Estratégia Concursos

Aula 00

PC-SP (Perito Criminal) Informática

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

23 de Abril de 2024

Índice

REDES DE COMPUTADORES

Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

REDES DE COMPUTADORES

Redes de computadores são sistemas interconectados de dispositivos que permitem a troca de dados e o compartilhamento de recursos entre diferentes dispositivos. Elas facilitam a comunicação e colaboração digital, abrangendo desde pequenas redes locais até a vasta rede global conhecida como Internet.

Fala, galera! **Vamos iniciar nossos estudos sobre os Conceitos Básicos de Redes de Computadores** – além de ser um assunto de suma importância, ele subsidia tudo que veremos mais à frente sobre Internet. *Beleza?* Agora vamos contar uma história! No Século XIX, enviar uma carta de Londres até Califórnia por meio dos correios demorava entre dois e três meses – isso se você tivesse grana suficiente para pagar pelo envio de cartas. *Incrível, não?*

Hoje em dia, enviar um correio eletrônico demora uma fração de segundos. Isso melhorou a eficiência das indústrias, dinamizou o comércio global e melhorou a economia mundial fazendo com que chegássemos em alta velocidade a praticamente qualquer ponto do planeta. Galera, vocês podem até pensar que os computadores e as redes de computadores sempre andaram juntos, mas não funcionava assim – as redes vieram bem depois!

Durante a década de 1970, os computadores ficavam isolados no mundo – praticamente não se comunicavam. **Nessa época, eles tinham o tamanho de uma geladeira, às vezes de uma sala**

e, às vezes, até de um andar inteiro de prédios ou universidades. Os computadores pessoais[1] ainda não tinham se popularizado, apesar de – em 1977 – um cara chamado Steve Jobs ter lançado um microcomputador com teclado integrado e... pasmem... capaz de gerar gráficos **coloridos**.

Enfim, nessa época, **era comum termos um processamento centralizado**, ou seja, um único computador de grande porte – chamado Mainframe – de alto custo e que rodava em geral poucas e simples aplicações. Na década seguinte, com a popularização dos computadores pessoais, as Redes de Computadores foram ganhando espaço, uma vez que as pessoas descobriram que era muito mais interessante compartilhar dados e recursos.

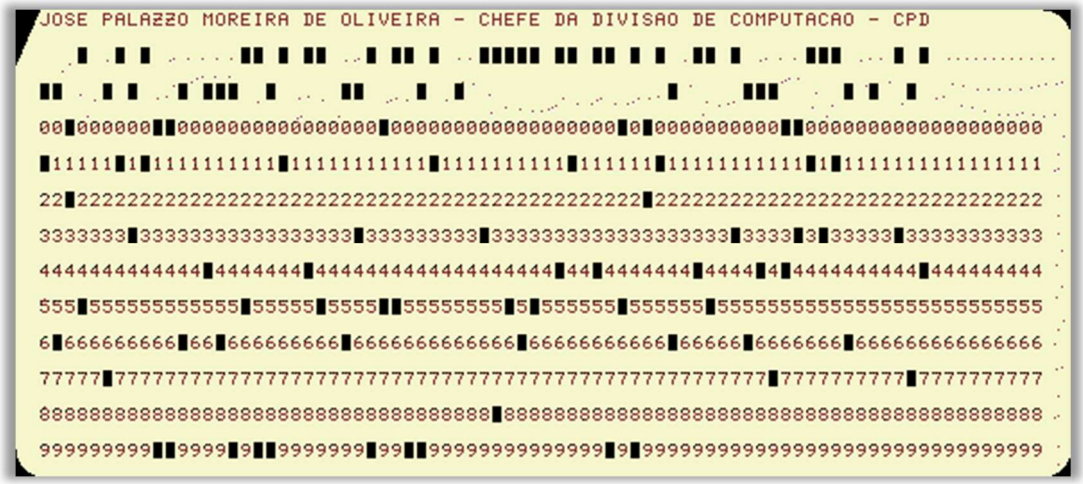
Do processamento que ocorria integralmente centralizado nos computadores de grande porte, **passamos para um processamento distribuído nos computadores pessoais de uma rede**. Dessa forma, em vez de um único mainframe ser responsável por todo processamento, computadores distintos espalhados em uma rede realizavam parte desse trabalho. Dito isso, chegou a hora de saber o conceito de uma rede:

> *"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 organização**.

[1] Computadores Pessoais são também conhecidos como *Personal Computers* (PC), *Workstations* ou Estações de Trabalho.



Sim, antigamente os dados de um computador ficavam armazenados em pequenos cartões de papel cheios de furinhos, chamado de cartões perfurados; ou em um rolo enorme de fita magnética. Se você quisesse trocar informações entre pessoas ou equipamentos, **você tinha que transportar pilhas enormes desses cartões perfurados ou de fitas magnéticas até o local onde se encontrava o destinatário**. *Já imaginaram isso?*

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?*

(PROF. DIEGO / INÉDITA – 2024) Redes de computadores consistem em um conjunto de dispositivos eletrônicos interconectados para compartilhar recursos e informações.

Comentários: essa é uma das definições fundamentais de redes de computadores. As redes de computadores realmente permitem a conexão de dispositivos para compartilhar recursos, como arquivos, impressoras e acesso à internet, além de permitir a troca de informações entre esses dispositivos (Correto).

(PROF. DIEGO / INÉDITA – 2024) Redes de computadores não desempenham um papel fundamental na comunicação e conectividade global na era da informação.

Comentários: as redes de computadores desempenham um papel crítico na comunicação global, conectividade e na disseminação de informações na era da informação – elas são a espinha dorsal da comunicação digital global (Errado).

(PROF. DIEGO / INÉDITA – 2024) As redes de computadores são sistemas centralizados que não permitem a comunicação distribuída.

Comentários: as redes de computadores permitem comunicação distribuída, conectando dispositivos em todo o mundo e permitindo a troca de informações de forma descentralizada (Errado).

(PROF. DIEGO / INÉDITA – 2024) As redes de computadores representam uma infraestrutura de comunicação que possibilita a troca de dados apenas em nível local.

Comentários: redes de computadores não se limitam a nível local; elas permitem a comunicação e a troca de dados em níveis locais, regionais, nacionais e globais, tornando possível a comunicação em alta escala (Errado).

(PROF. DIEGO / INÉDITA – 2024) As redes de computadores servem como um meio para conectar o mundo digital e não têm impacto na vida cotidiana das pessoas.

Comentários: redes de computadores têm um impacto profundo na vida cotidiana das pessoas, desde permitir a comunicação instantânea via internet até fornecer acesso a serviços online, como compras, bancos e mídias sociais – a primeira parte da questão está perfeita (Errado).

(UEG / Assembleia Legislativa de Goiás – 2006) Um conjunto de unidades processadoras interconectadas que permite, inclusive, o compartilhamento de recursos tais como impressoras, discos, entre outros, denomina-se:

a) Time Sharing
b) Redes de Computadores
c) Compartilhamento do Windows
d) Interligação de Redes de Computadores

Comentários: quando a banca diz "*um conjunto de unidades processadoras*", ela só está usando um nome técnico para "*um conjunto de computadores*". Logo, um conjunto de computadores interconectados que permite o compartilhamento de recursos tais como impressoras, discos, entre outros, só pode ser uma... rede de computadores (Letra B).

Tipos de Conexão/Enlace

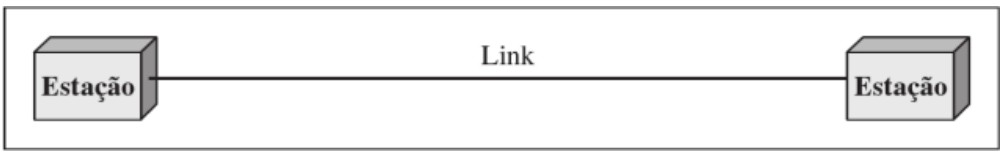
INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Tipos de Conexão

Um link, conexão ou enlace refere-se ao meio físico ou lógico que conecta dois ou mais dispositivos, permitindo a transmissão de dados entre eles. Este link pode ser estabelecido usando uma variedade de mídias, como cabos de fibra óptica, fios de cobre, ou através de conexões sem fio como Wi-Fi ou rádio.

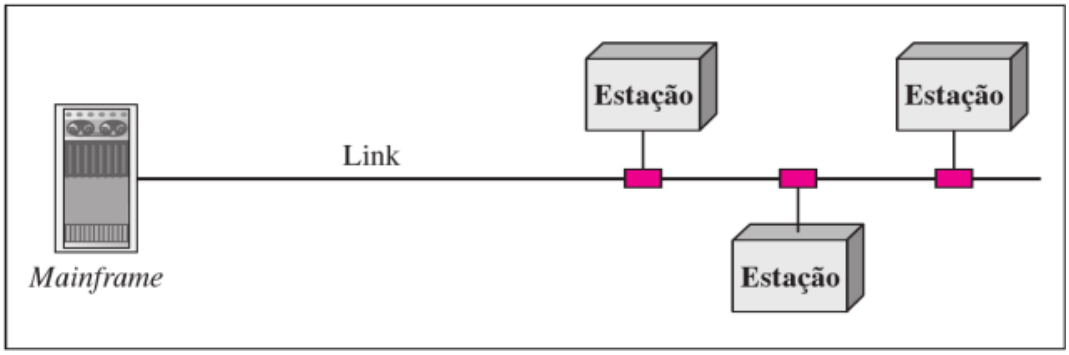
Redes são dois ou mais dispositivos conectados através de links. *O que é um link?* **Também chamado de enlace, trata-se de um caminho de comunicação que transfere dados de um dispositivo para outro.** Para fins de visualização, é mais simples imaginar qualquer link como uma reta entre dois pontos. Para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

(PROF. DIEGO / INÉDITA – 2023) Uma conexão ponto-a-ponto é aquela em que vários dispositivos compartilham o mesmo meio de transmissão, e a comunicação ocorre diretamente entre dois dispositivos, sem a necessidade de compartilhar o meio com outros.

Comentários: a descrição inicial refere-se a uma conexão ponto-multiponto, onde vários dispositivos compartilham o mesmo meio. A conexão ponto-a-ponto é uma conexão direta entre exatamente dois dispositivos – sem compartilhamento (Errado).

(PROF. DIEGO / INÉDITA – 2023) Uma conexão ponto-multiponto permite a comunicação direta entre dois dispositivos, sem a necessidade de compartilhar o meio de transmissão com outros.

Comentários: uma conexão ponto-multiponto é aquela em que vários dispositivos compartilham o mesmo meio de transmissão, e a comunicação ocorre entre um dispositivo central e vários dispositivos remotos (Errado).

(CESPE / MPU – 2010) Em rede multiponto, há diversos computadores interligados em um mesmo circuito, no entanto o circuito só pode ser utilizado por um computador de cada vez.

Comentários: todos os computadores estão conectados a um link compartilhado – denominado pela questão como circuito. Somente um computador por vez pode enviar dados, caso contrário ocorrerá uma colisão. Se a questão não detalhar qual é o tipo de conexão compartilhada, consideramos que se trata compartilhamento no tempo como padrão (Correto).

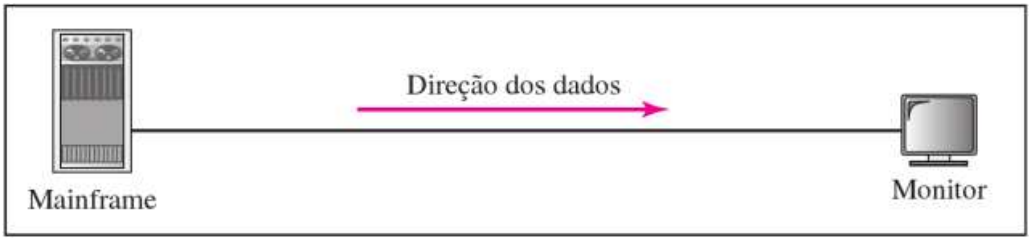
Direções de Transmissão

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

DIREÇÃO DE TRANSMISSÃO

As direções de transmissão em redes de computadores referem-se ao fluxo de dados entre dispositivos e são categorizadas principalmente em: Simplex, Half-Duplex e Full-Duplex.

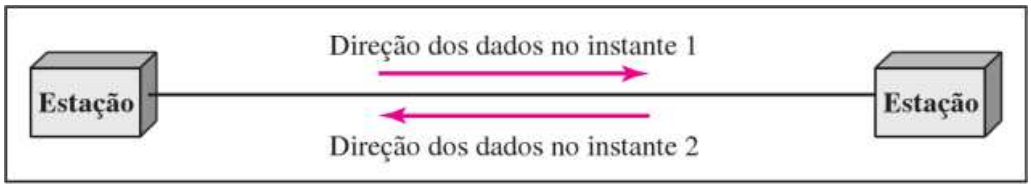
Simplex



O enlace é utilizado apenas em um dos dois possíveis sentidos de transmissão
Exemplo: TV, Rádio AM/FM, Teclado, etc.

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. Quando você vê TV, sua antena recebe um sinal de um satélite, mas ela jamais envia/transmite sinais para o satélite. Logo, o satélite é o transmissor, sua antena é o receptor, e esses papéis não são trocados – o mesmo serve para Rádio AM/FM ou para o teclado de um computador.

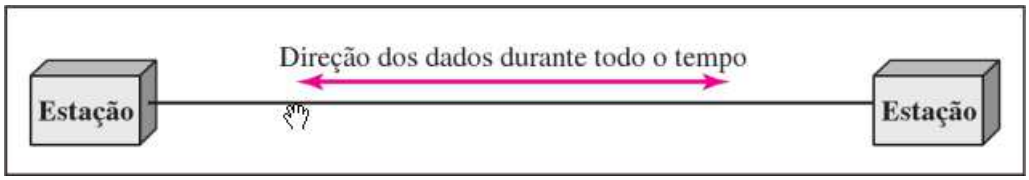
Half-Duplex



O enlace é utilizado nos dois possíveis sentidos de transmissão, porém apenas um por vez
Exemplo: Walk&Talk e Nextel

Uma comunicação é dita *half-duplex* quando temos um transmissor e um receptor, sendo que ambos podem transmitir e receber dados, porém nunca simultaneamente. Quando você fala em um Walk&Talk com outra pessoa, você pode falar e ela também. Porém, quando você apertar o botãozinho para falar, o receptor apenas ouvirá. Se ele tentar falar junto, a comunicação é cortada e nenhum dos dois se ouvem.

Full-Duplex



O enlace é utilizado nos dois sentidos de transmissão simultaneamente
Ex: Celular, VoIP.

Uma comunicação é dita *full-duplex* quando temos um transmissor e um receptor, sendo que ambos podem transmitir e receber dados simultaneamente. Quando você fala com outra pessoa por meio do seu smartphone, ela pode te responder simultaneamente. Você não tem que falar, depois ouvir, depois falar de novo. Vocês dois podem falar juntos sem problema porque se trata de uma transmissão bidirecional.

(FEPESE / Prefeitura de Balneário Camboriú-SC – 2023) No contexto de redes de computadores, dentre as formas de transmissão, aquela na qual a comunicação ocorre em uma só direção, com papéis definidos de transmissor (Tx) e receptor (Rx), porém passíveis de inversão, é denominada:

a) Simples
b) Monoplex
c) Half Duplex
d) Full Duplex
e) Auto Duplex.

Comentários: a forma de transmissão na qual a comunicação ocorre em uma única direção, com papéis definidos de transmissor (Tx) e receptor (Rx), mas passíveis de inversão, é denominada Half Duplex (Letra C).

(CONSULPLAN / Câmara de Paraupebas-PA – 2022) Comunicação de dados são as trocas de dados entre dois dispositivos por intermédio de algum tipo de meio de transmissão, como um cabo condutor formado por fios. O modo de comunicação no qual cada estação pode transmitir, assim como receber, mas não ao mesmo tempo denomina-se:

a) Duplex
b) Simplex
c) Full-Duplex
d) Half-Duplex.

Comentários: a comunicação no qual cada estação pode transmitir e receber, mas não ao mesmo tempo, é denominada Half-Duplex (Letra D).

(QUADRIX / CRF-PR – 2022) Assinale a alternativa que apresenta o tipo de transmissão de dados em que a transmissão é considerada unidirecional, ou seja, um dispositivo é o transmissor e o outro é o receptor.

a) half-duplex
b) full-duplex
c) full-simplex

d) duplex
e) Simplex

Comentários: a alternativa que apresenta o tipo de transmissão de dados em que a transmissão é considerada unidirecional, ou seja, um dispositivo é o transmissor e o outro é o receptor é Simplex (Letra E).

(QUADRIX / SEDF – 2022) O modo como cada estação pode, ao mesmo tempo, transmitir e receber é conhecido como half-duplex.

Comentários: o modo como cada estação pode, simultaneamente, transmitir e receber é conhecido como full-duplex (Errado).

Modos de Transmissão

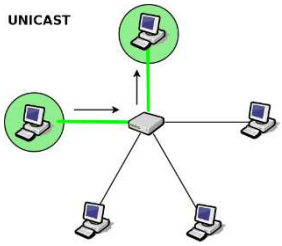
INCIDÊNCIA EM PROVA: BAIXÍSSIMA

MODOS DE TRANSMISSÃO

Em redes de computadores, os modos de transmissão descrevem como os dados são enviados entre os dispositivos na rede com relação à quantidade de destinatários e são categorizados principalmente em: Unicast, Multicast e Broadcast.

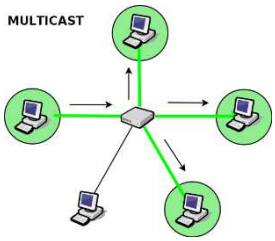
A transmissão de dados em uma rede de computadores pode ser realizada em três modos diferentes: *Unicast*, *Multicast* e *Broadcast*[2]. Vamos vê-los em detalhes:

Unicast [*uni* = um e *cast* = transmitir]



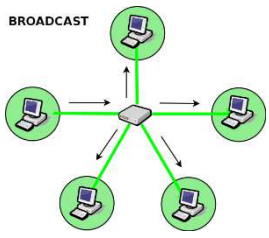
Nessa comunicação, **uma mensagem só pode ser enviada para um destino**. Observem que a primeira estação de trabalho está enviando uma mensagem endereçada especificamente para a 2ª estação de trabalho. Analogamente, quando você envia uma mensagem no Whatsapp para uma pessoa específica, você está enviando 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*.

[2] Existe um quarto tipo bem raro em provas chamado **Anycast**. Nesse modo de transmissão, ocorre a comunicação de um remetente para o destinatário mais próximo em um grupo de destinatários. Esse modo de transmissão é bastante útil em algumas situações bem específicas.

Cuidado: as questões não prezam por um rigor formal com o nome da classificação. *Como assim, Diego?* Vocês encontrarão questões falando sobre Modo, Tipo, Direção, Sentido, Modalidade ou Fluxo de Transmissão (e ainda há outros nomes). **Cada autor chama de uma maneira assim como cada questão – o que vocês precisam saber é que uma classificação se divide em: Simplex, Half-Duplex e Full-Duplex e a outra é Unicast, Multicast e Broadcast.**

(PROF. DIEGO / INÉDITA – 2023) Unicast é um modo de transmissão onde os dados são enviados para vários destinatários ao mesmo tempo.

_____

Comentários: Unicast é um modo de transmissão em que os dados são para um único destinatário e, não, para vários destinatários ao mesmo tempo – trata-se de uma comunicação ponto a ponto (Errado).

(PROF. DIEGO / INÉDITA – 2023) Multicast é um modo de transmissão em que os dados são enviados de um único remetente para um grupo específico de destinatários que se inscreveram no grupo multicast.

_____

Comentários: Multicast é, de fato, um modo de transmissão em que os dados são enviados de um único remetente para um grupo específico de destinatários que expressaram interesse ou se inscreveram nesse grupo multicast (Correto).

(PROF. DIEGO / INÉDITA – 2023) Anycast é um modo de transmissão em que os dados são enviados de um único remetente para o destinatário mais próximo em um grupo de destinatários com o mesmo endereço IP.

_____

Comentários: Anycast é uma técnica de roteamento em que os dados são enviados para o destinatário mais próximo em um grupo de destinatários que compartilham o mesmo endereço IP. Não é necessário entender nada disso agora – é simplesmente entender que esse modo de transmissão existe, é utilizado em casos muito específicos e cai muito raramente em prova (Correto).

(PROF. DIEGO / INÉDITA – 2023) Unicast é amplamente utilizado em redes de difusão de streaming de vídeo para alcançar muitos assinantes ao mesmo tempo.

_____

Comentários: Unicast é geralmente inadequado para redes de difusão de streaming de vídeo – Multicast é mais adequado para essa finalidade, uma vez que permite que os dados sejam enviados eficientemente para um grupo de assinantes interessados, economizando largura de banda e recursos da rede (Errado).

(QUADRIX / CRBM4 – 2021) Quanto à difusão, uma rede de computadores pode ser *anycast*, *multicast*, *broadcast* e *unicast*. No modo unicast, a comunicação não pode ocorrer de forma simultânea entre emissor e receptor.

_____

Comentários: quando a comunicação não pode ocorrer de forma simultânea entre emissor e receptor, temos uma comunicação simplex. A comunicação unicast é aquela em que os dados são enviados para um único destinatário (Errado).

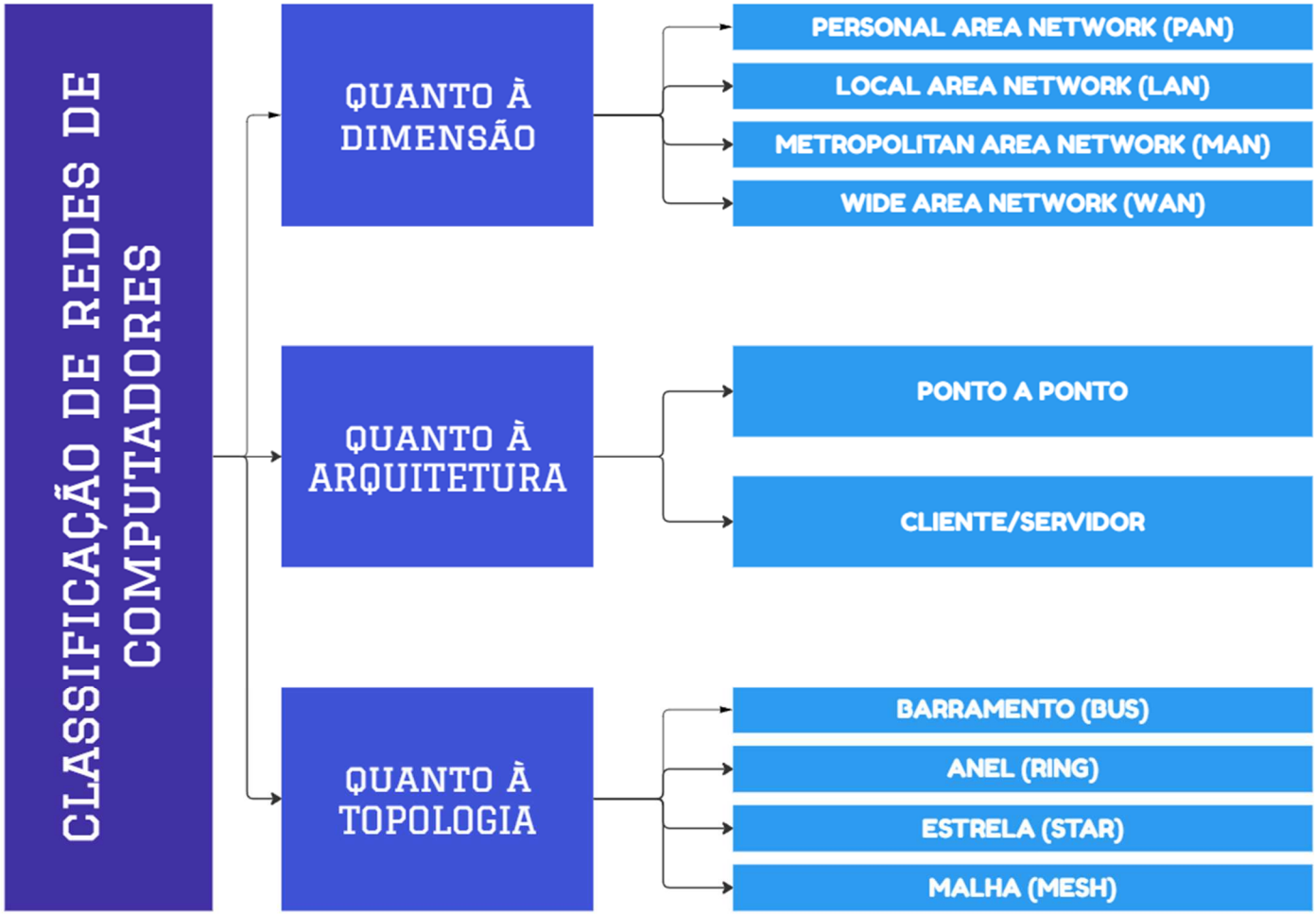
(FCC / TRE-AM – 2010) Uma única mensagem gerada pelo emissor que é destinada a todos os elementos da rede caracteriza uma mensagem:

a) broadcast
b) multicast
c) unicast
d) anycast
e) fullcast

Comentários: quando uma única mensagem é destinada a todos os elementos da rede, temos um broadcast (Letra A).

Classificação de Redes

Neste tópico, vamos falar sobre diversas formas de classificar redes de computadores! Vamos falar da classificação quanto à dimensão, cobertura, tamanho ou área geográfica (PAN, LAN, MAN e WAN); quanto à arquitetura de rede ou forma de interação (ponto-a-ponto e cliente/servidor); e quanto à topologia (barramento, anel, estrela e malha). Existem outras classificações, mas elas não são relevantes para provas de concursos.



Quanto à Dimensão, Tamanho ou Área Geográfica

Uma rede de computadores pode ser classificada quanto à dimensão, tamanho ou abrangência de área geográfica. Galera, nós veremos detalhes sobre as características dessa classificação logo abaixo, no entanto é importante ressaltar uma particularidade a respeito da distância que essas redes de computadores podem abranger. Nós vamos passar algumas noções de distância, mas saibam que não existe nenhuma convenção rígida sobre isso.

PAN (Personal Area Network)

INCIDÊNCIA EM PROVA: BAIXA

DISTÂNCIA

ALGUNS CENTÍMETROS A POUCOS METROS

A **Rede de Área Pessoal** é definida como uma rede de computadores utilizada para conectar e transmitir dados entre dispositivos localizados em uma área pessoal. Pode ser chamada também de WPAN (Wireless Personal Area Network), uma vez que seu principal meio de transmissão é o Bluetooth. Em suma, ela é basicamente uma rede de computadores ou dispositivos que abrange um espaço pequeno (em geral, alguns metros).

Sabe aquele domingo que você leva sua caixinha de som para ouvir uma música na beira da piscina e a conecta ao seu smartphone? **Pois é, isso é uma PAN!** *Sabe quando você vai dar aquela corridinha segunda-feira (para se recuperar da cachaça de domingo) e leva seu fone de ouvido sem fio conectado ao seu smartphone também para ouvir uma música?* **Adivinha... isso também é uma PAN!** *Enfim... entenderam, não é?* PAN nem sempre é tratada em questões como uma classificação padrão!

CARACTERÍSTICAS	DESCRIÇÃO
DEFINIÇÃO	Rede pessoal que cobre uma área pequena, geralmente cerca de alguns metros.
COBERTURA	Alguns centímetros a poucos metros.
FINALIDADE	Conectar dispositivos pessoais de curto alcance.
VELOCIDADE	Geralmente de alta velocidade devido à proximidade dos dispositivos.
TECNOLOGIAS	Em geral, Bluetooth, Wi-Fi, USB.
SEGURANÇA	Geralmente mais segura devido à proximidade física.
COMPLEXIDADE	Menos complexa devido à simplicidade da conexão.
ISOLAMENTO	Fácil de isolar problemas devido à proximidade.
APLICAÇÕES	Conexão de dispositivos pessoais (Ex: fones de ouvido sem fio, teclados, etc).

(INSTITUTO VERBENA / IFG – 2022) Uma classificação para os tipos de redes de comunicação de dados, ou redes de computadores, e que é muito adotada na literatura técnica dessa área, leva em conta o alcance máximo de transmissão, seja por meio de cabo, seja sem fio. Considerando o critério acima mencionado, a tecnologia de rede sem fio denominada Bluetooth® é um exemplo de classificação do tipo:

a) Local Area Network (LAN).
b) Wide Area Network (WAN).
c) Personal Area Network (PAN).
d) Metropolitan Area Network (MAN).

_____

Comentários: o bluetooth é comumente associado a redes de curto alcance (Personal Area Networks), que são projetadas para conectar dispositivos em uma área pessoal próxima, geralmente dentro de alguns metros de alcance (Letra C).

(QUADRIX / CRF-MA – 2021) Assinale a alternativa que apresenta a rede de curto alcance que permite a conexão de componentes sem a utilização de fios, como, por exemplo, a conexão de um computador com uma impressora.

a) Wide Area Network
b) Storage Area Network
c) Personal Area Network
d) Metropolitan Area Network
e) Regional Area Network

Comentários: a alternativa é PAN – trata-se de uma rede de curto alcance que permite a conexão de dispositivos pessoais, como computadores, smartphones, tablets e impressoras, geralmente dentro de um raio de alguns metros (Letra C).

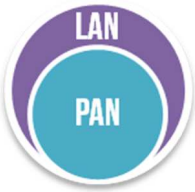
(CIEE / TJ-RR – 2019) "Redes de Computadores, de curta distância (poucos metros), que têm como principal tecnologia o Bluetooth e permitem a conexão sem fio de fones de ouvido a telefones celulares, assim como teclados e mouses sem fio a computadores dotados desta tecnologia". Trata-se de:

a) LAN (Local Área Network).
b) CAN (Campus Área Network)
c) PAN (Personal Área Network).
d) MAN (Metropolitan Área Network).

Comentários: a alternativa é PAN – trata-se de uma rede de curta distância que usa tecnologias como o Bluetooth para permitir a conexão sem fio de dispositivos pessoais, como fones de ouvido, teclados, mouses e smartphones, dentro de uma área física limitada, geralmente poucos metros (Letra C).

LAN (Local Area Network)

INCIDÊNCIA EM PROVA: ALTÍSSIMA



DISTÂNCIA

DE ALGUMAS CENTENAS DE METROS A ALGUNS QUILÔMETROS

A **Rede de Área Local** é definida como uma rede de computadores utilizada para conectar e transmitir dados entre dispositivos localizados em uma área de abrangência local. *Quem aí já foi a uma Lan House?* O nome já dá a dica, trata-se de uma LAN. A rede da sua casa também, assim como a rede do andar de um prédio ou a rede de um órgão localizado em um único espaço físico também são redes locais.

Dessa forma, podemos dizer que uma LAN é uma rede de computadores que abrange uma área geográfica relativamente pequena, como um escritório, uma residência, um prédio ou um campus. **Ela é projetada para a interconexão de dispositivos próximos, geralmente dentro de um único local geográfico.** Ela permite a troca de informações, a comunicação eficaz entre os dispositivos conectados e o compartilhamento de recursos (como impressoras e arquivos).

As redes de área local oferecem uma velocidade de comunicação relativamente alta, permitindo uma rápida transferência de dados entre dispositivos, podendo ser configuradas em várias topologias, como barramento, anel ou estrela (mais comum). Além disso, elas podem ser cabeadas ou não. **Em geral, esse tipo de rede possui baixa ocorrência de erros por serem redes pequenas e contidas em um local específico.**

CARACTERÍSTICAS	DESCRIÇÃO
DEFINIÇÃO	Rede local que abrange uma área geográfica limitada (Ex: edifício ou campus).
COBERTURA	De algumas centenas de metros a alguns quilômetros.
FINALIDADE	Facilitar a comunicação dentro de uma organização local.
VELOCIDADE	Alta velocidade dentro da rede local.
TECNOLOGIAS	Em geral, Ethernet e Wi-Fi.
SEGURANÇA	Pode ser configurada com medidas de segurança, como firewalls.
COMPLEXIDADE	De complexidade moderada, dependendo do tamanho da rede.
ISOLAMENTO	Problemas podem ser isolados com relativa facilidade.
APLICAÇÕES	Uso em escritórios, escolas e redes corporativas locais.

(AMEOSC / Prefeitura de São João do Oeste-SC – 2023) "No contexto da informática, uma rede consiste em diversos processadores que estão interligados e compartilham recursos entre si". (Tanenbaun, 2014). Os principais tipos de redes de computadores são: LAN, MAN, WAN, WLAN. Assinale a seguir a alternativa que fala corretamente sobre as redes tipo LAN:

a) As LANs são redes de computadores que abrangem uma área restrita, como um escritório, uma escola ou um prédio, permitindo a comunicação entre dispositivos próximos.

b) As LANs são redes de computadores que utilizam apenas tecnologias sem fio (Wi-Fi) para conectar dispositivos dentro de uma área restrita, como um escritório ou uma casa.

c) As LANs são redes de computadores que conectam dispositivos em longas distâncias, utilizando cabos submarinos e satélites para comunicação global.

d) As LANs são redes de computadores que abrangem uma ampla área geográfica, como um país inteiro, permitindo a conexão entre diferentes regiões.

Comentários: (a) Correto, ela realmente é projetada para abranger uma área geograficamente restrita, como um escritório, uma escola, um prédio ou uma residência, permitindo a comunicação entre dispositivos próximos; (b) Errado, elas podem empregar tanto tecnologias com fio quanto sem fio, dependendo das necessidades e da infraestrutura do ambiente; (c) Errado, redes de longas distâncias são chamadas de WAN (Wide Area Network); (d) Errado, Elas abrangem áreas restritas e não têm a capacidade de conectar diferentes regiões ou países (Letra A).

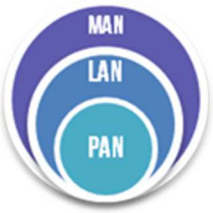
(COMPERVE / TJ-RN – 2020) Um analista de Suporte Pleno foi designado para escolher a rede de computadores mais adequada, em relação à área geográfica, para instalação em um laboratório do Tribunal de Justiça do RN. Foram estabelecidos alguns critérios para a escolha da rede, que deveria ser utilizada para conexão de estações de trabalho em escritórios, para permitir o compartilhamento de arquivos entre os membros e restringir o acesso apenas a quem estivesse dentro do prédio. O tipo de rede adequado para atender a essa demanda é:

a) WAN.
b) MAN.
c) LAN.
d) PAN.

Comentários: o tipo de rede é a LAN (Local Area Network). Ela é adequada para conectar estações de trabalho em um ambiente geograficamente limitado, como um prédio ou escritório, e permite o compartilhamento de arquivos entre os membros da rede dentro dessa área – ela restringe o acesso a dispositivos dentro de sua área geográfica (Letra C).

MAN (Metropolitan Area Network)

INCIDÊNCIA EM PROVA: ALTÍSSIMA



DISTÂNCIA

ALGUMAS DEZENAS DE QUILÔMETROS

A **Rede de Área Metropolitana** é definida como uma rede de computadores utilizada para conectar e transmitir dados entre dispositivos localizados em locais distintos. Elas possuem abrangência maior que a de uma rede local e menor que a de uma rede extensa – que veremos a seguir. Normalmente uma rede metropolitana resulta da interligação de várias redes locais em uma cidade, formando assim uma rede de maior porte.

Na imagem anterior, temos uma foto aérea de Brasília! Eu não sei se vocês sabem, mas foi aqui que foi criada a Rede de Fast-food Giraffas! Na imagem, temos a localização de dezenas de filiais dessa empresa em uma mesma cidade – **essas filiais podem se conectar formando uma única rede de área metropolitana espalhada em diferentes locais dentro de uma mesma cidade ou metrópole** a uma distância maior que a de uma rede local e menor que a de uma rede extensa.

CARACTERÍSTICAS	DESCRIÇÃO
DEFINIÇÃO	Rede metropolitana que abrange uma cidade ou uma área metropolitana.

COBERTURA	Algumas dezenas de quilômetros
FINALIDADE	Conectar redes locais dentro de uma área metropolitana.
VELOCIDADE	Velocidade variável, dependendo da infraestrutura da rede.
TECNOLOGIAS	Em geral, Ethernet e fibra óptica.
SEGURANÇA	Maior risco devido à extensão geográfica, exigindo segurança adicional.
COMPLEXIDADE	Moderadamente complexa devido à necessidade de infraestrutura metropolitana.
ISOLAMENTO	Pode ser desafiador isolar problemas devido à extensão geográfica.
APLICAÇÕES	Integração de redes locais em uma área metropolitana.

(VUNESP / ALESP – 2022) O aspecto principal que distingue as tecnologias de rede do tipo A das tecnologias de rede do tipo B é a escalabilidade, pois uma rede do tipo A deve ter a capacidade de crescer o quanto for necessário para permitir a conexão de uma grande quantidade de sites espalhados a grandes distâncias geográficas, com muitos computadores presentes em cada site.

A e B são, respectivamente:

a) LAN (Local Area Network) e WAN (Wide Area Network).
b) LAN (Local Area Network) e MAN (Metropolitan Area Network).
c) WAN (Wide Area Network) e LAN (Local Area Network).
d) PAN (Personal Area Network) e WMAN (Wireless Metropolitan Area Network).
e) PAN (Personal Area Network) e WAN (Wide Area Network).

_____

Comentários: escalabilidade é a capacidade de um sistema, rede, aplicativo ou recurso de expandir sua capacidade para acomodar um aumento crescente na carga de trabalho ou no volume de dados. Em termos mais simples, significa que um sistema escalável é capaz de crescer e lidar com demandas crescentes sem perder desempenho ou eficiência.

As redes WAN são projetadas para abranger grandes distâncias geográficas e interconectar sites distribuídos globalmente, o que requer escalabilidade para suportar muitos computadores em cada site. Por outro lado, as LANs são redes locais que normalmente abrangem uma área geográfica restrita, como um escritório, escola ou prédio, e geralmente não precisam suportar a mesma escala que as WANs (Letra C).

(CESPE / PC-AL – 2021) Rede metropolitana (MAN) é aquela que abrange uma grande área geográfica — com frequência um país ou continente — e contém um conjunto de máquinas cuja finalidade é executar os programas (ou seja, as aplicações) do usuário.

_____

Comentários: MAN não abrange uma grande área geográfica como um país ou continente, mas – sim – uma área geográfica menor, como uma cidade ou região metropolitana. Ademais, a definição menciona a execução de programas de usuário, o que não é o foco principal de uma MAN. Seu objetivo principal é fornecer conectividade de rede eficiente em uma área metropolitana para facilitar a comunicação e o compartilhamento de recursos entre organizações localizadas nessa região (Errado).

(QUADRIX / CRP-MS – 2021) Uma MAN é uma rede doméstica que ocupa o espaço de uma sala. Ela é destinada à conexão de, no máximo, dois computadores.

_____

Comentários: ela não se refere a uma rede doméstica ou uma rede que ocupa o espaço de uma sala. Trata-se de uma rede de comunicação de dados que abrange uma área geográfica maior do que uma rede local, como uma cidade ou uma região metropolitana. Ela é projetada para conectar várias redes locais em uma área geográfica maior, permitindo a comunicação de dados entre essas redes. Não há restrição para o número de computadores em uma rede metropolitana, e seu propósito é fornecer conectividade de rede em uma área metropolitana para instituições, empresas ou organizações (Errado).

(QUADRIX / CRO-AC – 2019) A Internet é uma rede do tipo MAN, pois consegue interligar computadores localizados em diferentes cidades por meio das linhas de comunicação fornecidas pelas empresas de telecomunicação.

_____

Comentários: a Internet não é classificada como uma rede do tipo MAN (Metropolitan Area Network). A Internet é, na verdade, uma rede global de escala muito maior e complexa, que se enquadra na categoria de WAN (Wide Area Network), ou seja, uma rede de longa distância que cobre vastas áreas geográficas, frequentemente de alcance global (Errado).

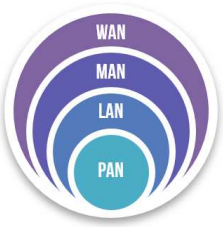
(CESPE / PF – 2014) Embora apresentem abrangência ampla e sejam utilizadas para interligar cidades distantes, as redes MAN (Metropolitan Area Network) não utilizam tecnologias de transmissão sem fio.

_____

Comentários: embora as redes MAN (Metropolitan Area Networks) sejam tipicamente usadas para interligar cidades ou áreas metropolitanas, elas podem utilizar uma variedade de tecnologias de transmissão, incluindo tanto tecnologias com fio (cabeadas) quanto tecnologias sem fio. Ademais, se as cidades forem distantes, o ideal é utilizar uma WAN (Errado).

WAN (Wide Area Network)

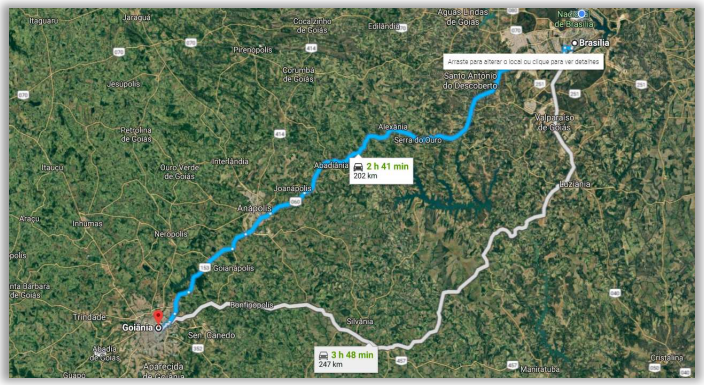
INCIDÊNCIA EM PROVA: ALTÍSSIMA



DISTÂNCIA

CENTENAS A MILHARES DE QUILÔMETROS

A **Rede de Área Extensa** é definida como uma rede de computadores utilizada para conectar e transmitir dados entre dispositivos localizados em uma grande área geográfica. E quando eu digo grande, é grande mesmo – podendo ser entre cidades, entre países ou – até mesmo – entre continentes diferentes. O Programa Antártico Brasileiro (PROANTAR) – por exemplo – realiza pesquisas nesse continente e envia os dados para o Brasil por meio de uma rede extensa.



Quando uma empresa possui filiais em cidades ou países diferentes, ela pode criar uma Rede WAN. *Aliás, vocês sabem qual é o melhor e mais clássico exemplo de WAN?* A Internet! Sim, a Internet é uma WAN – conforme mostra a imagem ao lado. Outro exemplo seria uma rede entre filiais de empresas localizadas em Brasília e Goiânia – como apresentado na imagem acima. **Essa rede formaria o que nós chamamos de rede de área extensa.**

CARACTERÍSTICAS	DESCRIÇÃO
DEFINIÇÃO	Uma rede de grande área que pode abranger cidades, países ou até mesmo continentes.
COBERTURA	Centenas a milhares de quilômetros.
FINALIDADE	Conectar redes em diferentes locais geograficamente distantes.
VELOCIDADE	Geralmente menor velocidade devido a longas distâncias.
TECNOLOGIAS	Frame Relay, MPLS, Internet.
SEGURANÇA	Requer medidas de segurança rigorosas devido ao alcance e à exposição a ameaças.
COMPLEXIDADE	Geralmente complexa devido à escala global e aos diferentes tipos de tecnologia.
ISOLAMENTO	Requer ferramentas avançadas para isolar problemas em redes extensas.
APLICAÇÕES	Comunicação em escala regional, nacional ou global.

(IBFC / DETRAN-AM – 2022) Segundo MANZANO (2207) a rede de computadores que abrange um país, continente ou mesmo dois continentes, como a Internet, é considerada tipicamente como sendo uma:

a) PAN
b) MAN
c) LAN
d) WAN

_____

Comentários: WAN (Wide Area Network) é uma rede de computadores que abrange uma ampla área geográfica, que pode incluir países, continentes ou até mesmo em escala global (Letra D).

(QUADRIX / CFT – 2021) A Internet, que é uma rede global, é um exemplo de rede WAN (Wide Area Network).

_____

Comentários: a Internet é um exemplo clássico de uma rede WAN (Wide Area Network). Uma WAN abrange uma grande área geográfica, conectando dispositivos em diferentes locais, como cidades, países ou mesmo continentes. A Internet é a maior rede WAN do mundo, conectando bilhões de dispositivos em todo o planeta, permitindo a troca de dados e comunicação entre eles (Correto).

(AOCP / UFFS – 2019) Para que possa ser implementada uma correta e adequada interconexão de redes de computadores, é muito importante definir que tipo de rede será construída e utilizada para a comunicação. Dentro desse cenário, a rede a ser desenvolvida possui as seguintes características: deve cobrir áreas geograficamente dispersas, abrangendo uma grande área; deve possuir a interconexão de várias sub-redes de comunicação; e deve conter inúmeras linhas de transmissão. Com base nas características apresentadas, qual é o melhor tipo de rede para implementação?

a) MAN (Metropolitan Area Networks).
b) LAN (Local Area Networks).
c) WAN (Wide Area Networks).
d) PAN (Personal Area Networks).
e) VLAN (Virtual Local Area Networks).

_____

Comentários: o melhor tipo de rede para implementação é o WAN – ela é projetada para cobrir áreas geograficamente dispersas e permite a interconexão de várias sub-redes de comunicação. Também é caracterizada por utilizar inúmeras linhas de transmissão para possibilitar a comunicação em larga escala, geralmente em âmbito nacional ou internacional (Letra C).

(CESPE / MPC-PA – 2019) Considere que quatro empresas distintas, localizadas em países e continentes diferentes, tenham de acessar e compartilhar dados entre si. Essa demanda pode ser atendida mediante a elaboração de projeto em que se conste a implementação de uma rede:

a) VoIP (voice over IP).
b) PGP (Pretty Good Privacy).
c) LAN (local area network).
d) SSL (secure sockets layer).
e) WAN (wide area network).

_____

Comentários: WANs são projetadas para cobrir amplas áreas geográficas, interconectar redes em locais remotos e fornecer conectividade em nível regional, nacional ou internacional, o que atenderia às necessidades de empresas em diferentes países e continentes (Letra E).

Em suma, a classificação quanto à dimensão pode ser resumida na seguinte tabela:

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 correspondência 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. Apenas a título de curiosidade, existem diversas outras classificações menos tradicionais. Duas são bastante interessantes: Body Area Network (BAN) e Interplanetary Area Network (IAN).

A BAN se trata de uma rede de área corporal que está geralmente relacionada à área de saúde e tem ganhado enorme destaque recentemente. Dispositivos podem ser implantados dentro do corpo humano ou vestidos em sua superfície. *Vocês sabem esses smartwatches que estão na moda agora?* Eles são capazes de realizar diversas medidas no seu corpo e enviar para o seu smartphone formando uma rede corporal, no entanto existem dezenas de outras possibilidades...

Existe também uma classificação chamada ***Interplanetary Area Network***. *Sabe a Curiosity?* Ela é um veículo-sonda que está percorrendo a superfície de Marte desde 2012 e enviando dados para a Terra. Pois é, pode-se classificar a rede formada entre a sonda e nosso planeta como uma IAN – uma Rede de Área Interplanetária cuja distância é de... alguns milhões de quilômetros. Diz se informática não é a melhor disciplina do universo :)

Quanto à Arquitetura de Rede ou Forma de Interação

Antes de entrar nessa classificação, é importante entender alguns conceitos. Primeiro, uma rede é composta por dispositivos intermediários e dispositivos finais. Os dispositivos intermediários são aqueles que fornecem conectividade e direcionam o fluxo de dados em uma rede (Ex: roteadores, switches, etc). Já os dispositivos finais são aqueles que fazem a interface entre o usuário e a rede de computadores (Ex: computadores, notebooks, smartphones, etc).

Na imagem acima, temos quatro dispositivos finais e quatro dispositivos intermediários. Nesse momento, nós vamos tratar apenas dos dispositivos finais – **também chamados de hosts ou sistemas finais**. Esses dispositivos podem ser classificados basicamente em clientes (aqueles que consomem serviços) ou servidores (aqueles que oferecem serviços). Todos nós somos clientes de diversos serviços todos os dias e, às vezes, nem percebemos. Vamos entender isso melhor...

Antigamente, computadores funcionavam de forma isolada. **Foram criadas as redes de computadores com o intuito de otimizar processos, melhorar a comunicação e facilitar o compartilhamento de recursos.** Imagine uma empresa com 100 funcionários que precisam com frequência imprimir documentos. *Faz mais sentido comprar uma impressora para cada funcionário ou comprar uma impressora bem mais potente e compartilhá-la com todos?*

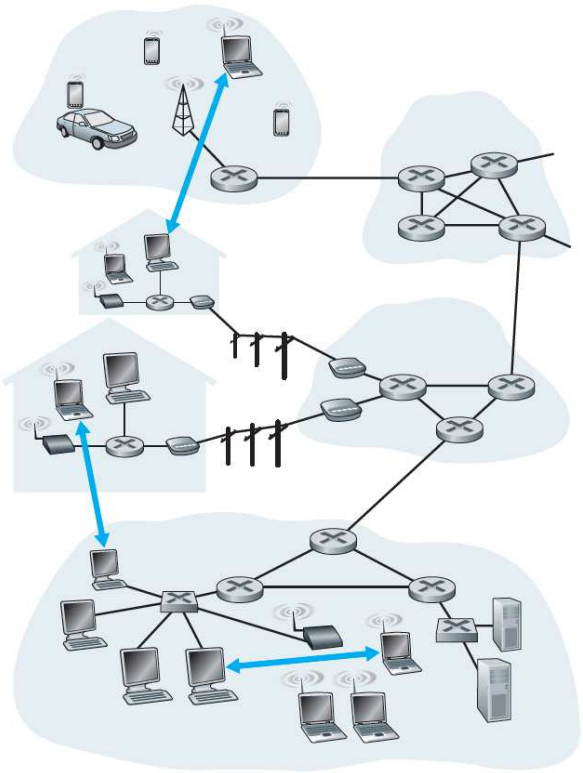
Ora, raramente alguém precisa de uma impressora só para si, portanto o compartilhamento de recursos otimizava bastante os custos e processos de uma organização. No entanto, outros recursos podiam ser compartilhados, como softwares, backups, e-mails e – principalmente – dados. **Uma forma eficiente de compartilhar dados é disponibilizá-los em um servidor, que é geralmente uma máquina especializada e poderosa capaz de oferecer serviços a vários clientes.**

Em contraste, os funcionários da empresa possuem em suas mesas uma máquina mais simples chamada de cliente. *Essas máquinas mais simples acessam dados que estão armazenados onde?* No servidor! E tanto os clientes quanto os servidores estão conectados entre si por uma rede. Como na vida real, cliente é aquele que consome algum serviço ou recurso; e servidor é aquele que fornece algum serviço ou recurso. *Simples, não?*

Informalmente, clientes costumam ser computadores de mesa, notebooks, smartphones e assim por diante; ao passo que servidores costumam ser máquinas mais poderosas, que armazenam e distribuem páginas web, vídeo em tempo real, transmissão de e-mails e assim por diante. Hoje, a maioria dos servidores dos quais recebemos resultados de busca, e-mail, páginas e vídeos reside em grandes centros de dados chamados **Datacenters**. Agora nós podemos estudar as arquiteturas!

Rede Ponto-a-Ponto

INCIDÊNCIA EM PROVA: BAIXA



Também chamada de Rede Par-a-Par ou Peer-to-Peer (P2P), **trata-se do modelo não hierárquico de rede mais simples em que máquinas se comunicam diretamente, sem passar por nenhum servidor dedicado, podendo compartilhar dados e recursos umas com as outras**. Essas redes são comuns em residências e entre filiais de empresas, porque demandam um baixo custo, são facilmente configuráveis, escaláveis e possibilitam altas taxas de velocidade.

Notem pela imagem que não há uma hierarquia entre os dispositivos finais – todas as máquinas são iguais e, por essa razão, são chamadas de pares (ou peers). Observem também que afirmar que as máquinas se comunicam diretamente não significa que exista um link dedicado entre elas, significa que não há um servidor intermediando a comunicação. **A classificação quanto à arquitetura trata dos papeis que um dispositivo final pode exercer e, não, da conexão entre os dispositivos.**

Nesse tipo de rede, todas as máquinas oferecem e consomem recursos umas das outras, atuando ora como clientes, ora como servidoras. No entanto, nem tudo são flores! Dependendo do contexto, o gerenciamento pode ser bastante complexo. Quando essa arquitetura é utilizada em redes domésticas com poucos computadores e cuja finalidade é compartilhar impressoras, trocar arquivos e compartilhar internet – não há problema[3].

Por outro lado, quando utilizada em redes de grandes organizações com muitos usuários, o gerenciamento pode ser problemático e sua utilização pode se tornar insegura (por não contar com serviços de autenticação, criptografia, controle de acesso, entre outros). Galera, existem diversas aplicações que utilizam a arquitetura ponto-a-ponto para compartilhar arquivos. *Quem já ouviu falar de BitTorrent?*

Trata-se de um protocolo de comunicação que utiliza um modelo P2P para compartilhar arquivos eletrônicos na Internet. Diversos softwares utilizam esse protocolo para permitir o download/upload de arquivos, programas, músicas, vídeos e imagens entre usuários. **Em geral,**

[3] Aliás, a maioria das redes domésticas são Redes P2P. Eu tenho uma rede na minha casa para compartilhar arquivos entre o meu computador e o notebook da minha esposa. Logo, ambos os dispositivos fazem o papel de cliente e servidor simultaneamente.

trata-se de um compartilhamento ilegal que favorece a pirataria – inclusive é proibido em diversos países.

Por anos, a indústria fonográfica e cinematográfica lutou na justiça para impedir a utilização desse tipo de serviço por conta dos prejuízos incalculáveis das gravadoras de discos e produtoras de filmes. *Por que não deu certo, professor?* Pessoal, se esse serviço utilizasse um modelo cliente/servidor, bastava derrubar o servidor que estava disponibilizando os arquivos aos usuários. **No entanto, em uma rede P2P, todas as máquinas são servidores e clientes...**

Galera, esse modelo possui uma arquitetura descentralizada em que não existe um repositório central armazenando os arquivos. *E onde estão os arquivos, professor?* **Eles estão espalhados nas máquinas de milhares de usuários ao redor do mundo.** Vamos imaginar um cenário em que eu estou fazendo o download de uma música da máquina de um usuário chamado João. No meio do download, acaba a energia na casa do João. *E agora? Perdi tudo? Já era?*

Nada disso, o software imediatamente busca outro usuário – que também possua a música – e prossegue o download normalmente. Enfim... desistiram de tentar acabar com esse tipo de serviço e atualmente continua bem simples baixar filmes que estão atualmente no cinema. **Claro que é importante tomar cuidado porque os arquivos compartilhados podem conter códigos maliciosos e, assim, infectar um computador ou permitir que ele seja invadido.**

Por fim, é importante mencionar que tratamos acima da **Arquitetura P2P Pura**. Nesse caso, ela é completamente descentralizada e não há um elemento central, sendo o completo oposto do modelo cliente-servidor. Por conta dos problemas de gerenciamento, foi criada a **Arquitetura P2P Híbrida**, que possui alguns nós especiais (chamados supernós) para realizar ações de coordenação (Ex: concede acesso, indexar dados compartilhados, liberar busca por recursos, etc).

Saiba mais:

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.

(CESPE / PO-AL – 2023) Em uma rede ponto a ponto (peer to peer) de computadores, que não depende de servidores interconectados, cada ponto torna-se tanto um cliente quanto um servidor, possibilitando a troca de informações entre si ou até mesmo compartilhando periféricos conectados à rede.

_____

Comentários: note que aqui estamos tratando da arquitetura ponto-a-ponto, que realmente não depende de servidores interconectados e cada ponto se torna tanto um cliente quanto um servidor. Nesse tipo de rede, cada computador (ponto) atua tanto como cliente quanto como servidor, o que permite a comunicação direta entre os pontos da rede sem depender de servidores centralizados. Além disso, os dispositivos em uma rede ponto a ponto podem compartilhar informações e recursos, como impressoras ou pastas de arquivos, tornando-a uma solução comum para redes menores ou domésticas (Correto).

(QUADRIX / CFFA – 2022) Em uma rede ponto a ponto, formada por uma coleção de estações de trabalho sem a presença de um servidor, os computadores fornecem recursos para a rede, mas também são usuários dos recursos fornecidos por outros computadores.

_____

Comentários: em uma rede ponto a ponto, os computadores individuais (estações de trabalho) atuam como tanto fornecedores quanto usuários de recursos na rede. Isso significa que cada computador pode compartilhar seus recursos, como pastas de arquivos, impressoras, ou conexões à internet com outros na rede, enquanto também acessa os recursos compartilhados por outras estações (Correto).

(IDIB / Câmara de Planaltina-GO – 2021 – Letra C) Peer-to-peer (do inglês par-a-par ou simplesmente ponto-aponto, com sigla P2P) é uma arquitetura de redes de computadores onde um dos pontos ou nós da rede funciona como servidor central, compartilhando os serviços e dados entre os demais nós da rede.

_____

Comentários: na arquitetura P2P, não há um servidor central que compartilhe serviços e dados entre os nós da rede. Em vez disso, os nós da rede (ou pares) são igualmente responsáveis por compartilhar recursos e informações entre si, sem depender de um servidor central (Errado).

(AOCP / ITEP-RN – 2018) Assinale a alternativa que apresenta o modo de funcionamento utilizado por programas como BitTorrent e aplicativos VoIP que permitem que os usuários compartilhem arquivos ou dados entre si pela Internet.

a) Bluetooth
b) FTP
c) POP3
d) P2P
e) B2B

_____

Comentários: BitTorrent e Aplicações VoIP (Voz sobre IP) utilizam P2P (Letra D).

(PaqTcPB / Prefeitura de Patos-PB – 2010) Qual dos itens abaixo caracteriza uma rede de computadores peer-to-peer (par a par)?

a) Nós com diferentes capacidades funcionais e responsabilidades.
b) Presença de um único nó servidor.
c) Gerenciamento descentralizado.
d) Uso apenas em redes locais.
e) Interligação de até dois nós.

_____

Comentários: (a) Errado, os nós são pares, por isso possuem as mesmas capacidades funcionais e responsabilidades; (b) Errado, não há servidores intermediários; (c) Correto; (d) Errado, há diversas aplicações; (e) Errado, não há limites de nós (Letra C).

(PUC-PR / DPE-PR – 2012) Arquitetura de serviço de rede onde todos os participantes são ao mesmo tempo servidores e clientes entre si. Está-se falando de:

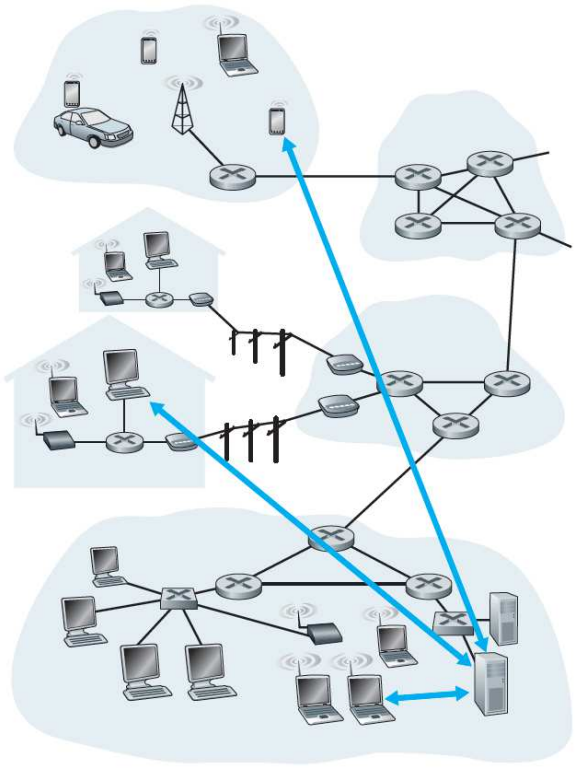
a) Two-Tier.
b) Three-Tier.
c) Peer-to-Peer.
d) Middleware.
e) Multi-Tier.

_____

Comentários: a arquitetura onde todos os participantes são simultaneamente clientes e servidores é a P2P (Letra C).

Rede Cliente/Servidor

INCIDÊNCIA EM PROVA: MÉDIA



Trata-se um modelo hierárquico de redes mais complexo, porém potencialmente mais robusto e confiável. **Nesse modelo, existe uma máquina especializada, dedicada e geralmente remota**, respondendo rapidamente aos pedidos vindos dos demais computadores da rede – o que aumenta bastante o desempenho de algumas tarefas.

É a escolha natural para redes grandes, como a Internet, que funciona tipicamente a partir do Modelo Cliente/Servidor. Observem na imagem ao lado que há diversos dispositivos clientes se comunicando diretamente com um único servidor – um cliente jamais se comunica diretamente com outro cliente.

Ao contrário do que ocorre nas redes par-a-par, os computadores que funcionam como clientes – em regra – não fornecem recursos e serviços aos outros computadores da rede. *Que servidores são esses, Diego?*

Galera, existem vários tipos de servidores, como por exemplo: servidor de impressão, servidor de e-mails, servidor de arquivos, servidor de comunicação, servidor de banco de dados, servidor de páginas web, entre outros.

Quer um exemplo? Quando você faz o download um vídeo no site do Estratégia Concursos, você está consumindo um recurso do servidor do Estratégia. Sim, o Estratégia possui uma máquina especializada chamada de servidor, onde fica hospedado o seu site. **Quando você faz o download da sua aula de informática, você está exercendo um papel de Cliente – e quem fornece o recurso solicitado por você está exercendo o papel de Servidor.**

(CESPE / DP-DF – 2022) Em ambiente cliente-servidor, os clientes se conectam aos servidores para obter acesso aos recursos compartilhados.

_____

Comentários: nessa arquitetura, os servidores fornecem serviços ou recursos, e os clientes solicitam e utilizam esses recursos por meio da conexão com o servidor (Correto).

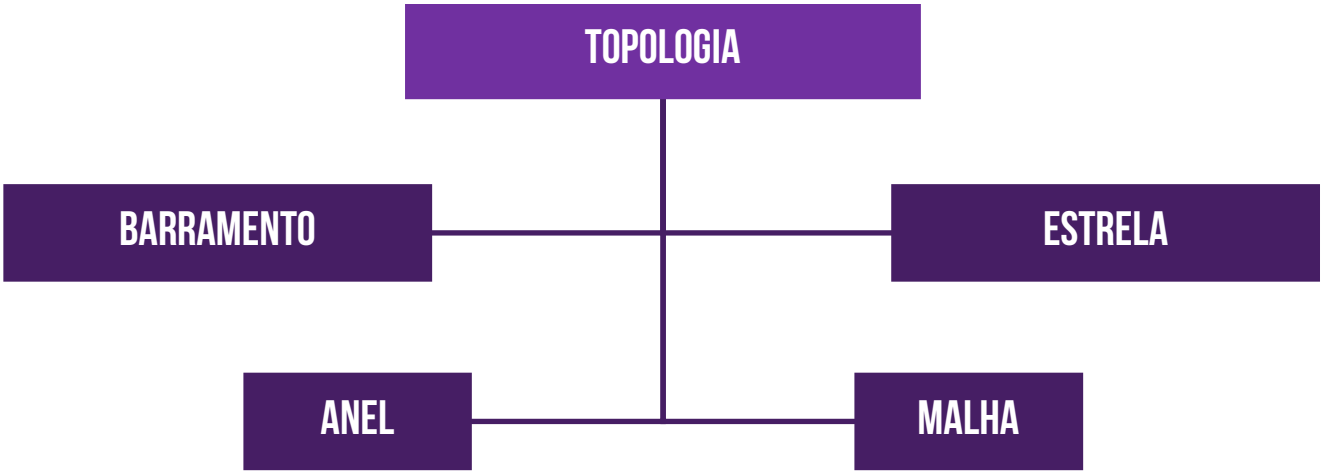
(QUADRIX / COFECI – 2017) Os principais componentes da arquitetura cliente-servidor são um conjunto de servidores, um conjunto de clientes e uma rede.

_____

Comentários: de fato, os principais componentes são clientes, servidores e uma rede (Correto).

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[4] 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.

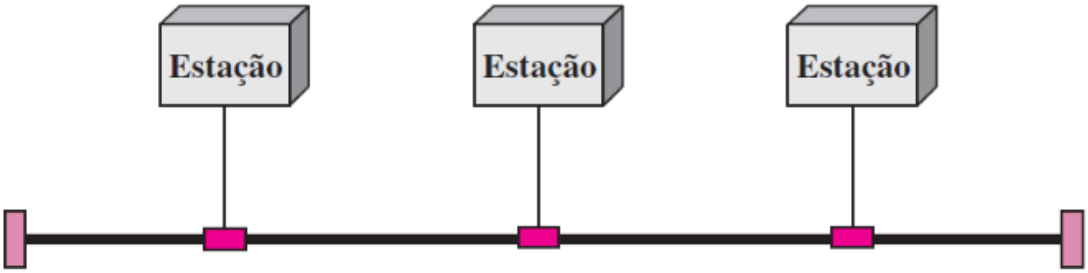
Se uma questão de prova não deixar explícito em sua redação qual é o tipo de topologia, pode-se assumir que ela se refere à **Topologia Física, e não à Topologia Lógica!**

[4] 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.

Barramento (Bus)

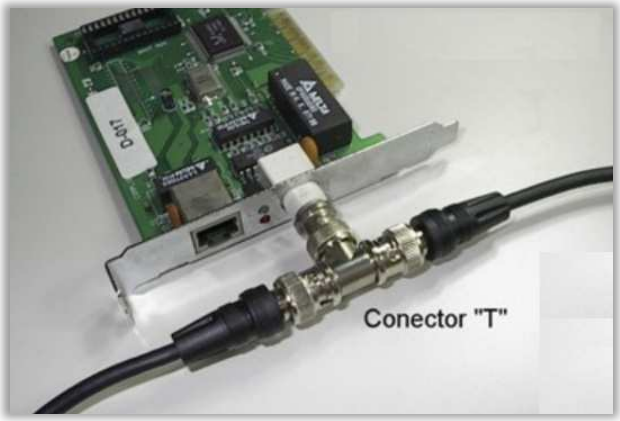
INCIDÊNCIA EM PROVA: ALTA

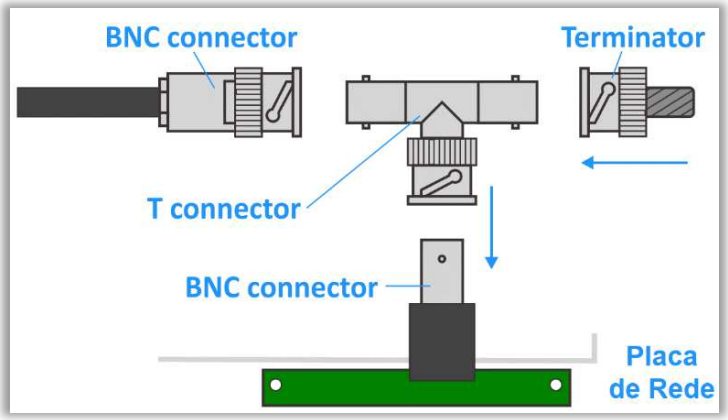
Nessa topologia, todas as estações ficam conectadas ao mesmo meio de transmissão em uma conexão ponto-multiponto[5]**.** *Qual seria esse meio de transmissão, professor?* Trata-se de um cabo coaxial, que veremos em detalhes mais adiante. Notem na imagem seguinte que temos um único enlace compartilhado em que diversos nós se ligam por meio de conectores – o nome desse enlace é *backbone* ou espinha dorsal.



Qual é a consequência de ter um único enlace compartilhado por todos os nós da rede? **Galera, um sinal gerado por um nó de origem qualquer se propagará por todo o barramento em ambas as direções e, portanto, será recebido por todos os demais nós em um modo de transmissão conhecido como *broadcast* – que nós já estudamos.** *Então, todos os nós acessarão dados mesmo que não sejam os destinatários originais da mensagem?* Calma, não é bem assim...

Cada estação de trabalho é conectada ao backbone por meio de uma placa de rede, que tem a responsabilidade de fazer a interface entre a estação de trabalho e o enlace (cabo coaxial). Essa placa de rede receberá os dados, mas somente acessará aqueles que foram endereçados a ela. Em suma: dados são enviados em *broadcast* e recebidos por todas as máquinas conectadas ao *backbone*, porém somente as estações a quem os dados foram endereçados poderão acessá-los.





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

Outra característica dessa topologia é que todas as estações de trabalho podem enviar dados em qualquer direção, mas jamais simultaneamente. Quando uma estação de trabalho estiver transmitindo dados, todas as outras devem ficar em espera até que ela finalize e que o barramento fique disponível. Só então, outra estação poderá enviar dados. **Em outras palavras, essa topologia trabalha com uma direção de transmissão half-duplex.**

Professor, o que ocorre se duas estações esperarem o barramento ficar disponível e enviarem dados ao mesmo tempo? **Nesse caso, ocorrerá o que chamamos de colisão, isto é, o sinal enviado por uma estação colidirá com o sinal enviado por outra estação.** *Vocês se lembram do walk&talk?* Como ele também é half-duplex, se duas pessoas falarem simultaneamente, ocorrerá uma colisão e as pessoas não conseguirão se comunicar. *E como resolve isso, professor?* Veremos mais para frente...

Além disso, uma falha ou ruptura no cabo de backbone implica a interrupção da transmissão, até mesmo entre os dispositivos que se encontram do mesmo lado em que ocorreu o problema.

Saiba mais:

Em uma topologia em barramento, todos os dispositivos da rede estão conectados a um único cabo principal, conhecido como backbone. Se você imaginar esse backbone como um varal de roupas, cada dispositivo conectado à rede seria como uma peça de roupa pendurada no varal.

Agora, pense no que acontece se o varal (backbone) sofre uma ruptura ou falha em qualquer ponto: todas as roupas (dispositivos) caem ou, no mínimo, ficam inacessíveis. Da mesma forma, se o cabo de backbone em uma rede em barramento tem uma falha, todos os dispositivos conectados a ele perdem a capacidade de se comunicar.

Assim como o varal não pode mais sustentar as roupas, o backbone danificado não pode mais transmitir dados, levando a uma falha de rede. Essa analogia ilustra o ponto crítico de uma topologia em barramento - a dependência de um único canal de comunicação. Qualquer dano a esse canal pode incapacitar toda a rede, assim como uma ruptura no varal impede que ele desempenhe sua função de sustentar as roupas.

Em suma: caso haja um rompimento do varal, todas as roupas caem; no entanto, caso haja um problema apenas no pregador de uma roupa e ela cair, nada acontece com o restante.

Vantagens: facilidade de instalação e economia de cabeamento. Em outras palavras, como se trata apenas de um conjunto de nós conectados a um único cabo, trata-se de uma fácil instalação, além de uma patente economia de cabeamento. **Desvantagens: aumento do atraso e dificuldade de isolar falhas.** Como o link é compartilhado, quanto maior o número de máquinas, maior o atraso (delay) na comunicação e menor o desempenho da rede.

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.
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.

(QUADRIX / CREFITO-CE – 2022) Assinale a alternativa que apresenta a topologia física de rede de computadores em que há a utilização de um único cabo backbone, que é terminado em ambas as extremidades, e cujos hosts são conectados diretamente a esse cabo.

a) topologia em anel
b) topologia em estrela
c) topologia hierárquica
d) topologia em malha
e) topologia em barramento

Comentários: a questão trata da topologia em barramento, em que os dispositivos são conectados a um único cabo de backbone, que atua como o canal de comunicação principal. Esse cabo é terminado em ambas as extremidades. Os dispositivos, como computadores ou outros dispositivos de rede, são conectados diretamente a esse cabo. Quando um dispositivo envia dados, esses dados são transmitidos por todo o cabo e todos os dispositivos na rede recebem esses dados. No entanto, apenas o dispositivo de destino apropriado processa os dados, enquanto os outros dispositivos simplesmente os ignoram (Letra E).

(IBFC / IDAM – 2019) Uma das topologias de rede mais simples de montar, todos os computadores estão ligados a uma mesma linha de transmissão através de cabo, geralmente coaxial:

a) em árvore b) anel c) barramento d) estrela

Comentários: simples de montar e todos os cabos ligados a uma mesma linha de transmissão coaxial são características da topologia em barramento (Letra C).

(QUADRIX / CRA-PA – 2019) Na topologia em barramento, apenas os computadores das extremidades (pontas) é que podem enviar dados para quaisquer computadores, pois, nesse tipo de topologia, eles são os gerenciadores da rede.

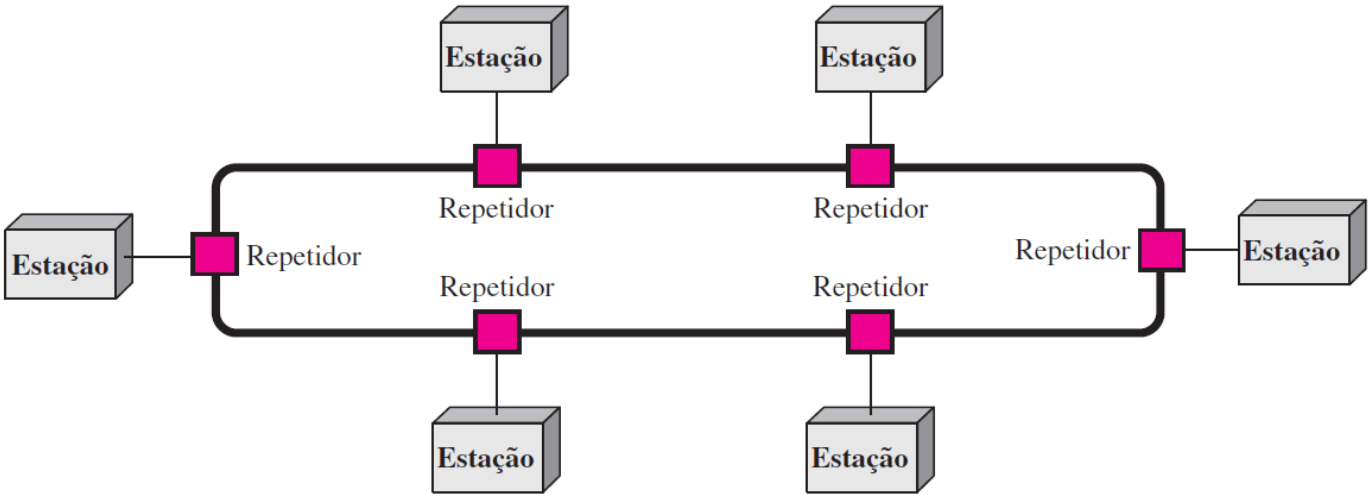
_____

Comentários: nessa topologia, não há um nó central ou gerenciador de rede – todos podem enviar dados (Errado).

Anel (Ring)

INCIDÊNCIA EM PROVA: MÉDIA

Nessa topologia, **cada dispositivo tem uma conexão ponto-a-ponto com outros dois dispositivos conectados lado a lado**, e fazendo uso de uma comunicação com transmissão unidirecional (chamada *simplex*). Nesse caso, a mensagem circula o anel, sendo regenerada e retransmitida a cada nó, passando pelo dispositivo de destino que copia a informação enviada, até retornar ao emissor original. Nesse momento, o link é liberado para que possa ser utilizado pelo nó seguinte.



Imagine que um dispositivo deseje enviar mensagem para outro dispositivo do anel. Ele enviará para o dispositivo ao lado; ele verificará que não é o destinatário da mensagem e repetirá a mensagem para seu dispositivo ao lado (**por isso os repetidores**); o próximo dispositivo fará o mesmo procedimento até chegar ao dispositivo de destino, que receberá os dados e enviará uma mensagem para o dispositivo remetente original para informá-lo de que recebeu os dados.

Dessa forma, pode-se afirmar que os dados são transmitidos em *broadcast*, isto é, dados enviados em uma rede com essa topologia são recebidos por todos os outros dispositivos. Outra característica interessante é a ausência de colisões. *Como assim, Diego?* Guardem na memória: colisões só ocorrem quando a direção de transmissão é *half-duplex* – jamais ocorre quando a direção de transmissão é *simplex* ou *full-duplex*.

Professor, ainda assim não ocorreria aquele problema de duas máquinas enviarem dados ao mesmo tempo causando colisão? **Não, porque a topologia em anel utiliza um envelope de dados chamado Token!** Trata-se de um envelope para transmissão de dados que permanece circulando pelo anel até que alguma estação de trabalho que deseje transmitir dados a outra estação de trabalho o capture. *Como é, Diego?*

Pessoal, existe uma modalidade do atletismo chamada Corrida de Revezamento. Quatro atletas percorrem uma pista circular segurando um bastão: o primeiro corre e passa o bastão para o segundo; o segundo corre e passa o bastão para o terceiro; o terceiro corre e passa o bastão para o

quarto; e o quarto corre até o final do circuito. Em outras palavras, um atleta somente pode correr caso ele esteja com o bastão em suas mãos. **Aqui funciona de maneira semelhante...**

Uma estação de trabalho somente pode enviar dados quando estiver de posse do token. Em suma, um token fica circulando pelo anel. Quando alguma estação de trabalho deseja enviar dados, ela captura o token, insere seus dados dentro dele e o envia para a estação adjacente, e assim por diante até chegar ao destinatário final. Esse recebe o envelope, verifica que ele é o destinatário do token, captura os dados e insere dentro do envelope um sinal de recebimento.

O envelope continua percorrendo o anel para a próxima estação, e a próxima, e a próxima, até chegar à estação que enviou os dados. **Essa estação abre o envelope, verifica o sinal recebido, confirma que a estação de destino recebeu as informações enviadas e devolve o *token* para a rede para que ele continue circulando pelo anel**. Quando outra estação quiser enviar outra mensagem, é só capturar o *token* e fazer o mesmo processo. Assim, não há chances de colisões!

Nessa topologia, um anel é relativamente fácil de ser instalado e reconfigurado, com isolamento de falhas simplificado. *Por quê?* Porque para instalar, basta conectar os dispositivos e, caso uma nova máquina seja adicionada/eliminada, exige-se apenas a mudança de poucas conexões. Outra vantagem é o isolamento de falhas simplificado, isto é, se um dispositivo não receber o sinal de que os dados foram recebidos, ele pode emitir um alerta – facilitando a identificação do problema.

Por outro lado, há também desvantagens: se algum enlace for rompido, a rede inteira para de funcionar. Além disso, como o tráfego de dados é simplex, se alguma estação se tornar inoperante por alguma razão, a rede também para de funcionar. Existem também uma limitação quanto ao comprimento máximo do anel e o número máximo de dispositivos. *Como assim?* Em um anel com 100 máquinas, por exemplo, o atraso para recebimento dos dados seria enorme.

Existiram implementações dessa tecnologia que utiliza anéis duplos para mitigar grande parte desses riscos e desvantagens (Ex: FDDI).

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.

(QUADRIX / CRESS-AL – 2023) Na topologia em anel, a comunicação entre os nós da rede somente pode ser realizada no sentido horário.

_____

Comentários: na topologia em anel, a comunicação entre os nós da rede pode ocorrer em ambas as direções: sentido horário e sentido anti-horário (Errado).

(QUADRIX / CRECI-PR – 2023) Na topologia em anel de uma rede de computadores, todos os dispositivos (computadores) estão conectados a um hub central.

_____

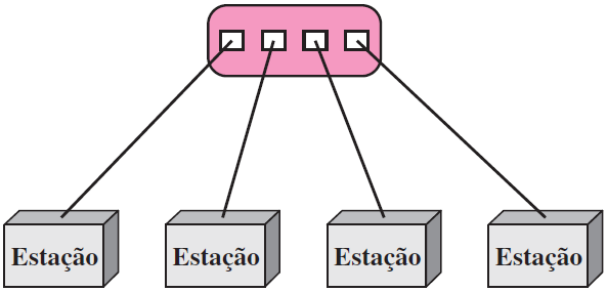
Comentários: na topologia em anel de uma rede de computadores, os dispositivos não estão conectados a um hub central. Na verdade, cada dispositivo está conectado diretamente ao dispositivo vizinho, formando um circuito fechado, seja fisicamente (anel físico) ou logicamente (anel lógico). Não há um hub central na topologia em anel; em vez disso, os dispositivos são conectados em série, e a comunicação ocorre passando de um dispositivo para o próximo até chegar ao destino (Errado).

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[6], 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.



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.

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

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.

(CESPE / POLITEC-RO – 2022) Assinale a opção que apresenta a topologia de rede em que os hosts são conectados a um ponto central compartilhado.

a) em barramento
b) hierárquica
c) em anel
d) em estrela
e) em malha

_____

Comentários: na topologia de rede em estrela, todos os dispositivos (ou hosts) na rede estão conectados a um ponto central. Esse ponto central atua como o concentrador da rede e é responsável por encaminhar o tráfego de dados entre os dispositivos (Letra D).

(QUADRIX / CRT-SP – 2021) Na topologia em estrela, a comunicação entre duas estações deve passar, obrigatoriamente, pelo equipamento central, já que todas as estações estão diretamente conectadas a ele.

_____

Comentários: na topologia em estrela, todas as estações da rede estão diretamente conectadas a um equipamento central, como um switch ou um hub. Para que duas estações se comuniquem entre si, a comunicação deve passar obrigatoriamente pelo equipamento central, que atua como intermediário. Isso significa que o equipamento central é responsável por encaminhar os dados de uma estação para a estação de destino na rede em uma configuração típica de topologia em estrela (Correto).

(IDECAN / PEFOCE – 2021) No que diz respeito aos conceitos básicos das redes de computadores, o termo topologia diz respeito ao layout físico empregado na implementação da rede e à forma como são feitas as conexões, havendo diversas configurações, sendo uma delas a mais empregada pelas características e vantagens que propicia. A figura abaixo ilustra o esquema básico dessa topologia:

Do ponto de vista físico, essa topologia é conhecida por

a) anel ou cíclica.
b) malha ou mesh.
c) distribuída ou descentralizada.
d) árvore ou hierárquica.
e) estrela ou radial.

_____

Comentários: a imagem claramente representa uma topologia em estrela, em que temos um layout de rede com todos os dispositivos conectados a um único ponto central. Note que cada dispositivo (como computadores, impressoras, servidores, etc) tem uma conexão direta com o concentrador (Letra E).

(CONSULPLAN / IDAM – 2019) "*Topologia de Rede que se caracteriza pela presença de um elemento central de comunicação que coordena toda a rede – caso esse elemento falhe, a rede é interrompida (ponto único de falhas)".* Trata-se de:

a) Mesh
b) Estrela
c) Híbrida
d) Barramento

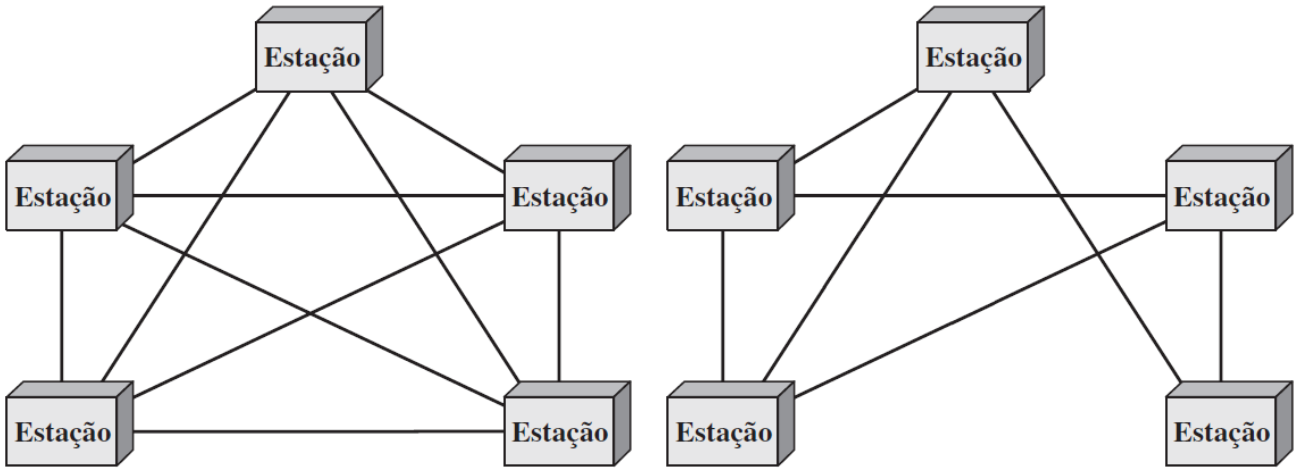
_____

Comentários: presença de um elemento central que coordena a rede e que pode ser um ponto único de falha são características da topologia em estrela (Letra B).

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[7].



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

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

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.**

Em outras palavras, essa topologia é mais adequada para poucas máquinas, caso contrário sua implementação pode se tornar inviável. Pensa comigo: se um computador estiver ligado diretamente a outros quatro, nós precisaremos de 20 portas ou placas de rede e 10 cabos. Na verdade, para cada *n* computadores, são necessário **n.(n-1)/2** cabos e **n.(n-1)** portas ou placas de rede. Para 20 computadores, seriam 190 cabos e 380 placas de rede! 😱

A utilização mais comum desse tipo de rede é para interligar – por exemplo – matrizes e filiais em uma rede metropolitana cabeada. Galera, na prática quase ninguém usa topologia em malha em Redes LAN (cabeadas): ou ela é utilizada em Redes WAN ou é utilizada em Redes WLAN (não cabeadas). Aliás, esse último caso tem sido cada vez mais comum: a topologia em *mesh* são comumente utilizadas em redes locais *wireless* para interligar dispositivos sem fio.

Talvez vocês já tenham visto que recentemente aumentou o número de vendas de kits de **roteadores *mesh* capazes de criar uma rede em malha em casas ou escritórios**. Um exemplo:

Eles são muito úteis para cobrir uma área grande com wi-fi. *Sabe aquele ponto da casa que o sinal de wi-fi é ruim?* Pois é, ele ajuda a melhorar esse sinal! *Professor, não basta comprar um roteador e dois repetidores – que são bem mais baratos?* Você pode fazer isso, mas você criará três redes diferentes e sempre que você quiser ter o melhor sinal possível, você terá que acessar o seu dispositivo, ir até as configurações e trocar de rede.

Na prática, sempre que você se mover pela casa ou escritório, você terá que ir trocando de rede para ter o melhor sinal possível. Já em redes *mesh*, isso não é necessário: **ela identifica onde está o nó**

com o sinal mais forte e se conecta automaticamente à medida que você vai se movendo pela casa. E essa é apenas uma das vantagens! Enfim... trata-se de um belo investimento para quem tem problema de sinal.

CARACTERÍSTICAS	DESCRIÇÃO
DEFINIÇÃO	Uma topologia de rede onde cada dispositivo está conectado a vários outros dispositivos, formando uma rede interconectada.
ESCALABILIDADE	Baixa, no caso de redes mesh cabeadas; e alta, no caso de redes mesh wireless.
CONFIABILIDADE	Muito alta, devido a múltiplos caminhos entre dispositivos, minimizando o impacto de falhas individuais.
DESEMPENHO	Bom, especialmente em redes com muitos dispositivos, pois múltiplos caminhos evitam congestionamentos.
MANUTENÇÃO	Pode ser desafiadora, devido à complexidade da rede e à quantidade de conexões individuais.
COMPLEXIDADE	Alta, especialmente em grandes redes, devido ao grande número de conexões e caminhos possíveis.
LATÊNCIA	Geralmente baixa, pois há muitos caminhos alternativos para a transmissão de dados, reduzindo o tempo de viagem.
SEGURANÇA	Alta, pois a rede não depende de um único ponto; no entanto, gerenciar a segurança em todas as conexões pode ser desafiador.
ISOLAMENTO DE PROBLEMAS	Eficiente, já que problemas em um dispositivo ou conexão geralmente não afetam a rede inteira.
TIPOS DE APLICAÇÃO	Ideal para redes que requerem alta confiabilidade e robustez, como redes militares ou de emergência.

Agora para finalizar essa parte de classificação de redes de computadores, eu fiz a tabelinha seguinte: ela mostra a relação entre topologia física, direção/modo de transmissão e tipo de enlace:

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

(CONSULPLAN / MPE-PA – 2022) As formas como os dispositivos em uma rede estão distribuídas e conectadas entre si é chamada de topologia de rede. Em uma das topologias de rede, todos os dispositivos estão conectados com todos os outros dispositivos, sendo a topologia com o maior nível de confiabilidade e robustez. Podemos afirmar que trata-se de topologia em:

a) Anel (ring).
b) Estrela (star).
c) Malha (mesh).
d) Barramento (bus).

_____

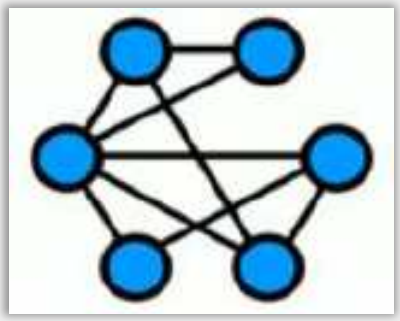
Comentários: a questão trata da topologia em malha, em que todos os dispositivos estão conectados a todos os outros dispositivos, o que aumenta a confiabilidade e robustez da rede, uma vez que, em caso de falha em um dos dispositivos ou conexões, ainda é possível alcançar outros dispositivos por meio de rotas alternativas. Essa topologia é especialmente utilizada em situações em que a alta disponibilidade e a redundância são críticas (Letra C).

(CESPE / TELEBRÁS – 2022) Topologias em malha, que permitem rotas alternativas entre nós, são adotadas para se garantir disponibilidade em WANs.

_____

Comentários: topologias em malha, nas quais cada nó está conectado a vários outros nós, são frequentemente utilizadas em WANs (Wide Area Networks) para garantir disponibilidade e redundância. Essa topologia permite que o tráfego de dados encontre rotas alternativas em caso de falha em uma parte da rede, garantindo que a rede permaneça operacional (Correto).

(IBADE / Prefeitura de Acrelândia-AC – 2022) Com relação às topologias de rede, analise a imagem abaixo e responda corretamente.



A topologia representada na imagem acima é a:

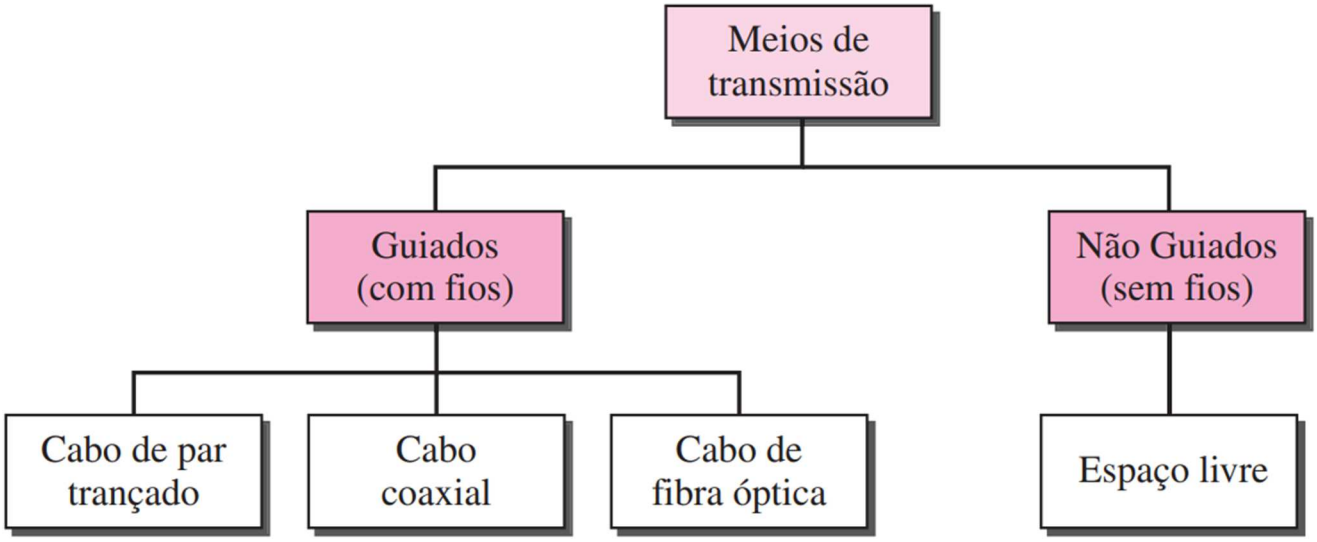
a) barramento.
b) mista.
c) malha.
d) árvore.
e) estrela.

_____

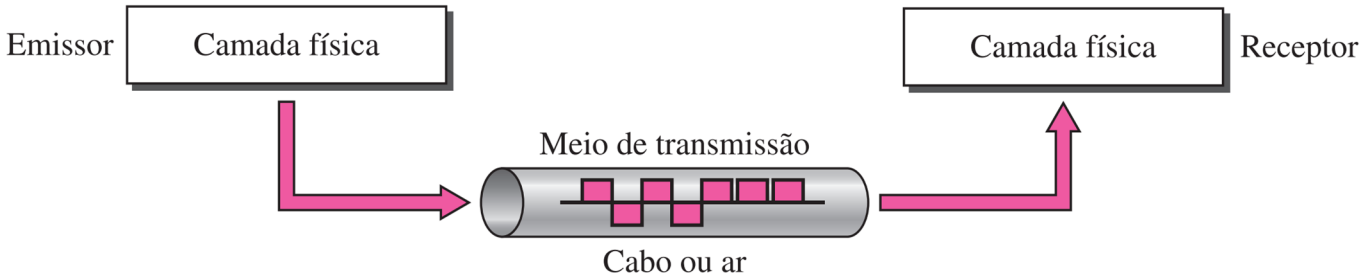
Comentários: a topologia apresentada é uma topologia em malha. Note que ela é caracterizada por um layout de rede em que os dispositivos estão interconectados, criando uma rede altamente redundante. Em uma topologia em malha, cada dispositivo é conectado diretamente aos outros dispositivos, formando uma teia de conexões e não há um único ponto central como em uma topologia em estrela (Letra C).

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.



(IBEST / CRF-SC – 2023) Em redes de computadores, para que um dado seja transferido, é necessário um meio de transmissão. Assinale a alternativa que apresenta apenas os meios de transmissão não guiados.

a) cabo de par trançado e ondas de rádio

b) cabo coaxial e micro-ondas
c) micro-ondas e cabo de fibra ótica
d) cabo de par trançado e micro-ondas
e) ondas de rádio e micro-ondas

_____

Comentários: (a) Guiado e Não-Guiado; (b) Guiado e Não-Guiado; (c) Não-Guiado e Guiado; (d) Guiado e Não-Guiado; (e) Correto, ambos são não guiados (Letra E).

(IBADE / Prefeitura de Colider – 2022) São considerados meios de transmissão guiados:

a) cabo coaxial, cabo de par trançado e cabo de fibra óptica.
b) transmissão via satélite e transmissão via rádio.
c) cabo de fibra óptica, apenas.
d) cabo de par trançado e transmissão via satélite.
e) transmissão via rádio, apenas.

_____

Comentários: (a) Correto; (b) Não-Guiado e Não-Guiado; (c) Guiado; (d) Guiado e Não-Guiado; (e) Não-Guiado (Letra A).

(QUADRIX / CRC-MG – 2022) O cabo UTP e as fibras ópticas são exemplos de meios de transmissão não guiados em uma rede de computadores.

_____

Comentários: na verdade, ambos são considerados meios guiados em uma rede de computadores (Errado).

(AOCP / Prefeitura de Pinhais-PR – 2017) Os meios de transmissão em uma rede podem ser classificados como meios guiados e não guiados. Selecione a alternativa que exemplifica um meio de transmissão não guiado.

a) Meios que não utilizam sinal elétrico para transmitir, como a fibra ótica.
b) Cabo do tipo par trançado.
c) Rede sem fio.
d) Internet.
e) Cabo coaxial.

_____

Comentários: (a) Errado, fibra óptica é um meio guiado; (b) Errado, cabo de par trançado é um meio guiado; (c) Correto; (d) Errado, Internet é a rede mundial de computadores; (e) Errado, cabo coaxial é um meio guiado (Letra C).

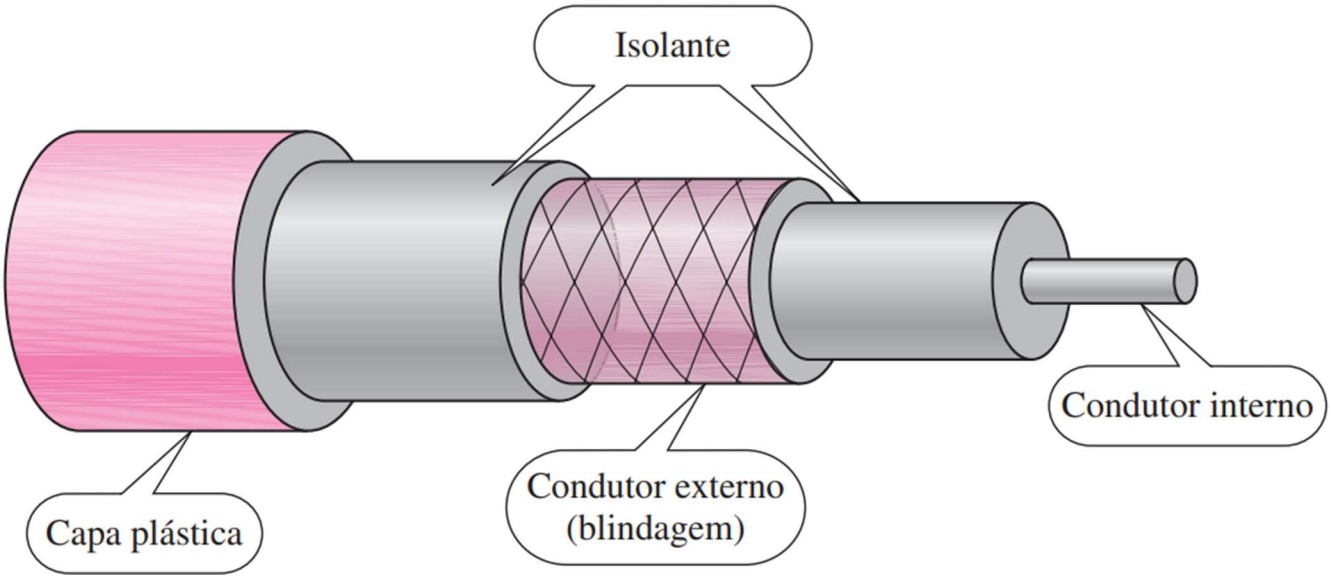
(CESPE / PC-AL – 2012) Cabos de par trançado, coaxiais e fibras ópticas são os tipos mais populares de meios de transmissão não guiados.

_____

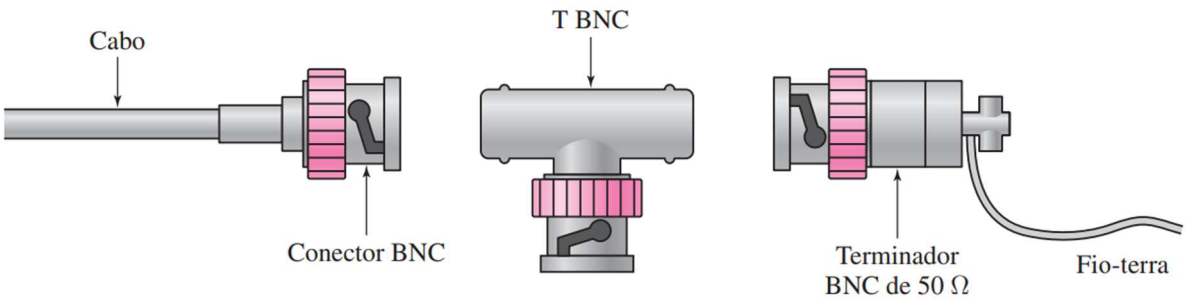
Comentários: cabos de par trançado, coaxial e fibras ópticas são populares meios de transmissão de dados guiados, ou seja, são materiais que conduzem a informação enviada do transmissor ao receptor (Errado).

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[8].



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.

[8] 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.

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...

*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.*

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.

(PROF. DIEGO / INÉDITA – 2023) Cabos coaxiais são mais finos e flexíveis em comparação com cabos de fibra óptica.

_____

Comentários: em comparação com cabos de par trançado e cabos de fibra óptica, os cabos coaxiais tendem a ser mais espessos e menos flexíveis, o que pode dificultar a instalação em espaços apertados (Errado).

(PROF. DIEGO / INÉDITA – 2023) Cabos coaxiais geralmente usam conectores do tipo BNC (Bayonet Neill-Concelman) para estabelecer conexões.

_____

Comentários: cabos coaxiais, de fato, frequentemente utilizam conectores do tipo BNC para fazer conexões seguras e estáveis (Correto).

(QUADRIX / CRESS-PB – 2021) O cabo coaxial não pode ser usado em redes de computadores, sendo permitido apenas o uso do cabo de par trançado e do cabo de fibra óptica.

_____

Comentários: o cabo coaxial pode ser usado em redes de computadores e já foi amplamente utilizado em tecnologias de redes mais antigas, como Ethernet coaxial (por exemplo, 10Base2 e 10Base5). No entanto, a tecnologia evoluiu, e atualmente, o cabo de par trançado e a fibra óptica são opções de cabos de rede mais comuns em ambientes de rede modernos. A escolha do cabo depende das necessidades de largura de banda, distância e aplicação da rede. Portanto, o cabo coaxial, embora menos comum do que o cabo de par trançado e a fibra óptica nas redes modernas, ainda pode ser usado em alguns cenários (Errado).

(CESPE / FUB – 2015) O cabo coaxial, meio físico de comunicação, é resistente à água e a outras substâncias corrosivas, apresenta largura de banda muito maior que um par trançado, realiza conexões entre pontos a quilômetros de distância e é imune a ruídos elétricos.

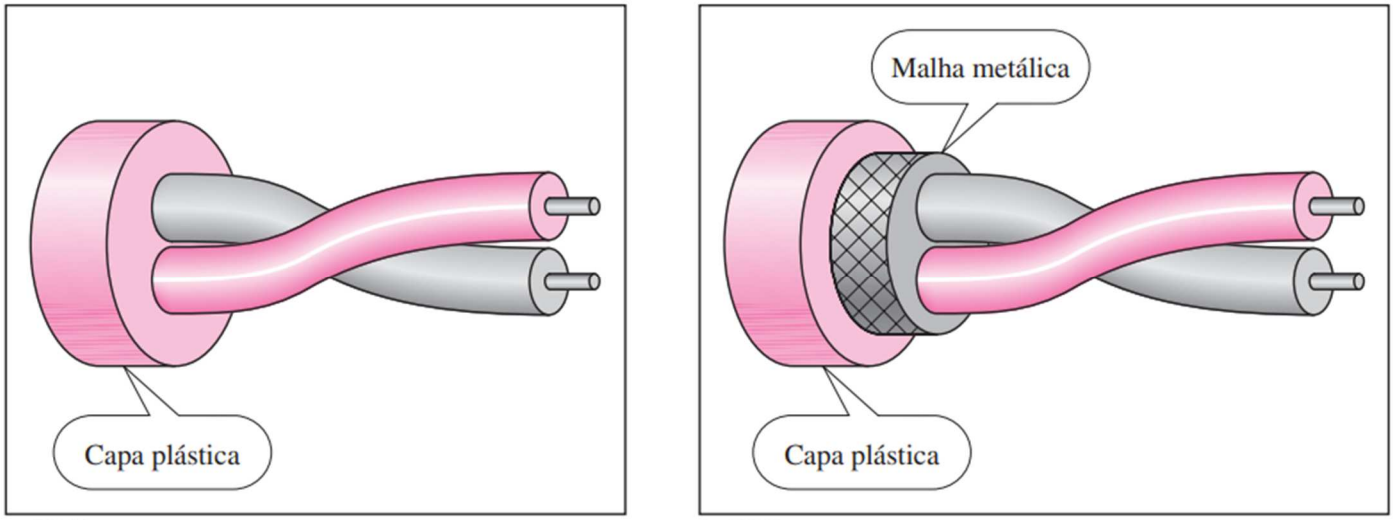
_____

Comentários: sobre a largura de banda: quando em hz (hertz), significa o intervalo de frequências contido em um canal; quando em bits por segundo (bps), significa o número de bits por segundo que um canal, enlace ou rede é capaz de transmitir. A largura de banda é a capacidade máxima teórica de um canal, já a taxa de transferência é a capacidade efetiva de dados transmitidos. A largura de banda é um conceito mais independente, já a taxa de transmissão depende de outros fatores. Cabos coaxiais, por exemplo, possuem uma largura de banda maior que cabos de par trançado, isto é, uma capacidade teórica maior de transmitir dados. No entanto, ele sofre bastante com atenuação de sinal, requerendo o uso frequente de repetidores e, por essa razão, possui uma taxa de transmissão efetiva menor que os cabos de par trançado. Dito isso...

O Cabo Coaxial não é imune a ruídos elétricos (apesar de ser muito resistente). Ademais, ele é relativamente resistente a substâncias corrosivas, mas não vai resistir – por exemplo – a ácido sulfúrico. Por fim, ele realmente apresenta uma largura de banda maior que o cabo de par traçado, apesar de ter uma taxa de transmissão menor (Errado).

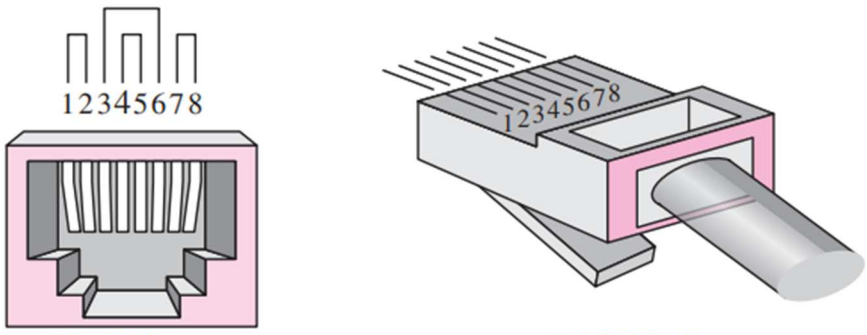
Cabo de Par Trançado

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!**).

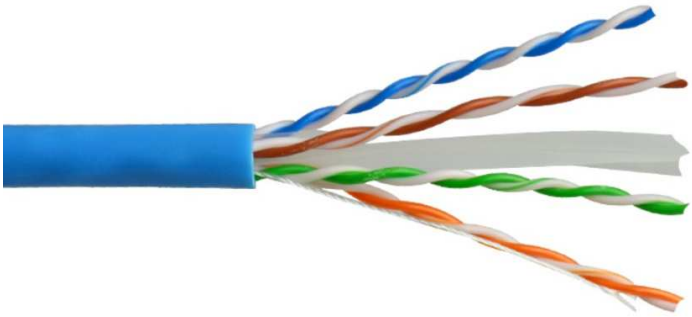


RJ-45 Fêmea RJ-45 Macho

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.

(QUADRIX / IIER-SP – 2023) O meio de transmissão, usado em redes de computadores, que se constitui de um cabo com quatro pares de fio de cobre trançados, usado para interligação de dispositivos em um raio de 100 metros, é denominado cabo:

a) coaxial.
b) de par trançado.
c) de fibra ótica.
d) serial.
e) paralelo.

_____

Comentários: a questão trata do cabo de par trançado. Ele possui quatro pares de fios de cobre trançados e é amplamente utilizado em redes de computadores devido à sua capacidade de transmissão confiável de dados em curtas distâncias, como até 100 metros (Letra B).

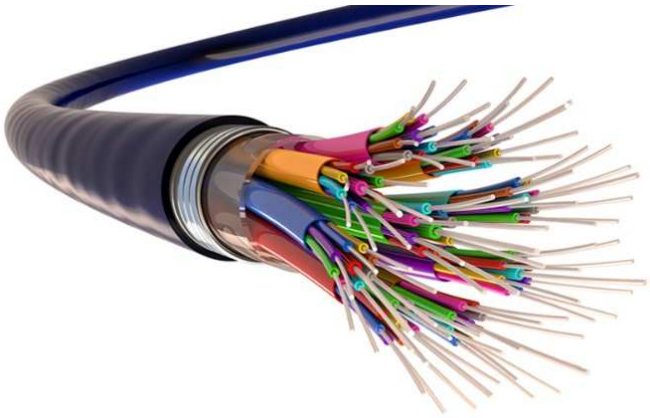
(QUADRIX / CRC-MG – 2022) Quanto aos meios de transmissão em redes de computadores, é comum a utilização de cabos de pares trançados sem blindagem.

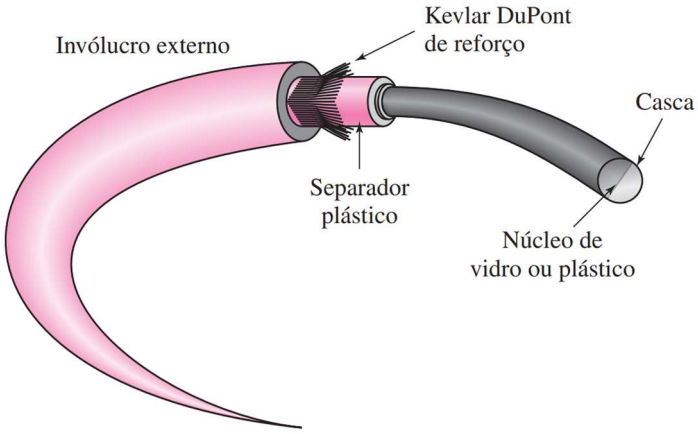
_____

Comentários: a questão está perfeita, sendo o cabo de par trançado sem blindagem mais comum, dado que a blindagem é um revestimento que torna o cabo mais caro e é mais útil em ambientes que tendem a sofrer maior interferência eletromagnética (Correto).

Cabo de Fibra Óptica

INCIDÊNCIA EM PROVA: MÉDIA





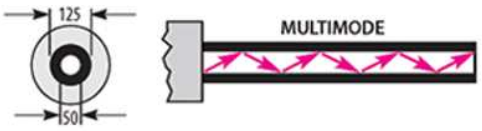
O cabo de fibra óptica consiste em uma casca e um núcleo (de vidro, mais comum; ou plástico) para transmissão de luz. Esse tipo de cabo é normalmente encontrado em backbones de redes por apresentar excelente relação entre ampla largura de banda e custo. Hoje em dia, podemos transferir dados à velocidade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

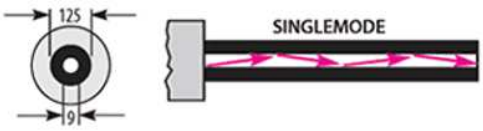
DESVANTAGENS	DESCRIÇÃO
INSTALAÇÃO E MANUTENÇÃO	O cabo de fibra óptica é uma tecnologia relativamente nova. Sua instalação e sua manutenção exigem mão de obra especializada, que não se encontra com facilidade.

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.

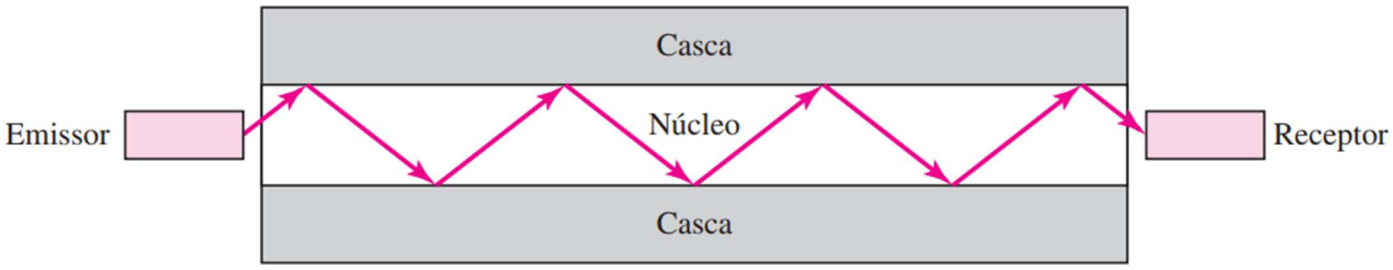
A tecnologia atual suporta dois modos para propagação da luz ao longo de canais ópticos, cada um dos quais exigindo fibras ópticas com características físicas diferentes: **Monomodo e Multimodo**.



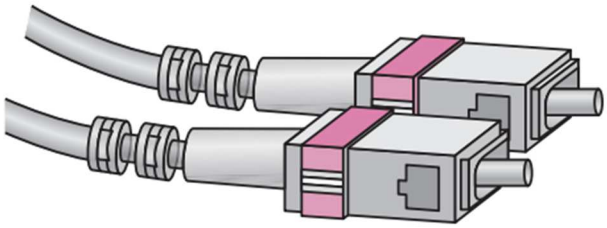
A Fibra Multimodo leva o feixe de luz **por vários modos ou caminhos**, por uma distância menor, com menores taxas de transmissão, mais imprecisa, diâmetro maior e alto índice de refração e atenuação, mas possui construção mais simples, é mais barata e utilizada em LANs.

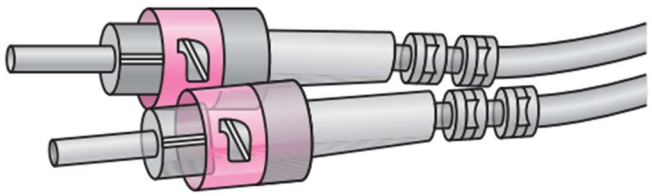


A Fibra Monomodo leva o feixe de luz **por um único modo ou caminho**, por uma distância maior, com maiores taxas de transmissão, mais precisa, diâmetro menor e baixo índice de refração e atenuação, mas possui construção mais complexa, é mais cara e utilizada em WANs.



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

(QUADRIX / CRT-BA – 2023) Na topologia em estrela, devido ao arranjo dos computadores, não é permitido o uso de fibras ópticas.

_____

Comentários: a topologia em estrela não impede o uso de fibras ópticas. A topologia em estrela se refere principalmente à forma como os dispositivos estão conectados, com todos os dispositivos ligados a um hub ou switch central. A escolha do meio de transmissão, como cabos de cobre ou fibras ópticas, pode variar independentemente da topologia (Errado).

(QUADRIX / CRMV-MS – 2022) A fibra óptica, devido à sua alta taxa de interferência, não pode ser utilizada em redes MAN (Metropolitan Area Network).

_____

Comentários: a fibra óptica é uma escolha comum e altamente eficiente em redes MAN (Metropolitan Area Network). Ela é frequentemente usada para transmitir dados em distâncias metropolitanas, devido à sua capacidade de alta largura de banda e imunidade a interferências eletromagnéticas (Errado).

(FACET / Prefeitura de Capim-PB – 2020) Sobre redes de computadores, analise as afirmativas sobre fibra óptica:

I – Utiliza feixes de luz para transmitir dados
II – Não sofre com interferência eletromagnética
III – Seu custo é maior do que os cabos metálicos

Estão corretas:

a) Todas
b) Apenas I
c) I e II
d) Apenas II
e) II e III

_____

Comentários: (I) Correto, ela realmente utiliza feixes de luz para transmitir dados; (II) Correto, ela – de fato – não sofre interferência eletromagnética; (III) Correto, ela é mais cara que cabos metálicos (Letra A).

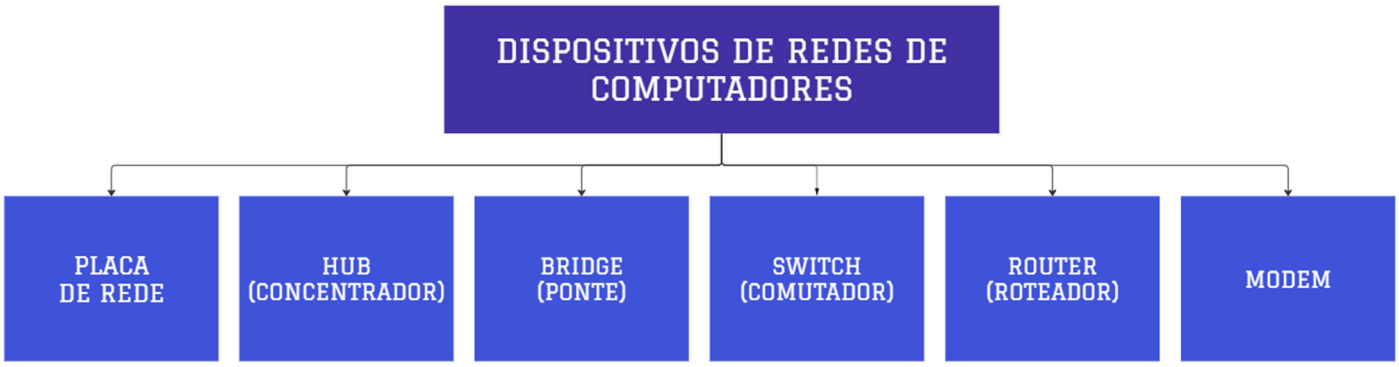
(CESPE / EMBASA – 2010) A fibra ótica é composta basicamente de um núcleo de cobre e uma casca de plástico ou fibra de vidro concêntricos entre si. A transmissão de dados por meio de fibra ótica é realizada pelo envio de um sinal de luz codificado imune a ruídos eletromagnéticos.

_____

Comentários: a fibra óptica consiste em uma casca e um núcleo de vidro ou plástico (extrudido), e não cobre, para transmissão de luz. Por outro lado, é realmente imune a ruídos eletromagnéticos (Errado).

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

PLACAS DE REDE	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.

(PROF. DIEGO / INÉDITA – 2023) Uma placa de rede não é necessária em um computador para conexão com a Internet, pois os modems modernos desempenham essa função.

_____

Comentários: uma placa de rede é necessária para conectar o computador à rede local, e muitos modems modernos têm uma placa de rede embutida para conectar o computador à Internet (Errado).

(PROF. DIEGO / INÉDITA – 2023) Placas de rede são adequadas apenas para redes com fio e não podem ser usadas em redes sem fio (Wi-Fi).

_____

Comentários: placas de rede podem ser usadas tanto em redes com fio quanto em redes sem fio (Wi-Fi). No entanto, é importante usar o tipo de placa de rede apropriado para a infraestrutura da rede em questão. Placas de rede com fio são usadas em redes Ethernet com cabos, enquanto placas de rede sem fio são usadas em redes Wi-Fi, que funcionam de maneira wireless (sem fio) (Errado).

(QUADRIX / CRO-SC – 2023) A placa de rede, ou adaptador de rede, é o dispositivo de hardware utilizado para que um computador se conecte a uma rede de computadores; esse dispositivo possui um número único de identificação, chamado endereço IP.

_____

Comentários: a placa de rede, ou adaptador de rede, é, de fato, um dispositivo de hardware utilizado para conectar um computador ou dispositivo a uma rede de computadores. No entanto, ela é identificada pelo seu endereço MAC (Media Access Control), que é um número único atribuído a cada placa de rede. Não é o endereço IP, mas o endereço MAC que serve como identificação exclusiva da placa de rede (Errado).

(QUADRIX / CRQ-MS – 2021) Assinale a alternativa que apresenta o nome do endereço físico, que é atribuído por seu fabricante, de uma placa de rede, seja ela para rede cabeada ou sem fio.

a) endereço MAC
b) endereço IP
c) DHCP
d) DNS
e) UDP

_____

Comentários: o endereço MAC é o endereço físico único atribuído por um fabricante a uma placa de rede. É usado para identificar exclusivamente uma placa de rede em uma rede local (Letra A).

(CESPE / APEX – 2021) Os computadores comunicam-se entre si e com os demais meios de transmissão de dados por meio de placas de rede, as quais possuem um número único denominado:

a) Endereço WWW (World Wide Web).
b) Endereço IP (Internet Protocol).
c) Endereço MAC (Media Access Control).
d) Endereço de email (correio eletrônico).

_____

Comentários: o número único e exclusivo de placas de rede é o Endereço MAC (Letra C).

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:

HUBS	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.

(QUADRIX / CRMV-MS – 2022) Um hub simula o comportamento de um barramento, ou seja, quando uma estação transmite, a transmissão é recebida por uma porta do hub e retransmitida para as outras.

_____

Comentários: um hub é um dispositivo que opera na camada física da rede e funciona de forma semelhante a um barramento. Quando uma estação conectada a um hub transmite dados, o hub recebe esses dados em uma porta e os retransmite para todas as outras portas. Isso significa que todos os dispositivos conectados ao hub recebem a transmissão, independentemente do destinatário final, o que pode levar a colisões de dados em redes maiores (Correto).

(IDIB / CREMERJ – 2019) A respeito dos equipamentos de interconexão utilizados em redes de computadores, marque a alternativa que indica CORRETAMENTE o nome do dispositivo que, com o passar do tempo, caiu em desuso pelo fato de não ser capaz de direcionar a transmissão de dados em uma rede, limitando-se a atuar como um simples repetidor.

a) Host.
b) Router.
c) Hub.
d) Switch.

_____

Comentários: o dispositivo em desuso incapaz de direcionar a transmissão de dados em uma rede porque só transmite dados em broadcast é o Hub (Letra C).

(CESPE / FUB – 2016) Caso algum cabo de um hub apresente problema, todos os cabos de rede a ele conectados devem ser substituídos, pois, dada a simplicidade de funcionamento do hub, não é possível identificar o cabo defeituoso.

_____

Comentários: em uma rede em que todos os dispositivos estão conectados a um hub, não é necessário substituir todos os cabos se um cabo específico apresentar problemas. Se houver um problema em um cabo específico, você pode substituir apenas esse cabo defeituoso, sem a necessidade de substituir todos os cabos da rede. O hub não é capaz de identificar cabos defeituosos, mas isso não afeta a capacidade de substituir apenas o cabo com defeito (Errado).

(CESPE / SERPRO – 2010) Um hub é, em termos físicos, uma topologia em estrela, mas que pode ser caracterizado, em termos lógicos, como uma topologia em barramento.

_____

Comentários: ele realmente possui topologia física em estrela e lógica em barramento (Correto).

(FCC / SEFAZ-PB – 2006) Dispositivo físico que tem por função básica apenas interligar os computadores de uma rede local. Recebe dados vindos de um computador e os transmite às outras máquinas. Conhece-se também por concentrador:

a) o parser
b) o hub
c) o router
d) a bridge
e) o gateway

_____

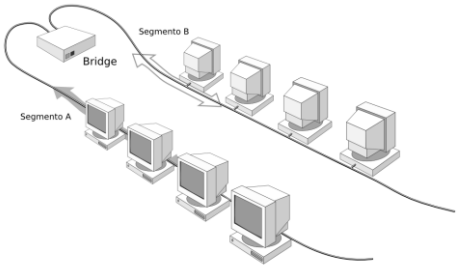
Comentários: dispositivo que tem por função **básica** interligar computadores de uma rede local é o Hub (Letra B).

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.

BRIDGES	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.

(PROF. DIEGO / INÉDITA – 2023) Bridges ajudam a dividir uma rede em segmentos para reduzir o tráfego e melhorar o desempenho.

_____

Comentários: as bridges segmentam redes em segmentos menores para limitar o tráfego e, assim, melhorar o desempenho (Correto).

(PROF. DIEGO / INÉDITA – 2023) As pontes são utilizadas – na grande maioria das vezes – para conectar redes com diferentes protocolos de comunicação.

_____

Comentários: embora possam ser utilizadas para conectar redes com diferentes protocolos de comunicação, as pontes são mais frequentemente utilizadas para conectar segmentos de rede com o mesmo protocolo de comunicação, reduzindo o tráfego entre os segmentos (Errado).

(FUNDATEC / IFFAR – 2023) Qual o dispositivo de rede utilizado para juntar várias LANs físicas em uma única LAN lógica?

a) Gateway.
b) Roteador.
c) Repetidor.
d) Bridge.
e) Hub.

_____

Comentários: o dispositivo utilizado para juntar várias LANs físicas em uma única LAN lógica é a Bridge. Elas desempenham um papel importante na interconexão de redes locais, permitindo a comunicação entre diferentes segmentos de rede enquanto mantêm a segurança e o desempenho da rede (Letra D).

(IADES / CFM – 2018) Uma bridge é um mecanismo usado para conectar dois segmentos de rede diferentes e enviar quadros de um segmento ao outro de forma transparente.

_____

Comentários: ela realmente conecta dois segmentos de rede diferentes e envia quadros (dados) de um segmento a outro. Transparente significa que não se enxerga! *Sabe quando você vai aos Correios e paga para entregar um pacote para alguém?* Se o pacote vai de avião, navio ou carro não importa para você, logo o método de entrega é transparente (ele não enxerga o método). No caso da questão, a bridge envia quadros de um segmento ao outro de forma transparente, isto é, ela consegue enviar dados de um segmento para outro como se estivessem todos em um mesmo segmento sem problema algum, visto que os dispositivos não têm conhecimento de sua existência (Correto).

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?*

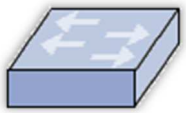
O recurso de autonegociação do switch permite que seja negociado tanto a taxa de transmissão de dados quanto a direção de transmissão, isto é, se um trabalha com uma taxa de transmissão maior e o outro com uma taxa de transmissão menor, eles negociam o envio de dados a uma taxa de transmissão menor, 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*[9]. A representação de um Switch é apresentada abaixo:



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

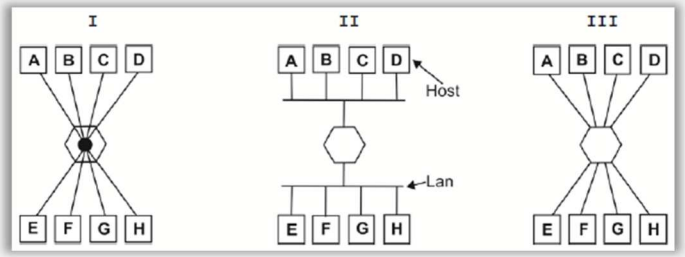
(QUADRIX / CRO-SC – 2023) O switch é um dispositivo de rede que roteia pacotes entre redes de computadores.

_____

Comentários: o switch não roteia pacotes entre redes de computadores – ele opera em um nível mais baixo do modelo OSI, especificamente na camada de enlace de dados – o dispositivo de rede responsável por rotear pacotes é o roteador (Errado).

(FCC / TRT19 – 2022) As figuras a seguir mostram configurações de interconexão de computadores, representados pelas letras de A até H, em rede.

[9] 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.



Observando as configurações I, II e III, um Analista classificou-as, correta e respectivamente, como:

a) bridge gateway e switch.
b) hub, roteador e gateway.
c) repetidor, switch e roteador.
d) gateway, repetidor e switch.
e) hub, bridge e switch.

Comentários: (I) o primeiro dispositivo é um hub, dado que todas as mensagens são transmitidas para todos os demais dispositivos – é possível ver pelo desenho no centro do hub; (II) o segundo dispositivo é uma bridge, dado que interconecta dois segmentos de rede diferentes; (III) o terceiro dispositivo é um switch – ele se parece bastante com o hub pela imagem, mas perceba que as mensagens não são transmitidas para todos os dispositivos da rede. Os desenhos poderiam ser melhores na questão para facilitar a diferenciação dos dispositivos (Letra E).

(SELECON / Prefeitura de Cuiabá-MT – 2018) Tendo por foco o modelo OSI/ISO, um equipamento de interconexão de nível 2 opera por meio da segmentação como comutador de rede na camada de enlace, além de representar um dispositivo para solucionar problemas de congestionamento. Esse equipamento é conhecido por:

a) hub b) router c) gateway d) switch

Comentários: nível 2, segmentação de redes, comutador, camada de enlace são todas palavras-chave para Switch (Letra D).

(IBFC / Prefeitura de Araraquara-SP – 2017) Em uma rede de computadores, que é utilizada a topologia em estrela, existe a necessidade de se utilizar o equipamento de rede denominado em inglês como:

a) gateway b) switch c) modem d) bridge

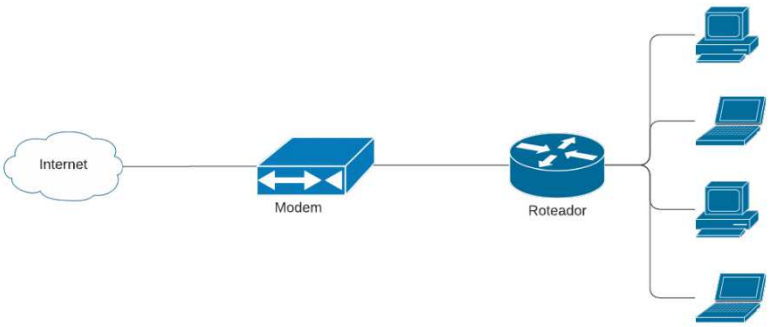
Comentários: (a) Errado. Um gateway é um dispositivo que atua como um ponto de entrada para outra rede. Embora seja um componente importante em redes, não é especificamente relacionado à topologia em estrela; (b) Correto. O switch é um dispositivo de rede que encaminha dados apenas para o dispositivo específico ao qual eles são destinados em uma rede local. É comumente usado em topologias em estrela para conectar vários dispositivos a um ponto central; (c) Errado. Um modem é um dispositivo que converte os sinais digitais de um computador em sinais analógicos para transmissão através de linhas de comunicação, como linhas telefônicas. Não é exclusivamente usado em topologias de estrela, mas pode ser encontrado em várias configurações de rede; (d) Errado. Uma bridge é um dispositivo que conecta redes locais diferentes e pode operar em várias topologias. No entanto, sua função principal é conectar redes, não necessariamente em topologias de estrela (Letra B).

Router (Roteador)

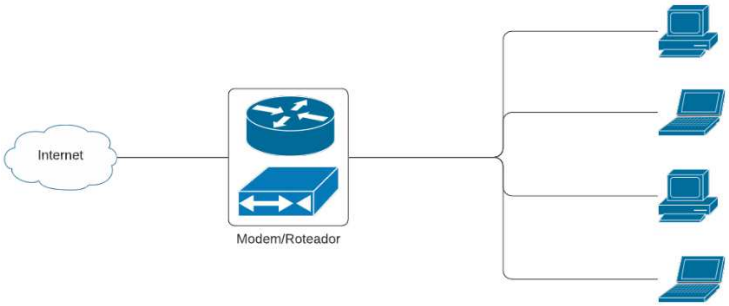
INCIDÊNCIA EM PROVA: ALTA

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.

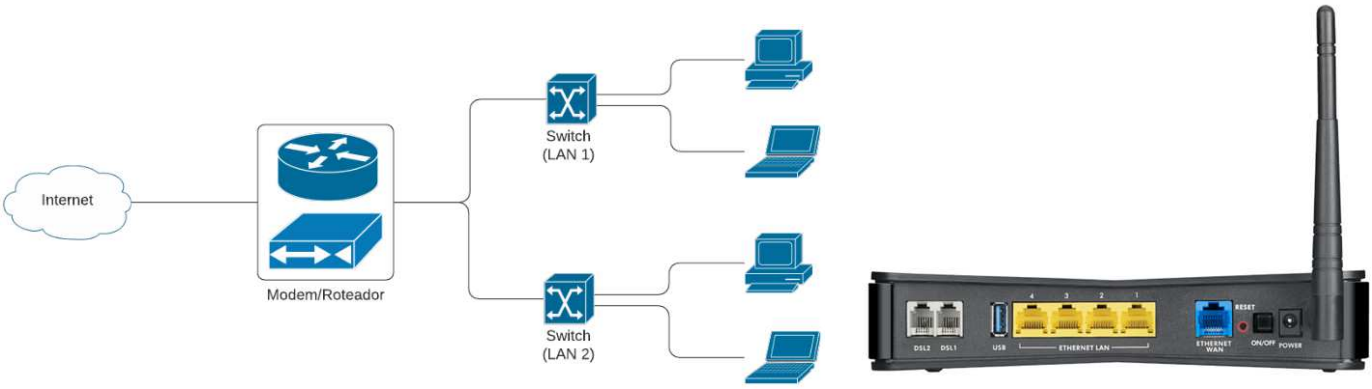


Atualmente, nós estamos na era dos combos, isto é, um único provedor fornece Internet, Telefone e TV a Cabo (Ex: NET/Claro, GVT/Vivo, etc). Nesse caso, um único aparelho condensa as funções de modem e roteador – você provavelmente tem esse aparelho na sua casa! Em geral, um cabo coaxial branco entra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

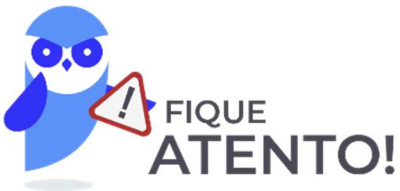
computadores, impressora e banco de dados da cafeteria. **O hotspot é – apenas e tão somente – um local onde uma rede sem fio está disponível para ser utilizada.** Alguns estabelecimentos oferecem de forma gratuita (bares, restaurantes, etc) e outros são pagos (aeroportos e hotéis).

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.

ROTEADORES	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.

(IDECAN / IF-PB – 2019) A respeito dos diversos tipos de equipamentos de rede, assinale a alternativa que indica corretamente o nome do equipamento de rede capaz de realizar uma conexão entre diferentes redes de modo a permitir a troca de informações entre elas, mas que seja capaz também de controlar o fluxo da informação, possibilitando, por exemplo, a criação de rotas mais curtas e rápidas:

a) Modem
b) Repetidor
c) Bridges
d) Switch
e) Roteador

_____

Comentários: conexão entre diferentes redes (Ex: Internet e LAN) e controlar fluxo de informações pelas rotas são responsabilidades do roteador (Letra E).

(IBADE / Prefeitura de João Pessoa-PB – 2018) Um equipamento de rede que permite que computadores de uma rede possam se conectar a Internet é o:

a) HDCD.
b) pen drive.
c) roteador.
d) scanner.
e) VGA.

_____

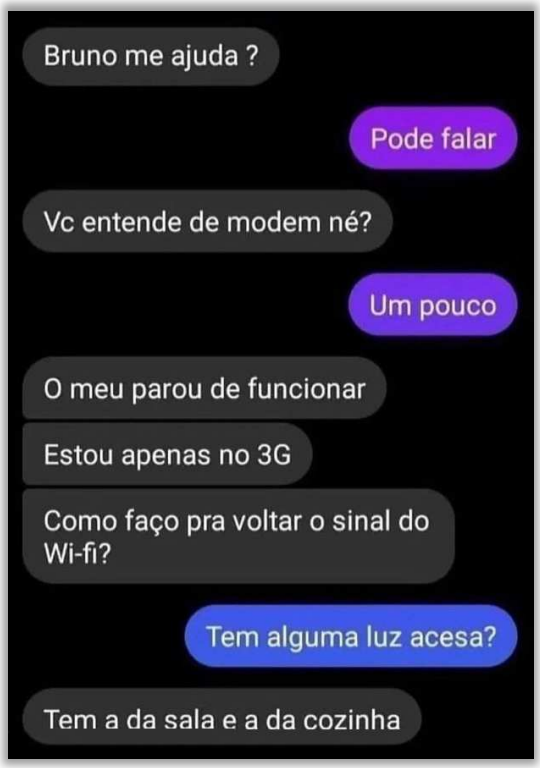
Comentários: o dispositivo responsável por permitir a conectividade entre dispositivos como computadores, smartphones, tablets, etc em uma Rede LAN com a internet é o Roteador (Letra C).

Modem

INCIDÊNCIA EM PROVA: MÉDIA

Galera, imaginem que eu preciso enviar um e-mail para o Prof. Renato! **Para que essa mensagem saia do meu computador e chegue no computador dele, é necessário que ela seja transmitida por um meio de comunicação**. Pode ser através de fibras ópticas, ondas de rádio, entre outros – no entanto há uma alternativa interessante de infraestrutura que já existe na imensa maioria dos lugares. *Qual, professor?* A infraestrutura de linha telefônica!

Isso não é tão simples assim, porque os computadores possuem uma linguagem diferente da linguagem dos telefones. Quando eu envio um e-mail para o Prof. Renato, a mensagem é convertida em um conjunto de dígitos binários (Ex: 0111010001000111010). Os telefones não conseguem entender essa linguagem porque eles utilizam sinais analógicos que, inclusive, não são entendidos por computadores. É como se um falasse húngaro e o outro aramaico!



Como resolver esse problema? **Evidentemente nós precisamos de um tradutor**! E é aí que entra o papel do Modem (**Mo**dulador/**Dem**odulador). Esse dispositivo converterá os dígitos binários do meu computador em sinais analógicos que podem ser transmitidos em linhas telefônicas; e também converterá os sinais analógicos das linhas telefônicas em dígitos binários. *Ficou mais fácil de entender agora?* Então vamos ver a definição...

O Modem é um dispositivo eletrônico de entrada/saída de dados que modula um sinal digital em um sinal analógico a ser transmitido por meio de uma linha telefônica e que demodula o sinal analógico e o converte para o sinal digital original. **Hoje em dia, existem basicamente três tipos: Acesso Discado, Modem ADSL e Cable Modem.**

O Modem de Acesso Discado é inserido na placa-mãe do seu computador. Quem aí é mais velho sabe que antigamente a internet era bem lenta e muito cara! *Sabe como eu fazia para me conectar à internet?* Eu esperava passar de meia-noite (porque o minuto cobrado ficava bem mais barato), desconectava o cabo do telefone fixo e conectava esse mesmo cabo no modem de acesso discado na parte de trás do gabinete do computador. O telefone, é claro, parava de funcionar!

Depois disso, você abria um discador e tinha que fazer infinitas tentativas para conseguir se conectar! Quando você finalmente conseguia, você ficava todo feliz, mas demorava mais ou menos uns dois minutos para abrir qualquer página na internet e quando ela estava quase toda aberta... a conexão caía! É, criançada... a vida era um bocado mais difícil, mas era divertido! Deixa eu contar uma historinha que aconteceu comigo...

Naquela época, poucas pessoas tinham condição de possuir um celular. Se você quisesse falar com alguém, teria que ligar em um telefone fixo e torcer para que o destinatário estivesse no local. Minha irmã mais velha estava grávida de nove meses e eu – aos 13 anos – estava doido para que chegasse meia-noite, **assim eu poderia acessar à internet de graça e ler meus fóruns sobre o jogo que virou febre na época: Pokemon (não é Pokemon Go, eu sou raiz...)**.

Como vocês sabem, ao se conectar utilizando um Modem Dial-Up, o telefone ficava ocupado. Você não conseguiria ligar para ninguém e, se alguém te ligasse, ouviria o sinal de ocupado. Ocorre que a bolsa da minha irmã estourou e nem ela nem o esposo possuíam carro, logo ela ligou para minha mãe buscá-la. *O que aconteceu?* Tu-tu-tu-tu-tu – sinal de ocupado porque eu estava vendo meus fóruns. *Tomei uma surra monumental: sim ou não?* Pois é! Ainda bem que ela conseguiu outro transporte e meu sobrinho está hoje com 20 anos! **Até que chegaram os Modens ADSL.**

Empresas de telefonia fixa ofereciam acesso em banda larga[10] por meio de cabos ou wireless. Pessoal, era muito mais rápido (velocidade de download/upload) e não ocupavam o telefone, ou seja, você podia utilizar o telefone e a internet simultaneamente. Por fim, temos o Modem Cabeado (*Cable Modem*)! Eles não utilizam as linhas telefônicas – eles são conectados por meio de cabos coaxiais normalmente fornecido pela sua fornecedora de TV a Cabo. *Como é, professor?*

[10] Banda é a quantidade de bits que podem trafegar por uma conexão em uma determinada unidade de tempo, isto é, velocidade (Ex: 100Mbps).

Você tem NET ou GVT? Pois é, elas te oferecem serviços diferentes! Um serviço interessante é o combo: TV, Internet e Telefone! Em vez de utilizar três meios para te fornecer cada um desses serviços, ela transmite todos esses dados via cabo coaxial. **Algumas vezes, esse modem virá com um roteador acoplado internamente**; outras vezes, você terá que comprar um roteador e utilizar ambos para ter acesso à internet. *Entendido?* Então vamos seguir...

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.

(QUADRIX / CRESS-SE – 2021) Caso o usuário possua somente um modem ADSL para acessar a Internet, não será possível compartilhar essa conexão na rede para outros usuários.

_____

Comentários: é possível compartilhar uma conexão de Internet por meio de um modem ADSL com outros usuários em uma rede. Para fazer isso, normalmente é necessário utilizar um roteador. O roteador permite que vários dispositivos se conectem à Internet através do modem ADSL, compartilhando assim a conexão. Isso é um cenário comum em redes domésticas e de pequenos escritórios, onde diversos dispositivos, como computadores, laptops, smartphones e tablets, precisam acessar a Internet a partir de um único modem ADSL (Errado).

(IBADE / Prefeitura de Linhares-ES – 2020) Um dispositivo ao qual está conectada uma linha telefônica, permitindo a transmissão de dados através dela chama-se:

a) Modem.
b) Barramento.
c) Switch.
d) Hub.
e) Transceiver.

_____

Comentários: o dispositivo ao qual está conectada uma linha telefônica, permitindo a transmissão de dados através dela, é chamado de modem (Letra A).

(UFGD / UFGD – 2019 – Letra C) O modem é um dispositivo eletrônico que modula um sinal digital numa onda analógica, pronta a ser transmitida pela linha telefônica, e que demodula o sinal analógico e reconverte-o para o formato digital original.

_____

Comentários: o modem realmente é um dispositivo utilizado para a conversão de sinais digitais em sinais analógicos para transmissão e vice-versa para recepção (Correto).

(CESPE / CET – 2011) O modem:

a) é um tipo de memória semicondutora não volátil.

b) é um tipo de interface paralela que permite a comunicação sem fio entre um computador e seus periféricos.

c) é um roteador wireless para redes sem fio.

d) tem função de garantir o fornecimento ininterrupto de energia elétrica ao computador.

e) pode auxiliar na comunicação entre computadores através da rede telefônica.

_____

Comentários: (a) Errado, modem não tem nenhuma relação com memória semicondutora; (b) Errado, modems são usados para comunicação de dados via linhas telefônicas ou redes semelhantes, mas não estão diretamente relacionados à comunicação sem fio entre computadores e periféricos; (c) Errado, um modem e um roteador são dispositivos distintos. Enquanto o modem lida com a conversão de sinais para comunicação através da infraestrutura de rede, um roteador é responsável pela distribuição de conexões em redes locais, como redes sem fio (Wi-Fi); (d) Errado, isso descreve uma função de um no-break (UPS) ou um estabilizador de energia, não do modem; (e) Correto, O modem é projetado para auxiliar na comunicação entre computadores e outros dispositivos através da rede telefônica, convertendo os sinais digitais dos computadores em sinais analógicos que podem ser transmitidos pela linha telefônica e vice-versa (Letra E).

(FUNRIO / DEPEN – 2008) Quais as características a tecnologia de conexão à Internet denominada ADSL:

a) Conexão permanente, custo fixo, linha telefônica liberada e velocidade maior do que as linhas tradicionais.

b) Conexão permanente, custo variável, linha telefônica liberada e velocidade maior do que as linhas tradicionais.

c) Conexão permanente, custo fixo, linha telefônica não liberada e velocidade maior do que as linhas tradicionais.

d) Conexão não-permanente, custo variável, linha telefônica liberada e velocidade igual às linhas tradicionais.

e) Conexão não-permanente, custo fixo, linha telefônica não liberada e velocidade igual às linhas tradicionais.

Comentários: *conexão permanente* – ADSL permite que você se mantenha sempre conectado, em contraste com as linhas tradicionais (Ex: Dial-up) em que – para acessar a internet – precisa se conectar; *custo fixo* – ADSL possui um custo fixo, visto que você não paga mais por conta do horário, etc, em contraste com linhas tradicionais em que você paga valores adicionais a depender do horário; *linha telefônica liberada* – ADSL permite que se utilize a internet e o telefone simultaneamente, em contraste com linhas tradicionais em que você ou utiliza a internet ou utiliza o telefone; *velocidade maior do que as linhas tradicionais* – ADSL possui a grande vantagem de permitir uma velocidade (muito) maior do que as linhas tradicionais (Letra A).

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)[11]
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)

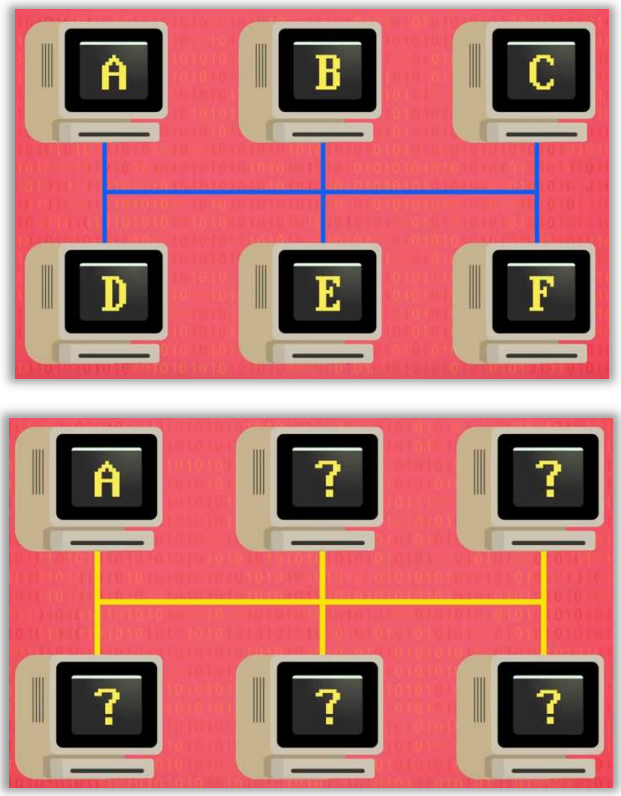
[11] Sendo rigorosamente técnico, há uma diferença entre IEEE 802.3 e Ethernet relacionado a um campo de endereço de origem e destino, mas eu só vi essa diferença ser cobrada em prova uma vez até hoje. Além disso, para lembrar da numeração do Padrão Ethernet, lembre-se de: **ETHERNET → 3TH3RN3T**; e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

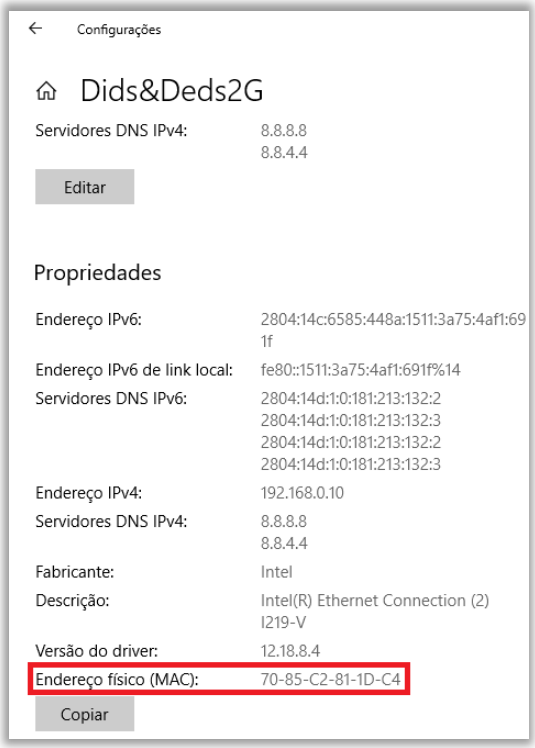
Padrão Ethernet (IEEE 802.3)

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?*



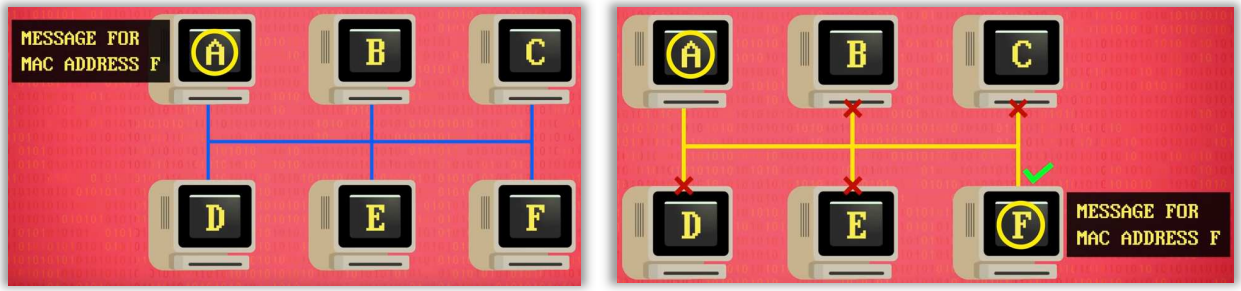


Na imagem acima, temos o *backbone* em azul porque nenhum sinal está sendo transmitido; e na imagem abaixo, temos o *backbone* em amarelo onde o sinal está sendo transmitido. **Notem que o *backbone* está todo amarelo porque – como a transmissão ocorre em *broadcast* – todas as máquinas o recebem.** 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.**

(CESPE / TRF1 – 2017) No padrão Ethernet, após detectar e sinalizar uma colisão, o método CSMA/CD determina que a estação que deseja transmitir espere por um tempo aleatório, conhecido como backoff, e, em seguida, tente realizar a transmissão novamente.

_____

Comentários: no CSMA/CD, as estações primeiro "escutam" a rede para verificar se está ociosa antes de transmitir dados. Se a rede estiver ocupada, elas aguardam um momento aleatório antes de tentar novamente. Isso ajuda a evitar colisões, já que várias estações podem tentar acessar a rede ao mesmo tempo. Se ocorrer uma colisão (ou seja, duas estações tentarem transmitir simultaneamente), elas detectarão a colisão e aguardarão um período aleatório antes de tentar novamente. Esse processo permite um acesso relativamente justo à rede para todas as estações (Correto).

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...

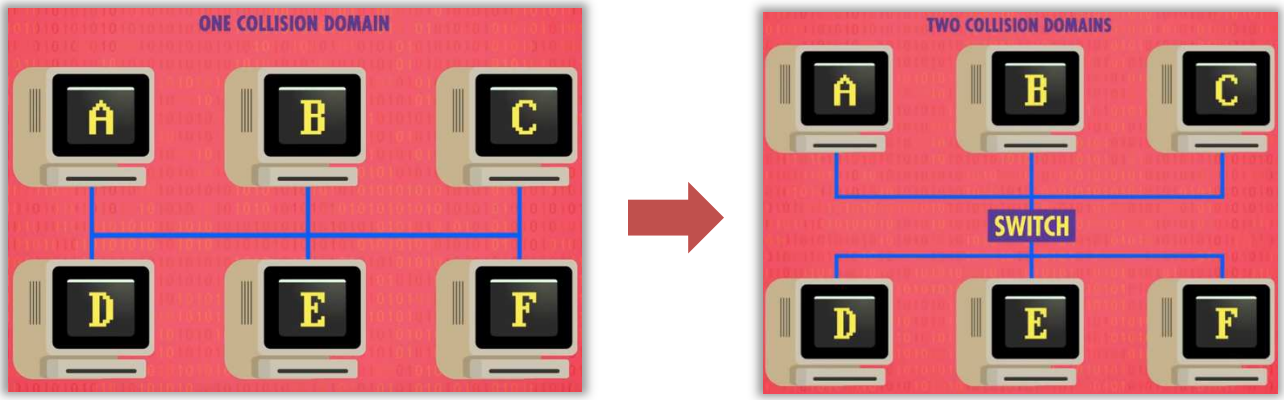
(QUADRIX / CRMV-MS – 2022) Uma das desvantagens das redes ethernet é que todas as estações possuem acesso à rede de maneira diferente, com relação ao tempo de acesso.

_____

Comentários: em redes Ethernet, todas as estações acessam a rede de maneira semelhante – por meio do protocolo CSMA/CD. Várias estações compartilhem o mesmo meio de transmissão e quando uma estação deseja transmitir dados, verificam se o meio está ocupado (*Carrier Sense*) e, se estiver livre, a estação começa a transmitir. Se duas estações tentarem transmitir ao mesmo tempo e ocorrer uma colisão, ambas detectarão a colisão (*Collision Detection*) e interromperão suas transmissões – após uma pausa aleatória, ambas tentarão de novo (Errado).

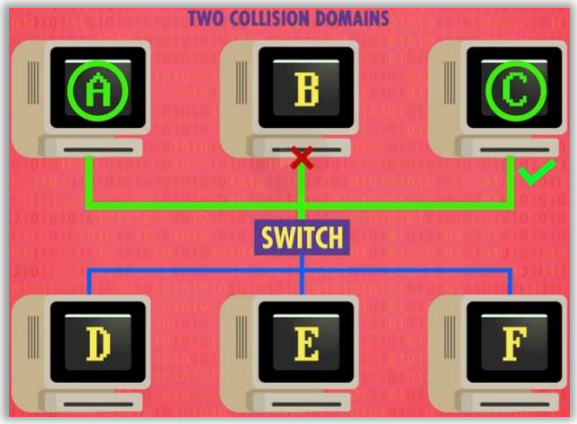
Para reduzir o número de colisões e melhorar a eficiência, nós precisamos diminuir a quantidade de dispositivos nos meios de transmissão compartilhados. Nesse momento, entra o conceito de Domínio de Colisão. *O que é isso, Diego?* Trata-se de uma área onde pacotes podem colidir uns contra os outros.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

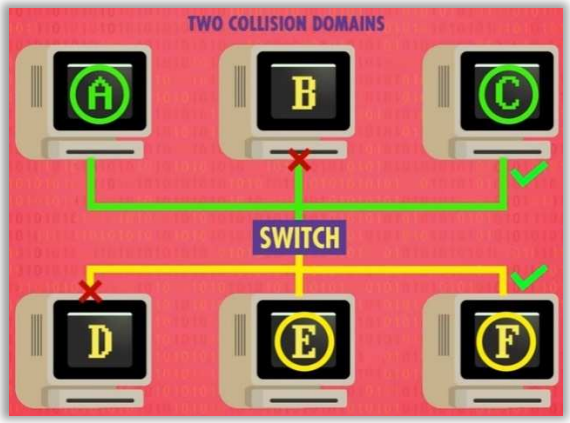
> *Pequena analogia para entender o que é um domínio de colisão: Imagine um corredor estreito em uma escola, em que os alunos estão indo para as aulas. Cada aluno representa um dispositivo de rede, como um computador. O corredor é a rede de cabos físicos ou meio compartilhado (por exemplo, um cabo Ethernet) 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[12]. **Ele segmentará nossa rede em duas partes e ficará posicionado entre elas**.

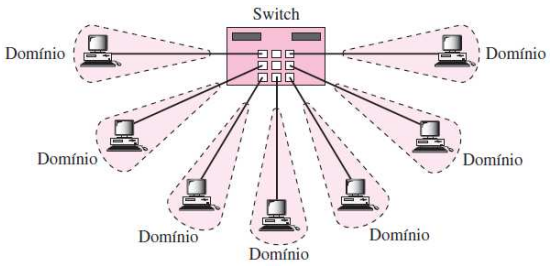
[12] Utilizar a topologia em estrela com um hub não adiantaria nada porque esse dispositivo tem topologia lógica em barramento.

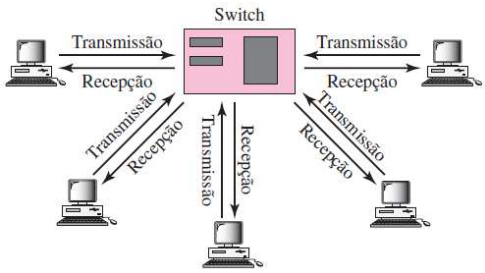




Dessa forma, ele só passará dados para o outro domínio de colisão se a mensagem for destinada a algum computador presente nesse domínio de colisão. *Como ele faz isso, professor?* Ele guarda uma lista de Endereços MAC dos computadores de cada rede. **Assim, se o Computador A deseja transmitir dados para 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! :)

(CONSULPAM / ICTIM-RJ – 2023) Nas redes de computadores, é possível que ocorra uma colisão entre pacotes de dados quando duas ou mais estações pertencentes ao mesmo segmento de rede compartilhado transmitem quadros ao mesmo tempo. Assinale a alternativa que traz CORRETAMENTE um exemplo de domínio de colisão.

a) Todos os dispositivos estão conectados a um hub ethernet.

b) Todos os dispositivos estão conectados a um comutador ethernet.
c) Todos os dispositivos estão conectados a um roteador wireless.
d) Dois computadores, ambos conectados através de um cabo crossover.

_____

Comentários: (a) Correto. Quando todos os dispositivos estão conectados a um hub Ethernet, eles compartilham o mesmo segmento de rede e fazem parte do mesmo domínio de colisão; (b) Errado. Nesse caso, cada porta do comutador (switch) cria seu próprio domínio de colisão, o que significa que as colisões são evitadas na medida do possível; (c) Errado. Os dispositivos estão conectados a um roteador wireless, que não compartilha o mesmo meio físico, logo não é um domínio de colisão; (d) Errado. Apenas dois computadores estão conectados através de um cabo crossover, o que significa que não há mais dispositivos no mesmo segmento de rede (Letra A).

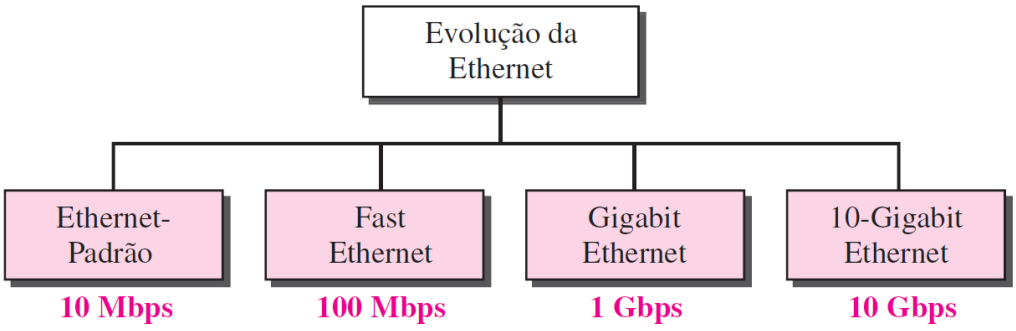
O que temos até agora sobre o Padrão Ethernet? **Sabemos que ele pode funcionar por meio da topologia em barramento.** Como pode haver colisões, entra em ação o CSMA/CD, que utiliza um algoritmo para evitar colisões. Ainda assim, sabemos que a topologia em barramento tem diversas limitações, inclusive 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.

(CESPE / DATAPREV – 2023) O IEEE 802.3 define o método de acesso à rede local usando o CSMA/CD (Carrier-Sense Nultiple Access with Collision Detection).

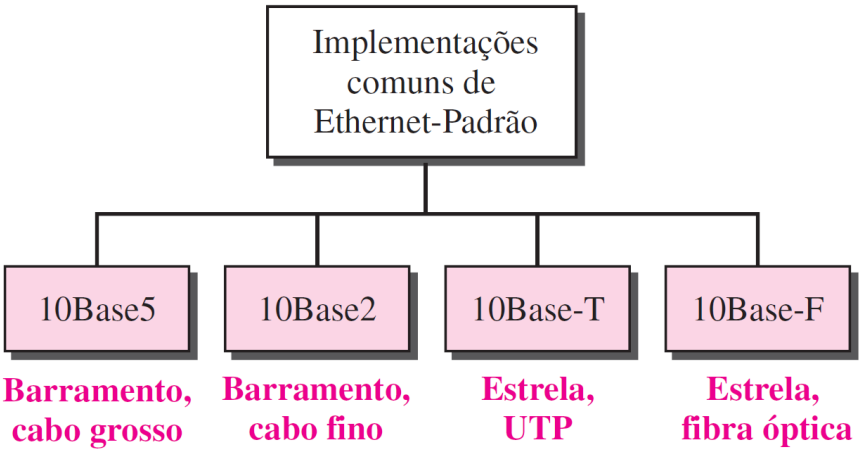
_____

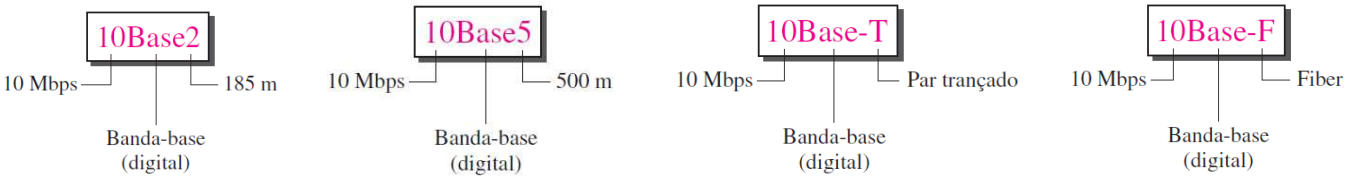
Comentários: perfeito... o método de acesso à rede local no na Ethernet (IEEE 802.3) é o CSMA/CD (Correto).

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).

(QUADRIX / CREME-RN – 2022) No padrão Ethernet, uma largura de banda de 100 Gbps permite a transmissão de até 100 milhões de bits por segundo.

Comentários: na verdade, ele permite a transmissão de até 100 **bilhões** de bits por segundo (Errado).

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.

(QUADRIX / CRMV-MS – 2022) Em função de o desenho das redes ethernet ser muito complexo, esse tipo de rede não permite manutenção após sua implementação.

Comentários: o desenho das redes Ethernet pode ser complexo, dependendo do tamanho e da topologia da rede, mas isso não significa que não permita manutenção após a implementação. Na realidade, as redes Ethernet são altamente mantidas e administradas, e as equipes de TI frequentemente realizam tarefas de manutenção, como monitoramento, solução de problemas, atualizações e expansões, para garantir que a rede funcione de maneira eficiente e confiável. A complexidade pode exigir conhecimento e planejamento adequados, mas a manutenção é uma parte essencial da gestão de qualquer rede Ethernet (Errado).

(QUADRIX / CRN6 – 2022) Em função de seu alto custo, o Ethernet, canal lógico pelo qual os dados podem fluir de um computador para outro, é a tecnologia menos utilizada em redes de computadores.

Comentários: Ethernet é uma das tecnologias de rede mais amplamente utilizadas em redes de computadores em todo o mundo devido à sua eficiência, confiabilidade e custo geralmente acessível. É verdade que, em alguns casos específicos, outras tecnologias de rede, como redes de fibra óptica, podem ser mais caras de implementar. No entanto, em geral, o Ethernet é uma tecnologia muito comum e amplamente adotada em redes empresariais e domésticas devido à sua relação custo-benefício e ampla compatibilidade com uma variedade de dispositivos de rede (Errado).

(MGA / TCE-CE – 2015) As taxas nominais de transmissão definidas em bits por segundo de 10M, 1000M, e 100M são, respectivamente, atribuídas aos padrões:

a) Fast Ethernet, Ethernet e Gigabit Ethernet;
b) Ethernet, Gigabit Ethernet e Fast Ethernet;
c) Gigabit Ethernet, Ethernet e Fast Ethernet;
d) Fast Ethernet, Ethernet e Gigabit Ethernet.

Comentários: 10M é a taxa atribuída à Ethernet; 1000M é a taxa atribuída à Gigabit Ethernet; e 100M é a taxa atribuída à Fast Ethernet (Letra B).

Padrão Token Ring (IEEE 802.5)

INCIDÊNCIA EM PROVA: MÉDIA

O Padrão Token Ring é outro padrão cabeado e foi, até o início da década de 90, o principal concorrente do Padrão Ethernet, quando possuía taxa de transmissão de dados de 4 Mbps, comunicação unidirecional (chamada *simplex)*, arquitetura ponto-a-ponto e topologia lógica em anel. Por falar nisso, quando falamos em Topologia em Estrela, havia um risco de colisão – no Padrão Token Ring esse risco não existe porque utiliza Topologia em Anel.

Por que esse padrão se chama Token Ring? **Isso ocorre basicamente porque cada estação de trabalho dessa rede de computadores se conecta com a adjacente até fechar um circuito fechado chamado Anel (*Ring*).** Para que uma estação de trabalho possa transmitir dados para outra estação de trabalho, ela precisa possuir uma espécie de envelope chamado *token*. Vamos entender isso melhor...

(IADES / UFBA – 2014) Uma rede local de computadores pode ser classificada quanto a sua arquitetura. Assinale a alternativa que indica um exemplo de rede, cuja arquitetura se caracteriza por uma topologia em anel em que as estações devem aguardar a sua recepção para transmitir.

a) Ethernet.
b) FDDI.
c) Token ring.
d) Frame relay.
e) DSL.

_____

Comentários: topologia em anel em que as estações devem aguardar a sua recepção para transmitir por meio de um token é o Token Ring (Letra C).

Uma analogia que pode ser usada para explicar a comunicação no Token Ring é a de uma corrida de revezamento. Em uma corrida de revezamento, cada equipe tem um bastão que deve ser passado de um corredor para outro até que todos os corredores da equipe tenham completado uma volta na pista. **Nós podemos dizer que um token é basicamente uma espécie de autorização ou envelope que dá ao dispositivo o direito de transmitir dados.**

O token circula pela rede, de dispositivo em dispositivo, até que um dispositivo o pegue. Quando um dispositivo pega o token, ele pode transmitir os dados que deseja enviar. **Assim como em uma corrida de revezamento, apenas um dispositivo na rede pode transmitir dados por vez.** O token garante que os dispositivos não transmitam dados ao mesmo tempo, o que evitaria colisões de dados. Então seria mais ou menos assim...

(IBADE / Prefeitura de Cujubim-RO – 2018) Um administrador de rede precisa configurar uma rede que funcione na camada física e de enlace dados do modelo OSI,

que use um símbolo (que consiste em um sinal de três bytes) que vai circular nos computadores em uma topologia do tipo anel e na qual esses computadores devem aguardar a recepção desse símbolo para transmitir. Essa rede é do tipo:

a) Barramento.
b) Ethernet.
c) Estrela.
d) Netware.
e) Token Ring.

_____

Comentários: no Token Ring, os dispositivos formam um anel lógico e aguardam a recepção de um símbolo especial (o token) antes de transmitir dados (Letra E).

O token é o bastão; o dispositivo que tem o token é o corredor que está com o bastão; os dados que o dispositivo está transmitindo são a mensagem que o corredor está carregando; e os outros dispositivos na rede são os espectadores da corrida. **A analogia da corrida de revezamento é uma maneira simples e fácil de entender o conceito de comunicação no Token Ring.** Vamos ver agora as principais vantagens e desvantagens desse padrão:

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.

Token Ring oferece confiabilidade e baixa latência devido à falta de colisões, mas tende a ser mais caro e menos flexível em termos de escalabilidade. A Ethernet é mais acessível, fácil de implementar e altamente escalável, embora possa ter colisões em redes congestionadas. A escolha entre as duas depende das necessidades específicas da rede e das limitações orçamentárias. *Entendido?*

(CESPE / MPU – 2010) As arquiteturas de rede Token Ring e Ethernet, padronizadas pelo modelo IEEE 802.5, possuem o mesmo funcionamento em todas as suas camadas, no entanto diferem-se quanto ao tempo de envio de quadro de dados, pois em redes Ethernet não há colisões, já que cada máquina envia um quadro por vez.

Comentários: as arquiteturas de rede Token Ring e Ethernet são padronizadas pelo IEEE 802.5 e IEEE 802.3, respectivamente, e não pelo mesmo padrão. Além disso, a afirmação de que em redes Ethernet não há colisões não é correta. Colisões podem ocorrer em redes Ethernet, especialmente em hubs, que compartilham o meio de transmissão. Redes Ethernet usam o método CSMA/CD para lidar com colisões (Errado).

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.

(QUADRIX / CRECI22 – 2023) O uso de redes Wi-Fi públicas não deve ser evitado, pois essas redes são totalmente seguras.

_____

Comentários: é importante ter precauções ao usar redes Wi-Fi públicas, como evitar a transmissão de informações sensíveis e considerar o uso de uma VPN (Rede Virtual Privada) para criptografar sua conexão e proteger sua privacidade. Não é aconselhável considerar redes Wi-Fi públicas como totalmente seguras (Errado).

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.

(CESPE / BB – 2007) Wi-Fi (Wireless Fidelity) refere-se a produtos que utilizam tecnologias para acesso sem fio à Internet, com velocidade que pode chegar a taxas superiores a 10 Mbps. A conexão é realizada por meio de pontos de acesso denominados hot spots. Atualmente, o usuário consegue conectar-se em diferentes lugares, como hotéis, aeroportos, restaurantes, entre outros. Para que seja acessado um hot spot, o computador utilizado deve possuir a tecnologia Wi-Fi específica.

_____

Comentários: tudo impecável – um hotspot é simplesmente o nome dado ao local em que a tecnologia Wi-Fi está disponível. São encontrados geralmente em locais públicos, tais como cafés, restaurantes, hotéis e aeroportos, onde é possível se conectar à Internet utilizando qualquer computador portátil que esteja preparado para se comunicar com uma Rede Wi-Fi (Correto).

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.

(OBJETIVA / Prefeitura de Pedras Altas – 2022) Wi-Fi (Wireless Fidelity) é um tipo de rede local que utiliza sinais de rádio para comunicação. Redes Wi-Fi se tornaram populares; contudo, embora bastante convenientes, há alguns riscos, e, para resolver alguns desses riscos, foram desenvolvidos mecanismos de segurança. Sobre esses mecanismos de segurança, assinalar a alternativa que preenche as lacunas abaixo CORRETAMENTE:

O _____ foi o primeiro mecanismo de segurança a ser lançado, é considerado frágil e, por isso, seu uso deve ser evitado. O _____ é o mecanismo mais recomendado.

a) WPA-2 | WPA
b) WPA | WEP
c) WEP | WPA-2
d) WPA | WPA-2

_____

Comentários: WEP foi o primeiro mecanismo de segurança a ser lançado, é considerado frágil e, por isso, seu uso deve ser evitado. O WPA-2 é o mecanismo mais recomendado (Letra C).

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.

(FUNDATEC / PROCERGS – 2023) O padrão 802.11 é o principal padrão de LAN sem fio chamada de Wireless Fidelity (Wi-fi). Atualmente, as redes Wi-fi tornaram-se bastante usuais pela mobilidade que proporcionam e pela facilidade de instalação e de uso em diferentes tipos de ambientes. Em relação à rede Wi-fi, analise assertivas abaixo:

I. As redes Wi-fi são compostas de clientes, como notebooks e telefones móveis, e infraestrutura, chamada pontos de acesso ou Access Points (APs), que são instalados nos prédios.

II. Este tipo de rede caracteriza-se por dois modos básicos de operação: o modo Infraestrutura (que faz uso de um concentrador de acesso ou roteador wireless) e o modo ponto a ponto (chamado ad-hoc, que permite criar redes pequenas, com as máquinas se comunicando entre si, sem o uso de um concentrador de acesso).

III. Em redes Wi-Fi públicas, que não utilizam mecanismos de criptografia, os dados podem ser indevidamente coletados por atacantes.

Quais estão corretas?

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

Comentários: (I) Correto. Redes Wi-Fi são compostas por clientes (como notebooks, smartphones, tablets) e infraestrutura, que inclui os pontos de acesso ou Access Points, que são dispositivos instalados em prédios ou locais que fornecem a conectividade Wi-Fi; (II) Correto. Redes Wi-Fi possuem dois modos básicos de operação: o modo Infraestrutura é o mais comum, em que os dispositivos se conectam a um concentrador de acesso (como um roteador Wi-Fi) e o modo ponto a ponto (ad-hoc) permite que as máquinas se comuniquem diretamente entre si, sem a necessidade de um concentrador de acesso. Esse modo é útil para criar redes pequenas e temporárias; (III) Correto. Em redes Wi-Fi públicas que não utilizam mecanismos de criptografia, os dados transmitidos podem ser capturados por atacantes. Isso ocorre porque, sem criptografia, os dados são transmitidos em formato aberto, tornando-os vulneráveis à interceptação. É importante ter cuidado ao usar redes Wi-Fi públicas não seguras, especialmente ao lidar com informações sensíveis (Letra E).

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[13].**

EVOLUÇÃO DO PADRÃO WI-FI (802.11)[14]		
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

(IFMG / IFMG – 2023) Qual o padrão IEEE está relacionado à tecnologia WI-FI 6?

a) 802.11ac b) 802.11ax c) 802.11b d) 802.11g e) 802.11n

Comentários: o padrão conhecido Wi-Fi 6 é o 802.11ax (Letra B).

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

[14] Para decorar a ordem, lembre-se da palavra **BAG**U**NÇA** (lembrando que CA é AC).

(FGV / TCE-AM – 2021) Uma aplicação precisa operar em um ambiente de rede sem fio, com velocidade de 200 Mbps. Além disso, a frequência usada nessa rede deve ser de 2.4 GHz. O padrão de rede sem fio mais indicado para essa aplicação é o:

a) 802.11ac; b) 802.11n; c) 802.11g; d) 802.11b; e) 802.11a.

Comentários: (a) Errado, esse padrão não trabalha na faixa de 2.4 GHz; (b) Correto; (c) Errado, esse padrão trabalha no máximo até 54 Mbps; (d) Errado, esse padrão trabalha no máximo até 11 Mbps; (e) Errado, esse padrão não trabalha na faixa de 2.4 GHz e trabalha no máximo até 54 Mbps (Letra B).

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[15] 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:

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.

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

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.

(FUMARC / PC-MG – 2022) Em relação aos tipos de redes de acordo com a arquitetura IEEE 802, as redes pessoais sem fio utilizadas por dispositivos que suportam Bluetooth são representadas pelo padrão:

a) 802.3
b) 802.11
c) 802.15
d) 802.16

_____

Comentários: percebam que saber a numeração do padrão já é o suficiente para responder algumas questões. No caso, trata-se do IEEE 802.15 (Letra C).

Uma *piconet* possui uma topologia em estrela e uma configuração ou arquitetura do tipo Mestre-Escravo[16]. 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.

(QUADRIX / CRN1 – 2014) As redes denominadas piconet estão diretamente associadas a qual destas tecnologias?

a) Infravermelho
b) Wi-Fi.
c) Bluetooth.
d) WiMAX.
e) Mesh

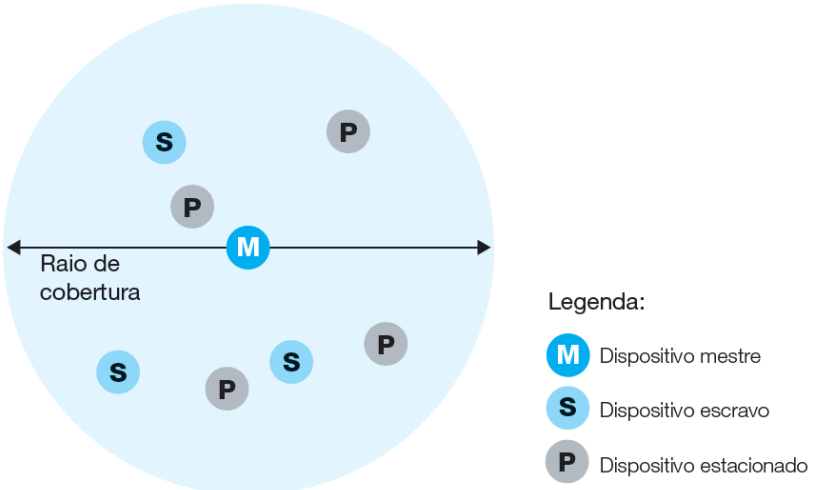
_____

Comentários: as redes denominadas piconet estão diretamente associadas à tecnologia Bluetooth – cada grupo de dispositivos conectados em uma rede Bluetooth é chamado de piconet (Letra C).

[16] 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.

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 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.



(FGV / SEPOG-RO – 2017) Assinale a opção que indica o número de dispositivos slaves (escravos) ativos que podem estar conectados a um master (mestre), simultaneamente, em uma rede piconet Bluetooth.

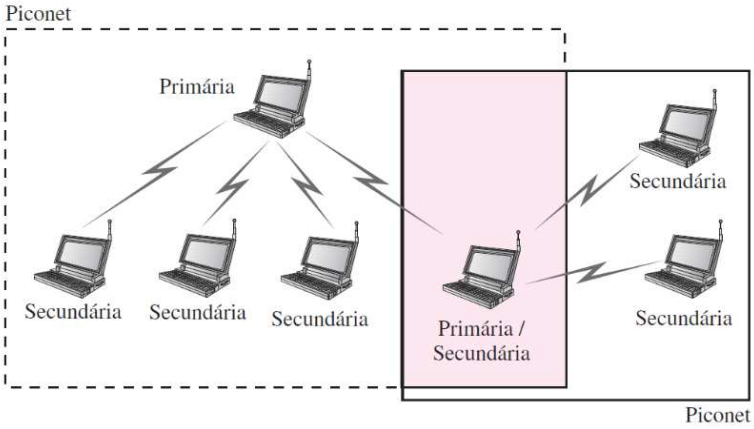
a) 7
b) 15
c) 127
d) 255
e) 1023

Comentários: o número máximo de dispositivos escravos que podem estar conectados a um dispositivo mestre em uma rede piconet Bluetooth é 7, logo um dispositivo mestre pode se comunicar com até sete dispositivos escravos ao mesmo tempo em uma rede Bluetooth (Letra A).

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

(CESPE / TRT-ES – 2013) Uma rede bluetooth possui alcance ilimitado e possibilita a conexão de componentes a um computador sem a utilização de fios.

_____

Comentários: ilimitado? Ele possui alcance bastante limitado (Errado).

(CESPE / MEC – 2015) A piconet, unidade básica de um sistema Bluetooth, consiste em um nó mestre e em escravos ativos situados próximos ao mestre. A distância máxima permitida entre um escravo e o mestre depende da potência dos seus transmissores.

_____

Comentários: uma piconet consiste em um dispositivo mestre e vários dispositivos escravos ativos que estão em comunicação próxima ao mestre. A distância máxima permitida entre um escravo e o mestre pode variar dependendo da potência dos transmissores dos dispositivos, bem como de outros fatores, como obstáculos e interferências no ambiente. Logo, a distância máxima pode ser afetada pela potência de transmissão dos dispositivos Bluetooth (Correto).

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.

(SELECON / IF-RJ – 2023) O IEEE (Institute of Eletrical and Eletronics Engineers) foi iniciado na década de 80 com o objetivo de elaborar padrões de rede, sendo responsável pela criação da arquitetura IEEE 802. A tecnologia WIMAX utiliza o padrão:

a) 802.16
b) 802.15
c) 802.11
d) 802.5
e) 802.3

_____
Comentários: a tecnologia WiMAX utiliza o padrão IEEE 802.16 (Letra A).

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).

(CESPE / TCE-PA – 2016) WiMAX é um padrão de comunicação sem fio utilizado em redes MAN.

_____
Comentários: WiMAX é realmente um padrão de comunicação sem fio de redes MAN (Correto).

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.

(IBFC / EBSERH – 2017) Assinale a alternativa correta. O padrão IEEE 802.16 estabelece redes do tipo MAN (*Metropolitan Area Network*) sem fio, ou seja, WMAN (*Wireless Metropolitan Area Network*). Um exemplo prático desse tipo de rede é:

a) ADSL
b) GSM
c) LTE
d) WiMAX
e) HSPA

_____
Comentários: o Padrão IEEE 802.16 se trata do WiMAX (Letra D).

(VUNESP / Prefeitura de Birigui-SP – 2019) Assinale a alternativa que apresenta uma tecnologia de rede sem fio de longa distância.

a) WiMAX.
b) ZigBee.
c) IEEE 802.11a.
d) IEEE 802.11g.
e) Bluetooth.

_____
Comentários: a tecnologia que apresenta uma tecnologia de rede sem fio de longa distância é o WiMAX (Letra A).

INTERNET

Conceitos Básicos

INCIDÊNCIA EM PROVA: MÉDIA

A Internet é basicamente um vasto conjunto de redes de computadores diferentes que utilizam um padrão comum de comunicação e oferece um determinado conjunto de serviços. *Hoje é muito comum o acesso à internet, mas vocês já pararam para pensar como tudo isso surgiu?* Para entendê-la melhor, vamos contar um pouquinho dessa interessante história e vamos observar como e por que ela foi desenvolvida.

Tudo começa no final da década de 1950. Estávamos no auge da Guerra Fria entre EUA e URSS. *Vocês se lembram qual era o maior medo daquela época?* Lembrem-se que a 2ª Guerra Mundial havia acabado na década anterior com a explosão de uma bomba atômica. **Dessa forma, o Departamento de Defesa dos EUA decidiu que precisava de uma rede de controle e comando capaz de sobreviver inclusive a uma futura guerra nuclear com a União Soviética.**

Nessa época, a telefonia pública já era comum na vida das pessoas e todas as comunicações militares passavam por essa rede subterrânea de cabos de telefonia, mas ela era considerada vulnerável no caso de uma guerra. *Por quê?* Porque essa rede funcionava de forma semelhante a uma arquitetura cliente/servidor – havia centrais telefônicas espalhadas por todo país. **Logo, bastava destruir algumas dessas centrais e toda comunicação telefônica seria interrompida.**

Em 1957, o mundo testemunhou um evento histórico para a humanidade: a União Soviética bateu os Estados Unidos na corrida espacial e lançou o primeiro satélite artificial do mundo – o Sputnik. O presidente americano Dwight Eisenhower ficou com muito medo de perder novas batalhas tecnológicas para o país rival e **criou uma organização única de pesquisas de defesa composta pelo Exército, Marinha e Aeronáutica chamada ARPA (Advanced Research Projects Agency).**

Na verdade, essa organização não possuía cientistas nem laboratórios – era basicamente um escritório. No entanto, ela era capaz de oferecer concessões e contratos a universidades públicas ou empresas que possuíssem ideias promissoras, uma vez que se tratava de uma agência de projetos de pesquisa avançada. **A ideia dessa organização era se manter sempre um passo à frente da União Soviética em tecnologia militar.**

Durante os primeiros anos, a agência financiou diversos projetos diferentes, mas em determinado momento seu diretor – Larry Roberts – se encantou novamente com a ideia de uma rede de controle e comando. Em 1969, algumas poucas universidades importantes concordaram em ingressar no projeto e começou a construir essa rede. **Como se tratava de uma rede financiada pela ARPA, seu nome inicial foi ARPANET.**

(MOURA MELO / Prefeitura de Cajamar-SP – 2016) A Internet surgiu nos tempos da Guerra Fria com o nome de:

a) Extranet
b) ArpaNet.
c) OnlyNet.
d) Unix.

_____

Comentários: o nome inicial era ArpaNet (Letra B).

Tudo começou bem pequeno, como um serviço de mensagens entre computadores da Universidade da Califórnia, Universidade de Stanford e a Universidade de Utah. Nas décadas seguintes, os cientistas e engenheiros adicionaram diversos outros recursos e serviços que ainda hoje compõem o que fazemos na Internet. **A primeira grande inovação da ARPANET foi a comutação por pacotes!** Vamos falar um pouco sobre comutação antes de seguir nossa história.

Antigamente havia um emprego que hoje em dia não existe mais: telefonista! *Quem aí já ouviu falar?* Pois é! Naquela época, quando alguém queria ligar para um amigo, era necessário ligar primeiro para uma central telefônica. Nesse local, havia centenas de operadoras que recebiam a sua ligação, perguntavam para quem você queria ligar, e só então conectavam você ao telefone do seu amigo[17]. **Essa comunicação funcionava por meio da comutação por circuito!**

[17] Curiosidade: em 1935 foi realizada a primeira ligação telefônica que circundava o planeta – ela demorou 3h25min apenas para tocar no destinatário.

Professor, não entendi! Vamos observar com mais atenção a imagem! Temos cinco operadoras com fones de ouvido e microfones. Na frente delas, é possível ver um painel com pequenos buracos e cabos plugados em alguns desses buracos. Em todo telefone, saía um cabo e passava por debaixo da terra por quilômetros e quilômetros até chegar a uma central telefônica. **Esses cabos que vocês estão vendo são os mesmos cabos conectados aos telefones residenciais.**

Pois bem... quando você queria telefonar para o seu amigo, você falava primeiro com a operadora por meio do cabo que saía da sua casa até a central telefônica. Ela perguntava com quem você queria falar e simplesmente plugava o cabo telefônico da sua casa ao cabo telefônico da casa do seu amigo. Pronto! **A partir desse momento vocês possuíam a reserva de um canal de comunicação dedicado e poderiam conversar sem interferências.**

É claro que se outra pessoa estivesse tentando te ligar, você não conseguiria atendê-la porque você está com o seu canal de comunicação ocupado/reservado. Pois bem... isso que nós acabamos de descrever se chama comutação por circuito. *Professor, o que significa esse termo comutação?* **No contexto de telecomunicações, é o processo de interligar dois ou mais pontos. No caso da telefonia, as centrais telefônicas comutam ou interligam terminais.**

Observem que a comutação por circuito estabelece um caminho fim a fim dedicado, reservando um canal de comunicação temporariamente, para que dados de voz sejam transmitidos. Nesse caso, a informação de voz sempre percorre a mesma rota e sempre chega na mesma ordem. **O processo de comutação por circuito possui uma fase de estabelecimento da conexão, uma fase de transferência de dados e uma fase de encerramento da conexão.**

Galera, eu vou contar uma coisa surpreendente para vocês agora! *Vocês acreditam que ainda hoje a telefonia funciona por meio da comutação de circuitos?* **Pois... é claro que não precisamos mais de operadores porque os circuitos são capazes de se mover automaticamente em vez de manualmente.** Legal, mas a comutação por circuito é completamente inviável na internet. *Por quê, Diegão?* Cara, vamos lá...

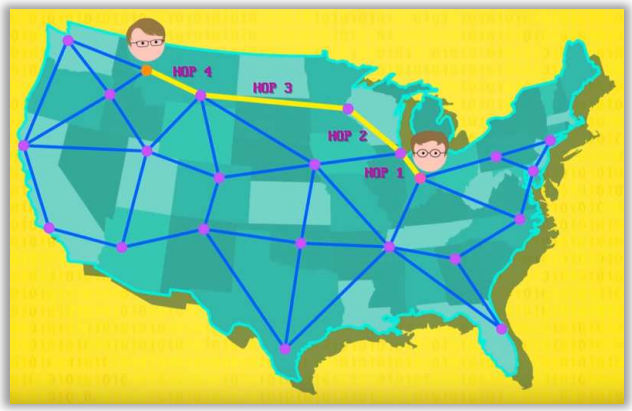
O principal problema é o desperdício de recursos! **Poxa... quando um dispositivo de origem estabelece uma conexão com um dispositivo de destino, fecha-se uma conexão e ambas as linhas permanecem dedicadas mesmo que não esteja havendo comunicação.** Imaginem que eu estou falando com um amigo no telefone, mas estou apertado para ir ao banheiro! Se eu passar meia hora no banheiro, a linha continuará reservada mesmo sem eu estar utilizando.

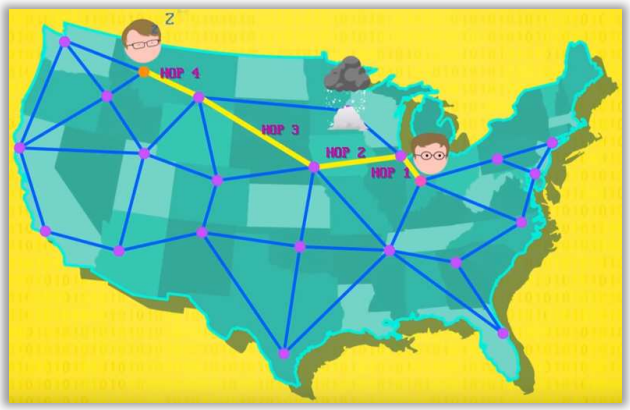
Além disso, a comutação por circuito só permite que eu telefone para uma única pessoa simultaneamente – eu não consigo conversar com dois amigos simultaneamente. *Já imaginaram se a internet funcionasse assim?* Nesse caso, seu computador só poderia se conectar a um único dispositivo ao mesmo tempo. **Seria impossível acessar dois sites simultaneamente – você teria que fechar um site para poder acessar outro.**

Além disso, o tráfego na internet é muito inconstante. Por exemplo: você começa a estudar uma aula de informática em nosso site, depois você sai para comer, depois você volta e entra em um site para ouvir uma música relaxante. *Vocês percebem que o perfil de utilização é totalmente diferente?* **Se utilizássemos a comutação por circuito na internet, você sairia para comer e deixaria a linha reservada mesmo sem a estar utilizando, desperdiçando recursos.**

Algumas vezes, por questão de segurança ou por questão de relevância, é necessário manter uma linha exclusiva e dedicada. Por essa razão, forças armadas, bancos e outras organizações que possuem processos de alta criticidade mantêm linhas ou circuitos dedicados para conectar seus centros de dados como mostra a imagem anterior. **Voltando à história: a ARPANET trouxe um novo paradigma chamado Comutação por Pacotes.** *Como funcionava?*

Vamos fazer uma analogia com uma empresa de entrega. Vamos supor que se John deseja enviar uma carta para David. **Em vez de ter uma estrada dedicada entre a cidade de John e a cidade de David, eles poderiam utilizar as diferentes rotas possíveis entre as duas cidades.** Exemplo: um caminhão poderia pegar a carta e transportá-la apenas de Indianapolis para *Chicago*. Ao chegar nessa cidade, ela poderia ir consultar a melhor rota e levaria de *Chicago* para *Minneapolis*.





Em seguida, a rota seria de *Minneapolis* para *Billings;* e finalmente de *Billings* até *Missoula* – como mostra a imagem à esquerda. Ao parar em cada cidade, o motorista do caminhão poderia perguntar na estação de correio da cidade qual era a melhor rota até chegar ao destino final. **A parte mais interessante dessa abordagem é que ela pode utilizar rotas diferentes, tornando a comunicação mais confiável e tolerante a falhas**.

Como assim, professor? Imaginem que haja uma tempestade de neve na cidade de *Minneapolis* que congestionou absolutamente todas as vias. Não tem problema – o motorista do caminhão poderia utilizar outra rota passando por *Omaha* – como mostra a imagem acima à direita. **Voltando para o mundo das redes de computadores, não há necessidade de uma conexão estabelecer previamente uma rota dedicada para a transmissão de dados.**

Na comutação por pacotes, há uma malha de nós conectados ponto-a-ponto em que cada nó verifica a rota de menor custo para entrega da informação. *Como assim, Diego?* O caminho de menor custo é o caminho mais rápido entre dois pontos. Nas imagens anteriores, nós temos dois caminhos entre dois pontos. O primeiro é até mais curto, mas está congestionado – logo, o segundo caminho tem menor custo porque é o caminho mais rápido entre dois pontos.

Quem aí já usou o Waze? Por vezes, você já sabe o caminho entre seu trabalho e sua casa e você sabe que ele é o caminho mais curto. No entanto, ainda assim é interessante utilizar o Waze. *Por quê?* Porque se houver um acidente no percurso, o caminho mais curto em distância pode ser mais lento em tempo do que eventualmente um caminho mais longo em distância. **O software sugerirá um caminho mais distante, mas que você chegará mais rápido.**

Agora tem outro ponto interessante sobre esse tipo de comutação! Por vezes, os dados transmitidos são grandes demais ao ponto de eventualmente obstruir uma rede completamente (Ex: envio de um arquivo de 100Mb). **A comutação por pacotes trouxe uma ideia genial: dividir as informações em pequenos pedaços chamados de pacotes.** Logo, em vez de enviar o arquivo integral, você o divide em milhares de pacotinhos. *O que tem de genial nisso, professor?*

Galera... se eu fragmento ou segmento uma informação em milhares de pacotes, eu posso enviá-los separadamente de modo que cada um possa percorrer uma rota totalmente diferente. *Professor, está muito complexo!* Vamos voltar ao exemplo dos correios: imagine que eu preciso enviar um relatório de 100 páginas para outro estado, mas que os correios só permitam o envio de 10 páginas por envelope.

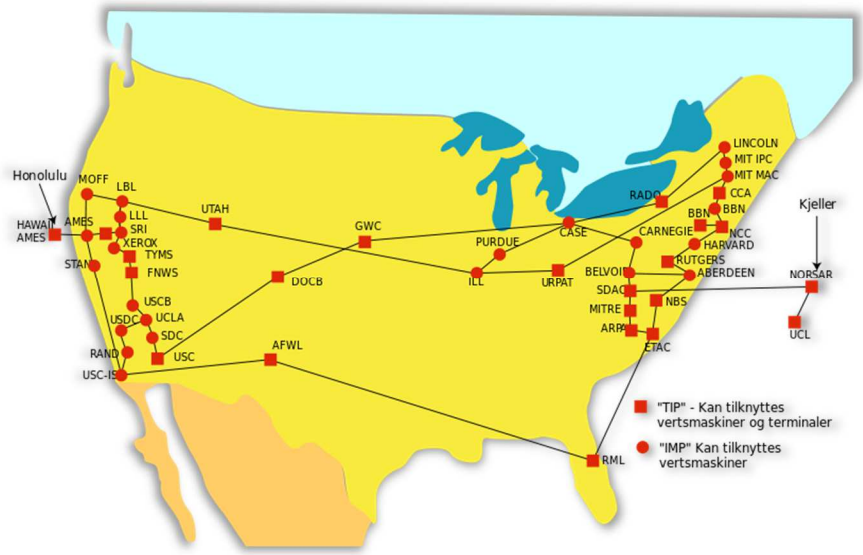
Não tem problema! **Eu posso dividir meu relatório em dez pacotes de dez páginas e fazer dez envios diferentes.** Como os correios vão entregar os pacotes separadamente, cada pacote pode percorrer uma rota até o destino final. E digo mais: pode ser que as dez primeiras páginas cheguem por último e as últimas dez páginas cheguem primeiro. Cara... acontece quase igualzinho no contexto de internet.

Quando se envia dados pela internet, não é possível prever o caminho percorrido pelo pacote até chegar ao seu destino final. Cada pacote enviado pode seguir por uma rota diferente chegando em ordem diferente da ordem enviada (claro que, após todos os pacotes chegarem, o arquivo é remontado na forma original). Pessoal, deixa eu contar uma coisa para vocês: nós só temos internet hoje em dia por conta dessa ideia genial...

A comutação por pacotes permite aproveitar melhor os canais de transmissão de dados de modo que sua utilização seja compartilhada pelos usuários da forma mais eficiente e tolerante a falhas possível. Ela utiliza um tipo de transmissão **store-and-forward**, em que o pacote recebido é armazenado por um equipamento e encaminhado ao próximo destino. Em cada equipamento, o pacote recebido tem um endereço de destino, que possibilita indicar o caminho final.

Pessoal... os engenheiros testaram a comutação por pacotes e foi um sucesso, mas – com o passar dos anos – a quantidade de novos computadores e dispositivos conectados à rede começou a aumentar e surgiu um problema. Nós vimos que o equipamento que recebe e armazena o pacote era responsável por encaminhá-lo ao próximo destino. No entanto, isso implicava que todo computador deveria manter uma lista **atualizada** do endereço de outros computadores da rede.

E se a lista não estivesse atualizada? **Esse equipamento não saberia para onde enviar ou enviaria o pacote para um local que não existia mais, entre outras possibilidades.** Com o aumento da quantidade de computadores na rede, era cada vez mais comum que computadores mudassem seu endereço e a atualização para os outros computadores da rede não era tão rápida. *Como eles resolveram esse problema, Diego?* Os caras eram sinistros...



Mapa da Arpanet em 1974

Em 1973, eles decidiram abolir esse sistema em que cada dispositivo possuía uma lista de endereços dos outros e escolheram a Universidade de Stanford como uma espécie de registro central oficial de endereços. Em 1978, já havia mais de cem computadores conectados à Arpanet por todo Estados

Unidos e até Inglaterra. **Nos anos seguintes, começaram a surgir redes semelhantes à Arpanet em diferentes lugares do mundo com mais computadores.**

Legal, professor! É legal, mas originou alguns problemas. Cada rede criada formatava seus pacotes de maneira diferente, então – apesar de ser possível conectar redes diferentes – isso causava uma dor de cabeça. **Para resolver esse problema, a solução foi utilizar um conjunto de protocolos comuns de comunicação chamado TCP/IP.** *O que é um protocolo, professor?* Basicamente é uma convenção que controla e possibilita conexões, comunicações e transferências de dados.

Professor, você pode explicar de outra forma? **Claro, vamos fazer uma analogia!** Se eu comprar um notebook e ele vier com uma tomada de cinco pinos, eu não conseguirei utilizá-lo. Se ele funcionar em 110v, eu não conseguirei utilizá-lo em Brasília. Se eu comprar um mouse sem fio para utilizar com o notebook, mas eles operarem em faixas de frequência diferentes, eu também não conseguirei utilizá-los.

No primeiro caso, eu ainda posso comprar um adaptador; no segundo caso, eu ainda posso comprar um transformador; mas no terceiro caso, não há nada a se fazer. *O que vocês podem concluir de tudo isso?* É possível concluir que se os fabricantes de equipamentos não conversarem entre si, haverá sérios problemas de comunicação de dados. **Por essa razão, foram criados protocolos comuns de comunicação, sendo o conjunto mais utilizado chamado de TCP/IP.**

Quando duas ou mais redes se conectam utilizando a pilha de protocolos TCP/IP, fica bem mais fácil conectá-las. O conjunto de redes de computadores que utilizam esses protocolos e que consiste em milhões de empresas privadas, públicas, acadêmicas e de governo, com alcance local ou global e que está ligada a uma grande variedade de tecnologias de rede é também conhecida popularmente como...

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).

(CONSULPAM / Câmara de Juiz de Fora-MG – 2018) A possibilidade de redigir, enviar e receber mensagens de correio eletrônico é uma realidade criada já na fase inicial da ARPANET (precursora da Internet) e é imensamente popular.

_____

Comentários: é um serviço anterior à Internet e que já surgiu na fase inicial da ArpaNet (Correto).

(ESAF / Ministério da Integração – 2012) Os serviços de Internet mais populares e difundidos são:

a) Wide Worring Web, correio eletrônico, sequenciamento de arquivos, login remoto e desktop remoto.

b) World Wide Web, correio eletrônico, transferência de arquivos, login remoto e desktop remoto.

c) World Wide Web, comutação de servidores, transferência de arquivos, login remoto e debugging remoto.

d) World Wide Wedge, correio eletrônico, transferência de endereços, controle remoto e desktop local.

e) Wood Wide Weed, controle eletrônico, transferência de arquivos, login remoto e backup remoto.

_____

Comentários: os serviços mais comuns são World Wide Web, Correio Eletrônico, Transferência de Arquivos, Login Remoto e Desktop Remoto (Letra B).

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. Vejamos alguns exemplos:

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**.

COMPONENTES 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.

(COTEC / Prefeitura de São Francisco-MG – 2020) Os termos internet e World Wide Web (WWW) são frequentemente usados como sinônimos na linguagem corrente, e não são porque:

a) a internet é uma coleção de documentos interligados (páginas web) e outros recursos, enquanto a WWW é um serviço de acesso a um computador.

b) a internet é um conjunto de serviços que permitem a conexão de vários computadores, enquanto WWW é um serviço especial de acesso ao Google.

c) a internet é uma rede mundial de computadores especial, enquanto a WWW é apenas um dos muitos serviços que funcionam dentro da internet.

d) a internet possibilita uma comunicação entre vários computadores, enquanto a WWW, o acesso a um endereço eletrônico.

e) a internet é uma coleção de endereços eletrônicos, enquanto a WWW é uma rede mundial de computadores com acesso especial ao Google.

Comentários: a internet é a infraestrutura de rede global que conecta computadores em todo o mundo, enquanto a World Wide Web (WWW) é um serviço específico dentro da internet que permite o acesso a documentos interligados (páginas web) e outros recursos por meio de navegadores da web. A WWW é apenas uma parte dos muitos serviços e recursos disponíveis na internet (Letra C).

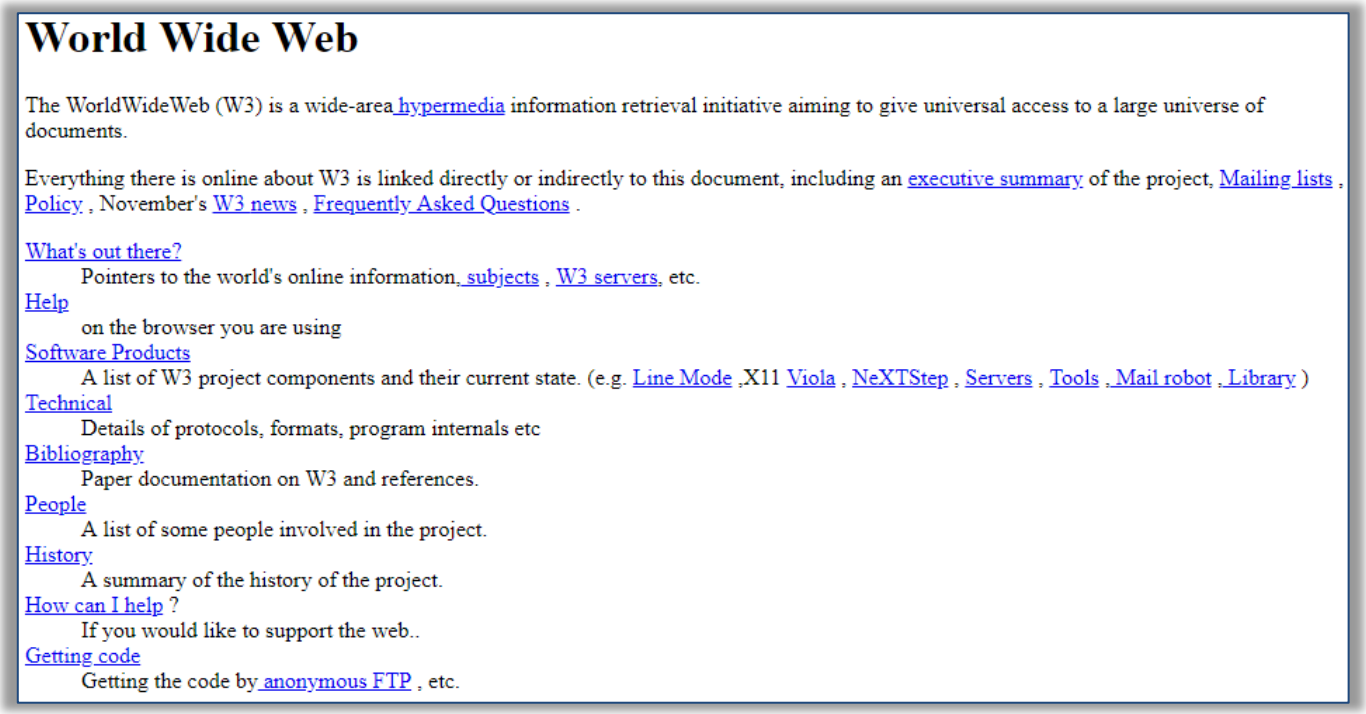
Agora vamos falar um pouco sobre as gerações da web (note que elas não se excluem, elas se sobrepõem). Vamos vê-las em detalhes...

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**!



World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.
Help
on the browser you are using
Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)
Technical
Details of protocols, formats, program internals etc
Bibliography
Paper documentation on W3 and references.
People
A list of some people involved in the project.
History
A summary of the history of the project.
How can I help ?
If you would like to support the web..
Getting code
Getting the code by anonymous FTP , etc.

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.

Imagine a Web 1.0 como uma grande biblioteca virtual. Nessa biblioteca, você pode encontrar uma enorme quantidade de livros e revistas, mas eles são todos impressos e não podem ser alterados. Você pode navegar pelos corredores, pegar um livro e lê-lo, mas não pode escrever ou adicionar suas próprias anotações nos livros. A biblioteca é um recurso de leitura valioso, mas é estática, sem interatividade.

Nesse cenário, as empresas e instituições são como os curadores da biblioteca, selecionando e disponibilizando informações para os visitantes. Os visitantes podem encontrar informações úteis, mas não têm a capacidade de contribuir com seu próprio conteúdo ou interagir com outros visitantes. **A Web 1.0 é semelhante a essa biblioteca digital, onde o conteúdo é fornecido para leitura, mas não há recursos avançados de interatividade, colaboração ou personalização.**

(QUADRIX / SEDF – 2022) A Web 1.0 foi a primeira fase de desenvolvimento da Web, na qual o volume de usuários com acesso à rede era alto.

_____

Comentários: a Web 1.0, na verdade, foi a primeira geração da World Wide Web, caracterizada pelo acesso predominantemente de leitura. Nessa fase, os usuários podiam acessar informações estáticas na forma de páginas da web, mas não tinham as mesmas capacidades de interação e contribuição que as gerações subsequentes, como a Web 2.0. Logo, a Web 1.0 não se destacou pelo alto volume de usuários com acesso à rede, mas sim pela limitação da interatividade e da contribuição dos usuários (Errado).

(QUADRIX / CREF3 – 2023) A web 1.0 é a terceira fase da web, que está sendo vivenciada hoje: ela é marcada pelo uso da inteligência artificial, para que os computadores executem, de forma automática, funções que antes seriam executadas pelo usuário.

_____

Comentários: a descrição apresentada na afirmação não corresponde à Web 1.0. A Web 1.0 é, na verdade, a primeira fase da web, que se estendeu até meados dos anos 2000. Nessa fase, a web era caracterizada principalmente pela apresentação de informações estáticas e não interativas. Não havia um uso generalizado de inteligência artificial para automação de funções. A afirmação se assemelha mais à descrição da Web 3.0, que se refere à web semântica e à automação inteligente de tarefas por meio de máquinas e algoritmos (Errado).

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.

Imagine a Web 2.0 como uma biblioteca em que você não apenas lê os livros, mas pode adicionar seus próprios capítulos, comentários e até mesmo escrever seus próprios livros. Além disso, você pode se conectar com outros leitores, discutir ideias, fazer recomendações e criar novas histórias juntos. É como se a biblioteca se transformasse em um espaço de colaboração ativa, onde todos são autores e leitores ao mesmo tempo.

Da mesma forma, a Web 2.0 permitiu que os usuários não apenas consumissem informações, mas também as criassem, compartilhassem e colaborassem em um ambiente online, tornando a internet mais interativa e participativa. **É uma mudança de uma web estática e informativa para uma web dinâmica e social, onde os usuários desempenham um papel ativo na criação e compartilhamento de conteúdo.**

(CONSULPLAN / TJM-MG – 2021) Alguns recursos das mídias sociais estão inovando os processos de comunicação organizacional de empresas e instituições. Quais características fazem parte dos critérios de identificação do ambiente da WEB 2.0?

a) Compartilhamento de imagens.
b) Predomínio do emissor sobre o controle do conteúdo.
c) Compartilhamento de conteúdo, opiniões, ideias e mídias, possibilitando conversações
d) Baixa capacidade de personalização do conteúdo e baixa intervenção do usuário ou receptor no conteúdo da comunicação.

_____

Comentários: (a) Errado, essa é uma característica da Web 2.0, mas não é a característica que a identifica; (b) Errado, há uma democratização do conteúdo, permitindo que os usuários tenham mais controle e influência sobre o conteúdo compartilhado, ao contrário do predomínio exclusivo do emissor; (c) Correto, a Web 2.0 é marcada pelo compartilhamento de conteúdo, pela interatividade e pela participação ativa dos usuários, que podem compartilhar suas opiniões, ideias e mídias, bem como engajar-se em conversas e colaboração online; (d) Errado, a Web 2.0 é caracterizada por uma maior capacidade de personalização e interação dos usuários com o conteúdo, o que a torna uma descrição inadequada desse ambiente (Letra C).

(QUADRIX / CRT4 – 2022) Os princípios da Web 2.0 desmotivam o público a participar da construção e da customização de serviços e mensagens.

_____

Comentários: os princípios da Web 2.0, na verdade, têm o efeito oposto: eles incentivam ativamente o público a participar da construção e da customização de serviços e mensagens. A Web 2.0 é caracterizada pela colaboração, interatividade e

participação dos usuários na criação e compartilhamento de conteúdo online, o que a torna uma abordagem muito mais aberta e envolvente em comparação com a Web 1.0 (Errado).

(FUNCERN / Câmara de Natal-RN – 2023) É um conjunto de arquiteturas e ferramentas, na Internet, que permite gerar uma inteligência coletiva, baseando-se no conteúdo produzido pelos próprios usuários. Essa descrição conceitua:

a) WIKI
b) TAGS
c) WEB 2.0
d) WEB 1.0

_____

Comentários: a Web 2.0 é caracterizada por permitir a geração de conteúdo por parte dos próprios usuários, bem como a colaboração, compartilhamento e interatividade online, contribuindo para a formação de uma inteligência coletiva na Internet. As outras opções, como WIKI e TAGS, são elementos e tecnologias associados à Web 2.0, mas não representam a descrição geral da Web 2.0 (Letra C).

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.

Agora, a biblioteca é inteligente o suficiente para entender o conteúdo de cada livro. Ela sabe o enredo, os personagens, as informações-chave e como os livros se relacionam uns com os outros. Quando você faz uma pergunta ao bibliotecário, ele não apenas recomenda os livros certos, mas também pode dizer coisas como "*Há um livro que menciona isso que você está procurando na seção de história, mas também pode estar relacionado à política na seção de não ficção*".

A biblioteca está interconectada e usa inteligência artificial para fornecer informações significativas instantaneamente. Então, na analogia, a Web 1.0 é como uma biblioteca sem catálogo, a Web 2.0 é como uma biblioteca com etiquetas e um bibliotecário eficiente, e a Web 3.0 é como uma biblioteca ultra-inteligente que compreende o conteúdo de todos os livros e fornece respostas detalhadas com base em seu conhecimento profundo.

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

(CEPUERJ / UERJ – 2022) A Web 3.0 é identificada como web:

a) pragmática
b) semântica
c) semiótica

d) ubíqua

_____

Comentários: a Web 3.0 é conhecida como Web Semântica, dado que – nessa fase – os sistemas de computação têm a capacidade de entender o significado dos dados e relacioná-los de maneira mais eficaz (Letra B).

(QUADRIX / SEDF – 2022) A Web 3.0, alcunhada como Web semântica por Tim Berners-Lee, aumenta a capacidade de busca e autorreconhecimento dos conteúdos por meio de metadados.

_____

Comentários: a Web 3.0 de fato envolve o uso de metadados para aumentar a capacidade de busca e autorreconhecimento dos conteúdos na internet. Metadados são informações que descrevem outros dados, ajudando a máquina a entender o contexto e o significado dos dados, o que, por sua vez, melhora a precisão da busca e a interpretação das informações na web. Tim Berners-Lee é um dos pioneiros na promoção da web semântica e do uso de metadados para tornar a internet mais inteligente e significativa (Correto).

Deep Web e Dark Web

INCIDÊNCIA EM PROVA: MÉDIA

Galera, vamos falar agora sobre um assunto que interessa grande parte dos alunos! *Qual seria a sua reação se eu te dissesse que tudo que você conhece sobre a web é, na verdade, apenas 4% da realidade?* Sim, todos os sites que você já visitou, todos os vídeos que você já assistiu, todas as músicas que você já ouviu, todos os textos que você já leu, todas as notícias que você já leu, todo material do Estratégia, Google, Wikipedia, etc... **tudo isso corresponde somente a cerca de 4% da web!**

Nós podemos dizer que a parte da web que pode ser indexada por **Ferramentas de Busca** (Ex: Google, Bing, etc) de modo que seja visível e acessível diretamente por navegadores comuns **sem a necessidade de autenticação** (Ex: Login e Senha) é chamada de **Surface Web (Superfície da Web ou Web Navegável).** Você só encontra a página do Estratégia no Google porque ele possui rastreadores que ficam circulando pela web procurando páginas e inserindo-as em um índice.

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.

Logo, tudo que ele consegue indexar (isto é, inserir em seu índice de pesquisa) são as páginas da web navegável. *E onde é que estão os outros 96%?* **Estão na Deep Web (Web Profunda)!** Lá está a parte da web que está protegida por mecanismos de autenticação ou que não pode ser acessada por meio de links tradicionais ou ferramentas de buscas, tais como seus e-mails ou sua conta no Internet Banking. *Uma página aberta no Facebook?* Surface Web! *Um grupo fechado?* Deep Web!

(UECE-CEV / DETRAN-CE – 2018) A zona obscura na Internet, inacessível através dos mecanismos mais populares de busca como o Google e o Bing é denominada:

a) Gray web.
b) Deep web.
c) Surface Web.
d) Navegação anônima.

_____

Comentários: (a) Errado, esse termo sequer existe; (b) Errado, a zona obscura fica na Dark Web; (c) Errado, essa é a web navegável e acessível aos mecanismos de buscas; (d) Errado, a navegação anônima apenas impede que o browser salve alguns dados de navegação. A questão foi anulada sob a seguinte justificativa:

"A questão pergunta como se denomina a zona obscura da Internet, inacessível ao Google e aos demais motores de busca. A resposta dada como correta no gabarito é "Deep Web". Os requerentes alegam que a zona obscura da grande rede é conhecida como "Dark Web" e não "Deep Web". De fato, nem todos os sites têm suas informações acessíveis ao Google. Dados como extrato bancário, conteúdo de e-mails, histórico escolar etc não são normalmente indexados pelos motores de busca tradicionais, formando a assim chamada "Deep Web". Já a zona obscura da Internet, onde dizem estar o submundo da rede, e que normalmente só é acessível por meio de ferramentas especiais de anonimato como o navegador Tor, é realmente conhecida como "Dark Web" (Anulada).

A Deep Web é invisível para todos aqueles que não tenham autorização para acessá-la. *Como assim, professor?* Vamos imaginar a Intranet do Senado Federal! *Você consegue acessá-la?* Em princípio, não – a não ser que você seja um servidor desse órgão! Dessa forma, podemos afirmar que a Intranet do Senado Federal está na Deep Web (apesar de esse ser um assunto bem polêmico)! **Agora faz sentido para você que a maioria dos dados estejam na Deep Web e, não, na Surface Web...**

No entanto, estar na Deep Web não é nenhuma garantia inquebrável de privacidade. Toda vez que acessamos uma página por meio de um navegador comum, nosso computador se comunica com o servidor que armazena a página que desejamos acessar. Essa conexão entre computador e servidor percorre uma rota que passa por diversos intermediários ao redor do planeta, deixando rastros quem podem ser utilizados para descobrir quem está acessando e o que está acessando.

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.

Vocês se lembram quando um juiz tentou bloquear o acesso ao Whatsapp por 72 horas? Pois é, seu intuito era obrigar a empresa a quebrar o sigilo das mensagens trocadas por criminosos. *E qual é o problema de bloquear um serviço, professor?* **O problema é que – se é possível fazer isso por motivos legítimos – também é possível por motivos ilegítimos.** A China, por exemplo, proíbe seus cidadãos de acessarem o Google, Facebook, Youtube, Twitter, etc.


MENU G1 TECNOLOGIA E GAMES

19/07/2016 11h28 - Atualizado em 19/07/2016 17h08

WhatsApp: Justiça do RJ manda bloquear aplicativo em todo o Brasil

Facebook recusou ceder informações para uma investigação policial. Operadoras de telefonia foram notificadas para suspender acesso ao app.

Do G1, em São Paulo e no Rio

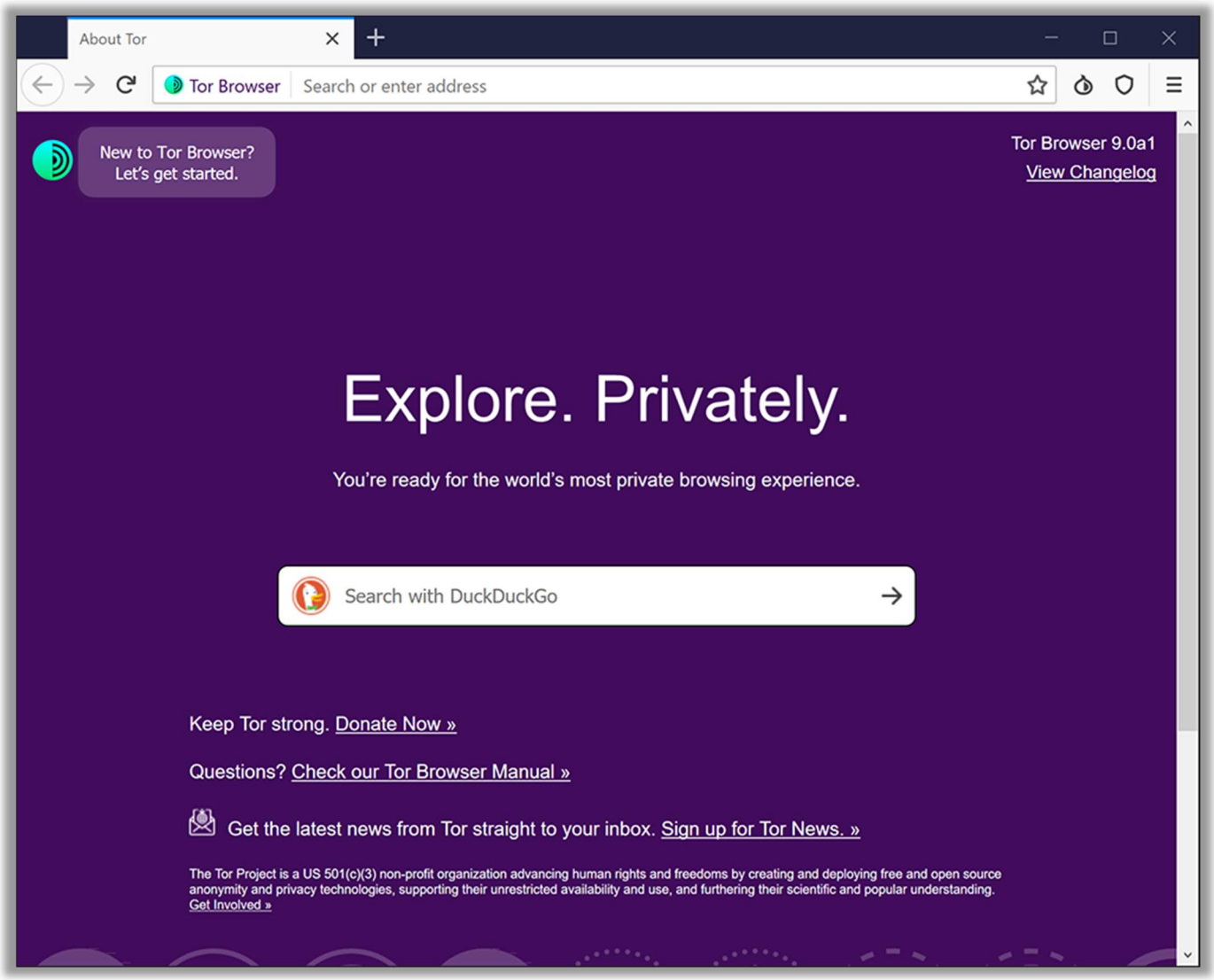
FACEBOOK

Essa falta de privacidade pode ser um problema gravíssimo para cidadãos que vivem em países com censura, jornalistas, informantes, ativistas e até usuários comuns. Caso essas pessoas façam alguma crítica ao governo na Surface Web, elas podem eventualmente ser rastreadas e perseguidas por agentes governamentais. **Logo, os recursos da Deep Web permitem que ela possa manter sua privacidade e ter sua identidade preservada.** *E o que elas podem fazer?*

Bem, uma alternativa é utilizar a Dark Web! Trata-se de uma parte da Deep Web que não é indexada por mecanismos de busca e nem possuem um endereço comum[18], logo é basicamente invisível e praticamente impossível de ser rastreada. **Para acessá-la, é necessário se conectar a uma rede específica – a mais famosa se chama Tor.** Essa rede foi inicialmente um projeto militar americano para se comunicar sem que outras nações pudessem descobrir informações confidenciais.

Eita, professor... deixa eu acessar rapidinho aqui essa tal de Rede Tor! Nope, você não conseguirá! A Dark Web não é acessível por meio de navegadores comuns, tais como Chrome, Firefox, entre outros (exceto com configurações específicas de proxy). Para acessar a Rede Tor, é necessário utilizar um navegador específico – **também chamado de Tor** – que permite acessar qualquer página da Surface Web, Deep Web ou Dark Web (aliás, é assim que chineses conseguem acessar o Google).

[18] Na Dark Web, as páginas não usam os domínios tradicionais como .com, .org, .net, ou domínios nacionais como .br (para o Brasil). Em vez disso, muitos sites da Dark Web usam o domínio .onion (Exemplo: *http://3g2upl4pq6kufc4m.onion* ou *http://msydqstlz2kzerdg.onion*).



(CESPE / ABIN – 2018) O uso de domínios web de final .on e de roteadores em formato de proxy são características da dark web.

_____

Comentários: na verdade, o domínio característico da Dark Web termina com **.onion** e, não, **.on** (Errado).

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**[19]. 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.

DARK WEB	DESCRIÇÃO

[19] 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.

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.

(CESPE / ABIN – 2018) O aplicativo TOR permite o acesso a sítios na deep web, isto é, sítios que não possuem conteúdo disponibilizado em mecanismos de busca.

_____

Comentários: vamos analisar por partes. *O aplicativo Tor permite o acesso a sítios na Deep Web?* Sim, ele permite o acesso a sítios da Surface Web, Deep Web e Dark Web. *Sítios da Deep Web não possuem conteúdo disponibilizado em mecanismos de busca?* Perfeito, eles não podem ser indexados por mecanismos de busca! (Correto).

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 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.

(COPEVE / UFAL – 2016) A Web Profunda (do inglês, Deep Web) permite que usuários naveguem em sites e acessem conteúdos de forma anônima. A Deep Web é organizada através de redes totalmente independentes entre si, tais como Onion (TOR), I2P, Freenet, Loky, Clos, Osiris etc. Nesse contexto, dadas as seguintes afirmativas,

I. Tor é um browser web que permite navegar na rede TOR.

II. Para navegar na rede TOR, pode-se utilizar quaisquer browsers web, tais como Firefox e Chrome, configurando propriedades de proxy.

III. Existe a possibilidade de trafegar dados na rede TOR de forma criptografada.

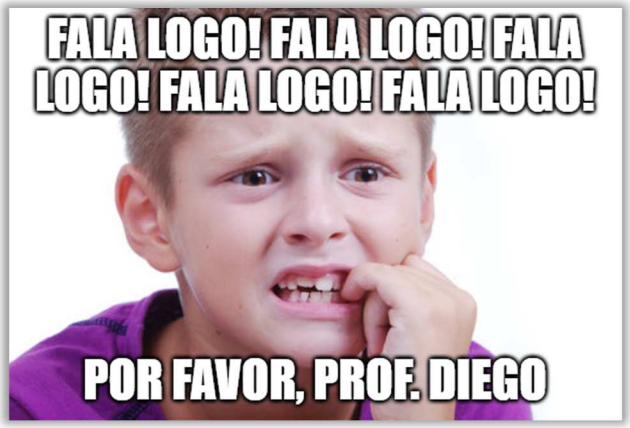
Verifica-se que está(ão) correta(s):

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

_____

Comentários: (I) Correto, ele permite navegar na Rede Tor; (II) Correto, é possível navegar na Rede Tor por meio de navegadores comuns, no entanto é necessário fazer diversas configurações de proxy – isso é exceção, não deveria ser cobrado em prova. Para mim, o item está incorreto; (III) Correto, essa rede funciona de forma criptografada e anônima – o gabarito definitivo mudou para Letra D, mas eu não vejo nada errado no Item I, portanto discordo veementemente dessa questão (Letra D).

Professor, você disse que as pessoas acessam a Dark Web por motivos legítimos e ilegítimos. Eu estou agoniado, desembucha logo e fala o que é que tem de ilegítimo lá!



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.

(CESPE / TJDFT – 2015) Deep Web é o conjunto de conteúdos da Internet não acessível diretamente por sítios de busca, o que inclui, por exemplo, documentos hospedados em sítios que exigem login e senha. A origem e a proposta original da Deep Web são legítimas, afinal nem todo material deve ser acessado por qualquer usuário. O problema é que, longe da vigilância pública, essa enorme área secreta foi tomada pelo desregramento, e está repleta de atividades ilegais.

_____

Comentários: Deep Web é, de fato, composta por conteúdos não acessíveis diretamente por motores de busca, e isso inclui documentos que requerem login e senha, bem como dados que não são públicos ou não estão indexados nos mecanismos de busca convencionais. No entanto, afirmar que a Deep Web está repleta de atividades ilegais é uma generalização imprecisa. Embora a Deep Web seja usada por pessoas em busca de privacidade, não se pode concluir que todas as atividades lá sejam ilegais. Há uma variedade de conteúdos legítimos e privados na Deep Web, como informações de empresas, intranets corporativas, bancos de dados acadêmicos e muito mais.

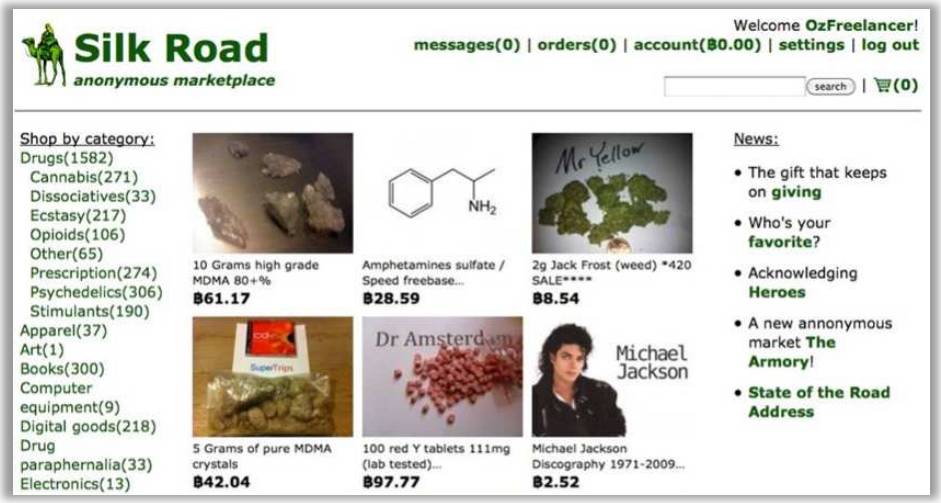
A parte mais obscura da Internet é a Dark Web, onde atividades ilegais podem ocorrer, mas essa é apenas uma pequena fração da Deep Web como um todo. Logo, em minha visão, a questão caberia recurso (Correto).

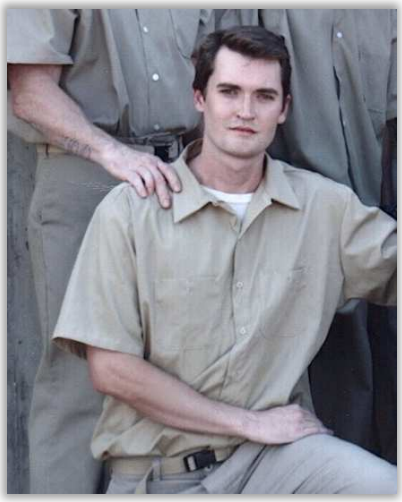
Eu sei que essa aula atiça a curiosidade de várias pessoas, mas eu já adianto que não recomendo que vocês acessem esses sites. Saibam que se trata de um ambiente em que é possível encontrar um bocado de hackers, cibercriminosos e outros profissionais desse tipo. Eu já recebi perguntas de alunos perguntando 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.**





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

Comentários: (a) Errado. Sites da Dark Web (e, não, da deepweb) podem utilizar o domínio .onion, que é um domínio de nível superior específico para sites acessíveis na rede Tor. Isso geralmente é usado para sites que desejam ocultar seu local e operar anonimamente; (b) Errado. A Deep Web refere-se a conteúdos que não são indexados pelos mecanismos de busca convencionais, mas ainda podem ser acessados com navegadores comuns. A Dark Web é uma parte obscura da Deep Web que é intencionalmente oculta e acessada por meio de redes criptografadas, como o Tor; (c) Errado. O Silk Road era um mercado ilegal online que operava na Dark Web – que é uma parte da Deep Web, logo caberia recurso; (d) Errado. Existem navegadores, como o Tor Browser, que são projetados para acessar a Dark Web. Esses navegadores usam redes criptografadas para permitir o acesso a sites na Dark Web; (e) Correto. Os sites na Dark Web não são indexados por navegadores convencionais, como o Google Chrome ou o Firefox. Eles são acessados por meio de navegadores especializados, como o Tor Browser, que roteiam o tráfego por redes criptografadas para ocultar a identidade do usuário (Letra E).

Um outro caso que vocês devem estar familiarizados é o Massacre de Suzano. Em 2019, dois ex-alunos de uma escola entraram armados nessa escola, mataram cinco estudantes e duas funcionárias – depois um dos atiradores matou o comparsa e, em seguida, cometeu suicídio. Os dois atiradores organizaram o crime em um fórum da Dark Web chamado Dogolochan – eles foram incitados por outros usuários e entraram na "Galeria de Ídolos" do fórum com outros criminosos.

Fóruns na dark web incitam violência e mortes e desafiam polícia

Massacre em Suzano foi comemorado em comunidades virtuais de criminosos

Luiz tinha 25 anos e era conhecido no fórum como "luhkrcher666"; Guilherme tinha 17 anos e era conhecido no fórum como "1guY-55chaN". Bem, esse é um assunto ainda bastante incipiente em concurso público, mas que deve ganhar importância nos próximos anos. Quem estiver curioso e quiser descobrir mais detalhes sobre esse assunto, recomendo dois documentários: **Dark Web (2015)** e **Don't F**k With Cats (2019)** – esse segundo está na Netflix :)

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.

- **Surface Web (Web Superficial):** imagine a Internet como um iceberg (como o apresentado na imagem no início do tópico) no meio do oceano. A parte que você vê exposta acima da água é a Surface Web, que representa aquelas páginas acessíveis por mecanismos de busca convencionais, como o Google, Bing ou Yahoo. Essas páginas são públicas e facilmente encontradas, assim como a parte visível de um iceberg que está acima da água.

- **Deep Web (Web Profunda):** abaixo da superfície da água, onde o iceberg se estende, está a Deep Web. Nessa área, estão os conteúdos que não são indexados pelos motores de busca comuns, como páginas de bancos de dados, e-mails privados, áreas de login e muito mais. Você pode pensar na Deep Web como a parte do iceberg que está submersa, não visível à primeira vista, mas ainda acessível com as ferramentas certas, como senhas ou autorizações.

- **Dark Web (Web Escura):** agora, vá mais fundo nas águas escuras e misteriosas, onde a luz do sol não alcança. Lá você encontrará a Dark Web. Esta é a parte mais obscura e oculta da Internet, acessível por meio de redes criptografadas, como o Tor. A Dark Web é como a parte do iceberg que está profundamente submersa, invisível e intencionalmente oculta. É onde você pode encontrar sites que não querem ser rastreados e, às vezes, atividades ilegais.

(IESES / IGP-SC – 2017) Analise as seguintes definições e assinale a INCORRETA:

a) A Dark Web é uma parte não indexada e restrita da Deep Web e é normalmente utilizada para comércio ilegal e pornografia infantil.

b) A computação em nuvem refere-se a um modelo de computação que fornece acesso a um pool compartilhado de recursos de computação (computadores, armazenamento, aplicativos e serviços) em uma rede.

c) A Deep Web refere-se ao conteúdo da World Wide Web que não é indexada pelos mecanismos de busca padrão, ou seja, não faz parte da Surface Web.

d) Moedas virtuais, como o Bitcoin, são moedas criptografadas. Trata-se de uma forma de dinheiro que existe apenas digitalmente. O Banco Mundial define as regras e efetua o monitoramento do comércio deste tipo de moeda.

Comentários: (a) Correto, tudo perfeito; (b) Correto, definição impecável de computação em nuvem – apesar de não ser o tema da nossa aula; (c) Correto, definição perfeita de Deep Web; (d) Errado, o Banco Mundial não define nenhuma regra! Primeiro: quem define regras bancárias são as autoridades monetárias (Bancos Centrais) dos respectivos países e, não, o Banco Mundial. Segundo: bitcoin é uma moeda virtual que não obedece a regras de autoridades monetárias – trata-se de um sistema monetário alternativo cujo controle é descentralizado e sem intermediários (Letra D).

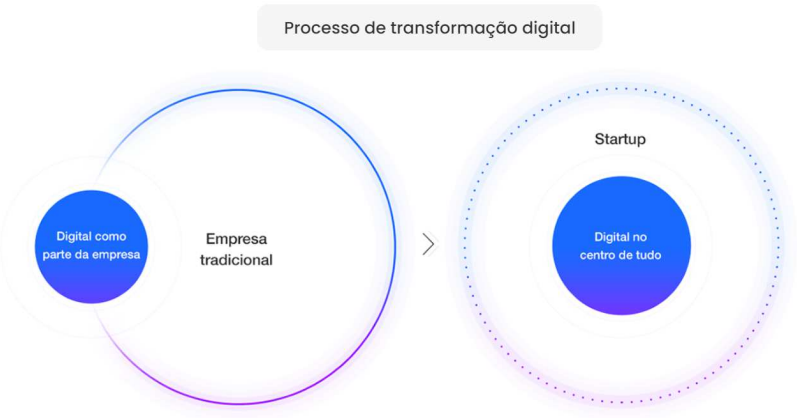
Internet das Coisas (IoT)

INCIDÊNCIA EM PROVA: BAIXA

Vamos falar inicialmente sobre **Transformação Digital**. Para tal, vamos utilizar como referência um texto da Cisco Networking Academy:

> *Diga a verdade ... quantos de vocês realmente poderiam passar o dia sem o smartphone?*
>
> *No mundo de hoje, há mais dispositivos smart que pessoas. Um número cada vez maior de pessoas está conectado à Internet, de uma maneira ou de outra, 24 horas por dia. Um número crescente de pessoas possui e depende de três, quatro ou mais dispositivos smart. Esses dispositivos podem incluir smartphones, monitores de exercícios e saúde, leitores eletrônicos e tablets. Até 2020, prevê-se que cada consumidor terá em média 6,58 dispositivos smart. Como é possível que tantos dispositivos sejam conectados?*
>
> *As redes digitais modernas tornam tudo isso possível. O mundo está sendo coberto rapidamente por redes que permitem a interconexão e a transmissão de dispositivos digitais. Pense na malha de redes como uma película digital ao redor do planeta. Com essa película digital, todos os dispositivos móveis, sensores eletrônicos, dispositivos de medição eletrônicos, dispositivos médicos e medidores podem se conectar. Eles monitoram, comunicam, avaliam e, em alguns casos, se adaptam automaticamente aos dados que estão sendo coletados e transmitidos.*
>
> *À medida que a sociedade adota desses dispositivos digitais, as redes digitais continuam crescendo ao redor do mundo e os benefícios econômicos da digitalização continuam aumentando; podemos ver uma transformação digital. A transformação digital é a aplicação de tecnologia digital para fornecer o estágio para as empresas e a indústria inovarem. Agora esta inovação digital está sendo aplicada a todos os aspectos da sociedade humana.*

Notem que a transformação digital pode ser definida como o **processo em que empresas usam tecnologias digitais inovadoras para integrar todas as áreas do negócio a fim de solucionar problemas, melhorar o desempenho, aumentar seu alcance e entregar valor ao cliente**. Trata-se de uma mudança estrutural/cultural nas organizações – e consequentemente na sociedade –, colocando a tecnologia como papel essencial para seu sucesso. Vejam a imagem a seguir:



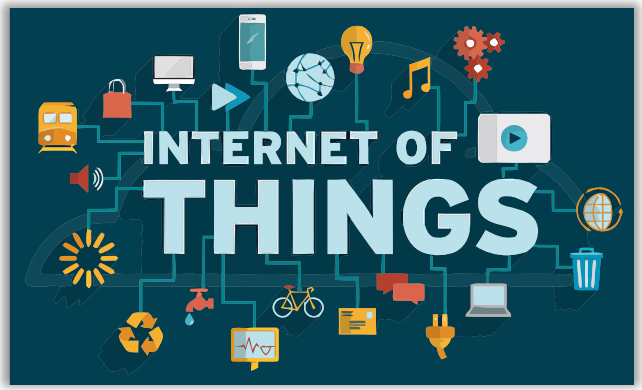
Galera, não há como fugir da transformação digital! *Querem um exemplo óbvio?* Eu estou desde o início da pandemia de coronavírus trabalhando remotamente. **O vírus basicamente acelerou de forma brutal o processo de transformação digital de órgãos e empresas – talvez, inclusive, de**

forma definitiva! Em poucos dias, salas virtuais de reunião foram configuradas, acesso remoto foi concedido e novas formas de trabalho e avaliação surgiram. É a tecnologia no centro de tudo...

A retração econômica inicial por conta da COVID-19 obrigou empresas a fazerem difíceis cortes no orçamento. De forma simultânea, a pandemia impulsionou essas empresas a acelerarem seus esforços de transformação digital devido à demanda dos clientes, à limitação de interações pessoais e às necessidades dos funcionários em trabalho remoto. **Dito isso, vamos falar de uma tecnologia que vem para acelerar ainda mais o processo de transformação digital...**

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.

(QUADRIX / CRT4 – 2022) Na Internet das coisas, o termo "coisas" pode ser compreendido como qualquer dispositivo que possa ser incorporado com eletrônicos, software, ou sensores para se comunicar com outro dispositivo.

_____

Comentários: na Internet das Coisas (IoT), o termo "coisas" refere-se a qualquer dispositivo ou objeto que pode ser equipado com eletrônicos, software e sensores para coletar, processar e compartilhar dados com outros dispositivos, sistemas ou a nuvem. Esses dispositivos podem variar desde eletrodomésticos inteligentes, veículos, sensores ambientais, máquinas

industriais até wearables e muitos outros. O objetivo é permitir que essas "coisas" se comuniquem, coletem dados e tomem ações com base nessas informações, criando um ambiente conectado e inteligente (Correto).

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.

CONTEXTO	DESCRIÇÃO
HOSPITALAR	Pacientes podem utilizar dispositivos conectados que medem batimentos cardíacos ou pressão sanguínea, por exemplo, e os dados coletados serem enviados em tempo real para o sistema que controla os exames.
AGRICULTURA	Sensores espalhados em plantações podem dar informações precisas sobre temperatura, umidade do solo, probabilidade de chuvas, velocidade do vento e outras informações essenciais para o bom rendimento do plantio.
PECUÁRIA	Sensores conectados aos animais conseguem ajudar no controle do gado: um chip colocado na orelha do boi pode fazer o rastreamento do animal, informar seu histórico de vacinas e assim por diante.
INDÚSTRIA	Sensores podem medir, em tempo real, a produtividade de máquinas ou indicar quais setores da planta industrial precisam de mais equipamentos ou suprimentos.
COMÉRCIO	Prateleiras inteligentes podem informar, em tempo real, quando determinado item está começando a faltar, qual produto está tendo menos saída ou em quais horários determinados itens vendem mais.
TRANSPORTE	Usuários podem saber, pelo smartphone ou em telas instaladas nos pontos, qual a localização de determinado ônibus. Os sensores também podem ajudar a empresa a descobrir que um veículo apresenta defeitos mecânicos, assim como saber como está o cumprimento de horários.
LOGÍSTICA	Dados de sensores instalados em caminhões, contêineres e até caixas individuais combinados com informações do trânsito podem ajudar a definir melhores rotas, escolher veículos mais adequados para determinada área, quais encomendas distribuir entre a frota ativa, 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.

(QUADRIX / CRECI-GO – 2018) A evolução do endereçamento IPv4 de 32 bits para o endereçamento IPv6 de 128 bits vai de encontro às necessidades e tendências IoT.

_____

Comentários: a evolução do endereçamento de IPv4 para IPv6, que se caracteriza pelo aumento significativo da capacidade de endereçamento, indo de 32 bits para 128 bits, é uma resposta às necessidades da IoT (Internet das Coisas). A IoT envolve a conexão de bilhões de dispositivos e objetos à internet, e cada um deles requer um endereço IP único para a comunicação. O IPv6 fornece um espaço de endereçamento muito maior em comparação com o IPv4, o que o torna mais adequado para suportar a crescente demanda de endereços gerada pela IoT. No entanto, o examinador vacilou na língua portuguesa porque a evolução do IPv4 para o IPv6 vai ao encontro das tendências da IoT e, não, de encontro à. Logo, caberia recurso! (~~Correto~~).

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.

(CESPE / ABIN – 2018) Em uma residência, caracteriza uma solução de IoT a instalação de um detector de fumaças capaz de gerar alertas em caso de fumaça e ser acionado, a partir de um smartphone, para iniciar um mecanismo de reação.

_____

Comentários: a instalação de um detector de fumaça em uma residência, que pode gerar alertas em caso de fumaça e ser acionado por meio de um smartphone para iniciar um mecanismo de reação, caracteriza uma solução de Internet das Coisas (IoT). Nesse cenário, o detector de fumaça está conectado à internet e pode ser controlado remotamente, tornando-se parte de uma rede de dispositivos interconectados, o que é uma das características fundamentais da IoT. Essa tecnologia permite monitorar e controlar objetos do cotidiano de forma mais eficiente e conveniente (Correto).

Tecnologias de Acesso

TECNOLOGIAS DE ACESSO À INTERNET

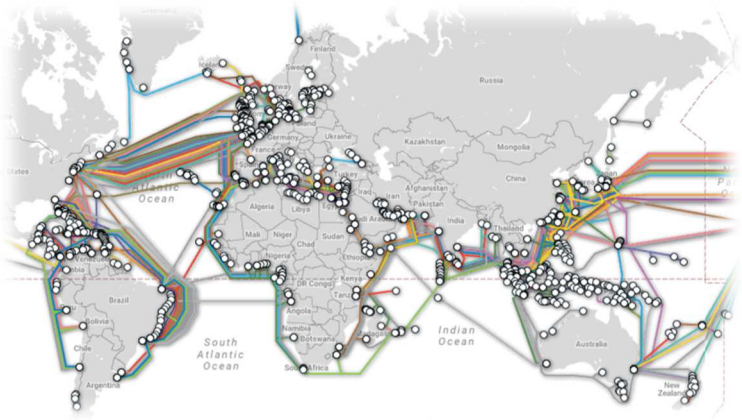
Referem-se aos métodos e infraestruturas utilizados para conectar dispositivos, como computadores, smartphones e outros equipamentos, à Internet. Essas tecnologias permitem que os dispositivos acessem os serviços e recursos disponíveis na World Wide Web e em outros serviços online. Existem várias tecnologias 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.

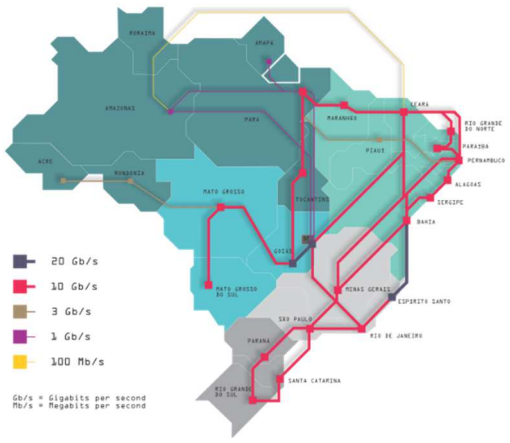
Galera, até o início da década de noventa, só quem sabia o que era internet eram pesquisadores ligados a universidades, ao governo ou à indústria. No entanto, quando um físico chamado Tim Berners-Lee criou a Web (WWW), houve uma mudança nessa realidade e a internet ganhou milhões de novos usuários sem a menor pretensão acadêmica. **O serviço de disponibilização de páginas web facilitou e popularizou bastante o uso da internet.**

Junto com o primeiro navegador da história (chamado Mosaic), a web tornou possível a configuração de diversas páginas web contendo informações, textos, imagens, sons e vídeos disponíveis através de links para outras páginas. Clicando em um link, o usuário é repentinamente transportado para a página indicada por esse link. **Com o passar dos anos, foram criadas muitas páginas em um período de tempo muito curto.**

Grande parte desse crescimento foi impulsionado por empresas denominadas Provedores de Serviços da Internet (ISP – Internet Service Provider). Essas empresas oferecem a usuários individuais a possibilidade de se conectar à Internet, obtendo assim acesso aos diversos serviços fornecidos. Essas empresas reuniram milhões de novos usuários, alterando completamente o perfil de usuário, sendo utilizada como um serviço de utilidade pública (como a telefonia).

Vamos detalhar isso melhor! A internet pode ser fornecida por meio de satélites, ondas de rádio ou uma rede de milhares de cabos de fibra óptica terrestres ou submarinos, que conectam diversos países, respondendo por 80% de toda a comunicação. **Essa infraestrutura de redes – que forma a espinha dorsal da internet – é chamada de Backbone. Ela possui alta velocidade, desempenho e interliga várias redes, garantindo o fluxo da informação por dimensões continentais**.





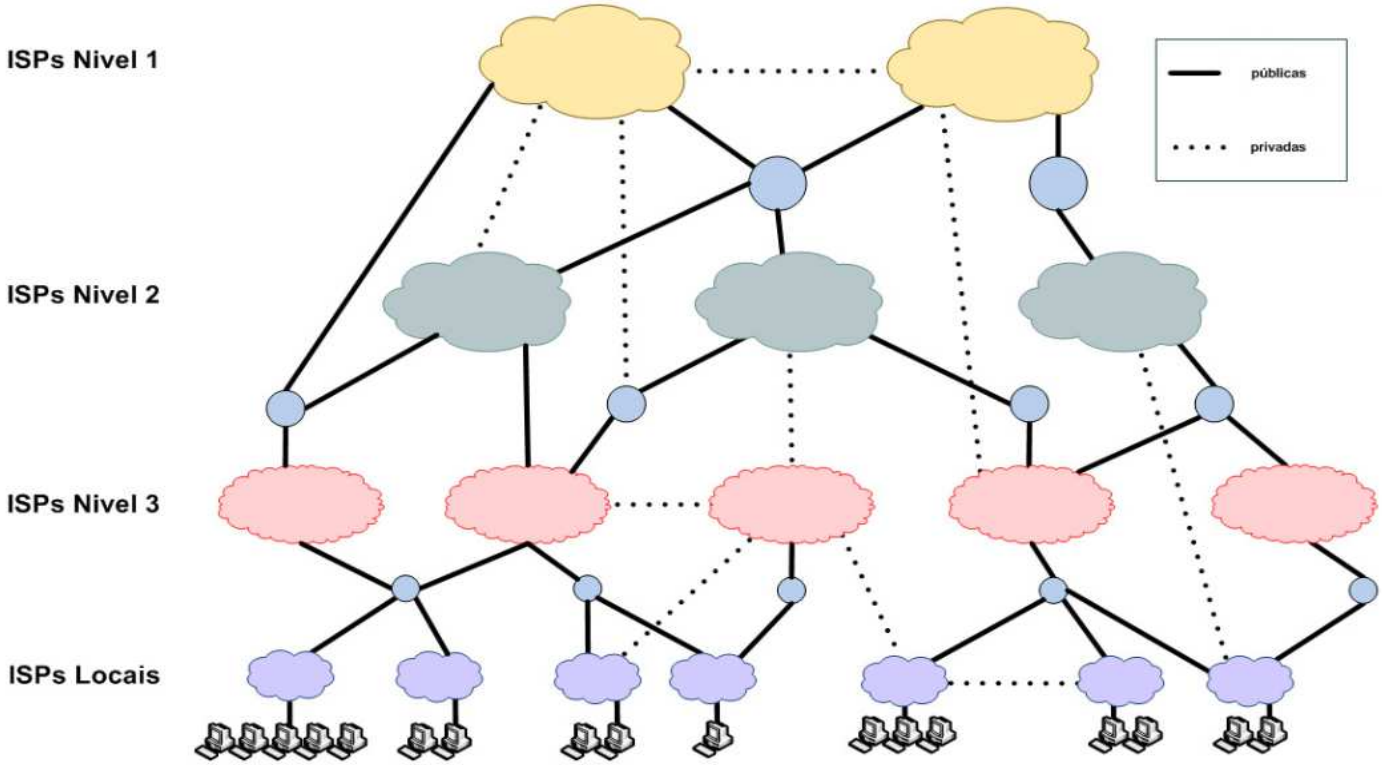
Diego, quem constrói esses backbones? Eles são construídos por provedores de serviço de internet, que administram troncos de longo alcance com o objetivo de fornecer acesso à internet para diversas outras redes. Em geral, eles pertencem a companhias telefônicas de longa distância (Ex: Embratel) ou a governos nacionais (Ex: Rede Nacional de Ensino e Pesquisa – RNP), **que vendem o acesso para Provedores de Serviço de Internet (ISP – Internet Service Provider)**.

Os provedores de internet nacionais mais conhecidos atualmente são: NET/CLARO, GVT/VIVO e SKY. Por sua vez, esses provedores de internet vendem o acesso a provedores menores ou a usuários comuns. Na imagem anterior, é possível visualizar os maiores troncos de backbones espalhados pelo mundo entre os continentes e também os troncos de backbones brasileiros. Notem que eles podem ser terrestres ou submarinos. 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.



(CESPE / Correios – 2011) Redes de acesso situadas na borda da Internet são conectadas ao restante da rede segundo uma hierarquia de níveis de ISPs (Internet service providers). Os ISPs de nível 1 estão no nível mais alto dessa hierarquia.

Comentários: ISPs de Nível 1 estão no topo da hierarquia de ISPs da Internet. Esses provedores de serviços de Internet não compram largura de banda de nenhum outro ISP, mas sim interconectam suas próprias redes em uma escala global. Eles formam a espinha dorsal da Internet e estão envolvidos no roteamento do tráfego entre redes autônomas. A hierarquia de ISPs da Internet é organizada em camadas, e os ISPs de Nível 1 são a camada mais alta, responsável por rotear o tráfego global da Internet. ISPs de Nível 2 e Nível 3 geralmente se conectam aos de Nível 1 e servem áreas geográficas menores (Correto).

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

Trata-se de uma conexão discada através de um modem e uma linha de telefonia fixa. Era a maneira mais popular de acesso da década de 90, hoje encontra-se em desuso. Apresenta um alto custo de implementação, é bastante instável e possui baixas taxas de transmissão. *Era banda larga?* Não, era banda estreita – com taxas máximas de 56Kbps. Se hoje você reclama que a sua internet de 100 Mbps está lenta, lembre-se que uma internet discada era 2000x mais lenta!

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.

(QUADRIX / CRECI-GO – 2018) Assim como a Internet, a dial-up é considerada como uma rede de computadores. A única diferença é que a dial-up é uma rede pequena, com pouca abrangência, e, por isso, extremamente rápida.

Comentários: dial-up é uma tecnologia de acesso à internet e, não, uma rede de computadores (Errado).

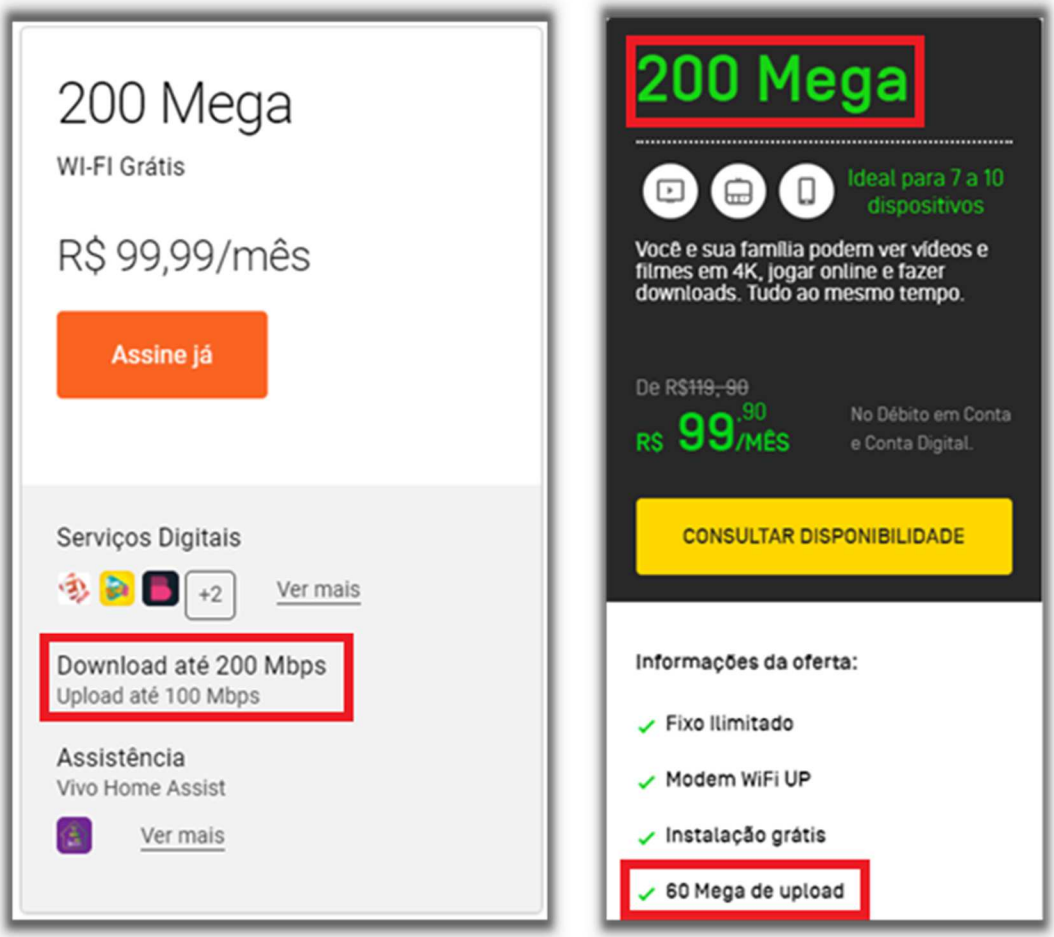
ADSL

INCIDÊNCIA EM PROVA: MÉDIA

Trata-se da conexão de banda larga (assim como todas as outras que veremos a seguir) oferecida por empresas de telefonia fixa. ADSL é a sigla para *Asymmetric Digital Subscriber Line* ou Linha de Assinante Digital Assimétrica. Essa tecnologia possui uma grande vantagem: embora utilize a mesma infraestrutura da telefonia, a transmissão de dados ocorre em frequências mais altas que as de voz, permitindo – portanto – o uso da internet sem ocupar o telefone.

Professor, por que essa é uma tecnologia assimétrica? **Porque as taxas de download e de upload são diferentes – sendo a velocidade de download maior que a de upload.** *Vocês sabiam disso?* Quando nós contratamos um serviço de internet via ADSL, nós sempre olhamos a taxa de download e esquecemos a taxa de upload. Na minha casa, eu assinei um serviço de 100mbps! Notem que essa é a taxa (máxima) de download – a taxa de upload é bem menor.

Vejam no exemplo seguinte que a taxa de download à esquerda é de 200 mbps e a taxa de upload é de 100 mbps; a taxa de download à direita é de 200 mbps e a taxa de upload é 60 mbps. *Isso faz diferença, Diego?* Dependerá do seu perfil de utilização! **Se você costuma apenas fazer navegar na web, assistir um filme, baixar aulas – não há nenhum problema; mas se você tem um canal no Youtube e precisa fazer uploads de vídeos grandes – pode ser inconveniente.**



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.

(FUNDEP / UFVJM-MG – 2017) Assinale a alternativa que apresenta a sigla que representa uma tecnologia com finalidade de permitir o uso de linha telefônica para transmissão digital de dados em alta velocidade.

a) ADSL
b) AUP
c) IP
d) FTP

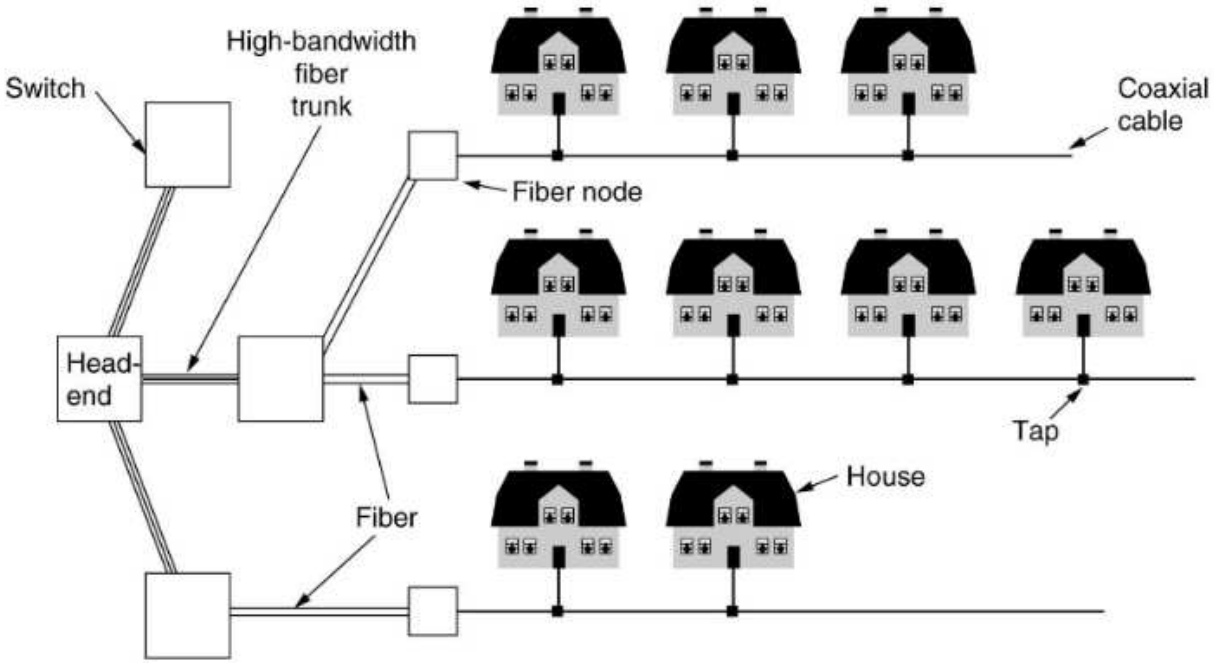
_____
Comentários: tecnologia que permite uso da linha telefônica para transmissão de alta velocidade é o ADSL (Letra A).

HFC

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Trata-se da conexão híbrida de banda larga via cabos de concessionárias de TV a Cabo (NET, GVT, OI). HFC é a sigla para *Hybrid Fiber-Coax* e representa o hibridismo entre fibra óptica e cabo coaxial. *Por que é um hibridismo, Diego?* Porque os cabos de fibra óptica partem do backbone central, passam pelos postes até chegar mais próximo das residências e se conectar a um receptor óptico. A partir daí, cabos coaxiais saem do receptor e distribuem o sinal entre as casas[20].

[20] Atualmente, temos uma tecnologia chamada FTTH (Fiber To The Home) que envolve a instalação de cabos de fibra óptica diretamente da central de telecomunicações até a residência ou local de trabalho do usuário.



É interessante mencionar que esses cabos coaxiais que saem do receptor para distribuir o sinal entre as casas funciona como um barramento compartilhado, logo com transmissão em broadcast. HFC e ASDL são tecnologias concorrentes: **ambas são assimétricas e possuem taxas de transmissão semelhantes, porém a primeira é fornecida por empresas de TV a Cabo e a segunda é oferecida por empresas de telefonia fixa.**

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.

(PROF. DIEGO / INÉDITA – 2023) HFC é uma tecnologia que utiliza tanto fibra óptica quanto cabos coaxiais para fornecer serviços de internet e TV a cabo.

_____

Comentários: na verdade, as redes HFC têm uma parte inicial de fibra óptica, que é usada para transmitir dados a longas distâncias, e uma parte final de cabos coaxiais, que levam os dados diretamente para as casas dos assinantes. É uma solução híbrida que combina as vantagens de ambas as tecnologias (Correto).

Fibra Óptica

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Trata-se da conexão direta via fibra óptica até a residência do contratante do serviço de internet. Pois é, já existe tecnologia que permite uma conexão direta até a sua casa por meio de um cabo de fibra óptica. Ainda não está disponível em diversas localizações (como a minha casa), mas essa tecnologia tende a se popularizar. *Você já tem na sua região?* Vamos ver agora as suas principais características:

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.

(PROF. DIEGO / INÉDITA – 2023) A fibra óptica é uma tecnologia de acesso à internet que possui maior latência em comparação com conexões de cabo.

Comentários: a fibra óptica é conhecida por ter menor latência em comparação com muitas outras tecnologias de acesso à internet, tornando essa afirmação falsa (Errado).

PLC

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Trata-se da tecnologia que permite o acesso à internet banda larga via rede elétrica. PLC é a sigla para *Power Line Communication*. *Como assim, professor?* Como vantagem, é uma tecnologia bastante portátil, visto que basta plugar o modem em uma tomada compatível com o serviço para se obter o acesso. No Brasil, embora o serviço seja autorizado pelas agências responsáveis, os investimentos foram baixos por questões estratégicas e econômicas.

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.

(CESPE / FUB – 2011) A tecnologia Power Line Communication (PLC) possibilita a transmissão de dados através das redes de energia elétrica, utilizando-se uma faixa de

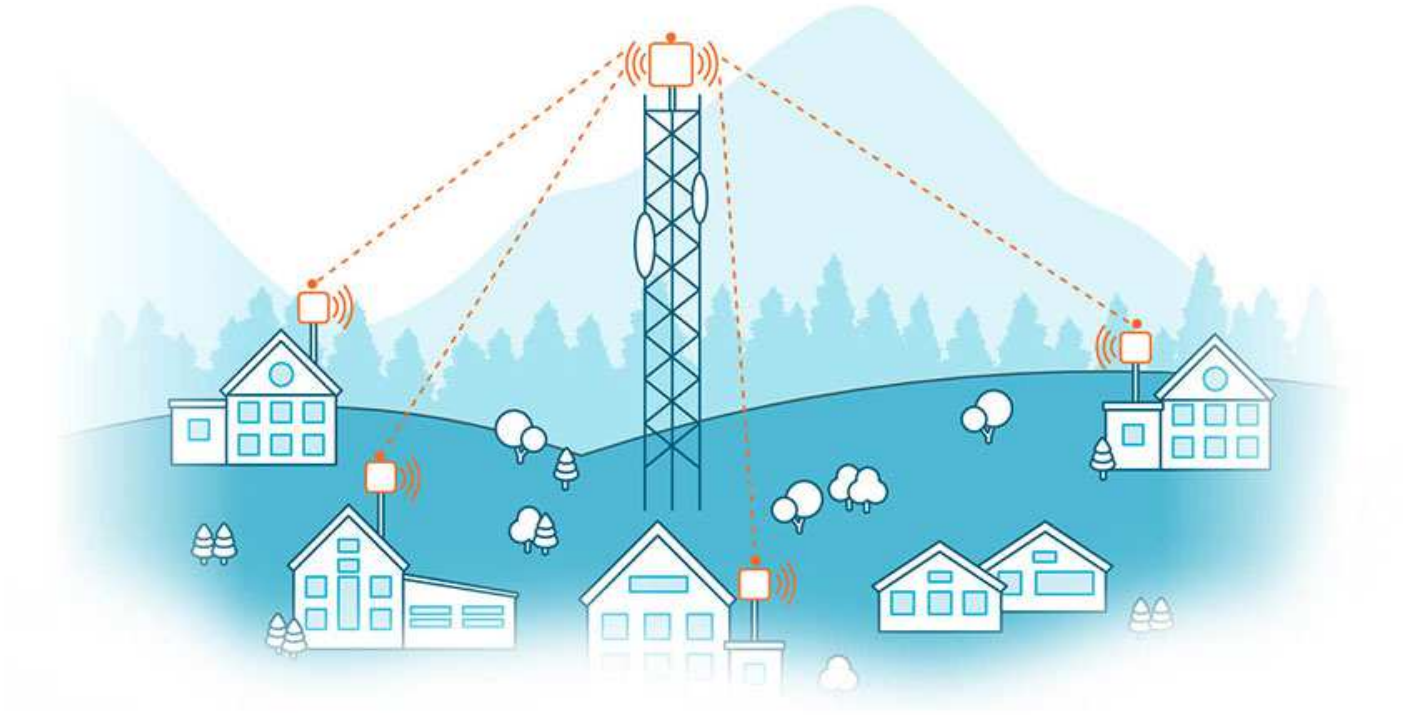
frequência diferente da normalmente utilizada na rede elétrica para a distribuição de energia.

_____

Comentários: PLC realmente possibilita a transmissão de dados através das redes de energia elétrica, utilizando-se uma faixa de frequência diferente da normalmente utilizada na rede elétrica para a distribuição de energia (Correto).

Radiodifusão

INCIDÊNCIA EM PROVA: BAIXÍSSIMA



Trata-se da tecnologia que permite o acesso à internet banda larga via radiofrequência. As ondas de rádio, em sua maior parte, são omnidirecionais, isto é, quando uma antena transmite ondas de rádio, elas se propagam em todas as direções em broadcast. Elas podem percorrer grandes distâncias e podem atravessar paredes, não necessitando que antenas transmissoras estejam completamente alinhadas.

No entanto, não pode haver grandes obstáculos entre o emissor e o receptor de sinal, como montanhas. **Trata-se de uma boa alternativa quando não é possível utilizar uma rede cabeada**, no entanto existem também diversas desvantagens: ondas de rádio podem sofrer interferências de outras ondas; a geografia entre as antenas pode ser um impeditivo; está bastante sujeito a intempéries climáticas como tempestades e vendavais; entre outros.

Não é muito utilizado em meios urbanos, mas é uma boa alternativa para meios rurais, onde cabos não estão disponíveis. Vejamos as principais características de redes de radiodifusão:

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.

(FUNIVERSA / CEB – 2010) A transmissão de sinais está condicionada à qualidade do meio de comunicação, que pode variar de acordo com as condições físicas a que esteja sujeito. Parâmetros como velocidade de transmissão, atraso e variação no atraso de pacotes, taxa de erro são afetados quando há perda na qualidade do meio físico. Assinale a alternativa que apresenta o meio físico que sofre maiores interferências das variações climáticas, como acúmulo de nuvens e precipitações.

a) Fibra óptica
b) Cabo de par trançado
c) Enlace de rádio
d) Cabo coaxial
e) Rede elétrica

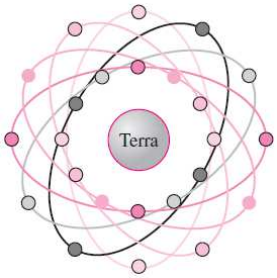
_____

Comentários: quem sofre maiores interferências com acúmulo de nuvens e precipitações é o enlace de rádio (Letra C).

Satélite

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Uma rede via satélite é uma combinação de nós que fornecem comunicação de um ponto a outro na Terra. Nesse contexto, um nó pode ser um satélite, uma estação terrestre ou o terminal/telefone de um usuário final. *Vocês sabiam que é possível utilizar a Lua como satélite?* Não há nenhum problema, mas prefere-se o emprego de satélites artificiais que permitem a instalação de equipamentos eletrônicos para regenerar o sinal que perdeu intensidade durante seu trajeto.



Outra restrição no emprego de satélites naturais são suas distâncias até o nosso planeta, que criam um longo retardo nas comunicações. Os satélites podem oferecer recursos de transmissão de/para qualquer ponto da Terra, não importando sua distância. Essa vantagem possibilita a disponibilização de comunicação de alto padrão em partes subdesenvolvidas do mundo sem exigir grandes investimentos em infraestrutura terrestre. *Como assim, Diego?*

Galera, existem algumas regiões que não existe absolutamente nenhuma infraestrutura – nem sequer via radiodifusão. Um nômade em um deserto, um navio no meio do oceano, um cientista no meio da floresta amazônica – não existe infraestrutura! **Como vantagem, ele permite o acesso à internet de qualquer lugar do planeta em broadcast; por outro lado, ele é bastante caro e também está sujeito a intempéries climáticas.**

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.

(FUNRIO / IFBA – 2014) Qual o meio de comunicação importante para o Ensino à Distância em razão da possibilidade de realizar cobertura global, de possuir elevada largura de banda e de possibilitar transmissões de difusão?

a) Cabo coaxial
b) Canal de HF
c) Fibra Óptica
d) Par trançado
e) Satélite

_____
Comentários: o meio de acesso que permite realizar uma cobertura global de difusão/broadcast é o Satélite (Letra E).

Telefonia Móvel

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Trata-se da tecnologia projetada para estabelecer comunicação entre duas unidades móveis, denominadas Estações Móveis; ou entre uma unidade móvel e outra fixa, normalmente chamada Unidade Terrestre. Um provedor de serviços tem de ser capaz de localizar e rastrear uma unidade que faz chamada, alocar um canal à chamada e transferir o canal de uma estação rádio base a outra à medida que o usuário que faz a chamada deixa a área de cobertura.

Para permitir esse rastreamento, cada área de serviço é dividida em pequenas regiões chamadas células e cada célula contém uma antena (por essa razão, é chamada de telefonia celular). O tamanho da célula não é fixo e pode ser aumentado ou diminuído, dependendo da população da região. **A telefonia celular encontra-se agora na quinta geração, porém vai demorar um pouco para chegar a todos os brasileiros.** Vejamos as principais gerações de telefonia celular:

- **Primeira Geração (1G):** a primeira geração foi projetada para comunicação de voz usando sinais analógicos. Introduzida em 1982 e encerrada em 1990, era usada apenas para serviços de voz e baseado em tecnologia chamada Advanced Mobile Phone System (AMPS).

- **Segunda Geração (2G):** a segunda geração de redes móveis foi a primeira a utilizar a tecnologia digital para transmissão de voz. As principais tecnologias 2G incluíam o GSM (Sistema Global para Comunicações Móveis) e o CDMA (Acesso Múltiplo por Divisão de Código).

- **Segunda Geração (2,5G):** também chamada de GPRS (Serviço de Rádio Geral), essa geração representou uma melhoria nas redes 2G com maior capacidade de transferência de dados e suporte limitado à internet móvel.

- **Terceira Geração (3G):** as redes 3G introduziram a transmissão de voz e vídeo digital, bem como a capacidade de acesso à internet móvel em alta velocidade. Tecnologias como o UMTS (Sistema Universal de Telecomunicações Móveis) e o CDMA2000 foram comuns.

- **Quarta Geração (4G):** o 4G foi projetado para oferecer velocidades de internet móvel significativamente mais rápidas em comparação com as gerações anteriores. Tecnologias, como o LTE (Evolução a Longo Prazo) e o WiMAX, foram amplamente utilizadas.

- **Quinta Geração (5G):** baseado na tecnologia OFDM, trata-se da geração atual de telefonia celular. Começou a ser implantada em alguns lugares ao final de 2018 e possuem uma largura de banda maior, proporcionando maiores velocidades de download.

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.

RESUMO

REDES DE COMPUTADORES

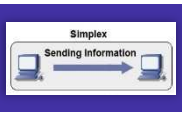
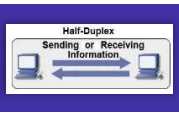
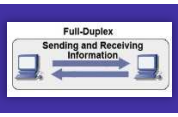
DEFINIÇÃO DE REDE DE COMPUTADORES

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

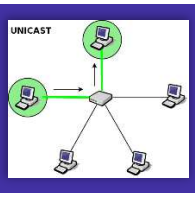
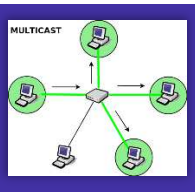
TIPOS DE CONEXÃO/ENLACE

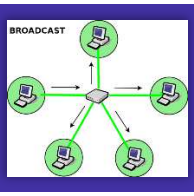
TIPO DE CONEXÃO	DESCRIÇÃO
PONTO-A-PONTO	Conexão que fornece um link dedicado entre dois dispositivos.
PONTO-MULTIPONTO	Conexão que fornece um link compartilhado entre mais de dois dispositivos.

DIREÇÕES DE TRANSMISSÃO

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.
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.
FULL-DUPLEX		Uma comunicação é dita full-duplex quando temos um transmissor e um receptor, sendo que ambos podem transmitir e receber dados simultaneamente.

MODOS DE TRANSMISSÃO

TIPO	REPRESENTAÇÃO	DESCRIÇÃO
UNICAST		Uma mensagem só pode ser enviada para um destino. Grosso modo, quando você envia uma mensagem no Whatsapp para uma pessoa específica, você está enviando uma mensagem unicast.
MULTICAST		Uma mensagem é enviada para um grupo de destino. Grosso modo, 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		Uma mensagem é enviada para todos os destinos. Grosso modo, 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

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.

CLASSIFICAÇÃO DE REDES: QUANTO À ARQUITETURA

TIPO DE REDE	DESCRIÇÃO
PONTO A PONTO	Também chamada de Rede Par-a-Par, é o modelo de rede mais simples de ser montado. Nesse modelo, todas as máquinas podem compartilhar dados e periféricos umas com as outras. Essas redes são comuns em residências e entre filiais de empresas, porque demandam um baixo custo, são facilmente configuráveis e possibilitam altas taxas de velocidade de conexão.
CLIENTE/ SERVIDOR	É um modelo de redes mais complexo, porém mais robusto e confiável. Nesse modelo, existe uma máquina especializada, dedicada e geralmente remota, respondendo rapidamente aos pedidos vindos dos demais computadores da rede – o que aumenta bastante o desempenho de algumas tarefas. É a escolha natural para redes grandes, como a Internet – que funciona tipicamente a partir do Modelo Cliente/Servidor.

CLASSIFICAÇÃO DE REDES: QUANTO À TOPOLOGIA

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.

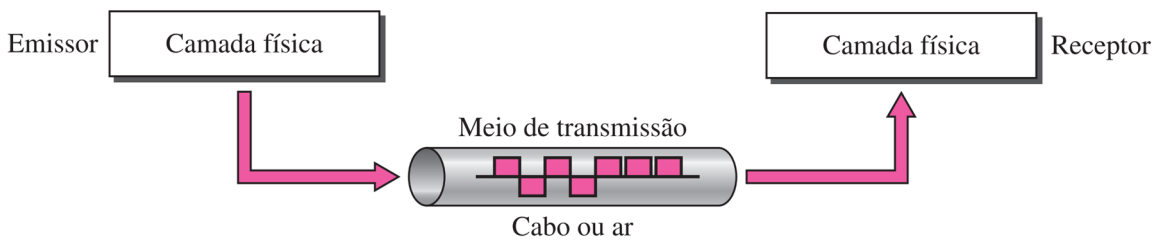
TIPO	REPRESENTAÇÃO	DESCRIÇÃO
BARRAMENTO (BUS)		Todas as estações ficam ligadas ao mesmo meio de transmissão, isto é, um único cabo (chamado backbone) em que os nós se ligam através de conectores. Há maior facilidade na instalação e economia de cabeamento, mas não há isolamento de falhas – uma ruptura no cabo implica a interrupção da comunicação.

ANEL (RING)		Cada dispositivo possui uma conexão ponto-a-ponto com outros dois dispositivos conectados lado a lado, e fazendo uso de uma comunicação com transmissão unidirecional (simplex). Nesse caso, a mensagem circula o anel, sendo regenerada e retransmitida a cada nó, passando pelo dispositivo de destino que copia a informação enviada, até retornar ao emissor original. Nesse momento, o link é liberado para que possa ser utilizado pelo nó seguinte.
ESTRELA (STAR)		As estações estão ligadas a um nó central controlador, pelo qual passam todas as mensagens, não havendo tráfego direto entre os dispositivos. O enlace entre estações e o nó central é Ponto-a-Ponto. É a topologia mais usada atualmente por facilitar a adição de novas estações e a identificação ou isolamento de falhas, em que – se uma conexão se romper – não afetará a comunicação de outras estações.
MALHA (MESH)		Cada estação possui um link ponto a ponto dedicado geralmente com transmissão bidirecional (full duplex) entre cada uma das demais estações. Em outras palavras, todos os computadores estão interligados entre si, de modo que caso haja uma ruptura em algum cabo, não cai a rede inteira, somente o nó conectado a esse cabo.

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

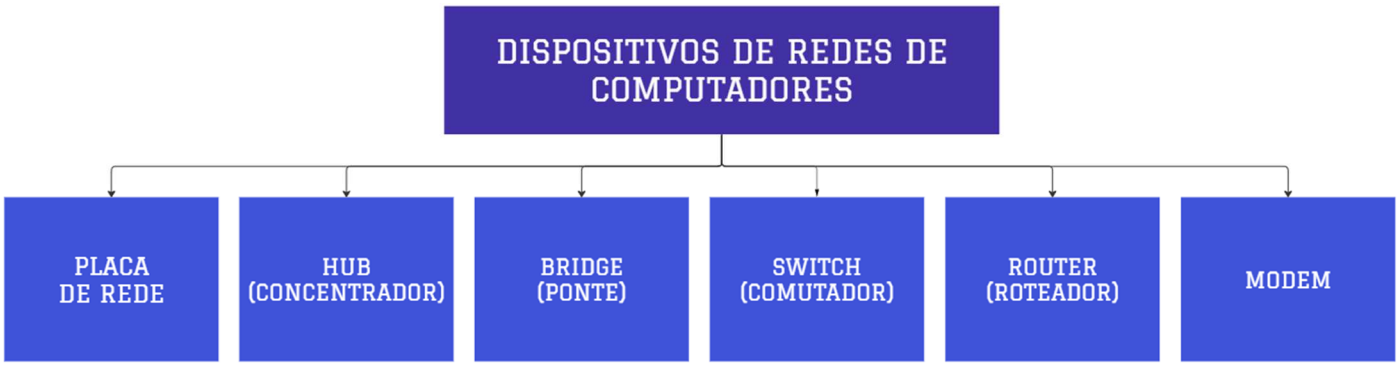
MEIOS DE TRANSMISSÃO

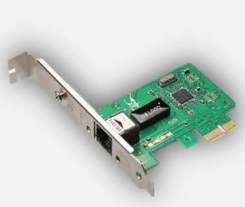
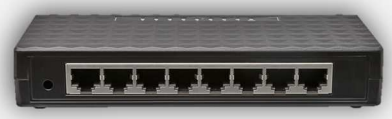
TIPO DE MEIO	DESCRIÇÃO
GUIADO	Trata-se da transmissão por cabos ou fios de cobre, onde os dados transmitidos são convertidos em sinais elétricos que propagam pelo material condutor. Exemplo: cabos coaxiais, cabos de par traçado, fibra óptica, entre outros.
NÃO-GUIADO	Trata-se da transmissão por irradiação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



TIPO	REPRESENTAÇÃO	DESCRIÇÃO
CABO COAXIAL		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, relativamente flexível e muito resistente à interferência eletromagnéticas graças à malha de proteção que possui. Esse cabo cobre distâncias maiores que o cabo de par trançado e utiliza um conector chamado BNC.
CABO DE PAR TRANÇADO		Consiste de 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!).
CABO DE FIBRA ÓPTICA		Consiste em uma Casca e um Núcleo (de vidro) para transmissão de luz. Possui capacidade de transmissão virtualmente infinita, é imune a interferências eletromagnéticas e consegue ligar distâncias maiores sem a necessidade de repetidores. Como desvantagens, podemos dizer que é incapaz de fazer curvas acentuadas, além de ter um custo de instalação e manutenção muito alto em relação ao par trançado. Há dois tipos de fibra: Monomodo e Multimodo.

EQUIPAMENTOS DE REDES



PLACA DE REDE	HUB (CONCENTRADOR)	BRIDGE (PONTE)
		
Equipamento de rede de comunicação bidirecional (entrada e saída de dados) conectado à placa-	Dispositivo de rede capaz de aumentar o alcance de uma rede local por meio da regeneração de	Equipamento capaz de separar uma rede em segmentos menores,

mãe do computador. Toda placa de rede possui um número identificador chamado Endereço MAC (48 Bits).	sinais. É capaz de trabalhar apenas com broadcast, isto é, ao receber um pacote de dados, distribui para todas as máquinas da rede.	reduzindo as chances de colisões quando várias máquinas desejam transmitir dados ao mesmo tempo. São dispositivos capazes de enviar dados para máquinas específicas.
SWITCH (COMUTADOR)	**ROUTER (ROTEADOR)**	**MODEM**
		
Equipamento semelhante às Bridges, no entanto possuem mais portas. Em contraste com hubs, são capazes de transmitir dados para máquinas específicas (unicast ou multicast). Por segmentarem a rede, reduzem as colisões e diminuem o fluxo de informações.	Equipamento que permite interligar redes distintas e são capazes de escolher as melhores rotas para transmissão de pacotes de dados. É responsável por interligar dispositivos de uma rede local (Ex: Computador, Notebook, Smartphone, Impressora, etc) à internet.	Equipamento capaz de converter sinais digitais em sinais analógicos e vice-versa, em geral por meio de uma linha telefônica. Os três modelos principais são: Acesso Discado; Modem ADSL; e Cable Modem.

PLACAS DE REDE	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.

HUBS	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.

BRIDGES	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede utilizado 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.

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

ROTEADORES	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	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

PADRÕES DE REDES OU ARQUITETURA DE INTERCONEXÃO
Trata-se de um conjunto de padrões de interconexão de redes de computadores.

PADRÃO	NOME
IEEE 802.3	Ethernet (LAN)

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)

PADRÕES DE REDES: 802.3

PADRÃO ETHERNET (IEEE 802.3)
Padrão de interconexão atualmente em redes locais cabeadas baseada no envio de pacotes de dados – possui diversas variantes como Fast Ethernet, Gigabit Ethernet, 10G Ethernet, etc.

EVOLUÇÃO DOS PADRÕES ETHERNET	
PADRÃO (CABO DE PAR TRANÇADO)	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

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.

PADRÕES DE REDES: 802.5

PADRÃO TOKEN RING (IEEE 802.5)
Arquitetura de conexão de redes locais cabeada atualmente em desuso. Possui comunicação unidirecional (simplex), arquitetura ponto-a-ponto e topologia lógica em anel.

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.

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.

PADRÕES DE REDES: 802.11

PADRÃO WIRELESS (IEEE 802.11)
Arquitetura de conexão de redes locais sem fio que define um conjunto de padrões de transmissão e codificação para comunicações não cabeadas.

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.

EVOLUÇÃO DO PADRÃO WI-FI (802.11)[1]		
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

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.

[1] Para decorar a ordem, lembre-se da palavra **BAG**U**NÇA** (lembrando que CA é AC).

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.

PADRÕES DE REDES: 802.15

PADRÃO BLUETOOTH (IEEE 802.15)
O Padrão Bluetooth tem o objetivo de integrar equipamentos periféricos. Utilizado em Rede WPAN (Wireless PAN) – eles padronizam uma rede de baixo custo, curto alcance, baixas taxas de transmissão e sem fio.

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

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.

PADRÕES DE REDES: 802.16

PADRÃO WIMAX (IEEE 802.16)
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.

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

INTERNET
A Internet é basicamente um vasto conjunto de redes de computadores diferentes que utilizam um padrão comum de comunicação e oferece um determinado conjunto de serviços.

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

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

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.

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.

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.

TECNOLOGIAS DE ACESSO

TECNOLOGIAS DE ACESSO À INTERNET

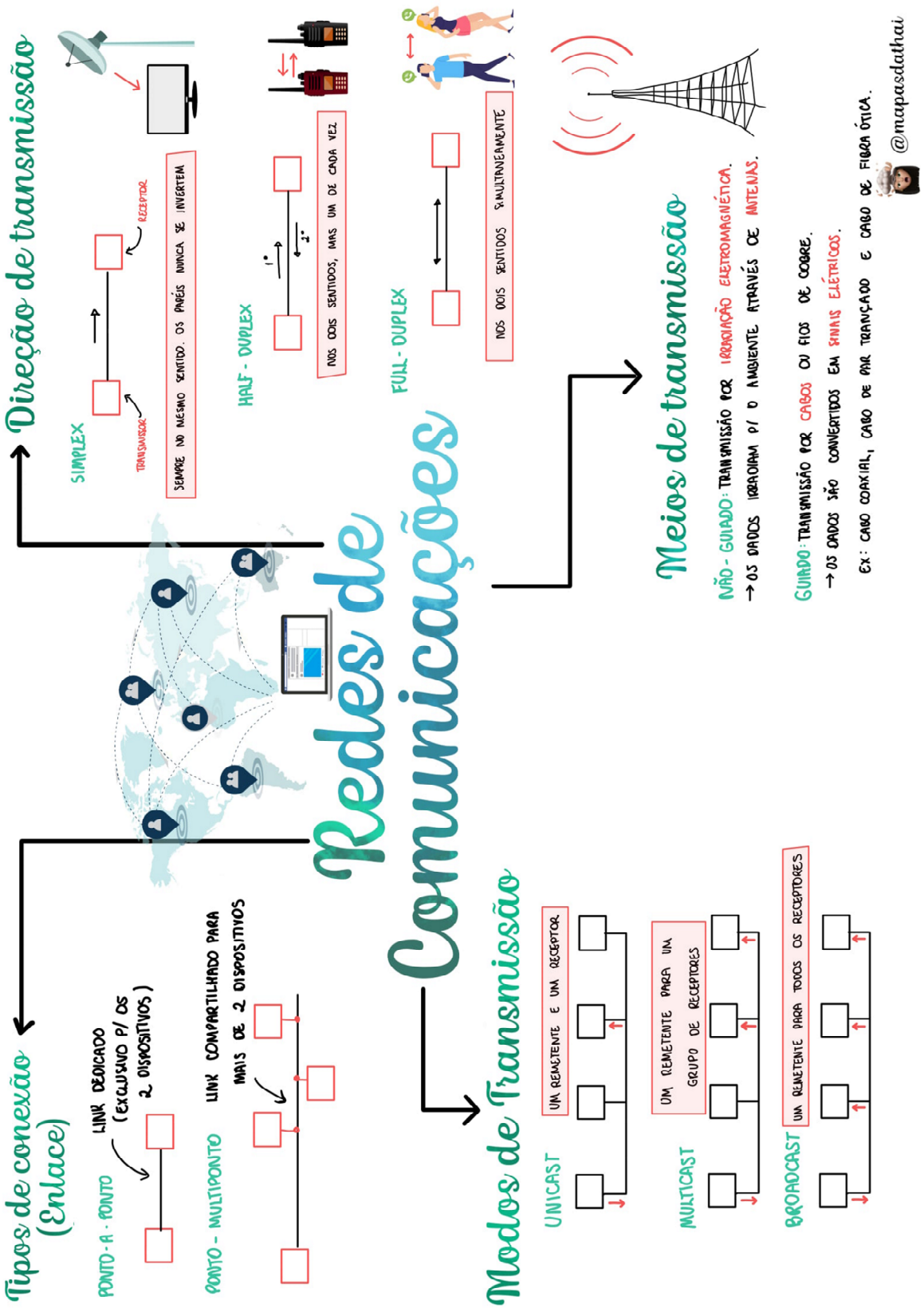
Referem-se aos métodos e infraestruturas utilizados para conectar dispositivos, como computadores, smartphones e outros equipamentos, à Internet. Essas tecnologias permitem que os dispositivos acessem os serviços e recursos disponíveis na World Wide Web e em outros serviços online. Existem várias tecnologias 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.

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.

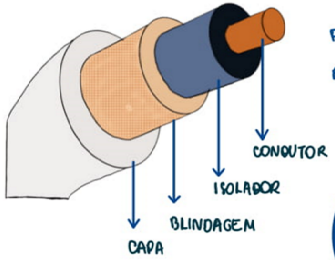
TECNOLOGIAS DE ACESSO	DESCRIÇÃO
DIAL-UP	Uma tecnologia de acesso discado à internet que utiliza a linha telefônica tradicional. É lenta e está em desuso na maioria das áreas.
ADSL	Uma tecnologia de acesso de banda larga que utiliza a linha telefônica para fornecer velocidades mais rápidas do que o dial-up.
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.

MAPA MENTAL

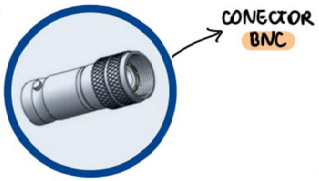

Redes de Comunicações
Direção de transmissão
SIMPLEX
TRANSMISSOR
RECEPTOR
SEMPRE NO MESMO SENTIDO. OS PAPÉIS NUNCA SE INVERTEM
HALF - DUPLEX
1.º
2.º
NOS DOIS SENTIDOS, MAS UM DE CADA VEZ
FULL - DUPLEX
NOS DOIS SENTIDOS SIMULTANEAMENTE
Meios de transmissão
NÃO - GUIADO: TRANSMISSÃO POR IRRADIAÇÃO ELETROMAGNÉTICA.
→ OS DADOS IRRADIAM P/ O AMBIENTE ATRAVÉS DE ANTENAS.
GUIADO: TRANSMISSÃO POR CABOS OU FIOS DE COBRE.
→ OS DADOS SÃO CONVERTIDOS EM SINAIS ELÉTRICOS.
EX: CABO COAXIAL, CABO DE PAR TRANÇADO E CABO DE FIBRA ÓTICA.
@mapasdathai
Tipos de conexão (Enlace)
PONTO - A - PONTO
LINK DEDICADO (EXCLUSIVO P/ OS 2 DISPOSITIVOS)
PONTO - MULTIPONTO
LINK COMPARTILHADO PARA MAIS DE 2 DISPOSITIVOS
Modos de Transmissão
UNICAST
UM REMETENTE E UM RECEPTOR
MULTICAST
UM REMETENTE PARA UM GRUPO DE RECEPTORES
BROADCAST
UM REMETENTE PARA TODOS OS RECEPTORES

Meios de Transmissão Guiados

Cabo coaxial



FIO METAL DE COBRE, ENVOLVIDO POR UMA BLINDAGEM METÁLICA.

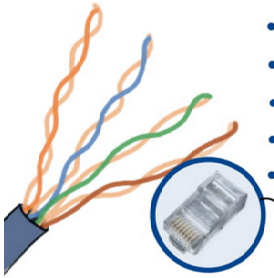


- MAIS BARATO
- RELATIVAMENTE FLEXÍVEL
- MUITO RESISTENTE (NÃO IMUNE) À INTERFERÊNCIA ELETROMAGNÉTICA
  - GRAÇAS À MALHA/CAPA DE PROTEÇÃO
- COBRE DISTÂNCIAS MAIORES
- TAXA DE TRANSMISSÃO MENOR
- LARGURA DE BANDA MAIOR

  → QUE O CABO DE PAR TRANÇADO
- AINDA É USADO EM TELECOMUNICAÇÕES

Cabo de par trançado

QUATRO PARES DE FIOS TRANÇADOS, BLINDADOS OU NÃO, ENVOLTOS DE UM REVESTIMENTO EXTERNO FLEXÍVEL.



- SÃO TRANÇADOS PARA DIMINUIR A INTERFERÊNCIA ELETROMAG.
- É O CABO + BARATO
- BASTANTE FLEXÍVEL
- TRANSMITE SINAL ANALÓGICO E DIGITAL
- 2 PARES P/ TRANSMISSÃO E 2 P/ RECEPÇÃO (FULL-DUPLEX)

CONECTOR RJ-45

- BLINDADO: STP (SHIELDED TWISTED PAIR)
- NÃO BLINDADO: UTP (UNSHIELDED TWIFTED PAIR)

Cabo de Fibra Ótica

CONSISTE EM UMA CASCA E UM NÚCLEO (DE VIDRO) PARA TRANSMISSÃO DE LUZ.

- CAPACIDADE DE TRANSMISSÃO VIRTUALMENTE INDEFINIDA.
- IMUNE A INTERFERÊNCIAS ELETROMAGNÉTICAS
- LIGA DISTÂNCIAS MAIORES SEM NECESSIDADE DE UM REPETIDOR
- É INCAPAZ DE FAZER CURVAS ACENTUADAS
- ALTO CUSTO DE INSTALAÇÃO E MANUTENÇÃO

FIBRA MULTIMODO

- LEVA O FEIXE DE LUZ POR VÁRIOS MODOS/CAMINHOS
- DISTÂNCIA MENOR
- TAXA DE TRANSMISSÃO MENOR
- PRECISÃO MENOR
- DIÂMETRO MAIOR
- ALTO ÍNDICE DE REFRAÇÃO E ATENUAÇÃO
- CONSTRUÇÃO MAIS SIMPLES E MAIS BARATA
- USADA NAS LANs

FIBRA MONOMODO

- LEVA O FEIXE DE LUZ POR UM ÚNICO MODO/CAMINHO
- DISTÂNCIA MAIOR
- TAXA DE TRANSMISSÃO MAIOR
- PRECISÃO MAIOR
- DIÂMETRO MENOR
- BAIXO ÍNDICE DE REFRAÇÃO E ATENUAÇÃO
- CONSTRUÇÃO MAIS COMPLEXA E MAIS CARA
- USADA NAS WANs

@mapasdathai

Tipos de Rede

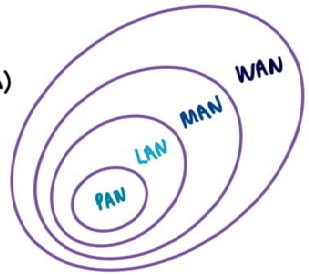
Por Dimensão

PAN: REDE PESSOAL. COMPUTADOR, CELULAR, ACESSÓRIOS (TUDO P/ UMA SÓ PESSOA)

LAN: REDE DE LARES, ESCRITÓRIOS, ANDAR DE PRÉDIO, CAMPUS, ETC.

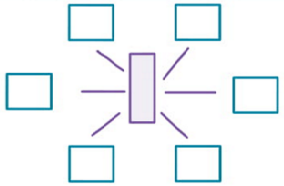
MAN: REDE ENTRE UMA MATRIZ E FILIAIS EM UMA MESMA CIDADE

WAN: REDE ENTRE CIDADES, PAÍSES OU CONTINENTES



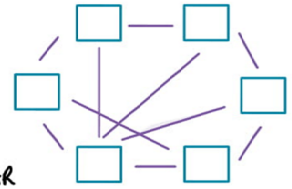
Por Arquitetuta/Forma de Interação

REDE CLIENTE-SERVIDOR



- AS MÁQUINAS (CLIENTES) ESTÃO TODAS LIGADAS A UMA ESPECIALIZADA (SERVIDOR)

REDE PONTO-A-PONTO



- PEER-TO-PEER (P2P) OU PAR-A-PAR
- TODAS AS ESTAÇÕES PODEM COMPARTILHAR DADOS E PERIFÉRICOS UMAS COM AS OUTRAS
- BAIXO CUSTO
- ALTA VELOCIDADE
- FÁCIL CONFIGURAÇÃO

OBS: NÃO HÁ HIERARQUIA, NEM GERENCIAMENTO DE USUÁRIO. TODAS PODEM SER CLIENTES. TODAS PODEM SER SERVIDORES.

@mapasdathai

Tipos de Rede

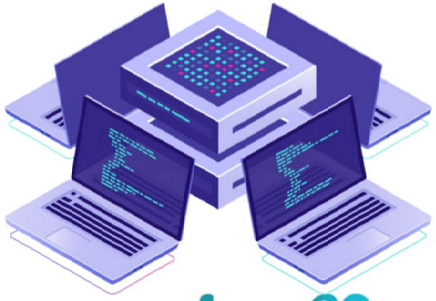
Por Topologia/Layout

BARRAMENTO (BUS)

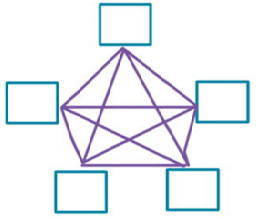
- TODAS AS ESTAÇÕES SÃO LIGADAS A UM MESMO MEIO DE TRANSMISSÃO (BACKBONES)
- CONEXÃO PONTO-MULTIPONTO
- HALF-DUPLEX (SINAL EM AMBAS AS DIREÇÕES)
- BROADCAST (SINAL RECEBIDO POR TODOS OS NÓS)

→ VANTAGENS:
- FÁCIL E BARATO

→ DESVANTAGENS:
- AUMENTO DO ATRASO
- FALHA NO BACKBONE INTERROMPE A TRANSMISSÃO PARA TODOS OS NÓS (COMO NUM VARAL DE ROUPAS)



MALHA (MESH)

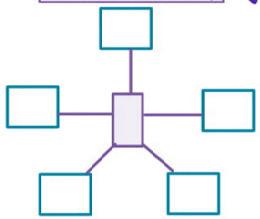


- TODAS AS ESTAÇÕES ESTÃO LIGADAS ENTRE SI
- LINKS PONTO-A-PONTO, DEDICADOS E COM TRANSMISSÃO FULL-DUPLEX

→ VANTAGENS:
- MAIS CONFIÁVEL POR SER MAIS REDUNDANTE
- A RUPTURA DE UM LINK NÃO PREJUDICA A REDE INTEIRA, MAS SÓ O NÓ QUE ESTAVA POR ELE CONECTADO

→ DESVANTAGENS:
- NÃO SERVE P/ REDES GRANDES
- A REDUNDÂNCIA A TORNA CARA

ESTRELA (STAR)

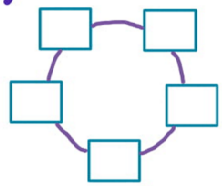


- AS ESTAÇÕES ESTÃO LIGADAS POR UMA CONEXÃO PONTO-A-PONTO A UM NÓ CENTRAL CONTROLADOR, PELO QUAL PASSAM TODAS AS INFORMAÇÕES
- NÃO HÁ TRAFEGO DIRETO ENTRE ESTAÇÕES

→ VANTAGENS:
- FÁCIL ADICIONAR ESTAÇÕES E IDENTIFICAR/ISOLAR FALHAS
- SE UMA CONEXÃO SE ROMPER, NÃO AFETA AS DEMAIS

→ DESVANTAGENS:
- SE O DISPOSITIVO CENTRAL FALHAR, TODA A REDE SERÁ AFETADA

ANEL (RING)



- CADA ESTAÇÃO TEM UMA CONEXÃO PONTO-A-PONTO COM OUTRAS DUAS, CONECTADAS LADO A LADO
- SINAL SIMPLEX
- O SINAL É REGENERADO E RETRANSMITIDO A CADA NÓ

→ VANTAGENS:
- FÁCIL DE INSTALAR E RECONFIGURAR
- ISOLAMENTO DE FALHAS SIMPLIFICADO

→ DESVANTAGENS:
- TRÁFEGO UNIDIRECIONAL
- LIMITAÇÃO DO TAMANHO → QUANTO MAIOR, PIOR O DESEMPENHO
- UMA INTERRUPÇÃO NO ANEL PODE DERRUBAR TODA A REDE → COMO NAS LUZES DE NATAL

@mapasdathai

Equipamentos de Redes

NIC (PLACA DE REDE)

- RECURSO DE HARDWARE MÍNIMO PARA SE OBTER UMA COMUNICAÇÃO BIDIRECIONAL.
- POSSUI UM IDENTIFICADOR CHAMADO DE ENDEREÇO MAC (MEDIUM ACCESS CONTROL)
  - ↳ 48 BITS
  - ↳ HEXADECIMAL
  - ↳ SEPARADOS POR DOIS PONTOS

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

HUB (CONCENTRADOR)

CONCENTRA O TRÁFEGO DE REDE QUE PROVÉM DE VÁRIOS DISPOSITIVOS

REGENERA O SINAL E DEPOIS ENVIA PARA TODAS AS PORTAS

BROADCAST (PODEQUEIRO)

HALF-DUPLEX

TOPOLOGIA FÍSICA: ESTRELA

TOPOLOGIA LÓGICA: BARRAMENTO

ACCESS POINT (PONTO DE ACESSO)

- OFERECE ACESSO SEM FIO A UMA REDE CABEADA
- ESTENDE A COBERTURA DE UMA REDE SEM FIO
- REPETIDOR DE SINAL WIRELESS
- NÃO DISPENSA O USO DE UM ROTEADOR

@mapasdathai

BRIDGE MULTIPORTAS

SWITCH (COMUTADOR)

- CONECTA COMPUTADORES À REDE OU CONECTA SEGMENTOS DE UMA REDE
- UNICAST OU MULTICAST (LEAL)
- FULL-DUPLEX
- TOPOLOGIA FÍSICA: ESTRELA
- TOPOLOGIA LÓGICA: ESTRELA
- TEM MAIS PORTAS QUE UM HUB OU UMA PONTE

BRIDGE (PONTE)

- CONECTA SEGMENTOS DE REDES DIFERENTES QUE FORAM DIVIDIDAS PARA REDUZIR O TRÁFEGO
- GERALMENTE SÓ POSSUI 2 PORTAS, LOGO SÓ PODE SEPARAR A REDE EM 2 SEGMENTOS
- É CAPAZ DE ENVIAR DADOS EM UNICAST

MODEM (MODULADOR/DEMODULADOR)

É O INTÉRPRETE QUE PERMITE A TRANSMISSÃO DE DADOS DIGITAIS POR UM MEIO QUE SÓ ENTENDE SINAL ANALÓGICO (A LINHA TELEFÔNICA)

MODEM DIAL-UP – ACESSO DISCADO

MODEM ADSL – ACESSO A BANDA LARGA POR CABO OU WIRELESS

CABLE MODEM – CABOS COAXIAIS / NÃO USA A LINHA TELEFÔNICA

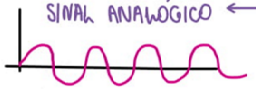
ROUTER (ROTEADOR)

- CONECTA VÁRIAS REDES DIFERENTES
- ESCOLHE A MELHOR ROTA P/ QUE A INFORMAÇÃO CHEGUE AO DESTINO
- EX: CONECTAR A LAN DOMÉSTICA À WAN

ATENÇÃO! ROTEADORES CONECTAM REDES DIFERENTES, SWITCHES SEGMENTAM UMA MESMA REDE

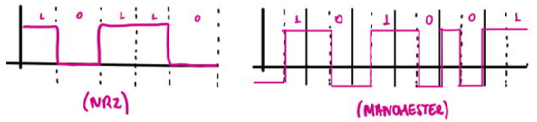
TIPOS DE SINAIS

SINAL ANALÓGICO



- NÚMERO INFINITO DE VALORES
- MAIS NÍVEIS DE INTENSIDADE

SINAL DIGITAL

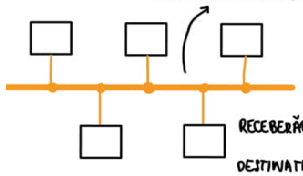


- NÚMERO LIMITADO DE VALORES
- 0 OU 1 (BITS)
- COMPUTADORES SÓ ENTENDEM BITS

Padrões de Redes

Ethernet

PERMITE QUE 2 OU MAIS COMPUTADORES SE CONECTEM POR UMA LAN CABEADA

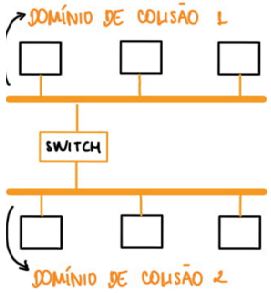


CSMA - CARRIER SYSTEM MULTIPLE ACCESS: TODOS OS COMPUTADORES RECEBERÃO A MENSAGEM, MAS SÓ O DESTINATÁRIO IRÁ PROCESSÁ-LA.

DESVANTAGEM: TRÁFEGO ALTO PODE GERAR COLISÃO = MENSAGENS ININTELIGÍVEIS

SOLUÇÃO: ESPERAR EM SILÊNCIO DURANTE UM PERÍODO DE TEMPO ALEATÓRIO ANTES DE TENTAR NOVAMENTE

QUANDO A REDE É MUITO GRANDE:



DOMÍNIO DE COLISÃO: É UMA SEGMENTAÇÃO DA REDE. DIMINUI A QUANTIDADE DE DISPOSITIVOS NOS MEIOS DE TRANSMISSÃO COMPARTILHADOS PARA DIMINUIR A PROBABILIDADE DE COLISÕES.

EVOLUÇÃO DOS PADRÕES ETHERNET		
CABO COAXIAL	ETHERNET	10 BASE-2 / 10Mbs / 185 m
	ETHERNET	10 BASE-5 / 10Mbs / 500 m
CABO PAR TRANÇADO	ETHERNET	10 BASE-T / 10 Mbs
	FAST ETHERNET	100 BASE-T / 100 Mbs
	GIGABIT ETHERNET	1000 BASE-T / 1000 Mbs
	10G ETHERNET	10 G BASE-T / 10.000 Mbs

Wireless

- SUA CONEXÃO UTILIZA ONDAS DE RÁDIO

EVOLUÇÃO DO PADRÃO WIRELESS		
PADRÃO	FREQUÊNCIA	TAXA DE TRANSMISSÃO
IEEE 802.11B	2.4 GHz	11 Mbs
IEEE 802.11A	5.0 GHz	54 Mbs
IEEE 802.11G	2.4 GHz	54 Mbs
IEEE 802.11N	2.4 ou 5.0 GHz	150, 300 até 600 Mbs
IEEE 802.11AC	5.0 GHz	500Mbs, 1Gbs ou +

OBSERVAÇÕES:

- 802.11B e 802.11A NÃO SÃO EVOLUÇÃO UM DO OUTRO, ELES SURGIRAM SIMULTANEAMENTE
- O 802.11B ENTROU NO MERCADO PRIMEIRO
- O 802.11N É DUAL-BAND (PERMITE DUAS BANDAS DE FREQUÊNCIA

Wi Fi

- BASEADA NO PADRÃO WIRELESS 802.11
- CONEXÃO POR PONTOS DE ACESSO (HOT SPOT)
- P/ TER ACESSO, O DISPOSITIVO DEVE POSSUIR A TECNOLOGIA WI-FI INTEGRADA

IEEE 802.3	Ethernet (LAN)
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)

Bluetooth

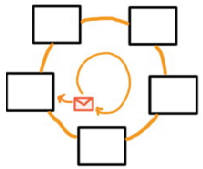
OBJETIVO: INTEGRAR EQUIPAMENTOS PERIFÉRICOS NA WPAN

- REDE DE BAIXO CUSTO
- CURTO ALCANCE
- BAIXAS TAXAS DE TRANSMISSÃO
- FAIXA DE 2.4 GHz
- CONECTA ATÉ 7 DISPOSITIVOS
- ARQUITETURA MASTER / SLAVE
  - MESTRE: PODE SE CONECTAR A VÁRIOS ESCRAVOS
  - ESCRAVO: SE CONECTA A APENAS UM MESTRE

WiMAX

- PADRÃO SEM FIO DE ALTA VELOCIDADE PARA REDES METROPOLITANAS (WMAN)
- CRIADO P/ OFERECER INTEROPERABILIDADE ENTRE OS EQUIPAMENTOS
- RAIO DE ATÉ 40 KM
- OPERA NO ESPECTRO DE FREQUÊNCIA 2,4 GHz, 3,5 GHz E 10,5 GHz
- NECESSÁRIO CONCESSÃO DA ANATEL
- POSSUI 3 ESQUEMAS DE MODULAÇÃO: QAM - 64, QAM - 16 E QPSK

Token Ring



- PADRÃO CABEADO QUE ERA CONCORRENTE DO PADRÃO ETHERNET
- TOPOLOGIA EM ANEL / COMUNICAÇÃO SIMPLEX
- ARQUITETURA PONTO-A-PONTO
- NÃO TEM COLISÃO

@mapasdathai

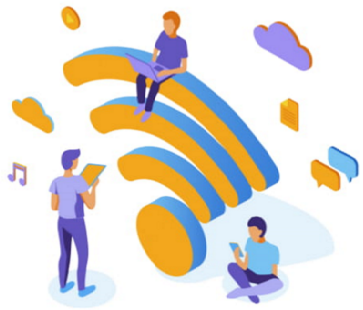
Internet

Arpanet

- REDE DE CONTROLE DE COMANDO CRIADA P/ FINS MILITARES E FINANCIADA PELA ARPA (ADVANCED RESEARCH PROJECTS AGENCY).
- PRIMEIRA GRANDE INOVAÇÃO: COMUTAÇÃO POR PACOTES.

World Wide Web (WWW)

- SERVIÇO DE VISUALIZAÇÃO DE PÁGINAS WEB ORGANIZADAS EM SITES COM INFORMAÇÃO ONLINE EM HIPERMÍDIA.
- ACESSO VIA NAVEGADOR
- PROTOCOLOS: EM GERAL, HTTP E HTTPS



Correio Eletrônico

- SERVIÇO DE COMPOSIÇÃO, ENVIO E RECEBIMENTO DE MENSAGENS ELETRÔNICAS ENTRE PARTES.
- PROTOCOLOS: EM GERAL, POP3, IMAP E SMTP

Acesso Remoto

- PERMITE QUE USUÁRIOS SE CONECTEM A OUTROS COMPUTADORES, MESMO QUE ELES ESTEJAM EM LOCALIDADES DISTANTES NO MUNDO.
- PROTOCOLOS: EM GERAL, SSH E TELNET

Comutação por circuito

- UTILIZADA NA TELEFONIA
- A INFORMAÇÃO DE VOZ SEMPRE PERCORRE A MESMA ROTA E SEMPRE CHEGA NA MESMA ORDEM
- FASES:
  1. ESTABELECIMENTO DA CONEXÃO
  2. TRANSFERÊNCIA DE DADOS
  3. ENCERRAMENTO DA CONEXÃO
- É INVIÁVEL P/ A INTERNET PORQUE DESPERDIÇARIA RECURSOS POR FECHAR UMA CONEXÃO DEDICADA AINDA QUE NÃO ESTEJA HAVENDO COMUNICAÇÃO E PORQUE SÓ SERIA POSSÍVEL ACESSAR UM SITE POR VEZ.

Comutação por pacotes

- HÁ UMA MALHA DE NÓS PONTO-A-PONTO EM QUE CADA NÓ VERIFICA A ROTA DE MENOR CUSTO (+ RÁPIDA) P/ A ENTREGA DA INFORMAÇÃO
- DIVIDE AS INFORMAÇÕES EM PEQUENOS PEDAÇOS (PACOTES)
- OS PACOTES SÃO ENVIADOS SEPARADAMENTE E PODEM PERCORRER ROTAS DIFERENTES E CHEGAR NO DESTINO FORA DE ORDEM
- QUANDO TODOS OS PACOTES CHEGAM, A INFORMAÇÃO É REORGANIZADA
- UTILIZA TRANSMISSÃO STORE-AND-FOWARD

Protocolos TCP/IP

- MUITAS REDES COMO A ARPANET COMEÇARAM A SURGIR, MAS CADA UMA FORMATAVA SEUS PACOTES A SEU MODO, CAUSANDO PROBLEMAS DE COMUNICAÇÃO.

SOLUÇÃO: CRIAR UM CONJUNTO DE PROTOCOLOS COMUNS DE COMUNICAÇÃO CHAMADO TCP/IP.

Transferência de Arquivos

TORNA ARQUIVOS DISPONÍVEIS PARA OUTROS USUÁRIOS POR MEIO DE DOWNLOADS E DE UPLOADS.

PROTOCOLOS: EM GERAL: FTP E P2P

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.