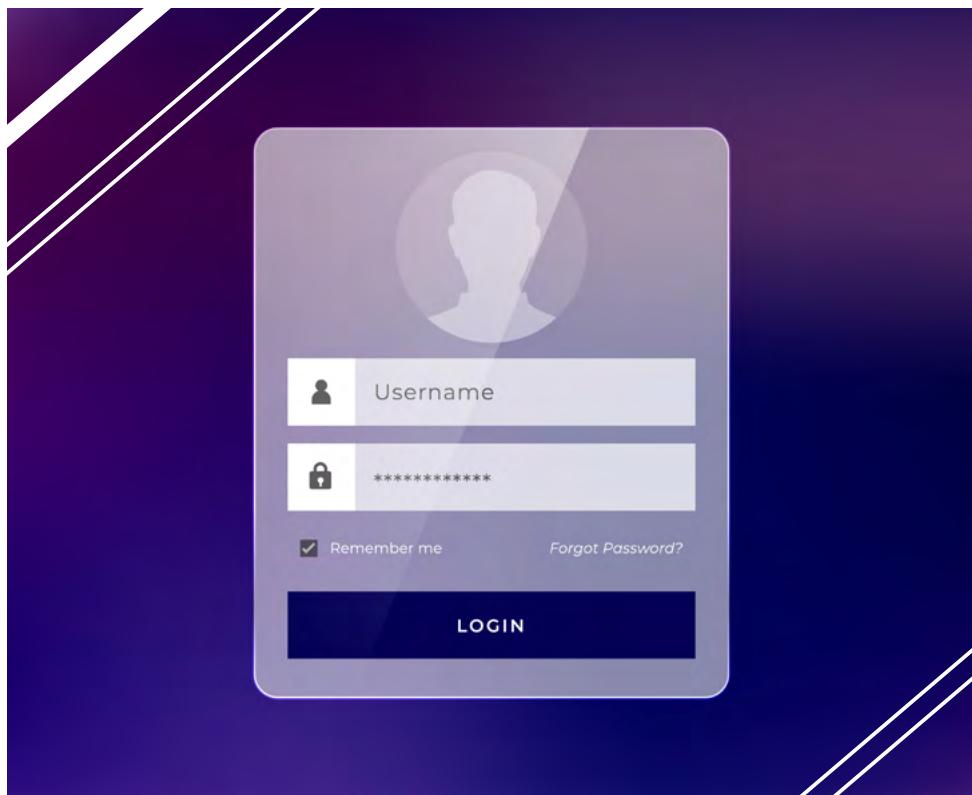
- **Segurança de Distribuição de Chaves**: a criptografia assimétrica elimina o problema de distribuição de chaves secretas, pois a chave pública pode ser compartilhada livremente.
- **Autenticidade e Assinaturas Digitais**: a criptografia assimétrica permite a criação de assinaturas digitais que garantem a integridade dos dados e a autenticidade de quem os enviou.
- **Desempenho**: a criptografia assimétrica é computacionalmente mais intensa e, portanto, mais lenta do que a criptografia simétrica, o que a torna menos ideal para cifrar grandes volumes de dados.

A seguir, apresento alguns dos protocolos criptográficos:

- **TLS/SSL (*Transport Layer Security/Secure Sockets Layer*)**: protocolos usados para proteger a comunicação via internet, como em transações bancárias ou acessos a sites seguros. Usam uma combinação de criptografia assimétrica para o *handshake* inicial e criptografia simétrica para as sessões de dados.

AUTENTICAÇÃO AVANÇADA

De acordo com Kurose e Ross (2021), a autenticação é o processo de verificar a identidade de um usuário ou dispositivo antes de permitir o acesso a um sistema. Com a crescente sofisticação dos ataques cibernéticos, a autenticação básica, como o uso de uma senha, tornou-se insuficiente. A autenticação avançada busca aumentar a segurança, adicionando camadas extras de verificação.



A **autenticação multifator** (MFA) é um método que combina dois ou mais fatores de autenticação de diferentes categorias, aumentando significativamente a segurança. Segundo a IBM (2024) os fatores de autenticação são geralmente categorizados em três tipos:

 ZOOM NO CONHECIMENTO

1. **Algo que você sabe (fator de conhecimento)**: senhas, PINs ou respostas a perguntas secretas.
2. **Algo que você tem (fator de posse)**: cartões inteligentes, tokens físicos ou aplicativos de autenticação (como o Google Authenticator).
3. **Algo que você é (fator de inherência)**: dados biométricos, como impressões digitais, reconhecimento facial ou varredura de íris.

As vantagens:

- **Segurança Adicional**: mesmo que um fator seja comprometido (por exemplo, uma senha), os outros fatores ainda protegem a conta.
- **Flexibilidade**: organizações podem implementar MFA com base em suas necessidades e os níveis de risco associados aos diferentes tipos de dados ou sistemas.
- **Experiência do Usuário**: o uso de múltiplos fatores pode tornar o processo de login mais demorado ou inconveniente.
- **Custo e Complexidade**: implementar MFA pode ser mais caro e complexo para organizações, especialmente aquelas que precisam autenticar muitos usuários (IBM, 2024).

 EU INDICO

Podemos explorar cada vez mais os tipos de autenticação. Acompanhem o artigo a seguir, muito interessante, desenvolvido pela Alura. <https://www.alura.com.br/artigos/tipos-de-autenticacao>

Certificados digitais

Você já se perguntou como garantimos a identidade em um mundo digital tão vasto? É aqui que entram os certificados digitais! Eles são essenciais para garantir a identidade de usuários, dispositivos ou servidores. Mas como funcionam?

Um **certificado digital** é emitido por uma autoridade certificadora (CA) confiável, como a *VeriSign* ou a *Let's Encrypt*. Ele inclui uma chave pública que está associada à identidade do titular. Como podemos identificar isso na prática?

Estudante, confira algumas aplicações, segundo Stallings (2014):

- **Certificados SSL/TLS:** garantem que a comunicação entre seu navegador e um servidor web seja segura, além de confirmar que o servidor é autêntico. Você já reparou no cadeado verde na barra de endereços? É um sinal de que o site é seguro!
- **Assinaturas Digitais:** asseguram que um documento não foi alterado e que foi assinado pelo remetente legítimo. É como ter uma assinatura física em um documento digital.
- **Autenticação de Dispositivos:** os certificados digitais também são utilizados para autenticar dispositivos em uma rede, como roteadores, servidores e dispositivos IoT. Isso ajuda a garantir que apenas dispositivos confiáveis possam se conectar.

Entretanto, nem tudo são flores na criptografia e autenticação avançada. Infelizmente, existem várias ameaças e desafios a serem enfrentados. Confira o que Stallings (2014) nos apresenta sobre isso:

ATAQUES DE FORÇA BRUTA

Essas são tentativas repetidas de adivinhar chaves de criptografia ou senhas, especialmente em sistemas que usam chaves mais fracas ou senhas simples.

ATAQUES DE MAN-IN-THE-MIDDLE (MITM)

Em sistemas sem criptografia adequada, um invasor pode interceptar e manipular a comunicação entre duas partes sem que elas percebam. Imagine alguém ouvindo uma conversa sem que você saiba!

VULNERABILIDADES DE IMPLEMENTAÇÃO

Falhas na implementação de algoritmos criptográficos ou sistemas de autenticação podem ser exploradas por invasores, como no caso de protocolos desatualizados ou certificados comprometidos.

ATAQUES DE ENGENHARIA SOCIAL

Técnicas de *phishing* podem ser usadas para enganar usuários e fazer com que revelem seus dados de autenticação. É como um truque para fazer você entregar suas chaves!

Com a ascensão da computação quântica, a preocupação só aumenta. Muitos dos algoritmos criptográficos atuais, especialmente os baseados em criptografia assimétrica, podem ser quebrados por computadores quânticos. Isso gerou o desenvolvimento da criptografia pós-quântica, que busca criar algoritmos que permaneçam seguros mesmo em um mundo dominado pela computação quântica.

FIREWALLS, IDS/IPS E SEGURANÇA DE ENDPOINT

Os *firewalls* são a primeira linha de defesa em uma rede. Eles monitoram e controlam o tráfego de rede de acordo com regras de segurança predefinidas, bloqueando ou permitindo o tráfego de entrada e saída com base nessas políticas. Seu objetivo principal é restringir o acesso não autorizado e prevenir a exposição de serviços internos vulneráveis. Com *firewalls* robustos, a superfície de ataque inicial da rede é significativamente reduzida.

Enquanto os *firewalls* atuam como guardiões do perímetro da rede, os **Sistemas de Detecção e Prevenção de Intrusão (IDS/IPS)** acrescentam uma camada adicional de vigilância e resposta ativa. O **IDS** identifica atividades suspeitas e alerta sobre tentativas de ataques, permitindo que a equipe de segurança investigue a ameaça. O **IPS** vai um passo além, bloqueando ativamente os ataques em tempo real, prevenindo a intrusão antes que ela cause danos.

A segurança de *endpoint* é igualmente vital, pois protege os dispositivos conectados à rede, como laptops, smartphones e servidores, que podem ser alvos vulneráveis. Ataques em *endpoints* podem servir como ponto de entrada para malware, comprometendo a rede como um todo. Soluções de segurança para *endpoints* garantem que cada dispositivo tenha medidas de proteção, como antivírus, firewalls locais e criptografia, evitando que dispositivos inseguros comprometam a rede.



EU INDICO

O que é um sistema de prevenção de intrusão (IPS)? Acompanhe o artigo a seguir para desvendarmos o que é IPS e o que difere do IDS. [https://www.ibm.com/br-pt/topics/intrusion-prevention-system](https://www.ibm.com.br-pt/topics/intrusion-prevention-system)

POLÍTICAS DE SEGURANÇA DE REDE

Os firewalls, IDS/IPS e segurança de *endpoints* são apenas tão eficazes quanto as políticas de segurança de rede implementadas. Essas políticas estabelecem as diretrizes sobre como os recursos de uma rede podem ser utilizados e protegidos, definindo permissões, atribuindo responsabilidades e estipulando os processos de resposta a incidentes.

Para criar uma política robusta, é crucial:

- **Identificar ativos críticos**, como servidores de dados sensíveis e sistemas de pagamento.
- **Avaliar possíveis ameaças** à infraestrutura, como malware, ataques DDoS ou comprometimento de dispositivos.
- **Desenvolver planos de mitigação**, implementando controles que restrinjam o acesso a esses ativos, como a autenticação multifator (MFA), o controle de privilégios e a segmentação de rede (IBM, 2024).

Por que investir em segurança de redes é importante? A segurança de redes tem ganhado uma grande importância no ambiente corporativo moderno.

Hoje, não há mais como empresas executarem serviços e desenvolverem produtos de qualidade sem o apoio da rede. Até mesmo na agricultura, agora dominada pelos sensores da Internet das Coisas, a *web* é uma ferramenta que está integrada a todos os processos (Kurose; Ross, 2021).

“Políticas de segurança bem definidas não apenas protegem a infraestrutura, mas também permitem uma resposta eficiente e coordenada em caso de incidente, minimizando o impacto sobre a organização” (Sousa, 2013, p. 231).

Em função disso, ter uma boa política de gestão de segurança de redes é algo crítico. De acordo com Stallings (2014) a empresa precisa garantir que a sua infraestrutura poderá ser utilizada por todos os profissionais sem que a sua privacidade seja impactada. Isso ocorre, principalmente, nos ambientes em que a transformação digital está presente.

Ter uma boa política de gestão de segurança de redes é algo crítico

Segundo Stallings (2014) os processos digitalizados modernos contam com a *web* para garantir a integração e a colaboração entre equipes. A computação na nuvem está por trás de muitas tecnologias, que facilitam a flexibilização de rotinas e o aumento dos níveis de inovação. No entanto, os ganhos relacionados a esses fatores só são possíveis caso os usuários tenham confiança na rede.

SEGURANÇA EM REDES SEM FIO (WPA3, 5G SECURITY)

Você já parou para pensar nos desafios que as redes sem fio enfrentam em termos de segurança? O meio de transmissão aberto torna tudo mais vulnerável, facilitando o acesso de atacantes. Para lidar com isso, surgiu o protocolo WPA3. Mas como ele faz isso?

WPA3 foi desenvolvido para fornecer uma camada extra de proteção, corrigindo as vulnerabilidades do WPA2. Ele oferece segurança até mesmo em redes com senhas fracas, graças ao método de criptografia avançado chamado *Simultaneous Authentication of Equals* (SAE). Isso significa que, mesmo que a sua senha não seja a mais forte, você ainda pode contar com uma proteção robusta contra-ataques de força bruta.



O que dizer da nova era do 5G? Com a chegada dessa tecnologia, a segurança das redes sem fio deu um grande salto. A arquitetura 5G foi projetada para conectar bilhões de dispositivos, muitos dos quais são IoT e, portanto, têm pouca ou nenhuma segurança. Mas não se preocupe, pois a 5G traz várias melhorias importantes, conforme Stallings (2014):

- **Autenticação e criptografia reforçadas:** isso garante que a privacidade dos usuários seja protegida, mesmo em um ambiente tão conectado.
- **Slicing de rede:** essa funcionalidade permite a criação de redes virtuais separadas para diferentes tipos de serviços. Imagine um cenário em que, se uma parte da rede for violada, as outras partes ainda estarão seguras. Isso é exatamente o que o *slicing* oferece!
- **Gerenciamento de ameaças melhorado:** a 5G vem equipada com mecanismos avançados de segurança, adaptados ao alto volume e à diversidade de dispositivos conectados. Assim, as redes podem se proteger de maneira mais eficaz contra novas ameaças.

Estudante, está claro como a segurança das redes sem fio está se adaptando e evoluindo?



EU INDICO

Como funciona a **WPA3**? Para entendermos melhor esse tópico tão importante segue o link de um artigo interessante detalhando alguns pontos sobre esse protocolo. <https://www.computerweekly.com/br/tutorial/Seguranca-sem-fio-diferencias-entre-WEP-WPA-WPA2-e-WPA3>

O WPA3 e o 5G são passos fundamentais para garantir que a conectividade seja não apenas rápida, mas também segura.

A REVOLUÇÃO DO **MACHINE LEARNING** NA SEGURANÇA CIBERNÉTICA

Já se perguntou como o *Machine Learning* está transformando a segurança cibernética? Essa tecnologia não só revoluciona a maneira como as ameaças são detectadas, mas também as mitiga de forma mais eficaz. Ao invés de depender apenas de regras fixas, o *Machine Learning* analisa grandes volumes de dados em busca de padrões.

Com relação à detecção de anomalias, imagine um algoritmo que observa o comportamento normal de uma rede. Se um dispositivo começa a enviar uma quantidade incomum de dados para um servidor desconhecido, isso acende um alerta. Esse é um exemplo clássico de detecção de anomalias, crucial para identificar ameaças desconhecidas (Kurose; Ross, 2021).

Quando se tratar de *malware*? Antigamente, as ferramentas de detecção se baseavam em assinaturas fixas. Contudo, os *malwares* estão sempre evoluindo! Agora, o *Machine Learning* vai além: ele analisa o comportamento de arquivos e programas. Por exemplo, um arquivo pode ser marcado como suspeito se agir como *ransomware*, mesmo que não tenha uma assinatura conhecida.

Um dos maiores trunfos do *Machine Learning* é sua evolução contínua. À medida que novos dados são processados, os algoritmos se tornam mais precisos. Você sabia que existem **dois tipos** principais de algoritmos? Os supervisionados, que aprendem a partir de dados rotulados, e os não supervisionados, que tentam

identificar padrões sozinhos. Isso significa que, além de responder a ameaças conhecidas, o sistema se adapta rapidamente a novas táticas utilizadas por cibercriminosos (Kurose; Ross, 2021).

VOCÊ SABE RESPONDER?

Como isso se aplica na prática?

O *Machine Learning* é utilizado em diversas áreas da segurança cibernética, como a análise comportamental. Sistemas de segurança podem monitorar o comportamento de usuários e dispositivos, identificando atividades incomuns que podem indicar comprometimento. Isso é especialmente útil em ambientes de *Zero Trust*, onde cada ação precisa ser verificada.

Ah, e não podemos esquecer da detecção de *phishing*! Ferramentas baseadas em *Machine Learning* analisam e-mails e páginas da web para identificar sinais de *phishing*, como padrões de escrita suspeitos ou URLs estranhas. Assim, você se protege melhor contra tentativas de fraude.

E a segurança de *endpoint*? Ferramentas modernas, como antivírus de nova geração e sistemas de resposta a *endpoints* (EDR), usam *Machine Learning* para detectar ameaças em dispositivos como laptops e smartphones. Esses sistemas podem identificar *malwares* polimórficos e comportamentos suspeitos, mesmo que a assinatura não seja conhecida.

O que podemos esperar do futuro? À medida que as ameaças cibernéticas continuam a evoluir, o papel do *Machine Learning* na segurança deve crescer. Técnicas avançadas de *deep learning* estão sendo exploradas para melhorar a precisão da detecção de ameaças em ambientes complexos. Além disso, a integração com inteligência artificial permitirá que os sistemas de segurança se tornem ainda mais sofisticados, capazes de prever ataques com base em padrões de comportamento.

E há mais! A automatização preditiva é uma área promissora. Sistemas de *Machine Learning* podem prever vulnerabilidades futuras e sugerir medidas preventivas, permitindo que as organizações se protejam antes mesmo de um ataque acontecer.

Viu como o *Machine Learning* está mudando a forma como abordamos a segurança cibernética? Com a capacidade de detectar anomalias, identificar *malwares* desconhecidos e automatizar respostas a incidentes, essa tecnologia está se tornando essencial na proteção de nossos ativos.

 **EM FOCO**

Estudante, para expandir seus conhecimentos sobre o assunto abordado, gostaríamos de lhe indicar a aula que preparamos especialmente para você. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

NOVOS DESAFIOS

Ao longo do estudo sobre Segurança em Redes, você teve a oportunidade de se aprofundar nos princípios fundamentais, como a tríade CIA (confidencialidade, integridade e disponibilidade), e em ferramentas essenciais como *firewalls*, IDS/IPS, e políticas de segurança. Esses conceitos formam a base que qualquer profissional precisa dominar para atuar na área de segurança cibernética.

Como isso se conecta com o mercado de trabalho? sabemos que as empresas, hoje, de todos os setores, estão cada vez mais expostas a ameaças digitais. Elas precisam de profissionais que entendam, na prática, como proteger suas redes, dados e sistemas. O conhecimento que você adquiriu aqui vai muito além da teoria. Cada conceito estudado pode ser aplicado diretamente no dia a dia de funções como analista de segurança, engenheiro de segurança, ou até mesmo como consultor de cibersegurança.



O mercado está evoluindo constantemente, e tecnologias emergentes, como 5G, IoT, e *Machine Learning*, trazem novos desafios e oportunidades. Com a base que você construiu, estará preparado não só para resolver problemas técnicos, mas também para ser um líder em iniciativas estratégicas de segurança. A demanda por profissionais de segurança de redes está crescendo rápido, então as oportunidades de emprego são vastas.

Tudo que você aprendeu até aqui é diretamente aplicável no ambiente profissional. O mercado está esperando você! Com o conhecimento que você tem agora, está pronto para fazer a diferença na proteção das infraestruturas digitais.

VAMOS PRATICAR

1. A segurança em redes, especialmente em ambientes digitais e corporativos, é fundamentada em três princípios centrais conhecidos como a Tríade CIA: Confidencialidade, Integridade e Disponibilidade. A confidencialidade garante que informações sensíveis só sejam acessadas por indivíduos com a devida permissão. Ela protege dados contra visualização, cópia ou interceptação por pessoas não autorizadas, sendo essencial para a segurança de informações privadas, financeiras e de saúde (Kurose; Ross, 2021).

Com base no princípio da confidencialidade na Tríade CIA, qual das seguintes alternativas exemplifica corretamente uma medida voltada para garantir a confidencialidade de dados em uma rede?

- a) Realizar backups periódicos de dados sensíveis.
 - b) Implementar sistemas de balanceamento de carga para servidores.
 - c) Utilizar criptografia para proteger informações durante a transmissão.
 - d) Criar *clusters* de servidores redundantes para evitar falhas.
 - e) Usar algoritmos de *hash* para verificar a integridade dos dados.
2. Ataques de Interceptação, como *Man-in-the-Middle* (MITM), ocorrem quando um invasor intercepta a comunicação entre duas partes sem que elas percebam, o que pode resultar em modificação ou roubo de dados. A integridade é o princípio que garante que os dados permaneçam precisos e consistentes, sem alterações não autorizadas. Medidas de segurança como assinaturas digitais e *hashes* criptográficos são amplamente utilizadas para verificar se os dados não foram alterados desde sua criação. Ataques como *phishing*, *malware* (*keyloggers* e *spyware*) e acessos não autorizados também ameaçam a integridade e confidencialidade das informações (Steinberg, 2021).

Considerando as ameaças e as medidas de proteção mencionadas, identifique as afirmativas corretas sobre o princípio da integridade.

- I - A integridade protege os dados de acessos não autorizados, garantindo que apenas pessoas autorizadas possam acessá-los.
- II - A integridade protege os dados contra interceptações durante sua transmissão em redes inseguras.
- III - A integridade assegura que os dados permaneçam consistentes e não sejam alterados sem autorização.
- IV - A integridade pode ser garantida por meio de ferramentas como assinaturas digitais e algoritmos de *hash* criptográficos.

VAMOS PRATICAR

É correto o que se afirma em:

- a) I, apenas.
 - b) II e IV, apenas.
 - c) III e IV, apenas.
 - d) I, II e III, apenas.
 - e) I, II, III e IV.
3. Os *firewalls* são a primeira linha de defesa em uma rede, monitorando e controlando o tráfego de rede de acordo com regras de segurança predefinidas. Seu objetivo principal é restringir o acesso não autorizado e prevenir a exposição de serviços internos vulneráveis. Além dos *firewalls*, os Sistemas de Detecção e Prevenção de Intrusão (IDS/IPS) adicionam uma camada de vigilância e resposta ativa, sendo que o IDS identifica atividades suspeitas e o IPS bloqueia ataques em tempo real. A segurança de *endpoint* é vital para proteger dispositivos conectados à rede, evitando que ataques comprometam a infraestrutura. A eficácia dessas medidas depende de políticas de segurança bem definidas, que estabelecem diretrizes sobre como os recursos devem ser utilizados e protegidos (Stallings, 2014).

Analise as afirmativas a seguir sobre segurança de redes e identifique as corretas:

- I - Os *firewalls* são responsáveis apenas por bloquear o tráfego de entrada e não monitoram o tráfego de saída da rede.
- II - A segurança de *endpoint* é irrelevante para a proteção da rede, pois apenas os *firewalls* são suficientes para garantir a segurança.
- III - O IDS (Sistema de Detecção de Intrusão) alerta sobre atividades suspeitas, enquanto o IPS (Sistema de Prevenção de Intrusão) bloqueia ataques em tempo real.
- IV - Políticas de segurança bem definidas são essenciais para garantir a proteção da infraestrutura e permitir uma resposta coordenada em caso de incidentes.

É correto o que se afirma em:

- a) I e IV, apenas.
- b) II e III, apenas.
- c) III e IV, apenas.
- d) I, II e III, apenas.
- e) II, III e IV, apenas.

REFERÊNCIAS

- BARRETO, J. dos S.; ZANIN, A.; SARAIVA, M. de O. **Fundamentos de redes de computadores**. Porto Alegre: SAGAH, 2018. *E-book*.
- KUROSE, J. F.; ROSS, K;W. **Redes de computadores e a internet**: uma abordagem top-down. São Paulo: Pearson, 2021.
- IBM. O que é criptografia? **IBM**, [202-?]. Disponível em: <https://www.ibm.com/br-pt/topics/cryptography>. Acesso em: 18 out. 2024.
- IBM. Política de Segurança. **IBM**, 2024. Disponível em: <https://www.ibm.com/docs/pt-br/i/7.5?topic=strategy-security-policy-objectives>. Acesso em: 18 out. 2024.
- INFORTREND. Princípios básicos de criptografia e sua importância na segurança de dados. **Infortrend Blog**, [202-?]. Disponível em: <https://www.infortrend.com.br/post/principios-basicos-de-criptografia-e-sua-importancia-na-seguranca-de-dados>. Acesso em: 18 out. 2024.
- SOUZA, L. B. de. **Projetos e implementação de redes**. São Paulo: Érica, 2013.
- SOUZA, D. C. de et al. **Gerenciamento de redes de computadores**. Porto Alegre: SAGAH, 2021. *E-book*.
- STALLINGS, W. **Criptografia e segurança de redes**: princípios e práticas. São Paulo: Pearson, 2014.
- STEINBERG, J. **Cibersegurança para leigos**. Rio de Janeiro: Alta Books, 2021.
- TORRES, G. **Redes de computadores**. Rio de Janeiro: Nova terra, 2016.

CONFIRA SUAS RESPOSTAS

1. Alternativa C.

A criptografia é uma medida essencial para garantir a confidencialidade, pois protege os dados, tornando-os ilegíveis para usuários não autorizados durante sua transmissão ou armazenamento. Diferente de mecanismos de backup ou redundância, a criptografia foca em impedir o acesso indevido a informações sensíveis, assegurando que somente aqueles com a chave correta possam decifrá-las.

2. Alternativa C.

A integridade refere-se à precisão e consistência dos dados, garantindo que eles não sejam alterados sem autorização (afirmativa III) e pode ser verificada com assinaturas digitais e *hashes* criptográficos (afirmativa IV). Afirmativas I e II se relacionam à confidencialidade e segurança de transporte, respectivamente, e não diretamente à integridade.

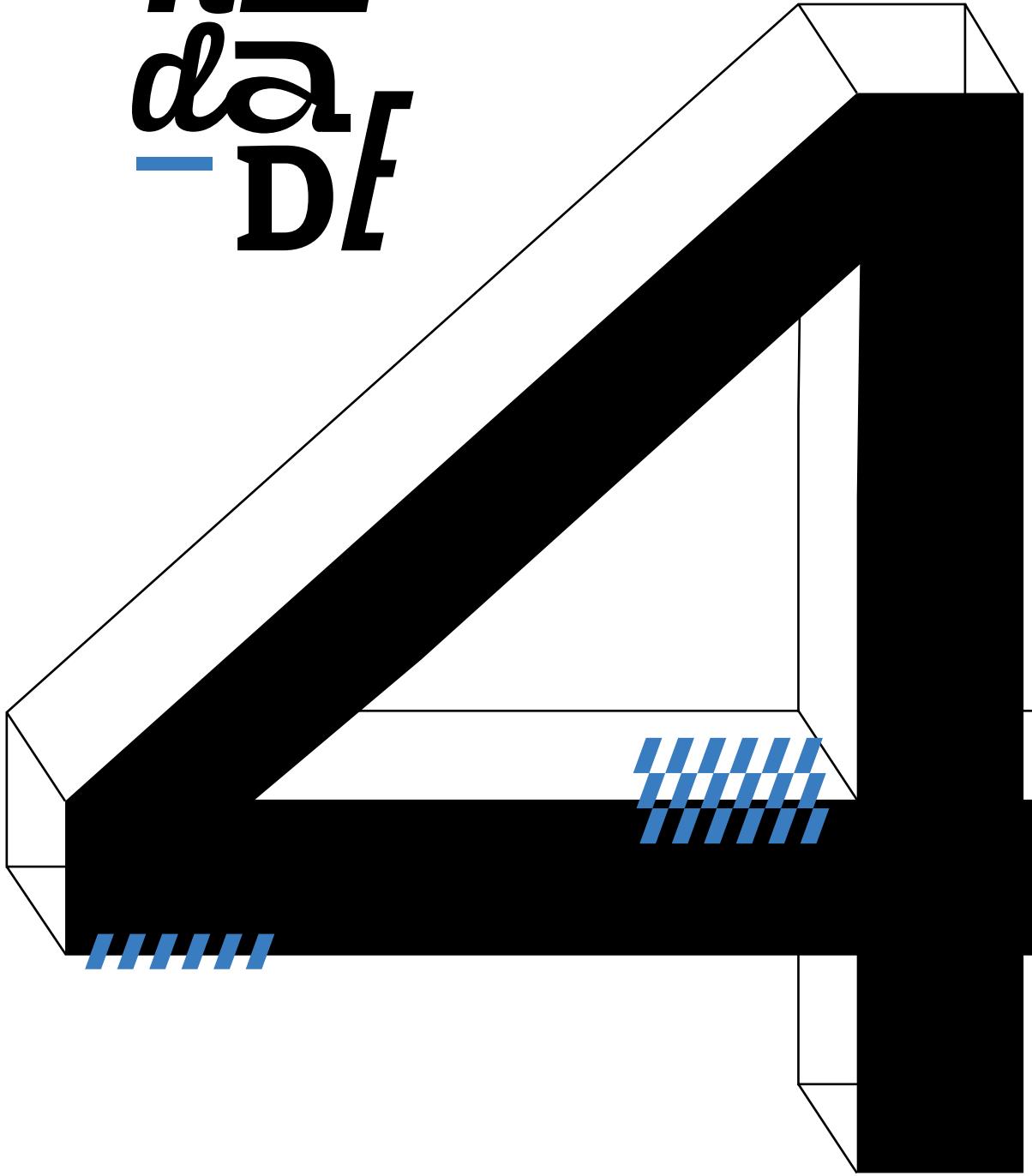
3. Alternativa C.

A afirmativa III está correta, pois descreve corretamente as funções do IDS e do IPS: o IDS identifica e alerta sobre atividades suspeitas, enquanto o IPS bloqueia ataques em tempo real. A afirmativa IV também está correta, pois enfatiza a importância de políticas de segurança bem definidas para proteger a infraestrutura e coordenar respostas a incidentes. As afirmativas I e II estão incorretas, uma vez que os *firewalls* monitoram tanto o tráfego de entrada quanto o de saída, e a segurança de endpoint é crucial para a proteção da rede, complementando as funções dos *firewalls*.

MEU ESPAÇO



uni
da
- DF





TEMA DE APRENDIZAGEM 6

REDES SEM FIO E MOBILIDADE

MINHAS METAS

- Compreender os princípios e a evolução das tecnologias de redes sem fio.
- Entender os conceitos e aplicações da mobilidade em redes e do 5G NR.
- Analisar e projetar redes Mesh e MEC para otimizar conectividade e processamento local.
- Aplicar práticas de segurança avançada em redes sem fio.
- Explorar as aplicações de IoT em diferentes setores.
- Identificar e mitigar potenciais vulnerabilidades em redes de IoT e mobilidade.
- Desenvolver uma visão crítica sobre o impacto das redes sem fio e da mobilidade na sociedade.

INICIE SUA JORNADA

Imagine seu dia a dia sem uma rede Wi-Fi para checar e-mails ou uma rede móvel para se comunicar. No contexto atual, em que a conectividade está profundamente integrada a todos os aspectos da vida pessoal e profissional, é difícil conceber um mundo sem redes sem fio, não é?

No entanto, muitas das tecnologias de conexão que usamos diariamente envolvem mais do que apenas ‘conectar à internet.’ **Tecnologias como Wi-Fi 6, 6G e LoRaWAN estão sendo desenvolvidas e aprimoradas para responder a demandas específicas do mundo moderno**, como a Internet das Coisas (IoT), que já conecta desde eletrodomésticos até veículos inteligentes. Mas como essas redes funcionam em um nível mais técnico? E o que faz delas ferramentas essenciais para a mobilidade e o desenvolvimento profissional no campo da tecnologia?

Compreender como essas tecnologias funcionam pode ser um diferencial significativo em várias áreas profissionais. Para os estudantes de tecnologia é uma oportunidade de entender como redes sem fio e protocolos de conectividade estão relacionados a aplicações que vão desde entretenimento até os sistemas de monitoramento médico.

Profissionais que entendem esses conceitos se tornam valiosos não apenas por seu conhecimento técnico, mas também pela capacidade de inovar e adaptar essas ferramentas a necessidades específicas. Em outras palavras, estar a par dessas tecnologias é fundamental para quem quer se destacar no mercado de trabalho e atuar em um ambiente cada vez mais digital e móvel.



PLAY NO CONHECIMENTO

Estudante, Já pensou como objetos do dia a dia, como geladeiras, carros e até plantações podem ‘conversar’ entre si e transformar nossas rotinas? Isso é a Internet das Coisas! No episódio de hoje, entenderemos como essa tecnologia está criando novas oportunidades no mercado de trabalho e como vocês podem se preparar para essa revolução.

Conecte-se conosco para descobrir como sensores, inteligência artificial e redes sem fio estão criando um mundo mais inteligente – e onde vocês, futuros profissionais, podem se encaixar nesse cenário incrível.. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

Para começar a explorar esses conceitos, que tal uma prática simples? Considere o que acontece quando você se conecta a uma rede Wi-Fi. Mesmo para uma conexão comum, como a de sua casa, diversas etapas ocorrem: da busca de um ponto de acesso (*Access Point*) à autenticação e à definição de padrões de segurança, como o WPA3. Cada uma dessas etapas representa um avanço nas tecnologias de redes sem fio, e o que vemos na prática é apenas a superfície de um processo complexo. Nos próximos tópicos, faremos uma jornada por essas camadas para entender o que cada uma traz de diferente e como elas transformam o modo como interagimos com o mundo.

Ao fim deste tema, você estará apto a responder perguntas como: ‘o que faz do Wi-Fi 6 uma tecnologia superior em redes locais?’ ou ‘Por que o 6G é tão aguardado para o desenvolvimento de cidades inteligentes?’ Também será capaz de refletir sobre como essas redes ampliam a mobilidade e flexibilizam os acessos. Esse conteúdo serve não apenas para expandir seu conhecimento técnico, mas também para abrir portas para uma nova visão sobre o futuro das redes sem fio e seu impacto em nosso cotidiano.



VAMOS RECORDAR?

Neste vídeo do Manual do Mundo, exploraremos o que é o Wi-Fi e como ele funciona de maneira simples e prática. Descobriremos juntos como o sinal chega até você, o que são frequências, como os roteadores operam e por que, às vezes, a conexão pode ficar lenta. Tópico essencial para abordarmos e seguirmos com o conteúdo do nosso tema. <https://www.youtube.com/watch?v=V2XW8nxNjcc>

DESENVOLVA SEU POTENCIAL

WI-FI 6: A NOVA GERAÇÃO DE REDES SEM FIO

O Wi-Fi 6, também conhecido como 802.11ax, é a mais recente geração de Wi-Fi, projetada para ambientes onde muitos dispositivos estão conectados ao mesmo tempo. Essa tecnologia aumenta a capacidade de tráfego e a velocidade de conexão, permitindo uma experiência de internet mais rápida e eficiente, especialmente em locais com alta demanda de conexão.

Imagine um cenário em que estamos em um evento com muitos dispositivos tentando se conectar à mesma rede Wi-Fi. A antiga tecnologia de Wi-Fi começaria a sofrer, causando lentidão e desconexões, pois não conseguia gerenciar adequadamente tantos acessos simultâneos. O Wi-Fi 6, por outro lado, foi projetado para lidar com esses ambientes de alta densidade, permitindo que todos se conectem com mais estabilidade e rapidez.

O Wi-Fi 6 utiliza uma técnica chamada OFDMA (*Orthogonal Frequency Division Multiple Access*), que permite a divisão do canal Wi-Fi em subcanais menores, aumentando a eficiência da transmissão de dados. Pense nisso como um sistema de faixas em uma estrada: enquanto o Wi-Fi antigo tinha apenas uma faixa para tráfego de dados, o Wi-Fi 6 tem várias, permitindo que mais dados passem simultaneamente. Essa tecnologia reduz a latência e melhora a duração

da bateria dos dispositivos conectados. “A evolução das tecnologias de rede reflete o avanço da sociedade digital, onde a necessidade de velocidade e segurança tornou-se indispensável em praticamente todas as áreas” (Torres, 2016, p. 121).

Podemos perceber algumas das vantagens do Wi-Fi 6 e o impacto dessas vantagens: em primeiro lugar, uma velocidade maior, em que são proporcionadas velocidades de até 40% maiores que as versões anteriores; outra vantagem é uma menor latência, ideal para atividades que exigem resposta rápida, como jogos on-line e videoconferências.

Além das vantagens supracitadas contamos também com uma eficiência energética em que, com o recurso TWT (*Target Wake Time*), os dispositivos conectados gastam menos energia, pois o roteador e os dispositivos podem coordenar momentos específicos para transmitir dados, “uma rede bem estruturada deve permitir crescimento e mudanças com o mínimo de impacto possível no funcionamento geral da infraestrutura” de acordo com Sousa (2013, p. 203).

O Wi-Fi 6 e o Wi-Fi 6E (com a banda de 6 GHz) estão começando a transformar os ambientes urbanos. Com o Wi-Fi 6E, que amplia o espectro de frequência, temos uma capacidade ainda maior de conectividade. Isso é particularmente útil em áreas com congestionamento de sinais, como centros urbanos e grandes eventos, nos quais a qualidade de conexão geralmente é um desafio.

VOCÊ SABE RESPONDER?

Como você acha que o **Wi-Fi 6** pode impactar o desenvolvimento de cidades inteligentes, onde múltiplos dispositivos IoT (Internet das Coisas) precisam se comunicar simultaneamente em uma mesma rede?

O Wi-Fi 6 é mais do que apenas uma internet ‘mais rápida’. Ele representa uma atualização essencial para um mundo hiperconectado, trazendo melhorias significativas para empresas e ambientes públicos, bem como para o uso doméstico.

6G: O FUTURO DAS REDES MÓVEIS

Proponho refletirmos, embora ainda esteja em fase de pesquisa, o 6G representa a próxima evolução das redes móveis, com previsões de velocidades até 100 vezes mais rápidas que o 5G e uma latência extremamente baixa, possivelmente de 1 milissegundo ou menos. Esse avanço permitiria que dispositivos se comunicassem de maneira quase instantânea, algo essencial para aplicações como realidade aumentada, realidade virtual e cidades inteligentes.

APROFUNDANDO

Agora imagine um cenário em que uma ambulância autônoma precisa navegar em tempo real pelas ruas de uma cidade movimentada para chegar rapidamente a um paciente. Com uma conexão de alta velocidade e baixa latência, como a que o 6G promete, a ambulância conseguiria trocar dados constantemente com semáforos, carros e sensores de trânsito, criando uma rota dinâmica e segura, adaptada a cada segundo.

O 6G deve explorar frequências na faixa de THz (terahertz), enquanto o 5G usa atualmente as faixas de GHz. Esse salto em frequência permite uma transmissão muito mais rápida de dados, mas também apresenta novos desafios. A cobertura do 6G tende a ser mais limitada, exigindo infraestrutura densa, como redes Mesh e pontos de acesso distribuídos, para assegurar a estabilidade do sinal. Aqui, a inteligência artificial desempenha um papel importante para adaptar a rede às condições dinâmicas do ambiente.



“O crescimento exponencial da Internet, impulsionado pela inovação e demanda, traz não apenas grandes oportunidades, mas também desafios técnicos significativos para engenheiros e cientistas da computação” (Kurose; Ross, 2021, p. 50).

A transição para o 6G não significa apenas internet mais rápida, ela traz a promessa de um novo nível de conectividade e interação entre dispositivos. Aplicações em áreas como saúde, educação e transporte poderão se beneficiar de recursos antes inviáveis.

Por exemplo, com o 6G, cirurgias remotas podem se tornar rotineiras, e o monitoramento de pacientes por dispositivos de IoT em tempo real poderia ser extremamente preciso e ágil. Veremos na sequência alguns dos principais benefícios do 6G e seu desempenho durante sua utilização. Um dos principais benefícios é a alta velocidade, permitindo aplicações como streaming de realidade virtual em altíssima definição.

Outro tópico importante é a baixa latência, essencial para aplicações que exigem resposta em tempo real, como veículos autônomos e controle remoto de dispositivos. A capacidade de conexão em massa poderá suportar bilhões de dispositivos conectados simultaneamente, potencializando o uso de IoT.



PENSANDO JUNTOS

Como você imagina que o 6G possa transformar a experiência de realidade aumentada e virtual? Quais setores, na sua opinião, poderiam se beneficiar mais com o 6G?

O 6G é mais do que uma continuação do 5G; ele simboliza a chegada de uma infraestrutura de redes completamente nova, pensada para suportar uma conectividade em massa e instantânea. Se o 5G já está moldando a indústria significativamente, o 6G promete levar isso a um novo patamar, com impacto direto em como trabalhamos, vivemos e interagimos.

LoRaWAN: conectividade para dispositivos de baixo consumo

LoRaWAN (*Long Range Wide Area Network*) é uma tecnologia de rede projetada para conectar dispositivos de IoT (Internet das Coisas) que precisam

enviar pequenas quantidades de dados a longas distâncias com baixo consumo de energia. Diferente do Wi-Fi ou do 5G, os quais são mais comuns em redes de alta velocidade e baixa latência, o LoRaWAN se destaca justamente por seu baixo consumo energético e alcance de até 15 km em ambientes abertos.

Imaginemos uma cidade que utiliza sensores em postes de iluminação para monitorar a intensidade da luz, consumo de energia e até mesmo a qualidade do ar. Esses sensores enviam dados regularmente, mas não precisam de uma conexão de alta velocidade.

O LoRaWAN é ideal para esse cenário porque permite que esses dispositivos operem por vários anos com uma única bateria, enquanto mantém uma conexão de longo alcance e de baixo custo.

O LoRaWAN trabalha em frequências sub-GHz (como 868 MHz na Europa e 915 MHz nos Estados Unidos), o que permite que o sinal atravesse obstáculos como prédios e árvores com maior facilidade. A estrutura de rede do LoRaWAN é tipicamente formada por três componentes principais, vejamos quais são eles:

DISPOSITIVOS DE IOT

Sensores ou atuadores que coletam e enviam dados.

GATEWAYS

Pontos de acesso que recebem dados dos dispositivos e os encaminham para um servidor central.

SERVIDORES DE REDE

Responsáveis por gerenciar e processar os dados recebidos dos dispositivos.

Uma característica importante do LoRaWAN é o uso de um mecanismo de transmissão chamado *chirp spread spectrum*, que permite um alcance maior com menos interferência. Essa tecnologia é usada, por exemplo, em sensores para agricultura, monitoramento ambiental e gerenciamento de ativos em áreas remotas, vejamos agora alguns dos benefícios do LoRaWAN.

Um dos benefícios é o baixo consumo de energia ideal para dispositivos que precisam operar por anos com uma única bateria. Um alcance de longa distância de até 15 km em áreas abertas e contando também com um baixo custo de operação além das configurações de LoRaWAN que geralmente têm menos necessidade de manutenção.



PENSANDO JUNTOS

Como você vê o impacto de tecnologias de conectividade de baixo consumo, como o **LoRaWAN**, na gestão de cidades inteligentes?

Com seu alcance e baixo custo, o LoRaWAN permite a implementação de redes de IoT em larga escala, mesmo em áreas rurais ou locais de difícil acesso, democratizando o uso da tecnologia e promovendo o desenvolvimento de soluções inteligentes para diversas áreas.

Mobilidade em redes e 5G NR: desafios da conectividade

O 5G NR (New Radio) é a nova interface de rádio para o 5G. Ele marca uma evolução importante em relação às gerações anteriores de redes móveis. Com uma capacidade de dados muito maior e latência ultrabaixa, o 5G NR foi projetado para suportar uma grande quantidade de dispositivos conectados, como carros autônomos, dispositivos IoT e aplicações em realidade aumentada. Essas características tornam o 5G um facilitador essencial para o futuro da mobilidade e da conectividade inteligente.

Imagine um sistema de transporte público em que cada veículo se comunica em tempo real com uma central de controle e com outros veículos ao redor, ajustando sua rota para evitar engarrafamentos ou minimizar o consumo de combustível. O 5G NR possibilita essa comunicação ultrarrápida e estável, o que antes era um desafio com as gerações anteriores de redes móveis.

O 5G NR não só aumenta a velocidade de transmissão dos dados, mas também introduz conceitos como as redes virtuais (*slicing*), que permitem dividir uma mesma infraestrutura de rede para oferecer diferentes serviços com distintas qualidades de conexão. Isso significa que uma mesma rede 5G pode atender simultaneamente um carro autônomo, que precisa de baixa latência e alta confiabilidade, e um dispositivo de monitoramento de saúde, que requer uma conexão constante, mas não necessariamente em tempo real.



Figura 1 - Conceito 5G NR / Fonte: <https://www.cavliwireless.com/assets/images/wireless-by-design/5g-nr/5g-nr.webp>. Acesso em: 9 nov. 2024.

Descrição da Imagem: a figura apresenta um infográfico do conceito 5G NR. Imagem exibindo o conceito da conexão 5G NR. Fim da descrição..

Um dos recursos do 5G NR para melhorar a mobilidade e cobertura em redes é o uso de MIMO massivo (*Multiple Input, Multiple Output*), que permite a transmissão simultânea de múltiplos sinais de dados, aumentando a capacidade da rede e a cobertura para ambientes urbanos e áreas densamente povoadas.

A seguir, veremos alguns dos benefícios do 5G NR para Mobilidade:

LATÊNCIA ULTRABAIXA

Fundamental para aplicações como controle de drones e automação industrial em tempo real.

ALTA DENSIDADE DE DISPOSITIVOS

Suporta milhões de dispositivos conectados por quilômetro quadrado, ideal para IoT e cidades inteligentes.

SLICING DE REDE

Permite personalizar as funcionalidades da rede para diferentes tipos de serviço.

Quais seriam os impactos do 5G NR na mobilidade urbana e no cotidiano das grandes cidades?

Com o 5G NR, temos a possibilidade de integrar veículos autônomos, dispositivos inteligentes e aplicações em realidade aumentada de maneira totalmente sincronizada e com baixo tempo de resposta. A mobilidade e a comunicação entre dispositivos evoluem para um novo patamar, impactando áreas como o transporte, a saúde e a segurança.

Redes Mesh e Multi-Access Edge Computing (MEC)

As redes Mesh oferecem uma infraestrutura flexível, nela os nós de rede atuam como transmissores e receptores, ampliando a cobertura de forma descentra-

lizada e adaptativa. Já o MEC (*Multi-Access Edge Computing*) permite que a computação seja realizada na borda da rede, próxima dos usuários e dispositivos, melhorando o tempo de resposta e aliviando a sobrecarga de servidores centrais.



EU INDICO

Para nos aprofundarmos em Redes mesh, recomendo o artigo *O que é rede Mesh e quais suas vantagens?* Nele há tópicos e exemplos muito interessantes para entendermos as redes Mesh. Acesse em: <https://blog.intelbras.com.br/o-que-e-rede-Mesh-e-quais-suas-vantagens/>

Imagine que você está em um grande estádio, onde milhares de pessoas tentam acessar a internet simultaneamente para compartilhar fotos e vídeos. Uma rede Mesh permite que cada ponto de acesso auxilie no compartilhamento do sinal, enquanto o MEC processa os dados mais próximos dos usuários, reduzindo a latência e melhorando a experiência.



ZOOM NO CONHECIMENTO

As **redes Mesh** são compostas por dispositivos conectados entre si em uma estrutura de múltiplos nós, permitindo a expansão do sinal em áreas amplas ou de difícil acesso, e são muito utilizadas em locais como grandes empresas e residências de grande porte. Em paralelo, o MEC possibilita que dispositivos de IoT e usuários finais tenham processamento de dados localmente, diminuindo a dependência de um servidor central e tornando as respostas mais rápidas, o que é essencial em situações de mobilidade e IoT.

O MEC permite que dados críticos, como os gerados por sensores em carros autônomos, sejam processados instantaneamente sem precisar enviar os dados a uma nuvem distante, reduzindo o tempo de resposta (latência) e permitindo uma tomada de decisão mais rápida. Isso é fundamental em áreas de mobilidade, onde qualquer atraso pode impactar diretamente na segurança e eficiência das operações.

Entendamos alguns dos benefícios das redes Mesh e do MEC:

- **Maior cobertura** em redes locais, adaptando-se a áreas extensas ou com múltiplos obstáculos físicos.
- **Resiliência** no caso de um nó falhar, a rede pode redirecionar o tráfego por meio de outros nós.
- **Menor latência** com o processamento de dados próximo ao usuário, o MEC permite uma experiência mais rápida e eficiente.

Redes Mesh, juntamente com o MEC, viabilizam uma infraestrutura distribuída e resiliente, em que os dados são processados localmente e o acesso à rede se expande de maneira dinâmica e flexível.

Segurança em redes sem fio avançada

Segundo Tanenbaum e Wetherall (2011, p. 489),



com o aumento da conectividade, surge também a necessidade de protocolos e medidas de segurança avançadas, garantindo a integridade dos dados e a privacidade dos usuários contra uma variedade de ameaças.

A segurança em redes sem fio se tornou mais crítica com o crescimento de tecnologias como IoT e 5G, que ampliam a conectividade, mas também a superfície de ataque. Tecnologias como WPA3, segmentação de redes, e autenticação multifatorial ajudam a fortalecer a proteção das redes e a privacidade dos usuários.

Imagine um ambiente corporativo onde colaboradores, dispositivos de IoT e convidados estão conectados à mesma rede sem fio. Como garantir que cada usuário acesse somente as informações de que precisa?

De acordo com Torres (2016, p. 501), “em um ambiente de rede, a segurança não é uma opção, mas uma necessidade fundamental para garantir que os dados sejam protegidos contra acessos não autorizados e ataques cibernéticos”. A segmentação de redes e o uso de senhas fortes, além do monitoramento constante, são medidas essenciais para proteger essa rede contra acessos não autorizados.



O protocolo WPA3 é um avanço importante em segurança para redes Wi-Fi. Ele oferece autenticação mais robusta e criptografia aprimorada em relação ao WPA2. Um dos principais recursos do WPA3 é o SAE (*Simultaneous Authentication of Equals*), que protege contra ataques de força bruta, tornando as redes Wi-Fi mais seguras. A autenticação multifatorial também adiciona uma camada extra de segurança, garantindo que apenas dispositivos autorizados se conectem. Acompanhemos algumas técnicas de segurança avançada em redes sem fio (Kurose; Ross, 2021):

- **WPA3:** esse é o protocolo de segurança mais atual para Wi-Fi, projetado para substituir o WPA2, oferecendo maior proteção contra ataques de força bruta e criptografia mais forte.
- **Segmentação de Rede:** dividir a rede em segmentos menores (por exemplo, uma rede para dispositivos IoT e outra para usuários) pode ajudar a conter uma possível violação.
- **Autenticação Multifatorial:** combina diferentes fatores de autenticação para assegurar que apenas usuários e dispositivos confiáveis tenham acesso.

- **VPN (Virtual Private Network):** ajuda a proteger a privacidade e a integridade dos dados transmitidos, criptografando o tráfego entre o dispositivo do usuário e o servidor.



APROFUNDANDO

Ao proteger redes sem fio, é crucial monitorar ativamente o tráfego de dados para detectar anomalias ou padrões suspeitos. Ferramentas de segurança em redes, como sistemas de detecção de intrusão (IDS) e firewalls, podem ser integradas para criar uma proteção de várias camadas, identificando e respondendo rapidamente a ameaças.

Suponha que você tenha uma rede doméstica com diversos dispositivos, incluindo TVs, smartphones, e câmeras de segurança conectadas. Ao ativar o WPA3 no seu roteador e separar as redes para diferentes tipos de dispositivos (IoT e pessoal), você aumenta a segurança geral. Essa segmentação evita que, caso um dispositivo IoT seja comprometido, o invasor acesse também seus dispositivos pessoais.

Aplicações de IoT e mobilidade

As aplicações de IoT, em conjunto com as redes móveis, são essenciais para suportar uma variedade de dispositivos conectados em movimento, como veículos autônomos, sensores de saúde e equipamentos agrícolas inteligentes. Essas tecnologias integram dispositivos, processam dados em tempo real e promovem a automação, melhorando a eficiência e a qualidade dos serviços.



PENSANDO JUNTOS

Imagine uma cidade inteligente onde sensores monitoram o tráfego, a qualidade do ar e o consumo de energia. Esses dados permitem a automação do trânsito, o controle de emissões e a gestão eficiente de recursos. Como esses sistemas auxiliam as cidades a serem mais sustentáveis e responsivas?

A IoT utiliza sensores e dispositivos conectados para capturar dados em tempo real, e a mobilidade permite que esses dispositivos funcionem em qualquer lugar, seja em ambientes urbanos, rurais ou até mesmo em veículos em movimento. Tecnologias como 5G e LoRaWAN têm um papel fundamental nesse processo, ao permitirem a conectividade necessária para esses dispositivos, independente de distância ou consumo de energia.

“A Internet das Coisas representa uma nova onda de conectividade, onde cada objeto se torna um nó dentro da rede, trazendo consigo não só benefícios, mas também desafios em termos de escalabilidade e segurança” (Tanenbaum; Wetherall, 2011, p. 512).

Vale a pena acompanhamos algumas das principais aplicações da IoT em cenários de mobilidade como:

SAÚDE

Dispositivos de monitoramento remoto ajudam a acompanhar condições de pacientes, permitindo que médicos intervenham em tempo real se necessário.

AGRICULTURA INTELIGENTE

Sensores de solo e drones ajudam agricultores a monitorar e melhorar a produção, ajustando a irrigação e o uso de fertilizantes com base em dados.

VEÍCULOS AUTÔNOMOS

Sensores e câmeras capturam dados sobre o ambiente e enviam para sistemas que controlam a navegação e segurança do veículo.

CIDADES INTELIGENTES

IoT permite o controle de iluminação pública, coleta de lixo automatizada e gestão de energia eficientemente (Totvs, 2022, on-line).

No contexto da mobilidade, o 5G NR (New Radio) fornece a largura de banda e a baixa latência necessárias para suportar aplicações complexas, como carros autônomos, nos quais uma resposta rápida é essencial para a segurança. Já o LoRaWAN é ideal para dispositivos em áreas rurais ou em locais onde o consumo de energia precisa ser mínimo, como sensores em áreas de cultivo.



INDICAÇÃO DE FILME

Black Mirror

Essa é uma série de televisão britânica antológica de ficção científica criada por Charlie Brooker e centrada em temas obscuros e satíricos que examinam a sociedade moderna, particularmente a respeito das consequências imprevistas das novas tecnologias.



A série *Black Mirror* aborda alguns cenários de IoT e mobilidade que demonstram as possibilidades e os dilemas éticos dessas tecnologias. Embora fictícia, ela levanta questões interessantes sobre os impactos da conectividade em tempo integral. Vale a pena conferir para refletir sobre os potenciais de uso (e os desafios) da IoT!

Pensemos em uma fazenda conectada: sensores de solo e de clima enviam dados sobre umidade, temperatura e nutrientes para uma central, que determina as necessidades da plantação. Com base nesses dados, o sistema pode ativar a irrigação automaticamente ou informar ao agricultor o melhor momento para adubar. Essa aplicação reduz o uso de água e insumos, otimizando a produção e contribuindo para a sustentabilidade.



EM FOCO

Estudante, para expandir seus conhecimentos sobre o assunto abordado, gostaríamos de lhe indicar a aula que preparamos especialmente para você. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

NOVOS DESAFIOS

Tenho certeza de que você já percebeu que o que você estudou aqui não são apenas conceitos abstratos. Cada tópico – seja Wi-Fi 6, 5G, segurança avançada em redes sem fio, IoT ou computação de borda (MEC) – representa habilidades e conhecimentos que estão em alta demanda no mercado de trabalho. A teoria que vimos serve como base para você se destacar em um ambiente no qual a inovação tecnológica avança a passos largos.

Imagine que em breve você configurará uma rede 5G para uma grande empresa, ou projetando uma rede segura para uma infraestrutura de IoT em uma cidade inteligente. Esse conhecimento dá a você mais que uma habilidade técnica: ele o torna um agente ativo da transformação digital. Você não está só aprendendo redes, está se preparando para ser um dos profissionais que levam conectividade, segurança e eficiência a novos patamares.

As perspectivas profissionais nessa área são amplas e empolgantes. Empresas e setores de todo o mundo precisam de especialistas para projetar, manter e proteger suas redes sem fio. E cada vez mais, a mobilidade e o volume de dados exigem soluções rápidas e seguras. Se seu interesse é em segurança, imagine atuar protegendo dados críticos em setores como saúde e finanças. Se você gosta de inovação, a área de IoT e redes de sensores abre portas para trabalhar em projetos de automação, logística e até agricultura inteligente.

Essa jornada de aprendizado é, na verdade, uma porta para o seu futuro. A tecnologia está em constante mudança, e com ela, as demandas e oportunidades de trabalho. Agora você já tem uma base sólida para apoiá-lo em qualquer direção que escolher seguir.

Espero que esse conteúdo tenha mostrado o quanto as redes sem fio e a mobilidade são áreas empolgantes, cheias de oportunidades. Cada conceito que aprendemos é a peça de um quebra-cabeça que, no mercado, faz toda a diferença. Como disse Steve Jobs, “a única maneira de fazer um excelente trabalho é amar o que você faz”. Então, leve essa paixão e curiosidade adiante, porque o que você aprendeu aqui pode ser o primeiro passo para uma carreira promissora.

**A mobilidade e o
volume de dados
exigem soluções
rápidas e seguras**

VAMOS PRATICAR

1. O Wi-Fi 6 utiliza a técnica OFDMA (*Orthogonal Frequency Division Multiple Access*), que permite dividir o canal Wi-Fi em subcanais menores, aumentando a eficiência de transmissão. Essa tecnologia reduz a latência e melhora a duração da bateria dos dispositivos conectados. Além de proporcionar maior velocidade – cerca de 40% superior às versões anteriores – o Wi-Fi 6 reduz a latência, ideal para jogos on-line e videoconferências. Com o recurso *Target Wake Time* (TWT), o Wi-Fi 6 também oferece maior eficiência energética, ao permitir que roteador e dispositivos sincronizem momentos específicos para transmissão de dados. Além disso, o Wi-Fi 6E, que opera na banda de 6 GHz, traz melhorias em ambientes congestionados, como centros urbanos, onde há maior necessidade de estabilidade e qualidade de conexão. Com essas características, o Wi-Fi 6 é uma atualização importante para um mundo cada vez mais conectado (Kurose; Ross, 2021).

Com relação às vantagens do Wi-Fi 6 em comparação com as gerações anteriores, analise as afirmativas a seguir:

- I - O Wi-Fi 6 utiliza OFDMA, permitindo que um canal Wi-Fi seja dividido em subcanais menores, melhorando a eficiência de transmissão e reduz a latência.
- II - Com o *Target Wake Time* (TWT), o Wi-Fi 6 oferece maior eficiência energética, ao permitir que os dispositivos conectados coordenem o envio de dados em horários específicos, reduzindo o consumo de energia.
- III - O Wi-Fi 6E, uma extensão do Wi-Fi 6, aumenta a capacidade de conectividade ao operar na banda de 6 GHz, melhorando o desempenho em áreas urbanas com alta densidade de sinal.

É correto o que se afirma em:

- a) I, apenas.
- b) III, apenas.
- c) I e II, apenas.
- d) II e III, apenas.
- e) I, II e III.

VAMOS PRATICAR

2. O 6G, ainda em fase de pesquisa, representa a próxima evolução das redes móveis, prometendo velocidades até 100 vezes mais rápidas que o 5G e latência extremamente baixa, possivelmente de 1 milissegundo ou menos. Esse avanço permitirá uma comunicação quase instantânea entre dispositivos, essencial para aplicações como realidade aumentada, realidade virtual e cidades inteligentes. A tecnologia 6G deve explorar frequências na faixa de terahertz (THz), permitindo uma transmissão mais rápida de dados, mas exige uma infraestrutura densa devido à cobertura limitada. A inteligência artificial terá papel crucial na adaptação da rede às condições dinâmicas do ambiente, e o 6G promete revolucionar áreas como saúde, educação e transporte, facilitando o controle remoto de dispositivos e permitindo o monitoramento em tempo real de pacientes, além de suportar bilhões de dispositivos conectados simultaneamente (Tanenbaum; Wetherall, 2011).

Qual das alternativas a seguir descreve corretamente uma das principais características ou aplicações previstas para a tecnologia 6G?

- a) O 6G deve operar na faixa de GHz, como o 5G, mas com uma largura de banda mais ampla.
- b) O 6G manterá a mesma velocidade e latência do 5G, com foco apenas na ampliação da cobertura de rede.
- c) O 6G permitirá a comunicação quase instantânea entre dispositivos, com uma latência de cerca de 1 milissegundo, o que é essencial para aplicações como veículos autônomos e cirurgias remotas.
- d) A tecnologia 6G deverá apresentar maior cobertura de sinal, exigindo menos infraestrutura densa em áreas urbanas.
- e) A principal melhoria do 6G em relação ao 5G será a capacidade de suportar mais de um dispositivo por rede, sem grandes avanços na velocidade de conexão.

VAMOS PRATICAR

3. As redes Mesh oferecem uma infraestrutura flexível, em que os nós atuam como transmissores e receptores, ampliando a cobertura de forma descentralizada e adaptativa. Por sua vez, o MEC (*Multi-Access Edge Computing*) permite que a computação ocorra na borda da rede, próxima dos usuários e dispositivos, melhorando o tempo de resposta e aliviando a sobrecarga dos servidores centrais. Isso é especialmente útil em locais como grandes estádios, onde milhares de pessoas tentam acessar a internet simultaneamente. As redes Mesh permitem que cada ponto de acesso amplie o sinal, enquanto o MEC processa dados localmente, reduzindo a latência e melhorando a experiência do usuário. Juntas, essas tecnologias viabilizam uma infraestrutura resiliente e eficiente, essencial em aplicações de mobilidade e Internet das Coisas (IoT) (Torres, 2016).

Com base no texto sobre redes Mesh e MEC, analise as afirmativas a seguir:

- I - O MEC centraliza o processamento de dados, resultando em maior latência nas aplicações de IoT.
- II - As redes Mesh são eficazes em ambientes de alta densidade de usuários, ao permitirem que cada ponto de acesso compartilhe o sinal de internet.
- III - As redes Mesh oferecem maior resiliência, pois podem redirecionar o tráfego por meio de outros nós, no caso de falha de um nó.
- IV - O uso de redes Mesh e MEC é fundamental para a redução de latência, melhorando a experiência do usuário em áreas de mobilidade.

É correto o que se afirma em:

- a) I e IV, apenas.
- b) II e III, apenas.
- c) III e IV, apenas.
- d) I, II e III, apenas.
- e) II, III e IV, apenas.

REFERÊNCIAS

KUROSE, J. F.;ROSS, K. W. **Redes de computadores e a internet**: uma abordagem top-down. São Paulo: Pearson, 2021.

SOUZA, L. B. de. **Projetos e implementação de redes**. São Paulo: Érica, 2013.

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores**. São Paulo: Pearson, 2011.

TORRES, G. **Redes de computadores**. Senhor do Bonfim, BA: Nova terra, 2016.

TOTVS. Internet das Coisas: o que é, exemplos e impactos. **Blog totvs**, 10 out. 2022. Disponível em: <https://www.totvs.com/blog/inovacoes/aplicacoes-da-internet-das-coisas/>. Acesso em: 15 out. 2024.

CONFIRA SUAS RESPOSTAS

1. Alternativa E.

A afirmativa I está correta, pois o Wi-Fi 6 utiliza a tecnologia OFDMA, que divide o canal Wi-Fi em subcanais menores. Isso permite que mais dados sejam transmitidos simultaneamente, aumentando a eficiência da rede e reduzindo a latência.

A afirmativa II está correta, pois o *Target Wake Time* (TWT) do Wi-Fi 6 coordena a transmissão de dados em momentos específicos, ajudando a economizar energia e aumentando a duração da bateria dos dispositivos conectados.

A afirmativa III está correta, pois o Wi-Fi 6E opera na nova banda de 6 GHz, ampliando o espectro disponível e melhora o desempenho em áreas congestionadas, proporcionando uma conexão mais estável em locais urbanos e em eventos com grande número de dispositivos.

2. Alternativa C.

A alternativa c) está correta porque a principal inovação do 6G é sua capacidade de oferecer uma conexão extremamente rápida e de baixa latência, com previsão de uma latência de cerca de 1 milissegundo ou menos. Essa característica permitirá uma comunicação quase instantânea, essencial para aplicações que exigem respostas em tempo real, como veículos autônomos e cirurgias remotas. A alternativa a) está incorreta, pois o 6G deve operar na faixa de terahertz (THz), não GHz. A alternativa b) está incorreta, pois o 6G deve trazer grandes avanços em velocidade e latência em relação ao 5G. A alternativa d) está incorreta porque o 6G, devido à sua frequência mais alta, terá uma cobertura mais limitada, exigindo uma infraestrutura densa para manter a estabilidade. A alternativa e) está incorreta porque o 6G promete melhorias significativas em velocidade e latência, além de suporte a uma maior quantidade de dispositivos.

3. Alternativa E.

Afirmativa I, incorreta. O MEC visa descentralizar o processamento de dados, permitindo que os dados sejam processados localmente, reduzindo a latência e não a aumenta.

Afirmativa I, correta. As redes Mesh são projetadas para ambientes de alta densidade, onde a comunicação entre pontos de acesso é crucial para garantir um sinal robusto e confiável.

Afirmativa III, correta. O MEC e as redes Mesh trabalham juntos para reduzir a latência e melhorar a experiência do usuário, especialmente em aplicações de mobilidade e IoT.

Afirmativa IV, correta. As redes Mesh são resilientes, pois se um nó falha, o tráfego pode ser redirecionado por outros nós, garantindo a continuidade da rede.

MEU ESPAÇO



ADMINISTRAÇÃO E GERENCIAMENTO DE REDES

MINHAS METAS

- Compreender o Monitoramento de Redes Avançado.
- Entender a Automação e Orquestração de Redes.
- Planejar a Capacidade e Escalabilidade de Redes.
- Executar *Troubleshooting* e Análise de Desempenho.
- Explorar Redes Autônomas e o Uso de IA.
- Implementar Segurança e Confiabilidade em Redes.
- Conhecer Ferramentas de Gestão e Relatórios de Desempenho.

INICIE SUA JORNADA

Imagine um dia normal de trabalho em uma empresa: os sistemas estão lentos e muitos funcionários reclamam que a internet não responde. Nesse cenário, problemas de rede afetam diretamente a produtividade, gerando perdas de tempo e dinheiro. Situações como essa destacam a importância de uma boa administração e gerenciamento de redes, que vai além de simplesmente ‘conectar cabos’. Como garantir uma rede rápida, segura e escalável, preparada para lidar com o crescente volume de dados e usuários?

Com o avanço da transformação digital, redes de computadores se tornaram o coração de qualquer organização. Elas são responsáveis por conectar equipes, armazenar dados e suportar aplicativos críticos. Hoje, mais do que nunca, empresas dependem da tecnologia para operar eficientemente. É aqui que a administração de redes se torna crucial, permitindo que os profissionais planejem, monitorem e ajustem a infraestrutura para atender às demandas da empresa e do mercado.

PLAY NO CONHECIMENTO

Você já se perguntou como a Netflix sabe exatamente o que você quer assistir, como carros autônomos conseguem dirigir sozinhos ou como seu assistente de voz entende o que você diz? No episódio de hoje, mergulharemos no universo fascinante da Inteligência Artificial! Descubra o que é IA e como ela aprende, em que ela já está presente em nosso cotidiano e como está moldando o futuro.. Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.

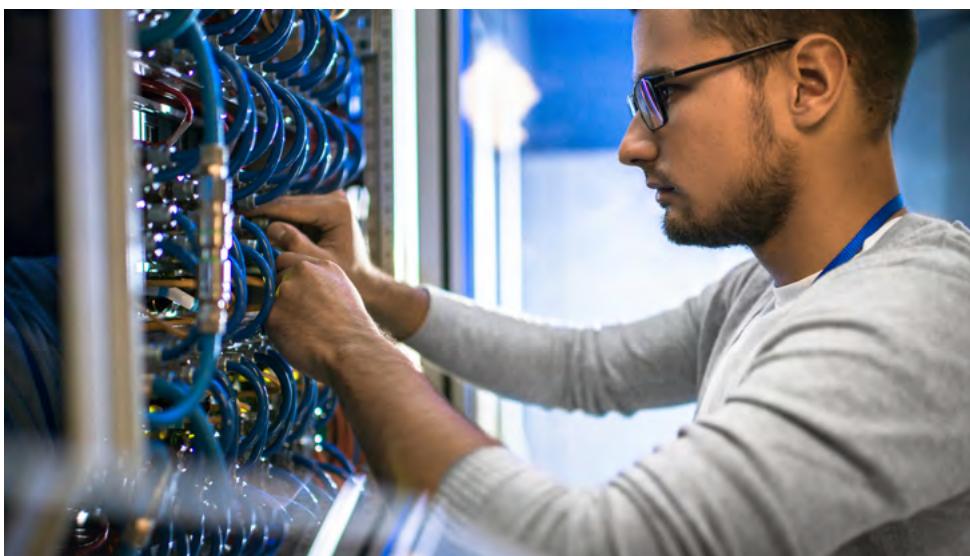
Estudante, como seria o dia a dia de um administrador de redes? É uma função dinâmica e desafiadora, que exige habilidades para monitorar tráfego, configurar dispositivos, automatizar tarefas e solucionar problemas complexos. Imagine implementar um sistema de monitoramento para identificar gargalos antes que eles afetem os usuários ou utilizar scripts para automatizar processos que levariam horas manualmente. A prática de administração de redes envolve decisões técnicas que impactam diretamente a eficiência e a segurança de uma organização.

À medida que avançarmos no conteúdo, reflita sobre o papel da administração de redes em sua futura carreira. Você será responsável por garantir a estabilidade e o bom desempenho de sistemas que suportem o funcionamento de uma empresa. Pense nas habilidades que você pode desenvolver para se destacar: conhecer ferramentas de monitoramento, aprender a planejar a capacidade da rede e entender o potencial da inteligência artificial para automatizar processos. Como você pode aplicar esses conhecimentos para se tornar um profissional estratégico e valorizado no mercado de trabalho?

VAMOS RECORDAR?

É importante entendermos os conceitos por trás do *Firewall*, como se comporta e qual a importância de termos um *firewall* configurado e ativo. Acesse o link a seguir e saiba mais: <https://www.kaspersky.com.br/resource-center/definitions/firewall>

DESENVOLVA SEU POTENCIAL



A ADMINISTRAÇÃO E O GERENCIAMENTO DE REDES

A administração e o gerenciamento de redes são áreas essenciais da infraestrutura de TI, envolvendo um conjunto abrangente de processos, técnicas e ferramentas que garantem o funcionamento seguro, eficiente e contínuo da rede de uma organização. O administrador de redes tem a responsabilidade de configurar, monitorar, atualizar e resolver problemas em diversos dispositivos de rede, como roteadores, *switches*, *firewalls* e servidores. Ele também deve assegurar a comunicação eficiente entre esses dispositivos, o que é crucial para a operação de serviços e sistemas de uma empresa.

Os sistemas de gerenciamento de redes se tornaram uma solução promissora para a implementação de teorias e técnicas no gerenciamento de redes de computadores (Souza; Soares; Silva, 2021).

Na sequência, nos aprofundaremos nas principais tarefas e explorar os conceitos essenciais de gerenciamento de redes.

Configuração e implementação

Essa etapa envolve a instalação física e a configuração lógica dos dispositivos de rede, garantindo que a infraestrutura esteja alinhada com as necessidades da organização. De acordo com Souza; Soares e Silva (2021, on-line) a configuração inclui:

ENDEREÇAMENTO IP E SUB-REDES

Planejamento e atribuição de endereços IP adequados para evitar conflitos e otimizar o uso dos recursos de rede.

CONFIGURAÇÃO DE VLANS (VIRTUAL LANS)

Segmentação da rede em sub-redes lógicas para melhorar a segurança e o desempenho.

CONFIGURAÇÃO DE ROTEADORES E SWITCHES

Implementação de roteamento dinâmico (como OSPF e BGP) e configuração de protocolos de comunicação para assegurar a conectividade.

DEFINIÇÃO DE POLÍTICAS DE SEGURANÇA

Configuração de regras de *firewall*, controle de acesso e políticas de filtragem para proteger a rede contra acessos não autorizados.

Imagine que uma empresa esteja implementando uma nova rede local (LAN). O administrador de redes precisa configurar diferentes VLANs para isolar o tráfego do departamento financeiro, de TI e de vendas, criando regras de *firewall* específicas para restringir o acesso entre essas VLANs.

Gerenciamento de desempenho

O gerenciamento de desempenho envolve o monitoramento contínuo da rede para garantir que ela opere dentro dos parâmetros estabelecidos, como latência, throughput e disponibilidade. Conforme Tanenbaum e Wetherall (2011), as técnicas e ferramentas comuns incluem:

- **Monitoramento de Latência:** avaliar o tempo de resposta da rede para detectar gargalos ou problemas de congestionamento.
- **Medição de Largura de Banda:** analisar o uso da largura de banda para evitar sobrecargas e otimizar o tráfego.
- **SLAs (Service Level Agreements):** garantir que a rede atenda aos níveis de serviço acordados, fornecendo desempenho consistente aos usuários.

Vejamos algumas ferramentas utilizadas para o gerenciamento de desempenho:

- **Zabbix:** monitorar o desempenho de dispositivos de rede e gerar alertas em tempo real quando os parâmetros ultrapassam os limites definidos.
- **Grafana e Prometheus:** utilizados para a visualização e análise de métricas de desempenho em tempo real.

Gerenciamento de falhas

De acordo com Kurose e Ross (2021), o gerenciamento de falhas visa identificar, diagnosticar e resolver problemas na rede o mais rápido possível para minimizar o tempo de inatividade.

- **Detecção de Anomalias:** utilizar ferramentas de monitoramento para detectar problemas antes que afetem o funcionamento da rede.
- **Diagnóstico de Problemas:** usar métodos como *ping*, *traceroute* e análise de logs para identificar a causa raiz da falha.
- **Correção e Recuperação:** aplicar soluções e documentar as mudanças feitas para evitar a recorrência do problema.

O gerenciamento de falhas se torna mais simples quando esse tipo de tecnologia é aplicado como solução, de acordo com Souza; Soares e Silva (2021). Em caso de uma falha em um *switch* core que afeta toda a conectividade de uma empresa, o administrador pode utilizar protocolos de redundância como HSRP (*Hot Standby Router Protocol*) ou VRRP (*Virtual Router Redundancy Protocol*) para alternar automaticamente para um dispositivo de backup, reduzindo o impacto da falha.

Gerenciamento de segurança

O gerenciamento de segurança é crucial para proteger a rede contra ameaças internas e externas. De acordo com Souza, Soares e Silva (2021) ele inclui:

- **Configuração de Firewalls e IDS/IPS:** definir regras de *firewall* para controlar o acesso e usar sistemas de detecção e prevenção de intrusões (IDS/IPS) para identificar atividades maliciosas.
- **Aplicação de Patches e Atualizações:** manter dispositivos e sistemas de rede atualizados para corrigir vulnerabilidades conhecidas.
- **Gerenciamento de Acessos:** implementar controle de acesso baseado em funções (RBAC) e autenticação multifator para proteger os recursos da rede.

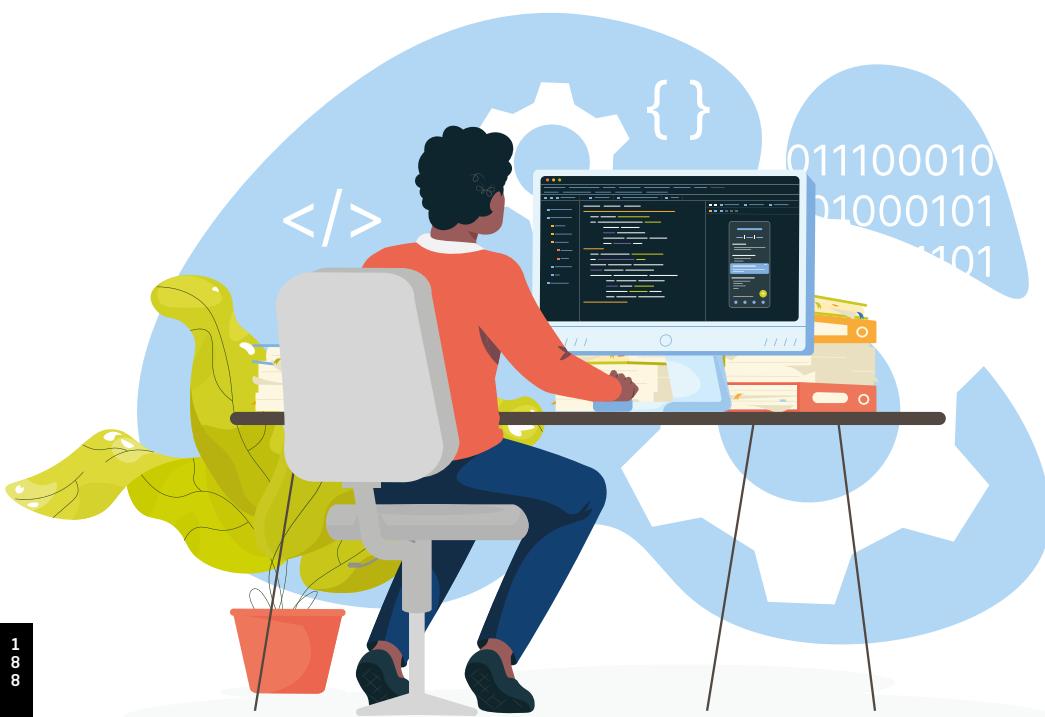
Gerenciamento de configuração

O gerenciamento de configurações envolve documentar e manter registros precisos de todas as configurações de rede, o que é fundamental para recuperação em caso de falha e *troubleshooting*. Conforme Souza, Soares e Silva (2021) as práticas incluem:

- **Versionamento de Configurações:** utilizar ferramentas para armazenar e controlar versões de arquivos de configuração (ex.: Git).
- **Automação de Configuração:** utilizar scripts e ferramentas como *ansible* para aplicar configurações de forma consistente e rápida.
- **Documentação Detalhada:** manter registros atualizados das topologias de rede, dispositivos, endereçamento IP e políticas de segurança.

Monitoramento de redes avançado

O monitoramento avançado de redes vai além do simples acompanhamento de métricas básicas, envolvendo uma análise detalhada de padrões de tráfego, desempenho e segurança. Conforme Kurose e Ross (2021), ele é essencial para prevenir problemas, identificar gargalos e otimizar a operação da rede.



DEEP PACKET INSPECTION (DPI)

Técnica que analisa o conteúdo dos pacotes em vez de apenas os cabeçalhos. É útil para detectar tráfego anômalo e evitar ataques de injeção de SQL e malware.

NETFLOW E SFLOW

Protocolos para coletar informações sobre o tráfego de rede. *NetFlow*, desenvolvido pela Cisco, permite análise detalhada de fluxos de tráfego sendo utilizado para planejamento de capacidade e segurança.

ANÁLISE PREDITIVA

Utiliza aprendizado de máquina para prever falhas e identificar padrões anômalos antes que ocorram problemas.

Uma empresa utiliza o Zabbix para monitorar sua infraestrutura de TI. O Zabbix coleta métricas de desempenho, como latência e uso de CPU, e gera alertas automaticamente quando detecta uma anomalia. Com a integração de scripts automatizados, a empresa consegue corrigir problemas imediatamente, sem intervenção manual.

Algumas Ferramentas e Tecnologias utilizadas para o monitoramento de redes, conforme Souza, Soares e Silva (2021) são:

- **Grafana e Prometheus:** usados para monitoramento em tempo real e visualização de métricas.
- **Nagios:** permite monitoramento de serviços, dispositivos e recursos de rede.

Automação e orquestração de redes

A automação e orquestração de redes são práticas que visam reduzir a complexidade e o trabalho manual na configuração e gerenciamento de redes. Elas permitem a criação de redes mais ágeis, escaláveis e menos propensas a erros.

Vejamos alguns conceitos importantes para a automação e orquestração de redes conforme Souza, Soares e Silva (2021):

- **Automação:** uso de scripts e ferramentas para executar tarefas de forma repetitiva e consistente. Por exemplo, configurar VLANs em *switches* usando o Ansible.
- **Orquestração:** coordenação de múltiplos processos automatizados para garantir que as mudanças sejam aplicadas sincronizadamente e sem impacto negativo.
- **Infraestrutura como Código (IaC):** prática de gerenciar e provisionar redes e infraestrutura por meio de scripts, utilizando ferramentas como Terraform e Ansible.

Uma grande empresa precisa configurar políticas de segurança em centenas de dispositivos. Usando Ansible, o administrador escreve um *playbook* que configura regras de *firewall* em todos os roteadores e *switches* simultaneamente, reduzindo o tempo e evitando inconsistências.

Conheça algumas ferramentas importantes para a automação:

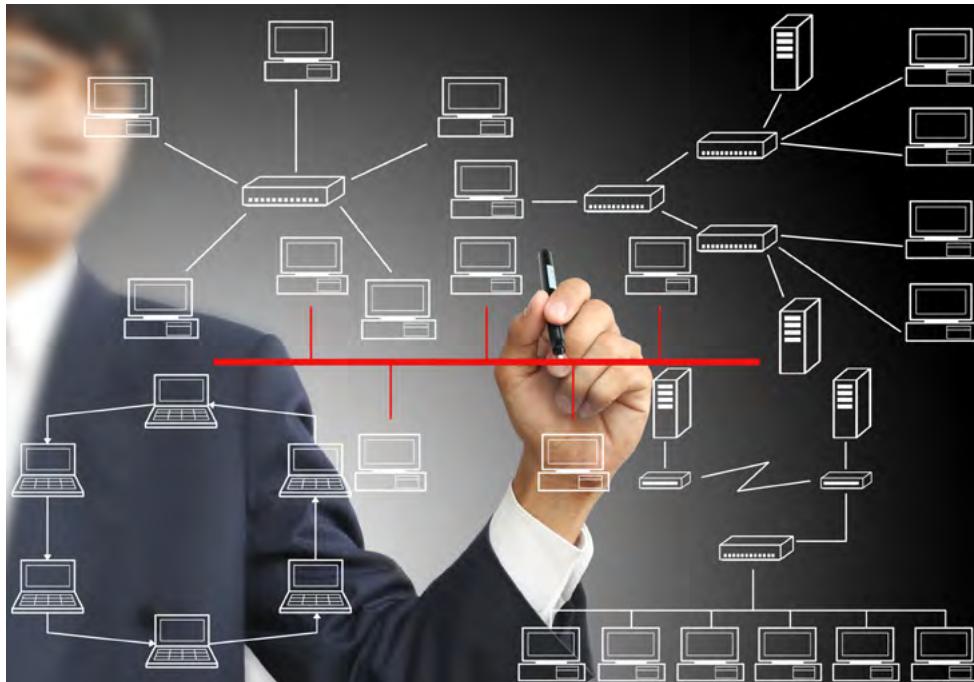
- **Terraform:** utilizado para gerenciar infraestruturas complexas, definindo-as como código.
- **Cisco DNA Center:** plataforma de automação que permite gerenciar e configurar redes de forma centralizada.

PLANEJAMENTO DE CAPACIDADE E ESCALABILIDADE

Conforme Sousa (2013), planejar a capacidade de uma rede envolve prever a demanda futura e ajustar os recursos para acomodar o crescimento. Escalabilidade refere-se à capacidade da rede de se expandir eficientemente à medida que a carga aumenta. Conheça as abordagens para Planejamento:

- **Análise de Tendências de Tráfego:** utilizando ferramentas como *NetFlow* para analisar padrões de tráfego e prever picos de uso.
- **Planejamento Proativo:** considerar o crescimento da empresa, o aumento de dispositivos conectados e novas aplicações que demandam alta largura de banda.

- **Testes de Carga e Estresse:** usar simuladores de tráfego para testar a capacidade da rede e identificar gargalos.



Troubleshooting e análise de desempenho

Troubleshooting é o processo de identificar e corrigir problemas em uma rede. Envolve um diagnóstico metódico para determinar a causa raiz dos problemas, que podem incluir lentidão, perda de conectividade ou mau desempenho. Vejamos algumas das etapas de *troubleshooting* de acordo com Souza, Soares e Silva (2021):

- **Identificação do Problema:** usar ferramentas de monitoramento para coletar informações e definir o escopo do problema.
- **Diagnóstico:** utilizar técnicas como teste de *ping*, *traceroute* e análise de logs para determinar a causa.
- **Correção:** aplicar a solução identificada, como reconfiguração de dispositivos ou ajuste de parâmetros de rede.

Redes autônomas e IA na administração de redes

Redes autônomas utilizam inteligência artificial (IA) para gerenciar, monitorar e otimizar a infraestrutura de rede de forma automática. Com o uso de aprendizado de máquina, essas redes são capazes de detectar anomalias, ajustar configurações e até corrigir problemas sem intervenção humana.

Você já imaginou uma rede que se autogerencia, como se tivesse uma mente própria? Pois é exatamente isso que as redes autônomas estão começando a fazer, utilizando Inteligência Artificial e aprendizado de máquina, essas redes prometem transformar a maneira como administraremos e gerenciamos nossa infraestrutura. Entendamos como isso funciona e por que é uma revolução tão importante.

VOCÊ SABE RESPONDER?

O que são Redes Autônomas?

Imagine uma rede que consegue se ajustar automaticamente, identificar problemas e corrigi-los sem precisar de um administrador de redes para cada detalhe. Redes autônomas são capazes disso porque utilizam IA para monitorar o tráfego, prever falhas e tomar decisões em tempo real. É como se a rede fosse um organismo vivo, que aprende e reage ao ambiente.

Em uma empresa grande, se um roteador apresentar problemas, uma rede tradicional provavelmente enviará um alerta ao administrador. Este, então, teria que analisar o problema e fazer ajustes manualmente. Em uma rede autônoma, a IA detecta o problema, identifica possíveis soluções e corrige automaticamente, muitas vezes, antes que os usuários percebam.

A IA utilizada nas redes autônomas é baseada em dados. O componente principal aqui é o aprendizado de máquina ou *Machine Learning*, um tipo de IA que permite que sistemas aprendam com grandes volumes de dados históricos e em tempo real. O apren-

A IA utilizada nas redes autônomas é baseada em dados

dizado de máquina identifica padrões e anomalias na rede, ajudando a prever problemas e melhorar a performance.

Conversaremos, agora, sobre alguns componentes principais que tornam isso possível, de acordo com Kurose e Ross (2021):

- A rede está constantemente analisando o tráfego, o uso de recursos e o desempenho dos dispositivos.
- A IA coleta dados sobre o comportamento normal da rede para criar uma 'linha de base' (ou perfil de operação normal).
- Se algo diferente da linha de base acontecer, como um aumento repentino de tráfego em um servidor, a rede detecta isso como uma anomalia e investiga o que pode estar errado.
- Quando a rede detecta uma anomalia, ela analisa o problema e sugere correções. Em muitos casos, ela pode aplicar essas correções automaticamente.

Imagine que um *switch* está sobrecarregado, a rede pode identificar esse problema e, automaticamente, redirecionar o tráfego para aliviar a carga, evitando uma possível queda.

A IA também ajuda a otimizar a rede. Ela aprende com o comportamento dos usuários e ajusta as configurações para melhorar a performance. Se a IA perceber que a maioria dos usuários acessa um servidor específico durante o horário de pico, ela pode ajustar a largura de banda para priorizar esse tráfego, reduzindo a latência e melhorando a experiência dos usuários.

Conversando com os alunos, talvez o maior ponto a ser destacado seja como as redes autônomas facilitam a vida dos administradores e melhoram a eficiência da empresa. Exploremos alguns benefícios:

- **Redução de Erros Humanos:** menos configurações manuais significa menos chance de erro. A IA pode automatizar tarefas complexas, eliminando a possibilidade de falhas causadas por erro humano.
- **Escalabilidade:** à medida que a rede cresce, fica cada vez mais difícil gerenciar tudo manualmente. As redes autônomas lidam bem com o aumento de complexidade.
- **Melhoria na Segurança:** as redes autônomas conseguem identificar e reagir a ameaças rapidamente, bloqueando ataques e protegendo os dados (Kurose; Ross, 2021).

**PENSANDO JUNTOS**

Se a rede faz tudo sozinha, o que o administrador de redes faz? Na verdade, o papel do administrador não desaparece, ele evolui. Em vez de gastar tempo configurando dispositivos manualmente e resolvendo problemas triviais, o administrador pode focar em estratégias mais complexas e na otimização da infraestrutura. Pense assim, o administrador se torna responsável por trabalhar e alimentar a IA com dados, define as políticas de segurança e analisa os relatórios de desempenho para fazer ajustes mais estratégicos.

Desafios das redes autônomas

Claro, como qualquer nova tecnologia, as redes autônomas enfrentam alguns desafios, de acordo com Souza, Soares e Silva (2021):

- **Dados de Treinamento:** a IA precisa de grandes volumes de dados para aprender. Sem dados suficientes ou com dados incorretos, a IA poderá fazer suposições erradas.
- **Complexidade:** implementar uma rede autônoma pode ser complexo e caro, inicialmente, especialmente para empresas que ainda utilizam infraestruturas legadas.
- **Segurança:** embora a IA possa melhorar a segurança, ela também pode ser alvo de ataques sofisticados. Um atacante que comprometa a IA pode potencialmente controlar a rede.

Algumas das tecnologias utilizadas para o monitoramento de forma inteligente e autônoma, de acordo com Kurose e Ross (2021), são:

SDN (SOFTWARE-DEFINED NETWORKING)

Permite separar o controle da rede da infraestrutura física, tornando a administração da rede programável, centralizada e flexível.

Facilita a automação de tarefas e o gerenciamento dinâmico de recursos, simplificando a configuração e o monitoramento da rede.

APRENDIZADO DE MÁQUINA

Análises avançadas de grandes volumes de dados coletados da rede, permitindo a identificação de padrões e anomalias de tráfego.

Utilizado para otimizar o desempenho da rede, prever possíveis problemas e ajustar configurações automaticamente com base em tendências observadas.

REDES AUTÔNOMAS DE NÍVEL 4 E 5

Redes com capacidade de autogerenciamento, que não apenas detectam e corrigem falhas, mas também se adaptam proativamente a mudanças nas condições de operação. Incluem previsão de falhas, ajuste dinâmico de parâmetros e automação total, oferecendo um nível superior de resiliência e eficiência.

Um provedor de serviços de internet implementa uma rede autônoma que, ao detectar tráfego incomum indicativo de um ataque DDoS, ajusta automaticamente as regras de *firewall* para mitigar o ataque sem intervenção manual.

De acordo com Kurose e Ross (2021), as redes autônomas representam um avanço significativo na administração de redes, permitindo que a infraestrutura se adapte de forma inteligente e automática. Ao integrar IA

e aprendizado de máquina, as redes se tornam mais resilientes, eficientes e seguras. E, para os administradores de redes, isso significa menos tempo lidando com problemas operacionais e mais tempo focado em inovação e melhoria contínua.

EM FOCO

Estudante, acreditamos que essa aula complementará e aprofundará ainda mais o seu entendimento sobre o tema. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

NOVOS DESAFIOS

Ao longo deste conteúdo, você foi apresentado a conceitos teóricos fundamentais, desde o monitoramento de redes até a automação, passando pela escalabilidade, segurança e o uso de inteligência artificial em redes. Agora, proponho conectarmos tudo isso ao mercado de trabalho e às suas possíveis oportunidades.

Em um mundo cada vez mais digital, as empresas dependem de redes robustas e confiáveis para operar, inovar e entregar valor aos seus clientes. Com a transformação digital em andamento, o gerenciamento eficiente dessas redes tornou-se uma competência essencial. **O que você aprendeu aqui não é apenas teoria, mas a base para solucionar problemas reais que surgem diariamente nas empresas.** Por exemplo, ao dominar o *troubleshooting*, você estará preparado para resolver falhas de rede que, se não solucionadas rapidamente, podem resultar em perdas significativas para a organização.

O foco na automação e orquestração de redes reflete uma tendência crescente no setor de tecnologia. Empresas estão buscando profissionais que saibam otimizar processos, automatizar tarefas repetitivas e implementar soluções escaláveis. O mercado exige administradores de rede que entendam como prever demandas futuras e planejar a capacidade da rede de forma estratégica, garantindo assim a continuidade dos negócios.

A segurança, um dos pilares do conteúdo, é outro exemplo prático de como a teoria se aplica ao ambiente profissional. Com o aumento dos ataques cibernéticos, a proteção dos dados se tornou uma prioridade máxima. Conhecer boas práticas de segurança e saber configurá-las na infraestrutura de rede é uma habilidade valorizada em qualquer empresa, seja uma pequena startup ou uma grande corporação.

O uso de ferramentas de gestão e relatórios de desempenho é o que permite a você, futuro profissional, ter controle e visão completa da rede. Essas ferramentas são indispensáveis para o dia a dia de um administrador de redes e facilitam a tomada de decisões com base em dados concretos. Ao demonstrar essas habilidades para seus empregadores, você se destaca como um profissional capacitado e preparado para enfrentar os desafios do setor.

O que você aprendeu aqui vai além da sala de aula, você está se preparando para um ambiente profissional dinâmico, que exige a combinação de conhecimento técnico, habilidades práticas e uma visão estratégica. As perspectivas de carreira são promissoras: com a crescente demanda por administradores de rede qualificados, suas chances de atuar em empresas de tecnologia, data centers, provedores de serviços de internet e grandes corporações são vastas.

VAMOS PRATICAR

1. A instalação e configuração de dispositivos de rede é uma etapa crucial para garantir que a infraestrutura atenda às necessidades da organização. O processo inclui o planejamento e a atribuição de endereços IP, a segmentação da rede em VLANs para segurança e desempenho, a configuração de roteadores e *switches* para assegurar a conectividade e a definição de políticas de segurança, como regras de *firewall* e controle de acesso (Sousa, 2013).

Durante o processo de configuração lógica de uma rede, qual dos seguintes itens é responsável por segmentar a rede em sub-redes lógicas, proporcionando melhor segurança e desempenho?

- a) Configuração de roteadores e *switches*.
 - b) Endereçamento IP e Sub-redes.
 - c) Configuração de VLANs.
 - d) Definição de Políticas de Segurança.
 - e) Implementação de Roteamento Dinâmico.
2. O monitoramento avançado de redes é fundamental para uma gestão eficiente, indo além da coleta de métricas básicas. Ele analisa padrões de tráfego, desempenho e segurança para prevenir problemas, identificar gargalos e otimizar a operação. Técnicas e ferramentas importantes incluem *Deep Packet Inspection* (DPI), que analisa o conteúdo dos pacotes; *NetFlow* e *sFlow*, protocolos para coletar dados de tráfego; e análise preditiva, que utiliza aprendizado de máquina para antecipar falhas. Ferramentas como Zabbix, Grafana, Prometheus e Nagios são amplamente utilizadas para monitoramento e alertas em tempo real (Souza; Soares; Silva, 2021).

Com base nas práticas de monitoramento avançado de redes, analise as afirmativas:

- I - *NetFlow* e *sFlow* são protocolos usados exclusivamente para monitoramento de segurança e não têm aplicação em planejamento de capacidade de rede.
- II - A análise preditiva, baseada em aprendizado de máquina, ajuda a prever falhas e identificar padrões anômalos antes que ocorra algum problema.
- III - *Deep Packet Inspection* (DPI) permite analisar o conteúdo dos pacotes, detectando tráfego anômalo e ataques, como injeção de SQL e malware.
- IV - Ferramentas como Grafana e Prometheus são usadas para monitoramento em tempo real e visualização de métricas de desempenho.

VAMOS PRATICAR

É correto o que se afirma em:

- a) I, apenas.
 - b) II e IV, apenas.
 - c) III e IV, apenas.
 - d) I, II e III, apenas.
 - e) I, II, III e IV.
3. Redes autônomas utilizam inteligência artificial (IA) para gerenciar, monitorar e otimizar a infraestrutura de rede de forma automática. Com o uso de aprendizado de máquina, essas redes conseguem detectar anomalias, ajustar configurações e até corrigir problemas sem intervenção humana. Redes autônomas podem aprender e reagir ao ambiente, ajustando-se automaticamente para evitar falhas e melhorar o desempenho (Souza; Soares; Silva, 2021).

Com base nas informações apresentadas, avalie as asserções a seguir e a relação proposta entre elas:

I - Redes autônomas utilizam inteligência artificial para monitorar e ajustar as configurações da rede automaticamente, sem a necessidade de intervenção humana.

PORQUE

II - Em uma rede autônoma, quando um problema é detectado, um administrador de rede é notificado e precisa corrigir manualmente o problema.

A respeito dessas asserções, assinale a alternativa correta:

- a) As asserções I e II são verdadeiras, e a II é uma justificativa correta da I.
- b) As asserções I e II são verdadeiras, mas a II não é uma justificativa correta da I.
- c) A asserção I é uma proposição verdadeira e a II é uma proposição falsa.
- d) A asserção I é uma proposição falsa e a II é uma proposição verdadeira.
- e) As asserções I e II são falsas.

REFERÊNCIAS

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet**: uma Abordagem Top-Down. São Paulo: Pearson, 2021.

SOUZA, L. B.de. **Projetos e implementação de redes**. São Paulo: Érica, 2013.

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores**. São Paulo: Pearson, 2011.

SOUZA, D. C. de; SOARES, J. A.; SILVA, F. R. da *et al.* **Gerenciamento de redes de computadores**. Porto Alegre: SAGAH, 2021. *E-book*.

CONFIRA SUAS RESPOSTAS

1. Alternativa C.

A configuração de VLANs permite segmentar a rede em sub-redes lógicas, melhorando tanto a segurança quanto o desempenho ao isolar o tráfego de diferentes segmentos da rede. As demais alternativas, embora importantes, não se referem diretamente à segmentação lógica da rede para esses propósitos.

2. Alternativa C.

A afirmativa III descreve corretamente a função do *Deep Packet Inspection* (DPI), que analisa o conteúdo dos pacotes para detectar tráfego anômalo. A afirmativa IV também é correta, pois Grafana e Prometheus são ferramentas comumente utilizadas para monitoramento em tempo real e visualização de métricas.

3. Alternativa C.

A Asserção I está correta, pois o texto descreve que redes autônomas utilizam inteligência artificial (IA) e aprendizado de máquina para monitorar, ajustar configurações e corrigir problemas automaticamente, sem necessidade de intervenção humana. A Asserção II é falsa, pois a principal característica das redes autônomas é que a IA não apenas detecta problemas, mas também os corrige automaticamente, sem necessidade de intervenção de um administrador, como descrito no texto.

MEU ESPAÇO



unidate





TEMA DE APRENDIZAGEM 8

REDES EM NUVEM E VIRTUALIZAÇÃO

MINHAS METAS

- Compreender conceitos fundamentais de redes em nuvem.
- Apreender os Fundamentos de Virtualização.
- Entender a importância da virtualização.
- Explorar a configuração de ambientes virtuais.
- Conceituar a utilização de contêineres e *Kubernetes*.
- Analisar Arquiteturas de Redes em Nuvem.
- Refletir sobre a implementação de segurança em ambientes virtualizados.

INICIE SUA JORNADA

No cenário atual, no qual empresas e organizações demandam escalabilidade, eficiência e segurança em suas operações digitais,

VOCÊ SABE RESPONDER?

Como atender a essas necessidades utilizando recursos limitados e infraestrutura física tradicional? Problemas como custos elevados de hardware, dificuldades de expansão e falta de flexibilidade desafiam a TI convencional. Como a computação em nuvem e a virtualização podem transformar esse paradigma?

Redes em nuvem e virtualização representam um avanço significativo na forma como gerenciamos e otimizamos recursos de TI. A nuvem permite acessar recursos sob demanda, enquanto a virtualização maximiza o uso do hardware disponível, proporcionando economia e flexibilidade. Essas tecnologias se tornaram essenciais para **aplicações modernas**, desde hospedagem de sites até a execução de grandes sistemas corporativos.



PLAY NO CONHECIMENTO

Neste podcast você vai descobrir como a computação em nuvem está transformando a maneira como armazenamos, processamos e acessamos dados. Entenda suas aplicações no dia a dia, os benefícios para empresas e indivíduos, além dos desafios e inovações que moldam o futuro dessa tecnologia essencial. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

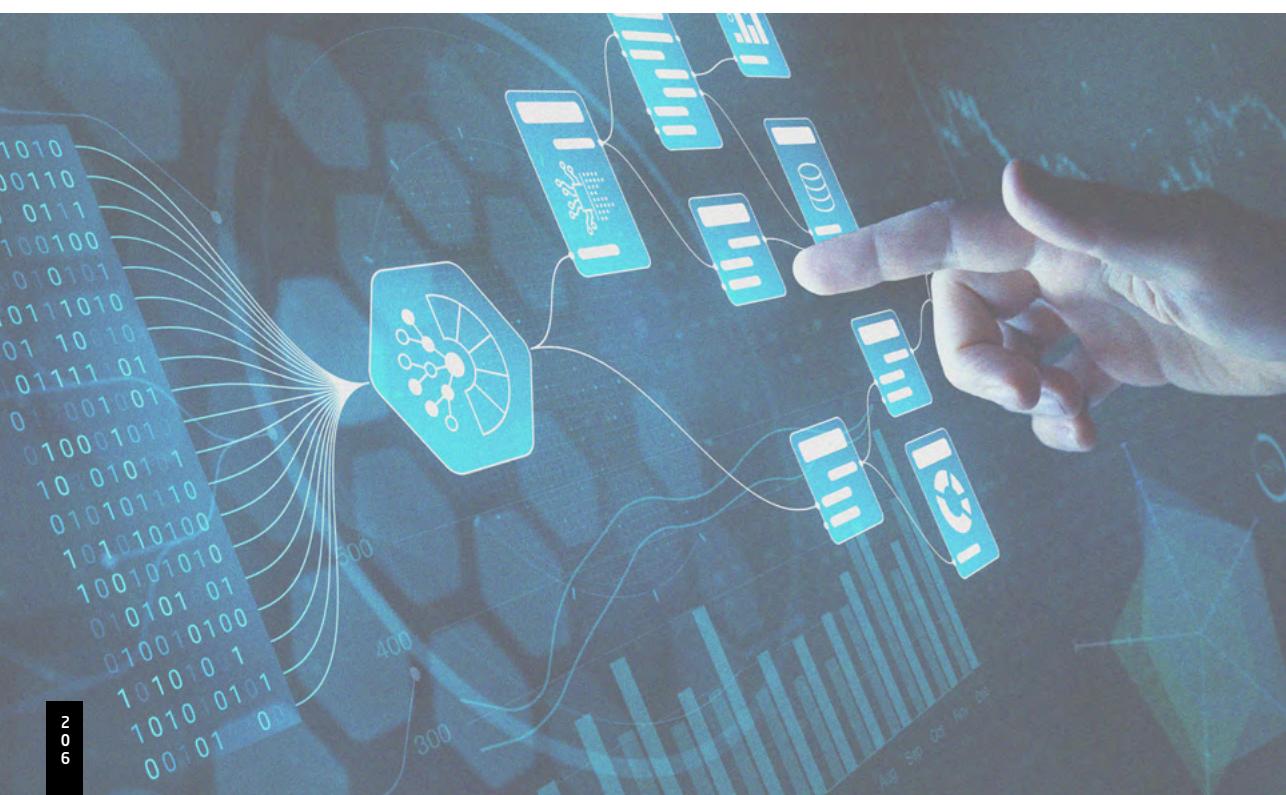
O aprendizado sobre essas tecnologias envolve a prática direta: configurar máquinas virtuais, criar redes privadas em nuvem, gerenciar contêineres e simular cenários reais de aplicação. Essa abordagem prática não apenas solidifica os

conceitos, mas também prepara para os desafios do mercado de trabalho, no qual essas ferramentas são indispensáveis.

Ao explorar redes em nuvem e virtualização, é importante refletir sobre os impactos dessas tecnologias. Como elas afetam a forma de trabalhar e interagir com sistemas digitais? Quais os desafios relacionados à segurança, custo e sustentabilidade? Compreender esses aspectos ajuda a desenvolver uma visão crítica e estratégica sobre a adoção dessas ferramentas.

VAMOS RECORDAR?

Que tal revisarmos *Cloud Computing*? O termo você já conhece, provavelmente deve ter visto em uma das nossas aulas. Acesse o link a seguir para assistir um vídeo muito interessante do canal Código Fonte TV: <https://www.youtube.com/watch?v=97loAhu2efE>



DESENVOLVA SEU POTENCIAL

FUNDAMENTOS DA VIRTUALIZAÇÃO

A virtualização é um dos pilares da computação moderna, permitindo maior eficiência no uso dos recursos físicos e simplificando a gestão de infraestrutura de TI. Essa tecnologia cria uma camada de abstração entre o hardware físico e os serviços que utilizam esses recursos, oferecendo flexibilidade, escalabilidade e redução de custos (Kurose; Ross, 2021).

Virtualização é o processo de abstrair os recursos físicos de servidores e redes, permitindo que múltiplos ambientes virtuais independentes sejam executados em uma única infraestrutura física. Isso é realizado por meio de softwares específicos que gerenciam o acesso aos recursos de hardware.

Existem **dois tipos** principais de virtualização que serão abordados na sequência: Virtualização de Servidores e Virtualização de Redes. Vamos entender qual a diferença entre um e outro nas próximas etapas do nosso tema.

**A virtualização é
um dos pilares da
computação moderna**

Virtualização de servidores

A **virtualização de servidores** utiliza *Hypervisors* para criar e gerenciar Máquinas Virtuais (conhecido também como VM). Cada máquina virtual opera como um sistema completamente independente, com seu próprio sistema operacional, aplicativos e recursos alocados, mesmo estando em um único servidor físico.

Mas o que é virtualização de servidores? Vamos começar com uma ideia simples: imagine que você pode transformar um único servidor físico em vários computadores independentes. Isso é possível graças às máquinas virtuais, e o segredo por trás delas é um software chamado *Hypervisor*.

VOCÊ SABE RESPONDER?

E o que é um *Hypervisor*, o que ele faz e como funciona?

O *Hypervisor* é como um maestro, que divide os recursos do servidor físico (Processador, Memória, Armazenamento) e distribui entre as máquinas virtuais. Assim, cada máquina virtual pode rodar seu próprio sistema operacional e aplicativos como se fosse um computador de verdade. Existem dois tipos de instalação de Hypervisor: a instalação direta no hardware (bare-metal), que visa o máximo desempenho, e a instalação sobre um sistema operacional (hospedada), mais comum em ambientes de desenvolvimento ou testes.

Agora vamos conhecer quais os *Hypervisors* mais utilizados para a virtualização conforme Silva *et al.* (2020):

VMware ESXi

O VMware ESXi é um *Hypervisor* bare-metal (instalado diretamente no hardware) amplamente usado em ambientes corporativos devido à sua robustez e confiabilidade. Ele é projetado para oferecer:

ALTA PERFORMANCE

Utiliza recursos físicos de maneira eficiente, otimizando o desempenho das VMs.

GERENCIAMENTO CENTRALIZADO

Pode ser integrado ao VMware vCenter, permitindo controle de múltiplos hosts em um único painel.

SEGURANÇA AVANÇADA

Oferece recursos como criptografia de VMs e detecção de ameaças.

RECURSOS EMPRESARIAIS

Suprimento ao balanceamento de carga, alta disponibilidade e recuperação automática em caso de falhas.

É amplamente adotado por empresas que precisam executar dezenas ou centenas de VMs com requisitos de alta disponibilidade, como bancos e data centers.

Microsoft Hyper-V

O Hyper-V é uma solução desenvolvida pela Microsoft e vem integrada gratuitamente nas edições Server do Windows e em algumas versões do Windows 10 e 11 (Pro e Enterprise). Ele oferece:

- **Integração Nativa com Windows:** funciona perfeitamente com *Active Directory*, *Azure* e outras soluções da Microsoft.
- **Facilidade de Uso:** a interface é intuitiva para administradores já acostumados com o ambiente Windows.
- **Suporte a Containers:** além das máquinas virtuais, também suporta contêineres, como *Docker*.
- **Migração ao Vivo (*Live Migration*):** permite transferir VMs em execução entre hosts sem interrupções.

Ideal para empresas que já possuem infraestrutura baseada em Windows e desejam consolidar servidores ou criar ambientes híbridos com *Azure*.

KVM (*Kernel-based Virtual Machine*)

O KVM transforma o *kernel* do Linux em um *Hypervisor*, aproveitando sua flexibilidade e desempenho. Ele é uma solução *open-source* robusta e muito poderosa.

- **Integra-se nativamente no Linux:** permite gerenciar as máquinas virtuais diretamente com ferramentas como *libvirt* e *virt-manager*.
- **Compatibilidade Ampla:** suporta uma variedade de sistemas operacionais convidados, incluindo Windows e BSD.
- **Escalabilidade e Desempenho:** é amplamente utilizado em provedores de nuvem, como AWS, para hospedar milhares de máquinas virtuais.
- **Economia:** por ser *open-source*, reduz os custos em comparação com soluções proprietárias.

Popular em ambientes de data centers e na nuvem, nos quais a escalabilidade e o controle granular são cruciais. Aqui estão alguns benefícios que fazem da virtualização uma solução interessante para as empresas, conforme Silva *et al.* (2020):

OTIMIZAÇÃO DE RECURSOS

Use o hardware ao máximo, consolidando vários servidores físicos em apenas um.

REDUÇÃO DE CUSTOS

Menos equipamentos significa menos gastos com hardware e energia.

FLEXIBILIDADE E ESCALABILIDADE

Precisa de mais VMs? É só criar. Quer migrar? Super simples.

FACILIDADE NA RECUPERAÇÃO DE DESASTRES

Snapshots e backups tornam a restauração de sistemas muito prática.

MULTIPLATAFORMA

Linux e Windows podem rodar no mesmo servidor sem problemas.

Continuando com Silva *et al.* (2020), apresentamos alguns exemplos de virtualização de servidores:

- **Data Centers:** consolidar múltiplos servidores físicos em uma infraestrutura compacta, reduzindo custos operacionais.
- **Desenvolvimento e Teste:** criação de ambientes isolados para testar software sem afetar o sistema principal.
- **Recuperação de Desastres:** backup e recuperação rápida usando *snapshots* de VMs.

A virtualização não é apenas uma ferramenta técnica, ela é uma forma revolucionária de gerenciar servidores, economizar recursos e aumentar a flexibilidade.

VIRTUALIZAÇÃO DE REDES

Conforme Comer (2016), a virtualização de redes cria **redes lógicas** abstraídas do hardware físico subjacente. Isso inclui a criação de **VLANs (Redes Locais Virtuais)**, *switches* e roteadores virtuais, que permitem maior controle, flexibilidade e automação no gerenciamento de redes. Utiliza softwares para simular funções de rede, como *switches*, roteadores e *firewalls*, que normalmente exigem um hardware dedicado.

Vejamos alguns componentes-chaves da virtualização e como se comporta mediante a sua utilização, de acordo com Sousa (2013):

- **VLAN (Virtual Local Area Network):** as VLANs são redes locais virtuais que dividem uma rede física em várias sub-redes lógicas. A segmentação da rede é feita sem a necessidade de adicionar mais equipamentos físicos, como *switches* ou roteadores. Cada rede local virtual age como uma rede independente, com seu próprio domínio de *broadcast*, embora compartilhe a infraestrutura física. Dispositivos em redes locais virtuais diferentes não se comunicam diretamente, a menos que seja configurado um roteamento entre elas.

Agora vejamos a importância de sua utilização para fundamentar a importância das redes locais virtuais e sua implementação:

- **Redução de tráfego desnecessário:** ao dividir a rede em redes locais virtuais, você isola o tráfego dentro de cada sub-rede lógica. Isso reduz o tráfego de *broadcast* e melhora a eficiência da rede.
- **Segurança:** redes locais virtuais podem ser usadas para isolar departamentos ou grupos de usuários em uma empresa, tornando mais difícil para usuários de uma rede local virtual acessarem recursos em outra rede sem passar por dispositivos de segurança como *firewalls*.
- **Gerenciamento Simplificado:** a segmentação facilita o gerenciamento e controle de recursos, além de permitir uma maior flexibilidade na alocação de endereços IP.

Conforme conhecemos e nos aprofundamos neste tema, também é de grande valia entender em qual momento usar cada uma dessas vertentes, conforme Kurose e Ross (2021).

Quando há a necessidade de dividir uma rede física em sub-redes lógicas para melhorar o desempenho e a segurança em empresas com diferentes departamentos, um exemplo é o departamento de TI e o departamento de marketing que precisam ser isolados uns dos outros e também quando se deseja reduzir o tráfego de *broadcast* ou organizar melhor a rede.

***Switches* virtuais**

Os *switches* virtuais são dispositivos de rede que operam em ambientes virtualizados, controlando o tráfego de dados entre máquinas virtuais no mesmo servidor ou em servidores diferentes. Eles funcionam de maneira semelhante aos *switches* tradicionais, mas em vez de conectar dispositivos físicos, eles conectam máquinas virtuais.

Cada máquina virtual em um servidor pode se comunicar com outras máquinas virtuais por meio de *switches* virtuais, isolando o tráfego de diferentes máquinas. Conforme Sousa (2013), vamos conhecer a importância de entendermos a sua utilização para fundamentar o tópico de *switches* virtuais:

CONECTIVIDADE ENTRE AS MÁQUINAS VIRTUAIS

Em um ambiente de virtualização, as máquinas virtuais podem se comunicar de maneira eficiente sem a necessidade de hardware físico adicional. Os *switches* virtuais tornam isso possível.

EFICIÊNCIA

Eles reduzem a necessidade de hardware de rede adicional, já que toda a infraestrutura de rede pode ser virtualizada.

SEGURANÇA E ISOLAMENTO

Eles permitem o isolamento entre máquinas virtuais, o que é crucial para garantir que uma máquina virtual comprometida não afete outras máquinas em um servidor.

Se faz necessário em data centers e ambientes de virtualização nos quais há a necessidade de comunicação eficiente e segura entre máquinas virtuais, quando você precisa otimizar recursos e reduzir custos com hardware físico, já que *switches* virtuais podem ser implementados em software e, por fim, em arquiteturas de nuvem privadas ou públicas nas quais as máquinas virtuais precisam se comunicar entre si de maneira controlada.

Roteadores virtuais

Os roteadores virtuais são instâncias de roteadores implementadas em software. Eles permitem que diferentes redes ou redes locais virtuais se comuniquem entre si, realizando funções de roteamento como um roteador físico, mas sem a necessidade de dispositivos de hardware dedicados.

Os roteadores virtuais podem operar em ambientes de nuvem ou servidores virtualizados, sendo configurados para rotear pacotes entre diferentes sub-redes. De acordo com Sousa (2013), vamos entender a importância dos roteadores virtuais e como se comportam:

- **Roteamento entre Redes Locais Virtuais:** permitem a comunicação entre as redes locais virtuais ou redes isoladas logicamente, fazendo com que os dispositivos em diferentes segmentos de rede possam trocar dados.
- **Flexibilidade e Escalabilidade:** assim como os *switches* virtuais, os roteadores virtuais proporcionam maior flexibilidade e escalabilidade em redes virtualizadas ou em nuvens.
- **Redução de Custos:** eliminam a necessidade de roteadores físicos, permitindo que a infraestrutura de rede seja mais econômica e fácil de gerenciar.

Quando é necessário rotear tráfego entre diferentes VLANs ou redes, especialmente em ambientes virtualizados ou de nuvem, em cenários de rede em que há um grande número de redes locais virtuais ou sub-redes e a implementação de roteadores físicos seria extremamente complexa ou difícil de gerenciar, quando se busca uma rede escalável e flexível sem depender de hardware físico.

NFV (*Network Functions Virtualization*)

O NFV é uma abordagem que utiliza virtualização para substituir equipamentos de rede tradicionais (como *firewalls*,平衡adores de carga, roteadores etc.) por versões virtuais desses dispositivos.

Em vez de usar hardware dedicado, as funções de rede são implementadas em software e executadas em servidores comuns, permitindo maior flexibilidade, escalabilidade e eficiência no gerenciamento da rede, destacamos a importância da NFV.

De acordo com Sousa (2013):

- **Flexibilidade e Escalabilidade:** NFV permite que as funções de rede sejam facilmente escaladas ou ajustadas conforme as necessidades da rede, sem a necessidade de adicionar ou substituir hardware físico.
- **Redução de custos:** ao eliminar a necessidade de dispositivos de rede dedicados e aproveitando a infraestrutura existente, NFV pode reduzir significativamente os custos de hardware e operação.
- **Agilidade:** as funções de rede virtualizadas podem ser rapidamente implantadas, configuradas e modificadas, aumentando a agilidade em ambientes de TI dinâmicos.

Em *data centers*, operadoras de telecomunicações ou ambientes de nuvem, em que há uma necessidade constante de evoluir e expandir as funções de rede sem adicionar hardware físico, quando se deseja substituir ou modernizar a infraestrutura de rede com maior flexibilidade e menos custos operacionais. Em ambientes de rede complexos, nos quais a virtualização de funções de rede pode trazer vantagens significativas em termos de automação e gerenciamento centralizado.

De acordo com Silva *et al.* (2020), veja no Quadro 1 e compreenda alguns desafios e algumas soluções na utilização de virtualização de redes:

DESAFIO	DESCRÍÇÃO	SOLUÇÃO
COMPLEXIDADE DE GERENCIAMENTO	Redes e servidores virtualizados podem se tornar complexos para equipes não especializadas.	Investir em treinamento ou contratar profissionais especializados para lidar com a complexidade da virtualização.
PERFORMANCE	A camada de virtualização pode introduzir latência ou <i>overhead</i> no desempenho.	Utilização de técnicas de otimização de virtualização, como alocação eficiente de recursos e utilização de hardware compatível.
SEGURANÇA	Vulnerabilidades nos <i>Hyper-visors</i> ou no gerenciamento de redes virtuais podem ser exploradas.	Aplicação de <i>patches</i> e atualizações regulares, bem como a utilização de práticas de segurança como segmentação de rede.
FERRAMENTAS DE AUTOMAÇÃO	Uso de plataformas como VMware vCenter ou OpenStack para simplificar o gerenciamento.	Implementação dessas plataformas para automatizar o gerenciamento, provisionamento e configuração de recursos.
MONITORAMENTO CONTÍNUO	Implementação de ferramentas para monitorar a performance e detectar anomalias.	Uso de ferramentas de monitoramento em tempo real, como Zabbix, Nagios ou vRealize Operations, para análise contínua.

Quadro 1 - Desafios e soluções de virtualização / Fonte: adaptado de Silva *et al.* (2020).

Esses tópicos são essenciais em ambientes de redes modernas, especialmente quando há a necessidade de escalabilidade, flexibilidade e eficiência operacional, como em data centers, ambientes de nuvem ou arquiteturas de rede virtualizada. O uso adequado dessas tecnologias pode otimizar o desempenho, reduzir custos e melhorar a segurança e o gerenciamento de redes complexas.

REDES DEFINIDAS POR SOFTWARE

As Redes Definidas por Software são uma abordagem de arquitetura de rede que separa o plano de controle do plano de dados, permitindo o gerenciamento programático e dinâmico da rede. Ao invés de depender de dispositivos de rede físicos (como *switches* e roteadores) para a tomada de decisões de roteamento e controle, o SDN centraliza essa função em um controlador de software, que pode ser programado e ajustado conforme necessário.

As tecnologias de Redes Definidas por Software estão transformando a forma como redes corporativas são projetadas, gerenciadas e otimizadas. Elas oferecem uma abordagem baseada em software para o controle e gerenciamento das redes, proporcionando flexibilidade, automação e maior eficiência no uso dos recursos, são conhecidos também como SDN e SDN-WAN.

Redes definidas por software (*Software-Defined Networking*) SDN

O SDN é uma arquitetura de rede que separa o **plano de controle** (que decide como o tráfego deve fluir) do **plano de dados** (que encaminha efetivamente o tráfego). Essa separação permite que redes sejam gerenciadas de forma centralizada, usando softwares que configuram e controlam dispositivos de rede, como *switches* e roteadores, essa arquitetura é altamente eficaz quando as redes exigem agilidade, escalabilidade, flexibilidade e um gerenciamento centralizado e automatizado.

Ela se aplica de maneira excelente em ambientes em constante evolução, como nuvens, data centers e organizações com alto crescimento ou complexidade em suas infraestruturas de rede. Vamos acompanhar alguns dos componentes principais dessa arquitetura SDN, conforme Comer (2016):

- **Controlador SDN:** é o cérebro da rede, responsável por tomar decisões de roteamento e configurá-las nos dispositivos de rede. Exemplos incluem *OpenDaylight*, ONOS e Cisco ACI.
- **Plano de Dados:** dispositivos de rede que executam as decisões feitas pelo controlador, como *switches* e roteadores.
- **Plano de Controle:** software que toma decisões de roteamento, priorização e segurança.



Ainda com o mesmo autor, observemos alguns dos benefícios que essas redes definidas por software trazem ao serem utilizadas:

AUTOMAÇÃO

Configurações podem ser feitas de forma programável, eliminando a necessidade de alterações manuais nos dispositivos.

ESCALABILIDADE

Facilita o crescimento da rede, pois o gerenciamento centralizado reduz a complexidade de configurações individuais.

CUSTOMIZAÇÃO

Permite ajustar o comportamento da rede às necessidades específicas de aplicações e serviços.

SEGURANÇA

Implementação centralizada de políticas de segurança e monitoramento contínuo.

As redes definidas por software oferecem uma série de benefícios significativos que transformam a gestão de redes corporativas. Esses recursos tornam as redes definidas por softwares essenciais para ambientes dinâmicos e em constante evolução, possibilitando redes mais ágeis, seguras e fáceis de gerenciar.

Rede WAN definida por software (*Software-Defined Wide Area Network*) SD-WAN

O SD-WAN é uma aplicação do conceito SDN focada em redes de longa distância (WAN), especialmente para conectar filiais, data centers e ambientes de nuvem. Ele permite que organizações substituam ou complementem links MPLS (*Multiprotocol Label Switching*) por conexões de internet de alta velocidade e menor custo, mantendo alta performance e segurança.

Vejamos como funciona o SD-WAN e alguns dos seus benefícios, de acordo com Kurose e Ross (2021):

- **Controlador Centralizado:** gerencia todas as conexões WAN, otimizando o tráfego com base em políticas de negócios e desempenho.
- **Multiplicidade de Links:** pode usar diferentes tipos de links (MPLS, internet banda larga, LTE/5G) de forma transparente, redirecionando o tráfego conforme necessário.
- **Monitoramento Contínuo:** mede a qualidade dos links (latência, perda de pacotes, *jitter*) para garantir a melhor experiência para os usuários.
- **Redução de Custos:** utiliza conexões de internet mais econômicas em vez de depender exclusivamente de MPLS.
- **Otimização do Desempenho:** direciona automaticamente o tráfego pela rota mais eficiente, garantindo qualidade de serviço (QoS) para aplicativos críticos.
- **Facilidade de Gerenciamento:** políticas são configuradas e gerenciadas centralmente, reduzindo a complexidade.
- **Flexibilidade:** permite adicionar novos sites rapidamente, sem a necessidade de grandes investimentos em infraestrutura física.

Apresentaremos, a seguir, um infográfico comparativo entre SDN (*Software-Defined Networking*) e SD-WAN (*Software-Defined Wide Area Network*) para esclarecer as diferenças fundamentais e destacar as aplicações específicas de cada tecnologia:

SDN	SD-WAN
Objetivo principal: Gerenciamento de redes locais (LAN e data centers).	Objetivo principal: Gerenciamento de redes geograficamente distribuídas (WAN).
Qual o foco? Controle programável de dispositivos de rede.	Qual o foco? Otimização de conectividade entre filiais, nuvens e data centers.
Quais são os Componentes chave? Controlador SDN, switches e roteadores programáveis.	Quais são os Componentes chave? Controlador SD-WAN, múltiplos links WAN e gateways.
Quais são os casos de uso? Data centers, redes definidas por políticas e automação de redes locais.	Quais são os casos de uso? Redes corporativas que conectam filiais e ambientes híbridos.
Quais são os benefícios primário? Automação e controle centralizado da infraestrutura.	Quais são os benefícios primário? Redução de custos e otimização de desempenho em redes distribuídas.



ARQUITETURAS DE REDES EM NUVEM

Redes em nuvem suportam a conectividade necessária para serviços distribuídos em plataformas como Amazon AWS, Microsoft Azure e Google Cloud. A seguir, vamos conhecer duas das principais arquiteturas de redes, como exemplo de Kurose e Ross (2021):

VPC (Virtual Private Cloud): rede isolada em uma nuvem pública, permitindo controle total sobre a configuração e segurança.

Arquitetura Híbrida: integra redes locais e em nuvem, permitindo elasticidade e flexibilidade enquanto mantém dados críticos no local.

As arquiteturas de redes em nuvem são projetadas para suportar a conectividade de serviços e aplicações distribuídos em ambientes de nuvem pública, privada e híbrida. Essas arquiteturas utilizam recursos como redes privadas virtuais (VPCs), sub-redes, *gateways* de internet,平衡adores de carga e mecanismos de segurança avançados para garantir uma infraestrutura segura, escalável e eficiente.

Vejamos, na sequência, as arquiteturas de Redes Virtuais e VPC (*Virtual Private Cloud*) ou Nuvem Privada Virtual, sua utilização e seus componentes principais.

Redes virtuais e VPC (*Virtual Private Cloud*)

Uma **VPC (Virtual Private Cloud)** é uma rede isolada dentro de uma nuvem pública (como AWS, Azure ou Google Cloud). Ela fornece controle completo sobre a configuração da rede, incluindo sub-redes, tabelas de roteamento e *gateways* de internet, permitindo a personalização conforme as necessidades de cada aplicação.

Componentes de uma VPC

A **VPC (Virtual Private Cloud)** é uma rede privada isolada dentro de um ambiente de nuvem pública, permitindo o controle sobre a comunicação e a segurança dos recursos. Para compreender melhor seu funcionamento, é essencial

não apenas conhecer seus componentes, mas também entender onde, quando e como utilizá-los.

Os principais componentes de uma VPC incluem:

SUB-REDES

Dividem a VPC em segmentos menores. As sub-redes podem ser públicas, acessíveis pela internet, ou privadas, restritas a comunicações internas.

TABELAS DE ROTEAMENTO

Definem como o tráfego será direcionado dentro da VPC e para redes externas.

GATEWAYS

Permitem a comunicação da VPC com redes externas, como a internet (via Internet Gateway) ou redes locais (via VPN Gateway ou Direct Connect).

NAT GATEWAYS

Permitem que instâncias privadas acessem a internet de forma segura, sem serem diretamente expostas.

LISTAS DE CONTROLE DE ACESSO (ACLS) E GRUPOS DE SEGURANÇA

Definem políticas de segurança para controlar quais conexões são permitidas dentro e fora da VPC.

FLEXIBILIDADE

Permite a criação de redes personalizadas para atender requisitos específicos, como separação de ambientes de desenvolvimento, teste e produção.

Vejamos um exemplo prático para compreender a utilização e facilitar seu entendimento sobre o assunto: imagine uma empresa que precisa hospedar um aplicativo web na nuvem. Para garantir segurança e eficiência, a empresa pode configurar sua VPC da seguinte maneira:

- Criar uma **sub-rede pública** para hospedar servidores web acessíveis aos clientes.
- Criar uma **sub-rede privada** para armazenar bancos de dados e serviços internos.
- Utilizar uma **tabela de roteamento** que direcione tráfego externo para a sub-rede pública e manter a comunicação interna protegida.
- Configurar um **Internet Gateway** para permitir que os servidores web sejam acessados pela internet.
- Adicionar um **NAT Gateway** para as instâncias privadas poderem atuarizar pacotes sem exposição direta.
- Aplicar **grupos de segurança e ACLs** para restringir acessos, permitindo conexões apenas nas portas necessárias.

Essa abordagem garante que o sistema seja escalável, seguro e otimizado para atender às necessidades do negócio.

Os componentes da VPC são ferramentas poderosas para construir redes seguras, escaláveis e eficientes na nuvem. Quando usados corretamente, eles oferecem uma flexibilidade notável para atender às necessidades específicas de uma organização, desde o isolamento de ambientes até a criação de redes personalizadas.

A aplicação correta desses componentes em cenários do mundo real como em ambientes de produção, desenvolvimento e integração de redes híbridas, é fundamental para garantir que sua infraestrutura na nuvem seja segura, eficiente e fácil de gerenciar.

Sub-redes

As sub-redes são divisões de uma VPC que organizam recursos em grupos lógicos, permitindo o controle granular sobre o tráfego de rede e a segurança, veja as definições a seguir, conforme Kurose e Ross (2021):

- **Sub-redes Públicas:** usadas para recursos que precisam de acesso direto à internet, como servidores web.
- **Sub-redes Privadas:** projetadas para recursos internos, como bancos de dados e serviços *backend*, protegidos de acessos externos.

ZOOM NO CONHECIMENTO

Sub-redes desempenham um papel essencial no design de redes em uma VPC (*Virtual Private Cloud*), pois permitem segmentar recursos de forma lógica, atendendo a requisitos específicos de segurança, conectividade e desempenho.

Sub-redes públicas são ideais para hospedar recursos que precisam de acesso direto à internet, como servidores web e平衡adores de carga, proporcionando a visibilidade necessária para interagir com usuários externos. Já as **sub-redes privadas** são projetadas para recursos sensíveis e internos, como bancos de dados e serviços *backend*, que não devem ser acessados diretamente do exterior, garantindo um nível adicional de proteção.

A escolha e configuração adequada de sub-redes impactam diretamente na eficiência e nos custos da infraestrutura. Sub-redes privadas, por exemplo, podem ser combinadas com NAT *Gateways* para permitir acesso seguro à internet, mantendo o isolamento necessário. Já as sub-redes públicas podem exigir *gateways* de internet, o que pode agregar custos adicionais, dependendo do provedor de nuvem.

A segmentação em sub-redes contribui para a separação de ambientes (desenvolvimento, teste e produção), ajudando a gerenciar e escalar recursos de forma mais organizada. Desse modo, a aplicação estratégica de sub-redes não só melhora a segurança e o desempenho da rede, mas também pode otimizar custos operacionais a longo prazo.

Balanceadores de carga

Os balanceadores de carga distribuem o tráfego de rede uniformemente entre várias instâncias de um aplicativo. Eles aumentam a escalabilidade e melhoram a disponibilidade de serviços. Escalar automaticamente para lidar com aumento no tráfego pode reduzir o impacto de falhas ao redirecionar solicitações para instâncias saudáveis.

A seguir, de acordo com Comer (2016), conhiceremos alguns tipos de平衡adores de carga:

Balanceador de Carga Físico: esse tipo de balanceador é uma máquina física dedicada que distribui o tráfego de rede entre os servidores. Ele pode ser usado em ambientes nos quais as necessidades de performance e controle são mais específicas e em larga escala.

Exemplo: uma organização pode usar平衡adores de carga físicos em seus data centers para garantir que o tráfego seja distribuído de maneira eficiente entre os servidores de aplicação. Esses dispositivos são frequentemente usados quando a necessidade de controle de tráfego é mais rigorosa ou quando a organização já possui uma infraestrutura de TI robusta.

Balanceador de Carga Virtual: essa solução é baseada em software e pode ser implementada em servidores, máquinas virtuais ou até mesmo na nuvem. O balanceamento de carga virtual é mais flexível e escalável, sendo uma opção popular em ambientes dinâmicos e de nuvem.

Exemplo: empresas que utilizam AWS *Elastic Load Balancing* (ELB) ou Azure *Load Balancer*. Esses平衡adores de carga baseados em software podem escalar automaticamente conforme o tráfego de rede aumenta ou diminui.



Tipos de balanceadores de carga

Ainda segundo Comer (2016), os balanceadores de carga podem ser classificados em duas categorias principais com base no nível de camada no qual atuam, como podemos observar neste quadro comparativo:

L4 (CAMADA DE TRANSPORTE)	L7 (CAMADA DE APLICAÇÃO)
<p>Como funciona: o balanceador de carga da camada L4 trabalha com informações de endereços IP e portas, operando no nível de pacotes de rede (TCP/UDP).</p>	<p>Como funciona: o balanceador de carga da camada L7 analisa informações mais detalhadas da requisição, como cabeçalhos HTTP/HTTPS, URLs, ou dados de sessão. Ele pode tomar decisões mais complexas com base no conteúdo da solicitação.</p>
<p>Exemplo de uso: suponha uma aplicação de <i>e-commerce</i> na qual muitos usuários estão acessando simultaneamente. O balanceador L4 distribuiria o tráfego entre servidores de forma eficiente com base nos endereços IP e portas, garantindo que cada servidor tenha uma carga equilibrada de tráfego, mas sem examinar o conteúdo da requisição.</p>	<p>Exemplo de uso: imagine um site de streaming de vídeo no qual o tráfego é direcionado para diferentes servidores dependendo do tipo de conteúdo (por exemplo, vídeos de alta definição versus vídeos em baixa definição). O balanceador L7 analisaria o cabeçalho da requisição HTTP e redirecionaria o tráfego para os servidores apropriados com base na necessidade de largura de banda ou outros critérios.</p>

Quadro 2 - Comparação entre L4 e L7 / Fonte: adaptado de Comer (2016).

Suponha que uma empresa de *e-commerce* tem um site que recebe picos de tráfego, especialmente durante a *Black Friday*. Se a carga não for balanceada corretamente, o site pode ficar lentamente sobrecarregado ou até mesmo indisponível, resultando em uma perda significativa de vendas.

Vejamos o uso dessas camadas:

- **Uso de L4:** em um cenário no qual o tráfego precisa ser distribuído uniformemente entre os servidores, o balanceador L4 pode ser usado para garantir que o tráfego seja distribuído com base em IP e portas. Isso ajudaria a garantir que os servidores de aplicação recebam uma carga equilibrada.

- **Uso de L7:** se o site de *e-commerce* precisar lidar com diferentes tipos de tráfego, como páginas de produtos, carrinho de compras e processamento de pagamentos, um balanceador L7 pode ser usado para direcionar as requisições com base no conteúdo da URL ou tipo de solicitação. Por exemplo, tráfego de checkout pode ser redirecionado para servidores especializados, enquanto o tráfego de visualização de produto é distribuído de forma equilibrada entre servidores gerais.

O balanceamento de carga pode escalar automaticamente para lidar com o aumento do tráfego, com instâncias de servidor sendo adicionadas conforme necessário. Caso algum servidor falhe, o tráfego pode ser redirecionado para outras instâncias saudáveis, minimizando o impacto de falhas e garantindo a continuidade do serviço.

Portanto, o balanceamento de carga pode ser feito tanto de forma física (usando dispositivos dedicados) quanto virtual (via software). A escolha entre L4 e L7 depende do nível de controle e complexidade necessário para distribuir o tráfego de forma eficiente e segura.

Em situações de alto tráfego ou onde há necessidade de flexibilidade, como em empresas de *e-commerce* ou serviços de streaming, o balanceamento de carga pode ser uma solução essencial para garantir alta disponibilidade e desempenho da rede.

ARQUITETURA HÍBRIDA

A arquitetura híbrida conecta ambientes locais (*on-premises*) a nuvens públicas, combinando os benefícios de ambos os modelos. A abordagem de arquitetura híbrida é útil para empresas que precisam de flexibilidade, mas desejam manter dados críticos ou aplicativos específicos em suas próprias instalações.

Vamos conferir algumas características da arquitetura híbrida, conforme Comer (2016).

REDE PRIVADA VIRTUAL

Conectam redes locais a uma nuvem pública por meio de túneis criptografados.

GERENCIAMENTO UNIFICADO

Ferramentas que permitem monitorar e gerenciar recursos locais e em nuvem de forma centralizada.

ELASTICIDADE

Permite que cargas de trabalho sejam transferidas para a nuvem em momentos de pico.

SEGURANÇA

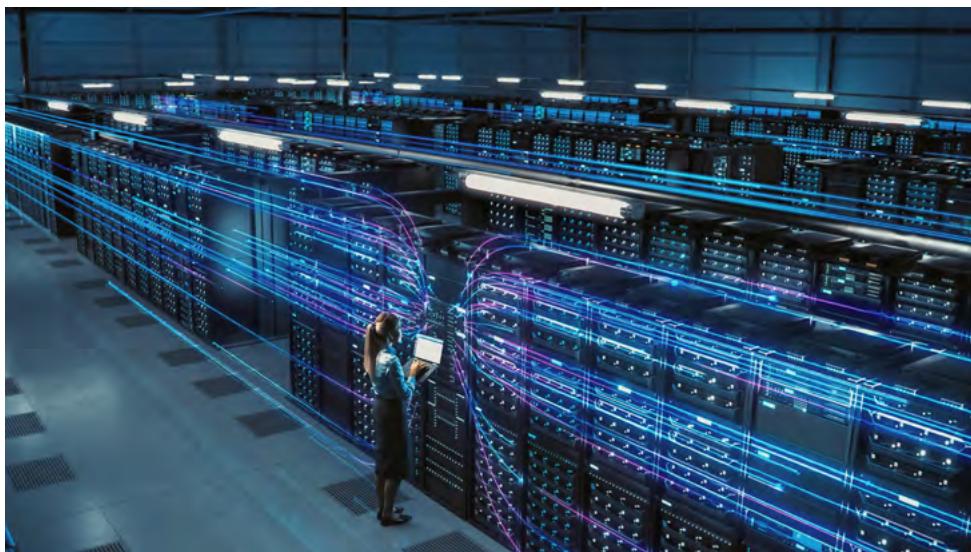
Mantém dados críticos em infraestrutura local, atendendo às regulamentações de conformidade.

REDUÇÃO DE CUSTOS

Aloca recursos em nuvem apenas quando necessário, otimizando gastos.

Silva *et al.* (2020) apontam algumas dicas práticas que podem ser realizadas para a implementação de arquitetura híbrida em uma empresa. Vamos conhecê-las:

- **Redundância e Alta Disponibilidade:** implemente平衡adores de carga que operem entre diferentes zonas de disponibilidade e configure gateways redundantes para eliminar pontos únicos de falha, garantindo continuidade operacional.
- **Monitoramento e Logs:** adote ferramentas como AWS *CloudWatch*, Azure Monitor ou Google *Cloud Operations* para acompanhar o desempenho da rede. Ative logs de acesso e tráfego para facilitar auditorias e detectar anomalias rapidamente.
- **Automação e Infraestrutura como Código:** utilize ferramentas como *Terraform* ou AWS *CloudFormation* para projetar e gerenciar redes de maneira automatizada, garantindo consistência e controle de versões nos ambientes.



- **Políticas de Segurança:** aplique criptografia para proteger dados em trânsito e armazenados. Configure regras de firewall estritas e políticas de entrada e saída para reforçar a segurança da infraestrutura.

CONTÊINERES, KUBERNETES E ORQUESTRAÇÃO DE CONTÊINERES

A tecnologia de contêineres e orquestração revolucionou o desenvolvimento e a implantação de aplicativos, oferecendo portabilidade, escalabilidade e eficiência. Este conceito combina contêineres (unidades leves e independentes que empacotam um aplicativo e suas dependências) e ferramentas de orquestração, como o *Kubernetes*, para gerenciar, escalar e garantir a alta disponibilidade de aplicativos.

Por exemplo o *Docker*, que facilita o empacotamento de aplicativos e suas dependências em unidades leves e portáteis. O *Kubernetes*, por sua vez, automatiza o gerenciamento de contêineres em *clusters*, permitindo escalabilidade e alta disponibilidade.

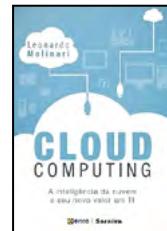
Para nos aprofundarmos cada vez mais, é importante conhecermos novas obras e conteúdos sobre o tema que estamos estudando, por isso indico a leitura a seguir sobre *Cloud Computing*.



INDICAÇÃO DE LIVRO

Cloud Computing: a inteligência na nuvem e seu novo valor em TI

Essa obra de Leonardo Molinari, apresenta uma introdução à computação em nuvem, abordando conceitos fundamentais, tendências e tecnologias emergentes. Explora o impacto da nuvem nas organizações, destacando aplicações práticas, infraestrutura e desafios da migração de sistemas tradicionais. A obra aprofunda temas como desenvolvimento e testes na nuvem, além de analisar serviços e estratégias alinhadas ao mercado. Também aborda a relação da nuvem com a transformação digital, explorando Inteligência Artificial (IA), Internet das Coisas (IoT) e Big Data.



Conceito de contêineres

Os **contêineres** são ambientes isolados que encapsulam um aplicativo junto com todas as suas dependências (bibliotecas, configurações e arquivos de sistema) em uma única unidade. Eles são mais leves do que máquinas virtuais, pois compartilham o mesmo *kernel* do sistema operacional subjacente.

Conforme Silva *et al.* (2020), vejamos algumas características principais dos contêineres:

- **Leveza:** compartilham o *kernel* do sistema operacional, tornando-os mais rápidos para iniciar e consumir menos recursos.
- **Portabilidade:** um contêiner criado em uma máquina funciona de forma idêntica em qualquer ambiente compatível.
- **Consistência:** reduzem problemas de dependência, garantindo que o ambiente do desenvolvedor seja idêntico ao de produção.

Agora vamos conhecer algumas ferramentas comuns para conteinerização, de acordo com Silva *et al.* (2020):

- **Docker:** a tecnologia mais amplamente usada para criar e gerenciar contêineres.
- **Podman:** uma alternativa ao Docker, sem a necessidade de daemon centralizado.
- **CRI-O:** implementação leve para execução de contêineres em clusters Kubernetes.

A utilização de contêineres permite maior eficiência, escalabilidade e portabilidade no desenvolvimento e gerenciamento de aplicações, simplificando a integração em ambientes *multicloud* e híbridos.

Kubernetes: orquestração de contêineres

Kubernetes é uma plataforma *open-source* para gerenciar contêineres em *clusters*. Ele automatiza tarefas como provisionamento, escalabilidade, balanceamento de carga, monitoramento e recuperação de falhas, permitindo a execução eficiente de aplicativos distribuídos.

A seguir, alguns dos componentes principais do *Kubernetes*, conforme Silva *et al.* (2020):

- **Cluster:** conjunto de máquinas (físicas ou virtuais) que executam os contêineres e são gerenciadas pelo *Kubernetes*.
- **Master Node (Control Plane):** coordena o *cluster*, gerenciando o agendamento e a escala.
- **Worker Nodes:** executam os contêineres e se comunicam com o nó mestre.
- **Pod:** unidade mínima do *Kubernetes*, que encapsula um ou mais contêineres com recursos compartilhados, como IP e sistema de arquivos.
- **Service:** expõe um conjunto de *pods* como uma única entidade, garantindo conectividade estável mesmo com mudanças dinâmicas no *cluster*.
- **Ingress:** gerencia o acesso externo ao *cluster*, como HTTP e HTTPS.
- **Deployment:** define o estado desejado de um aplicativo (número de réplicas, versão do contêiner etc.) e garante que o *cluster* alcance esse estado.
- **ConfigMaps e Secrets:** armazenam configurações e credenciais sensíveis separadamente dos contêineres.
- **Kubelet:** agente que roda em cada nó e gerencia os pods alocados para ele.

Outro tópico importante de ser abordado em nossa disciplina é a orquestração de containers. Segundo Kurose e Ross (2021):

- **A orquestração de contêineres:** é o processo de gerenciar múltiplos contêineres, que pode garantir:
 - **Automação:** gerenciamento automático de escalabilidade, implementação e atualizações.



- **Escalabilidade:** ajustar dinamicamente o número de réplicas de contêineres com base na demanda.
- **Alta Disponibilidade:** reimplantar automaticamente contêineres em caso de falhas.
- **Distribuição de Recursos:** alocar recursos do *cluster* de forma eficiente.

Segurança em ambientes virtuais e multicloud

A segurança em ambientes virtualizados e *multicloud* é essencial para proteger recursos críticos, incluindo dados, aplicações e infraestruturas, de ameaças como violações de dados, ataques DDoS, falhas de configuração e malware. A complexidade desses ambientes, nos quais diferentes plataformas e tecnologias coexistem, aumenta a superfície de ataque, exigindo estratégias robustas de segurança.

Em um mundo cada vez mais digital, refletir sobre a segurança em ambientes virtuais tornou-se indispensável. A infraestrutura de TI sustenta operações críticas de empresas, governos e indivíduos, tornando-se um alvo constante de ameaças.

VOCÊ SABE RESPONDER?

Diante desse cenário, como garantir que os serviços permaneçam disponíveis e protegidos?

A adoção de boas práticas de segurança vai além de uma obrigação técnica, trata-se de uma postura estratégica e preventiva. A automatização e a infraestrutura como código surgem como ferramentas essenciais para manter a coerência e a integridade das configurações de segurança, reduzindo erros humanos e garantindo que as políticas de proteção sejam aplicadas de maneira uniforme. Além disso, a criptografia desempenha um papel crucial na proteção das informações, assegurando que apenas pessoas autorizadas possam acessá-las.

Vamos conversar sobre a segurança em ambientes virtuais e como ela pode ser trabalhada de maneira eficaz. Conforme Comer (2016), há várias frentes que precisam de atenção para garantir que seus sistemas estejam protegidos. Vamos explorar cada uma delas juntos:

- **Máquinas Virtuais (VMs) e Contêineres:** primeiro, é importante entender que as máquinas virtuais (VMs) devem estar bem isoladasumas das outras. Isso evita que dados de uma máquina acabem sendo acessados por outra no mesmo hardware físico. Já os contêineres, como os usados no *Docker* ou *Kubernetes*, precisam de recursos como *namespaces* e *cgroups* para manter os processos isolados e os recursos bem distribuídos. Aqui, o foco é minimizar qualquer possibilidade de invasão ou mau uso.
- **Redes Virtuais:** as redes virtuais também desempenham um papel central. Com o uso de redes privadas virtuais bem configuradas e *firewalls* robustos, você pode controlar o tráfego que entra e sai da sua infraestrutura, segmentando as comunicações de forma segura. Imagine sua rede como uma cidade com zonas bem definidas: cada segmento tem suas regras e restrições para manter a ordem e a segurança.
- **Gestão de Identidades e Acessos:** agora vamos falar de quem pode acessar o quê. A autenticação multifator (MFA) é como ter uma chave e um alarme para entrar em um cofre, só a senha não basta. O princípio do menor privilégio garante que cada usuário ou aplicação tenha apenas as

permissões essenciais para sua função, reduzindo riscos desnecessários. Ferramentas como AWS IAM e *Azure Active Directory* ajudam a padronizar essas permissões de maneira eficiente.

- **Monitoramento e Auditoria:** a segurança não termina com a configuração; é preciso estar sempre atento. Logs centralizados e monitoramento contínuo ajudam a registrar tudo o que acontece e a detectar anomalias em tempo real. Por exemplo, se algo estranho surgir, como acessos incomuns, ferramentas como *Splunk* ou *CloudTrail* podem alertá-lo imediatamente. Melhor ainda, respostas automatizadas podem bloquear ameaças assim que forem identificadas.
- **Proteção contra Ameaças:** por último, mas não menos importante, temos a proteção contra ameaças. Configurar *firewalls* virtuais com regras precisas ajuda a barrar tráfego indesejado. Já para ataques como DDoS, serviços especializados como AWS *Shield* podem aliviar o impacto. Soluções anti-malware e de detecção de intrusão são como guardiões que analisam o ambiente constantemente em busca de atividades maliciosas.
- Com tudo isso em mente, lembre-se de que a segurança em ambientes *multicloud* apresenta desafios extras. Cada provedor tem suas particularidades, o que pode aumentar a complexidade na padronização de políticas e ferramentas, configurações incorretas e a falta de visibilidade sobre eventos entre nuvens podem criar brechas. Por isso, é essencial adotar uma abordagem integrada e sempre revisar as práticas de segurança.

A segurança em ambientes virtuais não é apenas uma obrigação, mas uma estratégia para garantir a continuidade e a proteção do seu trabalho. Quando bem implementada, ela proporciona tranquilidade e confiança, permitindo que você aproveite ao máximo os benefícios das tecnologias em nuvem.

Uma reflexão sobre a implementação de boas práticas de segurança em ambientes virtuais é essencial para proteger a infraestrutura e garantir a continuidade dos serviços. A automatização e a infraestrutura como código ajudam a manter a consistência e a integridade das configurações de segurança, enquanto a criptografia de dados assegura a confidencialidade das informações.

Estratégias robustas de backup e recuperação garantem a resiliência em caso de desastres, e a segmentação de redes contribui para a proteção de sistemas críticos contra acessos não autorizados, de acordo com Souza (2021, on-line):

- **Automatização e Infraestrutura como Código:** utilize ferramentas como *Terraform* ou *AWS CloudFormation* para implementar e validar configurações de segurança consistentemente.
- **Criptografia de Dados:** criptografe dados em repouso e em trânsito utilizando TLS/SSL e chaves gerenciadas por serviços como AWS KMS ou *Azure Key Vault*.
- **Backups e Recuperação de Desastres:** planeje estratégias de backup e recuperação utilizando soluções como *snapshots* de VMs e replicação multirregional.
- **Segmentação de Rede e Controle de Tráfego:** configure sub-redes privadas para servidores críticos e limite o acesso externo.
- **Educação e Treinamento:** treine equipes em práticas de segurança específicas para ambientes *multicloud*, como identificação de riscos e resposta a incidentes.

Dessa forma, mais do que uma preocupação técnica, a segurança em ambientes virtuais deve ser encarada como uma cultura organizacional, na qual a prevenção, a automação e a resiliência caminham juntas para garantir a proteção da infraestrutura e a continuidade dos serviços, conforme reforça Souza (2021, on-line).

Por fim, investir em educação e treinamento contínuos para as equipes fortalece a capacidade de identificar riscos e responder rapidamente a incidentes, criando uma cultura de segurança sólida e eficaz em ambientes *multicloud*.



EM FOCO

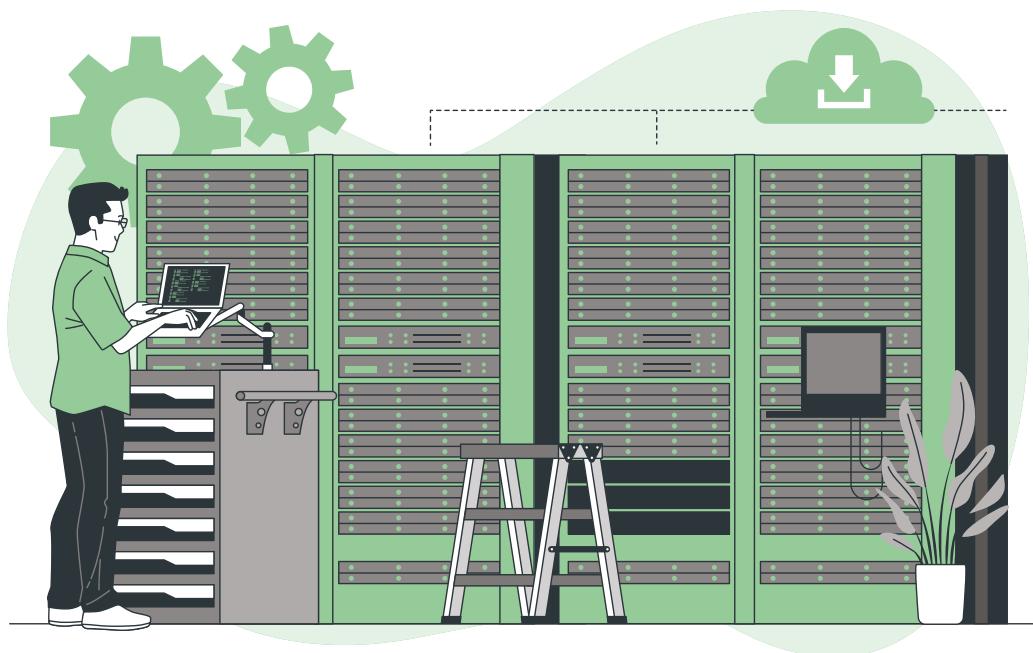
Estudante, acreditamos que essa aula complementará e aprofundará ainda mais o seu entendimento sobre o tema. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

NOVOS DESAFIOS

Com este tema, você pôde explorar como virtualização, redes em nuvem, contêineres e segurança formam a base das infraestruturas de TI modernas. Mais do que conceitos técnicos, essas tecnologias representam habilidades práticas essenciais para o mercado de trabalho atual, que busca profissionais capazes de resolver problemas reais, como otimizar custos e escalar aplicações com eficiência.

O conhecimento adquirido aqui não é apenas uma ferramenta acadêmica, mas um **diferencial competitivo**. Entender como configurar redes em nuvem, orquestrar contêineres ou implementar medidas de segurança prepara você para os desafios práticos que encontrará em setores em alta, como computação em nuvem, DevOps e cibersegurança. Essas competências são altamente valorizadas pelas empresas, que buscam profissionais estratégicos e inovadores.

Ao conectar teoria e prática, você está dando um passo importante para construir uma carreira sólida em áreas que não param de crescer. A adoção crescente de soluções baseadas em virtualização e nuvem abre portas para uma ampla gama de oportunidades. Você não está apenas aprendendo, mas se preparando para se destacar como um profissional inovador e essencial para o futuro da tecnologia.



VAMOS PRATICAR

1. A virtualização é uma tecnologia essencial na computação moderna, proporcionando maior eficiência no uso dos recursos físicos e simplificando a gestão de infraestruturas de TI. Ela abstrai os recursos físicos de servidores e redes, permitindo que múltiplos ambientes virtuais independentes operem em uma única infraestrutura. Para virtualizar servidores, utiliza-se o *Hypervisor*, que divide os recursos físicos em várias máquinas virtuais (VMs), oferecendo benefícios como otimização de recursos, redução de custos e maior flexibilidade. Exemplos de *Hypervisors* incluem VMware, Hyper-V e KVM (Kurose; Ross, 2021).

A virtualização de servidores é uma tecnologia que proporciona eficiência ao utilizar recursos físicos. Com relação à virtualização, assinale a alternativa correta sobre como ela funciona e os seus benefícios:

- a) A virtualização utiliza servidores físicos exclusivamente para rodar um único sistema operacional, sem necessidade de um *Hypervisor*.
 - b) A virtualização de servidores permite rodar múltiplos sistemas operacionais independentes no mesmo hardware físico, utilizando *Hypervisores* como VMware ESXi e KVM.
 - c) A virtualização de servidores exige a instalação de um sistema operacional em cada servidor físico, o que não envolve o uso de *Hypervisores*.
 - d) A virtualização de servidores não oferece benefícios como otimização de recursos ou redução de custos.
 - e) A virtualização é exclusiva para ambientes corporativos e não pode ser aplicada em servidores pessoais.
2. O SDN (*Software-Defined Networking*) é uma arquitetura que separa o plano de controle do plano de dados, permitindo um gerenciamento centralizado e programável das redes. Com isso, o SDN possibilita a automação das configurações e a escalabilidade das redes, além de oferecer maior flexibilidade e segurança. O controlador SDN, como o *OpenDaylight* ou o Cisco ACI, toma as decisões de roteamento, enquanto os dispositivos de rede (*switches* e roteadores) executam essas decisões. Entre os benefícios do SDN estão a automação de configurações, a personalização da rede conforme as necessidades das aplicações e a centralização de políticas de segurança (Comer, 2016).

Com base no texto sobre a arquitetura SDN, analise as afirmativas a seguir:

- I - O plano de dados no SDN é responsável por tomar decisões de roteamento e priorização do tráfego, enquanto o plano de controle executa o tráfego de rede efetivo.
- II - O controlador SDN é responsável pela automação e centralização das configurações de rede, permitindo uma gestão programável e simplificada.

VAMOS PRATICAR

III - A principal vantagem do SDN é a redução de custos com hardware, já que ele não utiliza mais *switches* e roteadores.

IV - A separação entre o plano de controle e o plano de dados no SDN facilita a escalabilidade e a customização da rede para necessidades específicas.

É correto o que se afirma em:

- a) I, apenas.
- b) II e IV, apenas.
- c) III e IV, apenas.
- d) I, II e III, apenas.
- e) I, II, III e IV.

3. Uma VPC (*Virtual Private Cloud*) é uma rede isolada dentro de uma nuvem pública, como AWS, Azure ou Google Cloud, que oferece controle completo sobre a configuração da rede. Ela inclui sub-redes, tabelas de roteamento e *gateways* de internet, permitindo uma personalização conforme as necessidades de cada aplicação. A VPC proporciona isolamento e segurança, criando uma camada lógica separada para diferentes projetos ou organizações. Dentro da VPC, é possível configurar sub-redes públicas e privadas, cada uma com propósitos específicos, como acesso à internet ou recursos internos, além de平衡adores de carga que distribuem o tráfego de forma eficiente (Sousa, 2013).

Com base nas informações apresentadas, avalie as asserções a seguir e a relação proposta entre elas:

I - Uma VPC oferece controle completo sobre a configuração da rede, permitindo a criação de sub-redes públicas e privadas com diferentes níveis de segurança.

PORQUE

II - Uma VPC não permite a criação de sub-redes privadas, limitando todos os recursos a sub-redes públicas, acessíveis diretamente pela internet.

A respeito dessas asserções, assinale a alternativa correta:

- a) As asserções I e II são verdadeiras, e a II é uma justificativa correta da I.
- b) As asserções I e II são verdadeiras, mas a II não é uma justificativa correta da I.
- c) A asserção I é uma proposição verdadeira e a II é uma proposição falsa.
- d) A asserção I é uma proposição falsa e a II é uma proposição verdadeira.
- e) As asserções I e II são falsas.

REFERÊNCIAS

- COMER, D. E. **Redes de computadores e internet**. Porto Alegre: Bookman, 2016.
- KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet**: uma abordagem top-down. Londres: Pearson, 2021.
- SOUZA, L. B. de. **Projetos e implementação de redes**. São Paulo: Érica, 2013.
- SOUZA, D. C. et al. **Gerenciamento de redes de computadores**. Porto Alegre: SAGAH, 2021. *E-book*.
- TORRES, Gabriel. **Redes de computadores**. Senhor do Bonfim, BA: Nova terra, 2016.
- SILVA et al. **Cloud Computing**. Porto Alegre: SAGAH, 2020. *E-book*.

CONFIRA SUAS RESPOSTAS

1. Alternativa B.

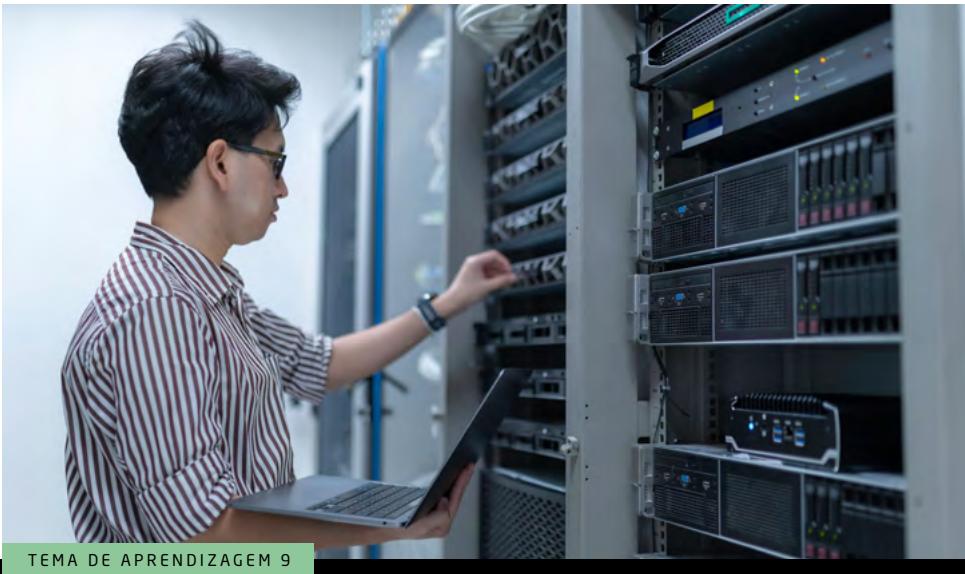
A tecnologia permite que vários sistemas operacionais sejam executados simultaneamente em um único servidor físico, utilizando *Hypervisores* para gerenciar e dividir os recursos do hardware. Esse processo oferece benefícios como a otimização de recursos, redução de custos e flexibilidade na gestão da infraestrutura.

2. Alternativa B.

No SDN, o controlador é responsável por configurar e automatizar as redes de forma centralizada, simplificando o gerenciamento. Além disso, a separação entre o plano de controle e o plano de dados facilita a escalabilidade e a customização da rede, permitindo que ela seja ajustada às necessidades específicas de diferentes aplicações e serviços. Esses benefícios tornam o SDN uma arquitetura eficiente e flexível para redes modernas.

3. Alternativa C.

A VPC realmente oferece controle completo sobre a rede, permitindo a criação de sub-redes públicas e privadas com diferentes níveis de segurança, conforme as necessidades da aplicação. Já a asserção I está incorreta, pois uma VPC permite a criação tanto de sub-redes públicas, acessíveis pela internet, quanto de sub-redes privadas, projetadas para recursos internos, sem exposição direta à internet.



TEMA DE APRENDIZAGEM 9

TÓPICOS AVANÇADOS EM REDES

MINHAS METAS

- Compreender Redes de Alto Desempenho e Redes Quânticas.
- Explorar Redes de Data Center Moderno.
- Analisar Redes de Sensoriamento Remoto e IoT Industrial.
- Introduzir *Blockchain* em Redes.
- Avaliar alguns exemplos de implementação das tecnologias emergentes.
- Refletir o Futuro das Redes.
- Explorar Tecnologias Emergentes em Redes.

INICIE SUA JORNADA

Pense um pouco, você já parou para imaginar como a internet consegue transmitir bilhões de informações por segundo ou como fábricas automatizadas se conectam com sensores espalhados por todo o chão de produção? E mais, como garantir que essas informações sejam seguras e cheguem no tempo certo? Esses desafios não são apenas de gigantes da tecnologia, mas também de futuros profissionais como você. Então, que tal pensar em como as redes avançadas impactam diretamente o mundo que estamos construindo?

Agora, reflita: tudo isso vai muito além de tecnologia. A maneira como nos comunicamos, fazemos negócios, aprendemos e até nos divertimos depende de redes eficientes. Imagine um mundo no qual carros autônomos precisam de decisões em milissegundos, ou médicos realizam cirurgias remotas. Consegue perceber a importância? Aprender redes modernas e suas aplicações, não é só estudar, é construir o futuro e você faz parte disso!



PLAY NO CONHECIMENTO

Descubra como as Tecnologias Emergentes estão revolucionando setores como saúde, educação e indústria, enquanto levantam desafios éticos e sociais. Neste podcast, exploramos essas inovações, seus impactos e como você pode se preparar para o futuro. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

Mas como entender isso, na prática? Vamos imaginar juntos: você cria a simulação de uma rede de alta velocidade, ou programa um sensor IoT para monitorar uma máquina em tempo real. Parece complicado? Não se preocupe, porque é aqui que começamos a experimentar e explorar essas tecnologias. E o mais interessante é que você vai descobrir que está mais próximo de dominar esses desafios do que imagina.

Por fim, pense no impacto do que você está aprendendo. Quando você desenvolve habilidades para trabalhar com redes avançadas, não está apenas garantindo um bom emprego, está se tornando parte de uma geração que define como a sociedade será conectada. Então, a pergunta é: como você pode usar

esse conhecimento para fazer a diferença? A resposta está em como você decide aplicar o que aprender; sempre com ética, inovação e um olhar para o futuro.

VAMOS RECORDAR?

É importante, durante a sua jornada de estudos, relembrar tópicos vistos em nosso curso. Portanto, indico a leitura sobre virtualização no site da IBM. Acesse em: <https://www.ibm.com/br-pt/topics/virtualization>

DESENVOLVA SEU POTENCIAL

REDES DE ALTO DESEMPENHO E REDES QUÂNTICAS

Redes de alto desempenho são projetadas para atender às demandas de comunicação e processamento intensivo, especialmente em aplicações que exigem baixa latência, alta largura de banda e alta confiabilidade. Isso é obtido mediante tecnologias como interconexões de alta velocidade (*Infiniband*, *Ethernet* de 400 Gbps), otimizações no protocolo TCP/IP e soluções de balanceamento de carga.

Já as redes quânticas utilizam princípios de física quântica, como entrelaçamento e superposição, para oferecer comunicações seguras baseadas em distribuição de chaves quânticas (QKD). A integração de redes clássicas e quânticas promete avanços em áreas como criptografia e simulações quânticas (Kurose; Ross, 2021).

Redes de alto desempenho

As **redes de alto desempenho** são infraestruturas voltadas para maximizar a comunicação entre nós de supercomputadores, otimizando latência e *throughput*. Na sequência, podemos ver algumas tecnologias principais com relação às redes de alto desempenho. É importante conhecermos, pois muitas dessas ferramentas estão sendo utilizadas cada dia mais. Vejamos duas muito utilizadas, conforme Soares (2020):

- *InfiniBand*: Protocolo com baixa latência e alto *throughput*, usado em *clusters*.
- *Ethernet de alta velocidade*: Padrões acima de 100 Gbps para aplicações empresariais.

Seguindo com o aprofundamento em nosso material, observamos um exemplo teórico importante para a área de bioinformática, acompanhe: imagine um laboratório de bioinformática que processa dados genômicos, ele utiliza HPC para realizar cálculos complexos, como o sequenciamento genético.

Redes quânticas

Nas redes que exploram princípios como o entrelaçamento para comunicação segura, algumas das aplicações práticas incluem criptografia inquebrável com Distribuição de Chave Quântica (QKD) e experimentos com repetidores quânticos para longas distâncias. Duas das práticas que poderiam ser realizadas para aplicações em redes quânticas envolvem:

- **Simular redes HPC usando Mininet**: instalar o *Mininet* em um ambiente virtualizado. Configurar uma topologia do tipo *fat-tree* e medir a latência com diferentes tamanhos de pacotes.
- **Explorar algoritmos quânticos básicos (Qiskit)**: usar o *Qiskit (Python)* para implementar o protocolo BB84, simulando a troca de chaves quânticas.

Com o exemplo a seguir, poderemos entender na prática o Protocolo BB84, construindo um fundamento e pensarmos na complexidade desse tipo de rede.

APROFUNDANDO

O que é o Protocolo BB84? O BB84 é um protocolo de distribuição de chave quântica (QKD). Ele usa os princípios da mecânica quântica, como a superposição e a medição que perturba o estado quântico, para permitir que duas partes (geralmente chamadas de Alice e Bob) compartilhem uma chave secreta com segurança (Stallings, 2014).

Vejamos, na Figura 1, um exemplo de implementação das etapas do Protocolo BB84, é claro que o primeiro passo é o *script* para implementação:

```
#Implementação do Protocolo BB84
def bb84_protocol(num_qubits):
    print("PROTÓCOLO BB84")
```

Figura 1 - Implementação do Protocolo BB84 / Fonte: o autor.

Descrição da Imagem: imagem exibindo o código em Python para a implementação do Protocolo BB84, com a criação da função e utilização do print para exibir o texto na tela. Fim da descrição.

Na Figura 2, da etapa 1, Alice gera uma sequência aleatória de bits e escolhe aleatoriamente uma base de medição (reta ou diagonal) para cada bit.

```
#Etapa 1: Alice gera bits e bases aleatórios
alice_bits, alice_bases = generate_random_sequence(num_qubits)
print("Alice - Bits:", alice_bits)
print("Alice - Bases:", alice_bases)
```

Figura 2 - Alice gera bits em sequência aleatória / Fonte: o autor.

Descrição da Imagem: imagem exibindo o código em Python para a implementação de bits aleatórios, com a utilização do print para exibir os Bits e as Bases. Fim da descrição.

Na Figura 3, da etapa 2, Alice envia os qubits correspondentes a Bob.

```
#Etapa 2: Alice cria e envia qubits
qubits = create_qubits(alice_bits, alice_bases)
```

Figura 3 - Alice cria e envia os qubits / Fonte: o autor.

Descrição da Imagem: imagem exibindo o código em Python para a implementação dos qubits criado e enviado por Alice utilizando o método qubits. Fim da descrição.

Na Figura 4, da etapa 3, Bob mede os qubits recebidos em bases escolhidas aleatoriamente.

```
#Etapa 3: Bob escolhe bases aleatórias e mede os qubits
bob_bases = np.random.randint(2, size=num_qubits)
print("Bob - Bases:", bob_bases)
bob_measurements = measure_qubits(qubits, bob_bases)
print("Bob - Medições:", bob_measurements)
```

Figura 4 - Bob mede os qubits / Fonte: o autor.

Descrição da Imagem: imagem exibindo o código em Python, no qual Bob utiliza um método para gerar bases aleatórias e fazer a medição dos qubits, além de exibir as Bases e as Medições através do Print. Fim da descrição.

Na Figura 5, da etapa 4, Alice e Bob compartilham publicamente suas bases de medição e descartam bits em que suas bases diferem.

```
# Etapa 4: Alice e Bob compartilham bases e geram a chave final
sifted_key = sift_key(alice_bits, alice_bases, bob_bases, bob_measurements)
print("Chave Final Compartilhada:", sifted_key)
return sifted_key
```

Figura 5 - Alice e Bob compartilham as bases de medição / Fonte: o autor.

Descrição da Imagem: imagem exibindo o código em Python, no qual Alice e Bob utilizam um método para gerar uma chave final e deixam essa chave compartilhada por meio do Print e tendo o retorno da chave. Fim da descrição.

Na Figura 6, da etapa 5, a sequência restante é a chave secreta, desde que nenhum interceptador (Eve) tenha perturbado os qubits.

```
#PROTÓCOLO BB84
Alice - Bits: [1 0 1 0 1 1 0 0 1 0]
Alice - Bases: [0 1 1 0 1 0 1 0 1 0]
Bob - Bases: [1 1 0 0 1 1 1 0 0 0]
Bob - Medições: [0 0 0 0 1 1 0 0 1 0]
Chave Final Compartilhada: [1, 0, 1, 0]
```

Figura 6 - Resultado do Protocolo BB84 / Fonte: o autor.

Descrição da Imagem: imagem exibindo o resultado final da chave compartilhada por Alice e Bob. Fim da descrição.

É claro que esse é um exemplo ilustrativo para entendermos melhor um passo a passo relacionado ao conceito de redes quânticas.

REDES DE DATA CENTER MODERNO

Os data centers modernos são arquitetados com foco em escalabilidade, eficiência energética e suporte a tecnologias emergentes como *edge computing* e 5G. Arquiteturas como *spine-leaf* substituem hierarquias tradicionais, reduzindo a latência. Tecnologias como virtualização, contêineres e SDN (*Software-Defined Networking*) otimizam a alocação de recursos e a flexibilidade operacional. Práticas sustentáveis, como refrigeração com água e uso de energias renováveis, minimizam o impacto ambiental.

Arquiteturas modernas:

- *Spine-Leaf*: reduz latência e melhora a escalabilidade em data centers.
- *Hyper-Converged Infrastructure (HCI)*: combina computação, armazenamento e rede em uma única solução.

Práticas sustentáveis:

- Uso de energia renovável e técnicas como *free cooling*.
- Ferramentas de monitoramento (ex.: DCIM – Data Center *Infrastructure Management*).

Uma empresa de streaming global utiliza uma rede de data center moderno integrada com *edge computing* para reduzir a latência de entrega de vídeos aos clientes.

Projeto de um mini datacenter virtual:

- Utilizar simuladores como *Cisco Packet Tracer* ou GNS3 para projetar uma topologia *spine-leaf*, conforme observaremos na Figura 7:

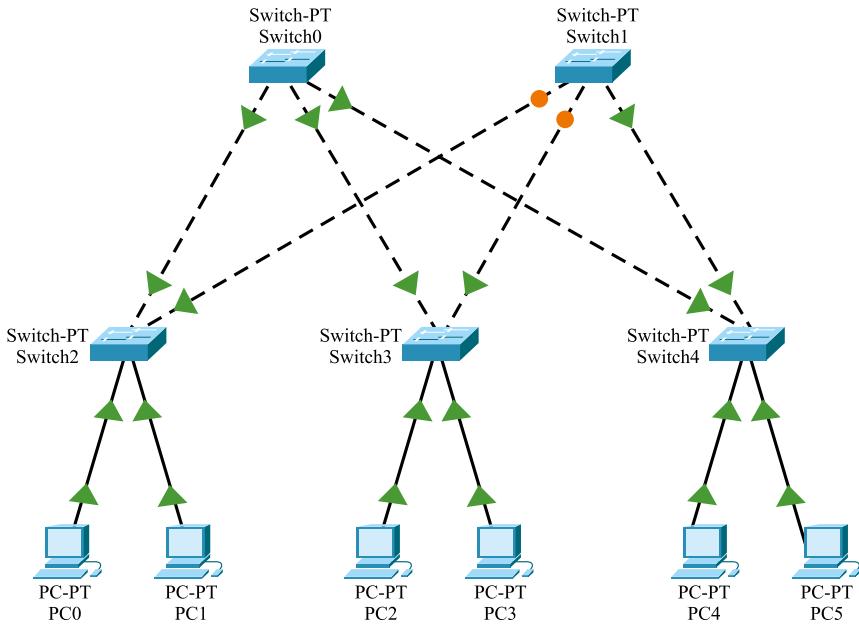


Figura 7 - Datacenter em Topologia *Spine-Leaf* / Fonte: o autor.

Descrição da Imagem: a imagem é um exemplo de topologia *Spine-Leaf* com switches principais com switches conectados a esses switches principais para a criação de um pequeno data center. Fim da descrição.

Monitoramento de consumo energético:

- Simular cargas de trabalho em um ambiente virtualizado e calcular o impacto energético.

REDES DE SENSORIAMENTO REMOTO E IOT INDUSTRIAL

Redes de sensoriamento remoto envolvem dispositivos que capturam e transmitem dados ambientais ou industriais para análise. Esses sistemas são baseados em tecnologias como LoRaWAN, ZigBee e NB-IoT, que oferecem conectividade de longa distância e baixo consumo de energia.

No contexto industrial, a IoT impulsiona a automação e a monitoria em tempo real, integrando sensores, atuadores e sistemas de controle em soluções como manufatura 4.0 e gerenciamento de cadeias logísticas.

Vamos conhecer alguns exemplos teóricos sobre o tema, muito utilizados atualmente:

- **Sensoriamento Remoto:**

- Coleta de dados por dispositivos como satélites e drones.
- Protocolo *LoRaWAN*: longo alcance e baixa potência.
- *Exemplo*: monitoramento da qualidade do ar em áreas urbanas.

- **IoT Industrial:**

- Sensores em ambientes industriais permitem manutenção preditiva e automação.
- Protocolo *MQTT*: comunicação leve e eficiente para IoT.
- *Exemplo*: fábricas inteligentes que otimizam a produção com sensores de vibração e temperatura.



INDICAÇÃO DE LIVRO

Projetos com Python e Arduino

Essa obra apresenta projetos que unem essas tecnologias com o objetivo de criar projetos didáticos, mas que podem ser utilizados ou adaptados para diversos fins. Os projetos apresentados na obra abordam conceitos básicos de eletrônica e programação, utilizando LEDs, botões e sensores, assim como projetos mais avançados, utilizando interface gráfica e voltados à Internet das Coisas. O livro indicado nos traz uma bagagem aprofundada dessa área, que hoje está se tornando cada vez mais essencial para o mundo do trabalho. Portanto, é válido dar uma atenção especial a essa leitura.



Desenvolver uma rede IoT usando Arduino

Configurar um sensor de temperatura com um módulo ESP8266 para enviar dados via MQTT a um servidor central.

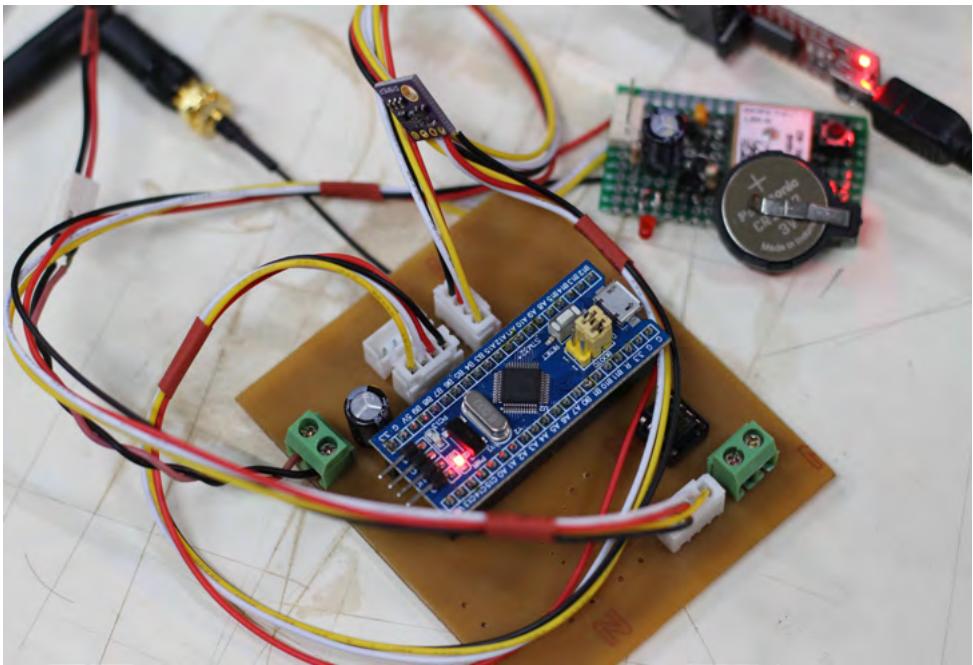


Figura 8 - LoRaWAN

Descrição da Imagem: Exemplo de um arduino utilizando o protocolo LoRaWAN e um sensor de temperatura.
Fim da descrição.

Hoje, temos a possibilidade de construir projetos físicos utilizando arduino e outros componentes com um custo baixo, até mesmo para aprendermos como são desenvolvidos esses equipamentos e suas aplicações.

BLOCKCHAIN EM REDES

O *blockchain* é uma tecnologia distribuída que garante segurança e transparência em transações de dados. Aplicado a redes, fortalece a autenticação, a privacidade e a resiliência, eliminando pontos únicos de falha. Contratos inteligentes automatizam processos, enquanto aplicações como redes 5G e IoT aproveitam sua capacidade para gerenciar identidades e proteger comunicações, conforme Sinclair (2018). Exemplos práticos incluem rastreamento de ativos e autenticação de dispositivos IoT.

■ Fundamentos do *Blockchain*

- Consenso descentralizado por algoritmos como *Proof of Work* ou *Proof of Stake*.
- Criação de registros imutáveis para transações distribuídas.

 EU INDICO

Estudante, observe que conteúdo interessante sobre o Blockchain, com perspectivas de utilização para 2030, como será utilizada essa tecnologia?! Acompanhe o link do vídeo desenvolvido pelo canal Código Fonte TV: <https://www.youtube.com/watch?v=Z8wZBGD2uks>

Contratos inteligentes

Programas autoexecutáveis que garantem confiança e eficiência em redes distribuídas são um exemplo, como um contrato inteligente que libera pagamento a um fornecedor assim que o envio for confirmado. Utilizar a rede *Ethereum* e o framework *Remix* para criar e executar um contrato que registre autenticação de dispositivos IoT, conforme Figura 9:

```
# Endereço do contrato e ABI
contract_address = "0xSeuContratoEndereco" # Substitua pelo endereço do contrato
contract_abi = [ # ABI copiada do Remix
    {
        "inputs": [{"internalType": "string", "name": "deviceId", "type": "string"}],
        "name": "registerDevice",
        "outputs": [],
        "stateMutability": "nonpayable",
        "type": "function",
    },
    {
        "inputs": [{"internalType": "string", "name": "deviceId", "type": "string"}],
        "name": "authenticateDevice",
        "outputs": [{"internalType": "bool", "name": "", "type": "bool"}],
        "stateMutability": "view",
        "type": "function",
    }
]
# Conectar ao contrato
contract = web3.eth.contract(address=contract_address, abi=contract_abi)
```

Figura 9 - Implementação de Contrato Inteligente em Python / Fonte: o autor.

Descrição da Imagem: temos um exemplo de implementação de contrato inteligente em Python, realizando conexão com o contrato por meio do script em Python. Fim da descrição.

Podemos observar mediante esses exemplos, a forma que são implementados, pois no dia a dia utilizamos sistemas de contratos digitais assinados virtualmente e, por isso, devemos dar atenção a esses tópicos, faz parte do seu futuro como profissional.

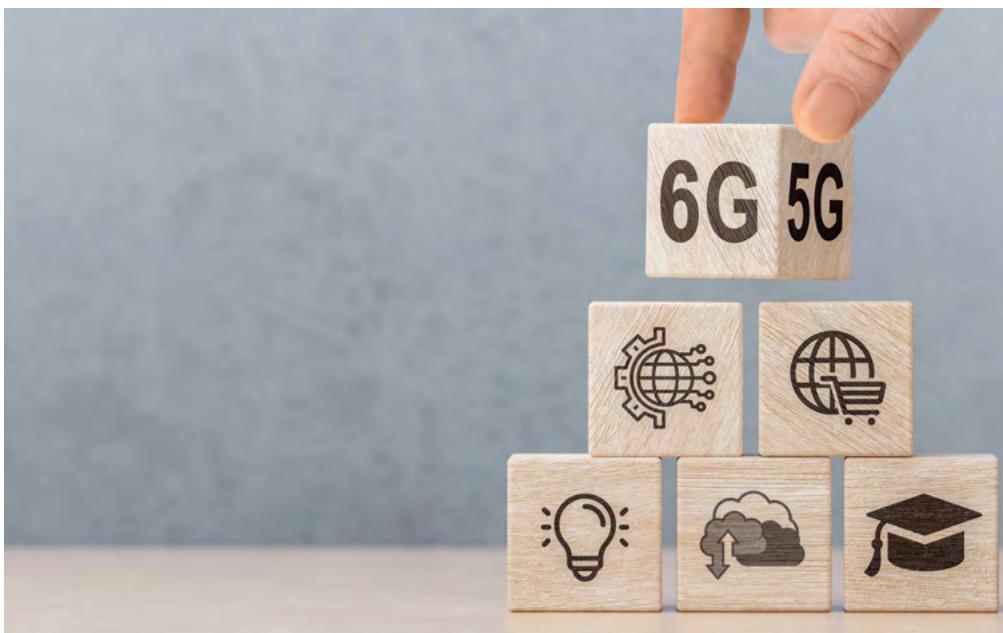
FUTURO DAS REDES

A evolução das redes aponta para tecnologias como 6G, holografia de rede e integração com IA. O 6G promete taxas de dados da ordem de terabits por segundo, permitindo aplicações como realidade aumentada e virtual hiper-realista. Holografia de rede trará comunicações tridimensionais e interativas. A IA contribuirá na gestão automatizada e no monitoramento preditivo, garantindo eficiência e segurança.

**A evolução das
redes aponta para
tecnologias como 6G**

6G

As redes 6G são a próxima evolução das redes móveis, planejadas para suceder o 5G. Elas prometem velocidades extremamente altas, latências ultrabaixas e uma integração profunda com tecnologias emergentes como inteligência artificial, computação em borda e comunicação quântica.



Conheça os principais objetivos do 6G, conforme Kurose e Ross (2021):

- **Velocidade e Banda Larga:** taxas de dados acima de 1 Tbps (terabit por segundo), capacidade de suportar aplicações como holografia em tempo real.
- **Latência Ultrabaixa:** latência de menos de 1 milissegundo, permitindo respostas quase instantâneas.
- **Conexão Ubíqua:** cobertura universal, incluindo áreas remotas e ambientes subaquáticos, Integração com satélites de baixa órbita (LEO).
- **Sustentabilidade e Eficiência Energética:** consumo de energia reduzido por bit transmitido, uso de energias renováveis e técnicas de economia de energia em dispositivos e torres.
- **Comunicação Confiável e Segura:** implementação de criptografia baseada em tecnologias quânticas para segurança.

Conheça as características principais e as possibilidades do 6G, de acordo com Silva *et al.* (2021):

- **Espectro de Altíssima Frequência (THz):** o 6G explora ondas terahertz (THz), acima de 100 GHz, para transmissões rápidas e de alta capacidade.
- **Inteligência Artificial e Aprendizado de Máquina:** gerenciamento autônomo de redes, Personalização em tempo real de serviços baseados em padrões de uso.
- **Redes Quânticas:** a combinação de redes tradicionais com comunicações quânticas para criptografia ultrassegura e transmissão de informações sensíveis.
- **Sensoriamento Móvel:** sensores integrados às redes para detectar mudanças no ambiente, como condições climáticas ou localização de usuários.
- **Holografia e Realidade Estendida (XR):** suporte para experiências imersivas e interativas com hologramas em tempo real e realidades aumentadas.
- Agora, conheça as aplicações possíveis com a utilização do 6G, de acordo com Soares (2020):
- **Cidades Inteligentes e IoT:** integração massiva com dispositivos IoT, otimizando transporte, energia e segurança.

- **Saúde:** cirurgias remotas avançadas com realidade aumentada, Monitoramento de saúde em tempo real usando dispositivos biomédicos.
- **Indústria 5.0:** comunicação ultrarrápida entre robôs e humanos para fabricação sob demanda.
- **Espaço e Submarinos:** conexão em ambientes inóspitos usando drones, satélites LEO e dispositivos subaquáticos.

Na sequência, Sinclair (2018) apresenta os desafios no desenvolvimento do 6G:

- **Infraestrutura:** implementação de torres capazes de suportar frequências THz, Integração com satélites e drones para ampliar a cobertura.
- **Consumo Energético:** necessidade de balancear a alta performance com eficiência energética.
- **Regulação de Espectro:** organização e licenciamento de novas faixas de frequência.
- **Cibersegurança:** proteção contra ataques quânticos e ameaças digitais avançadas.
- **Custo:** altos custos de pesquisa, desenvolvimento e implantação.

Conheça também algumas expectativas e estimativas com relação à evolução dessas tecnologias, segundo Soares (2020):

- **2024-2026:** experimentação e definição de padrões.
- **2026-2030:** desenvolvimento inicial, testes em larga escala e primeiros protótipos.
- **2030 em diante:** comercialização e adoção global.

Agora, vamos observar o infográfico com a comparação entre o 5G e 6G, de acordo com Kurose e Ross (2021):

Comparação

5G

Velocidade:
Até 10 Gbps

Frequência:
Até 100 GHz

Latência:
~1 ms

Cobertura:
Principalmente terrestre

Inteligência Artificial:
Limitada

6G

Velocidade:
Até 1 Tbps

Frequência:
Até 1 THz

Latência:
<1 ms

Cobertura:
Terrestre, satélite, ar e mar

Inteligência Artificial:
Totalmente integrada

Fonte: Kurose; Ross (2021).

O 6G promete transformar profundamente a nossa interação com a tecnologia e a sociedade. Com maior velocidade, segurança e conectividade, ele pode viabilizar inovações revolucionárias. Contudo, será necessário enfrentar desafios significativos relacionados à infraestrutura, regulamentação e sustentabilidade para concretizar essa visão ambiciosa.

Holografia de rede

Utiliza transmissões 3D para criar interações imersivas, um exemplo são as cirurgias realizadas remotamente com hologramas interativos em tempo real.

 EU INDICO

Mas o que é um holograma?

Para responder essa pergunta, indico esse vídeo do canal Mundo Conectado. Nele há a explicação de forma muito interessante e científica de como surgiu o holograma. Acesse em: <https://www.youtube.com/watch?v=R4jbuLrgD1A>

INTEGRAÇÃO DE TECNOLOGIAS EMERGENTES EM REDES

Conforme Comer (2016), a convergência de tecnologias como IoT, IA, 5G e *blockchain* transforma redes em sistemas mais eficientes e adaptáveis. A integração dessas soluções permite criar ecossistemas conectados, como cidades inteligentes e fábricas autônomas. Desafios incluem interoperabilidade e segurança, exigindo novas abordagens para arquiteturas e protocolos.

A capacitação de profissionais aptos a projetar e gerenciar essas soluções será crucial no mercado futuro. Podemos combinar *blockchain*, IoT, SDN e 5G para criar redes resilientes e adaptativas, um exemplo são as Cidades inteligentes que usam *blockchain* para gerenciar tráfego e segurança.

Projeto de uma rede inteligente

Integrar sensores IoT, SDN e *blockchain* em um simulador para criar um ambiente inteligente, como uma rede de controle de semáforos (Silva *et al.*, 2021). Vejamos a primeira etapa desse ambiente inteligente na Figura 10:

```

import paho.mqtt.client as mqtt
import random
import time

BROKER = "test.mosquitto.org"
TOPIC = "traffic/sensor_data"

def simulate_sensor_data():
    while True:
        # Simulando dados do sensor (ex.: número de veículos em um cruzamento)
        sensor_data = {
            "sensor_id": "sensor_1",
            "vehicles": random.randint(0, 50),
            "timestamp": time.time()
        }
        client.publish(TOPIC, str(sensor_data))
        print(f"Published: {sensor_data}")
        time.sleep(5)

# Configurando o cliente MQTT
client = mqtt.Client()
client.connect(BROKER)
simulate_sensor_data()

```

Figura 10 - Configuração de Sensores IoT / Fonte: o autor.

Descrição da Imagem: a imagem exibe o exemplo de configuração de sensores IoT implementado em Python.
Fim da descrição.

Nosso próximo passo é implementar a configuração de Rede SDN (Figura 11):

```

from scapy.all import *

def monitor_traffic(pkt):
    # Monitorando pacotes ICMP como exemplo
    if pkt.haslayer(ICMP):
        print(f"ICMP Packet detected: {pkt.summary()}")
        # Exemplo: modificar roteamento ou agir com base nos pacotes

    # Escutando pacotes em tempo real
sniff(filter="icmp", prn=monitor_traffic)

```

Figura 11 - Configuração da Rede SDN / Fonte: o autor.

Descrição da Imagem: a imagem exibe o exemplo de configuração de rede SDN implementado em Python, para controlar os pacotes ICMP. Fim da descrição.

Nosso próximo passo é a implementação e utilização do *Blockchain* utilizando *Solidity* para gerar o contrato inteligente:

```
pragma solidity ^0.8.0;
contract TrafficLight {
    event LightChanged(string light_id, string new_state, uint256 timestamp);
    function changeLight(string memory light_id, string memory new_state) public
    {
        emit LightChanged(light_id, new_state, block.timestamp);
    }
}
```

A seguir, na Figura 12, temos a relação do *Blockchain* com *Python*:

```
from web3 import Web3

# Conexão com o Ganache
ganache_url = "http://127.0.0.1:8545"
web3 = Web3(HTTPProvider(ganache_url))

# Carregar o contrato
contract_address = "0xYourContractAddress"
abi = [...] # ABI gerado após a compilação do contrato

contract = web3.eth.contract(address=contract_address, abi=abi)

# Função para registrar mudança de semáforo
def log_light_change(light_id, new_state):
    tx = contract.functions.changeLight(light_id, new_state).buildTransaction({
        'from': web3.eth.accounts[0],
        'gas': 2000000,
        'gasPrice': web3.toWei('50', 'gwei'),
        'nonce': web3.eth.getTransactionCount(web3.eth.accounts[0]),
    })
    signed_tx = web3.eth.account.signTransaction(tx, "your_private_key")
    tx_hash = web3.eth.sendRawTransaction(signed_tx.rawTransaction)
    print(f"Transaction Hash: {tx_hash.hex()}")

# Exemplo de registro
log_light_change("light_1", "green")
```

Figura 12 - Interação do Blockchain com Python / Fonte: o autor.

Descrição da Imagem: a imagem exibe a implementação do código em Python fazendo a interação com o Blockchain, quando realiza a mudança de uma cor para outra do semáforo. Fim da descrição.

Para a conclusão, implementamos a coordenação do sistema (Figura 13):

```
def process_sensor_data(data):
    # Decisão com base nos dados de tráfego
    vehicles = data.get("vehicles")
    light_state = "green" if vehicles < 20 else "red"

    # Atualizar no blockchain
    log_light_change(data["sensor_id"], light_state)
```

Figura 13 – Implementação da Coordenação do Sistema / Fonte: o autor.

Descrição da Imagem: a imagem exibe a implementação em *Python* da condição para realizar a mudança de cor do semáforo. Fim da descrição.

É claro que são exemplos do que podem ser realizados e também de projetos que hoje já são realidades, alguns exemplos constam partes de sistemas reais, mas isso permite que você imagine o quão desafiador e interessante é esse mundo e suas oportunidades.

EM FOCO

Estudante, acreditamos que essa aula complementará e aprofundará ainda mais o seu entendimento sobre o tema. **Recursos de mídia disponíveis no conteúdo digital do ambiente virtual de aprendizagem.**

NOVOS DESAFIOS

Ao tratarmos de redes avançadas, como as de alto desempenho, redes quânticas, IoT industrial ou *blockchain*, estamos lidando com tecnologias que já moldam o presente e são fundamentais para o futuro do mercado de trabalho.

VOCÊ SABE RESPONDER?

Como o que você está aprendendo agora se conecta a essas demandas do mundo profissional?

A teoria que você estuda, conceitos como arquiteturas de redes, protocolos de comunicação, ou a estrutura de data centers é a base para entender o funcionamento das tecnologias que dão suporte a grandes empresas, hospitais, indústrias e até mesmo serviços que usamos no dia a dia, como streaming ou compras on-line. O domínio dessa teoria não é apenas para tirar boas notas, mas para preparar você para resolver problemas reais, como melhorar a eficiência de uma rede corporativa ou criar soluções inovadoras para conectividade em larga escala.

Por outro lado, a prática vem como um complemento essencial. Imagine-se configurando redes IoT para automação de uma fábrica ou programando contratos inteligentes para transações seguras em *blockchain*. Esses exercícios práticos simulam situações reais que você enfrentará em ambientes profissionais. É durante essas experiências que você adquire confiança para aplicar os conceitos teóricos de forma eficiente e criativa.

No mercado de trabalho, há uma crescente demanda por profissionais que dominem essas tecnologias emergentes. Empresas estão buscando especialistas em redes que saibam implementar soluções modernas, garantir segurança de dados e acompanhar as rápidas mudanças tecnológicas. Mais do que isso, espera-se que esses profissionais tenham visão estratégica e saibam como essas tecnologias impactam o negócio como um todo.

A boa notícia é que o conhecimento que você está construindo agora já está alinhado com essas demandas. Cada conceito aprendido e cada prática realizada é um passo em direção a um ambiente profissional no qual a inovação e a tecnologia são protagonistas. E o melhor: você está se preparando não apenas para se adaptar ao mercado, mas para liderar a transformação que ele exige, com isso, a conexão entre teoria e prática se torna clara: é ela que transforma aprendizado em ação.

VAMOS PRATICAR

- Redes de alto desempenho são infraestruturas projetadas para maximizar a comunicação entre nós de supercomputadores, otimizando latência e *throughput*. Tecnologias como *InfiniBand*, que oferece baixa latência e alto *throughput*, e *Ethernet* de alta velocidade, com padrões acima de 100 Gbps, são amplamente utilizadas (SOARES, 2020). Por outro lado, redes quânticas utilizam princípios como o entrelaçamento para comunicação segura, com aplicações como Distribuição de Chave Quântica (QKD) e experimentos com repetidores quânticos. Simulações práticas de redes quânticas incluem o uso de ferramentas como Qiskit, para implementar algoritmos como o protocolo BB84, simulando a troca de chaves quânticas (Soares, 2020).

Com base no texto, assinale a alternativa que não está relacionada a redes de alto desempenho:

- a) Uso do protocolo *InfiniBand* para comunicação em *clusters*.
 - b) Aplicação do padrão *Ethernet* acima de 100 Gbps em empresas.
 - c) Simulação da troca de chaves quânticas com o Qiskit.
 - d) Otimização de latência em supercomputadores.
 - e) Maximização do *throughput* em aplicações críticas.
- O *blockchain* é uma tecnologia distribuída que promove segurança e transparência em redes, eliminando pontos únicos de falha. Ele utiliza algoritmos de consenso descentralizado, como *Proof of Work* ou *Proof of Stake*, para validar transações e criar registros imutáveis. Contratos inteligentes, uma de suas aplicações principais, automatizam processos e aumentam a eficiência. No contexto de redes como IoT e 5G, o *blockchain* é aplicado para autenticação de dispositivos e gerenciamento seguro de identidades (Sinclair, 2018).

Com base no texto, analise as afirmativas a seguir sobre as características e aplicações do blockchain:

- I - O *blockchain* é totalmente dependente de um ponto central de controle para validar transações.
- II - Contratos inteligentes automatizam processos, aumentando a confiança em redes distribuídas.
- III - Algoritmos de consenso como *Proof of Work* e *Proof of Stake* eliminam a necessidade de consenso descentralizado.
- IV - Em redes IoT, o *blockchain* é utilizado para autenticação de dispositivos e proteção de dados.

VAMOS PRATICAR

É correto o que se afirma em:

- a) I, apenas.
 - b) II e IV, apenas.
 - c) III e IV, apenas.
 - d) I, II e III, apenas.
 - e) I, II, III e IV.
3. As redes 6G estão sendo desenvolvidas com tecnologias avançadas que incluem ondas terahertz (THz) para transmissões rápidas e de alta capacidade. Além disso, integram inteligência artificial para gerenciar redes autonomamente, redes quânticas para comunicações ultrasseguras e sensoriamento móvel para monitorar o ambiente. Aplicações potenciais incluem suporte a cidades inteligentes, avanços em saúde com cirurgias remotas, integração na Indústria 5.0 e conexão em ambientes desafiadores, como o espaço e regiões subaquáticas (Kurose; Ross, 2021).

Com base nas informações apresentadas, avalie as asserções a seguir e a relação proposta entre elas:

I - As redes 6G utilizam ondas terahertz (THz) acima de 100 GHz, permitindo transmissões de alta capacidade e velocidade.

PORQUE

II - O 6G não terá capacidade de conexão em ambientes inóspitos, como regiões subaquáticas ou espaciais, devido às limitações tecnológicas das ondas terahertz.

A respeito dessas asserções, assinale a alternativa correta:

- a) As asserções I e II são verdadeiras, e a II é uma justificativa correta da I.
- b) As asserções I e II são verdadeiras, mas a II não é uma justificativa correta da I.
- c) A asserção I é uma proposição verdadeira e a II é uma proposição falsa.
- d) A asserção I é uma proposição falsa e a II é uma proposição verdadeira.
- e) As asserções I e II são falsas.

REFERÊNCIAS

COMER, D. E. **Redes de computadores e internet**. Porto Alegre: Bookman, 2016.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet**: uma abordagem top-down. Londres: Pearson, 2021.

SINCLAIR, B. **IoT**: Como usar a internet das coisas para alavancar seus negócios. [S. l.]: Autêntica Business, 2018.

SILVA, F. R. da *et al.* **Programação em ambientes de redes de computadores**. Porto Alegre: SAGAH, 2021.

STALLINGS, W. **Criptografia e segurança de redes**: princípios e práticas. Londres: Pearson, 2014.

SOARES, J. A. *et al.* **Redes de alta disponibilidade**. Porto Alegre: SAGAH, 2020.

CONFIRA SUAS RESPOSTAS

1. Alternativa C.

A alternativa c) descreve uma aplicação associada a redes quânticas que utilizam ferramentas como o Qiskit para simular a troca de chaves quânticas com base no protocolo BB84. Todas as outras alternativas (a), (b), (d), (e)) estão diretamente relacionadas a redes de alto desempenho.

2. Alternativa C.

Afirmativa II está correta. Contratos inteligentes são programas autoexecutáveis que automatizam processos em redes distribuídas, aumentando a confiança e eficiência.

Afirmativa IV está correta. Em redes IoT, o *blockchain* é aplicado para autenticação de dispositivos e proteção de dados, como destacado no texto.

3. Alternativa C.

I) Verdadeira. O uso de ondas terahertz (THz) acima de 100 GHz é uma característica das redes 6G, permitindo transmissões rápidas e de alta capacidade.

II) Falsa. As redes 6G estão sendo projetadas para superar desafios de conexão em ambientes inóspitos, incluindo áreas subaquáticas e espaciais, por meio de tecnologias como drones e satélites de baixa órbita (LEO).

MEU ESPAÇO