Estratégia Concursos

Aula 00

Informática p/ PC-SP (Polícia Científica - Perito Criminal e Médico Legista) - 2021 Pré-Edital

Autor:
Diego Carvalho, Equipe Informática e TI, Renato da Costa

05 de Fevereiro de 2021

Índice

1) Redes de Computadores - Parte 1 3

2) Redes de Computadores - Parte 1 - Glossário 67

3) Questões Comentadas - Redes de Computadores - Parte 1 - Vunesp 71

4) Lista de Questões - Redes de Computadores - Parte 1 - Vunesp 78

REDES DE COMPUTADORES

Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Vamos iniciar pela definição de redes de computadores:

> *"Uma rede é um conjunto de terminais, equipamentos, meios de transmissão e comutação que interligados possibilitam a prestação de serviços".*

Bem, eu gosto de uma definição mais simples que afirma que uma rede é um conjunto de dispositivos (normalmente conhecidos como nós) conectados por links de comunicação. Em uma rede, um nó pode ser um computador, uma impressora, um notebook, um *smartphone*, um *tablet*, um *Apple Watch* ou qualquer outro dispositivo de envio ou recepção de dados, desde que ele esteja conectado a outros nós da rede.

As primeiras redes de computadores surgiram dentro de organizações – como uma empresa ou um laboratório de pesquisa – para facilitar a troca de informações entre diferentes pessoas e computadores. **Esse método era mais rápido e confiável do que o anterior, que consistia em pessoas carregando pilhas e pilhas de cartões perfurados ou fitas magnéticas de um lado para o outro dentro de uma organiazação**.

Um segundo benefício das redes de computadores é a capacidade de compartilhar recursos físicos. Por exemplo: em vez de cada computador possuir sua própria impressora, todos em um departamento poderiam compartilhar apenas uma impressora conectada à rede de computadores. Outro uso comum era compartilhar dispositivos de armazenamento, que na época eram muito caros e não era viável ter um para cada computador.

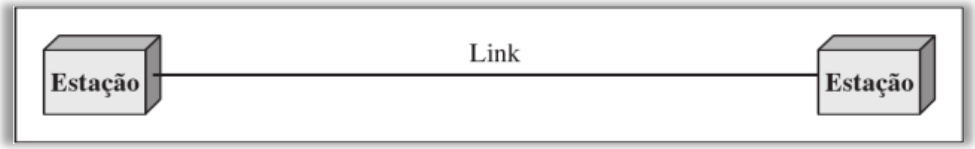
Como nós podemos resumir tudo isso? **Bem, uma rede de computadores basicamente tem como objetivo o compartilhamento de recursos, deixando equipamentos, programas e principalmente dados ao alcance de múltiplos usuários**, sem falar na possibilidade de servir como meio de comunicação entre pessoas através da troca de mensagens de texto, áudio ou vídeo entre os dispositivos. *Fechado?*

Tipos de Conexão/Enlace

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

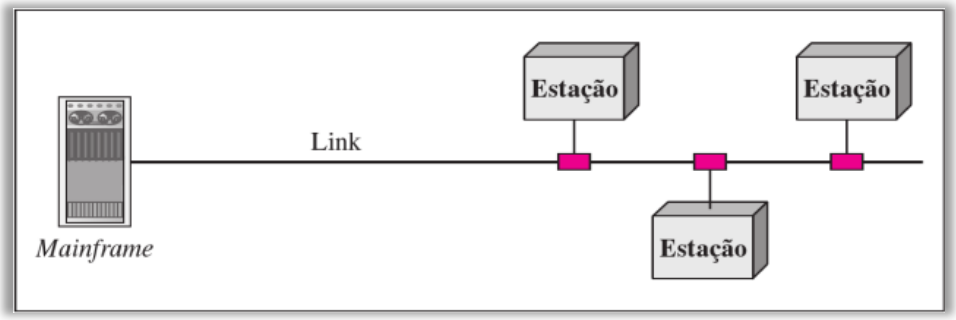
Redes são dois ou mais dispositivos conectados através de links. *O que é um link?* **Também chamado de enlace, trata-se de um caminho de comunicação que transfere dados de um dispositivo para outro.** Para fins de visualização, é mais simples imaginar qualquer link como uma reta entre dois pontos. Para ocorrer a comunicação, dois dispositivos devem ser conectados de alguma maneira ao mesmo link ao mesmo tempo.

Existem dois tipos possíveis de conexão: ponto-a-ponto e ponto-multiponto. Ambos se diferenciam em relação à utilização de um link dedicado ou compartilhado. *Como assim, Diego?* Um link dedicado é aquele que transporta tráfego de dados apenas entre os dois dispositivos que ele conecta. Exemplo: para que eu acesse à internet, eu compartilho vários cabos subterrâneos espalhados pelo nosso planeta com todas as pessoas que têm acesso à internet.



Nesse contexto, pode-se afirmar que, quando eu acesso à internet, eu utilizo um link dedicado ou um link compartilhado? Galera, eu utilizo um link compartilhado porque o enlace de comunicação é compartilhado com várias pessoas. **No entanto, só é possível ter links dedicados apenas à comunicação entre dois – e apenas dois – dispositivos.** Nesse caso, existe um tipo de conexão conhecido como ponto-a-ponto.

A maioria das conexões ponto-a-ponto utiliza um cabo para conectar dois dispositivos. No entanto, é possível haver links via satélite ou micro-ondas também de forma dedicada. Quando mudamos os canais de televisão por meio da utilização de um controle remoto infravermelho, nós estamos estabelecendo uma conexão ponto-a-ponto entre o controle remoto e o sistema de controle de TV. *Bacana?*

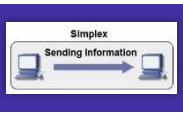
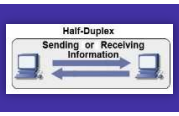
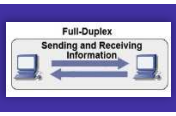


Já em uma conexão ponto-multiponto, mais de dois dispositivos compartilham um único link. Em um ambiente multiponto, a capacidade do canal de comunicação é compartilhada, seja de forma espacial, seja de forma temporal. Se diversos dispositivos puderem usar o link simultaneamente, ele é chamado de conexão compartilhada no espaço. Se os usuários tiverem de se revezar entre si, trata-se de uma conexão compartilhada no tempo – esse é o modo padrão.

TIPO DE CONEXÃO	DESCRIÇÃO
PONTO-A-PONTO	Conexão que fornece um link dedicado entre dois dispositivos.
PONTO-MULTIPONTO	Conexão que fornece um link compartilhado entre mais de dois dispositivos.

Direções de Transmissão

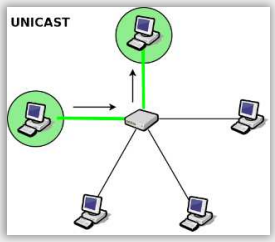
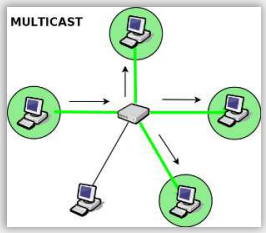
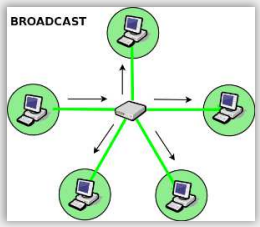
INCIDÊNCIA EM PROVA: BAIXÍSSIMA

TIPO	REPRESENTAÇÃO	DESCRIÇÃO
SIMPLEX		Uma comunicação é dita simplex quando há um transmissor de mensagem, um receptor de mensagem e esses papéis nunca se invertem no período de transmissão (Ex: TV, Rádio AM/FM, Teclado, etc).
HALF-DUPLEX		Uma comunicação é dita half-duplex quando temos um transmissor e um receptor, sendo que ambos podem transmitir e receber dados, porém nunca simultaneamente (Ex: Walk&Talk, Nextel, etc).
FULL-DUPLEX		Uma comunicação é dita full-duplex quando temos um transmissor e um receptor, sendo que ambos podem transmitir e receber dados simultaneamente (Ex: Telefone, VoIP, etc).

Modos de Transmissão

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

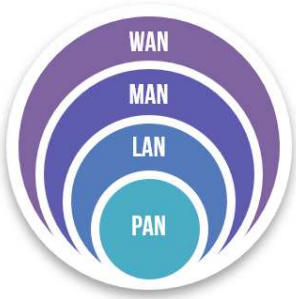
A transmissão de dados em uma rede de computadores pode ser realizada em três modos diferentes: *Unicast*, *Multicast* e *Broadcast*. Vamos vê-los em detalhes:

UNICAST [UNI = UM; CAST = TRANSMITIR]		Nessa comunicação, uma mensagem só pode ser enviada para um destino. Observem que a primeira estação de trabalho está enviando uma mensagem endereçada especificamente para a 2ª estação de trabalho. Analogamente, quando você envia uma mensagem no Whatsapp para uma pessoa específica, você está enviando uma mensagem *unicast*.
MULTICAST [MULTI = VÁRIOS E CAST = TRANSMITIR]		Nessa comunicação, uma mensagem é enviada para um grupo de destino. Observem que a primeira estação de trabalho está enviando uma mensagem endereçada para o grupo da 2ª, 3ª e 4ª estações. Analogamente, quando você cria uma lista de transmissão no Whatsapp com um grupo de pessoas e os envia uma mensagem, você está enviando uma mensagem multicast.
BROADCAST [BROAD = TODOS E CAST = TRANSMITIR]		Nessa comunicação, uma mensagem é enviada para todos os destinos. Observem que a primeira estação de trabalho está enviando uma mensagem endereçada a todas as estações de trabalho. Analogamente, quando você cria uma lista de transmissão no Whatsapp com todos os seus contatos e os envia uma mensagem, você está enviando uma mensagem broadcast.

Classificação de Redes

Quanto à Dimensão, Tamanho ou Área Geográfica

TIPO	SIGLA	DESCRIÇÃO	DISTÂNCIA
PERSONAL AREA NETWORK	PAN	Rede de computadores pessoal (celular, tablet, notebook, entre outros).	De alguns centímetros a alguns poucos metros.
LOCAL AREA NETWORK	LAN	Rede de computadores de lares, escritórios, prédios, entre outros.	De algumas centenas de metros a alguns quilômetros.
METROPOLITAN AREA NETWORK	MAN	Rede de computadores entre uma matriz e filiais em uma cidade.	Cerca de algumas dezenas de quilômetros.
WIDE AREA NETWORK	WAN	Rede de computadores entre cidades, países ou até continentes.	De algumas dezenas a milhares de quilômetros.



Essas classificações apresentadas possuem uma classificação correspondente quando se trata de um contexto de transmissão sem fio (*wireless*). Em outras palavras, há também WPAN, WLAN, WMAN e WWAN. Por outro lado, as questões de prova nem sempre são rigorosas na utilização desses termos (Ex: é comum enunciados tratando de redes locais sem fio como LAN e, não, WLAN). Infelizmente, desencanem na hora de resolver questões de prova...

Quanto à Arquitetura de Rede ou Forma de Interação

Uma rede de computadores é composta basicamente por **dispositivos intermediários**, como roteadores e switches, que conectam e direcionam dados, e por dispositivos finais, como computadores e smartphones, que interagem com o usuário. Os **dispositivos finais**, também conhecidos como hosts, são classificados em clientes, que consomem serviços, e servidores, que os fornecem.

As redes surgiram para otimizar processos e compartilhar recursos, como impressoras e dados, de forma eficiente. Servidores, geralmente máquinas poderosas, disponibilizam esses serviços para múltiplos clientes, que são dispositivos mais simples. Hoje, muitos servidores estão em Datacenters, armazenando e distribuindo conteúdos digitais. Na imagem seguinte, temos quatro dispositivos finais e quatro dispositivos intermediários.



Rede Ponto-a-Ponto

INCIDÊNCIA EM PROVA: BAIXA

Redes ponto-a-ponto, ou Peer-to-Peer (P2P), são redes não hierárquicas onde dispositivos se conectam diretamente entre si, sem intermediários, como servidores dedicados. Essas redes são vantajosas por serem de baixo custo, fáceis de configurar, escaláveis e rápidas, sendo populares em residências e empresas. Em P2P, todos os dispositivos, chamados pares, são equivalentes e podem agir tanto como clientes quanto como servidores.

Apesar das vantagens, redes P2P podem ser complexas para gerenciar, especialmente em grandes organizações, devido à falta de autenticação e segurança. Exemplificando a utilização do P2P, o BitTorrent é um protocolo que compartilha arquivos na Internet, empregado em muitos softwares para downloads, por vezes associado à pirataria e proibido em alguns países.

Diferente de redes cliente-servidor, as redes P2P são descentralizadas, sem um repositório central, com arquivos distribuídos entre múltiplos usuários. Isso torna difícil interromper o compartilhamento de arquivos, já que, se um usuário se desconecta, outros podem continuar o compartilhamento. Ainda que úteis, essas redes exigem cautela por poderem conter arquivos maliciosos. Há dois tipos principais de arquiteturas P2P:

- **P2P Puro:** completamente descentralizada e sem elementos centrais para realizar funções de coordenação;
- **P2P Híbrido:** introduz supernós para funções de coordenação, como acesso e indexação de dados, solucionando parcialmente problemas de gerenciamento.



O termo ponto-a-ponto costuma confundir porque pode ser utilizado em dois contextos com significados diferentes. No contexto de **Tipos de Conexão**, ele pode ser utilizado como contraponto ao enlace ponto-multiponto, ou seja, trata-se de um link dedicado entre dois dispositivos, em contraste com o enlace ponto-multiponto, em que o link é compartilhado entre dispositivos. Já vimos isso...

No contexto de **Arquitetura ou Forma de Interação**, ele pode ser utilizado como contraponto ao modelo cliente/servidor. Nesse caso, trata-se de uma máquina que é simultaneamente cliente e servidor, diferente do modelo cliente/servidor, em que uma máquina ou é um cliente ou é um servidor. Vamos resumir para que vocês nunca mais confundam esses termos:

Se existe um link dedicado entre dois dispositivos, trata-se de um tipo de **conexão ponto-a-ponto**. Por outro lado, se um mesmo dispositivo pode exercer função de cliente ou servidor em diferentes momentos, trata-se de um tipo de **arquitetura ponto-a-ponto**. O nome utilizado é exatamente o mesmo, porém tem significados diferentes dependendo do contexto utilizado.

Rede Cliente/Servidor

INCIDÊNCIA EM PROVA: MÉDIA

O modelo Cliente/Servidor é uma estrutura de rede hierárquica, mais complexa e eficiente, ideal para redes de grande escala como a Internet. Neste sistema, há uma máquina especializada, o servidor, que responde rapidamente aos pedidos dos outros computadores, os clientes. Este modelo aprimora o desempenho de certas tarefas e é distinto das redes P2P, onde cada máquina pode atuar como cliente e servidor.

Existem diversos tipos de servidores, como servidores de impressão, servidores de e-mails, servidores de arquivos, servidores de comunicação, servidores de banco de dados e servidores de páginas web. Um exemplo prático é ao fazer o download de um vídeo no site do Estratégia Concursos; o usuário atua como cliente, utilizando recursos do servidor do site, que hospeda e disponibiliza o conteúdo solicitado.

Quanto à Topologia (*Layout*)

Quando falamos em topologia, estamos tratando da forma como os dispositivos estão organizados. Dois ou mais dispositivos se conectam a um link; dois ou mais links formam uma topologia. A topologia é a representação geométrica da relação de todos os links e os dispositivos de uma conexão entre si. Existem quatro topologias básicas[1] possíveis: barramento, estrela, anel e malha. No entanto, vamos primeiro entender a diferença entre topologia física e lógica.

A topologia lógica exibe o fluxo de dados na rede, isto é, como as informações percorrem os links e transitam entre dispositivos – lembrando que links são os meios de transmissão de dados. Já a topologia física exibe o layout (disposição) dos links e nós de rede. **Em outras palavras, o primeiro trata do percurso dos dados e o segundo trata do percurso dos cabos, uma vez que não necessariamente os dados vão percorrer na mesma direção dos cabos.**

TIPO DE TOPOLOGIA	DESCRIÇÃO
FÍSICA	Exibe o layout (disposição) dos links e nós de rede.
LÓGICA	Exibe o fluxo ou percurso dos dados na rede.

[1] Existem outras topologias, como a topologia em árvore, daisy chain, ponto a ponto, entre outras, mas não é o foco desse curso. Há também topologias híbridas, que combinam duas ou mais topologias.

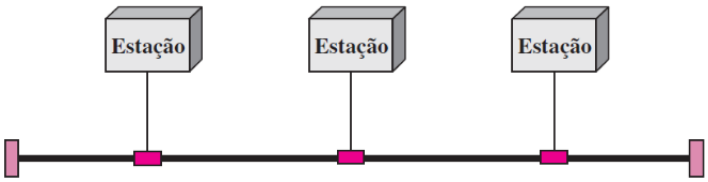


Se uma questão de prova não deixar explícito em sua redação qual é o tipo de topologia, pode-se assumir que ela se refere à **Topologia Física, e não à Topologia Lógica!**

Barramento (Bus)

INCIDÊNCIA EM PROVA: ALTA

A topologia de barramento[2] usa um meio de transmissão ponto-multiponto, geralmente um cabo coaxial, onde todas as estações são conectadas. **Esse único meio de transmissão, chamado de backbone ou espinha dorsal, permite que um sinal de um nó qualquer se propague em ambas as direções (broadcast), sendo recebido por todos os nós.** No entanto, apenas as estações endereçadas acessam os dados, apesar de todos receberem o sinal.



Cada estação se conecta ao backbone por uma placa/adaptador de rede, responsável pela interface entre a estação e o cabo. É importante destacar que a transmissão não é simultânea: enquanto uma estação transmite, as outras esperam – isso define essa topologia como half-duplex. Logo, nesse sentido, se duas estações transmitirem dados ao mesmo tempo, ocorre uma colisão de sinais. *Entendido?*

Um aspecto crítico dessa topologia é que qualquer falha no cabo de backbone afeta toda a rede, mesmo se o problema ocorrer em apenas um ponto específico. As vantagens incluem a facilidade de instalação e a economia de cabeamento. **Entretanto, as desvantagens são o aumento do atraso na comunicação e a dificuldade em isolar falhas, especialmente em redes com muitas máquinas.**

CARACTERÍSTICAS	DESCRIÇÃO
DEFINIÇÃO	A topologia em barramento é um design de rede em que todos os dispositivos compartilham um único cabo (*backbone*).
ESCALABILIDADE	Menos escalável, pois a adição de novos dispositivos pode resultar em colisões de dados.
CONFIABILIDADE	Menos confiável, pois uma falha em qualquer ponto do barramento pode afetar toda a rede.

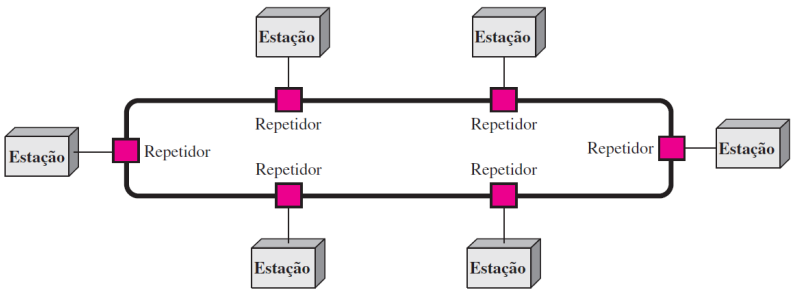
[2] Assim como a topologia em anel (que veremos adiante), está em desuso há muitos anos, mas continua sendo cobrada em concursos públicos.

DESEMPENHO	O desempenho pode degradar quando muitos dispositivos tentam acessar o barramento ao mesmo tempo.
MANUTENÇÃO	Apresenta dificuldades de manutenção por conta de problemas de colisão de dados e dificuldades na localização de falhas.
COMPLEXIDADE	Menos complexa de implementar, pois envolve um único cabo, mas pode se tornar complicada em redes maiores.
LATÊNCIA	A latência (atraso na comunicação de uma rede) é variável, dependendo do tráfego da rede. Pode ocorrer colisão de dados que exige retransmissões.
SEGURANÇA	Menos segura, uma vez que qualquer dispositivo pode "ouvir" todas as comunicações na rede.
ISOLAMENTO DE PROBLEMAS	Problemas podem ser isolados com certa dificuldade, pois é difícil localizar fisicamente o ponto de falha no barramento.
TIPOS DE APLICAÇÃO	Adequada para redes menores, onde o tráfego é limitado, como redes domésticas ou de laboratórios.

Anel (Ring)

INCIDÊNCIA EM PROVA: MÉDIA

A Topologia em Anel (Ring) é um arranjo de rede onde cada dispositivo se conecta a dois outros dispositivos, formando um anel. A comunicação é unidirecional (simplex), com as mensagens circulando o anel e sendo retransmitidas em cada nó até chegar ao destinatário, que envia uma confirmação de recebimento ao remetente. A imagem seguinte apresenta uma possível configuração dessa topologia:



Nessa topologia, a transmissão de dados é semelhante a uma corrida de revezamento: um "token" (envelope de dados) circula pelo anel e só a estação que possui o token pode enviar dados. Após a estação de destino receber e reconhecer os dados, o token segue circulando até voltar à estação remetente, garantindo que não haja colisões de dados, uma vez que apenas um dispositivo transmite por vez.

Essa topologia permite fácil instalação e reconfiguração e oferece isolamento de falhas simplificado. **No entanto, há desvantagens: se um link é rompido ou uma estação falha, toda a rede pode parar.** O desempenho também pode ser limitado pelo número de dispositivos e comprimento do anel. Para mitigar esses riscos, foram desenvolvidas versões com anéis duplos, como o FDDI, que oferecem maior robustez.

CARACTERÍSTICAS	DESCRIÇÃO
DEFINIÇÃO	Uma topologia de rede onde cada dispositivo está conectado a dois outros, formando um ciclo fechado.
ESCALABILIDADE	Limitada, adicionando novos dispositivos pode exigir a reconfiguração da rede.
CONFIABILIDADE	Moderada, depende do funcionamento de cada nó e das conexões entre eles.
DESEMPENHO	Pode ser afetado à medida que a rede cresce, devido ao tráfego passar por vários nós.
MANUTENÇÃO	Pode ser complexa, uma vez que a falha em um nó pode afetar toda a rede.
COMPLEXIDADE	Relativamente alta, especialmente em redes maiores devido à gestão de conexões.
LATÊNCIA	Pode ser alta, já que os dados podem ter que passar por vários nós antes de chegar ao destino.
SEGURANÇA	Moderada, a interceptação de dados é possível, mas mais difícil do que em redes de topologia estrela.
ISOLAMENTO DE PROBLEMAS	Simplificado, pois se um dispositivo não receber o sinal de que os dados foram recebidos, ele pode emitir um alerta – facilitando a identificação do problema.
TIPOS DE APLICAÇÃO	Adequada para sistemas que requerem conexões ponto a ponto, como sistemas de controle de tráfego.

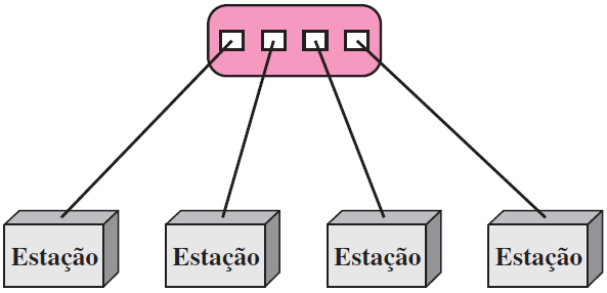
Estrela (*Star*)

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Nessa topologia, as estações são ligadas através de uma conexão ponto-a-ponto dedicada a um nó central controlador[3], pelo qual passam todas as mensagens, não admitindo tráfego direto entre os dispositivos. Notem que eu disse que o enlace entre estações e o nó central é ponto-a-ponto e, não, que a arquitetura de rede é ponto-a-ponto. Não confundam! Cada dispositivo se conecta ao nó central por meio de um link dedicado, portanto usa um tipo de enlace ponto-a-ponto.

Trata-se da topologia mais utilizada atualmente por facilitar a adição de novas estações de trabalho e pela fácil identificação ou isolamento de falhas. No primeiro caso, para adicionar ou remover uma nova estação de trabalho, basta conectá-la ou desconectá-la da porta do nó central. No segundo caso, caso um cabo venha a se romper, não afetará as outras estações – afetará apenas a estação conectada por esse cabo. Logo, torna-se fácil identificar e isolar as falhas.

[3] Nó central é um dispositivo que concentra conexões – em geral, ele liga os cabos dos computadores de uma rede (Ex: Hub ou Switch).



Observem que para que uma estação de trabalho envie uma informação para outra, haverá sempre uma passagem pelo nó central. Aliás, essa é uma das desvantagens dessa topologia: existe um ponto único de falha, isto é, se o dispositivo central falhar, toda a rede será prejudicada. Para reduzir essa probabilidade, utilizam-se dispositivos redundantes para que, caso algum pare de funcionar, o outro entra em ação.

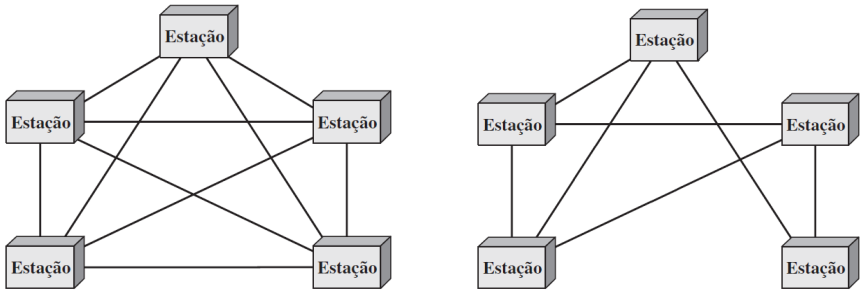
CARACTERÍSTICAS	DESCRIÇÃO
DEFINIÇÃO	Uma topologia de rede onde todos os dispositivos estão conectados a um ponto central, como um hub ou switch.
ESCALABILIDADE	Alta, fácil de adicionar novos dispositivos sem afetar significativamente a rede existente.
CONFIABILIDADE	Alta, uma vez que a falha em um dispositivo geralmente não afeta os outros.
DESEMPENHO	Bom, pois o tráfego de dados é gerenciado pelo ponto central, reduzindo congestionamentos.
MANUTENÇÃO	Relativamente fácil, pois problemas geralmente se limitam a dispositivos individuais e são fáceis de isolar.
COMPLEXIDADE	Baixa a moderada, devido à simplicidade da configuração e gerenciamento da rede.
LATÊNCIA	Geralmente baixa, especialmente em redes com switches modernos que gerenciam o tráfego de forma eficiente.
SEGURANÇA	Boa, pois é mais fácil monitorar e controlar o acesso à rede através do ponto central.
ISOLAMENTO DE PROBLEMAS	Excelente, falhas em dispositivos individuais geralmente não impactam o resto da rede.
TIPOS DE APLICAÇÃO	Adequada para redes domésticas e empresariais onde a facilidade de manutenção e a confiabilidade são prioritárias.

Malha (Mesh)

INCIDÊNCIA EM PROVA: BAIXA

Nessa topologia, cada estação de trabalho possui uma conexão ponto a ponto direta e dedicada entre as demais estações da rede, de modo que não exista uma hierarquia entre elas. Nas imagens seguintes, temos dois exemplos de Topologia em Malha: à esquerda, temos uma

malha completa (também chamada de *Full Mesh*), isto é, cada nó se conecta a todos os outros nós; à direita, temos uma malha parcial, isto é, nem todos os nós se conectam aos outros nós[4].



Uma topologia em malha oferece várias vantagens em relação às demais topologias de rede. **Em primeiro lugar, o uso de links dedicados garante que cada conexão seja capaz de transportar seu próprio volume de dados, eliminando, portanto, os problemas de tráfego que possam ocorrer quando os links tiverem de ser compartilhados por vários dispositivos.** Em segundo, uma topologia de malha é robusta.

Se um link tornar-se inutilizável, ele não afeta o sistema como um todo. O terceiro ponto é que há uma vantagem de privacidade e segurança. Quando qualquer mensagem trafega ao longo de uma linha dedicada, apenas o receptor pretendido a vê. Os limites físicos impedem que outros usuários acessem essa mensagem. **Finalmente, os links ponto a ponto facilitam a identificação de falhas, bem como o isolamento destas.**

O tráfego pode ser direcionado de forma a evitar links com suspeita de problemas. Essa facilidade permite ao administrador de redes descobrir a localização exata da falha e ajuda na descoberta de sua causa e solução. *E as desvantagens, Diego?* **As principais desvantagens de uma topologia em malha estão relacionadas à escalabilidade e ao custo, isto é, crescimento da quantidade de cabeamento e o número de portas necessárias para sua implementação.**

Em primeiro lugar, como cada dispositivo tem de estar conectado a cada um dos demais, a instalação e a reconstrução são trabalhosas. Em segundo, o volume de cabos pode ser maior que o espaço disponível seja capaz de acomodar (nas paredes, tetos ou pisos). Finalmente, o hardware necessário para conectar cada link (portas, placas e/ou cabos) pode ter um custo proibitivo. **Por tais razões, uma topologia de malha normalmente é implementada de forma limitada.**

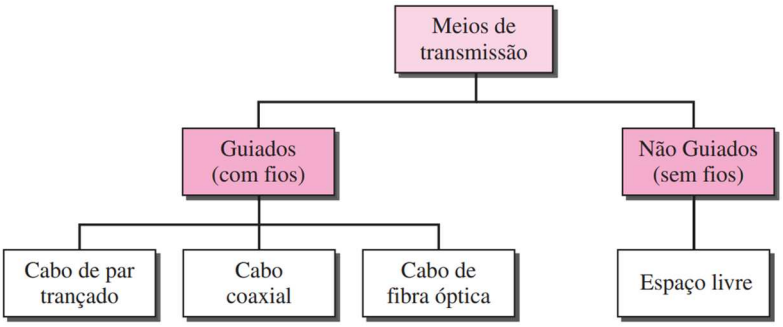
TOPOLOGIA FÍSICA	DIREÇÃO DE TRANSMISSÃO	TIPO DE ENLACE	MODOS DE TRANSMISSÃO
BARRAMENTO	Half-Duplex	Multiponto	Broadcast
ANEL	Simplex	Ponto-a-Ponto	Broadcast

[4] Caso a banca não deixe explícito de qual tipo está tratando, considere que se trata de uma malha completa.

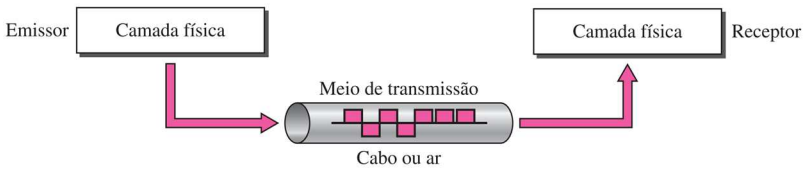
ESTRELA	Half-Duplex, se usar Hub; caso contrário Full-Duplex	Ponto-a-Ponto	Broadcast, se usar Hub; caso contrário, Unicast, Multicast ou Broadcast
MALHA	Depende	Ponto-a-Ponto	Unicast, Multicast ou Broadcast

Meios de Transmissão

Um meio de transmissão, em termos gerais, pode ser definido como qualquer coisa capaz de transportar informações de uma origem a um destino. Por exemplo: o meio de transmissão para duas pessoas conversando durante um jantar é o ar; para uma mensagem escrita, o meio de transmissão poderia ser um carteiro, um caminhão ou um avião. **Em telecomunicações, meios de transmissão são divididos em duas categorias: meios guiados e não-guiados.**

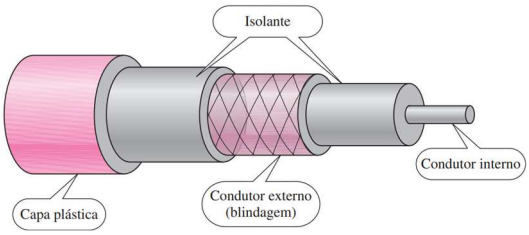


TIPO DE MEIO	DESCRIÇÃO
GUIADO	Trata-se da transmissão por cabos ou fios de cobre, onde os dados transmitidos são convertidos em sinais elétricos que propagam pelo material condutor. Exemplo: cabos coaxiais, cabos de par traçado, fibra óptica, entre outros.
NÃO-GUIADO	Trata-se da transmissão por irradiação eletromagnética, onde os dados transmitidos são irradiados através de antenas para o ambiente. Exemplo: ondas de rádio, infravermelho, microondas, bluetooth e wireless.

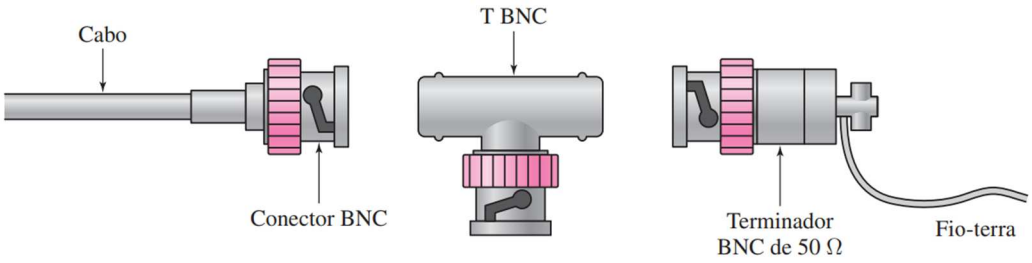


Cabo Coaxial

INCIDÊNCIA EM PROVA: BAIXA



Consiste em um fio central de cobre, envolvido por uma blindagem metálica. Isolantes de plástico flexível separam os condutores internos e externos e outras camadas do revestimento que cobrem a malha externa. Esse meio de transmissão é mais barato, pouco flexível e muito resistente à interferência eletromagnéticas graças a sua malha de proteção. Ele cobre distâncias maiores que o cabo de par trançado e utiliza um conector chamado BNC[5].



Foi utilizado até meados da década de 90 em redes de computadores, quando começou a ser substituído pelo cabo de par trançado. Ele ainda é utilizado em telecomunicações, basta dar uma olhadinha no decodificador da sua TV por Assinatura. **O cabo que chega na sua casa/prédio e que entra em um modem é geralmente um cabo coaxial** – ele é capaz de transportar sinais de Internet e TV.



Hoje em dia, provedores de TV/Internet têm substituído boa parte da mídia por cabos de fibra óptica. **Informação importante:** embora o cabo coaxial tenha uma largura de banda muito maior e cubra maiores distâncias que o cabo de par trançado, a sua taxa de transmissão é menor, o sinal se enfraquece mais rapidamente e ele requer o uso frequente de repetidores. É importante saber essas diferenças, mas veremos esses conceitos com mais detalhes à frente...

> *A **Taxa de Transferência** (Throughput) mede a quantidade de dados real que é transferida em uma quantidade específica de tempo. Em outras palavras, mede a velocidade da transmissão de dados. Obviamente, quanto maior a taxa de transferência, melhor, pois mais rapidamente dados poderão ser transferidos na rede.*
>
> *Ex: em uma rede com largura de banda de 100 Mbps, a taxa de transmissão pode ser apenas de 70 Mbps devido a fatores como atrasos na rede e sobrecarga de comunicação.*
>
> *Já a **Largura de Banda** é uma medida da capacidade de transmissão teórica de uma rede e refere-se à quantidade máxima de dados que pode ser transmitida por um canal de comunicação em um determinado período de tempo.*

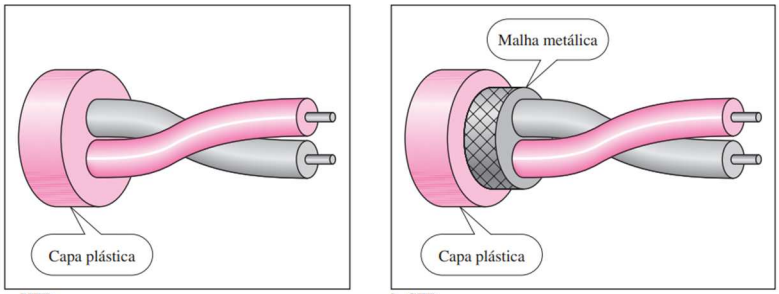
[5] O BNC é usado para conectar a extremidade de um cabo a um dispositivo, mas existe também o conector T-BNC, usado para dividir uma conexão em duas; e também o Terminador BNC, usado no final do cabo para impedir a reflexão do sinal.

Ex: uma conexão de internet com uma largura de banda de 100 Mbps tem a capacidade de transmitir 100 milhões de bits de dados a cada segundo sob condições ideais.

Em resumo, podemos afirmar que a largura de banda representa um cenário ideal sob condições perfeitas, enquanto a taxa de transmissão reflete a realidade prática, incluindo todas as imperfeições e limitações da rede.

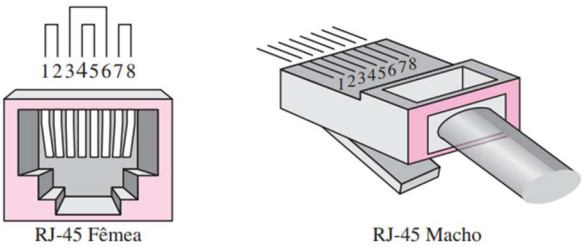
Cabo de Par Trançado

INCIDÊNCIA EM PROVA: ALTA



a. UTP b. STP

Consiste em quatro pares de fios trançados blindados ou não, e envolto de um revestimento externo flexível. Eles são trançados para diminuir a interferência eletromagnética externa e interna – quanto mais giros, maior a atenuação. Este é o cabo mais utilizado atualmente por ser o mais barato de todos e ser bastante flexível. Esse cabo cobre distâncias menores que o cabo coaxial e utiliza um conector chamado RJ-45 (**Memorizem!**).

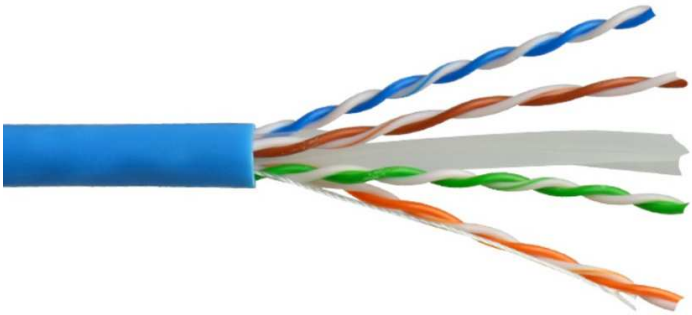


RJ-45 Fêmea RJ-45 Macho

Quando é blindado, ele é chamado de Cabo STP (*Shielded Twisted Pair*) e quando não é blindado, ele é chamado de Cabo UTP (*Unshielded Twisted Pair*). **Galera, esse é aquele cabinho azul que fica atrás do seu computador ligado provavelmente a um roteador**. *Sabe aquele cabo do telefone fixo da sua casa?* Ele é mais fininho, mas ele também é um cabo de par trançado. Comparado ao cabo coaxial, tem largura de banda menor, mas taxas de transmissão maiores. Vejamos suas categorias:

CATEGORIA	TAXA MÁXIMA DE TRANSMISSÃO	LARGURA DE BANDA	DISTÂNCIA MÁXIMA
CAT3	Até 10 MBPS	16 MHz	100 Metros
CAT4	Até 16 MBPS	20 MHz	100 Metros
CAT5	Até 100 MBPS	100 MHz	100 Metros
CAT5E	Até 1000 MBPS (1G)	100 MHz	100 Metros

CAT6	Até 10000 MBPS (10G)	250 MHz	100 Metros
CAT6A	Até 10000 MBPS (10G)	500 MHz	100 Metros
CAT7	Até 10000 MBPS (10G)	600 MHz	100 Metros
CAT7A	Até 10000 MBPS (10G)	1000 MHz	100 Metros
CAT8	Até 40000 MBPS (40G)	2000 MHz	100 Metros

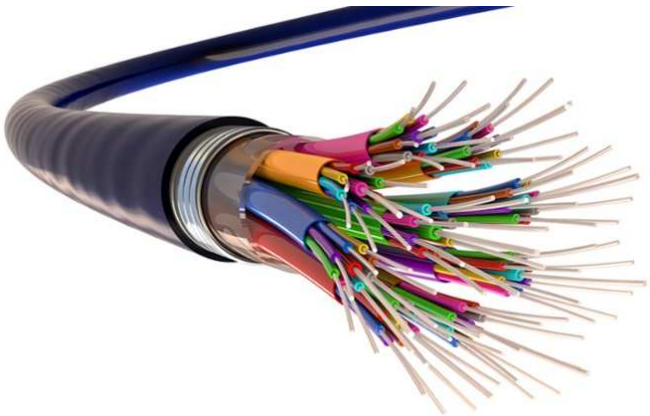


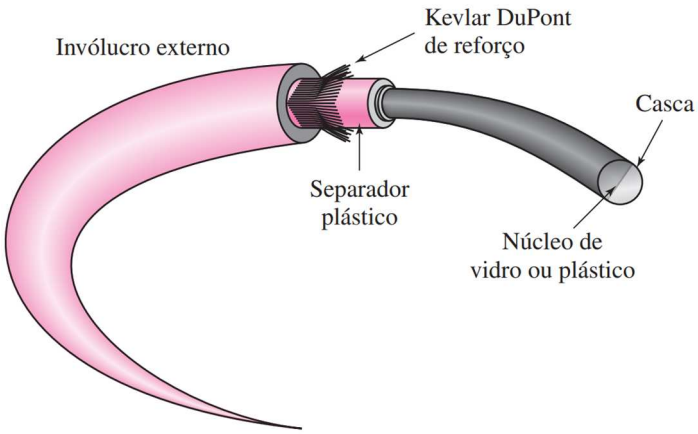


Os cabos de par trançado possuem quatro pares de fios, sendo alguns utilizados para transmissão e outros para recepção, permitindo uma comunicação *full duplex*. Para facilitar a identificação, os pares são coloridos e a ordem dos fios dentro do conector é padronizada. Eles podem ser utilizados na transmissão de sinais analógicos ou digitais. E a largura de banda depende da espessura do fio e da distância percorrida.

Cabo de Fibra Óptica

INCIDÊNCIA EM PROVA: MÉDIA





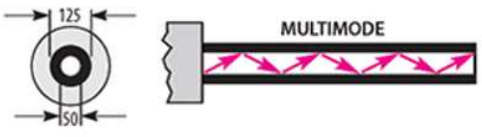
O cabo de fibra óptica consiste em uma casca e um núcleo (de vidro, mais comum; ou plástico) para transmissão de luz. Esse tipo de cabo é normalmente encontrado em backbones de redes por apresentar excelente relação entre ampla largura de banda e custo. Hoje em dia, podemos transferir dados à velocidade de até 1.600 Gbps. Vejamos algumas vantagens e desvantagens dessa tecnologia:

VANTAGENS	DESCRIÇÃO

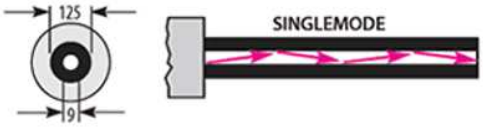
LARGURA DE BANDA MAIS AMPLA	Pode suportar larguras de banda muito maiores (e, consequentemente, maiores velocidades) que o cabo de par trançado ou coaxial. Atualmente, as taxas de dados e a utilização de largura de banda não são limitadas pelo meio de transmissão, mas sim pelas tecnologias de geração e recepção de sinais disponíveis.
MENOR ATENUAÇÃO DO SINAL	A distância de transmissão por fibra óptica é significativamente maior que a de qualquer outro meio de transmissão guiado. Um sinal pode percorrer 50 km sem precisar de regeneração. No caso de cabos coaxiais ou de par trançado, precisamos de repetidores a cada 5 km.
IMUNIDADE À INTERFERÊNCIA ELETROMAGNÉTICA	Ruídos eletromagnéticos não são capazes de afetar os cabos de fibra óptica.
RESISTÊNCIA A MATERIAIS CORROSIVOS E PESO LEVE	O vidro é mais resistente a materiais corrosivos que o cobre. Além disso, os cabos de fibra óptica são muito mais leves que os cabos de cobre.
MAIOR IMUNIDADE À INTERCEPTAÇÃO	Os cabos de fibra óptica são mais imunes à interceptação que os cabos de cobre. Os cabos de cobre criam efeitos antena que podem ser facilmente interceptados.

DESVANTAGENS	DESCRIÇÃO
INSTALAÇÃO E MANUTENÇÃO	O cabo de fibra óptica é uma tecnologia relativamente nova. Sua instalação e sua manutenção exigem mão de obra especializada, que não se encontra com facilidade.
PROPAGAÇÃO UNIDIRECIONAL DA LUZ	A propagação da luz é, por padrão, unidirecional. Se precisarmos de comunicação bidirecional, serão necessários dois cabos de fibra óptica; ou utilizar WDM (Wavelength Division Mutiplexing), que permite que uma única fibra seja bidirecional.
CUSTO	O cabo e as interfaces são relativamente mais caros que outros meios de transmissão guiados. Se a demanda por largura de banda não for alta, muitas vezes o uso de fibra óptica não pode ser justificado.

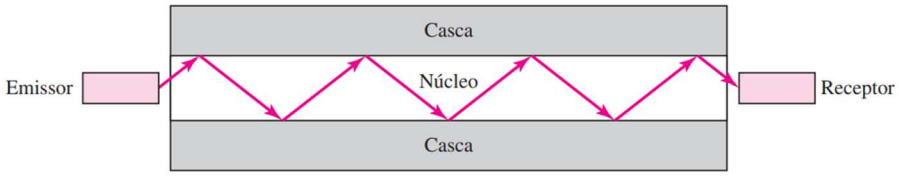
A tecnologia atual suporta dois modos para propagação da luz ao longo de canais ópticos, cada um dos quais exigindo fibras ópticas com características físicas diferentes: **Monomodo e Multimodo**.



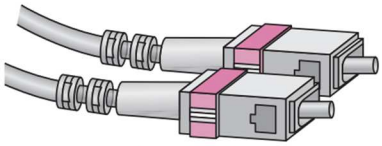
A Fibra Multimodo leva o feixe de luz **por vários modos ou caminhos**, por uma distância menor, com menores taxas de transmissão, mais imprecisa, diâmetro maior e alto índice de refração e atenuação, mas possui construção mais simples, é mais barata e utilizada em LANs.

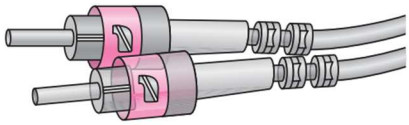


A Fibra Monomodo leva o feixe de luz **por um único modo ou caminho**, por uma distância maior, com maiores taxas de transmissão, mais precisa, diâmetro menor e baixo índice de refração e atenuação, mas possui construção mais complexa, é mais cara e utilizada em WANs.



Para fibras ópticas, existem dezenas de conectores diferentes no mercado, mas os mais comuns são os conectores ST (Straight Tip) e SC (Subscriber Connector). **Outra observação: antigamente uma fibra óptica era capaz de enviar dados em apenas uma direção (simplex). Atualmente ela já permite a comunicação bidirecional, isto é, são capazes de enviar dados em ambas as direções (full-duplex).**


Conector SC


Conector ST

Equipamentos de Redes

Galera, os equipamentos ou dispositivos de uma rede podem classificados como finais ou intermediários. No primeiro caso, trata-se daqueles dispositivos que permitem a entrada e/ou saída de dados (Ex: computador, impressora; câmeras, sensores, etc); no segundo caso, trata-se daqueles que compõem a infraestrutura de uma rede (Hub, Bridge, Switch, Router, etc). Nós vamos focar agora nos dispositivos intermediários. Venham comigo...

Network Interface Card (Placa/Adaptador de Rede)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Trata-se de um dispositivo eletrônico, interno ou externo a uma estação, contendo circuitos que permitem a uma estação se conectar a uma rede. Em outras palavras, trata-se de um hardware que permite que um computador se conecte a uma rede de computadores e se comunique com outros dispositivos na rede. Ela é responsável por fornecer uma interface entre o computador e o meio físico da rede (de forma cabeada ou não).





Essas são as famosas Placas de Rede – também chamada de Placas NIC. Na imagem apresentada à esquerda, temos uma placa de rede cabeada e, na imagem apresentada à direita, temos uma placa de rede não cabeada (*wireless*). Essas placas podem ser instaladas internamente em um computador (forma mais comum) ou podem ser dispositivos externos, como pequenos adaptadores USB.

Se vocês olharem na parte de trás do gabinete de um computador, vocês poderão vê-las (provavelmente com o cabo de par trançado conectado a ela). Elas permitem uma comunicação bidirecional – transmissão e recebimento de dados – com os demais elementos da rede. **Essas placas são essenciais para que um computador acesse uma rede local ou a internet – sendo amplamente utilizadas em desktops, notebooks, servidores e outros dispositivos de rede.**

As placas de rede podem oferecer suporte a diferentes tipos de conexões de rede, como Ethernet, Wi-Fi, entre outros. Elas são responsáveis por converter os dados do computador em sinais que podem ser transmitidos pela rede e também por receber sinais da rede e entregá-los ao sistema do computador. **Agora um ponto importante: placas de rede possui um identificador único e exclusivo chamado Endereço MAC (Media Access Control).**

Esse endereço é gravado na fábrica e não pode ser alterado, a menos que seja um processo excepcional. O endereço MAC é composto por uma sequência de 12 dígitos hexadecimais (portanto, 48 bits). Ele é usado para identificar de forma única dispositivos em uma rede local. **Cada fabricante de dispositivos de rede é atribuído a um conjunto exclusivo de endereços MAC, garantindo que não haja conflitos de identificação em escala global.**

Esse endereço desempenha um papel fundamental na comunicação de dados em uma rede, uma vez que é utilizado para rotear pacotes de dados para os dispositivos corretos na rede. Isso ajuda os dispositivos na mesma rede a se comunicarem entre si e garante que os dados sejam entregues ao destinatário adequado. Vejam a seguir um exemplo de endereço MAC (note que ele vem separado por dois-pontos).

```
00:1C:B3:09:85:15
```

CARACTERÍSTICA	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo que permite que um computador se conecte a uma rede de computadores, seja por meio de cabo ou sem fio.
CAMADA OSI	Camada 2 (Enlace). Atenção: vamos estudar o que são as camadas OSI mais à frente.
VANTAGENS	Permite que um computador se conecte a redes locais e à internet; facilita a comunicação entre dispositivos em uma rede; e oferece a capacidade de transmissão e recepção de dados.
DESVANTAGENS	Em redes sem fio, a qualidade do sinal pode afetar o desempenho; e pode ser uma vulnerabilidade de segurança se não configurada corretamente.

Hub (Concentrador)

INCIDÊNCIA EM PROVA: MÉDIA



Inicialmente, é importante saber que existem hubs ativos e passivos. **Um hub passivo é simplesmente um conector que concentra e conecta os cabos provenientes de diferentes ramificações. Esse dispositivo sequer é conectado na rede elétrica, portanto não é capaz de regenerar sinais digitais.** Pessoal, se uma questão não mencionar o tipo de hub, podemos assumir que ela está tratando de hubs ativos. Vamos estudá-lo com um pouco mais de detalhes...

Um hub ativo é um dispositivo para interligação de computadores que tem o objetivo de concentrar os enlaces e aumentar o alcance de uma rede local por meio da regeneração de sinais. Pessoal, sinais que transportam dados dentro de uma rede podem trafegar por uma distância fixa. Após essa distância, o sinal começa a se atenuar, colocando em risco a integridade dos dados (isto é, correndo risco de haver perda de dados).

Um hub ativo atua como repetidor, recebendo sinais digitais e, antes de se tornar muito fraco ou corrompido, regenerando-o para o seu padrão de bits original. O repetidor encaminha, então, o sinal regenerado. Pode-se afirmar, portanto, que ele pode estender o comprimento físico de uma rede local. **O hub ativo é considerado um repetidor multiportas porque ele regenera e transmite os sinais entre suas portas. Atualmente, esse equipamento está obsoleto.**

O Hub é considerado um dispositivo "burro" por trabalhar apenas com *broadcast*. *Como assim, professor?* **Ao receber dados, ele os distribui para todas as outras portas – ele não é capaz de transmitir dados somente para uma porta específica.** Dessa forma, apenas uma máquina pode transmitir dados de cada vez para evitar colisões, portanto ele trabalha com a direção de transmissão half-duplex.

Agora vamos ver se vocês entenderam mesmo o tópico de topologia de redes. Nós já sabemos que a topologia física trata de como estão dispostos os links (cabos) e os nós de uma rede. E sabemos que a topologia lógica trata de como os dados efetivamente percorrem os links e transitam entre dispositivos. Por outro lado, nós também sabemos que um hub ativo é responsável por concentrar os cabos em um único local e por trabalhar apenas em broadcast. Dito isso...

QUAL É A TOPOLOGIA FÍSICA E LÓGICA DE UM HUB ATIVO?

Ora, se ele concentra todos os cabos, então sua topologia física é em estrela; e se ele somente trabalha em broadcast, isto é, os dados são transmitidos para todos os dispositivos, então sua topologia lógica é em barramento. **Em suma: o hub ativo é um equipamento de rede concentrador de enlaces que permite também concentrar o tráfego de rede que provém de vários dispositivos, assim como regenerar o sinal.**

O seu objetivo é recuperar os dados que chegam a uma porta e enviá-los para todas as demais portas. A representação de um Hub é apresentada abaixo:



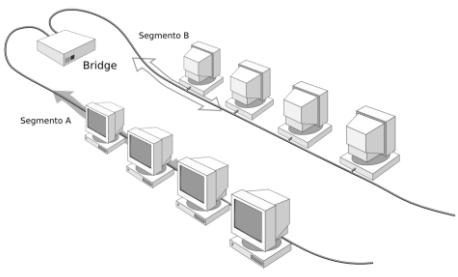
CARACTERÍSTICA	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo que simplesmente repete os dados recebidos em uma porta para todas as outras portas (está em desuso atualmente).
CAMADA OSI	Camada 1 (Física).
VANTAGENS	Custo geralmente baixo; simplicidade de operação; adequado para redes muito pequenas.
DESVANTAGENS	Pode causar tráfego ineficiente e colisões de dados; pode levar à degradação do desempenho em redes maiores; não possui inteligência para direcionar pacotes apenas para o destino certo.

Bridge (Ponte)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Uma bridge é um equipamento de rede que também é capaz de regenerar o sinal que recebe, porém ela tem uma função extra: possui capacidade de filtragem. *Como assim, Diego?* **Isso significa que ela é capaz de verificar o endereço de destino de um conjunto de dados e decidir se este deve ser encaminhado ou descartado.** Para tal, esse dispositivo possui uma tabela que associa endereços a portas, assim ela consegue decidir a quem os dados devem ser encaminhados.

Ela também permite conectar segmentos de redes que podem ou não utilizar tecnologias de enlace distintas (Ex: Ethernet + Token Ring) de forma que possam se comunicar como se fossem uma única rede. *O que é um segmento de rede?* É simplesmente subdivisão de uma rede. Vejam abaixo que uma rede foi separada em dois segmentos: Segmento A e Segmento B. Como a rede foi segmentada, nós temos uma redução no tráfego e uma menor chances de colisões.



Como assim uma redução no tráfego? Galera, os dados transmitidos para um segmento agora são enviados apenas para os computadores daquele segmento específico e, não, para todos os computadores da rede – como ocorria com o hub! Lembrem-se que o hub envia dados para todos os computadores da rede indiscriminadamente. Logo, o tráfego na rede reduz e a chance de colisões também.

As informações manipuladas por uma bridge são chamadas de quadros ou *frames* – assim como no switch. Há diversos tipos de bridge: (1) simples – quando possui apenas duas portas, logo conecta apenas dois segmentos; (2) multiporta – quando possui diversas portas, logo conectam vários

segmentos; (3) transparente – quando é invisível para outros dispositivos da rede, não necessitando de configurações; (4) de tradução – quando conecta redes de tecnologias de enlace diferentes.

Em suma: uma bridge é um equipamento de rede que permite conectar segmentos de rede diferentes que podem ou não utilizar tecnologias de enlace distintas de forma que sua agregação pareça uma única rede, permitindo filtrar os quadros para que somente passe para o outro segmento da bridge dados enviados para algum destinatário presente nele, e que permite a redução de tráfego de dados, o aumento da largura de banda e a separação dos domínios de colisão.

CARACTERÍSTICA	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede utilizada para dividir uma rede em segmentos menores, reduzindo colisões e tráfego de rede desnecessário (está em desuso atualmente).
CAMADA OSI	Camada 2 (Enlace).
VANTAGENS	Filtra o tráfego, melhorando o desempenho; pode conectar diferentes tipos de redes (Ex: Ethernet e Wi-Fi); aumenta a segurança da rede, criando domínios de colisão separados.
DESVANTAGENS	Pode ser mais caro do que um hub simples; requer configuração e gerenciamento adequados; limitação da extensão da rede e a complexidade de gerenciamento em redes maiores.

Switch (Comutador)

INCIDÊNCIA EM PROVA: MÉDIA



Também conhecido como comutador, o switch é uma evolução dos hubs! **Eles são inteligentes, permitindo fechar canais exclusivos de comunicação entre a máquina que está enviando e a que está recebendo**. Em outras palavras, o switch é capaz de receber uma informação e enviá-la apenas ao seu destinatário. Ele não é como o hub, que recebia uma informação de fora e a repassava para todo mundo que estivesse na rede.

O hub é aquele seu amigo fofoqueiro que você pede para ele contar algo para outro amigo e ele sai contando para todo mundo. Já o switch é aquele amigo leal – se você pede para ele contar algo para outro amigo, ele conta apenas para esse amigo e, não, para os demais. **O nome dessa característica é encaminhamento ou filtragem, porque ele filtra as mensagens recebidas e encaminha apenas para o destinatário original.**

Outra característica importante desse equipamento é a **autonegociação**, isto é, a compatibilidade com diferentes Padrões Ethernet. Vamos ver padrões de redes em detalhes no próximo tópico, mas por enquanto basta saber que as tecnologias de padrões de rede vão evoluindo com o passar do tempo e passam a funcionar, por exemplo, com taxas de transmissão mais altas. *Como fazer para dois dispositivos com padrões diferentes conectados ao mesmo link possam conversar sem problemas?*

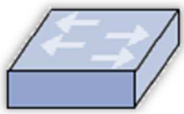
O recurso de autonegociação do switch permite que seja negociado tanto a taxa de transmissão de dados quanto a direção de transmissão, isto é, se um trabalha com uma taxa de transmissão maior e o outro com uma taxa de transmissão menor, eles negociam o envio de dados a uma taxa de transmissão menor, de modo a manter uma compatibilidade e uma comunicação de dados eficiente e boa para todos.

Outro recurso interessante é o autoaprendizado, ou seja, switches são equipamentos que não precisam ser configurados manualmente. *Como assim, Diego?* Quando você conecta um computador ao switch, você não precisa acessar o switch e informá-lo que o computador com endereço X está localizado na porta Y. O switch possui uma tabela dinâmica que automaticamente associa endereços físicos aos computadores conectados.

A segmentação realizada pelo dispositivo possibilita que diferentes pares possam conversar simultaneamente na rede, sem colisões. A transmissão para canais específicos faz com que uma rede com switch possua topologia física e lógica em estrela. **Além disso, o Hub funciona apenas em half-duplex e o Switch em full-duplex. Dessa forma, a rede fica menos congestionada com o fluxo de informações e é possível estabelecer uma série de conexões paralelas.**

Por fim, é importante tomar cuidado com a utilização do termo switch, visto que pode significar coisas distintas. Existe Switch de Camada 2 ou Switch de Camada 3. *Que camada é essa, professor?* Um Switch de Camada 3 é utilizado na camada de rede, funcionando de forma mais similar a um roteador; e um Switch de Camada 2 opera nas camadas física e de enlace. Veremos essas camadas na próxima aula. **Se a questão não especificar, considere se tratar do Switch de Camada 2.**

Em suma: um switch (comutador) é um equipamento de rede semelhante a uma **ponte com múltiplas portas, capaz de analisar dados que chegam em suas portas de entrada e filtrá-los para repassar apenas às portas específicas de destino**. Além disso, ele tem recursos como autonegociação e autoaprendizagem, sendo capaz de funcionar em *full duplex*[6]. A representação de um Switch é apresentada abaixo:



CARACTERÍSTICA	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede projetado para encaminhar pacotes de dados com base nos Endereços MAC (Media Access Control).
CAMADA OSI	Camada 2 (Enlace).
VANTAGENS	Rápido encaminhamento de pacotes; reduz colisões na rede; segmenta o tráfego da rede em diferentes portas; suporta redes com fio e sem fio; melhora o desempenho da rede.

[6] Cada porta do switch possui um buffer (uma espécie de banco de memória) em que os dados são armazenados/enfileirados, não ocorrendo colisões, portanto não necessitando utilizar o Protocolo CSMA/CD.

DESVANTAGENS	Mais caro do que um hub; requer configuração e gerenciamento adequados; pode ter uma curva de aprendizado para administradores de rede.

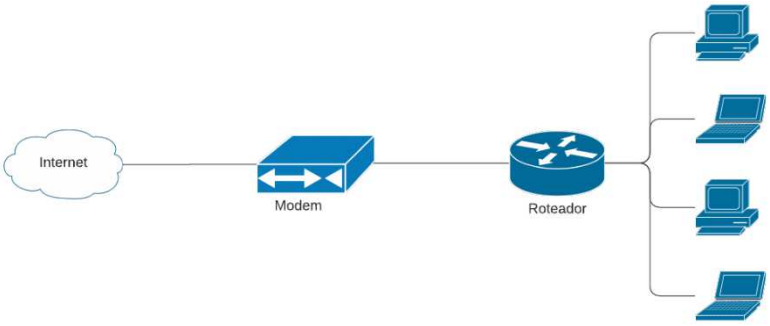
Router (Roteador)

INCIDÊNCIA EM PROVA: ALTA

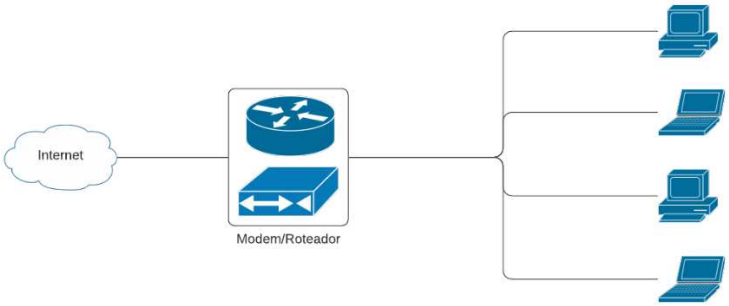


Os roteadores são equipamentos que permitem interligar redes diferentes e escolher a melhor rota para que uma informação chegue ao destino. Esse dispositivo encaminha ou direciona pacotes de dados entre redes de computadores, geralmente funcionando como um elo entre redes diferentes. Hoje em dia, são muito comuns em residências para permitir a conexão entre redes locais domésticas (Rede LAN) e a Internet (Rede WAN).

Quem é mais velho se lembrará que uma configuração muito comum em casas antigamente consistia em um modem, um roteador e até quatro dispositivos. **O modem era responsável por receber o sinal de internet (veremos em detalhes mais adiante) e o roteador era responsável por interligar os quatro computadores à internet.** *Por que somente quatro dispositivos, professor?* Porque era o número máximo de portas em um roteador comum.

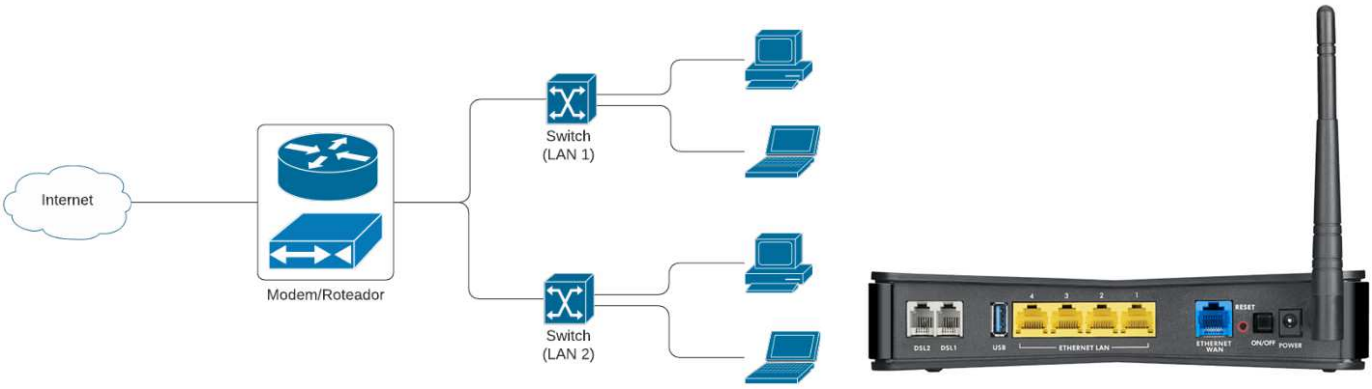


Atualmente, nós estamos na era dos combos, isto é, um único provedor fornece Internet, Telefone e TV a Cabo (Ex: NET/Claro, GVT/Vivo, etc). Nesse caso, um único aparelho condensa as funções de modem e roteador – você provavelmente tem esse aparelho na sua casa! Em geral, um cabo coaxial branco entra nesse dispositivo, que possui geralmente quatro portas. Em empresas, nós temos geralmente uma configuração um pouco diferente.



Primeiro, uma empresa pode ter uma centena de computadores, logo as quatro portas de um roteador não seriam suficientes. Além disso, ela pode ter redes locais diferentes dentro dela por motivos de segurança. *Como assim, Diego?* **Galera, é interessante separar dados sensíveis de dados não sensíveis em redes diferentes. Caso a rede de dados não sensíveis seja invadida, não afetará a rede de dados sensíveis, por exemplo.**

Dessa forma, uma terceira configuração pode ter um modem/roteador e dois switches, segmentando a rede local em duas, conforme apresenta a imagem à esquerda. Já na imagem à direita, temos a parte traseira de um roteador: observem que temos quatro portas em amarelo e uma porta azul. As portas amarelas – Portas LAN – são dedicadas a conectar equipamentos da rede interna e a porta azul – Porta WAN – é utilizada para conectar uma rede externa (Internet).



Um roteador pode ser com fio ou sem fio (wireless). Atualmente, a maioria dos roteadores do mercado são sem fio – apesar de permitirem conexão cabeada também. Nós já sabemos que um roteador é capaz de interligar redes diferentes. **No entanto, um roteador wireless é um dispositivo mais flexível, podendo trabalhar em outros três modos diferentes: Hotspot, Access Point ou Repetidor de Sinal.** Vamos falar sobre cada um deles...

No modo Hotspot, o roteador tem o simples objetivo de oferecer acesso à internet. *Como assim, Diego?* Vamos imaginar que você enjoou de estudar informática em casa e resolveu levar seu notebook e estudar em uma cafeteria. Você chama o garçom, pede um espresso, uma água e... a senha do wi-fi! Vamos supor que a rede local da cafeteria é composta por cinco computadores, uma impressora e um banco de dados conectados em rede.

Ora... se o roteador wireless da cafeteria estiver configurado em modo hotspot, eu terei acesso simplesmente à internet, mas não terei acesso a notebooks de outros clientes ou aos

computadores, impressora e banco de dados da cafeteria. **O hotspot é – apenas e tão somente – um local onde uma rede sem fio está disponível para ser utilizada.** Alguns estabelecimentos oferecem de forma gratuita (bares, restaurantes, etc) e outros são pagos (aeroportos e hotéis).

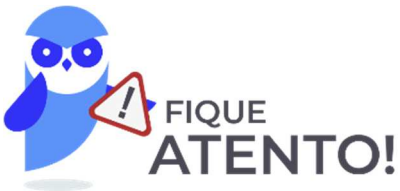


Atualmente, é possível configurar até o próprio celular como um hotspot. *Quem aí já compartilhou o 4G do celular com um amigo?* Se sim, você configurou seu celular como um hotspot! Agora eu gostaria que vocês fizessem um experimento social: na próxima vez que vocês forem a um bar, restaurante, academia, estádio, universidade, aeroporto, etc, olhem para o teto ou para as paredes! **Eu tenho certeza que vocês encontrarão vários dispositivos como esses da imagem ao lado: Hotspots.**

O segundo modo de configuração de um roteador wireless é como Access Point. **Nesse caso, a ideia é estender os recursos da rede local para a rede sem fio.** Quando um roteador wireless é configurado no modo Hotspot, a ideia era oferecer acesso à internet e, não, aos outros recursos de rede compartilhados. Já quando ele é configurado no modo Access Point, ele oferece – sim – acesso a todos os recursos da rede.

Apesar dessa diferença, é importante mencionar que um Hotspot pode ser considerado um Access Point de acesso público – algumas provas os consideram sinônimos. Por fim, esse roteador wireless pode também ser configurado como repetidor de sinais. *Sabe quando você se desloca da sala um quarto distante ou de um andar para outro em uma casa e o sinal da wi-fi piora vertiginosamente?* Pois é, o repetidor vai regenerar o sinal e propagá-lo por uma distância maior.

Apesar de existirem essas configurações do roteador wireless, é possível comprar um Hotspot, Access Point ou Repetidor de Sinal separadamente. No entanto, é importante salientar que todo roteador wireless é capaz de funcionar como um Hotspot, Access Point ou Repetidor de Sinal, porém o contrário nem sempre é verdadeiro. Por exemplo: nem todo Access Point é capaz de funcionar como um roteador. *Fechou?*



QUAL É A DIFERENÇA ENTRE UM ROTEADOR E UM ACCESS POINT?

Uma pergunta frequente no fórum de dúvidas é: qual é a diferença entre um Roteador e um Access Point? Em primeiro lugar, nós já vimos que um Roteador pode ser configurado para funcionar como um Access Point. Em segundo lugar, um Roteador tem o objetivo de interligar redes diferentes. Já um Access Point tem o objetivo de estender os recursos da rede local para a rede sem fio.

CARACTERÍSTICA	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede que filtra, encaminha e controla pacotes de dados entre redes, determinando a melhor rota com base em endereços IP.
CAMADA OSI	Camada 3 (Rede).
VANTAGENS	Roteia tráfego entre redes, permitindo conectividade inter-redes; ajuda a dividir redes em sub-redes para melhor organização e segurança.
DESVANTAGENS	Pode ser mais complexo de configurar em comparação com switches/hubs; pode ser um ponto único de falha se não houver redundância.

Modem

INCIDÊNCIA EM PROVA: MÉDIA



O Modem (Modulador/Demodulador) é um dispositivo crucial na comunicação entre computadores e a internet, especialmente quando se utiliza a infraestrutura de linha telefônica. Esse dispositivo atua como um tradutor, convertendo os dígitos binários de um computador em sinais analógicos para transmissão em linhas telefônicas e vice-versa. Existem três tipos principais de modems:

- **Modem de Acesso Discado:** conecta-se à internet via linha telefônica tradicional. Era comum antes do advento da banda larga, mas tinha limitações como velocidade lenta e ocupação da linha telefônica durante o uso.

- **Modem ADSL (Asymmetric Digital Subscriber Line):** oferece acesso à internet de banda larga através de linhas telefônicas, mas com uma tecnologia mais avançada que permite o uso simultâneo da linha telefônica para chamadas.

- **Cable Modem:** usa cabos coaxiais, geralmente fornecidos por empresas de TV a cabo, para acesso à internet. Esses modems podem ser combinados com serviços de TV e telefone, oferecendo um "combo" de serviços através de um único cabo.

Uma dúvida que aparece de vez em quando no fórum trata de Gateway. Esse equipamento tem a função de interligar redes com arquiteturas e protocolos diferentes permitindo que essas duas redes distintas possam se comunicar, realizando a conversão entre os protocolos de cada uma das redes – qualquer equipamento que realize essa função genericamente é chamado de gateway. Ele geralmente trabalha em todas as camadas da Arquitetura TCP/IP (veremos em outra aula).

MODEM	DESCRIÇÃO

DEFINIÇÃO	Dispositivo que modula e demodula sinais para permitir a comunicação digital através de meios analógicos, como linhas telefônicas.
CAMADA OSI	Camada 1 (Física) e 2 (Enlace).
VANTAGENS	Permitem a comunicação de dados através de redes analógicas; são amplamente utilizados para acesso discado à Internet; facilitam a conexão com redes de banda larga.
DESVANTAGENS	Velocidade de transmissão baixa comparada com tecnologias de banda larga; suscetíveis a ruídos em linhas telefônicas; largura de banda e capacidade de transmissão limitadas.

Padrões de Redes

Seus lindos... existe lá nos Estados Unidos um instituto bastante famoso chamado IEEE (*Institute of Electrical and Electronics Engineers*)! Trata-se da maior organização profissional do mundo dedicada ao avanço da tecnologia em benefício da humanidade. **Esse tal de IEEE (lê-se "I3E") mantém o Comitê 802, que é o comitê responsável por estabelecer padrões de redes de computadores**. *Professor, o que seriam esses padrões de redes?*

Padrões de Redes são uma especificação completamente testada que é útil e seguida por aqueles que trabalham com Internet – trata-se de uma regulamentação formal que deve ser seguida. **O Padrão IEEE 802 é um grupo de normas que visa padronizar redes locais e metropolitanas nas camadas física e de enlace do Modelo OSI.** Os padrões de rede descrevem vários aspectos das redes, incluindo:

ASPECTOS	DESCRIÇÃO
MEIO DE TRANSMISSÃO	Podem especificar se a rede é com ou sem fio. Também podem especificar a largura de banda e as características físicas do meio de transmissão.
TOPOLOGIA	Podem definir a topologia da rede, como barramento, estrela, anel ou malha.
PROTOCOLOS	Podem definir protocolos de comunicação que os dispositivos de rede devem seguir para trocar dados, como protocolos de camada física e protocolos de camada de aplicação.
SEGURANÇA	Podem incluir diretrizes de segurança, como criptografia e autenticação, para proteger a rede contra ameaças.
COMPATIBILIDADE	Garantem que os dispositivos de diferentes fabricantes possam funcionar juntos na mesma rede, desde que sigam o mesmo padrão.
DESEMPENHO	Podem abordar questões de desempenho, como largura de banda, latência e qualidade de serviço.

Na tabela a seguir, é possível ver diversos padrões diferentes de redes de computadores que são comuns em provas de concurso:

PADRÃO	NOME

IEEE 802.3	Ethernet (LAN)[7]
IEEE 802.5	Token Ring (LAN)
IEEE 802.11	Wi-Fi (WLAN)
IEEE 802.15	Bluetooth (WPAN)
IEEE 802.16	WiMAX (WMAN)
IEEE 802.20	Mobile-Fi (WWAN)

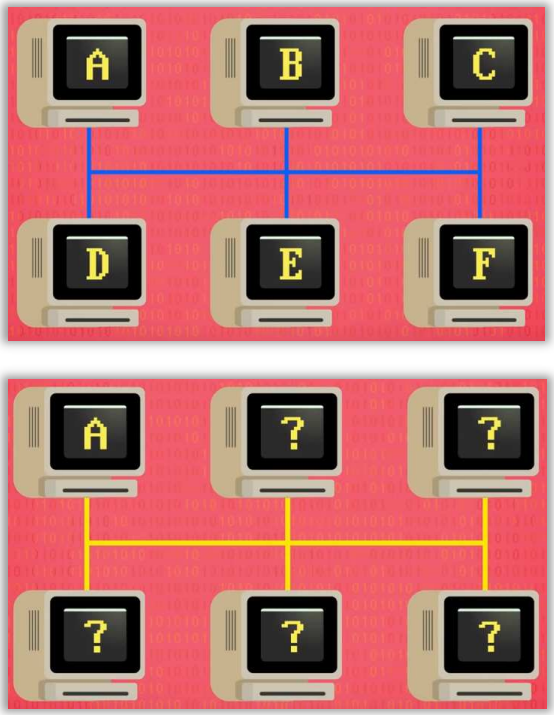
Padrão Ethernet (IEEE 802.3)

INCIDÊNCIA EM PROVA: ALTA

Ethernet é um conjunto de tecnologias e padrões que permite que dois ou mais computadores se comuniquem utilizando meios cabeados em uma Rede de Área Local (LAN). Notem que eu afirmei que é um conjunto de tecnologias e padrões, portanto nós vamos estudá-los por partes. Em relação à topologia utilizada, pode ser em Barramento ou Estrela. Vamos falar inicialmente sobre Padrão Ethernet com topologia em barramento.

Nós já sabemos que essa topologia conecta todos os dispositivos a um único cabo comum (*backbone*). Quando um computador deseja transmitir dados a outro computador, ele traduz os dados em sinais elétricos e os envia pelo cabo. **Como o cabo é compartilhado, todo computador que estiver conectado à rede receberá os dados transmitidos, uma vez que a difusão ocorre em *broadcast*.** *Lembram?*

[7] Sendo rigorosamente técnico, há uma diferença entre IEEE 802.3 e Ethernet relacionado a um campo de endereço de origem e destino, mas eu só vi essa diferença ser cobrada em prova uma vez até hoje. Além disso, para lembrar da numeração do Padrão Ethernet, lembre-se de: **ETHERNET → 3TH3RN3T**; e para lembrar da numeração do Padrão Wi-Fi (que também cai bastante), lembre-se de: **WI-FI → W1-F1**.

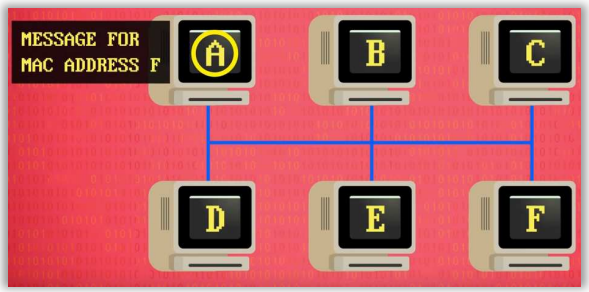


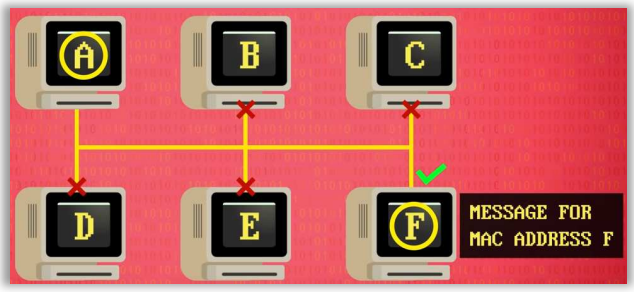


Na imagem acima, temos o *backbone* em azul porque nenhum sinal está sendo transmitido; e na imagem abaixo, temos o *backbone* em amarelo onde o sinal está sendo transmitido. **Notem que o *backbone* está todo amarelo porque – como a transmissão ocorre em *broadcast* – todas as máquinas o recebem.** Por outro lado, apesar de todos os computadores receberem os dados enviados, apenas o destinatário original poderá processá-los.

Professor, como os computadores vão saber se os dados recebidos de outro computador são direcionados a eles ou não? **Para resolver esse problema, a Ethernet requer que cada computador tenha um único endereço físico – também chamado de Endereço MAC (*Media Access Control Address*).** Esse endereço único é colocado em um prefixo junto com os dados a serem transmitidos (vejam na imagem anterior o Endereço MAC do meu computador).

Dessa forma, computadores na rede continuam recebendo os dados, mas só os processam quando eles verificam que é o endereço deles que está contido no prefixo. Vejam abaixo que o Computador A deseja enviar uma mensagem para o Computador F. Para tal, ele coloca o Endereço MAC do Computador F no prefixo da mensagem, que será processada por esse computador e ignorada pelos outros. Toda placa de rede de um computador possui um Endereço MAC único!





O termo genérico para essa abordagem vista acima é *Carrier Sense Mutiple Access* (CSMA), também conhecido como Acesso Múltiplo com Detecção de Portadora. Em outras palavras, trata-se de um protocolo utilizado na Ethernet para monitorar o meio de transmissão e evitar colisões quando ocorrem múltiplos acessos. Nós já estudamos esse problema no tópico de topologia em barramento, mas agora vamos detalhar um pouco mais.



Infelizmente, utilizar um meio de transmissão compartilhado possui desvantagens. Quando o tráfego na rede está baixo, computadores podem simplesmente esperar que ninguém esteja utilizando o meio de transmissão para transmitir seus dados. No entanto, à medida que o tráfego aumenta, a probabilidade de que dois ou mais computadores tentem transmitir dados ao mesmo tempo também aumenta. **Quando isso ocorre, temos uma colisão!**

A colisão deixa os dados ininteligíveis, como duas pessoas falando ao telefone ao mesmo tempo – ninguém se entende! Felizmente, computadores podem detectar essas colisões por meio de um protocolo chamado *Collision Detection*. Quando duas pessoas começam a falar ao mesmo tempo ao telefone, a solução mais óbvia para resolver esse problema é **parar a transmissão, esperar em silêncio e tentar novamente**. Ora... aqui é exatamente do mesmo jeito!

O problema é que o outro computador também vai tentar a mesma estratégia. Além disso, outros computadores da mesma rede podem perceber que o meio de transmissão está vazio e tentar enviar seus dados. *Vocês percebem que isso nos leva a mais e mais colisões?* Pois é, mas a Ethernet possui uma solução simples e efetiva para resolver esse problema. **Quando um computador detecta uma colisão, eles esperam um breve período de tempo antes de tentar novamente**.

Esse período poderia ser, por exemplo, um segundo! *Professor, se todos os computadores esperarem um segundo, isso não vai resultar no mesmo problema anterior?* Isso é verdade! Se todos esperarem um segundo para retransmitir, eles vão colidir novamente após um segundo. **Para resolver esse problema, um período aleatório – chamado de backoff – é adicionado: um computador espera 1,3 segundos; outro espera 1,5 segundos; e assim por diante.**

Lembrem-se de que – para o mundo dos computadores – essa diferença de 0,2 segundos é uma eternidade. Logo, o primeiro computador verá que o meio de transmissão não está sendo utilizado e pode transmitir seus dados. 0,2 segundos depois, o segundo computador verá que o meio de transmissão não está sendo utilizado e poderá transmitir seus dados. *Professor, calma aí, isso ajuda bastante, mas e se tivermos muitos computadores não resolverá o problema!*

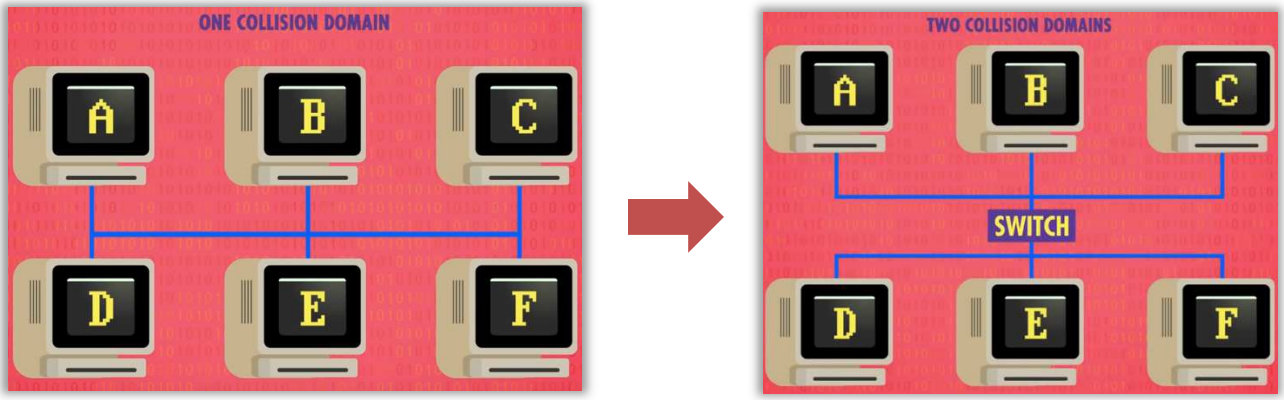
Para resolver esse problema, nós temos mais um truque! Sabemos que se um computador detecta uma colisão, ele esperará um segundo mais um tempo aleatório. Se mesmo assim houver outra

colisão, pode ser que a rede esteja congestionada, logo ele não esperará mais um segundo, esperará dois segundos. Se mesmo assim houver colisão, esperará quatro segundos. **Se continuar havendo colisões, esperará oito segundos, e assim por diante até conseguir transmitir**.

Você – meu melhor aluno – vai continuar argumentando que isso não resolve o problema para muitos computadores. Imaginem uma universidade inteira com 1000 alunos acessando simultaneamente a rede local em um, e apenas um, cabo compartilhado. *Complicado, não é?* **A topologia em barramento possui várias limitações, tanto que atualmente está em completo desuso.** A coisa está ficando legal...

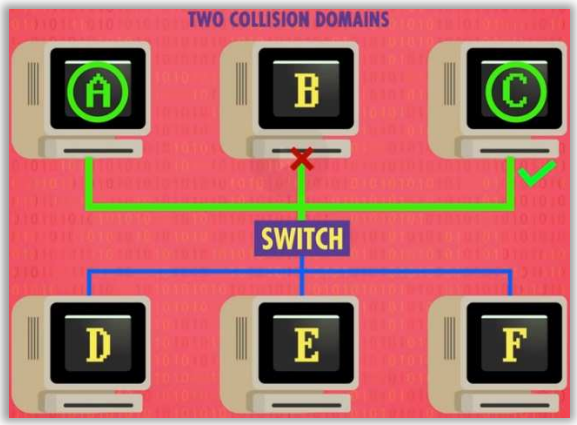
Para reduzir o número de colisões e melhorar a eficiência, nós precisamos diminuir a quantidade de dispositivos nos meios de transmissão compartilhados. Nesse momento, entra o conceito de Domínio de Colisão. *O que é isso, Diego?* Trata-se de uma área onde pacotes podem colidir uns contra os outros. A ideia aqui é segmentar a nossa rede em domínios de colisão menores, reduzindo – portanto – a probabilidade de colisões.

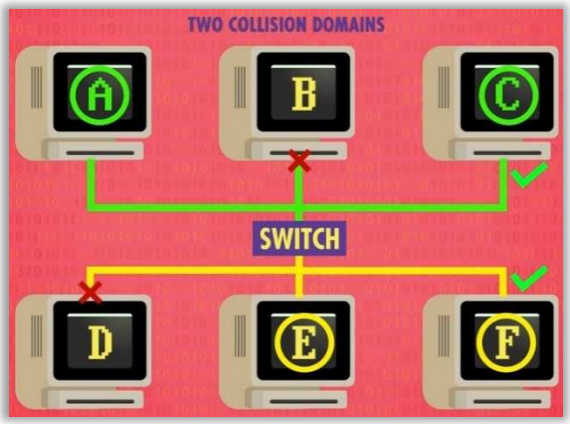
> *Pequena analogia para entender o que é um domínio de colisão: Imagine um corredor estreito em uma escola, em que os alunos estão indo para as aulas. Cada aluno representa um dispositivo de rede, como um computador. O corredor é a rede de cabos físicos ou meio compartilhado (por exemplo, um cabo Ethernet) que permite que os dispositivos se comuniquem.*
>
> *Dessa forma, um domínio de colisão em uma rede Ethernet é como o corredor estreito em que os dispositivos precisam coordenar seu acesso para evitar colisões e permitir uma comunicação eficiente. Cada domínio de colisão representa uma área onde as colisões podem ocorrer, e as redes Ethernet foram projetadas para minimizar essas colisões e tornar a comunicação confiável.*



No exemplo anterior, nós tínhamos seis computadores conectados em um único meio de transmissão compartilhado, logo nós tínhamos um único domínio de colisão. Para reduzir a probabilidade de colisões, nós podemos segmentar a rede em dois domínios de colisão. *Como,*

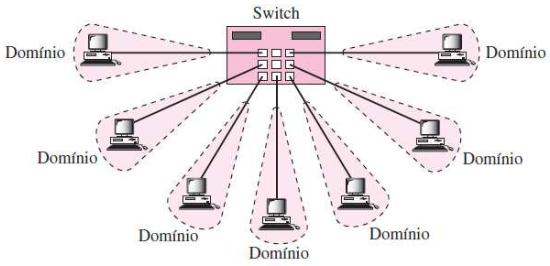
Diego? Nós podemos utilizar uma topologia em estrela com uso de um switch[8]. **Ele segmentará nossa rede em duas partes e ficará posicionado entre elas**.

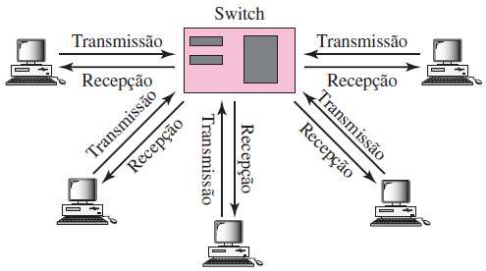




Dessa forma, ele só passará dados para o outro domínio de colisão se a mensagem for destinada a algum computador presente nesse domínio de colisão. *Como ele faz isso, professor?* Ele guarda uma lista de Endereços MAC dos computadores de cada rede. **Assim, se o Computador A deseja transmitir dados para o Computador C, o switch não encaminhará os dados para o outro domínio de colisão – como mostra a imagem acima à esquerda**.

Notem que, se o Computador E quiser transmitir dados para o Computador F ao mesmo tempo que o Computador A transmite dados para o Computador C, a rede estará livre e as duas transmissões poderão ocorrer simultaneamente porque temos duas comunicações ocorrendo em dois domínios de colisão diferentes – como mostra a imagem acima à direita. **Percebam que os domínios de colisão criados reduziram as chances de colisões na rede.**



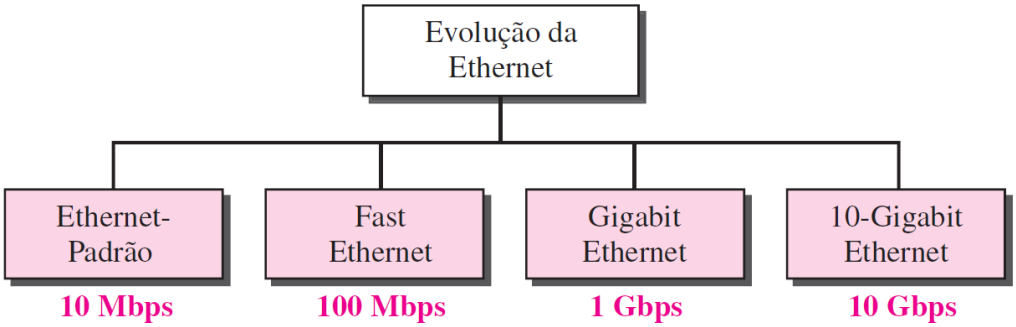


E digo mais: é possível criar um domínio de colisão para cada uma das portas de um switch (conforme apresenta à esquerda). Dessa forma, é possível eliminar toda e qualquer colisão! **Além disso, lembremos que o switch trabalha em full-duplex, ou seja, é capaz de enviar e receber dados simultaneamente, logo não há nenhuma chance de haver colisões!** A probabilidade foi reduzida à zero e o nosso problema foi resolvido! :)

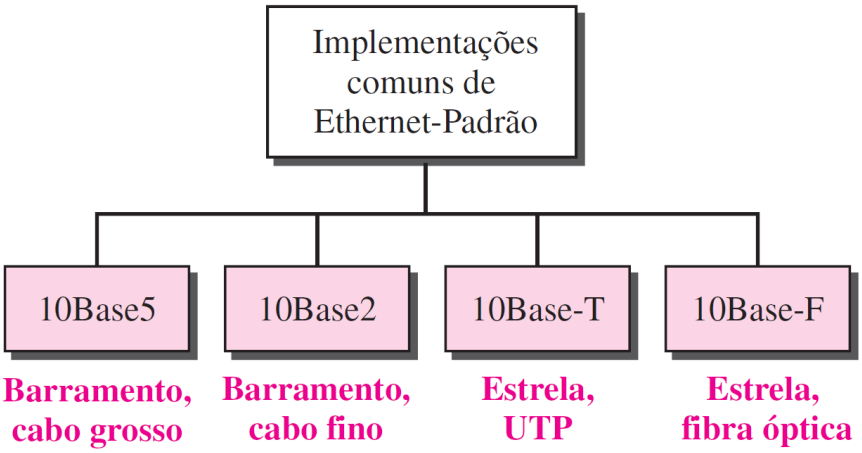
[8] Utilizar a topologia em estrela com um hub não adiantaria nada porque esse dispositivo tem topologia lógica em barramento.

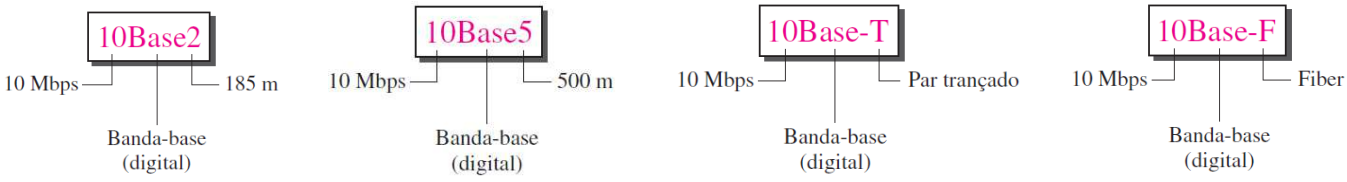
O que temos até agora sobre o Padrão Ethernet? **Sabemos que ele pode funcionar por meio da topologia em barramento.** Como pode haver colisões, entra em ação o CSMA/CD, que utiliza um algoritmo para evitar colisões. Ainda assim, sabemos que a topologia em barramento tem diversas limitações, inclusive em relação a colisões em um contexto de uma rede com muitos computadores. Podemos utilizar a topologia em estrela com um hub, mas retornaríamos ao mesmo problema.

Para superar essa limitação, podemos utilizar a topologia em estrela com um switch. *Por quê?* Porque ele funciona em full-duplex e segmenta a rede em domínios de colisão – eliminando chances de colisões e o seu consequente congestionamento da rede. Tudo isso que falamos diz respeito à Ethernet-Padrão, porém existem outras gerações: Ethernet-Padrão (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps) e 10 Gigabit Ethernet (10 Gbps). Estudaremos cada uma delas...



A Ethernet-Padrão possui quatro implementações comuns apresentadas na imagem seguinte. *Vamos entender isso melhor?* Note que temos um padrão: **NúmeroBaseNúmero ou NúmeroBase-Letra**. Em laranja, temos a taxa de transmissão (Ex: **10Base2** trabalha com 10Mbps); em azul, temos a distância máxima (Ex: **10Base5** percorre no máximo 500 metros); em verde, temos o tipo de enlace (Ex: **10Base5** é cabo coaxial, **10Base-T** é par trançado e **10Base-F** é fibra óptica).





Esses se referem à Ethernet-Padrão! *E quanto às outras evoluções?* **Bem, temos a Fast Ethernet, que é compatível com as versões anteriores da Ethernet-Padrão, mas é capaz de transmitir dados dez vezes mais rápido, a uma velocidade de 100 Mbps.** Ainda havia necessidade de uma taxa de dados mais alta, logo surgiu o projeto do protocolo Gigabit Ethernet (1.000 Mbps ou 1Gbps). Por fim, surgiu o 10 Gigabit (10 Gbps).

EVOLUÇÃO DOS PADRÕES ETHERNET	
PADRÃO (CABO DE PAR TRANÇADO OU FIBRA ÓPTICA)	PADRÃO – TAXA MÁXIMA DE TRANSMISSÃO
Ethernet	10BASE-T / 10 Mbps
Fast Ethernet	100BASE-T / 100 Mbps
Gigabit Ethernet	1000BASE-T / 1000 Mbps
10G Ethernet	10GBASE-T / 10000 Mbps



Sabendo que Mega (M) = Milhão, Giga (G) = Bilhão e que 1G = 1000M, fica mais fácil lembrar que a Gigabit Ethernet tem a velocidade de 1000Mbps e que a 10G Ethernet tem a velocidade de 10.000Mbps. Além disso, uma largura de 100Gbps - por exemplo - permite transmitir até 100 Bilhões de bits por segundo (100.000.000.000 bits/segundo).

VANTAGENS DO PADRÃO ETHERNET	DESVANTAGENS DO PADRÃO ETHERNET
Trata-se de uma das tecnologias de rede mais amplamente adotadas em todo o mundo.	Em redes Ethernet compartilhadas, as colisões de dados podem ocorrer, diminuindo o desempenho.
É relativamente fácil configurar e implantar, tornando-as acessíveis a muitas organizações.	Pode ser desafiador de escalar para redes maiores ou mais complexas.
Equipamentos e infraestruturas são geralmente mais acessíveis do que algumas alternativas.	Podem requerer cabeamento mais complexo e dispendioso.
Oferece boas taxas de transferência de dados e largura de banda adequada para muitos casos de uso.	Em redes Ethernet não criptografadas, os dados podem ser mais vulneráveis à interceptação.
A maioria dos dispositivos é compatível com Ethernet, facilitando a conectividade.	Em redes congestionadas, o desempenho do Ethernet pode diminuir.
Tende a ter latência baixa, o que é importante para aplicativos sensíveis à latência.	Não é adequada para redes sem fio, o que pode ser um problema em ambientes móveis.

Padrão Token Ring (IEEE 802.5)

INCIDÊNCIA EM PROVA: MÉDIA

O **Padrão Token Ring** é um método de comunicação de rede cabeada que foi bastante popular até o início da década de 90, competindo com o Padrão Ethernet. Suas características incluem:

- **Taxa de Transmissão de Dados:** originalmente 4 Mbps.
- **Comunicação Unidirecional (Simplex):** o sinal circula em uma única direção.

- **Arquitetura Ponto-a-Ponto:** cada estação de trabalho conecta-se diretamente à outra.
- **Topologia Lógica em Anel:** as estações estão conectadas em forma de anel.

A principal característica do Token Ring é a utilização de um "token" para controlar a transmissão de dados. **Este token é como um "envelope" ou uma "autorização" que permite a uma estação de trabalho transmitir dados.** Funciona assim: o token circula pela rede de dispositivo em dispositivo; quando um dispositivo pega o token, ele tem o direito de transmitir dados; apenas um dispositivo pode transmitir dados por vez, prevenindo colisões de dados.

Esta dinâmica é similar a uma corrida de revezamento, onde o token é o bastão, o dispositivo com o token é o corredor com o bastão, e os dados transmitidos são a mensagem que o corredor carrega. O Token Ring é conhecido por sua confiabilidade e baixa latência, principalmente devido à ausência de colisões. No entanto, tende a ser mais caro e menos flexível em termos de escalabilidade em comparação com a Ethernet.

A Ethernet, por outro lado, é mais acessível, fácil de implementar e altamente escalável, embora possa sofrer de colisões em redes congestionadas. A escolha entre Token Ring e Ethernet depende das necessidades específicas de uma rede e das limitações orçamentárias. Enquanto o Token Ring já foi uma opção popular, a Ethernet acabou predominando devido ao seu custo mais baixo e maior facilidade de implementação e escalabilidade. Vejamos suas principais vantagens e desvantagens:

VANTAGENS DO PADRÃO TOKEN RING	DESVANTAGENS DO PADRÃO TOKEN RING
O Token Ring é altamente confiável devido à sua estrutura em anel, que evita colisões de dados.	A implementação inicial do Token Ring pode ser mais cara devido ao hardware específico.
A topologia do anel elimina colisões de dados, o que leva a uma transmissão de alta qualidade.	Requer configuração complexa e habilidades técnicas para instalação e manutenção.
O tempo de latência é baixo, pois os dispositivos podem transmitir quando possuem o token.	Menos flexível do que outras topologias, tornando difícil adicionar ou mover dispositivos.
Permite a priorização de tráfego, garantindo que dados críticos sejam transmitidos primeiro.	A taxa de transmissão é geralmente mais baixa em comparação com tecnologias mais recentes.
Escalabilidade limitada, o que a torna menos adequada para redes maiores e em constante crescimento.	O Token Ring é um padrão em declínio, com pouca inovação e suporte em comparação com Ethernet.

Por fim, vejamos agora uma pequena comparação entre os padrões **Ethernet** e **Token Ring** na tabela seguinte:

CARACTERÍSTICA	PADRÃO TOKEN RING	PADRÃO ETHERNET
TOPOLOGIA	Usa uma topologia em anel, onde os dispositivos são conectados em círculo e os dados são transmitidos em sequência – um dispositivo após o outro.	Usa uma topologia em estrela ou em barramento. Os dispositivos são conectados a um hub ou switch central.
DESEMPENHO	Oferece um desempenho consistente devido à ausência de colisões de dados. A largura de banda é dividida igualmente entre os dispositivos no anel.	Pode ter colisões de dados, especialmente em redes ocupadas. A largura de banda é compartilhada entre todos os dispositivos na rede.

CUSTO	Geralmente é mais caro devido ao hardware específico necessário, como conectores de cabo MAU (*Media Access Unit*).	Geralmente é mais econômico, pois o hardware é amplamente disponível e menos caro.
IMPLEMENTAÇÃO	Requer configuração mais complexa, como a definição de endereços de estação e prioridades de token.	É mais fácil de implementar, com menos requisitos de configuração.
ESCALABILIDADE	Pode ser menos flexível para adicionar ou remover dispositivos sem interromper a rede.	É escalável e permite adicionar dispositivos com facilidade, especialmente em redes comutadas.
POPULARIDADE	Foi popular nas décadas de 1980 e 1990, mas agora é menos comum, pois a Ethernet se tornou dominante.	É a tecnologia de rede mais amplamente usada e suportada, com constante evolução.

Padrão Wi-Fi (IEEE 802.11)

INCIDÊNCIA EM PROVA: ALTA

A comunicação móvel está entre as tendências mais significativas, e os usuários esperam estar conectados à internet de forma contínua. A maioria dos hotéis oferece conexão online aos seus hóspedes, e as companhias aéreas agora disponibilizam serviços de internet em muitos de seus aviões. **A demanda por comunicação móvel tem despertado interesse pelas tecnologias wireless, e muitos padrões wireless foram criados.**

O Padrão Wi-Fi – diferentemente dos padrões anteriores – não é cabeado. Logo, um usuário pode ficar conectado mesmo deslocando-se num perímetro geográfico mais ou menos vasto – redes sem fio fornecem mobilidade aos usuários. **O Padrão Wi-Fi se baseia em uma conexão que utiliza a tecnologia de radiodifusão e define uma série de padrões de transmissão e codificação para comunicações sem fio.**

Sim, o controle remoto da sua televisão é um dispositivo wireless porque é capaz de trabalhar com infravermelho. *Qual é o problema dessa tecnologia?* Se houver algum obstáculo entre o controle e o receptor da televisão, a luz não atravessa e a comunicação não acontece. **Em outras palavras, é necessário ter uma linha de visada, isto é, uma linha sem obstáculos entre o emissor e o receptor.** Além disso, essa tecnologia permite apenas uma comunicação de curto alcance.

Foi, então, que surgiu a tecnologia de radiodifusão. Para tal, é necessário ter antenas e uma frequência comum de onda eletromagnética. *Qual é a grande vantagem dessa tecnologia?* Se houver uma parede entre as antenas, a onda consegue atravessá-la. Claro, pessoal... se for uma parede de um metro de espessura, provavelmente ela não conseguirá atravessar. E mesmo para paredes normais, haverá alguma perda, mas a comunicação funcionará normalmente.

Logo, podemos afirmar que a tecnologia de radiodifusão não trabalha com linha de visada, porque é capaz de atravessar obstáculos. Em contraste com o infravermelho, essa tecnologia tem como grande vantagem a ampla mobilidade. Um dispositivo cabeado tem baixíssima mobilidade, assim como o infravermelho (por conta da linha de visada). Por outro lado, um dispositivo com tecnologia de radiodifusão permite o deslocamento sem perda considerável de sinal.

Além disso, as redes wireless – em regra – possuem taxas de transmissão bem mais baixas. Vocês já devem ter notado que um download no computador ocorre bem mais rápido que um download em seu celular. *E as desvantagens, professor?* **Bem, toda tecnologia wireless é mais vulnerável a interceptações que redes cabeadas.** *Como, Diego?* Para interceptar dados em uma rede cabeada, é necessário ter acesso direto ao cabeamento (Ex: invadindo a casa de alguém).

Já para interceptar dados em uma rede wireless, é possível fazer a interceptação bastando estar próximo. Aliás, por essa razão, todo cuidado é pouco com a rede wireless da sua casa...

RISCO	DESCRIÇÃO
ACESSO NÃO AUTORIZADO	Pessoas não autorizadas podem tentar se conectar à rede.
INTEREFERÊNCIA DE SINAL	Objetos físicos ou outras redes podem afetar a qualidade do sinal.
ATAQUES DE FORÇA BRUTA	Tentativas de adivinhar senhas por meio de força bruta.
MONITORAMENTO DE TRÁFEGO	Espionagem do tráfego de rede para coletar informações.
PONTO DE ACESSO FALSO	Atacantes podem criar redes falsas para enganar os usuários.
VULNERABILIDADES DE SEGURANÇA	Falhas de segurança podem ser exploradas por invasores.
ATAQUES DE NEGAÇÃO DE SERVIÇO	Sobrecarregar a rede para torná-la inacessível.
USO EXCESSIVO DE LARGURA DE BANDA	Usuários podem consumir toda a largura de banda disponível.
COMPARTILHAMENTO INADEQUADO	Compartilhamento de senhas com pessoas não confiáveis.
CONFIGURAÇÕES INADEQUADAS	Configurações de segurança fracas ou inadequadas.

Percebam que Wireless é diferente de WiFi. Wireless é qualquer tecnologia sem fio. **Wi-Fi (WIreless-FIdelity)** é uma marca registrada baseada no Padrão Wireless IEEE 802.11 que permite a comunicação entre computadores em uma rede sem fio (vejam que o logo possui um TM – TradeMark). Todo Wi-Fi é wireless, mas nem todo wireless é Wi-Fi.

Para resolver alguns destes riscos e proteger a integridade e a privacidade dos dados transmitidos, foram desenvolvidos mecanismos/protocolos de segurança, tais como:

MECANISMOS	DESCRIÇÃO
WEP WIRED EQUIVALENT PRIVACY	O WEP foi um dos primeiros protocolos de segurança usados em redes Wi-Fi. No entanto, ele é considerado inseguro atualmente. Ele usa uma chave de criptografia compartilhada entre o roteador e os dispositivos para criptografar os dados que são transmitidos, mas tem vulnerabilidades que tornam relativamente fácil para um atacante comprometer a segurança da rede e acessar os dados. Devido a essas fraquezas, ele não é mais recomendado para uso.

WPA WI-FI PROTECTED ACCESS	O WPA foi desenvolvido para substituir o WEP e corrigir suas vulnerabilidades. Ele introduziu melhorias significativas na criptografia e na autenticação, tornando a rede mais segura. No entanto, ao longo do tempo, ele também mostrou algumas vulnerabilidades. Ele usa uma chave de segurança e um método de autenticação mais forte do que o WEP.
WPA2 WI-FI PROTECTED ACCESS 2	O WPA2 é uma evolução do WPA e é atualmente um dos protocolos de segurança mais seguros para redes Wi-Fi. Ele utiliza criptografia forte e o padrão IEEE 802.11i para proporcionar uma camada sólida de segurança. O WPA2 oferece autenticação forte e protege os dados transmitidos na rede Wi-Fi de maneira eficaz. É altamente recomendado configurar sua rede Wi-Fi com WPA2 para garantir a segurança.
WPA3 WI-FI PROTECTED ACCESS 3	O WPA3 é uma versão mais recente que oferece ainda mais melhorias de segurança, incluindo criptografia mais forte e proteção contra-ataques de força bruta. Dessa forma, ao configurar uma rede Wi-Fi, é aconselhável usar WPA2 ou WPA3, se disponível, para garantir a proteção adequada.

É importante também notar que redes wireless podem trabalhar em dois modos de operação: **Ad-hoc** ou **Infraestrutura**. A tabela apresentada a seguir oferece uma visão geral das diferenças entre redes wireless ad-hoc e redes wireless de infraestrutura. A escolha entre esses dois tipos de redes depende das necessidades específicas de um cenário de implementação, com base na topologia, escalabilidade e requisitos de segurança.

CARACTERÍSTICA	MODO DE OPERAÇÃO AD-HOC	MODO DE OPERAÇÃO INFRAESTRUTURA
DESCRIÇÃO	Comunicação direta entre equipamentos e válida somente naquele momento, conexão temporária, apresentando alcance reduzido (Ex: 5m).	Comunicação que faz uso de equipamento para centralizar fluxo da informação na WLAN (Ex: Access Point ou Hotspot) e permite um alcance maior (Ex: 500m).
TOPOLOGIA DE REDE	Tipo de topologia de malha, onde cada dispositivo se conecta diretamente a outros dispositivos na rede.	Os dispositivos se conectam a um ponto de acesso central, como um roteador, que age como intermediário para encaminhar o tráfego.
CONFIGURAÇÃO DE REDE	Configurada sem a necessidade de um ponto de acesso central. Os dispositivos podem se comunicar diretamente uns com os outros.	Requer um ponto de acesso central (como um roteador) para gerenciar e encaminhar o tráfego na rede.
FLEXIBILIDADE	Mais flexível e útil em cenários onde não há acesso a uma infraestrutura de rede. Pode ser configurada rapidamente para conexões ponto a ponto.	Menos flexível em termos de implantação, pois depende de um ponto de acesso central. Ideal para redes com vários dispositivos em um único local.
ESCALABILIDADE	Menos escalável para grandes redes devido à complexidade de gerenciar muitas conexões ponto a ponto.	Mais escalável para redes maiores, pois o ponto de acesso central gerencia eficientemente as conexões.

SEGURANÇA	Geralmente menos segura, pois não existe um ponto de controle central. As comunicações podem ser vulneráveis a ataques.	Mais segura, pois o ponto de acesso central pode implementar medidas de segurança, como criptografia e autenticação, em nome de todos os dispositivos.
EXEMPLOS DE UTILIZAÇÃO	Redes temporárias de curto prazo, comunicação direta entre dispositivos móveis (por exemplo, compartilhamento de arquivos entre smartphones).	Redes domésticas, redes empresariais, hotspots públicos e ambientes onde múltiplos dispositivos precisam se conectar a uma rede comum.

Galera, alguém aí tem dispositivos da Apple? Se sim, vocês devem saber que existe uma funcionalidade chamada AirDrop, que permite a transferência de arquivos entre dispositivos Apple. Ao escolher o arquivo, o seu dispositivo identificará todos os outros dispositivos Apple próximos e uma conexão temporária será estabelecida. **Toda comunicação será descentralizada, direta entre os dispositivos, sem passar por um nó intermediário – logo, ela será ad-hoc[9].**

EVOLUÇÃO DO PADRÃO WI-FI (802.11)[10]		
PADRÃO	FREQUÊNCIA	TAXA MÁXIMA DE TRANSMISSÃO
IEEE 802.11B	2.4 Ghz	11 Mbps
IEEE 802.11A	5.0 Ghz	54 Mbps
IEEE 802.11G	2.4 Ghz	54 Mbps
IEEE 802.11N	2.4 ou 5.0 Ghz	150, 300 até 600 Mbps
IEEE 802.11AC	5.0 Ghz	500 Mbps, 1 Gbps ou +
IEEE 802.11AX (WIFI 6)	2.4 ou 5.0 Ghz	3.5Gbps a 14Gbps

Assim como nas redes cabeadas, as Redes Wi-Fi (WLAN – Wireless LAN) também sofreram diversas evoluções. Observem a tabela apresentada acima: os padrões 802.11b e 802.11a surgiram simultaneamente, porém utilizaram tecnologias diferentes – **um não é evolução do outro**. O Padrão 802.11b entrou no mercado antes do Padrão 802.11a, se consolidando no mercado no início da década passada. Em seguida, veio o Padrão 802.11g...

Ele mantinha a compatibilidade com o Padrão 802.11b e precedia o Padrão 802.11n, que permitia maiores taxas de transmissão e operação em duas bandas de frequências (Dual Band). *Por quê, professor?* Porque alguns aparelhos domésticos como controle de garagem, micro-ondas e bluetooth[11] trabalham na frequência de 2.4Ghz – isso poderia causar problemas de interferência. Como alternativa, ele pode trabalhar em outra frequência de onda de rádio!

Já o Padrão 802.11ac é uma novidade e pode vir a ser uma solução para tráfegos de alta velocidade, com taxas superiores a 1Gbps. Por fim, vejamos as principais vantagens e desvantagens:

[9] Em geral, Bluetooth tem um caráter mais ad-hoc e Wi-Fi tem um caráter mais de infraestrutura (apesar de não ser obrigatório).

[10] Para decorar a ordem, lembre-se da palavra **BAGUNÇA** (lembrando que CA é AC).

[11] Se você usa teclado sem fio, provavelmente embaixo dele está informando a frequência 2.4 Ghz. Verifiquem aí :)

VANTAGENS DO PADRÃO WI-FI	DESVANTAGENS DO PADRÃO WI-FI
Permite conectividade sem fio, possibilitando o uso de dispositivos em movimento, como laptops e smartphones.	Redes sem fio estão suscetíveis a interferências de outros dispositivos e redes, afetando o desempenho.
Fácil instalação e expansão de redes sem fio, evitando a necessidade de cabos físicos.	As redes sem fio podem ser vulneráveis a invasões se as medidas de segurança, como criptografia, não forem implementadas adequadamente.
Geralmente mais econômico do que a instalação de cabos em locais com vários dispositivos.	A velocidade da rede sem fio pode ser mais lenta do que as redes com fio, especialmente em locais congestionados.
Oferece opções de configuração, como redes ad-hoc e infraestrutura, para atender a diversas necessidades.	A qualidade da conexão pode ser afetada por obstáculos físicos, distância do roteador e interferências.
Disponível em várias faixas de frequência, permitindo cobertura em diferentes distâncias.	Redes sem fio podem apresentar maior latência do que redes com fio, o que pode ser crítico para algumas aplicações.

Padrão Bluetooth (IEEE 802.15)

INCIDÊNCIA EM PROVA: BAIXA



O Padrão Bluetooth tem o objetivo de integrar equipamentos periféricos. **Utilizado em Rede WPAN (Wireless Personal Area Network) – eles padronizam uma rede de baixo custo, curto alcance, baixas taxas de transmissão e sem fio**. Eles operam na faixa de 2.4 Ghz de forma ad-hoc por meio de sua unidade básica: uma piconet. Também conhecida como picorrede ou pequena rede, trata-se de um grupo de dispositivos bluetooth que compartilham um canal comum de rádio-frequência.

Uma *piconet* possui uma topologia em estrela e uma configuração ou arquitetura do tipo Mestre-Escravo[12]. No centro dessa estrela, um dispositivo mestre (também chamado de *master* ou primário) coordena a comunicação com até outros sete dispositivos escravos (também chamados de *slave* ou secundários). Um dispositivo *bluetooth* pode desempenhar qualquer um dos papéis, mas em uma *piconet* só pode haver um dispositivo mestre.

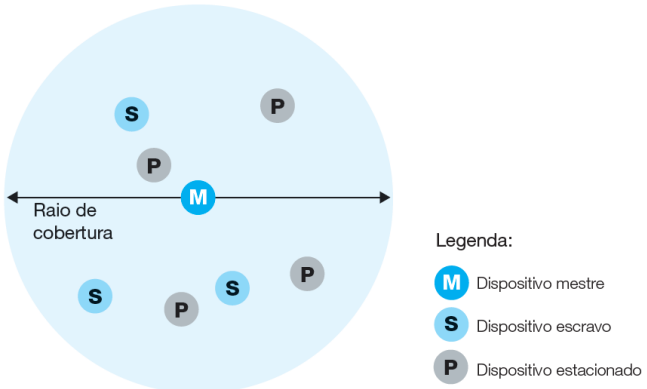
Além dos dispositivos escravos, a piconet também pode conter até 255 dispositivos estacionados. *Como assim, Diego?* Um dispositivo estacionado não pode se comunicar até que o dispositivo mestre altere seu estado de inativo para ativo. **Um dispositivo escravo que se encontre no estado estacionado permanece sincronizado com o mestre, porém não pode fazer parte da comunicação até deixar o estado estacionado.**

Como apenas oito estações podem estar ativas ao mesmo tempo em uma piconet, retirar uma estação do estado estacionado significa que uma estação ativa terá de ir para o estado estacionado. **Em suma, uma piconet é um conjunto de oito dispositivos: 1 mestre, até 7 escravos e até 255**

[12] Atenção: alguns alunos enviaram reclamações pedindo para retirar o termo mestre/escravo da aula por ter cunho racista. No entanto, esse é o termo técnico utilizado em bibliografias consagradas e em questões de concurso, logo infelizmente não há como retirá-lo.

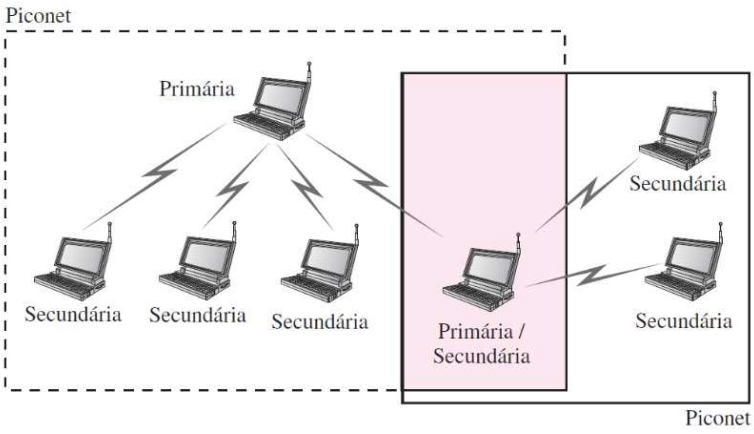


estacionados. Vejam na imagem seguinte um esquema em que um dispositivo mestre tem um raio de cobertura com três dispositivos escravos e quatro dispositivos estacionados.



E se eu disser para vocês que um dispositivo pode ser escravo em uma piconet e mestre em outra piconet? **Pois é, quando redes piconets se combinam, forma-se uma scatternet.** Vejam no esquema abaixo que temos duas piconets em que cada uma possui apenas uma estação primária (ou mestre). Em rosa, há um dispositivo que é uma estação secundária (escrava) da piconet à esquerda e uma estação primária (mestre) da piconet à direita. Temos, portanto, uma scatternet :)

Vamos deixar um pouquinho a teoria de lado e ver um exemplo mais prático. Imagine que você está em seu churrasco de posse após ter passado no sonhado concurso público! Só que o *churras* está desanimado porque não está rolando música alguma. Você – então – decide conectar seu smartphone (dispositivo mestre) a uma caixinha de som (dispositivo escravo). Lembrando que o seu smartphone também pode estar sendo mestre de outros dispositivos.



Na minha casa, meu computador (mestre) forma uma piconet por estar conectado ao meu teclado, ao meu mouse e ao meu fone de ouvido (escravos). Por outro lado, meu smartphone (mestre) também está conectado ao meu fone de ouvido (escravo). **Logo, meu fone de ouvido é escravo em duas piconets diferentes. Agora vamos imaginar que o meu computador (mestre) também está conectado ao meu smartphone (escravo). Nesse caso, eu terei uma scatternet...**

Vamos resumir esses pontos: (1) uma piconet possui apenas um dispositivo mestre; (2) um dispositivo só pode ser mestre de uma piconet; (3) um dispositivo pode ser escravo de mais de uma piconet; (4) um dispositivo pode ser mestre de uma piconet e escravo de outra piconet; (5) mestres só se comunicam com escravos e escravos só se comunicam com mestres – não há comunicação direta entre escravos ou comunicação direta entre mestres.

PADRÃO BLUETOOTH – WPAN 802.15		
CLASSE	POTÊNCIA	DISTÂNCIA
1	100 mW	Até 100 Metros
2	2.5 mW	Até 10 Metros
3	1 mW	Até 1 Metro

Por fim, vejamos na tabela seguinte as vantagens e desvantagens do padrão IEEE 802.15, que podem variar dependendo da implementação específica e do contexto de uso:

VANTAGENS DO PADRÃO BLUETOOTH	DESVANTAGENS DO PADRÃO BLUETOOTH
O padrão IEEE 802.15 é projetado para dispositivos de baixo consumo de energia, adequados para baterias.	As redes IEEE 802.15 têm alcance limitado, geralmente cobrindo apenas algumas dezenas de metros.
O padrão é ideal para comunicações de curto alcance, como sensores e dispositivos IoT em uma área próxima.	A largura de banda é limitada, o que a torna inadequada para aplicações que requerem alta taxa de transferência.
Permite a criação de redes de malha, onde dispositivos podem rotear dados entre si, aumentando a cobertura.	Pode ser afetada por interferências de outras redes sem fio e dispositivos, especialmente em ambientes lotados.
Usado em aplicações como IoT, sensores sem fio, automação residencial, dispositivos médicos e muito mais.	Não é a melhor opção para redes de grande escala, devido ao seu alcance limitado e limitações de largura de banda.
Substitui a necessidade de cabos em ambientes onde a conectividade com fio não é prática ou possível.	A segurança é uma preocupação, pois dispositivos dentro do alcance de uma rede IEEE 802.15 podem acessá-la.

Padrão WiMAX (IEEE 802.16)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

O Padrão WiMAX especifica um padrão sem fio de alta velocidade para Redes Metropolitanas (WMAN), criado por um consórcio de empresas para promover interoperabilidade entre equipamentos. Seu raio de comunicação com o ponto de acesso pode alcançar até cerca de 40 km, sendo recomendável para prover acesso à internet banda larga a empresas e residências em que o acesso ADSL ou HFC se torna inviável por questões geográficas.

Opera em faixas licenciadas do espectro de frequência (2,5GHz, 3,5GHz, 10,5GHz), portanto é necessário que empresas adquiram a concessão junto à ANATEL (Agência Nacional de Telecomunicações) para oferecer esse serviço. A potência percebida na estação-base, que

oferecerá o serviço, pode ter uma grande variação, o que influencia a relação sinal/ruído e, por isso, a tecnologia possui três esquemas de modulação (QAM-64, QAM-16 e QPSK).

Por fim, vejamos na tabela seguinte as vantagens e desvantagens do padrão IEEE 802.16, que podem variar dependendo da implementação específica e do contexto de uso:

VANTAGENS DO PADRÃO WIMAX	DESVANTAGENS DO PADRÃO WIMAX
O IEEE 802.16 pode fornecer serviços de banda larga em uma ampla área geográfica, incluindo áreas urbanas e rurais.	A implantação de infraestrutura 802.16 pode ser cara, especialmente em áreas com baixa densidade populacional.
Oferece largura de banda significativa, o que é adequado para aplicações que exigem altas taxas de transferência de dados.	Apresenta latência mais alta em comparação com tecnologias como fibra óptica, o que pode afetar aplicativos sensíveis à latência.
Suporta mobilidade, permitindo a conexão de dispositivos em movimento, como em veículos ou trens de alta velocidade.	Pode ser suscetível a interferências de obstáculos, como edifícios altos e outros dispositivos sem fio na mesma faixa.
Comparado com tecnologias como DSL, o IEEE 802.16 pode oferecer conectividade de banda larga em áreas rurais remotas.	A compatibilidade entre diferentes implementações de 802.16 nem sempre é garantida, o que pode levar a problemas de interoperabilidade.
Oferece QoS para garantir que diferentes tipos de tráfego, como voz e vídeo, tenham desempenho adequado na rede.	A gestão eficaz do espectro é necessária para evitar interferências e garantir o desempenho da rede.

INTERNET

Conceitos Básicos

INCIDÊNCIA EM PROVA: MÉDIA

A Internet surgiu como um sistema de redes interconectadas, desenvolvida principalmente para fins militares dos EUA durante a Guerra Fria, visando a comunicação segura em caso de guerra nuclear. Iniciada nos anos 50, a criação da **ARPA (Advanced Research Projects Agency)** foi um marco, buscando manter os EUA na vanguarda tecnológica militar, especialmente após a URSS lançar o Sputnik.

A **ARPANET**, precursora da Internet, começou nos anos 60 ligando universidades. Era uma rede de comutação por pacotes, uma inovação comparada à antiga comutação por circuito usada em telefonia. Na comutação por pacotes, a informação é dividida em blocos (pacotes) que viajam independentemente pela rede, tornando a comunicação mais eficiente e robusta contra falhas, ao contrário da comutação por circuito, que reservava uma linha dedicada para cada comunicação.

Esse método permite um uso mais eficiente dos recursos da rede, evitando que canais fiquem reservados quando não estão sendo usados. Por exemplo, enviar um arquivo grande é como dividir um relatório volumoso em vários envelopes para enviar pelos correios. Cada pacote pode seguir uma rota diferente e chegar em ordem distinta, sendo remontado na ordem correta no destino.

Com o crescimento da ARPANET, surgiu o desafio de manter listas atualizadas de endereços de computadores na rede. Em 1973, optou-se por um registro central de endereços na Universidade de Stanford, facilitando a organização e o encaminhamento de pacotes. As diversas redes emergentes usavam formatos diferentes para pacotes, criando um desafio de compatibilidade. **A solução foi adotar um conjunto comum de protocolos de comunicação chamado TCP/IP.**

Esse conjunto de protocolos que padroniza a forma como os dados são transmitidos e recebidos, garantindo a comunicação eficaz entre diferentes redes e dispositivos. Dessa forma, a interconexão de redes usando o TCP/IP evoluiu para a moderna Internet. Atualmente, a internet oferece uma infinidade de serviços disponibilizados! Dentro os principais serviços, os mais conhecidos são:

SERVIÇOS	DESCRIÇÃO
WORLD WIDE WEB (WWW)	Trata-se do serviço de visualização de páginas web organizadas em sites em que milhares de pessoas possuem acesso instantâneo a uma vasta gama de informação online em hipermídia que podem ser acessadas via navegador – é o serviço mais utilizado na Internet. Em geral, esse serviço utiliza protocolos como HTTP e HTTPS.
CORREIO ELETRÔNICO	Trata-se do serviço de composição, envio e recebimento de mensagens eletrônicas entre partes de uma maneira análoga ao envio de cartas – é anterior à criação da

	Internet. Utiliza tipicamente um modo assíncrono de comunicação que permite a troca de mensagens dentro de uma organização. Em geral, esse serviço utiliza protocolos como POP3, IMAP e SMTP.
ACESSO REMOTO	Trata-se do serviço que permite aos usuários facilmente se conectarem com outros computadores, mesmo que eles estejam em localidades distantes no mundo. Esse acesso remoto pode ser feito de forma segura, com autenticação e criptografia de dados, se necessário. Em geral, esse serviço utiliza protocolos como SSH, RDP, VNC.
TRANSFERÊNCIA DE ARQUIVOS	Trata-se do serviço de tornar arquivos disponíveis para outros usuários por meio de downloads e uploads. Um arquivo de computador pode ser compartilhado ou transferido com diversas pessoas através da Internet, permitindo o acesso remoto aos usuários. Em geral, esse serviço utiliza protocolos como FTP e P2P.

Esses são os serviços principais, mas existem muitos outros oferecidos via Internet (Ex: grupos de discussão, mensagens instantâneas, bate-papo, redes sociais, computação em nuvem, etc).

Web (WWW)

INCIDÊNCIA EM PROVA: BAIXA

Web é uma contração do termo World Wide Web (WWW). *Ah, professor... você tá falando de internet, não é?* Não! Muito cuidado porque são coisas diferentes! **A internet é uma rede mundial de computadores que funciona como uma estrutura que transmite dados para diferentes aplicações**. A Web é apenas uma dessas aplicações – uma gigantesca aplicação distribuída rodando em milhões de servidores no mundo inteiro usando navegadores.

Vamos entender isso melhor por meio de uma analogia: a Internet pode ser vista como uma vasta rede rodoviária que conecta cidades, estados e países. Essas estradas permitem que você vá de um lugar para outro, independentemente de qual seja o seu destino. Nessa rede rodoviária, você pode dirigir um carro, andar de bicicleta, caminhar, pegar um ônibus ou usar qualquer outro meio de transporte que desejar. **A estrutura das estradas e rodovias é o que torna tudo isso possível.**

Agora, pense na web como lojas, casas, escritórios e pontos de interesse que você encontra ao longo das estradas da Internet. Cada loja ou local representa um site da web, e você pode visitá-los para obter informações, fazer compras, se divertir, etc. Os sites da web são destinos ao longo da estrada. Em suma: a web é composta por uma vasta coleção de documentos e recursos interconectados, que são acessados por **meio de navegadores da web**.

COMPONENTS DA WEB	DESCRIÇÃO
HIPERTEXTO	A Web é baseada em documentos que contêm links (hiperlinks) para outros documentos relacionados. Isso permite que os usuários naveguem de uma página para outra, seguindo os links.
URL	Cada documento ou recurso na Web é identificado por um URL exclusivo, que é um endereço usado para acessar o recurso em um navegador.

NAVEGADORES DA WEB	São aplicativos que permitem aos usuários visualizar e interagir com documentos da Web. Exemplos populares de navegadores incluem o Google Chrome, Mozilla Firefox, Microsoft Edge e Safari.
PROTOCOLOS DE COMUNICAÇÃO	A Web utiliza protocolos de comunicação, como HTTP (Hypertext Transfer Protocol) e HTTPS (HTTP Secure), para transferir dados entre navegadores e servidores web.
SERVIDORES WEB	São computadores que hospedam documentos e recursos da Web. Eles respondem às solicitações dos navegadores e fornecem os conteúdos solicitados.
PÁGINAS DA WEB	São documentos criados usando linguagens de marcação, como HTML (Hypertext Markup Language). As páginas da web podem conter texto, imagens, links e outros elementos interativos.
MOTORES DE BUSCA	São ferramentas que ajudam os usuários a encontrar informações na Web, indexando e classificando páginas da web com base em palavras-chave.

Agora vamos falar um pouco sobre as gerações da web (note que elas não se excluem, elas se sobrepõem). Vamos vê-las em detalhes...

Web 0.0



Em março de 1989, a World Wide Web teve a primeira especificação composta pelo Protocolo HTTP e a Linguagem HTML lançada por Tim Berners-Lee. Sim, se utilizamos a web atualmente, devemos agradecer a esse senhor aqui do lado! Até então, a web era uma fonte de acesso a informações, onde páginas de hipertexto (textos com links), de conteúdo estático, escritas por jornalistas e outros profissionais eram publicadas em Servidores Web e podiam apenas ser lidas pelos demais usuários. *Galera, vocês querem conhecer a primeira página web da história?* Segue o link abaixo:

HTTP://INFO.CERN.CH/HYPERTEXT/WWW/THEPROJECT.HTML

Em 1991, a página web acima era a única do mundo; em 1994, já havia 2.738 páginas web – inclusive o **Yahoo!**; em 1998, já havia 2.410.067 páginas web – inclusive o **Google**; em 2001, já havia 29.254.370 páginas web – inclusive a **Wikipedia**; em 2005, já havia 64.780.617 páginas web – inclusive o **Youtube**; em 2008, já havia 172.338.776 páginas web – inclusive o **Dropbox**; e em 2018, temos 1.805.260.010 páginas web – inclusive o **Estratégia Concursos**!

Web 1.0

A Web 1.0 refere-se à primeira geração da World Wide Web, **que se originou nos anos 90 e durou até o início dos anos 2000.** Ela foi caracterizada por vários elementos distintos:

CARACTERÍSTICAS DA WEB 1.0	DESCRIÇÃO
ESTÁTICA E SOMENTE LEITURA	Sites da Web 1.0 eram predominantemente estáticos e unidirecionais. Eles consistiam principalmente em páginas HTML simples, que ofereciam informações estáticas aos visitantes. Os usuários podiam apenas ler o conteúdo e não interagir de forma significativa com o site.
CONTEÚDO LIMITADO	O conteúdo disponível na Web 1.0 era limitado à publicação de texto e imagens. Vídeos, áudios e outros formatos de mídia não eram comuns.
FALTA DE INTERATIVIDADE	Não havia recursos avançados de interatividade. Os visitantes podiam, no máximo, clicar em links para navegar entre páginas e preencher formulários de contato simples.
USO LIMITADO DE TECNOLOGIA	A tecnologia subjacente era principalmente HTML, com poucas opções para dinamizar o conteúdo da web. Não havia ferramentas avançadas de desenvolvimento web, como APIs (Interfaces de Programação de Aplicativos) ou tecnologias AJAX.
FALTA DE REDES SOCIAIS E COLABORAÇÃO	Redes sociais como as conhecemos hoje não existiam na Web 1.0. A interação social on-line era limitada, e não havia plataformas de compartilhamento de conteúdo ou colaboração em tempo real.
BUSCA INEFICIENTE	Os mecanismos de busca eram primitivos e muitas vezes geravam resultados imprecisos. A indexação de conteúdo era baseada em palavras-chave, o que tornava a busca menos eficaz.
ERA DA INFORMAÇÃO	A Web 1.0 era predominantemente uma fonte de informações. Os sites eram usados para publicar informações sobre empresas, instituições, produtos e serviços, mas havia pouca ênfase na interação ou na criação de conteúdo pelos usuários.
MARCAS E EMPRESAS	A Web 1.0 foi dominada por empresas e marcas que criaram sites institucionais para fornecer informações sobre si mesmas e seus produtos.

Web 2.0

A Web 2.0 se refere a uma internet mais **dinâmica**, **interativa** e **colaborativa**, onde os usuários desempenham um papel central na criação e compartilhamento de conteúdo. Vejamos:

CARACTERÍSTICAS DA WEB 2.0	DESCRIÇÃO
INTERATIVIDADE	Os sites e aplicativos da Web 2.0 oferecem uma experiência mais interativa para os usuários. Eles podem deixar comentários, avaliações, compartilhar conteúdo e até mesmo contribuir com suas próprias informações. Plataformas como redes sociais, blogs, wikis e fóruns permitem que as pessoas se envolvam ativamente.

CONTEÚDO GERADO PELO USUÁRIO	Os usuários não são mais apenas consumidores de conteúdo; eles são produtores ativos. Eles criam blogs, carregam vídeos, compartilham fotos e colaboram em wikis. Plataformas como YouTube, Wikipedia e WordPress são exemplos disso.
REDES SOCIAIS	As redes sociais desempenham um papel fundamental na Web 2.0. Elas conectam pessoas, permitindo que compartilhem informações, conversem e construam relacionamentos online. Exemplos incluem Facebook, Twitter, LinkedIn e Instagram.
COLABORAÇÕES	A colaboração é promovida por meio de ferramentas que permitem que várias pessoas trabalhem juntas em projetos, como Google Docs ou sistemas de gerenciamento de projetos online.
PERSONALIZAÇÃO	A Web 2.0 oferece serviços mais personalizados, adaptando o conteúdo com base nas preferências do usuário. Isso é visível em recomendações de produtos da Amazon, playlists personalizadas do Spotify e anúncios direcionados do Google.
MASH-UPS	A capacidade de combinar dados e funcionalidades de diferentes fontes é uma característica da Web 2.0. Os desenvolvedores podem criar aplicativos que agregam informações de várias fontes, como mapas do Google que mostram informações do tráfego em tempo real.
WEB SEMÂNTICA	Embora em desenvolvimento, a Web Semântica é uma parte importante da visão da Web 2.0. Envolve a criação de um ambiente onde as máquinas podem entender o conteúdo da web, tornando-o mais significativo e útil para os usuários.

Web 3.0

A Web 3.0 é uma evolução da World Wide Web que visa tornar a internet **mais inteligente** e capaz de **compreender o conteúdo que está disponível online**. Vejamos suas principais características:

CARACTERÍSTICAS DA WEB 3.0	DESCRIÇÃO
SEMÂNTICA	A Web 3.0 se concentra em adicionar metadados semânticos aos dados, permitindo que as máquinas compreendam melhor o conteúdo. Isso significa que os computadores podem entender o significado dos dados, em vez de simplesmente processar texto e números.
INTELIGÊNCIA ARTIFICIAL	A IA desempenha um papel fundamental na Web 3.0. Máquinas e algoritmos podem aprender, raciocinar e tomar decisões com base nos dados disponíveis.
CONECTIVIDADE	A Web 3.0 visa criar uma rede de informações altamente conectada, onde os dados podem ser relacionados e combinados de maneira mais inteligente. Isso facilita a recuperação de informações relevantes.
PERSONALIZAÇÃO	A personalização é uma parte importante da Web 3.0. Os sistemas podem entender as preferências do usuário e fornecer conteúdo adaptado às necessidades individuais.

INTEROPERABILIDADE	A Web 3.0 se esforça para tornar os dados e serviços interoperáveis, de modo que diferentes aplicativos e sistemas possam funcionar juntos de maneira eficaz.
WEB SEMÂNTICA	A Web Semântica é uma iniciativa importante na Web 3.0. Ela envolve a marcação de dados com metadados semânticos para que as máquinas possam entender as relações e conexões entre diferentes conjuntos de dados.
APLICAÇÕES DIVERSIFICADAS	A Web 3.0 tem aplicações em várias áreas, como comércio eletrônico, assistentes virtuais, pesquisa avançada, automação residencial, cuidados com a saúde, cidades inteligentes e muito mais.

CARACTERÍSTICAS	WEB 1.0	WEB 2.0	WEB 3.0
INTERATIVIDADE	Baixa	Alta	Muito Alta
CONTEÚDO	Estático e somente leitura	Dinâmico, com feedback do usuário	Inteligente, com semântica
USUÁRIOS	Consumidores passivos	Produtores de conteúdos	Participantes ativos
SOCIALIZAÇÃO	Ausente	Integração de redes sociais	Integração com IA e Internet das Coisas
EXPERIÊNCIA DO USUÁRIO	Limitada	Melhorada e personalizada	Altamente personalizada
TECNOLOGIA	HTML	AJAX, APIs e RSS	IA e Aprendizado de Máquina
EXEMPLOS	Sites estáticos de início da web	Redes sociais, blogs e wikis	Assistentes virtuais
PRINCIPAIS APLICAÇÕES	Sites informativos e institucionais	Redes sociais e colaboração online	Assistentes virtuais e Internet das Coisas

Deep Web e Dark Web

INCIDÊNCIA EM PROVA: MÉDIA

A web é dividida em diferentes camadas, sendo a Surface Web apenas cerca de 4% dela. Ela é composta por sites e páginas que podem ser indexados por mecanismos de busca comuns (Ex: Google ou Bing), e acessados sem autenticação. Por exemplo, páginas abertas em redes sociais como Facebook são parte da Surface Web. Os outros 96% compõem a Deep Web, que inclui páginas não indexáveis por mecanismos de busca padrão e protegidas por autenticação.

SURFACE WEB	DESCRIÇÃO
ACESSIBILIDADE	Facilmente acessível por meio de mecanismos de busca e navegadores padrão.
CONTEÚDO PÚBLICO	Compreende sites, páginas e conteúdo que são acessíveis ao público em geral.

INDEXAÇÃO POR MECANISMOS DE BUSCA	Os motores de busca, como Google e Bing, indexam e exibem o conteúdo da Surface Web em resultados de pesquisa.
INFORMAÇÕES AMPLAMENTE VISÍVEIS	Notícias, blogs, lojas online, fóruns públicos e outros tipos de sites podem ser encontrados na Surface Web.
SEM RESTRIÇÕES SIGNIFICATIVAS	Os usuários podem navegar e acessar conteúdo sem a necessidade de credenciais ou permissões especiais.
EXEMPLOS	Páginas de notícias, blogs, lojas online e outros sites acessíveis ao público em geral.

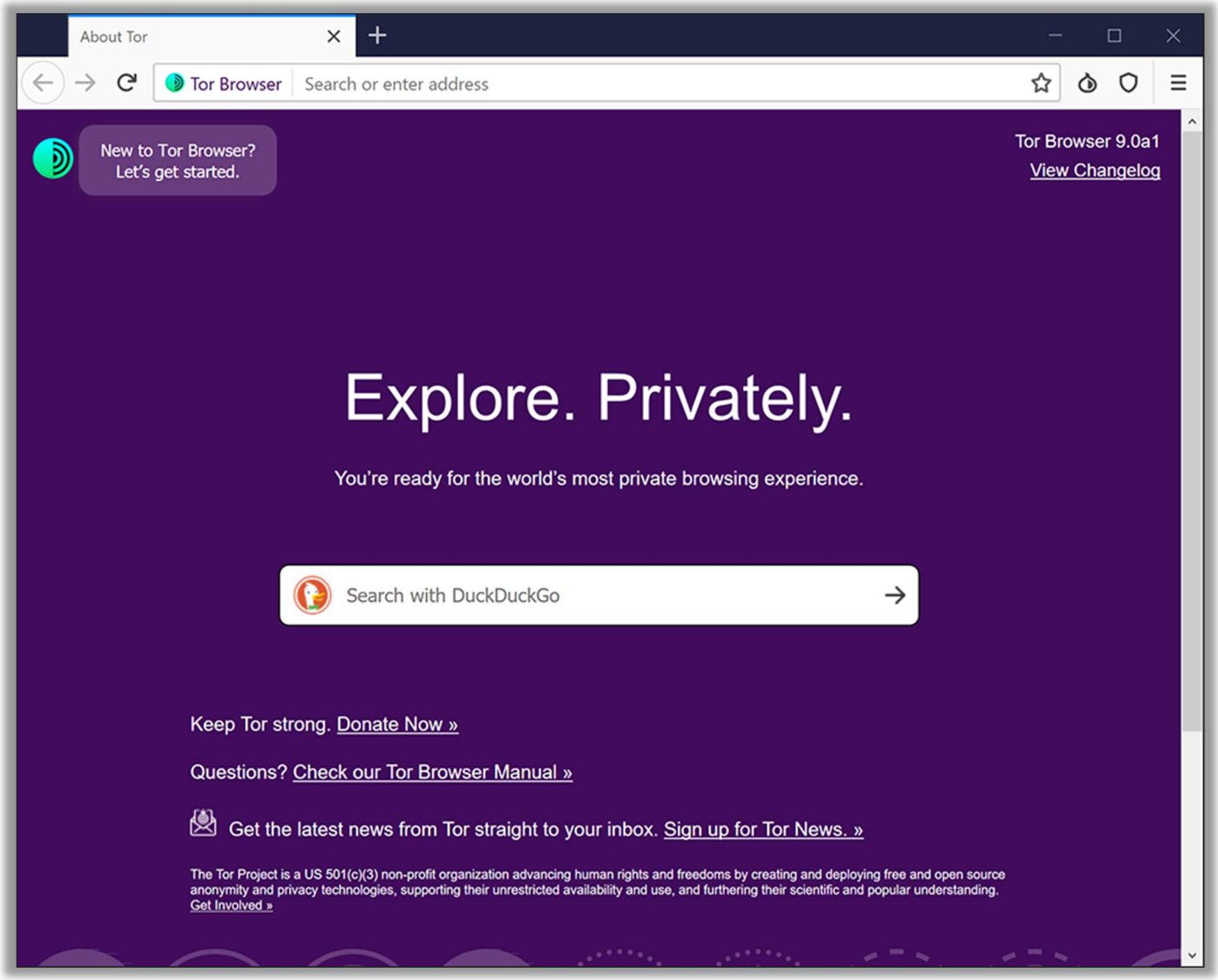
Um exemplo disso é a Intranet do TCU, acessível somente a servidores autorizados, o que a coloca na Deep Web. **Embora não visível para quem não tem autorização, não é completamente segura em termos de privacidade.** A comunicação entre computadores e servidores deixa rastros, que podem ser usados para identificar usuários e suas atividades na web. Isso levanta preocupações sobre privacidade, especialmente em países com regimes repressivos ou censura.

DEEP WEB	DESCRIÇÃO
CONTEÚDO NÃO INDEXADO POR MOTORES DE BUSCA	O conteúdo da Deep Web não é indexado pelos mecanismos de busca tradicionais, o que o torna invisível nas pesquisas comuns.
REQUER AUTENTICAÇÃO	Muitos sites da Deep Web exigem credenciais ou autenticação para acessar, tornando o conteúdo acessível apenas a usuários autorizados.
INFORMAÇÕES CONFIDENCIAIS	Inclui informações privadas, como dados de empresas, registros médicos, sistemas de gerenciamento de bibliotecas e muito mais.
NÃO ACESSÍVEL POR LINKS COMUNS	Você não pode simplesmente clicar em um link para acessar o conteúdo da Deep Web; geralmente, precisa de informações de login ou URLs específicas.
VARIEDADE DE CONTEÚDO	A Deep Web abrange uma ampla gama de informações, desde bancos de dados privados a sistemas de gerenciamento de conteúdo corporativo.

A Dark Web, uma subseção da Deep Web, oferece maior privacidade e anonimato. Ela não é indexada por mecanismos de busca e requer o uso de redes e navegadores especiais para ser acessada. A mais conhecida dessas redes é a Tor, originalmente um projeto militar dos EUA para comunicação segura. O navegador Tor permite acessar a Surface Web, Deep Web e Dark Web, sendo uma ferramenta crucial para pessoas em países com restrições de acesso à Internet.

DARK WEB	DESCRIÇÃO
ACESSÍVEL COM SOFTWARE ESPECÍFICO	A Dark Web é acessada por meio de redes criptografadas, como o Tor (The Onion Router), que requerem software especial para acesso.
CONTEÚDO ILEGAL E OBSCURO	Inclui sites que hospedam atividades ilegais, como tráfico de drogas, armas, venda de informações roubadas e outros conteúdos obscuros.
ANONIMATO É VALORIZADO	Os usuários da Dark Web muitas vezes valorizam o anonimato, pois os serviços são frequentemente anônimos e transações são criptografadas.
RISCOS À SEGURANÇA	A Dark Web é um ambiente de alto risco, onde os usuários podem ser vítimas de fraudes e ataques cibernéticos.

NÍVEIS MAIS PROFUNDOS DE ANONIMATO Diferentemente da Deep Web, a Dark Web oferece um nível mais profundo de anonimato e criptografia, tornando difícil rastrear usuários.



O Navegador Tor direciona as requisições de uma página através de uma rota que passa por uma série de servidores proxy da Rede Tor operados por milhares de voluntários em todo o mundo, **tornando o endereço IP não identificável e não rastreável**[13]. Vocês não precisam entender como isso funciona, vocês só precisam entender que os dados passam por uma série de camadas de encriptação de modo que seja praticamente impossível identificar de onde veio a requisição.

Conforme eu disse anteriormente, pode-se acessar páginas da Surface Web por meio desse navegador. Nesse caso, não é possível identificar quem está acessando, mas é possível identificar qual serviço está acessando (Ex: Google). Por outro lado, há algumas páginas da Dark Web que

[13] O nome **Tor** vem de **T**he **O**nion **R**outer (O Roteador Cebola) porque os dados passam por diversas camadas de encriptação como em uma cebola.

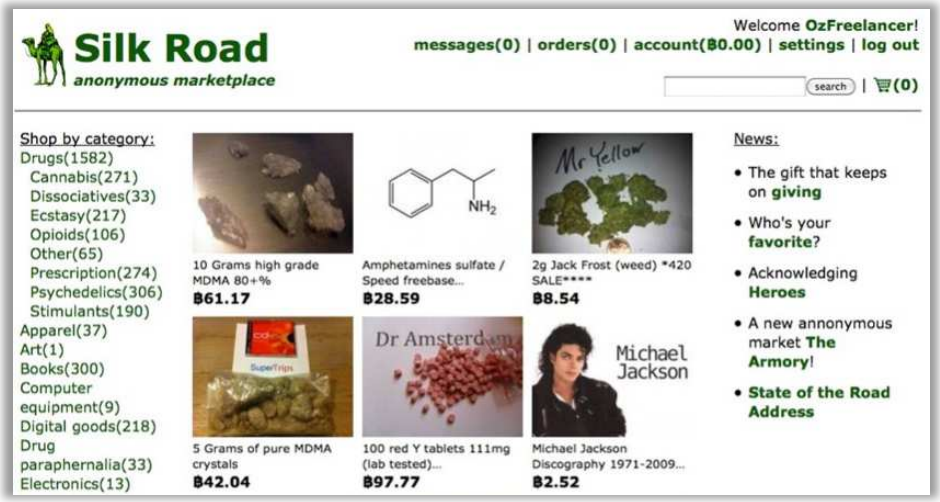
realmente só existem dentro da Rede Tor. Nesse caso, é absolutamente impossível identificar quem está acessando, quando está acessando, o que está acessando, etc – é completamente anônimo.

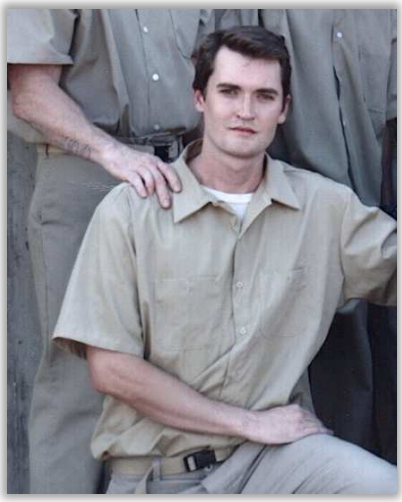
Galera, você pode encontrar usuários negociando entorpecentes e armas, contratando matadores de aluguel, planejando atentados terroristas, enviando vídeos de suicídio, compartilhando fotos de pedofilia, vazando documentos de empresas ou governos, trocando fotos de nudez, exibindo fotos/vídeos de torturas, estupros e homicídios de pessoas e animais, conteúdos racistas e xenófobos, canibalismo, esquisitices, falsificação de documentos, entre outros.

Eu sei que essa aula atiça a curiosidade de várias pessoas, mas eu já adianto que não recomendo que vocês acessem esses sites. Saibam que se trata de um ambiente em que é possível encontrar um bocado de hackers, cibercriminosos e outros profissionais desse tipo. Eu já recebi perguntas de alunos perguntando sobre "hipóteses" de atividades não muito legítimas. **Para terminar, vamos apenas falar um pouco sobre a relação entre a Dark Web e Criptomoedas.**

Em 2013, havia uma página na Rede Tor – chamada Silk Road – que vendia de tudo (desde metanfetaminas à discografia do Michael Jackson). *Professor, como havia vendas? Colocar o cartão de crédito não deixaria rastros?* Não eram utilizados cartões de créditos – era utilizado uma criptomoeda (moeda virtual/digital) chamada Bitcoin. **Essa moeda virtual não passa pelo sistema financeiro nacional dos países e, quando usada em uma Rede Tor, não pode ser rastreada.**

Por meio dessa moeda, é possível comprar produtos e serviços. Só para que vocês saibam como não é possível ficar totalmente anônimo, o dono desse site (imagem acima) vacilou e fez uma pergunta utilizando seu nome verdadeiro em um fórum de programadores da Surface Web. O FBI já estava o investigando por conta de outras atividades ilícitas, acabou ligando os pontos **e ele foi preso e condenado a duas sentenças de prisão perpétua + 40 anos e sem liberdade condicional.**





Por fim, vamos resumir tudo o que vimos na tabela apresentada a seguir e, por fim, uma analogia para finalmente consolidar o entendimento sobre esse conteúdo.

CARACTERÍSTICAS	SURFACE WEB	DEEP WEB	DARK WEB
ACESSIBILIDADE	Acessível por mecanismos de busca e navegadores comuns.	Requer credenciais específicas ou URLs exclusivas.	Acessível apenas por redes criptografadas, como o Tor.
CONTEÚDO COMUM	Contém informações e sites disponíveis publicamente.	Inclui conteúdo não indexado por mecanismos de busca, como bancos de dados privados.	Contém conteúdo obscuro e frequentemente ilegal.
ANONIMATO	Não oferece anonimato especial para usuários.	Pode exigir credenciais de login, mas não enfatiza o anonimato.	Valoriza altos níveis de anonimato e segurança.
CONTEÚDO COMERCIAL	Amplamente usado para negócios, educação, entretenimento e informações públicas.	Inclui recursos protegidos por senha, como e-mails, serviços bancários online e redes corporativas.	Muitas vezes associada a atividades ilegais e conteúdo obscuro.
EXEMPLOS	Sites de notícias, blogs, redes sociais, sites de compras online.	E-mails privados, intranets corporativas, bancos de dados de bibliotecas.	Sites de venda de drogas, mercados negros, fóruns de hackers.

Internet das Coisas (IoT)

INCIDÊNCIA EM PROVA: BAIXA

A transformação digital é um processo em que empresas e sociedades utilizam tecnologias digitais inovadoras para integrar e melhorar todas as áreas do negócio. Isso inclui resolver problemas, aprimorar desempenho, expandir alcance e entregar mais valor aos clientes. Ela representa uma mudança estrutural e cultural, com a tecnologia desempenhando um papel central para o sucesso.

Com a crescente adoção de dispositivos digitais inteligentes, como smartphones, tablets e sensores, prevê-se que cada consumidor terá, em média, 6,58 dispositivos inteligentes até 2020. **Esses dispositivos são conectados através de redes digitais modernas, que envolvem o planeta como uma "película digital", permitindo que uma variedade de dispositivos se comunique e interaja.**

A transformação digital tem sido acelerada por eventos como a pandemia de COVID-19, que forçou muitas empresas a adotar práticas de trabalho remoto e reconfigurar rapidamente suas operações. Isso levou a uma aceleração da adoção de tecnologias digitais para atender à demanda de clientes, limitar interações pessoais e apoiar funcionários em trabalho remoto, apesar das restrições orçamentárias e da retração econômica inicial.

Logo, a transformação digital não é apenas uma tendência, mas uma realidade em constante evolução, fundamental para o sucesso e a resiliência das empresas e da sociedade em um mundo

cada vez mais digitalizado. **Dito isso, vamos falar um pouco sobre uma tecnologia que vem para acelerar ainda mais o processo de transformação digital e, sem perceber, ela está cada vez mais entrando em nossas casas...**

INTERNET DAS COISAS
Trata-se de uma revolução tecnológica que se refere à conexão de dispositivos físicos e objetos do mundo real à internet. Esses dispositivos, também chamados de "coisas" na IoT, são integrados com sensores, software e outras tecnologias para coletar e trocar dados com outros dispositivos e sistemas pela internet.

Essa tecnologia que tem começado a cair em concurso público e que deve se popularizar com a chegada do 5G é a *Internet of Things* (IoT) – também conhecida como Internet das Coisas. *Como é que é, professor?* Galera, pensem rapidinho em todos os seus objetos que possuem acesso à internet: computador, notebook, *tablet*, smartphone, relógio, entre outros. Beleza, esses são os mais comuns em nosso dia a dia mesmo. *Porém, vocês conseguem pensar em outros?*

A câmera de segurança da portaria do seu prédio? **Ela tem acesso à internet!** *A Smart TV que você assiste aquele filminho bacana na Netflix?* **Ela tem acesso à internet!** *Quem curte jogar um videogame de vez em quando?* **Ele tem acesso à internet!** Galera, isso porque estamos no Brasil. Em outros países mais desenvolvidos, já existem outras coisas: geladeiras, máquina de lavar roupa, forno de micro-ondas, termostato, alarme de incêndio, sistema de som e iluminação, entre outros.

Isso não significa que seja possível baixar uma aula de informática no site do Estratégia Concursos usando sua geladeira! A proposta, na verdade, é que a conectividade auxiliará esses objetos a ficarem mais eficientes em seus contextos específicos. Agora vamos parar de pensar na nossa casa e vamos pensar no mundo: isso tem aplicabilidades na agricultura, pecuária, hospitais, escolas, fábricas, transporte público, logística, etc.

IoT não é uma tecnologia monolítica. Logo, seus componentes principais podem variar bastante, mas – em regra – incluem:

COMPONENTES	DESCRIÇÃO
DISPOSITIVOS	São os elementos físicos que compõem a IoT, como sensores, atuadores e outros dispositivos conectados, como câmeras, medidores inteligentes, veículos e eletrodomésticos. Eles coletam dados do mundo real e podem executar ações com base nesses dados.
TECNOLOGIAS DE COMUNICAÇÃO	São os meios pelos quais os dispositivos IoT se comunicam entre si e com a nuvem. Isso pode incluir Wi-Fi, Bluetooth, 3G/4G/5G, Zigbee, LoRa, entre outros. As redes de comunicação são responsáveis pela transferência de dados dos dispositivos para a nuvem e vice-versa.
SENSORES E ATUADORES	Os sensores coletam informações do ambiente, como temperatura, umidade, localização, movimento e muito mais. Os atuadores são responsáveis por tomar ações, como ligar ou desligar um dispositivo. Eles são os olhos e as mãos da IoT.
NUVEM (CLOUD)	A nuvem é onde os dados coletados pelos dispositivos IoT são processados, armazenados e disponibilizados para acesso. Plataformas de nuvem fornecem recursos de computação,

	armazenamento e análise de dados em grande escala, tornando possível o processamento de grandes volumes de informações.

Imagine uma casa que tem monitoramento de segurança, controle de temperatura ambiente e gerenciamento de iluminação integrados. Os dados de câmeras, alarmes contra incêndio, aparelhos de ar-condicionado, lâmpadas e outros itens são enviados para um sistema que controla cada aspecto. **Esse sistema pode ser um serviço em nuvem, garantindo acesso a ele a partir de qualquer lugar**.

Lembrando que o IPv6 (evolução do IPv4) permitiu a oferta de um número absurdamente gigantesco de endereços, logo a quantidade de dispositivos e sensores não deverá ser um problema por um bom tempo. É importante destacar também que a comunicação é um elemento essencial para a transmissão de dados entre dispositivos, sensores e sistemas de IoT. Abaixo, veremos algumas das principais tecnologias e protocolos de comunicação utilizados na IoT:

TECNOLOGIAS DE COMUNICAÇÃO	DESCRIÇÃO
WI-FI (802.11)	Trata-se de uma das tecnologias de comunicação sem fio mais amplamente utilizadas e oferece alta largura de banda. É adequado para dispositivos que têm acesso a redes locais de alta velocidade e energia suficiente.
BLUETOOTH (802.15)	Trata-se de uma tecnologia de comunicação sem fio de curto alcance, adequada para dispositivos pessoais, como fones de ouvido sem fio e dispositivos vestíveis. O Bluetooth Low Energy (BLE) é uma variante de baixo consumo de energia.
ZIGBEE	Trata-se de um padrão de comunicação sem fio de baixa potência projetado para redes de sensores e dispositivos IoT em ambientes domésticos e industriais.
LORA (LONG RANGE)	Trata-se de uma tecnologia de comunicação de longo alcance e baixa potência usada em aplicações de IoT em áreas remotas. É ideal para sensores que precisam de comunicação em longas distâncias.
SIGFOX	Trata-se de uma rede de baixa potência e baixa largura de banda projetada para aplicações de IoT que enviam pequenas quantidades de dados.
NB-IOT	Trata-se de um padrão de comunicação de baixa potência baseado em redes celulares para dispositivos IoT que exigem baixo consumo de energia e cobertura ampla.

Poxa, Diego... IoT só tem coisas boas! Calma, não é bem assim! **Os dispositivos podem eventualmente estar vulneráveis a ataques de segurança e privacidade.** Existe uma infinidade de riscos associados à IoT, tais como: riscos de um dispositivo permitir o acesso não autorizado e o uso indevido de informações pessoais; riscos de facilitar ataques em outros sistemas, escalonando privilégios ao invasor; riscos de os dispositivos servirem de escravos em botnets; entre outros.

VANTAGENS	DESVANTAGENS
Varejistas podem fornecer bônus de fidelidade para clientes preferenciais.	A dependência de compras online pode custar empregos.

As cidades podem avaliar as necessidades futuras de transporte.	Os varejistas podem saber tudo o que você está comprando.
Indivíduos podem reduzir os custos de energia e dos sistemas de aquecimento residenciais.	Os indivíduos podem receber mais e-mails de spam.
Fabricantes podem reduzir a inatividade prevendo as necessidades de manutenção dos equipamentos.	Uma falha da rede pode ser catastrófica.
Os governos podem monitorar o ambiente.	As empresas que criam dispositivos vestíveis têm muitas informações pessoais sobre os usuários.

É importante mencionar que a IoT – em geral – utiliza uma tecnologia chamada Long-Range Low-Power Wide Area Network, isto é, um tipo de rede sem fio de longa distância que permite comunicações com baixa taxa de transmissão de dados e baixo consumo de energia. A ideia do IoT é transmitir dados a grandes distâncias e, inclusive, a partir de dispositivos à bateria. **Apenas para comparação, o Bluetooth é uma tecnologia Short-Range Low-Power Personal Area Network.**

Finalmente, a IoT poderia ser definida, portanto, como uma tecnologia que permite que uma malha de dispositivos – **tais como dispositivos móveis, wearables (tecnologias para vestir), sensores, aparelhos eletrônicos de consumo e domésticos, dispositivos automotivos e dispositivos ambientais** – possam ser integrados para acessar aplicativos e informações ou para a interação com pessoas, redes sociais, governos e empresas.

Tecnologias de Acesso

TECNOLOGIAS DE ACESSO À INTERNET
Referem-se aos métodos e infraestruturas utilizados para conectar dispositivos, como computadores, smartphones e outros equipamentos, à Internet. Essas tecnologias permitem que os dispositivos acessem os serviços e recursos disponíveis na World Wide Web e em outros serviços online. Existem várias tecnologias de acesso à Internet (Ex: Dial-Up, ADSL, HFC, Fibra Óptica, PLC, Radiodifusão, Satélite e Telefonia Móvel), e a escolha depende das necessidades e da disponibilidade em uma determinada região.

Até o início dos anos 90, a internet era conhecida principalmente por pesquisadores e profissionais ligados a universidades, governo ou indústria. **Com o surgimento da Web, a internet se tornou acessível a milhões de usuários com diferentes interesses.** Este crescimento explosivo foi impulsionado por Provedores de Serviços da Internet (ISPs), que permitiram a conexão de usuários individuais à internet, transformando-a em um serviço de utilidade pública, semelhante à telefonia.

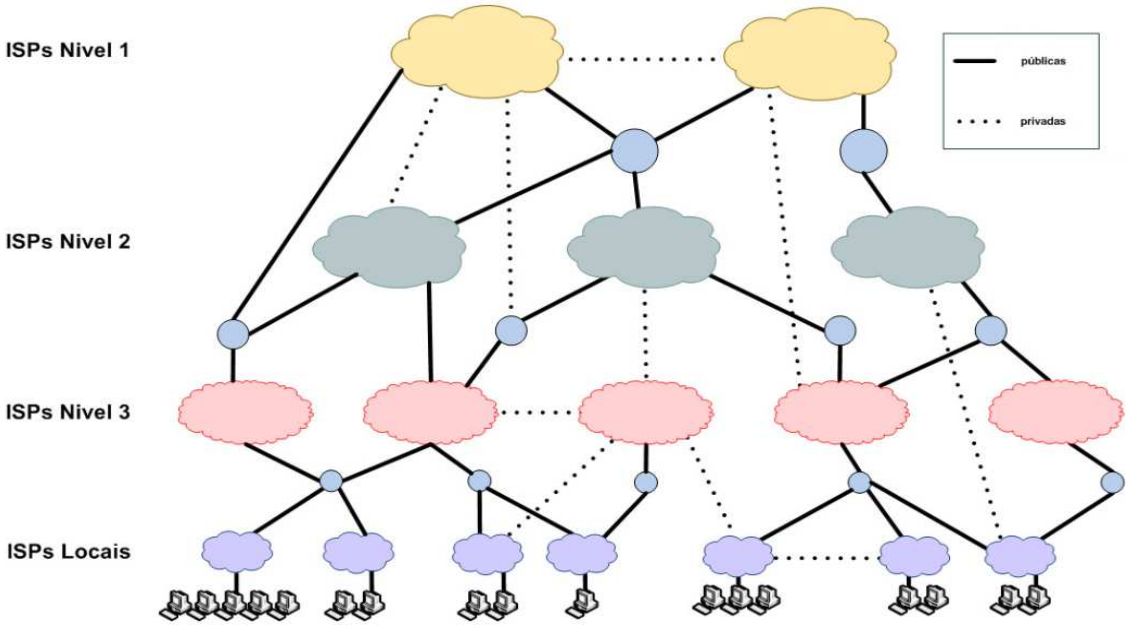
A infraestrutura de rede da internet, conhecida como Backbone, desempenha um papel crucial nesse processo. Composta por satélites, ondas de rádio e de cabos de fibra óptica terrestres e submarinos, essa rede interliga diferentes países e continentes, sendo responsável por cerca de 80% de toda a comunicação global. Os backbones são construídos e administrados por provedores de serviço de internet, incluindo companhias telefônicas de longa distância e governos nacionais.

Esses troncos de rede de alta velocidade e desempenho fornecem acesso à internet para várias outras redes. Os ISPs, como NET/CLARO, GVT/VIVO e SKY, são os responsáveis por vender o

acesso à internet a provedores menores e usuários finais. Os backbones, que podem ser terrestres ou submarinos, formam uma rede essencial que sustenta a comunicação e o acesso à internet em todo o mundo. **Existem três níveis de provedores de acesso:**

NÍVEIS	DESCRIÇÃO
ISP NÍVEL 1	São os provedores de acesso à internet de nível mais alto na hierarquia. Eles não precisam comprar acesso à internet de outros provedores, pois possuem uma rede global de alta capacidade e trocam tráfego diretamente uns com os outros. Exemplos de provedores de Nível 1 incluem AT&T, Verizon, NTT Communications e CenturyLink. Eles têm uma presença global e fornecem acesso à internet em escala internacional. Imagine ISPs de Nível 1 como rodovias federais, como a Rodovia Presidente Dutra (BR-116). Essas rodovias cruzam continentes e países sem precisar pagar pedágio a outras estradas menores. Os provedores de Nível 1 constroem e mantêm essas "rodovias da internet" e interconectam-se diretamente para permitir um tráfego rápido e eficiente.
ISP NÍVEL 2	Estes são provedores de acesso à internet que não possuem redes globais como os Nível 1, mas ainda têm uma rede significativa em uma área geográfica específica. Eles geralmente compram acesso à internet de Nível 1 ISPs e podem vender serviços a ISPs de nível inferior ou a empresas e consumidores diretos. Exemplos de provedores de Nível 2 incluem Cogent, Orange, Charter, Deutsche Telekom, entre outros. ISPs de Nível 2 podem ser comparados a rodovias estaduais. Eles atendem a áreas geográficas maiores, como estados ou regiões inteiras. Essas rodovias estaduais se conectam às autoestradas globais (Nível 1) e podem cobrar pedágio por permitir que o tráfego flua entre essas grandes autoestradas e áreas locais.
ISP NÍVEL 3	São provedores regionais ou locais que não possuem redes globais. Eles compram acesso à internet de provedores de Nível 1 ou 2 para fornecer conectividade a empresas e consumidores em áreas geográficas específicas. Esses ISPs podem se concentrar em uma única cidade, região ou país. Alguns provedores de Nível 3 podem ser ISPs de acesso final, que fornecem serviços diretamente a residências e empresas locais. ISPs de Nível 3 são como as estradas locais e ruas em cidades. Eles atendem áreas geográficas muito específicas, como uma cidade ou bairro. Essas estradas locais se conectam às rodovias regionais (Nível 2) ou diretamente às autoestradas globais (Nível 1) e permitem que o tráfego alcance destinos locais.

ISPs Locais normalmente se enquadram como ISPs de Nível 3. Eles são responsáveis por fornecer conectividade à Internet para áreas locais específicas e são mais próximos dos usuários finais.



Dito isso, os enlaces que conectam as redes de acesso residenciais aos ISP Nível 3 ou Locais podem ser de diferentes tecnologias, vamos conhecê-las a seguir:

TECNOLOGIAS DE ACESSO	DESCRIÇÃO
DIAL-UP	Uma tecnologia de acesso discado à internet que utiliza a linha telefônica tradicional. É lenta e está em desuso na maioria das áreas.
ADSL	Uma tecnologia de acesso de banda larga que utiliza a linha telefônica para fornecer velocidades mais rápidas do que o dial-up.
HFC	Uma tecnologia que combina fibra óptica e cabos coaxiais para fornecer serviços de internet de alta velocidade e TV a cabo.
FIBRA ÓPTICA	Uma tecnologia de alta velocidade que utiliza cabos de fibra óptica para transmitir dados em alta velocidade por meio de pulsos de luz.
PLC	Utiliza a rede elétrica para transmitir dados, tornando a fiação elétrica existente uma rede de comunicação.
RADIODIFUSÃO	Utiliza ondas de rádio para transmitir dados. Pode incluir tecnologias como Wi-Fi e redes celulares.
SATÉLITE	Acesso à internet via satélite – os dados são enviados e recebidos por meio de satélites em órbita terrestre.
TELEFONIA MÓVEL	Acesso à internet usando redes móveis (3G, 4G, 5G), permitindo a conexão em movimento a partir de dispositivos móveis.

Dial-Up

INCIDÊNCIA EM PROVA: MÉDIA

DIAL-UP	DESCRIÇÃO
CONEXÃO POR LINHA	A conexão Dial-Up utiliza a linha telefônica convencional para estabelecer a conexão com a Internet. Isso significa que o acesso à Internet é estabelecido por meio de uma chamada telefônica.

BAIXA VELOCIDADE	Uma das principais desvantagens da conexão Dial-Up é a baixa velocidade de transmissão de dados. As velocidades típicas variam de 56 kbps a 128 kbps, o que é significativamente mais lento do que tecnologias mais recentes.
CONEXÃO DISCADA	Os usuários precisam discar para o Provedor de Serviços de Internet (ISP) toda vez que desejam se conectar à web. Isso envolve o uso de um modem Dial-Up para criar a conexão, o que pode levar um tempo considerável.
LINHA OCUPADA	Uma das desvantagens mais notáveis é que, enquanto você está conectado via Dial-Up, a linha telefônica fica ocupada. Isso significa que você não pode fazer ou receber chamadas telefônicas ao mesmo tempo em que está conectado à Internet.
CUSTOS DE CHAMADA TELEFÔNICA	A conexão Dial-Up requer uma chamada telefônica para o ISP. Dependendo do plano telefônico, isso pode resultar em custos adicionais. Em alguns lugares, as chamadas telefônicas locais eram gratuitas, enquanto em outros lugares eram tarifadas.
DESCONEXÕES FREQUENTES	A conexão Dial-Up é vulnerável a quedas frequentes devido a interferências na linha telefônica ou outras questões técnicas. Isso pode ser frustrante para os usuários, pois eles precisam se reconectar repetidamente.
INCOMPATIBILIDADE COM CONTEÚDO RICO	Devido à baixa velocidade, a conexão Dial-Up não é adequada para acessar conteúdo rico em multimídia, como vídeos de alta qualidade ou jogos online. O streaming de mídia pode ser lento e de baixa qualidade.
OBSOLETA	A tecnologia Dial-Up é considerada obsoleta na maioria das regiões do mundo, com provedores de serviços migrando para tecnologias de banda larga mais rápidas, como DSL, cabo, fibra óptica e redes móveis 3G/4G/5G.
BAIXA LARGURA DE BANDA	A largura de banda limitada da conexão Dial-Up torna o uso de aplicativos intensivos em largura de banda, como videoconferências ou transferências de arquivos grandes, uma tarefa lenta e complicada.
ADEQUADA PARA TAREFAS BÁSICAS	Embora seja inadequada para muitas atividades online modernas, a conexão Dial-Up ainda pode ser adequada para tarefas básicas, como envio e recebimento de e-mails, navegação na web com páginas leves e chat online.

ADSL

INCIDÊNCIA EM PROVA: MÉDIA

ADSL	DESCRIÇÃO
ASSIMÉTRICA	O "A" em ADSL significa assimétrico, o que indica que a taxa de upload (envio de dados) é diferente da taxa de download (recebimento de dados). Geralmente, a taxa de download é significativamente mais rápida do que a de upload.
UTILIZAÇÃO DAS LINHAS TELEFÔNICAS	O ADSL utiliza as linhas telefônicas convencionais para transmitir dados. Ele é compatível com a infraestrutura de telefone existente, permitindo que os usuários acessem a Internet e façam chamadas telefônicas simultaneamente.
FREQUÊNCIAS DIFERENTES	Linhas telefônicas transmitem dados em diferentes frequências. As frequências mais baixas são reservadas para voz, enquanto as frequências mais altas são usadas para transmitir dados. Isso permite que a Internet e as chamadas coexistam na mesma linha.
VELOCIDADE VARIÁVEL	A velocidade da conexão ADSL pode variar de acordo com a distância entre o usuário e a central telefônica. Quanto mais longa a linha telefônica, mais lenta é a conexão. Isso ocorre porque o sinal ADSL enfraquece à medida que viaja por distâncias maiores.
TAXA DE UPLOAD LIMITADA	A taxa de upload no ADSL é geralmente menor do que a de download. Isso significa que o envio de dados, como o carregamento de arquivos ou o envio de e-mails com anexos grandes, é mais lento do que o download.

LARGURA DE BANDA COMPARTILHADA	A largura de banda em uma linha ADSL é compartilhada entre todos os usuários conectados a essa linha. Isso significa que, em horários de pico, a velocidade da conexão pode diminuir devido à concorrência por largura de banda.
ADEQUADA PARA APLICAÇÕES RESIDENCIAIS	O ADSL é frequentemente usado em ambientes residenciais. É adequado para atividades como navegação na web, streaming de vídeos em qualidade padrão e jogos online.
AMPLA DISPONIBILIDADE	Devido à utilização das linhas telefônicas existentes, o ADSL é amplamente disponível em muitas áreas urbanas e rurais. No entanto, a velocidade da conexão pode variar dependendo da localização geográfica.
REQUER UM MODEM ADSL	Os usuários precisam de um modem ADSL para estabelecer a conexão. Esse modem é fornecido pelo provedor de serviços de Internet ou pode ser adquirido separadamente.
SUPERADO POR TECNOLOGIAS MAIS RÁPIDAS	Embora ainda seja utilizado, o ADSL foi superado por tecnologias de banda larga mais rápidas, como a fibra óptica e o cabo, que oferecem velocidades mais altas e uma experiência de Internet mais fluida.

HFC

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

HFC	DESCRIÇÃO
HÍBRIDA	A sigla HFC significa "Híbrido de Fibra-Coaxial". Essa tecnologia combina o uso de cabos de fibra óptica e cabos coaxiais para a transmissão de dados. A fibra óptica é utilizada na infraestrutura principal, enquanto os cabos coaxiais são usados para a distribuição local.
CANAIS SEPARADOS	No HFC, os dados são transmitidos em canais separados. Isso permite a transmissão simultânea de vários serviços, como Internet, TV a cabo e voz sobre IP (VoIP), sem interferência.
VELOCIDADE DE DOWNLOAD E UPLOAD	O HFC geralmente oferece uma largura de banda significativa, permitindo altas velocidades de download e upload. Isso é adequado para atividades que requerem largura de banda, como streaming de vídeo em alta definição e jogos online.
BAIXA LATÊNCIA	A tecnologia HFC tende a ter baixa latência, o que a torna adequada para aplicações em tempo real, como chamadas de vídeo e jogos online.
ADEQUADO P/ REDES DE TV A CABO	Além do acesso à Internet, o HFC é frequentemente usado para fornecer serviços de televisão a cabo. Os provedores de TV a cabo aproveitam a alta capacidade da fibra óptica para transmitir uma grande variedade de canais de TV.
MODENS E ROTEADORES ESPECÍFICOS	Os usuários de HFC precisam de modems e roteadores específicos para se conectarem à Internet. Esses dispositivos são fornecidos pelos provedores de serviços ou podem ser adquiridos separadamente.
AMPLA DISPONIBILIDADE URBANA	A tecnologia HFC é amplamente disponível em áreas urbanas e suburbanas, onde a infraestrutura de cabo coaxial já está estabelecida.
OFERECE PACOTES DE SERVIÇOS	Os provedores de serviços de HFC geralmente oferecem pacotes que incluem acesso à Internet, TV a cabo e serviços de voz. Isso permite que os usuários escolham o que desejam com base em suas necessidades.
CONCORRÊNCIA NO MERCADO	Em muitas áreas, o HFC enfrenta concorrência de outras tecnologias de acesso à Internet, como fibra óptica, DSL e conexões sem fio. Isso muitas vezes leva a preços competitivos e opções variadas para os consumidores.

Fibra Óptica

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

FIBRA ÓPTICA	DESCRIÇÃO
ALTA VELOCIDADE	A principal característica da fibra óptica é a alta velocidade de transmissão de dados. A luz é usada para transmitir informações através das fibras, o que permite taxas de transferência de dados extremamente rápidas.
ALTA LARGURA DE BANDA	A fibra óptica oferece uma largura de banda significativa, tornando-a adequada para lidar com grandes volumes de dados, incluindo streaming de vídeo em alta definição, videoconferências, jogos online e transferências de arquivos pesados.
BAIXA ATENUAÇÃO	A luz viaja por longas distâncias na fibra óptica com pouca perda de sinal, resultando em alta qualidade e consistência na transmissão de dados.
IMUNIDADE A INTERFERÊNCIA	As fibras ópticas não são suscetíveis a interferências eletromagnéticas, o que significa que não são afetadas por campos elétricos ou magnéticos.
SEGURANÇA DE DADOS	Como os sinais são transmitidos como luz, é difícil interceptar ou invadir uma conexão de fibra óptica, tornando-a uma opção segura para a transmissão de dados sensíveis.
DISTÂNCIAS LONGAS	A fibra óptica pode transmitir dados a distâncias muito maiores do que outros meios de transmissão, sem perda significativa de sinal.
BAIXA LATÊNCIA	A baixa latência é uma característica da fibra óptica, o que a torna ideal para aplicações que exigem respostas rápidas, como jogos online e videoconferências.
VARIEDADE DE SERVIÇOS	A fibra óptica é usada para fornecer serviços de Internet de alta velocidade, televisão digital, telefonia VoIP e muito mais.
LEVEZA E DIMENSÕES REDUZIDAS	Os cabos de fibra óptica são leves e têm um tamanho compacto em comparação com cabos de cobre, tornando a instalação mais fácil e econômica.
MENOS SUSCETIBILIDADES A INTEMPÉRIES	Os cabos de fibra óptica são menos suscetíveis a danos causados por condições climáticas adversas, como tempestades e raios.
INFRAESTRUTURA DE PRÓXIMA GERAÇÃO	A fibra óptica é considerada uma tecnologia de acesso que atende às demandas das futuras redes de alta velocidade e é um componente importante para o desenvolvimento de infraestruturas de comunicação de próxima geração.
CRESCENTE DISPONIBILIDADE	Embora ainda não esteja disponível em todas as áreas, a disponibilidade de redes de fibra óptica está aumentando, especialmente em áreas urbanas.
MAIOR PREÇO	A fibra óptica tende a ser mais cara de implementar em comparação com outras tecnologias de acesso, devido aos custos de infraestrutura.
MANUTENÇÃO COMPLEXA	Embora a fibra óptica seja durável, a manutenção pode ser mais complexa e cara quando comparada a outros meios de transmissão.

NECESSIDADE DE CONVERSORES	Para uso em dispositivos convencionais, é necessário o uso de conversores para transformar os sinais ópticos em sinais elétricos.

PLC

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

PLC	DESCRIÇÃO
USO DE INFRAESTRUTURA ELÉTRICA	O PLC utiliza a rede elétrica preexistente para transmitir dados. Isso significa que não são necessários cabos de rede adicionais, como os usados em conexões Ethernet tradicionais.
FACILIDADE DE INSTALAÇÃO	A instalação é relativamente simples. Em geral, usuários precisam de um adaptador PLC que é conectado a uma tomada elétrica e ao roteador. Outros adaptadores podem ser conectados a tomadas em diferentes partes da residência para estender a cobertura.
VELOCIDADE VARIÁVEL	A velocidade da conexão pode variar dependendo de vários fatores, incluindo a qualidade da fiação elétrica e a distância entre os adaptadores. Em comparação com outras tecnologias, como fibra óptica ou DSL, o PLC tende a oferecer velocidades mais baixas.
ALCANCE LIMITADO	A eficácia do PLC pode diminuir à medida que a distância entre os adaptadores aumenta. Isso pode limitar a sua utilidade em residências maiores ou edifícios com fiação elétrica mais antiga.
CONEXÃO ESTÁVEL	Em condições ideais, a conexão PLC pode ser bastante estável. No entanto, a presença de ruídos na rede elétrica ou dispositivos elétricos que geram interferências pode afetar a qualidade da conexão.
SEGURANÇA	Os adaptadores PLC geralmente oferecem recursos de segurança, como criptografia, para proteger a comunicação de dados transmitida pela rede elétrica.
CUSTO ACESSÍVEL	O PLC é geralmente considerado uma opção de custo acessível para fornecer acesso à internet, pois aproveita a infraestrutura elétrica existente.
COMPATIBILIDADE UNIVERSAL	A tecnologia PLC é compatível com a maioria dos dispositivos que podem ser conectados à rede por meio de uma conexão com fio, como computadores, impressoras, TVs inteligentes e sistemas de segurança.
DESAFIOS AMBIENTAIS	A qualidade da conexão PLC pode ser afetada por interferências causadas por dispositivos elétricos e circuitos elétricos ruidosos.

Radiodifusão

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

RADIODIFUSÃO	DESCRIÇÃO
TRANSMISSÃO POR ONDAS DE RÁDIO	A transmissão de dados é realizada por meio de ondas de rádio, que são transmitidas por uma estação base para receptores localizados nas residências ou empresas dos usuários.
SEM FIOS	A radiodifusão é uma tecnologia sem fio, o que significa que não requer cabos físicos para conectar os usuários à internet. Isso a torna especialmente útil em áreas geograficamente desafiadoras.

AMPLA COBERTURA	As redes de radiodifusão podem oferecer uma cobertura mais ampla em comparação com outras tecnologias sem fio, como redes de celular. Isso as torna adequadas para áreas rurais e afastadas.
PROVEDORES DE SERVIÇO ESPECÍFICOS	A maioria dos serviços de radiodifusão de internet é fornecida por provedores de serviço específicos que possuem e operam a infraestrutura de transmissão de rádio.
EQUIPAMENTO DO CLIENTE	Os usuários precisam de equipamentos receptores, como antenas ou roteadores específicos para se conectarem à rede de radiodifusão. Esses equipamentos podem ser instalados em telhados, torres ou locais elevados para melhorar a recepção do sinal.
LATÊNCIA E VELOCIDADE	A latência e a velocidade da conexão de radiodifusão podem variar dependendo da qualidade do sinal e do congestionamento da rede. Em alguns casos, a latência pode ser mais alta do que em tecnologias com fio, como fibra óptica.
LARGURA DE BANDA LIMITADA	As redes de radiodifusão podem ter largura de banda limitada, o que pode afetar a capacidade de suportar múltiplos dispositivos e aplicativos simultaneamente.
CUSTOS VARIÁVEIS	Os custos de assinatura de serviços de radiodifusão podem variar dependendo da localização do usuário e do provedor de serviço específico. Além disso, os custos de equipamento inicial também podem ser relevantes.
NECESSIDADE DE LINHA DE VISÃO DIRETA	Em algumas configurações de radiodifusão, pode ser necessário ter uma linha de visão direta entre a antena receptora e a torre de transmissão para obter uma boa qualidade de sinal.
USOS DIVERSOS	Além de fornecer acesso à internet, a tecnologia de radiodifusão é usada em comunicações de rádio em duas direções, como rádio por satélite, que pode ser usada para acesso à internet e transmissão de conteúdo de áudio e vídeo.

Satélite

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

SATÉLITE	DESCRIÇÃO
TRANSMISSÃO VIA SATÉLITE	A tecnologia de satélite envolve o uso de satélites de comunicação em órbita da Terra. Esses satélites atuam como retransmissores de sinais, permitindo que os provedores de serviço transmitam dados de internet para os usuários e vice-versa.
COBERTURA GLOBAL	Uma das principais vantagens da tecnologia de satélite é sua capacidade de fornecer cobertura global. Isso significa que ela pode ser usada em áreas rurais, remotas ou em locais onde a infraestrutura terrestre é limitada.
EQUIPAMENTO DO USUÁRIO	Os usuários precisam de equipamentos específicos para se conectarem à internet via satélite. Isso inclui uma antena parabólica e um modem via satélite. A antena parabólica é instalada no local do usuário e aponta para o satélite de comunicação.
LATÊNCIA	Possui latência relativamente alta, porque os sinais de internet devem viajar para o satélite e depois retornar à Terra. Embora a latência venha sendo reduzida, ainda pode ser notada em aplicações sensíveis à latência, como jogos online em tempo real.
VELOCIDADE VARIÁVEL	A velocidade da conexão via satélite pode variar dependendo da oferta do provedor de serviço e das condições atmosféricas. Em geral, as conexões de satélite podem oferecer velocidades que variam de moderadas a muito altas, dependendo do plano escolhido.
CUSTO	Os custos de assinatura de serviços de satélite podem variar e tendem a ser mais caros do que os de tecnologias de acesso à internet por cabo ou DSL. Além disso, o equipamento inicial, como a antena parabólica e o modem, também tem um custo associado.

USO EM LOCAIS REMOTOS	A tecnologia de satélite é especialmente útil em locais remotos, onde outras opções de banda larga não estão disponíveis.
REDES VSAT	Em algumas configurações empresariais, a tecnologia de satélite é usada em redes de satélite de pequena abertura de terminal de terra (VSAT). Isso permite a conectividade de dados de alta velocidade para empresas e locais em áreas remotas.
APLICAÇÕES DIVERSAS	Além do acesso à internet, a tecnologia de satélite é usada em comunicações globais, TV via satélite e comunicações por satélite em locais sem infraestrutura de telecomunicações.

Telefonia Móvel

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

TELEFONIA MÓVEL	DESCRIÇÃO
REDES DE COMUNICAÇÃO SEM FIO	A tecnologia de telefonia móvel é baseada em redes de comunicação sem fio, como 3G, 4G (LTE) e 5G. Essas redes são projetadas para fornecer conectividade à internet em áreas urbanas e rurais, bem como em movimento.
SMARTPHONES E DISPOSITIVOS MÓVEIS	Os dispositivos móveis, como smartphones e tablets, são usados para acessar a internet por meio de redes móveis. Eles são equipados com módulos de comunicação que suportam diferentes gerações de redes, como 3G, 4G e 5G.
COBERTURA AMPLA	As redes de telefonia móvel geralmente oferecem uma ampla cobertura geográfica. Isso significa que os usuários podem acessar a internet em uma variedade de locais, desde áreas urbanas densamente povoadas até áreas rurais remotas.
VELOCIDADE VARIÁVEL	A velocidade da conexão à internet por telefonia móvel pode variar dependendo da geração da rede e das condições locais. As redes 4G e 5G oferecem velocidades mais altas em comparação com as redes 3G.
PLANOS DE DADOS MÓVEIS	Os usuários normalmente adquirem planos de dados móveis de seus provedores de serviços. Esses planos podem variar em termos de dados disponíveis, velocidade e preço.
WI-FI	Além da conectividade de rede móvel, muitos dispositivos móveis também suportam conexões Wi-Fi. Isso permite que os usuários se conectem a redes locais de alta velocidade, como as disponíveis em residências, cafés, aeroportos e locais públicos.
APLICAÇÕES MÓVEIS	Os smartphones e tablets executam uma variedade de aplicativos que facilitam o acesso à internet. Isso inclui navegadores da web, aplicativos de mídia social, serviços de e-mail, aplicativos de streaming de vídeo e muito mais.
ROAMING INTERNACIONAL	Alguns planos de telefonia móvel oferecem a capacidade de acessar a internet enquanto viajam internacionalmente. Isso pode ser útil para turistas e viajantes de negócios.
ACESSO EM MOVIMENTO	A capacidade de acessar a internet em movimento é uma das principais vantagens da tecnologia de telefonia móvel. Os usuários podem acessar informações, navegar na web, verificar e-mails e muito mais enquanto estão em trânsito.
5G E O FUTURO	A introdução da tecnologia 5G representa um avanço significativo na velocidade e capacidade de conexão da telefonia móvel. Isso possibilita uma variedade de novas aplicações, como Internet das Coisas (IoT) e realidade aumentada (AR).

GLOSSÁRIO

TERMO	DEFINIÇÃO
REDES DE COMPUTADORES	Conjunto de sistemas computacionais interligados que compartilham informações, recursos e comunicações, utilizando conexões de dados entre eles.
BODY AREA NETWORK (BAN)	Rede de dispositivos de comunicação sem fio situados no ou próximos ao corpo humano, utilizados principalmente para aplicações de monitoramento da saúde.
PERSONAL AREA NETWORK (PAN)	Rede de comunicação destinada ao uso pessoal dentro de uma área pequena, geralmente envolvendo dispositivos como computadores, telefones e periféricos pessoais.
LOCAL AREA NETWORK (LAN)	Rede que conecta computadores e dispositivos em uma área geográfica limitada, como uma casa, escritório ou campus, facilitando a comunicação e o compartilhamento de recursos.
METROPOLITAN AREA NETWORK (MAN)	Rede que cobre uma área geográfica maior que uma LAN mas menor que uma WAN, típica em uma cidade ou área metropolitana, interligando várias LANs.
WIDE AREA NETWORK (WAN)	Rede de computadores que abrange uma grande área geográfica do tamanho de países ou continentes geralmente através de linhas de telecomunicação públicas ou privadas.
TOPOLOGIA	Arranjo de elementos como links, nós, etc em uma rede de computadores que descreve a estrutura física ou lógica de como diferentes dispositivos estão interconectados.
TOPOLOGIA FÍSICA	Refere-se à disposição física real dos dispositivos e cabos em uma rede – inclui a localização dos dispositivos e como os cabos são executados para conectá-los.
TOPOLOGIA LÓGICA	Refere-se ao modo como os dados são efetivamente transmitidos entre nós em uma rede, independentemente de sua configuração física.
BARRAMENTO (BUS)	Topologia de rede em que todos os dispositivos são conectados a um único cabo central ou barramento, e todos os dados passam por esse cabo.
ESTRELA (STAR)	Topologia de rede onde cada dispositivo é conectado a um hub ou switch central, formando uma configuração em forma de estrela.
ANEL (RING)	Topologia de rede onde cada dispositivo está conectado exatamente a dois outros dispositivos, formando um anel, e os dados viajam em uma única direção através do anel.
MALHA (MESH)	Topologia de rede de computadores em que cada dispositivo está interconectado a múltiplos outros dispositivos.
WI-FI	Tecnologia de rede sem fio que permite que dispositivos se conectem à Internet ou se comuniquem entre si sem fio dentro de uma área específica.
BLUETOOTH	Tecnologia de comunicação sem fio de curto alcance projetada para substituir cabos físicos, conectando e trocando dados entre dispositivos sobre distâncias curtas.
ETHERNET	Uma família de tecnologias de rede para redes locais, caracterizada pelo uso de cabos para a conexão de dispositivos dentro de uma área limitada.
TOKEN RING	Tecnologia de rede que utiliza um 'token' que circula pela rede e um dispositivo só pode transmitir dados quando recebe o token, garantindo uma transmissão de dados sem colisões.
FRAME RELAY	Tecnologia de rede de alta velocidade para comunicação de dados em redes WAN que utiliza pacotes de tamanho variável para transmitir dados entre LANs e dispositivos de rede.
MPLS	Mecanismo que direciona dados de um nó para o próximo com base em etiquetas de curto prazo, em vez de endereços de rede longos, permitindo roteamento mais rápido e eficiente.
FDDI	Padrão para transmissão de dados em redes locais (LAN) que utiliza fibra óptica como meio principal, oferecendo alta velocidade e grande capacidade de banda.

VOIP	Tecnologia que permite a realização de chamadas de voz através da Internet ou outras redes de dados, convertendo voz em pacotes de dados digitais.
TOKEN	Sequência de dados que é passada entre os nós para conceder a permissão para transmitir informações. É uma parte fundamental em topologias de rede como Token Ring.
CSMA	Protocolo de controle de acesso ao meio usado em redes de comunicação para verificar se a linha de transmissão está livre antes de enviar dados, reduzindo colisões.
DISPOSITIVOS (OU NÓS)	Qualquer equipamento eletrônico conectado à rede, capaz de enviar, receber ou transmitir informações, como computadores, impressoras e switches.
DISPOSITIVOS INTERMEDIÁRIOS	Equipamentos em uma rede que facilitam a comunicação e o fluxo de dados entre dispositivos finais, como roteadores, switches e hubs.
DISPOSITIVOS FINAIS	Equipamentos em uma rede que são os destinatários ou origem de dados na rede, como computadores, telefones e servidores.
HUB	Dispositivo que conecta múltiplos dispositivos em uma rede, retransmitindo pacotes de dados a todas as portas.
BRIDGE	Dispositivo que conecta e gerencia o tráfego entre dois segmentos de rede, responsável por filtrar ou encaminhar frames baseando-se nos Endereços MAC.
SWITCH	Dispositivo de rede que conecta múltiplos dispositivos em uma rede local, podendo enviar dados diretamente de um dispositivo para outro de maneira eficiente.
ROTEADOR	Dispositivo que encaminha pacotes de dados entre redes. Ele utiliza endereços IP para determinar o melhor caminho para encaminhar cada pacote de dados.
ACCESS POINT	Dispositivo em uma rede sem fio que permite a dispositivos sem fio se conectarem a uma rede com fio, atuando como um intermediário entre dispositivos sem fio e a rede.
HOTSPOT	Local que oferece acesso à Internet por meio de uma rede sem fio, geralmente usando Wi-Fi, disponível em locais públicos como cafés, aeroportos ou hotéis.
MODEM	Dispositivo que modula e demodula sinais digitais e analógicos, permitindo a comunicação de dados por meio de linhas telefônicas ou outras mídias de transmissão.
GATEWAY	Dispositivo de rede que atua como um ponto de entrada ou saída de uma rede, permitindo a comunicação entre redes diferentes, geralmente com protocolos e arquiteturas diferentes.
SIMPLEX	Direção de Transmissão em que os dados são transmitidos em apenas uma direção, sem a capacidade de resposta do receptor, como um sistema de radiodifusão.
HALF-DUPLEX	Direção de Transmissão em que os dados podem ser transmitidos em ambas as direções, mas não simultaneamente.
FULL-DUPLEX	Direção de Transmissão em que os dados são transmitidos em ambas as direções simultaneamente.
UNICAST	Modo de transmissão de dados em que os dados são enviados de um único remetente para um único receptor.
MULTICAST	Modo de transmissão de dados em que os dados são enviados de um único remetente para múltiplos receptores simultaneamente.
BROADCAST	Modo de transmissão de dados em que uma mensagem é enviada de um único remetente para todos os receptores dentro de uma rede.
FLUXO DE DADOS	Movimento de dados entre locais, dispositivos ou componentes, geralmente referindo-se ao transporte de informações em redes de computadores.
LATÊNCIA	Tempo que leva para um pacote de dados viajar de sua origem até seu destino, medindo o atraso na comunicação de dados.
COLISÃO	Evento em redes em que dois ou mais dispositivos tentam enviar um pacote de dados simultaneamente na mesma rede ou canal, resultando em interferência e perda de dados.

LINK DEDICADO	Conexão de rede estabelecida exclusivamente entre dois dispositivos, garantindo uma via constante e exclusiva para a transmissão de dados.
LINK COMPARTILHADO	Conexão de rede na qual múltiplos dispositivos utilizam o mesmo canal ou meio de comunicação, compartilhando a largura de banda disponível.
CONEXÃO PONTO-A-PONTO	Tipo de conexão de rede onde dois dispositivos são conectados diretamente um ao outro sem intermediários, permitindo comunicação direta.
CONEXÃO PONTO-MULTIPONTO	Tipo de conexão em que um único dispositivo central se conecta a múltiplos dispositivos, formando uma rede de comunicação de uma para muitas conexões.
ARQUITETURA PONTO-A-PONTO	Modelo de rede em que cada dispositivo pode funcionar tanto como cliente quanto como servidor, permitindo compartilhamento direto de arquivos e recursos.
ARQUITETURA CLIENTE/SERVIDOR	Modelo de rede em que um servidor central fornece recursos ou serviços, e os clientes acessam esses serviços.
MEIO GUIADO	Tipo de meio de transmissão em que os sinais são direcionados ao longo de um caminho físico, como cabos e fios.
MEIO NÃO GUIADO	Meio de transmissão que utiliza ondas de rádio, micro-ondas ou infravermelho para transmitir dados pelo ar ou espaço, sem a necessidade de um caminho físico.
CABO COAXIAL	Tipo de cabo usado para transmitir sinais elétricos, caracterizado por um núcleo interno de metal rodeado por um isolante, um condutor externo de metal e uma capa externa.
CABO DE PAR TRANÇADO	Cabo composto por pares de fios entrelaçados que são usados para reduzir a interferência eletromagnética e aumentar a confiabilidade na transmissão de dados.
FIBRA ÓPTICA	Meio de transmissão de dados que utiliza luz para transmitir informações através de fibras de vidro ou plástico.
CONECTOR BNC	Tipo de conector usado principalmente com cabos coaxiais, caracterizado por sua conexão de baioneta que oferece uma conexão rápida e segura.
CONECTOR RJ-45	Tipo de conector usado principalmente em cabos de par trançado para redes Ethernet, comumente utilizado para conectar computadores a redes locais.
ARQUITETURA TCP/IP	Conjunto de protocolos usados para interligar dispositivos em redes. Baseia-se em camadas de protocolos que abrangem funções desde a comunicação básica até aplicações avançadas.
MODELO OSI	Modelo conceitual criado para padronizar as funções de um sistema de telecomunicações ou computação em sete camadas abstratas, desde a camada física até a camada de aplicação.
INTERNET	Rede global de computadores interconectados que utilizam o padrão TCP/IP para servir bilhões de usuários em todo o mundo, facilitando a troca de informações e comunicação.
WWW	Sistema de documentos e recursos interligados por links de hipertexto, acessíveis pela Internet e visualizados por navegadores web.
SURFACE WEB	Parte da Web que é indexada por motores de busca convencionais e acessível ao público em geral.
DEEP WEB	Parte da Internet que não é indexada por motores de busca convencionais, incluindo páginas protegidas por senha, bancos de dados privados, entre outros.
DARK WEB	Parte da Deep Web intencionalmente escondida e inacessível através de navegadores web convencionais, frequentemente associada com atividades ilegais.
FERRAMENTAS DE BUSCA	Programas ou serviços online que permitem aos usuários pesquisar conteúdo na Internet, geralmente através de palavras-chave ou consultas (Ex: Google, Bing, etc).
REDE TOR	Rede de servidores voluntários que permite o anonimato na Internet através do encaminhamento de tráfego através de múltiplas camadas de servidores.

INTELIGÊNCIA ARTIFICIAL	Área computacional que envolve a criação de máquinas capazes de realizar tarefas que normalmente requerem inteligência humana, como aprendizado, raciocínio e adaptação.
NAVEGADOR WEB	Software utilizado para acessar e visualizar páginas da Web na Internet, interpretando e exibindo conteúdos HTML e outros.
BITTORRENT	Protocolo para compartilhamento de arquivos Peer-To-Peer (P2P), permitindo a distribuição de dados e arquivos eletrônicos pela Internet de maneira descentralizada.
REDES CELULARES	Sistemas que usam uma rede distribuída de estações base (antenas de celular) para fornecer conectividade móvel e comunicação sem fio em uma área geográfica ampla.
ISP	Empresa que fornece serviços de acesso à Internet para clientes, oferecendo diferentes tipos de conexões, como banda larga, fibra óptica, entre outras.
DIAL-UP	Tipo de acesso à Internet de baixa velocidade que utiliza linhas telefônicas convencionais e um modem para conectar-se à Internet.
ADSL	Tipo de conexão de banda larga que utiliza as linhas telefônicas existentes para transmitir dados, oferecendo maior velocidade de download em relação ao upload.
HFC	Tecnologia de rede que combina fibra óptica e cabos coaxiais para entrega de serviços de Internet e TV a Cabo.
FIBRA ÓPTICA	Tecnologia de transmissão de dados de alta velocidades que utiliza fibras de vidro ou plástico para conduzir luz.
PLC	Tecnologia que permite a transmissão de dados por meio das linhas de energia elétrica existentes, utilizando-as simultaneamente para transmissão de energia e dados.
RADIODIFUSÃO	Método de transmissão de sinais de áudio e vídeo (rádio e TV) através de ondas eletromagnéticas no espaço livre, sem a necessidade de uma conexão física.
SATÉLITE	Tecnologia de comunicação que utiliza satélites artificiais em órbita terrestre para transmitir e receber sinais.
INTERNET DAS COISAS (IOT)	Conexão de dispositivos do cotidiano à internet, permitindo que eles enviem e recebam dados, como eletrodomésticos, carros e sistemas de segurança.
NUVEM (CLOUD)	Armazenamento e processamento de dados em servidores remotos acessíveis pela internet, possibilitando acesso a informações e aplicativos de qualquer lugar.
IPV6	Versão mais recente do Protocolo de Internet, desenvolvida para substituir o IPv4.
AIRDROP	Tecnologia que permite o compartilhamento de arquivos entre dispositivos Apple (como iPhones e Macs) usando Wi-Fi e Bluetooth.
PICONET	Tipo de rede sem fio formada pela conexão entre dispositivos Bluetooth, geralmente consistindo em um dispositivo principal e até sete dispositivos secundários.
SCATTERNET	Rede que interliga várias piconets bluetooth, permitindo que dispositivos comuniquem entre diferentes piconets.
WIMAX	Tecnologia de comunicação sem fio de alta velocidade, destinada a oferecer acesso à internet de banda larga a longas distâncias.
WEP, WPA, WPA2, WPA3	Protocolos de segurança para redes Wi-Fi. WEP é o mais antigo e menos seguro, enquanto WPA, WPA2 e WPA3 são evoluções com segurança aprimorada.
BITCOIN	Primeira e mais conhecida criptomoeda, um tipo de moeda digital que utiliza criptografia para controlar sua criação e gestão, sem a necessidade de uma autoridade central.
CRIPTOMOEDAS	Moedas digitais que usam criptografia para segurança. São descentralizadas e baseadas em tecnologia blockchain, permitindo transações seguras e anônimas.

QUESTÕES COMENTADAS – VUNESP

1. **(VUNESP / TCM-SP - 2023)** O protocolo de segurança WPA2, baseado no padrão sem-fio 802.11i,

a) introduziu melhorias em relação ao WPA, como o uso do Advanced Encryption Standard (AES), aprovado pelo governo dos EUA para ser usado como padrão para a criptografia de informações classificadas como secretas.

b) apresenta uma vantagem em relação ao WPA, que é a menor quantidade de processamento que ele necessita para proteger a rede, devido à otimização realizada nesse protocolo, que pode apresentar bom desempenho mesmo em um hardware menos potente.

c) ao contrário do WPA, não é vulnerável a ataques por meio do Wi-Fi Protected Setup (WPS), recomendando-se sempre a ativação deste para proteger a rede.

d) suporta apenas a criptografia Temporal Key Integrity Protocol (TKIP), enquanto o WPA suporta apenas a Advanced Encryption Standard (AES)

e) tem a sua segurança dependente do tamanho da senha que for definida, permitindo o uso de senhas de até 255 caracteres, ao contrário do WPA, que permite usar senhas de até 31 caracteres.

Comentários:

(a) Correto. O protocolo de segurança WPA2, baseado no padrão sem-fio 802.11i, introduziu melhorias em relação ao WPA, como o uso do Advanced Encryption Standard (AES), aprovado pelo governo dos EUA para ser usado como padrão para a criptografia de informações classificadas como secretas. O AES é um algoritmo de criptografia de bloco simétrico que é considerado muito seguro e difícil de quebrar. O WPA também usa criptografia, mas o algoritmo usado é o Temporal Key Integrity Protocol (TKIP). O TKIP é mais vulnerável a ataques do que o AES, por isso o WPA2 é considerado mais seguro.

(b) Errado. WPA2 exige mais processamento do que o WPA. Isso ocorre porque o WPA2 usa o AES, que é um algoritmo de criptografia mais complexo do que o TKIP; (c) Errado. WPA2 é vulnerável a ataques por meio do WPS. O WPS é um protocolo que facilita a configuração de redes sem fio, mas ele também é um ponto fraco de segurança; (d) Errado. O WPA2 suporta tanto o AES quanto o TKIP. O WPA, por outro lado, só suporta o TKIP; (e) Errado. A segurança do WPA2 não depende do tamanho da senha. O WPA2 é seguro mesmo com senhas curtas. No entanto, senhas mais longas são mais difíceis de serem adivinhadas, por isso são recomendadas.

Gabarito: Letra A

2. **(VUNESP / PC-SP – 2022)** No mundo da Internet, mais recentemente têm vindo à tona dois termos a ela relativos, ou seja, *deepweb* e *darkweb*, sobre os quais é correto afirmar que:

a) a *darkweb* não tem seus sites indexados por navegadores convencionais como Google Chrome ou Firefox.
b) os sites da *deepweb* utilizam o domínio .onion.
c) não há navegadores que consigam acessar a *darkweb*.
d) *deepweb* e darkweb são duas denominações que endereçam ao mesmo conteúdo da Internet.
e) o site Silk Road tinha seu acesso por meio da *deepweb*.

Comentários:

(a) Errado, navegadores não indexam sites – quem o faz são mecanismos de busca e pesquisa, como Google, Bing, etc; (b) Errado, sites da *dark web* (que é parte da *deep web*) utilizam o domínio .onion; (c) Errado, há navegadores específicos para acessar a *dark web*; (d) Errado, *deep web* se refere a qualquer página que não é indexada por mecanismos de busca e *dark web* é a parte da *deep web* que é destinada geralmente a atividades ilegais; (e) Errado, o seu acesso era por meio da *dark web*.

O gabarito preliminar foi Letra (a), no entanto navegadores jamais seriam capazes de indexar conteúdos quaisquer, seja da Surface web da Deep web ou da Dark web, não sendo esta portanto uma característica que pudesse apontar alternativa a ser considerada como correta. Acredito que a questão será anulada no gabarito definitivo!

Gabarito: Letra A

---

3. **(VUNESP / PC-SP – 2022)** Existe uma parte da Internet considerada como uma Internet invisível, também chamada de deep web. Assinale a afirmação correta relacionada com a deep web:

a) A deep web tem como sinônimo dark web, não existindo diferenças entre esses termos.

b) Ela é acessível pelos mecanismos de busca tradicionais, e é composta de *sites* e conteúdos que não são públicos por serem todos ilegais.

c) Ela é uma zona da internet que pode ser detectada e acessada facilmente por qualquer motor de busca tradicional, como o Google ou o Bing.

d) Na deep web, o conteúdo invisível é sempre mais inseguro e ilegal.

e) A maioria das páginas presentes na deep web é mantida oculta do navegador de Internet para proteger informações e privacidade do usuário.

Comentários:

(a) Errado, são conceitos diferentes! Deep Web é a parte da Web que não pode ser indexada por mecanismos de busca tradicionais e Dark Web é uma parte da Deep Web que é voltada geralmente para a prática de atividades ilegais; (b) Errado, ela não é acessível pelos mecanismos de busca tradicionais e os sites/conteúdos podem ser totalmente legais; (c) Errado, ela não pode ser detectada ou acessada facilmente por motores de busca tradicionais; (d) Errado, a maioria dos conteúdos da deep web são seguros e legais; (e) Correto.

Gabarito: Letra E

---

4. **(VUNESP / PC-SP – 2018)** Atualmente, é muito comum realizar o acesso à Internet por meio de uma conexão sem fio disponibilizado por Access Points ou Roteadores fixos ou móveis. Dentre os esquemas de segurança disponibilizados nesse tipo de comunicação, o que fornece mais proteção é o:

a) WPA.
b) WiFi.
c) WPS.
d) WEP.
e) WPA2.

Comentários:

(a) Errado. WPA (Wi-Fi Protected Access) é mecanismo desenvolvido para resolver algumas das fragilidades do WEP – é o nível mínimo de segurança que é recomendado atualmente; (b) Errado, Wi-Fi é o nome da tecnologia wireless; (c) Errado. WPS (Wi-Fi Protected Setup) é um recurso de roteadores para configurar uma rede Wi-Fi; (d) Errado. WEP (Wired Equivalent Privacy) é primeiro mecanismo de segurança a ser lançado – é considerado frágil e, por isto, o uso deve ser evitado; (e) Correto. WPA-2 (Wi-Fi Protected Access 2) é similar ao WPA, mas com criptografia considerada mais forte – é o mecanismo mais recomendado atualmente.

Gabarito: Letra E

---

5. **(VUNESP / PC-SP – 2018)** Para se realizar a comunicação de dados (comunicação digital), pode-se utilizar diversos tipos de meios de transmissão. Dentre os tipos de meios, o que apresenta maior velocidade de transmissão é:

a) Satélite.
b) PLC (comunicação pelo cabo de energia).
c) Fibra ótica.
d) Sem fio Wi-Fi.
e) Cabo ADSL.

Comentários:

Atualmente, o tipo de meio que apresenta maior velocidade de transmissão é a fibra óptica (até 10 Gbps).

Gabarito: Letra C

---

6. **(VUNESP / PC-SP – 2018)** Considere o seguinte cenário típico de acesso à Internet:

Um usuário doméstico faz acesso à Internet por meio de um serviço contratado de acesso por fibra ótica, tendo na sua residência um equipamento conectado à fibra e que disponibiliza acesso sem fio.

Nesse cenário, o acesso à Internet disponibilizado pelo serviço contratado é realizado pelo:

a) Portal Internet.
b) Servidor.
c) Web server.
d) Cliente Internet.
e) Provedor.

Comentários:

O acesso à internet é disponibilizado pelo serviço contratado é realizado pelo Provedor de Serviço de Internet (ISP – Internet Service Provider). Portal Internet é apenas um site que oferece diversos recursos web; Servidor é uma máquina especializada em fornecer diversos serviços; Web Server é um servidor de internet; Cliente Internet é uma aplicação local que permite acessar a web.

Gabarito: Letra E

---

7. **(VUNESP / PC-SP – 2014)** Na montagem de uma rede local, para interligar um grupo de 4 computadores, é utilizado cabeamento estruturado padrão CAT-5. O elemento de rede usado para interligar esses computadores chama-se comutador, e o cabo usado para interligar o computador com o comutador chama-se "cabo fim a fim". O conector usado na montagem desse cabo é:

a) TI-578.
b) RX-45.
c) RJ-45.
d) BSI-8.
e) ATC-32.

Comentários:

O conector utilizado em um cabo do tipo CAT-5 (Par Trançado) é o RJ-45.

Gabarito: Letra C

---

8. **(VUNESP / TJ-SP – 2012)** Uma rede sem fio de computadores é muito vulnerável ao acesso indevido às informações. Assim, os padrões de rede sem fio, como o IEEE 802.11g, oferecem esquemas que melhoram a segurança. Dentre as alternativas apresentadas, a que oferece maior segurança no IEEE 802.11g é:

a) SSID.
b) TKP
c) WEP.
d) WiFi.
e) WPA.

Comentários:

Atualmente, o mecanismo que oferece mais segurança é o WPA-2. No entanto, a questão pergunta qual é o mecanismo dentre os listados que fornecem mais segurança. (a) Errado, SSID (Service Set IDentification) é simplesmente o nome que identifica uma rede sem fio; (b) Errado, TKP (Temporal Key Integrity Protocol) é um protocolo de segurança de redes sem fio que foi criado para resolver problemas de segurança do WEP, mas foi logo descontinuado; (c) Errado. WEP (Wired Equivalent Privacy) é primeiro mecanismo de segurança a ser lançado – é considerado frágil e, por isto, o uso deve ser evitado; (e) Correto. WPA (Wi-Fi Protected Access) é mecanismo desenvolvido para resolver algumas das fragilidades do WEP – é o nível mínimo de segurança que é recomendado atualmente.

Gabarito: Letra E

---

9. **(VUNESP / TJ-SP – 2012)** Os padrões para a rede sem fio em computadores, utilizados para as redes locais (LANs), são originários do padrão IEEE 802.11. Nesse padrão, a versão IEEE 802.11.b estabelece uma largura de banda de até:

a) 11 Mbps.
b) 20 Mbps.
c) 54 Mbps.
d) 100 Mbps.
e) 200 Mbps.

Comentários:

PADRÃO	FREQUÊNCIA	TAXA MÁXIMA DE TRANSMISSÃO
IEEE 802.11B	2.4 Ghz	11 Mbps
IEEE 802.11A	5.0 Ghz	54 Mbps
IEEE 802.11G	2.4 Ghz	54 Mbps
IEEE 802.11N	2.4 ou 5.0 Ghz	150, 300 até 600 Mbps
IEEE 802.11AC	5.0 Ghz	500 Mbps, 1 Gbps ou +

Conforme podemos ver na tabela, a largura de banda é de 11 Mbps.

Gabarito: Letra A

---

10. (VUNESP / TJ-SP – 2012) Considere a implantação física de uma rede local de computadores com cabeamento estruturado. Utilizando a tecnologia com cabos de pares trançados, a topologia estabelecida para a arquitetura física da rede é denominada:

a) Anel.
b) Estrela.
c) Distribuída.
d) Ramificada.
e) Barramento.

Comentários:

Em regra, a tecnologia que utiliza cabos de par trançado em uma rede local possui uma arquitetura física denominada Estrela (o mais correto seria chamar de topologia física e, não, arquitetura).

Gabarito: Letra B

---

11. (VUNESP / TJ-SP – 2012) Para realizar a conexão física e o gerenciamento das conexões por meio do endereço MAC (ou Ethernet) entre os computadores de uma rede local de computadores (LAN), deve-se utilizar o equipamento de rede denominado:

a) Bridge.
b) Switch.
c) Router.
d) Firewall.
e) Gateway.

Comentários:

Gerenciamento de conexões por meio do Endereço MAC? Trata-se do Switch! Bridge possui apenas duas portas; Router trabalho com Endereço IP; Firewall é um mecanismo de segurança para controle de tráfego entre redes; Gateway é um equipamento que conecta redes distintas.

Gabarito: Letra B

LISTA DE QUESTÕES – VUNESP

1. **(VUNESP / TCM-SP - 2023)** O protocolo de segurança WPA2, baseado no padrão sem-fio 802.11i,

   a) introduziu melhorias em relação ao WPA, como o uso do Advanced Encryption Standard (AES), aprovado pelo governo dos EUA para ser usado como padrão para a criptografia de informações classificadas como secretas.

   b) apresenta uma vantagem em relação ao WPA, que é a menor quantidade de processamento que ele necessita para proteger a rede, devido à otimização realizada nesse protocolo, que pode apresentar bom desempenho mesmo em um hardware menos potente.

   c) ao contrário do WPA, não é vulnerável a ataques por meio do Wi-Fi Protected Setup (WPS), recomendando-se sempre a ativação deste para proteger a rede.

   d) suporta apenas a criptografia Temporal Key Integrity Protocol (TKIP), enquanto o WPA suporta apenas a Advanced Encryption Standard (AES)

   e) tem a sua segurança dependente do tamanho da senha que for definida, permitindo o uso de senhas de até 255 caracteres, ao contrário do WPA, que permite usar senhas de até 31 caracteres.

2. **(VUNESP / PC-SP – 2022)** No mundo da Internet, mais recentemente têm vindo à tona dois termos a ela relativos, ou seja, *deepweb* e *darkweb*, sobre os quais é correto afirmar que:

   a) a *darkweb* não tem seus sites indexados por navegadores convencionais como Google Chrome ou Firefox.
   b) os sites da *deepweb* utilizam o domínio .onion.
   c) não há navegadores que consigam acessar a *darkweb*.
   d) *deepweb* e darkweb são duas denominações que endereçam ao mesmo conteúdo da Internet.
   e) o site Silk Road tinha seu acesso por meio da *deepweb*.

3. **(VUNESP / PC-SP – 2022)** Existe uma parte da Internet considerada como uma Internet invisível, também chamada de deep web. Assinale a afirmação correta relacionada com a deep web:

   a) A deep web tem como sinônimo dark web, não existindo diferenças entre esses termos.

   b) Ela é acessível pelos mecanismos de busca tradicionais, e é composta de *sites* e conteúdos que não são públicos por serem todos ilegais.

c) Ela é uma zona da internet que pode ser detectada e acessada facilmente por qualquer motor de busca tradicional, como o Google ou o Bing.

d) Na deep web, o conteúdo invisível é sempre mais inseguro e ilegal.

e) A maioria das páginas presentes na deep web é mantida oculta do navegador de Internet para proteger informações e privacidade do usuário.

4. **(VUNESP / PC-SP – 2018)** Atualmente, é muito comum realizar o acesso à Internet por meio de uma conexão sem fio disponibilizado por Access Points ou Roteadores fixos ou móveis. Dentre os esquemas de segurança disponibilizados nesse tipo de comunicação, o que fornece mais proteção é o:

a) WPA.
b) WiFi.
c) WPS.
d) WEP.
e) WPA2.

5. **(VUNESP / PC-SP – 2018)** Para se realizar a comunicação de dados (comunicação digital), pode-se utilizar diversos tipos de meios de transmissão. Dentre os tipos de meios, o que apresenta maior velocidade de transmissão é:

a) Satélite.
b) PLC (comunicação pelo cabo de energia).
c) Fibra ótica.
d) Sem fio Wi-Fi.
e) Cabo ADSL.

6. **(VUNESP / PC-SP – 2018)** Considere o seguinte cenário típico de acesso à Internet:

Um usuário doméstico faz acesso à Internet por meio de um serviço contratado de acesso por fibra ótica, tendo na sua residência um equipamento conectado à fibra e que disponibiliza acesso sem fio.

Nesse cenário, o acesso à Internet disponibilizado pelo serviço contratado é realizado pelo:

a) Portal Internet.
b) Servidor.
c) Web server.
d) Cliente Internet.
e) Provedor.

7. **(VUNESP / PC-SP – 2014)** Na montagem de uma rede local, para interligar um grupo de 4 computadores, é utilizado cabeamento estruturado padrão CAT-5. O elemento de rede usado para interligar esses computadores chama-se comutador, e o cabo usado para interligar o computador com o comutador chama-se "cabo fim a fim". O conector usado na montagem desse cabo é:

a) TI-578.
b) RX-45.
c) RJ-45.
d) BSI-8.
e) ATC-32.

8. **(VUNESP / TJ-SP – 2012)** Uma rede sem fio de computadores é muito vulnerável ao acesso indevido às informações. Assim, os padrões de rede sem fio, como o IEEE 802.11g, oferecem esquemas que melhoram a segurança. Dentre as alternativas apresentadas, a que oferece maior segurança no IEEE 802.11g é:

a) SSID.
b) TKP
c) WEP.
d) WiFi.
e) WPA.

9. **(VUNESP / TJ-SP – 2012)** Os padrões para a rede sem fio em computadores, utilizados para as redes locais (LANs), são originários do padrão IEEE 802.11. Nesse padrão, a versão IEEE 802.11.b estabelece uma largura de banda de até:

a) 11 Mbps.
b) 20 Mbps.
c) 54 Mbps.
d) 100 Mbps.
e) 200 Mbps.

10. **(VUNESP / TJ-SP – 2012)** Considere a implantação física de uma rede local de computadores com cabeamento estruturado. Utilizando a tecnologia com cabos de pares trançados, a topologia estabelecida para a arquitetura física da rede é denominada:

a) Anel.
b) Estrela.
c) Distribuída.
d) Ramificada.
e) Barramento.

11. **(VUNESP / TJ-SP – 2012)** Para realizar a conexão física e o gerenciamento das conexões por meio do endereço MAC (ou Ethernet) entre os computadores de uma rede local de computadores (LAN), deve-se utilizar o equipamento de rede denominado:

a) Bridge.
b) Switch.
c) Router.
d) Firewall.
e) Gateway.

GABARITO – VUNESP

1. LETRA A
2. LETRA A
3. LETRA E
4. LETRA E
5. LETRA C
6. LETRA E
7. LETRA C
8. LETRA E
9. LETRA A
10. LETRA B
11. LETRA B

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.



Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.