Faculdades Oswaldo Cruz

NÚCLEO DE TECNOLOGIAS EDUCACIONAIS

Redes de Computadores e Cloud Computing

Redes de Computadores e Cloud Computing

Público-alvo: Estudantes universitários do curso de Análise e Desenvolvimento de Sistemas da Faculdade Oswaldo Cruz.

Objetivo: Capacitar os alunos nos conhecimentos básicos dos componentes ativos e passivos que compõem a estrutura de uma rede de computadores e as principais tecnologias e arquiteturas de redes locais. Tratar os conceitos, definições, aspectos, arquitetura de sistemas distribuídos e a computação distribuída e paralela.

Cloud Computing é um conceito e um modelo de utilização de recursos e serviços, que tem tido um enorme impacto na indústria das Tecnologias de Informação (TI). Praticamente tudo o que é consumido atualmente na Internet — redes sociais, armazenamento de arquivos, streaming de vídeo e música — provém de aplicativos e serviços baseados na nuvem. Este curso visa apresentar os principais conceitos e modelos implementados para essa nova realidade das aplicações.

Professor: Robson Carmo, mestre pelo programa de mestrado profissional em Gestão e Tecnologia em Sistemas Produtivos do Centro Paula Souza, concluiu 3 MBAs (Inovação e Transformação Digital, Gestão de Empresarial, Engenharia de Software). Instrutor de certificações da SAFE, auto e coautor de vários livros e ebooks.

Lattes: http://lattes.cnpq.br/8753112683856964

Orcid: https://orcid.org/0009-0002-7102-4993

LLM utilizada: Gemini 3 – Fevereiro de 2026.

Módulos e Conteúdo

Módulo 1: Infraestrutura Física e Sinais

- **Bases e Evolução:** Histórico das redes, evolução tecnológica e a classificação geográfica (PAN, LAN, MAN, WAN).
- **A Física da Comunicação:** Conceitos de transmissão Simplex, Half-Duplex e Full-Duplex. Diferença entre comunicação Síncrona vs. Assíncrona e Serial vs. Paralelo.
- **Sinais e Transmissão:** Entendendo sinais analógicos e digitais. Definições de Banda Passante (largura do canal) e Banda Base (transmissão direta sem modulação).
- **O Desenho da Rede:** Topologias física e lógica: Estrela, Barramento, Anel e Mista. Vantagens e desvantagens de cada uma.
- **Cabeamento Estruturado:** Práticas de organização de infraestrutura física, conectores e normas para ambientes profissionais.

Módulo 2: Padronização e Camadas Iniciais

- **Padrões IEEE 802.x:** Mergulho nos padrões .3 (Ethernet), .4 (Token Bus), (Token Ring), .11 (Wi-Fi), .15 (Bluetooth), .16 (WiMAX) e .20 (Mobile Broadband).
- **Modelos de Referência:** A evolução da Internet (TCP/IP) e a padronização das redes pelo modelo RM ISO-OSI.
- **Camada Física e Enlace:** Características da camada 1 e 2. Estudo detalhado do protocolo **CSMA/CD** (como as máquinas evitam colisões de dados).
- **Componentes de Enlace:** O papel do **Switch** na rede e como ele difere de hubs antigos, criando caminhos dedicados para a informação.

Módulo 3: O Protocolo da Internet e Transporte

- **Camada de Rede (IP):** O papel da camada 3. Estudo do **Endereço IP**, divisão em classes (A, B, C, D, E) e o conceito de máscara de subrede.
- **Prática de Subredes:** Exercícios detalhados de divisão de redes para otimização de tráfego e segurança.
- **Camada de Transporte:** Funcionalidades do **TCP** (focado em conexão e entrega garantida) e do **UDP** (focado em velocidade e baixa latência).

- **Camada de Aplicação:** As funcionalidades das camadas superiores que o usuário final acessa (HTTP, DNS, DHCP, FTP).

Módulo 4: Cloud Computing - Estratégia e Tecnologia

- **Fundamentos e Negócio:** Características da nuvem sob a ótica de negócio e o valor estratégico (escalabilidade e redução de custos). Modelos SaaS, PaaS e IaaS.
- **Perspectiva Técnica e Adoção:** Tipos de nuvem (Pública, Privada e Híbrida). Como as empresas decidem pela adoção da computação em nuvem e os impactos na gestão de serviços de TI.
- **Riscos e Consequências:** Análise crítica sobre segurança, governança de dados, riscos de interrupção e o impacto real da transformação digital nas organizações.

Módulo 5: Segurança, Qualidade e Diagnóstico

- **Segurança e Aspectos Legais**: Triângulo C.I.A (Confidencialidade, Integridade, Disponibilidade). Lei Carolina Dieckmann e LGPD."
- **Diagnóstico e VPN**: Comandos de terminal (ipconfig, ping, tracert, nmap). Conceitos de Tunelamento e Criptografia em VPNs.
- **Laboratório de Auditoria Wi-Fi e Revisão**: Simulação de auditoria com a suíte Aircrack-ng e fechamento do curso.

Módulo 6: Infraestrutura Moderna, Automação e Observabilidade

- **Infraestrutura como Código (IaC) e DevOps:** Automação do provisionamento de redes e servidores utilizando **Terraform**. Integração entre cultura de desenvolvimento e operações.
- **Microsserviços e Containers:** Virtualização em nível de sistema operacional com **Docker**. Orquestração e alta disponibilidade de aplicações com **Kubernetes**.
- **Redes Definidas por Software (SDN):** Separação entre o plano de controle e o plano de dados, tornando a rede programável via software.
- **Observabilidade e Telemetria:** Monitoramento avançado através de Logs, Métricas e Tracing para garantir a performance de sistemas complexos.
- **Segurança Avançada (DevSecOps):** Implementação de segurança contínua no ciclo de vida do software e princípios de *Zero Trust*.
- **Laboratório Prático:** Implementação de uma arquitetura multicontainer (PHP + MariaDB) integrada em rede virtualizada via Docker.

Módulo 1: Fundamentos, Infraestrutura Física e Sinais

Este módulo inicial tem como objetivo desmistificar a camada invisível das comunicações, transformando conceitos abstratos de eletricidade e luz em conhecimento estratégico para o desenvolvedor de sistemas. Antes de codificarmos aplicações complexas ou estruturarmos bancos de dados na nuvem, precisamos compreender como a informação é convertida em sinais, como os meios físicos limitam ou impulsionam a performance e de que maneira a organização física de uma rede impacta diretamente a eficiência operacional e a continuidade dos negócios em ambientes de missão crítica.

1.1. O Contexto Histórico: Do Isolamento à Rede Global

A história das redes de computadores é marcada pela transição de sistemas isolados e proprietários para um modelo de colaboração global e padronizado.

- **Décadas de 1950 e 1960:** Os computadores eram máquinas gigantescas conhecidas como mainframes, que operavam de forma isolada, processando dados localmente sem qualquer capacidade de diálogo com outras máquinas.

IBM 704

Fonte: https://www.computer-history.info/Page4.dir/pages/IBM.704.dir/index.html

- **A ARPANET e a Resiliência:** No auge da Guerra Fria, o Departamento de Defesa dos EUA criou a ARPANET com o objetivo de estabelecer uma rede que pudesse sobreviver a falhas parciais (como um ataque nuclear). Se um ponto fosse destruído, a informação deveria ser capaz de encontrar rotas alternativas.

Computador da ARPANET

Fonte: https://www.researchgate.net/figure/Figura-14-Computadores-da-ARPANET_fig1_281240965

- **Evolução Comercial:** Na década de 1970, tecnologias como a Ethernet começaram a surgir, permitindo que empresas menores conectassem seus computadores para compartilhar recursos caros, como impressoras e unidades de armazenamento.
- **O Impacto da Padronização:** O surgimento de padrões abertos permitiu que fabricantes diferentes pudessem conversar entre si, o que foi o estopim para a explosão da Internet que conhecemos hoje.

Filme: Eis os Delírios do Mundo Conectado (2016)

Acesso: https://drive.google.com/drive/folders/1-C6cey09_dTlExo15bwKTksyao_ZlxQP

1.2. Comparativo: A Evolução do Poder de Processamento e Redes

Ao comparar a escala de grandeza da evolução tecnológica é possível observar que na década de 1970 lutávamos para conectar terminais "burros" a um cérebro central limitado, hoje operamos em uma realidade onde a capacidade de processamento é distribuída, elástica e virtualmente infinita através da nuvem.

Característica	Década de 1970 (Mainframe/ARPANET)	Atualidade (Cloud/Hyper-scale)	Fator de Evolução
Velocidade de Rede	50 Kbps (Canais alugados ARPANET)	400 Gbps - 800 Gbps (Backbones de Fibra)	~16.000.000x
Processamento (CPU)	~1 MIPS (Ex: IBM 360/370)	Centenas de Milhões de MIPS (Clusters de CPUs/GPUs)	~100.000.000x
Latência (Ping)	Segundos ou centenas de milissegundos	< 1 a 10 milissegundos (Edge Computing)	~100x mais rápido
Meio Físico	Cabos coaxiais grossos e fios de cobre	Fibra Óptica e Wi-Fi 7	Salto Tecnológico
Modelo de Acesso	Terminais locais conectados via cabo	SaaS / Cloud / Mobile (Anywhere)	Mudança de Paradigma

O **PING** (Packet InterNet Groper) é um utilitário que utiliza o protocolo **ICMP** para testar a conectividade entre equipamentos. Ele funciona como um sonar: o seu computador envia um "eco" (request) e espera o "eco" de volta (reply). O tempo que esse ciclo leva é o que chamamos de **latência**.

Ao analisarmos dois exemplos PING (cnet.com e g1.globo.com.br), vemos a aplicação direta dos conceitos de **Classificação Geográfica** e **Meios de Transmissão**:

PING cnet.com (118ms):

- **Distância (WAN):** Este tempo elevado confirma que os pacotes estão percorrendo uma **WAN** (Wide Area Network), provavelmente atravessando cabos submarinos de fibra óptica até servidores nos Estados Unidos.
- **Impacto Físico:** Mesmo a luz viajando a velocidades altíssimas na fibra, a distância física e a passagem por dezenas de roteadores (saltos) geram esse atraso de ~120 milissegundos.

PING g1.globo.com (5ms):

- **Proximidade (LAN/MAN):** Uma latência de 5ms indica que o servidor está geograficamente "ao seu lado". Isso ocorre porque grandes portais utilizam **CDNs** ou infraestruturas de borda (Edge) localizadas em grandes centros como São Paulo.
- **Eficiência:** Para o usuário, a sensação é de que o site abre instantaneamente. Em termos de **SLA** (Acordo de Nível de Serviço), este é o patamar de excelência que buscamos em plataformas de missão crítica.

```
ping cnet.com

Disparando cnet.com [199.232.194.154] com 32 bytes de dados:
Resposta de 199.232.194.154: bytes=32 tempo=118ms TTL=55
Resposta de 199.232.194.154: bytes=32 tempo=119ms TTL=55
Resposta de 199.232.194.154: bytes=32 tempo=120ms TTL=55
Resposta de 199.232.194.154: bytes=32 tempo=118ms TTL=55

Estatísticas do Ping para 199.232.194.154:
   Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
         perda),
Aproximar um número redondo de vezes em milissegundos:
   Mínimo = 118ms, Máximo = 120ms, Média = 118ms
```

```
ping g1.globo.com

Disparando g1.cache.gcp.cloud.globo [186.192.83.7] com 32 bytes de dados:
Resposta de 186.192.83.7: bytes=32 tempo=5ms TTL=249
Resposta de 186.192.83.7: bytes=32 tempo=8ms TTL=249
Resposta de 186.192.83.7: bytes=32 tempo=5ms TTL=249
Resposta de 186.192.83.7: bytes=32 tempo=4ms TTL=249

Estatísticas do Ping para 186.192.83.7:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
        perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 4ms, Máximo = 8ms, Média = 5ms
```

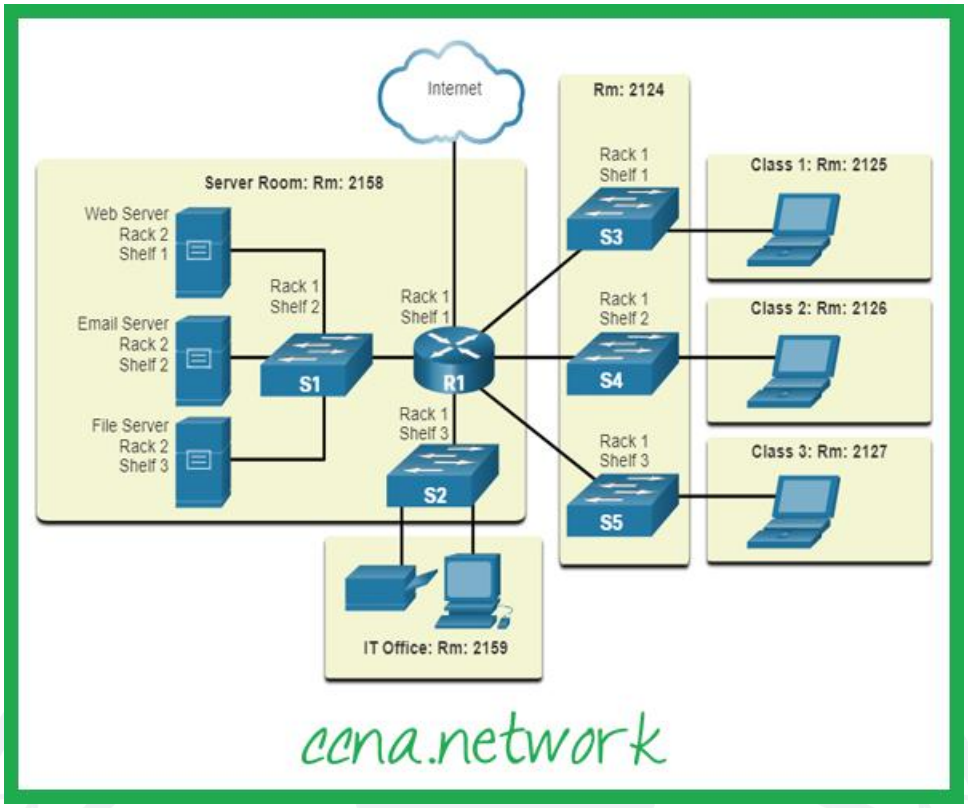
1.3. Classificação Geográfica das Redes

Dependendo da distância e da finalidade, as redes recebem classificações distintas que determinam as tecnologias de transmissão utilizadas.

- **PAN (Personal Area Network):** Redes de curtíssimo alcance, focadas no uso pessoal. Exemplo: a conexão via Bluetooth entre seu smartphone e o sistema de som do carro.

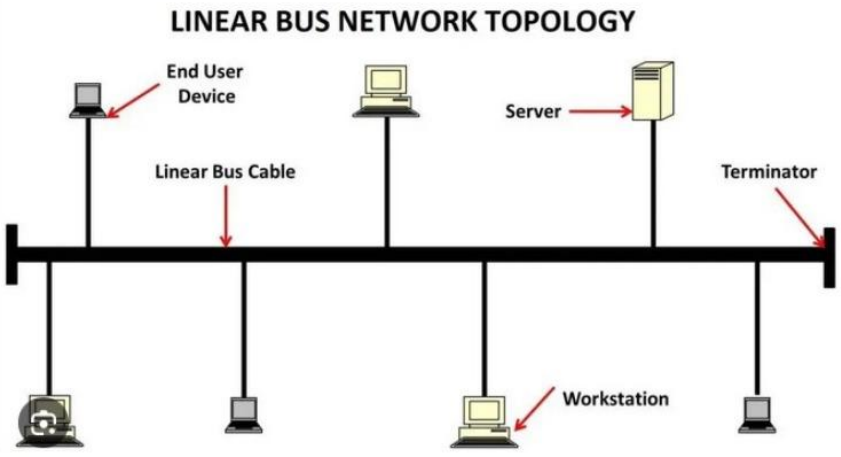
Fonte: https://pplware.sapo.pt/tutoriais/networking/lan-man-wan-pan-san-%E2%80%A6-sabe-a-diferenca/

- **LAN (Local Area Network):** Redes locais que abrangem uma área limitada, como uma residência, um escritório ou um laboratório da faculdade. Caracterizam-se por altas velocidades e baixa taxa de erro.



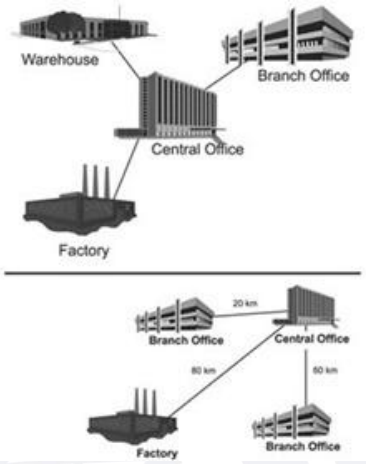
Fonte: https://ccna.network/topologias-de-lan/

- CAN (Campus Area Network): Uma variação que interconecta diversas LANs dentro de uma área geográfica específica, como um campus universitário ou um complexo industrial.



Fonte: https://www.gta.ufrj.br/ensino/eel878/redes1-2024-1/trabalhos/Grupo_13/paginas/arquitetura.html

- **MAN (Metropolitan Area Network):** Redes que conectam diversas LANs espalhadas por uma cidade ou região metropolitana. É comum em redes de TV a cabo ou conexões entre sedes de uma mesma empresa na mesma capital.

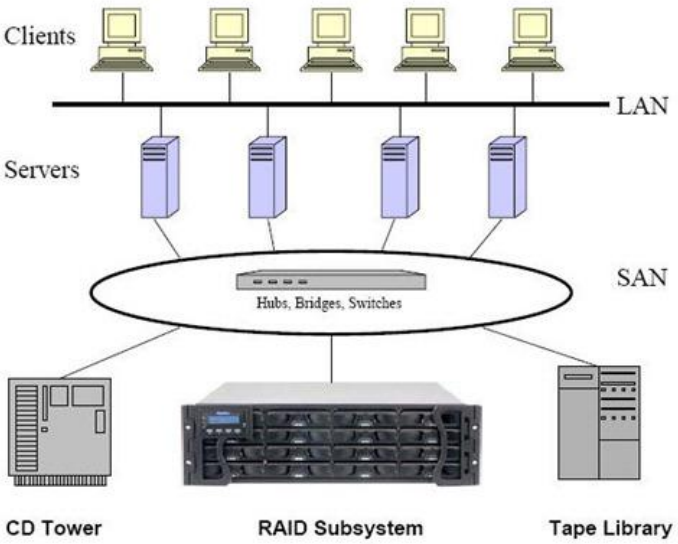


Fonte: https://pplware.sapo.pt/tutoriais/networking/lan-man-wan-pan-san-%E2%80%A6-sabe-a-diferenca/

- **WAN (Wide Area Network):** Redes de longa distância que atravessam fronteiras nacionais e continentais. A Internet é o maior exemplo de WAN do planeta.

Fonte: https://pplware.sapo.pt/tutoriais/networking/lan-man-wan-pan-san-%E2%80%A6-sabe-a-diferenca/

- **SAN (Storage Area Networks)**: Redes de armazenamento, têm como objetivo a interligação entre vários computadores e dispositivos de storage (armazenamento).



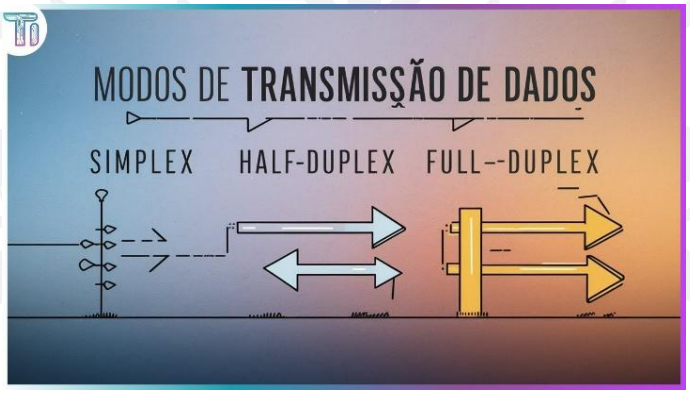
Fonte: https://pplware.sapo.pt/tutoriais/networking/lan-man-wan-pan-san-%E2%80%A6-sabe-a-diferenca/

1.3. Conceitos de Comunicação: Do Bit ao Sinal

A comunicação de dados envolve a transferência de informações entre dois pontos de forma eficiente e confiável.

1.3.1. Modos de Fluxo de Dados

- **Simplex:** A comunicação ocorre em um único sentido, sem possibilidade de resposta. Exemplo: sistemas de pager ou transmissão de TV.
- **Half-Duplex:** A comunicação é bidirecional, mas apenas um lado pode transmitir por vez. Se ambos tentarem falar, ocorre uma colisão. Exemplo: Rádios Walkie-Talkie.
- **Full-Duplex:** Transmissão e recepção ocorrem simultaneamente. É o padrão de switches modernos e conexões de fibra óptica de alta performance.



https://www.youtube.com/watch?v=NZZCDwGF3p4

1.3.2. Sincronismo, Banda e Sinais

- **Síncrona vs. Assíncrona:** Na síncrona, um sinal de relógio coordena a transmissão de grandes blocos de dados. Na assíncrona, os dados são enviados caractere a caractere, usando bits de "início" e "parada".
- **Sinais Analógicos vs. Digitais:** Sinais analógicos são ondas contínuas sujeitas a interferências. Sinais digitais são discretos (0 e 1), permitindo uma regeneração mais limpa da informação e menor taxa de erro.
- **Banda Passante (Bandwidth):** Representa a largura do canal de comunicação, ou seja, a quantidade máxima de bits que podem trafegar por segundo.
- **Banda Base (Baseband):** O sinal digital é aplicado diretamente ao meio físico sem modulação, utilizando toda a frequência disponível para uma única transmissão por vez.

1.4. Topologias de Rede: O Esqueleto Lógico

A topologia de rede é a disposição estrutural de uma rede, definindo como os diferentes nós (computadores, servidores e switches) são interconectados e como os dados trafegam entre eles. Ela é dividida em topologia física (a configuração real dos cabos e hardware) e topologia lógica (o caminho que os dados percorrem através do layout físico). A escolha da topologia impacta diretamente na escalabilidade, no custo e na facilidade de manutenção de uma empresa.

Fonte: https://www.ibm.com/br-pt/think/topics/network-topology

Barramento (Bus):

- **Estrutura:** Todos os dispositivos são conectados a um único cabo central (chamado de backbone ou espinha dorsal).
- **Vantagem:** É simples de instalar e exige pouco cabeamento, sendo ideal para redes muito pequenas ou temporárias.
- **Desvantagem:** É altamente vulnerável; se o cabo central sofrer um rompimento ou falha, toda a rede fica inativa imediatamente.

Estrela (Star):

- **Estrutura:** Cada nó da rede é conectado individualmente a um dispositivo central de conexão, geralmente um **Switch**.
- **Vantagem:** É a mais resiliente e comum no mercado atual. Se um cabo de usuário falha, apenas aquela estação fica offline, sem afetar os demais. Além disso, facilita a gestão e a localização de problemas físicos.
- **Desvantagem:** Depende totalmente do dispositivo central. Se o Switch falhar, todos os nós conectados a ele perdem a comunicação.

Anel (Ring):

- **Estrutura:** Cada dispositivo possui exatamente dois vizinhos, formando um circuito fechado. Os dados viajam em uma única direção (ou em duas, no caso de anéis duplos).
- **Vantagem:** Não há colisões de dados, pois o tráfego é ordenado por um "token" (ficha) que circula na rede.
- **Desvantagem:** Em anéis simples, a falha de um único computador pode derrubar toda a rede, pois o fluxo de dados é interrompido.

Árvore (Tree):

- **Estrutura:** Consiste em uma combinação de topologias em estrela interconectadas em uma hierarquia. Geralmente, possui um nó raiz central conectado a um ou mais nós de nível inferior (como switches), que por sua vez se conectam a estações de trabalho individuais.
- **Vantagem:** Oferece excelente escalabilidade e organização hierárquica, facilitando a expansão da rede por segmentos ou departamentos. Além disso, permite que a rede isole falhas em ramos específicos sem derrubar toda a estrutura, facilitando a manutenção em grandes infraestruturas corporativas.
- **Desvantagem:** Se o nó raiz (o topo da hierarquia) ou os switches principais que conectam os ramos falharem, todos os dispositivos conectados abaixo deles perdem a comunicação. Além disso, exige um planejamento de cabeamento mais complexo e caro em comparação com topologias simples.

Malha (Mesh):

- **Estrutura:** Cada nó está conectado a vários outros nós, criando múltiplos caminhos para o dado.
- **Vantagem:** Oferece o nível máximo de redundância e tolerância a falhas. É a topologia base da Internet e de sistemas críticos de alta disponibilidade.
- **Desvantagem:** Alto custo de implementação devido à enorme quantidade de cabos e portas de conexão necessários.

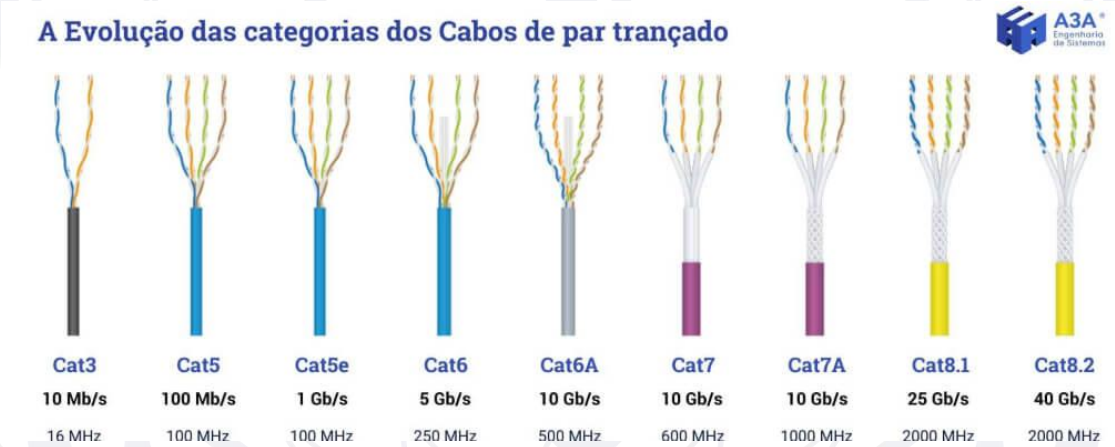
Mista (Hybrid):

- **Estrutura:** É a combinação de duas ou mais topologias (ex: várias redes em Estrela conectadas por um Barramento central).
- **Vantagem:** Oferece flexibilidade e equilíbrio entre custo e redundância, sendo a escolha padrão para grandes infraestruturas corporativas complexas

1.5. Cabeamento Estruturado e Meios Físicos

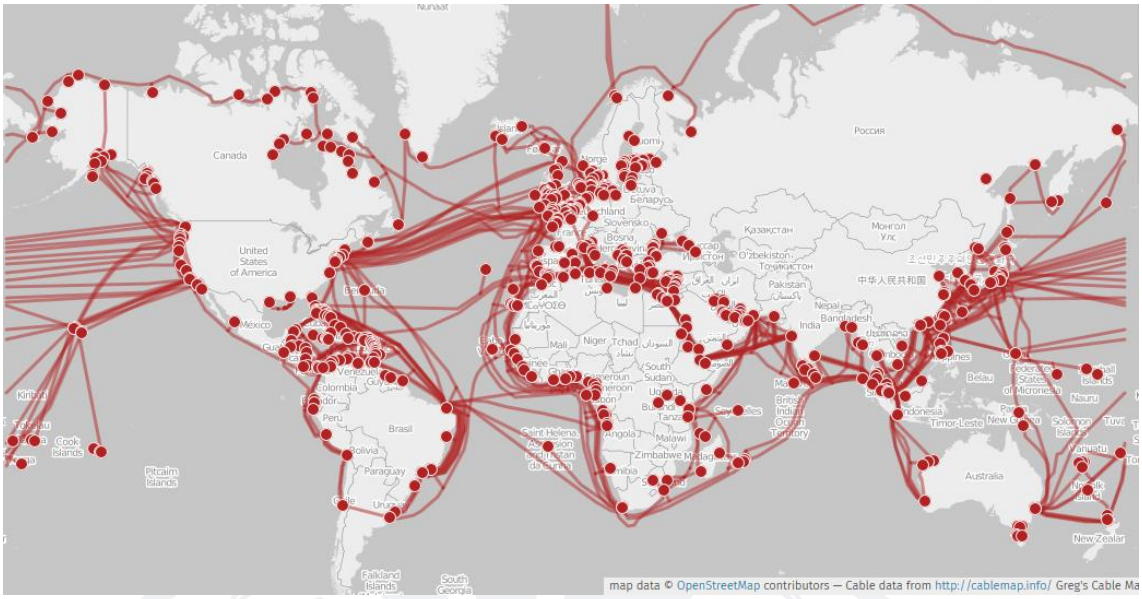
O cabeamento estruturado é a padronização da infraestrutura física para permitir flexibilidade e manutenção rápida.

- **Cabo de Par Trançado (UTP):** O meio mais utilizado em LANs. Os fios são trançados em pares para cancelar interferências eletromagnéticas externas.



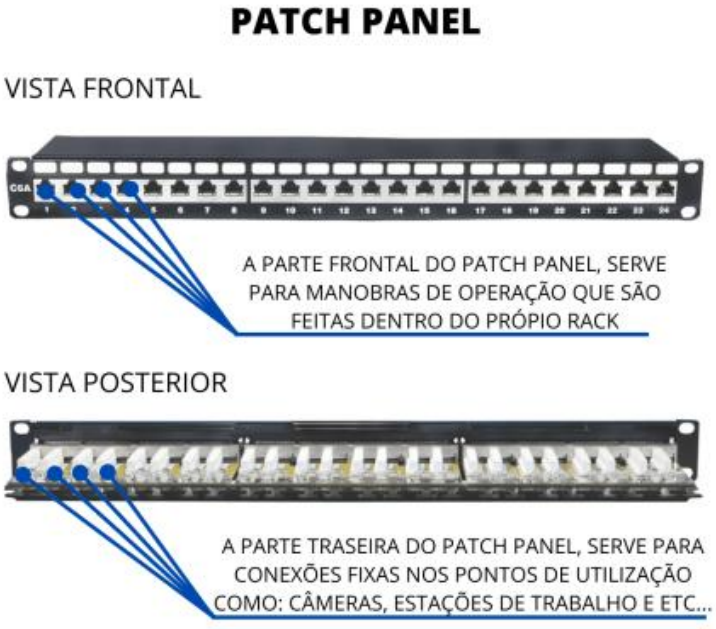
Fonte: https://a3aengenharia.com.br/conteudo/artigos-tecnicos/cabo-utp-tudo-que-voce-precisa-saber/

- **Fibra Óptica:** Transmite pulsos de luz em vez de eletricidade. É imune a ruídos elétricos, segura contra interceptações e alcança velocidades de terabits em longas distâncias.



Fonte: https://pt.wikipedia.org/wiki/Cabo_submarino

- **Normatização:** O uso de Patch Panels e Racks organizados reduz o MTTR (Tempo Médio de Reparo), permitindo que problemas físicos sejam isolados em minutos, em vez de horas.



Fonte: https://projetistapleno.com/o-que-e-um-patch-panel/

Fonte: https://www.eziblank.com/patch-panel-what-it-is-and-why-your-data-center-needs-it/

Exercícios de Fixação

1. Qual foi a principal motivação militar para o desenvolvimento da ARPANET, precursora da Internet?

a) Criar um sistema centralizado de alta velocidade.

b) Desenvolver uma rede descentralizada capaz de sobreviver a ataques parciais.

c) Permitir a transmissão de sinais analógicos de longa distância.

d) Reduzir o custo de cabeamento estruturado em bases militares.

2. Um técnico de redes precisa conectar três prédios de uma mesma empresa localizados em bairros distintos de São Paulo. Que tipo de classificação de rede ele está implementando?

a) PAN

b) LAN

c) MAN

d) CAN

3. O modo de transmissão Full-Duplex é superior ao Half-Duplex principalmente porque:

a) Utiliza sinais analógicos mais potentes.

b) Permite o envio e recebimento de dados simultaneamente, evitando colisões.

c) É o único modo que funciona com cabos de par trançado.

d) Garante que a transmissão seja sempre assíncrona.

4. Na topologia em Estrela, o que ocorre com o restante da rede se o cabo que conecta uma estação de trabalho ao Switch se romper?

a) Toda a rede para de funcionar imediatamente.

b) A rede entra em modo "barramento" automaticamente.

c) Apenas aquela estação específica fica sem conexão, enquanto o restante da rede opera normalmente.

d) O dado começa a circular em anel para encontrar outro caminho.

5. Por que a fibra óptica é o meio preferido para interconectar datacenters de missão crítica?

a) Por ser feita de cobre de alta pureza.

b) Por utilizar conectores RJ45 banhados a ouro.

c) Por ser imune a interferências eletromagnéticas e suportar altíssimas bandas passantes.

d) Por ser o meio mais barato e de fácil instalação manual.

Exemplos Práticos de Aplicação

Exemplo 1: Eficiência Operacional no Setor Financeiro

Em grandes bancos como o **Itaú/Bradesco/Santander**, a substituição de conexões antigas por infraestruturas **Full-Duplex** e cabeamento de categoria superior (CAT6A) é uma decisão estratégica. Isso reduz o número de retransmissões de pacotes de dados causadas por colisões ou ruídos, resultando em um aumento de eficiência operacional entre 35% e 45% nas plataformas de transação em tempo real.

Exemplo 2: Resiliência em Centros de Dados (Equinix)

Ao projetar a conectividade de um datacenter global como os da **Equinix**, aplicamos a **Topologia em Malha (Mesh)** nos links de fibra óptica. Isso garante que, se um cabo submarino for rompido, o sistema de roteamento encontre instantaneamente uma nova rota através de outro continente, mantendo a disponibilidade do serviço para o cliente final e reduzindo incidentes críticos em até 60%.

Módulo 2: Padronização e Camadas Iniciais

Este módulo é o coração técnico da disciplina. Ele foi desenhado para que você compreenda que a comunicação em rede não é um processo único, mas uma sucessão de etapas organizadas. Entender a padronização IEEE e a hierarquia do Modelo OSI permitirá que você, como futuro Analista de Sistemas, consiga isolar problemas de software de falhas de infraestrutura, garantindo a resiliência de plataformas de larga escala e a governança técnica necessária em ambientes corporativos de missão crítica.

2.1. Padrões IEEE 802.X: A Regulamentação do Meio

O Instituto de **Engenheiros Eletricistas e Eletrônicos** (IEEE) criou a série **802** para padronizar as redes locais e metropolitanas. Sem esses padrões, cada fabricante criaria sua própria tecnologia, impedindo a comunicação global.

https://www.youtube.com/watch?v=cjYwvEi2Dnk

- **IEEE 802.3 (Ethernet):** É o padrão mais utilizado para redes locais cabeadas. Define como os quadros de dados são montados e como as colisões são tratadas no cabo de cobre ou fibra.

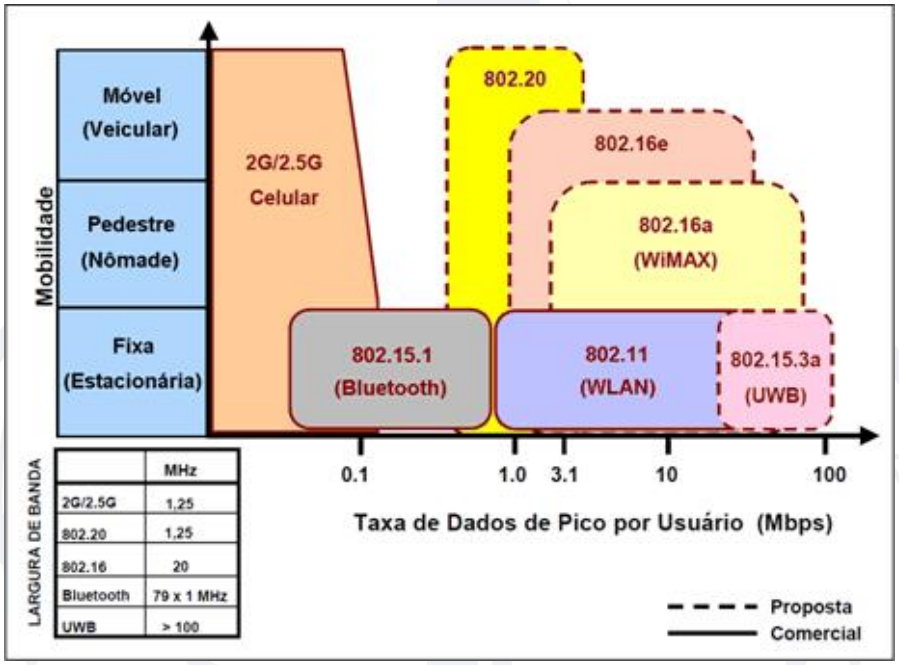
- **IEEE 802.4 (Token Bus) e 802.5 (Token Ring):** Padrões baseados na passagem de uma "ficha" (token). Embora em desuso em escritórios, foram fundamentais para entender o tráfego ordenado sem colisões.

- **IEEE 802.11 (Wi-Fi):** Padroniza a comunicação sem fio (WLAN). Evoluiu drasticamente de versões como 802.11b até o moderno Wi-Fi 6/7 (802.11ax/be).

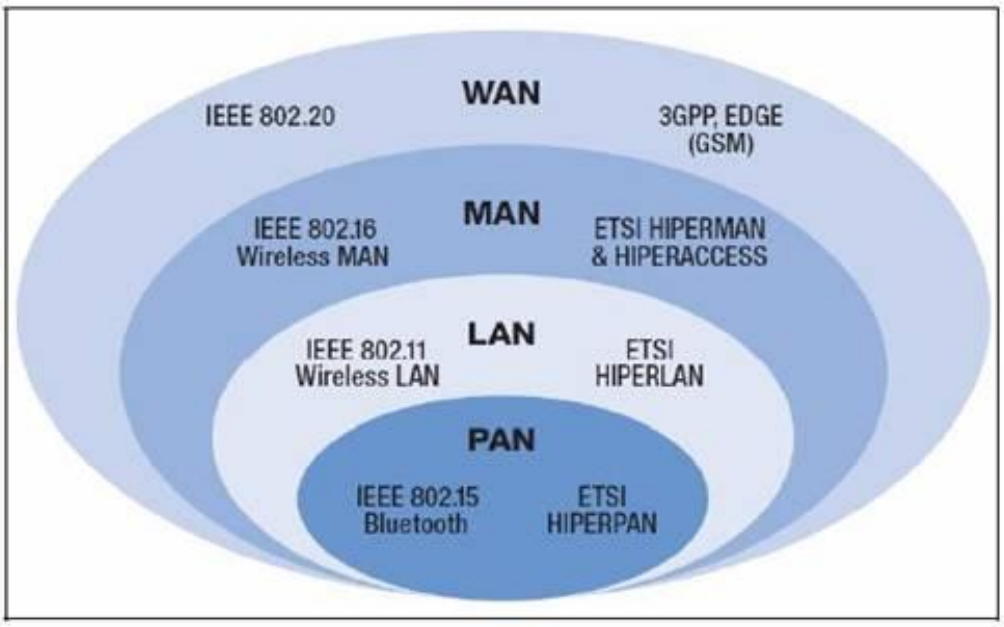
- **IEEE 802.15 (Bluetooth/WPAN):** Focado em redes de área pessoal com baixo consumo de energia.

- **IEEE 802.16 (WiMAX):** Projetado para acesso sem fio em banda larga de longa distância (WMAN), cobrindo áreas metropolitanas.

- **IEEE 802.20 (Mobile Broadband):** Especificações para redes de dados móveis de alta velocidade em ambientes com movimentação (trens, carros).



Fonte: https://www.teleco.com.br/tutoriais/tutorialww3/pagina_2.asp



Fonte: https://www.teleco.com.br/tutoriais/tutoriawimaxpa1/pagina_2.asp

Curiosidade: Starlink vs. WiMAX

É fundamental não confundir padrões de redes terrestres com protocolos de comunicação via satélite. Embora ambos usem radiofrequência, as arquiteturas são distintas:

- **IEEE 802.16 (WiMAX):** Foi projetado para fornecer acesso banda larga sem fio em áreas metropolitanas (WMAN), conectando torres de transmissão fixas no solo a antenas em prédios ou residências. Ele opera em distâncias de alguns quilômetros e enfrenta desafios de "linha de visada" terrestre.
- **Starlink (Protocolo Proprietário):** A Starlink utiliza uma arquitetura de órbita terrestre baixa (LEO) com protocolos proprietários de rádio que operam nas bandas **Ku, Ka** e **E**. Diferente do WiMAX, a Starlink utiliza tecnologias de **antenas de fase (Phased Array)** e enlaces de laser entre os satélites para gerenciar a latência e o roteamento espacial.

Por que a confusão ocorre?

Muitas pessoas associam o **WiMAX** ao **Starlink** porque ambos prometem **"internet sem fio de longa distância"**. No entanto, no nosso Modelo OSI (visto no Módulo 2):

1. **Camada Física:** O WiMAX usa modulação específica para torres terrestres; a Starlink usa feixes direcionais dinâmicos para rastrear satélites em movimento a 27.000 km/h.
2. **Escopo Geográfico:** O WiMAX é uma **MAN**; a Starlink é tecnicamente uma **WAN** global.

2.2. Modelos de Referência: OSI e TCP/IP

A comunicação em rede envolve uma vasta gama de tarefas: desde a modulação de sinais elétricos em um cabo de cobre até a renderização de uma página web complexa no seu navegador. Para gerenciar essa complexidade, os engenheiros de rede adotaram uma abordagem de "dividir para conquistar", conhecida como **arquitetura em camadas**. Cada camada tem uma função específica e fornece serviços para a camada superior, enquanto utiliza os serviços da camada inferior, criando um sistema modular onde uma mudança em uma tecnologia (como trocar o cabo de cobre por fibra óptica) não exige que o software (como o seu navegador) seja reescrito.

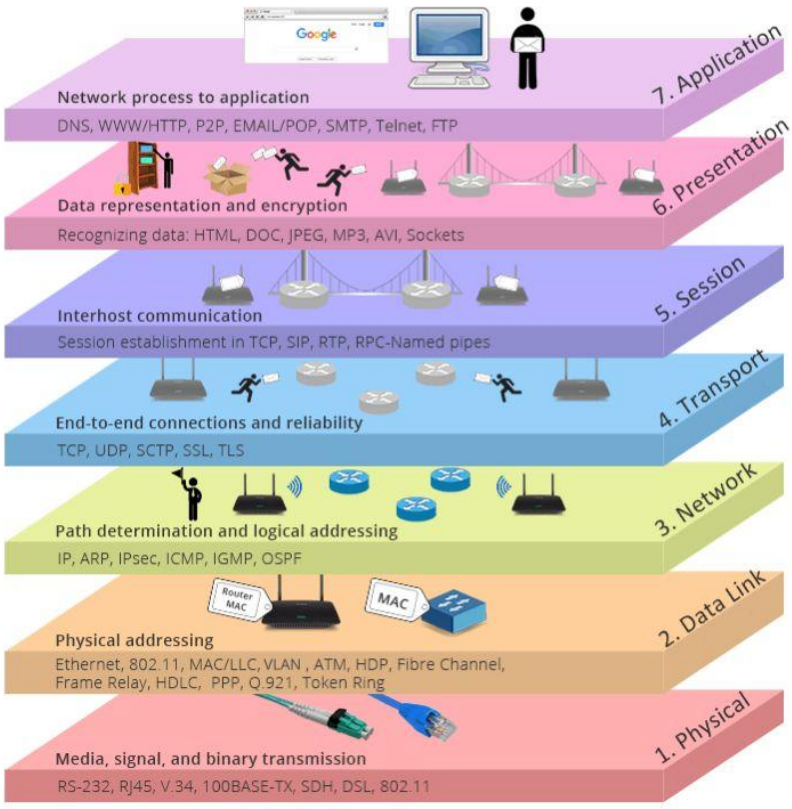
Esses modelos de referência funcionam como uma linguagem comum universal. Eles permitem que dispositivos de fabricantes completamente diferentes, operando em diferentes partes do mundo, consigam trocar informações de forma transparente

O **Modelo OSI** serve como mapa teórico e educacional para entender cada etapa do processo, e o **Modelo TCP/IP** é a implementação prática e simplificada que realmente faz a Internet e as redes corporativas funcionarem no dia a dia.

2.2.1. O Modelo RM ISO-OSI (Teórico)

O modelo OSI (Open Systems Interconnection) possui **7 camadas**. Ele é um modelo conceitual para que entendamos o "quem faz o quê":

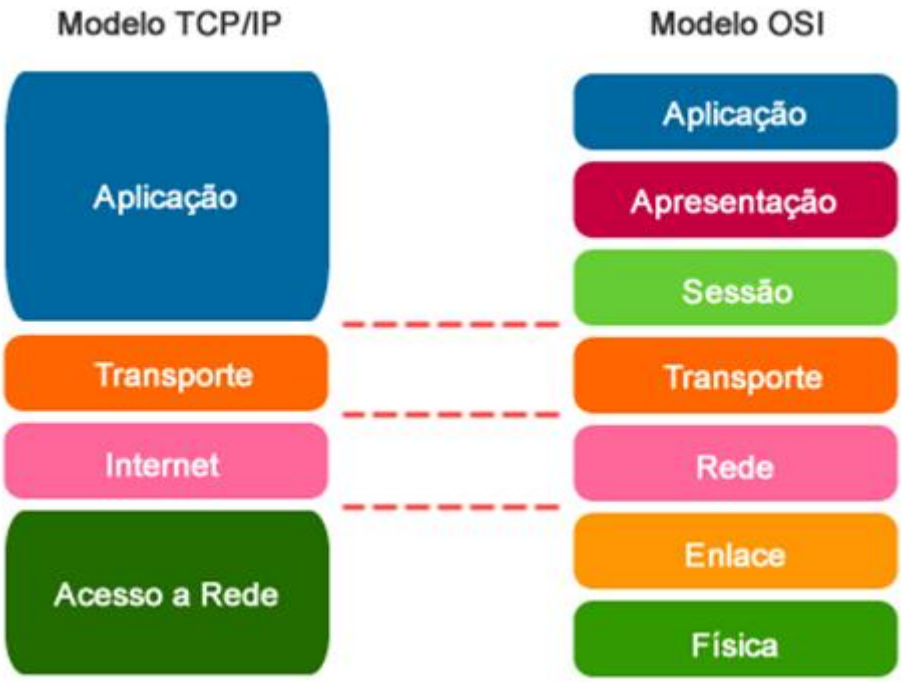
1. **Física:** Transmissão de bits brutos pelo meio físico.
2. **Enlace:** Organiza os bits em quadros e faz o controle de erros físico.
3. **Rede:** Endereçamento lógico e roteamento (IP).
4. **Transporte:** Transferência de dados fim-a-fim e correção de erros (TCP/UDP).
5. **Sessão:** Gerencia a comunicação entre aplicações.
6. **Apresentação:** Tradução, criptografia e compressão de dados.
7. **Aplicação:** Interface direta com o usuário (HTTP, E-mail).



Fonte: https://toledoesouza.com/post-jornada/o-que-e-o-modelo-osi/

2.2.2. O Modelo TCP/IP (Prático)

Enquanto que o modelo OSI foca em uma divisão teórica de sete camadas, o modelo **TCP/IP (Transmission Control Protocol/Internet Protocol)** foi desenvolvido com um foco pragmático: conectividade e resiliência. Ele é o conjunto de protocolos que sustenta a Internet e quase todas as redes corporativas modernas.



Fonte: https://www.dltec.com.br/blog/redes/4-motivos-para-aprender-modelo-osi/

O modelo TCP/IP aglutina as funções do OSI em apenas **quatro camadas principais**, tornando o processamento de rede mais ágil e menos burocrático para o hardware:

i. **Camada de Aplicação (Application):**
   - Equivale às camadas 5, 6 e 7 do modelo OSI (Sessão, Apresentação e Aplicação).
   - É onde residem os protocolos que as aplicações utilizam para trocar dados. Se você está desenvolvendo um sistema web, você opera aqui.
   - **Protocolos principais:** HTTP/HTTPS (web), DNS (resolução de nomes), SMTP (e-mail), FTP (arquivos) e DHCP (configuração automática de IP).

ii. Camada de Transporte (Transport):

- Equivale à camada 4 do OSI.
- Sua função é garantir que os dados cheguem ao destino de forma íntegra e ordenada. É o "correio" que verifica se o destinatário recebeu o pacote.
- **Protocolos principais:** * **TCP:** Focado em conexão e confiabilidade (retransmite o dado se houver erro).
    - **UDP:** Focado em velocidade e baixa latência (envia o dado sem confirmar recebimento, ideal para streaming e jogos).

iii. Camada de Internet (Internet):

- Equivale à camada 3 do OSI.
- É o "GPS" da rede. Ela define o endereço lógico (**IP**) e escolhe o melhor caminho (roteamento) para o pacote atravessar a rede global.
- **Protocolos principais:** IP (IPv4 e IPv6), ICMP (usado pelo comando PING) e ARP.

iv. Camada de Acesso à Rede (Network Access):

- Equivale às camadas 1 e 2 do OSI (Física e Enlace).
- Define como os bits são colocados no meio físico (cabos, rádio ou fibra) e como os dispositivos são identificados fisicamente pelo **MAC Address**.
- **Tecnologias principais:** Ethernet (802.3) e Wi-Fi (802.11).

Aglutinação no TCP/IP: Observe que o modelo TCP/IP simplifica a arquitetura ao unir as camadas de **Sessão, Apresentação e Aplicação** em uma única camada de Aplicação. Isso reduz a sobrecarga de processamento no software.

Acesso à Rede: Da mesma forma, as camadas **Física e Enlace** do OSI são tratadas como uma só no TCP/IP, pois na prática, o hardware (placa de rede) e o driver (enlace) trabalham de forma integrada.

Importância para o ADS: Ao depurar um sistema, se o erro for de criptografia, você está na camada de **Apresentação** (OSI) ou **Aplicação** (TCP/IP). Se o problema for o cabo desconectado, você está na camada **Física** (OSI) ou **Acesso à Rede** (TCP/IP).

2.3. Protocolos por Camada: O "Quem é Quem" na Rede

Abaixo, detalhamos os protocolos mais importantes que você encontrará no mercado de trabalho, mapeados conforme as camadas do Modelo TCP/IP.

2.3.1. Camada de Aplicação (Onde o Software reside)

Nesta camada, o foco é o serviço entregue ao usuário final.

- **HTTP / HTTPS:** O protocolo da Web. O "S" indica segurança (SSL/TLS), essencial para proteger dados sensíveis.
- **DNS (Domain Name System):** O "catálogo telefônico" da Internet. Ele traduz nomes como google.com em endereços IP.
- **DHCP:** Atribui automaticamente endereços IP para as máquinas que entram na rede, evitando conflitos manuais.
- **SMTP / IMAP:** Protocolos para envio e recebimento de e-mails.
- **FTP:** Protocolo padrão para transferência de arquivos entre servidores.

2.3.2. Camada de Transporte (A Logística do Dado)

Responsável por como o dado é levado, garantindo (ou não) a entrega.

- **TCP (Transmission Control Protocol):** É orientado à conexão. Ele verifica se cada pacote chegou; se não chegou, ele pede para reenviar. Ideal para arquivos e sites.
- **UDP (User Datagram Protocol):** Não é orientado à conexão. Ele apenas "dispara" os dados. Se algo se perder, não há reenvio. Essencial para streaming de vídeo e jogos online.

2.3.3. Camada de Internet (O GPS da Rede)

Onde ocorre o endereçamento lógico e o roteamento entre diferentes redes.

- **IP (IPv4 e IPv6):** O protocolo principal que identifica a origem e o destino na rede global.
- **ICMP:** Protocolo de mensagens de controle. É o "combustível" do comando **PING** que estudamos.
- **ARP:** Faz a ponte entre o endereço lógico (IP) e o endereço físico (MAC) da placa de rede.

2.3.4. Camada de Acesso à Rede (O Meio Físico)

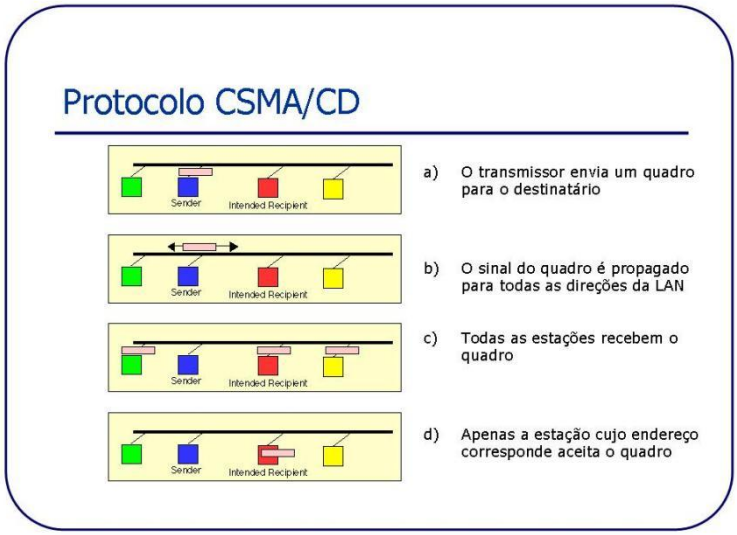
A interface entre o software e o hardware.

- **Ethernet (IEEE 802.3):** O protocolo que governa os cabos físicos e switches.
- **Wi-Fi (IEEE 802.11):** O protocolo para transmissões via rádio frequência.

2.4. Camada Física e Enlace: O Protocolo CSMA/CD

Na camada de Enlace, o maior desafio é o acesso ao meio compartilhado.

- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection):** É o "protocolo de educação" da Ethernet.
    1. **Carrier Sense:** A placa "escuta" o cabo para ver se está vazio.
    2. **Multiple Access:** Várias máquinas podem acessar o cabo.
    3. **Collision Detection:** Se duas máquinas transmitem ao mesmo tempo, elas detectam a colisão, param e esperam um tempo aleatório para tentar de novo.



Fonte: https://efagundes.com/networking/subcamada-de-acesso-ao-meio/protocolo-csmacd/

2.4. Componentes de Enlace: Switch vs. Hub vs Roteador

A evolução da performance e da inteligência das redes modernas deve-se à forma como esses dispositivos processam e encaminham os quadros e pacotes de dados.

2.4.1. Hub (O Repetidor de Sinais)

O Hub opera na **Camada 1 (Física)** do Modelo OSI.

- **Funcionamento:** É um dispositivo "burro" que simplesmente replica qualquer sinal elétrico recebido em uma porta para todas as outras portas (Broadcast).
- **Domínio de Colisão:** Todos os dispositivos conectados a um Hub compartilham um único domínio de colisão. Se dois computadores transmitem simultaneamente, ocorre uma colisão e os dados precisam ser reenviados pelo protocolo CSMA/CD.
- **Uso Atual:** Considerado obsoleto para redes profissionais devido à baixa eficiência e falta de segurança.

2.4.2. Switch (A Inteligência na Rede Local)

O Switch opera primariamente na **Camada 2 (Enlace)**.

- **Funcionamento:** É um dispositivo inteligente que aprende e armazena os endereços físicos (**MAC Address**) de cada dispositivo conectado em uma tabela interna.
- **Segmentação:** Ele cria um canal dedicado entre a origem e o destino (Unicast), eliminando colisões.
- **Domínio de Colisão:** Cada porta do Switch é seu próprio domínio de colisão, permitindo a comunicação **Full-Duplex**.
- **Uso Atual:** É o padrão para interconectar dispositivos dentro da mesma rede (LAN).

Spanning Tree Protocol (STP)

O switch é um dispositivo inteligente que pode causar um desastre se você conectar dois cabos entre os mesmos switches (criando um **loop de rede**). O STP é o protocolo que detecta isso e "desliga" logicamente uma das portas para evitar que a rede caia.

Camada 2 vs. Camada 3 (Switches L3)

Switches podem operar na **Camada 3**. Isso é fundamental para grandes empresas:

- **Layer 2:** Encaminha por endereço MAC (dentro da mesma subrede).

- **Layer 3 (Multilayer):** Consegue fazer roteamento básico entre VLANs sem precisar enviar o tráfego para um roteador externo, o que aumenta muito a performance da rede local.

2.4.3. Roteador (O GPS das Redes)

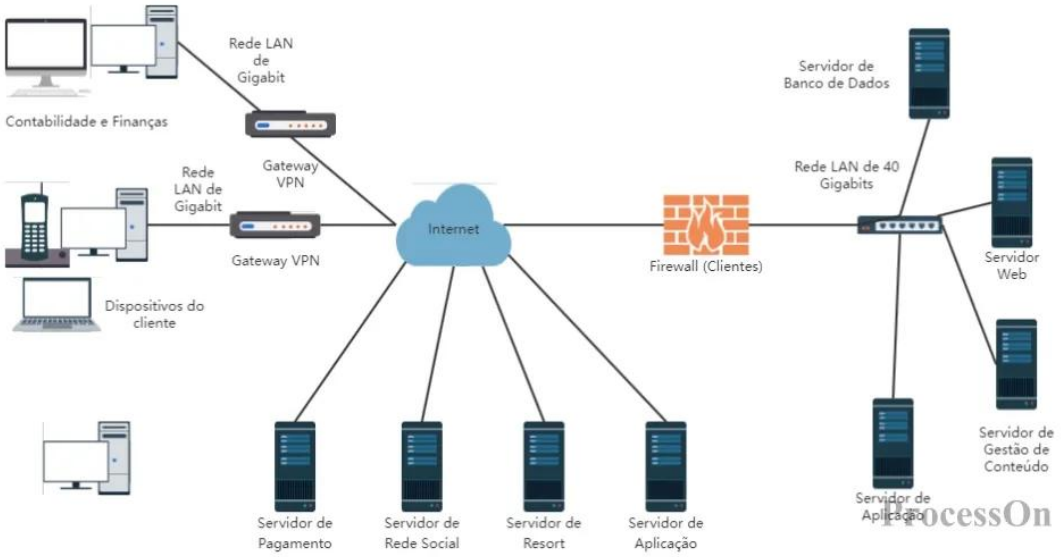
O Roteador opera na **Camada 3 (Rede)**.

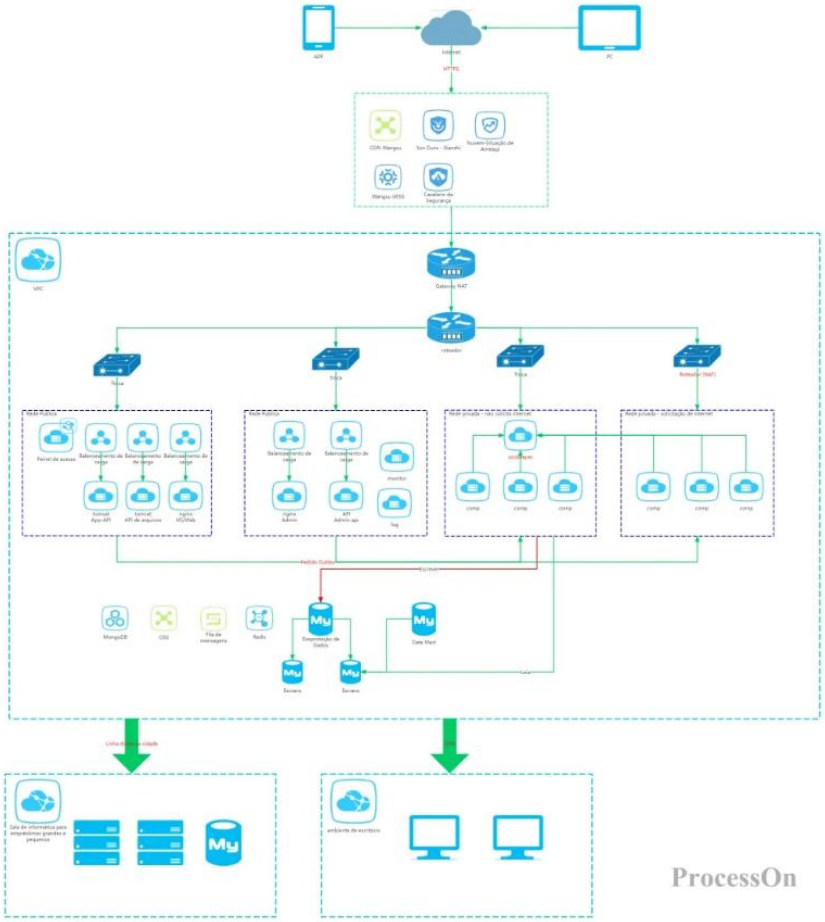
- **Funcionamento:** Enquanto o Switch conecta computadores, o Roteador conecta **redes inteiras**. Ele utiliza endereços lógicos (**IP**) para determinar o melhor caminho para o dado.
- **Isolamento:** Ele atua como o **Gateway Padrão**, servindo de porta de saída da rede local para a Internet (WAN).
- **Domínio de Broadcast:** Diferente do Switch, o Roteador bloqueia mensagens de broadcast, impedindo que o tráfego desnecessário de uma rede local "inunde" outra rede.

Aspecto	Hub	Switch	Roteador
Camada de Operação	Camada 1 (Física)	Camada 2 (Enlace) e às vezes Camada 3	Camada 3 (Rede) +2
Funcionalidade	Transmite dados (broadcast) para todos os dispositivos	Encaminha dados para dispositivos específicos via MAC	Encaminha pacotes entre redes diferentes via IP +3
Quantidade de Portas	Poucas portas (4-24)	Alta densidade (8-48+ portas)	Baixa densidade (2-8 portas WAN/LAN)
Domínios de Colisão	Único para todos os dispositivos	Separado por porta	Separado por porta
Tipo de Dispositivo	Passivo, apenas repete sinais	Ativo, processa e direciona dados	Ativo e inteligente (Roteamento) +2
Velocidade	Mais baixas (10-100 Mbps)	Mais altas (1-10 Gbps ou mais)	Variável, alcançando Tbps em backbones
Tipo de Transmissão	Half-duplex (uma via por vez)	Full-duplex (vias simultâneas)	Full-duplex
Uso	Redes pequenas ou legadas	Redes profissionais e LANs	Interconexão de redes e acesso à Internet +2
Spanning Tree Protocol	Não suporta	Suporta (prevenção de loops)	Não (usa protocolos de roteamento)
Vulnerabilidade	Alta (transmissão aberta para todos)	Menor (direcionamento por porta)	Foco em segurança de borda (Firewall/NAT) +1

Exemplo de Topologia de Rede Integrada

Imagine a estrutura de uma pequena empresa que precisa conectar seus departamentos à Internet.





Fonte: https://www.processon.io/pt/blog/network-topology-pt

i. O Roteador (A Borda)

No topo da topologia, temos o **Roteador**. Ele possui uma interface conectada ao **ISP** (Link de Internet) e outra conectada à nossa rede interna.

- **Função no exemplo:** Ele atua como o **Gateway Padrão**, realizando o roteamento de pacotes entre a rede local (LAN) e a rede mundial (WAN).

ii. O Switch (O Núcleo da LAN)

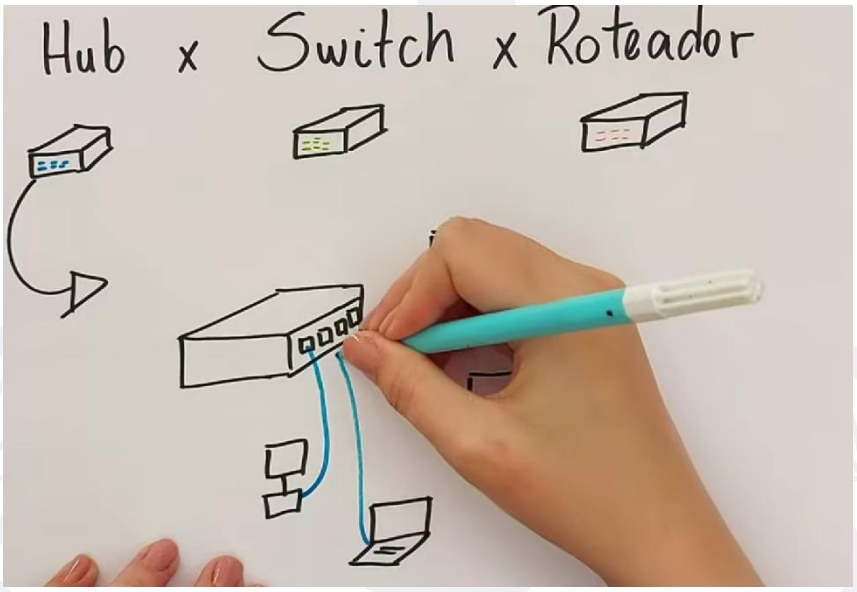
Conectado a uma das portas do Roteador, temos um **Switch de alta performance**.

- **Função no exemplo:** Ele centraliza a conexão de todos os dispositivos do escritório, como servidores, impressoras e as estações de trabalho dos desenvolvedores. Ele garante que o tráfego entre o computador do RH e a impressora não interfira no tráfego do desenvolvedor, pois cria canais dedicados via **MAC Address**.

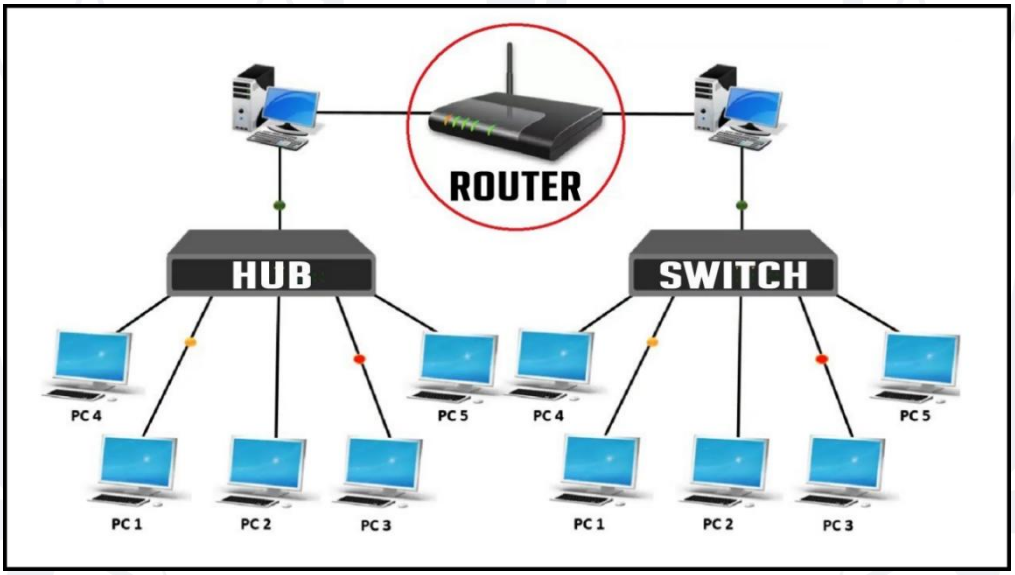
iii. O Hub (Legado para Testes)

Em uma das portas desse Switch, poderíamos ter um **Hub** conectado para um laboratório específico de monitoramento ou uma rede legada muito simples.

- **Função no exemplo:** O Hub receberia o sinal do Switch e o replicaria para todos os dispositivos nele conectados. Note que isso criaria um **domínio de colisão** único dentro dessa ramificação, reduzindo a eficiência naquele ponto específico.



Diferença entre HUB, SWITCH e ROTEADOR | Redes de computadores
Acesso: https://www.youtube.com/watch?v=BmBPhA5b-Lc



Fonte: https://ascentoptics.com/blog/pt/the-complete-guide-to-different-types-of-network-switches-for-your-network/

2.4.4. Domínios de Colisão vs. Domínios de Broadcast

Entender a segmentação de tráfego é o que permite projetar redes que não "engasgam" com o aumento de usuários. Apresenta-se uma tabela comparativa focada especificamente nos domínios de colisão e broadcast, consolidando o que vimos nos módulos de hardware e protocolos.

Esta distinção é a maior diferença prática no desempenho e na segurança da infraestrutura.

Dispositivo	Domínios de Colisão	Domínios de Broadcast
Hub	1 (Único): Todos os dispositivos compartilham o mesmo canal e "disputam" o meio físico.	1 (Único): Qualquer mensagem enviada é replicada para todas as portas (Broadcast).
Switch	1 por porta: Cada porta é seu próprio domínio de colisão, permitindo a comunicação Full-Duplex sem conflitos.	1 (Único): Por padrão, o Switch encaminha mensagens de broadcast para todos os dispositivos da rede local.
Roteador	1 por porta: As colisões são completamente isoladas entre as diferentes redes interconectadas.	1 por porta (Múltiplos): O roteador bloqueia mensagens de broadcast, impedindo que elas "inundem" outras redes conectadas.

Domínio de Colisão: Área da rede onde dois dispositivos podem transmitir dados ao mesmo tempo, causando interferência. O **Switch** resolveu este problema ao criar canais dedicados por porta.

Domínio de Broadcast: Área da rede onde uma mensagem enviada para "todos" é recebida. O **Roteador** é o único dos três que consegue segmentar esses domínios, servindo como o **Gateway Padrão** entre redes distintas.

Exercícios de Fixação

1. Qual padrão IEEE é responsável por regulamentar as redes locais sem fio, conhecidas como Wi-Fi?

a) IEEE 802.3

b) IEEE 802.15

c) IEEE 802.11

d) IEEE 802.1

2. No modelo OSI, qual camada é responsável pelo endereçamento físico (MAC Address) e pela detecção de erros na transmissão de quadros?

a) Camada 1 (Física)

b) Camada 2 (Enlace)

c) Camada 3 Rede)

d) Camada 7 (Aplicação)

3. O protocolo CSMA/CD é essencial para redes Ethernet que compartilham o mesmo meio físico. O que ele faz ao detectar uma colisão?

a) Reinicia o computador.

b) Ignora a colisão e continua transmitindo.

c) Interrompe a transmissão e aguarda um tempo aleatório antes de tentar novamente.

d) Aumenta a voltagem do cabo para "empurrar" o dado.

4. Qual a principal vantagem de um Switch em relação a um Hub antigo?

a) O Switch é mais barato.

b) O Switch envia os dados apenas para o destinatário correto, reduzindo tráfego desnecessário.

c) O Switch funciona apenas com sinais analógicos.

d) O Hub é capaz de rotear endereços IP, o Switch não.

5. Qual camada do modelo OSI é responsável pela criptografia e compressão dos dados antes de serem enviados?

a) Aplicação

b) Sessão

c) Apresentação

d) Transporte

Exemplos Práticos de Aplicação

Exemplo 1: Modernização de Agências Bancárias

Em projetos de infraestrutura para uma grande empresa, a substituição de Hubs por Switches de alta performance foi um marco. Ao implementar switches, eliminamos as colisões de pacotes (CSMA/CD), permitindo que o tráfego de dados de centenas de terminais ocorresse de forma isolada e simultânea. Isso elevou a previsibilidade da entrega em cerca de 30%, garantindo que o cliente no caixa não sofresse com lentidão por causa de outro usuário baixando arquivos pesados na mesma rede local.

Exemplo 2: Wi-Fi Corporativo e Alta Densidade

Em datacenters, ao projetar escritórios para centenas de engenheiros, utilizamos o padrão **IEEE 802.11ax (Wi-Fi 6)**. Diferente dos padrões antigos, ele gerencia melhor o acesso ao meio por múltiplos dispositivos simultaneamente. Isso reduz o tempo de resposta (latência) e garante que chamadas de vídeo de missão crítica não caiam, mesmo com centenas de dispositivos conectados no mesmo ambiente.

Módulo 3: O Protocolo da Internet e Transporte (Conteúdo Técnico Profundo)

Este módulo foi estruturado para levar o aluno do entendimento básico à capacidade de projetar arquiteturas de endereçamento complexas. Vamos explorar o IPv4 em nível de bit, entender a mecânica de fragmentação do IPv6 e dissecar o "aperto de mão" do TCP, conectando esses conceitos ao valor de negócio e eficiência operacional que as empresas buscam hoje.

https://www.youtube.com/watch?v=cwxx2c2jScE&t=24s

3.1. Endereçamento IPv4: Anatomia e Hierarquia

O IPv4 não é apenas uma sequência de números; é uma estrutura hierárquica desenhada para permitir o roteamento global eficiente.

3.1.1. Representação Binária e Decimal

Cada endereço IPv4 de 32 bits é dividido em quatro octetos.

Para o computador, o endereço **192.168.1.10** é lido como:

```
11000000.10101000.00000001.00001010
```

3.1.2. Classes de Endereçamento (Legado e Fundamentos)

- Classe A (0-127)
    - Projetada para governos e Internet Service Provider (ISPs).
    - O primeiro bit é sempre 0.
    - Permite 2^{24}, possibilita conectar a **16.777.214** dispositivos ou 16.777.216 - 2 hosts.
    - **Faixa de IPs:** 0.0.0.0 a 127.255.255.255.
    - **Exemplo de IP:** 10.50.1.1.
    - **Estrutura:** O **primeiro octeto identifica a rede** e os **outros três identificam os hosts**.

- Classe B (128-191)
    - Para grandes empresas.
    - Os dois primeiros bits são 10.
    - Permite 2^{16}, possibilita conectar a **65.534** dispositivos ou 65.536 - 2 hosts.
    - **Faixa de IPs:** 128.0.0.0 a 191.255.255.255.
    - **Exemplo de IP:** 172.16.5.1.
    - **Estrutura:** Os dois primeiros octetos identificam a rede e os **dois últimos os hosts**.

- Classe C (192-223)
    - Para pequenas empresas.
    - Os três primeiros bits são 110.
    - Permite 2^{8}, possibilita conectar a **254** dispositivos ou 256 - 2 hosts.
    - **Faixa de IPs:** 192.0.0.0 a 223.255.255.255.
    - **Exemplo de IP:** 192.168.10.1.
    - **Estrutura:** Os **três primeiros octetos identificam a rede** e o **último identifica o host**.

- Classe D (224-239)
    - Reservada para *Multicast* (transmissão para grupos específicos).
    - **Faixa de IPs:** 224.0.0.0 a 239.255.255.255.
    - **Exemplo de IP:** 224.0.0.1 (endereço usado para falar com todos os sistemas na subrede via multicast).

- Classe E (240-255)
    - Reservada para testes e pesquisas futuras.
    - **Exemplo de IP Experimental: 240.0.0.1** — Poderia ser utilizado em laboratórios de pesquisa para testar novos protocolos de roteamento antes de serem implementados em larga escala.
    - **Endereço de Teste de Rede: 244.1.2.3** — Um endereço dentro desta faixa pode ser usado por desenvolvedores de hardware para validar o comportamento de chips de rede em cenários não padronizados.
    - **O Caso Especial (255.255.255.255):** Este é o último endereço do bloco Classe E e representa o Broadcast Limitado. Ele é usado por um dispositivo para enviar uma mensagem a todos os outros dispositivos na sua rede local atual, sem que o roteador repasse essa mensagem para outras redes.

Ter 16 milhões de dispositivos em uma única rede **Classe A** parece tentador, mas na prática isso é um pesadelo técnico se não for subdividido:

- **Domínio de Broadcast:** Imagine 16 milhões de dispositivos enviando mensagens de "olá, estou aqui" ao mesmo tempo. A rede ficaria congestionada apenas com o tráfego de controle, reduzindo a eficiência operacional drasticamente.
- **Segurança e Governança:** Se você não usa subredes para dividir esse espaço, um vírus em um computador de um estagiário poderia, teoricamente, "enxergar" e atacar 16 milhões de outros servidores sem passar por um firewall interno.
- **Uso Estratégico:** Por isso, usamos a Classe A (como a rede privada 10.0.0.0) para grandes corporações, mas a **subdividimos** em milhares de pequenas redes (subredes) para garantir segurança, performance e redução de incidentes críticos.

Classes de Endereçamento Reservadas

Embora o modelo atual utilize o CIDR, os fundamentos mantêm blocos reservados para fins específicos:

- **Classe D (224.0.0.0 a 239.255.255.255):** Reservada exclusivamente para **Multicast**, ou seja, transmissões destinadas a grupos específicos de dispositivos.
- **Classe E (240.0.0.0 a 255.255.255.255):** Reservada para **testes, pesquisas e uso futuro**.

Por que não vemos a Classe E no dia a dia?

Diferente das Classes A, B e C, que você configura em servidores ou roteadores domésticos, a maioria dos sistemas operativos e equipamentos de rede descarta pacotes destinados à Classe E, a menos que estejam configurados especificamente para fins de investigação. Com a exaustão do IPv4, houve debates sobre "libertar" a Classe E para uso comum, mas a transição para o **IPv6** (que oferece um espaço de endereçamento virtualmente infinito) tornou essa mudança desnecessária

O CIDR

Se uma empresa precisasse de 300 endereços, ela não podia usar uma Classe C (limite de 254) e era obrigada a usar uma Classe B (65.534 endereços), desperdiçando milhares de IPs. Para evitar este desperdício, foi criado o CIDR () que servirá para dividir redes maiores em subredes menores.

- **Eficiência**: Com o CIDR, é possível entregar blocos de tamanho exato à necessidade da organização.
- **Redução de Tabelas de Roteamento**: Ele permite a "agregação de rotas", onde um único prefixo CIDR pode representar várias redes menores, diminuindo a carga de processamento nos roteadores da internet.

Como funciona a notação CIDR

Em vez de utilizar máscaras fixas, o CIDR utiliza um sufixo (uma barra seguida de um número) para indicar **quantos bits do endereço pertencem à rede**.

- **Exemplo**: No endereço **192.168.10.0/24**
- O **/24** indica que os **primeiros 24 bits** são a máscara de rede.
- **Flexibilidade**: O CIDR permite "emprestar" bits da parte de host para criar subredes personalizadas, como um **/26** (que utiliza 26 bits para rede e deixa 6 para hosts).

Bloco CIDR	IPs Disponíveis (Úteis)	Exemplo de Subrede e Máscara
/8	16.777.214	10.0.0.0 Máscara: 255.0.0.0
/16	65.534	172.16.0.0 Máscara: 255.255.0.0
/18	16.382	172.16.0.0 Máscara: 255.255.192.0
/20	4.094	172.16.0.0 Máscara: 255.255.240.0
/22	1.022	10.0.0.0 Máscara: 255.255.252.0
/24	254	192.168.10.0 Máscara: 255.255.255.0
/25	126	192.168.1.128 Máscara: 255.255.255.128
/26	62	192.168.10.0 Máscara: 255.255.255.192
/27	30	192.168.10.0 Máscara: 255.255.255.224
/28	14	10.50.100.32 Máscara: 255.255.255.240
/29	6	192.168.1.0 Máscara: 255.255.255.248
/30	2	10.0.0.0 Máscara: 255.255.255.252
/32	1 (Host único)	127.0.0.1 Máscara: 255.255.255.255

Exemplo Prático de Cálculo

Rede Original: 192.168.1.0/25 (128 endereços)

Ao "emprestar" 1 bit da parte de host (25 + 1 = 26), dividimos o bloco original em dois segmentos de 64 endereços cada ($2^6 = 64$).

- **Subrede A (192.168.1.0/26):**
  - **Endereço de Rede:** 192.168.1.0
  - **Intervalo de IPs úteis:** 192.168.1.1 até 192.168.1.62
  - **Endereço de Broadcast:** 192.168.1.63
  - **Máscara de Subrede:** 255.255.255.192

- Subrede B (192.168.1.64/26):
    - **Endereço de Rede:** 192.168.1.64
    - **Intervalo de IPs úteis:** 192.168.1.65 até 192.168.1.126
    - **Endereço de Broadcast:** 192.168.1.127
    - **Máscara de Subrede:** 255.255.255.192

Exemplo 2: Subdivisão de Bloco na Nuvem (VPC)

Rede Original: 10.0.0.128/25 (128 endereços)

Este cenário é comum em ambientes de Cloud, como a AWS, para separar camadas de aplicação.

- Subrede C (10.0.0.128/26):
    - **Endereço de Rede:** 10.0.0.128.
    - **Intervalo de IPs úteis:** 10.0.0.129 até 10.0.0.190.
    - **Endereço de Broadcast:** 10.0.0.191.
    - **Máscara de Subrede:** 255.255.255.192.

- Subrede D (10.0.0.192/26):
    - **Endereço de Rede:** 10.0.0.192.
    - **Intervalo de IPs úteis:** 10.0.0.193 até 10.0.0.254.
    - **Endereço de Broadcast:** 10.0.0.255.
    - **Máscara de Subrede:** 255.255.255.192.

Resumo da Lógica de Alocação

1. **Cálculo de Hosts:** Em cada subrede /26, temos 64 endereços totais, mas apenas **62 são utilizáveis** para dispositivos.
2. **IPs Reservados:** O primeiro IP identifica a rede e o último é o broadcast; nenhum dos dois pode ser atribuído a uma interface.
3. **Gateway Padrão:** Geralmente, o primeiro IP útil (.1, .65, .129 ou .193) é configurado no roteador para servir como a porta de saída da rede.

Endereços de Redes Privadas (RFC 1918) (IPV4)

Estes blocos são reservados para uso em redes locais (LANs) e não são roteáveis na Internet pública. Eles permitem que empresas e residências criem infraestruturas internas seguras:

- **10.0.0.0 a 10.255.255.255 (10.0.0.0/8):** Bloco de Classe A usado por grandes corporações.
- **172.16.0.0 a 172.31.255.255 (172.16.0.0/12):** Bloco de Classe B.
- **192.168.0.0 a 192.168.255.255 (192.168.0.0/16):** Bloco de Classe C, o mais comum em redes domésticas.

Endereços Reservados em Cada Subrede

Em qualquer divisão de rede ou subrede, existem dois endereços que nunca podem ser atribuídos a um computador ou servidor:

- **Endereço de Rede:** O primeiro IP da faixa, utilizado para identificar a rede logicamente.
- **Endereço de Broadcast:** O último IP da faixa, reservado para enviar mensagens simultâneas a todos os hosts daquela rede.

locos Especiais de Diagnóstico e Autoconfiguração

- **Loopback (127.0.0.0/8):** Reservado para testes internos do próprio computador. O endereço **127.0.0.1** é o mais conhecido, referindo-se ao "localhost".
- **APIPA (169.254.0.0/16):** Bloco reservado para atribuição automática privada quando o computador não consegue encontrar um servidor DHCP na rede.

3.1.3. O que são ISPs (Internet Service Providers)?

ISP é a sigla para **Internet Service Provider** (Provedor de Serviços de Internet). São empresas que fornecem o acesso físico e lógico à rede mundial de computadores para indivíduos, empresas e governos. Sem um ISP, você teria um computador e cabos, mas não teria uma "rota" para sair da sua rede local (LAN) para a rede mundial (WAN).

Os ISPs operam em diferentes níveis de hierarquia:

- **Tier 1 (Provedores de Espinha Dorsal):** São os gigantes que possuem os cabos submarinos e backbones de fibra óptica nacionais e internacionais. Eles não pagam pelo tráfego de rede entre si (Peering).
- **Tier 2 (Provedores Regionais):** Empresas que compram tráfego de grandes backbones para distribuir em regiões específicas, como cidades ou estados.
- **Tier 3 (Provedores Locais):** São aqueles que entregam a "última milha" (Last Mile) até a sua casa ou empresa, utilizando tecnologias como fibra (FTTH), rádio ou satélite.

Os ISPs não entregam apenas "sinal", mas gerenciam protocolos.

1. **Endereçamento IP:** O ISP é quem fornece o endereço IP (geralmente via DHCP ou PPPoE) para que seu roteador possa ser identificado na internet.
2. **Roteamento:** Eles operam roteadores de alta performance que decidem o melhor caminho para os seus pacotes atravessarem as WANs.
3. **Resolução de Nomes (DNS):** A maioria dos ISPs oferece seus próprios servidores DNS para traduzir domínios (como cnet.com) em IPs, influenciando no tempo de resposta que vimos nos testes de PING.

3.2. A Matemática do Subnetting (Subdivisão de Redes)

A subdivisão de redes é a técnica de "roubar" bits da parte de host para criar novas subredes.

3.2.1. O Cálculo Passo a Passo

Imagine que sua empresa recebeu a rede 192.168.10.0/24 e precisa de **4 subredes** para departamentos diferentes.

1. **Fórmula de subredes:** $2^n \geq$ número de subredes desejadas, onde **n** é o número de bits emprestados.
2. Para 4 redes, $2^2 = 4$. Portanto, emprestamos **2 bits**.
3. **Nova Máscara:** Os 24 bits originais + 2 bits emprestados = /26.
4. Em binário, o último octeto da máscara muda de 00000000 para 11000000 (decimal **192**).

5. **O Salto (Block Size):** 256 - 192 = 64.

6. **As Subredes resultantes:**
    - Subrede 1: **192.168.10.0** (IPs úteis de .1 a .62)
    - Subrede 2: **192.168.10.64** (IPs úteis de .65 a .126)
    - Subrede 3: **192.168.10.128** (IPs úteis de .129 a .190)
    - Subrede 4: **192.168.10.192** (IPs úteis de .193 a .254)

3.2.2. Endereços Reservados

Em toda subrede, dois endereços **nunca** podem ser usados por hosts:

- **Endereço de Rede:** O primeiro da faixa (identifica a rede).
- **Endereço de Broadcast:** O último da faixa (usado para falar com todos na rede simultaneamente).

3.3. IPv6: O Futuro Inevitável

O IPv6 não é apenas um "IP maior"; ele redesenha a eficiência da camada de rede.

- **Espaço de Endereçamento:** Com 128 bits, o IPv6 permite que cada grão de areia na Terra tenha seu próprio endereço IP público.
- **Simplificação do Cabeçalho:** Enquanto o IPv4 tem um cabeçalho variável com checksum, o IPv6 tem um cabeçalho fixo de 40 bytes, o que acelera o processamento nos roteadores.
- **Auto-configuração (SLAAC):** O dispositivo pode gerar seu próprio endereço IP sem depender de um servidor DHCP, facilitando o uso de IoT (Internet das Coisas).

3.4. Comparativo Técnico: IPv4 vs. IPv6

Esta tabela resume as principais mudanças arquiteturais. Para um aluno de ADS, é vital entender que o IPv6 foi desenhado para ser mais eficiente no processamento de hardware, além de oferecer um espaço de endereçamento virtualmente infinito.

Característica	IPv4 (Internet Protocol v4)	IPv6 (Internet Protocol v6)
Tamanho do	32 bits	128 bits

Endereço		
Formato de Notação	Decimal pontuado (ex: 192.168.0.1)	Hexadecimal (ex: 2001:0db8:85a3::8a2e:0370:7334)
Número de Endereços	~4,3 bilhões (232)	~340 undecilhões (2128)
Configuração de Endereço	Manual ou via DHCP	Autoconfiguração (SLAAC) ou DHCPv6
Segurança (IPsec)	Opcional (implementada via software)	Nativa e Obrigatória (no design do protocolo)
Cabeçalho do Pacote	Variável (20 a 60 bytes)	Fixo (40 bytes) - Mais rápido para roteadores
Fragmentação	Feita por roteadores e hosts	Feita apenas pelo host de origem
Checksum no Cabeçalho	Sim (exige reprocessamento em cada salto)	Não (delegado às camadas superiores)
Uso de NAT	Essencial para contornar a escassez de IPs	Desnecessário (cada dispositivo tem IP público)
Broadcast	Utilizado para falar com todos na rede	Substituído por Multicast e Anycast

Exercícios: Divisão de Subredes

1. Planejamento de Rede Corporativa Uma empresa recebeu o bloco **192.168.10.0/24** e precisa dividi-lo em exatamente **4 subredes** para isolar os departamentos.

- Qual será a nova máscara CIDR?
- Qual a máscara em formato decimal?
- Quantos hosts úteis cada subrede terá?

2. Endereçamento de Link Ponto-a-Ponto Para conectar dois roteadores (Gateway) em um link direto, utilizamos a máscara **/30**.

- Por que essa máscara é a mais eficiente para este cenário?
- Liste o endereço de rede, os dois IPs úteis e o broadcast para a subrede **10.0.0.4/30**.

3. Identificação de Host e Rede Dado o endereço IP 172.16.45.100/26, determine:

- O endereço de rede ao qual este host pertence.
- O endereço de broadcast desta subrede.
- A máscara de subrede correspondente.

4. Segmentação para Cloud (VPC) Ao projetar uma rede na AWS, você decide subdividir o bloco 10.0.0.0/20.

- Quantos IPs totais (incluindo reservados) existem em um bloco /20?
- Se você dividir este bloco em subredes /24, quantas subredes conseguirá criar?

5. Cálculo de Máscara Mínima Você precisa criar uma subrede que comporte, no mínimo, 500 hosts úteis.

- Qual é a menor máscara CIDR (o maior número de bits de rede) que atende a essa necessidade?
- Qual o total de IPs desperdiçados se você usar essa máscara para exatamente 500 hosts?

6. Diagnóstico de Configuração Errada Um analista configurou um servidor com o IP 192.168.1.63 e máscara 255.255.255.192 (/26).

- Por que este servidor não conseguirá se comunicar com outros hosts da rede?
- Qual é a função técnica desse endereço específico nessa subrede?

7. Desafio de Subredes IPv6 Diferente do IPv4, o IPv6 utiliza blocos muito maiores.

- Qual é o tamanho padrão de máscara CIDR recomendado para uma rede local (LAN) em IPv6?
- Explique por que o conceito de "broadcast" não existe no IPv6 e por qual método ele foi substituído.

3.5. Gateway Padrão (Default Gateway): A Saída da Rede

O **Gateway Padrão** é o nó (roteador) em uma rede de computadores que serve como um ponto de acesso a outra rede. Imagine que cada subrede é uma sala em um prédio; o Gateway é a **porta de saída** para o corredor que leva a outras salas ou para fora do edifício (a Internet).

3.5.1. Como ele funciona na prática?

Quando um dispositivo (host) tenta enviar um pacote de dados, ele primeiro verifica o endereço IP de destino:

- **Destino Local:** Se o destino estiver na mesma subrede (identificado pela máscara de subrede), o dado é entregue diretamente via Switch.
- **Destino Remoto:** Se o destino estiver fora da subrede local (como o site da Faculdade Oswaldo Cruz), o host envia o pacote para o endereço do **Gateway Padrão**.

3.5.2. Configuração e Roteamento

- **Endereçamento:** Geralmente, por convenção de engenharia, o Gateway recebe o primeiro ou o último IP útil de uma subrede (ex: em uma rede 192.168.1.0/24, o gateway costuma ser 192.168.1.1).
- **Tabela de Roteamento:** O Gateway mantém uma tabela que diz para onde cada pacote deve ser enviado para chegar ao seu destino final na WAN.
- **DHCP:** O endereço do Gateway é um dos parâmetros que o servidor DHCP entrega automaticamente para as máquinas da rede.

3.6. Camada de Transporte: O Mecanismo de Entrega

3.6.1. TCP (Protocolo de Controle de Transmissão)

É um protocolo "orientado à conexão".

- **Three-Way Handshake:** Para iniciar a conversa, ocorre o processo: **SYN** (cliente pede) -> **SYN-ACK** (servidor aceita) -> **ACK** (cliente confirma).
- **Controle de Fluxo:** Se o receptor estiver sobrecarregado, ele avisa o transmissor para diminuir a velocidade (Janela Deslizante).

- **Recuperação de Erros:** Se um pacote não chega, o TCP retransmite automaticamente.

3.6.2. UDP (Protocolo de Datagrama do Usuário)

É um protocolo "não orientado à conexão".

- **Baixa Sobrecarga:** Não perde tempo com apertos de mão ou confirmações. Ele envia e "esquece".
- **Aplicações Críticas:** Sem o UDP, chamadas de vídeo (como as que fazemos no Teams ou Zoom) seriam impossíveis devido ao atraso causado pelas retransmissões do TCP.

3.7. IoT (Internet of Things) e Tendências Tecnológicas

A Internet das Coisas (IoT) refere-se à rede de objetos físicos incorporados com sensores, software e outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela internet. Essa tendência é um dos principais motores para a migração definitiva para o **IPv6**, visto que o modelo antigo de endereçamento (IPv4) não suporta a escala de bilhões de novos dispositivos conectados simultaneamente.

3.7.1. A Arquitetura de Redes para IoT

Diferente de um computador tradicional, um dispositivo IoT muitas vezes opera em redes com restrição de energia e banda.

- **Conectividade de Baixo Consumo:** Tecnologias como **LoRaWAN** e **NB-IoT** permitem que sensores enviem dados por quilômetros consumindo o mínimo de bateria.
- **Edge Computing (Computação de Borda):** Para reduzir o tempo de resposta (latência) que vimos nos testes de PING, o processamento de dados da IoT ocorre o mais próximo possível da origem (na "borda" da rede), em vez de enviar tudo para um servidor central distante.
- **Protocolos Leves:** Enquanto a web usa o pesado HTTP/TCP, a IoT utiliza protocolos como o **MQTT** ou **CoAP**, que rodam frequentemente sobre o **UDP** para garantir agilidade e baixo consumo de recursos.

3.7.2. Tendências Tecnológicas em Redes e Cloud

Como líderes de tecnologia, observamos movimentos que moldarão os próximos anos:

1. **Redes 5G e 6G:** Além da velocidade, o foco é a densidade (milhares de dispositivos por km^2) e a latência ultrabaixa, essencial para carros autônomos e cirurgias remotas.
2. **SDN (Software Defined Networking):** A rede deixa de ser configurada manualmente cabo a cabo e passa a ser controlada por software.
3. **AIOps (Inteligência Artificial para Operações de TI):** O uso de IA para monitorar o tráfego de rede e prever falhas antes que elas aconteçam, reduzindo o MTTR (tempo de reparo) de forma drástica.
4. **Zero Trust Security:** Um modelo de segurança onde nenhum dispositivo é confiável por padrão, exigindo verificação constante em todas as camadas da rede, do IP à aplicação.

3.8. Comandos de Terminal: Ferramentas de Diagnóstico

Para gerenciar redes, utilizamos interfaces de linha de comando (CLI) que permitem interagir diretamente com a pilha de protocolos TCP/IP do sistema operacional. Abaixo, detalho os comandos essenciais para os três principais sistemas do mercado.

3.8.1. Comandos para Windows (Prompt de Comando / PowerShell)

- **ipconfig**: Exibe todas as configurações atuais da rede TCP/IP, incluindo endereço IP, máscara de subrede e gateway padrão.
    - *Uso comum*: ipconfig /all para ver detalhes como o servidor DNS e o endereço físico (MAC).
- **ping**: Testa a conectividade com um host remoto e mede a latência.
- **tracert**: Mostra o caminho exato (os saltos ou *hops*) que um pacote percorre até o destino. Útil para identificar onde a conexão está "travada".
- **nslookup**: Ferramenta para diagnosticar problemas de resolução de nomes (DNS).
- **netstat**: Exibe todas as conexões de rede ativas e as portas TCP/UDP abertas no seu computador.

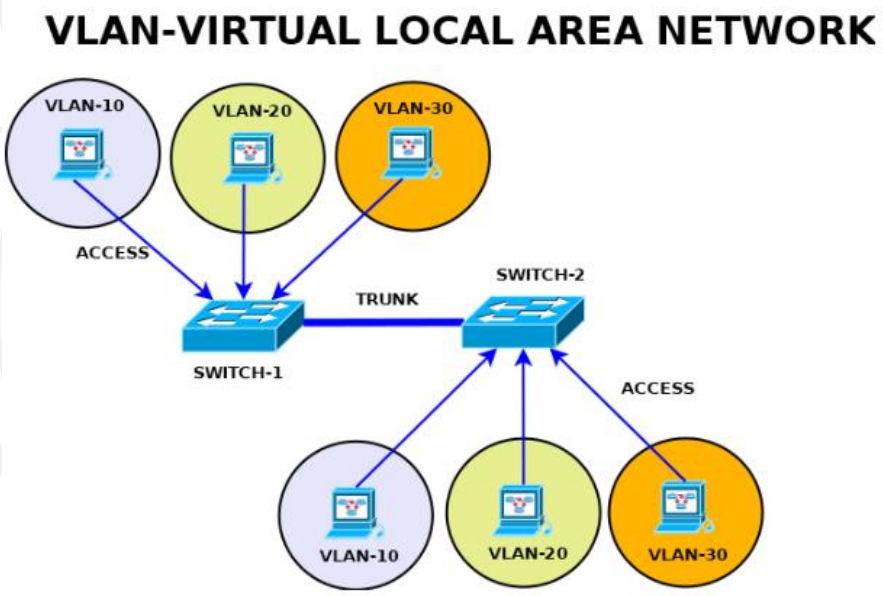
3.8.2. Comandos para Linux e macOS (Terminal)

No mundo Linux/Unix, os comandos são poderosos e amplamente usados na administração de servidores de missão crítica.

- **ifconfig ou ip addr**: Equivalente ao ipconfig, mostra os endereços e o status das interfaces de rede.
- **ping**: Funciona de forma similar ao Windows, mas no Linux ele continua disparando até que você o interrompa (Ctrl+C).
- **traceroute**: O equivalente ao tracert do Windows para mapear os saltos da rede.
- **dig**: Uma ferramenta mais moderna e detalhada que o nslookup para consultas DNS.
- **ss ou netstat**: Utilizados para investigar sockets e portas abertas (essencial para segurança).

3.9. VLANs (Virtual Local Area Networks)

As **VLANs** são redes locais virtuais que permitem segmentar uma rede física em várias redes lógicas isoladas dentro do mesmo hardware (Switch). É a tecnologia que nos permite separar, por exemplo, o tráfego de "Visitantes" do tráfego de "Servidores" sem precisar comprar cabos ou aparelhos extras.



https://www.youtube.com/watch?v=I5cKKEqIuPk

3.9.1. A Diferença Fundamental: LAN vs. VLAN

- **LAN (Local Area Network):** É uma rede definida pela conectividade física. Todos os dispositivos conectados ao mesmo conjunto de switches pertencem ao

mesmo domínio de broadcast. Se um computador envia um "Olá" para a rede, todos os outros recebem.

- **VLAN (Virtual LAN):** É uma rede definida por software. Ela ignora a localização física dos cabos. Dois computadores podem estar lado a lado no mesmo switch, mas em VLANs diferentes; eles não se "enxergarão" a menos que um roteador permita.

3.9.2. Vantagens e Desvantagens do Uso de VLANs

Vantagens:

- **Segurança:** Dados sensíveis (como o banco de dados) podem ser isolados em uma VLAN que os computadores da recepção não conseguem acessar.
- **Redução de Custos:** Menos necessidade de hardware caro e infraestrutura de cabeamento complexa.
- **Performance (Controle de Broadcast):** Reduz o tráfego desnecessário. Um broadcast enviado na VLAN do "Financeiro" não inunda a rede do "Marketing".
- **Flexibilidade:** Se um funcionário muda de mesa, basta reconfigurar a porta do switch via software, sem mexer nos cabos do forro.

Desvantagens:

- **Complexidade de Gestão:** Exige profissionais qualificados para configurar e manter as tabelas de VLAN e o roteamento entre elas.
- **Risco de Falha Centralizada:** Se o Switch principal (Core) que gerencia as VLANs falhar, todas as redes virtuais caem simultaneamente.
- **Latência de Inter-VLAN:** Para que uma VLAN fale com outra, o tráfego precisa passar por um roteador ou Switch L3, o que pode gerar um pequeno atraso.

3.9.3. Tipos de VLAN

1. **VLAN de Dados (Padrão):** Projetada para o tráfego comum de usuários (e-mails, web, arquivos).
2. **VLAN de Voz:** Prioritária. Garante que as chamadas VoIP tenham **QoS** (Qualidade de Serviço) para não sofrerem com Jitter ou quedas.
3. **VLAN de Gerenciamento:** Acesso restrito apenas aos administradores para configurar os switches e roteadores.

4. **VLAN Nativa:** Usada em links de tronco (Trunk) para tráfego que não possui uma "etiqueta" (tag).

Exemplo Prático e Roteamento Inter-VLAN

Imagine o escritório da **Faculdade Oswaldo Cruz**. Temos um único Switch de 48 portas, mas precisamos de isolamento:

- **VLAN 10 (Acadêmico):** Rede 192.168.10.0/24. Portas 1 a 20.
- **VLAN 20 (Financeiro):** Rede 192.168.20.0/24. Portas 21 a 40.

O Desafio: Por padrão, o Switch não deixará a VLAN 10 falar com a VLAN 20. **A Solução:** Precisamos de um **Roteador** (ou Switch Layer 3). Ele atuará como o Gateway para ambas as redes.

O Padrão IEEE 802.1Q (Trunking)

Para que o Switch consiga enviar o tráfego de várias VLANs para o Roteador usando apenas um cabo, utilizamos o protocolo **802.1Q**. Ele adiciona uma "etiqueta" (tag) ao quadro Ethernet para dizer: "este pacote pertence à VLAN 10".

3.10. IPv6 (Internet Protocol version 6)

O IPv6 foi desenvolvido para substituir o IPv4, cujo limite de aproximadamente 4,3 bilhões de endereços se esgotou. O novo protocolo não apenas expande o espaço de endereçamento, mas simplifica o processamento nos roteadores e melhora a segurança nativa.

3.10.1. Principais Características

- **Espaço de Endereçamento Gigantesco:** Utiliza endereços de **128 bits**, permitindo 2^{128} combinações (aproximadamente 340 undecilhões de endereços).
- **Cabeçalho Simplificado:** O cabeçalho do IPv6 é fixo em 40 bytes, o que torna o roteamento mais rápido e eficiente.
- **Segurança Nativa (IPsec):** Ao contrário do IPv4, onde o IPsec é opcional, no IPv6 ele foi projetado para ser parte integrante do protocolo.
- **Configuração Automática (SLAAC):** Dispositivos podem gerar seu próprio endereço IP sem a necessidade obrigatória de um servidor DHCP.

3.10.2. Estrutura de Endereçamento

Diferente do IPv4 (decimal), o IPv6 utiliza **notação hexadecimal**.

- O endereço é dividido em **8 grupos de 4 dígitos hexadecimais** (chamados de quartetos ou hextetos), separados por dois pontos (:).
- **Exemplo:** 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Estrutura de um Grupo (Hexteto)

Cada grupo é composto por **4 dígitos hexadecimais**. Como cada dígito hexadecimal representa 4 bits (2^4 = 16 combinações), um grupo inteiro de 4 dígitos soma **16 bits** (4x4=16).

- **Início (Valor Mínimo):** 0000
  - Em binário: 0000 0000 0000 0000
- **Término (Valor Máximo):** ffff
  - Em binário: 1111 1111 1111 1111 (onde 'f' em hexadecimal equivale ao decimal 15).

Quando juntamos os 8 grupos separados por dois pontos (:), temos o intervalo total do protocolo:

- **O Primeiro Endereço Possível (Tudo Zero):** 0000:0000:0000:0000:0000:0000:0000:0000 *(Abreviado como :: ou Endereço Não Especificado)*.
- **O Último Endereço Possível (Tudo F):** ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Regras de Abreviação:

1. **Omissão de Zeros à Esquerda:** 0db8 pode ser escrito como db8.
2. **Compressão de Zeros (::):** Grupos sequenciais de zeros podem ser substituídos por dois pontos duplos (::), mas isso só pode ser feito <u>uma única vez</u> por endereço para evitar ambiguidade.
   - *Exemplo abreviado:* 2001:db8:85a3::8a2e:370:7334

3.10.3. O que muda em relação ao IPv4?

Característica	IPv4	IPv6
Tamanho do Endereço	32 bits	128 bits
Formato	Decimal (192.168.1.1)	Hexadecimal (2001:db8::1)
Broadcast	Sim (Envia para todos)	Não existe (Substituído por Multicast)
Configuração	Manual ou DHCP	SLAAC ou DHCPv6
Checksum no Cabeçalho	Sim (Lento)	Não (Processamento mais rápido)
Fragmentação	Feita pelos roteadores	Feita apenas pela origem

3.10.4. Tipos de Endereços (As "Classes" do IPv6)

No IPv6, não usamos mais o conceito de Classes A, B ou C. Utilizamos escopos de alcance:

1. **Unicast Global (2000::/3):** Equivalente aos IPs públicos do IPv4. São roteáveis em toda a Internet.
2. **Unique Local (fc00::/7):** Equivalente aos IPs privados (RFC 1918). Usados apenas dentro de redes corporativas.
3. **Link-Local (fe80::/10):** Obrigatório em todas as interfaces. Funciona apenas no link físico local (não passa pelo roteador). É usado para comunicação básica entre vizinhos e descoberta de rede.
4. **Multicast (ff00::/8):** Usado para enviar dados a um grupo específico de dispositivos.
5. **Loopback (::1):** Equivalente ao 127.0.0.1 do IPv4.

3.10.5. O Endereço de Escopo Local (Link-Local) e o Zone Index

Ao executar comandos de diagnóstico como ipconfig (Windows) ou ip addr (Linux), é comum encontrar endereços IPv6 que terminam com um sufixo peculiar, como por exemplo: fe80::145e:4ede:9aa9:730a%3.

Para um Analista de Sistemas, entender essa anatomia é vital para o *troubleshooting* de redes locais.

A. O Identificador de Interface (730a)

Os últimos 64 bits de um endereço IPv6 (os 4 grupos finais) formam o **Interface ID**.

- **Privacidade:** Antigamente, esse ID era gerado a partir do endereço físico (MAC) da placa de rede. Hoje, por segurança, sistemas modernos geram esses grupos

de forma aleatória e temporária para evitar que o dispositivo seja rastreado entre diferentes redes.

B. O Zone Index ou Scope ID (%3)

O símbolo de porcentagem seguido de um número (%3, %11, %eth0) **não faz parte do endereço IP real**. Ele é um identificador interno do Sistema Operacional chamado **Zone Index** ou **Scope ID**.

- **Por que é necessário?** Como o prefixo fe80::/10 é obrigatório em **todas** as placas de rede do mundo, um computador com Wi-Fi e Ethernet ativos terá dois endereços "iguais" em termos de rede.
- **A Função:** O sufixo diz ao computador por qual "porta de saída" física ele deve enviar o tráfego. O número 3 no exemplo indica que aquele endereço pertence à interface de índice 3 no inventário do sistema.

Característica	IPv4 (O Clássico)	IPv6 (O Moderno)
Formato da Máscara	Decimal e CIDR (255.255.255.0 ou /24)	Apenas CIDR (ex: /64)
Identificação	Máscara de subrede	Prefix Length (Comprimento do Prefixo)
Flexibilidade	Máscaras variáveis (pode ser /24, /25, /30...)	Padrão fixo /64 para redes locais
Cálculo de Hosts	Fórmula $2^n - 2$ (complexo)	Fixo em 264 endereços por subrede
Endereço de Rede	Primeiro IP do bloco (ex: .0)	Prefixo da rede (ex: 2001:db8::/64)
Broadcast	Último IP do bloco (ex: .255)	Não existe (usamos Multicast)
Divisão de subredes	"Rouba" bits de host para a rede	Usa bits do campo "Subnet ID" (4º grupo)

🎯 Resumo para o Aluno (O "Pulo do Gato")

- No IPv4: Você calcula a máscara para economizar endereços. Se tem 10 máquinas, usa um /28. Se tem 100, usa um /25. Cada bit conta para não desperdiçar IPs.
- No IPv6: Você não economiza. O espaço é tão vasto que o foco é a organização. Toda rede local recebe um /64, o que permite trilhões de dispositivos. A "subdivisão" acontece nos grupos anteriores ao 4º hexteto, geralmente gerenciada pelo provedor ou pelo administrador da rede.

Exercícios de Fixação

1. Dada a rede 172.16.0.0/16, qual seria a máscara de subrede se precisássemos dividir essa rede em subredes de tamanho /20?

a) 255.255.0.0

b) 255.255.240.0

c) 255.255.255.0

d) 255.255.255.192

2. Qual é a principal função do campo TTL (Time to Live) no cabeçalho de um pacote IP?

a) Definir a velocidade do pacote.

b) Indicar o tempo de vida do hardware.

c) Impedir que um pacote circule eternamente na rede em caso de erro de roteamento (cada salto subtrai 1 do valor).

d) Criptografar a carga útil do dado.

3. No protocolo TCP, o que acontece se o transmissor não receber o pacote ACK (confirmação) dentro de um tempo esperado?

a) Ele encerra a conexão imediatamente.

b) Ele envia o dado novamente (retransmissão).

c) Ele muda automaticamente para o protocolo UDP.

d) Ele ignora e envia o próximo pacote.

4. Quantos endereços IPs úteis (para hosts) existem em uma subrede com máscara /29?

a) 8

b) 6 (8 total - 2 reservados)

c) 30

d) 254

5. Qual protocolo de aplicação utiliza o UDP para garantir respostas rápidas a consultas de nomes de domínio?

a) HTTP

b) FTP

c) DNS

d) SMTP

Exercícios Práticos de Aplicação

Exemplo 1: Planejamento de IP para SaaS

Ao estruturar uma rede na AWS ou Azure, não usamos uma única rede "/24". Dividimos em subredes públicas (para o site) e privadas (para o banco de dados). Isso garante que, se alguém tentar um ataque via IP, ele ficará "preso" na subrede pública e não conseguirá rotear pacotes para a subrede privada onde estão os dados dos clientes.

Exemplo 2: Otimização de MTTR

Aplicamos o monitoramento de **TCP Retransmissions**. Se esse KPI sobe, sabemos que há um problema físico (cabo ruim ou switch falhando) causando perda de pacotes. Isso permite que a equipe de SRE atue antes que o cliente perceba a lentidão no aplicativo.

Bateria de Exercícios Práticos

1. Dada a rede 192.168.10.0/24, se aplicarmos uma máscara /26, quantas subredes criaremos e quantos hosts úteis teremos em cada uma?

- **Dica:** Utilize a fórmula 2^n.

2. Qual é o endereço de Broadcast da subrede onde se encontra o host 192.168.1.130/25?

3. Um servidor na rede interna possui o IP 10.50.100.40 com máscara 255.255.255.240. Qual é o endereço de rede deste servidor?

4. Você precisa criar 6 subredes distintas a partir de uma rede Classe C. Qual é a menor máscara CIDR que atende a essa necessidade?

5. Converta o endereço IP 172.16.5.1 para binário.

6. Identifique a classe original (A, B ou C) do endereço 130.200.5.10.

7. Em um cenário de streaming de vídeo ao vivo, onde a latência baixa é prioritária, qual protocolo de transporte e qual porta padrão seriam utilizados?

8. Por que o endereço 127.0.0.1 é especial e não pode ser atribuído a uma interface física de rede?

9. Quantos endereços IPs são desperdiçados em uma rede /30 usada para um link ponto-a-ponto entre dois roteadores?

10. Se um pacote IPv4 tem o TTL (Time to Live) definido como 64 e atravessa 10 roteadores, qual será o valor do TTL ao chegar no destino?

11. Qual é o equivalente em IPv6 para o endereço de loopback (localhost) do IPv4?

12. Em um diagnóstico via PING, você recebe "Esgotado o tempo limite do pedido". Liste duas possíveis falhas nas camadas 1 ou 3 que causariam isso.

13. Diferencie um endereço IP Público de um IP Privado com base no roteamento na Internet.

14. Qual protocolo da camada de aplicação é responsável por converter o nome portal.oswaldocruz.br no IP 186.192.83.7?

15. Calcule o número máximo de hosts para uma máscara /22.

16. Explique o que acontece no "ACK" (terceiro passo) do Three-Way Handshake do TCP.

17. O IP 192.168.5.0/24 pode ser atribuído a um computador? Justifique.

18. Qual a máscara de subrede em formato decimal para o CIDR /18?

19. Em uma arquitetura de IoT, se um sensor envia dados a cada 1 segundo sem precisar de confirmação, qual protocolo de transporte minimiza o consumo de bateria?

20. O que é o Gateway Padrão (Default Gateway) em uma configuração de rede local?

21. O que acontece com um computador que possui IP e Máscara corretos, mas o campo "Gateway Padrão" está em branco?

a) Ele não consegue ligar.

b) Ele se comunica com computadores da mesma rede local, mas não acessa a Internet ou outras redes.

c) Ele queima a placa de rede por excesso de voltagem.

d) Ele assume automaticamente o IP do Google como gateway.

22. Em uma configuração típica de rede doméstica, quem geralmente desempenha o papel de Gateway Padrão?

a) O computador mais potente da casa.

b) O roteador fornecido pelo ISP (Provedor de Internet).

c) A impressora Wi-Fi. d) O servidor DNS da Google.

23. Qual comando de rede pode ser usado para verificar se o seu Gateway Padrão está respondendo corretamente?

a) DHCP –config

b) PING [IP do Gateway]

c) FORMAT C:

d) OSI --layer1

24. Se você trocar o roteador da sua empresa por um novo com um IP diferente, o que deve ser atualizado nas estações de trabalho?

a) Apenas a cor dos cabos.

b) O endereço do Gateway Padrão (manualmente ou via atualização do escopo DHCP).

c) O endereço físico (MAC) de todos os computadores.

d) A versão do protocolo IPv4 para IPv6.

25. Por que é comum usar o primeiro IP útil de uma rede como gateway?

a) Porque o protocolo IP exige que seja o número 1.

b) É apenas uma convenção de organização para facilitar a administração da rede.

c) Porque o número 1 trafega mais rápido no cabo de cobre.

d) Para evitar colisões de CSMA/CD.

26. Se um usuário relata que não consegue acessar o site da empresa, mas o comando ping [IP do servidor] funciona, qual comando você usaria para verificar se o problema é na resolução de nomes?

a) ipconfig /release

b) nslookup ou dig

c) tracert

d) netstat

27. No Linux, qual comando substituiu o antigo ifconfig em distribuições modernas para exibir endereços IP?

a) ip addr

) network-show

c) ping -a

d) traceroute

28. Qual a função do comando netstat em um servidor que hospeda a plataforma ISY.ONE?

a) Medir a velocidade da fibra óptica.

b) Listar quais portas (como a 80 ou 443) estão "ouvindo" conexões de usuários.

c) Formatar o disco rígido remotamente.

d) Alterar a máscara de subrede.

29. O comando tracert (Windows) ou traceroute (Linux) utiliza qual campo do cabeçalho IP para forçar os roteadores a responderem durante o caminho?

a) Endereço MAC

b) TTL (Time to Live)

c) Checksum

d) Payload

30. Ao executar ipconfig /all, você percebe que o endereço IP começa com "169.254.x.x". O que isso geralmente indica?

a) Que a internet está extremamente rápida.

b) Que o computador não conseguiu falar com o servidor DHCP e atribuiu um IP automático privado (APIPA).

c) Que o gateway padrão é um satélite da Starlink.

d) Que o DNS está configurado em modo analógico.

31. Qual das alternativas abaixo representa o endereço IPv6 2001:0db8:0000:0000:0001:0000:0000:0001 de forma corretamente abreviada?

a) 2001:db8::1:0:0:1

b) 2001:db8::1::1

c) 2001:db8:0:0:1::1

d) As alternativas A e C estão corretas.

Guia de Resolução e Exemplos Práticos

Para ajudar na resolução, lembrem-se da minha regra de ouro como gestor de tecnologia: **"A rede nunca mente"**.

- **Exemplo de Subnetting:** Para o exercício 1, se pegamos 2 bits emprestados ($2^2 = 4$), transformamos uma rede de 256 endereços em 4 de 64. Tirando o endereço de rede e broadcast, sobram **62 hosts úteis** por subrede.
- **Exemplo de Resiliência:** No exercício 12, se o PING falha, verificamos o cabo (Camada Física) e depois o roteamento (Camada de Rede).

Módulo 4: Cloud Computing - Estratégia e Tecnologia

Este módulo explora a transição da infraestrutura rígida para a infraestrutura fluida e programável. Vamos dissecar as camadas de serviço, os modelos de implantação e as métricas de crescimento que tornaram a nuvem o motor da economia digital moderna.

4.1. Fundamentos e Valor Estratégico

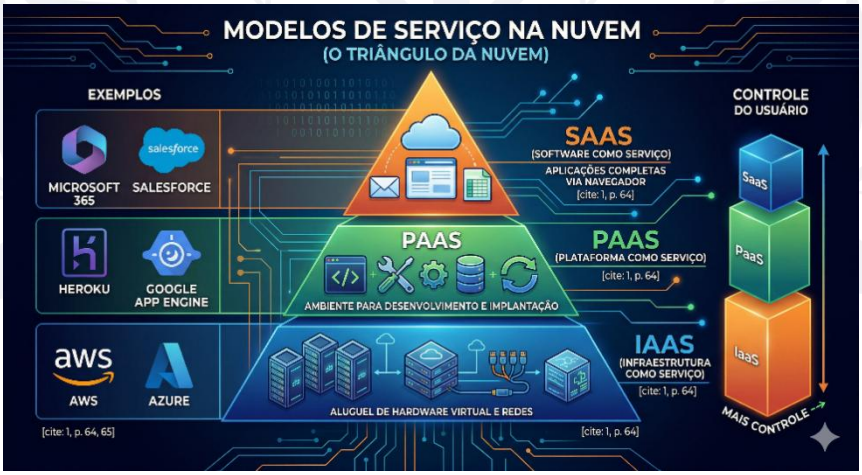
A computação em nuvem é o fornecimento de serviços de computação (servidores, armazenamento, bancos de dados, rede, software) pela Internet com tarifação baseada no uso ("pay-as-you-go").

4.1.1. Pilares sob a Ótica de Negócio

O valor estratégico da nuvem reside em quatro pilares fundamentais:

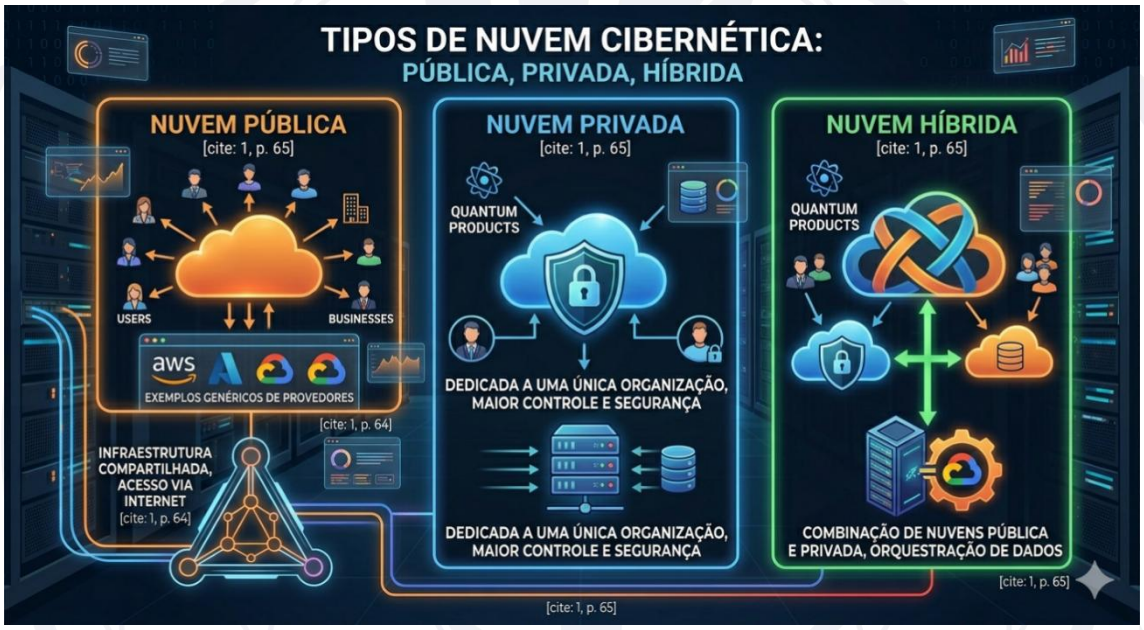
- **Agilidade:** A capacidade de subir um servidor em segundos, permitindo que o tempo de colocação no mercado (*Time-to-Market*) seja reduzido drasticamente.
- **Elasticidade e Escalabilidade:** A infraestrutura cresce ou diminui automaticamente conforme a demanda do usuário. Se seu aplicativo SaaS, como o **ISY.ONE**, recebe um pico de acessos, a nuvem aloca mais recursos sem intervenção humana.
- **Redução de Custos (CapEx vs. OpEx):** As empresas deixam de gastar milhões em hardware antecipadamente (Despesas de Capital - CapEx) e passam a pagar apenas pelo que consomem mensalmente (Despesas Operacionais - OpEx).
- **Alcance Global:** Com um clique, você pode implantar sua aplicação em data centers na Virgínia (EUA), Frankfurt (Alemanha) ou São Paulo, aproximando o dado do usuário final para reduzir a latência (o PING que estudamos).

4.1.2. Modelos de Serviço (O Triângulo da Nuvem)



- **IaaS (Infrastructure as a Service):** O nível mais básico. Você aluga o hardware virtualizado (servidores e rede). Exemplo: Amazon EC2. É onde você tem mais controle e mais trabalho de administração.
- **PaaS (Platform as a Service):** Fornece um ambiente para desenvolvedores criarem e implantarem aplicativos sem se preocupar com o sistema operacional ou patches de segurança do servidor. Exemplo: Heroku, Google App Engine.
- **SaaS (Software as a Service):** O software é entregue pronto para o usuário final via navegador. Exemplo: Microsoft 365, Salesforce. É o modelo de maior valor agregado.

4.2. Perspectiva Técnica, Adoção e Tamanho do Mercado



4.2.1. Tipos de Nuvem

- **Nuvem Pública:** Os recursos pertencem a um provedor terceirizado (como AWS, Azure ou Google Cloud) e são compartilhados por vários clientes (multi-tenancy). Oferece o menor custo e maior escalabilidade.
- **Nuvem Privada:** Recursos usados exclusivamente por uma única organização. Pode estar fisicamente no data center da empresa ou hospedada em um provedor, mas o acesso é isolado. Focada em segurança extrema e conformidade regulatória.
- **Nuvem Híbrida:** O melhor dos dois mundos. A empresa mantém dados sensíveis em sua nuvem privada e utiliza a nuvem pública para lidar com picos de demanda.

A Solução em Nuvem Pública (Cloud Bursting)

Utilizando uma nuvem pública (AWS, Azure ou Google Cloud), você projeta uma **Nuvem Híbrida**:

1. **Operação Normal:** O site roda nos seus servidores locais.
2. **O Pico de Demanda:** O sistema detecta que os servidores locais atingiram 80% de processamento.
3. **Transbordamento (Bursting):** Automaticamente, a infraestrutura "transborda" para a nuvem pública. Em minutos, 100 novas instâncias de servidores virtuais (VPS) são criadas na nuvem para absorver o tráfego extra.
4. **Encerramento:** Assim que a promoção acaba e o tráfego volta ao normal, essas 100 instâncias são desligadas automaticamente.

- **O Resultado:** Você pagou apenas pelas 24 horas de uso desses servidores (modelo **OpEx**). A empresa economizou milhares de reais em hardware e garantiu que nenhum cliente ficasse sem acesso.

4.2.2. O Gigantismo do Setor

A nuvem pública não para de crescer. Estima-se que o mercado global de serviços em nuvem pública ultrapasse os **US$ 600 bilhões** anuais. O crescimento médio anual do setor (CAGR) gira em torno de 20%. Hoje, cerca de 90% das empresas já utilizam algum tipo de serviço em nuvem. As "Big Three" dominam o mercado: **AWS (Amazon Web Services)** na liderança, seguida pela **Microsoft Azure** e **Google Cloud (GCP)**.

4.2.3. Quando usar Nuvem Pública vs. Data Center Clássico (On-Premise)

- **Recomendado Nuvem Pública:** Startups, aplicativos web com demanda variável, projetos que exigem implantação global rápida e empresas que desejam focar no "core business" em vez de gerenciar hardware físico.
- **Recomendado Data Center Clássico:** Instituições que lidam com segredos de estado, setores com regulamentações rígidas de soberania de dados que exigem armazenamento físico local, ou aplicações de baixíssima latência que precisam de processamento "ao lado" de máquinas industriais específicas.

4.3. Riscos, Segurança e Governança

A adoção da nuvem traz o desafio da **Responsabilidade Compartilhada**: o provedor cuida da segurança "da" nuvem (hardware, data center), e o cliente cuida da segurança "na" nuvem (dados, senhas, firewalls).

- **Vendor Lock-in:** O risco de ficar "preso" a um único fornecedor devido ao custo de migrar dados e reescrever código para outra nuvem.
- **Segurança e Privacidade:** Incidentes de vazamento geralmente ocorrem por má configuração do cliente (como deixar um bucket S3 aberto ao público).
- **Riscos de Interrupção:** Embora raro, as nuvens podem cair. A estratégia de **Multi-Cloud** (usar mais de um provedor) é uma tendência para mitigar esse risco.

4.4. Certificações de Mercado: O Diferencial do Profissional

Para um aluno de ADS, obter uma certificação é o caminho mais rápido para altos salários:

1. **AWS Certified Cloud Practitioner:** A porta de entrada para entender a nuvem da Amazon.
2. **Microsoft Certified: Azure Fundamentals:** Excelente para quem foca no ecossistema corporativo Microsoft.
3. **Google Associate Cloud Engineer:** Focado em quem deseja trabalhar com Kubernetes e análise de dados massiva.

🛠️ Laboratório Prático: Criando sua Primeira VPS (AWS EC2)

Para consolidar o conhecimento, vamos simular os passos para criar um servidor virtual (VPS) na AWS.

1. **Acesso ao Console:** Faça login no console da AWS e selecione o serviço **EC2**.
2. **Launch Instance:** Clique em "Executar Instância".
3. **Escolha da Imagem (AMI):** Selecione o Amazon Linux ou Ubuntu (Camada Gratuita).
4. **Tipo de Instância:** Escolha t2.micro (ideal para estudos).
5. **Configuração de Rede:**
    - Crie uma **VPC** (Virtual Private Cloud) - sua rede isolada na nuvem.
    - Atribua um **Endereço de IP Público** para que possamos acessá-lo via Internet.
6. **Security Group (Firewall):** Configure as regras de entrada. Libere a porta **22 (SSH)** para acesso remoto e a porta **80 (HTTP)** se for hospedar um site.
7. **Chave de Acesso (.pem):** Baixe a chave privada. Sem ela, você não entra no servidor.
8. **Deploy:** Clique em Executar. Em segundos, seu servidor estará ativo.

Exercícios de Fixação

1. No modelo de responsabilidade compartilhada da nuvem, quem é o responsável por aplicar patches de segurança no Sistema Operacional de uma instância IaaS?

a) O provedor de nuvem (AWS/Azure).

b) O usuário/cliente.

c) O fabricante do hardware (Intel/AMD).

d) Ninguém, a nuvem é segura por natureza.

2. Qual modelo de serviço é mais indicado para uma empresa que deseja apenas usar um software de RH pronto, sem se preocupar com infraestrutura ou desenvolvimento?

a) IaaS

b) PaaS

c) SaaS

d) VPC

3. O que define uma "Nuvem Híbrida"?

a) O uso de cabos de fibra e sinal de rádio ao mesmo tempo.

b) A combinação de infraestrutura local (On-Premise/Privada) com serviços de Nuvem Pública.

c) Uma nuvem que só funciona durante o dia.

d) Uma rede que usa IPv4 e IPv6 simultaneamente.

4. O conceito de "Elasticidade" na nuvem refere-se a:

a) A capacidade do cabo de fibra óptica de se esticar.

b) A habilidade da rede de aumentar ou diminuir recursos computacionais automaticamente conforme a demanda.

c) O preço da nuvem que nunca muda.

d) A velocidade física de rotação dos discos rígidos.

5. Por que o modelo de custos da nuvem é classificado como OpEx (Despesas Operacionais)?

a) Porque exige a compra de servidores físicos antecipadamente.

b) Porque o pagamento é baseado no consumo mensal, como uma conta de luz ou água.

c) Porque a nuvem é gratuita para empresas.

d) Porque o custo é fixo por 10 anos.

Exemplo Prático de Aplicação

Modernização: Inicialmente, poderíamos hospedar uma aplicação em um servidor físico local. No entanto, se o número de clientes triplicar em um mês, o servidor travaria. Ao migrar para a **Nuvem Pública (AWS)**, utilizamos o **Auto Scaling**. Quando o tráfego aumenta, a AWS percebe e liga automaticamente mais 2 ou 3 instâncias EC2, mantendo a experiência do usuário perfeita e a disponibilidade em 99,99%.

O Cenário Tradicional (On-Premise)

Sua empresa possui um Data Center próprio. Para suportar o tráfego normal, você utiliza 5 servidores físicos. No entanto, no dia do lançamento, o tráfego aumenta 20 vezes.

- **O Problema:** Para não deixar o site cair, você precisaria comprar, instalar e configurar mais 95 servidores.
- **O Desperdício:** Após as 24 horas de promoção, esses 95 servidores ficariam ociosos, gerando custos de energia, refrigeração e manutenção por meses, sem serem utilizados. Isso é um uso ineficiente do **CapEx** (Investimento em Capital).

Módulo 5: Segurança e Qualidade de Redes de Computadores

Este módulo foi desenhado para capacitar o aluno a identificar vulnerabilidades, entender as implicações jurídicas de atos cibernéticos e aplicar metodologias de diagnóstico para garantir que a rede seja resiliente e confiável.

5.1. Principais Aspectos sobre Segurança e Qualidade

A segurança da informação é sustentada por três pilares fundamentais, conhecidos como a **Tríade CID**. Para garantir a integridade de sistemas como o **ISY.ONE**, cada um desses pontos deve ser protegido contra ameaças específicas.

i. Confidencialidade

Garante que a informação seja acessada apenas por pessoas ou sistemas devidamente autorizados. O objetivo é evitar o vazamento de dados sensíveis.

- **Exemplo Prático 1 (Criptografia):** Quando um usuário acessa o portal acadêmico da Oswaldo Cruz, o uso do protocolo **HTTPS (SSL/TLS)** garante que a senha enviada não seja lida por invasores "escutando" a rede (ataque *Sniffing*).
- **Exemplo Prático 2 (Controle de Acesso):** Em um sistema de RH, apenas os gestores financeiros podem visualizar os salários dos funcionários. Um desenvolvedor sem essa permissão não deve ter acesso a essas tabelas no banco de dados, mesmo que tenha acesso ao servidor.

ii. Integridade

Garante que a informação não seja alterada de forma indevida ou acidental durante o armazenamento ou transmissão. A informação deve ser fidedigna e exata.

- **Exemplo Prático 1 (Hashing):** Ao baixar uma imagem ISO do Linux Ubuntu para o laboratório, o site fornece um código **SHA-256**. O aluno calcula o hash do arquivo baixado; se os códigos forem iguais, a integridade está garantida e o arquivo não foi corrompido ou alterado por malware.
- **Exemplo Prático 2 (Assinatura Digital):** No envio de um contrato em PDF via e-mail, a assinatura digital garante que nenhuma cláusula foi alterada após a assinatura do remetente. Se um único caractere for mudado, a assinatura torna-se inválida.

iii. Disponibilidade

Garante que o sistema e os dados estejam acessíveis aos usuários autorizados sempre que necessário.

- **Exemplo Prático 1 (Redundância/Cloud):** Se o servidor principal da **ISY.ONE** sofrer um problema de hardware, um balanceador de carga (Load Balancer) direciona automaticamente o tráfego para um servidor reserva na nuvem (AWS/Azure), mantendo o sistema online.
- **Exemplo Prático 2 (Ataques DoS):** Um ataque de Negação de Serviço (DoS) tenta derrubar a disponibilidade inundando o servidor com tráfego falso. A implementação de um **Firewall** com regras de bloqueio de IP ajuda a mitigar esse risco e manter o serviço disponível para os alunos.

5.1.2. Qualidade de Serviço (QoS)

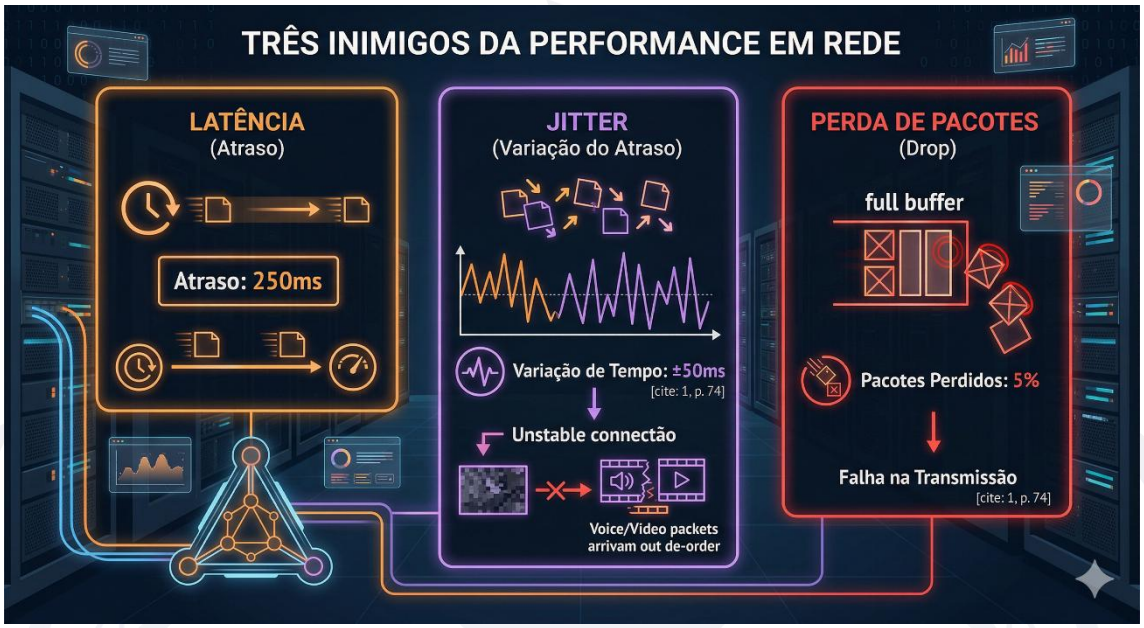
O QoS não "aumenta" a largura de banda física, mas sim **prioriza** como essa banda é utilizada. Imagine uma rodovia com uma faixa exclusiva para ambulâncias; o QoS é o "policiamento" que garante que o tráfego prioritário chegue ao destino sem atrasos, mesmo em horários de pico.

A. Os Três Inimigos da Performance

Para entender o QoS, o aluno deve dominar os três problemas que ele visa mitigar:

1. **Latência (Atraso):** O tempo que um pacote leva para ir da origem ao destino. Latência alta torna chamadas de voz e vídeo impossíveis.
2. **Jitter (Variação do Atraso):** É a oscilação na latência. Se um pacote de áudio chega em 10ms e o seguinte em 50ms, o som sairá "picotado" ou robotizado.

3. **Perda de Pacotes (Loss):** Ocorre quando os buffers dos roteadores lotam e pacotes são descartados. Para dados (TCP), isso causa lentidão pela retransmissão; para voz (UDP), causa falhas no som.



B. Mecanismos de Funcionamento

O QoS opera através de etapas sequenciais nos ativos de rede (switches e roteadores):

- **Classificação e Marcação:** O tráfego é identificado. Pacotes de voz podem ser marcados com um valor de **DSCP** (Differentiated Services Code Point) no cabeçalho IP para que todos os roteadores saibam que eles são prioritários.
- **Gerenciamento de Filas (Queuing):** Em vez de uma fila única (FIFO), o roteador cria várias "filas de espera". A fila de voz é processada sempre antes da fila de downloads de e-mail.
- **Policiamento e Modelagem (Shaping):** Limita o tráfego de aplicações não essenciais (ex: limitar o YouTube a 10% da banda) para garantir que o sistema **ISY.ONE** tenha sempre banda disponível.

C. Modelos de Implementação

1. **Best Effort:** Sem QoS. O primeiro que chega é o primeiro que sai.
2. **IntServ (Integrated Services):** Reserva banda de ponta a ponta antes da transmissão começar (complexo e pouco escalável).

3. **DiffServ (Differentiated Services):** O modelo mais usado. Cada pacote carrega sua própria "prioridade" no cabeçalho, e cada roteador decide como tratá-lo com base em políticas locais.

5.2. Aspectos Legais e Invasão de Sistemas

A segurança cibernética não é apenas um desafio técnico, mas um imperativo jurídico. No Brasil, o marco divisor foi a **Lei 12.737/2012** (conhecida como Lei Carolina Dieckmann), que alterou o Código Penal para tipificar crimes informáticos.

5.2.1. Invasão de Dispositivo Informático (Art. 154-A)

O crime ocorre ao invadir dispositivo alheio, conectado ou não à rede, mediante violação de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização.

- **Ponto Chave:** A lei pune a **invasão** em si. Mesmo que o invasor não "roube" nada, o simples fato de quebrar a segurança para entrar no sistema já configura o crime.
- **Qualificadoras:** A pena aumenta se a invasão resultar em obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, ou controle remoto do dispositivo.

5.2.2. A Lei Geral de Proteção de Dados (LGPD - Lei 13.709/2018)

Enquanto o Código Penal foca no "invasor", a LGPD foca no **controlador dos dados** (a empresa). Para qualquer plataforma **SaaS**, a conformidade com a LGPD é vital.

- **Responsabilidade Civil:** Se um sistema sofre uma invasão por negligência técnica (ex: falta de patches de segurança ou portas abertas desnecessariamente), a empresa pode ser multada e obrigada a indenizar os titulares dos dados.
- **Princípio da Transparência:** Em caso de incidentes de segurança, a lei exige que a empresa comunique a Autoridade Nacional de Proteção de Dados (ANPD) e os usuários afetados em prazo razoável.

5.2.3. Ética Profissional e "Hacking" Ético

O profissional de segurança ética deve operar sob um conjunto rígido de regras. A principal diferença entre um hacker ético e um invasor comum reside na **intenção** e na **autorização**.

Os Mandamentos do Hacker Ético:

1. **Autorização Explícita:** Nunca realizar testes sem um documento assinado (Termo de Engajamento).
2. **Respeito ao Escopo:** Se o contrato autoriza testar o servidor, o profissional não deve tentar acessar o e-mail pessoal dos funcionários.
3. **Confidencialidade:** Qualquer vulnerabilidade encontrada deve ser reportada exclusivamente ao cliente, nunca exposta publicamente ou vendida a terceiros.

Exemplos de Comportamentos Éticos vs. Antiéticos

Para facilitar a compreensão, aqui estão exemplos práticos de como a ética se aplica no dia a dia do Analista de Sistemas:

Situação	Comportamento Ético	Comportamento Antiético
Descoberta de Falha	Reportar imediatamente ao responsável pelo sistema via canais oficiais (como um programa de Bug Bounty).	Explorar a falha para obter dados ou postar a vulnerabilidade em fóruns públicos para "ganhar fama".
Acesso a Dados Sensíveis	Ao encontrar dados pessoais expostos durante um teste, interromper a visualização e reportar o vazamento sem copiar os dados.	Baixar o banco de dados de clientes para "provar" que a falha existia ou para uso pessoal futuro.

Uso de Ferramentas	Utilizar ferramentas de scan de rede apenas em ambientes de laboratório ou redes autorizadas.	Rodar um Nmap ou Wireshark na rede Wi-Fi da faculdade para capturar senhas de outros alunos.
Senhas e Acessos	Solicitar a criação de usuários de teste específicos para realizar auditorias.	Utilizar técnicas de engenharia social para enganar colegas e obter suas senhas reais de produção.

O Papel do Analista na Sociedade

Ser um Analista de Sistemas ético significa entender que você detém as "chaves do reino". A integridade do seu trabalho reflete diretamente na segurança de milhares de usuários que utilizam seus sistemas.

Exemplo de Dilema Ético para Sala de Aula: "Um administrador de redes nota que um colega de trabalho está acessando sites proibidos pela política da empresa. O administrador deve usar seus privilégios para ler o histórico privado do colega ou deve seguir o protocolo oficial de reporte sem invadir a privacidade além do necessário?"

Resposta Ética: O profissional deve agir estritamente conforme as políticas da empresa e a LGPD. O monitoramento deve ser feito sobre os logs da rede, e não através de invasão de privacidade pessoal desnecessária, garantindo que o processo seja legal e auditável.

5.3. Tipos de Invasão e Impactos no Negócio

As ameaças modernas são sofisticadas e podem destruir a reputação de uma empresa em minutos.

5.3.1. Principais Tipos de Ataque

No cenário atual de cibersegurança, os ataques evoluíram de simples brincadeiras para operações de espionagem e extorsão altamente sofisticadas. Como futuro Analista de Sistemas, você deve conhecer os mecanismos de operação das ameaças mais comuns:

A. Negação de Serviço (DoS e DDoS)

O objetivo principal não é roubar dados, mas sim ferir o pilar da **Disponibilidade**.

- **DoS (Denial of Service):** Um único atacante envia uma avalanche de requisições para um servidor até exaurir seus recursos (CPU, RAM ou banda).
- **DDoS (Distributed Denial of Service):** O ataque parte de milhares de dispositivos infectados (botnets) simultaneamente. É o pesadelo de qualquer serviço em nuvem, como o **ISY.ONE**, pois é muito difícil de filtrar devido à origem pulverizada.

B. Engenharia Social e Phishing

Exploram a "vulnerabilidade humana" em vez de falhas de software.

- **Phishing:** O atacante envia comunicações (e-mails, SMS) simulando ser uma entidade confiável (como o suporte da Oswaldo Cruz ou um banco) para induzir o usuário a clicar em links maliciosos ou entregar credenciais.
- **Spear Phishing:** Um ataque direcionado. O invasor estuda o alvo (ex: o setor financeiro da Quantum Products) para criar uma mensagem personalizada e altamente convincente.

C. Malware (Ransomware e Spyware)

- **Ransomware:** Atualmente a maior ameaça corporativa. O malware criptografa os dados do servidor e exige um resgate (geralmente em criptomoedas) para liberar a chave de descriptografia.
- **Spyware:** Softwares projetados para monitorar atividades e coletar informações silenciosamente, como senhas digitadas (Keyloggers).

D. Homem no Meio (Man-in-the-Middle - MitM)

O atacante se posiciona entre o usuário e o servidor, interceptando a comunicação.

- **Cenário comum:** O uso de Wi-Fi público não confiável. O invasor pode ler tudo o que você trafega se a conexão não estiver protegida por HTTPS/SSL.

E. Injeção de Código (SQL Injection)

Um ataque clássico contra aplicações web mal programadas.

- **Mecanismo:** O atacante insere comandos SQL em campos de formulário (ex: campo de login). Se o sistema não validar os dados, o invasor pode burlar a autenticação ou até apagar o banco de dados inteiro.

5.3.2. Consequências para o Negócio

Quando um dos ataques descritos no item anterior é bem-sucedido, as repercussões podem ser categorizadas em quatro dimensões críticas:

A. Impacto Financeiro Direto e Indireto

- **Perda de Receita:** Se o sistema sofrer um ataque de DDoS e ficar offline por 4 horas, a empresa deixa de processar vendas e de captar novos clientes durante esse período.
- **Custos de Remediação:** Incluem o pagamento de horas extras para a equipa de TI, contratação de consultorias forenses para investigar a invasão e a possível substituição de hardware danificado.
- **Resgates (Ransomware):** Embora não seja recomendado pelas autoridades, muitas empresas enfrentam o dilema financeiro de pagar resgates vultuosos para recuperar dados vitais.

B. Danos à Reputação e Marca

Este é frequentemente o dano mais difícil de recuperar. No mundo digital, a **confiança** é a base do negócio.

- **Churn (Perda de Clientes):** Clientes que sentem que os seus dados não estão seguros tendem a migrar para a concorrência.
- **Desvalorização de Mercado:** Para empresas listadas em bolsa, um incidente grave de segurança costuma gerar uma queda imediata no valor das ações.

C. Repercussões Legais e Regulatórias (Conformidade)

Com a vigência da **LGPD** no Brasil e regulamentações internacionais (como a GDPR), as consequências jurídicas tornaram-se severas:

- **Multas Administrativas:** A ANPD pode aplicar multas que chegam a 2% do faturamento da empresa (até 50 milhões de reais por infração).
- **Processos Judiciais:** Clientes cujos dados foram expostos podem entrar com ações individuais ou coletivas por danos morais e materiais.

D. Interrupção Operacional e Perda de Produtividade

- **Paralisia de Processos:** Em ataques de Ransomware, a empresa pode ficar dias sem acesso a e-mails, folhas de pagamento ou sistemas de gestão, forçando o retorno a processos manuais ineficientes.
- **Desvio de Foco:** A equipa de desenvolvimento, em vez de criar novas funcionalidades para o produto, precisa de parar tudo para focar na recuperação do ambiente.

5.4. Diagnóstico Minucioso da Rede

Um diagnóstico profissional exige uma abordagem em camadas, começando pelo monitoramento passivo até o teste ativo.

1. **Linha de Base (Baseline):** Conhecer o comportamento normal da rede (tráfego médio, latência padrão).
2. **Análise de Protocolo:** Utilizar sniffers para inspecionar o conteúdo dos pacotes.
3. **Varredura de Vulnerabilidades:** Identificar portas abertas e serviços desatualizados.
4. **Teste de Intrusão (Pentest):** Simular um ataque controlado para validar as defesas.

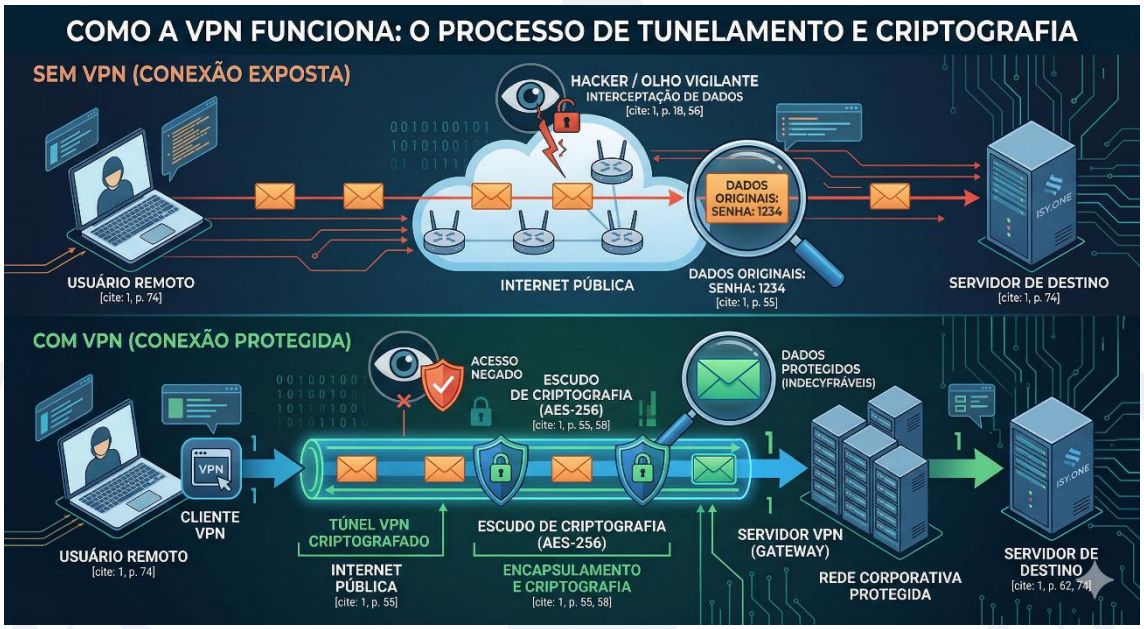
5.5. Ferramentas Gratuitas para Teste de Segurança

Existem ferramentas poderosas e gratuitas (Open Source) que são padrão na indústria:

- **Nmap:** O "canivete suíço" para descoberta de rede e auditoria de segurança. Permite mapear hosts e serviços ativos.
- **Wireshark:** Analisador de protocolos que permite ver o que está acontecendo dentro do cabo em nível de bit.
- **OpenVAS:** Um scanner completo para detectar vulnerabilidades em sistemas.
- **Wi-Fi Analyzer:** Para diagnosticar interferências e segurança em redes sem fio (IEEE 802.11).

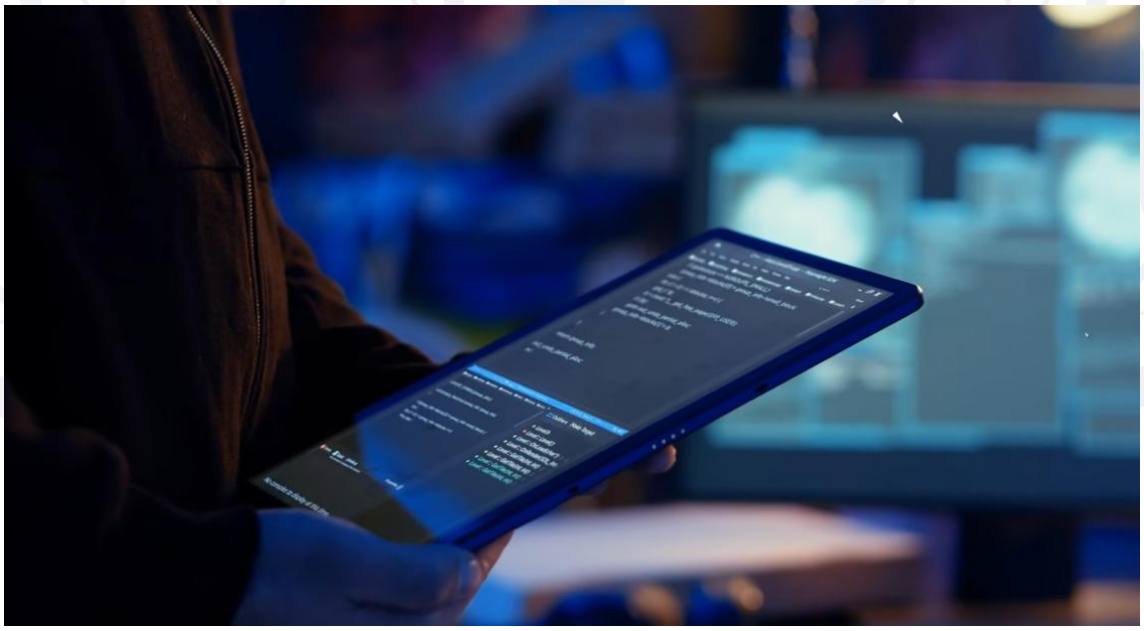
5.6. VPN (Virtual Private Network): O Túnel Seguro

Uma VPN é uma tecnologia que cria uma conexão segura e criptografada sobre uma rede menos segura, como a Internet pública. Ela permite que os dados trafeguem como se estivessem dentro de um "túnel" privado, invisível para atores mal-intencionados.



5.6.1. Como a VPN funciona?

O funcionamento de uma VPN pode ser resumido em um processo de três etapas que ocorre em milissegundos: **Tunelamento**, **Criptografia** e **Autenticação**.



https://www.youtube.com/watch?v=noMS5YizDeM

i. O Conceito de Tunelamento (Encapsulamento)

Imagine que a Internet é uma rodovia pública onde todos podem ver o que você carrega. A VPN cria um "túnel" dentro dessa rodovia.

- Tecnicamente, isso é feito através do **encapsulamento**: o pacote de dados original (com seu IP real e conteúdo) é colocado dentro de outro pacote de dados (com o IP do servidor VPN).
- Para os roteadores no meio do caminho, o pacote parece um tráfego comum indo para o servidor VPN, ocultando o destino final real.

ii. Criptografia de Ponta a Ponta

O túnel sozinho não basta; se alguém conseguir "furar" o túnel, não deve conseguir ler os dados. Por isso, a VPN utiliza algoritmos de criptografia (como o AES-256).

- Os dados são embaralhados na saída do seu dispositivo e só podem ser descriptografados quando chegam ao servidor VPN (ou no dispositivo de destino, em VPNs *Client-to-Client*).
- Isso garante o pilar da **Confidencialidade** da nossa Tríade CID.

iii. Protocolos de Comunicação

A "engrenagem" que controla o túnel e a criptografia é o protocolo. Os mais comuns no mercado atual são:

- **OpenVPN:** O padrão da indústria, equilibrando alta segurança e velocidade.
- **WireGuard:** Mais moderno e rápido, com menos linhas de código (fácil de auditar).
- **IPsec/L2TP:** Muito comum para conexões entre escritórios (Site-to-Site).

5.6.2. Tipos Comuns de VPN

- **Remote Access (Acesso Remoto):** Usada por funcionários em home office para acessar a rede da empresa com segurança.
- **Site-to-Site (Ponto a Ponto):** Conecta dois escritórios físicos (ex: filial e matriz) através da internet, fazendo com que pareçam estar na mesma rede local (LAN).

5.6.3. Protocolos de VPN

Nomes técnicos que garantem esse túnel:

- **IPsec (Internet Protocol Security):** Muito comum na camada de rede, oferece forte criptografia.
- **SSL/TLS:** Usado em VPNs baseadas em navegador (Web VPNs).
- **OpenVPN:** Um padrão de código aberto altamente seguro e versátil.

5.7. Laboratório Serverless

O Objetivo

Configurar um ambiente de nuvem onde o aluno não gerencia servidores (IaaS), mas consome o serviço de armazenamento como uma plataforma de entrega de conteúdo (PaaS/Serverless).

Arquitetura da Solução

Utilizaremos o **Amazon S3 (Simple Storage Service)**. Diferente de uma VM (EC2), o S3 é um serviço de objetos que possui uma funcionalidade nativa para servir arquivos web via HTTP.

Passo 1: Criação do Arquivo HTML

Crie um arquivo chamado index.html em suas máquinas com o código abaixo:

```
<!DOCTYPE html>
<html lang="pt-br">
<head>
    <meta charset="UTF-8">
    <title>Aula de Cloud - Oswaldo Cruz</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css"
rel="stylesheet">
</head>
<body class="bg-light">
    <div class="container mt-5">
        <div class="card shadow">
            <div class="card-body text-center">
                <h1 class="text-primary">Aplicação Serverless Ativa!</h1>
                <p class="lead">Hospedada com sucesso no Amazon S3.</p>
                <hr>
                <p>Aluno: <strong>[Nome do Aluno]</strong></p>
                <a href="https://oswaldocruz.br" target="_blank" class="btn btn-success">
Oswaldo Cruz - ADS</a>
            </div>
        </div>
    </div>
</body>
</html>
```

index.html

Passo 2: Configuração no Console AWS

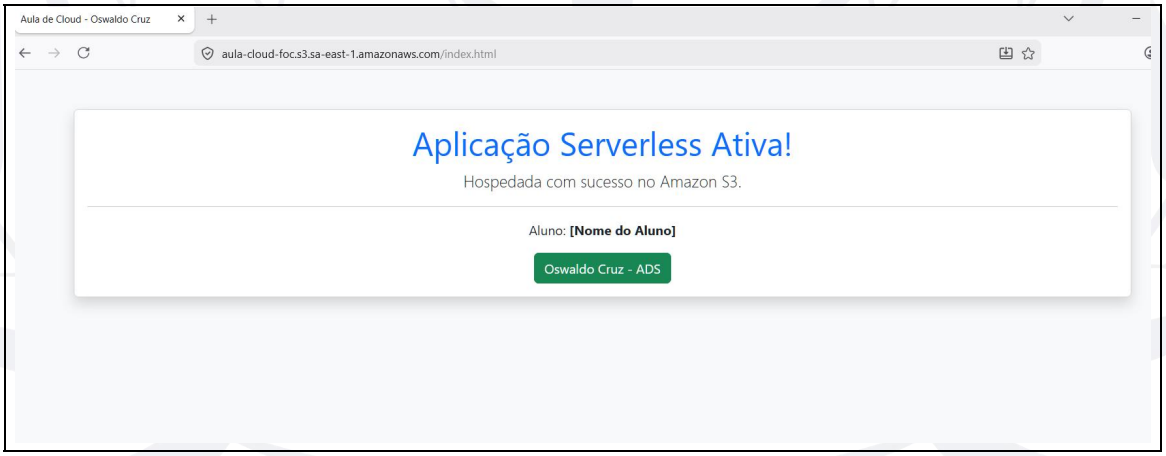
1. **Criar o Bucket:** O nome do bucket deve ser único globalmente (ex: aula-cloud-foc-2026).
2. **Desativar o Bloqueio de Acesso Público:** Para que a página seja acessível pela web, os alunos precisam desmarcar a opção "Block all public access.
3. **Habilitar Static Website Hosting:** Nas propriedades do bucket, ativar esta função e definir o documento de índice como index.html.

Passo 3: Política de Acesso (Bucket Policy)

Para que o S3 permita a leitura dos arquivos, é necessário colar esta política JSON na aba de Permissões:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::NOME-DO-SEU-BUCKET/*"
        }
    ]
}
```

Resultado Esperado



Pontos Importantes

1. **Escalabilidade:** "Se 1 milhão de pessoas acessarem essa página simultaneamente, o que acontece?" (Resposta: O S3 escala automaticamente sem precisarmos de Load Balancers).
2. **Custo:** "Qual a diferença de custo entre essa abordagem e manter uma Instância EC2 (VM) ligada 24/7?" (Resposta: No Serverless, pagamos apenas pelo armazenamento e tráfego; na VM, pagamos pelo tempo de processamento, mesmo ociosa).
3. **Segurança:** "Por que não usaríamos este método para hospedar um banco de dados?" (Resposta: O S3 é para arquivos estáticos; dados sensíveis e dinâmicos exigem camadas de segurança e processamento de backend como Lambda ou RDS).

5.8. Laboratório de Auditoria Wi-Fi: A Suíte Aircrack-ng (Detalhamento)

A auditoria de redes sem fio é um processo dividido em fases. O Aircrack-ng não é um "botão mágico", mas uma caixa de ferramentas que exige que o analista entenda o tráfego de frames 802.11.

Informações completas sobre o **Aircrack-ng** podem ser obitidas no site oficial: https://www.aircrack-ng.org/

Lab utilizando **Aircrack-ng** para descobrir senha **WEP, WAP e WAP2:** https://www.aircrack-ng.org/doku.php?id=aircrack-ng

Uma ferramenta muito útil para realizar a captura de pacotes transmitidos por uma interface wifi é o **Wireshark** (https://www.wireshark.org)

5.8.1 O 4-Way Handshake (Aperto de Mão de 4 Vias)

É o processo fundamental de segurança em redes Wi-Fi (WEP/WAP/WPA2/WPA3). Ele ocorre logo após o dispositivo se autenticar no roteador, mas antes de qualquer dado real começar a trafegar.

O grande objetivo deste processo é provar que tanto o cliente (celular/notebook) quanto o roteador conhecem a senha da rede, sem nunca enviá-la pelo ar, e gerar chaves temporárias para criptografar a sessão.

Os 4 Passos do Processo

Imagine que o roteador é o AP (Access Point) e o seu dispositivo é a Station (STA). Ambos já possuem a senha (PSK - Pre-Shared Key).

I. Mensagem 1 (M1): O Roteador inicia

O roteador envia um número aleatório chamado ANonce (Authenticator Nonce).

O que o cliente faz: Recebe o ANonce. Agora ele tem o ANonce, o seu próprio número aleatório (SNonce) e a senha da rede. Com isso, ele calcula uma chave única para essa sessão (PTK - Pairwise Transient Key).

II. Mensagem 2 (M2): O Cliente responde

O cliente envia o seu SNonce (Supplicant Nonce) para o roteador, junto com um código de integridade (MIC).

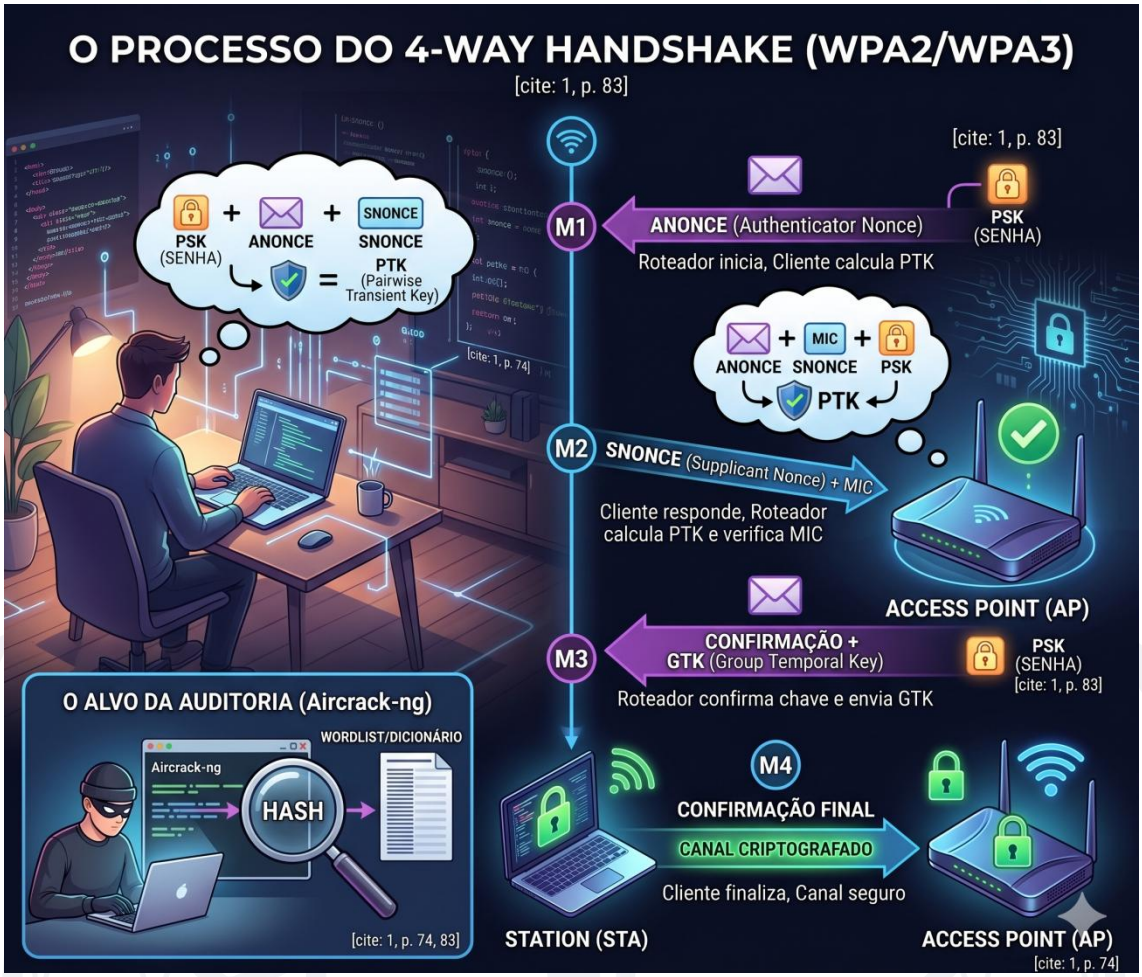
O que o roteador faz: Agora o roteador também tem tudo o que precisa (ANonce, SNonce e Senha) para calcular a mesma chave PTK. Ele verifica o MIC para garantir que o cliente usou a senha correta.

III. Mensagem 3 (M3): O Roteador confirma

O roteador envia uma confirmação ao cliente dizendo que a chave está correta. Ele também envia a GTK (Group Temporal Key), que é a chave usada para tráfego de transmissão geral (Broadcast) da rede.

IV. Mensagem 4 (M4): O Cliente finaliza

O cliente envia uma última confirmação informando que as chaves foram instaladas com sucesso. A partir deste milésimo de segundo, o canal está criptografado e o acesso à internet é liberado.



5.8.2. Fase 1: Preparação e Monitoramento (Reconhecimento)

Nesta fase, transformamos a placa de rede em um sensor passivo.

- **Comando airmon-ng start wlan0**: Este comando encerra processos que podem interferir na placa (como o NetworkManager) e ativa o **Modo Monitor**. A interface passa a se chamar, geralmente, wlan0mon.
- **Comando airodump-ng wlan0mon**: O analista começa a "ouvir" o ar. A tela exibirá:
  - **BSSID**: O endereço MAC do roteador (ponto de acesso).
  - **PWR**: A força do sinal (importante para saber a proximidade).
  - **CH**: O canal em que a rede opera (1 a 11/13).
  - **ENC**: O tipo de criptografia (WEP, WPA, WPA2).

5.8.4. Fase 2: Captura do Handshake (O Alvo)

Em redes WPA/WPA2, a senha não é transmitida. O que precisamos capturar é o **4-Way Handshake** — a troca de chaves que ocorre quando um dispositivo se conecta ao roteador.

- **Comando airodump-ng -c [canal] --bssid [MAC] -w [arquivo] wlan0mon**: Focamos a placa em um único canal e gravamos todos os dados dessa rede específica em um arquivo .cap.

3.8.5. Fase 3: Ataque de Desautenticação (Aceleração)

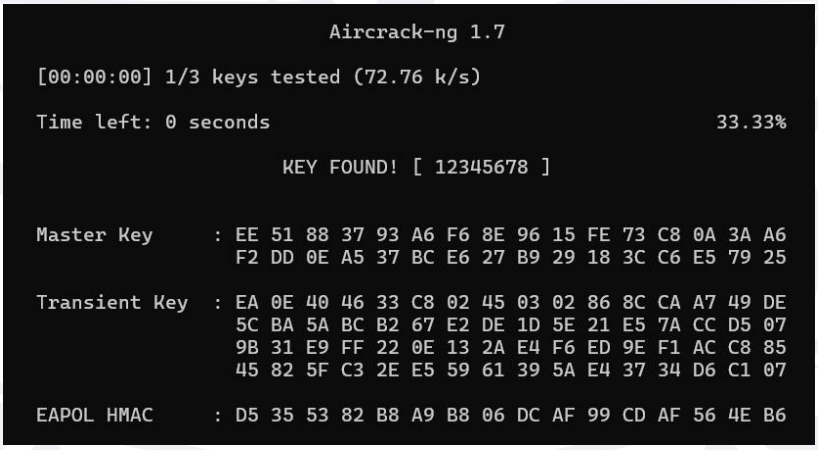
Se não houver ninguém se conectando no momento, o analista não capturará o handshake. Para forçar isso, usamos o **Aireplay-ng**.

- **Comando aireplay-ng -0 5 -a [MAC_Roteador] -c [MAC_Cliente] wlan0mon**: Este comando envia frames de desautenticação forjados. O cliente (celular ou notebook) cai da rede por um segundo e se reconecta automaticamente. Nesse milissegundo, o airodump-ng captura o handshake.

5.8.6. Fase 4: A Quebra (Cracking)

Com o arquivo de handshake em mãos, o trabalho agora é offline e depende do poder de processamento (CPU/GPU).

- **Comando aircrack-ng -w [dicionário.txt] arquivo.cap**: O software começa a testar cada palavra de uma lista (wordlist) contra o handshake capturado. Se a senha estiver na lista, ela é revelada em texto claro.
- Você deverá ver algo do tipo:



Exercícios de Fixação

1. Qual pilar da segurança é violado quando um ataque de Ransomware criptografa os arquivos de uma empresa e impede o acesso dos funcionários?

a) Confidencialidade

b) Integridade

c) Disponibilidade

d) Não-repúdio

2. De acordo com a legislação brasileira (Art. 154-A do Código Penal), a invasão de dispositivo informático só é crime se:

a) O computador for de marca famosa.

b) Houver violação de mecanismo de segurança (como senhas ou firewalls).

c) O invasor usar um sistema operacional Linux.

d) Ocorrer durante o horário comercial.

3. Qual ferramenta é ideal para capturar o tráfego de rede e analisar se as senhas de um sistema estão sendo enviadas sem criptografia (em texto claro)?

a) Nmap

b) Wireshark

c) DHCP Server

d) Google Chrome

4. O ataque de "Negação de Serviço Distribuído" (DDoS) tem como objetivo principal:

a) Roubar a senha do administrador.

b) Tornar um serviço ou servidor indisponível para os usuários legítimos através de sobrecarga.

c) Alterar o endereço IP do gateway padrão.

d) Aumentar a velocidade da fibra óptica.

5. Qual a diferença entre Latência e Jitter no contexto de Qualidade de Rede (QoS)?

a) Latência é o atraso; Jitter é a variação desse atraso.

b) Latência é a velocidade; Jitter é a cor do cabo.

c) São sinônimos para perda de pacotes.

d) Latência ocorre no Wi-Fi e Jitter no cabo Ethernet.

6. Qual é o principal benefício de utilizar uma VPN para um colaborador que trabalha em uma rede Wi-Fi pública (como a de uma cafeteria)?

a) Aumentar a velocidade física do download.

b) Criptografar o tráfego de dados, impedindo que outros usuários da rede interceptem suas senhas e informações.

c) Substituir a necessidade de ter um endereço IP.

d) Carregar a bateria do notebook via rede.

7. No contexto do Módulo 5, a VPN ajuda a garantir qual pilar da segurança da informação?

a) Apenas a disponibilidade.

b) A Confidencialidade e a Integridade dos dados em trânsito.

c) A cor dos cabos de fibra óptica.

d) O fim do uso de firewalls.

8. O processo de "Encapsulamento" em uma VPN consiste em:

a) Excluir o arquivo original para economizar espaço.

b) Colocar o pacote de dados original dentro de um novo pacote protegido para trânsito na rede pública.

c) Transformar o sinal digital em analógico.

d) Enviar o dado via satélite da Starlink obrigatoriamente.

9. Uma VPN "Site-to-Site" é mais indicada para:

a) Um usuário único acessar seu e-mail pessoal.

b) Interconectar duas redes de escritórios distantes de forma permanente e segura.

c) Baixar filmes de forma ilegal.

d) Testar a velocidade do PING entre dois computadores na mesma sala.

10. Qual protocolo é amplamente conhecido por ser a base de segurança nativa do IPv6 e também muito usado em VPNs?

a) HTTP

b) DHCP

c) IPsec

d) FTP

Exemplo Prático de Aplicação

Auditoria Preventiva

Em um projeto de infraestrutura, um Analista de Sistemas deve realizar varreduras periódicas com o **Nmap**. Se o analista descobre uma porta de banco de dados (ex: 3306) aberta diretamente para a Internet, ele identifica um risco crítico de segurança. A solução imediata seria configurar o **Firewall** para permitir conexões apenas de IPs autorizados, protegendo a integridade e confidencialidade dos dados da empresa antes que um ataque ocorra.

Mitigação de Riscos em Projetos ADS

Ao projetar a segurança de uma aplicação que rodará em tablets de vendedores, o Analista de Sistemas deve considerar que o Wi-Fi pode ser alvo dessas ferramentas. A solução não é apenas uma senha forte, mas a implementação de uma **VPN**. Mesmo que o invasor consiga quebrar a senha do Wi-Fi usando o Aircrack-ng, os dados da aplicação continuarão protegidos dentro do túnel criptografado da VPN, mantendo a integridade do negócio.

Módulo 6: Automação, Modernização e Operações Digitais

Este módulo foca na convergência entre o desenvolvimento de software e as operações de infraestrutura. Para um Analista de Sistemas, não basta saber como um pacote viaja na rede; é preciso saber como automatizar a criação de redes inteiras através de código e como gerenciar milhares de containers em ambientes de nuvem hyper-scale.

6.1. Infraestrutura como Código (IaC) e DevOps

A **Infraestrutura como Código (IaC)** é a prática de gerenciar e provisionar a infraestrutura de TI (redes, máquinas virtuais, balanceadores de carga) por meio de arquivos de definição legíveis por máquina, em vez de configurações físicas de hardware ou ferramentas de configuração interativas.

- **Cultura DevOps:** Trata-se da integração entre as equipes de Desenvolvimento (Dev) e Operações (Ops), focando na automação de processos para reduzir o *Time-to-Market*.
- **Valor Estratégico:** A IaC diminui o erro humano na configuração de Gateways e subredes. Se um ambiente da plataforma precisar ser replicado em outra região da AWS, o código garante que a nova infraestrutura seja idêntica à original.
- **Ferramentas de Mercado:** O **Terraform** e o **Ansible** são os padrões de mercado que permitem descrever a rede (VPC, IPs e Firewalls) como se fosse um software.

Como vimos, a IaC permite que a infraestrutura seja tratada com o mesmo rigor que o código de uma aplicação, incluindo controle de versão (Git) e testes automatizados.

Exemplo Prático: Provisionando uma Rede na AWS com Terraform

O código abaixo descreve a criação de uma **VPC** (Virtual Private Cloud), uma **Subrede** e uma **Instância EC2**.

```
# 1. Definindo o provedor (Nuvem Pública)
provider "aws" {
  region = "us-east-1" # Região da Virgínia
}

# 2. Criando a VPC (Rede Lógica Isolada)
resource "aws_vpc" "vpc_foc" {
  cidr_block = "10.0.0.0/16" # Classe A privada

  tags = {
    Name = "Rede-Principal"
  }
}
```

```
# 3. Criando uma Subrede para o Servidor Web
resource "aws_subnet" "subnet_web" {
  vpc_id     = aws_vpc.vpc_foc.id
  cidr_block = "10.0.1.0/24" # Subdivisão para 254 hosts

  tags = {
    Name = "Subnet-Publica-Web"
  }
}

# 4. Criando o Servidor Virtual (Instância EC2)
resource "aws_instance" "servidor_web" {
  ami           = "ami-0c55b159cbfafe1f0" # Imagem Ubuntu
  instance_type = "t2.micro"              # Instância gratuita
  subnet_id     = aws_subnet.subnet_web.id

  tags = {
    Name = "Servidor-PHP-App"
  }
}
```

Por que isso é revolucionário para o negócio?

- **Repetibilidade:** Se precisarmos de um ambiente idêntico para testes ou desastre, basta rodar o comando terraform apply e a rede inteira é recriada em segundos.
- **Documentação Viva:** O arquivo de código é a documentação exata da rede. Não há dúvida sobre qual IP ou Máscara de subrede foi configurada.
- **Agilidade:** O tempo gasto configurando Gateways e Tabelas de Roteamento manualmente cai drasticamente, permitindo que a equipe foque na qualidade do software.

6.2. Microsserviços e Containers (Docker & Kubernetes)

Diferente da virtualização clássica de máquinas virtuais (VMs), os containers permitem empacotar uma aplicação e todas as suas dependências em uma unidade leve que compartilha o mesmo núcleo (kernel) do sistema operacional.

- **Docker:** É a tecnologia que permite criar, implantar e executar aplicações em containers. Ele garante que o software funcione da mesma forma no computador do desenvolvedor e no servidor de produção na nuvem.
- **Redes no Docker:** Os containers utilizam drivers de rede (Bridge, Host, Overlay) para se comunicarem. Isso isola o tráfego de dados, aumentando a segurança e a governança.

- **Kubernetes (K8s):** É o orquestrador de containers. Ele gerencia a escalabilidade e a disponibilidade automática. Se um container falhar, o Kubernetes o reinicia instantaneamente (self-healing).

6.3. Redes Definidas por Software (SDN)

As **SDNs (Software Defined Networking)** representam uma mudança de paradigma: a inteligência da rede é movida do hardware (switches e roteadores físicos) para um controlador de software centralizado.

- **Plano de Controle vs. Plano de Dados:** No modelo tradicional, cada switch decide para onde enviar o dado. No SDN, um software central toma essa decisão, permitindo que a rede seja reconfigurada dinamicamente sem tocar nos cabos.
- **Agilidade em Cloud:** É a tecnologia base que permite à AWS ou Azure criar VPCs e subredes virtuais para milhões de clientes simultaneamente.

6.4. Conteúdo Prático de Observabilidade

A observabilidade vai além do simples monitoramento via PING ou comandos de terminal. Ela busca entender o estado interno do sistema através dos dados que ele gera.

- **Os Pilares da Observabilidade:**
  - **Logs:** Registros de eventos que ocorreram no sistema.
  - **Métricas:** Dados numéricos sobre o uso de CPU, memória e latência da rede (QoS).
  - **Tracing:** O rastreamento de uma requisição desde o navegador do usuário até o banco de dados na nuvem.
- **Ferramentas:** O uso de **Grafana** e **Prometheus** permite visualizar incidentes críticos em tempo real, reduzindo o MTTR (Tempo Médio de Reparo).

6.5. Segurança Avançada: DevSecOps

O **DevSecOps** integra a segurança em todas as etapas do ciclo de desenvolvimento, e não apenas no final do projeto.

- **Segurança na Camada de Aplicação:** Implementação de análise estática de código para evitar vulnerabilidades como Phishing e Injeção de dados.
- **Zero Trust:** Princípio de que nenhum dispositivo, mesmo dentro da rede local (LAN), é confiável por padrão.
- **Governança e LGPD:** Automação de políticas de conformidade para garantir a proteção de dados pessoais conforme a legislação brasileira.

Exercícios de Fixação

1. Qual o principal objetivo da Infraestrutura como Código (IaC)

a) Comprar mais cabos de fibra óptica.

b) Automatizar o provisionamento de recursos de rede e servidores via arquivos de configuração.

c) Substituir o uso de endereços IP por nomes analógicos.

d) Impedir que o desenvolvedor use a nuvem.

2. O que caracteriza o "Self-healing" em um orquestrador como o Kubernetes?

a) A capacidade de carregar a bateria do servidor via rede.

b) A reinicialização automática de containers que falharam para manter a disponibilidade.

c) O aumento físico da largura de banda passante.

d) A tradução automática de IPv4 para IPv6.

3. No modelo DevSecOps, quando a segurança deve ser aplicada?

a) Apenas quando ocorrer uma invasão ilegal de sistemas.

b) Somente após o software estar em produção.

c) De forma integrada e contínua em todo o ciclo de desenvolvimento e operação.

d) Apenas na camada física da rede (cabos e racks).

4. No laboratório prático de Docker, para que serve o comando de criação de rede (network create)?

a) Para conectar o computador diretamente a um satélite da Starlink.

b) Para criar um domínio de broadcast isolado onde os containers podem se comunicar com segurança.

c) Para mudar o endereço MAC da placa de rede física.

d) Para excluir o arquivo de handshake do Wi-Fi.

5. Qual a diferença entre monitoramento e observabilidade?

a) Nenhuma, são sinônimos para usar o comando PING.

b) Monitoramento foca no "se" o sistema está funcionando; Observabilidade foca no "porquê" ele está se comportando de certa forma através de logs, métricas e traces.

c) Monitoramento é para Linux e Observabilidade é para Windows

d) Observabilidade exige o uso de cabos coaxiais grossos.

Exemplo Prático de Aplicação: Escalabilidade da ISY.ONE

Ao utilizar Containers e SDN, a plataforma torna-se agnóstica à infraestrutura física. Se houver um pico de acessos, o controlador SDN aloca mais banda passante virtual, e o Kubernetes dispara novas instâncias da aplicação em containers. Todo esse processo ocorre sem intervenção manual, garantindo eficiência operacional.

PARTE 1: QUESTÕES DE MÚLTIPLA ESCOLHA

UNIDADE 1: INTRODUÇÃO ÀS REDES E CAMADA FÍSICA

Questão 1

A topologia física de uma rede de computadores define como os dispositivos estão conectados aos meios de transmissão, enquanto a topologia lógica descreve o fluxo de dados através dessa infraestrutura. Em uma rede configurada fisicamente em estrela, utilizando um switch centralizado, se um dos cabos UTP que conecta uma estação de trabalho ao switch for rompido, o impacto na rede será:

a) Toda a rede ficará indisponível devido à quebra do anel lógico.

b) Apenas a estação de trabalho cujo cabo foi rompido perderá a conectividade com a rede.

c) O switch redirecionará o tráfego daquela estação através de conexões de rádio vizinhas.

d) A rede continuará funcionando, mas a velocidade de transmissão de todos os outros nós cairá pela metade.

e) Ocorre o efeito de flooding contínuo, saturando a banda de toda a subrede.

Questão 2

Em ambientes industriais, a presença de grandes motores elétricos e geradores introduz altos níveis de Interferência Eletromagnética (EMI) e de Radiofrequência (RFI). Um Analista de Sistemas precisa projetar o cabeamento estruturado para conectar os sensores de uma linha de montagem ao data center local. Considerando as características dos meios de transmissão, assinale a alternativa que apresenta a solução tecnicamente mais adequada e imune a esse tipo de ruído:

a) Cabo de par trançado UTP Categoria 6.

b) Cabo de par trançado blindado STP Categoria 6A.

c) Cabo coaxial fino (10Base2).

d) Fibra óptica (seja monomodo ou multimodo).

e) Links sem fio operando na frequência de 2.4 GHz com criptografia WPA3.

Questão 3

Considere as seguintes asserções sobre os modos de transmissão de dados:

I. No modo Full-Duplex, a comunicação é bidirecional e síncrona, permitindo que ambos os dispositivos transmitam e recebam dados simultaneamente no mesmo canal físico.

PORQUE

II. O modo Half-Duplex utiliza canais físicos separados para a transmissão e para a recepção, eliminando a possibilidade de colisões de pacotes.

A respeito dessas asserções, assinale a opção correta:

a) As asserções I e II são proposições verdadeiras, e a II é uma justificativa correta da I.

b) As asserções I e II são proposições 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) Ambas as asserções I e II são proposições falsas.

Questão 4

O Modelo de Referência OSI (Open Systems Interconnection) da ISO divide a arquitetura de rede em sete camadas funcionais. Quando um dado é enviado de uma aplicação para outra, ele passa por um processo de encapsulamento. Associe as camadas do modelo OSI com suas respectivas unidades de dados (PDU):

1- Camada de Rede
2- Camada de Enlace
3- Camada de Transporte
4- Camada Física

( ) Quadro (Frame)
( ) Bit
( ) Pacote (Packet)
( ) Segmento (Segment)

A sequência correta de preenchimento dos parênteses é:
a) 2, 4, 1, 3
b) 1, 2, 3, 4
c) 3, 1, 4, 2
d) 2, 1, 4, 3
e) 4, 2, 1, 3

Questão 5

A atenuação é a perda de intensidade de um sinal à medida que ele se propaga através de um meio de transmissão. Para contornar as limitações físicas de distância impostas pela atenuação em cabos de par trançado UTP (limite nominal de 100 metros), engenheiros de redes devem utilizar na Camada Física:
a) Switches de camada 3 operando em modo promíscuo.
b) Repetidores ou hubs para regenerar o sinal elétrico.
c) Modulação em amplitude (AM) para aumentar a frequência do sinal.
d) Pontes (Bridges) baseadas em tabelas de roteamento dinâmico.
e) Protocolos de controle de fluxo baseados em janela deslizante.

Questão 6

Um engenheiro de telecomunicações precisa interligar dois data centers separados por uma distância de 15 quilômetros sem a possibilidade de instalação de repetidores

intermediários. Qual tipo de meio de transmissão atende às exigências de distância, largura de banda e atenuação mínima?
a) Cabo de par trançado UTP Categoria 8.
b) Cabo de par trançado blindado S/FTP Categoria 7.
c) Fibra óptica multimodo (MMF).
d) Fibra óptica monomodo (SMF).
e) Link de rádio micro-ondas operando na banda de 5 GHz.

Questão 7

A arquitetura de redes TCP/IP é a base da internet moderna. Diferente do modelo OSI, o modelo TCP/IP consolidou funções em menos camadas. As funções de criptografia, compressão de dados e formatação de caracteres, que no modelo OSI pertencem à Camada de Apresentação, no modelo TCP/IP são executadas na camada de:
a) Interface de Rede.
b) Internet.
c) Transporte.
d) Aplicação.
e) Sessão.

Questão 8

Na topologia lógica em Barramento (Bus), o meio de transmissão é compartilhado entre todos os nós. Para evitar que os sinais elétricos sofram reflexão e causem interferência destrutiva ao atingirem as extremidades físicas do cabo, é obrigatória a instalação de:
a) Transceivers ativos em cada interface de rede.
b) Conectores RJ-45 blindados com aterramento de carcaça.
c) Terminadores resistivos (terminadores de 50 ohms) nas pontas do barramento.
d) Concentradores do tipo Hub passivo.
e) Filtros passa-baixas em cada nó conectado.

Questão 9

A multiplexação é uma técnica que permite a transmissão simultânea de múltiplos sinais lógicos através de um único canal físico. Quando a banda passante do meio excede a largura de banda necessária dos sinais a serem transmitidos, e dividimos o meio em faixas de frequências distintas para cada canal, estamos utilizando a multiplexação por:
a) Divisão de Tempo (TDM).
b) Divisão de Frequência (FDM).
c) Divisão de Código (CDMA).
d) Divisão de Comprimento de Onda Denso (DWDM).
e) Pacotes Criptografados (SDM).

Questão 10

Durante uma auditoria na infraestrutura de rede de uma faculdade, constatou-se que cabos UTP de dados foram passados dentro das mesmas calhas elétricas que alimentam

as lâmpadas e tomadas de alta tensão do prédio. Os usuários reclamavam de quedas intermitentes na conexão. Esse fenômeno é conhecido tecnicamente como:
a) Atenuação por dispersão cromática.
b) Jitter induzido por atraso de propagação.
c) Diafonia (Crosstalk) por acoplamento eletromagnético externo.
d) Colisão de pacotes na camada física.
e) Latência assimétrica de enlace.

UNIDADE 2: ARQUITETURAS DE REDES E CAMADA DE ENLACE

Questão 11

O protocolo Ethernet utiliza o mecanismo CSMA/CD (Carrier Sense Multiple Access with Collision Detection) para gerenciar o acesso ao meio compartilhado em redes Half-Duplex. Quando duas estações transmitem simultaneamente e ocorre uma colisão, o algoritmo implementado para determinar o tempo de espera antes da retransmissão é o:
a) Algoritmo de Dijkstra.
b) Algoritmo de Vetor de Distância.
c) Algoritmo de Alocação de Janela Deslizante.
d) Algoritmo de Recuo Binário Exponencial (Binary Exponential Backoff).
e) Algoritmo Token Passing.

Questão 12

Um Analista de Sistemas está substituindo os antigos hubs de uma rede local por switches gerenciáveis de Camada 2. Essa alteração na infraestrutura impactará diretamente a topologia lógica e os domínios da rede. Com a introdução do switch, a rede passará a ter:
a) Um único grande domínio de colisão e múltiplos domínios de broadcast.
b) Múltiplos domínios de colisão (um por porta) e um único grande domínio de broadcast (caso não haja VLANs).
c) Um único domínio de colisão e um único domínio de broadcast.
d) A eliminação completa tanto dos domínios de colisão quanto dos domínios de broadcast.
e) Múltiplos domínios de colisão e múltiplos domínios de broadcast automáticos por dispositivo conectado.

Questão 13

A tabela CAM (Content Addressable Memory), também conhecida como tabela de endereços MAC, é o componente que confere inteligência ao Switch de Camada 2. Quando o switch recebe um quadro cujo endereço MAC de destino não está registrado em sua tabela CAM, o comportamento padrão do ativo é:
a) Descartar o quadro imediatamente e enviar uma mensagem ICMP de erro à origem.
b) Armazenar o quadro em cache até que a estação de destino envie uma requisição ARP.
c) Encaminhar o quadro exclusivamente para o Gateway Padrão da rede.

d) Realizar o flooding, ou seja, retransmitir o quadro por todas as portas ativas, exceto pela porta de origem.
e) Alterar o endereço MAC de destino para o endereço de broadcast (FF:FF:FF:FF:FF:FF).

Questão 14

Analise a estrutura de um quadro (frame) Ethernet padrão e assinale a alternativa que descreve corretamente a função do campo FCS (Frame Check Sequence):
a) Ele sincroniza o relógio (clock) entre os dispositivos transmissores e receptores.
b) Ele especifica qual protocolo de Camada Superior (Rede) deve receber os dados decapsulados.
c) Ele contém o algoritmo de CRC (Cyclic Redundancy Check) usado para detectar se houve corrupção de bits durante o trânsito.
d) Ele define o endereço físico exclusivo da interface de rede de destino.
e) Ele controla o tamanho da janela de transmissão para evitar o transbordo de buffers no receptor.

Questão 15

Considere o seguinte cenário: Em uma rede local, o Switch A está conectado ao Switch B por meio de dois cabos físicos simultâneos para criar redundância. No entanto, nenhum dos switches possui o protocolo STP (Spanning Tree Protocol) ativado. Esse cenário resultará em um problema crítico de Camada de Enlace conhecido como:
a) Conflito de Endereçamento IP Dinâmico.
b) Tempestade de Broadcast (Broadcast Storm) devido a loops na rede.
c) Saturação de Janela TCP.
d) Fragmentação Excessiva de Pacotes.
e) Envenenamento de Tabela ARP (ARP Spoofing).

Questão 16

O endereço MAC (Media Access Control) é um identificador físico composto por 48 bits, gravado na memória ROM da placa de rede. Sobre a sua estrutura, é correto afirmar que:
a) Os primeiros 24 bits representam o endereço lógico da subrede IP à qual a placa pertence.
b) Os 48 bits são gerados aleatoriamente pelo sistema operacional a cada inicialização da máquina.
c) Os primeiros 24 bits representam o OUI (Organization Unique Identifier), identificando o fabricante do hardware.
d) Ele é utilizado pelo protocolo de roteamento OSPF para determinar o menor caminho físico.
e) É composto por 6 blocos hexadecimais que mapeiam geograficamente a localização do nó.

Questão 17

O protocolo ARP (Address Resolution Protocol) desempenha um papel vital na pilha TCP/IP, agindo na fronteira entre as camadas de Rede e Enlace. A função primordial do ARP é:

a) Traduzir um nome de domínio (FQDN) em um endereço IP válido.
b) Mapear um endereço IP conhecido em seu respectivo endereço físico MAC.
c) Atribuir dinamicamente configurações de rede aos hosts clientes.
d) Encapsular pacotes IP dentro de túneis criptografados de VPN.
e) Garantir a entrega sequencial de quadros corrompidos.

Questão 18

Em redes sem fio organizadas sob o padrão IEEE 802.11 (Wi-Fi), as colisões não podem ser detectadas diretamente pelo hardware de rádio enquanto ele transmite. Por esse motivo, em vez do CSMA/CD da rede cabeada, o Wi-Fi utiliza o mecanismo:

a) CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) associado a quadros RTS/CTS.
b) Token Ring dinâmico baseado em prioridades de rádio.
c) Polling centralizado controlado pelo Ponto de Acesso (AP).
d) Multiplexação por divisão de espaço assíncrona.
e) Controle de Erros por Retransmissão Seletiva Automática.

Questão 19

Uma VLAN (Virtual Local Area Network) baseada no padrão IEEE 802.1Q introduz uma tag de identificação de 4 bytes no quadro Ethernet. A principal vantagem técnica da implementação de VLANs em uma infraestrutura de switches corporativa é:

a) Aumentar a velocidade física das portas de 1 Gbps para 10 Gbps via software.
b) Segmentar logicamente a rede local, reduzindo o tamanho dos domínios de broadcast e aumentando a segurança.
c) Permitir que o switch funcione sem a necessidade de um roteador para interligar redes externas.
d) Criptografar todo o tráfego da camada de enlace de ponta a ponta.
e) Eliminar a necessidade de endereçamento MAC nas estações.

Questão 20

A comutação de quadros em um switch pode ocorrer de diferentes formas. Quando o switch lê apenas os primeiros 14 bytes do quadro (os endereços MAC de destino, origem e o campo EtherType) e imediatamente começa a encaminhar o quadro para a porta de destino, sem realizar qualquer validação de erro para reduzir a latência ao mínimo, ele está operando no modo:

a) Store-and-Forward.
b) Fragment-Free.
c) Cut-Through.
d) Adaptive Switching.
e) Symmetric Switching.

UNIDADE 3: CAMADAS DE REDE, TRANSPORTE E PROTOCOLOS IP

Questão 21

Um Analista de Sistemas precisa configurar os parâmetros de rede de um servidor. Ele recebeu o endereço IP 192.168.100.14 com a máscara de subrede 255.255.255.240 (/28). Com base nessas configurações, assinale a alternativa que apresenta, respectivamente, o Endereço de Rede e o Endereço de Broadcast dessa subrede específica:

a) 192.168.100.0 e 192.168.100.15
b) 192.168.100.0 e 192.168.100.255
c) 192.168.100.14 e 192.168.100.15
d) 192.168.100.0 e 192.168.100.31
e) 192.168.100.0 e 192.168.100.14

Questão 22

A exaustão dos endereços IPv4 levou ao desenvolvimento de soluções paliativas, como o NAT (Network Address Translation), e à criação do IPv6. Sobre a estrutura e funcionamento do IPv6, analise as afirmativas a seguir:

I. O IPv6 utiliza endereços de 128 bits, representados em notação hexadecimal separada por dois-pontos.
II. O protocolo IPv6 elimina a necessidade do tráfego de Broadcast tradicional, substituindo-o por transmissões otimizadas de Multicast e Anycast.
III. O cabeamento físico da rede deve ser trocado obrigatoriamente para suportar o protocolo IPv6.
IV. O campo Hop Limit do cabeçalho IPv6 substitui a função do campo TTL (Time to Live) do IPv4.

É correto apenas o que se afirma em:

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

Questão 23

O protocolo TCP (Transmission Control Protocol) é um protocolo da Camada de Transporte orientado à conexão e que garante a entrega confiável de dados. O processo de estabelecimento de conexão conexa utilizado pelo TCP para sincronizar os números de sequência entre o cliente e o servidor é conhecido como:

a) Sliding Window.
b) Slow Start.
c) Three-Way Handshake (SYN, SYN-ACK, ACK).
d) Connection Flooding.
e) Quatro-Way Tear Down.

Questão 24

Diferente do TCP, o protocolo UDP (User Datagram Protocol) é um protocolo não orientado à conexão e não confiável (unreliable). Apesar de não garantir a entrega dos segmentos, o UDP é amplamente utilizado em aplicações de:

a) Transferência de arquivos via FTP e acesso a páginas Web seguras via HTTPS.

b) Sincronização de Bancos de Dados Relacionais estruturados.

c) Streaming de áudio/vídeo em tempo real (VoIP) e consultas ao sistema DNS, onde a baixa latência é prioritária.

d) Envio de e-mails corporativos via SMTP.

e) Gerenciamento e conexões remotas seguras via SSH.

Questão 25

O protocolo ICMP (Internet Control Message Protocol) opera na Camada de Rede corporativa e é utilizado para fornecer relatórios de erros e informações operacionais sobre o processamento de pacotes IP. Quando executamos o comando ping no terminal para testar a conectividade com um servidor, os dois tipos de mensagens ICMP trocadas são:

a) SYN e ACK.

b) Echo Request e Echo Reply.

c) Destination Unreachable e Time Exceeded.

d) Source Quench e Redirect.

e) Router Solicitation e Router Advertisement.

Questão 26

O cabeçalho do pacote IPv4 possui um campo chamado TTL (Time to Live), representado por um valor inteiro de 8 bits. A função técnica crucial do campo TTL durante o roteamento de pacotes na internet é:

a) Medir a velocidade de transmissão em megabits por segundo de ponta a ponta.

b) Definir o tempo em segundos que o pacote pode ficar armazenado no buffer do receptor.

c) Evitar loops infinitos de roteamento, fazendo com que o pacote seja descartado quando o valor chegar a zero.

d) Criptografar a carga útil do pacote caso ele passe por roteadores públicos.

e) Identificar a prioridade de QoS (Quality of Service) do pacote.

Questão 27

Uma empresa recebeu a faixa IP de rede privada 172.16.0.0/16. O administrador de sistemas precisa subdividir essa rede para acomodar 8 departamentos diferentes, maximizando o número de hosts disponíveis por subrede. Qual máscara de subrede atende perfeitamente a esse requisito?

a) 255.255.128.0 (/17)

b) 255.255.240.0 (/20)

c) 255.255.224.0 (/19)

d) 255.255.255.0 (/24)
e) 255.255.255.240 (/28)

Questão 28

Os roteadores utilizam tabelas de roteamento para tomar decisões de encaminhamento de pacotes na Camada de Rede. Quando um roteador recebe um pacote cujo endereço IP de destino não corresponde a nenhuma rota específica contida em sua tabela de roteamento, ele encaminha o pacote para a:
a) Interface de Loopback (127.0.0.1).
b) Rota Padrão (Default Route ou Rota 0.0.0.0/0).
c) subrede de Broadcast local.
d) Porta de gerência física do switch vizinho.
e) Lista de descarte de pacotes órfãos (Null0) sem notificação.

Questão 29

Em uma arquitetura cliente-servidor que utiliza a pilha de protocolos TCP/IP, a combinação exclusiva de um Endereço IP e de um Número de Porta de Camada de Transporte é denominada tecnicamente como:
a) Endereço FQDN.
b) Socket.
c) Registro DNS Tipo A.
d) Vetor de Inicialização (IV).
e) Payload Segmentado.

Questão 30

O protocolo DHCP (Dynamic Host Configuration Protocol) automatiza a atribuição de parâmetros de rede para os hosts clientes. O processo de negociação do DHCP ocorre por meio de quatro etapas sequenciais. Assinale a alternativa que apresenta a ordem correta dessas etapas:
a) Request, Discover, Offer, Acknowledge.
b) Discover, Offer, Request, Acknowledge (DORA).
c) Offer, Discover, Acknowledge, Request.
d) SYN, SYN-ACK, ACK, FIN.
e) Solicitation, Advertisement, Request, Reply.

UNIDADE 4: CLOUD COMPUTING E INFRAESTRUTURA EM NUVEM

Questão 31

O NIST (National Institute of Standards and Technology) define Cloud Computing por meio de cinco características essenciais, três modelos de serviço e quatro modelos de implantação. Assinale a alternativa que apresenta exclusivamente um Modelo de Serviço de Computação em Nuvem:
a) Nuvem Híbrida, Nuvem Pública, Nuvem Privada.
b) Autosserviço sob demanda, Acesso amplo à rede, Elasticidade rápida.

c) IaaS (Infraestrutura como Serviço), PaaS (Plataforma como Serviço), SaaS (Software como Serviço).
d) Virtualização de Hardware, Containers Docker, Servidores Bare-Metal.
e) Edge Computing, Serverless, Microserviços.

Questão 32

A plataforma SaaS (Software como Serviço) ISY.ONE, desenvolvida pela Quantum Products, oferece aos seus clientes pequenas e médias empresas um sistema de gestão completo acessível diretamente via navegador Web, eliminando a necessidade de os clientes instalarem ou gerenciarem infraestruturas locais. Com base no modelo de responsabilidade compartilhada da computação em nuvem, a gestão do sistema operacional, do hardware físico do servidor e da segurança física do data center onde o ISY.ONE está hospedado é de responsabilidade exclusiva:
a) Do cliente final que contrata o software.
b) Da equipa de desenvolvimento front-end do cliente.
c) Do provedor de nuvem subjacente (como AWS, Azure ou GCP) e da Quantum Products como provedora do software.
d) Do administrador de rede local da PME cliente.
e) Do consórcio internacional de governança da internet.

Questão 33

Considere as seguintes asserções sobre os modelos de implantação de nuvem:
I. Uma Nuvem Híbrida permite que uma organização mantenha sistemas legados e dados altamente confidenciais em uma Nuvem Privada local (on-premises), enquanto escala cargas de trabalho sazonais ou públicas utilizando recursos de uma Nuvem Pública.
PORQUE
II. Na arquitetura de Nuvem Híbrida, os dados e aplicações das duas nuvens independentes são integrados de forma segura por meio de tecnologias como VPNs ou links dedicados, permitindo a portabilidade de dados.

A respeito dessas asserções, assinale a opção correta:
a) As asserções I e II são proposições verdadeiras, e a II é uma justificativa correta da I.
b) As asserções I e II são proposições 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) Ambas as asserções I e II são proposições falsas.

Questão 34

No modelo de Infraestrutura como Serviço (IaaS), o cliente aluga recursos de computação como máquinas virtuais, armazenamento e redes. A tecnologia de software que atua diretamente sobre o hardware físico do servidor do provedor de nuvem, permitindo a abstração, o isolamento e a execução de múltiplos Sistemas

Operacionais convidados (Guest OS) de forma simultânea na mesma máquina física, é chamada de:
a) Kernel Espelhado.
b) Docker Engine.
c) Hypervisor (ou VMM - Virtual Machine Monitor).
d) Kubernetes Orchestrator.
e) Load Balancer Dinâmico.

Questão 35

O desenvolvimento moderno de aplicações em nuvem utiliza amplamente a tecnologia de Containers (como o Docker) em substituição ou complemento às Máquinas Virtuais (VMs) tradicionais. A principal diferença técnica estrutural entre um Container e uma VM reside no fato de que o Container:
a) Requer um Sistema Operacional completo e um Hypervisor dedicados para cada instância executada.
b) Não emula o hardware físico, mas virtualiza o Sistema Operacional no nível do Kernel, compartilhando o Kernel do sistema operacional hospedeiro.
c) É mais pesado e consome mais memória RAM que uma VM convencional.
d) Só pode ser executado em servidores locais (on-premises), sendo incompatível com nuvens públicas.
e) Dispensa o uso de isolamento de processos e de namespaces de segurança.

Questão 36

A computação Serverless (Arquitetura Sem Servidor), exemplificada por serviços como o AWS Lambda, representa uma evolução nos modelos de nuvem. Sobre as características do Serverless, assinale a alternativa correta:
a) Significa que a aplicação roda diretamente no navegador do usuário, sem a existência de servidores em nenhuma parte do processo.
b) O desenvolvedor precisa provisionar, atualizar patches e gerenciar a capacidade de escalabilidade de instâncias de servidores virtuais continuamente.
c) O modelo de cobrança é baseado no tempo de execução do código e na quantidade de requisições processadas, permitindo reduzir o custo a zero quando a aplicação está ociosa.
d) É uma tecnologia indicada exclusivamente para processamentos monolíticos de longa duração e bancos de dados pesados.
e) Elimina completamente o pilar da disponibilidade da tríade de segurança da informação.

Questão 37

Uma grande empresa de comércio eletrônico hospeda sua aplicação na nuvem pública. Durante a Black Friday, o volume de requisições aumenta em 500% em poucos minutos. O mecanismo automatizado da nuvem que detecta o aumento no uso de CPU e adiciona novas instâncias de servidores virtuais dinamicamente para manter a

performance da aplicação, e depois as remove quando o tráfego normaliza, é chamado de:
a) Armazenamento de Objetos Estáticos.
b) Redundância de Zona de Disponibilidade.
c) Auto Scaling associado a um Load Balancer.
d) Migração de Dados Forense.
e) Roteamento Estático de Borda.

Questão 38

O armazenamento em nuvem pode ser categorizado em diferentes tipos. Quando precisamos armazenar trilhões de arquivos de dados não estruturados, como imagens de produtos, PDFs de notas fiscais e arquivos de log, utilizando uma estrutura plana (sem hierarquia de pastas) onde cada arquivo é acessado por uma URL exclusiva e possui metadados customizados, estamos utilizando o:
a) Armazenamento em Bloco (Block Storage).
b) Armazenamento de Arquivos (File Storage / NAS).
c) Armazenamento de Objetos (Object Storage, ex: Amazon S3).
d) Banco de Dados Relacional Indexado.
e) Cache de Memória Volátil.

Questão 39

As Nuvens Públicas distribuem seus data centers globalmente para mitigar desastres e reduzir latências. Na terminologia dos grandes provedores de nuvem (como AWS), uma localização geográfica totalmente independente que contém um ou mais data centers físicos discretos, equipados com energia, refrigeração e redes redundantes, é denominada:
a) Ponto de Presença (PoP).
b) Região (Region), subdividida em Zonas de Disponibilidade (AZs).
c) Data Center Bare-Metal Central.
d) Cluster de Containerização Local.
e) subrede de Borda Virtual.

Questão 40

Ao migrar uma aplicação web tradicional de um ambiente local para uma arquitetura nativa em nuvem, o arquiteto de software decide utilizar um serviço de banco de dados gerenciado (como o Amazon RDS). Essa escolha caracteriza-se como um modelo de serviço do tipo:
a) IaaS, pois o cliente ainda precisa instalar o banco de dados e gerenciar as licenças.
b) SaaS, pois o usuário final consome a interface de banco de dados sem permissão de escrita.
c) PaaS, pois a plataforma gerencia o sistema operacional, atualizações de patches e backups, deixando para o cliente apenas o gerenciamento dos dados e tabelas.
d) On-premises distribuído por contêineres locais.
e) CaaS (Container as a Service) privado e síncrono.

PARTE 2: QUESTÕES DISCURSIVAS (41 a 44)

Questão 41: Camada Física e de Enlace (Unidade 1 e 2)

Cenário: Uma instituição de ensino expandiu suas instalações instalando laboratórios de informática em dois blocos de prédios diferentes, separados por uma distância de 250 metros em uma área aberta. O técnico de rede iniciante tentou interligar os switches centrais dos dois prédios utilizando um cabo de par trançado UTP Categoria 6 padrão. Após a instalação física, constatou-se que a comunicação entre os prédios não funcionava, apresentando perda total de pacotes.

Com base nos conceitos de meios de transmissão e limites físicos das tecnologias de rede abordados nas Unidades 1 e 2, responda:

1 - Explique o motivo técnico do fracasso da conexão utilizando o cabo UTP Categoria 6 nessa distância.

2 - Apresente a solução de cabeamento físico ideal para interligar os dois blocos de prédios, justificando sua escolha técnica com base em pelo menos dois fatores (ex: atenuação, interferência ou largura de banda).

Questão 42: Endereçamento IPv4 e Roteamento (Unidade 3)

Cenário: Uma empresa recebeu a faixa de endereços IPv4 privados 192.168.50.0/24. O CIO da empresa determinou que essa rede deve ser dividida estritamente em 4 subredes lógicas de tamanhos iguais para isolar o tráfego dos seguintes setores: Desenvolvimento (setor do sistema ISY.ONE), Comercial, Diretoria e Suporte Técnico.

Considerando as regras de subredes baseadas na notação CIDR (Classless Inter-Domain Routing) da Unidade 3, execute as seguintes tarefas:

1 - Determine o número total de hosts úteis (endereços válidos para atribuição a computadores) que cada uma das 4 subredes poderá comportar.

2 - Demonstre o intervalo completo da primeira subrede criada, especificando o seu Endereço de Rede, o intervalo de IPs Úteis e o seu Endereço de Broadcast.

Questão 43: Modelos de Serviço em Nuvem e Arquitetura SaaS (Unidade 4)

Cenário: Uma plataforma SaaS (Software como Serviço) que roda em nuvem pública. Durante uma reunião de planejamento com investidores, foi discutida a possibilidade de reescrever partes do sistema que sofrem picos de acesso imprevisíveis utilizando uma arquitetura Serverless (Funções como Serviço - FaaS), em substituição às máquinas virtuais (IaaS) que ficam ligadas continuamente.

Com base nos conceitos de Cloud Computing e arquiteturas de nuvem detalhados na Unidade 4, responda:

1 - Explique a diferença de responsabilidade de gerenciamento de infraestrutura entre o modelo de Máquinas Virtuais tradicionais (IaaS) e o modelo Serverless (FaaS).

2 - Justifique o benefício financeiro e operacional que a migração para a arquitetura Serverless trará diante do cenário de acessos imprevisíveis mencionado.

Questão 44: Segurança, Ética e Análise Forense de Redes (Unidade 5)

Cenário: Durante uma auditoria interna na rede corporativa da empresa, o Analista de Segurança descobriu um arquivo com a extensão .cap salvo no servidor local. Ao abrir o arquivo em uma ferramenta de análise de pacotes (como o Wireshark) e aplicar o filtro para o protocolo eapol, o analista visualizou a captura completa das quatro mensagens (M1, M2, M3 e M4) que compõem o processo conhecido como 4-Way Handshake de uma rede sem fio protegida por WPA2.

Com base nos conceitos de segurança, ferramentas de auditoria (Suíte Aircrack-ng) e ética profissional discutidos na Unidade 5, responda:

1 - Explique o que representa o processo de 4-Way Handshake e qual a utilidade técnica do arquivo .cap que foi encontrado pelo analista.

2 - Discorra sobre o comportamento ético e legal esperado desse profissional de segurança após a descoberta dessa vulnerabilidade (captura de handshake), contrapondo-o com uma atitude considerada antiética ou criminosa segundo as boas práticas de "Hacking" Ético.

Bibliografia Básica

BRANCO, Luiz Henrique Castelo; GURGEL, Paulo Henrique Moreira. Redes de computadores: da teoria a prática com Netkit. Rio de Janeiro: Elsevier, 2014.
FERREIRA, Miguel A. Introdução ao Cloud Computing. IaaS, PaaS, SaaS, Tecnologia, Conceito e Modelos de Negócio. São Paulo: FCA, 2015.
MOLINARI, Leonardo. Cloud Computing. Inteligência da Nuvem e Seu Novo Valor em TI. São Paulo: Érica, 2017.

Bibliografia Complementar:

COULOURIS, G.; ç, J.; KINDBERG, T. Sistemas distribuídos: conceitos e projeto. São Paulo: Bookman, 2013.
FLYNN, Ida M.; MCHOES, Ann McIver. Introdução aos sistemas operacionais. São Paulo: Pioneira, 2002.
OLIVEIRA, Romulo Silva de; TOSCANI, Simão Sirineo; CARRISIMI, Alexandre da Silva. Sistemas operacionais. Porto Alegre: Bookman, 2010. (11. Livros Didáticos Informática).
STALLINGS, W. Arquitetura e organização de computadores. São Paulo: Pearson Prentice Hall, 2010.
TANENBAUM, Andrew S. Sistemas operacionais modernos. Rio de Janeiro: Prentice Hall, 2010.

Periódicos Científicos:

Advances in Software Engineering - ISSN 1687-8655
Computación y Sistemas - ISSN 1405-5546
Computational & Applied Mathematics - ISSN 1807-0302
Journal of the Brazilian Computer Society - ISSN 0104-6500